

NSX 관리 가이드

업데이트 12

수정 날짜: 2020년 7월 09일

VMware NSX Data Center for vSphere 6.3



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2010 - 2020 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

NSX 관리 가이드 13

1 NSX의 시스템 요구 사항 14

2 NSX에 필요한 포트 및 프로토콜 17

3 NSX 개요 20

NSX 구성 요소 21

데이터부 22

제어부 23

관리부 24

소비 플랫폼 24

NSX Edge 24

NSX Services 27

4 크로스 vCenter Networking & Security 개요 29

크로스 vCenter NSX의 이점 29

크로스 vCenter NSX의 작동 방식 30

크로스 vCenter NSX의 NSX Services 지원 매트릭스 31

범용 컨트롤러 클러스터 32

범용 전송 영역 33

범용 논리적 스위치 33

범용 논리적 (분산) 라우터 33

범용 방화벽 규칙 34

범용 네트워크 및 보안 개체 34

크로스 vCenter NSX 토폴로지 35

다중 사이트 및 단일 사이트 크로스 vCenter NSX 35

로컬 송신 37

NSX Manager 역할 수정 38

5 전송 영역 40

전송 영역 추가 42

전송 영역 보기 및 편집 44

전송 영역 확장 44

전송 영역 축소 45

CDL(Controller Disconnected Operation) 모드 45

CDL(Controller Disconnected Operation) 모드 사용	46
CDL(Controller Disconnected Operation) 모드 사용 안 함	46

6 논리적 스위치 48

논리적 스위치 추가	50
논리적 스위치 추가	51
논리적 스위치를 NSX Edge에 연결	53
논리적 스위치에서 서비스 배포	53
논리적 스위치에 가상 시스템 연결	54
논리적 스위치 연결 테스트	54
논리적 스위치에서 스푸핑 방지	55
논리적 스위치 편집	55
논리적 스위치 시나리오	55
관리자 John이 NSX Manager에 세그먼트 ID 풀 및 멀티캐스트 주소 범위 할당	58
관리자 John이 VXLAN 전송 매개 변수 구성	59
관리자 John이 전송 영역 추가	60
관리자 John이 논리적 스위치 생성	60

7 하드웨어 게이트웨이 구성 61

시나리오: 하드웨어 게이트웨이 샘플 구성	62
복제 클러스터 설정	64
하드웨어 게이트웨이를 NSX Controller에 연결	65
하드웨어 게이트웨이 인증서 추가	65
논리적 스위치를 물리적 스위치에 바인딩	67

8 L2 브리지 69

L2 브리지 추가	70
논리적으로 라우팅된 환경에 L2 브리지 추가	71

9 라우팅 73

논리적(분산) 라우터 추가	73
Edge Services Gateway 추가	86
글로벌 구성 지정	96
NSX Edge 구성	98
인증서 사용	98
FIPS 모드	103
장치 관리	105
NSX Edge 장치 리소스 예약 관리	107
인터페이스 사용	109
하위 인터페이스 추가	112

자동 규칙 구성 변경	115
CLI 자격 증명 변경	115
고가용성 정보	115
NSX Edge를 NSX Manager와 강제 동기화	118
NSX Edge에 대한 Syslog 서버 구성	118
NSX Edge의 상태 보기	119
NSX Edge 다시 배포	119
NSX Edge에 대한 기술 지원 로그 다운로드	121
정적 경로 추가	121
논리적 (분산) 라우터에서 OSPF 구성	123
Edge Services Gateway에서 OSPF 구성	128
BGP 구성	133
경로 재배포 구성	138
NSX Manager 로케일 ID 보기	139
범용 논리적(분산) 라우터에서 로케일 ID 구성	139
호스트 또는 클러스터에서 로케일 ID 구성	140

10 논리적 방화벽 142

분산 방화벽	142
세션 타이머	144
가상 시스템에 대한 IP 검색	147
방화벽 보호 대상에서 가상 시스템 제외	148
방화벽 CPU 및 메모리 임계값 이벤트 보기	149
분산 방화벽 리소스 활용도	149
Edge 방화벽	150
NSX Edge 방화벽 규칙 사용	151
방화벽 규칙 섹션 사용	160
방화벽 규칙 섹션 추가	160
방화벽 규칙 섹션 병합	161
방화벽 규칙 섹션 삭제	161
방화벽 규칙 사용	162
기본 분산 방화벽 규칙 편집	163
분산 방화벽 규칙 추가	163
분산 방화벽 규칙 강제 동기화	169
범용 방화벽 규칙 추가	169
사용자 지정 계층 3 프로토콜을 사용하는 방화벽 규칙	173
게시되지 않은 구성 저장	174
저장된 방화벽 구성 로드	174
방화벽 규칙 필터링	175

방화벽 규칙 순서 변경	175
방화벽 규칙 삭제	176
Firewall 로그	176
11 ID 방화벽 개요	181
ID 방화벽 워크플로	182
12 Active Directory 도메인 사용	183
NSX Manager에 Windows 도메인 등록	183
Windows 도메인을 Active Directory와 동기화	185
Windows 도메인 편집	186
Windows 2008에서 보안 읽기 전용 로그 액세스 사용	186
디렉토리 권한 확인	187
13 SpoofGuard 사용	189
SpoofGuard 정책 생성	190
IP 주소 승인	191
IP 주소 편집	191
IP 주소 지우기	192
14 VPN(Virtual Private Network)	193
SSL VPN-Plus 개요	193
네트워크 액세스 SSL VPN-Plus 구성	195
SSL VPN-Plus Client 설치	205
SSL VPN-Plus Client에서 프록시 서버 설정 구성	208
SSL VPN-Plus 로그	209
클라이언트 구성 편집	209
일반 설정 편집	210
웹 포털 디자인 편집	211
SSL VPN에 대한 IP 풀 사용	211
전용 네트워크 사용	212
설치 패키지 사용	214
사용자 사용	215
로그인 및 로그오프 스크립트 사용	216
IPSec VPN 개요	217
IPSec VPN 서비스 구성	218
IPSec VPN 서비스 편집	223
IPSec VPN 사이트 사용 안 함	223
IPSec VPN 사이트 삭제	224
IPSec VPN 구성 예	224

L2 VPN 개요	235
L2 VPN 구성	236
L2 VPN 서버 구성	242
피어 사이트 추가	243
서버에서 L2 VPN 서비스 사용	244
L2 VPN 클라이언트 구성	245
클라이언트에서 L2 VPN 서비스 사용	246
독립형 Edge를 L2 VPN 클라이언트로 구성	247
L2 VPN 통계 보기	249
확장된 VLAN 제거	249

15 논리적 로드 밸런서 251

로드 밸런싱 설정	255
로드 밸런서 서비스 구성	257
서비스 모니터 생성	258
서버 풀 추가	264
애플리케이션 프로파일 생성	266
애플리케이션 규칙 추가	270
가상 서버 추가	277
애플리케이션 프로파일 관리	278
애플리케이션 프로파일 편집	278
로드 밸런서에 대한 SSL 종료 구성	279
애플리케이션 프로파일 삭제	280
서비스 모니터 관리	280
서비스 모니터 편집	281
서비스 모니터 삭제	281
서버 풀 관리	281
서버 풀 편집	281
투명 모드를 사용하도록 로드 밸런서 구성	282
서버 풀 삭제	283
풀 통계 표시	283
가상 서버 관리	283
가상 서버 편집	284
가상 서버 삭제	284
애플리케이션 규칙 관리	284
애플리케이션 규칙 편집	284
애플리케이션 규칙 삭제	285
NTLM 인증을 사용하는 로드 밸런스 웹 서버	285
로드 밸런서 HTTP 연결 모드	285

NSX 로드 밸런서 구성 시나리오	287
단일 암 로드 밸런서 구성	288
시나리오: Platform Services Controller에 대한 NSX 로드 밸런서 구성	293
시나리오: SSL 오프로딩	296
시나리오: SSL 인증서 가져오기	301
시나리오: SSL 패스스루	303
시나리오: SSL 클라이언트 및 서버 인증	305

16 기타 Edge 서비스 307

DHCP 서비스 관리	307
DHCP IP 풀 추가	307
DHCP 서비스 사용	309
DHCP IP 풀 편집	310
DHCP 정적 바인딩 추가	310
DHCP 바인딩 편집	311
DHCP 릴레이 구성	312
DHCP 릴레이 서버 추가	313
릴레이 에이전트 추가	314
DNS 서버 구성	314

17 Service Composer 316

Service Composer 사용	318
Service Composer에서 보안 그룹 생성	319
보안 정책 생성	321
보안 그룹에 보안 정책 적용	326
Service Composer 캔버스	326
보안 태그 사용	329
고유한 ID 선택	329
적용된 보안 태그 보기	330
보안 태그 생성	330
보안 태그 할당	331
보안 태그 편집	331
보안 태그 삭제	332
유효한 서비스 보기	332
보안 정책에 유효한 서비스 보기	332
보안 정책의 서비스 오류 확인	333
가상 시스템에 유효한 서비스 보기	333
보안 정책 사용	333
보안 정책 우선 순위 관리	333
보안 정책 편집	334

보안 정책 삭제	334
Service Composer 시나리오	335
감염된 시스템 차단 시나리오	335
보안 구성 백업	339
보안 정책 구성 가져오기 및 내보내기	341
보안 정책 구성 내보내기	341
보안 정책 구성 가져오기	342

18 Guest Introspection 343

호스트 클러스터에 Guest Introspection 설치	344
Windows 가상 시스템에서 Guest Introspection Thin Agent 설치	346
Linux 가상 시스템에서 Guest Introspection Thin Agent 설치	347
Guest Introspection 상태 보기	349
Guest Introspection 감사 메시지	349
Guest Introspection 문제 해결 데이터 수집	350
Guest Introspection 모듈 제거	350
Linux용 Guest Introspection 제거	351

19 네트워크 확장성 352

분산 서비스 삽입	353
Edge 기반 서비스 삽입	353
타사 서비스 통합	353
파트너 서비스 배포	354
Service Composer를 통한 벤더 서비스 이용	355
논리적 방화벽을 통해 벤더 솔루션으로 트래픽 리디렉션	355
파트너 로드 밸런서 이용	356
타사 통합 제거	357

20 사용자 관리 358

NSX 사용자 및 기능별 사용 권한	358
Single Sign On 구성	362
사용자 권한 관리	364
기본 사용자 계정 관리	365
vCenter 사용자에게 역할 할당	365
CLI를 사용하여 웹 인터페이스 액세스 권한이 있는 사용자 생성	368
사용자 계정 편집	370
사용자 역할 변경	371
사용자 계정 사용 또는 사용 안 함	371
사용자 계정 삭제	372

21	네트워크 및 보안 개체	373
	IP 주소 그룹 사용	373
	IP 주소 그룹 생성	373
	IP 주소 그룹 편집	374
	IP 주소 그룹 삭제	375
	MAC 주소 그룹 사용	375
	MAC 주소 그룹 생성	375
	MAC 주소 그룹 편집	376
	MAC 주소 그룹 삭제	376
	IP 풀 사용	376
	IP 풀 생성	376
	IP 풀 편집	377
	IP 풀 삭제	377
	보안 그룹 사용	377
	보안 그룹 생성	378
	보안 그룹 편집	381
	보안 그룹 삭제	381
	서비스 및 서비스 그룹 사용	381
	서비스 생성	381
	서비스 그룹 생성	382
	서비스 또는 서비스 그룹 편집	383
	서비스 또는 서비스 그룹 삭제	383
22	작업 및 관리	384
	NSX 대시보드 사용	384
	통신 채널 상태 확인	388
	NSX Controller	389
	컨트롤러 암호 변경	389
	NSX Controller용 기술 지원 로그 다운로드	390
	NSX Controller용 Syslog 서버 구성	390
	VXLAN 포트 변경	391
	고객 환경 향상 프로그램	393
	고객 환경 향상 프로그램 옵션 편집	393
	NSX 로그 정보	394
	감사 로그	395
	NSX 티켓 로거 사용	395
	감사 로그 보기	396
	시스템 이벤트	396
	시스템 이벤트 보고서 보기	396

시스템 이벤트 형식	396
경보	397
경보 형식	398
SNMP 트랩 사용	398
관리 시스템 설정	402
NSX Manager 가상 장치에 로그인	402
NSX Manager 날짜 및 시간 편집	403
NSX Manager에 대한 Syslog 서버 구성	403
NSX Manager에서 FIPS 모드 및 TLS 설정 변경	404
DNS 서버 편집	405
Lookup Service 세부 정보 편집	406
vCenter Server 편집	406
NSX용 기술 지원 로그 다운로드	406
NSX Manager SSL 인증	407
NSX 백업 및 복원	410
NSX Manager 백업 및 복원	411
vSphere Distributed Switch 백업	417
vCenter 백업	417
Flow Monitoring	417
Flow Monitoring 데이터 보기	418
Flow Monitoring 차트의 날짜 범위 변경	420
Flow Monitoring 보고서에서 방화벽 규칙 추가 또는 편집	420
라이브 흐름 보기	421
Flow Monitoring 데이터 수집 구성	422
IPFIX 구성	424
애플리케이션 규칙 관리자	435
모니터링 세션 생성	436
흐름 분석	437
흐름 통합 및 사용자 지정	438
흐름 레코드에서 서비스 사용자 지정	439
흐름 레코드에서 소스 및 대상 사용자 지정	440
애플리케이션 규칙 관리자에서 방화벽 규칙 생성	441
애플리케이션 규칙 관리자에서 방화벽 규칙 게시 및 관리	443
Activity Monitoring	444
Activity Monitoring 설정	445
Activity Monitoring 시나리오	449
데이터 수집 사용	451
가상 시스템 작업 보고서 보기	452
인바운드 작업 보기	453

아웃바운드 작업 보기	455
인벤토리 컨테이너 간 상호 작용 보기	456
아웃바운드 AD 그룹 작업 보기	458
데이터 수집 재정의	459
끝점 모니터링 데이터 수집	459
끝점 모니터링	460
Traceflow	462
Traceflow 정보	462
Traceflow를 사용하여 문제 해결	464

NSX 관리 가이드

NSX 관리 가이드에서는 "" NSX Manager 사용자 인터페이스 및 vSphere Web Client를 사용하여 VMware NSX[®] for vSphere[®] 시스템을 구성, 모니터링 및 유지 보수하는 방법을 설명합니다. 또한 단계별 구성 지침 및 권장 모범 사례에 대한 정보도 수록되어 있습니다.

대상 사용자

이 설명서는 VMware vCenter 환경에서 NSX를 설치하거나 사용하려는 모든 사용자를 대상으로 합니다. 이 설명서의 정보는 가상 시스템 기술 및 가상 데이터 센터 작업에 익숙한 숙련된 시스템 관리자를 대상으로 작성되었으며, 이 설명서에서는 VMware ESXi, vCenter Server 및 vSphere Web Client를 포함하는 VMware vSphere에 익숙하다고 가정합니다.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에 사용된 용어에 대한 정의를 보려면 <http://www.vmware.com/support/pubs>를 참조하십시오.

NSX의 시스템 요구 사항

1

NSX를 설치하거나 업그레이드하기 전에 네트워크 구성 및 리소스를 고려합니다. vCenter Server별로 NSX Manager 하나, ESXi™ 호스트별로 Guest Introspection 인스턴스를 하나 설치하고 데이터센터별로 NSX Edge 인스턴스를 여러 개 설치할 수 있습니다.

하드웨어

이 표에는 NSX 장치에 대한 하드웨어 요구 사항이 설명되어 있습니다.

표 1-1. 장치에 대한 하드웨어 요구 사항

장치	메모리	vCPU	디스크 용량
NSX Manager	16GB(더 큰 NSX 배포의 경우 24GB)	4(더 큰 NSX 배포의 경우 8)	60 GB
NSX Controller	4GB	4	28 GB
NSX Edge	소형: 512MB 중형: 1GB 대형: 2GB 초대형: 8GB	소형: 1 중형: 2 대형: 4 초대형: 6	소형, 중형: 584MB 디스크 1개 + 512MB 디스크 1개 대형: 584MB 디스크 1개 + 512MB 디스크 2개 초대형: 584 MB 디스크 1개 + 2 GB 디스크 1개 + 512 MB 디스크 1개
Guest Introspection	2 GB	2	5GB(프로비저닝된 공간: 6.26GB)

일반적인 지침에 따라 NSX 관리 환경에 256개가 넘는 하이퍼바이저 또는 2000개가 넘는 VM이 포함되어 있는 경우 NSX Manager 리소스를 vCPU 8개 및 24GB RAM으로 늘립니다.

특정 크기 조정 세부 정보는 VMware 지원팀에 문의하십시오.

가상 장치에 대한 메모리 및 vCPU 할당을 늘리는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리"에서 메모리 리소스 할당 및 가상 CPU의 수 변경을 참조하십시오.

Guest Introspection 장치에 대한 프로비저닝된 공간은 Guest Introspection에 대해 6.26GB로 표시됩니다. 이는 클러스터의 여러 호스트가 스토리지를 공유할 때 vSphere ESX Agent Manager가 빠른 복제를 생성하기 위해 서비스 VM의 스냅샷을 생성하기 때문입니다. ESX Agent Manager를 통해 이 옵션을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 *ESX Agent Manager* 설명서를 참조하십시오.

네트워크 지연 시간

구성 요소 간 네트워크 지연 시간이 설명된 최대 지연 시간 이하인지 확인해야 합니다.

표 1-2. 구성 요소 간 최대 네트워크 지연 시간

구성 요소	최대 지연 시간
NSX Manager 및 NSX Controller	150ms RTT
NSX Manager 및 ESXi 호스트	150ms RTT
NSX Manager 및 vCenter Server 시스템	150ms RTT
NSX Manager 및 크로스 vCenter NSX 환경의 NSX Manager	150ms RTT
NSX Controller 및 ESXi 호스트	150ms RTT

소프트웨어

최신 상호 운용성 정보는 제품 상호 운용성 매트릭스(http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)를 참조하십시오.

NSX, vCenter Server 및 ESXi의 권장 버전에 대해서는 업그레이드하려는 NSX 버전에 대한 릴리스 정보를 참조하십시오. 릴리스 정보는 다음 NSX for vSphere 설명서 사이트에서 확인할 수 있습니다. <https://docs.vmware.com/kr/VMware-NSX-for-vSphere/index.html>

NSX Manager가 크로스 vCenter NSX 배포에 참여하려면 다음과 같은 조건이 필요합니다.

구성 요소	버전
NSX Manager	6.2 이상
NSX Controller	6.2 이상
vCenter Server	6.0 이상
ESXi	<ul style="list-style-type: none"> ■ ESXi 6.0 이상 ■ NSX 6.2 이상 VIB를 사용하여 준비된 호스트 클러스터

크로스 vCenter NSX 배포 환경에서 단일 vSphere Web Client를 통해 모든 NSX Manager를 관리하려면 고급 연결 모드에서 vCenter Server를 연결해야 합니다. vCenter Server 및 호스트 관리에서 "" 고급 연결 모드 사용을 참조하십시오.

NSX와의 파트너 솔루션 호환성을 확인하려면 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>에서 네트워킹 및 보안에 대한 VMware 호환성 가이드를 참조하십시오.

클라이언트 및 사용자 액세스

다음 항목은 **NSX** 환경을 관리하는 데 필요합니다.

- 정방향 및 역방향 이름 확인. **ESXi** 호스트를 이름으로 **vSphere** 인벤토리에 추가한 경우에 필요합니다. 그렇지 않은 경우 **NSX Manager**는 IP 주소를 확인할 수 없습니다.
- 가상 시스템을 추가하고 가상 시스템의 전원을 켤 수 있는 권한이 필요합니다.
- 가상 시스템 파일을 저장하는 데이터스토어에 대한 액세스 권한과 해당 데이터스토어에 파일을 복사할 계정 사용 권한이 있어야 합니다.
- **NSX Manager** 사용자 인터페이스에 액세스할 수 있도록 웹 브라우저에서 쿠키를 사용하도록 설정해야 합니다.
- 포트 443은 **NSX Manager**와 **ESXi** 호스트, **vCenter Server** 및 배포할 **NSX** 장치 간에 열려 있어야 합니다. 이 포트는 배포할 **OVF** 파일을 **ESXi** 호스트에 다운로드하는 데 필요합니다.
- 사용 중인 **vSphere Web Client** 버전에서 지원되는 웹 브라우저. 자세한 내용은 "**vCenter Server** 및 호스트 관리" 설명서에서 **vSphere Web Client** 사용을 참조하십시오.

NSX에 필요한 포트 및 프로토콜

2

NSX가 올바르게 작동하려면 다음 포트가 열려 있어야 합니다.

참고 크로스 vCenter NSX 환경 및 vCenter Server 시스템이 고급 연결 모드인 경우, vCenter Server 시스템에서 NSX Manager를 관리하려면 각 NSX Manager 장치가 환경의 각 vCenter Server 시스템과 필요로 하는 연결이 되어 있어야 합니다.

표 2-1. NSX for vSphere에 필요한 포트 및 프로토콜

소스	대상	포트	프로토콜	용도	민감도	TLS	인증
클라이언트 PC	NSX Manager	443	TCP	NSX Manager 관리 인터페이스	아니요	예	PAM 인증
클라이언트 PC	NSX Manager	443	TCP	NSX Manager VIB 액세스	아니요	아니요	PAM 인증
ESXi 호스트	vCenter Server	443	TCP	ESXi 호스트 준비	아니요	아니요	
vCenter Server	ESXi 호스트	443	TCP	ESXi 호스트 준비	아니요	아니요	
ESXi 호스트	NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
ESXi 호스트	NSX Controller	1234	TCP	사용자 월드 에이전트 연결	아니요	예	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	컨트롤러 클러스터 - 상태 동기화	아니요	예	IPsec
NSX Controller	NSX Controller	7777	TCP	컨트롤러 간 RPC 포트	아니요	예	IPsec
NSX Controller	NSX Controller	30865	TCP	컨트롤러 클러스터 - 상태 동기화	아니요	예	IPsec
NSX Manager	NSX Controller	443	TCP	컨트롤러와 Manager 간 통신	아니요	예	사용자/암호
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	아니요	예	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	아니요	예	
NSX Manager	ESXi 호스트	443	TCP	관리 및 프로비저닝 연결	아니요	예	

표 2-1. NSX for vSphere에 필요한 포트 및 프로토콜 (계속)

소스	대상	포트	프로토콜	용도	민감도	TLS	인증
NSX Manager	ESXi 호스트	902	TCP	관리 및 프로비저닝 연결	아니요	예	
NSX Manager	DNS 서버	53	TCP	DNS 클라이언트 연결	아니요	아니요	
NSX Manager	DNS 서버	53	UDP	DNS 클라이언트 연결	아니요	아니요	
NSX Manager	Syslog 서버	514	TCP	Syslog 연결	아니요	아니요	
NSX Manager	Syslog 서버	514	UDP	Syslog 연결	아니요	아니요	
NSX Manager	NTP 시간 서버	123	TCP	NTP 클라이언트 연결	아니요	예	
NSX Manager	NTP 시간 서버	123	UDP	NTP 클라이언트 연결	아니요	예	
vCenter Server	NSX Manager	80	TCP	호스트 준비	아니요	예	
REST 클라이언트	NSX Manager	443	TCP	NSX Manager REST API	아니요	예	사용자/암호
VTEP(VXLAN Tunnel End Point)	VTEP(VXLAN Tunnel End Point)	8472(NSX 6.2.3 이전의 기본 값) 또는 4789(NSX 6.2.3 이상 새 설치의 기본 값)	UDP	VTEP 간 전송 네트워크 캡슐화	아니요	예	
ESXi 호스트	ESXi 호스트	6999	UDP	VLAN LIF의 ARP	아니요	예	
ESXi 호스트	NSX Manager	8301, 8302	UDP	DVS 동기화	아니요	예	
NSX Manager	ESXi 호스트	8301, 8302	UDP	DVS 동기화	아니요	예	
Guest Introspection VM	NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
기본 NSX Manager	보조 NSX Manager	443	TCP	크로스 vCenter NSX 범용 동기화 서비스	아니요	예	
기본 NSX Manager	vCenter Server	443	TCP	vSphere API	아니요	예	

표 2-1. NSX for vSphere에 필요한 포트 및 프로토콜 (계속)

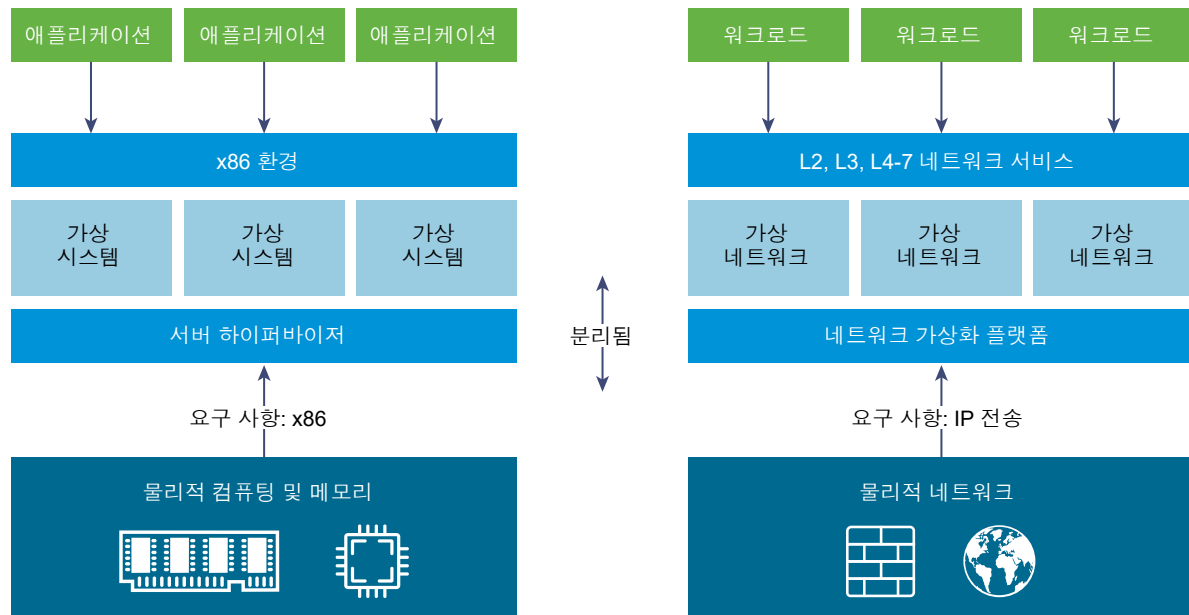
소스	대상	포트	프로토콜	용도	민감도	TLS	인증
보조 NSX Manager	vCenter Server	443	TCP	vSphere API	아니요	예	
기본 NSX Manager	NSX 범용 컨트롤러 클러스터	443	TCP	NSX Controller REST API	아니요	예	사용자/암호
보조 NSX Manager	NSX 범용 컨트롤러 클러스터	443	TCP	NSX Controller REST API	아니요	예	사용자/암호
ESXi 호스트	NSX 범용 컨트롤러 클러스터	1234	TCP	NSX 제어부 프로토콜	아니요	예	
ESXi 호스트	기본 NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
ESXi 호스트	보조 NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호

NSX 개요

3

IT 조직은 서버 가상화의 직접적인 결과로 많은 혜택을 얻고 있습니다. 서버 통합으로 물리적인 복잡도는 줄어들고, 운영 효율성 및 기본 리소스를 동적으로 용도 변경할 수 있는 기능은 증가하여 점점 더 동적인 비즈니스 애플리케이션의 요구 사항을 신속하게 최적으로 충족할 수 있습니다.

현재 VMware의 SDDC(소프트웨어 정의 데이터센터) 아키텍처는 전체 물리적 데이터센터 인프라에서 가상화 기술을 확장하고 있습니다. 네트워크 가상화 플랫폼인 VMware NSX[®]는 SDDC 아키텍처의 핵심 제품입니다. NSX를 사용한 가상화를 통해 계산 및 스토리지 부문에서 이미 구현된 뛰어난 성능을 네트워킹에서도 제공할 수 있게 되었습니다. 서버 가상화에서 소프트웨어 기반 가상 시스템(VM)을 프로그래밍 방식으로 생성, 스냅샷, 삭제 및 복원하는 것과 상당히 동일한 방법으로 NSX 네트워크 가상화에서도 소프트웨어 기반 가상 네트워크를 프로그래밍 방식으로 생성, 스냅샷, 삭제 및 복원하고 있습니다. 그 결과 데이터센터 관리자는 민첩성과 경제성 면에서 상당한 개선을 달성할 수 있을 뿐만 아니라 기본 물리적 네트워크의 운영 모델도 크게 단순화할 수 있는, 네트워킹에 대한 완전히 변화된 접근 방식이 탄생했습니다. 기존의 네트워킹 모델과 모든 벤더의 차세대 패브릭 아키텍처를 포함한 모든 IP 네트워크에서 배포할 수 있는 기능을 제공하는 NSX는 완벽한 무중단 솔루션입니다. 실제로 NSX를 사용하면 이미 구축된 물리적 네트워크 인프라에서도 소프트웨어 정의 데이터센터를 배포하기만 하면 됩니다.



위 그림에서는 계산 및 네트워크 가상화 간의 유사점을 보여줍니다. 서버 가상화를 사용하면 소프트웨어 추상화 계층(서버 하이퍼바이저)에서 x86 물리적 서버(예: CPU, RAM, 디스크, NIC)의 익숙한 특성을 재현하고 이들 특성을 임의 조합으로 프로그래밍 방식을 통해 구성할 수 있기 때문에 몇 초 만에 고유한 VM을 생성할 수 있습니다.

기능상 네트워크 하이퍼바이저에 해당하는 네트워크 가상화를 사용하면 소프트웨어에서 계층 2 - 계층 7 네트워킹 서비스(예: 스위칭, 라우팅, 액세스 제어, 방화벽 기능, QoS 및 로드 밸런싱)의 모든 기능을 재현할 수 있습니다. 따라서 이런 서비스를 프로그래밍 방식을 통해 임의 조합으로 구성함으로써 몇 초 만에 고유하고 분리된 가상 네트워크를 생성할 수 있습니다.

네트워크 가상화를 사용하면 서버 가상화와 유사한 이점을 얻을 수 있습니다. 예를 들어, VM은 기본 x86 플랫폼과 상관이 없고 VM을 통해 IT가 물리적 호스트를 계산 용량의 풀로 처리할 수 있는 것처럼, 가상 네트워크는 기본 IP 네트워크 하드웨어와 상관이 없고 가상 네트워크를 통해 IT는 물리적 네트워크를 요청 시 사용하고 용도 변경할 수 있는 전송 용량 풀로 처리할 수 있습니다. 레거시 아키텍처와 달리 기본 물리적 하드웨어 또는 토폴로지를 재구성하지 않고도 가상 네트워크를 프로그래밍 방식으로 프로비저닝, 변경, 저장, 삭제 및 복원할 수 있습니다. 널리 사용되는 서버 및 스토리지 가상화 솔루션의 기능 및 이점을 동등한 수준으로 제공하는 네트워킹에 대한 이러한 혁신적인 접근 방식은 소프트웨어 정의 데이터센터의 모든 잠재력을 발휘하게 만들 것입니다.

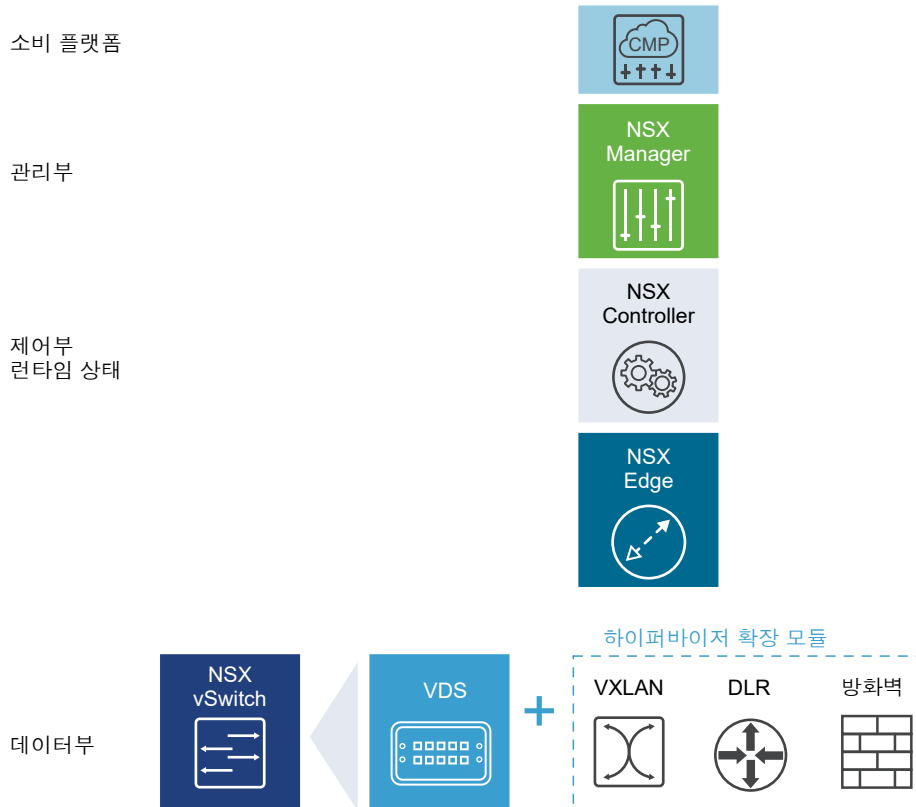
NSX는 vSphere Web Client, CLI(명령줄 인터페이스) 및 REST API를 통해 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- [NSX 구성 요소](#)
- [NSX Edge](#)
- [NSX Services](#)

NSX 구성 요소

이 섹션에서는 NSX 솔루션의 구성 요소에 대해 설명합니다.



CMP(Cloud Management Platform)는 NSX의 구성 요소가 아니지만 NSX는 REST API를 통한 거의 모든 CMP로의 통합과 VMware CMP와의 기본 통합을 제공합니다.

데이터부

NSX 데이터부는 서비스를 사용하도록 설정하는 추가 구성 요소가 포함된 VDS(vSphere Distributed Switch) 기반의 NSX vSwitch로 구성됩니다. NSX 커널 모듈, 사용자 공간 에이전트, 구성 파일 및 설치 스크립트가 VIB에 패키징되어 있고 하이퍼바이저 커널 내에서 실행됨으로써 분산 라우팅 및 논리적 방화벽 같은 서비스를 제공하고 VXLAN 브리징 기능을 사용하도록 설정합니다.

NSX vSwitch(VDS 기반)는 물리적 네트워크를 추상화하고 하이퍼바이저에서 액세스 수준에 따른 스위칭 기능을 제공합니다. 이는 VLAN 같은 물리적 구성체와 상관없이 논리적 네트워크를 사용하도록 하므로 네트워크 가상화의 중심입니다. vSwitch의 일부 이점은 다음과 같습니다.

- 프로토콜(예: VXLAN) 및 중앙 집중식 네트워크 구성을 사용하여 오버레이 네트워킹을 지원합니다. 오버레이 네트워킹을 통해 다음 기능을 제공합니다.
 - 물리적 네트워크에서 VLAN ID 사용을 줄입니다.
 - 데이터센터 네트워크를 다시 구축하지 않고도 기존 물리적 인프라의 기존 IP 네트워크에서 유연한 논리적 계층 2(L2) 오버레이를 생성할 수 있습니다.
 - 테넌트 간 분리를 유지하면서 통신(동-서/남-북)을 제공할 수 있습니다.
 - 애플리케이션 워크로드 및 가상 시스템이 오버레이 네트워크를 인지하지 않고도 물리적 L2 네트워크에 연결된 것처럼 작동합니다.

- 하이퍼바이저의 방대한 확장을 용이하게 합니다.
- 여러 기능(예: 포트 미러링, NetFlow/IPFIX, 구성 백업 및 복원, 네트워크 상태 점검, QoS 및 LACP)을 통해 가상 네트워크 내 트래픽 관리, 모니터링 및 문제 해결을 위한 종합적인 툴킷을 제공합니다.

논리적 라우터는 논리적 네트워킹 공간(VXLAN)에서 물리적 네트워크(VLAN)로 L2 브리징을 제공할 수 있습니다.

게이트웨이 디바이스는 일반적으로 NSX Edge 가상 장치입니다. NSX Edge는 L2, L3, 경계 방화벽, 로드 밸런싱 및 기타 서비스(예: SSL VPN 및 DHCP)를 제공합니다.

제어부

NSX 제어부는 NSX Controller 클러스터에서 실행됩니다. NSX Controller는 NSX 논리적 스위칭 및 라우팅 기능에 대한 제어부 기능을 제공하는 고급 분산 상태 관리 시스템입니다. 이 컨트롤러는 네트워크 내 모든 논리적 스위치에 대한 중앙 제어 지점이며 모든 호스트, 논리적 스위치(VXLAN) 및 논리적 분산 라우터에 대한 정보를 유지 관리합니다.

컨트롤러 클러스터는 하이퍼바이저에서 분산 스위칭 및 라우팅 모듈을 관리합니다. 컨트롤러를 통과하는 데이터부 트래픽은 없습니다. 컨트롤러 노드는 3개 멤버의 클러스터에 배포되어고가용성 및 확장을 사용하도록 설정합니다. 컨트롤러 노드가 실패해도 데이터부 트래픽에는 영향을 미치지 않습니다.

NSX CONTROLLER는 네트워크 정보를 호스트로 분산하는 방식으로 작동합니다. 높은 수준의 복원력을 달성할 수 있도록 NSX Controller는 스케일 아웃과 HA를 위해 클러스터링됩니다. NSX CONTROLLER를 3노드 클러스터에 배포해야 합니다. 세 개의 가상 장치는 NSX 도메인 내에서 작동하는 모든 네트워크의 상태를 제공, 유지 및 업데이트합니다. NSX Manager는 NSX Controller 노드를 배포하는 데 사용됩니다.

세 개의 NSX Controller 노드가 하나의 컨트롤러 클러스터를 구성합니다. "분할 브레인" 시나리오를 방지하려면 컨트롤러 클러스터에 쿼럼(과반수라고도 함)이 필요합니다. 분할 브레인 시나리오에서는 서로 겹치는 두 데이터 집합의 유지 보수로 인해 데이터 불일치가 발생합니다. 이러한 불일치는 실패 상태 및 데이터 동기화 문제로 인해 야기될 수 있습니다. 컨트롤러 노드를 세 개 사용할 경우 NSX Controller 노드 중 하나가 실패해도 데이터 중복성이 보장됩니다.

컨트롤러 클러스터에는 다음을 포함한 몇 가지 역할이 있습니다.

- API 제공자
- 지속성 서버
- 스위치 관리자
- 논리적 관리자
- 디렉토리 서버

각 역할에는 마스터 컨트롤러 노드가 있습니다. 특정 역할의 마스터 컨트롤러 노드가 실패하면 클러스터는 사용 가능한 NSX Controller 노드 중에서 해당 역할의 새로운 마스터를 선택합니다. 해당 역할의 새 마스터 NSX Controller 노드는 작업의 손실된 부분을 나머지 NSX Controller 노드 간에 재할당합니다.

NSX는 세 가지 논리적 스위치 제어부 모드를 지원하는데, 멀티캐스트, 유니캐스트 및 하이브리드입니다. 컨트롤러 클러스터를 사용하여 VXLAN 기반 논리적 스위치를 관리할 경우 물리적 네트워크 인프라에서 멀티캐스트를 지원할 필요가 없습니다. 멀티캐스트 그룹 IP 주소를 제공할 필요가 없고, 물리적 스위치 또는 라우터에서 PIM 라우팅 또는 IGMP 스누핑 기능을 사용하도록 설정할 필요가 없습니다. 따라서 유니캐스트 및 하이브리드 모드는 물리적 네트워크에서 NSX를 분리합니다. 유니캐스트 제어부 모드의 VXLAN은 더 이상 물리적 네트워크가 논리적 스위치 내의 BUM(브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트) 트래픽을 처리하기 위한 멀티캐스트를 지원하도록 요구하지 않습니다. 유니캐스트 모드에서는 모든 BUM 트래픽을 호스트에서 로컬로 복제하므로 물리적 네트워크 구성이 필요 없습니다. 하이브리드 모드에서는 성능 개선을 위해 일부 BUM 트래픽 복제가 첫 번째 홉 물리적 스위치로 오프로드됩니다. 하이브리드 모드에서는 첫 번째 홉 스위치에서 IGMP 스누핑과 각 VTEP 서브넷의 IGMP 쿼리 발송기에 대한 액세스 권한이 필요합니다.

관리부

NSX 관리부는 NSX의 중앙화된 네트워크 관리 구성 요소인 NSX Manager에 의해 구성됩니다. 여기에서는 단일 구성 지점 및 REST API 진입 지점을 제공합니다.

NSX Manager는 vCenter Server 환경의 모든 ESX™ 호스트에 가상 장치로 설치됩니다. NSX Manager와 vCenter는 일대일 관계에 있습니다. NSX Manager 인스턴스마다 하나의 vCenter Server가 있습니다. 이는 크로스 vCenter NSX 환경에서도 적용됩니다.

크로스 vCenter NSX 환경에는 기본 NSX Manager와 하나 이상의 보조 NSX Manager가 모두 있습니다. 기본 NSX Manager에서는 범용 논리적 스위치, 범용 논리적(분산) 라우터 및 범용 방화벽 규칙을 생성하고 관리할 수 있습니다. 보조 NSX Manager는 해당 NSX Manager의 로컬 네트워킹 서비스를 관리하는 데 사용됩니다. 크로스 vCenter NSX 환경에는 기본 NSX Manager와 연결된 보조 NSX Manager가 최대 7개 있을 수 있습니다.

소비 플랫폼

vSphere Web Client에서 사용할 수 있는 NSX Manager 사용자 인터페이스를 통해 NSX의 소비량을 직접 유도할 수 있습니다. 일반적으로 최종 사용자는 네트워크 가상화를 자신의 Cloud Management Platform에 연결하여 애플리케이션을 배포합니다. NSX는 REST API를 통해 실질적으로 모든 CMP에 다양한 통합을 제공합니다. VMware vCloud Automation Center, vCloud Director 및 NSX용 Neutron 플러그인이 포함된 OpenStack을 통해 기본 제공되는 통합 기능을 사용할 수도 있습니다.

NSX Edge

NSX Edge를 ESG(Edge Services Gateway) 또는 DLR(논리적 분산 라우터)로 설치할 수 있습니다.

Edge Services Gateway

ESG는 방화벽, NAT, DHCP, VPN, 로드 밸런싱 및 고가용성 같은 모든 NSX Edge 서비스에 대해 액세스를 제공합니다. 데이터 센터에 여러 ESG 가상 장치를 설치할 수 있습니다. 각 ESG 가상 장치는 총 10개의 업링크 및 내부 네트워크 인터페이스를 사용할 수 있습니다. 트렁크를 통해 ESG에는 최대 200개의 하위 인터페이스가 있을 수 있습니다. 내부 인터페이스는 보안 포트 그룹에 연결하여 포트 그룹에 있는 모든 보호된 가상 시스템의 게이트웨이 역할을 합니다. 내부 인터페이스에 할당된 서브넷은 라우팅된 공용 IP 공간이거나 NAT가 적용된/라우팅된 RFC 1918 전용 공간일 수 있습니다. 네트워크 인터페이스 간의 트래픽에는 방화벽 규칙 및 기타 NSX Edge 서비스가 적용됩니다.

ESG의 업링크 인터페이스는 업링크 포트 그룹에 연결하여 액세스 계층 네트워킹을 제공하는 서비스나 공유 회사 네트워크에 액세스할 수 있습니다. 로드 밸런서, 사이트 간 VPN 및 NAT 서비스에는 외부 IP 주소를 여러 개 구성할 수 있습니다.

논리적 분산 라우터

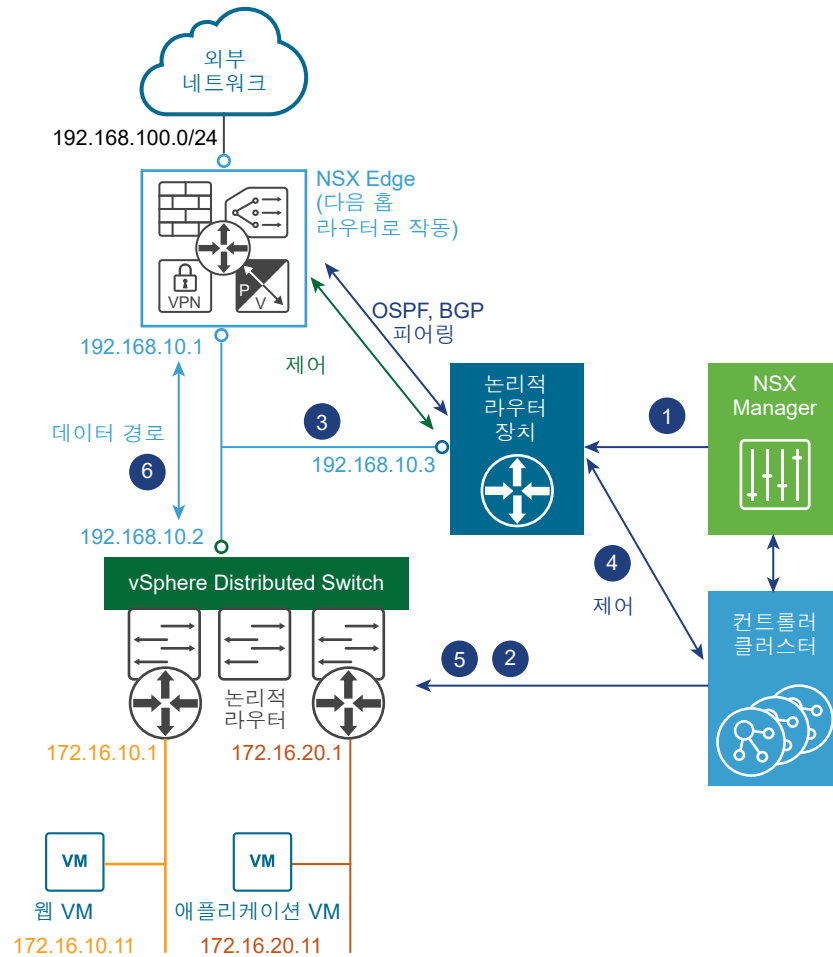
DLR은 테넌트 IP 주소 공간 및 데이터 경로 분리를 지원하는 동-서 분산 라우팅을 제공합니다. 서로 다른 서브넷의 동일한 호스트에 상주하는 가상 시스템 또는 워크로드는 기존 라우팅 인터페이스를 이동하지 않고도 서로 통신할 수 있습니다.

논리적 라우터에는 8개의 업링크 인터페이스와 최대 1,000개의 내부 인터페이스가 있을 수 있습니다. DLR의 업링크 인터페이스는 일반적으로 DLR과 ESG 사이에 개입하는 계층 2 논리적 전송 스위치를 통해, ESG와 피어 관계를 이룹니다. DLR의 내부 인터페이스는 가상 시스템과 DLR 사이에 개입하는 논리적 스위치를 통해, ESXi 하이퍼바이저에 호스트되는 가상 시스템과 피어 관계를 이룹니다.

DLR에는 두 개의 기본 구성 요소가 있습니다.

- DLR 제어부는 DLR 가상 장치에서 제공되며 제어 VM이라고도 합니다. 이 VM은 동적 라우팅 프로토콜(BGP 및 OSPF)을 지원하고 라우팅 업데이트를 다음 계층 3 홉 장치(대개 Edge Services Gateway)와 교환하며 NSX Manager 및 NSX Controller 클러스터와 통신합니다. DLR 가상 장치의 고가용성은 활성-대기 구성을 통해 제공됩니다. 즉, HA를 사용하도록 설정한 DLR을 생성할 경우 활성/대기 모드에서 작동하는 가상 시스템 쌍이 제공됩니다.
- 데이터부 수준에서는 NSX 도메인의 일부인 ESXi 호스트에 설치되는 DLR 커널 모듈(VIB)이 있습니다. 커널 모듈은 계층 3 라우팅을 지원하는 모듈식 새시의 라인 카드와 비슷합니다. 커널 모듈에는 컨트롤러 클러스터에서 푸시되고 라우팅 테이블이라고도 하는 RIB(Routing Information Base)가 있습니다. 경로 조회 및 ARP 항목 조회의 데이터부 기능은 커널 모듈에서 수행됩니다. 커널 모듈에는 다양한 논리적 스위치 및 VLAN 지원 포트 그룹에 연결하는 LIF라는 논리적 인터페이스가 장착되어 있습니다. 각 LIF에는 해당 LIF가 연결하는 논리적 L2 세그먼트의 기본 IP 게이트웨이를 나타내는 IP 주소와 vMAC 주소가 할당되어 있습니다. IP 주소는 LIF별로 고유하지만 모든 정의된 LIF에는 동일한 vMAC가 할당됩니다.

그림 3-1. 논리적 라우팅 구성 요소



- 1 DLR 인스턴스는 NSX Manager UI 또는 API 호출을 통해 생성되고 OSPF 또는 BGP를 사용하여 라우팅이 사용되도록 설정됩니다.
- 2 NSX Controller는 ESXi 호스트와 제어부를 사용하여 LIF 및 연결된 해당 IP 주소와 vMAC 주소를 비롯한 새로운 DLR 구성을 푸시합니다.
- 3 라우팅 프로토콜이 다음 홉 장치(이 예에서는 NSX Edge [ESG])에서도 사용되도록 설정된다고 가정하면 ESG와 DLR 제어 VM 사이에 OSPF 또는 BGP 피어링이 설정됩니다. 그러면 ESG와 DLR이 라우팅 정보를 교환할 수 있습니다.
 - 모든 연결된 논리적 네트워크(이 예에서는 172.16.10.0/24 및 172.16.20.0/24)에 대해 IP 접두사를 OSPF로 재배포하도록 DLR 제어 VM을 구성할 수 있습니다. 그러면 이 VM이 이러한 경로 알림을 NSX Edge에 푸시합니다. 이와 같은 접두사의 다음 홉은 제어 VM에 할당된 IP 주소(192.168.10.3)가 아니지만 DLR의 데이터부 구성 요소를 식별하는 IP 주소(192.168.10.2)입니다. 전자를 DLR "프로토콜 주소"라고 하고 후자를 "전달 주소"라고 합니다.
 - NSX Edge는 제어 VM에 접두사를 푸시하여 외부 네트워크의 IP 네트워크에 연결합니다. 대부분의 경우 NSX Edge에서 단일 기본 경로가 전송되는데, 이 경로는 물리적 네트워크 인프라로의 단일 출구 지점을 나타내기 때문입니다.

- 4 DLR 제어 VM은 NSX Edge에서 얻은 IP 경로를 컨트롤러 클러스터에 푸시합니다.
- 5 컨트롤러 클러스터는 DLR 제어 VM에서 얻은 경로를 하이퍼바이저로 배포합니다. 클러스터의 각 컨트롤러 노드는 특정 논리적 라우터 인스턴스에 대해 정보를 배포합니다. 여러 논리적 라우터 인스턴스가 배포된 배포 환경에서는 컨트롤러 노드 간에 로드가 분산됩니다. 일반적으로 별개의 논리적 라우터 인스턴스가 배포된 각 테넌트와 연결됩니다.
- 6 호스트의 DLR 라우팅 커널 모듈은 NSX Edge를 통한 외부 네트워크와의 통신에 대한 데이터-경로 트래픽을 처리합니다.

NSX Services

NSX 구성 요소는 함께 작동하여 다음의 기능 서비스를 제공합니다.

논리적 스위치

클라우드 배포 환경 또는 가상 데이터센터에는 여러 테넌트에 분산된 다양한 애플리케이션이 있습니다. 이러한 애플리케이션과 테넌트는 보안, 장애 분리 및 겹치지 않는 IP 주소를 위해 서로 분리되어야 합니다.

NSX에서는 각각 하나의 논리적 브로드캐스트 도메인에 해당하는 논리적 스위치를 여러 개 생성할 수 있습니다. 애플리케이션 또는 테넌트 가상 시스템은 논리적 스위치에 논리적으로 연결될 수 있습니다. 이 기능은 배포 유연성과 속도를 향상시킬 뿐 아니라 물리적 계층 2 확장 또는 스페닝 트리 문제 없이 물리적 네트워크의 브로드캐스트 도메인(VLAN)이 가진 모든 특성도 제공합니다.

논리적 스위치는 분산되며 vCenter의 모든 호스트(또는 크로스 vCenter NSX 환경의 모든 호스트)에 분산될 수 있습니다. 이러한 특성은 물리적 계층 2(VLAN) 경계의 제한 없이 데이터센터 내에서 가상 시스템의 이동성(vMotion)을 지원합니다. 소프트웨어의 논리적 스위치에 브로드캐스트 도메인이 포함되므로 물리적 인프라는 MAC/FIB 테이블 제한의 제약을 받지 않습니다.

논리적 라우터

라우팅은 계층 2 브로드캐스트 도메인 간에 필요한 정보 전달 기능을 제공하므로 계층 2 브로드캐스트 도메인의 크기를 줄이고 네트워크 효율성 및 확장성을 개선할 수 있습니다. NSX는 워크로드가 상주하는 위치로 이 인텔리전스 기능을 확장하여 동-서 라우팅을 수행합니다. 따라서 코스트나 시간을 들여 홉을 확장할 필요 없이 가상 시스템 간의 직접적인 통신이 가능합니다. 이와 동시에 NSX 논리적 라우터는 북-남 연결도 제공하므로 테넌트가 공용 네트워크에 액세스할 수 있습니다.

논리적 방화벽

논리적 방화벽은 동적 가상 데이터센터에 대한 보안 메커니즘을 제공합니다. 논리적 방화벽의 분산 방화벽 구성 요소를 이용하면 VM 이름과 특성, 사용자 ID, 데이터센터와 같은 vCenter 개체, 호스트 그리고 IP 주소나 VLAN 등과 같은 전통적 네트워킹 특성에 기반하여 가상 시스템과 같은 가상 데이터센터 엔티티를 분류할 수 있습니다. Edge Firewall 구성 요소는 IP/VLAN 구성에 기반한 DMZ 구성 및 멀티 테넌트 가상 데이터센터에서 테넌트 간 분리와 같은 주요 경계 보안 요구 사항을 충족하는 데 도움이 됩니다.

Flow Monitoring 기능은 애플리케이션 프로토콜 수준에서 가상 시스템 간의 네트워크 작업을 표시합니다. 이 정보를 사용하여 네트워크 트래픽을 감사하고, 방화벽 정책을 정의 및 구체화하며, 네트워크에 대한 위협을 식별할 수 있습니다.

논리적 VPN(Virtual Private Network)

SSL VPN-Plus를 통해 원격 사용자는 회사 전용 애플리케이션에 액세스할 수 있습니다. IPSec VPN은 NSX 또는 타사 벤더의 하드웨어 라우터/VPN 게이트웨이를 사용하여 NSX Edge 인스턴스와 원격 사이트 간에 사이트 대 사이트 연결을 제공합니다. L2 VPN을 사용하면 가상 시스템에서 지리적 경계를 넘어 동일한 IP 주소를 유지하면서 네트워크 연결을 유지할 수 있으므로 데이터센터를 확장할 수 있습니다.

논리적 로드 밸런서

NSX Edge 로드 밸런서는 단일 VIP(가상 IP 주소)로 방향 지정된 클라이언트 연결을 로드 밸런싱 풀의 구성원으로 구성된 여러 대상으로 분산합니다. 즉, 로드 분산이 사용자에게 투명하게 진행되도록 들어오는 서비스 요청을 여러 서버 간에 균일하게 분산합니다. 따라서 로드 밸런싱은 리소스 활용도를 최적화하고, 처리량을 극대화하며, 응답 시간을 최소화하고, 오버로드를 방지하는 데 도움이 됩니다.

Service Composer

Service Composer는 네트워크 및 보안 서비스를 가상 인프라의 애플리케이션에 프로비저닝하고 할당하는 데 도움이 됩니다. 이러한 서비스를 보안 그룹에 매핑하면 보안 정책을 사용하여 보안 그룹의 가상 시스템에 서비스가 적용됩니다.

NSX 확장성

타사 솔루션 제공자는 각자의 솔루션을 NSX 플랫폼에 통합할 수 있으므로 VMware 제품 및 파트너 솔루션 전체에서 통합된 환경을 고객에게 제공할 수 있습니다. 데이터센터 운영자는 복잡한 다중 계층 가상 네트워크를 기본 네트워크 토폴로지 또는 구성 요소와는 상관없이 몇 초 안에 프로비저닝할 수 있습니다.

크로스 vCenter Networking & Security 개요

4

NSX 6.2 이상에서는 단일 기본 NSX Manager에서 여러 vCenter NSX 환경을 관리할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 크로스 vCenter NSX의 이점
- 크로스 vCenter NSX의 작동 방식
- 크로스 vCenter NSX의 NSX Services 지원 매트릭스
- 범용 컨트롤러 클러스터
- 범용 전송 영역
- 범용 논리적 스위치
- 범용 논리적 (분산) 라우터
- 범용 방화벽 규칙
- 범용 네트워크 및 보안 개체
- 크로스 vCenter NSX 토폴로지
- NSX Manager 역할 수정

크로스 vCenter NSX의 이점

vCenter Server 시스템이 두 대 이상 포함된 NSX 환경을 중앙에서 관리할 수 있습니다.

vCenter Server 시스템이 여러 대 필요한 이유는 많으며 몇 가지 예를 들면 다음과 같습니다.

- vCenter Server의 확장 제한 해결
- Horizon View 또는 Site Recovery Manager처럼 전용 vCenter Server 시스템 또는 여러 대의 vCenter Server 시스템이 필요한 제품 수용
- 환경 구분(예: 비즈니스 단위, 테넌트, 조직 또는 환경 유형별로 구분)

NSX 6.1 및 이전 버전에서는 vCenter NSX 환경을 여러 개 배포할 경우 각 환경을 별도로 관리해야 합니다. NSX 6.2 이상에서는 기본 NSX Manager에 범용 개체를 생성할 수 있으며 해당 개체는 환경의 모든 vCenter Server 시스템 간에 동기화됩니다.

크로스 vCenter NSX에는 다음과 같은 기능이 포함되어 있습니다.

- NSX 논리적 네트워크의 범위 증가. 전체 vCenter NSX 환경에 걸쳐 동일한 논리적 네트워크를 사용할 수 있으므로 모든 vCenter Server 시스템에 있는 모든 클러스터의 VM이 동일한 논리적 네트워크에 연결될 수 있습니다.
- 보안 정책의 중앙 집중식 관리. 방화벽 규칙을 하나의 중앙 위치에서 관리하고 위치나 vCenter Server 시스템에 관계없이 모든 VM에 적용할 수 있습니다.
- vSphere 6의 새로운 이동성 경계 지원(크로스 vCenter 및 논리적 스위치 간 원거리 vMotion 포함)
- 다중 사이트 환경에 대한 지원 강화(메트로 거리에서 150ms RTT까지). 여기에는 액티브-액티브 데이터 센터와 액티브-패시브 데이터 센터가 모두 포함됩니다.

크로스 vCenter NSX 환경은 많은 이점을 갖추고 있습니다.

- 범용 개체의 중앙 관리를 통해 관리 부담이 줄어듭니다.
- 워크로드의 이동성 증가 - VM을 재구성하거나 방화벽 규칙을 변경할 필요 없이 vMotion을 통해 VM을 vCenter Server 간에 이동할 수 있습니다.
- NSX 다중 사이트 및 재해 복구 기능이 향상됩니다.

참고 크로스 vCenter NSX 기능은 vSphere 6.0 이상에서 지원됩니다.

크로스 vCenter NSX의 작동 방식

크로스 vCenter NSX 환경에 다중 vCenter Server가 있을 수 있는데, 각각은 고유한 NSX Manager와 쌍을 이루어야 합니다. 하나의 NSX Manager에 기본 NSX Manager 역할이 할당되고, 다른 NSX Manager에 보조 NSX Manager 역할이 할당됩니다.

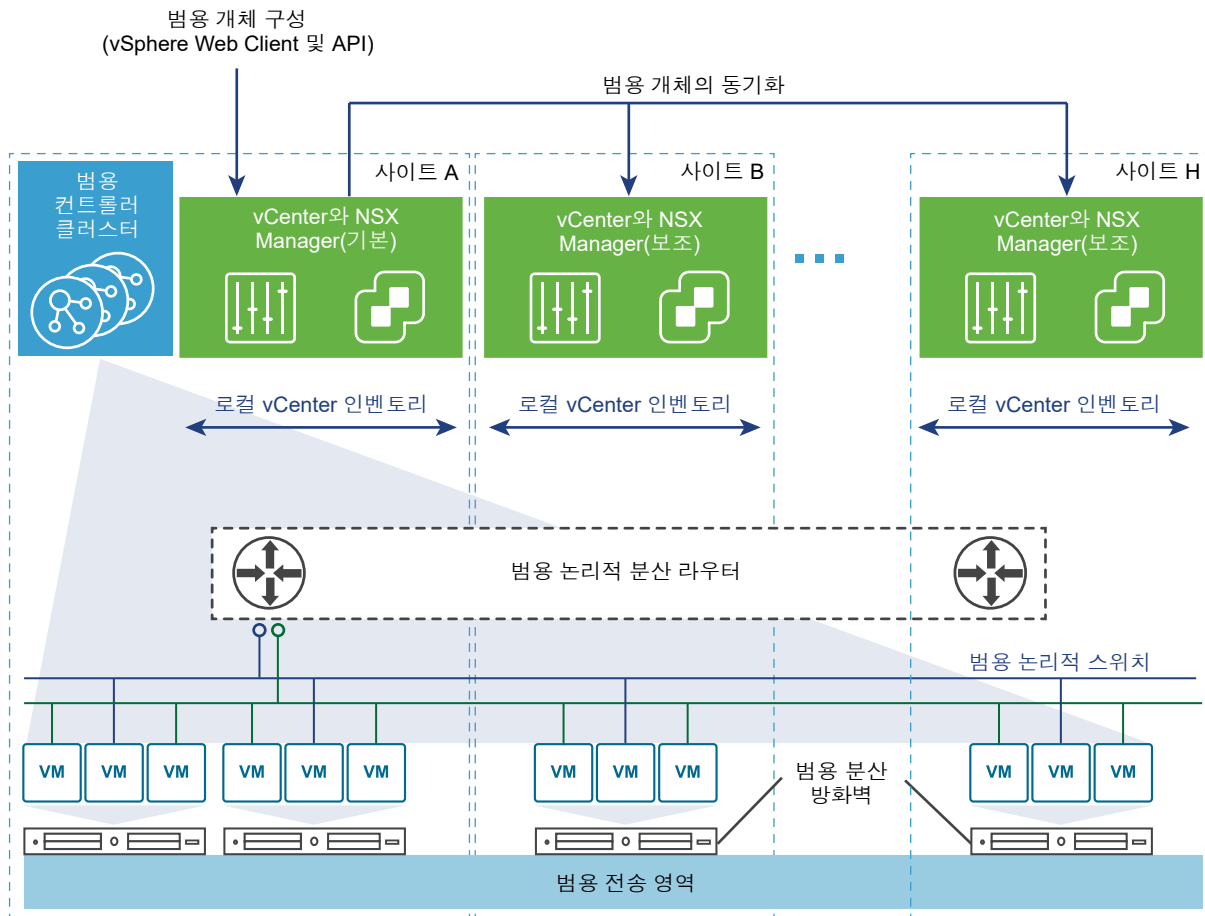
기본 NSX Manager를 사용하여 크로스 vCenter NSX 환경에 대한 제어부를 제공하는 범용 컨트롤러 클러스터를 배포합니다. 보조 NSX Manager에는 고유한 컨트롤러 클러스터가 없습니다.

기본 NSX Manager는 범용 논리적 스위치 같은 범용 개체를 생성할 수 있습니다. NSX 범용 동기화 서비스가 이 개체를 보조 NSX Manager에 동기화합니다. 보조 NSX Manager에서 이 개체를 볼 수 있지만, 보조 NSX Manager에서 편집할 수는 없습니다. 범용 개체를 관리하려면 기본 NSX Manager를 사용해야 합니다. 기본 NSX Manager를 사용하여 환경에 보조 NSX Manager를 구성할 수 있습니다.

기본 및 보조 NSX Manager 모두에서 논리적 스위치 및 논리적 (분산) 라우터 같은 특정 vCenter NSX 환경에 로컬인 개체를 생성할 수 있습니다. 이 개체는 자신이 생성된 vCenter NSX 환경 내에서만 존재합니다. 이 개체는 크로스 vCenter NSX 환경의 다른 NSX Manager에는 표시되지 않습니다.

NSX Manager에 독립 실행형 역할을 할당할 수 있습니다. 이는 단일 NSX Manager 및 단일 vCenter가 포함된 NSX 6.2 이전 환경에 해당합니다. 독립형 NSX Manager는 범용 개체를 생성할 수 없습니다.

참고 기본 NSX Manager의 역할을 독립형으로 변경할 경우 NSX 환경에 범용 개체가 있으면 NSX Manager가 전송 역할을 할당받습니다. 범용 개체는 유지되지만 변경할 수 없으며 다른 범용 개체를 생성할 수 없습니다. 범용 개체를 전송 역할에서 삭제할 수 있습니다. 전송 역할은 기본 NSX Manager를 변경하는 경우 등에 한해 일시적으로만 사용해야 합니다.



크로스 vCenter NSX의 NSX Services 지원 매트릭스

NSX Services 하위 그룹을 크로스 vCenter NSX에서 범용 동기화에 사용할 수 있습니다. 범용 동기화에 사용할 수 없는 서비스는 NSX Manager의 로컬로 사용하도록 구성할 수 있습니다.

표 4-1. 크로스 vCenter NSX의 NSX Services 지원 매트릭스

NSX 서비스	세부 정보	크로스 vCenter NSX 동기화 지원 여부
논리적 스위치	전송 영역	예
	논리적 스위치	예
L2 브리지		아니요

표 4-1. 크로스 vCenter NSX의 NSX Services 지원 매트릭스 (계속)

NSX 서비스	세부 정보	크로스 vCenter NSX 동기화 지원 여부
라우팅	논리적 (분산) 라우터	예
	논리적 (분산) 라우터 장치	아니요로 설계됨. 범용 논리적 라우터마다 다수의 장치가 필요한 경우, 장치는 각 NSX Manager에서 생성되어야 합니다. 따라서 장치별로 다른 구성을 사용할 수 있으며 이는 로컬 송신이 구성된 환경에서 필요할 수 있습니다.
	NSX Edge Services Gateway	아니요
논리적 방화벽	분산 방화벽	예
	제외 목록	아니요
	SpoofGuard	아니요
	전체 흐름에 대한 Flow Monitoring	아니요
	네트워크 서비스 삽입	아니요
	Edge 방화벽	아니요
VPN		아니요
논리적 로드 밸런서		아니요
기타 Edge 서비스		아니요
Service Composer		아니요
네트워크 확장성		아니요
네트워크 및 보안 개체	IP 주소 그룹(IP 집합)	예
	MAC 주소 그룹(MAC 집합)	예
	IP 풀	아니요
	보안 그룹	예. 멤버 자격 구성이 비범용 보안 그룹 멤버 자격과 다릅니다. 자세한 내용은 "NSX 관리 가이드"의 "보안 그룹 생성"을 참조하십시오.
	서비스	예
	서비스 그룹	예
보안 태그		예
하드웨어 게이트웨이(하드웨어 VTEP로도 알려져 있음)		아니요. 자세한 내용은 "NSX 관리 가이드"의 "하드웨어 게이트웨이 샘플 구성"을 참조하십시오.

범용 컨트롤러 클러스터

각 크로스 vCenter NSX 환경에는 기본 NSX Manager와 연결된 범용 컨트롤러 클러스터가 하나씩 있습니다. 보조 NSX Manager에는 컨트롤러 클러스터가 없습니다.

범용 컨트롤러 클러스터는 크로스 vCenter NSX 환경의 유일한 컨트롤러 클러스터이므로 vCenter NSX 쌍의 로컬 논리적 스위치 및 논리적 라우터에 대한 정보뿐 아니라 범용 논리적 스위치 및 범용 논리적 라우터에 대한 정보도 유지 관리합니다.

개체 ID가 겹치지 않도록 범용 개체와 로컬 개체에 대해 별도의 ID 풀이 사용됩니다.

범용 전송 영역

크로스 vCenter NSX 환경에서 범용 전송 영역은 하나만 있을 수 있습니다.

범용 전송 영역은 기본 NSX Manager에 생성되고 보조 NSX Manager에 동기화됩니다. 범용 논리적 네트워크에 참여해야 하는 클러스터는 해당 NSX Manager에서 범용 전송 영역에 추가해야 합니다.

범용 논리적 스위치

범용 논리적 스위치는 계층 2 네트워크를 여러 사이트로 확장할 수 있게 해 줍니다.

범용 전송 영역에 논리적 스위치를 생성하면 범용 논리적 스위치가 생성됩니다. 이 스위치는 범용 전송 영역의 모든 클러스터에서 이용할 수 있습니다. 범용 전송 영역은 크로스 vCenter NSX 환경의 모든 vCenter에 있는 클러스터를 포함할 수 있습니다.

논리적 스위치에 VNI를 할당하는 데는 세그먼트 ID 풀이 사용되고 범용 논리적 스위치에 VNI를 할당하는 데는 범용 세그먼트 ID 풀이 사용됩니다. 이 두 풀이 겹치지 않아야 합니다.

범용 논리적 스위치 간에 라우팅하기 위해서는 반드시 범용 논리적 라우터를 사용해야 합니다. 범용 논리적 스위치와 논리적 스위치 사이에 라우팅하려면 Edge Services Gateway를 이용해야만 합니다.

범용 논리적 (분산) 라우터

범용 논리적 (분산) 라우터는 사용자가 범용 논리적 라우터, 클러스터, 또는 호스트 수준에서 지정할 수 있는 중앙 집중식의 관리와 라우팅 구성을 제공합니다.

생성된 이후에는 변경이 불가능하므로 범용 논리적 라우터를 생성할 때 로컬 송신 사용 여부를 선택해야 합니다. 로컬 송신을 사용하면 식별자, 즉 로케일 ID를 기준으로 ESXi 호스트에 제공되는 경로를 제어할 수 있습니다.

각각의 NSX Manager는 로케일 ID를 하나씩 할당 받고 기본값은 NSX Manager UUID로 설정되어 있습니다. 논리적 라우터를 다음 수준으로 재정의할 수 있습니다.

- 범용 논리적 라우터
- 클러스터
- ESXi 호스트

로컬 송신을 사용하도록 설정하지 않으면 로케일 ID가 무시되고 범용 논리적 라우터에 연결된 모든 ESXi 호스트는 같은 경로를 수신합니다. 크로스 vCenter NSX 환경에서 로컬 송신을 사용하도록 설정할지 여부는 설계 고려 사항이며 모든 크로스 vCenter NSX 구성에 꼭 필요한 것은 아닙니다.

범용 방화벽 규칙

크로스 vCenter NSX 환경에서 분산 방화벽을 이용하면 환경 내의 모든 vCenter Server에 적용되는 규칙을 중앙 집중적으로 관리할 수 있습니다. 분산 방화벽은 vCenter Server 간에 워크로드 또는 가상 시스템을 이동하는 vCenter 간 vMotion을 지원하여 소프트웨어 정의 데이터센터의 보안을 현저하게 향상합니다.

데이터센터 스케일 아웃이 필요할 때 기존 vCenter Server는 동일한 수준으로 확장되지 못할 수 있습니다. 애플리케이션 집합을 다른 vCenter Server가 관리하는 새로운 호스트로 옮겨야 할 수도 있습니다. 또는, 스테이징 서버가 한 vCenter Server에서 관리되고 운영 서버가 다른 vCenter Server에서 관리되는 환경에서는 스테이징에서 운영으로 애플리케이션을 이동해야 할 수도 있습니다. 분산 방화벽은 기본 NSX Manager에 정의된 방화벽 정책을 최대 7개 보조 NSX Manager에서 복제하여 이러한 vCenter 간 vMotion 시나리오를 지원합니다.

기본 NSX Manager에서 범용 동기화로 표시되는 분산 방화벽 규칙 섹션을 생성할 수 있습니다. 둘 이상의 범용 L2 규칙 섹션과 둘 이상의 범용 L3 규칙 섹션을 생성할 수 있습니다. 범용 섹션은 항상 기본 및 보조 NSX Manager 맨 위에 표시됩니다. 이러한 섹션 및 해당 규칙은 환경의 모든 보조 NSX Manager와 동기화됩니다. 다른 섹션의 규칙은 해당 NSX Manager에 대한 로컬 상태를 유지합니다.

다음 분산 방화벽 기능은 크로스 vCenter NSX 환경에서는 지원되지 않습니다.

- 제외 목록
- SpoofGuard
- 전체 흐름에 대한 Flow Monitoring
- 네트워크 서비스 삽입
- Edge 방화벽

Service Composer는 범용 동기화를 지원하지 않으므로 이를 통해 범용 섹션에서 분산 방화벽 규칙을 생성할 수 없습니다.

범용 네트워크 및 보안 개체

범용 섹션의 분산 방화벽 규칙에 사용할 사용자 지정 네트워크와 보안 개체를 생성할 수 있습니다.

USG(범용 보안 그룹)에는 다음이 포함될 수 있습니다.

- 범용 IP 집합
- 범용 MAC 집합
- 범용 보안 그룹
- 범용 보안 태그
- 동적 조건

범용 네트워크 및 보안 개체는 기본 NSX Manager에서만 생성, 삭제 및 업데이트되지만 보조 NSX Manager에서 읽을 수 있습니다. 범용 동기화 서비스는 즉시, 그리고 필요할 때 강제 동기화를 사용해서 vCenter에서 범용 개체를 동기화합니다.

범용 보안 그룹은 두 가지 유형의 배포에서 사용됩니다. 하나는 다중 라이브 크로스 vCenter NSX 환경이고, 다른 하나는 한 사이트가 지정된 시간에 라이브 상태이고 나머지는 대기 상태를 유지하는 크로스 - vCenter NSX 활성 대기 배포입니다. 활성 대기 배포에만 범용 보안 태그를 기준으로 하는 VM 이름 정적 멤버 자격에 따라 동적 멤버 자격이 있는 범용 보안 그룹이 있을 수 있습니다. 범용 보안 그룹이 생성되면 활성 대기 시나리오 기능에 대해 사용하도록 설정할지 또는 사용하지 않도록 설정하지를 편집할 수 없습니다. 멤버 자격은 포함된 개체로만 정의되며 제외된 개체를 사용할 수 없습니다.

범용 보안 그룹은 Service Composer에서 생성할 수 없습니다. Service Composer에서 생성된 보안 그룹은 해당 NSX Manager에 로컬인 보안 그룹이 됩니다.

크로스 vCenter NSX 토폴로지

크로스 vCenter NSX를 단일 물리적 사이트에 배포하거나 여러 사이트 간에 배포할 수 있습니다.

다중 사이트 및 단일 사이트 크로스 vCenter NSX

크로스 vCenter NSX 환경에서는 여러 vCenter NSX 설치 간에 동일한 논리적 스위치 및 다른 네트워크 개체를 사용할 수 있습니다. vCenter Server 시스템을 모두 동일한 사이트에 배치하거나 서로 다른 사이트에 배치할 수 있습니다.

크로스 vCenter NSX 환경이 단일 사이트에 포함되어 있는지 또는 여러 사이트에 걸쳐 있는지에 관계없이 유사한 구성을 사용할 수 있습니다. 예로 나온 이 두 토폴로지는 다음으로 구성되어 있습니다.

- 사이트의 모든 클러스터가 포함된 범용 전송 영역
- 범용 전송 영역에 연결된 범용 논리적 스위치. 두 범용 논리적 스위치는 VM을 연결하는 데 사용되며 하나는 라우터 업링크를 위한 전송 네트워크로 사용됩니다.
- 범용 논리적 스위치에 추가된 VM
- 동적 라우팅을 사용하도록 설정하기 위한 NSX Edge 장치가 포함된 범용 논리적 라우터. 범용 논리적 라우터 장치의 VM 범용 논리적 스위치에는 내부 인터페이스가 있고 전송 네트워크 범용 논리적 스위치에는 업링크 인터페이스가 있습니다.
- 전송 네트워크 및 물리적 송신 라우터 네트워크에 연결된 ESG(Edge Services Gateway)

크로스 vCenter NSX 토폴로지에 대한 자세한 내용은 "크로스 vCenter NSX 설계 가이드" (<https://communities.vmware.com/docs/DOC-32552>)를 참조하십시오.

그림 4-1. 단일 사이트의 크로스 vCenter NSX

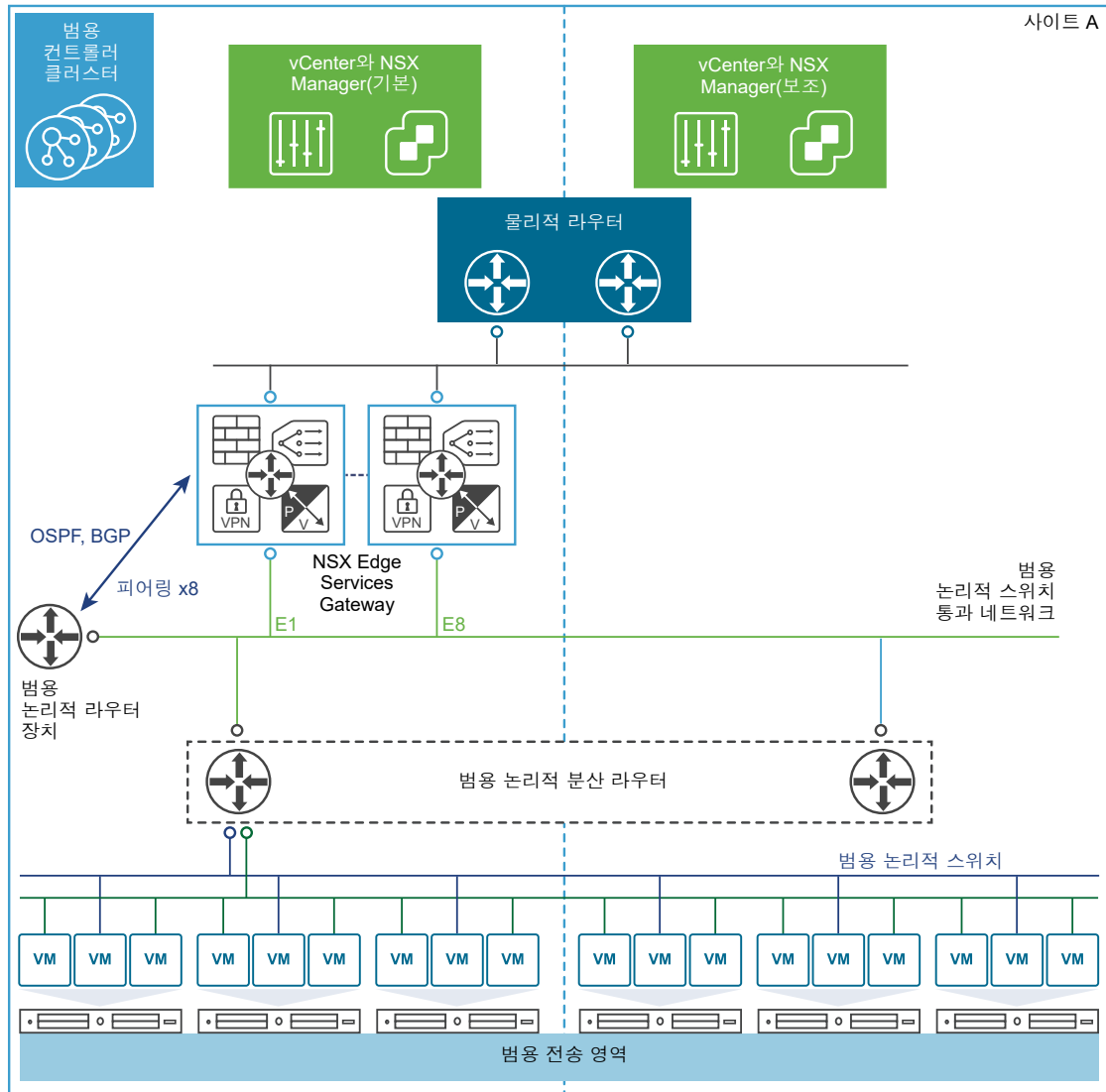
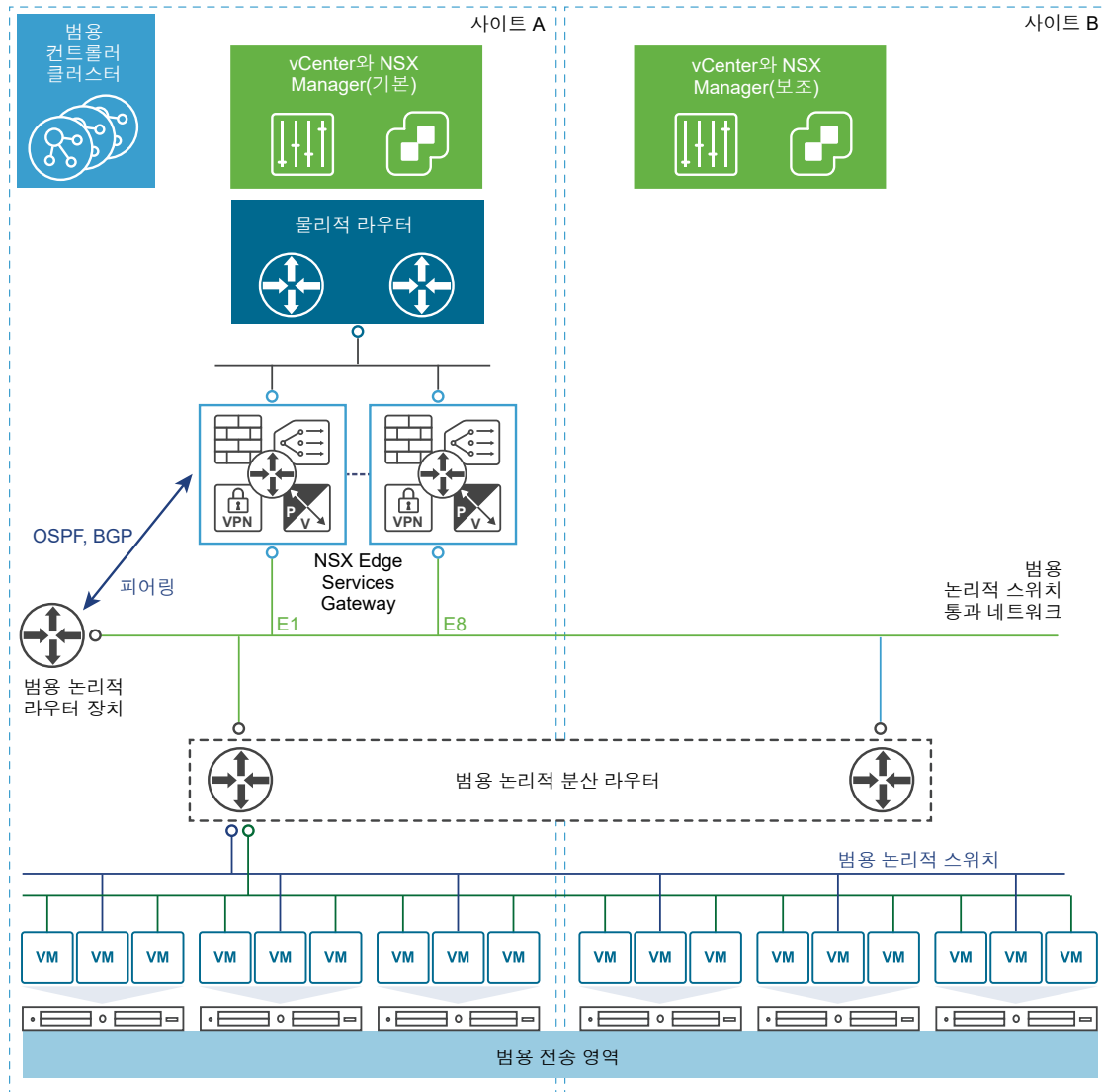


그림 4-2. 두 사이트로 확장된 크로스 vCenter NSX



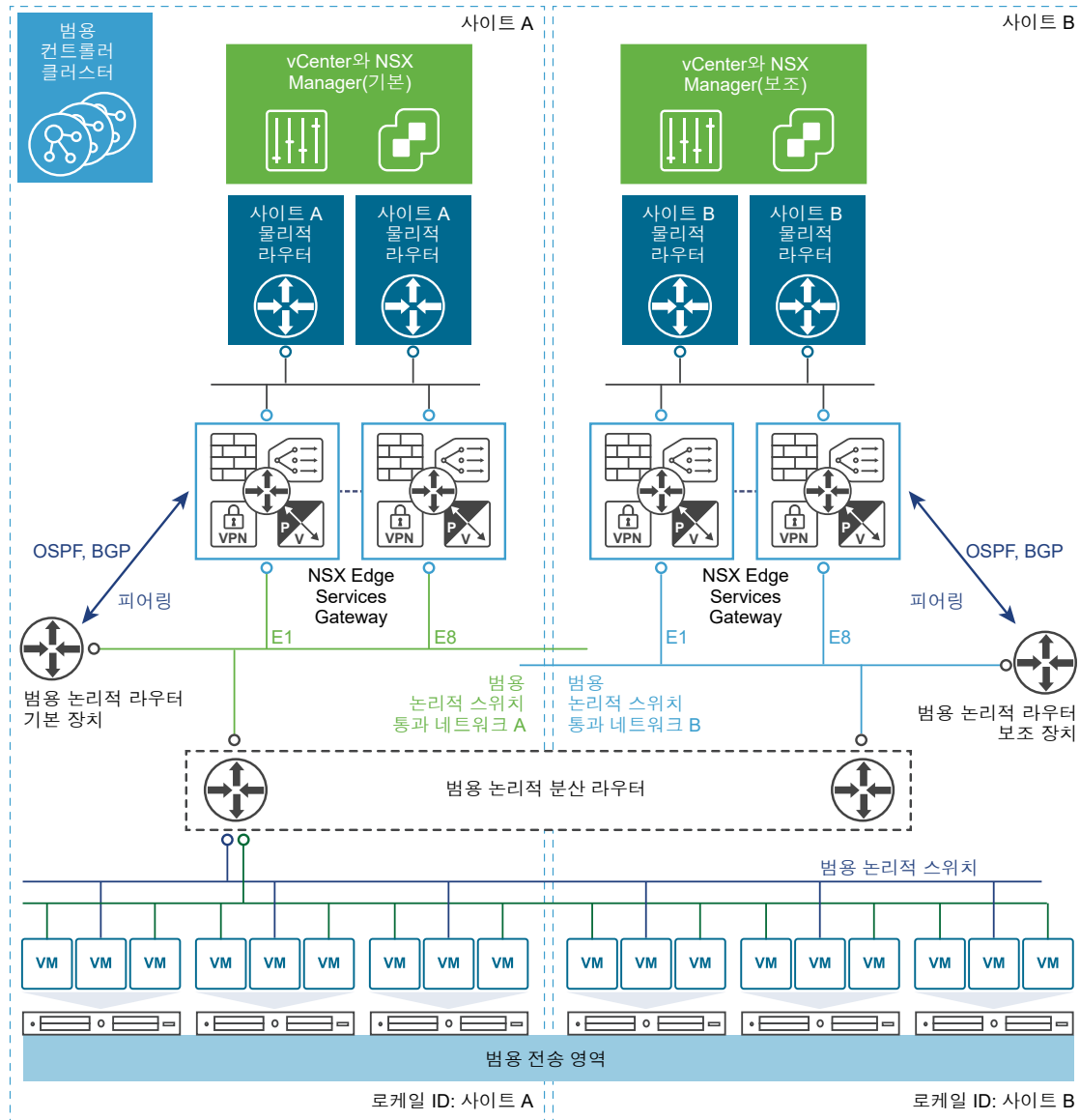
로컬 송신

다중 사이트 크로스 vCenter NSX 환경의 모든 사이트는 송신 트래픽에 동일한 물리적 라우터를 사용할 수 있습니다. 하지만 송신 경로를 사용자 지정해야 할 경우에는 범용 논리적 경로가 생성될 때 로컬 송신 기능이 사용되도록 설정되어 있어야 합니다.

로컬 송신을 사용하면 범용 논리적 라우터, 클러스터 또는 호스트 수준에서 경로를 사용자 지정할 수 있습니다. 이 다중 사이트 크로스 vCenter NSX 환경 예에서는 로컬 송신이 사용되도록 설정되어 있습니다. 각 사이트의 ESG(Edge Services Gateway)에는 사이트의 물리적 라우터를 통해 트래픽을 전송하는 기본 경로가 있습니다. 범용 논리적 라우터는 각 사이트에 하나씩 두 개의 장치를 사용하여 구성됩니다. 장치는 해

당 사이트의 **ESG**에서 경로를 검색합니다. 검색된 경로는 범용 컨트롤러 클러스터로 전송됩니다. 로컬 송신이 사용되도록 설정되어 있으므로 해당 사이트의 로케일 ID가 해당 경로에 연결됩니다. 범용 컨트롤러 클러스터가 일치하는 로케일 ID를 가진 경로를 호스트로 전송합니다. 사이트 **A** 장치에서 검색된 경로는 사이트 **A**의 호스트로 전송되고 사이트 **B** 장치에서 검색된 경로는 사이트 **B**의 호스트로 전송됩니다.

로컬 송신에 대한 자세한 내용은 "크로스 vCenter NSX 설계 가이드" (<https://communities.vmware.com/docs/DOC-32552>)를 참조하십시오.



NSX Manager 역할 수정

NSX Manager에는 기본, 보조, 독립형 또는 전송과 같은 역할이 있을 수 있습니다. 기본 NSX Manager에서는 모든 범용 개체를 보조 NSX Manager와 동기화하는 특수 동기화 소프트웨어가 실행됩니다.

NSX Manager의 역할을 변경하면 어떤 일이 발생하는지 이해하고 있어야 합니다.

기본으로 설정

이 작업은 NSX Manager의 역할을 기본으로 설정하고 동기화 소프트웨어를 시작합니다. NSX Manager가 이미 기본 또는 보조 역할인 경우에는 이 작업이 실패합니다.

독립형으로 설정(보조에서)

이 작업을 통해 NSX Manager의 역할을 독립형 또는 전송 모드로 설정합니다. NSX Manager에 독립형 역할이 이미 있는 경우에는 이 작업이 실패할 수 있습니다.

독립형으로 설정(기본에서)

이 작업을 통해 기본 NSX Manager를 독립형 또는 전송 모드로 다시 설정하고 동기화 소프트웨어를 중지하고 모든 보조 NSX Manager를 등록 해제합니다. NSX Manager가 이미 독립형이거나 보조 NSX Manager에 연결할 수 없는 경우에는 이 작업이 실패할 수 있습니다.

기본에서 연결 끊기

보조 NSX Manager에서 이 작업을 실행하면 보조 NSX Manager가 기본 NSX Manager에서 일방적으로 연결이 끊깁니다. 이 작업은 기본 NSX Manager에서 복구할 수 없는 오류가 발생하고 보조 NSX Manager를 새 기본 NSX Manager로 등록하려는 경우에 사용해야 합니다. 원래 기본 NSX Manager가 다시 활성화되면 해당 데이터베이스에 보조 NSX Manager가 등록된 상태로 나타납니다. 이 문제를 해결하려면 보조 NSX Manager를 원래 기본 NSX Manager에서 연결을 끊거나 등록을 취소할 때 **force** 옵션을 포함하십시오. **force** 옵션은 보조 NSX Manager를 원래 기본 NSX Manager의 데이터베이스에서 제거합니다.

전송 영역은 논리적 스위치가 연결할 수 있는 호스트를 제어합니다. 전송 영역은 하나 이상의 **vSphere** 클러스터에 걸쳐 있을 수 있습니다. 전송 영역에서 클러스터를 지정하므로 특정 네트워크 사용에 참여할 수 있는 **VM**도 지정합니다. 크로스 **vCenter NSX** 환경에서는 해당 환경에 있는 **vCenter**의 클러스터를 포함할 수 있는 범용 전송 영역을 생성할 수 있습니다. 범용 전송 영역은 하나만 생성할 수 있습니다.

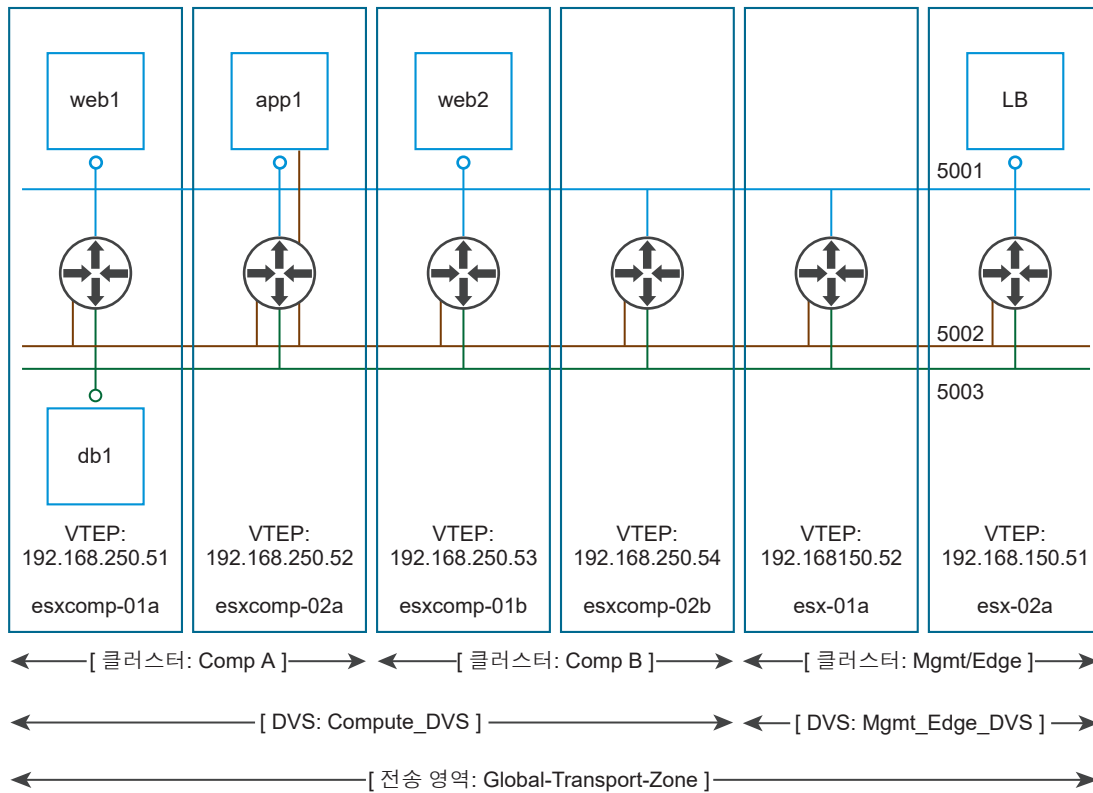
NSX 환경에는 요구 사항에 따라 하나 이상의 전송 영역이 포함될 수 있습니다. 호스트 클러스터는 여러 전송 영역에 속할 수 있습니다. 논리적 스위치는 하나의 전송 영역에만 속할 수 있습니다.

NSX는 다른 전송 영역에 있는 **VM**의 연결을 허용하지 않습니다. 논리적 스위치의 범위는 전송 영역으로 제한되므로 다른 전송 영역에 있는 가상 시스템이 동일한 계층 2 네트워크에 있을 수 없습니다. 논리적 분산 라우터는 다른 전송 영역에 있는 논리적 스위치에 연결할 수 없습니다. 첫 번째 논리적 스위치를 연결하면 동일한 전송 영역에 있는 논리적 스위치만 추가로 선택할 수 있도록 제한됩니다.

전송 영역을 설계하는 데 다음 지침이 도움이 될 수 있습니다.

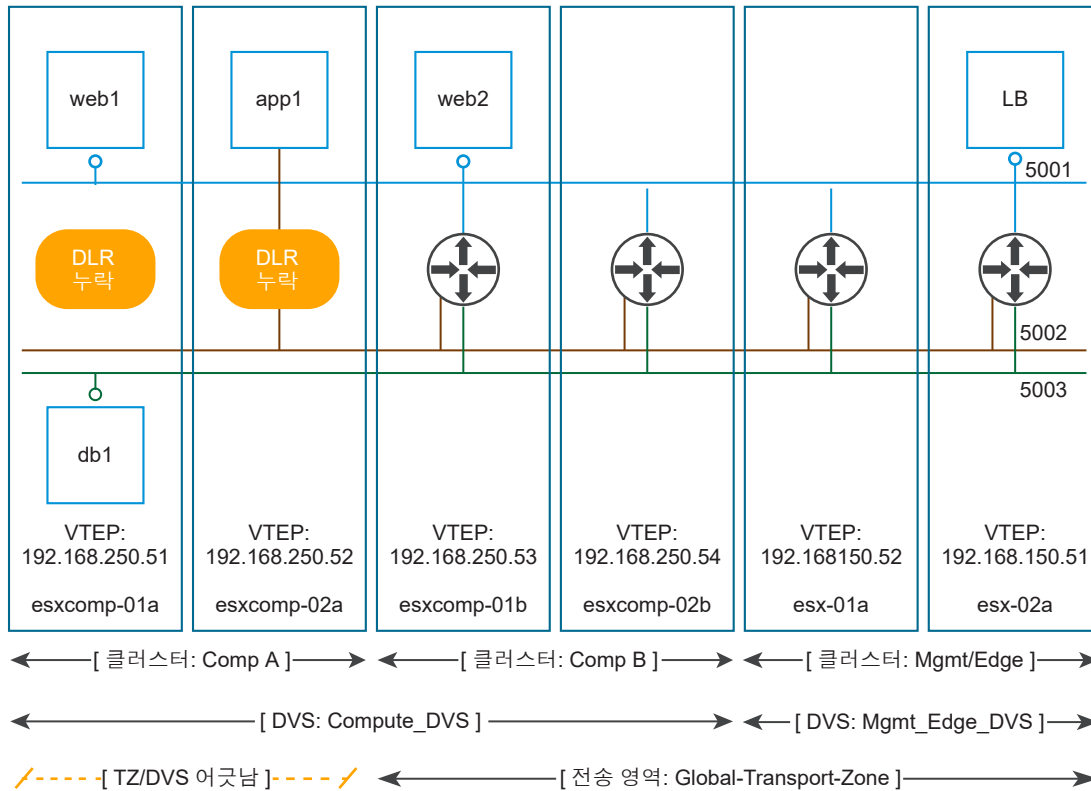
- 클러스터에 계층 3 연결이 필요한 경우 클러스터가 **Edge** 클러스터를 포함하는 전송 영역에 있어야 합니다. **Edge** 클러스터는 계층 3 **Edge** 디바이스(논리적 분산 라우터 및 **ESG(Edge Services Gateway)**)가 있는 클러스터를 의미합니다.
- 2개의 클러스터가 있는데 하나는 웹 서비스용이고 다른 하나는 애플리케이션 서비스용이라고 가정합니다. 이 두 클러스터에 있는 **VM** 간에 **VXLAN** 연결을 생성하려면 두 클러스터가 모두 전송 영역에 포함되어야 합니다.
- 전송 영역에 포함된 모든 논리적 스위치가 전송 영역에 포함된 클러스터 내 모든 **VM**에게 표시되고 이들 **VM**이 사용할 수 있습니다. 클러스터에 보안 환경이 포함된 경우 다른 클러스터의 **VM**이 사용할 수 없도록 만들고자 할 수 있습니다. 대신 더 격리된 전송 영역에 보안 클러스터를 배치할 수 있습니다.
- **vSphere Distributed Switch(VDS 또는 DVS)**의 범위는 전송 영역 범위와 일치해야 합니다. 다중 클러스터 **VDS** 구성에서 전송 영역을 생성할 경우 선택된 **VDS**의 모든 클러스터가 전송 영역에 포함되어 있는지 확인하십시오. 이는 **VDS dvPortgroup**이 사용 가능한 모든 클러스터에서 **DLR**을 사용할 수 있는지 확인하는 것입니다.

다음 다이어그램에서는 **VDS** 경계에 맞게 정렬된 전송 영역을 보여줍니다.



이 모범 사례를 따르지 않는다면 VDS가 둘 이상의 호스트 클러스터에 걸쳐 있고 전송 영역에 이 클러스터 중 하나(또는 하위 집합)만 포함된 경우 이 전송 영역에 포함된 모든 논리적 스위치가 VDS 범위의 모든 클러스터 내 VM에 액세스할 수 있습니다. 즉, 전송 영역에서 논리적 스위치 범위를 클러스터의 하위 집합으로 제한할 수 없습니다. 이 논리적 스위치가 나중에 DLR에 연결할 경우 계층 3 문제를 방지하기 위해 전송 영역에 포함된 클러스터에만 라우터 인스턴스가 생성되는지 확인해야 합니다.

예를 들어 전송 영역이 VDS 경계에 맞춰지지 않은 경우 논리적 스위치의 범위(5001, 5002 및 5003) 및 이 논리적 스위치가 연결된 DLR 인스턴스가 연결 해제되기 때문에 Comp A 클러스터의 VM이 DLR 논리적 인터페이스(LIF)에 액세스할 수 없게 됩니다.



본 장은 다음 항목을 포함합니다.

- 전송 영역 추가
- 전송 영역 보기 및 편집
- 전송 영역 확장
- 전송 영역 축소
- CDL(Controller Disconnected Operation) 모드

전송 영역 추가

전송 영역은 논리적 스위치가 연결할 수 있는 호스트를 제어하며 하나 이상의 vSphere 클러스터를 포함할 수 있습니다. 전송 영역에서 클러스터를 지정하므로 특정 네트워크 사용에 참여할 수 있는 VM도 지정합니다. 범용 전송 영역은 크로스 vCenter NSX 환경에서 vSphere 클러스터로 확장될 수 있습니다.

크로스 vCenter NSX 환경에는 단 하나의 범용 전송 영역만 있을 수 있습니다.

사전 요구 사항

변경할 적합한 NSX Manager를 결정합니다.

- 독립 실행형 또는 단일 vCenter NSX 환경에는 NSX Manager가 하나만 있기 때문에 선택할 필요가 없습니다.
- 범용 개체는 기본 NSX Manager에서 관리해야 합니다.

- NSX Manager에 로컬인 개체는 NSX Manager에서 관리해야 합니다.
- 고급 연결 모드가 사용되도록 설정되지 않은 크로스 vCenter NSX 환경에서는 수정하려는 NSX Manager에 연결된 vCenter에서 구성을 변경해야 합니다.
- 고급 연결 모드의 크로스 vCenter NSX 환경에서는 모든 연결된 vCenter에서 원하는 NSX Manager의 구성을 변경할 수 있습니다. NSX Manager 드롭다운 메뉴에서 적절한 NSX Manager를 선택합니다.

절차

- 1 홈 > Networking & Security > 설치(Home > Networking & Security > Installation)로 이동하고 논리적 네트워크 준비(Logical Network Preparation) 탭을 선택합니다.
- 2 전송 영역(Transport Zones)을 클릭하고 새 전송 영역(New Transport Zone)(+) 아이콘을 클릭합니다.
- 3 (선택 사항) 범용 전송 영역을 추가하려면 이 개체를 범용 동기화하도록 표시(Mark this object for universal synchronization)를 선택합니다.
- 4 복제 모드를 선택합니다.
 - **멀티캐스트(Multicast):** 물리적 네트워크의 멀티캐스트 IP 주소가 제어부에 사용됩니다. 이 모드는 이전 버전의 VXLAN 배포에서 업그레이드하는 경우에만 권장됩니다. 물리적 네트워크에서 PIM/IGMP가 필요합니다.
 - **유니캐스트(Unicast):** 제어부가 NSX Controller에서 처리됩니다. 모든 유니캐스트 트래픽에서 최적화된 헤드엔드 복제를 사용합니다. 멀티캐스트 IP 주소 또는 특별한 네트워크 구성이 필요하지 않습니다.
 - **하이브리드(Hybrid):** 로컬 트래픽 복제를 물리적 네트워크(L2 멀티캐스트)로 오프로드합니다. 이 모드를 사용하려면 첫 번째 홉 스위치에서 IGMP 스누핑과 각 VTEP 서브넷의 IGMP 쿼리 발송기에 대한 액세스 권한이 필요하지만 PIM은 필요하지 않습니다. 첫 번째 홉 스위치에서 서브넷의 트래픽 복제를 처리합니다.

중요 범용 전송 영역을 생성하고 복제 모드로 하이브리드를 선택한 경우 사용한 멀티캐스트 주소가 환경의 NSX Manager에 할당된 다른 멀티캐스트 주소와 충돌하지 않는지 확인해야 합니다.

- 5 전송 영역에 추가할 클러스터를 선택합니다.

결과

Transport-Zone은 해당 영역이 생성된 NSX Manager에 로컬인 전송 영역입니다.

Universal-Transport-Zone은 크로스 vCenter NSX 환경의 모든 NSX Manager에서 사용 가능한 범용 전송 영역입니다.

Name	Description	Control Plane Mode	Logical Switches
Transport-Zone		Unicast	1
Universal-Transport-Zone		Unicast	4

다음에 수행할 작업

전송 영역을 추가한 경우 논리적 스위치를 추가할 수 있습니다.

범용 전송 영역을 추가한 경우 범용 논리적 스위치를 추가할 수 있습니다.

범용 전송 영역을 추가한 경우 보조 NSX Manager를 선택하고 해당 클러스터를 범용 전송 영역에 추가할 수 있습니다.

전송 영역 보기 및 편집

선택한 전송 영역의 논리적 네트워크, 전송 영역에 포함된 클러스터 및 해당 전송 영역의 제어부 모드를 확인할 수 있습니다.

절차

- 1 전송 영역에서 전송 영역을 두 번 클릭합니다.

요약 탭에 전송 영역의 이름과 설명뿐 아니라 해당 영역에 연결된 논리적 스위치의 수가 표시됩니다. 전송 영역 세부 정보에 전송 영역에 포함된 클러스터가 표시됩니다.

- 2 **전송 영역 세부 정보(Transport Zone Details)** 섹션에서 **설정 편집(Edit Settings)** 아이콘을 클릭하여 전송 영역의 이름, 설명 또는 제어부 모드를 편집합니다.

전송 영역 제어부 모드를 변경할 경우 **기존 논리적 스위치를 새 제어부 모드로 마이그레이션(Migrate existing Logical Switches to the new control plane mode)**을 선택하고 이 전송 영역에 연결된 기존 논리적 스위치에 대한 제어부 모드를 추가로 변경합니다. 이 확인란을 선택하지 않으면 편집 후에 이 전송 영역에 연결된 논리적 스위치에서만 새 제어부 모드가 설정됩니다.

- 3 **확인(OK)**을 클릭합니다.


전송 영역 확장

전송 영역에 클러스터를 추가할 수 있습니다. 새로 추가된 클러스터에서 모든 기존 전송 영역을 사용할 수 있게 됩니다.

사전 요구 사항

전송 영역에 추가하는 클러스터에는 네트워크 인프라가 설치되어 있으며 VXLAN이 구성되어 있어야 합니다. "NSX 설치 가이드"를 참조하십시오.


절차

- 1 [전송 영역]에서 전송 영역을 클릭합니다.
- 2 **클러스터 추가(Add Cluster)**() 아이콘을 클릭합니다.
- 3 전송 영역에서 추가할 클러스터를 선택하고 **확인(OK)**을 클릭합니다.

전송 영역 축소

전송 영역에서 클러스터를 제거할 수 있습니다. 축소된 범위에 따라 기존 전송 영역의 크기가 줄어듭니다.

절차

- 1 **전송 영역(Transport Zones)**에서 전송 영역을 두 번 클릭합니다.
- 2 **전송 영역 세부 정보(Transport Zones Details)**에서 **클러스터 제거(Remove Clusters)**() 아이콘을 클릭합니다.
- 3 제거할 클러스터를 선택합니다.
- 4 **확인(OK)**을 클릭합니다.

CDL(Controller Disconnected Operation) 모드

CDO(Controller Disconnected Operation) 모드에서는 호스트와 컨트롤러 간에 연결이 끊어져도 데이터부 연결이 영향을 받지 않습니다. 컨트롤러와의 일시적인 연결 문제를 피하려면 CDO 모드를 사용하도록 설정할 수 있습니다.

전송 영역에 연결된 각 호스트 클러스터에 대해 CDO 모드를 사용하도록 설정할 수 있습니다. CDO 모드는 기본적으로 사용되지 않도록 설정됩니다.

참고 CDO 모드를 사용하도록 설정하려면 시스템의 준비된 모든 호스트를 NSX 6.3.2 이상으로 업그레이드해야 합니다.

CDO 모드가 사용되도록 설정되면 NSX Manager는 모든 전송 영역에 대해 하나씩 특수한 CDO 논리적 스위치를 생성합니다. 특수한 CDO 논리적 스위치의 VNI(VXLAN 네트워크 식별자)는 다른 모든 논리적 스위치에서 고유합니다. CDO 모드가 사용되도록 설정되면 클러스터의 한 컨트롤러가 모든 전송 노드에서 보고된 모든 VTEP 정보를 수집한 후 업데이트된 VTEP 정보를 다른 모든 전송 노드에 복제합니다. 한 컨트롤러에 오류가 발생하면 새 컨트롤러가 새 마스터로 선택되어 해당 책임을 인계받으며 원래 마스터에 연결된 모든 전송 노드는 새 마스터로 마이그레이션되고 전송 노드와 컨트롤러 간에 데이터가 동기화됩니다.

전송 영역에 새 클러스터를 추가하면 NSX Manager는 CDO 모드 설정 및 VNI를 새로 추가한 호스트에 푸시합니다. 클러스터를 제거하면 NSX Manager는 호스트에서 VNI 데이터를 제거합니다.

전송 영역에서 CDO 모드를 사용하지 않도록 설정하면 NSX Manager는 컨트롤러에서 CDO 논리적 스위치를 제거합니다.

크로스 vCenter NSX 환경에서 로컬 전송 영역 또는 기본 NSX Manager에 대해 로컬 전송 영역은 없고 단일 범용 전송 영역이 있는 토폴로지에서만 CDO 모드를 사용하도록 설정할 수 있습니다. CDO 모드는 모든 보조 NSX Manager에 대한 범용 전송 영역에서 복제됩니다.

보조 NSX Manager에 대한 로컬 전송 영역에서 CDO 모드를 사용하도록 설정할 수 있습니다.

CDL(Controller Disconnected Operation) 모드 사용

전송 영역을 통해 각 호스트 클러스터에 대해 CDO(Controller Disconnected Operation) 모드를 사용하도록 설정할 수 있습니다. CDO 모드는 기본적으로 사용되지 않도록 설정됩니다.

사전 요구 사항

- 시스템의 준비된 모든 호스트가 NSX 6.3.2 이상으로 업그레이드되어 있는지 확인합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security > 논리적 네트워크 준비(Logical Network Preparation)**를 클릭한 후 **전송 영역(Transport Zones)**을 클릭합니다.
- 3 필요한 전송 영역을 선택하고 **작업(Actions)** 아이콘을 클릭합니다. 전송 영역을 마우스 오른쪽 버튼으로 클릭할 수도 있습니다.
- 4 **CDO 모드 사용(Enable CDO mode)**을 클릭합니다.

확인 대화상자가 나타납니다.

참고 크로스 vCenter NSX 환경에서 오류 메시지가 표시되면 다음 조건을 확인하십시오.

- 기본 NSX Manager: 동일한 분산 가상 스위치를 공유하지 않는 전송 영역에서만 CDO 모드를 사용하도록 설정할 수 있습니다. 범용 전송 영역 및 로컬 전송 영역이 동일한 분산 가상 스위치를 공유하는 경우 범용 전송 영역에서만 CDO 모드를 사용하도록 설정할 수 있습니다.
 - 보조 NSX Manager: CDO 모드는 모든 보조 NSX Manager의 범용 전송 영역에서 복제됩니다. 동일한 분산 가상 스위치를 공유하지 않는 경우 로컬 전송 영역에서 CDO 모드를 사용하도록 설정할 수 있습니다.
-

- 5 **예(Yes)**를 클릭합니다.

선택한 전송 영역에 대해 CDO 모드가 사용되도록 설정됩니다.

결과

[CDO 모드] 열에 **사용(Enabled)** 상태가 표시됩니다.

NSX Manager는 컨트롤러에서 CDO 논리적 스위치를 생성합니다.

CDL(Controller Disconnected Operation) 모드 사용 안 함

컨트롤러에 대한 연결 문제가 해결될 때 전송 영역을 통해 이미 사용하도록 설정된 CDO(Controller Disconnected Operation) 모드를 사용하지 않도록 설정할 수 있습니다. CDO 모드는 기본적으로 사용되지 않도록 설정된 상태로 유지됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.

- 2 **Networking & Security > 논리적 네트워크 준비(Logical Network Preparation)**를 클릭한 후 **전송 영역(Transport Zones)**을 클릭합니다.
- 3 CDO 모드를 사용하지 않도록 설정하려는 전송 영역을 선택하고 **작업(Actions)** 아이콘을 클릭합니다. 전송 영역을 마우스 오른쪽 버튼으로 클릭할 수도 있습니다.
- 4 **CDO 모드 사용 안 함(Disable CDO mode)**을 클릭합니다.
확인 대화상자가 나타납니다.
- 5 **예(Yes)**를 클릭합니다.
선택한 전송 영역에 대해 CDO 모드가 사용되지 않도록 설정됩니다.

결과

[CDO 모드] 열에 **사용 안 함(Disabled)** 상태가 표시됩니다.

NSX Manager는 컨트롤러에서 CDO 논리적 스위치를 제거합니다.

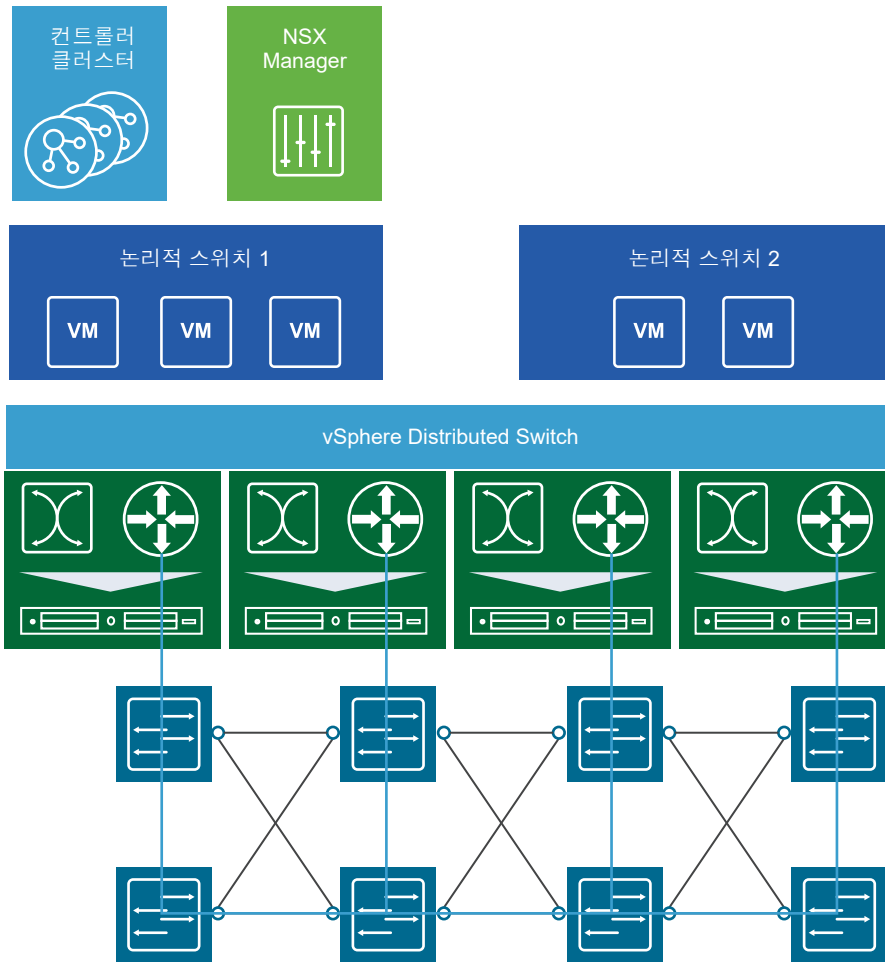
논리적 스위치

6

클라우드 배포 환경 또는 가상 데이터센터에는 여러 테넌트에 분산된 다양한 애플리케이션이 있습니다. 이러한 애플리케이션과 테넌트는 보안 및 장애 분리의 목적과 IP 주소 겹침 문제를 방지하기 위해 서로 분리되어야 합니다. NSX 논리적 스위치는 애플리케이션 또는 테넌트 가상 시스템을 논리적으로 연결할 수 있는 논리적 브로드캐스트 도메인 또는 세그먼트를 생성합니다. 이 기능은 배포 유연성과 속도를 향상시킬 뿐 아니라 물리적 계층 2 확장 또는 스페닝 트리 문제 없이 물리적 네트워크의 브로드캐스트 도메인(VLAN)이 가진 모든 특성도 제공합니다.

논리적 스위치는 대규모 계산 클러스터에서 자유롭게 배포하고 분산시킬 수 있습니다. 이러한 특성은 물리적 계층 2(VLAN) 경계의 제한 없이 데이터센터 내에서 가상 시스템의 이동성(vMotion)을 지원합니다. 소프트웨어의 논리적 스위치에 브로드캐스트 도메인이 포함되므로 물리적 인프라에서 MAC/FIB 테이블 제한을 처리할 필요가 없습니다.

논리적 스위치는 가상 시스템 트래픽을 캡슐화하고 물리적 IP 네트워크를 통해 전송하는 고유한 VXLAN에 매핑됩니다.



NSX Controller는 네트워크 내의 모든 논리적 스위치에 대한 중앙 제어 지점이며 모든 가상 시스템, 호스트, 논리적 스위치 및 **VXLAN**에 대한 정보를 유지합니다. 이 컨트롤러는 두 가지 새로운 논리적 스위치 제어부 모드인 유니캐스트와 하이브리드를 지원합니다. 이 두 모드는 **NSX**를 물리적 네트워크에서 분리합니다. 따라서 **VXLAN**은 더 이상 물리적 네트워크가 논리적 스위치 내의 **BUM**(브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트) 트래픽을 처리하기 위한 멀티캐스트를 지원하도록 요구하지 않습니다. 유니캐스트 모드에서는 모든 **BUM** 트래픽을 호스트에서 로컬로 복제하므로 물리적 네트워크 구성이 필요 없습니다. 하이브리드 모드에서는 성능 개선을 위해 일부 **BUM** 트래픽 복제가 첫 번째 홉 물리적 스위치로 오프로드됩니다. 이 모드에서는 첫 번째 홉 물리적 스위치에서 **IGMP** 스누핑을 설정해야 합니다. 논리적 스위치 내의 가상 시스템은 **IPv6** 및 멀티캐스트를 비롯한 모든 트래픽 유형을 사용하고 전송할 수 있습니다.

L2 브리지를 추가하여 논리적 스위치를 물리적 디바이스로 확장할 수 있습니다. [장 8 L2 브리지](#)를 참조하십시오.

논리적 스위치를 관리하려면 슈퍼 관리자 또는 엔터프라이즈 관리자 역할 사용 권한이 있어야 합니다.

본 장은 다음 항목을 포함합니다.

- [논리적 스위치 추가](#)
- [논리적 스위치에 가상 시스템 연결](#)

- 논리적 스위치 연결 테스트
- 논리적 스위치에서 스푸핑 방지
- 논리적 스위치 편집
- 논리적 스위치 시나리오

논리적 스위치 추가

사전 요구 사항

- 논리적 스위치를 구성 및 관리하려면 슈퍼 관리자 또는 엔터프라이즈 관리자 역할 사용 권한이 있어야 합니다.
- VXLAN UDP 포트가 방화벽 규칙에서 열려 있습니다(해당하는 경우). VXLAN UDP 포트는 API를 통해 구성할 수 있습니다.
- 물리적 인프라 MTU는 가상 시스템 vNIC의 MTU보다 50바이트 이상 큼니다.
- vCenter Server 런타임 설정에서 각 vCenter Server의 관리 IP 주소를 설정합니다. "vCenter Server 및 호스트 관리"를 참조하십시오.
- VMKNics를 위한 IP 할당에 DHCP를 사용할 경우 VXLAN 전송 VLAN에서 DHCP를 사용할 수 있습니다.
- 일치하는 Distributed Virtual Switch 유형(벤더 등) 및 버전이 지정한 전송 영역에서 사용됩니다. 스위치 종류가 다르면 논리적 스위치에서 정의되지 않은 동작이 발생할 수 있습니다.
- 적절한 LACP 팀 구성 정책을 구성했고 물리적 NIC를 포트에 연결했습니다. 팀 구성 모드에 대한 자세한 내용은 VMware vSphere 설명서를 참조하십시오.
- LACP(Link Aggregation Control Protocol)에 대해 5-튜플 해시 분산을 사용하도록 설정합니다.
- LACP를 사용할 모든 호스트에 대해 별도의 LACP 포트 채널이 분산 가상 스위치에 존재하는지 확인합니다.
- 멀티캐스트 모드의 경우 VXLAN 트래픽이 통과 라우터일 경우 멀티캐스트 라우팅이 사용하도록 설정되어 있습니다. 네트워크 관리자로부터 멀티캐스트 주소 범위를 얻었습니다.
- ESXi 호스트가 컨트롤러와 통신할 수 있도록 방화벽에서 포트 1234(기본 컨트롤러 수신 포트)가 열려 있습니다.
- (권장) 멀티캐스트 및 하이브리드 모드의 경우 VXLAN 참가 호스트가 연결되어 있는 L2 스위치에서 IGMP 스누핑을 사용하도록 설정했습니다. L2에서 IGMP 스누핑이 사용하도록 설정된 경우 멀티캐스트가 활성화된 네트워크에 연결한 상태에서 IGMP 쿼리 발송기를 라우터 또는 L3 스위치에서 사용하도록 설정해야 합니다.

논리적 스위치 추가

NSX 논리적 스위치는 기본 하드웨어와 완전히 분리된 가상 환경에서 스위칭 기능(유니캐스트, 멀티캐스트, 브로드캐스트)을 재현합니다. 논리적 스위치는 가상 시스템을 연결할 수 있는 네트워크 연결을 제공한다는 점에서 VLAN과 비슷합니다. 논리적 스위치는 단일 vCenter NSX 배포에 로컬입니다. 크로스 vCenter NSX 배포에서는 모든 vCenter를 포함할 수 있는 범용 논리적 스위치를 생성할 수 있습니다. 새 스위치가 논리적 스위치인지 범용 논리적 스위치인지 여부는 전송 영역 유형에 따라 결정됩니다.

논리적 스위치를 생성할 때 전송 영역 및 복제 모드를 선택하는 것 외에, 2가지 옵션인 IP 검색 및 MAC 학습을 구성합니다.

IP 검색은 개별 VXLAN 세그먼트 내에서, 즉 동일한 논리적 스위치에 연결된 VM 간에 ARP 트래픽 플러딩을 최소화합니다. IP 검색은 기본적으로 사용하도록 설정되어 있습니다.

참고 범용 논리적 스위치를 생성할 때는 IP 검색을 사용하지 않도록 설정할 수 없습니다. 범용 논리적 스위치가 생성된 후에 API를 통해 IP 검색을 사용하지 않도록 설정할 수 있습니다. 이 설정은 각 NSX Manager에서 별도로 관리됩니다. "NSX API 가이드"를 참조하십시오.

MAC 학습은 각 vNIC에 VLAN/MAC 쌍 학습 테이블을 구성합니다. 이 테이블은 dvfilter 데이터의 일부로 저장됩니다. vMotion 동안 dvfilter는 새 위치에서 테이블을 저장하고 복원합니다. 그런 다음 스위치가 테이블의 모든 VLAN/MAC 항목에 대해 RARP를 발급합니다. VLAN을 트렁킹하는 가상 NIC를 사용하는 경우 MAC 학습을 사용하도록 설정하는 것이 좋습니다.

사전 요구 사항

표 6-1. 논리적 스위치 또는 범용 논리적 스위치를 생성하기 위한 선행 조건

논리적 스위치	범용 논리적 스위치
<ul style="list-style-type: none"> ■ vSphere Distributed Switch를 구성해야 합니다. ■ NSX Manager가 설치되어야 합니다. ■ 컨트롤러를 배포해야 합니다. ■ NSX용 호스트 클러스터를 준비해야 합니다. ■ VXLAN을 구성해야 합니다. ■ 세그먼트 ID 풀을 구성해야 합니다. ■ 전송 영역을 생성해야 합니다. 	<ul style="list-style-type: none"> ■ vSphere Distributed Switch를 구성해야 합니다. ■ NSX Manager가 설치되어야 합니다. ■ 컨트롤러를 배포해야 합니다. ■ NSX용 호스트 클러스터를 준비해야 합니다. ■ VXLAN을 구성해야 합니다. ■ 기본 NSX Manager가 할당되어 있어야 합니다. ■ 범용 세그먼트 ID 풀이 구성되어 있어야 합니다. ■ 범용 전송 영역이 생성되어 있어야 합니다.

변경할 적합한 NSX Manager를 결정합니다.

- 독립 실행형 또는 단일 vCenter NSX 환경에는 NSX Manager가 하나만 있기 때문에 선택할 필요가 없습니다.
- 범용 개체는 기본 NSX Manager에서 관리해야 합니다.
- NSX Manager에 로컬인 개체는 NSX Manager에서 관리해야 합니다.
- 고급 연결 모드가 사용되도록 설정되지 않은 크로스 vCenter NSX 환경에서는 수정하려는 NSX Manager에 연결된 vCenter에서 구성을 변경해야 합니다.

- 고급 연결 모드의 크로스 vCenter NSX 환경에서는 모든 연결된 vCenter에서 원하는 NSX Manager의 구성을 변경할 수 있습니다. NSX Manager 드롭다운 메뉴에서 적절한 NSX Manager를 선택합니다.

절차

- 1 홈 > 네트워킹 및 보안 > 논리적 스위치(Home > Networking & Security > Logical Switches)로 이동합니다.
- 2 논리적 스위치를 생성할 NSX Manager를 선택합니다. 범용 논리적 스위치를 생성하려면 기본 NSX Manager를 선택해야 합니다.
- 3 새 논리적 스위치(New Logical Switch)(+)를 클릭합니다.
- 4 논리적 스위치의 이름과 설명(선택 사항)을 입력합니다.
- 5 논리적 스위치를 생성할 전송 영역을 선택합니다. 범용 전송 영역을 선택하면 범용 논리적 스위치가 생성됩니다.

기본적으로 논리적 스위치는 전송 영역에서 제어부 복제 모드를 상속합니다. 이 모드를 다른 사용 가능한 모드 중 하나로 변경할 수 있습니다. 사용 가능한 모드는 유니캐스트, 하이브리드 및 멀티캐스트입니다.







범용 논리적 스위치를 생성하고 복제 모드로 하이브리드를 선택한 경우 사용한 멀티캐스트 주소가 크로스 vCenter NSX 환경의 NSX Manager에 할당된 다른 멀티캐스트 주소와 충돌하지 않는지 확인해야 합니다.
- 6 (선택 사항) ARP 억제를 사용하도록 설정하려면 IP 검색 사용(Enable IP Discovery)을 클릭합니다.
- 7 (선택 사항) MAC 학습 사용(Enable MAC learning)을 클릭합니다.

예제: 논리적 스위치 및 범용 논리적 스위치

App은 전송 영역에 연결된 논리적 스위치입니다. 해당 스위치가 생성된 NSX Manager에서만 사용할 수 있습니다.

Universal-App은 범용 전송 영역에 연결된 범용 논리적 스위치입니다. 크로스 vCenter NSX 환경의 모든 NSX Manager에서 사용할 수 있습니다.

논리적 스위치와 범용 논리적 스위치는 여러 세그먼트 ID 풀의 세그먼트 ID를 가집니다.

     				
Virtual Wire ID	Segment ID	Name	Status	Transport Zone
virtualwire-1	5000	App	✓ Normal	Transport-Zone
universalwire-2	900000	Universal-App	✓ Normal	Universal-Transport-Zone

다음에 수행할 작업

논리적 스위치 또는 범용 논리적 스위치에 VM을 추가합니다.

다른 논리적 스위치에 연결된 VM 간 연결을 사용하도록 설정하려면 논리적 라우터를 생성하여 논리적 스위치에 연결합니다.


다른 범용 논리적 스위치에 연결된 VM 간 연결을 사용하도록 설정하려면 범용 논리적 라우터를 생성하여 범용 논리적 스위치에 연결합니다.

논리적 스위치를 NSX Edge에 연결

논리적 스위치를 NSX Edge 서비스 게이트웨이 또는 NSX Edge 논리적 라우터에 연결하면 동-서 트래픽 라우팅(논리적 스위치 간) 또는 외부 환경에 대한 북-남 트래픽 라우팅을 제공하거나 고급 서비스를 제공할 수 있습니다.

절차

절차

- 1 논리적 스위치에서 NSX Edge를 연결할 논리적 스위치를 선택합니다.
- 2 **Edge 연결(Connect an Edge)** () 아이콘을 클릭합니다.
- 3 논리적 스위치를 연결할 NSX Edge를 선택하고 **다음(Next)**을 클릭합니다.
- 4 논리적 스위치에 연결할 인터페이스를 선택하고 **다음(Next)**을 클릭합니다.
논리적 네트워크는 일반적으로 내부 인터페이스에 연결됩니다.
- 5 [NSX Edge 인터페이스 편집] 페이지에서 NSX Edge 인터페이스의 이름을 입력합니다.
- 6 **내부(Internal)** 또는 **업링크(Uplink)**를 클릭하여 내부 인터페이스인지, 업링크 인터페이스인지를 나타냅니다.
- 7 인터페이스의 연결 상태를 선택합니다.
- 8 논리적 스위치를 연결할 NSX Edge에 대해 **수동 HA 구성(Manual HA Configuration)**이 선택되어 있으면 두 개의 관리 IP 주소를 CIDR 형식으로 지정합니다.
- 9 필요한 경우 기본 MTU를 편집합니다.
- 10 **다음(Next)**을 클릭합니다.
- 11 NSX Edge 연결 세부 정보를 검토하고 **완료(Finish)**를 클릭합니다.


논리적 스위치에서 서비스 배포

논리적 스위치에서 타사 서비스를 배포할 수 있습니다.

사전 요구 사항

하나 이상의 타사 가상 장치가 인프라에 설치되어 있어야 합니다.

절차


- 1 **논리적 스위치(Logical Switches)**에서 서비스를 배포할 논리적 스위치를 선택합니다.
- 2 **서비스 프로파일 추가(Add Service Profile)**() 아이콘을 클릭합니다.

- 3 적용할 서비스 및 서비스 프로파일을 선택합니다.
- 4 **확인(OK)**을 클릭합니다.

논리적 스위치에 가상 시스템 연결

가상 시스템을 논리적 스위치 또는 범용 논리적 스위치에 연결할 수 있습니다.

절차

- 1 **논리적 스위치(Logical Switches)**에서 가상 시스템을 추가할 논리적 스위치를 선택합니다.
- 2 **가상 시스템 추가(Add Virtual Machine)**() 아이콘을 클릭합니다.
- 3 논리적 스위치에 추가할 가상 시스템을 선택합니다.
- 4 연결할 vNIC를 선택합니다.
- 5 **다음(Next)**을 클릭합니다.
- 6 선택한 vNIC를 검토합니다.
- 7 **완료(Finish)**를 클릭합니다.

논리적 스위치 연결 테스트

ping 테스트는 VXLAN 전송 네트워크에 있는 두 호스트가 서로 연결할 수 있는지 확인합니다.

- 1 **논리적 스위치(Logical Switches)**에서 **이름(Name)** 열의 테스트하고 싶은 논리적 스위치를 두 번 클릭합니다.
- 2 **모니터(Monitor)** 탭을 클릭합니다.
- 3 **호스트(Hosts)** 탭을 클릭합니다.
- 4 소스 호스트 섹션에서 **찾아보기(Browse)**를 클릭합니다. 호스트 선택 대화상자에서 대상 호스트를 선택합니다.
- 5 테스트 패킷의 크기를 선택합니다.

VXLAN 표준 크기는 조각화를 수행하지 않을 경우 1,550바이트이며 물리적 인프라 MTU와 일치해야 합니다. 이 경우 NSX를 통해 연결을 확인하고 인프라가 VXLAN 트래픽을 수용할 준비가 되었는지 확인할 수 있습니다.

최소 패킷 크기는 조각화를 허용합니다. 따라서 패킷 크기가 최소화된 상태에서 NSX를 통해 연결만 확인할 수 있고 인프라가 더 큰 프레임 크기를 수용할 준비가 되었는지는 확인할 수 없습니다.

- 6 대상 호스트 섹션에서 **찾아보기(Browse)**를 클릭합니다. 호스트 선택 대화상자에서 대상 호스트를 선택합니다.
- 7 **테스트 시작(Start Test)**을 클릭합니다.

호스트 간 ping 테스트 결과가 표시됩니다.

논리적 스위치에서 스푸핑 방지

vCenter Server와 동기화되면 NSX Manager가 각 가상 시스템의 VMware Tools 또는 IP 검색에서(IP 검색을 사용하도록 설정한 경우) 모든 vCenter 게스트 가상 시스템의 IP 주소를 수집합니다. NSX는 VMware Tools 또는 IP 검색에서 제공한 IP 주소를 모두 신뢰하지는 않습니다. 가상 시스템이 손상된 경우 IP 주소가 스푸핑되고 악의적인 전송이 방화벽 정책을 우회할 수 있습니다.

SpoofGuard를 사용하면 VMware Tools 또는 IP 검색에서 보고하는 IP 주소를 인증하고, 필요한 경우 이를 변경하여 스푸핑을 방지할 수 있습니다. SpoofGuard는 VMX 파일 및 vSphere SDK에서 수집된 가상 시스템의 MAC 주소를 기본적으로 신뢰합니다. 방화벽 규칙과 별도로 작동하므로, SpoofGuard를 사용하여 스푸핑된 것으로 확인된 트래픽을 차단할 수 있습니다.

자세한 내용은 [장 13 SpoofGuard 사용](#) 항목을 참조하십시오.

논리적 스위치 편집

논리적 스위치의 이름, 설명 및 제어부 모드를 편집할 수 있습니다.

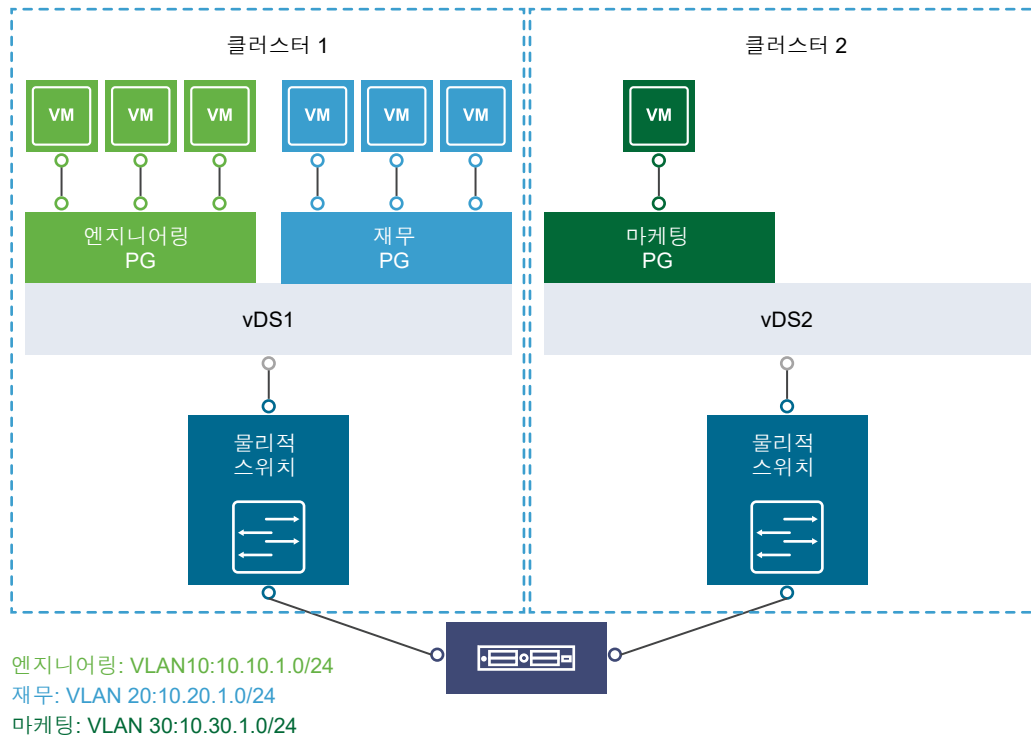
절차

- 1 **논리적 스위치(Logical Switches)**에서 편집할 논리적 스위치를 선택합니다.
- 2 **편집(Edit)** 아이콘을 클릭합니다.
- 3 필요한 내용을 변경합니다.
- 4 **확인(OK)**을 클릭합니다.

논리적 스위치 시나리오

이 시나리오에서는 ACME Enterprise라는 회사가 데이터센터 ACME_Datacenter의 두 클러스터에 여러 ESXi 호스트를 구축하는 경우를 보여 줍니다. 엔지니어링 부서(포트 그룹 Engineering PG)와 재무 부서(포트 그룹 Finance PG)는 클러스터 1에 있습니다. 마케팅 부서(Marketing PG)는 클러스터 2에 있습니다. 두 클러스터 모두 단일 vCenter Server에서 관리됩니다.

그림 6-1. 논리적 스위치를 구현하기 전의 ACME Enterprise 네트워크

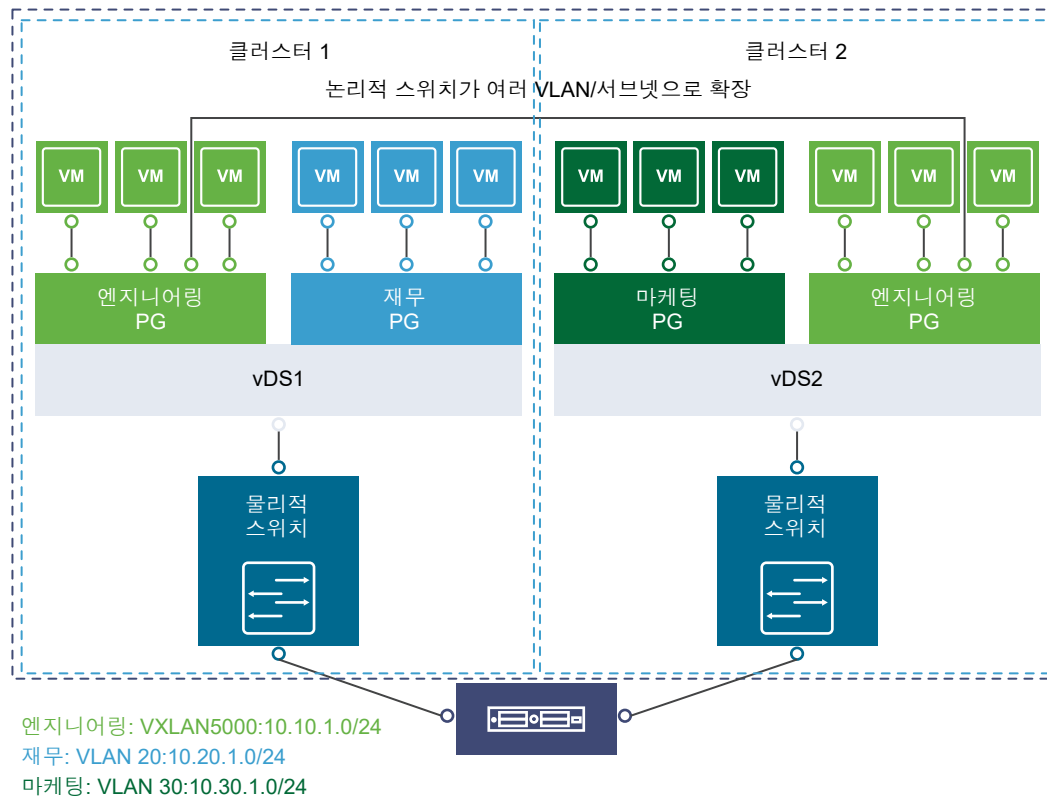


ACME의 클러스터 1에 있는 컴퓨팅 공간은 부족한 반면 클러스터 2는 충분히 활용되지 않고 있습니다. ACME 네트워크 감독자가 클러스터에서 모두 엔지니어링 부서에 속한 가상 시스템이 서로 통신할 수 있는 방식으로 엔지니어링 부서를 클러스터 2로 확장할 방법을 찾도록 ACME 가상화 관리자 John에게 요청합니다. 이렇게 하면 ACME의 L2 계층을 확장하여 두 클러스터의 컴퓨팅 용량을 모두 활용할 수 있습니다.

관리자 John이 기존 방식으로 이 작업을 수행할 경우 두 클러스터가 동일한 L2 도메인에 있을 수 있도록 특수한 방식으로 각각의 VLAN을 연결해야 합니다. 이 경우 ACME는 트래픽을 구분하기 위해 물리적 디바이스를 새로 구매해야 할뿐더러 무분별한 VLAN 확장, 네트워크 루프, 관리 부담 등의 문제를 일으킬 수도 있습니다.

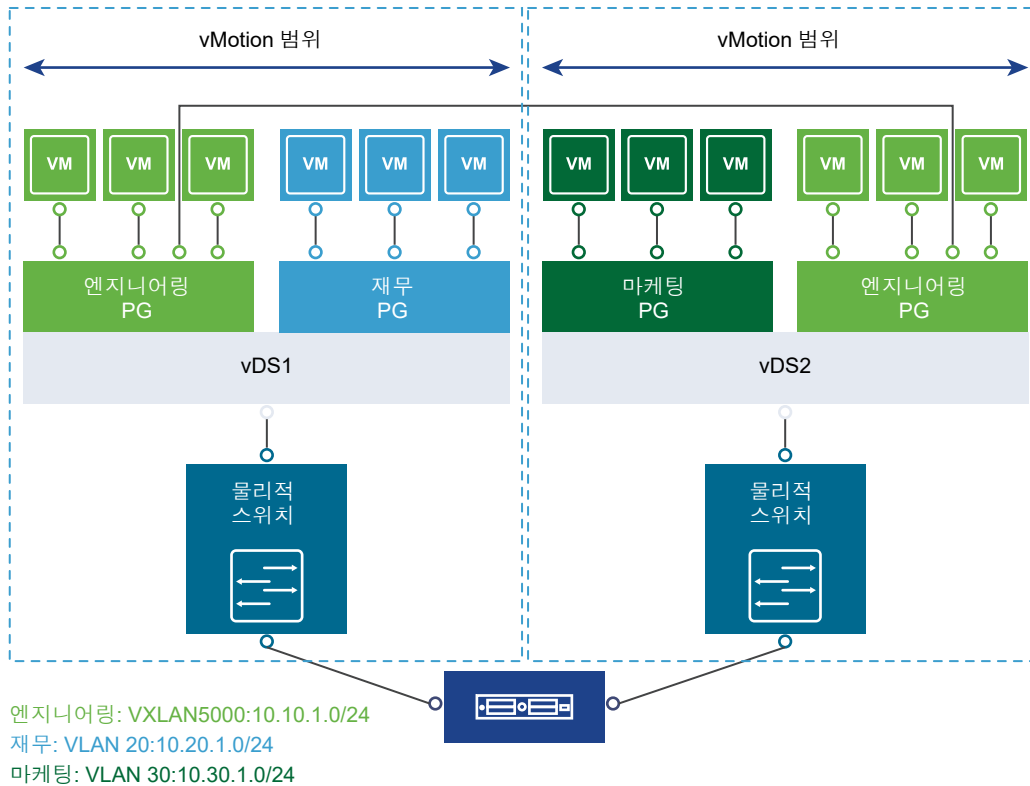
관리자 John은 이전에 보았던 VMworld의 논리적 네트워크 데모를 기억하고는 NSX를 평가하기로 결정합니다. 평가 결과, dvSwitch1 및 dvSwitch2 간에 논리적 스위치를 구축하면 ACME의 L2 계층을 확장할 수 있다는 것을 확인했습니다. John은 NSX Controller를 활용할 수 있으므로 ACME의 물리적 인프라를 변경할 필요가 없습니다. 이는 NSX가 기존 IP 네트워크 상에서 작동하기 때문입니다.

그림 6-2. ACME Enterprise에서 논리적 스위치 구현



관리자 John은 두 클러스터 간에 논리적 스위치를 구축한 후, 동일한 논리적 스위치에 연결된 상태를 유지 하면서 한 클러스터의 가상 시스템을 다른 클러스터로 vMotion할 수 있습니다.

그림 6-3. 논리적 네트워크 상의 vMotion



관리자 John이 ACME Enterprise에서 논리적 네트워크를 구축할 때 수행한 단계를 살펴보겠습니다.

관리자 John이 NSX Manager에 세그먼트 ID 풀 및 멀티캐스트 주소 범위 할당

관리자 John은 할당받은 세그먼트 ID 풀을 지정해야 ABC사의 네트워크 트래픽을 분리할 수 있습니다.

사전 요구 사항

- 1 관리자 John은 dvSwitch1 및 dvSwitch2가 VMware Distributed Switch 버전 5.5인지 확인합니다.
- 2 관리자 John은 vCenter Server에 대해 관리 IP 주소를 설정합니다.
 - a 먼저, **관리(Administration) > vCenter Server 설정(vCenter Server Settings) > 런타임 설정(Runtime Settings)**을 선택합니다.
 - b 그런 다음 vCenter Server 관리 IP에 **10.115.198.165**를 입력합니다.
 - c **확인(OK)**을 클릭합니다.
- 3 관리자 John은 클러스터 1 및 클러스터 2에 네트워크 가상화 구성 요소를 설치합니다. 자세한 내용은 "NSX 설치 가이드"를 참조하십시오.
- 4 관리자 John은 ACME의 NSX Manager 관리자로부터 세그먼트 ID 풀(5000 - 5250)을 얻습니다. 관리자 John은 NSX Controller를 이용 중이므로 물리적 네트워크에 멀티캐스트가 필요하지 않습니다.

- 5 관리자 John은 IP 풀의 정적 IP 주소를 VXLAN VTEP에 할당할 수 있도록 IP 풀을 생성합니다. [IP 풀 추가](#) 항목을 참조하십시오.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > 설치(Installation)**를 클릭합니다.
- 2 **논리적 네트워크 준비(Logical Network Preparation)** 탭을 클릭하고 **세그먼트 ID(Segment ID)**를 클릭합니다.
- 3 **편집(Edit)**을 클릭합니다.
- 4 세그먼트 ID 풀에 **5000 - 5250**을 입력합니다.
- 5 **멀티캐스트 주소 지정 사용(Enable multicast addressing)**을 선택하지 마십시오.
- 6 **확인(OK)**을 클릭합니다.

관리자 John이 VXLAN 전송 매개 변수 구성

관리자 John이 각각 vDS에 매핑할 클러스터 1과 클러스터 2에서 VXLAN을 구성합니다. 클러스터를 스위치에 매핑하면 해당 클러스터 내의 각 호스트가 논리적 스위치를 사용하도록 설정됩니다.

절차

- 1 **호스트 준비(Host Preparation)** 탭을 클릭합니다.
- 2 클러스터 1의 경우 VXLAN 열에서 **구성(Configure)**을 선택합니다.
- 3 VXLAN 네트워킹 구성 대화상자에서 dvSwitch1을 클러스터의 가상 Distributed Switch로 선택합니다.
- 4 ACME 전송 VLAN으로 사용할 dvSwitch1에 대해 **10**을 입력합니다.
- 5 전송 특성 지정 섹션에서 dvSwitch1의 MTU(최대 전송 단위)로 **1600**을 그대로 유지합니다.
MTU는 한 패킷이 작은 패킷으로 나뉘기 전에 해당 패킷에서 전송될 수 있는 최대 데이터 양입니다. 관리자 John은 VXLAN 논리적 스위치 트래픽 프레임이 캡슐화되어 크기가 약간 더 크기 때문에 각 스위치의 MTU를 1550 이상으로 설정해야 한다는 것을 알고 있습니다.
- 6 **VMKNic IP 주소 지정(VMKNic IP Addressing)**에서 **IP 풀 사용(Use IP Pool)**을 선택하고 IP 풀을 선택합니다.
- 7 **VMKNic 팀 구성 정책(VMKNic Teaming Policy)**에 대해 **페일오버(Failover)**를 선택합니다.
관리자 John은 논리적 스위치의 성능을 정상 조건과 장애 조건에서 동일하게 유지하여 네트워크에서 서비스 품질을 유지하고자 합니다. 따라서 팀 구성 정책으로 페일오버를 선택합니다.
- 8 **추가(Add)**를 클릭합니다.
- 9 4~8단계를 반복하여 클러스터 2에서 VXLAN을 구성합니다.

결과

관리자 John이 클러스터 1과 클러스터 2를 적절한 스위치에 매핑하면 논리적 스위치에 사용할 수 있도록 해당 클러스터의 호스트가 다음과 같이 준비됩니다.

- 1 VXLAN 커널 모듈과 vmknic가 클러스터 1 및 클러스터 2의 각 호스트에 추가됩니다.
- 2 논리적 스위치와 연결된 vSwitch에 특수 dvPortGroup이 생성되고 VMKNic가 이 그룹에 연결됩니다.

관리자 John이 전송 영역 추가

논리적 네트워크를 지원하는 물리적 네트워크를 **transport zone**이라고 합니다. 전송 영역은 가상화 네트워크가 확장한 컴퓨팅 범위입니다.

절차

- 1 **논리적 네트워크 준비(Logical Network Preparation)**를 클릭하고 **전송 영역(Transport Zones)**을 클릭합니다.
- 2 **새 전송 영역(New Transport Zone)** 아이콘을 클릭합니다.
- 3 이름에 **ACME 영역(ACME Zone)**을 입력합니다.
- 4 설명에 **ACME의 클러스터를 포함하는 영역(Zone containing ACME's clusters)**을 입력합니다.
- 5 클러스터 1과 클러스터 2를 전송 영역에 추가합니다.
- 6 **제어부 모드(Control Plane Mode)**에서 **유니캐스트(Unicast)**를 선택합니다.
- 7 **확인(OK)**을 클릭합니다.

관리자 John이 논리적 스위치 생성

관리자 John은 VXLAN 전송 매개 변수를 구성했으므로 논리적 스위치를 생성할 준비가 되었습니다.

절차

- 1 **논리적 스위치(Logical Switches)**를 클릭한 다음 **새 논리적 네트워크(New Logical Network)** 아이콘을 클릭합니다.
- 2 이름에 **ACME 논리적 네트워크**를 입력합니다.
- 3 설명에 **클러스터 2로 ACME Engineering 네트워크를 확장하기 위한 논리적 네트워크**를 입력합니다.
- 4 **전송 영역(Transport Zone)**에서 ACME 영역을 선택합니다.
- 5 **확인(OK)**을 클릭합니다.

NSX가 dvSwitch1과 dvSwitch2 간의 L2 연결을 제공하는 논리적 스위치를 생성합니다.

다음에 수행할 작업

이제 관리자 John은 ACME의 운영 가상 시스템을 논리적 스위치에 연결하고 논리적 스위치를 NSX Edge Services Gateway나 논리적 라우터에 연결할 수 있습니다.

하드웨어 게이트웨이 구성

7

하드웨어 게이트웨이 구성은 물리적 네트워크를 가상 네트워크에 매핑합니다. 이 매핑 구성을 통해 **NSX**는 **OVSDB(Open vSwitch Database)**를 사용할 수 있게 됩니다.

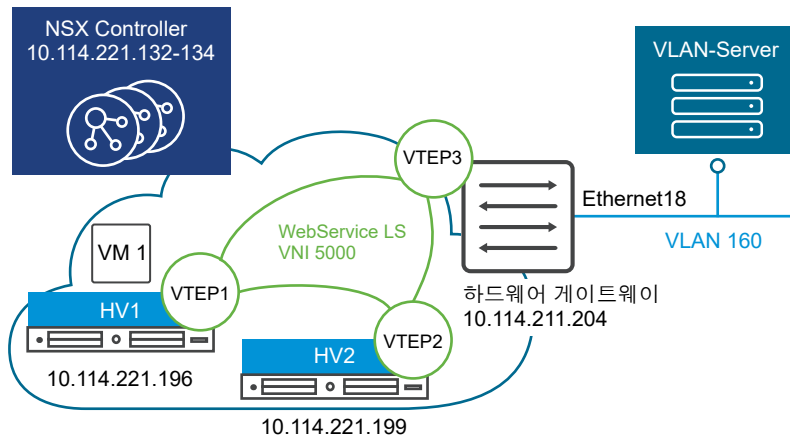
OVSDB 데이터베이스에는 물리적 하드웨어 및 가상 네트워크에 대한 정보가 포함되어 있습니다. 벤더 하드웨어는 데이터베이스 서버를 호스팅합니다.

NSX 논리적 네트워크의 하드웨어 게이트웨이 스위치는 **VXLAN** 터널을 종료합니다. 가상 네트워크의 경우 하드웨어 게이트웨이 스위치는 하드웨어 **VTEP**라고 합니다. **VTEP**에 대한 자세한 내용은 "**NSX 설치**" 가이드 및 "**NSX 네트워크 가상화 설계**" 가이드를 참조하십시오.

하드웨어 게이트웨이가 있는 최소 토폴로지에는 다음 구성 요소가 포함됩니다.

- 물리적 서버
- 하드웨어 게이트웨이 스위치(**L2** 포트)
- IP 네트워크
- VM이 있는 2개의 복제 클러스터를 포함하여 최소 4개의 하이퍼바이저
- 3개 이상의 노드가 있는 컨트롤러 클러스터

하드웨어 게이트웨이가 있는 샘플 토폴로지는 2개의 하이퍼바이저로 **HV1** 및 **HV2**를 표시합니다. **VM1** 가상 시스템은 **HV1**에 있습니다. **VTEP1**은 **HV1**에 있고, **VTEP2**는 **HV2**에 있으며 **VTEP3**는 하드웨어 게이트웨이에 있습니다. 하드웨어 게이트웨이는 동일한 서브넷 **221**에 있는 두 하이퍼바이저와 달리 다른 서브넷 **211**에 있습니다.



하드웨어 게이트웨이 기본 구성에는 다음 구성 요소 중 하나가 포함될 수 있습니다.

- 단일 스위치
- 다른 IP 주소를 갖는 다중 물리적 버스 스위치
- 다중 스위치를 포함하는 하드웨어 스위치 컨트롤러

NSX Controller는 포트 6640의 해당 IP 주소를 사용하여 하드웨어 게이트웨이와 통신합니다. 이 연결은 하드웨어 게이트웨이에서 **OVSDB** 트랜잭션을 주고받는 데 사용됩니다.

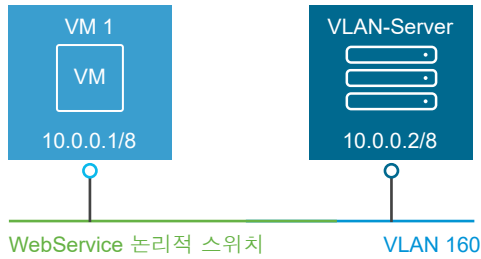
본 장은 다음 항목을 포함합니다.

- **시나리오: 하드웨어 게이트웨이 샘플 구성**

시나리오: 하드웨어 게이트웨이 샘플 구성

이 시나리오에서는 **NSX** 배포에서 하드웨어 게이트웨이 스위치를 구성하는 데 사용되는 일반적인 작업에 대해 설명합니다. 작업 순서에서는 하드웨어 게이트웨이를 사용하여 가상 시스템 **VM1**을 물리적 서버에 연결하고, **WebService** 논리적 스위치를 **VLAN-Server** **VLAN 160**에 연결하는 방법이 제공됩니다.

샘플 토폴로지는 가상 시스템 **VM1** 및 **VLAN-Server**가 서브넷 10에서 IP 주소로 구성되어 있음을 나타냅니다. **VM1**은 **WebService** 논리적 스위치에 연결됩니다. **VLAN-Server**는 물리적 서버의 **VLAN 160**에 연결됩니다.



중요 크로스 vCenter NSX 환경에서 하드웨어 게이트웨이 스위치 구성은 기본 NSX Manager에서만 지원됩니다. 하드웨어 게이트웨이 스위치는 범용이 아닌 논리적 스위치에 연결되어야 합니다. 보조 NSX Manager에서는 하드웨어 게이트웨이 구성이 지원되지 않습니다.

사전 요구 사항

- 물리적 네트워크 요구 사항을 충족하려면 벤더 설명서를 읽어보십시오.
- 하드웨어 게이트웨이 구성에 대한 NSX 시스템 및 하드웨어 요구 사항을 충족하는지 확인합니다. [장 1 NSX의 시스템 요구 사항](#)을 참조하십시오.
- 논리적 네트워크가 제대로 설정되어 있는지 확인합니다. "NSX 설치" 가이드를 참조하십시오.
- VXLAN의 전송 매개 변수 매핑이 정확한지 확인합니다. "NSX 설치" 가이드를 참조하십시오.
- 하드웨어 게이트웨이에 대한 벤더 인증서를 검색합니다.
- VXLAN 포트 값이 4789로 설정되어 있는지 확인합니다. [VXLAN 포트 변경](#)을 참조하십시오.

절차

1 복제 클러스터 설정

복제 클러스터는 하드웨어 게이트웨이에서 보낸 트래픽을 전달하는 하이퍼바이저 집합입니다. 트래픽은 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트 트래픽일 수 있습니다.

2 하드웨어 게이트웨이를 NSX Controller에 연결

하드웨어 게이트웨이를 NSX Controller에 연결하려면 ToR 물리적 스위치의 OVSDB 관리자 테이블을 구성해야 합니다.

3 하드웨어 게이트웨이 인증서 추가

구성이 작동하려면 하드웨어 디바이스에 하드웨어 게이트웨이 인증서를 추가해야 합니다.

4 논리적 스위치를 물리적 스위치에 바인딩

가상 시스템 VM1에 연결된 WebService 논리적 스위치는 동일한 서브넷의 하드웨어 게이트웨이와 통신해야 합니다.

복제 클러스터 설정

복제 클러스터는 하드웨어 게이트웨이에서 보낸 트래픽을 전달하는 하이퍼바이저 집합입니다. 트래픽은 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트 트래픽일 수 있습니다.

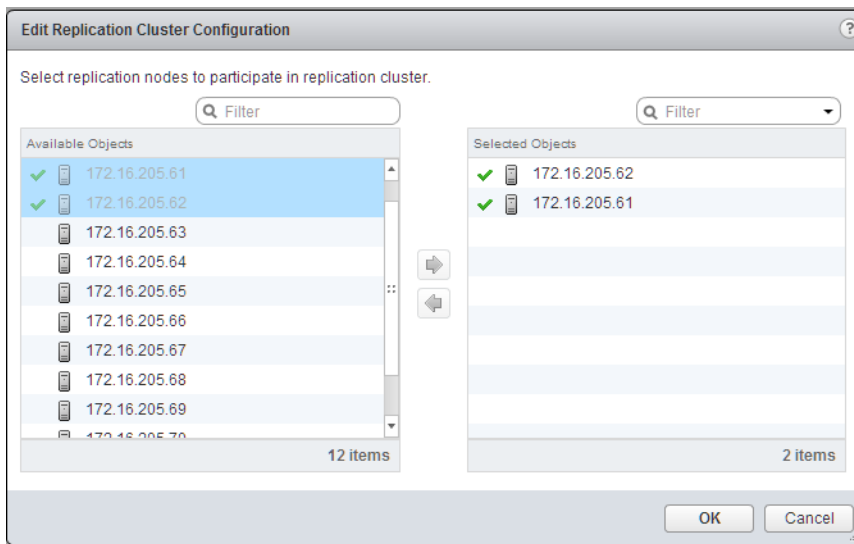
참고 복제 노드 및 하드웨어 게이트웨이 스위치를 포함하는 하이퍼바이저는 동일한 IP 서브넷에 있을 수 없습니다. 이 제한은 대부분의 하드웨어 게이트웨이에 사용되는 칩셋의 제한 때문에 발생합니다. 모두 그런 것은 아니지만 대부분의 하드웨어 게이트웨이는 하드웨어 게이트웨이와 하이퍼바이저 간에 계층 3 언더레이 네트워크가 반드시 필요한 **Broadcom Trident II** 칩셋을 사용합니다.

사전 요구 사항

복제 노드로 제공할 하이퍼바이저가 사용 가능한지 확인합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security > 서비스 정의(Service Definitions)**를 선택합니다.
- 3 **하드웨어 디바이스(Hardware Devices)** 탭을 클릭합니다.
- 4 [복제 클러스터] 섹션의 **편집(Edit)**을 클릭하여 이 복제 클러스터에서 복제 노드로 제공할 하이퍼바이저를 선택합니다.
- 5 하이퍼바이저를 선택하고 파란색 화살표를 클릭합니다.



선택한 하이퍼바이저가 선택한 개체 열로 이동됩니다.

- 6 **확인(OK)**을 클릭합니다.

결과

복제 노드가 복제 클러스터에 추가됩니다. 하나 이상의 호스트가 복제 클러스터에 존재해야 합니다.

하드웨어 게이트웨이를 NSX Controller에 연결

하드웨어 게이트웨이를 NSX Controller에 연결하려면 ToR 물리적 스위치의 OVSDB 관리자 테이블을 구성해야 합니다.

이 컨트롤러는 ToR의 연결 시도를 수동적으로 수신합니다. 따라서 하드웨어 게이트웨이는 OVSDB 관리자 테이블을 사용해서 연결을 시작해야 합니다.

사전 요구 사항

ToR 인스턴스를 구성하기 전에 컨트롤러를 배포해야 합니다. 컨트롤러를 먼저 배포하지 않으면 오류 메시지가 "컨트롤러에서 작업을 수행하지 못했습니다."가 표시됩니다.

절차

- 1 작업 환경에 적용되는 명령을 사용하여 하드웨어 게이트웨이를 NSX Controller에 연결합니다.

하드웨어 게이트웨이 및 NSX Controller를 연결하기 위한 샘플 명령

```
prmh-nsx-tor-7050sx-3#enable
prmh-nsx-tor-7050sx-3#configure terminal
prmh-nsx-tor-7050sx-3(config)#cvx
prmh-nsx-tor-7050sx-3(config-cvx)#service hsc
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#manager 172.16.2.95 6640
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#no shutdown
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#end
```

- 2 하드웨어 게이트웨이에서 OVSDB 관리자 테이블을 설정합니다.
- 3 OVSDB 포트 번호 값을 6640으로 설정합니다.
- 4 (선택 사항) 하드웨어 게이트웨이가 OVSDB 채널을 통해 NSX Controller에 연결되어 있는지 확인합니다.
 - 연결 상태가 UP인지 확인합니다.
 - VM1 및 VLAN 160을 Ping하여 연결이 성공적으로 수행되었는지 확인합니다.
- 5 (선택 사항) 하드웨어 게이트웨이가 올바른 NSX Controller에 연결되어 있는지 확인합니다.
 - a vSphere Web Client에 로그인합니다.
 - b **Networking & Security > > 설치(Installation) > NSX Controller 노드(NSX Controller nodes)**를 선택합니다.

하드웨어 게이트웨이 인증서 추가

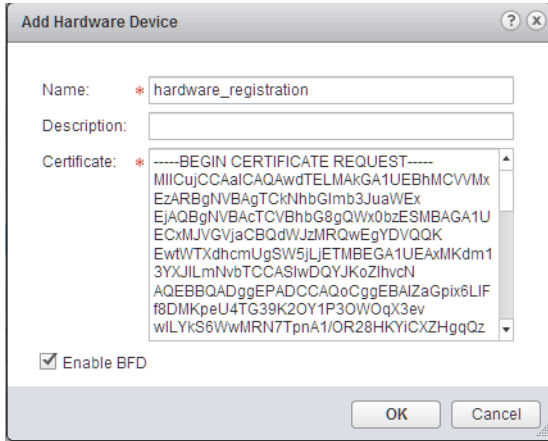
구성이 작동하려면 하드웨어 디바이스에 하드웨어 게이트웨이 인증서를 추가해야 합니다.

사전 요구 사항

작업 환경의 하드웨어 게이트웨이 인증서를 사용할 수 있는지 확인합니다.

절차

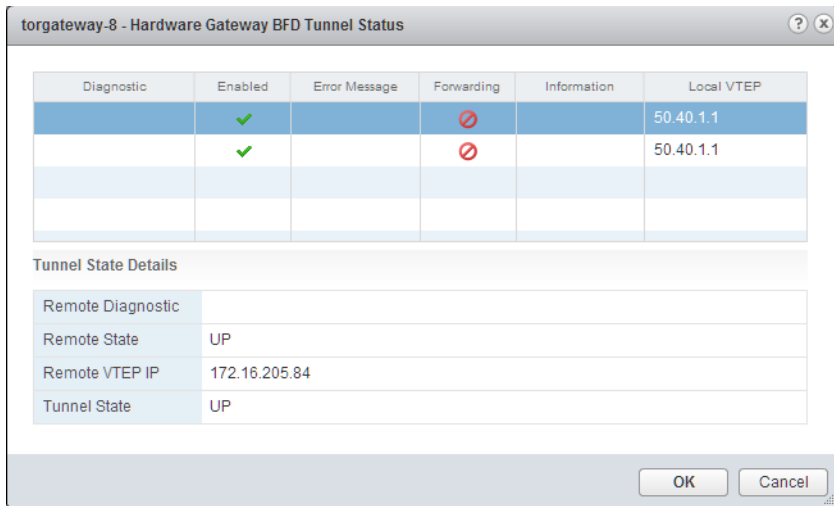
- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security) > 서비스 정의(Service Definitions)를 선택합니다.
- 3 하드웨어 디바이스(Hardware Devices) 탭을 클릭합니다.
- 4 추가(+) 아이콘을 클릭하여 하드웨어 게이트웨이 프로파일 세부 정보를 생성합니다.



옵션	설명
이름 및 설명	하드웨어 게이트웨이 이름을 지정합니다. 설명 섹션에 프로파일의 세부 정보를 추가할 수 있습니다.
인증서	작업 환경에서 추출한 인증서를 붙여넣습니다.
BFD 사용	BFD(Bidirectional Forwarding Detection) 프로토콜은 기본적으로 사용하도록 설정됩니다. 이 프로토콜은 하드웨어 게이트웨이 구성 정보를 동기화하는 데 사용됩니다.

- 5 확인(OK)을 클릭합니다.
하드웨어 게이트웨이를 나타내는 프로파일이 생성됩니다.
- 6 화면을 새로 고쳐 하드웨어 게이트웨이가 사용 가능하고 실행 중인지 확인합니다.
연결은 [UP] 상태여야 합니다.

- 7 (선택 사항) 하드웨어 게이트웨이 프로파일을 클릭하고 마우스 오른쪽 버튼을 클릭하여 드롭다운 메뉴에서 **BFD 터널 상태 보기(View the BFD Tunnel Status)**를 선택합니다.



이 대화상자에는 문제 해결을 위한 진단 터널 상태 세부 정보가 표시됩니다.

논리적 스위치를 물리적 스위치에 바인딩

가상 시스템 VM1에 연결된 **WebService** 논리적 스위치는 동일한 서브넷의 하드웨어 게이트웨이와 통신해야 합니다.

참고 여러 논리적 스위치를 하드웨어 포트에 바인딩하는 경우 각 논리적 스위치에 대해 다음 단계를 적용해야 합니다.

사전 요구 사항

- **WebService** 논리적 스위치를 사용할 수 있는지 확인합니다. [논리적 스위치 추가](#)를 참조하십시오.
- 물리적 스위치를 사용할 수 있는지 확인합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security) > 논리적 스위치(Logical Switches)**를 선택합니다.
- 3 **WebService** 논리적 스위치를 찾은 후 마우스 오른쪽 버튼을 클릭하고 드롭다운 메뉴에서 **하드웨어 바인딩 관리(Manage Hardware Bindings)**를 선택합니다.
- 4 하드웨어 게이트웨이 프로파일을 선택합니다.
- 5 추가(+) 아이콘을 클릭하고 드롭다운 메뉴에서 물리적 스위치를 선택합니다.

예: AristaGW

- 6 **선택(Select)**을 클릭하여 [사용 가능한 개체] 목록에서 물리적 포트를 선택합니다.

예: 이더넷 18

7 **확인(OK)**을 클릭합니다.

8 VLAN 이름을 지정합니다.

▼ AristaGW (1 Bindings)		
<div> + ✎ ✕ </div>		
Switch	Port	VLAN
prmh-nsx-tor-7150s-1	Ethernet18	160

예: 160

9 **확인(OK)**을 클릭합니다.

결과

바인딩이 완료되었습니다.

NSX Controller는 물리적 및 논리적 구성 정보를 하드웨어 게이트웨이와 동기화합니다.

L2 브리지

8

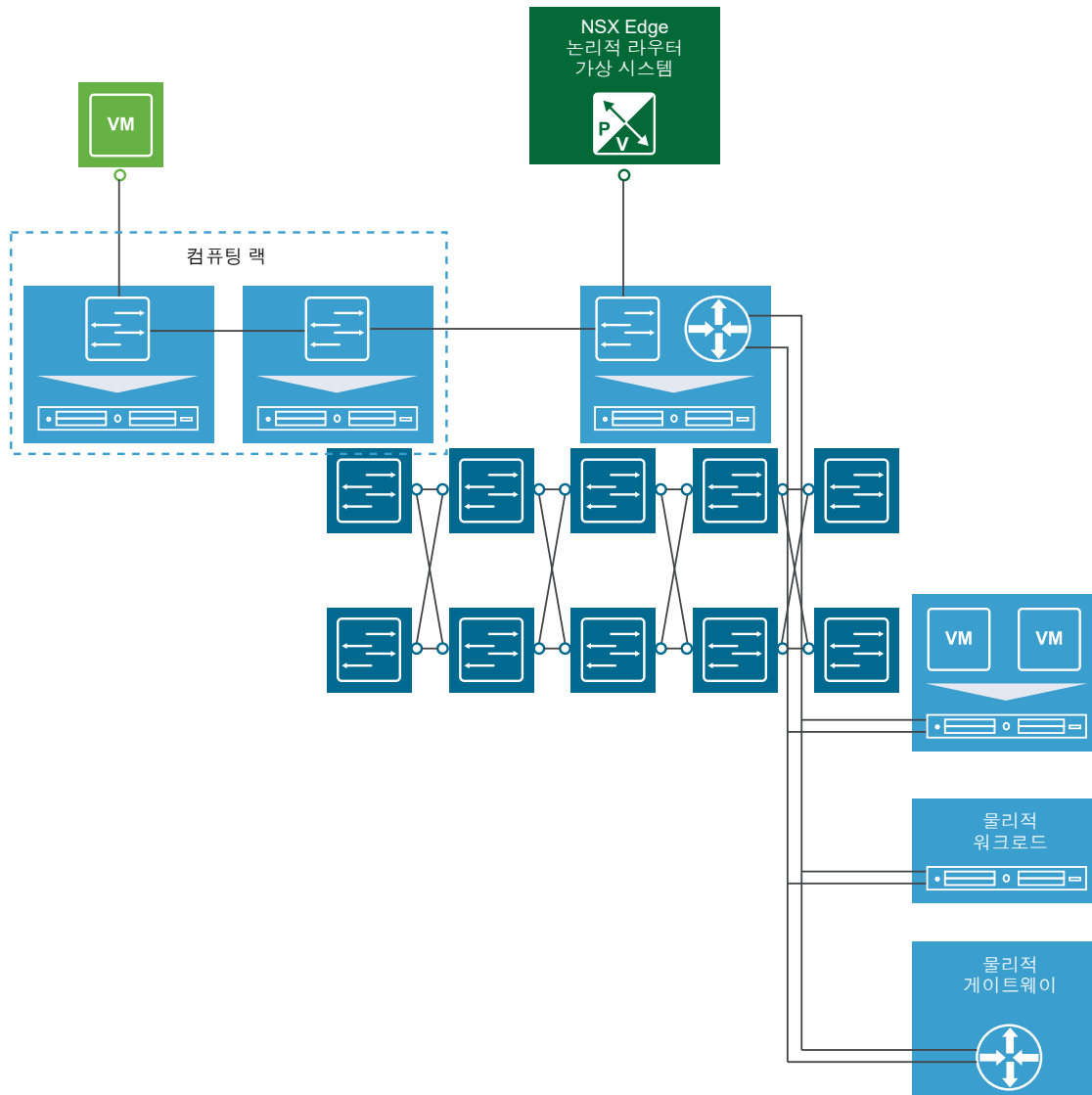
논리적 스위치와 VLAN 사이에 L2 브리지를 생성하여 IP 주소에 영향을 주지 않으면서 가상 워크로드를 물리적 디바이스로 마이그레이션할 수 있습니다.

계층 2 브리지를 사용하면 VM(가상 시스템)이 물리적 서버 또는 네트워크에 연결되도록 하여 가상 및 물리적 네트워크 간을 연결할 수 있습니다. 사용 사례에는 다음이 포함됩니다.

- 물리적-가상 또는 가상-가상 마이그레이션. L2 브리징을 사용하여 IP 주소를 다시 지정하지 않아도 NSX 내부 및 NSX 외부 워크로드 간에 연결을 유지할 수 있습니다.
- 가상화할 수 없으며 해당 클라이언트와 L2 연결이 필요한 장치의 NSX에 삽입. 이 사례는 일부 물리적 데이터베이스 서버에서 일반적입니다.
- 서비스 삽입. L2 브리지는 라우터, 로드 밸런서 또는 방화벽 같은 물리적 장치를 NSX에 투명하게 통합할 수 있도록 합니다.

논리적 스위치 브로드캐스트 도메인을 VLAN 브로드캐스트 도메인에 브리징하면 논리적 네트워크가 물리적 L3 게이트웨이를 활용하고 기존 물리적 네트워크 및 보안 리소스에 액세스할 수 있습니다. L2 브리지는 NSX Edge 논리적 라우터 가상 시스템이 있는 호스트에서 실행됩니다. L2 브리지 인스턴스는 단일 VLAN에 매핑되지만 브리지 인스턴스가 여러 개 있을 수 있습니다. 브리지에 연결된 디바이스에서는 논리적 라우터를 게이트웨이로 사용할 수 없습니다. 브리지된 VLAN 포트 그룹 및 VXLAN 논리적 스위치는 동일한 VDS(vSphere Distributed Switch)에 있어야 하며 둘 다 동일한 물리적 NIC를 공유해야 합니다.

VXLAN(VNI) 네트워크 및 VLAN 지원 포트 그룹은 동일한 VDS(분산 가상 스위치)에 있어야 합니다.



L2 브리지를 사용하여 논리적 스위치를 다른 논리적 스위치에 연결하거나, **VLAN** 네트워크를 다른 **VLAN** 네트워크에 연결하거나, 데이터 센터를 상호 연결하지 않아야 합니다. 또한 범용 논리적 라우터를 이용하여 브리징을 구성할 수 없으며 브리지를 범용 논리적 스위치에 추가할 수 없습니다.

본 장은 다음 항목을 포함합니다.

- L2 브리지 추가
- 논리적으로 라우팅된 환경에 L2 브리지 추가

L2 브리지 추가

논리적 스위치의 브리지를 분산 가상 포트 그룹에 추가할 수 있습니다.

사전 요구 사항

구성된 논리적 스위치 및 VLAN 지원 분산 가상 포트 그룹입니다.

함께 브리지될 논리적 스위치 및 VLAN 지원 분산 가상 포트 그룹은 동일한 VDS(가상 Distributed Switch)에 있어야 합니다.

논리적 스위치 및 VLAN 지원 분산 가상 포트 그룹이 있는 VDS가 인스턴스화되는 하이퍼바이저의 DLR 제어 VM을 작업 환경에 배포해야 합니다.

범용 논리적 라우터를 사용하여 브리징을 구성할 수 없고, 브리지를 범용 논리적 스위치에 추가할 수 없습니다.

경고 브리지된 트래픽은 VXLAN 트래픽에 사용되는 dvSwitch의 업링크 포트를 통해 ESXi 호스트에서 들어가고 나갈 수 있습니다. VLAN의 VDS 팀 구성 또는 페일오버 정책은 브리지된 트래픽에 사용되지 않습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 논리적 라우터를 두 번 클릭합니다.
- 4 관리(Manage)를 클릭한 다음, 브리징(Bridging)을 클릭합니다.
- 5 추가(Add)(+) 아이콘을 클릭합니다.
- 6 브리지의 이름을 입력합니다.

경고 브리지 이름은 40자를 초과할 수 없습니다. 이름이 40자를 초과하면 브리지 구성이 실패합니다.

- 7 브리지를 생성할 논리적 스위치를 선택합니다.
- 8 논리적 스위치를 브리지할 분산 가상 포트 그룹을 선택합니다.
- 9 확인(OK)을 클릭합니다.

논리적으로 라우팅된 환경에 L2 브리지 추가

지정된 논리적 스위치를 하나의 활성 브리지 인스턴스가 있는 단일 VLAN에 브리지할 수 있습니다. 하나의 논리적 라우터에 여러 개의 브리징 인스턴스가 있을 수 있지만 동일한 VXLAN와 VLAN이 둘 이상의 브리지 인스턴스에 연결될 수 없습니다.

논리적 스위치를 사용하여 논리적 분산 라우팅 및 계층 2 브리징 모두에 참여할 수 있습니다. 따라서 브리지된 논리적 스위치의 트래픽은 중앙 집중식 Edge VM을 통과해서 흐를 필요가 없습니다. 브리지된 논리적 스위치의 트래픽은 L2 브리지 인스턴스를 통해 물리적 VLAN으로 흐를 수 있습니다. DLR 제어 VM이 실행 중인 ESXi 호스트에서 브리지 인스턴스가 사용되도록 설정됩니다.

NSX의 L2 브리징에 대한 자세한 내용은 <https://communities.vmware.com/docs/DOC-27683>의 "NSX 네트워크 가상화 설계 가이드"에서 "NSX 분산 라우팅 및 계층 2 브리징 통합" 섹션을 참조하십시오.

사전 요구 사항

- NSX 논리적 라우터가 사용자 환경에 배포되어 있어야 합니다.
- 범용 논리적 라우터를 사용하여 브리징을 구성할 수 없고, 브리지를 범용 논리적 스위치에 추가할 수 없습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 브리징에 사용하려는 논리적 라우터를 두 번 클릭합니다.

참고 VXLAN이 연결된 동일한 라우팅 인스턴스에 브리지 인스턴스를 생성해야 합니다. 브리지 인스턴스 하나에 VXLAN과 VLAN을 하나씩 사용할 수 있으며, VXLAN과 VLAN이 겹치지 않아야 합니다. 동일한 VXLAN 및 VLAN을 둘 이상의 브리지 인스턴스에 연결할 수는 없습니다.

- 4 **관리(Manage)**를 클릭한 다음, **브리징(Bridging)**을 클릭합니다.
라우터로 사용되고 있는 논리적 스위치가 [라우팅 사용]으로 표시됩니다.
- 5 **추가(Add)**(+) 아이콘을 클릭합니다.
- 6 브리지의 이름을 입력합니다.
- 7 브리지를 생성할 논리적 스위치를 선택합니다.
- 8 논리적 스위치를 브리지할 분산 가상 포트 그룹을 선택합니다.
- 9 **확인(OK)**을 클릭합니다.
- 10 [브리지 추가] 창에서 **확인(OK)**을 다시 클릭합니다.
- 11 [게시]를 클릭하여 브리징 구성 변경 내용을 적용합니다.

이제 브리징에 사용되는 논리적 스위치가 **라우팅 사용(Routing Enabled)**으로 지정되어 나타납니다. 자세한 내용은 [논리적 스위치 추가](#) 및 [논리적 스위치에 가상 시스템 연결](#) 항목을 참조하십시오.

각 **NSX Edge**에 대해 정적 및 동적 라우팅을 지정할 수 있습니다.

동적 라우팅은 계층 2 브로드캐스트 도메인 간에 필요한 정보 전달 기능을 제공하므로 계층 2 브로드캐스트 도메인을 줄이고 네트워크 효율성 및 확장성을 개선할 수 있습니다. **NSX**는 워크로드가 상주하는 위치로 이 인텔리전스 기능을 확장하여 동-서 라우팅을 수행합니다. 따라서 추가 코스트나 시간을 들여 홉을 확장할 필요 없이 가상 시스템 간의 직접적인 통신이 가능합니다. 이와 동시에 **NSX**는 북-남 연결도 제공하므로 테넌트가 공용 네트워크에 액세스할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 논리적(분산) 라우터 추가
- **Edge Services Gateway** 추가
- 글로벌 구성 지정
- **NSX Edge** 구성
- 정적 경로 추가
- 논리적 (분산) 라우터에서 **OSPF** 구성
- **Edge Services Gateway**에서 **OSPF** 구성
- **BGP** 구성
- 경로 재배포 구성
- **NSX Manager** 로케일 ID 보기
- 범용 논리적(분산) 라우터에서 로케일 ID 구성
- 호스트 또는 클러스터에서 로케일 ID 구성

논리적(분산) 라우터 추가

호스트의 논리적 라우터 커널 모듈은 **VXLAN** 네트워크 간 그리고 가상 네트워크와 물리적 네트워크 간에 라우팅을 수행합니다. **NSX Edge** 장치는 필요에 따라 동적 라우팅 기능을 제공합니다. 논리적 라우터는 크로스 vCenter **NSX** 환경의 기본 및 보조 **NSX Manager** 모두에서 생성할 수 있지만 범용 논리적 라우터는 기본 **NSX Manager**에서만 생성할 수 있습니다.

새 논리적 라우터를 배포하는 경우 다음을 고려하십시오.

- NSX 버전 6.2 이상에서는 논리적 라우터로 라우팅된 논리적 인터페이스(LIF)를 VLAN에 브리징되는 VXLAN에 연결할 수 있습니다.
- VLAN ID를 0으로 설정한 상태에서 논리적 라우터 인터페이스와 브리징 인터페이스를 dvPortgroup에 연결할 수 없습니다.
- 지정한 논리적 라우터 인스턴스는 다른 전송 영역에 있는 논리적 스위치에 연결할 수 없습니다. 이를 통해 모든 논리적 스위치와 논리적 라우터 인스턴스가 정렬됩니다.
- 논리적 라우터가 둘 이상의 VDS(vSphere Distributed Switch)에 걸쳐 있는 논리적 스위치에 연결된 경우 VLAN 지원 포트 그룹에 연결할 수 없습니다. 따라서 논리적 라우터 인스턴스가 여러 호스트에 있는 논리적 스위치 dvPortgroups에 올바르게 맞춰질 수 있습니다.
- 두 개의 네트워크가 동일한 vSphere Distributed Switch에 있는 경우 동일한 VLAN ID를 가진 두 개의 다른 분산 포트 그룹(dvPortgroups)에서 논리적 라우터 인터페이스를 생성하면 안 됩니다.
- 두 개의 네트워크가 다른 vSphere Distributed Switch에 있지만 두 개의 vSphere Distributed Switch가 동일한 호스트를 공유할 경우 동일한 VLAN ID를 가진 두 개의 다른 dvPortgroups에서 논리적 라우터 인터페이스를 생성하면 안 됩니다. 즉 두 개의 dvPortgroups이 두 개의 다른 vSphere Distributed Switch에 있는 경우 vSphere Distributed Switch가 호스트를 공유하지 않는 한 동일한 VLAN ID를 가진 두 개의 다른 네트워크에서 논리적 라우터 인터페이스를 생성할 수 있습니다.
- VXLAN이 구성된 경우, 논리적 라우터 인터페이스를 vSphere VXLAN이 구성된 vSphere Distributed Switch의 분산 포트 그룹에 연결해야 합니다. 논리적 라우터 인터페이스를 다른 vSphere Distributed Switch의 포트 그룹에 연결하지 마십시오.

다음 목록에서는 논리적 라우터의 인터페이스 유형(업링크 및 내부)별로 지원되는 기능을 설명합니다.

- 동적 라우팅 프로토콜(BGP 및 OSPF)은 업링크 인터페이스에서만 지원됩니다.
- 방화벽 규칙은 업링크 인터페이스에서만 적용 가능하고 Edge 가상 장치로 전송되는 제어 및 관리 트래픽으로 제한됩니다.
- DLR 관리 인터페이스에 대한 자세한 내용은 기술 자료 문서 "관리 인터페이스 가이드: DLR 제어 VM - NSX" <http://kb.vmware.com/kb/2122060>을 참조하십시오.

중요 크로스 vCenter NSX 환경에서 NSX Edge에 대해고가용성을 사용하도록 설정하는 경우 활성 및 대기 NSX Edge 장치가 동일한 vCenter Server 내에 상주해야 합니다. NSX Edge HA 쌍의 한 멤버를 다른 vCenter Server 시스템으로 마이그레이션하면 두 HA 장치가 더 이상 HA 쌍으로 작동하지 않으며 트래픽 중단이 발생할 수 있습니다.

사전 요구 사항

- 엔터프라이즈 관리자 또는 NSX 관리자 역할을 할당받아야 합니다.
- NSX 논리적 스위치를 생성할 계획이 없어도 로컬 세그먼트 ID 풀을 생성해야 합니다.

- 논리적 라우터 구성을 생성하거나 변경하기 전에 컨트롤러 클러스터가 최신 상태이고 사용 가능한지 확인하십시오. 논리적 라우터는 **NSX Controller**를 사용하지 않으면 라우팅 정보를 호스트에 배포할 수 없습니다. 논리적 라우터는 **NSX Controller**를 사용하여 작동하는 반면, **ESG(Edge Services Gateway)**는 **NSX Controller**를 사용하지 않습니다.
- 논리적 라우터가 **VLAN dvPortgroup**에 연결될 경우 논리적 라우터 장치가 설치된 모든 하이퍼바이저 호스트가 **UDP 포트 6999**에서 서로 연결할 수 있는지 확인하십시오. 논리적 라우터 **VLAN** 기반 **ARP** 프로세스가 작동하려면 이 포트에서 통신할 수 있어야 합니다.
- 논리적 라우터 장치를 배포할 위치를 확인합니다.
 - 대상 호스트는 새 논리적 라우터의 인터페이스에 연결된 논리적 스위치와 동일한 전송 영역에 속해야 합니다.
 - **ECMP** 설정에서 **ESG**를 사용하는 경우 하나 이상의 업스트림 **ESG**와 동일한 호스트에 배치하지 않도록 합니다. **DRS** 반선회도 규칙을 사용하여 이를 적용함으로써 논리적 라우터 전달에 대한 호스트 실패의 영향을 줄일 수 있습니다. 업스트림 **ESG**가 하나 있거나 **HA** 모드인 경우 이 지침이 적용되지 않습니다. 자세한 내용은 <https://communities.vmware.com/docs/DOC-27683>에 있는 "VMware NSX for vSphere 네트워크 가상화 설계 가이드"를 참조하십시오.
- 논리적 라우터 장치를 설치하는 호스트 클러스터에서 **NSX** 사용 준비가 되었는지 확인하십시오. "NSX 설치 가이드"에서 "NSX에 대한 호스트 클러스터 준비"를 참조하십시오.
- 변경할 적합한 **NSX Manager**를 결정합니다.
 - 독립 실행형 또는 단일 **vCenter NSX** 환경에는 **NSX Manager**가 하나만 있기 때문에 선택할 필요가 없습니다.
 - 범용 개체는 기본 **NSX Manager**에서 관리해야 합니다.
 - **NSX Manager**에 로컬인 개체는 **NSX Manager**에서 관리해야 합니다.
 - 고급 연결 모드가 사용되도록 설정되지 않은 크로스 **vCenter NSX** 환경에서는 수정하려는 **NSX Manager**에 연결된 **vCenter**에서 구성을 변경해야 합니다.
 - 고급 연결 모드의 크로스 **vCenter NSX** 환경에서는 모든 연결된 **vCenter**에서 원하는 **NSX Manager**의 구성을 변경할 수 있습니다. **NSX Manager** 드롭다운 메뉴에서 적절한 **NSX Manager**를 선택합니다.
- 추가하려는 논리적 라우터 종류를 결정합니다.
 - 논리적 스위치를 연결해야 하는 경우에는 논리적 라우터를 추가해야 합니다.
 - 범용 논리적 스위치를 연결해야 하는 경우에는 범용 논리적 라우터를 추가해야 합니다.
- 범용 논리적 라우터를 추가하는 경우 로컬 송신을 사용하도록 설정할지 여부를 결정합니다. 로컬 송신을 사용하면 호스트 경로를 선택적으로 전송할 수 있습니다. 이 기능은 **NSX** 배포가 여러 사이트에서 사용되는 경우에 필요할 수 있습니다. 자세한 내용은 [크로스 vCenter NSX 토폴로지](#) 항목을 참조하십시오. 범용 로컬 라우터가 생성된 후에는 로컬 송신을 수정할 수 없습니다.

절차

- 1 vSphere Web Client에서 **홈 > Networking & Security > NSX Edge(Home > Networking & Security > NSX Edges)**로 이동합니다.
- 2 변경 내용을 적용할 적절한 **NSX Manager**를 선택합니다. 범용 논리적 라우터를 생성하는 경우에는 기본 **NSX Manager**를 선택해야 합니다.
- 3 **추가(Add)(+)** 아이콘을 클릭합니다.
- 4 추가하려는 논리적 라우터 유형을 선택합니다.

- 선택한 NSX Manager에 로컬인 논리적 라우터를 추가하려면 **논리적(분산) 라우터(Logical (Distributed) Router)**를 선택합니다.
- 크로스 vCenter NSX 환경으로 확장할 수 있는 논리적 라우터를 추가하려면 **범용 논리적(분산) 라우터(Universal Logical (Distributed) Router)**를 선택합니다. 이 옵션은 기본 NSX Manager를 할당할 경우에만 사용할 수 있으며, 기본 NSX Manager에서 변경됩니다.
- a **범용 논리적(분산) 라우터(Universal Logical (Distributed) Router)**를 선택하면 로컬 송신을 사용하도록 설정할지 여부도 선택해야 합니다.

- 5 디바이스의 이름을 입력합니다.

이 이름은 vCenter 인벤토리에 나타납니다. 이 이름은 단일 테넌트 내의 모든 논리적 라우터에서 고유해야 합니다.

필요한 경우 호스트 이름을 입력할 수도 있습니다. 이 이름이 CLI에 표시됩니다. 호스트 이름을 지정하지 않으면 자동으로 생성되는 Edge ID가 CLI에 표시됩니다.

필요한 경우 설명과 테넌트를 입력할 수 있습니다.

- 6 Edge Appliance를 배포합니다.

Edge Appliance 배포(Deploy Edge Appliance)가 기본적으로 선택됩니다. 논리적 라우터 ping, SSH 액세스 및 동적 라우팅 트래픽에 적용되는 동적 라우팅 및 논리적 라우터 장치의 방화벽에는 **Edge Appliance(논리적 라우터 가상 장치라고도 함)**가 필요합니다.

정적 경로만 필요하고 Edge Appliance를 배포하지 않을 경우 Edge Appliance 옵션을 선택 취소할 수 있습니다. 논리적 라우터를 생성한 후 Edge Appliance를 논리적 라우터에 추가할 수 없습니다.

- 7 (선택 사항) 고가용성을 사용하도록 설정합니다.

고가용성 사용(Enable High Availability)은 기본적으로 선택되어 있지 않습니다. HA(고가용성)를 사용하도록 설정하고 구성하려면 **고가용성 사용(Enable High Availability)** 확인란을 선택합니다. 동적 라우팅 수행을 계획하는 경우 고가용성이 필요합니다.

- 8 논리적 라우터의 암호를 입력하고 다시 입력합니다.

암호는 12 ~ 255자여야 하고 다음을 포함해야 합니다.

- 하나 이상의 대문자
- 하나 이상의 소문자

- 숫자 1개 이상
- 하나 이상의 특수 문자

9 (선택 사항) SSH를 사용하도록 설정합니다.

기본적으로 SSH는 사용하지 않도록 설정되어 있습니다. SSH를 사용하도록 설정하지 않은 경우 가상 장치 콘솔을 열어서 논리적 라우터에 액세스할 수 있습니다. 여기서 SSH를 사용하도록 설정하면 SSH 프로세스가 논리적 라우터 가상 장치에서 실행됩니다. 논리적 라우터의 프로토콜 주소에 대한 SSH 액세스를 허용하려면 논리적 라우터 방화벽 구성을 수동으로 조정해야 합니다. 논리적 라우터에서 동적 라우팅을 구성할 때 프로토콜 주소가 구성됩니다.

10 (선택 사항) FIPS 모드를 사용하도록 설정하고 로그 수준을 설정합니다.

기본적으로 FIPS 모드는 사용하지 않도록 설정되어 있습니다. **FIPS 모드 사용(Enable FIPS mode)** 확인란을 선택하여 FIPS 모드를 사용하도록 설정합니다. FIPS 모드를 사용하도록 설정하면 NSX Edge와의 모든 보안 통신에 FIPS에서 허용하는 암호화 알고리즘 또는 프로토콜이 사용됩니다.

기본적으로 로그 수준은 긴급입니다.

예:

Settings

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: *

Password: *

Confirm password: *

☐ Enable SSH access

☐ Enable FIPS mode

Edge Control Level Logging EMERGENCY ▼

Set the Edge Control Level Logging

11 배포를 구성합니다.

- ◆ **Edge Appliance 배포(Deploy Edge Appliance)**를 선택하지 않은 경우 **추가(Add)(+)** 아이콘이 회색으로 표시됩니다. 구성을 계속하려면 **다음(Next)**을 클릭합니다.
- ◆ **Edge Appliance 배포(Deploy Edge Appliance)**를 선택한 경우 논리적 라우터 가상 장치에 대한 설정을 입력합니다.

예:

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool:	*	Management & Edge ...	▼
Datastore:	*	ds-1	▼
Host:		esxmgmt-01a.corp.local	▼
Folder:		Discovered virtual mac...	▼

12 인터페이스를 구성합니다. 논리적 라우터에서는 IPv4 주소 지정만 지원됩니다.

- a HA 인터페이스 연결을 구성하고 필요한 경우 IP 주소도 구성합니다.

Edge Appliance 배포(Deploy Edge Appliance)를 선택한 경우 HA 인터페이스를 분산 포트 그룹 또는 논리적 스위치에 연결해야 합니다. 이 인터페이스를 HA 인터페이스로만 사용하는 경우 논리적 스위치를 사용합니다. /30 서브넷이 링크 로컬 범위 169.254.0.0/16에서 할당되고 두 NSX Edge 장치 각각의 IP 주소를 제공하는 데 사용됩니다.

필요에 따라 이 인터페이스를 사용하여 NSX Edge에 연결할 경우 HA 인터페이스에 대한 추가 IP 주소 및 접두사를 지정할 수 있습니다.

참고 NSX 6.2 이전에는 HA 인터페이스를 관리 인터페이스라고 지칭했습니다. HA 인터페이스와 동일한 IP 서브넷에 없는 모든 위치에서 HA 인터페이스로 SSH할 수 없습니다. HA 인터페이스를 가리키는 정적 경로를 구성할 수 없으므로, RPF가 들어오는 트래픽을 삭제하게 됩니다. 이론상 RPF를 사용하지 않도록 설정할 수 있지만 이런 경우 고가용성에는 역효과를 낼 수 있습니다. SSH 액세스의 경우 동적 라우팅을 구성할 때 나중에 구성되는 논리적 라우터의 프로토콜 주소를 사용할 수도 있습니다.

NSX 6.2 이상에서는 논리적 라우터의 HA 인터페이스가 경로 재배포에서 자동으로 제외됩니다.

- b 이 NSX Edge의 인터페이스를 구성합니다.

이 NSX Edge의 인터페이스 구성(Configure interfaces of this NSX Edge)에서 내부 인터페이스는 VM 대 VM 통신(때로 동-서 통신이라고도 함)을 허용하는 스위치에 연결하기 위한 것입니다. 논리적 라우터 가상 장치에서 내부 인터페이스가 유사 vNIC로 생성됩니다. 업링크 인터페이스는 북-남 통신용입니다. 논리적 라우터 업링크 인터페이스는 **Edge Services Gateway** 또는 타사 라우터 VM에 연결할 수 있습니다. 동적 라우팅이 작동하려면 업링크 인터페이스가 하나 이상 있어야 합니다. 논리적 라우터 가상 장치에서 업링크 인터페이스가 vNIC로 생성됩니다.

여기서 입력하는 인터페이스 구성을 나중에 수정할 수 있습니다. 논리적 라우터가 배포된 후 인터페이스를 추가, 제거 및 수정할 수 있습니다.

다음 예제에서는 관리 분산 포트 그룹에 연결된 HA 인터페이스를 보여줍니다. 또한 2개의 내부 인터페이스(app 및 web)와 업링크 인터페이스(to-ESG)를 보여줍니다.

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Ready to complete

Configure interfaces

HA interface Configuration

Connected To: [Change](#) [Remove](#)

+

x

IP Address	Subnet Prefix Length
192.168.110.60*	24

HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

+

x

Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back

Next

Finish

Cancel

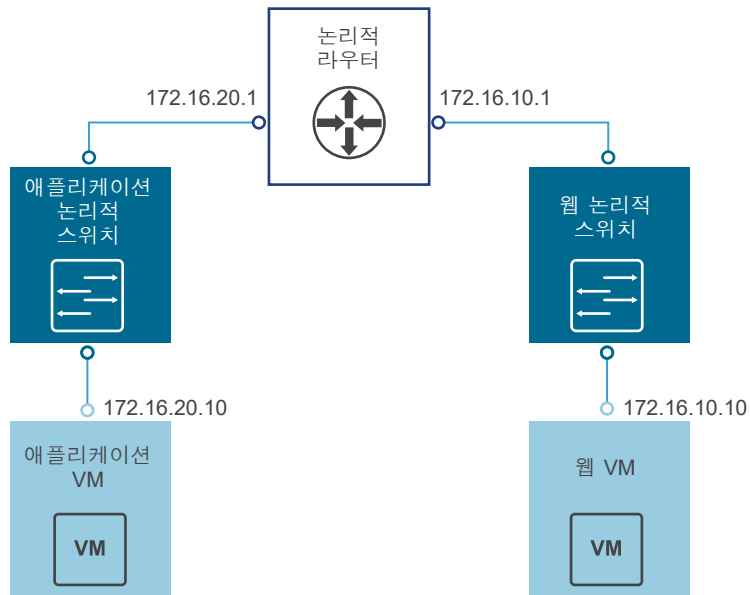
13 기본 게이트웨이를 구성합니다.

예:

14 논리적 스위치에 연결된 VM의 기본 게이트웨이가 논리적 라우터 인터페이스 IP 주소로 올바르게 설정되어 있는지 확인하십시오.

결과

다음 예제 토폴로지에서 App VM의 기본 게이트웨이는 172.16.20.1이고 웹 VM의 기본 게이트웨이는 172.16.10.1입니다. VM이 해당 기본 게이트웨이 및 서로를 Ping할 수 있는지 확인하십시오.



SSH 또는 콘솔을 사용하여 NSX Manager에 연결하고 다음 명령을 실행합니다.

- 모든 논리적 라우터 인스턴스 정보를 나열합니다.

```
nsxmgr-l-01a> show logical-router list all
```

Edge-id	Vdr Name	Vdr id	#Lifs
edge-1	default+edge-1	0x00001388	3

- 컨트롤러 클러스터에서 논리적 라우터에 대한 라우팅 정보를 수신한 호스트를 나열합니다.

```
nsxmgr-l-01a> show logical-router list dlr edge-1 host
```

ID	HostName
host-25	192.168.210.52
host-26	192.168.210.53
host-24	192.168.110.53

지정한 논리적 라우터(이 예제에서는 **edge-1**)에 연결된 논리적 스위치를 소유하는 전송 영역의 멤버로 구성된 모든 호스트 클러스터의 모든 호스트가 출력에 포함됩니다.

- 논리적 라우터가 호스트에 전달하는 라우팅 테이블 정보를 나열합니다. 모든 호스트에서 라우팅 테이블 항목이 일치해야 합니다.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 route
```

VDR default+edge-1 Route Table

Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]

Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	4101	138800000002

172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10195	13880000000b
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10196	13880000000a
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10196	138800000002
192.168.100.0	255.255.255.0	192.168.10.1	UG	1	AUTO	3802	138800000002

- 호스트 중 하나의 관점에서 라우터에 대한 추가 정보를 나열합니다. 이 출력은 호스트와 통신하고 있는 컨트롤러를 확인하는 데 유용합니다.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose
```

VDR Instance Information :

```
-----

Vdr Name:                default+edge-1
Vdr Id:                  0x00001388
Number of Lifs:          3
Number of Routes:        5
State:                   Enabled
Controller IP:           192.168.110.203
Control Plane IP:        192.168.210.52
Control Plane Active:    Yes
Num unique nexthops:     1
Generation Number:      0
Edge Active:             No
```

show logical-router host host-25 dlr edge-1 verbose 명령의 출력에서 컨트롤러 IP 필드를 확인합니다.

컨트롤러에 SSH하고, 다음 명령을 실행하여 컨트롤러의 확인된 VNI, VTEP, MAC 및 ARP 테이블 상태 정보를 표시합니다.

```
192.168.110.202 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled             Enabled      0
```

VNI 5000에 대한 출력에서 제로 연결을 표시하고 컨트롤러 192.168.110.201을 VNI 5000의 소유자로 나열합니다. 해당 컨트롤러에 로그인하여 VNI 5000에 대한 추가 정보를 수집합니다.

```
192.168.110.201 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled             Enabled      3
```

192.168.110.201에 대한 출력에서 세 개 연결을 표시합니다. 추가 VNI를 확인합니다.

```
192.168.110.201 # show control-cluster logical-switches vni 5001
VNI      Controller      BUM-Replication ARP-Proxy Connections
5001     192.168.110.201 Enabled             Enabled      3
```

```
192.168.110.201 # show control-cluster logical-switches vni 5002
VNI      Controller      BUM-Replication ARP-Proxy Connections
5002     192.168.110.201 Enabled             Enabled      3
```

192.168.110.201에서 3개의 VNI 연결을 모두 소유하기 때문에 다른 컨트롤러 192.168.110.203에서 연결이 표시되지 않을 것입니다.

```
192.168.110.203 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled           Enabled    0
```

- MAC 및 ARP 테이블을 확인하기 전에 하나의 VM에서 다른 VM으로 ping합니다.

App VM에서 웹 VM으로:

```
vmware@app-vm$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 ms
```

MAC 테이블을 확인합니다.

```
192.168.110.201 # show control-cluster logical-switches mac-table 5000
VNI      MAC                  VTEP-IP      Connection-ID
5000     00:50:56:a6:23:ae 192.168.250.52 7
```

```
192.168.110.201 # show control-cluster logical-switches mac-table 5001
VNI      MAC                  VTEP-IP      Connection-ID
5001     00:50:56:a6:8d:72 192.168.250.51 23
```

ARP 테이블을 확인합니다.

```
192.168.110.201 # show control-cluster logical-switches arp-table 5000
VNI      IP                   MAC                  Connection-ID
5000     172.16.20.10        00:50:56:a6:23:ae 7
```

```
192.168.110.201 # show control-cluster logical-switches arp-table 5001
VNI      IP                   MAC                  Connection-ID
5001     172.16.10.10        00:50:56:a6:8d:72 23
```

논리적 라우터 정보를 확인합니다. 각 논리적 라우터 인스턴스를 컨트롤러 노드 중 하나가 사용합니다.

`show control-cluster logical-routers` 명령의 `instance` 하위 명령에서 이 컨트롤러에 연결된 논리적 라우터 목록을 표시합니다.

`interface-summary` 하위 명령에서 컨트롤러가 NSX Manager에서 확인한 LIF를 표시합니다. 전송 영역에서 관리되는 호스트 클러스터에 있는 호스트로 이 정보가 전송됩니다.

routes 하위 명령에서 논리적 라우터의 가상 장치(컨트롤 VM이라고도 함)가 이 컨트롤러에 전송한 라우팅 테이블을 표시합니다. ESXi 호스트에서와 달리 이 라우팅 테이블에는 직접 연결된 서브넷은 포함되지 않습니다. 이 정보는 LIF 구성에서 제공하기 때문입니다. ESXi 호스트에 대한 경로 정보에는 직접 연결된 서브넷이 포함됩니다. 이 경우 ESXi 호스트의 데이터 경로에서 사용한 전달 테이블이기 때문입니다.

- 이 컨트롤러에 연결된 모든 논리적 라우터를 나열합니다.

```
controller # show control-cluster logical-routers instance all
LR-Id      LR-Name      Universal Service-Controller Egress-Locale
0x1388     default+edge-1 false      192.168.110.201 local
```

LR-Id를 기록하고 이를 다음 명령에서 사용하십시오.

- controller # show control-cluster logical-routers interface-summary 0x1388

Interface	Type	Id	IP[]
13880000000b	vxlan	0x1389	172.16.10.1/24
13880000000a	vxlan	0x1388	172.16.20.1/24
138800000002	vxlan	0x138a	192.168.10.2/29

- controller # show control-cluster logical-routers routes 0x1388

Destination	Next-Hop[]	Preference	Locale-Id	Source
192.168.100.0/24	192.168.10.1	110	00000000-0000-0000-0000-000000000000	CONTROL_VM
0.0.0.0/0	192.168.10.1	0	00000000-0000-0000-0000-000000000000	CONTROL_VM

```
[root@comp02a:~] esxcfg-route -l
```

VMkernel Routes:

Network	Netmask	Gateway	Interface
10.20.20.0	255.255.255.0	Local Subnet	vmk1
192.168.210.0	255.255.255.0	Local Subnet	vmk0
default	0.0.0.0	192.168.210.1	vmk0

- 특정 VNI에 대한 컨트롤러 연결을 표시합니다.

```
192.168.110.203 # show control-cluster logical-switches connection-table 5000
Host-IP      Port ID
192.168.110.53 26167 4
192.168.210.52 27645 5
192.168.210.53 40895 6
```

```
192.168.110.202 # show control-cluster logical-switches connection-table 5001
Host-IP      Port ID
192.168.110.53 26167 4
192.168.210.52 27645 5
192.168.210.53 40895 6
```

이 호스트-IP 주소는 VTEP가 아니라 vmk0 인터페이스입니다. ESXi 호스트와 컨트롤러 간의 연결이 관리 네트워크에 생성됩니다. 여기서 포트 번호는 호스트가 컨트롤러와 연결을 설정할 때 ESXi 호스트 IP 스택에서 할당하는 사용 후 삭제 TCP 포트입니다.

- 호스트에서 포트 번호와 일치하는 컨트롤러 네트워크 연결을 확인할 수 있습니다.

```
[root@192.168.110.53:~] #esxcli network ip connection list | grep 26167
tcp          0      0 192.168.110.53:26167      192.168.110.101:1234  ESTABLISHED
96416 newreno netcpa-worker
```

- 호스트의 활성 VNI를 표시합니다. 호스트에서 출력이 어떻게 다른지 관찰합니다. 모든 VNI가 모든 호스트에서 활성화되어 있는 것은 아닙니다. 논리적 스위치에 연결된 VM이 호스트에 있는 경우 VNI가 호스트에서 활성화되어 있습니다.

```
[root@192.168.210.52:~] # esxcli network vswitch dvs vmware vxlan network list --vds-name
Compute_VDS
```

VXLAN ID	Multicast IP	Control Plane	Controller Connection
Port Count	MAC Entry Count	ARP Entry Count	VTEP Count
5000	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.203
(up)	1	0	0
5001	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202
(up)	1	0	0

참고 vSphere 6.0 이상에서 vxlan 네임스페이스를 사용하도록 설정하려면 `/etc/init.d/hostd restart` 명령을 실행하십시오.

하이브리드 모드나 유니캐스트 모드에 있는 논리적 스위치의 경우 `esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>` 명령에 다음 출력이 포함됩니다.

- 제어부는 사용하도록 설정되어 있습니다.
- 멀티캐스트 프록시 및 ARP 프록시가 나열됩니다. IP 검색을 사용하지 않도록 설정한 경우에도 AARP 프록시가 나열됩니다.
- 유효한 컨트롤러 IP 주소가 나열되고 연결이 실행 중입니다.
- 논리적 라우터가 ESXi 호스트에 연결된 경우 논리적 스위치에 연결된 호스트에 VM이 없더라도 포트 수는 최소 1입니다. 이 포트는 ESXi 호스트의 논리적 라우터 커널 모듈에 연결된 특수한 dvPort 인 vdrPort입니다.

- 먼저 VM에서 다른 서브넷의 다른 VM으로 Ping한 다음, MAC 테이블을 표시합니다. 내부 MAC은 VM 항목이고, 외부 MAC과 외부 IP는 VTEP를 참조합니다.

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5000
```

Inner MAC	Outer MAC	Outer IP	Flags
00:50:56:a6:23:ae	00:50:56:6a:65:c2	192.168.250.52	00000111

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5001
```

Inner MAC	Outer MAC	Outer IP	Flags
02:50:56:56:44:52	00:50:56:6a:65:c2	192.168.250.52	00000101
00:50:56:f0:d7:e4	00:50:56:6a:65:c2	192.168.250.52	00000111

다음에 수행할 작업

NSX Edge 장치를 설치할 때 vSphere HA가 클러스터에서 사용되지 않도록 설정되어 있으면 NSX는 호스트에서 자동 VM 시작/종료를 사용하도록 설정합니다. 장치 VM이 나중에 클러스터의 다른 호스트로 마이그레이션되는 경우 새 호스트가 자동 VM 시작/종료를 사용하도록 설정하지 않을 수도 있습니다. 이러한 이유로 vSphere HA가 사용되지 않도록 설정된 클러스터에서 NSX Edge 장치를 설치할 때는 클러스터의 모든 호스트를 점검하여 자동 VM 시작/종료가 사용되도록 설정되어 있는지 확인해야 합니다. "vSphere 가상 시스템 관리"에서 "가상 시스템 시작 및 종료 설정 편집"을 참조하십시오.

논리적 라우터가 배포된 후 논리적 라우터 ID를 두 번 클릭하여 인터페이스, 라우팅, 방화벽, 브리징 및 DHCP 릴레이 같은 추가 설정을 구성합니다.

Edge Services Gateway 추가

데이터 센터에 여러 NSX Edge Services Gateway 가상 장치를 설치할 수 있습니다. 각 NSX Edge 가상 장치는 총 10개의 업링크 및 내부 네트워크 인터페이스를 사용할 수 있습니다. 내부 인터페이스는 보안 포트 그룹에 연결하여 포트 그룹에 있는 모든 보호된 가상 시스템의 게이트웨이 역할을 합니다. 내부 인터페이스에 할당된 서브넷은 라우팅된 공용 IP 주소 공간이거나 NAT가 적용된/라우팅된 RFC 1918 전용 공간일 수 있습니다. 인터페이스 간의 트래픽에는 방화벽 규칙 및 기타 NSX Edge 서비스가 적용됩니다.

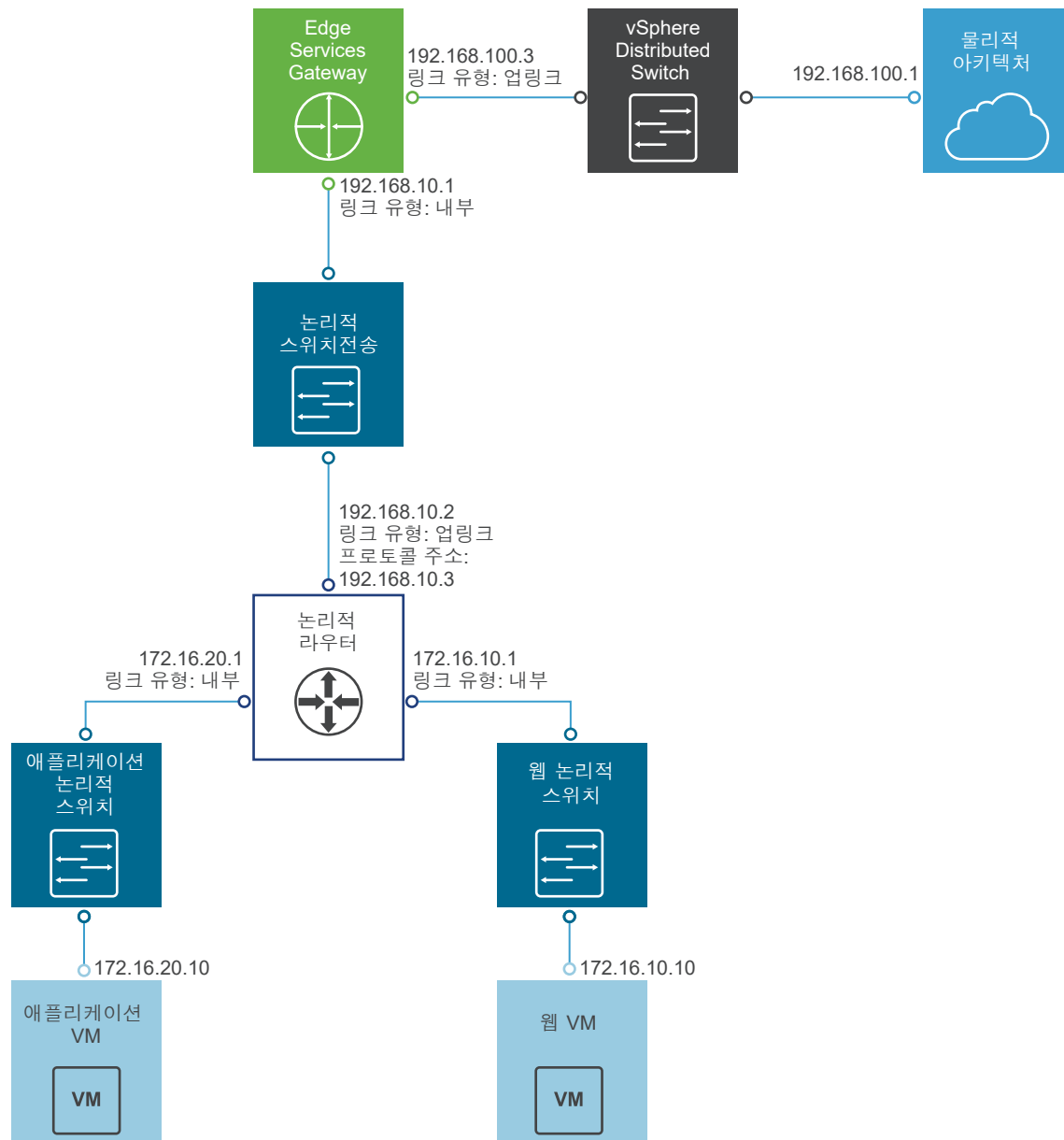
ESG의 업링크 인터페이스는 업링크 포트 그룹에 연결하여 액세스 계층 네트워킹을 제공하는 서비스나 공유 회사 네트워크에 액세스할 수 있습니다.

다음 목록에서는 ESG에서 인터페이스 유형(내부 및 업링크)별로 지원되는 기능을 설명합니다.

- DHCP: 업링크 인터페이스에서 지원되지 않습니다.
- DNS 전달자: 업링크 인터페이스에서 지원되지 않습니다.
- HA: 업링크 인터페이스에서 지원되지 않고, 하나 이상의 내부 인터페이스가 필요합니다.
- SSL VPN: 수신기 IP가 업링크 인터페이스에 속해야 합니다.

- **IPSec VPN:** 로컬 사이트 IP가 업링크 인터페이스에 속해야 합니다.
- **L2 VPN:** 내부 네트워크만 확장할 수 있습니다.

다음 그림에서는 **vSphere Distributed Switch**를 통해 물리적 인프라에 연결된 **ESG**의 업링크 인터페이스와 **NSX** 논리적 전송 스위치를 통해 **NSX** 논리적 라우터에 연결된 **ESG**의 내부 인터페이스가 포함된 샘플 토폴로지를 보여줍니다.



로드 밸런싱, 사이트 간 VPN 및 NAT 서비스에는 외부 IP 주소를 여러 개 구성할 수 있습니다.

중요 크로스 vCenter NSX 환경에서 NSX Edge에 대해 고가용성을 사용하도록 설정하는 경우 활성 및 대기 NSX Edge 장치가 동일한 vCenter Server 내에 상주해야 합니다. NSX Edge HA 쌍의 한 멤버를 다른 vCenter Server 시스템으로 마이그레이션하면 두 HA 장치가 더 이상 HA 쌍으로 작동하지 않으며 트래픽 중단이 발생할 수 있습니다.

사전 요구 사항

- 엔터프라이즈 관리자 또는 NSX 관리자 역할을 할당받아야 합니다.
- 리소스 풀에 ESG(Edge Services Gateway) 가상 장치를 배포하기에 충분한 용량이 있는지 확인합니다. [장 1 NSX의 시스템 요구 사항](#)을 참조하십시오.
- NSX Edge 장치가 설치될 호스트 클러스터가 NSX용으로 준비되어 있는지 확인합니다. "NSX 설치 가이드"에서 "NSX에 대한 호스트 클러스터 준비"를 참조하십시오.

절차

1 vCenter에서 **홈 > Networking & Security > NSX Edge(Home > Networking & Security > NSX Edges)**로 이동하고 **추가(Add) (+)** 아이콘을 클릭합니다.

2 **Edge Services Gateway**를 선택하고 디바이스 이름을 입력합니다.

이 이름은 vCenter 인벤토리에 나타납니다. 이 이름은 단일 테넌트 내의 모든 ESG에서 고유해야 합니다.

필요한 경우 호스트 이름을 입력할 수도 있습니다. 이 이름이 CLI에 표시됩니다. 호스트 이름을 지정하지 않으면 자동으로 생성되는 Edge ID가 CLI에 표시됩니다.

필요한 경우 설명과 테넌트를 입력하고 HA(고가용성)를 사용하도록 설정할 수 있습니다.

예:

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Name and description

Install Type: ☒ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☐ Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.

Name:

Hostname:

Description:

Tenant:

☒ Deploy NSX Edge
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☐ Enable High Availability
Enable HA, for enabling and configuring High Availability.

Back Next Finish Cancel

3 ESG의 암호를 입력하고 다시 입력합니다.

암호는 최소 12자여야 하고 다음 4개 규칙 중 3개를 준수해야 합니다.

- 하나 이상의 대문자
- 하나 이상의 소문자
- 하나 이상의 숫자
- 하나 이상의 특수 문자

4 (선택 사항) SSH, 고가용성, 자동 규칙 생성 및 FIPS 모드를 사용하도록 설정하고 로그 수준을 설정합니다.

자동 규칙 생성을 사용하도록 설정하지 않을 경우 로드 밸런싱, VPN 등의 NSX Edge 서비스에 대한 제어 트래픽을 허용하도록 방화벽, NAT 및 라우팅 구성을 수동으로 추가해야 합니다. 자동 규칙 생성을 사용해도 데이터 채널 트래픽에 대한 규칙은 생성되지 않습니다.

기본적으로 SSH 및 HA는 사용하지 않도록 설정되어 있고, 자동 규칙 생성은 사용하도록 설정되어 있습니다.

기본적으로 FIPS 모드는 사용하지 않도록 설정되어 있습니다.

기본적으로 로그 수준은 긴급입니다.

예:

- 5 시스템 리소스에 따라 NSX Edge 인스턴스의 크기를 선택합니다.

중형(Large) NSX Edge에는 **소형(Compact)** NSX Edge보다 CPU, 메모리 및 디스크 공간이 더 많이 있으므로 지원하는 동시 SSL VPN-Plus 사용자 수가 더 많습니다. **초대형(X-Large)** NSX Edge는 수백만 개의 동시 세션에서 로드 밸런서를 사용하는 환경에 적합합니다. 처리량이 많고 속도가 빠른 연결이 필요할 경우 대형 NSX Edge가 적합합니다.

[장 1 NSX의 시스템 요구 사항](#)을 참조하십시오.

- 6 Edge 장치를 생성합니다.

vCenter 인벤토리에 추가되는 ESG 가상 장치에 대한 설정을 입력합니다. 장치를 추가하지 않은 상태로 NSX Edge를 설치하면 장치를 추가할 때까지 NSX Edge가 오프라인 모드로 유지됩니다.

HA를 사용하도록 설정한 경우 두 개 장치를 추가할 수 있습니다. 한 장치만 추가하면 NSX Edge가 대기 장치를 위해 해당 구성을 복제합니다. 이는 DRS 및 vMotion을 사용한 후에도 두 HA NSX Edge 가상 시스템이 동일한 ESX 호스트에 있지 않도록 보장하기 위해서입니다(단, 수동으로 vMotion을 통해 동일한 호스트로 이동하는 경우는 제외). HA가 올바르게 작동하려면 공유 데이터스토어에 두 장치를 모두 배포해야 합니다.

예:

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool:	*	Management & Edge ...	▼
Datastore:	*	ds-1	▼
Host:		esxmgt-01a.corp.local	▼
Folder:		Discovered virtual mac...	▼

- 7 Edge를 배포 모드에서 추가하려면 **NSX Edge 배포(Deploy NSX Edge)**를 선택합니다. Edge를 배포하려면 먼저 Edge에 대한 장치 및 인터페이스를 구성해야 합니다.
- 8 인터페이스를 구성합니다.

ESG에서 IPv4 및 IPv6 주소가 모두 지원됩니다.

HA가 작동하려면 내부 인터페이스를 하나 이상 추가해야 합니다.

인터페이스에는 겹치지 않는 서브넷이 여러 개 포함될 수 있습니다.

인터페이스에 대한 IP 주소를 둘 이상 입력하는 경우 기본 IP 주소를 선택할 수 있습니다. 인터페이스는 하나의 기본 IP 주소와 여러 개의 보조 IP 주소를 사용할 수 있습니다. NSX Edge는 기본 IP 주소를 로컬에서 생성된 트래픽(예: 원격 syslog 및 운영자가 시작한 ping)의 소스 주소로 간주합니다.

IP 주소를 기능 구성에 사용하기 전 인터페이스에 추가해야 합니다.

필요한 경우 인터페이스에 대한 MAC 주소를 입력할 수 있습니다.

나중에 API 호출을 사용하여 MAC 주소를 변경하는 경우 MAC 주소를 변경한 후에 Edge를 다시 배포해야 합니다.

HA를 사용하도록 설정한 경우 두 개의 관리 IP 주소를 CIDR 형식으로 입력할 수도 있습니다. 두 NSX Edge HA 가상 시스템의 하트비트가 이러한 관리 IP 주소를 통해 통신합니다. 관리 IP 주소는 동일한 L2/서브넷에 있어야 하며 서로 통신할 수 있어야 합니다.

필요한 경우 MTU를 수정할 수 있습니다.

ESG가 다른 시스템을 대상으로 한 ARP 요청에 응답할 수 있도록 허용하려면 프로시 ARP를 사용하도록 설정합니다. 예를 들어, WAN 연결의 양쪽에 동일한 서브넷이 있는 경우 유용합니다.

라우팅 정보를 호스트에 전달하려면 ICMP 리디렉션을 사용하도록 설정합니다.

역방향 경로 필터링을 사용하도록 설정하여 전달될 패킷의 소스 주소가 연결되는지 확인합니다. 사용 모드에서는 라우터가 반환 패킷을 전달하는 데 사용할 인터페이스에서 패킷을 수신해야 합니다. 소프트웨어 모드에서는 소스 주소가 라우팅 테이블에 나타나야 합니다.

서로 다른 **fence** 환경에서 IP 및 MAC 주소를 다시 사용할 경우 **fence** 매개 변수를 구성합니다. 예를 들어, CMP(Cloud Management Platform)에서 Fence를 사용하면 완전히 분리되거나 "fence"된 동일한 IP 및 MAC 주소를 사용하여 여러 클라우드 인스턴스를 동시에 실행할 수 있습니다.

예:

Edit NSX Edge Interface

vNIC#: 1

Name:

Type: ☒ Internal ☐ Uplink

Connected To: [Change](#) [Remove](#)

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

IP Address	Subnet Prefix Length
192.168.10.1*	29

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect Reverse Path Filter [Disable](#) ▼

Fence Parameters:

Example: ethernet0.filter1.param1=1

[OK](#) [Cancel](#)

다음 예제에서 두 개 인터페이스를 보여주는데 하나는 vSphere Distributed Switch에서 업링크 포트 그룹을 통해 ESG를 외부에 연결하고 있고, 다른 하나는 논리적 분산 라우터가 연결되어 있는 논리적 전송 스위치에 ESG를 연결하고 있습니다.

New NSX Edge

✓ 1 Name and description
 ✓ 2 Settings
 ✓ 3 Configure deployment
 ✓ 4 **Configure interfaces**
 5 Default gateway settings
 6 Firewall and HA
 7 Ready to complete

Configure interfaces

Configure interfaces of this NSX Edge

+ ✎ ✕

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	uplink	192.168.100.3	24	Mgmt_VDS - HQ_Uplink
1	internal	192.168.10.1*	29	transit-switch

Back Next Finish Cancel

9 기본 게이트웨이를 구성합니다.

MTU 값을 편집할 수 있지만, 인터페이스에 구성된 MTU보다 클 수는 없습니다.

예:

New NSX Edge

✓ 1 Name and description
 ✓ 2 Settings
 ✓ 3 Configure deployment
 ✓ 4 Configure interfaces
5 Default gateway settings
 6 Firewall and HA
 7 Ready to complete

Default gateway settings

☒ Configure Default Gateway

vNIC: * uplink

Gateway IP: * 192.168.100.2

MTU: 1500

Back Next Finish Cancel

10 방화벽 정책, 로깅 및 HA 매개 변수를 구성합니다.

경고 방화벽 정책을 구성하지 않을 경우 모든 트래픽을 거부하도록 기본 정책이 설정됩니다.

기본적으로 모든 새 **NSX Edge** 장치에서 로그가 사용되도록 설정되어 있습니다. 기본 로깅 수준은 [알림]입니다. 로그가 **ESG**에 로컬로 저장된 경우 로깅을 수행하면 너무 많은 로그가 생성되고 **NSX Edge**의 성능에 영향을 줄 수 있습니다. 이러한 이유로 원격 **Syslog** 서버를 구성하고, 분석 및 모니터링을 위해 모든 로그를 중앙 수집기로 전달하는 것이 좋습니다.

HA를 사용하도록 설정한 경우 **HA** 섹션을 완료하십시오. 기본적으로 **HA**에서는 자동으로 내부 인터페이스를 선택하고 링크-로컬 **IP** 주소를 할당합니다. **NSX Edge**는 고가용성을 위해 두 개의 가상 시스템을 지원하며 둘 다 사용자 구성으로 최신으로 유지됩니다. 기본 가상 시스템에서 하트비트 오류가 발생하면 보조 가상 시스템이 활성 상태로 변경됩니다. 따라서 네트워크에서 **NSX Edge** 가상 시스템 하나는 항상 활성 상태입니다. **NSX Edge**는 대기 장치를 위해 기본 장치의 구성을 복제하며, **DRS** 및 **vMotion**을 사용한 후에도 두 **HA NSX Edge** 가상 시스템이 동일한 **ESX** 호스트에 있지 않도록 보장합니다. 두 가상 시스템은 구성된 장치와 동일한 리소스 풀 및 데이터스토어의 **vCenter**에 배포됩니다. 서로 통신할 수 있도록 **NSX Edge HA**의 **HA** 가상 시스템에 로컬 링크 **IP** 주소가 할당됩니다. **HA** 매개 변수

수를 구성할 내부 인터페이스를 선택합니다. 인터페이스에 대해 [임의]를 선택하지만 구성된 내부 인터페이스가 없는 경우 UI에서 오류를 표시합니다. 두 개의 Edge 장치가 생성되지만 구성된 내부 인터페이스가 없기 때문에 새 Edge는 대기 상태를 유지하고 HA는 사용하지 않도록 설정됩니다. 내부 인터페이스가 구성되면 Edge 장치에서 HA가 사용하도록 설정됩니다. 지정한 시간 내에 백업 장치가 기본 장치로부터 하트비트 신호를 받지 못하면 기본 장치를 비활성 상태로 간주하여 백업 장치가 작업을 맡도록 할 기간(초)을 입력합니다. 기본 간격은 15초입니다. 필요한 경우 HA 가상 시스템에 할당된 로컬 링크 IP 주소를 재정의하려면 관리 IP 주소 두 개를 CIDR 형식으로 입력할 수 있습니다. 관리 IP 주소가 다른 인터페이스에서 사용되는 IP 주소와 겹치지 않고 트래픽 라우팅을 방해하지 않는지 확인합니다. 네트워크가 NSX Edge에 직접 연결되어 있지 않은 경우에도 해당 네트워크상의 어딘가에 존재하는 IP 주소를 사용해서는 안 됩니다.

예:

결과

ESG가 배포된 후 호스트 및 클러스터 보기로 이동하고 Edge 가상 장치의 콘솔을 엽니다. 콘솔에서 연결된 인터페이스를 Ping할 수 있는지 확인합니다.

다음에 수행할 작업

NSX Edge 장치를 설치할 때 vSphere HA가 클러스터에서 사용되지 않도록 설정되어 있으면 NSX는 호스트에서 자동 VM 시작/종료를 사용하도록 설정합니다. 장치 VM이 나중에 클러스터의 다른 호스트로 마이그레이션되는 경우 새 호스트가 자동 VM 시작/종료를 사용하도록 설정하지 않을 수도 있습니다. 이러한 이유로 vSphere HA가 사용되지 않도록 설정된 클러스터에서 NSX Edge 장치를 설치할 때는 클러스터의 모든 호스트를 점검하여 자동 VM 시작/종료가 사용되도록 설정되어 있는지 확인해야 합니다. "vSphere 가상 시스템 관리"에서 "가상 시스템 시작 및 종료 설정 편집"을 참조하십시오.

이제 외부 디바이스에서 VM으로 연결을 허용하도록 라우팅을 구성할 수 있습니다.

글로벌 구성 지정

정적 경로에 대한 기본 게이트웨이를 구성하고 Edge Services Gateway 또는 논리적 분산 라우터에 대한 동적 라우팅 세부 정보를 지정할 수 있습니다.

작동하는 NSX Edge 인스턴스가 있어야 인스턴스에서 라우팅을 구성할 수 있습니다. NSX Edge 설정에 대한 자세한 내용은 [NSX Edge 구성](#) 항목을 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 라우팅(Routing)을 클릭한 후 글로벌 구성(Global Configuration)을 클릭합니다.
- 5 ECMP(동일 비용 다중 경로 라우팅)를 사용하도록 설정하려면 ECMP 옆의 시작(Start)을 클릭합니다.

ECMP는 단일 대상에게 다수의 최적의 경로로 다음 홉 패킷 전달을 가능하게 하는 라우팅 전략입니다. 이러한 최적의 경로는 정적 라우팅이나 OSPF 또는 BGP와 같은 동적 라우팅 프로토콜에 의한 메트릭 계산의 결과로 추가될 수 있습니다. 정적 경로에 다수의 경로를 추가하려면 정적 경로 대화 상자에 다수의 다음 홉을 쉼표로 구분하여 저장합니다. 자세한 내용은 [정적 경로 추가](#) 항목을 참조하십시오.

Edge Services Gateway는 임의성 구성 요소가 포함된 라운드 로빈 알고리즘에 해당하는 Linux 네트워크 스택 구현을 사용합니다. 특정 소스 및 대상 IP 주소 쌍에 대해 다음 홉이 선택된 후에 경로 캐시가 선택된 다음 홉을 저장합니다. 해당 흐름의 모든 패킷은 선택된 다음 홉으로 이동합니다. 기본 IPv4 경로의 캐시 시간 초과는 300초입니다 (gc_timeout). 이 시간 동안 입력이 없으면 경로 캐시에서 제거됩니다. 실제 제거는 가비지 수집 타이머가 활성화될 때(gc_interval = 60초) 발생합니다.

논리적 분산 라우터는 XOR 알고리즘을 이용하여 가능한 ECMP 다음 홉 목록에서 다음 홉을 결정합니다. 이 알고리즘은 송신 패킷의 소스 및 대상 IP 주소를 엔트로피 소스로 사용합니다.

로드 밸런싱, VPN, NAT 및 ESG 방화벽과 같은 상태 저장 서비스는 ECMP에서 작동하지 않습니다. 그렇지만 NSX 6.1.3 이후로 ECMP와 분산 방화벽이 함께 작동할 수 있습니다.

- 6 (UDLR에만 해당): **라우팅 구성(Routing Configuration)** 옆의 논리적 분산 라우터에서 **로케일 ID(Locale ID)**를 변경하려면 **편집(Edit)**을 클릭합니다. 로케일 ID를 입력한 후 **저장** 또는 **확인**을 클릭합니다.

기본적으로 로케일 ID는 NSX Manager UUID로 설정됩니다. 그러나 범용 논리적 분산 라우터를 생성할 때 로컬 송신을 사용하도록 설정하여 로케일 ID를 재정의할 수 있습니다. 로케일 ID는 크로스 vCenter NSX 또는 다중 사이트 환경에서 선택적으로 경로를 구성할 때 사용됩니다. 자세한 내용은 [크로스 vCenter NSX 토폴로지](#) 항목을 참조하십시오.

로케일 ID는 UUID 형식이어야 합니다. 예를 들어, XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX입니다. 여기서 각 X는 기본 16자리 영숫자(0-F)로 대체됩니다.

- 7 기본 게이트웨이를 지정하려면 **기본 게이트웨이(Default Gateway)** 옆의 **편집(Edit)**을 클릭합니다.

- 대상 네트워크로 향하는 그 다음 홉에 연결할 수 있는 인터페이스를 선택합니다.
- 게이트웨이 IP를 입력합니다.
- (선택 사항) 로케일 ID를 입력합니다. 로케일 ID는 범용 논리적 라우터에서만 사용할 수 있습니다.
- (선택 사항) MTU를 편집합니다.
- 메시지가 나타나면 **Admin Distance**를 입력합니다.

1에서 255 사이의 값을 선택합니다. 지정한 네트워크에 대해 다중 경로가 있는 경우 사용할 경로를 Admin Distance를 사용하여 선택합니다. Admin Distance가 낮을수록 경로에 대한 기본 설정이 높습니다.

표 9-1. 기본 Admin Distance

경로 소스	기본 Admin Distance
연결됨	0
정적	1
외부 BGP	20
OSPF 영역 내부	30
OSPF 영역 내부	110
내부 BGP	200

- (선택 사항) 기본 게이트웨이에 대한 설명을 입력합니다.
- 저장(Save)**을 클릭합니다.

8 동적 라우팅을 구성하려면 **동적 라우팅 구성(Dynamic Routing Configuration)** 옆의 **편집(Edit)**을 클릭합니다.

- a **라우터 ID(Router ID)**는 동적 라우팅을 위해 경로를 커널까지 보내는 NSX Edge의 첫 번째 업링크 IP주소를 나타냅니다.
- b 여기에는 어떤 프로토콜도 사용하지 않습니다.
- c 로깅 정보를 저장하려면 **로깅 사용(Enable Logging)**을 선택하고 로그 수준을 선택합니다.

참고 환경에 IPSec VPN이 구성되어 있는 경우 동적 라우팅을 사용해서는 안됩니다.

9 **변경 내용 게시(Publish Changes)**를 클릭합니다.

다음에 수행할 작업

라우팅 구성을 삭제하려면 **재설정(Reset)**을 클릭합니다. 그러면 기본, 정적, OSPF, BGP 구성 및 경로 재 배포까지 포함하여 모든 라우팅 구성이 삭제됩니다.

NSX Edge 구성

작동하는 NSX Edge를 설치하면(즉, 하나 이상의 장치와 인터페이스를 추가하고 기본 게이트웨이, 방화벽 정책 및고가용성 구성) NSX Edge 서비스를 사용할 수 있습니다.

인증서 사용

NSX Edge는 자체 서명 인증서, CA(인증 기관)에서 서명한 인증서 및 CA에서 생성하고 서명한 인증서를 지원합니다.

CA 서명된 인증서 구성

CSR를 생성하고 CA의 서명을 받을 수 있습니다. CSR를 글로벌 수준에서 생성하면 인벤토리의 모든 NSX Edge에서 CSR을 사용할 수 있습니다.

절차

1 다음 중 하나를 수행합니다.

옵션	설명
글로벌 인증서를 생성하려면	<ul style="list-style-type: none"> a NSX Manager 가상 장치에 로그인합니다. b [관리] 탭을 클릭하고 [SSL 인증서]를 클릭합니다. c CSR 생성(Generate CSR)을 클릭합니다.
NSX Edge용 인증서를 생성하려면	<ul style="list-style-type: none"> a vSphere Web Client에 로그인합니다. b Networking & Security를 클릭한 후 Edge 서비스(Edge Services)를 클릭합니다. c NSX Edge를 두 번 클릭합니다. d 관리(Manage) 탭을 클릭하고 설정(Settings)을 클릭합니다. e 인증서(Certificates) 링크를 클릭합니다. f 작업(Actions)을 클릭하고 CSR 생성(Generate CSR)을 선택합니다.

2 조직 구성 단위 및 이름을 입력합니다.

3 조직의 상세 주소, 구/군/시, 시/도 및 국가를 입력합니다.

4 호스트 간 통신에 대한 암호화 알고리즘을 선택합니다.

SSL VPN-Plus는 RSA 인증서만 지원합니다.

5 필요한 경우 기본 키 크기를 편집합니다.

6 글로벌 인증서의 경우 인증서에 대한 설명을 입력합니다.

7 **확인(OK)**을 클릭합니다.

CSR이 생성되고 인증서 목록에 표시됩니다.

8 온라인 인증 기관을 통해 이 CSR에 서명을 받습니다.

9 서명된 인증서를 가져옵니다.

a 서명된 인증서의 콘텐츠를 복사합니다.

b 다음 중 하나를 수행합니다.

- 글로벌 수준에서 서명된 인증서를 가져오려면 NSX Manager 가상 장치에서 **가져오기(Import)**를 클릭합니다.

- NSX Edge용으로 서명된 인증서를 가져오려면 **작업(Actions)**을 클릭하고 **인증서(Certificates)** 탭에서 **인증서 가져오기(Import Certificate)**를 선택합니다.

c CSR 가져오기 대화상자에서 서명된 인증서의 콘텐츠를 붙여 넣습니다.

d **확인(OK)**을 클릭합니다.

CA 서명된 인증서가 인증서 목록에 나타납니다.

CA 인증서 추가

CA 인증서를 추가하면 회사의 임시 CA가 될 수 있습니다. 그러면 사용자 본인의 인증서에 서명할 권한을 갖게 됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 설정(Settings) 탭에 있는지 확인합니다.
- 5 인증서(Certificates)를 클릭합니다.
- 6 추가(Add)(+) 아이콘을 클릭하고 CA 인증서(CA Certificate.)를 선택합니다.
- 7 인증서 콘텐츠를 복사하여 인증서 콘텐츠 텍스트 상자에 붙여 넣습니다.
- 8 CA 인증서에 대한 설명을 입력합니다.
- 9 확인(OK)을 클릭합니다.

이제 사용자 본인의 인증서에 서명할 수 있습니다.

체인 인증서 추가

중간 및 루트 CA 인증서를 사용하여 체인된 서버 인증서를 추가하려면 서버 인증서(PEM 파일), 서버용 개인 키, 중간 및 루트 인증서가 필요합니다.

서버 인증서를 NSX Edge에서 중간 인증서와 연결된 인증서로 가져오려면:

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 설정(Settings) 탭에 있는지 확인합니다.
- 5 인증서(Certificates)를 클릭합니다.
- 6 추가(Add)(+) 아이콘을 클릭하고 인증서(Certificate.)를 선택합니다.
- 7 인증서 콘텐츠(Certificates Contents) 텍스트 상자에서 서버 cert.pem 파일의 콘텐츠를 붙여넣고 중간 인증서 및 루트 인증서의 콘텐츠를 추가합니다.

인증서 체인에서 인증서의 순서는 다음과 같아야 합니다.

- 서버 인증서
- 중간 CA 인증서(개수는 상관 없음)
- 루트 CA 인증서

각 인증서에는 다음 예와 같이 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 줄이 포함되어야 합니다.

```
-----BEGIN CERTIFICATE-----
    Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Root cert
-----END CERTIFICATE-----
```

8 개인 키(Private Key) 텍스트 상자에 서버의 개인 키 콘텐츠를 붙여넣습니다.

다음은 개인 키 콘텐츠의 예입니다.

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END RSA PRIVATE KEY-----
```

9 서버 개인 키의 암호를 입력하고 확인을 위해 암호를 다시 입력합니다.

10 (선택 사항) 체인 인증서에 대한 설명을 입력합니다.

11 확인(OK)을 클릭합니다.

결과

인증서를 가져오면 해당 중간 인증서와 연결된 서버 인증서가 **인증서 세부 정보(Certificate Details)** 아래에 표시됩니다.

자체 서명된 인증서 구성

자체 서명된 서버 인증서를 생성, 설치 및 관리할 수 있습니다.

사전 요구 사항

사용자 본인의 인증서에 서명할 수 있도록 **CA** 인증서가 있는지 확인합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭에 있는지 확인합니다.
- 5 **인증서(Certificates)**를 클릭합니다.

6 아래에 있는 단계를 수행하여 **CSR**을 생성합니다.

- a **작업(Actions)**을 클릭하고 **CSR 생성(Generate CSR)**을 선택합니다.
- b 일반 이름에 **NSX Manager**의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.
- c 조직 이름 및 조직 구성 단위를 입력합니다.
- d 조직의 상세 주소, 구/군/시, 시/도 및 국가를 입력합니다.
- e 호스트 간 통신에 대한 암호화 알고리즘을 선택합니다.

SSL VPN-Plus는 RSA 인증서만 지원합니다. 이전 버전과 호환될 수 있도록 RSA를 사용하는 것이 좋습니다.

- f 필요한 경우 기본 키 크기를 편집합니다.
- g 인증서에 대한 설명을 입력합니다.
- h **확인(OK)**을 클릭합니다.

CSR이 생성되고 인증서 목록에 표시됩니다.

7 생성한 인증서가 선택되었는지 확인합니다.

8 **작업(Actions)**을 클릭하고 **인증서 자체 서명(Self Sign Certificate)**을 선택합니다.

9 자체 서명 인증서의 유효 기간(일)을 입력합니다.

10 **확인(OK)**을 클릭합니다.

클라이언트 인증서 사용

클라이언트 인증서를 생성한 후에 이 인증서를 원격 사용자에게 배포할 수 있습니다. 그러면 해당 사용자는 웹 브라우저에서 인증서를 설치할 수 있습니다.

클라이언트 인증서를 구현할 때의 주요 이점은 **NSX Edge** 로드 밸런서가 클라이언트에 해당 클라이언트 인증서를 요청하고, 유효성을 검사한 후 웹 요청을 백엔드 서버로 전달할 수 있다는 것입니다. 클라이언트 인증서가 손실되어 해지되었거나 클라이언트가 더 이상 회사에서 작동하지 않을 경우 **NSX Edge**는 해당 클라이언트 인증서가 인증 해지 목록에 속하지 않는지 확인합니다.

NSX Edge 클라이언트 인증서는 애플리케이션 프로파일에서 구성됩니다.

클라이언트 인증서 생성에 대한 자세한 내용은 [시나리오: SSL 클라이언트 및 서버 인증](#)을 참조하십시오.

인증서 해지 목록 추가

CRL(인증서 해지 목록)은 구독자와 각 구독자의 상태를 보여 주는 목록으로, **Microsoft**에서 제공하고 서명합니다.

인증서 해지 목록에는 다음 항목이 포함됩니다.

- 해지된 인증서와 해지 이유
- 인증서가 발급된 날짜

- 인증서를 발급한 단체
- 제안된 다음 릴리스 날짜

잠재적 사용자가 서버에 액세스하면 서버가 해당 특정 사용자의 **CRL** 항목을 기준으로 액세스를 허용하거나 거부합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭에 있는지 확인합니다.
- 5 **인증서(Certificates)**를 클릭합니다.
- 6 **추가(Add)(+)** 아이콘을 클릭하고 **CRL**을 선택합니다.
- 7 **인증서 콘텐츠(Certificate contents)**에서 목록을 붙여 넣습니다.
- 8 (선택 사항) 설명을 입력합니다.
- 9 **확인(OK)**을 클릭합니다.

FIPS 모드

FIPS 모드를 사용하도록 설정하면 NSX Edge와의 모든 보안 통신은 미국 FIPS(연방 정부 처리 표준)에서 허용하는 암호화 알고리즘/프로토콜을 사용합니다. FIPS 모드에서는 FIPS를 준수하는 암호 제품군이 켜집니다.

구성 요소를 구성할 때 구성 요소가 FIPS 사용 Edge에서 FIPS와 호환되지 않거나 FIPS와 호환되지 않는 암호화 또는 인증 메커니즘이 있는 Edge에서 FIPS를 사용하도록 설정하면 NSX Manager는 작업에 실패하며 유효한 오류 메시지를 제공합니다.

FIPS 모드 및 비 FIPS 모드 간 기능 차이

구성 요소	기능	FIPS 모드	비 FIPS 모드
SSL VPN	RADIUS 인증	사용할 수 없음	사용할 수 있음
SSL VPN	RSA 인증	사용할 수 없음	사용할 수 있음
TLS 프로토콜	TLSv1.0	사용할 수 없음	사용할 수 있음
라우팅	OSPF, BGP - 암호 MD5 인증	사용할 수 없음	사용할 수 있음
IPSec VPN	PSK 인증	사용할 수 없음	사용할 수 있음
IPSec VPN	DH2 및 DH5 그룹	사용할 수 없음	사용할 수 있음
IPSec VPN	DH14, DH15 및 DH16 그룹	사용할 수 있음	사용할 수 있음
IPSec VPN	AES-GCM 알고리즘	사용할 수 없음	사용할 수 있음

NSX Edge에서 FIPS 모드 변경

FIPS 모드를 사용하도록 설정하면 FIPS를 준수하는 암호 제품군이 켜집니다. 따라서 NSX Edge와의 모든 보안 통신에 FIPS에서 허용하는 암호화 알고리즘 또는 프로토콜이 사용됩니다.

경고 FIPS 모드를 변경하면 NSX Edge 장치가 재부팅되어 일시적인 트래픽 중단이 발생합니다. 이러한 현상은 고가용성의 사용 설정 여부와 관계없이 나타납니다.

요구 사항에 따라 일부 또는 전체 NSX Edge 장치에서 FIPS를 사용하도록 설정할 수 있습니다. FIPS 사용 가능 NSX Edge 장치는 FIPS가 사용하도록 설정되지 않은 NSX Edge 장치와 통신할 수 있습니다.

논리적(분산) 라우터가 NSX Edge 장치 없이 배포되면 FIPS 모드를 수정할 수 없습니다. 논리적 라우터에는 NSX Controller 클러스터와 동일한 FIPS 모드가 자동으로 적용됩니다. NSX Controller 클러스터가 NSX 6.3.0 이상이면 FIPS가 사용되도록 설정됩니다.

기본 및 보조 NSX Manager에 여러 NSX Edge 장치가 배포된 크로스 vCenter NSX 환경의 범용 논리적(분산) 라우터에서 FIPS 모드를 변경하려면 범용 논리적(분산) 라우터와 연결된 모든 NSX Edge 장치에서 FIPS 모드를 변경해야 합니다.

고가용성이 사용하도록 설정된 NSX Edge 장치에서 FIPS 모드를 변경하는 경우 두 장치에서 FIPS가 사용되도록 설정되고 장치는 하나씩 차례로 재부팅됩니다.

독립 실행형 Edge에 대해 FIPS 모드를 변경하려면 `fips enable` 또는 `fips disable` 명령을 사용하십시오. 자세한 내용은 "NSX 명령줄 인터페이스 참조"를 참조하십시오.

사전 요구 사항

- 파트너 솔루션이 인증된 FIPS 모드인지 확인합니다. 자세한 내용은 VMware 호환성 가이드(<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>)를 참조하십시오.
- 이전 버전의 NSX에서 업그레이드한 경우 NSX 6.3.0으로 업그레이드될 때까지 FIPS 모드를 사용하도록 설정하지 마십시오. "NSX 업그레이드 가이드"에서 "FIPS 모드 및 NSX 업그레이드 이해"를 참조하십시오.
- NSX Manager가 NSX 6.3.0 이상인지 확인하십시오.
- NSX Controller 클러스터가 NSX 6.3.0 이상인지 확인하십시오.
- NSX 워크로드가 실행되는 모든 호스트 클러스터가 NSX 6.3.0 이상으로 준비되어 있는지 확인하십시오.
- 모든 NSX Edge 장치가 버전 6.3.0 이상인지 확인하십시오.

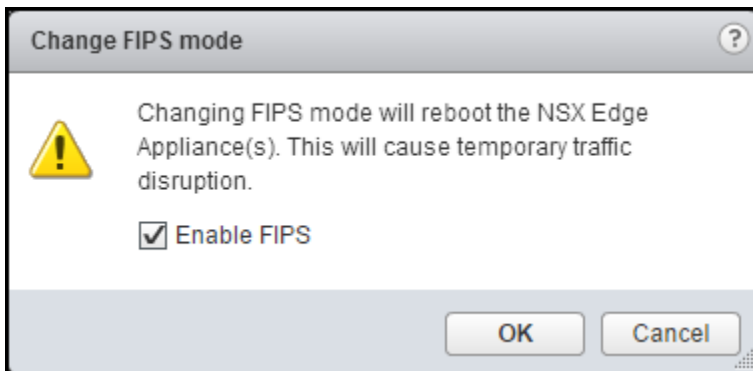
- 메시징 인프라의 상태가 녹색인지 확인하십시오. API 메서드 GET /api/2.0/nwfabric/status?resource={resourceId}를 사용합니다. 여기서 resourceId는 호스트 또는 클러스터의 vCenter 관리 개체 ID입니다. 응답 본문에서 com.vmware.vshield.vsm.messagingInfra의 featureId에 해당하는 status를 확인하십시오.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)을 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 필요한 Edge 또는 라우터를 선택하고 작업(Actions)(⚙️)을 클릭한 후 FIPS 모드 변경(Change FIPS mode)을 선택합니다.

FIPS 모드 변경(Change FIPS mode) 대화 상자가 나타납니다.



- 4 FIPS 사용(Enable FIPS) 확인란을 선택하거나 선택 취소합니다. 확인(OK)을 클릭합니다.

NSX Edge가 재부팅되고 FIPS 모드가 사용되도록 설정됩니다.

다음에 수행할 작업

필요한 경우 [NSX Manager](#)에서 FIPS 모드 및 TLS 설정 변경.


장치 관리

장치를 추가, 편집 또는 삭제할 수 있습니다. 장치를 하나 이상 추가할 때까지 NSX Edge 인스턴스는 오프라인 상태로 유지됩니다.

장치 추가

배포하기 전에 NSX Edge에 장치를 하나 이상 추가해야 합니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다.
- 5 **Edge Gateway Appliance(Edge Gateway Appliances)**에서 **추가(Add)**() 아이콘을 클릭합니다.
- 6 장치에 대한 클러스터를 선택하거나 리소스 풀과 데이터스토어를 선택합니다.
- 7 (선택 사항) 장치를 추가할 호스트를 선택합니다.
- 8 (선택 사항) 장치를 추가할 vCenter 폴더를 선택합니다.
- 9 **추가(Add)**를 클릭합니다.

장치 편집

NSX Edge 장치를 편집할 수 있습니다.

절차


- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다.
- 5 **Edge Gateway Appliance(Edge Gateway Appliances)**에서 변경할 장치를 선택합니다.
- 6 **편집(Edit)**() 아이콘을 클릭합니다.
- 7 Edge Appliance 편집 대화상자에서 필요한 내용을 변경합니다.
- 8 **저장(Save)**을 클릭합니다.

장치 삭제

NSX Edge 장치를 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다.
- 5 **Edge Gateway Appliance(Edge Gateway Appliances)**에서 삭제할 장치를 선택합니다.

6 삭제(Delete)() 아이콘을 클릭합니다.

NSX Edge 장치 리소스 예약 관리

NSX for vSphere는 vSphere 리소스 할당을 사용하여 NSX Edge 장치의 리소스를 예약합니다. NSX Edge에 대한 CPU 및 메모리 리소스를 예약하면 장치는 정상적으로 작동되는 데 필요한 충분한 리소스가 확보됩니다.

API를 사용하여 NSX Edge 장치의 리소스 예약을 설정할 수 있습니다. POST /api/4.0/edges를 사용하여 NSX Edge를 생성할 때 예약을 구성할 수 있습니다. PUT /api/4.0/edges/{edgeId}/appliances를 사용하여 기존 NSX Edge에 대한 예약을 업데이트할 수도 있습니다. cpuReservation> reservation 및 memoryReservation > reservation을 사용하여 리소스 예약을 설정했습니다. 자세한 내용은 "NSX API 가이드" 항목을 참조하십시오.

NSX 6.3.3부터는 vSphere Web Client를 사용하여 NSX Edge 장치의 리소스 예약을 설정할 수도 있습니다. NSX Edge를 생성할 때 예약 방법을 제공하라는 메시지가 표시됩니다. 장치를 편집하여 기존 NSX Edge의 예약을 변경할 수도 있습니다. **Networking & Security > NSX Edge > NSX Edge 인스턴스 > 관리 > 설정 > 구성**으로 이동한 후 장치를 편집합니다.

리소스 예약 방법에는 **시스템 관리**, **사용자 지정** 또는 **예약 없음**의 세 가지가 있습니다.

중요 NSX Edge 장치에 대해 **사용자 지정** 또는 **예약 없음** 예약을 선택한 경우 를 사용하여 **시스템 관리**로 다시 전환할 수 없습니다.

시스템 관리 리소스 예약

시스템 관리를 선택하면 시스템은 새 NSX Edge 장치에 사용할 CPU 및 메모리 리소스를 예약합니다. 예약된 리소스는 장치 크기에 대한 시스템 요구 사항과 동일하며, 조정 구성 API를 사용하여 설정한 백분율을 기준으로 수정됩니다.

API를 사용하여 NSX Edge 장치를 생성하고, 요청에 CPU 또는 메모리 예약을 명시적으로 설정하지 않는 것은 vSphere Web Client에서 리소스 예약을 **시스템 관리**로 설정하는 것과 같습니다.

시스템 관리 리소스 예약이 있는 NSX Edge 장치가 배포되면(설치, 업그레이드 또는 다시 배포 중에) 장치의 전원이 켜진 후 리소스 풀에 예약이 적용됩니다. 리소스가 부족한 경우 예약이 실패하고 시스템 이벤트가 생성되지만 장치 배포는 성공적으로 수행됩니다. 다음 번에 장치를 배포할 때(업그레이드 또는 배포 중에) 예약을 시도합니다.

시스템 관리 리소스 예약을 사용하는 경우 장치 크기를 변경하면 시스템에서 새 장치 크기의 시스템 요구 사항에 맞게 리소스 예약을 업데이트합니다.

사용자 지정 리소스 예약

사용자 지정을 선택하는 경우 사용자가 NSX Edge 장치에 대한 리소스 예약을 결정합니다.

API를 사용하여 NSX Edge 장치를 생성하고, 요청에 CPU 또는 메모리 예약을 명시적으로 설정하는 것은 vSphere Web Client에서 리소스 예약을 **사용자 지정**으로 설정하는 것과 같습니다.

사용자 지정 리소스 예약이 있는 NSX Edge 장치가 배포되면(설치, 업그레이드 또는 다시 배포 중에) 장치의 전원을 켜기 전에 리소스 풀에 예약이 적용됩니다. 리소스가 충분하지 않으면 장치의 전원이 켜지지 않고 장치 배포가 실패합니다.

NSX Edge 장치를 배포한 후 **사용자 지정** 예약을 적용할 수 있습니다. 리소스 풀에 충분한 리소스가 없는 경우 구성 변경이 실패합니다.

사용자 지정 리소스 예약을 사용하면 시스템에서 장치에 대한 리소스 예약을 추가하거나 변경하지 않습니다. 장치 크기를 변경하면 장치 시스템 요구 사항이 변경되지만 시스템에서 리소스 예약을 업데이트하지 않습니다. 새 장치 크기의 시스템 요구 사항을 반영하도록 리소스 예약을 변경해야 합니다.

vSphere Web Client 또는 API를 사용하여 사용자 지정 리소스 예약을 변경할 수 있습니다.

리소스 예약 없음

예약 없음을 선택하면 NSX Edge 장치에 대해 리소스가 예약되지 않습니다. 리소스가 부족한 호스트에는 NSX Edge 장치 배포가 허용되지 않지만, 리소스 경합이 있는 경우 장치가 정상적으로 작동하지 않을 수 있습니다.

API를 사용하여 NSX Edge 장치를 생성하고, CPU 및 메모리 예약을 명시적으로 0으로 설정하는 것은 vSphere Web Client에서 리소스 예약을 **예약 없음**으로 설정하는 것과 같습니다.

조정 구성을 사용하여 시스템 관리 리소스 예약 수정

리소스가 부족한 경우 일시적으로 **시스템 관리** 리소스 예약을 사용하지 않도록 설정하거나 기본값을 낮출 수 있습니다. 조정 구성 API PUT /api/4.0/edgePublish/tuningConfiguration에서 edgeVCpuReservationPercentage 및 edgeMemoryReservationPercentage 매개 변수 값을 구성하여 예약을 변경할 수 있습니다. 이 변경 내용은 새 NSX Edge 장치 배포에는 영향을 주지만 기존 장치에는 적용되지 않습니다. 해당 백분율 값에 따라 관련 NSX Edge 장치 크기에 대해 예약된 기본 CPU 및 메모리가 수정됩니다. 리소스 예약을 사용하지 않도록 설정하려면 값을 0으로 설정합니다. 자세한 내용은 "NSX API 가이드" 항목을 참조하십시오.

NSX Edge 장치 시스템 요구 사항

NSX Edge 장치의 시스템 요구 사항은 장치 크기(소형, 대형, 4배 대형 또는 초대형)에 따라 다릅니다. 이러한 값은 기본 **시스템 관리** 리소스 예약에 사용됩니다.

표 9-2. NSX Edge 시스템 요구 사항

장치 크기	CPU 예약	메모리 예약
소형	1000 MHz	512MB
중형	2000 MHz	1GB
대형	4000 MHz	2 GB
초대형	6000 MHz	8GB

인터페이스 사용

NSX Edge Services Gateway에는 최대 10개의 내부, 업링크 또는 트렁크 인터페이스가 있을 수 있습니다. NSX Edge 라우터에는 8개의 업링크 인터페이스와 최대 1,000개의 내부 인터페이스가 있을 수 있습니다.

NSX Edge는 내부 인터페이스가 하나 이상 있어야 배포할 수 있습니다.

인터페이스 구성


내부 인터페이스는 주로 동-서 트래픽에 사용되고 업링크 인터페이스는 북-남 트래픽에 사용됩니다.

DLR(논리적 라우터)가 ESG(Edge Services Gateway)에 연결된 경우 이 라우터의 인터페이스가 업링크 인터페이스이고 ESG의 인터페이스가 내부 인터페이스입니다. NSX 트렁크 인터페이스는 외부 네트워크가 아닌 내부 네트워크용입니다. 트렁크 인터페이스를 사용하여 여러 내부 네트워크(VLAN 또는 VXLAN)를 트렁킹할 수 있습니다.

NSX ESG(Edge Services Gateway)에는 최대 10개의 내부, 업링크 또는 트렁크 인터페이스가 있을 수 있습니다. 이러한 제한은 NSX Manager에 의해 적용됩니다.

NSX 배포 환경은 단일 ESXi 호스트에서 최대 1,000개 DLR(논리적 분산 라우터) 인스턴스를 포함할 수 있습니다. 단일 논리적 라우터에서 최대 8개 업링크 인터페이스와 최대 991개 내부 인터페이스로 구성할 수 있습니다. 이러한 제한은 NSX Manager에 의해 적용됩니다. NSX 배포 환경에서 인터페이스의 크기를 조정하는 방법에 대한 자세한 내용은 "VMware® NSX for vSphere 네트워크 가상화 설계 가이드" (<https://communities.vmware.com/docs/DOC-27683>)를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **인터페이스(Interfaces)** 탭을 클릭합니다.
- 5 인터페이스를 선택하고 **편집(Edit)**() 아이콘을 클릭합니다.
- 6 Edge 인터페이스 편집 대화상자에 인터페이스의 이름을 입력합니다.
- 7 **내부(Internal)** 또는 **업링크(Uplink)**를 선택하여 내부 인터페이스인지, 외부 인터페이스인지를 나타냅니다.

하위 인터페이스를 생성할 경우 **트렁크(Trunk)**를 선택합니다. 자세한 내용은 [하위 인터페이스 추가](#) 항목을 참조하십시오.
- 8 이 인터페이스가 연결되어야 하는 포트 그룹 또는 논리적 스위치를 선택합니다.
 - a **연결 대상(Connected To)** 필드 옆의 **선택(Select)**을 클릭합니다.
 - b 인터페이스에 연결할 항목에 따라 **논리적 스위치(Logical Switch)**, **표준 포트 그룹(Standard Portgroup)** 또는 **분산 포트 그룹(Distributed Portgroup)** 탭을 클릭합니다.

- c 적절한 논리적 스위치 또는 포트 그룹을 선택합니다.
 - d **선택(Select)**을 클릭합니다.
- 9 인터페이스의 연결 상태를 선택합니다.
- 10 **서브넷 구성(Configure Subnets)**에서 **추가(Add)**(+) 아이콘을 클릭하여 인터페이스의 서브넷을 추가합니다.
- 인터페이스에는 겹치지 않는 서브넷이 여러 개 포함될 수 있습니다.
- 11 **서브넷 추가(Add Subnet)**에서 **추가(Add)**(+) 아이콘을 클릭하여 IP 주소를 추가합니다.
- IP 주소를 하나 이상 입력하는 경우 기본 IP 주소를 선택할 수 있습니다. 인터페이스는 하나의 기본 IP 주소와 여러 개의 보조 IP 주소를 사용할 수 있습니다. NSX Edge는 기본 IP 주소를 로컬로 생성된 트래픽의 소스 주소로 간주합니다.
- IP 주소를 기능 구성에 사용하기 전 인터페이스에 추가해야 합니다.
- 12 인터페이스의 서브넷 마스크를 입력하고 **저장(Save)**을 클릭합니다.
- 13 필요한 경우 기본 MTU를 변경합니다.
- 14 **옵션(Options)**에서 필요한 옵션을 선택합니다.

옵션	설명
프록시 ARP 사용	서로 다른 인터페이스 간에 전달하는 네트워크가 겹칠 수 있습니다.
ICMP 리디렉션 보내기	호스트에 라우팅 정보를 전달합니다.
역방향 경로 필터	전달될 패킷의 소스 주소가 연결 가능한지 확인합니다. 사용 모드에서는 라우터가 반환 패킷을 전달하는 데 사용할 인터페이스에서 패킷을 수신해야 합니다. 소프트 모드에서는 소스 주소가 라우팅 테이블에 나타나야 합니다.

- 15 Fence 매개 변수를 입력하고 **추가(Add)**를 클릭합니다.
- 16 **확인(OK)**을 클릭합니다.

인터페이스 삭제

NSX Edge 인터페이스를 삭제할 수 있습니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **인터페이스(Interfaces)** 탭을 클릭합니다.
- 5 삭제할 인터페이스를 선택합니다.
- 6 **삭제(Delete)**(X) 아이콘을 클릭합니다.

인터페이스 사용

NSX Edge에 대해 인터페이스를 사용하도록 설정해야 해당 인터페이스(포트 그룹 또는 논리적 스위치) 내에서 가상 시스템을 분리할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 인터페이스(Interfaces) 탭을 클릭합니다.
- 5 사용하도록 설정할 인터페이스를 선택합니다.
- 6 사용(Enable)() 아이콘을 클릭합니다.

인터페이스 사용 안 함

NSX Edge에서 인터페이스를 사용하지 않도록 설정할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 인터페이스(Interfaces) 탭을 클릭합니다.
- 5 사용하지 않도록 설정할 인터페이스를 선택합니다.
- 6 사용 안 함(Disable) 아이콘을 클릭합니다.

트래픽 조절 정책 변경

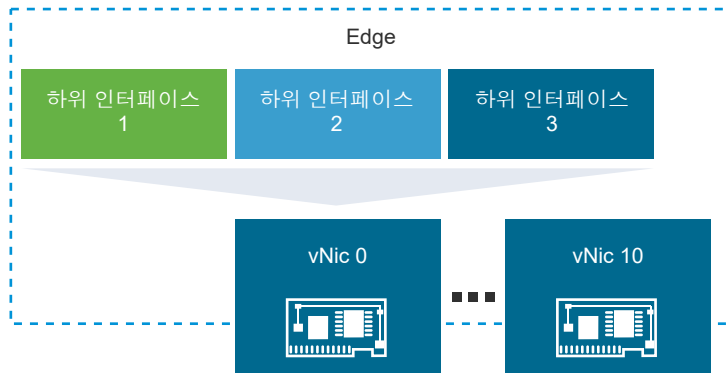
NSX Edge 인터페이스용 vSphere Distributed Switch에서 트래픽 조절 정책을 변경할 수 있습니다.

절차

- 1 NSX Edge를 두 번 클릭하고 관리(Manage) > 설정(Settings) > 인터페이스(Interfaces)로 이동합니다.
- 2 인터페이스를 선택합니다.
- 3 작업(Actions) > 트래픽 조절 정책 구성(Configure Traffic Shaping Policy)을 클릭합니다.
- 4 필요한 내용을 변경합니다.
 옵션에 대한 자세한 내용은 [트래픽 조절 정책](#)을 참조하십시오.
- 5 확인(OK)을 클릭합니다.

하위 인터페이스 추가

트렁크 vNIC에서 하위 인터페이스를 추가하면 이를 NSX Edge 서비스에서 사용할 수 있습니다.



트렁크 인터페이스 유형은 다음과 같습니다.


- VLAN 트렁크는 표준이고 모든 버전의 ESXi에서 작동합니다. 이 트렁크를 사용하여 태그 지정된 VLAN 트래픽을 Edge로 가져옵니다.
- VXLAN 트렁크는 NSX 버전 6.1 이상에서 작동합니다. 이 트렁크를 사용하여 VXLAN 트래픽을 Edge로 가져옵니다.

다음 Edge 서비스에서 하위 인터페이스를 사용할 수 있습니다.

- DHCP
- 라우팅(BGP 및 OSPF)
- 로드 밸런서
- IPsec VPN: IPsec VPN은 업링크 인터페이스로만 구성할 수 있습니다. 하위 인터페이스는 전용 트래픽이 IPsec 터널을 통해 이동되는 데 사용될 수 있습니다. IPsec 정책이 개인 트래픽에 대해 구성되면 하위 인터페이스는 전용 로컬 서버넷에 대한 게이트웨이로 작동합니다.
- L2 VPN
- NAT

. 하위 인터페이스는 HA 또는 논리적 방화벽에 사용할 수 없습니다. 그러나 하위 인터페이스의 IP 주소를 방화벽 규칙에서 사용할 수 있습니다.

절차

- 1 NSX Edge의 **설정(Manage) > 관리(Settings)** 탭에서 **인터페이스(Interfaces)**를 클릭합니다.
- 2 인터페이스를 선택하고 **편집(Edit)**() 아이콘을 클릭합니다.
- 3 Edge 인터페이스 편집 대화상자에 인터페이스의 이름을 입력합니다.
- 4 유형에서 **트렁크(Trunk)**를 선택합니다.

5 이 인터페이스가 연결되어야 하는 표준 포트 그룹 또는 분산 포트 그룹을 선택합니다.

- a **연결 대상(Change)** 필드 옆의 **변경(Connected To)**을 클릭합니다.
- b 인터페이스에 연결할 항목에 따라 **표준 포트 그룹(Standard Portgroup)** 또는 **분산 포트 그룹(Distributed Portgroup)** 탭을 클릭합니다.
- c 해당하는 포트 그룹을 선택하고 **확인(OK)**을 클릭합니다.
- d **선택(Select)**을 클릭합니다.

6 하위 인터페이스에서 **추가(Add)** 아이콘을 클릭합니다.

7 **하위 인터페이스 사용(Enable Sub interface)**을 클릭하고 하위 인터페이스 이름을 입력합니다.

8 **터널 ID(Tunnel Id)**에서 1과 4,094 사이의 숫자를 입력합니다.

터널 ID를 사용하여 확장할 네트워크를 연결합니다. 클라이언트 및 서버 사이트 모두에서 이 값이 동일해야 합니다.

9 [백업 유형]에서 다음 중 하나를 선택하여 하위 인터페이스에 대한 네트워크 백업을 표시합니다.

■ **VLAN 네트워크의 경우 VLAN.**

하위 인터페이스에서 사용해야 할 가상 LAN의 VLAN ID를 입력합니다. VLAN ID 범위는 0 ~ 4,094입니다.

■ **VLAN 또는 VXLAN 네트워크의 경우 네트워크(Network).**

선택(Select)을 클릭하고 분산 포트 그룹 또는 논리적 스위치를 선택하십시오. NSX Manager가 VLAN ID를 추출하여 트렁크 구성에서 사용합니다.

- 네트워크 또는 VLAN ID를 지정하지 않고 하위 인터페이스를 생성하려면 **없음(None)**을 클릭합니다. 이 하위 인터페이스는 NSX Edge 내부에 위치하고, 확장된 네트워크와 확장되지 않은(태그 해제된) 네트워크 간에 패킷을 라우팅하는 데 사용됩니다.

10 서브넷을 하위 인터페이스에 추가하려면 서브넷 구성 영역에서 **추가(Add)** 아이콘을 클릭하십시오.

11 서브넷 추가에서 **추가(Add)** 아이콘을 클릭하여 IP 주소를 추가하십시오. IP 주소를 입력하고 **확인(OK)**을 클릭하십시오.

IP 주소를 하나 이상 입력하는 경우 기본 IP 주소를 선택할 수 있습니다. 인터페이스는 하나의 기본 IP 주소와 여러 개의 보조 IP 주소를 사용할 수 있습니다. NSX Edge는 기본 IP 주소를 로컬로 생성된 트래픽의 소스 주소로 간주합니다.

12 서브넷 접두사 길이를 입력하고 **확인(OK)**을 클릭합니다.

13 필요한 경우 하위 인터페이스의 기본 MTU 값을 편집합니다.

트렁크 인터페이스의 기본 MTU는 1600이고 하위 인터페이스의 기본 MTU는 1500입니다. 하위 인터페이스의 MTU는 NSX Edge의 모든 트렁크 인터페이스 중에서 가장 낮은 MTU보다 작거나 같아야 합니다.

14 라우팅 정보를 호스트에 전달하려면 **리디렉션 보내기 사용(Enable Send Redirect)**을 선택합니다.

15 역방향 경로 필터를 **사용(Enable)** 또는 **사용 안 함(Disable)**으로 설정합니다.

역방향 경로 필터는 전달될 패킷의 소스 주소가 연결 가능한지 확인합니다. 사용 모드에서는 라우터가 반환 패킷을 전달하는 데 사용할 인터페이스에서 패킷을 수신해야 합니다. 소프트 모드에서는 소스 주소가 라우팅 테이블에 나타나야 합니다.

16 **확인(OK)**을 클릭하여 [트렁크 인터페이스] 창으로 돌아갑니다.**17** 필요한 경우 인터페이스에 대한 MAC 주소를 입력합니다. ESG HA를 사용하는 경우 두 개의 MAC 주소를 입력합니다.

필요하지 않으면 자동으로 생성됩니다.

18 필요한 경우 트렁크 인터페이스의 기본 MTU를 편집합니다.

트렁크 인터페이스의 기본 MTU는 1600이고 하위 인터페이스의 기본 MTU는 1500입니다. 트렁크 인터페이스의 MTU는 하위 인터페이스의 MTU보다 크거나 같아야 합니다.

19 **확인(OK)**을 클릭합니다.

결과

이제 Edge 서비스에서 하위 인터페이스를 사용할 수 있습니다.

다음에 수행할 작업

트렁크 vNic에 추가된 하위 인터페이스가 표준 포트 그룹의 지원을 받는 경우 VLAN 트렁크를 구성합니다. [VLAN 트렁크 구성](#) 를 참조하십시오.

VLAN 트렁크 구성

분산 포트 그룹에 연결된 Edge의 트렁크 vNic에 하위 인터페이스를 추가하면 VLAN 트렁크 및 VXLAN 트렁크가 둘 다 지원됩니다. 표준 포트 그룹에 연결된 Edge의 트렁크 vNic에 하위 인터페이스를 추가하면 VLAN 트렁크만 지원됩니다.

사전 요구 사항

표준 포트 그룹에 의해 트렁크 vNic가 지원되는 하위 인터페이스를 사용할 수 있는지 확인합니다. [하위 인터페이스 추가](#)를 참조하십시오.


절차

- 1** vCenter Web Client에 로그인합니다.
- 2** **네트워킹(Networking)**을 클릭합니다.
- 3** 표준 포트 그룹을 선택하고 **설정 편집(Edit Settings)**을 클릭합니다.
- 4** **VLAN** 탭을 클릭합니다.
- 5** VLAN 유형에서 VLAN 트렁킹을 선택하고 트렁킹할 VLAN ID를 입력합니다.
- 6** **확인(OK)**을 클릭합니다.

자동 규칙 구성 변경

자동 규칙 생성을 사용하도록 설정한 경우 **NSX Edge**에서 이러한 서비스에 대한 제어 트래픽 흐름을 허용하도록 방화벽, NAT 및 라우팅 경로를 추가합니다. 자동 규칙 생성을 사용하도록 설정하지 않은 경우 로드 밸런싱, VPN 등의 **NSX Edge** 서비스에 대한 제어 채널 트래픽을 허용하도록 방화벽, NAT 및 라우팅 구성을 수동으로 추가해야 합니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다. **구성(Configuration)**을 클릭합니다.
- 5 [세부 정보] 패널에서 **작업(Action)**()을 클릭하고 **자동 규칙 구성 변경(Change Auto Rule configuration)**을 선택합니다.
- 6 필요한 내용을 변경하고 **확인(OK)**을 클릭합니다.

CLI 자격 증명 변경

CLI(명령줄 인터페이스)에 로그인하는 데 사용할 자격 증명을 편집할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다. **구성(Configuration)**을 클릭합니다.
- 5 [세부 정보] 패널에서 **작업(Action)**()을 클릭하고 **CLI 자격 증명 변경(Change CLI Credentials)**을 선택합니다.
- 6 새 암호를 입력하고 확인한 후 **확인(OK)**을 클릭합니다.

고가용성 정보

HA(고가용성)는 하드웨어 또는 소프트웨어 장애로 인해 단일 장치를 사용할 수 없게 될 때 **NSX Edge** 장치에서 제공하는 서비스를 사용할 수 있게 해줍니다. **NSX Edge HA**는 장치 간 페일오버 시 일부 서비스를 다시 시작해야 할 수 있으므로 페일오버 다운타임을 없애는 대신 최소화합니다.

예를 들어 **NSX Edge HA**는 상태 저장 방화벽의 연결 추적기 또는 로드 밸런서에서 보유하는 상태 저장 정보를 동기화합니다. 모든 서비스 백업을 불러오는 데 필요한 시간은 **null**이 아닙니다. 알려진 다시 시작 서비스가 미치는 영향의 예로는 **NSX Edge**가 라우터로 작동되고 있을 때 동적 라우팅의 다운타임이 0이 아닌 경우가 있습니다.

경우에 따라 두 **NSX Edge HA** 장치가 통신할 수 없으며 일방적으로 활성 상태로 전환하려고 합니다. 이 동작은 대기 **NSX Edge**를 사용할 수 없는 경우 활성 **NSX Edge** 서비스의 가용성을 유지하기 위한 것입니다. 다른 장치가 여전히 존재하는 경우 통신이 다시 설정되면 두 **NSX Edge HA** 장치가 활성 및 대기 상태를 다시 조정합니다. 이러한 조정이 완료되지 않고, 연결이 다시 설정될 때 두 장치에서 활성 상태라고 선언되면 예기치 않은 동작이 발생합니다. 분할 브레인으로 알려진 이 상태는 다음 환경 조건에서 발생합니다.

- 네트워크 파티션을 포함하는 물리적 네트워크 연결 문제
- **NSX Edge**의 CPU 또는 메모리 경합
- 하나 이상의 **NSX Edge HA VM**을 사용할 수 없게 만들 수 있는 일시적인 스토리지 문제.

예를 들어 **VM**을 과도하게 프로비저닝된 스토리지 밖으로 이동하면 **NSX Edge HA** 안정성 및 성능이 향상됩니다. 특히 대규모 야간 백업 동안 스토리지 지연 시간이 급격히 증가하면 **NSX Edge HA** 안정성에 영향을 줄 수 있습니다.

- 패킷 교환과 관련된 물리적 또는 가상 네트워크 어댑터의 정체.

HA 구성 엔진이 잘못된 상태가 되거나 **HA** 데몬이 실패하면 환경 문제 외에 분할 브레인 상태가 발생합니다.

상태 저장 고가용성

기본 **NSX Edge** 장치는 활성 상태이며 보조 장치는 대기 상태입니다. **NSX Manager**는 대기 장치를 위해 기본 장치의 구성을 복제합니다. 또는 두 장치를 수동으로 추가할 수도 있습니다. 별도 리소스 풀 및 데이터 스토어에서 기본 및 보조 장치를 생성합니다. 기본 및 보조 장치를 동일한 데이터스토어에 생성하는 경우 **HA** 장치 쌍이 다른 **ESXi** 호스트에 배포될 수 있도록 클러스터에 있는 모든 호스트에서 데이터스토어를 공유해야 합니다. 데이터스토어가 로컬 스토리지인 경우에는 두 가상 시스템이 동일한 호스트에 배포됩니다.

모든 **NSX Edge** 서비스는 활성 장치에서 실행됩니다. 기본 장치는 대기 장치와의 하트비트를 유지하며 내부 인터페이스를 통해 서비스 업데이트를 전송합니다.

지정된 시간(기본값: 15초) 내에 기본 장치로부터 하트비트가 수신되지 않으면 기본 장치가 비활성(**dead**)으로 선언됩니다. 그러면 대기 장치가 활성 상태로 전환되고, 기본 장치의 인터페이스 구성을 이어받아 기본 장치에서 실행하던 **NSX Edge** 서비스를 시작합니다. 이와 같이 전환되면 시스템 이벤트가 설정 및 보고서의 **시스템 이벤트(System Events)** 탭에 표시됩니다. 로드 밸런서 및 **VPN** 서비스의 경우 **NSX Edge**와 **TCP**의 연결을 재설정해야 하므로 서비스가 잠시 중단되지만, 기본 및 대기 장치 간에 논리적 스위치 연결 및 방화벽 세션이 동기화됩니다. 그러나, 대기 장치가 활성화되고 서비스를 인계 받기를 기다리는 동안 전환이 이루어질 때 서비스가 중단됩니다.

NSX Edge 장치에서 장애가 발생하고 잘못된 상태가 보고되면 **HA**는 장애가 발생한 장치를 재활성화하기 위해 강제로 동기화합니다. 재활성화된 장치는 현재 활성 장치의 구성을 이어받고 대기 상태로 남아 있습니다. **NSX Edge** 장치가 비활성 상태인 경우 장치를 삭제하고 새 장치를 추가해야 합니다.

vMotion을 통해 동일한 호스트로 가상 시스템을 수동으로 이동하는 경우를 제외하고, **NSX Edge**는 **DRS** 및 **vMotion**을 사용한 후에도 두 **HA NSX Edge** 가상 시스템이 동일한 **ESXi** 호스트에 있지 않도록 보장합니다. 두 가상 시스템은 구성된 장치와 동일한 리소스 풀 및 데이터스토어의 **vCenter**에 배포됩니다. 통신할 수 있도록 **NSX Edge HA**의 **HA** 가상 시스템에 로컬 링크 IP가 할당됩니다. 관리 IP 주소를 지정하여 로컬 링크를 재정의할 수 있습니다.

Syslog 서버가 구성된 경우에는 활성 장치의 로그가 Syslog 서버로 전송됩니다.

크로스 vCenter NSX 환경의 고가용성

크로스 vCenter NSX 환경에서 NSX Edge에 대해 고가용성을 사용하도록 설정하는 경우 활성 및 대기 NSX Edge 장치가 동일한 vCenter Server 내에 상주해야 합니다. NSX Edge HA 쌍의 한 멤버를 다른 vCenter Server 시스템으로 마이그레이션하면 두 HA 장치가 더 이상 HA 쌍으로 작동하지 않으며 트래픽 중단이 발생할 수 있습니다.

vSphere HA(고가용성)

NSX Edge HA는 vSphere HA와 호환됩니다. NSX Edge 인스턴스를 실행하는 호스트가 비활성 상태가 되는 경우 NSX Edge가 대기 호스트에서 다시 시작되면 NSX Edge HA 쌍이 또 다른 페일오버를 수용할 수 있습니다.

vSphere HA가 사용되도록 설정되지 않는 경우에는 활성-대기 NSX Edge HA 쌍에서 페일오버가 한 번만 가능합니다. 하지만 두 번째 HA 쌍이 복원되기 전에 또 다른 페일오버가 발생하면 NSX Edge를 사용하지 못하게 될 수 있습니다.

vSphere HA에 대한 자세한 내용은 "vSphere 가용성"을 참조하십시오.

고가용성 구성 변경

NSX Edge 설치 시 지정한 HA 구성을 변경할 수 있습니다.

참고 NSX 6.2.3부터 두 번째 Edge VM 장치에 대해 충분한 리소스를 예약할 수 없는 경우 기존 Edge에서 HA(고가용성)를 사용하도록 설정할 수 없습니다. 구성은 마지막으로 알려져 있는 정상 구성으로 롤백됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 설정(Settings) 탭을 클릭합니다.
- 5 HA 구성(HA Configuration) 패널에서 변경(Change)을 클릭합니다.
- 6 [HA 구성 변경] 대화상자에서 NSX 설치 가이드 섹션, Edge Services Gateway 추가에 설명된 대로 변경을 수행합니다.

참고 HA를 사용할 수 있도록 설정하기 전에 이 Edge 장치에서 L2 VPN이 구성된 경우 2개 이상의 내부 인터페이스가 설정되어야 합니다. 이미 L2 VPN에서 사용하고 있는 이 Edge에 단일 인터페이스가 구성된 경우 Edge 장치에서 HA가 사용하지 않도록 설정되어 있습니다.

- 7 확인(OK)을 클릭합니다.

NSX Edge를 NSX Manager와 강제 동기화

NSX Manager에서 NSX Edge로 동기화 요청을 보낼 수 있습니다.

NSX Manager에 알려진 대로 Edge 구성을 모든 구성 요소에 동기화해야 할 때 강제 동기화를 사용합니다.


참고 6.2 이상의 경우 강제 동기화가 동-서 라우팅 트래픽의 데이터 손실을 방지하지만 북-남 라우팅 및 브리징은 방해받을 수 있습니다.

강제 동기화를 실행하면 다음과 같은 작업이 수행됩니다.

- Edge 장치가 재부팅되고 최신 구성이 적용됩니다.
- 호스트와의 연결이 끊어집니다.
- NSX Manager가 기본 또는 독립형이고 Edge가 논리적 분산 라우터일 경우 컨트롤러 클러스터가 동기화됩니다.
- 분산된 라우터 인스턴스를 동기화하기 위해 모든 관련 호스트로 메시지가 전송됩니다.

중요 크로스 vCenter NSX 환경에서는 기본 NSX Manager에서 NSX Edge 인스턴스가 먼저 강제로 동기화되어야 합니다. 이 작업이 완료되면 보조 NSX Manager의 NSX Edge 인스턴스를 강제로 동기화합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)을 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge 인스턴스를 선택합니다.
- 4 작업(Actions)()을 클릭하고 강제 동기화(Force Sync)를 선택합니다.

NSX Edge에 대한 Syslog 서버 구성

하나 또는 두 개의 원격 Syslog 서버를 구성할 수 있습니다. NSX Edge 장치에서 생성되는 방화벽 이벤트 관련 NSX Edge 이벤트 및 로그는 Syslog 서버로 전송됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)을 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리 탭을 클릭한 후 설정 탭을 클릭합니다.
- 5 세부 정보 패널에서 Syslog 서버 옆의 변경을 클릭합니다.
- 6 두 원격 Syslog 서버의 IP 주소를 입력하고 프로토콜을 선택합니다.
- 7 확인을 클릭하여 구성을 저장합니다.

NSX Edge의 상태 보기

상태 페이지에는 선택한 NSX Edge의 인터페이스를 통과하는 트래픽에 대한 그래프 외에도, 방화벽 및 로드 밸런서 서비스에 대한 연결 통계가 표시됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 모니터(Monitor) 탭을 클릭합니다.
- 5 통계를 볼 기간을 선택합니다.

다음에 수행할 작업

NSX Edge에 대한 더 자세한 정보를 보려면 **관리(Manage)**를 클릭한 다음 **설정(Settings)**을 클릭합니다.

NSX Edge 다시 배포

강제 동기화 후에 NSX Edge 서비스가 예상대로 작동하지 않는 경우 NSX Edge 인스턴스를 다시 배포할 수 있습니다.

참고 다시 배포는 지장을 주는 작업입니다. 먼저 강제 동기화를 적용한 후 문제가 해결되지 않으면 다시 배포하십시오.

NSX Edge 인스턴스를 다시 배포하면 다음 작업이 발생합니다.

- Edge 장치가 삭제되고 최신 구성이 적용된 상태로 새롭게 배포됩니다.
- 논리적 라우터가 컨트롤러에서 삭제된 다음 최신 구성이 적용된 상태로 다시 생성됩니다.
- 호스트의 논리적 분산 라우터 인스턴스가 삭제된 다음 최신 구성이 적용된 상태로 다시 생성됩니다.

정상적인 다시 시작이 사용되도록 설정되지 않은 경우 다시 배포 동안 OSPF 인접성이 취소됩니다.

중요 크로스 vCenter 환경에서는 먼저 기본 NSX Manager에서 NSX Edge 인스턴스를 다시 배포해야 합니다. 이 작업이 완료되면 보조 NSX Manager의 NSX Edge 인스턴스를 다시 배포합니다. 기본 및 보조 NSX Manager 둘 다에서 NSX Edge 인스턴스를 다시 배포해야 합니다.

사전 요구 사항

- 다시 배포하는 동안 호스트에 추가 NSX Edge Services Gateway 장치를 배포할 수 있는 충분한 리소스가 있는지 확인합니다. 각 NSX Edge 크기에 대해 필요한 리소스는 [장 1 NSX의 시스템 요구 사항](#)을 참조하십시오.
 - 단일 NSX Edge 인스턴스의 경우 다시 배포 동안 해당 크기의 NSX Edge 장치 2개가 poweredOn 상태로 존재합니다.


- 고가용성이 포함된 NSX Edge 인스턴스의 경우 이전 장치를 교체하기 전에 두 교체용 장치가 배포됩니다. 즉, 지정된 NSX Edge가 업그레이드되는 동안 poweredOn 상태를 갖는 해당 크기의 NSX Edge 장치가 4개 존재하게 됩니다. NSX Edge 인스턴스가 다시 배포된 후에 HA 장치 중 하나가 활성화될 수 있습니다.
- NSX Edge 장치에 대해 구성된 위치와 실시간 위치에 나열된 호스트 클러스터가 NSX에 대해 준비되어 있는지와 메시징 인프라 상태가 GREEN인지 확인합니다. 예를 들어 NSX Edge 장치를 생성한 후에 클러스터가 제거되었으므로 구성된 위치를 사용할 수 없는 경우 실시간 위치만 확인하십시오.
- GET `https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances` API 요청으로 구성된 원래 위치 (`configuredResourcePool > id`) 및 현재 실시간 위치(`resourcePoolId`) ID를 찾습니다.
- GET `https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}` API 요청으로 해당 클러스터의 호스트 준비 상태 및 메시징 인프라 상태를 찾습니다. 여기서 `resourceId`는 앞서 찾은 NSX Edge 장치의 구성된 실시간 위치에 대한 ID입니다.
- 응답 본문에서 `com.vmware.vshield.vsm.nwfabric.hostPrep`의 `featureId`에 해당하는 상태를 찾습니다. 상태는 GREEN이어야 합니다.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
  <featureVersion>6.3.1.5124716</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- 응답 본문에서 `com.vmware.vshield.vsm.messagingInfra`의 `featureId`에 해당하는 상태를 찾습니다. 상태는 GREEN이어야 합니다.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge 인스턴스를 선택합니다.
- 4 작업(Actions)() 아이콘을 클릭하고 Edge 다시 배포(Redeploy Edge)를 선택합니다.

결과

NSX Edge 가상 시스템이 새로운 가상 시스템으로 교체되고 모든 서비스가 복원됩니다. 다시 배포가 작동하지 않으면 NSX Edge 가상 시스템의 전원을 끄고 NSX Edge를 다시 배포하십시오.

참고 다음과 같은 경우에 다시 배포가 작동하지 않을 수 있습니다.

- NSX Edge가 설치된 리소스 풀이 더 이상 vCenter 인벤토리에 없거나 해당 Mold(vCenter Server에서의 ID)가 변경된 경우
- NSX Edge가 설치된 데이터스토어가 손상되었거나, 마운트 해제되었거나, 액세스 불가능한 경우
- NSX Edge 인터페이스가 연결된 dvportGroup이 더 이상 vCenter 인벤토리에 없거나 해당 Mold(vCenter Server에서의 ID)가 변경된 경우


위 조건 중 하나라도 해당하는 경우 REST API 호출을 사용하여 리소스 풀, 데이터스토어 또는 dvPortGroup의 Mold를 업데이트해야 합니다. 자세한 내용은 "NSX API 프로그래밍 가이드"를 참조하십시오.

NSX Edge에서 FIPS 모드가 사용하도록 설정되었으나 문제가 발생하면 NSX Manager는 Edge를 다시 배포하도록 허용하지 않습니다. Edge를 다시 배포하는 대신 통신 오류에 대한 인프라 문제를 해결해야 합니다.

NSX Edge에 대한 기술 지원 로그 다운로드

각 NSX Edge 인스턴스에 대한 기술 지원 로그를 다운로드할 수 있습니다. NSX Edge 인스턴스에 대해 고가용성을 사용하도록 설정한 경우 두 NSX Edge 가상 시스템의 지원 로그가 모두 다운로드됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge 인스턴스를 선택합니다.
- 4 작업()을 클릭하고 기술 지원 로그 다운로드를 선택합니다.
- 5 기술 지원 로그가 생성되면 다운로드를 클릭합니다.

정적 경로 추가

대상 서브넷 또는 호스트에 대한 정적 경로를 추가할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.

4 **관리(Manage)** 탭을 클릭한 후 **라우팅(Routing)** 탭을 클릭합니다.

5 왼쪽 패널에서 **정적 경로(Static Routes)**를 선택합니다.

6 **추가(Add)**(+) 아이콘을 클릭합니다.

7 CIDR 표기법으로 **네트워크(Network)**를 입력합니다.

8 **다음 홉(Next Hop)**의 IP 주소를 입력합니다.

라우터가 직접 다음 홉에 연결할 수 있어야 합니다.

ECMP를 사용하도록 설정한 경우 다음 홉을 여러 개 입력할 수 있습니다.

9 정적 경로를 추가할 **인터페이스(Interface)**를 선택합니다.

10 **MTU**에 대해 필요한 경우 데이터 패킷의 최대 전송 값을 편집합니다.

MTU는 NSX Edge 인터페이스에 설정된 MTU보다 높을 수 없습니다.

11 메시지가 나타나면 **Admin Distance**를 입력합니다.

1에서 255 사이의 값을 선택합니다. 지정한 네트워크에 대해 다중 경로가 있는 경우 사용할 경로를 Admin Distance를 사용하여 선택합니다. Admin Distance가 낮을수록 경로에 대한 기본 설정이 높습니다.

표 9-3. 기본 Admin Distance

경로 소스	기본 Admin Distance
연결됨	0
정적	1
외부 BGP	20
OSPF 영역 내부	30
OSPF 영역 내부	110
내부 BGP	200

관리 거리가 255이면 라우팅 테이블(RIB) 및 데이터부에서 정적 경로가 제외되므로 정적 경로가 사용되지 않습니다.

12 (선택 사항) **로케일 ID(Locale ID)**를 입력합니다.

기본적으로 경로에는 NSX Manager와 동일한 로케일 ID가 있습니다. 여기서 로케일 ID를 지정하면 경로가 이 로케일 ID와 연결됩니다. 일치하는 로케일 ID를 가진 호스트에만 이 경로가 전송됩니다. 자세한 내용은 [크로스 vCenter NSX 토폴로지](#) 항목을 참조하십시오.

13 (선택 사항) 정적 경로에 대한 **설명(Description)**을 입력합니다.

14 **확인(OK)**을 클릭합니다.

논리적 (분산) 라우터에서 OSPF 구성

논리적 라우터에서 OSPF를 구성하면 논리적 라우터 전체에서 VM을 연결하고 논리적 라우터에서 ESG(Edge Services Gateway)로 VM을 연결할 수 있습니다.

OSPF 라우팅 정책은 동일한 코스트의 경로 간에 트래픽 로드 밸런싱의 동적 프로세스를 제공합니다.

OSPF 네트워크가 라우팅 영역으로 구분되어 트래픽 흐름을 최적화하고 라우팅 테이블의 크기를 제한합니다. 영역은 동일한 영역 ID를 가진 OSPF 네트워크, 라우터 및 링크의 논리적 모음입니다.

영역은 영역 ID로 식별됩니다.

사전 요구 사항

논리적 (분산) 라우터에 구성된 OSPF에 표시된 대로 라우터 ID를 구성해야 합니다.

라우터 ID를 사용하도록 설정한 경우 기본적으로 논리적 라우터의 업링크 인터페이스로 필드가 채워집니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 논리적 라우터를 두 번 클릭합니다.
- 4 라우팅(Routing)을 클릭하고 OSPF를 클릭합니다.
- 5 OSPF를 사용하도록 설정합니다.
 - a 창의 오른쪽 상단에서 편집(Edit)을 클릭하고 OSPF 사용(Enable OSPF)을 클릭합니다.
 - b 전달 주소(Forwarding Address)에서 호스트의 라우터 데이터 경로 모듈이 데이터 경로 패킷을 전달하기 위해 사용할 IP 주소를 입력합니다.
 - c 프로토콜 주소(Protocol Address)에서 전달 주소(Forwarding Address)와 동일한 서브넷 내의 고유한 IP 주소를 입력합니다. 프로토콜에서 프로토콜 주소를 사용하여 피어와의 인접성을 형성합니다.
- 6 OSPF 영역을 구성합니다.
 - a 선택에 따라 기본적으로 구성되는 NSSA(not-so-stubby 영역) 51을 삭제합니다.
 - b 영역 정의(Area Definitions)에서 추가(Add) 아이콘을 클릭합니다.
 - c 영역 ID를 입력합니다. NSX Edge는 IP 주소 또는 십진수 형식의 영역 ID를 지원합니다.
 - d 유형(Type)에서 보통(Normal) 또는 NSSA를 선택합니다.

NSSA는 AS 외부 LSA(링크 상태 알림)가 NSSA로 플러딩되는 것을 방지합니다. NSSA는 외부 대 상에 대한 기본 라우팅을 사용합니다. 따라서 NSSA는 OSPF 라우팅 도메인의 종단에 있어야 합니다. NSSA는 외부 경로를 OSPF 라우팅 도메인에 가져올 수 있으므로 OSPF 라우팅 도메인에 포함 되지 않은 소규모 라우팅 도메인에 전송 서비스를 제공할 수 있습니다.

7 (선택 사항) 인증(Authentication) 유형을 선택합니다. OSPF가 영역 수준에서 인증을 수행합니다.

영역 내 모든 라우터에는 동일한 인증 및 해당하는 암호가 구성되어 있어야 합니다. MD5 인증이 작동하려면 수신 라우터와 전송 라우터가 동일한 MD5 키를 가지고 있어야 합니다.

- a **없음(None)**: 인증이 필요하지 않으며 기본값입니다.
- b **암호>Password**: 이 인증 방법을 사용할 경우 전송된 패킷에 암호가 포함됩니다.
- c **MD5**: 이 인증 방법은 MD5(메시지 다이제스트 유형 5) 암호화를 사용합니다. 전송된 패킷에 MD5 체크섬이 포함됩니다.
- d **암호>Password** 또는 **MD5** 인증 유형을 선택한 경우 암호나 MD5 키를 입력합니다.

참고

- FIPS 모드가 사용되도록 설정되어 있으면 MD5 인증을 구성할 수 없습니다.
- NSX는 항상 키 ID 값으로 1을 사용합니다. NSX Edge 또는 논리적 분산 라우터와 피어로 연결된 모든 비 NSX 디바이스는 MD5 인증이 사용될 때 키 ID로 값 1을 사용하도록 구성되어야 합니다. 그렇지 않으면 OSPF 세션이 설정되지 않습니다.

8 인터페이스를 영역에 매핑합니다.

- a **영역-인터페이스 매핑(Area to Interface Mapping)**에서 **추가(Add)** 아이콘을 클릭하여 OSPF 영역에 속한 인터페이스를 매핑합니다.
- b 매핑할 인터페이스를 선택하고 인터페이스를 매핑할 OSPF 영역을 선택합니다.

9 (선택 사항) 필요한 경우 기본 OSPF 설정을 편집합니다.

대부분의 경우 기본 OSPF 설정을 유지하는 것이 좋습니다. 설정을 변경할 경우 OSPF 피어에서 동일한 설정을 사용하는지 확인하십시오.

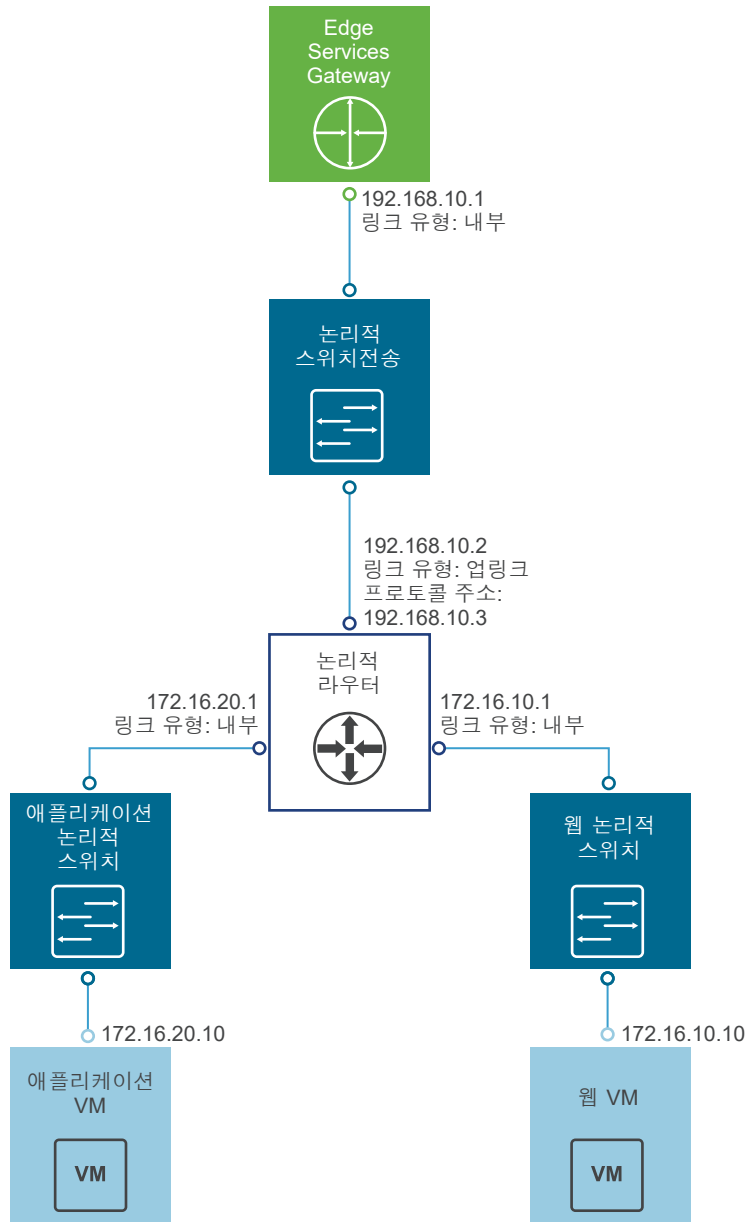
- a **Hello 간격(Hello Interval)**은 인터페이스에서 전송되는 hello 패킷 간의 기본 간격을 표시합니다.
- b **비활성 간격(Dead Interval)**은 인접 네트워크가 중단되었음을 라우터가 선언하기 전에 인접 네트워크로부터 하나 이상의 hello 패킷이 수신되어야 하는 기본 간격을 표시합니다.
- c **우선 순위(Priority)**는 인터페이스의 기본 우선 순위를 표시합니다. 우선 순위가 가장 높은 인터페이스는 지정 라우터입니다.
- d 인터페이스 **코스트(Cost)**는 해당 인터페이스 전체에서 패킷을 보내는 데 필요한 기본 오버헤드를 표시합니다. 인터페이스 코스트는 인터페이스 대역폭과 반비례합니다. 대역폭이 클수록 코스트가 적어집니다.

10 변경 내용 게시(Publish Changes)를 클릭합니다.

예제: 논리적 (분산) 라우터에 구성된 OSPF

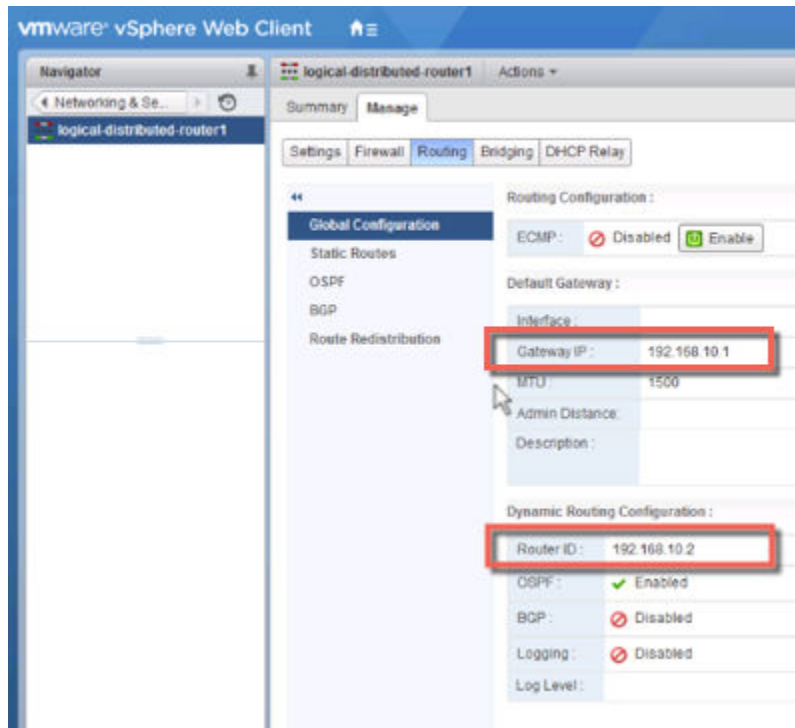
여기에 표시된 OSPF를 사용하는 간단한 NSX 시나리오에서는 DLR(논리적 라우터) 및 ESG(Edge Services Gateway)가 OSPF 인접 네트워크입니다.

그림 9-1. NSX 토폴로지

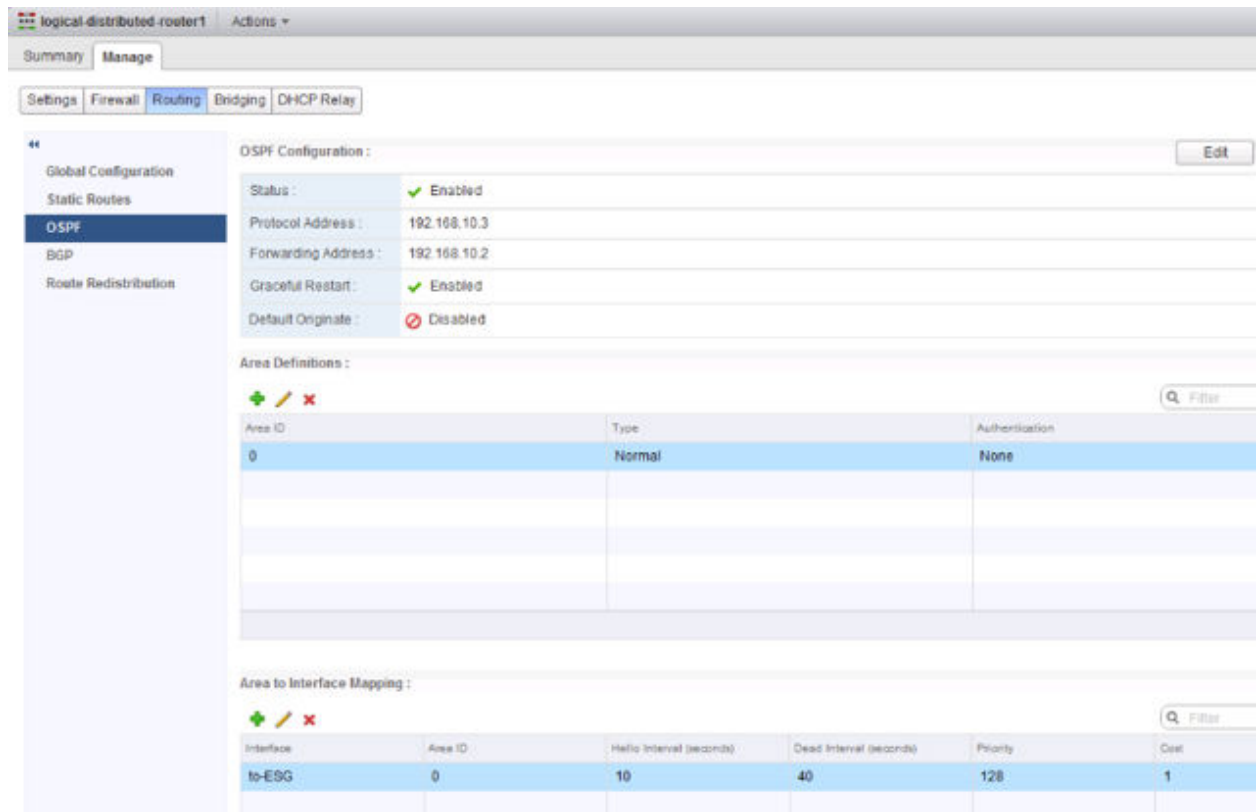


다음 화면에서 논리적 라우터의 기본 게이트웨이는 ESG의 내부 인터페이스 IP 주소(192.168.10.1)입니다.

라우터 ID는 논리적 라우터의 업링크 인터페이스입니다. 즉 ESG에 연결되는 IP 주소입니다 (192.168.10.2).



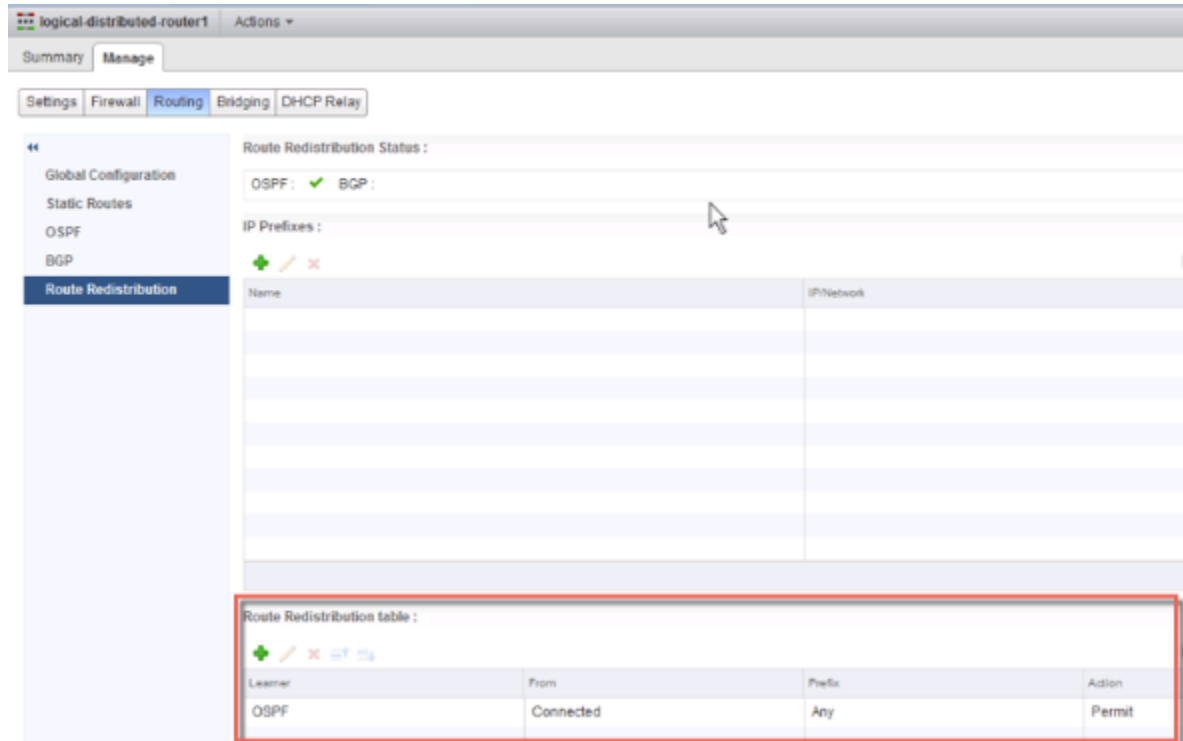
논리적 라우터 구성에서는 192.168.10.2를 전달 주소로 사용합니다. 동일한 서브넷에 있고 다른 곳에서 사용되지 않은 IP 주소가 프로토콜 주소가 될 수 있습니다. 이 경우 192.168.10.3이 구성됩니다. 구성된 영역 ID는 0이고 업링크 인터페이스(ESG에 연결되는 인터페이스)가 영역에 매핑됩니다.



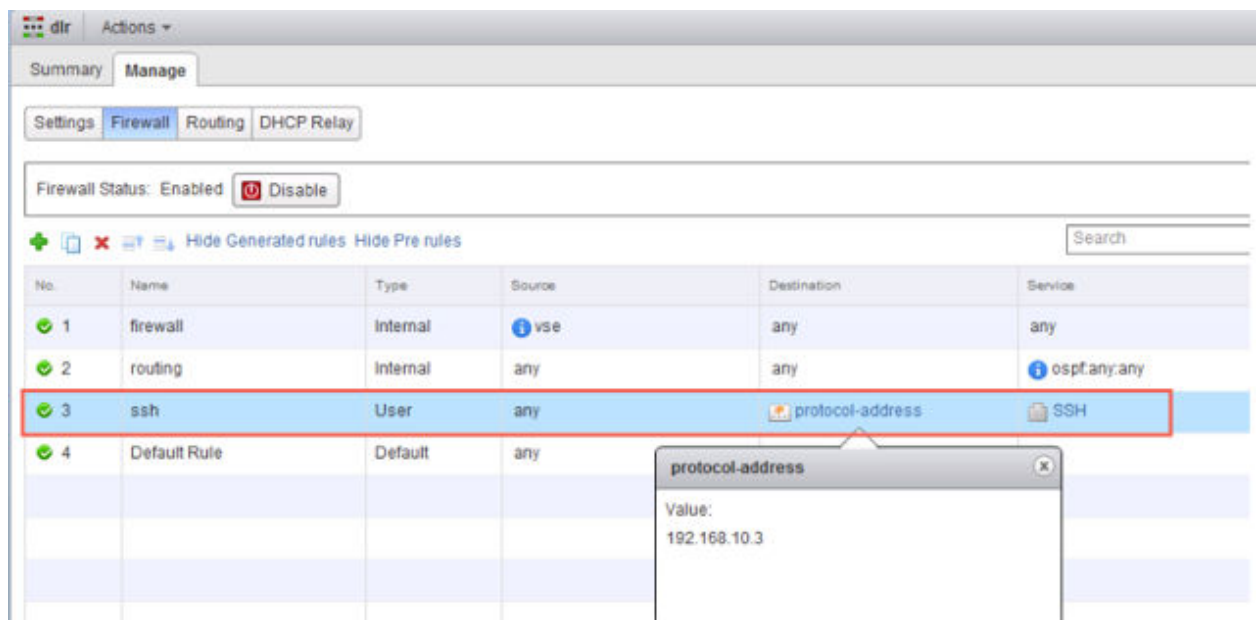
다음에 수행할 작업

경로 재배포 및 방화벽 구성에서 올바른 경로가 보급되도록 허용하는지 확인합니다.

이 예제에서는 논리적 라우터의 연결된 경로(172.16.10.0/24 및 172.16.20.0/24)가 OSPF에 보급됩니다.



논리적 라우터를 생성할 때 SSH를 사용하도록 설정한 경우 SSH를 논리적 라우터의 프로토콜 주소에 허용하는 방화벽 필터도 구성해야 합니다. 예:



Edge Services Gateway에서 OSPF 구성

ESG(Edge Services Gateway)에서 OSPF를 구성하면 ESG가 경로를 인식 및 보급할 수 있습니다. ESG에서 OSPF의 가장 일반적인 애플리케이션은 ESG와 논리적 (분산) 라우터 간의 링크에 있습니다. 이를 통해 ESG가 논리적 라우터에 연결된 LIFS(논리적 인터페이스)를 인식할 수 있습니다. OSPF, IS-IS, BGP 또는 정적 라우팅을 사용하여 이 목적을 달성할 수 있습니다.

OSPF 라우팅 정책은 동일한 코스트의 경로 간에 트래픽 로드 밸런싱의 동적 프로세스를 제공합니다.

OSPF 네트워크가 라우팅 영역으로 구분되어 트래픽 흐름을 최적화하고 라우팅 테이블의 크기를 제한합니다. 영역은 동일한 영역 ID를 가진 OSPF 네트워크, 라우터 및 링크의 논리적 모음입니다.

영역은 영역 ID로 식별됩니다.

사전 요구 사항

Edge Services Gateway에 구성된 OSPF에 표시된 대로 라우터 ID를 구성해야 합니다.

라우터 ID를 사용하도록 설정할 경우 기본적으로 ESG의 업링크 인터페이스 IP 주소로 필드가 채워집니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)을 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 ESG를 두 번 클릭합니다.
- 4 라우팅(Routing)을 클릭하고 OSPF를 클릭합니다.
- 5 OSPF를 사용하도록 설정합니다.
 - a 창의 오른쪽 상단에서 편집(Edit)을 클릭하고 OSPF 사용(Enable OSPF)을 클릭합니다.
 - b (선택 사항) OSPF 서비스를 다시 시작하는 중에 패킷 전달이 중단되지 않도록 하려면 정상적인 다시 시작 사용(Enable Graceful Restart)을 클릭합니다.
 - c (선택 사항) ESG가 자신을 기본 게이트웨이로 피어에 보급할 수 있도록 허용하려면 기본 시작 사용(Enable Default Originate)을 클릭합니다.
- 6 OSPF 영역을 구성합니다.
 - a (선택 사항) 기본적으로 구성되는 NSSA(not-so-stubby 영역) 51을 삭제합니다.
 - b 영역 정의(Area Definitions)에서 추가(Add) 아이콘을 클릭합니다.
 - c 영역 ID를 입력합니다. NSX Edge는 IP 주소 또는 십진수 형식의 영역 ID를 지원합니다.
 - d 유형(Type)에서 보통(Normal) 또는 NSSA를 선택합니다.

NSSA는 AS 외부 LSA(링크 상태 알림)가 NSSA로 플러딩되는 것을 방지합니다. NSSA는 외부 대 상에 대한 기본 라우팅을 사용합니다. 따라서 NSSA는 OSPF 라우팅 도메인의 종단에 있어야 합니다. NSSA는 외부 경로를 OSPF 라우팅 도메인에 가져올 수 있으므로 OSPF 라우팅 도메인에 포함되지 않은 소규모 라우팅 도메인에 전송 서비스를 제공할 수 있습니다.

7 (선택 사항) 유형으로 **NSSA**를 선택하면 **NSSA 변환기 역할(NSSA Translator Role)** 필드가 나타납니다. **항상(Always)** 확인란을 선택하여 Type-7 LSA를 Type-5 LSA로 변환합니다. 모든 Type-7 LSA는 NSSA에 의해 Type-5 LSA로 변환됩니다.

8 (선택 사항) **인증(Authentication)** 유형을 선택합니다. OSPF가 영역 수준에서 인증을 수행합니다.

영역 내 모든 라우터에는 동일한 인증 및 해당하는 암호가 구성되어 있어야 합니다. MD5 인증이 작동하려면 수신 라우터와 전송 라우터가 동일한 MD5 키를 가지고 있어야 합니다.

- a **없음(None)**: 인증이 필요하지 않으며 기본값입니다.
- b **암호>Password**: 이 인증 방법을 사용할 경우 전송된 패킷에 암호가 포함됩니다.
- c **MD5**: 이 인증 방법은 MD5(메시지 다이제스트 유형 5) 암호화를 사용합니다. 전송된 패킷에 MD5 체크섬이 포함됩니다.
- d **암호>Password** 또는 **MD5** 인증 유형을 선택한 경우 암호나 MD5 키를 입력합니다.

참고

- FIPS 모드가 사용되도록 설정되어 있으면 **MD5** 인증을 구성할 수 없습니다.
- NSX는 항상 키 ID 값으로 1을 사용합니다. NSX Edge 또는 논리적 분산 라우터와 피어로 연결된 모든 비 NSX 디바이스는 MD5 인증이 사용될 때 키 ID로 값 1을 사용하도록 구성되어야 합니다. 그렇지 않으면 OSPF 세션이 설정되지 않습니다.

9 인터페이스를 영역에 매핑합니다.

- a **영역-인터페이스 매핑(Area to Interface Mapping)**에서 **추가(Add)** 아이콘을 클릭하여 OSPF 영역에 속한 인터페이스를 매핑합니다.
- b 매핑할 인터페이스를 선택하고 인터페이스를 매핑할 OSPF 영역을 선택합니다.

10 (선택 사항) 기본 OSPF 설정을 편집합니다.

대부분의 경우 기본 OSPF 설정을 유지하는 것이 좋습니다. 설정을 변경할 경우 OSPF 피어에서 동일한 설정을 사용하는지 확인하십시오.

- a **Hello 간격(Hello Interval)**은 인터페이스에서 전송되는 hello 패킷 간의 기본 간격을 표시합니다.
- b **비활성 간격(Dead Interval)**은 인접 네트워크가 중단되었음을 라우터가 선언하기 전에 인접 네트워크로부터 하나 이상의 hello 패킷이 수신되어야 하는 기본 간격을 표시합니다.
- c **우선 순위(Priority)**는 인터페이스의 기본 우선 순위를 표시합니다. 우선 순위가 가장 높은 인터페이스는 지정 라우터입니다.
- d 인터페이스 **코스트(Cost)**는 해당 인터페이스 전체에서 패킷을 보내는 데 필요한 기본 오버헤드를 표시합니다. 인터페이스 코스트는 인터페이스 대역폭과 반비례합니다. 대역폭이 클수록 코스트가 적어집니다.

11 **변경 내용 게시(Publish Changes)**를 클릭합니다.

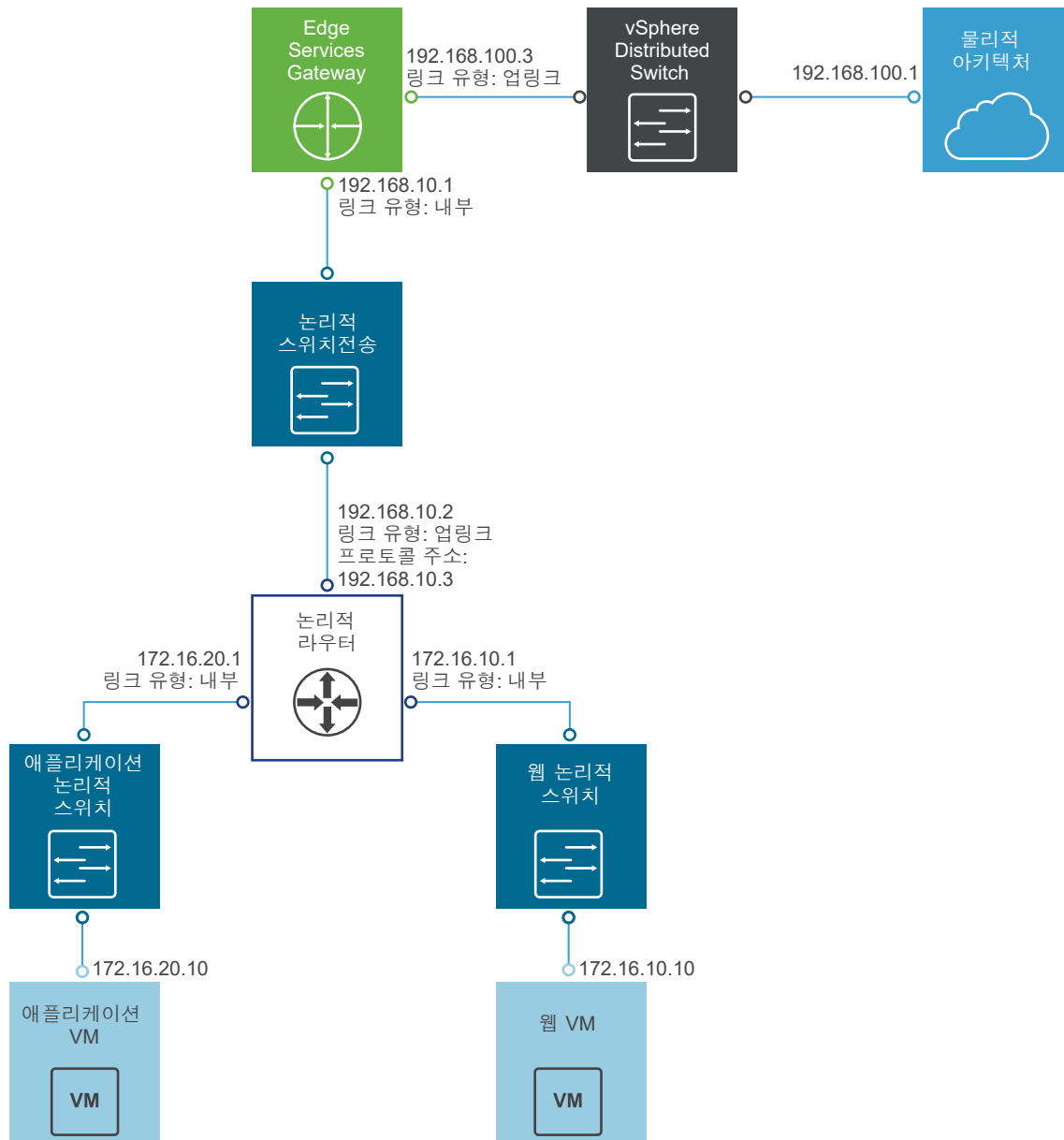
12 경로 재배포 및 방화벽 구성에서 올바른 경로가 보급되도록 허용하는지 확인합니다.

예제: Edge Services Gateway에 구성된 OSPF

여기에 표시된 OSPF를 사용하는 간단한 NSX 시나리오에서는 논리적 라우터 및 Edge Services Gateway가 OSPF 인접 네트워크입니다.

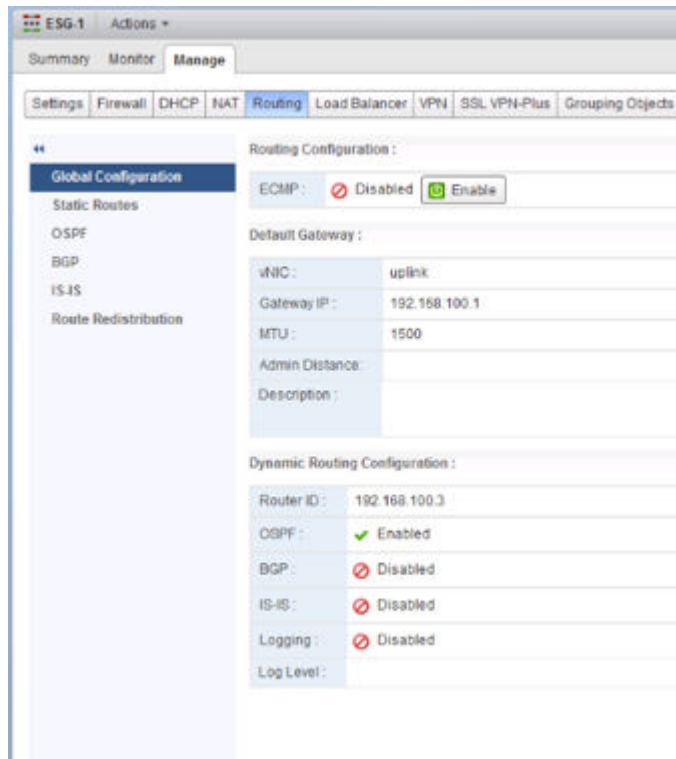
ESG는 브리지 또는 물리적 라우터를 통해 외부에 연결되거나 여기에 표시된 대로 vSphere Distributed Switch의 업링크 포트 그룹을 통해 외부에 연결할 수 있습니다.

그림 9-2. NSX 토폴로지

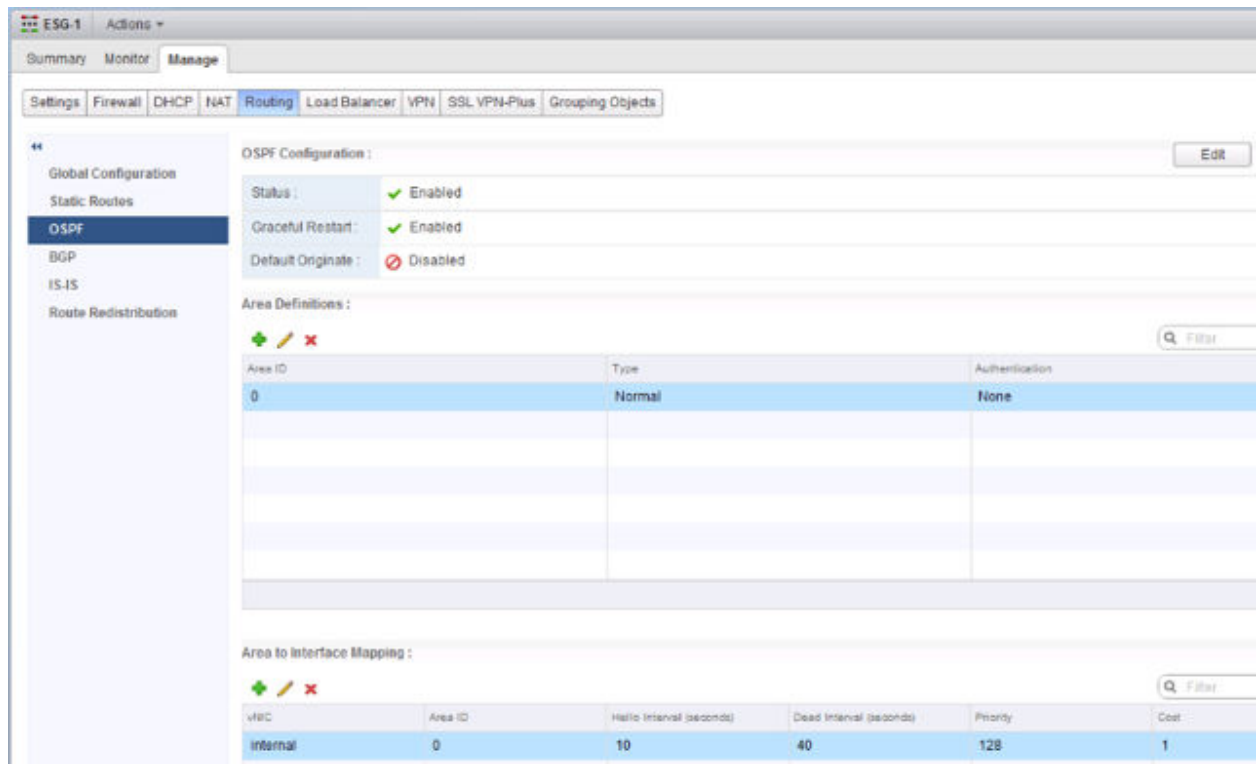


다음 화면에서 ESG의 기본 게이트웨이는 외부 피어에 대한 ESG의 업링크 인터페이스입니다.

라우터 ID는 ESG의 업링크 인터페이스 IP 주소입니다. 즉 외부 피어에 연결하는 IP 주소입니다.



구성된 영역 ID는 0이고 내부 인터페이스(논리적 라우터에 연결되는 인터페이스)가 영역에 매핑됩니다.



연결된 경로가 OSPF에 재배포되므로 OSPF 인접 네트워크(논리적 라우터)가 ESG의 업링크 네트워크를 인식할 수 있습니다.

Summary Monitor **Manage**

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects

Global Configuration
Static Routes
OSPF
BGP
IS-IS
Route Redistribution

Route Redistribution Status :

OSPF ☒ ISIS ☐ BGP ☐

IP Prefixes :

+ - ✎ ✖

Name	IP Network

Route Redistribution table :

+ - ✎ ✖

Learned	From	Prefix	Action
OSPF	Connected	Any	Permit

참고 그리고 ESG와 해당 외부 피어 라우터 간에 OSPF를 구성할 수 있지만 경로 보급을 위해 이 링크에서 BGP를 사용하는 것이 더 일반적입니다.

ESG가 논리적 라우터에서 OSPF 외부 경로를 인식하는지 확인하십시오.

```
NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 5

S      0.0.0.0/0          [0/0]          via 192.168.100.1
O E2  172.16.10.0/24     [110/1]        via 192.168.10.2
O E2  172.16.20.0/24     [110/1]        via 192.168.10.2
C      192.168.10.0/29   [0/0]          via 192.168.10.1
C      192.168.100.0/24  [0/0]          via 192.168.100.3
```

연결을 확인하려면 물리적 아키텍처의 외부 디바이스가 VM을 ping할 수 있는지 확인하십시오.

예:

```
PS C:\Users\Administrator> ping 172.16.10.10
```

```
Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.10.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

```
PS C:\Users\Administrator> ping 172.16.20.10
```

```
Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.20.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

BGP 구성

BGP(Border Gateway Protocol)는 라우팅과 관련된 핵심 결정을 내립니다. 여기에는 여러 자치 시스템 간의 네트워크 연결을 지정하는 IP 네트워크 테이블 또는 접두사 테이블이 포함됩니다.

먼저 두 **BGP Speaker** 간의 기본 연결이 설정된 후에 라우팅 정보가 교환됩니다. 이 관계를 유지하기 위해서는 **BGP Speaker**를 통해 연결 유지 메시지가 전송됩니다. 연결이 설정되면 **BGP Speaker**는 서로 라우팅 정보를 교환하고 해당 테이블을 동기화합니다.

절차

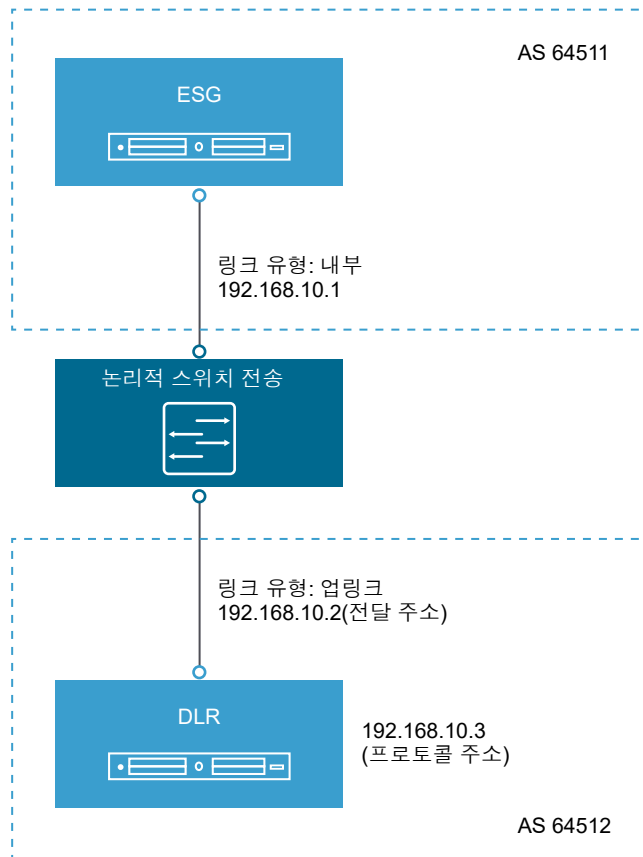
- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **라우팅(Routing)**을 클릭하고 **BGP**를 클릭합니다.
- 5 **편집(Edit)**을 클릭합니다.
- 6 [BGP 구성 편집] 대화상자에서 **BGP 사용(Enable BGP)**을 클릭합니다.
- 7 BGP 서비스를 다시 시작하는 중에 패킷 전달이 중단되지 않도록 하려면 **정상적인 다시 시작 사용(Enable Graceful Restart)**을 클릭합니다.
- 8 NSX Edge가 자신을 기본 게이트웨이로 피어에 보급할 수 있도록 허용하려면 **기본 시작 사용(Enable Default Originate)**을 클릭합니다.
- 9 **로컬 AS(Local AS)**에 라우터 ID를 입력합니다. 로컬 AS를 입력합니다. BGP가 다른 AS(자치 시스템)의 라우터와 피어 관계이면 이 정보가 보급됩니다. 경로 이동에 사용되는 AS의 경로는 대상에 대한 최상의 경로를 선택할 때 단일 메트릭으로 사용됩니다.
- 10 **확인(OK)**을 클릭합니다.
- 11 **인접 네트워크(Neighbors)**에서 **추가(Add)** 아이콘을 클릭합니다.
- 12 인접 네트워크의 IP 주소를 입력합니다.
ESG(Edge Services Gateway) 및 논리적 라우터 간에 BGP 피어링을 구성할 경우 논리적 라우터의 프로토콜 IP 주소를 ESG의 BGP 인접 네트워크 주소로 사용합니다.
- 13 (논리적 라우터에만 해당) 전달 주소를 입력합니다.
BGP 인접 네트워크를 대상으로 하는 논리적 분산 라우터의 인터페이스(해당 업링크 인터페이스)에 할당된 IP 주소가 전달 주소입니다.
- 14 (논리적 라우터에만 해당) 프로토콜 주소를 입력합니다.
BGP 인접 네트워크 관계를 구성하기 위해 논리적 라우터에서 사용하는 IP 주소가 프로토콜 주소입니다. 다른 위치에서 사용하지 않는 한 전달 주소와 동일한 서브넷에 있는 모든 IP 주소일 수 있습니다.
ESG(Edge Services Gateway) 및 논리적 라우터 간에 BGP 피어링을 구성할 경우 논리적 라우터의 프로토콜 IP 주소를 ESG의 인접 네트워크 IP 주소로 사용합니다.
- 15 원격 AS를 입력합니다.
- 16 필요한 경우 인접 네트워크 연결의 기본 가중치를 편집합니다.

- 17 보류 타이머(Hold Down Timer)**에 피어가 비활성임을 선언하는 연결 유지 메시지를 소프트웨어가 받지 못하게 된 후부터의 간격(180초)이 표시됩니다. 필요한 경우 편집할 수 있습니다.
- 18 연결 유지 타이머(Keep Alive Timer)**에 소프트웨어가 해당 피어에게 연결 유지 메시지를 보내는 기본 빈도(60초)가 표시됩니다. 필요한 경우 편집할 수 있습니다.
- 19** 인증이 필요한 경우 인증 암호를 입력합니다. 인접 네트워크 간 연결에서 전송된 각 세그먼트가 확인됩니다. 두 BGP 인접 네트워크에서 동일한 암호를 사용하여 MD5 인증을 구성해야 합니다. 그렇지 않으면 두 네트워크 간에 연결이 설정되지 않습니다.
- FIPS 모드가 사용되도록 설정되어 있으면 암호를 입력할 수 없습니다.
- 20** 인접 네트워크에서 경로 필터링을 지정하려면 **BGP 필터(BGP Filters)** 영역에서 **추가(Add)** 아이콘을 클릭합니다.

경고 필터 끝에서 "모두 차단" 규칙이 적용됩니다.

- 21** 인접 네트워크로 들어가는 트래픽을 필터링하는지 또는 인접 네트워크에서 나오는 트래픽을 필터링하는지를 나타내는 방향을 선택합니다.
- 22** 트래픽을 허용하는지 또는 거부하는지를 나타내는 작업을 선택합니다.
- 23** 인접 네트워크로 들어가거나 인접 네트워크에서 나오는 트래픽을 필터링할 네트워크를 CIDR 형식으로 입력합니다.
- 24** 필터링할 IP 접두사를 입력하고 **확인(OK)**을 클릭합니다.
- 25 변경 내용 게시(Publish Changes)**를 클릭합니다.

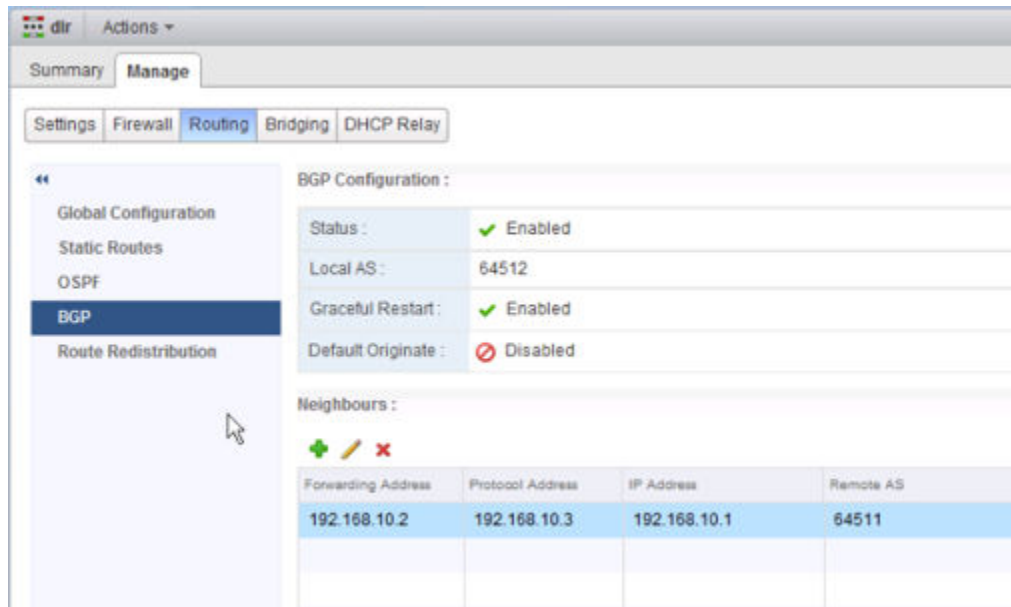
예제: ESG 및 논리적 라우터 간에 BGP 구성



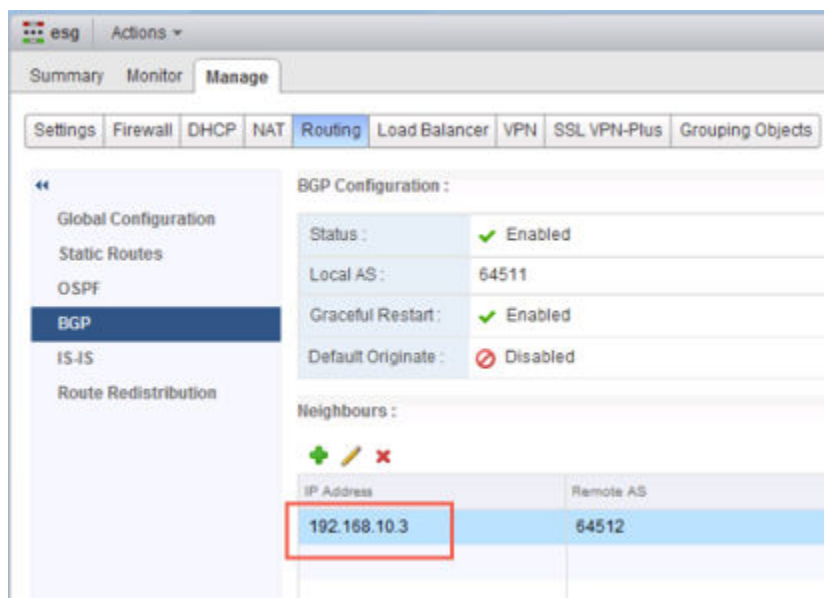
이 토폴로지에서 **ESG**는 **AS 64511**에 있습니다. 논리적 라우터(**DLR**)는 **AS 64512**에 있습니다.

논리적 라우터의 전달 주소는 **192.168.10.2**입니다. 이는 논리적 라우터의 업링크 인터페이스에 구성된 주소입니다. 논리적 라우터의 프로토콜 주소는 **192.168.10.3**입니다. 이는 **ESG**가 논리적 라우터와 **BGP** 피어링 관계를 형성하기 위해 사용하는 주소입니다.

논리적 라우터에서 **BGP**를 다음과 같이 구성합니다.



ESG에서 BGP를 다음과 같이 구성합니다.



ESG의 인접 네트워크 주소는 192.168.10.3입니다. 이는 논리적 라우터의 프로토콜 주소입니다.

show ip bgp neighbors 명령을 논리적 라우터에서 실행하고 BGP 상태가 설정되었는지 확인합니다.

```

NSX-edge-6-0> show ip bgp neighbors

BGP neighbor is 192.168.10.1,    remote AS 64511,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 120 messages, Sent 125 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x9aa20f3c
  Route refresh request:received 0 sent 0
  Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 5
Local host: 192.168.10.3, Local port: 179
Remote host: 192.168.10.1, Remote port: 43846

```

show ip bgp neighbors 명령을 ESG에서 실행하고 BGP 상태가 설정되었는지 확인합니다.

```

NSX-edge-7-0> show ip bgp neighbors

BGP neighbor is 192.168.10.3,    remote AS 64512,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 121 messages, Sent 120 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 3 Identifier 0x40212c6c
  Route refresh request:received 0 sent 0
  Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 1
Local host: 192.168.10.1, Local port: 43846
Remote host: 192.168.10.3, Remote port: 179

```

경로 재배포 구성

기본적으로 라우터는 동일한 프로토콜을 실행하는 다른 라우터와 경로를 공유합니다. 다중 프로토콜 환경에서는 교차 프로토콜 경로 공유를 위해 경로 재배포를 구성해야 합니다.

인터페이스를 경로 재배포에서 제외하려는 경우 인터페이스 네트워크에 대한 거부 조건을 추가하면 됩니다. NSX 6.2에서는 논리적(분산) 라우터의 HA(관리) 인터페이스가 경로 재배포에서 자동으로 제외됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **라우팅(Routing)**을 클릭하고 **경로 재배포(Route Redistribution)**를 클릭합니다.
- 5 **경로 재배포 상태(Route Redistribution Status)** 옆의 **편집(Edit)**을 클릭합니다.
- 6 경로 재배포를 사용하도록 설정할 프로토콜을 선택하고 **확인(OK)**을 클릭합니다.
- 7 IP 접두사를 추가합니다.
IP 접두사 목록의 항목은 순차적으로 처리됩니다.
 - a **IP 접두사(IP Prefixes)**에서 **추가(Add)** 아이콘을 클릭합니다.
 - b 네트워크의 이름과 IP 주소를 입력합니다.
보다 작거나 같음(LE) 또는 보다 크거나 같음(GE) 수정자를 포함하는 경우를 제외하고 입력한 IP 접두사가 정확하게 일치됩니다.
 - c **확인(OK)**을 클릭합니다.
- 8 IP 접두사의 재배포 조건을 지정합니다.
 - a **경로 재배포 테이블(Route Redistribution table)**에서 **추가(Add)** 아이콘을 클릭합니다.
 - b **학습자 프로토콜(Learner Protocol)**에서 다른 프로토콜의 경로를 학습할 프로토콜을 선택합니다.
 - c **다음에서 학습 허용(Allow Learning from)**에서 경로를 학습할 프로토콜을 선택합니다.
 - d **확인(OK)**을 클릭합니다.
- 9 **변경 내용 게시(Publish Changes)**를 클릭합니다.

NSX Manager 로케일 ID 보기

각 NSX Manager마다 하나의 로케일 ID가 있습니다. 기본적으로 이 ID는 NSX Manager UUID로 설정됩니다. 범용 논리적 라우터, 클러스터 또는 호스트 수준에서 이 설정을 덮어쓸 수 있습니다.

절차

- 1 vSphere Web Client에서 **Networking & Security**로 이동한 후, **Networking & Security 인벤토리(Networking & Security Inventory)** 아래의 NSX Manager를 클릭하십시오.
- 2 **요약(Summary)** 탭을 클릭합니다. ID 필드는 NSX Manager의 UUID를 포함합니다.

범용 논리적(분산) 라우터에서 로케일 ID 구성

범용 논리적 라우터를 생성할 때 로컬 송신을 사용하도록 설정한 경우 호스트 로케일 ID가 경로와 연관된 로케일 ID와 일치할 경우에만 경로가 호스트로 송신됩니다. 라우터에서 로케일 ID를 변경할 수 있고, 이 업

데이트된 로케일 ID는 이 라우터의 모든 경로(정적 및 동적)와 연결됩니다. 일치하는 로케일 ID를 가진 호스트 및 클러스터에 경로가 전송됩니다.

크로스 vCenter NSX 환경에 대한 라우팅 구성 정보는 [크로스 vCenter NSX 토폴로지](#) 항목을 참조하십시오.

사전 요구 사항

로컬 송신을 사용하도록 설정한 상태로 범용 논리적(분산) 라우터를 생성해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 범용 논리적(분산) 라우터를 두 번 클릭합니다.
- 4 **라우팅(Routing)** 탭을 클릭한 후 **글로벌 구성(Global Configuration)**을 클릭합니다.
- 5 **라우팅 구성(Routing Configuration)** 옆의 **편집(Edit)**을 클릭합니다.
- 6 새 로케일 ID를 입력합니다.

중요 로케일 ID는 UUID 형식이어야 합니다. 예를 들어, XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX입니다. 여기서 각 X는 기본 16자리 영숫자(0-F)로 대체됩니다.


호스트 또는 클러스터에서 로케일 ID 구성

범용 논리적 라우터를 생성할 때 로컬 송신을 사용하도록 설정한 경우 호스트 로케일 ID가 경로와 연관된 로케일 ID와 일치할 경우에만 경로가 호스트로 송신됩니다. 호스트 또는 호스트의 클러스터에서 로케일 ID를 구성하여 호스트에 경로를 선택적으로 전송할 수 있습니다.

사전 요구 사항

호스트 또는 클러스터에 대한 라우팅을 수행하는 범용 논리적(분산) 라우터는 로컬 송신을 사용하도록 설정한 상태로 생성해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**을 클릭하고 **설치(Installation)**를 클릭합니다.
- 3 **호스트 준비(Host Preparation)** 탭을 클릭합니다.
- 4 구성해야 할 호스트 또는 클러스터를 관리하는 **NSX Manager**를 선택합니다.
- 5 수정할 호스트 또는 클러스터를 선택하고, 필요한 경우 클러스터를 확장하여 호스트를 표시합니다.
- 6 **설정(Settings)** 아이콘 ()을 클릭하고 **로케일 ID 변경(Change Locale ID)**을 클릭합니다.

7 새 로케일 ID를 입력하고 **확인(OK.)**을 클릭합니다.

참고 로케일 ID는 UUID 형식이어야 합니다. 예를 들어, XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX입니다. 여기서 각 X는 기본 16자리 영숫자(0-F)로 대체됩니다.

결과

범용 컨트롤러 클러스터는 이 새 로케일 ID와 일치하는 경로만 호스트에 전송합니다.

다음에 수행할 작업

지정된 로케일 ID를 사용하여 정적 경로를 구성합니다.

논리적 방화벽은 동적 가상 데이터센터를 위한 보안 메커니즘을 제공하며 다양한 배포 사용 사례를 수용하기 위한 두 개의 구성 요소로 이루어집니다. 분산 방화벽은 동-서 액세스 제어에 중점을 두고 **Edge** 방화벽은 테넌트 또는 데이터센터 경계에서의 북-남 트래픽 적용에 중점을 둡니다. 이 두 구성 요소는 가상 데이터센터의 종단 간 방화벽 요구 사항을 해결합니다. 두 기술을 독립적으로 배포하거나 함께 배포할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 분산 방화벽
- **Edge** 방화벽
- 방화벽 규칙 섹션 사용
- 방화벽 규칙 사용
- **Firewall** 로그

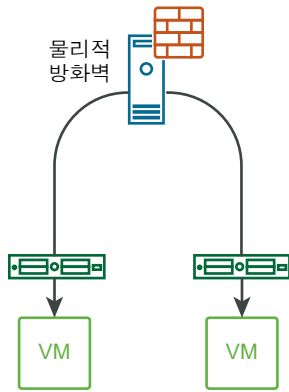
분산 방화벽

DFW(분산 방화벽)는 NSX용으로 준비한 모든 **ESXi** 호스트 클러스터의 **VIB** 패키지로 커널에서 실행됩니다. 호스트 준비 과정에서 **ESXi** 호스트 클러스터에서 **DFW**가 자동으로 활성화됩니다.

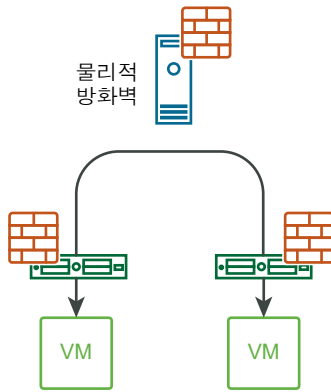
기존 경계 중심 보안 아키텍처의 기본 제약 조건은 최신 데이터 센터의 보안 상태 및 애플리케이션 확장성 둘 다에 영향을 줍니다. 예를 들어, 네트워크의 경계에서 물리적 방화벽을 통해 트래픽을 고정하면 특정 애플리케이션에 대한 추가 지연 시간이 생성됩니다.

DFW는 물리적 방화벽에서 불필요한 고정을 제거하고 네트워크의 트래픽 양을 줄여 물리적 보안을 보완하고 향상시킵니다. 거부된 트래픽은 **ESXi** 호스트를 나가기 전에 차단됩니다. 트래픽이 네트워크를 통과할 필요 없이 물리적 방화벽을 통해 주변 장치에서 중지됩니다. 동일한 호스트나 다른 호스트의 다른 **VM**으로 향하는 트래픽은 네트워크를 통과하지 않아도 물리적 방화벽을 지난 다음, 대상 **VM**으로 돌아갑니다. **ESXi** 수준에서 트래픽이 검사되고 대상 **VM**으로 전달됩니다.

NSX DFW를 사용하지 않는 보안



NSX DFW를 사용하는 보안



NSX DFW는 상태 저장 방화벽입니다. 즉, 활성 연결의 상태를 모니터링하며, 이 정보를 사용하여 방화벽을 통과하도록 허용할 네트워크 패킷을 결정합니다. DFW는 하이퍼바이저에서 구현되고 vNIC 기준으로 가상 시스템에 적용됩니다. 즉, 방화벽 규칙이 각 가상 시스템의 vNIC에서 적용됩니다. 트래픽이 VM을 나간 후 가상 스위치(송신)에 들어가려고 할 때 VM의 vNIC에서 트래픽 검사가 발생합니다. 또한 트래픽이 스위치를 떠난 후 VM(수신)에 들어가기 전에도 vNIC에서 검사가 발생합니다.

NSX Manager 가상 장치, NSX Controller VM 및 NSX Edge Service Gateway는 DFW에서 자동으로 제외됩니다. VM에 DFW 서비스가 필요하지 않은 경우 제외 목록에 수동으로 추가할 수 있습니다.

DFW가 모든 ESXi 호스트의 커널에 분산되어 있으므로 클러스터에 호스트를 추가할 때 방화벽 용량이 수평으로 확장됩니다. 호스트를 더 추가하면 DFW 용량이 증가합니다. 인프라가 확장되고 점점 증가하는 VM을 관리하기 위해 더 많은 서버를 구입하면 DFW 용량이 증가합니다.

DFW 정책 규칙

DFW 정책 규칙은 vSphere Web Client를 사용하여 생성되며 규칙은 NSX Manager 데이터베이스에 저장됩니다. DFW를 사용하면 이더넷 규칙(L2 규칙) 및 일반 규칙(L3-L7 규칙)을 생성할 수 있습니다. 규칙은 NSX Manager에서 ESXi 클러스터로 게시된 다음, ESXi 호스트에서 VM 수준으로 내려갑니다. 동일한 클러스터에 있는 모든 ESXi 호스트의 DFW 정책 규칙이 동일합니다.

ESXi 호스트의 분산 방화벽 인스턴스에는 다음 두 테이블이 포함됩니다.

- 모든 보안 정책 규칙을 저장하기 위한 규칙 테이블
- "허용" 작업을 포함하는 규칙에 대한 흐름 항목을 캐시하는 연결 추적기 테이블

DFW 규칙은 "하향식"으로 실행됩니다. 방화벽을 통과해야 하는 트래픽은 먼저 방화벽 규칙 목록과 일치하는지 확인됩니다. 각 패킷은 규칙 테이블의 맨 위에 있는 규칙에 대하여 확인된 후 테이블의 다음 규칙 순서에 따라 확인됩니다. 테이블에서 트래픽 매개 변수와 일치하는 첫 번째 규칙이 적용됩니다. 테이블의 마지막 규칙은 DFW 기본 규칙입니다. 어떤 규칙과도 일치하지 않는 패킷에는 기본 규칙이 적용됩니다.

각 VM에는 고유한 방화벽 정책 규칙 및 컨텍스트가 있습니다. vMotion 중에 VM이 한 ESXi 호스트에서 다른 호스트로 이동하면 DFW 컨텍스트(규칙 테이블, 연결 추적기 테이블)가 VM과 함께 이동합니다. 또한 vMotion 동안 모든 활성 연결은 그대로 유지됩니다. 즉, DFW 보안 정책은 VM 위치와는 별개입니다.

DFW를 사용한 마이크로 세분화

마이크로 세분화를 사용하면 각 관련 가상 시스템 그룹을 고유한 논리적 네트워크 세그먼트로 분리하여 데이터 센터 네트워크를 보다 안전하게 보호할 수 있습니다. 마이크로 세분화를 통해 관리자는 데이터 센터의 한 논리적 세그먼트에서 다른 논리적 세그먼트(동-서 트래픽)로 방화벽 트래픽을 이동할 수 있습니다. 따라서 동-서 트래픽을 방화벽으로 차단하면 공격자가 데이터 센터에서 좌우로 이동하는 능력이 제한됩니다.

마이크로 세분화는 NSX의 DFW(분산 방화벽) 구성 요소를 통해 작동됩니다. DFW가 작동한다는 것은 네트워크 토폴로지가 더 이상 보안 적용을 가로막지 못한다는 것을 의미합니다. 유형과 관계없이 모든 네트워크 토폴로지로 동일한 수준의 트래픽 액세스 제어를 구현할 수 있습니다.

마이크로 세분화 사용 사례의 자세한 예제를 보려면 <https://communities.vmware.com/docs/DOC-27683>의 "NSX 네트워크 가상화 설계 설명서"에서 "NSX DFW를 사용한 마이크로 세분화 및 구현" 섹션을 참조하십시오.

사용자 ID를 기준으로 하는 DFW 정책 규칙

분산 방화벽을 사용하면 ID 기반 규칙을 생성할 때도 유용합니다. 보안 관리자는 엔터프라이즈 Active Directory에 정의된 사용자 ID 및 사용자의 그룹 멤버 자격을 기반으로 액세스 제어를 적용할 수 있습니다. 예를 들어, ID 기반 분산 방화벽 규칙은 다음과 같은 시나리오에서 사용할 수 있습니다.

- 사용자가 사용자 인증에 Active Directory가 사용되는 랩톱 또는 모바일 디바이스를 사용하는 가상 애플리케이션에 액세스하려고 합니다.
- 사용자가 가상 시스템이 Microsoft Windows 운영 체제를 실행하는 VDI 인프라를 사용하여 가상 애플리케이션에 액세스하려고 합니다.

Active Directory 사용자 기반 DFW 규칙에 대한 자세한 내용은 [장 11 ID 방화벽 개요](#)를 참조하십시오.

세션 타이머

TCP, UDP 및 ICMP 세션에 대해 세션 타이머를 구성할 수 있습니다.

세션 타이머는 비활성 상태가 된 후에 방화벽에서 세션이 유지되는 기간을 정의합니다. 프로토콜에 대한 세션 제한 시간이 만료되면 세션이 닫힙니다.

방화벽에서 사용자 정의 가상 시스템의 일부 또는 vNIC에 TCP, UDP 및 ICMP 세션에 대한 여러 시간 초과를 적용하도록 지정할 수 있습니다. 기본적으로 사용자 정의 타이머에 포함되지 않는 모든 가상 장치 또는 vNIC는 글로벌 세션 타이머에 포함되어 있습니다. 이러한 모든 시간 초과는 글로벌로 적용됩니다. 즉, 호스트에서 해당 유형을 갖는 모든 세션에 적용됩니다.

기본 세션 값은 네트워크 요구에 따라 수정될 수 있습니다. 값을 너무 낮게 설정하면 시간 초과가 너무 자주 발생하고, 값을 너무 높게 설정하면 실패 감지가 지연될 수 있습니다.

세션 타이머 생성

세션 타이머는 세션에서 비활성 상태가 된 후에 방화벽에서 세션이 유지되는 기간을 정의합니다.

방화벽에서 사용자 정의 VM 또는 vNICs 집합의 TCP, UDP 및 ICMP 세션에 대해 시간 초과를 정의할 수 있습니다. 기본 타이머는 글로벌입니다. 즉, 방화벽으로 보호되는 모든 가상 시스템에 적용됩니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Networking & Security > Firewall)**으로 이동합니다.
- 2 **설정(Settings)** 탭에 있는지 확인합니다. 둘 이상의 NSX Manager를 사용할 수 있으면 드롭다운 목록에서 하나를 선택합니다.
- 3 **추가(Add)**(+) 아이콘을 클릭합니다.
기본값으로 채워진 [시간 초과 구성 추가] 대화 상자가 나타납니다.
- 4 세션 타이머에 대해 **이름(name)**(필수) 및 **설명(description)**(옵션)을 입력합니다.
- 5 프로토콜을 선택합니다. 기본값을 그대로 적용하거나 자체 값을 입력합니다.

TCP 변수	설명
첫 번째 패킷	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 120초입니다.
열림	두 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 30초입니다.
설정됨	연결이 완전히 설정된 다음 연결에 대한 시간 초과 값입니다.
닫는 중	첫 번째 핀이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 120초입니다.
핀 대기	두 핀이 교환되고 연결이 닫힌 이후 연결에 대한 시간 초과 값입니다. 기본값은 45초입니다.
닫힘	한 끝점이 RST를 전송한 이후 연결에 대한 시간 초과 값입니다. 기본값은 20초입니다.

UDP 변수	설명
첫 번째 패킷	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 새 UDP 흐름에 대한 초기 시간 초과입니다. 기본값은 60초입니다.
단일	소스 호스트가 둘 이상의 패킷을 전송하고 대상 호스트가 하나를 전송받지 못한 경우 연결에 대한 시간 초과 값입니다. 기본값은 30초입니다.
다중	두 호스트가 패킷을 전송한 경우 연결에 대한 시간 초과 값입니다. 기본값은 60초입니다.

ICMP 변수	설명
첫 번째 패킷	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 새 ICMP 흐름에 대한 초기 시간 초과입니다. 기본값은 20초입니다.
오류 응답	ICMP 패킷에 대한 응답으로 ICMP 오류가 반환된 후 연결에 대한 시간 초과 값입니다. 기본값은 10초입니다.

- 6 개체 유형으로 **vNIC** 또는 **VM**을 선택합니다.
[사용 가능한 개체] 목록이 자동으로 채워집니다.
- 7 하나 이상의 개체를 선택하고 화살표를 클릭하여 **선택한 개체(Selected Objects)** 열로 이동합니다.
- 8 **확인(OK)**을 클릭합니다.

결과

사용자 정의 호스트 집합에 적용할 타이머가 생성되었습니다.

세션 타이머 편집

TCP, UDP 및 ICMP 프로토콜에 대한 시간 초과 매개 변수를 구성합니다.

세션 타이머가 생성된 후에는 필요에 따라 변경할 수 있습니다. 기본 세션 타이머도 편집할 수 있습니다.

절차

- 1 vSphere Web Client에서 **Networking & Security --> 방화벽(Networking & Security --> Firewall)**으로 이동합니다.
- 2 **설정(Settings)** 탭에 있는지 확인합니다. 둘 이상의 NSX Manager를 사용할 수 있으면 드롭다운 목록에서 하나를 선택합니다.
- 3 편집할 타이머를 선택합니다. 기본 타이머 값도 편집할 수 있습니다. **연필(pencil)** 아이콘을 클릭합니다.
기본값으로 채워진 [시간 초과 구성 편집] 대화 상자가 나타납니다.
- 4 세션 타이머에 대해 **이름(name)**(필수) 및 **설명(description)**(옵션)을 입력합니다.
- 5 프로토콜을 선택합니다. 변경하려는 기본값을 편집합니다.

TCP 변수	설명
첫 번째 패킷	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 120초입니다.
열림	두 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 30초입니다.
설정됨	연결이 완전히 설정된 다음 연결에 대한 시간 초과 값입니다.
닫는 중	첫 번째 핀이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 120초입니다.
핀 대기	두 핀이 교환되고 연결이 닫힌 이후 연결에 대한 시간 초과 값입니다. 기본값은 45초입니다.
닫힘	한 끝점이 RST를 전송한 이후 연결에 대한 시간 초과 값입니다. 기본값은 20초입니다.

UDP 변수	설명
첫 번째 패킷	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 새 UDP 흐름에 대한 초기 시간 초과입니다. 기본값은 60초입니다.
단일	소스 호스트가 둘 이상의 패킷을 전송하고 대상 호스트가 하나를 전송받지 못한 경우 연결에 대한 시간 초과 값입니다. 기본값은 30초입니다.
다중	두 호스트가 패킷을 전송한 경우 연결에 대한 시간 초과 값입니다. 기본값은 60초입니다.

ICMP 변수	설명
첫 번째 패킷	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 새 ICMP 흐름에 대한 초기 시간 초과입니다. 기본값은 20초입니다.
오류 응답	ICMP 패킷에 대한 응답으로 ICMP 오류가 반환된 후 연결에 대한 시간 초과 값입니다. 기본값은 10초입니다.

6 개체 유형으로 **vNIC** 또는 **VM**을 선택합니다.

[사용 가능한 개체] 목록이 자동으로 채워집니다.

7 하나 이상의 개체를 선택하고 화살표를 클릭하여 **선택한 개체(Selected Objects)** 열로 이동합니다.

8 **확인(OK)**을 클릭합니다.

가상 시스템에 대한 IP 검색

VMware Tools는 VM에서 실행되고 여러 가지 서비스를 제공합니다. 분산 방화벽에 꼭 필요한 한 가지 서비스는 VM과 해당 vNIC를 IP 주소로 연결하는 것입니다. NSX 6.2 이전에는 VM에 VMware Tools가 설치되어 있지 않으면 해당 IP 주소가 확인되지 않았습니다. NSX 6.2 이상에서는 DHCP 스누핑, ARP 스누핑 또는 둘 모두를 사용하여 가상 시스템 IP 주소를 검색하도록 클러스터를 구성할 수 있습니다. 따라서 가상 시스템에 VMware Tools가 설치되어 있지 않아도 NSX가 IP 주소를 검색할 수 있습니다. 가상 시스템에 VMware Tools가 설치되어 있는 경우에는 DHCP 및 ARP 스누핑과 함께 작동할 수 있습니다.

사용 중인 환경의 각 가상 시스템에 VMware Tools를 설치하는 것이 좋습니다. VMware Tools는 vCenter에 VM의 IP 주소뿐만 아니라 다른 많은 기능을 제공합니다.

- VM과 호스트 또는 클라이언트 데스크톱 간 복사 및 붙여넣기 허용
- 호스트 운영 체제와 시간 동기화
- vCenter에서 VM 종료 또는 다시 시작 허용
- VM에서 네트워크, 디스크 및 메모리 사용량을 수집하여 호스트로 전송
- 하트비트를 전송 및 수집하여 VM 사용 가능 여부 확인


동일한 네트워크에 VM용 vNIC가 2개 있는 것은 지원되지 않으며 이 경우 차단 또는 허용되는 트래픽과 관련하여 예기치 않은 결과가 발생할 수 있습니다.

VMware Tools가 설치되지 않은 VM의 경우 NSX는 ARP 또는 DHCP 스누핑을 통해 IP 주소를 확인합니다 (VM의 클러스터에서 ARP 및 DHCP 스누핑을 사용하도록 설정한 경우).

IP 감지 유형 변경

VM에 설치된 VMware Tools나 호스트 클러스터에서 사용하도록 설정된 DHCP 스누핑 또는 ARP 스누핑은 가상 시스템의 IP 주소를 감지할 수 있습니다. 동일한 NSX 설치에서 이러한 IP 검색 방법을 함께 사용할 수 있습니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 설치(Installation) > 호스트 준비(Host Preparation)**로 이동합니다.
- 2 변경할 클러스터를 클릭한 다음 **작업(Actions)**() > **IP 감지 유형 변경(Change IP Detection Type)**을 클릭합니다.
- 3 원하는 감지 유형을 선택하고 **확인(OK)**을 클릭합니다.

다음에 수행할 작업

SpoofGuard를 구성합니다.

기본 방화벽 규칙을 구성합니다.

방화벽 보호 대상에서 가상 시스템 제외

NSX 분산 방화벽으로 보호되는 대상에서 가상 시스템 집합을 제외할 수 있습니다.

NSX Manager, NSX Controller 및 NSX Edge 가상 시스템은 NSX 분산 방화벽 보호 대상에서 자동으로 제외됩니다. 또한 다음 서비스 가상 시스템은 제외 목록에 배치하여 트래픽의 자유로운 흐름을 허용하는 것이 좋습니다.

- **vCenter Server.** 방화벽으로 보호되는 클러스터로 vCenter Server를 이동할 수는 있지만, 연결 문제를 방지하려면 해당 vCenter Server가 이미 제외 목록에 있는 상태여야 합니다.

참고 "any any" 기본 규칙을 허용에서 차단으로 변경하기 전에 vCenter Server를 제외 목록에 추가하는 것이 중요합니다. 이렇게 하지 못하면 모두 거부 규칙을 생성(또는 작업을 차단하도록 기본 규칙 수정)한 후에 vCenter Server에 대한 액세스가 차단됩니다. 이 경우 다음 API 명령을 실행하여 DFW를 기본 방화벽 규칙 집합으로 롤백합니다. https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config. 요청은 상태 204를 반환해야 합니다. 이렇게 하면 DFW에 대한 기본 규칙(허용 기본 규칙)이 복원되고 vCenter Server 및 vSphere Web Client에 대한 액세스가 다시 사용되도록 설정됩니다.

- 파트너 서비스 가상 시스템.
- 비규칙 모드가 필요한 가상 시스템. NSX 분산 방화벽에서 이 가상 시스템을 보호하는 경우 성능에 부정적인 영향을 줄 수 있습니다.
- Windows 기반 vCenter에서 사용하는 SQL Server.
- vCenter 웹 서버(별도로 실행할 경우).

절차

- 1 vSphere Web Client에서 **Networking & Security**를 클릭합니다.
- 2 **Networking & Security 인벤토리(Networking & Security Inventory)**에서 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 **이름(Name)** 열에서 NSX Manager를 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **제외 목록(Exclusion List)** 탭을 클릭합니다.
- 5 **추가(Add)(+)** 아이콘을 클릭합니다.
- 6 제외하려는 가상 시스템을 선택하고 **추가(Add)**를 클릭합니다.
- 7 **확인(OK)**을 클릭합니다.

결과

가상 시스템에 여러 vNIC가 있는 경우에는 모두 보호 대상에서 제외됩니다. 가상 시스템을 제외 목록에 추가한 후 vNIC를 가상 시스템에 추가한 경우 새로 추가된 vNIC에서 방화벽이 자동으로 배포됩니다. 이 vNIC를 방화벽 보호 대상에서 제외하려면 제외 목록에서 가상 시스템을 제거한 다음, 가상 시스템을 제외 목록에 다시 추가해야 합니다. 다른 해결 방법은 가상 시스템의 전원을 껐다가 다시 켜는 것입니다. 그러나 첫 번째 옵션이 지장을 적게 줍니다.

방화벽 CPU 및 메모리 임계값 이벤트 보기

클러스터가 네트워크 가상화를 위해 준비되면 방화벽 모듈이 해당 클러스터의 모든 호스트에 설치됩니다. 이 모듈은 모듈 매개 변수에 대한 모듈 힙, 규칙, 컨테이너, 필터에 대한 규칙 힙 및 트래픽 흐름에 대한 상태 힙 등 세 가지 힙을 할당합니다. 힙 크기 할당은 호스트의 사용 가능한 물리적 메모리에 의해 결정됩니다. 규칙, 컨테이너 집합 및 연결의 수에 따라 힙 크기가 시간에 따라 증가하거나 감소할 수 있습니다. 또한 하이퍼바이저에서 실행되는 방화벽 모듈은 패킷 처리를 위해 호스트 CPU를 사용합니다.

언제든지 호스트 리소스 사용을 확인 가능하면 서버 사용률과 네트워크 설계를 더 잘 조직하는데 도움이 됩니다.

기본 CPU 임계값은 100이고 메모리 임계값은 100입니다. REST API 호출을 통해 기본 임계값을 수정할 수 있습니다. 메모리와 CPU 사용이 임계값을 초과하면 방화벽 모듈은 시스템 이벤트를 생성합니다. 기본 임계값 구성에 대해서는 "NSX API 가이드"의 메모리 및 CPU 임계값 사용을 참조하십시오.

절차

- 1 vSphere Web Client에서 **Networking & Security**를 클릭한 후 **NSX Manager(NSX Managers)**를 클릭합니다.
- 2 **이름(Name)** 열에서 해당 NSX Manager의 IP 주소를 클릭합니다.
- 3 **모니터(Monitor)** 탭을 클릭하고 **시스템 이벤트(System Events)**를 클릭합니다.

분산 방화벽 리소스 활용도

메모리는 분산 방화벽 내부 데이터 구조에서 사용되며, CPU, RAM 및 초당 연결 수에 대해 구성될 수 있습니다.

각 ESXi 호스트에는 DFW 리소스 활용도에 대한 세 개의 임계값 매개 변수인 CPU, RAM 및 CPS(초당 연결 수)가 구성되어 있습니다. 200초 동안 해당 임계값을 연속해서 20회 초과하면 경보가 발생합니다. 10초마다 샘플이 수집됩니다.

CPU 100%는 호스트에서 사용할 수 있는 총 CPU에 해당합니다.

RAM 100%는 분산 방화벽에 할당된 메모리에 해당하며("총 최대 크기") 호스트에 설치된 총 RAM에 따라 달라집니다.

표 10-1. 총 최대 크기

물리적 메모리	총 최대 크기(MB)
0 - 8GB	160
8GB - 32GB	608
32GB - 64GB	992
64GB - 96GB	1920
96GB - 128GB	2944
128GB	4222

메모리는 분산 방화벽 내부 데이터 구조에 사용되며 이 구조에는 필터, 규칙, 컨테이너, 연결 상태, 검색된 IP 및 삭제 흐름이 포함됩니다. 다음 API 호출을 사용하여 이러한 매개 변수를 조작할 수 있습니다.

```
https://NSX-MGR-IP/api/4.0/firewall/stats/eventthresholds
```

Request body:

```
<eventThresholds>
  <cpu>
    <percentValue>100</percentValue>
  </cpu>
  <memory>
    <percentValue>100</percentValue>
  </memory>
  <connectionsPerSecond>
    <value>100000</value>
  </connectionsPerSecond>
</eventThresholds>
```

Edge 방화벽

Edge 방화벽은 북-남 트래픽을 모니터링하여 방화벽, NAT(네트워크 주소 변환), 사이트 간 IPSec, SSL VPN 기능과 경계 보안 기능을 제공합니다. 이 솔루션은 가상 시스템 폼 팩터로 제공되며 고가용성 모드에서 배포할 수 있습니다.

방화벽 지원은 논리적 라우터로 제한됩니다. 관리 또는 업링크 인터페이스의 규칙만 작동하고, 내부 인터페이스의 규칙은 작동하지 않습니다.

참고 NSX-V Edge는 공격자가 SYN 패킷을 폭발적으로 증가시켜 방화벽 상태 추적 테이블을 채우는 SYN 플러드(Syn-Flood) 공격에 취약합니다. 이 DOS/DDOS 공격은 정품 사용자에게 서비스 중단을 야기합니다. Edge는 bogus TCP 연결을 감지하고 방화벽 상태 추적 리소스를 소비하지 않으면서 이러한 연결을 중지하는 논리를 구현하여 SYN 플러드(Syn-Flood) 공격으로부터 방어해야 합니다. 이 기능은 기본적으로 사용되지 않도록 설정되어 있습니다. 고위험 환경에서 이 기능을 사용하도록 설정하려면 방화벽 글로벌 구성의 일부로 REST API enableSynFloodProtection 값을 true로 설정합니다.

SynFloodProtection이 NSX Edge에서 사용하도록 설정된 경우 수행되는 동작에 대한 자세한 내용은 <https://kb.vmware.com/s/article/54527>의 VMware 기술 자료 문서를 참조하십시오.

NSX Edge 방화벽 규칙 사용

NSX Edge로 이동하여 적용되는 방화벽 규칙을 볼 수 있습니다.

논리적 라우터에 적용되는 방화벽 규칙은 논리적 라우터 제어 가상 시스템의 수신 또는 송신하는 제어부 트래픽만을 보호합니다. 데이터부 보호를 적용하지 않습니다. 데이터부 트래픽을 보호하기 위해, 동-서 보호를 위한 논리적 방화벽 규칙을 생성하거나 북-남 보호를 위한 NSX Edge Services Gateway 수준에서 규칙을 생성합니다.

규칙은 다음과 같은 순서대로 나타나며 적용됩니다.


- 1 Edge에 적용되는 미리 정의된 분산 방화벽 규칙.
 - 이러한 규칙은 방화벽 사용자 인터페이스(**네트워킹 및 보안 > 보안 > 방화벽**)에서 정의됩니다.
 - 이 규칙은 NSX Edge 방화벽 사용자 인터페이스에서 **읽기 전용** 모드로 표시됩니다.
- 2 Edge 서비스에서 제어 트래픽이 흐르도록 하는 내부 규칙. 예를 들어 내부 규칙에는 다음과 같은 자동 연결 규칙이 포함됩니다.
 - a SSL VPN 자동 연결 규칙: 서버 설정이 구성되고 SSL VPN 서비스가 사용되도록 설정되면 [Edge 방화벽] 탭에 sslvpn 자동 연결 규칙이 표시됩니다.
 - b DNAT 자동 연결 규칙: [Edge NAT] 탭에는 기본 SSL VPN 구성의 일부로 DNAT 자동 연결 규칙이 표시됩니다.
- 3 NSX Edge 방화벽 사용자 인터페이스에 추가되는 사용자 정의 규칙
- 4 기본 규칙

기본 NSX Edge 방화벽 규칙 편집

기본 방화벽 설정은 사용자 정의 방화벽 규칙과 일치하지 않는 트래픽에 적용됩니다. 기본 Edge 방화벽 정책은 들어오는 트래픽을 모두 차단합니다. 기본 작업 및 로깅 설정을 변경할 수 있습니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)** 탭을 클릭한 후 **방화벽(Firewall)**을 클릭합니다.
- 4 방화벽 테이블의 마지막 규칙인 **기본 규칙(Default Rule)**을 선택합니다.

- 5 새 규칙의 **작업(Action)** 셀을 가리키고  을 클릭하십시오.
- a 지정된 소스 및 대상의 송신 또는 수신 트래픽을 허용하려면 **수락(Accept)**을 클릭합니다.
 - b 이 규칙과 일치하는 모든 세션을 로깅하려면 **로그(Log)**를 클릭합니다.
로깅을 사용하도록 설정하면 성능에 영향을 줄 수 있습니다.
 - c **확인(OK)**을 클릭합니다.
- 6 **변경 내용 게시(Publish Changes)**를 클릭합니다.

NSX Edge 방화벽 규칙 추가

Edge 방화벽 탭에는 중앙 집중식 방화벽 탭에서 읽기 전용 모드로 생성된 규칙이 표시됩니다. 여기서 추가한 모든 규칙이 중앙 집중식 방화벽 탭에 표시되는 것은 아닙니다.

방화벽 규칙의 소스와 대상으로 여러 개의 NSX Edge 인터페이스 및/또는 IP 주소 그룹을 추가할 수 있습니다.

그림 10-1. NSX Edge 인터페이스에서 HTTP 서버로 전송되는 트래픽에 대한 방화벽 규칙

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to HTTP server	User	vnic-index-0:any	HTTP Address Group	For HTTP server	Accept
3	Default Rule	Default	any			Deny

HTTP Address Group

Value:
10.20.222.34

For HTTP server

Value:
TCP:8080

그림 10-2. NSX Edge의 모든 내부 인터페이스(내부 인터페이스에 연결된 포트 그룹의 서브넷)에서 HTTP 서버로 전송되는 트래픽에 대한 방화벽 규칙

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to HTTP server	User	internal	HTTP Address Group	For HTTP server	Accept
3	Default Rule	Default	any			Deny

HTTP Address Group

Value:
10.20.222.34

For HTTP server

Value:
TCP:8080

참고 소스로 **내부(internal)**를 선택하면 추가 내부 인터페이스를 구성할 때 규칙이 자동으로 업데이트됩니다.

그림 10-3. 내부 네트워크의 m/c에 대한 SSH를 허용하는 트래픽의 방화벽 규칙

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to internal network	User	any	VM in internal network	Internal VM	Accept
3	Default Rule	Default	any			Deny

VM in internal network





Value:
192.168.0.10

Internal VM




Value:
TCP:22

절차

- 1 vSphere Web Client에서 **Networking & Security > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)** 탭을 클릭한 후 **방화벽(Firewall)** 탭을 클릭합니다.
- 4 다음 중 하나를 수행합니다.

옵션	설명
방화벽 테이블의 특정 위치에 규칙을 추가하려면	<p>a 규칙을 선택합니다.</p> <p>b 번호 열에서  을 클릭하고 위에 추가(Add Above) 또는 아래에 추가(Add Below)를 선택합니다.</p> <p>새로운 허용 규칙이 선택한 규칙 아래에 추가됩니다. 방화벽 테이블에 시스템 정의 규칙만 있을 경우 새 규칙은 기본 규칙 위에 추가됩니다.</p>
규칙을 복사하여 추가하려면	<p>a 규칙을 선택합니다.</p> <p>b 복사() 아이콘을 클릭합니다.</p> <p>c 규칙을 선택합니다.</p> <p>d 번호 열에서  을 클릭하고 위에 붙여넣기(Paste Above) 또는 아래에 붙여넣기(Paste Below)를 선택합니다.</p>
방화벽 테이블에서 원하는 위치에 규칙을 추가하려면	<p>a 추가(Add)() 아이콘을 클릭합니다.</p> <p>새로운 허용 규칙이 선택한 규칙 아래에 추가됩니다. 방화벽 테이블에 시스템 정의 규칙만 있을 경우 새 규칙은 기본 규칙 위에 추가됩니다.</p>

새 규칙은 기본적으로 사용하도록 설정됩니다.

- 5 새 규칙의 **이름(Name)** 셀을 가리키고  을 클릭합니다.
- 6 새 규칙의 이름을 입력합니다.
- 7 새 규칙의 **소스(Source)** 셀을 가리키고  또는  를 클릭합니다.

 를 클릭한 경우에는 IP 주소를 입력합니다.

- a 드롭다운에서 개체를 선택하고 필요한 사항을 선택합니다.

vNIC 그룹(vNIC Group)을 선택한 다음 **vse**를 선택하면 NSX Edge에서 생성한 트래픽에 규칙이 적용됩니다. **내부(internal)** 또는 **외부(external)**를 선택하면 선택한 NSX Edge 인스턴스의 내부 또는 업링크 인터페이스에서 나오는 트래픽에 규칙이 적용됩니다. 추가 인터페이스를 구성하는 경우 규칙이 자동으로 업데이트됩니다. 내부 인터페이스의 방화벽 규칙은 논리적 라우터에 대해 작동하지 않습니다.

IP 집합(IP Sets)을 선택하면 새 IP 주소 그룹을 생성할 수 있습니다. 새 그룹을 생성하면 해당 그룹이 소스 열에 자동으로 추가됩니다. IP 집합을 생성하는 방법에 대한 자세한 내용은 [IP 주소 그룹 생성](#) 항목을 참조하십시오.

- b **확인(OK)**을 클릭합니다.

8 새 규칙의 대상(Destination) 셀을 가리키고 또는 를 클릭합니다.



a 드롭다운에서 개체를 선택하고 필요한 사항을 선택합니다.

vNIC 그룹(vNIC Group)을 선택한 다음 **vse**를 선택하면 NSX Edge에서 생성한 트래픽에 규칙이 적용됩니다. **내부(internal)** 또는 **외부(external)**를 선택하면 선택한 NSX Edge 인스턴스의 내부 또는 업링크 인터페이스로 들어가는 트래픽에 규칙이 적용됩니다. 추가 인터페이스를 구성하는 경우 규칙이 자동으로 업데이트됩니다. 내부 인터페이스의 방화벽 규칙은 논리적 라우터에 대해 작동하지 않습니다.

IP 집합(IP Sets)을 선택하면 새 IP 주소 그룹을 생성할 수 있습니다. 새 그룹을 생성하면 해당 그룹이 소스 열에 자동으로 추가됩니다. IP 집합을 생성하는 방법에 대한 자세한 내용은 [IP 주소 그룹 생성](#) 항목을 참조하십시오.

b **확인(OK)**을 클릭합니다.

9 새 규칙의 서비스(Service) 셀을 가리키고 또는 을 클릭합니다.

- 을 클릭한 경우에는 서비스를 선택합니다. 새 서비스 또는 서비스 그룹을 생성하려면 **새로 만들기(New)**를 클릭합니다. 새 서비스를 생성하면 해당 서비스가 서비스 열에 자동으로 추가됩니다. 새 서비스를 생성하는 방법에 대한 자세한 내용은 [서비스 생성](#) 항목을 참조하십시오.
- 을 클릭한 경우에는 프로토콜을 선택합니다. **[고급]** 옵션 옆의 화살표를 클릭하여 소스 포트를 지정할 수 있습니다. 릴리스 5.1 이상부터는 소스 포트를 지정하지 않는 것이 좋습니다. 대신, 프로토콜-포트 조합에 대한 서비스를 생성할 수 있습니다.



참고 NSX Edge는 L3 프로토콜로 정의된 서비스만 지원합니다.


10 새 규칙의 작업(Action) 셀을 가리키고 을 클릭하십시오. 아래 표에서 설명한 대로 적절하게 선택하고 **확인(OK)**을 클릭하십시오.

선택한 작업	결과
허용	지정된 소스 및 대상의 송신 또는 수신 트래픽을 허용합니다.
차단	지정된 소스 및 대상의 송신 또는 수신 트래픽을 차단합니다.
거부	허용되지 않는 패킷에 대해 거부 메시지를 전송합니다. TCP 패킷에 대해 RST 패킷이 전송됩니다. 다른 패킷에 대해 ICMP 연결 불가(관리상 제한됨) 패킷이 전송됩니다.
로그	이 규칙과 일치하는 모든 세션을 로깅합니다. 로깅을 사용하도록 설정하면 성능에 영향을 줄 수 있습니다.
로깅 안 함	세션을 로깅하지 않습니다.
주석	필요한 경우 주석을 입력합니다.
고급 옵션 > 일치 기준: 변환 결과	NAT 규칙의 변환된 IP 주소 및 서비스에 규칙을 적용합니다.
규칙 방향 사용	규칙이 수신 또는 송신 규칙인지 나타냅니다. 방화벽 규칙의 방향을 지정하지 않는 것이 좋습니다.

11 변경 내용 게시(Publish Changes)를 클릭하여 새 규칙을 NSX Edge 인스턴스로 푸시합니다.

다음에 수행할 작업

- 규칙을 사용하지 않도록 설정하려면  (**번호(No.)**) 열의 규칙 번호 옆에 있음)을 클릭합니다.
- 생성된 규칙 또는 사전 규칙(중앙 집중식 방화벽 탭에서 추가된 규칙)을 숨기려면 **생성된 규칙 숨기기(Hide Generated rules)** 또는 **사전 규칙 숨기기(Hide Pre rules)**를 클릭합니다.
- 규칙 테이블에서 추가 열을 표시하려면  을 클릭하고 해당 열을 선택합니다.

열 이름	표시되는 정보
규칙 태그	각 규칙에 대해 생성된 고유 시스템 ID
로그	이 규칙에 대한 트래픽을 로깅하거나 로깅하지 않습니다.
통계	 를 클릭하면 이 규칙(세션 수, 트래픽 패킷 및 크기)에 영향을 받는 트래픽이 표시됩니다.
주석	규칙에 대한 주석입니다.

- 검색 필드에 텍스트를 입력하여 규칙을 검색합니다.

NSX Edge 방화벽 규칙 편집

사용자 정의 Edge 방화벽 규칙만 편집할 수 있고 시스템에서 생성한 기본 방화벽 규칙을 제한적으로 변경할 수 있습니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)** 탭을 클릭한 후 **방화벽(Firewall)** 탭을 클릭합니다.
- 4 편집할 규칙을 선택합니다.

참고 NSX Edge 방화벽 사용자 인터페이스에서는 다음 유형의 규칙을 편집할 수 없습니다.

- 내부 규칙(예: Edge 서비스에서 제어 트래픽이 흐르도록 하는 자동 연결 규칙)
- Edge에 적용되는 미리 정의된 분산 방화벽 규칙. 이러한 방화벽 규칙은 방화벽 사용자 인터페이스(**네트워킹 및 보안 > 보안 > 방화벽**)에서 정의됩니다.

- 5 변경하고 **확인(OK)**을 클릭합니다.
- 6 **변경 내용 게시(Publish Changes)**를 클릭합니다.

NSX Edge 방화벽 규칙의 우선 순위 변경



Edge 방화벽 탭에서 추가된 사용자 정의 방화벽 규칙의 순서를 변경하여 NSX Edge에서 트래픽 흐름을 사용자 지정할 수 있습니다. 예를 들어 로드 밸런서 트래픽을 허용하는 규칙이 있다고 가정하면 특정 IP 주소

그룹의 로드 밸런서 트래픽을 거부하는 규칙을 추가하고 이 규칙을 로드 밸런서 트래픽 허용 규칙보다 위에 배치할 수 있습니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)** 탭을 클릭한 후 **방화벽(Firewall)** 탭을 클릭합니다.
- 4 우선 순위를 변경할 규칙을 선택합니다.

참고 자동 생성된 규칙 또는 기본 규칙의 우선 순위는 변경할 수 없습니다.

- 5 위로 이동(Move Up)() 또는 아래로 이동(Move Down)() 아이콘을 클릭합니다.
- 6 **확인(OK)**을 클릭합니다.
- 7 **변경 내용 게시(Publish Changes)**를 클릭합니다.


NSX Edge 방화벽 규칙 삭제

NSX Edge 방화벽 탭에서 추가한 사용자 정의 방화벽 규칙을 삭제할 수 있습니다. 중앙 집중식 방화벽 탭에서 추가된 규칙은 여기서 삭제할 수 없습니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)** 탭을 클릭한 후 **방화벽(Firewall)** 탭을 클릭합니다.
- 4 삭제할 규칙을 선택합니다.

참고 자동 생성된 규칙이나 기본 규칙은 삭제할 수 없습니다.

- 5 **삭제>Delete**() 아이콘을 클릭합니다.

NAT 규칙 관리

NSX Edge는 전용 네트워크의 컴퓨터 또는 컴퓨터 그룹에 공용 주소를 할당하는 NAT(네트워크 주소 변환) 서비스를 제공합니다. 이 기술을 사용하면 경제성과 보안 목적으로 조직 또는 회사에서 사용해야 하는 공용 IP 주소의 개수가 제한됩니다. 전용 주소가 지정된 가상 시스템에서 실행되는 서비스에 대한 액세스 권한을 제공하도록 NAT 규칙을 구성해야 합니다.

NAT 서비스 구성은 SNAT(소스 NAT) 규칙과 DNAT(대상 NAT) 규칙으로 구분됩니다.

SNAT 규칙 추가

SNAT(소스 NAT) 규칙을 생성하여 소스 IP 주소를 공용 IP 주소에서 전용 IP 주소로 변경하거나 전용 IP 주소에서 공용 IP 주소로 변경할 수 있습니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)** 탭을 클릭한 후 **NAT** 탭을 클릭합니다.
- 4 **추가(Add)**(+) 아이콘을 클릭하고 **SNAT 규칙 추가(Add SNAT Rule)**를 선택합니다.
- 5 규칙을 추가할 인터페이스를 선택합니다.
- 6 필요한 프로토콜을 선택합니다.
- 7 원래 소스(공용) IP 주소를 다음 형식 중 하나로 입력합니다.

형식	예
IP 주소	192.0.2.0
IP 주소 범위	192.0.2.0-192.0.2.24
IP 주소/서브넷	192.0.2.0/24
임의	

- 8 원래 소스 포트 또는 포트 범위를 입력합니다.

형식	예
포트 번호	80
포트 범위	80-85
임의	

- 9 대상 IP 주소를 다음 형식 중 하나로 입력합니다.

형식	예
IP 주소	192.0.2.0
IP 주소 범위	192.0.2.0 -192.0.2.24
IP 주소/서브넷	192.0.2.0 /24
임의	

10 대상 포트 또는 포트 범위를 입력합니다.

형식	예
포트 번호	80
포트 범위	80-85
임의	

11 변환된 소스 IP 주소를 다음 형식 중 하나로 입력합니다.

형식	예
IP 주소	192.0.2.0
IP 주소 범위	192.0.2.0-192.0.2.24
IP 주소/서브넷	192.0.2.0/24
임의	

12 변환된 포트 또는 포트 범위를 입력합니다.

형식	예
포트 번호	80
포트 범위	80-85
임의	

13 규칙을 사용하도록 설정하려면 **사용(Enabled)**을 선택합니다.

14 주소 변환을 기록하려면 **로깅 사용(Enable logging)**을 클릭합니다.

15 규칙을 추가하려면 **확인(OK)**을 클릭합니다.

16 **변경 내용 게시(Publish Changes)**를 클릭합니다.

DNAT 규칙 추가

DNAT(대상 NAT) 규칙을 생성하여 대상 IP 주소를 공용 IP 주소에서 전용 IP 주소로 변경하거나 전용 IP 주소에서 공용 IP 주소로 변경할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **NAT** 탭을 클릭합니다.
- 5 **추가(Add)**(+) 아이콘을 클릭하고 **DNAT 규칙 추가(Add DNAT Rule)**를 선택합니다.
- 6 DNAT 규칙을 적용할 인터페이스를 선택합니다.

7 필요한 프로토콜을 선택합니다.

8 소스 IP 주소를 다음 형식 중 하나로 입력합니다.

형식	예
IP 주소	192.0.2.0
IP 주소 범위	192.0.2.0 -192.0.2.24
IP 주소/서브넷	192.0.2.0 /24
임의	

9 소스 포트 또는 포트 범위를 입력합니다.

형식	예
포트 번호	80
포트 범위	80-85
임의	

10 원래(공용) IP 주소를 다음 형식 중 하나로 입력합니다.

형식	예
IP 주소	192.0.2.0
IP 주소 범위	192.0.2.0 -192.0.2.24
IP 주소/서브넷	192.0.2.0 /24
임의	

11 원래 포트 또는 포트 범위를 입력합니다.

형식	예
포트 번호	80
포트 범위	80-85
임의	

12 변환된 IP 주소를 다음 형식 중 하나로 입력합니다.

형식	예
IP 주소	192.0.2.0
IP 주소 범위	192.0.2.0 -192.0.2.24
IP 주소/서브넷	192.0.2.0 /24
임의	

13 변환된 포트 또는 포트 범위를 입력합니다.

형식	예
포트 번호	80
포트 범위	80-85
임의	

14 규칙을 사용하도록 설정하려면 **사용(Enabled)**을 선택합니다.

15 주소 변환을 기록하려면 **로깅 사용(Enable logging)**을 선택합니다.

16 규칙을 추가하려면 **확인(OK)**을 클릭합니다.

17 **변경 내용 게시(Publish Changes)**를 클릭합니다.

방화벽 규칙 섹션 사용

섹션을 추가하여 방화벽 규칙을 분리할 수 있습니다. 예를 들어 영업 및 엔지니어링 부서에 대한 규칙을 별도의 섹션으로 분리할 수 있습니다.

L2 및 L3 규칙에 대한 여러 방화벽 규칙 섹션을 생성할 수 있습니다.

크로스 vCenter NSX 환경에는 여러 범용 규칙 섹션이 있을 수 있습니다. 여러 범용 섹션에서는 테넌트 및 애플리케이션에 따라 규칙을 쉽게 구성할 수 있습니다. 범용 섹션 내에서 규칙이 수정되거나 편집될 경우 해당 섹션에 대해 범용 분산 방화벽만 보조 NSX Manager와 동기화됩니다. 기본 NSX Manager에 대한 범용 규칙을 관리해야 하며, 범용 규칙을 추가하기 전에 범용 섹션을 생성해야 합니다. 범용 섹션은 항상 기본 및 보조 NSX Manager의 로컬 섹션 위에 나열됩니다.

범용 섹션 외부의 규칙은 규칙이 추가된 기본 또는 보조 NSX Manager에 계속 로컬 상태로 남아 있습니다.

방화벽 규칙 섹션 추가

방화벽 테이블에서 섹션을 새로 추가하여 규칙을 구성하거나 크로스 vCenter NSX 환경에서 사용할 범용 섹션을 생성할 수 있습니다.


사전 요구 사항

변경할 적합한 NSX Manager를 결정합니다.


- 독립 실행형 또는 단일 vCenter NSX 환경에는 NSX Manager가 하나만 있기 때문에 선택할 필요가 없습니다.
- 범용 개체는 기본 NSX Manager에서 관리해야 합니다.
- NSX Manager에 로컬인 개체는 NSX Manager에서 관리해야 합니다.
- 고급 연결 모드가 사용되도록 설정되지 않은 크로스 vCenter NSX 환경에서는 수정하려는 NSX Manager에 연결된 vCenter에서 구성을 변경해야 합니다.

- 고급 연결 모드의 크로스 vCenter NSX 환경에서는 모든 연결된 vCenter에서 원하는 NSX Manager의 구성을 변경할 수 있습니다. NSX Manager 드롭다운 메뉴에서 적절한 NSX Manager를 선택합니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동하십시오.
- 2 사용 가능한 NSX Manager가 둘 이상 있는 경우 하나를 선택하십시오. 범용 섹션을 추가하려면 기본 NSX Manager를 선택해야 합니다.
- 3 L3 규칙에 대한 섹션을 추가하려면 **일반(General)** 탭으로 이동합니다. L2 규칙에 대한 섹션을 추가하려면 **이더넷(Ethernet)** 탭을 클릭합니다.
- 4 **섹션 추가(Add Section)**() 아이콘을 클릭합니다.
- 5 섹션의 이름을 입력하고 새 섹션의 위치를 지정합니다. 섹션 이름은 NSX Manager 내에서 고유해야 합니다.
- 6 (선택 사항) 범용 섹션을 생성하려면 이 섹션을 범용 동기화에 대해 표시(Mark this section for Universal Synchronization)를 선택합니다.
- 7 **확인(OK)**을 클릭하고 **변경 내용 게시(Publish Changes)**를 클릭합니다.

다음에 수행할 작업


섹션에 규칙을 추가합니다. 해당 섹션의 **섹션 편집(Edit section)**() 아이콘을 클릭하여 섹션의 이름을 편집할 수 있습니다.

방화벽 규칙 섹션 병합

섹션을 병합하고 병합한 섹션 내의 규칙을 통합할 수 있습니다. Service Composer 또는 기본 섹션과는 섹션을 병합할 수 없습니다. 크로스 vCenter NSX 환경에서는 섹션을 범용 섹션과 병합할 수 없습니다.

복잡한 방화벽 구성을 병합 및 통합하면 유지 보수 및 가독성에 도움이 될 수 있습니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동하십시오.
- 2 병합할 섹션에 대해 **병합(Merge)**() 아이콘을 클릭하고 이 섹션을 위의 섹션과 병합할지 아니면 아래의 섹션과 병합할지를 지정합니다.


두 섹션의 규칙이 병합됩니다. 새로 생성된 섹션의 이름은 병합된 섹션이 아니라 원래 섹션의 이름을 유지합니다.
- 3 **변경 내용 게시(Publish Changes)**를 클릭합니다.

방화벽 규칙 섹션 삭제

방화벽 규칙 섹션을 삭제할 수 있습니다. 해당 섹션의 모든 규칙이 삭제됩니다.

섹션을 삭제한 후 방화벽 테이블의 다른 위치에 다시 추가할 수는 없습니다. 이렇게 하려면 섹션을 삭제하고 구성을 게시해야 합니다. 그런 다음 삭제한 섹션을 방화벽 테이블에 추가하고 구성을 다시 게시하면 됩니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동하십시오.
- 2 L3 규칙에 대한 섹션을 삭제하려면 **일반(General)** 탭으로 이동합니다. **이더넷(Ethernet)** 탭을 클릭하여 L2 규칙에 대한 섹션을 삭제합니다.
- 3 삭제할 섹션에 대해 **섹션 삭제(Delete section)**() 아이콘을 클릭합니다.
- 4 **확인(OK)**을 클릭하고 **변경 내용 게시(Publish Changes)**를 클릭합니다.

결과

섹션과 해당 섹션에 포함된 모든 규칙이 삭제됩니다.

방화벽 규칙 사용

분산 방화벽 규칙과 **Edge** 방화벽 규칙은 방화벽 탭에서 중앙 집중식으로 관리할 수 있습니다. 다중 테넌트 환경에서 제공자는 높은 수준의 중앙 집중식 방화벽 사용자 인터페이스에 대한 트래픽 흐름 규칙을 정의할 수 있습니다.

각 트래픽 세션에서 방화벽 테이블의 맨 위에 있는 규칙을 확인한 후에 테이블의 다음 규칙을 순서대로 확인합니다. 테이블에서 트래픽 매개 변수와 일치하는 첫 번째 규칙이 적용됩니다. 규칙은 다음 순서로 표시됩니다.

- 1 사용자가 방화벽 사용자 인터페이스에서 정의한 규칙이 가장 높은 우선 순위를 가지며 가상 NIC 수준별 우선 순위에 따라 하향식으로 순서 지정됩니다.
- 2 **Auto-plumbed** 규칙(제어 트래픽이 **Edge** 서비스를 위해 흐르도록 하는 규칙)
- 3 사용자가 **NSX Edge** 인터페이스에서 정의한 규칙
- 4 **Service Composer** 규칙 - 각 정책마다 별도의 섹션. 방화벽 테이블에서 이 규칙을 편집할 수는 없지만 보안 정책 방화벽 규칙 섹션의 위쪽에서 규칙을 추가할 수는 있습니다. 규칙을 추가할 경우 **Service Composer**에서 해당 규칙을 다시 동기화해야 합니다. 자세한 내용은 [장 17 Service Composer](#) 항목을 참조하십시오.
- 5 기본 분산 방화벽 규칙

방화벽 규칙은 방화벽을 사용하도록 설정한 클러스터에서만 적용됩니다. 클러스터 준비에 대한 자세한 내용은 **"NSX 설치 가이드"** 항목을 참조하십시오.

기본 분산 방화벽 규칙 편집

기본 방화벽 설정은 사용자 정의 방화벽 규칙과 일치하지 않는 트래픽에 적용됩니다. 분산 방화벽 기본 규칙이 중앙 집중식 방화벽 사용자 인터페이스에 표시되고, 각 **NSX Edge**에 대한 기본 규칙이 **NSX Edge** 수준에서 표시됩니다.

기본 분산 방화벽 규칙은 모든 **L3** 및 **L2** 트래픽이 인프라의 모든 준비된 클러스터를 통과하도록 허용합니다. 기본 규칙은 항상 규칙 테이블의 맨 아래에 있으며 삭제하거나 추가할 수 없습니다. 하지만 규칙의 작업 요소를 허용에서 차단 또는 거부로 변경하고, 규칙에 대한 주석을 추가하고, 해당 규칙에 대해 트래픽이 기록되어야 하는지 여부를 지정할 수 있습니다.

크로스 **vCenter NSX** 환경에서 기본 규칙은 범용 규칙이 아닙니다. 모든 **NSX Manager**에서 기본 규칙을 변경해야 합니다.

절차

1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동합니다.

2 기본 섹션을 확장하고 필요한 내용을 변경합니다.

작업(Action) 및 **로그(Log)**를 편집하거나 기본 규칙에 주석을 추가하는 것만 가능합니다.

분산 방화벽 규칙 추가

방화벽 규칙은 **NSX Manager** 범위에서 추가합니다. [적용 대상] 필드를 사용하면 규칙을 적용할 범위를 좁힐 수 있습니다. 각 규칙에 대해 소스 및 대상 수준에서 여러 개체를 추가할 수 있어 추가해야 할 총 방화벽 규칙 수가 줄어듭니다.

다음 **vCenter** 개체를 방화벽 규칙의 소스 또는 대상으로 지정할 수 있습니다.

표 10-2. 방화벽 규칙에 지원되는 개체

소스 또는 대상	적용 대상
<ul style="list-style-type: none"> ■ 클러스터 ■ 데이터센터 ■ 분산 포트 그룹 ■ IP 집합 ■ 레거시 포트 그룹 ■ 논리적 스위치 ■ 리소스 풀 ■ 보안 그룹 ■ vApp ■ 가상 시스템 ■ vNIC ■ IP 주소(IPv4 또는 IPv6) 	<ul style="list-style-type: none"> ■ 분산 방화벽이 설치된 모든 클러스터(네트워크 가상화를 위해 준비된 모든 클러스터) ■ 준비된 클러스터에 설치된 모든 Edge Gateway ■ 클러스터 ■ 데이터센터 ■ 분산 포트 그룹 ■ Edge ■ 레거시 포트 그룹 ■ 논리적 스위치 ■ 보안 그룹 ■ 가상 시스템 ■ vNIC

사전 요구 사항

NSX 분산 방화벽의 상태가 이전 버전과 호환되는 모드가 아닌지 확인하십시오. 현재 상태를 확인하려면 REST API 호출 GET `https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state`를 사용하십시오. 현재 상태가 이전 버전과 호환되는 모드이면 REST API 호출 PUT `https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state`를 사용하여 상태를 이후 버전과 호환되는 모드로 변경할 수 있습니다. 분산 방화벽이 이전 버전과 호환되는 모드에 있을 때는 분산 방화벽 규칙을 게시하지 마십시오.

범용 방화벽 규칙을 추가할 경우 [범용 방화벽 규칙 추가](#) 항목을 참조하십시오.

ID 기반 방화벽 규칙을 추가할 경우 다음을 확인하십시오.

- 하나 이상의 도메인이 NSX Manager에 등록되어 있습니다. NSX Manager는 등록된 각 도메인에서 그룹 및 사용자 정보와 서로 간의 관계를 가져옵니다. [NSX Manager에 Windows 도메인 등록](#)을 참조하십시오.
- Active Directory 개체를 기반으로 보안 그룹이 생성되고 이는 규칙의 소스 또는 대상으로 사용될 수 있습니다. [보안 그룹 생성](#)을 참조하십시오.


VMware vCenter 개체 기반의 규칙을 추가할 경우 가상 시스템에 VMware Tools가 설치되어 있는지 확인하십시오. "NSX 설치 가이드"를 참조하십시오.


6.1.5에서 6.2.3으로 마이그레이션된 VM은 TFTP ALG를 지원하지 않습니다. 마이그레이션 후에 TFTP ALG 지원을 사용하도록 설정하려면 예외 목록에서 VM을 추가했다가 제거하거나 VM을 다시 시작하십시오. TFTP ALG가 지원되는 새 6.2.3 필터가 생성됩니다.

절차




- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동하십시오.
- 2 L3 규칙을 추가하려면 **일반(General)** 탭으로 이동합니다. L2 규칙을 추가하려면 **이더넷(Ethernet)** 탭을 클릭합니다.
- 3 규칙을 추가할 섹션에서 **규칙 추가(Add rule)(+)** 아이콘을 클릭합니다.
- 4 **변경 내용 게시(Publish Changes)**를 클릭합니다.

새로 생성한 규칙은 섹션의 맨 위에 추가됩니다. 섹션에 시스템 정의 규칙만 있는 경우 새 규칙이 기본 규칙 위에 추가됩니다.




규칙을 섹션의 특정 위치에 추가하려면 규칙을 선택합니다. 번호 옆에서  을 클릭하고 **위에 추가(Add Above)** 또는 **아래에 추가(Add Below)**를 선택합니다.

- 5 새 규칙의 **이름(Name)** 셀을 가리키고  을 클릭합니다.
- 6 새 규칙의 이름을 입력합니다.




7 새 규칙의 **소스(Source)** 셀을 가리킵니다. 아래 표에서 설명하는 추가 아이콘이 표시됩니다.

옵션	설명
 클릭	<p>소스를 IP 주소로 지정하려면</p> <ol style="list-style-type: none"> IP 주소 형식을 선택합니다. 방화벽은 IPv4와 IPv6 형식을 모두 지원합니다. IP 주소를 입력합니다. 섬표로 구분된 목록에 IP 주소를 여러 개 입력할 수 있습니다. 목록에는 최대 255자가 포함될 수 있습니다.
 클릭	<p>소스를 특정 IP 주소 이외의 개체로 지정하려면</p> <ol style="list-style-type: none"> 보기(View)에서 통신이 시작된 컨테이너를 선택합니다. 선택한 컨테이너에 대한 개체가 표시됩니다. 개체를 하나 이상 선택하고  를 클릭합니다. 새 보안 그룹 또는 IPSet를 생성할 수 있습니다. 새 개체를 생성하면 기본적으로 소스 옆에 추가됩니다. 새 보안 그룹 또는 IPSet를 생성하는 방법에 대한 자세한 내용은 장 21 네트워크 및 보안 개체의 내용을 참조하십시오. 규칙에서 소스를 제외하려면 고급 옵션(Advanced options)을 클릭하십시오. 규칙에서 이 소스를 제외하려면 소스 부정(Negate Source)을 선택합니다. 소스 부정(Negate Source)을 선택하면 이전 단계에서 지정한 소스를 제외한 모든 소스에서 들어오는 트래픽에 규칙이 적용됩니다. 소스 부정(Negate Source)을 선택하지 않으면 이전 단계에서 지정한 소스에서 들어오는 트래픽에 규칙이 적용됩니다. 확인(OK)을 클릭합니다.

8 새 규칙의 **대상(Destination)** 셀을 가리킵니다. 아래 표에서 설명하는 추가 아이콘이 표시됩니다.

옵션	설명
 클릭	<p>대상을 IP 주소로 지정하려면</p> <ol style="list-style-type: none"> IP 주소 형식을 선택합니다. 방화벽은 IPv4와 IPv6 형식을 모두 지원합니다. IP 주소를 입력합니다. 섬표로 구분된 목록에 IP 주소를 여러 개 입력할 수 있습니다. 목록에는 최대 255자가 포함될 수 있습니다.
 클릭	<p>대상을 특정 IP 주소 이외의 개체로 지정하려면</p> <ol style="list-style-type: none"> 보기(View)에서 통신이 향하는 대상 컨테이너를 선택합니다. 선택한 컨테이너에 대한 개체가 표시됩니다. 개체를 하나 이상 선택하고  를 클릭합니다. 새 보안 그룹 또는 IPSet를 생성할 수 있습니다. 새 개체를 생성하면 기본적으로 대상 열에 추가됩니다. 새 보안 그룹 또는 IPSet를 생성하는 방법에 대한 자세한 내용은 장 21 네트워크 및 보안 개체의 내용을 참조하십시오. 대상 포트를 제외하려면 고급 옵션(Advanced options)을 클릭하십시오. 규칙에서 이 대상을 제외하려면 대상 부정(Negate Destination)을 선택합니다. 대상 부정(Negate Destination)을 선택하면 이전 단계에서 지정한 대상을 제외한 모든 대상으로 이동하는 트래픽에 규칙이 적용됩니다. 대상 부정(Negate Destination)을 선택하지 않으면 이전 단계에서 지정한 대상으로 이동하는 트래픽에 규칙이 적용됩니다. 확인(OK)을 클릭합니다.

9 새 규칙의 서비스(Service) 셀을 가리킵니다. 아래 표에서 설명하는 추가 아이콘이 표시됩니다.

옵션	설명
 클릭	<p>포트-프로토콜 조합으로 서비스를 지정하려면</p> <p>a 서비스 프로토콜을 선택합니다.</p> <p>분산 방화벽은 TFTP, FTP, ORACLE TNS, MS-RPC 및 SUN-RPC 프로토콜에 대해 ALG(Application Level Gateway)를 지원합니다.</p> <p>Edge는 FTP, TFTP 및 SNMP_BASIC에 대해 ALG를 지원합니다.</p> <p>참고: 6.1.5에서 6.2.3으로 마이그레이션된 VM은 TFTP ALG를 지원하지 않습니다. 마이그레이션 후에 TFTP ALG 지원을 사용하도록 설정하려면 예외 목록에서 VM을 추가했다가 제거하거나 VM을 다시 시작하십시오. TFTP ALG가 지원되는 새 6.2.3 필터가 생성됩니다.</p> <p>b 포트 번호를 입력하고 확인(OK)을 클릭합니다.</p>
 클릭	<p>미리 정의된 서비스/서비스 그룹을 선택하거나 새 서비스/서비스 그룹을 정의하려면</p> <p>a 개체를 하나 이상 선택하고  를 클릭합니다.</p> <p>새 서비스 또는 서비스 그룹을 생성할 수 있습니다. 새 개체를 생성하면 기본적으로 선택한 개체 열에 추가됩니다.</p> <p>b 확인(OK)을 클릭합니다.</p>

ACK 또는 SYN 과부하로부터 네트워크를 보호하기 위해 서비스를 TCP-all_ports 또는 UDP-all_ports로 선택하고 기본 규칙으로 차단 작업을 설정할 수 있습니다. 기본 규칙을 수정하는 방법에 대한 자세한 내용은 [기본 분산 방화벽 규칙 편집](#) 항목을 참조하십시오.

10 새 규칙의 작업(Action) 셀을 가리키고 을 클릭하십시오. 아래 표에서 설명한 대로 적절하게 선택하고 **확인(OK)**을 클릭하십시오.

작업	결과
허용	지정된 소스, 대상 및 서비스와의 트래픽을 허용합니다.
차단	지정된 소스, 대상 및 서비스와의 트래픽을 차단합니다.
거부	<p>허용되지 않는 패킷에 대해 거부 메시지를 전송합니다.</p> <p>TCP 연결에 대해 RST 패킷이 전송됩니다.</p> <p>UDP, ICMP 및 기타 IP 연결에 대해 관리 목적으로 금지된 코드가 포함된 ICMP 메시지가 전송됩니다.</p>
로그	이 규칙과 일치하는 모든 세션을 로깅합니다. 로깅을 사용하도록 설정하면 성능에 영향을 줄 수 있습니다.
로깅 안 함	세션을 로깅하지 않습니다.

- 11 적용 대상(Applied To)**에서 이 규칙이 적용될 수 있는 범위를 정의하십시오. 아래 표에서 설명한 대로 적절하게 선택하고 **확인(OK)**을 클릭하십시오.

규칙 적용 대상	작업
사용자 환경에서 준비된 모든 클러스터	이 규칙을 분산 방화벽이 설치된 모든 클러스터에 적용합니다 (Apply this rule on all clusters on which Distributed Firewall is enabled)를 선택하십시오. 확인을 클릭하면 이 규칙에 대한 적용 대상 열에 분산 방화벽(Distributed Firewall)이 표시됩니다.
사용자 환경의 모든 NSX Edge Gateway	이 규칙을 모든 Edge Gateway에 적용합니다(Apply this rule on all Edge gateways)를 선택하십시오. [확인]을 클릭하면 이 규칙에 대한 적용 대상 열에 모든 Edge(All Edges)가 표시됩니다. 위 옵션을 모두 선택하면 적용 대상 열에 임의(Any)가 표시됩니다.
하나 이상의 클러스터, 데이터센터, 분산 가상 포트 그룹, NSX Edge, 네트워크, 가상 시스템, vNIC 또는 논리적 스위치	1 컨테이너 유형(Container type)에서 해당하는 개체를 선택하십시오. 2 사용 가능 목록에서 하나 이상의 개체를 선택하고  를 클릭하십시오.




규칙의 소스 및 대상 필드에 가상 시스템/vNIC가 있는 경우 규칙이 제대로 작동하려면 소스 및 대상 가상 시스템/vNIC를 **적용 대상(Applied To)**에 추가해야 합니다.


- 12 변경 내용 게시(Publish Changes)**를 클릭합니다.

잠시 후 게시 작업이 성공했음을 나타내는 메시지가 표시됩니다. 실패한 경우 규칙이 적용되지 않은 호스트가 나열됩니다. 실패한 게시에 대한 추가 세부 정보를 보려면 **NSX Managers > NSX_Manager_IP_Address > 모니터링(Monitor) > 시스템 이벤트(System Events)**로 이동하십시오.

변경 내용 게시(Publish Changes)를 클릭하면 방화벽 구성이 자동으로 저장됩니다. 이전 구성으로 되돌리기에 대한 자세한 내용은 [저장된 방화벽 구성 로드](#) 항목을 참조하십시오.

다음에 수행할 작업

- 규칙을 사용하지 않도록 설정하려면 을 클릭하고, 규칙을 사용하도록 설정하려면 을 클릭하십시오.
- 규칙 테이블에서 추가 열을 표시하려면 을 클릭하고 해당 열을 선택합니다.

열 이름	표시되는 정보
규칙 ID	각 규칙에 대해 생성된 고유 시스템 ID
로그	이 규칙에 대한 트래픽을 로깅하거나 로깅하지 않습니다.
통계	 를 클릭하면 이 규칙과 관련된 트래픽(트래픽 패킷 수 및 크기)이 표시됩니다.
주석	규칙에 대한 주석입니다.


- 검색 필드에 텍스트를 입력하여 규칙을 검색합니다.
- 방화벽 테이블에서 규칙을 위 아래로 이동합니다.
- **섹션 병합(Merge section)** 아이콘을 클릭한 후 **위 섹션과 병합(Merge with above section)** 또는 **아래 섹션과 병합(Merge with below section)**을 선택하여 섹션을 병합합니다.

분산 방화벽 규칙 강제 동기화

방화벽 규칙을 호스트에 게시할 수 없으면 강제 동기화를 수행합니다.

개별 호스트의 방화벽 규칙을 NSX Manager와 동기화해야 할 경우 강제 동기화가 사용됩니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 설치(Installation) > 호스트 준비(Host Preparation)**로 이동합니다.
- 2 강제 동기화를 수행할 클러스터를 선택하고 **작업(Actions)**() > **서비스 강제 동기화 서비스(Force Sync Services)**를 클릭합니다.
- 3 강제로 동기화할 서비스에서 **방화벽(Firewall)**을 선택합니다. **확인(OK)**을 클릭합니다.
동기화하는 동안 방화벽 상태가 [사용 중]으로 변경됩니다.

범용 방화벽 규칙 추가

크로스 vCenter NSX 환경에서 범용 규칙은 범용 규칙 섹션의 기본 NSX Manager에 정의된 분산 방화벽 규칙을 참조합니다. 사용자 환경의 모든 보조 NSX Manager에서 이 규칙이 복제되므로 vCenter 경계에서 일관된 방화벽 정책을 유지할 수 있습니다. 여러 vCenter Server 사이의 vMotion에 대해 Edge 방화벽 규칙이 지원되지 않습니다.

기본 NSX Manager에는 범용 L2 규칙에 대한 여러 범용 섹션과 범용 L3 규칙에 대한 여러 범용 섹션이 포함될 수 있습니다. 범용 섹션은 모든 로컬 및 Service Composer 섹션 위쪽에 있습니다. 보조 NSX Manager에서 범용 섹션 및 범용 규칙을 볼 수 있지만 편집은 할 수 없습니다. 로컬 섹션에 따라 범용 섹션을 배치해도 규칙 우선 순위를 방해하지 않습니다.

표 10-3. 범용 방화벽 규칙에 지원되는 개체


소스 및 대상	적용 대상	서비스
<ul style="list-style-type: none"> ■ 범용 MAC 집합 ■ 범용 IP 집합 ■ 범용 보안 그룹(범용 보안 태그, IP 집합, MAC 집합 또는 범용 보안 그룹을 포함할 수 있음) 	<ul style="list-style-type: none"> ■ 범용 보안 그룹(범용 보안 태그, IP 집합, MAC 집합 또는 범용 보안 그룹을 포함할 수 있음) ■ 범용 논리적 스위치 ■ 분산 방화벽 - 이 규칙을 분산 방화벽이 설치된 모든 클러스터에 적용합니다. 	<ul style="list-style-type: none"> ■ 사전 생성된 범용 서비스 및 서비스 그룹 ■ 사용자가 생성한 범용 서비스 및 서비스 그룹




다른 vCenter 개체는 범용 규칙에 지원되지 않습니다.

사전 요구 사항




범용 규칙을 생성하려면 먼저 범용 규칙 섹션을 생성해야 합니다. [방화벽 규칙 섹션 추가](#)를 참조하십시오.

절차




- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동하십시오.
- 2 NSX Manager에서 기본 NSX Manager가 선택되었는지 확인합니다.
범용 규칙은 기본 NSX Manager에서만 추가할 수 있습니다.
- 3 L3 범용 규칙을 추가하려면 **일반(General)** 탭에 있어야 합니다. L2 범용 규칙을 추가하려면 **이더넷(Ethernet)** 탭을 클릭합니다.
- 4 범용 섹션에서 **규칙 추가(Add rule)** (+) 아이콘을 클릭한 다음 **변경 내용 게시(Publish Changes)**를 클릭합니다.
새로 생성한 규칙은 범용 섹션의 맨 위에 추가됩니다.
- 5 새 규칙의 **이름(Name)** 셀을 가리키고  을 클릭합니다. 규칙의 이름을 입력합니다.
- 6 새 규칙의 **소스(Source)** 셀을 가리킵니다. 아래 표에서 설명하는 추가 아이콘이 표시됩니다.

옵션	설명
 클릭	<p>소스를 IP 주소로 지정하려면</p> <ol style="list-style-type: none"> a IP 주소 형식을 선택합니다. 방화벽은 IPv4와 IPv6 형식을 모두 지원합니다. b IP 주소를 입력합니다.
 클릭	<p>범용 IPSet, MACSet 또는 보안 그룹을 소스로 지정하려면</p> <ol style="list-style-type: none"> a 개체 유형(Object Type)에서 통신이 시작된 컨테이너를 선택합니다. 선택한 컨테이너에 대한 개체가 표시됩니다. b 개체를 하나 이상 선택하고  를 클릭합니다. 새 보안 그룹 또는 IPSet를 생성할 수 있습니다. 새 개체를 생성하면 기본적으로 소스 열에 추가됩니다. 새 보안 그룹 또는 IPSet를 생성하는 방법에 대한 자세한 내용은 장 21 네트워크 및 보안 개체의 내용을 참조하십시오. c 규칙에서 소스를 제외하려면 고급 옵션(Advanced options)을 클릭하십시오. d 규칙에서 이 소스를 제외하려면 소스 부정(Negate Source)을 선택합니다. 소스 부정(Negate Source)을 선택하면 이전 단계에서 지정한 소스를 제외한 모든 소스에서 들어오는 트래픽에 규칙이 적용됩니다. 소스 부정(Negate Source)을 선택하지 않으면 이전 단계에서 지정한 소스에서 들어오는 트래픽에 규칙이 적용됩니다. e 확인(OK)을 클릭합니다.


7 새 규칙의 대상(Destination) 셀을 가리킵니다. 아래 표에서 설명하는 추가 아이콘이 표시됩니다.

옵션	설명
 클릭	<p>대상을 IP 주소로 지정하려면</p> <ol style="list-style-type: none"> IP 주소 형식을 선택합니다. 방화벽은 IPv4와 IPv6 형식을 모두 지원합니다. IP 주소를 입력합니다.
 클릭	<p>범용 IPSet, MACSet 또는 보안 그룹을 대상으로 지정하려면</p> <ol style="list-style-type: none"> 개체 유형(Object Type)에서 통신이 향하는 대상 컨테이너를 선택합니다. 선택한 컨테이너에 대한 개체가 표시됩니다. 개체를 하나 이상 선택하고  를 클릭합니다. 새 보안 그룹 또는 IPSet를 생성할 수 있습니다. 새 개체를 생성하면 기본적으로 대상 열에 추가됩니다. 새 보안 그룹 또는 IPSet를 생성하는 방법에 대한 자세한 내용은 장 21 네트워크 및 보안 개체의 내용을 참조하십시오. 규칙에서 대상을 제외하려면 고급 옵션(Advanced options)을 클릭하십시오. 규칙에서 이 대상을 제외하려면 대상 부정(Negate Destination)을 선택합니다. 대상 부정(Negate Destination)을 선택하면 이전 단계에서 지정한 대상을 제외한 모든 대상으로 이동하는 트래픽에 규칙이 적용됩니다. 대상 부정(Negate Destination)을 선택하지 않으면 이전 단계에서 지정한 대상으로 이동하는 트래픽에 규칙이 적용됩니다. 확인(OK)을 클릭합니다.


8 새 규칙의 서비스(Service) 셀을 가리킵니다. 아래 표에서 설명하는 추가 아이콘이 표시됩니다.

옵션	설명
 클릭	<p>포트-프로토콜 조합으로 서비스를 지정하려면</p> <ol style="list-style-type: none"> 서비스 프로토콜을 선택합니다. 분산 방화벽은 FTP, CIFS, ORACLE TNS, MS-RPC 및 SUN-RPC 프로토콜에 대해 ALG(Application Level Gateway)를 지원합니다. 포트 번호를 입력하고 확인(OK)을 클릭합니다.
 클릭	<p>미리 정의된 범용 서비스/범용 서비스 그룹을 선택하거나 새 범용 서비스/범용 서비스 그룹을 정의하려면</p> <ol style="list-style-type: none"> 개체를 하나 이상 선택하고  를 클릭합니다. 새 서비스 또는 서비스 그룹을 생성할 수 있습니다. 새 개체를 생성하면 기본적으로 선택한 개체 열에 추가됩니다. 확인(OK)을 클릭합니다.

ACK 또는 SYN 과부하로부터 네트워크를 보호하기 위해 서비스를 TCP-all_ports 또는 UDP-all_ports로 선택하고 기본 규칙으로 차단 작업을 설정합니다. 기본 규칙을 수정하는 방법에 대한 자세한 내용은 [기본 분산 방화벽 규칙 편집](#) 항목을 참조하십시오.


- 9 새 규칙의 **작업(Action)** 셀을 가리키고  을 클릭합니다. 아래 표에서 설명한 대로 적절하게 선택하고 **확인(OK)**을 클릭하십시오.

작업	결과
허용	지정된 소스, 대상 및 서비스와의 트래픽을 허용합니다.
차단	지정된 소스, 대상 및 서비스와의 트래픽을 차단합니다.
거부	허용되지 않는 패킷에 대해 거부 메시지를 전송합니다. TCP 연결에 대해 RST 패킷이 전송됩니다. UDP, ICMP 및 기타 IP 연결에 대해 관리 목적으로 금지된 코드가 포함된 ICMP 메시지가 전송됩니다.
로그	이 규칙과 일치하는 모든 세션을 로깅합니다. 로깅을 사용하도록 설정하면 성능에 영향을 줄 수 있습니다.
로깅 안 함	세션을 로깅하지 않습니다.

- 10 **적용 대상(Applied To)** 셀에서 기본 설정(분산 방화벽)을 수락하여 분산 방화벽을 사용하도록 설정된 모든 클러스터에 규칙을 적용하십시오. 또는 편집 아이콘  을 클릭하여 규칙을 적용할 범용 논리적 스위치를 선택하십시오.

- 11 **변경 내용 게시(Publish Changes)**를 클릭합니다.

결과




모든 보조 NSX Manager에서 범용 규칙이 복제됩니다. 모든 NSX 인스턴스에서 규칙 ID가 동일합니다. 규칙 ID를 표시하려면  을 클릭한 다음 규칙 ID를 클릭하십시오.

기본 NSX Manager에서 범용 규칙을 편집할 수 있습니다. 보조 NSX Manager에서 범용 규칙은 읽기 전용입니다.


범용 섹션 계층 3 및 기본 섹션 계층 3이 포함된 방화벽 규칙:

No.	Name	Source	Destination	Service	Action	Applied To
▼ Universal Section Layer3 (Rule 1 - 2)						
1	Web Micro-Segmentation	Web USG	Web USG	* any	Block	Distributed Firewall
2	Allow Web Access	* any	Web USG	HTTPS SSH	Allow	Distributed Firewall
▼ Default Section Layer3 (Rule 3 - 7)						
3	Web Micro-Segmentation	Web SG	Web SG	* any	Allow	Distributed Firewall
4	Allow Web Access	* any	Web SG	HTTPS SSH	Allow	Distributed Firewall
5	Default Rule NDP	* any	* any	IPv6-ICMP Neighbor ... IPv6-ICMP Neighbor ...	Allow	Distributed Firewall
6	Default Rule DHCP	* any	* any	DHCP-Client DHCP-Server	Allow	Distributed Firewall
7	Default Rule	* any	* any	* any	Block	Distributed Firewall

다음에 수행할 작업

- 번호 열에서  을 클릭하여 규칙을 사용하지 않도록 설정하거나  을 클릭하여 규칙을 사용하도록 설정하십시오.
- 규칙 테이블에서 추가 열을 표시하려면  을 클릭하고 해당 열을 선택합니다.

열 이름 표시되는 정보

규칙 ID	각 규칙에 대해 생성된 고유 시스템 ID
로그	이 규칙에 대한 트래픽을 로깅하거나 로깅하지 않습니다.
통계	 를 클릭하면 이 규칙과 관련된 트래픽(트래픽 패킷 수 및 크기)이 표시됩니다.
주석	규칙에 대한 주석입니다.


- 검색 필드에 텍스트를 입력하여 규칙을 검색합니다.
- 방화벽 테이블에서 규칙을 위 아래로 이동합니다.

사용자 지정 계층 3 프로토콜을 사용하는 방화벽 규칙


방화벽 규칙은 프로토콜 드롭다운 메뉴에 나열되지 않은 사용자 지정 프로토콜 번호를 사용하여 생성할 수 있습니다.


사용자 지정 프로토콜 번호를 사용하는 방화벽 규칙은 분산 방화벽 또는 NSX Edge 방화벽에 대해 생성할 수 있습니다.


절차

- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동하십시오.
- 2 L3 규칙을 추가하려면 **일반(General)** 탭으로 이동합니다. **규칙 추가(Add rule)**() 아이콘을 클릭합니다.
- 3 **변경 내용 게시(Publish Changes)**를 클릭합니다.

새로 생성한 규칙은 섹션의 맨 위에 추가됩니다. 섹션에 시스템 정의 규칙만 있는 경우 새 규칙이 기본 규칙 위에 추가됩니다.

규칙을 섹션의 특정 위치에 추가하려면 규칙을 선택합니다. 번호 열에서  을 클릭하고 **위에 추가(Add Above)** 또는 **아래에 추가(Add Below)**를 선택합니다.

- 4 새 규칙의 **이름(Name)** 셀을 가리키고  을 클릭합니다.
- 5 새 규칙의 이름을 입력합니다.
- 6 새 규칙의 **소스(Source)**를 지정합니다. 아이콘에 대한 자세한 내용은 [분산 방화벽 규칙 추가](#)를 참조하십시오.
- 7 새 규칙의 **대상(Destination)**을 지정합니다. 자세한 내용은 [분산 방화벽 규칙 추가](#)를 참조하십시오.

- 8 새 규칙의 **서비스(Service)** 셀을 가리킵니다. **서비스 추가(Add Service)()** 아이콘을 클릭합니다.
- 9 **서비스 지정(Specify Service)** 창 왼쪽 아래에 있는 **새 서비스(New Service)**를 클릭합니다.
- 10 새 프로토콜의 **이름(Name)**(예: OSPF)을 입력합니다.
- 11 [프로토콜] 드롭다운 메뉴에서 **L3_OTHERS**를 선택합니다.
드롭다운 메뉴 아래에 **프로토콜 번호(Protocol Number)** 필드가 표시됩니다.
- 12 **프로토콜 번호(Protocol Number)**(예: OSPF의 경우 89)를 입력합니다.
- 13 **확인(OK)**을 클릭합니다.

결과

사용자 지정 프로토콜 번호를 사용하여 방화벽 규칙이 생성되었습니다.

게시되지 않은 구성 저장

규칙을 추가하고 구성을 저장한 후 바로 게시하지 않아도 됩니다. 저장한 구성을 나중에 로드하여 게시할 수 있습니다.

절차

- 1 방화벽 규칙을 추가합니다. [분산 방화벽 규칙 추가](#)를 참조하십시오.
- 2 **변경 내용 저장(Save Changes)**을 클릭합니다.
- 3 구성의 이름과 설명을 입력하고 **확인(OK)**을 클릭합니다.
- 4 **구성 보존(Preserve Configuration)**을 클릭하여 이 변경 내용을 보존합니다.
NSX에서는 최대 100개의 구성을 저장할 수 있습니다. 이 한도를 초과한 후에도 **구성 보존(Preserve Configuration)**이라고 표시된 저장된 구성은 보존되지만, 보존된 구성을 위한 공간을 확보하기 위해 이전의 보존되지 않은 구성은 삭제됩니다.
- 5 다음 중 하나를 수행합니다.
 - 규칙을 추가하기 전의 상태로 구성을 되돌리려면 **변경 내용 되돌리기(Revert Changes)**를 클릭합니다. 방금 추가한 규칙을 게시하려면 **구성 로드(Load Configuration)** 아이콘을 클릭하고 3단계에서 저장한 규칙을 선택한 후 **확인(OK)**을 클릭합니다.
 - 규칙 추가를 계속하려면 **변경 내용 업데이트(Update Changes)**를 클릭합니다.

저장된 방화벽 구성 로드

자동 저장되거나 가져온 방화벽 구성을 로드할 수 있습니다. 현재 구성에 **Service Composer**가 관리하는 규칙이 포함된 경우 구성을 가져오면 규칙이 재정의됩니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 방화벽(Firewall)**으로 이동하십시오.

- 2 L3 방화벽 구성을 로드하려면 **일반(General)** 탭으로 이동합니다. **이더넷(Ethernet)** 탭을 클릭하고 L2 방화벽 구성을 로드합니다.

- 3 **구성 로드(Load configuration)**() 아이콘을 클릭합니다.

- 4 로드할 구성을 선택하고 **확인(OK)**을 클릭합니다.

현재 구성이 선택한 구성으로 바뀝니다.

다음에 수행할 작업

구성의 **Service Composer** 규칙이 로드된 구성으로 재정의된 경우 **Service Composer** 내의 보안 정책 탭에서 **작업(Actions) > 방화벽 규칙 동기화(Synchronize Firewall Rules)**를 클릭합니다.

방화벽 규칙 필터링

많은 조건을 사용하여 규칙 집합을 필터링할 수 있고, 이를 통해 규칙을 쉽게 수정할 수 있습니다. 소스 또는 대상 가상 시스템이나 IP 주소, 규칙 작업, 로깅, 규칙 이름, 주석 및 규칙 ID별로 규칙을 필터링할 수 있습니다.

절차

- 1 [방화벽] 탭에서 **필터 적용(Apply Filter)** () 아이콘을 클릭합니다.

- 2 필요에 따라 필터링 조건을 입력하거나 선택합니다.

- 3 **적용(Apply)**을 클릭합니다.

필터링 조건과 일치하는 규칙이 표시됩니다.

다음에 수행할 작업

모든 규칙을 다시 표시하려면 **적용된 필터 제거(Remove applied filter)** () 아이콘을 클릭합니다.

방화벽 규칙 순서 변경



방화벽 규칙은 규칙 테이블에 있는 순서대로 적용됩니다.

규칙은 다음 순서로 표시 및 적용됩니다.

- 1 사용자가 정의한 사전 규칙이 가장 높은 우선 순위를 갖고 가상 NIC 수준별 우선 순위에 따라 위에서 아래로 적용됩니다.
- 2 자동 연결 규칙.
- 3 NSX Edge 수준에서 정의된 로컬 규칙.
- 4 **Service Composer** 규칙 - 각 정책마다 별도의 섹션. 방화벽 테이블에서 이 규칙을 편집할 수는 없지만 보안 정책 방화벽 규칙 섹션의 위쪽에서 규칙을 추가할 수는 있습니다. 규칙을 추가할 경우 **Service Composer**에서 해당 규칙을 다시 동기화해야 합니다. 자세한 내용은 [장 17 Service Composer](#) 항목을 참조하십시오.
- 5 기본 분산 방화벽 규칙.

사용자 지정 규칙을 테이블에서 위나 아래로 이동할 수 있습니다. 기본 규칙은 항상 테이블의 맨 아래에 있으며 이동할 수 없습니다.


절차

- 1 **방화벽(Firewall)** 탭에서 이동할 규칙을 선택합니다.
- 2 규칙 위로 이동(Move rule up)() 또는 규칙 아래로 이동(Move rule down)() 아이콘을 클릭합니다.
- 3 **변경 내용 게시(Publish Changes)**를 클릭합니다.

방화벽 규칙 삭제

생성한 방화벽 규칙을 삭제할 수 있습니다. **Service Composer**가 관리하는 기본 규칙은 삭제할 수 없습니다.

절차

- 1 **방화벽(Firewall)** 탭에서 규칙을 선택합니다.
- 2 방화벽 테이블 위의 **선택된 규칙 삭제>Delete selected rule**() 아이콘을 클릭합니다.
- 3 **변경 내용 게시(Publish Changes)**를 클릭합니다.

Firewall 로그

Firewall은 감사 로그, 규칙 메시지 로그 및 시스템 이벤트 로그와 같은 로그 파일을 생성하고 저장합니다. 방화벽을 사용하도록 설정된 각 클러스터에 대해 **syslog** 서버를 구성해야 합니다. **syslog** 서버는 **Syslog.global.logHost** 특성에 지정되어 있습니다.

방화벽은 다음 표에 설명된 대로 로그를 생성합니다.

표 10-4. Firewall 로그

로그 유형	설명	위치
규칙 메시지 로그	각 규칙에 대해 허용 또는 거부된 트래픽 같은 모든 액세스 결정 사항이 포함됩니다(해당 규칙에 대한 로깅이 사용하도록 설정된 경우). 로깅이 사용되도록 설정된 규칙에 대한 DFW 패킷 로그를 포함합니다.	/var/log/dfwpktlogs.log
감사 로그	관리 로그 및 분산 방화벽 구성 변경 사항이 포함됩니다.	/home/secureall/secureall/logs/vsm.log
시스템 이벤트 로그	적용된 분산 방화벽 구성, 생성 또는 삭제되거나 실패한 필터, 보안 그룹에 추가된 가상 시스템 등이 포함됩니다.	/home/secureall/secureall/logs/vsm.log

표 10-4. Firewall 로그 (계속)

로그 유형	설명	위치
데이터부/VMKernel 로그	방화벽 커널 모듈(VSIP)과 관련된 작업을 캡처합니다. 시스템에서 생성된 메시지에 대한 로그 항목이 포함됩니다.	/var/log/vmkernel.log
메시지 버스 클라이언트/ VSFWFWD 로그	방화벽 에이전트의 활동을 캡처합니다.	/var/log/vsfwd.log

참고 *vsm.log* 파일은 NSX Manager CLI(명령줄 인터페이스)에서 **show log manager** 명령을 실행하고 키워드 *vsm.log*에 대해 **grep**를 수행하여 액세스할 수 있습니다. 이 파일은 루트 권한이 있는 사용자 또는 사용자 그룹에서만 액세스할 수 있습니다.

규칙 메시지 로그

규칙 메시지 로그에는 각 규칙에 대해 허용 또는 거부된 트래픽 같은 모든 액세스 결정 사항이 포함됩니다 (해당 규칙에 대한 로깅이 사용하도록 설정된 경우). 이러한 로그는 각 호스트의 **/var/log/dfwpktlogs.log**에 저장됩니다.

방화벽 로그 메시지의 예는 다음과 같습니다.

```
# more /var/log/dfwpktlogs.log
2015-03-10T03:22:22.671Z INET match DROP domain-c7/1002 IN 242 UDP 192.168.110.10/138->192.168.110.255/138

# more /var/log/dfwpktlogs.log
2017-04-11T21:09:59.877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST
10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070
```

자세한 예:

```
2017-10-19T22:38:05.586Z 58734 INET match PASS domain-c8/1006 OUT 84 ICMP 172.18.8.121->172.18.8.119
RULE_TAG
2017-10-19T22:38:08.723Z 58734 INET match PASS domain-c8/1006 OUT 60 TCP 172.18.8.121/36485->172.18.8.119/22 S RULE_TAG
2017-10-19T22:38:18.785Z 58734 INET TERM domain-c8/1006 OUT ICMP 8 0 172.18.8.121->172.18.8.119 2/2
168/168 RULE_TAG
2017-10-19T22:38:20.789Z 58734 INET TERM domain-c8/1006 OUT TCP FIN 172.18.8.121/36484->172.18.8.119/22 44/33 4965/5009 RULE_TAG
```

다음 예에서 각각의 의미는 다음과 같습니다.

- 1002는 분산 방화벽 규칙 ID입니다.
- domain-c7은 vCenter MOB(Managed Object Browser)에서의 클러스터 ID입니다.
- 192.168.110.10/138은 소스 IP 주소입니다.

- 192.168.110.255/138은 대상 IP 주소입니다.
- **RULE_TAG**는 방화벽 규칙을 추가 또는 편집하는 동안 **태그** 텍스트 상자에 추가하는 텍스트의 예입니다.

다음 예에서는 192.168.110.10에서 172.16.10.12로의 ping 결과를 보여 줍니다.

```
# tail -f /var/log/dfwptlogs.log | grep 192.168.110.10
```

```
2015-03-10T03:20:31.274Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
2015-03-10T03:20:35.794Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
```

다음 표에서는 방화벽 로그 메시지의 텍스트 상자에 대해 설명합니다.

표 10-5. 로그 파일 항목의 구성 요소

구성 요소	예제 값
타임 스탬프	2017-04-11T21:09:59
방화벽 관련 부분	877Z ESXi_FQDN dfwptlogs: 50047 INET TERM domain-c1/1001 IN TCP RST 10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070

표 10-6. 로그 파일 항목의 방화벽 특정 부분

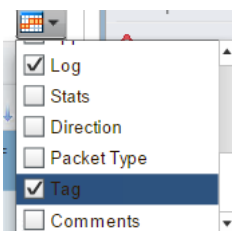
엔티티	가능한 값
필터 해시	필터 이름 및 기타 정보를 가져오는 데 사용할 수 있는 숫자입니다.
AF 값	INET, INET6
이유	<ul style="list-style-type: none"> ■ match: 패킷이 규칙과 일치하는지 확인합니다. ■ bad-offset: 패킷을 가져오는 동안 데이터 경로 내부 오류가 발생했습니다. ■ fragment: 첫 번째 조각으로 어셈블된 후 첫 번째가 아닌 조각입니다. ■ short: 패킷이 너무 짧습니다(예를 들어 IP 헤더 또는 TCP/UDP 헤더를 포함하는 데 완전하지 않은 경우도 포함). ■ normalize: 올바른 헤더 또는 페이로드가 없는 잘못된 형식의 패킷입니다. ■ memory: 데이터 경로의 메모리가 부족합니다. ■ bad-timestamp: 잘못된 TCP 타임 스탬프입니다. ■ proto cksum: 잘못된 프로토콜 체크섬입니다. ■ state-mismatch: TCP 상태 시스템을 확인을 통과하지 못한 TCP 패킷입니다. ■ state-insert: 중복된 연결이 발견되었습니다. ■ state-limit: 데이터 경로에서 추적할 수 있는 최대 상태 수에 도달했습니다. ■ SpoofGuard: SpoofGuard에서 패킷을 삭제했습니다. ■ TERM: 연결이 종료됩니다.

표 10-6. 로그 파일 항목의 방화벽 특정 부분 (계속)

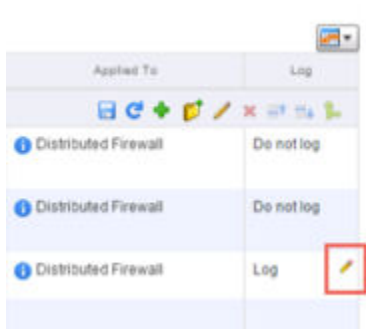
엔티티	가능한 값
작업	<ul style="list-style-type: none"> ■ PASS: 패킷을 수락합니다. ■ DROP: 패킷을 삭제합니다. ■ NAT: SNAT 규칙입니다. ■ NONAT: SNAT 규칙과 일치하는 항목을 찾았으나 주소를 변환할 수 없습니다. ■ RDR: DNAT 규칙입니다. ■ NORDR: DNAT 규칙과 일치하는 항목을 찾았으나 주소를 변환할 수 없습니다. ■ PUNT: 현재 VM의 동일한 하이퍼바이저에서 실행되는 서비스 VM으로 패킷을 보냅니다. ■ REDIRECT: 현재 VM의 하이퍼바이저 외부에서 실행되는 네트워크 서비스에 패킷을 보냅니다. ■ COPY: 패킷을 수락하고 현재 VM의 동일한 하이퍼바이저에서 실행되는 서비스 VM을 복사합니다. ■ REJECT: 패킷을 거부합니다.
규칙 집합 및 규칙 ID	규칙 집합/규칙 ID
방향	IN, OUT
패킷 길이	길이
프로토콜	<p>TCP, UDP, ICMP 또는 PROTO(프로토콜 번호)</p> <p>TCP 연결의 경우 연결이 종료되는 실제 이유는 키워드 TCP 다음에 표시됩니다.</p> <p>TERM이 TCP 세션의 원인인 경우 PROTO 행에 추가 설명이 표시됩니다. TCP 연결 종료의 가능한 원인에는 RST(TCP RST 패킷), FIN(FIN TCP 패킷) 및 TIMEOUT(너무 오랫동안 유휴 상태임)이 포함됩니다.</p> <p>위 예제에서는 RST입니다. 따라서 재설정해야 하는 연결에 RST 패킷이 있음을 의미합니다.</p> <p>TCP 이외의 연결(UDP, ICMP 또는 다른 프로토콜)에서는 연결 종료 이유가 TIMEOUT뿐입니다.</p>
소스 IP 주소 및 포트	IP 주소/포트
대상 IP 주소 및 포트	IP 주소/포트
TCP 플래그	S (SYN), SA (SYN-ACK), A (ACK), P (PUSH), U (URGENT), F (FIN), R (RESET)
패킷 수	<p>패킷의 수입니다.</p> <p>22/14 - 수신 패킷/송신 패킷</p>
바이트 수	<p>바이트의 수입니다.</p> <p>7684/1070 - 수신 바이트/송신 바이트</p>

규칙 메시지를 사용하도록 설정하려면 vSphere Web Client에 로그인합니다.

1 **Networking & Security > 방화벽** 페이지에서 **로그** 열을 사용하도록 설정합니다.



- 2 [로그] 테이블 셀 위로 마우스를 이동하고 연필 아이콘을 클릭하여 로깅을 사용하도록 규칙을 설정합니다.



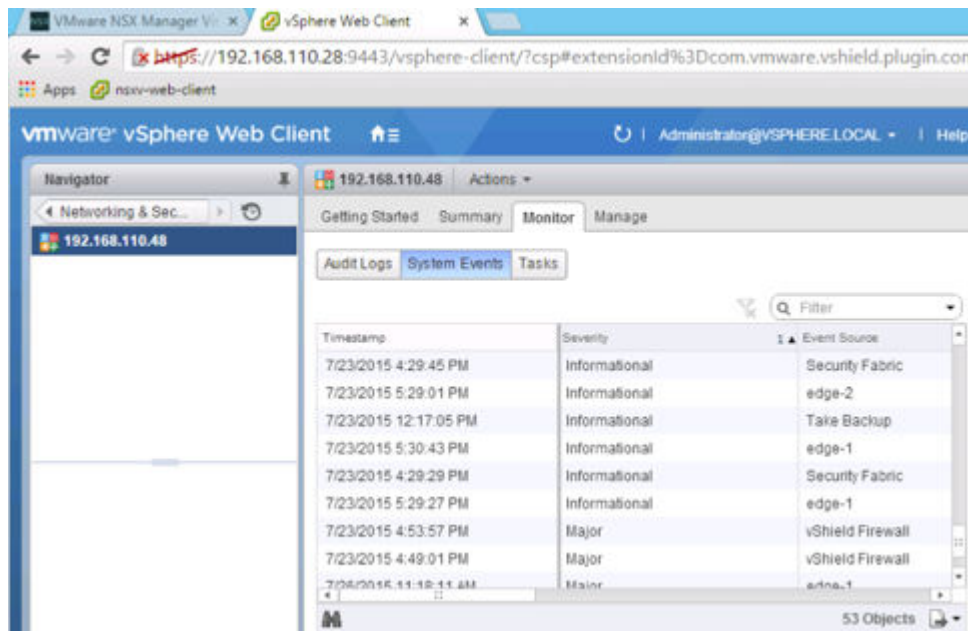
참고 사용자 지정된 텍스트를 방화벽 로그 메시지에 표시하려는 경우 **태그** 열을 사용하도록 설정하고 연필 아이콘을 클릭하여 필요한 텍스트를 추가할 수 있습니다.

감사 및 시스템 이벤트 로그

감사 로그에는 관리 로그 및 분산 방화벽 구성 변경 사항이 포함됩니다. 이 로그는 `/home/secureall/secureall/logs/vsm.log`에 저장됩니다.

시스템 이벤트 로그에는 적용된 분산 방화벽 구성, 생성 또는 삭제되거나 실패한 필터, 보안 그룹에 추가된 가상 시스템 등이 포함됩니다. 이러한 로그는 `/home/secureall/secureall/logs/vsm.log`에 저장됩니다.

UI에서 감사 및 시스템 이벤트 로그를 보려면 **Networking & Security > 설치 > 관리**로 이동한 다음 NSX Manager의 IP 주소를 두 번 클릭합니다. 그런 다음 **모니터** 탭을 클릭합니다.



자세한 내용은 "NSX 로깅 및 시스템 이벤트"를 참조하십시오.

ID 방화벽 기능을 사용하여 **NSX** 관리자는 **Active Directory** 사용자 기반 **DFW** 규칙을 생성할 수 있습니다.

고급 수준의 **IDFW** 구성 워크플로 개요는 인프라의 준비에서 시작됩니다. 여기에는 관리자가 보호된 각 클러스터에서 호스트 준비 구성 요소를 설치하고 **Active Directory** 동기화를 설정하여 **NSX**에서 **AD** 사용자 및 그룹을 사용할 수 있도록 하는 과정이 포함됩니다. 다음으로 **IDFW**는 **Active Directory** 사용자가 **DFW** 규칙을 적용하기 위해 로그인하는 데스크톱을 알고 있어야 합니다. **IDFW**가 로그인 감지에 사용하는 방법으로는 **Guest Introspection** 및/또는 **Active Directory** 이벤트 로그 스크레이퍼 두 가지가 있습니다. **Guest Introspection**은 **IDFW** 가상 시스템이 실행되고 있는 **ESXi** 클러스터에 배포됩니다. 사용자가 네트워크 이벤트를 생성하면 **VM**에 설치된 게스트 에이전트는 **Guest Introspection** 프레임워크를 통해 **NSX Manager**로 정보를 전달합니다. 두 번째 옵션은 **Active Directory** 이벤트 로그 스크레이퍼입니다. **NSX Manager**의 **Active Directory** 이벤트 로그 스크레이퍼가 **Active Directory** 도메인 컨트롤러의 인스턴스를 가리키도록 구성합니다. 그러면 **NSX Manager**는 **AD** 보안 이벤트 로그에서 이벤트를 추출합니다. 작업 환경에서 두 방법을 모두 사용하거나 한 가지만 사용할 수 있습니다. **AD** 이벤트 로그 스크레이퍼와 **Guest Introspection**을 둘 다 사용하는 경우 두 기능은 상호 배타적입니다. 두 기능 중 하나가 작동을 중지하면 다른 기능이 백업으로 작동하지 못합니다.

인프라가 준비되면 관리자는 **NSX** 보안 그룹을 생성하고 새로 사용 가능해진 **AD** 그룹(디렉토리 그룹)을 추가합니다. 그러면 관리자는 연결된 방화벽 규칙으로 보안 정책을 생성하고 해당 정책을 새로 생성한 보안 그룹에 적용할 수 있습니다. 이제 사용자가 데스크톱에 로그인하면 시스템은 사용되는 **IP** 주소에 따라 해당 이벤트를 감지하고, 해당 사용자와 연결된 방화벽 정책을 조회하고, 해당 규칙을 푸시다운합니다. 물리적 데스크톱과 가상 데스크톱 둘 다 마찬가지입니다. 물리적 데스크톱의 경우 사용자가 물리적 데스크톱에 로그인되었는지 감지하기 위해 **AD** 이벤트 로그 스크레이퍼도 필요합니다.

IDFW에서 지원되는 OS

AD 지원 서버

- Windows 2012
- Windows 2008
- Windows 2008 R2

지원되는 게스트 OS

- Windows 2012
- Windows 2008
- Windows 2008 R2
- Windows 10
- Windows 8 32/64
- Windows 7 32/64

본 장은 다음 항목을 포함합니다.

- ID 방화벽 워크플로

ID 방화벽 워크플로

IDFW(ID 방화벽)는 사용자 기반 DFW(분산 방화벽 규칙)를 허용합니다.

사용자 기반 분산 방화벽 규칙은 AD(Active Directory) 그룹 멤버 자격의 자격에 따라 결정됩니다. IDFW는 Active Directory 사용자가 로그인된 위치를 모니터링하고 DFW에서 방화벽 규칙을 적용하는 데 사용하는 IP 주소에 로그인을 매핑합니다. ID 방화벽에는 Guest Introspection 프레임워크 또는 Active Directory 이벤트 로그 스크랩이 필요합니다.

절차

- 1 NSX에서 Active Directory 동기화를 구성합니다. [Windows 도메인을 Active Directory와 동기화](#)를 참조하십시오. 이 작업은 Service Composer에서 Active Directory 그룹을 사용하는 데 필요합니다.
- 2 DFW에 대해 ESXi 클러스터를 준비합니다. "NSX 설치 가이드"에서 "NSX에 대한 호스트 클러스터 준비"를 참조하십시오.
- 3 ID 방화벽 로그온 감지 옵션을 구성합니다. 이러한 옵션 중 하나 또는 둘 다를 구성해야 합니다.

참고 다중 도메인 AD 아키텍처가 있으며 보안 제약 때문에 로그 스크래퍼에 액세스할 수 없는 경우 Guest Introspection을 사용하여 로그인 및 로그아웃 이벤트를 생성하십시오.

- Active Directory 이벤트 로그 액세스를 구성합니다. [NSX Manager에 Windows 도메인 등록](#)를 참조하십시오.
- 게스트 에이전트가 설치된 Windows 게스트 OS입니다. 여기에는 VMware Tools TM의 전체 설치가 포함됩니다. 보호된 클러스터에 Guest Introspection 서비스를 배포합니다. [호스트 클러스터에 Guest Introspection 설치](#)를 참조하십시오. Guest Introspection 문제 해결을 위해서는 [Guest Introspection 문제 해결 데이터 수집](#)을 참조하십시오.

Active Directory 도메인 사용

12

하나 이상의 Windows 도메인을 NSX Manager 및 관련 vCenter Server에 등록할 수 있습니다. NSX Manager는 등록된 각 도메인에서 그룹 및 사용자 정보와 서로 간의 관계를 가져옵니다. NSX Manager는 AD(Active Directory) 자격 증명도 가져옵니다.

NSX Manager가 AD(Active Directory) 자격 증명을 가져오면 사용자 ID 기반 Security Group, ID 기반 방화벽 규칙을 생성할 수 있으며 Activity Monitoring 보고서를 실행할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- NSX Manager에 Windows 도메인 등록
- Windows 도메인을 Active Directory와 동기화
- Windows 도메인 편집
- Windows 2008에서 보안 읽기 전용 로그 액세스 사용
- 디렉토리 권한 확인

NSX Manager에 Windows 도메인 등록

사전 요구 사항

도메인 계정에는 도메인 트리의 모든 개체에 대한 AD 읽기 권한이 있어야 합니다. 이벤트 로그 판독기 계정에는 보안 이벤트 로그에 대한 읽기 권한이 있어야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 **이름(Name)** 옆의 NSX Manager를 클릭한 후 **관리(Manage)** 탭을 클릭합니다.
- 4 **도메인(Domain)** 탭을 클릭하고 **도메인 추가(Add domain)**(+) 아이콘을 클릭합니다.

- 5 **도메인 추가(Add Domain)** 대화상자에서 정규화된 도메인 이름(예: `eng.vmware.com`)과 도메인의 NetBIOS 이름을 입력합니다.

도메인에 대한 netBIOS 이름을 검색하려면 도메인에 포함되거나 도메인 컨트롤러에 있는 Windows 워크스테이션의 명령 창에서 `nbtstat -n`을 입력합니다. NetBIOS 로컬 이름 테이블에서 <00> 접두사가 있고 유형이 그룹인 항목이 NetBIOS 이름입니다.

- 6 하위 도메인을 추가할 때 **자동 병합(Auto Merge)**을 선택합니다.
- 7 동기화 동안 더 이상 활성 계정이 없는 사용자를 필터링하려면 **비활성화된 사용자 무시(Ignore disabled users)**를 클릭합니다.
- 8 **다음(Next)**을 클릭합니다.
- 9 [LDAP 옵션] 페이지에서 도메인과 동기화할 도메인 컨트롤러를 지정하고 프로토콜을 선택합니다.
- 10 필요한 경우 포트 번호를 편집합니다.
- 11 도메인 계정의 사용자 자격 증명을 입력합니다. 이 사용자는 디렉토리 트리 구조에 액세스할 수 있는 권한이 있어야 합니다.
- 12 **다음(Next)**을 클릭합니다.
- 13 (선택 사항) [보안 이벤트 로그 액세스] 페이지에서 연결 방법으로 **CIFS** 또는 **WMI**를 선택하여 지정된 AD 서버의 보안 이벤트 로그에 액세스합니다. 필요한 경우 포트 번호를 변경합니다. 이 단계는 Active Directory 이벤트 로그 스크레이퍼에서 사용됩니다. **ID 방화벽 워크플로**를 참조하십시오.

참고 이벤트 로그 판독기는 AD 보안 이벤트 로그에서 ID가 Windows 2008/2012: 4624, Windows 2003: 540인 이벤트를 찾습니다. 이벤트 로그 서버의 크기 제한은 128MB입니다. 이 제한에 도달하면 보안 로그 판독기에서 이벤트 ID 1104가 표시될 수 있습니다. 자세한 내용은 <https://technet.microsoft.com/en-us/library/dd315518> 항목을 참조하십시오.

- 14 LDAP 서버 사용자 자격 증명을 사용하려면 **도메인 자격 증명 사용(Use Domain Credentials)**을 선택합니다. 로그 액세스에 사용할 대체 도메인 계정을 지정하려면 **도메인 자격 증명 사용(Use Domain Credentials)**을 선택 해제하고 사용자 이름과 암호를 지정합니다.
- 지정한 계정은 10단계에서 지정한 도메인 컨트롤러의 보안 이벤트 로그를 읽을 수 있는 권한이 있어야 합니다.
- 15 **다음(Next)**을 클릭합니다.
- 16 [완료 준비] 페이지에서 입력한 설정을 검토합니다.
- 17 **완료(Finish)**를 클릭합니다.

주의

- 도메인 충돌로 인해 엔티티에 대한 도메인 추가 작업이 실패했다는 오류 메시지가 표시되면 [자동 병합]을 선택합니다. 도메인이 생성되고 도메인 목록 아래에 설정이 표시됩니다.
-

결과

도메인이 생성되고 도메인 목록 아래에 해당 설정이 표시됩니다.

다음에 수행할 작업

이벤트 로그 서버의 로그인 이벤트가 사용하도록 설정되어 있는지 확인합니다.

도메인 목록 아래에 있는 패널에서 **LDAP 서버(LDAP Servers)** 탭을 선택하여 LDAP 서버를 추가, 편집, 삭제 또는 사용하거나 사용하지 않도록 설정할 수 있습니다. 도메인 목록 아래에 있는 패널에서 **이벤트 로그 서버(Event Log Servers)** 탭을 선택하여 이벤트 로그 서버에 대해서도 동일한 작업을 수행할 수 있습니다. 둘 이상의 Windows 서버(도메인 컨트롤러, Exchange 서버 또는 파일 서버)를 이벤트 로그 서버로 추가하면 사용자 ID 연결 성능이 향상됩니다.

참고 IDFW를 사용하는 경우 AD 서버만 지원됩니다.

Windows 도메인을 Active Directory와 동기화

기본적으로 등록된 모든 도메인은 3시간마다 자동으로 Active Directory와 동기화됩니다. 필요할 때 직접 동기화를 수행할 수도 있습니다.

vSphere Web Client UI를 통해 Active Directory 도메인에 대한 강제 동기화를 수행할 수 있습니다. 정기적인 동기화는 매주 1회 자동으로 수행되고, 델타 동기화는 3시간마다 수행됩니다. UI를 통해 하위 트리를 선택적으로 동기화할 수는 없습니다.

NSX 6.4 이상에서는 API 호출을 사용하여 Active Directory 하위 트리를 선택적으로 동기화할 수 있습니다. 루트 도메인은 상위-하위 관계를 가질 수 없으므로 유효한 디렉토리 고유 이름이 있어야 합니다.



- `/api/1.0/directory/updateDomain`에는 루트 도메인 아래에 폴더를 지정할 수 있는 옵션이 있습니다. 또한 강제 업데이트를 수행하는 옵션인 `private boolean forceUpdate` 도 있습니다.
- `/api/directory/verifyRootDN`. rootDN 목록에 상위-하위 관계가 없는지 확인합니다. 각 rootDN이 유효한 Active Directory 고유 이름인지 확인합니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > 시스템(System) > 사용자 및 도메인(Users and Domains)**으로 이동합니다.
- 2 **도메인(Domains)** 탭을 클릭하고 동기화할 도메인을 선택합니다.

중요 델타 또는 전체 동기화가 수행될 때까지 Active Directory에서 변경한 사항이 NSX Manager에 표시되지 않습니다.

3 다음 중 하나를 선택합니다.

클릭	수행되는 작업
	마지막 동기화 이벤트 이후에 변경된 로컬 AD 개체만 업데이트하는 델타 동기화를 수행합니다.
	모든 AD 개체의 로컬 상태를 업데이트하는 전체 동기화를 수행합니다.

Windows 도메인 편집

도메인의 이름, netBIOS 이름, 기본 LDAP 서버 및 계정 자격 증명을 편집할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 **이름(Name)** 열의 NSX Manager를 클릭한 후 **관리(Manage)** 탭을 클릭합니다.
- 4 도메인을 선택하고 **도메인 편집(Edit domain)** 아이콘을 클릭합니다.
- 5 필요한 내용을 변경하고 **완료(Finish)**를 클릭합니다.

Windows 2008에서 보안 읽기 전용 로그 액세스 사용

IDFW의 이벤트 로그 스크레이퍼에서는 읽기 전용 보안 로그 액세스를 사용합니다.

새 사용자 계정을 생성한 후에 Windows 2008 서버 기반 도메인 섹션에서 읽기 전용 보안 로그 액세스를 사용하도록 설정하여 사용자에게 읽기 전용 액세스 권한을 부여해야 합니다.

참고 도메인, 트리 또는 포리스트의 도메인 컨트롤러 하나에 대해 다음 단계를 수행해야 합니다.

절차

- 1 **시작 > 관리 도구 > Active Directory 사용자 및 컴퓨터(Start > Administrative Tools > Active Directory Users and Computers)**로 이동합니다.
- 2 탐색 트리에서 보안 로그 액세스를 사용하도록 설정할 도메인에 해당하는 노드를 확장합니다.
- 3 방금 확장한 노드에서 **기본 제공(Builtin)** 노드를 선택합니다.
- 4 그룹 목록에서 **이벤트 로그 판독기(Event Log Readers)**를 두 번 클릭합니다.
- 5 [이벤트 로그 판독기 속성] 대화상자에서 **멤버(Members)** 탭을 선택합니다.
- 6 **추가...(Add...)** 버튼을 클릭합니다.

[사용자, 연락처, 컴퓨터 또는 그룹 선택] 대화상자가 나타납니다.

- 7 “AD 판독기” 사용자에게 대한 그룹을 이전에 생성했으면 [사용자, 연락처, 컴퓨터 또는 그룹 선택] 대화상자에서 해당 그룹을 선택합니다. 사용자만 생성하고 그룹은 생성하지 않았으면 [사용자, 연락처, 컴퓨터 또는 그룹 선택] 대화상자에서 해당 사용자를 선택합니다.
- 8 **확인(OK)**을 클릭하여 [사용자, 연락처, 컴퓨터 또는 그룹 선택] 대화상자를 닫습니다.
- 9 **확인(OK)**을 클릭하여 [이벤트 로그 판독기 속성] 대화상자를 닫습니다.
- 10 [Active Directory 사용자 및 컴퓨터] 창을 닫습니다.

다음에 수행할 작업

보안 로그 액세스를 사용하도록 설정한 후에 **디렉토리 권한 확인**의 단계에 따라 디렉토리 권한을 확인합니다.

디렉토리 권한 확인

사용자 계정이 보안 로그를 읽는 데 필요한 권한이 있는지 확인합니다.

새 계정을 생성하고 보안 로그 액세스를 사용하도록 설정한 후에는 보안 로그를 읽을 수 있는 권한이 있는지 확인해야 합니다.

사전 요구 사항

보안 로그 액세스를 사용하도록 설정합니다. [Windows 2008에서 보안 읽기 전용 로그 액세스 사용](#)을 참조하십시오.

절차

- 1 도메인에 속하는 워크스테이션에서 관리자로 해당 도메인에 로그인합니다.
- 2 **시작 > 관리 도구 > 이벤트 뷰어(Start > Administrative Tools > Event Viewer)**로 이동합니다.
- 3 **작업(Action)** 메뉴에서 **다른 컴퓨터에 연결...(Connect to Another Computer...)**을 선택합니다. [컴퓨터 선택] 대화상자가 나타납니다. (이벤트 로그를 보려는 시스템에 이미 로그인한 경우에도 이 작업을 수행해야 합니다.)
- 4 **다른 컴퓨터(Another computer)** 라디오 버튼을 아직 선택하지 않았으면 선택합니다.
- 5 **다른 컴퓨터(Another computer)** 라디오 버튼 옆의 텍스트 필드에 도메인 컨트롤러의 이름을 입력합니다. 또는 **찾아보기...(Browse...)** 버튼을 클릭한 다음 [도메인 컨트롤러]를 선택합니다.
- 6 **다른 사용자로 연결(Connect as another user)** 확인란을 선택합니다.
- 7 **사용자 설정...(Set User...)** 버튼을 클릭합니다. [이벤트 뷰어] 대화상자가 나타납니다.
- 8 **사용자 이름(User name)** 필드에 생성한 사용자의 사용자 이름을 입력합니다.
- 9 **암호(Password)** 필드에 생성한 사용자의 암호를 입력합니다.
- 10 **확인(OK)**을 클릭합니다.
- 11 **확인(OK)**을 다시 클릭합니다.

12 탐색 트리에서 **Windows 로그(Windows Logs)** 노드를 확장합니다.

13 **Windows 로그(Windows Logs)**에서 [보안] 노드를 선택합니다. 로그 이벤트를 볼 수 있는 경우 계정에 필요한 권한이 있는 것입니다.

SpoofGuard 사용

13

vCenter Server와 동기화되면 NSX Manager가 각 가상 시스템의 VMware Tools에서 모든 vCenter 게스트 가상 시스템의 IP 주소를 수집합니다. 가상 시스템이 손상된 경우 IP 주소가 스푸핑되고 악의적인 전송이 방화벽 정책을 우회할 수 있습니다.

특정 네트워크에 대해 SpoofGuard 정책을 생성하면 VMware Tools에서 보고되는 IP 주소를 인증하고, 필요한 경우 이를 변경하여 스푸핑을 방지할 수 있습니다. SpoofGuard는 VMX 파일 및 vSphere SDK에서 수집된 가상 시스템의 MAC 주소를 기본적으로 신뢰합니다. 방화벽 규칙과 별도로 작동하므로, SpoofGuard를 사용하여 스푸핑된 것으로 확인된 트래픽을 차단할 수 있습니다.

SpoofGuard는 IPv4와 IPv6 주소를 모두 지원합니다. SpoofGuard 정책은 VMwareTools 및 DHCP 스누핑을 사용할 때 vNIC에 할당된 다중 IP 주소를 지원합니다. ARP 스누핑이 사용되도록 설정되면 다중 IP 주소가 지원되지 않습니다. SpoofGuard 정책은 다음 모드 중 하나에서 가상 시스템이 보고한 IP 주소를 모니터링하고 관리합니다.

최초 사용 시 IP 할당 자동 신뢰

이 모드에서는 vNIC-IP 주소 할당 테이블이 작성되는 동안 가상 시스템의 모든 트래픽이 통과하도록 허용됩니다. 언제든지 이 테이블을 검토하고 IP 주소를 변경할 수 있습니다. 이 모드에서는 vNIC에서 처음 확인된 모든 IPv4 및 IPv6 주소를 자동으로 승인합니다.

사용하기 전 모든 IP 할당 수동 검사 및 승인

이 모드에서는 사용자가 각 vNIC-IP 주소 할당을 승인할 때까지 모든 트래픽이 차단됩니다. 이 모드에서는 다중 IPv4 주소가 승인될 수 있습니다.

참고 기본적으로 SpoofGuard는 사용하도록 설정된 모드에 관계없이 DHCP 요청을 허용합니다. 하지만 수동 검사 모드에서는 DHCP로 할당된 IP 주소가 승인될 때까지 트래픽이 통과되지 않습니다.

SpoofGuard에는 다른 SpoofGuard 정책에서 처리하지 않는 포트 그룹 및 논리적 네트워크에 적용되는 시스템 생성 기본 정책이 포함되어 있습니다. 새로 추가된 네트워크의 경우 기존 정책에 추가하거나 네트워크에 대해 새 정책을 생성할 때까지 자동으로 기본 정책에 추가됩니다.

SpoofGuard는 NSX 분산 방화벽 정책이 가상 시스템의 IP 주소를 확인할 수 있는 방법 중 한 가지입니다. 자세한 내용은 [가상 시스템에 대한 IP 검색](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- SpoofGuard 정책 생성
- IP 주소 승인
- IP 주소 편집
- IP 주소 지우기

SpoofGuard 정책 생성

특정 네트워크에 대한 작업 모드를 지정하는 SpoofGuard 정책을 생성할 수 있습니다. 시스템 생성(기본) 정책은 기존 SpoofGuard 정책의 적용을 받지 않는 포트 그룹 및 논리적 스위치에 적용됩니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > SpoofGuard**로 이동하십시오.
- 2 **추가(Add)** 아이콘을 클릭합니다.
- 3 정책의 이름을 입력합니다.
- 4 **사용(Enabled)** 또는 **사용 안 함(Disabled)**을 선택하여 정책을 사용하도록 설정할지 여부를 지정합니다.
- 5 **작업 모드(Operation Mode)**의 경우 다음 중 하나를 선택합니다.

옵션	설명
최초 사용 시 IP 할당 자동 신뢰	NSX Manager에 처음 등록할 때 모든 IP 할당을 신뢰하려면 이 옵션을 선택합니다.
사용하기 전 모든 IP 할당 수동 검사 및 승인	모든 IP 주소를 반드시 수동으로 승인하도록 요구하려면 이 옵션을 선택합니다. 승인되지 않은 IP 주소에서 들어오거나 나가는 모든 트래픽이 차단됩니다.

- 6 **로컬 주소를 이 네임스페이스에서 유효한 주소로 허용합니다.(Allow local address as valid address in this namespace)**를 클릭하여 설치 환경에서 로컬 IP 주소를 허용합니다.

가상 시스템의 전원을 켜지만 가상 시스템을 DHCP 서버에 연결할 수 없는 경우 로컬 IP 주소가 가상 시스템에 할당됩니다. 이 로컬 IP 주소는 SpoofGuard 모드가 **로컬 주소를 이 네임스페이스에서 유효한 주소로 허용합니다.(Allow local address as valid address in this namespace)**로 설정된 경우에만 유효한 것으로 간주됩니다. 그렇지 않은 경우 로컬 IP 주소가 무시됩니다.

- 7 **다음(Next)**을 클릭합니다.
- 8 정책의 범위를 지정하려면 **추가(Add)**를 클릭하고 이 정책을 적용할 네트워크, 분산 포트 그룹 또는 논리적 스위치를 선택합니다.

포트 그룹 또는 논리적 스위치는 하나의 SpoofGuard 정책에만 속할 수 있습니다.

- 9 **확인(OK)** 및 **완료(Finish)**를 차례로 클릭합니다.

다음에 수행할 작업

편집(Edit) 아이콘을 클릭하여 정책을 편집하고 **삭제(Delete)** 아이콘을 클릭하여 정책을 삭제할 수 있습니다.

IP 주소 승인

모든 IP 주소 할당을 반드시 수동으로 승인하도록 **SpoofGuard**를 설정하는 경우에는 IP 주소 할당을 승인해야 해당 가상 시스템의 트래픽이 통과할 수 있습니다.

절차

- 1 **SpoofGuard** 탭에서 정책을 선택합니다.

정책 세부 정보가 정책 테이블 아래에 표시됩니다.

- 2 **보기(View)**에서 옵션 링크 중 하나를 클릭합니다.

옵션	설명
활성 가상 NIC	유효성이 검사된 모든 IP 주소의 목록
마지막 게시 후 활성 가상 NIC	정책이 마지막으로 업데이트된 후 유효성이 검사된 IP 주소의 목록
승인이 필요한 가상 NIC IP	해당 가상 시스템의 트래픽 전송 또는 수신에 위해 사전 승인이 필요한 IP 주소 변경
중복 IP가 있는 가상 NIC	선택한 데이터센터 내에 할당된 기존 IP 주소와 중복되는 IP 주소
비활성 가상 NIC	현재 IP 주소가 게시된 IP 주소와 일치하지 않는 IP 주소의 목록
게시되지 않은 가상 NIC IP	IP 주소 할당을 편집했지만 아직 게시하지 않은 가상 시스템의 목록

- 3 다음 중 하나를 수행합니다.

- 단일 IP 주소를 승인하려면 IP 주소 옆의 **승인(Approve)**을 클릭합니다.
- 여러 IP 주소를 승인하려면 적절한 vNIC를 선택하고 **검색된 IP 승인(Approve Detected IP(s))**을 클릭합니다.

IP 주소 편집

MAC 주소에 할당된 IP 주소를 편집하여 할당된 IP 주소를 수정할 수 있습니다.

참고 SpoofGuard는 가상 시스템의 고유 IP 주소를 수락합니다. 하지만 IP 주소는 단 한 번만 할당할 수 있습니다. 승인된 IP 주소는 NSX 전체에서 고유합니다. 중복 승인된 IP 주소는 허용되지 않습니다.

절차

- 1 **SpoofGuard** 탭에서 정책을 선택합니다.

정책 세부 정보가 정책 테이블 아래에 표시됩니다.

2 보기(View)에서 옵션 링크 중 하나를 클릭합니다.

옵션	설명
활성 가상 NIC	유효성이 검사된 모든 IP 주소의 목록
마지막 게시 후 활성 가상 NIC	정책이 마지막으로 업데이트된 후 유효성이 검사된 IP 주소의 목록
승인이 필요한 가상 NIC IP	해당 가상 시스템의 트래픽 전송 또는 수신을 위해 사전 승인이 필요한 IP 주소 변경
중복 IP가 있는 가상 NIC	선택한 데이터센터 내에 할당된 기존 IP 주소와 중복되는 IP 주소
비활성 가상 NIC	현재 IP 주소가 게시된 IP 주소와 일치하지 않는 IP 주소의 목록
게시되지 않은 가상 NIC IP	IP 주소 할당을 편집했지만 아직 게시하지 않은 가상 시스템의 목록

3 편집(Edit) 아이콘을 클릭하고 필요한 내용을 변경하여 vNIC를 적절히 수정합니다.

4 확인(OK)을 클릭합니다.

IP 주소 지우기

SpoofGuard 정책에서 승인된 IP 주소 할당을 지울 수 있습니다.

절차

1 SpoofGuard 탭에서 정책을 선택합니다.

정책 세부 정보가 정책 테이블 아래에 표시됩니다.

2 보기(View)에서 옵션 링크 중 하나를 클릭합니다.

옵션	설명
활성 가상 NIC	유효성이 검사된 모든 IP 주소의 목록
마지막 게시 후 활성 가상 NIC	정책이 마지막으로 업데이트된 후 유효성이 검사된 IP 주소의 목록
승인이 필요한 가상 NIC IP	해당 가상 시스템의 트래픽 전송 또는 수신을 위해 사전 승인이 필요한 IP 주소 변경
중복 IP가 있는 가상 NIC	선택한 데이터센터 내에 할당된 기존 IP 주소와 중복되는 IP 주소
비활성 가상 NIC	현재 IP 주소가 게시된 IP 주소와 일치하지 않는 IP 주소의 목록
게시되지 않은 가상 NIC IP	IP 주소 할당을 편집했지만 아직 게시하지 않은 가상 시스템의 목록

3 다음 중 하나를 수행합니다.

- 단일 IP 주소를 지우려면 해당 IP 주소 옆의 **지우기(Clear)**를 클릭합니다.
- 여러 IP 주소를 지우려면 해당 vNIC를 선택한 다음 **승인된 IP 지우기(Clear Approved IP(s))**를 클릭합니다.

VPN(Virtual Private Network)

14

NSX Edge는 여러 가지 유형의 VPN을 지원합니다. SSL VPN-Plus를 통해 원격 사용자는 회사 전용 애플리케이션에 액세스할 수 있습니다. IPSec VPN은 NSX Edge 인스턴스와 원격 사이트 사이에서 사이트 간 연결을 제공합니다. L2 VPN을 사용하면 가상 시스템에서 지리적 경계를 넘어 네트워크 연결 구성을 보존할 수 있으므로 데이터센터를 확장할 수 있습니다.

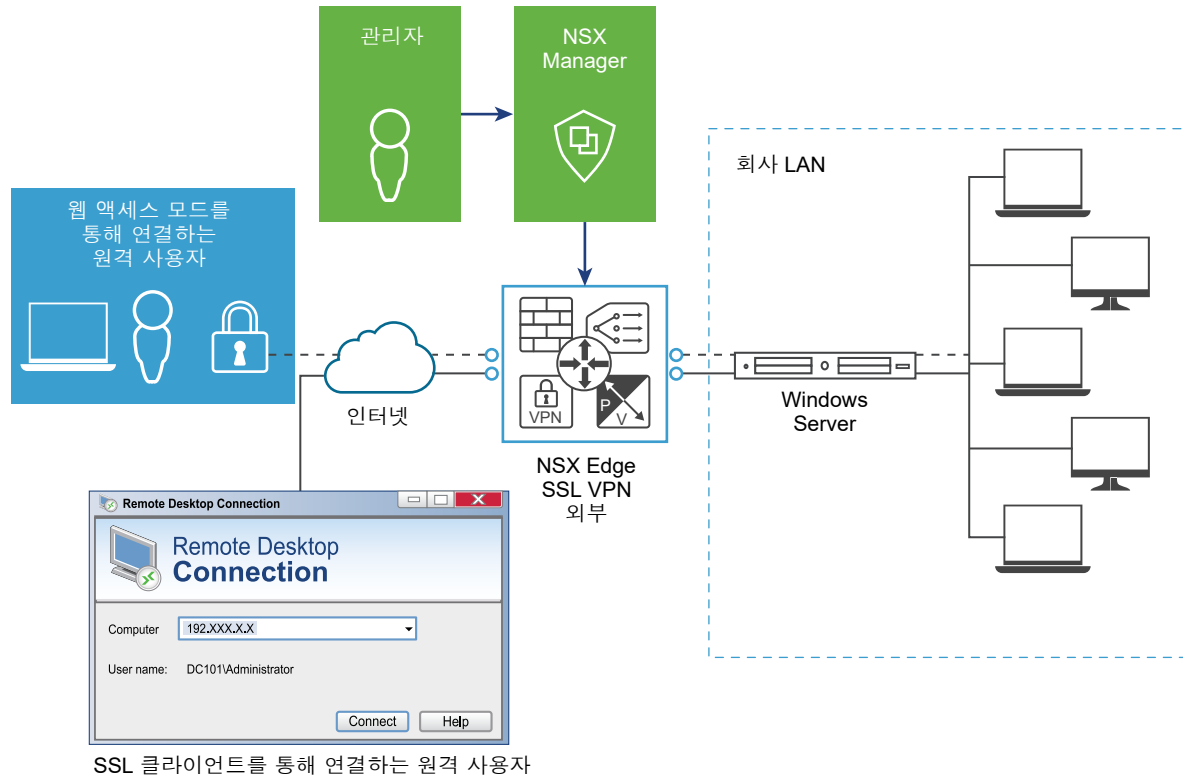
VPN을 사용하려면 작동 중인 NSX Edge 인스턴스가 있어야 합니다. NSX Edge 설정에 대한 자세한 내용은 [NSX Edge 구성](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [SSL VPN-Plus 개요](#)
- [IPSec VPN 개요](#)
- [L2 VPN 개요](#)

SSL VPN-Plus 개요

SSL VPN-Plus를 통해 원격 사용자는 NSX Edge Gateway로 보호되는 전용 네트워크에 안전하게 연결할 수 있습니다. 원격 사용자는 전용 네트워크의 서버 및 애플리케이션에 액세스할 수 있습니다.



지원되는 클라이언트 운영 체제는 다음과 같습니다.

운영 체제	지원되는 버전
Windows	8, 10(Windows 10 보안 부팅 옵션 사용)
Mac OS Sierra	10.12.6
Mac OS High Sierra	10.13.4
Linux Fedora	26, 28
Linux CentOS	6.0, 7.5
Linux Ubuntu	18.04

중요

- SSL VPN Plus Client는 ARM 기반 프로세서를 사용하는 컴퓨터에서 지원되지 않습니다.
- Windows의 SSL VPN Plus Client에서 Npcap 루프백 어댑터를 "사용하도록 설정"할 경우 "자동 다시 연결" 기능이 예상대로 작동하지 않습니다. 이 루프백 어댑터는 Windows 컴퓨터의 Npcap 드라이버 기능을 방해합니다. Windows 컴퓨터에 Npcap 드라이버(0.9983 이상)의 최신 버전이 설치되어 있는지 확인하십시오. 이 버전의 드라이버는 패킷 캡처를 위해 루프백 어댑터가 필요하지 않습니다.
- Linux TCL, TK 및 네트워크 보안 서비스(NSS) 라이브러리가 작동하려면 UI가 있어야 합니다.

네트워크 액세스 SSL VPN-Plus 구성

네트워크 액세스 모드에서는 원격 사용자가 SSL 클라이언트를 다운로드하고 설치하면 전용 네트워크에 액세스할 수 있습니다.

사전 요구 사항

SSL VPN 게이트웨이를 사용하려면 외부 네트워크에서 포트 443에 액세스할 수 있어야 하고, SSL VPN 클라이언트를 사용하려면 클라이언트 시스템에서 NSX Edge 게이트웨이 IP 및 포트 443에 연결할 수 있어야 합니다.

SSL VPN-Plus 서버 설정 추가

NSX Edge 인터페이스에서 SSL을 사용하도록 설정하려면 SSL VPN 서버 설정을 추가해야 합니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **서버 설정 (Server Settings)**을 선택합니다.
- 2 **변경 (Change.)**을 클릭합니다.
- 3 IPv4 또는 IPv6 주소를 선택합니다.
- 4 필요한 경우 포트 번호를 편집합니다. 이 포트 번호는 설치 패키지를 구성하는 데 필요합니다.
- 5 하나 이상의 암호화 방법 또는 암호를 선택합니다.

참고 다음 GCM 암호 중 하나라도 SSL VPN 서버에 구성되면 일부 브라우저에서 이전 버전과의 호환성 문제가 발생할 수 있습니다.

- AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA38

- 6 (선택 사항) 서버 인증서 테이블에서 기본 서버 인증서를 사용하거나 **기본 인증서 사용 (Use Default Certificate)** 확인란을 선택 취소한 후 추가하려는 서버 인증서를 클릭합니다.

제한 사항

- SSL VPN-Plus 서비스는 RSA 인증서만 지원합니다.
- SSL VPN-Plus 서비스는 루트 CA에서 서명된 서버 인증서를 지원합니다. 중간 CA가 서명한 서버 인증서는 지원되지 않습니다.

- 7 **확인 (OK.)**을 클릭합니다.

IP 풀 추가

추가한 IP 풀의 가상 IP 주소가 원격 사용자에게 할당됩니다.

절차

- 1 **SSL Vpn-Plus** 탭에서 왼쪽 패널에 있는 **IP 풀(IP Pools)**을 선택합니다.
- 2 **추가(Add)**(+) 아이콘을 클릭합니다.
- 3 IP 풀의 시작 및 종료 IP 주소를 입력합니다.
- 4 IP 풀의 넷마스크를 입력합니다.
- 5 **NSX Edge Gateway**의 라우팅 인터페이스를 추가할 IP 주소를 입력합니다.
- 6 (선택 사항) IP 풀에 대한 설명을 입력합니다.
- 7 IP 풀을 사용하도록 설정할지 여부를 선택합니다.
- 8 (선택 사항) **고급(Advanced)** 패널에서 **DNS** 이름을 입력합니다.
- 9 (선택 사항) 보조 **DNS** 이름을 입력합니다.
- 10 도메인 기반 호스트 이름 확인에 대해 연결별 **DNS** 접미사를 입력합니다.
- 11 **WINS** 서버 주소를 입력합니다.
- 12 **확인(OK)**을 클릭합니다.

전용 네트워크 추가

원격 사용자가 액세스할 수 있는 네트워크를 추가할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **전용 네트워크(Private Networks)**를 선택합니다.
- 2 **추가(Add)**(+) 아이콘을 클릭합니다.
- 3 전용 네트워크 IP 주소를 입력합니다.
- 4 전용 네트워크의 넷마스크를 입력합니다.
- 5 (선택 사항) 네트워크에 대한 설명을 입력합니다.
- 6 **SSL VPN-Plus**를 사용하는 **NSX Edge**를 통해 전용 네트워크 및 인터넷 트래픽을 전송할 것인지, **NSX Edge**를 우회하고 전용 서버로 직접 전송할 것인지를 지정합니다.
- 7 **터널을 통해 트래픽 전송(Send traffic over the tunnel)**을 선택한 경우에는 **TCP 최적화 사용(Enable TCP Optimization)**을 선택하여 인터넷 속도를 최적화합니다.

기존 전체 액세스 **SSL VPN** 터널은 인터넷을 통해 암호화용 두 번째 **TCP/IP** 스택에 **TCP/IP** 데이터를 전송합니다. 따라서 서로 다른 두 개의 **TCP** 스트림에서 애플리케이션 계층 데이터가 두 번 캡슐화됩니다. 인터넷 환경이 최적화된 조건에서도 생기는 패킷 손실이 발생할 경우 **TCP-over-TCP** 멜트다운(**Meltdown**)이라는 성능 저하 현상이 일어납니다. 기본적으로 두 개의 **TCP** 장비가 **IP** 데이터의 단일 패킷을 수정하는 것이므로 네트워크 처리량이 저하되고 연결 시간이 초과됩니다. **TCP** 최적화는 이러한 **TCP-over-TCP** 문제를 없애고 최적화된 성능을 보장합니다.

- 8 최적화를 사용하도록 설정한 경우 트래픽이 최적화되어야 할 포트 번호를 지정합니다.

해당 네트워크에서 나머지 포트의 트래픽은 최적화되지 않습니다.

참고 포트 번호가 지정되지 않으면 모든 포트에 대한 트래픽이 최적화됩니다.

TCP 트래픽이 최적화되면 클라이언트 대신 **SSL VPN** 서버가 TCP 연결을 엽니다. **SSL VPN** 서버가 TCP 연결을 열기 때문에 자동 생성된 첫 번째 규칙이 적용됩니다. 이 규칙은 **Edge**에서 열린 모든 연결이 통과되도록 허용합니다. 최적화되지 않은 트래픽은 일반 **Edge** 방화벽 규칙에 의해 평가됩니다. 기본 규칙은 모든 트래픽을 허용합니다.

- 9 전용 네트워크를 사용하도록 설정할지 여부를 지정합니다.

- 10 **확인(OK)**을 클릭합니다.

다음에 수행할 작업

전용 네트워크 트래픽을 허용하도록 해당 방화벽 규칙을 추가합니다.

인증 추가

로컬 사용자 인증 외에, **SSL** 게이트웨이에 바인딩되는 외부 인증 서버(**AD**, **LDAP**, **Radius** 또는 **RSA**)를 추가할 수 있습니다. 바인딩된 인증 서버에 계정이 있는 모든 사용자는 인증됩니다.

SSL VPN에서 인증할 수 있는 최대 시간은 **3분**입니다. 비인증 시간 초과는 **3분**이고 이는 구성할 수 있는 속성이 아니기 때문입니다. 따라서 **AD** 인증 시간 초과가 **3분** 넘게 설정되거나 체인 권한 부여에 여러 인증 서버가 있으며 사용자 인증에 걸리는 시간이 **3분**을 초과하는 시나리오에서는 사용자가 인증되지 않습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **인증 (Authentication)**을 선택합니다.
- 2 **추가 (Add)**(+) 아이콘을 클릭합니다.
- 3 인증 서버 유형을 선택합니다.
- 4 선택한 인증 서버 유형에 따라 다음 필드를 작성합니다.

◆ AD 인증 서버

표 14-1. AD 인증 서버 옵션

옵션	설명
SSL 사용 (Enable SSL)	SSL을 사용하도록 설정하면 웹 서버와 브라우저 간에 암호화된 링크가 설정됩니다. 참고 SSL을 사용하지 않도록 설정하고 나중에 SSL VPN-Plus 탭을 사용하여 또는 클라이언트 시스템에서 암호를 변경하려고 하면 문제가 발생할 수 있습니다.
IP 주소 (IP Address)	인증 서버의 IP 주소입니다.
포트 (Port)	기본 포트 이름을 표시합니다. 필요한 경우 편집할 수 있습니다.
시간 초과 (Timeout)	AD 서버가 응답해야 하는 제한 시간(초)입니다.

표 14-1. AD 인증 서버 옵션 (계속)

옵션	설명
상태 (Status)	사용 (Enabled) 또는 사용 안 함 (Disabled) 을 선택하여 서버를 사용하도록 설정할지 여부를 지정합니다.
검색 기준 (Search base)	검색할 외부 디렉토리 트리의 일부입니다. 검색 기준이 외부 디렉토리의 OU(조직 구성 단위), DC(도메인 컨트롤러) 또는 도메인 이름(AD)과 동일한 것일 수 있습니다. 예: <ul style="list-style-type: none"> ■ OU=Users,DC=aslan,DC=local ■ OU=VPN,DC=aslan,DC=local
Bind DN	정의된 검색 기준 내에서 AD 디렉토리를 검색하도록 허용된 외부 AD 서버의 사용자입니다. 대부분의 경우 Bind DN은 전체 디렉토리를 검색할 수 있습니다. Bind DN의 역할은 AD 사용자 인증을 위한 DN(고유 이름)에 대해 쿼리 필터 및 검색 기준을 사용하는 디렉토리를 쿼리하는 것입니다. DN이 반환되면 해당 DN과 암호를 사용하여 AD 사용자를 인증합니다. 예: CN=ldap.edge,OU=users,OU=Datacenter Users,DC=aslan,DC=local
바인딩 암호 (Bind Password)	AD 사용자를 인증하기 위한 암호입니다.
바인딩 암호 다시 입력 (Retype Bind Password)	암호를 다시 입력합니다.
로그인 특성 이름 (Login Attribute Name)	원격 사용자가 입력한 사용자 ID와 일치하는 이름입니다. Active Directory의 경우 로그인 특성 이름은 sAMAccountName입니다.
검색 필터 (Search Filter)	검색을 제한하는 필터 값입니다. 검색 필터는 특성 연산자 값 형식을 취합니다. 검색 기준을 AD의 특정 그룹으로 제한해야 하며 전체 OU에서 검색을 허용하지 않으려면 <ul style="list-style-type: none"> ■ 검색 기준에 그룹 이름을 포함하지 말고 OU 및 DC만 포함합니다. ■ 동일한 검색 필터 문자열 내에 objectClass 및 memberOf를 함께 포함하지 마십시오. 검색 필터의 올바른 형식 예: memberOf=CN=VPN_Users,OU=Users,DC=aslan,DC=local
보조 인증에 이 서버 사용 (Use this server for secondary authentication)	선택할 경우 이 AD 서버가 보조 인증에 사용됩니다.
인증 실패 시 세션 종료 (Terminate Session if authentication fails)	선택할 경우 인증에 실패하면 세션이 종료됩니다.

◆ LDAP 인증 서버

표 14-2. LDAP 인증 서버 옵션

옵션	설명
SSL 사용 (Enable SSL)	SSL을 사용하도록 설정하면 웹 서버와 브라우저 간에 암호화된 링크가 설정됩니다.
IP 주소 (IP Address)	외부 서버의 IP 주소입니다.
포트 (Port)	기본 포트 이름을 표시합니다. 필요한 경우 편집할 수 있습니다.
시간 초과 (Timeout)	AD 서버가 응답해야 하는 제한 시간(초)입니다.
상태 (Status)	사용 (Enabled) 또는 사용 안 함 (Disabled) 을 선택하여 서버를 사용하도록 설정할지 여부를 지정합니다.
검색 기준 (Search base)	검색할 외부 디렉토리 트리의 일부입니다. 검색 기준은 외부 디렉토리의 조직, 그룹 또는 도메인 이름(AD)과 동일하게 간주될 수 있습니다.
Bind DN	정의된 검색 기준 내에서 AD 디렉토리를 검색하도록 허용된 외부 서버의 사용자입니다. 대부분의 경우 Bind DN은 전체 디렉토리를 검색할 수 있습니다. Bind DN의 역할은 AD 사용자 인증을 위한 DN(고유 이름)에 대해 쿼리 필터 및 검색 기준을 사용하는 디렉토리를 쿼리하는 것입니다. DN이 반환되면 해당 DN과 암호를 사용하여 AD 사용자를 인증합니다.
바인딩 암호 (Bind Password)	AD 사용자를 인증하기 위한 암호입니다.
바인딩 암호 다시 입력 (Retype Bind Password)	암호를 다시 입력합니다.
로그인 특성 이름 (Login Attribute Name)	원격 사용자가 입력한 사용자 ID와 일치하는 이름입니다. Active Directory의 경우 로그인 특성 이름은 sAMAccountName 입니다.
검색 필터 (Search Filter)	검색을 제한하는 필터 값입니다. 검색 필터는 특성 연산자 값 형식을 취합니다.
보조 인증에 이 서버 사용 (Use this server for secondary authentication)	선택할 경우 이 서버가 보조 인증에 사용됩니다.
인증 실패 시 세션 종료 (Terminate Session if authentication fails)	선택할 경우 인증에 실패하면 세션이 종료됩니다.

◆ RADIUS 인증 서버

RADIUS 인증은 FIPS 모드에서 사용되지 않도록 설정됩니다.

표 14-3. RADIUS 인증 서버 옵션

옵션	설명
IP 주소 (IP Address)	외부 서버의 IP 주소입니다.
포트 (Port)	기본 포트 이름을 표시합니다. 필요한 경우 편집할 수 있습니다.
시간 초과 (Timeout)	AD 서버가 응답해야 하는 제한 시간(초)입니다.

표 14-3. RADIUS 인증 서버 옵션 (계속)

옵션	설명
상태 (Status)	사용 (Enabled) 또는 사용 안 함 (Disabled) 을 선택하여 서버를 사용하도록 설정할지 여부를 지정합니다.
암호 (Secret)	RSA 보안 콘솔에서 인증 에이전트를 추가할 때 지정한 공유 암호입니다.
암호 다시 입력 (Retype secret)	공유 암호를 다시 입력합니다.
NAS IP 주소 (NAS IP Address)	RADIUS 패킷의 IP 헤더에서 소스 IP 주소를 변경하지 않고 RADIUS 특성 4, NAS IP 주소로 구성하고 사용하는 IP 주소입니다.
재시도 횟수 (Retry Count)	인증에 실패하기 전에 RADIUS 서버가 응답하지 않을 경우 RADIUS 서버에 연결하려고 시도하는 횟수입니다.
보조 인증에 이 서버 사용 (Use this server for secondary authentication)	선택할 경우 이 서버가 보조 인증에 사용됩니다.
인증 실패 시 세션 종료 (Terminate Session if authentication fails)	선택할 경우 인증에 실패하면 세션이 종료됩니다.

◆ RSA-ACE 인증 서버

RSA 인증은 FIPS 모드에서 사용되지 않도록 설정됩니다.

표 14-4. RSA-ACE 인증 서버 옵션

옵션	설명
시간 초과 (Timeout)	AD 서버가 응답해야 하는 제한 시간(초)입니다.
구성 파일 (Configuration File)	찾아보기 (Browse) 를 클릭하고 RSA Authentication Manager에서 다운로드한 <code>sdconf.rec</code> 파일을 선택합니다.
상태 (Status)	사용 (Enabled) 또는 사용 안 함 (Disabled) 을 선택하여 서버를 사용하도록 설정할지 여부를 지정합니다.
소스 IP 주소 (Source IP Address)	RSA 서버에 액세스할 때 사용되는 NSX Edge 인터페이스의 IP 주소입니다.

표 14-4. RSA-ACE 인증 서버 옵션 (계속)

옵션	설명
보조 인증에 이 서버 사용 (Use this server for secondary authentication)	선택할 경우 이 서버가 보조 인증에 사용됩니다.
인증 실패 시 세션 종료 (Terminate Session if authentication fails)	선택할 경우 인증에 실패하면 세션이 종료됩니다.

◆ 로컬 인증 서버

표 14-5. 로컬 인증 서버 옵션

옵션	설명
암호 정책 사용 (Enable password policy)	선택할 경우 암호 정책을 정의합니다. 필요한 값을 지정합니다.
암호 정책 사용 (Enable password policy)	<p>선택할 경우 계정 잠금 정책을 정의합니다. 필요한 값을 지정합니다.</p> <ol style="list-style-type: none"> 원격 사용자가 잘못된 암호를 입력한 후 자신의 계정에 액세스하기 위해 시도할 수 있는 횟수를 재시도 횟수에 입력합니다. 특정 시간 내에 로그인 시도에 실패하는 경우 원격 사용자의 계정을 잠금도록 재시도 기간에 기간을 입력합니다. 예를 들어 재시도 횟수를 5로 지정하고, 재시도 기간을 1분으로 지정하면 1분 내에 5회 시도하여 로그인하지 못하면 원격 사용자의 계정이 잠깁니다. 사용자 계정을 잠금 상태로 유지하는 기간을 잠금 기간에 입력합니다. 이 시간이 경과하면 계정이 자동으로 잠금 해제됩니다.
상태 (Status)	사용 (Enabled) 또는 사용 안 함 (Disabled)을 선택하여 서버를 사용하도록 설정할지 여부를 지정합니다.
보조 인증에 이 서버 사용 (Use this server for secondary authentication)	선택할 경우 이 서버가 보조 인증에 사용됩니다.
인증 실패 시 세션 종료 (Terminate Session if authentication fails)	선택할 경우 인증에 실패하면 세션이 종료됩니다.

5 (선택 사항) 클라이언트 인증서 인증을 추가합니다.

- a 인증서 인증 (Certificate Authentication) 옆의 변경 (Change)을 클릭합니다.
- b 클라이언트 인증서 인증 사용 (Enable client certificate authentication) 확인란을 선택합니다.
- c 루트 CA에서 발급한 클라이언트 인증서를 선택하고 확인 (OK)을 클릭합니다.

제한 사항

- SSL VPN-Plus 웹 포털 및 SSL VPN-Plus 전체 액세스 권한 클라이언트(PHAT 클라이언트)에서는 루트 CA에서 서명한 클라이언트 또는 사용자 인증서만 지원됩니다. 중간 CA가 서명한 클라이언트 인증서는 지원되지 않습니다.
 - 클라이언트 인증서 인증은 Windows 컴퓨터에 설치된 SSL VPN-Plus Client에서만 지원됩니다. 이 인증이 Linux 및 Mac 컴퓨터에 설치된 SSL VPN-Plus Client에서는 지원되지 않습니다.
-

설치 패키지 추가

원격 사용자를 위해 SSL VPN-Plus Client의 설치 패키지를 생성합니다.

절차

1 SSL VPN-Plus 탭에서 왼쪽 패널에 있는 설치 패키지(Installation Package)를 선택합니다.

2 추가(Add)(+) 아이콘을 클릭합니다.

3 설치 패키지의 프로파일 이름을 입력합니다.

4 게이트웨이(Gateway)에서 NSX Edge 공용 인터페이스의 IP 주소 또는 FQDN을 입력합니다.

이 IP 주소 또는 FQDN은 SSL 클라이언트에 바인딩되어 있습니다. 클라이언트가 설치되면 이 IP 주소 또는 FQDN이 SSL 클라이언트에 표시됩니다.

5 SSL VPN-Plus의 서버 설정에서 지정한 포트 번호를 입력합니다. [SSL VPN-Plus 서버 설정 추가](#)를 참조하십시오.

6 (선택 사항) 추가 NSX Edge 업링크 인터페이스를 SSL 클라이언트에 바인딩하려면

- a 추가(Add)(+) 아이콘을 클릭합니다.
- b IP 주소 및 포트 번호를 입력합니다.
- c 확인(OK)을 클릭합니다.

7 기본적으로 설치 패키지는 Windows 운영 체제용으로 생성됩니다. Linux 또는 Mac 운영 체제용 설치 패키지도 생성하려면 Linux 또는 Mac을 선택합니다.

8 (선택 사항) 설치 패키지에 대한 설명을 입력합니다.

9 사용(Enable)을 선택하여 [설치 패키지] 페이지에 설치 패키지를 표시합니다.

10 필요한 경우 다음 옵션을 선택합니다.

옵션	설명
로그온 시 클라이언트 시작	원격 사용자가 해당 시스템에 로그인하면 SSL VPN 클라이언트가 시작됩니다.
암호 기억 허용	이 옵션을 사용하도록 설정합니다.
자동 모드 설치 사용	원격 사용자에게 설치 명령을 숨깁니다.
SSL 클라이언트 네트워크 어댑터 숨기기	원격 사용자의 컴퓨터에 SSL VPN 설치 패키지와 함께 설치되는 VMware SSL VPN-Plus 어댑터를 숨깁니다.
클라이언트 시스템 트레이 아이콘 숨기기	VPN 연결이 활성 상태인지 여부를 표시하는 SSL VPN 트레이 아이콘을 숨깁니다.
바탕 화면 아이콘 생성	SSL 클라이언트 를 호출하는 아이콘을 사용자의 바탕 화면에 생성합니다.
자동 모드 작업 사용	설치가 완료되었음을 나타내는 팝업을 숨깁니다.
서버 보안 인증서 검증	SSL VPN 클라이언트가 보안 연결을 설정하기 전에 SSL VPN 서버 인증서의 유효성을 검사합니다.
인증서 유효성 검사 실패 시 사용자 차단	인증서 유효성 검사에 실패하면 SSL VPN 사용자를 차단합니다.

11 확인(OK.)을 클릭합니다.

사용자 추가

원격 사용자를 로컬 데이터베이스에 추가할 수 있습니다.

절차

- 1 **SSL Vpn-Plus** 탭에서 왼쪽 패널에 있는 **사용자(Users)**를 선택합니다.
- 2 **추가(Add)(+)** 아이콘을 클릭합니다.
- 3 사용자 ID를 입력합니다.
- 4 암호를 입력합니다.
- 5 암호를 다시 입력합니다.
- 6 (선택 사항) 사용자의 이름과 성을 입력합니다.
- 7 (선택 사항) 사용자에 대한 설명을 입력합니다.
- 8 암호 세부 정보에서 **암호가 만료되지 않음(Password never expires)**을 선택하면 항상 해당 사용자에게 대해 동일한 암호를 유지할 수 있습니다.
- 9 사용자가 암호를 변경할 수 있도록 하려면 **암호 변경 허용(Allow change password)**을 선택합니다.
- 10 사용자가 다음에 로그인할 때 암호를 변경하도록 하려면 **다음 로그인 시 암호 변경(Change password on next login)**을 선택합니다.
- 11 사용자 상태를 설정합니다.
- 12 **확인(OK)**을 클릭합니다.

SSL VPN-Plus 서비스 사용

SSL VPN-Plus 서비스를 구성한 후에 이 서비스를 사용하도록 설정하면 원격 사용자가 전용 네트워크에 액세스할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **대시보드(Dashboard)**를 선택합니다.

- 2 그런 다음  **Enable** 아이콘을 클릭합니다.

대시보드에 서비스 상태, 활성 **SSL VPN** 세션 수, 세션 통계 및 데이터 흐름 세부 정보가 표시됩니다.

NSX Edge Gateway 뒤에 있는 전용 네트워크에 대한 동시 연결 정보를 보려면 활성 세션 수 옆에 있는 **세부 정보(Details)**를 클릭합니다.

다음에 수행할 작업

- 1 **NSX Edge Appliance**의 IP 주소를 **VPN Edge IP** 주소로 변환하기 위한 **SNAT** 규칙을 추가합니다.
- 2 웹 브라우저에서 **https://NSXEdgeIPAddress**를 입력하여 **NSX Edge** 인터페이스의 IP 주소로 이동합니다.
- 3 **사용자 추가** 섹션에서 생성한 사용자 이름 및 암호를 사용하여 로그인하고 설치 패키지를 다운로드합니다.
- 4 **SSL VPN-Plus 서버 설정 추가**에서 사용된 포트 번호에 대해 라우터에서 포트 전달을 사용하도록 설정합니다.
- 5 **VPN** 클라이언트를 시작하고 **VPN** 서버를 선택한 후 로그인합니다. 이제 네트워크의 서비스로 이동할 수 있습니다. **SSL VPN-Plus Gateway** 로고는 **NSX Edge Appliance**에 구성된 **Syslog** 서버로 전송됩니다. **SSL VPN-Plus Client** 로고는 원격 사용자의 컴퓨터에 있는 **%PROGRAMFILES%/VMWARE/SSLVPN Client/** 디렉토리에 저장됩니다.

스크립트 추가

로그인 또는 로그오프 스크립트를 여러 개 추가할 수 있습니다. 예를 들어 **Internet Explorer**를 **gmail.com**으로 시작하는 로그인 스크립트를 바인딩할 수 있습니다. 원격 사용자가 **SSL** 클라이언트에 로그인하면 **Internet Explorer**에서 **gmail.com**이 열립니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **로그인/로그오프 스크립트(Login/Logoff Scripts)**를 선택합니다.
- 2 **추가(Add)(+)** 아이콘을 클릭합니다.
- 3 **스크립트(Script)**에서 **찾아보기(Browse)**를 클릭하고 **NSX Edge Gateway**에 바인딩할 스크립트를 선택합니다.

4 스크립트의 유형(Type)을 선택합니다.

옵션	설명
로그인	원격 사용자가 SSL VPN에 로그인할 때 스크립트 작업을 수행합니다.
로그오프	원격 사용자가 SSL VPN에서 로그아웃할 때 스크립트 작업을 수행합니다.
둘 다	원격 사용자가 SSL VPN에 로그인/로그아웃할 때 모두 스크립트 작업을 수행합니다.

5 스크립트에 대한 설명을 입력합니다.

6 사용(Enabled)을 선택하여 스크립트를 사용하도록 설정합니다.

7 확인(OK)을 클릭합니다.

SSL VPN-Plus Client 설치

SSL VPN 전체 액세스 권한(PHAT) 클라이언트를 사용하여 구성된 전용 네트워크에 원격 사용자로 연결합니다. 이 클라이언트는 Windows, Mac 및 Linux 데스크톱에서 지원됩니다.

원격 Windows 사이트에 SSL VPN-Plus Client 설치

원격 Windows 사이트에서 SSL VPN-Plus Client를 설치하려면 이 항목의 단계를 사용합니다.

절차

- 1 원격 클라이언트 사이트에서 브라우저 창을 열고 **https://ExternalEdgeInterfaceIP/sslvpn-plus/**를 입력합니다. 여기서 **ExternalEdgeInterfaceIP**는 SSL VPN-Plus 서비스를 사용하도록 설정한 Edge 외부 인터페이스의 IP 주소입니다.
- 2 원격 사용자의 자격 증명을 사용하여 포털에 로그인합니다.
- 3 **전체 액세스 권한(Full Access)** 탭을 클릭합니다.
- 4 목록에서 설치 관리자 패키지의 이름을 클릭합니다.
- 5 **여기를 클릭(click here)** 링크를 클릭하여 설치 관리자 패키지를 다운로드합니다.
SSL 클라이언트가 다운로드됩니다.
- 6 다운로드한 파일의 압축을 풀고 **Installer.exe** 파일을 실행하여 클라이언트를 설치합니다.

다음에 수행할 작업

사용자 섹션에 지정된 자격 증명을 사용하여 SSL 클라이언트에 로그인합니다. SSL VPN-Plus Client는 SSL VPN 서버 인증서가 유효한지 검사합니다.

설치 패키지를 생성할 때 기본적으로 **서버 보안 인증서 검증(Server security certificate validation)** 옵션을 선택한 경우 Windows 클라이언트가 인증됩니다.

IE(Internet Explorer) 브라우저에서 신뢰할 수 있는 CA를 신뢰할 수 있는 인증서 저장소에 추가합니다. 서버 인증서 검증이 실패한 경우 시스템 관리자에게 문의하라는 메시지가 표시됩니다. 서버 인증서 검증이 성공한 경우 로그인 프롬프트가 표시됩니다.

신뢰할 수 있는 CA를 신뢰 저장소에 추가하는 것은 SSL VPN 워크플로우와 상관이 없습니다.

원격 Linux 사이트에 SSL VPN-Plus Client 설치

원격 Linux 사이트에서 SSL VPN-Plus Client를 설치하려면 이 항목의 단계를 사용합니다.

사전 요구 사항

원격 컴퓨터에 Linux TCL 및 TK 패키지를 설치합니다.

SSL VPN-Plus Client를 설치하려면 루트 권한이 있어야 합니다.

절차

- 1 원격 클라이언트 사이트에서 브라우저 창을 열고 **`https://ExternalEdgeInterfaceIP/sslvpn-plus/`**를 입력합니다. 여기서 **`ExternalEdgeInterfaceIP`**는 SSL VPN-Plus 서비스를 사용하도록 설정한 Edge 외부 인터페이스의 IP 주소입니다.
- 2 원격 사용자의 자격 증명을 사용하여 포털에 로그인합니다.
- 3 **전체 액세스 권한(Full Access)** 탭을 클릭합니다.
- 4 설치 관리자 패키지의 이름을 클릭하고 원격 컴퓨터에 압축된 **`linux_phat_client.tgz`** 파일을 저장합니다.
- 5 압축된 파일의 압축을 풉니다. **`linux_phat_client`** 디렉토리가 생성됩니다.
- 6 Linux CLI를 열고 **`linux_phat_client`** 디렉토리로 변경합니다.
- 7 **`./install_linux_phat_client.sh`** 명령을 실행합니다.

다음에 수행할 작업

사용자 섹션에 지정된 자격 증명을 사용하여 SSL VPN GUI에 로그인합니다.

주의

- Linux 운영 체제에서 SSL VPN 클라이언트로 로그인하기 위한 2단계 RSA 인증은 지원되지 않습니다.
- SSL VPN Linux Client CLI는 서버 인증서가 유효한지 검사하지 않습니다. 서버 인증서 유효성 검사가 필요한 경우 게이트웨이에 연결하는 데 SSL VPN GUI를 사용합니다.

SSL VPN Linux 클라이언트는 기본적으로 브라우저의 인증서 저장소를 기준으로 서버 인증서의 유효성을 검사합니다. 서버 인증서 검증이 실패한 경우 시스템 관리자에게 문의하라는 메시지가 표시됩니다. 서버 인증서 검증이 성공한 경우 로그인 프롬프트가 표시됩니다.

신뢰할 수 있는 CA를 신뢰 저장소(예: Firefox의 인증서 저장소)에 추가하는 것은 SSL VPN 워크플로우와 상관이 없습니다.

원격 Mac 사이트에 SSL VPN-Plus Client 설치

원격 Mac 컴퓨터에서 SSL VPN-Plus Client를 설치하려면 이 항목의 단계를 사용합니다.

사전 요구 사항

SSL VPN-Plus Client를 설치하려면 루트 권한이 있어야 합니다.

절차

- 1 원격 클라이언트 사이트에서 브라우저 창을 열고 **`https://ExternalEdgeInterfaceIP/sslvpn-plus/`**를 입력합니다. 여기서 **`ExternalEdgeInterfaceIP`**는 SSL VPN-Plus 서비스를 사용하도록 설정한 Edge 외부 인터페이스의 IP 주소입니다.
- 2 원격 사용자의 자격 증명을 사용하여 포털에 로그인합니다.
- 3 **전체 액세스 권한(Full Access)** 탭을 클릭합니다.
- 4 설치 관리자 패키지의 이름을 클릭하고 원격 컴퓨터에 **`mac_phat_client.tgz`** 압축된 파일을 저장합니다.
- 5 압축된 파일의 압축을 풉니다. **`mac_phat_client`** 디렉토리가 생성됩니다.
- 6 SSL VPN-Plus Client를 설치하려면 **`naclient.pkg`** 파일을 두 번 클릭합니다.
마법사의 단계에 따라 설치를 완료합니다.
SSL VPN 클라이언트 설치가 실패하는 경우 **`/tmp/naclient_install.log`**에서 설치 로그 파일을 확인합니다.
Mac OS High Sierra에서 설치 문제를 해결하려면 "NSX 문제 해결 가이드"를 참조하십시오.

다음에 수행할 작업

사용자 섹션에 지정된 자격 증명을 사용하여 SSL 클라이언트에 로그인합니다.

주의 Mac 운영 체제에서 SSL VPN 클라이언트로 로그인하기 위한 2단계 RSA 인증은 지원되지 않습니다.

SSL VPN Mac 클라이언트는 Mac OS에서 기본적으로 인증서를 저장하는 데이터베이스인 키체인을 기준으로 서버 인증서가 유효한지 검사합니다. 서버 인증서 검증이 실패한 경우 시스템 관리자에게 문의하라는 메시지가 표시됩니다. 서버 인증서 검증이 성공한 경우 로그인 프롬프트가 표시됩니다.

SSL VPN-Plus Client에서 프록시 서버 설정 구성

프록시 서버 구성은 Windows 컴퓨터의 SSL VPN-Plus Client에서 지원되지만 Mac 및 Linux 컴퓨터에서는 지원되지 않습니다.

경고

- Mac OS의 SSL VPN-Plus Client는 프록시 서버 설정을 구성하기 위해 시설을 제공하지만 원격 사용자는 프록시 서버 설정을 구성해서는 안 됩니다.
- 원격 Linux OS 사용자는 Linux CLI를 통해 SSL VPN-Plus Client에서 프록시 서버 설정을 구성하는 것을 방지해야 합니다.

다음 절차에서는 Windows 컴퓨터의 SSL VPN-Plus Client에서 프록시 서버 설정을 구성하는 단계를 설명합니다.

사전 요구 사항

SSL VPN-Plus Client는 원격 Windows 컴퓨터에 설치됩니다.

절차

- 1 Windows 컴퓨터에서 SSL VPN-Plus Client의 바탕 화면 아이콘을 두 번 클릭합니다.
SSL VPN-Plus Client - 로그인 창이 열립니다.
- 2 **설정 (Settings)**을 클릭하고 **프록시 설정 (Proxy Settings)** 탭을 클릭합니다.
- 3 프록시 서버 설정을 지정합니다.
 - a **프록시 사용 (Use Proxy)** 확인란을 선택합니다.
 - b **프록시 유형 (Type Of Proxy)**에서 프록시 서버 유형 중 하나를 구성합니다.

옵션	설명
IE 설정 사용	IE 브라우저에 지정된 프록시 서버 구성을 사용합니다.
HTTP	HTTP 프록시 서버에 대한 다음 설정을 지정합니다. <ul style="list-style-type: none"> ■ 프록시 서버 이름 또는 IP 주소. ■ 프록시 서버 포트. 기본 포트는 80이며 편집할 수 있습니다.
SOCKS 버전 4	SOCKS 4.0 프록시 서버에 대한 다음 설정을 지정합니다. <ul style="list-style-type: none"> ■ 프록시 서버 이름 또는 IP 주소. ■ 프록시 서버 포트. 기본 포트는 1080으로, 편집할 수 있습니다.
SOCKS 버전 5	SOCKS 5.0 프록시 서버에 대한 다음 설정을 지정합니다. <ul style="list-style-type: none"> ■ 프록시 서버 이름 또는 IP 주소. ■ 프록시 서버 포트. 기본 포트는 1080으로, 편집할 수 있습니다. ■ (선택 사항) SOCKS 5.0 서버에 액세스하기 위한 사용자 이름 및 암호.

- 4 프록시 서버 설정을 저장하려면 **확인 (OK)**을 클릭합니다.

SSL VPN-Plus 로그

SSL VPN-Plus Gateway 로그는 NSX Edge 장치에 구성된 Syslog 서버로 전송됩니다.

다음 표에는 원격 사용자 컴퓨터에서 SSL VPN-Plus Client 로그가 저장된 위치가 나와 있습니다.

운영 체제	로그 파일의 위치
Windows 8	C:\Users\username\AppData\Local\VMware\vpn\svp_client.log
Windows 10	C:\Users\username\AppData\Local\VMware\vpn\svp_client.log
Linux	시스템 로그 파일
Mac	/tmp/naclient_install.log의 설치 로그 파일 시스템 로그 파일

SSL VPN-Plus Client 로그 및 로그 수준 변경

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **서버 설정(Server Settings)**을 클릭합니다.
- 2 [로그 정책] 섹션으로 이동한 후 섹션을 확장하여 현재 설정을 봅니다.
- 3 **변경(Change)**을 클릭합니다.
- 4 **로깅 사용(Enable logging)** 확인란을 선택하여 로깅을 사용하도록 설정합니다.

또는

로깅 사용(Enable logging) 확인란을 선택 취소하여 로깅을 사용하지 않도록 설정합니다.

- 5 필요한 로그 수준을 선택합니다.

참고 SSL VPN-Plus 클라이언트 로그는 기본적으로 사용되지 않도록 설정되며 로그 수준은 [알림]으로 설정됩니다.

- 6 **확인(OK)**을 클릭합니다.

클라이언트 구성 편집

원격 사용자가 SSL VPN에 로그인할 때 SSL VPN 클라이언트 터널이 응답하는 방식을 변경할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **클라이언트 구성(Client Configuration)**을 선택합니다.
- 2 **터널링 모드(Tunneling Mode)**를 선택합니다.

분할 터널 모드에서는 VPN만 NSX Edge Gateway를 통과합니다. 전체 터널에서는 NSX Edge Gateway가 원격 사용자의 기본 게이트웨이가 되며 VPN, 로컬, 인터넷 등의 모든 트래픽은 이 게이트웨이를 통과합니다.

3 전체 터널 모드를 선택한 경우:

- a **로컬 서브넷 제외(Exclude local subnets)**를 선택하여 VPN 터널을 통과하지 못하도록 로컬 트래픽을 제외합니다.
 - b 원격 사용자 시스템의 기본 게이트웨이 IP 주소를 입력합니다.
- 4 연결이 끊긴 후 원격 사용자가 **SSL VPN 클라이언트**에 자동으로 다시 연결되도록 하려면 **자동 재연결 사용(Enable auto reconnect)**을 선택합니다.
 - 5 클라이언트에 대한 업데이트를 사용할 수 있을 때 원격 사용자에게 알려려면 **클라이언트 업그레이드 알림(Client upgrade notification)**을 선택합니다. 그러면 원격 사용자가 업그레이드 설치를 선택할 수 있습니다.
 - 6 **확인(OK)**을 클릭합니다.

일반 설정 편집

기본 VPN 설정을 편집할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **일반 설정(General Settings)**을 선택합니다.
- 2 필요한 항목을 선택합니다.

선택	수행되는 작업
동일한 사용자 이름을 사용하는 다중 로그인 금지	원격 사용자가 사용자 이름을 사용하여 한 번만 로그인할 수 있도록 허용합니다.
압축 사용	TCP 기반의 지능형 데이터 압축을 사용하도록 설정하여 데이터 전송 속도를 높입니다.
로깅 사용	SSL VPN 게이트웨이를 통과하는 트래픽의 로그를 유지합니다.
가상 키보드 강제	원격 사용자가 가상 키보드를 통해서만 웹 또는 클라이언트 로그인 정보를 입력할 수 있도록 허용합니다.
가상 키보드의 키 임의 지정	가상 키보드 키를 무작위로 표시합니다.
강제 시간 초과 사용	지정된 시간 초과 기간이 경과하면 원격 사용자의 연결을 끊습니다. 시간 초과 기간을 분 단위로 입력합니다.
세션 유휴 시간 제한	지정된 기간 동안 사용자 세션에서 어떤 작업도 감지되지 않으면 해당 기간이 지난 후 사용자 세션을 종료합니다. SSLVPN 유휴 시간 초과는 애플리케이션 및 사용자 데이터가 시간 초과 감지를 위해 전송하는 제어 패킷을 비롯한 모든 패킷을 고려합니다. 따라서 사용자 데이터가 없더라도 주기적인 제어 패킷(예: MDNS)을 전송하는 애플리케이션이 있는 경우 세션은 시간 초과되지 않습니다.
사용자 알림	원격 사용자가 로그인하면 해당 사용자에게 표시할 메시지를 입력합니다.

- 3 **확인(OK)**을 클릭합니다.

웹 포털 디자인 편집

SSL VPN 클라이언트에 바인딩된 클라이언트 배너를 편집할 수 있습니다.

절차

- 1 **NSX Edge(NSX Edges)** 탭에서 NSX Edge를 두 번 클릭합니다.
- 2 **관리(Manage)** 탭을 클릭한 후 **SSL VPN-Plus** 탭을 클릭합니다.
- 3 왼쪽 패널에서 **포털 사용자 지정(Portal Customization)**을 선택합니다.
- 4 포털 제목을 입력합니다.
- 5 원격 사용자의 회사 이름을 입력합니다.
- 6 **로고(Logo)**에서 **변경(Change)**을 클릭하고 회사 로고에 대한 JPEG 이미지를 선택합니다.
로고 크기에 대한 기본 설정 차원이 없습니다.
- 7 **색(Colors)**에서 색을 변경하려는 번호가 지정된 항목 옆의 색 상자를 클릭하고 원하는 색을 선택합니다.
- 8 필요한 경우 클라이언트 배너를 변경합니다. 배너에 대한 BMP 이미지를 선택합니다.
클라이언트 배너의 기본 크기는 390X75 픽셀입니다.
- 9 **확인(OK)**을 클릭합니다.

SSL VPN에 대한 IP 풀 사용


IP 풀을 편집하거나 삭제할 수 있습니다.

IP 풀을 추가하는 방법에 대한 자세한 내용은 [네트워크 액세스 SSL VPN-Plus 구성](#) 항목을 참조하십시오.

IP 풀 편집

IP 풀을 편집할 수 있습니다.


절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **IP 풀(IP Pool)**을 클릭합니다.
- 2 편집할 IP 풀을 선택합니다.
- 3 **편집(Edit)**() 아이콘을 클릭합니다.
IP 풀 편집 대화상자가 열립니다.
- 4 필요한 내용을 편집합니다.
- 5 **확인(OK)**을 클릭합니다.

IP 풀 삭제

IP 풀을 삭제할 수 있습니다.


절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **IP 풀(IP Pool)**을 클릭합니다.
- 2 삭제할 IP 풀을 선택합니다.
- 3 **삭제(Delete)**() 아이콘을 클릭합니다.
선택한 IP 풀이 삭제됩니다.

IP 풀 사용

IP 풀의 IP 주소를 원격 사용자에게 할당하려는 경우 해당 풀을 사용하도록 설정할 수 있습니다.


절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **IP 풀(IP Pool)**을 클릭합니다.
- 2 사용하도록 설정할 IP 풀을 선택합니다.
- 3 **사용(Enable)**() 아이콘을 클릭합니다.

IP 풀 사용 안 함

IP 풀의 IP 주소를 원격 사용자에게 할당하지 않으려는 경우 해당 IP 풀을 사용하지 않도록 설정할 수 있습니다.



절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **IP 풀(IP Pool)**을 선택합니다.
- 2 사용하지 않도록 설정할 IP 풀을 선택합니다.
- 3 **사용 안 함(Disable)**() 아이콘을 클릭합니다.

IP 풀의 순서 변경

SSL VPN은 IP 풀 테이블에 있는 순서에 따라 IP 풀의 IP 주소를 원격 사용자에게 할당합니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **IP 풀(IP Pool)**을 클릭합니다.
- 2 순서를 변경할 IP 풀을 선택합니다.
- 3 **위로 이동(Move Up)**() 또는 **아래로 이동(Move Down)**() 아이콘을 클릭합니다.

전용 네트워크 사용


원격 사용자가 액세스할 수 있는 전용 네트워크를 편집하거나 삭제할 수 있습니다.

전용 네트워크를 추가하는 방법에 대한 자세한 내용은 [네트워크 액세스 SSL VPN-Plus 구성](#) 항목을 참조하십시오.

전용 네트워크 삭제

전용 네트워크를 삭제할 수 있습니다.


절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **전용 네트워크(Private Networks)**를 클릭합니다.
- 2 삭제할 네트워크를 선택한 다음 **삭제(Delete)**() 아이콘을 클릭합니다.

전용 네트워크 사용

전용 네트워크를 사용하도록 설정하면 원격 사용자는 **SSL VPN-Plus**를 통해 전용 네트워크에 액세스할 수 있습니다.

절차


- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **전용 네트워크(Private Networks)**를 클릭합니다.
- 2 사용하도록 설정할 네트워크를 클릭합니다.
- 3 **사용(Enable)** 아이콘()을 클릭합니다.

선택한 네트워크가 사용하도록 설정됩니다.

전용 네트워크 사용 안 함

전용 네트워크를 사용하지 않도록 설정하면 원격 사용자는 **SSL VPN-Plus**를 통해 전용 네트워크에 액세스할 수 없습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **전용 네트워크(Private Networks)**를 클릭합니다.
- 2 사용하지 않도록 설정할 네트워크를 클릭합니다.
- 3 **사용 안 함(Disable)**() 아이콘을 클릭합니다.




선택한 네트워크가 사용하지 않도록 설정됩니다.

전용 네트워크의 순서 변경

SSL VPN-Plus를 통해 원격 사용자는 전용 네트워크 패널에 표시되는 순서대로 전용 네트워크에 액세스할 수 있습니다.

전용 네트워크에 대해 **TCP 최적화 사용(Enable TCP Optimization)**을 선택할 경우 활성 모드의 **FTP** 같은 일부 애플리케이션이 해당 서브넷 내에서 작동하지 않을 수 있습니다. 활성 모드로 구성된 **FTP** 서버를 추가하려면 해당 **FTP** 서버에 대해 또 다른 전용 네트워크를 추가하고 **TCP** 최적화를 사용하지 않도록 설정해야 합니다. 또한 활성 **TCP** 전용 네트워크를 사용하도록 설정하고 서브넷 전용 네트워크 위에 배치해야 합니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **전용 네트워크(Private Networks)**를 클릭합니다.
- 2 **순서 변경(Change Order)**() 아이콘을 클릭합니다.
- 3 순서를 변경할 네트워크를 선택합니다.
- 4 **위로 이동(Move Up)**() 또는 **아래로 이동(Move Down)**() 아이콘을 클릭합니다.
- 5 **확인(OK)**을 클릭합니다.

다음에 수행할 작업

활성 모드로 구성된 FTP 서버를 추가하려면 **활성 FTP 서버에 대한 전용 네트워크 구성**을 참조하십시오.

활성 FTP 서버에 대한 전용 네트워크 구성

활성 모드로 구성된 FTP 서버를 전용 네트워크에 추가할 수 있습니다. 활성 FTP의 경우 TCP 최적화를 지원하지 않는 클라이언트 시스템으로의 제어 연결이 백엔드 FTP 서버에 의해 시작됩니다.

사전 요구 사항

FTP 서버는 활성 모드로 구성됩니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **전용 네트워크(Private Networks)**를 클릭합니다.
- 2 활성 FTP에 대해 구성하려는 전용 네트워크를 추가합니다. 자세한 내용은 **전용 네트워크 추가**를 참조하십시오.
- 3 **TCP 최적화 사용(Enable TCP Optimization)** 확인란을 선택 취소합니다.
- 4 **포트(Ports)** 필드에서 전용 네트워크의 포트 번호를 추가합니다.
- 5 상태를 **사용(Enabled)**으로 선택하여 전용 네트워크를 사용하도록 설정합니다.
- 6 활성 FTP용으로 구성하려는 전용 네트워크를 구성된 다른 전용 네트워크 위에 배치합니다. 자세한 내용은 **전용 네트워크의 순서 변경**를 참조하십시오.

다음에 수행할 작업

전용 네트워크 트래픽을 허용하도록 해당 방화벽 규칙을 추가합니다.

설치 패키지 사용


SSL 클라이언트용 설치 패키지를 삭제하거나 편집할 수 있습니다.

설치 패키지를 생성하는 방법에 대한 자세한 내용은 **네트워크 액세스 SSL VPN-Plus 구성** 항목을 참조하십시오.

설치 패키지 편집

설치 패키지를 편집할 수 있습니다.


절차

- 1 **SSL VPN-Plus** 탭의 왼쪽 패널에 있는 **설치 패키지(Installation Package)**를 클릭합니다.
- 2 편집할 설치 패키지를 선택합니다.
- 3 편집() 아이콘을 클릭합니다.
설치 패키지 편집 대화상자가 열립니다.
- 4 필요한 내용을 편집합니다.
- 5 **확인(OK)**을 클릭합니다.

설치 패키지 삭제

설치 패키지를 삭제할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭의 왼쪽 패널에 있는 **설치 패키지(Installation Package)**를 클릭합니다.
- 2 삭제할 설치 패키지를 선택합니다.
- 3 **삭제>Delete)()** 아이콘을 클릭합니다.

사용자 사용


로컬 데이터베이스에서 사용자를 편집하거나 삭제할 수 있습니다.

사용자를 추가하는 방법에 대한 자세한 내용은 [네트워크 액세스 SSL VPN-Plus 구성](#) 항목을 참조하십시오.

사용자 편집

사용자 ID를 제외한 사용자의 세부 정보를 편집할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **사용자(Users)**를 클릭합니다.
- 2 편집(Edit)() 아이콘을 클릭합니다.
- 3 필요한 내용을 편집합니다.
- 4 **확인(OK)**을 클릭합니다.

사용자 삭제

사용자를 삭제할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **사용자(Users)**를 클릭합니다.
- 2 **구성(Users)** 패널에서 **사용자(Configure)**를 클릭합니다.

- 3 삭제할 사용자를 선택한 다음 **삭제(Delete)**() 아이콘을 클릭합니다.

사용자의 암호 변경

사용자의 암호를 변경할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **사용자(Users)**를 클릭합니다.
- 2 **암호 변경(Change Password)** 아이콘을 클릭합니다.
- 3 새 암호를 입력하고 한 번 더 입력합니다.
- 4 사용자가 다음 번에 시스템에 로그인할 때 암호를 변경하도록 하려면 **[다음 로그인 시 암호 변경]**을 클릭합니다.
- 5 **확인(OK)**을 클릭합니다.


로그인 및 로그오프 스크립트 사용

로그인 또는 로그오프 스크립트를 NSX Edge Gateway에 바인딩할 수 있습니다.

스크립트 편집

NSX Edge Gateway에 연결된 로그인 또는 로그오프 스크립트의 유형, 설명 및 상태를 편집할 수 있습니다.


절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **로그인/로그오프 스크립트(Login/Logoff Scripts)**를 클릭합니다.
- 2 스크립트를 선택하고 **편집(Edit)**() 아이콘을 클릭합니다.
- 3 필요한 내용을 변경합니다.
- 4 **확인(OK)**을 클릭합니다.

스크립트 삭제

로그인 또는 로그오프 스크립트를 삭제할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **로그인/로그오프 스크립트(Login/Logoff Scripts)**를 클릭합니다.
- 2 스크립트를 선택하고 **삭제(Delete)**() 아이콘을 클릭합니다.

스크립트 사용

스크립트는 사용하도록 설정해야 작동합니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **로그인/로그오프 스크립트(Login/Logoff Scripts)**를 클릭합니다.
- 2 스크립트를 선택하고 **사용(Enable)(✓)** 아이콘을 클릭합니다.

스크립트 사용 안 함

로그인/로그오프 스크립트를 사용하지 않도록 설정할 수 있습니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **로그인/로그오프 스크립트(Login/Logoff Scripts)**를 클릭합니다.
- 2 스크립트를 선택하고 **사용 안 함(Disable)(✗)** 아이콘을 클릭합니다.

스크립트 순서 변경

스크립트의 순서를 변경할 수 있습니다. 예를 들어 Internet Explorer에서 gmail.com을 열기 위한 로그인 스크립트가 yahoo.com을 열기 위한 로그인 스크립트보다 위에 있는 경우, 원격 사용자가 SSL VPN에 로그인할 때 gmail.com이 yahoo.com보다 먼저 표시됩니다. 이제 로그인 스크립트를 역순으로 바꾸면 yahoo.com이 gmail.com보다 먼저 표시됩니다.

절차

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **로그인/로그오프 스크립트(Login/Logoff Scripts)**를 클릭합니다.
- 2 순서를 변경할 스크립트를 선택하고 **위로 이동(Move Up)(⇩↑)** 또는 **아래로 이동(Move Down)(⇩↓)** 아이콘을 클릭합니다.
- 3 **확인(OK)**을 클릭합니다.

IPSec VPN 개요

NSX Edge는 NSX Edge 인스턴스와 원격 사이트 사이에서 사이트 간 IPSec VPN을 지원합니다. NSX Edge 인스턴스와 원격 VPN 라우터 간에 인증서 인증, 미리 공유한 키 모드 및 IP 유니캐스트 트래픽을 지원하지만 동적 라우팅 프로토콜은 지원하지 않습니다.

각 원격 VPN 라우터 뒤에서 IPSec 터널을 통해 NSX Edge 뒤의 내부 네트워크에 연결하는 여러 서브넷을 구성할 수 있습니다.

참고 NSX Edge 뒤에 있는 서브넷 및 내부 네트워크의 주소 범위는 겹치면 안 됩니다.

IPSec VPN의 로컬 및 원격 피어의 IP 주소가 겹치면, 연결된 로컬 경로 및 자동으로 연결된 경로가 존재하는지에 따라 터널을 통한 트래픽 전달이 일관되지 않을 수 있습니다.

NAT 디바이스 뒤에 NSX Edge 에이전트를 배포할 수 있습니다. 이 배포에서 NAT 디바이스는 NSX Edge 인스턴스의 VPN 주소를 인터넷에 연결하는 공용 액세스 가능 주소로 변환합니다. 원격 VPN 라우터는 이 공용 주소를 사용하여 NSX Edge 인스턴스에 액세스합니다.

NAT 디바이스 뒤에 원격 VPN 라우터를 배치할 수도 있습니다. 터널을 설정하기 위해 VPN 기본 주소와 VPN 게이트웨이 ID를 제공해야 합니다. 양쪽 끝점에서 VPN 주소에 대해 정적 일대일 NAT가 필요합니다.

필요한 터널 수는 로컬 서브넷 수에 피어 서브넷 수를 곱해서 정의됩니다. 예를 들어 로컬 서브넷이 10개 있고 피어 서브넷이 10개 있는 경우 터널이 100개 필요합니다. 지원되는 최대 터널 수는 아래와 같이 ESG 크기를 기준으로 결정됩니다.

표 14-6. ESG당 IPSec 터널 수

ESG	IPSec 터널 수
소형	512
대형	1600
대형	4096
초대형	6000

지원되는 IPSec VPN 알고리즘은 다음과 같습니다.

- AES(AES128-CBC)
- AES256(AES256-CBC)
- Triple DES(3DES192-CBC)
- AES-GCM(AES128-GCM)
- DH-2(Diffie – Hellman group 2)
- DH-5(Diffie – Hellman group 5)
- DH-14(Diffie – Hellman group 14)
- DH-15(Diffie – Hellman group 15)
- DH-16(Diffie – Hellman group 16)

IPSec VPN 구성 예는 [IPSec VPN 구성 예](#) 항목을 참조하십시오.

IPSec VPN 문제 해결에 대해서는 <https://kb.vmware.com/kb/2123580> 항목을 참조하십시오.

IPSec VPN 서비스 구성

로컬 서브넷과 피어 서브넷 간에 NSX Edge 터널을 설정할 수 있습니다.

참고 IPSec VPN을 통해 원격 사이트에 연결할 경우 Edge 업링크의 동적 라우팅에서 해당 사이트의 IP 주소를 인식할 수 없습니다.

IPSec VPN 서비스 사용

로컬 서브넷에서 피어 서브넷으로 트래픽이 전송되려면 **IPSec VPN** 서비스를 사용하도록 설정해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **VPN** 탭을 클릭합니다.
- 5 **IPSec VPN**을 클릭합니다.
- 6 **사용(Enable)**을 클릭합니다.

OpenSSL을 사용하여 IPSec VPN용 CA 서명된 인증서 생성

IPSec에 대해 인증서 인증을 사용하도록 설정하려면 서버 인증서 및 해당 CA 서명된 인증서를 가져와야 합니다. 필요한 경우 OpenSSL과 같은 오픈 소스 명령줄 도구를 사용하여 CA 서명된 인증서를 생성할 수 있습니다.

사전 요구 사항

OpenSSL이 설치되어 있어야 합니다.

절차

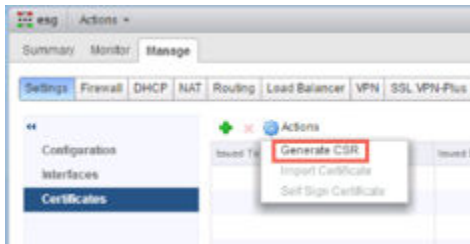
- 1 OpenSSL이 설치된 Linux 또는 Mac 시스템에서 `/opt/local/etc/openssl/openssl.cnf` 또는 `/System/Library/OpenSSL/openssl.cnf` 파일을 엽니다.
- 2 `dir = .`인지 확인합니다.
- 3 다음 명령을 실행합니다.

```
mkdir newcerts
mkdir certs
mkdir req
mkdir private
echo "01" > serial
touch index.txt
```

- 4 다음 명령을 실행하여 CA 서명된 인증서를 생성합니다.

```
openssl req -new -x509 -newkey rsa:2048 -keyout private/cakey.pem -out cacert.pem -days 3650
```

- 5 NSX Edge1에서 CSR을 생성하고 PEM(Privacy Enhanced Mail) 파일 콘텐츠를 복사한 다음 req/edge1.req에 있는 파일에 저장합니다.



CA 서명된 인증서 구성을 참조하십시오.

- 6 다음 명령을 실행하여 CSR에 서명합니다.

```
sudo openssl ca -policy policy_anything -out certs/edge1.pem -in req/edge1.req
```

- 7 NSX Edge2에서 CSR을 생성하고 PEM(Privacy Enhanced Mail) 파일 콘텐츠를 복사한 다음 req/edge2.req에 있는 파일에 저장합니다.

- 8 다음 명령을 실행하여 CSR에 서명합니다.

```
sudo openssl ca -policy policy_anything -out certs/edge2.pem -in req/edge2.req
```

- 9 certs/edge1.pem 파일의 끝에 있는 PEM 인증서를 Edge1에 업로드합니다.

- 10 certs/edge2.pem 파일의 끝에 있는 PEM 인증서를 Edge2에 업로드합니다.

- 11 cacert.pem 파일의 CA 인증서를 CA 서명된 인증서로 Edge1 및 Edge2에 업로드합니다.

- 12 Edge1 및 Edge2에 대한 IPSec 글로벌 구성에서 업로드한 PEM 인증서 및 업로드한 CA 인증서를 선택하고 구성을 저장합니다.

- 13 인증서(Certificate) 탭에서 업로드한 인증서를 클릭하고 DN 문자열을 기록합니다.

- 14 DN 문자열을 C=IN, ST=ka, L=blr, O=bmware, OU=vmware, CN=edge2.eng.vmware.com 형식에 따라 역방향으로 구성하고 Edge1 및 Edge2용으로 저장합니다.

- 15 지정된 형식의 DN(고유 이름) 문자열로 된 로컬 ID 및 피어 ID를 사용하여 Edge1 및 Edge2에 IPSec VPN 사이트를 생성합니다.

결과

IPSec 통계 표시(Show IPsec Statistics)를 클릭하여 상태를 확인합니다. 채널을 클릭하여 터널 상태를 확인합니다. 채널과 터널의 상태가 모두 녹색으로 나타나야 합니다.

글로벌 IPSec VPN 구성 지정

이렇게 하면 NSX Edge 인스턴스에서 IPSec VPN을 사용할 수 있습니다.

사전 요구 사항

인증서 인증을 사용하도록 설정하려면 서버 인증서 및 해당 CA 서명된 인증서를 가져와야 합니다. 필요한 경우 OpenSSL과 같은 오픈 소스 명령줄 도구를 사용하여 CA 서명된 인증서를 생성할 수 있습니다.

자체 서명된 인증서는 IPsec VPN에 사용할 수 없습니다. 이러한 인증서는 로드 밸런싱 및 SSL VPN에만 사용할 수 있습니다.

절차


- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **VPN** 탭을 클릭합니다.
- 5 **IPsec VPN**을 클릭합니다.
- 6 글로벌 구성 상태 옆의 **변경(Change)**을 클릭합니다.
- 7 피어 끝점이 임의로 설정된 사이트에 대해 사전 공유된 글로벌 키를 입력하고 **공유 키 표시(Display shared key)**를 선택하여 키를 표시합니다.
- 8 인증서 인증 사용을 선택하고 적절한 인증서를 선택합니다.
- 9 **확인(OK)**을 클릭합니다.

IPsec VPN에 대한 로깅 사용

모든 IPsec VPN 트래픽 로깅을 사용하도록 설정할 수 있습니다.

기본적으로 로깅이 사용되도록 설정되고 주의 수준으로 설정됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **VPN** 탭을 클릭합니다.
- 5 **IPsec VPN**을 클릭합니다.
- 6 **로깅 정책(Logging Policy)** 옆의 을 클릭하고 **로깅 사용(Enable logging)**을 클릭하여 로컬 서브넷과 피어 서브넷 간의 트래픽 흐름을 기록하도록 설정하고 로깅 수준을 선택합니다.
- 7 로그 수준을 선택하고 **변경 내용 게시(Publish Changes)**를 클릭합니다.

IPsec VPN 매개 변수 구성

IPsec VPN 서비스를 제공하려면 NSX Edge에 외부 IP 주소를 하나 이상 구성해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **VPN** 탭을 클릭합니다.
- 5 **IPSec VPN**을 클릭합니다.
- 6 **추가(Add)(+)** 아이콘을 클릭합니다.
- 7 IPSec VPN의 이름을 입력합니다.
- 8 **로컬 ID(Local Id)**에 NSX Edge 인스턴스의 IP 주소를 입력합니다. 이 로컬 ID는 원격 사이트의 피어 ID가 됩니다.
- 9 로컬 끝점의 IP 주소를 입력합니다.
사전 공유 키를 사용하는 IP 터널에 IP를 추가하는 경우에는 로컬 ID와 로컬 끝점 IP가 같을 수 있습니다.
- 10 사이트 간에 공유할 서브넷을 CIDR 형식으로 입력합니다. 서브넷을 여러 개 입력하려면 구분 문자로 쉼표를 사용합니다.
- 11 피어 사이트를 고유하게 식별할 피어 ID를 입력합니다. 인증서 인증을 사용하는 피어의 경우 이 ID는 피어 인증서의 일반 이름이어야 합니다. PSK 피어의 경우에는 이 ID가 임의의 문자열일 수 있습니다. VPN 서비스의 FQDN 또는 VPN의 공용 IP 주소를 피어 ID로 사용하는 것이 좋습니다.
- 12 피어 끝점에 피어 사이트의 IP 주소를 입력합니다. 이 항목을 비워 둘 경우 NSX Edge는 피어 디바이스가 연결을 요청할 때까지 대기합니다.
- 13 피어 서브넷의 내부 IP 주소를 CIDR 형식으로 입력합니다. 서브넷을 여러 개 입력하려면 구분 문자로 쉼표를 사용합니다.
- 14 암호화 알고리즘을 선택합니다.
AES-GCM 암호화 알고리즘은 FIPS와 호환되지 않습니다.
- 15 인증 방법에서 다음 중 하나를 선택합니다.

옵션	설명
PSK(사전 공유 키)	NSX Edge와 피어 사이트 간에 공유되는 비밀 키가 인증에 사용됨을 나타냅니다. 비밀 키는 최대 길이가 128바이트인 문자열일 수 있습니다. PSK 인증은 FIPS 모드에서 사용되지 않도록 설정됩니다.
인증서	글로벌 수준에서 정의된 인증서가 인증에 사용됨을 나타냅니다.

- 16 익명 사이트가 VPN 서비스에 연결할 경우 공유 키를 입력합니다.
- 17 피어 사이트에 키를 표시하려면 **공유 키 표시(Display Shared Key)**를 클릭합니다.

18 DH(Diffie-Hellman) 그룹에서 피어 사이트 및 NSX Edge가 보안되지 않는 통신 채널에 공유 암호를 설정하도록 허용할 암호화 체계를 선택합니다.

DH14는 FIPS 및 비 FIPS 모드 둘 다에 대한 기본 선택 옵션입니다. FIPS 모드가 사용되도록 설정되면 DH2 및 DH5를 사용할 수 없습니다.

19 확장에서 다음 중 하나를 입력하십시오.

- **securelocaltrafficbyip=IPAddress**(IPSec VPN 터널에서 Edge의 로컬 트래픽이 리디렉션됨) 이 옵션이 기본값입니다. 자세한 내용은 <http://kb.vmware.com/kb/20080007>을 참조하십시오.
- **passthroughSubnets=PeerSubnet/IPAddress**(서브넷의 겹침을 지원).

20 확인(OK)을 클릭합니다.

NSX Edge는 로컬 서브넷에서 피어 서브넷으로 연결되는 터널을 생성합니다.


다음에 수행할 작업

IPSec VPN 서비스를 사용하도록 설정합니다.

IPSec VPN 서비스 편집

IPSec VPN 서비스를 편집할 수 있습니다.

절차


- 1 vSphere Web Client에 로그인합니다.**
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.**
- 3 NSX Edge를 두 번 클릭합니다.**
- 4 관리(Manage) 탭을 클릭하고 VPN 탭을 클릭합니다.**
- 5 IPSec VPN을 클릭합니다.**
- 6 편집할 IPSec 서비스를 선택합니다.**
- 7 편집(Edit)() 아이콘을 클릭합니다.**
- 8 필요한 내용을 편집합니다.**
- 9 확인(OK)을 클릭합니다.**

IPSec VPN 사이트 사용 안 함

IPSec VPN 사이트를 사용하지 않도록 설정할 수 있습니다.

절차


- 1 vSphere Web Client에 로그인합니다.**
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.**

- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **VPN** 탭을 클릭합니다.
- 5 **IPSec VPN**을 클릭합니다.
- 6 사용하지 않도록 설정할 IPSec VPN 사이트를 선택합니다.
- 7 **사용 안 함(Disable)**() 아이콘을 클릭합니다.

IPSec VPN 사이트 삭제

IPSec VPN 사이트를 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭하고 **VPN** 탭을 클릭합니다.
- 5 **IPSec VPN**을 클릭합니다.
- 6 삭제할 IPSec VPN 사이트를 선택합니다.
- 7 **삭제>Delete**() 아이콘을 클릭합니다.

IPSec VPN 구성 예

이 시나리오에는 NSX Edge와 다른 끝의 Cisco 또는 WatchGuard VPN 사이의 기본적인 지점 간 IPSEC VPN 연결을 보여 주는 구성 예가 포함되어 있습니다.

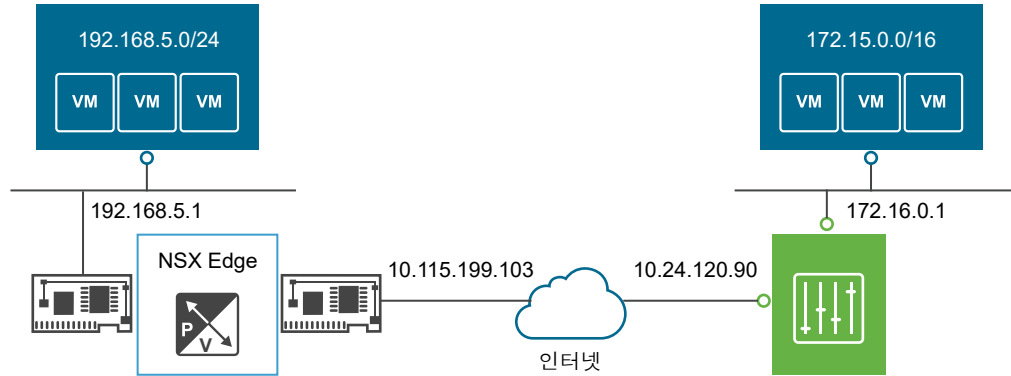
이 시나리오에서 NSX Edge는 내부 네트워크 192.168.5.0/24를 인터넷에 연결합니다. NSX Edge 인터페이스는 다음과 같이 구성됩니다.

- 업링크 인터페이스: 192.168.5.1
- 내부 인터페이스: 10.115.199.103

원격 게이트웨이는 172.15.0.0/16 내부 네트워크를 인터넷에 연결합니다. 원격 게이트웨이 인터페이스는 다음과 같이 구성됩니다.

- 업링크 인터페이스: 10.24.120.90
- 내부 인터페이스: 172.16.0.1

그림 14-1. 원격 VPN 게이트웨이에 연결하는 NSX Edge



참고 NSX Edge에서 NSX Edge IPSEC로 연결되는 터널에 대해 두 번째 NSX Edge를 원격 게이트웨이로 설정하여 동일한 시나리오를 사용할 수 있습니다.

용어

IPSec는 개방형 표준 프레임워크입니다. NSX Edge 및 기타 VPN 장치의 로그에는 IPSec VPN 문제를 해결하는 데 사용할 수 있는 다양한 기술 용어가 있습니다.

다음은 로그에서 접할 수 있는 몇 가지 표준입니다.

- ISAKMP(Internet Security Association and Key Management Protocol)는 인터넷 환경에서 SA(보안 연결) 및 암호화 키를 설정하기 위해 RFC 2408에 의해 정의된 프로토콜입니다. 인증 및 키 교환용 프레임워크만 제공하는 ISAKMP는 키 교환과 무관하도록 설계되었습니다.
- Oakley는 인증된 당사자가 Diffie-Hellman 키 교환 알고리즘을 사용하여 보안되지 않는 연결 상태에서 키 관련 자료를 교환할 수 있는 키 결정 프로토콜입니다.
- IKE(Internet Key Exchange)는 ISAKMP 프레임워크와 Oakley가 조합된 것으로, NSX Edge는 IKEv1을 제공합니다.
- DH(Diffie-Hellman) 키 교환은 서로 모르는 두 당사자가 보안되지 않는 통신 채널에서 공유 비밀 키를 공동 설정할 수 있는 암호화 프로토콜입니다. VSE는 DH 그룹 2(1024비트) 및 그룹 5(1536비트)를 지원합니다.

IKE 1단계 및 2단계

IKE는 인증된 보안 통신을 배열하는 데 사용되는 표준 방법입니다.

1단계 매개 변수

1단계에서는 피어의 상호 인증을 설정하고, 암호화 매개 변수를 협상하며, 세션 키를 생성합니다. NSX Edge에서 사용되는 1단계 매개 변수는 다음과 같습니다.

- 기본 모드
- TripleDES/AES[구성 가능]
- SHA-1

- MODP 그룹 2(1024비트)
- 사전 공유 암호[구성 가능]
- 28800초(8시간)의 SA 수명(데이터(KB) 기반 키 재생성 없음)
- ISAKMP 적극적 모드 사용 안 함

2단계 매개 변수

IKE 2단계에서는 IKE 1단계 키를 기본 키로 사용하거나 새 키를 교환하여 사용할 IPSec 터널에 대한 키 관련 자료를 생성함으로써 IPSec 터널을 협상합니다. NSX Edge에서 지원되는 IKE 2단계 매개 변수는 다음과 같습니다.

- TripleDES/AES[1단계 설정과 일치]
- SHA-1
- ESP 터널 모드
- MODP 그룹 2(1024비트)
- 키 재생성을 위한 PFS(Perfect Forward Secrecy)
- 3600초(1시간)의 SA 수명(데이터(KB) 기반 키 재생성 없음)
- IPv4 서브넷을 사용하는 두 네트워크 간의 모든 IP 프로토콜과 포트에 대한 선택기

트랜잭션 모드 샘플

NSX Edge에서는 1단계에 기본 모드를 지원하고, 2단계에 빠른 모드를 지원합니다.

NSX Edge는 PSK, 3DES/AES128, sha1 및 DH 그룹 2/5를 사용해야 하는 정책을 제안합니다. 피어는 이 정책을 수락해야 하며, 그렇지 않으면 협상 단계가 실패합니다.

1단계: 기본 모드 트랜잭션

이 예에서는 NSX Edge에서 시작되어 Cisco 디바이스로 향하는 1단계 협상의 교환을 보여 줍니다.

기본 모드에서 NSX Edge와 Cisco VPN 디바이스 간에 다음 트랜잭션이 순서대로 수행됩니다.

1 NSX Edge에서 Cisco로

- 제안 사항: 3des-cbc, sha, psk, 그룹 5(그룹 2) 암호화
- DPD 사용

2 Cisco에서 NSX Edge로

- Cisco에서 선택한 제안 사항 포함
- Cisco 디바이스가 1단계에서 NSX Edge가 보낸 매개 변수를 모두 수락하지 않으면 Cisco 디바이스는 NO_PROPOSAL_CHOSEN 플래그가 지정된 메시지를 보내고 협상을 종료합니다.

3 NSX Edge에서 Cisco로

- DH 키 및 nonce

4 Cisco에서 NSX Edge로

- DH 키 및 nonce

5 NSX Edge에서 Cisco로(암호화됨)

- ID(PSK) 포함

6 Cisco에서 NSX Edge로(암호화됨)

- ID(PSK) 포함
- Cisco 디바이스는 PSK가 일치하지 않는 사실을 확인하면 INVALID_ID_INFORMATION 플래그가 지정된 메시지를 보내고 1단계는 실패합니다.

2단계: 빠른 모드 트랜잭션

빠른 모드에서 NSX Edge와 Cisco VPN 디바이스 간에 다음 트랜잭션이 순서대로 수행됩니다.

1 NSX Edge에서 Cisco로

NSX Edge는 피어에 2단계 정책을 제안합니다. 예:

```
Aug 26 12:16:09 weiqing-desktop
ipsec[5789]:
"s1-c1" #2: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:d20849ac
proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=OAKLEY_GROUP_MODP1024}
```

2 Cisco에서 NSX Edge로

Cisco 디바이스가 제안 사항과 일치하는 정책을 찾지 못하면 NO_PROPOSAL_CHOSEN을 다시 보내고, 일치하는 정책을 찾으면 Cisco 디바이스가 선택된 매개 변수 집합을 보냅니다.

3 NSX Edge에서 Cisco로

디버깅이 원활히 수행되도록 NSX Edge에서 IPsec 로깅을 사용하도록 설정하고 Cisco에서 crypto debug를 사용하도록 설정할 수 있습니다(debug crypto isakmp <수준>).

IPsec VPN 서비스 구성 예

VPN 매개 변수를 구성한 후에 IPsec 서비스를 사용하도록 설정해야 합니다.

절차

1 IPsec VPN 매개 변수 구성 예

IPsec VPN 서비스를 제공하려면 NSX Edge에 외부 IP 주소를 하나 이상 구성해야 합니다.

2 IPsec VPN 서비스 사용 예

로컬 서브넷에서 피어 서브넷으로 트래픽이 전송되려면 IPsec VPN 서비스를 사용하도록 설정해야 합니다.

IPSec VPN 매개 변수 구성 예

IPSec VPN 서비스를 제공하려면 NSX Edge에 외부 IP 주소를 하나 이상 구성해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 VPN 탭을 클릭합니다.
- 5 IPSec VPN을 클릭합니다.
- 6 추가(Add)(+) 아이콘을 클릭합니다.
- 7 IPSec VPN의 이름을 입력합니다.
- 8 로컬 ID(Local Id)에 NSX Edge 인스턴스의 IP 주소를 입력합니다. 이 로컬 ID는 원격 사이트의 피어 ID가 됩니다.
- 9 로컬 끝점의 IP 주소를 입력합니다.
사전 공유 키를 사용하는 IP 터널에 IP를 추가하는 경우에는 로컬 ID와 로컬 끝점 IP가 같을 수 있습니다.
- 10 사이트 간에 공유할 서브넷을 CIDR 형식으로 입력합니다. 서브넷을 여러 개 입력하려면 구분 문자로 쉼표를 사용합니다.
- 11 피어 사이트를 고유하게 식별할 피어 ID를 입력합니다. 인증서 인증을 사용하는 피어의 경우 이 ID는 피어 인증서의 일반 이름이어야 합니다. PSK 피어의 경우에는 이 ID가 임의의 문자열일 수 있습니다. 피어 ID로는 VPN 서비스의 FQDN 또는 VPN의 공용 IP 주소를 사용하는 것이 좋습니다.
- 12 피어 끝점에 피어 사이트의 IP 주소를 입력합니다. 이 항목을 비워 둘 경우 NSX Edge는 피어 디바이스가 연결을 요청할 때까지 대기합니다.
- 13 피어 서브넷의 내부 IP 주소를 CIDR 형식으로 입력합니다. 서브넷을 여러 개 입력하려면 구분 문자로 쉼표를 사용합니다.
- 14 암호화 알고리즘을 선택합니다.
- 15 인증 방법에서 다음 중 하나를 선택합니다.

옵션	설명
PSK(사전 공유 키)	NSX Edge와 피어 사이트 간에 공유되는 비밀 키가 인증에 사용됨을 나타냅니다. 비밀 키는 최대 길이가 128바이트인 문자열일 수 있습니다.
인증서	글로벌 수준에서 정의된 인증서가 인증에 사용됨을 나타냅니다.

- 16 익명 사이트가 VPN 서비스에 연결할 경우 공유 키를 입력합니다.
- 17 피어 사이트에 키를 표시하려면 공유 키 표시(Display Shared Key)를 클릭합니다.

- 18 DH(Diffie-Hellman) 그룹에서 피어 사이트 및 NSX Edge가 보안되지 않는 통신 채널에 공유 암호를 설정하도록 허용할 암호화 체계를 선택합니다.
- 19 필요한 경우 MTU 임계값을 변경합니다.
- 20 PFS(Perfect Forward Secrecy) 임계값을 사용하도록 설정할지 여부를 선택합니다. IPSec 협상에서 PFS(Perfect Forward Secrecy)를 사용하면 새로운 각 암호화 키에서 이전의 모든 키와 연관된 관계가 해제됩니다.
- 21 **확인(OK)**을 클릭합니다.

NSX Edge는 로컬 서브넷에서 피어 서브넷으로 연결되는 터널을 생성합니다.

다음에 수행할 작업

IPSec VPN 서비스를 사용하도록 설정합니다.

IPSec VPN 서비스 사용 예

로컬 서브넷에서 피어 서브넷으로 트래픽이 전송되려면 IPSec VPN 서비스를 사용하도록 설정해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **VPN** 탭을 클릭합니다.
- 5 **IPSec VPN**을 클릭합니다.
- 6 **사용(Enable)**을 클릭합니다.

다음에 수행할 작업

로컬 서브넷과 피어 서브넷 사이의 트래픽 흐름을 로깅하려면 **로깅 사용(Enable Logging)**을 클릭합니다.

Cisco 2821 통합 서비스 라우터 사용

다음은 Cisco IOS를 사용하여 수행하는 구성 작업에 대해 설명합니다.

절차

- 1 인터페이스 및 기본 경로를 구성합니다.

```
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
```

```
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.24.123.253
```

2 IKE 정책을 구성합니다.

```
Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
Router(config-isakmp)# authentication
    pre-share
Router(config-isakmp)# exit
```

3 사전 공유 암호와 각 피어를 일치시킵니다.

```
Router# config term
Router(config)# crypto isakmp key vshield
    address 10.115.199.103
Router(config-isakmp)# exit
```

4 IPSEC 변환을 정의합니다.

```
Router# config term
Router(config)# crypto ipsec transform-set
    myset esp-3des esp-sha-hmac
Router(config-isakmp)# exit
```

5 IPSec 액세스 목록을 생성합니다.

```
Router# config term
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# access-list 101 permit ip
    172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit
```

6 정책을 암호화 맵과 바인딩하고 레이블을 지정합니다.

다음 예에서는 암호화 맵의 레이블을 MYVPN으로 지정합니다.

```
Router# config term
Router(config)# crypto map MYVPN 1
    ipsec-isakmp
% NOTE: This new crypto map will remain
    disabled until a peer and a valid
    access list have been configured.
Router(config-crypto-map)# set transform-set
    myset
Router(config-crypto-map)# set pfs group1
```

```
Router(config-crypto-map)# set peer
    10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
```

예제: 구성

```
router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des
    esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
set peer 10.115.199.103
set transform-set myset
set pfs group1
match address 101
!
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
```

```

duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.0.0
    0.0.255.255 192.168.5.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
scheduler allocate 20000 1000
!
end

```

Cisco ASA 5510 사용

다음 출력 결과를 사용하여 Cisco ASA 5510을 구성합니다.

```

ciscoasa# show running-config output
: Saved
:
ASA Version 8.2(1)18
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KY0U encrypted
passwd 2KFQnbNIdI.2KY0U encrypted
names
!
interface Ethernet0/0
nameif untrusted
security-level 100
ip address 10.24.120.90 255.255.252.0
!
interface Ethernet0/1
nameif trusted
security-level 90

```

```

ip address 172.16.0.1 255.255.0.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
boot system disk0:/asa821-18-k8.bin
ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0
    192.168.5.0 255.255.255.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.255.0
    172.16.0.0 255.255.0.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
    udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
    mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
    sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac

```

```

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map MYVPN 1 match address ACL1
crypto map MYVPN 1 set pfs
crypto map MYVPN 1 set peer 10.115.199.103
crypto map MYVPN 1 set transform-set MYSET
crypto map MYVPN interface untrusted
crypto isakmp enable untrusted
crypto isakmp policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 10.0.0.0 255.0.0.0 untrusted
telnet timeout 5
ssh timeout 5
console timeout 0
no threat-detection basic-threat
no threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 10.115.199.103 type ipsec-l2l
tunnel-group 10.115.199.103 ipsec-attributes
pre-shared-key *
!
!
prompt hostname context
Cryptochecksum:29c3cc49460831ff6c070671098085a9
: end

```

WatchGuard Firebox X500 구성

WatchGuard Firebox X500을 원격 게이트웨이로 구성할 수 있습니다.

참고 정확한 단계는 WatchGuard Firebox 설명서를 참조하십시오.

절차

- 1 Firebox System Manager에서 **도구(Tools) > 정책 관리자(Policy Manager)**를 선택합니다.
- 2 Policy Manager에서 **네트워크(Network) > 구성(Configuration)**을 선택합니다.
- 3 인터페이스를 구성하고 **확인(OK)**를 클릭합니다.
- 4 (선택 사항) **네트워크(Network) > 경로(Routes)**를 선택하여 기본 경로를 구성합니다.
- 5 **네트워크(Network) > 지사 VPN(Branch Office VPN) > 수동 IPSec(Manual IPSec)**를 선택하여 원격 게이트웨이를 구성합니다.
- 6 IPSec 구성 대화상자에서 **게이트웨이(Gateways)**를 클릭하여 IPSec 원격 게이트웨이를 구성합니다.
- 7 IPSec 구성 대화상자에서 **터널(Tunnels)**을 클릭하여 터널을 구성합니다.

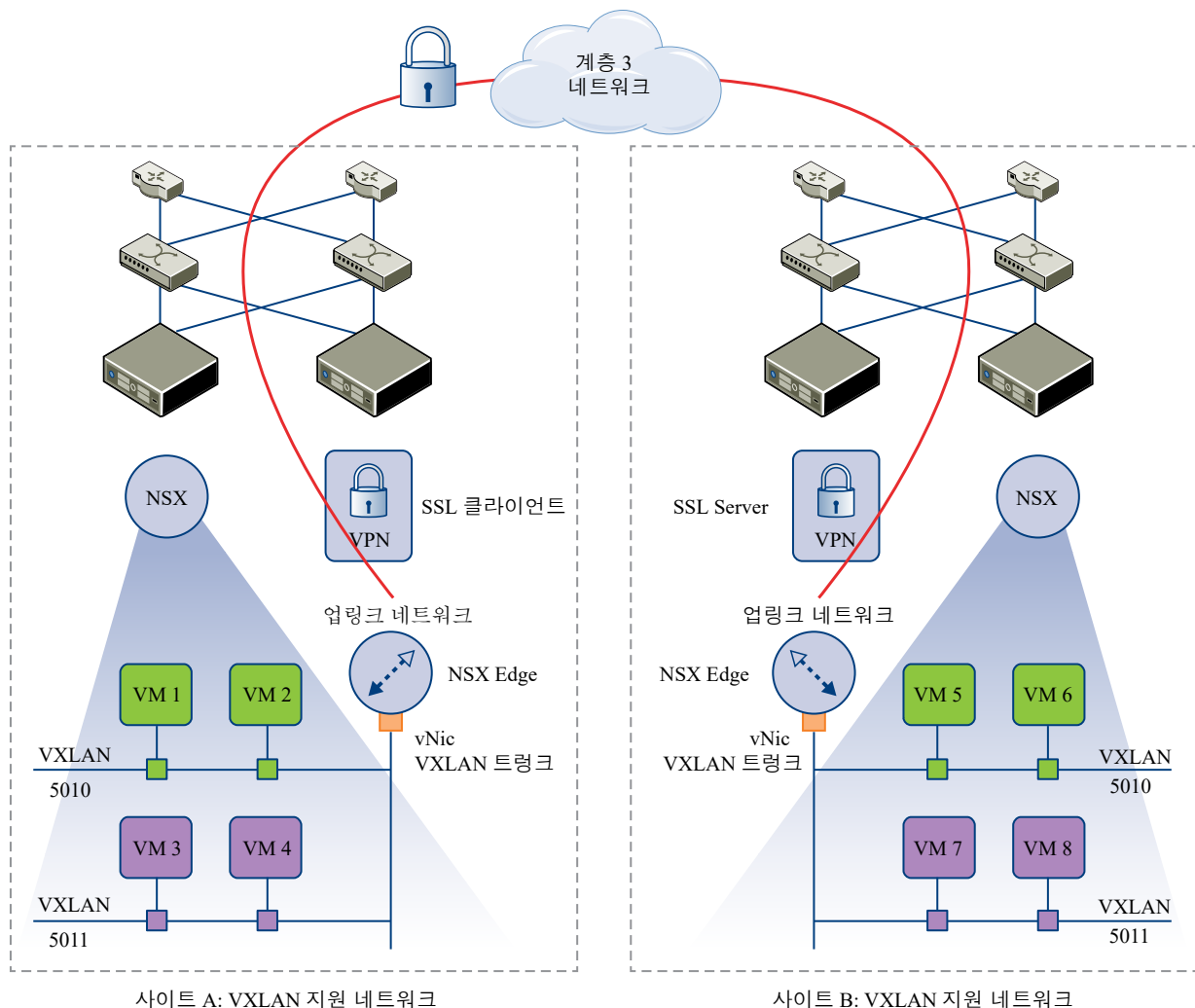
- 8 IPsec 구성 대화상자에서 **추가(Add)**를 클릭하여 라우팅 정책을 추가합니다.
- 9 **닫기(Close)**를 클릭합니다.
- 10 터널이 작동되는지 확인합니다.

L2 VPN 개요

L2 VPN을 사용하면 여러 논리적 네트워크(VLAN과 VXLAN 모두)를 지리적 사이트 경계를 넘어 확장할 수 있습니다. 또한 L2 VPN 서버에서 여러 사이트를 구성할 수 있습니다. 가상 시스템은 사이트 간에 이동할 때 동일한 서브넷에 남아 있으며 해당 IP 주소는 바뀌지 않습니다. 송신 최적화를 통해 Edge는 모든 패킷을 송신 최적화 IP 주소에 로컬로 전송하고 다른 모든 것을 브리지할 수 있습니다.

따라서 **L2 VPN**을 사용하는 엔터프라이즈는 **VXLAN** 또는 **VLAN**으로 지원되는 워크로드를 물리적으로 분리된 위치 간에 원활하게 마이그레이션할 수 있습니다. 클라우드 제공자의 경우 **L2 VPN**은 워크로드 및 애플리케이션에 대한 기존 **IP** 주소를 수정하지 않고 온보드 테넌트를 수용하는 메커니즘을 제공합니다.

그림 14-2. L2 VPN을 사용하여 VXLAN을 여러 사이트로 확장

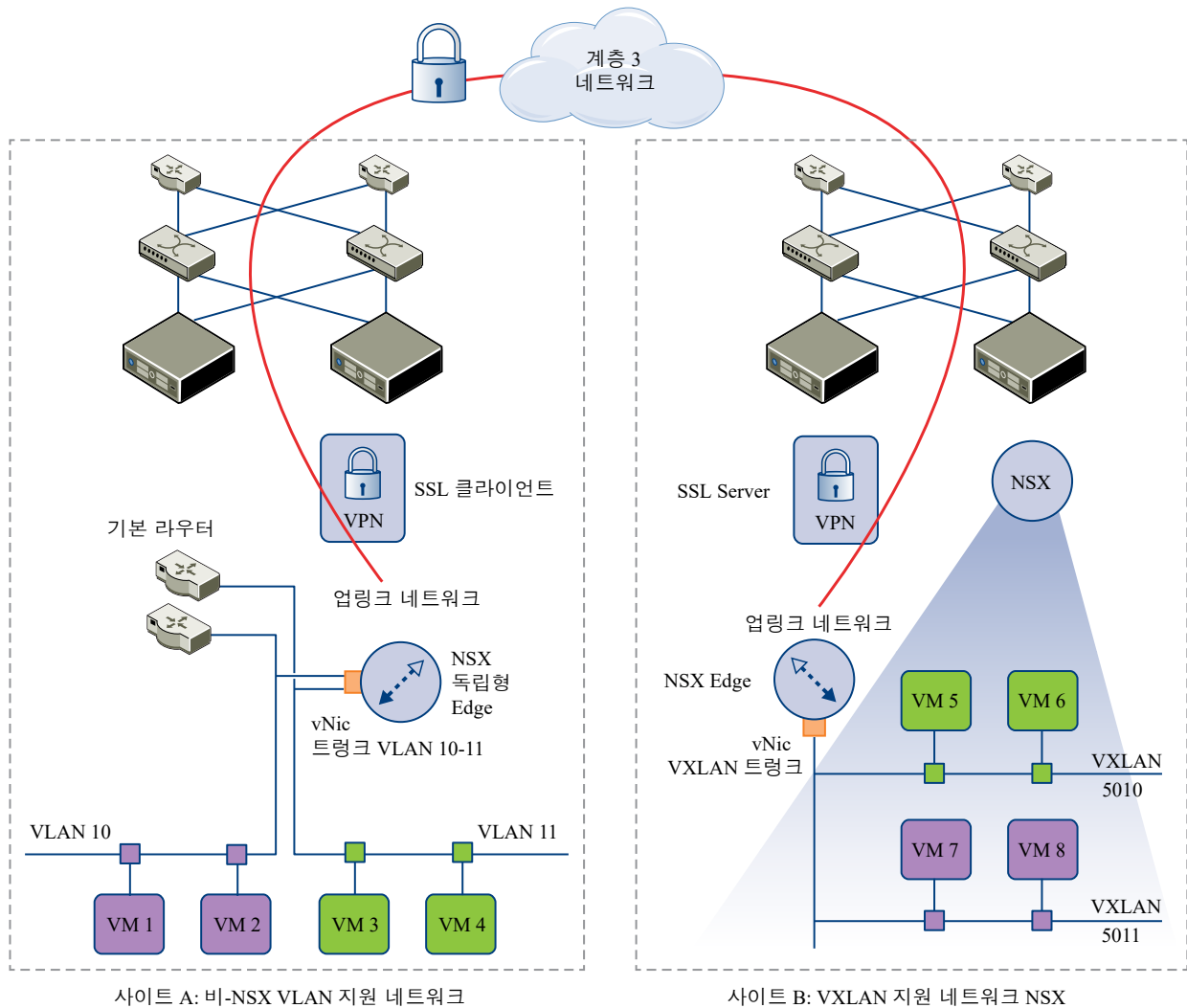


L2 VPN 클라이언트 및 서버는 각각을 통과하는 트래픽에 기반하여 로컬 사이트와 원격 사이트 모두에서 MAC 주소를 인식합니다. 모든 가상 시스템의 기본 게이트웨이는 항상 방화벽 규칙을 사용하여 로컬 게이트웨이로 확인되기 때문에 송신 최적화는 로컬 라우팅을 유지합니다. 사이트 B로 이동된 가상 시스템은 사이트 A에서 확장되지 않은 L2 세그먼트에도 액세스할 수 있습니다.

사이트 중 하나가 NSX로 지원되지 않는 경우에는 해당 사이트에 독립형 NSX Edge를 배포할 수 있습니다.

다음 그래픽에서 L2 VPN은 네트워크 VLAN 10을 VXLAN 5010으로, VLAN 11을 VXLAN 5011로 확장합니다. 따라서 VLAN 10과 브리지된 VM 1은 VM 2, 5 및 6에 액세스할 수 있습니다.

그림 14-3. VLAN 기반 네트워크를 사용하는 비-NSX 사이트를 VXLAN 기반 네트워크를 사용하는 NSX-사이트로 확장



L2 VPN 구성

L2 VPN을 사용하여 네트워크를 확장하려면 L2 VPN 서버(대상 Edge) 및 L2 VPN 클라이언트(소스 Edge)를 구성합니다. 서버 및 클라이언트 모두에서 L2 VPN 서비스를 사용하도록 설정해야 합니다.

사전 요구 사항

하위 인터페이스를 NSX Edge의 트렁크 인터페이스에서 추가했어야 합니다. [하위 인터페이스 추가](#)를 참조하십시오.

L2 VPN 모범 사례

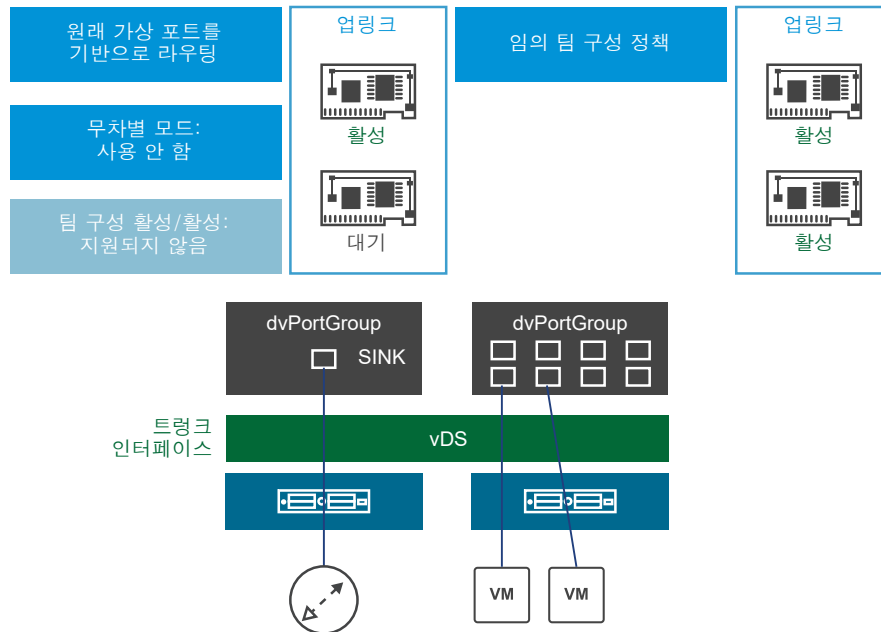
모범 사례에 따라 L2 VPN을 구성하면 반복 및 중복 ping과 중복 응답 등의 문제를 방지할 수 있습니다.

반복을 완화하기 위한 L2VPN 옵션

반복을 완화하기 위한 두 가지 옵션이 있습니다. NSX Edge와 VM을 서로 다른 ESXi 호스트에 배치할 수도 있고 또는 동일한 ESXi 호스트에 배치할 수도 있습니다.

옵션 1: L2VPN Edge용 ESXi 호스트와 VM용 ESXi 호스트 구분

1. 별도 ESXi 호스트에 L2VPN Edge 및 VM 배포



- 1 Edge와 VM을 별도의 ESXi 호스트에 배포합니다.
- 2 다음과 같이 Edge의 트렁크 vNic에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
 - a 로드 밸런싱을 "원래 가상 포트를 기반으로 라우팅"으로 설정합니다.
 - b 업링크 하나만 활성화로 설정하고 나머지 업링크는 대기로 설정합니다.
- 3 다음과 같이 VM에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
 - a 모든 팀 구성 정책이 허용됩니다.
 - b 활성화 업링크를 여러 개 구성할 수 있습니다.

- 4 SINK 포트 모드를 사용하도록 Edge를 구성하고 트렁크 vNic에서 비규칙 모드를 사용하지 않도록 설정합니다.

참고

- 비규칙 모드 사용 안 함: vSphere Distributed Switch를 사용하는 경우
- 비규칙 모드 사용: 가상 스위치를 사용하여 트렁크 인터페이스를 구성하는 경우

가상 스위치의 비규칙 모드가 사용으로 설정된 경우 현재 비규칙 포트에서 사용되지 않는 업링크의 패킷 일부가 삭제되지 않습니다. ReversePathFwdCheckPromisc를 사용하도록 설정했다가 사용하지 않도록 설정하면 비규칙 포트에 대해 현재 사용되지 않은 업링크에서 들어오는 모든 패킷이 명시적으로 삭제됩니다.

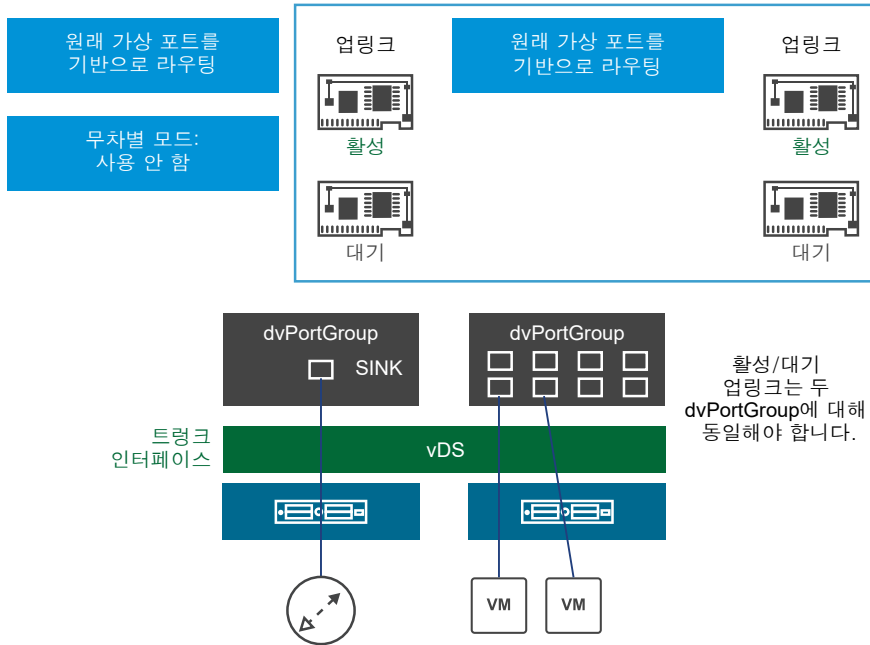
중복된 패킷을 차단하려면 NSX Edge가 있는 ESXi CLI에서 비규칙 모드에 대한 RPF 확인을 활성화합니다.

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
esxcli system settings advanced list -o /Net/ReversePathFwdCheckPromisc
Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value:
Default String Value:
Valid Characters:
Description: Block duplicate packet in a teamed environment when the virtual switch is set to
Promiscuous mode.
```

포트 그룹(PortGroup) 보안 정책에서 비규칙 모드(PromiscuousMode)를 수락(Accept)에서 거부(Reject)로 설정했다가 다시 수락(Accept)으로 설정하여 구성된 변경 사항을 활성화합니다.

- 옵션 2: 동일한 ESXi 호스트의 Edge 및 VM

2. 동일한 호스트에 L2VPN Edge 및 VM 배포



- a 다음과 같이 **Edge**의 트렁크 vNic에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
- 1 로드 밸런싱을 "원래 가상 포트를 기반으로 라우팅"으로 설정합니다.
 - 2 업링크 하나만 활성으로 설정하고 나머지 업링크는 대기로 설정합니다.
- b 다음과 같이 **VM**에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
- 1 모든 팀 구성 정책이 허용됩니다.
 - 2 업링크 중 하나만 활성 상태일 수 있습니다.
 - 3 **VM**의 분산 포트 그룹과 **Edge**의 트렁크 vNic 분산 포트 그룹에 대해 활성/대기 업링크의 순서가 동일해야 합니다.
- c **SINK** 포트 모드를 사용하도록 클라이언트 측 독립형 **Edge**를 구성하고 트렁크 vNic에서 비규칙 모드를 사용하지 않도록 설정합니다.

싱크 포트 구성

NSX 관리 NSX Edge가 L2 VPN 클라이언트로 설정되는 경우 일부 구성이 NSX에서 자동으로 수행됩니다. 독립형 NSX Edge가 L2 VPN 클라이언트로 설정되는 경우에는 이러한 구성 단계를 수동으로 수행해야 합니다.

VPN 사이트 중 하나에 NSX가 배포되지 않은 경우 해당 사이트에 독립형 NSX Edge를 배포하여 L2 VPN을 구성할 수 있습니다. 독립형 Edge는 NSX에서 관리되지 않는 호스트에서 OVF 파일을 사용하여 배포됩니다. 이렇게 하면 Edge Services Gateway 장치가 L2 VPN 클라이언트로 작동하도록 배포됩니다.

독립형 Edge 트렁크 vNIC가 vSphere Distributed Switch에 연결되는 경우 L2 VPN 기능을 위해 비규칙 모드 또는 싱크 포트가 필요합니다. 비규칙 모드를 사용할 경우 중복 ping과 중복 응답을 야기할 수 있습니다. 이러한 이유로 L2 VPN 독립형 NSX Edge 구성에서는 싱크 포트 모드를 사용합니다.

절차

- 1 싱크 포트 구성하려는 트렁크 vNIC에 대한 포트 번호를 검색합니다.
 - a vSphere Web Client에 로그인하고 **홈(Home) > 네트워킹(Networking)**으로 이동합니다.
 - b NSX Edge 트렁크 인터페이스가 연결된 분산 포트 그룹을 클릭하고 **포트(Ports)**를 클릭하여 포트 및 연결된 VM을 확인합니다. 트렁크 인터페이스와 연결된 포트 번호를 기억해 둡니다.
불투명한 데이터를 가져오고 업데이트할 때 이 포트 번호를 사용합니다.
- 2 vSphere Distributed Switch에 대한 dvsUuid 값을 검색합니다.
 - a `https://<vc-ip>/mob`에서 vCenter Mob UI에 로그인합니다.
 - b **컨텐츠(content)**를 클릭합니다.
 - c **rootFolder**에 연결된 링크(예: *group-d1 (Datacenters)*)를 클릭합니다.
 - d **childEntity**에 연결된 링크(예: *datacenter-1*)를 클릭합니다.
 - e **networkFolder**에 연결된 링크(예: *group-n6*)를 클릭합니다.
 - f NSX Edge에 연결된 vSphere Distributed Switch에 대한 DVS 이름 링크(예: *dvs-1 (Mgmt_VDS)*)를 클릭합니다.
 - g UUID 문자열 값을 복사합니다.
불투명한 데이터를 가져오고 업데이트할 때 **dvsUuid**에 대해 이 값을 사용합니다.
- 3 지정된 포트에 대해 불투명 데이터가 있는지를 확인합니다.
 - a `https://<vc-ip>/mob/?moid=DVSManager&vmidl=1`로 이동합니다.
 - b **fetchOpaqueDataEx**를 클릭합니다.
 - c **selectionSet** 값 상자에 다음 XML 입력을 붙여 넣습니다.

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

NSX Edge 트렁크 인터페이스에 대해 검색한 포트 번호 및 **dvsUuid** 값을 사용합니다.

- d **isRuntime**을 **false**로 설정합니다.
- e **메서드 호출(Invoke Method)**을 클릭합니다.

결과에 `vim.dvs.OpaqueData.ConfigInfo`에 대한 값이 표시되며 이미 불투명한 데이터 집합이 있는 경우 싱크 포트를 설정할 때 **edit** 작업을 사용합니다. `vim.dvs.OpaqueData.ConfigInfo`에 대한 값이 비어 있으면 싱크 포트를 설정할 때 **add** 작업을 사용합니다.

4 vCenter MOB(관리 개체 브라우저)에서 싱크 포트를 구성합니다.

- a `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`로 이동합니다.
- b **updateOpaqueDataEx**를 클릭합니다.
- c **selectionSet** 값 상자에 다음 XML 입력을 붙여 넣습니다.

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid --
>
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

vCenter MOB에서 검색한 `dvsUuid` 값을 사용합니다.

- d `opaqueDataSpec` 값 상자에 다음 XML 입력 중 하나를 붙여 넣습니다.

불투명 데이터가 설정되어 있지 않으면(`operation`이 `add`로 설정) 이 입력을 사용하여 싱크 포트를 사용하도록 설정합니다.

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmidl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAA=</opaqueData>
    </opaqueData>
  </opaqueDataSpec>
```

불투명 데이터가 이미 설정되어 있으면(`operation`이 `edit`로 설정) 이 입력을 사용하여 싱크 포트를 사용하도록 설정합니다.

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmidl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAA=</opaqueData>
    </opaqueData>
  </opaqueDataSpec>
```

싱크 포트를 사용하지 않도록 설정하려면 다음 입력을 사용합니다.

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmidl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAA=</opaqueData>
    </opaqueData>
  </opaqueDataSpec>
```

- e `isRuntime`을 `false`로 설정합니다.
- f **메서드 호출(Invoke Method)**을 클릭합니다.

L2 VPN 서버 구성

L2 VPN 서버는 클라이언트가 연결되는 대상 NSX Edge입니다.

절차

- 1 **L2 VPN** 탭에서 **서버 (Server)**를 선택하고 **변경 (Change)**을 클릭합니다.
- 2 **수신기 IP (Listener IP)**에서 **NSX Edge**의 외부 인터페이스에 대한 기본 또는 보조 IP 주소를 입력합니다.
- 3 **L2 VPN** 서비스의 기본 포트는 **443**입니다. 필요한 경우 포트 번호를 편집합니다.
- 4 서버와 클라이언트 간 통신을 위한 암호화 알고리즘을 선택합니다.
- 5 **SSL VPN** 서버에 바인딩되는 인증서를 선택합니다.

중요 SSL을 통한 **L2 VPN** 서비스는 **RSA** 인증서만 지원합니다.

- 6 **확인 (OK)**을 클릭합니다.

피어 사이트 추가

여러 사이트를 **L2 VPN** 서버에 연결할 수 있습니다.

참고 사이트 구성 설정을 변경하면 **NSX Edge**가 기존의 모든 연결을 끊었다가 다시 연결합니다.

절차

- 1 **L2 VPN** 탭에서 **L2 VPN 모드 (L2 VPN Mode)**가 **서버 (Server)**인지 확인합니다.
- 2 **사이트 구성 세부 정보 (Site Configuration Details)**에서 **추가 (Add)** 아이콘을 클릭합니다.
- 3 피어 사이트에 대한 고유한 이름을 입력합니다.
- 4 피어 사이트를 인증할 사용자 이름 및 암호를 입력합니다. 피어 사이트의 사용자 자격 증명은 클라이언트 쪽 사용자 자격 증명과 동일해야 합니다.
- 5 **확장된 인터페이스 (Stretched Interfaces)**에서 **하위 인터페이스 선택 (Select Sub Interfaces)**을 클릭하여 클라이언트와 함께 확장할 하위 인터페이스를 선택합니다.
 - a [개체 선택]에서 **Edge**에 대한 트렁크 인터페이스를 선택합니다.
트렁크 vNIC에 구성된 하위 인터페이스가 표시됩니다.
 - b 확장할 하위 인터페이스를 두 번 클릭합니다.
 - c **확인 (OK)**을 클릭합니다.
- 6 가상 시스템의 기본 게이트웨이가 2개의 사이트에서 동일하면 **송신 최적화 게이트웨이 주소 (Egress Optimization Gateway Address)** 텍스트 상자에 게이트웨이 IP 주소를 입력합니다. 이러한 IP 주소는 트래픽이 로컬로 라우팅되거나 트래픽이 터널을 통과하지 못하게 차단되는 주소입니다.

- 7 (선택 사항) 확장되지 않은 네트워크의 VM이 확장된 네트워크의 L2 VPN 클라이언트 Edge 뒤에 있는 VM과 통신하도록 하려면 **확장되지 않은 네트워크 사용 (Enable Unstretched Networks)** 확인란을 선택합니다. 또한 이 통신이 동일한 L2 VPN 터널을 통해 라우팅되도록 하려면 확장되지 않은 서브넷을 L2 VPN 서버 Edge 또는 L2 VPN 클라이언트 Edge 중 하나의 뒤에 두거나 둘 다의 뒤에 둘 수 있습니다.

예를 들어 NSX L2 VPN 서비스를 사용하여 2개의 데이터 센터 사이트 사이에서 192.168.10.0/24 하위 네트워크를 확장하기 위해 L2 VPN 터널을 생성했다고 가정합니다.

L2 VPN 서버 Edge 뒤에 2개의 추가 서브넷(예: 192.168.20.0/24 및 192.168.30.0/24)을 둡니다. 확장되지 않은 네트워크를 사용하도록 설정한 경우 192.168.20.0/24 및 192.168.30.0/24 서브넷의 VM은 확장된 네트워크의 L2 VPN 클라이언트 Edge 뒤에 있는 VM(192.168.10.0/24)과 통신할 수 있습니다. 이 통신은 동일한 L2 VPN 터널을 통해 라우팅됩니다.

- 8 확장되지 않은 네트워크를 사용하도록 설정한 경우 확장되지 않은 서브넷이 있는 위치에 따라 다음 단계를 수행합니다.
- 확장되지 않은 서브넷이 L2 VPN 클라이언트 Edge 뒤에 있는 경우 L2 VPN 서버 Edge에서 피어(클라이언트) 사이트를 추가하는 동안 확장되지 않은 네트워크의 네트워크 주소를 CIDR 형식으로 입력합니다. 확장되지 않은 다중 네트워크를 입력하려면 네트워크 주소를 쉼표로 구분합니다.
 - 확장되지 않은 서브넷이 L2 VPN 서버 Edge 뒤에 있는 경우 **확장되지 않은 네트워크 (Unstretched Networks)** 텍스트 상자를 비워둡니다. 즉, L2 VPN 서버에서 클라이언트(피어) 사이트를 추가하는 동안 확장되지 않은 네트워크의 네트워크 주소를 입력하지 마십시오.
- 이전 예에서 확장되지 않은 서브넷이 L2 VPN 서버 Edge 뒤에 있기 때문에 **피어 사이트 추가** 창에서 **확장되지 않은 네트워크 (Unstretched Networks)** 텍스트 상자를 비워 두어야 합니다.

- 9 **확인 (OK)**를 클릭하고 **변경 내용 게시 (Publish Changes)**를 클릭합니다.

서버에서 L2 VPN 서비스 사용

L2 VPN 서버(대상 NSX Edge)에서 L2 VPN 서비스를 사용하도록 설정해야 합니다. 이 Edge Appliance에 HA가 이미 구성된 경우 Edge에 둘 이상의 내부 인터페이스가 구성되어 있는지 확인하십시오. 이미 HA에서 사용한 단일 인터페이스만 있는 경우 동일한 내부 인터페이스의 L2 VPN 구성이 실패합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 대상 NSX Edge를 두 번 클릭하고 **관리(Manage) > VPN > L2 VPN**으로 이동합니다.
- 4 **L2 VPN 서비스 상태(L2 VPN Service Status)** 옆에 있는 **시작(Start)**을 클릭합니다.

다음에 수행할 작업

방화벽 쪽에 연결된 인터넷에서 NAT 또는 방화벽 규칙을 생성하여 클라이언트 및 서버가 서로 연결할 수 있도록 합니다.

L2 VPN 클라이언트 구성

L2 VPN 클라이언트는 대상 Edge(L2 VPN 서버)와 통신을 시작하는 소스 NSX Edge입니다.

독립 실행형 Edge를 L2 VPN 클라이언트로 구성할 수도 있습니다. [독립형 Edge를 L2 VPN 클라이언트로 구성](#)을 참조하십시오.

절차

- 1 L2 VPN 탭에서 **L2 VPN 모드 (L2 VPN Mode)**를 **클라이언트 (Client)**로 설정하고 **변경 (Change)**을 클릭합니다.
- 2 클라이언트가 연결될 L2 VPN 서버의 주소를 입력합니다. 이 주소로 호스트 이름 또는 IP 주소를 지정할 수 있습니다.
- 3 필요한 경우 L2 VPN 클라이언트가 연결되어야 하는 기본 포트를 편집합니다.
- 4 서버와의 통신에 대한 암호화 알고리즘을 선택합니다.
- 5 **확장된 인터페이스 (Stretched Interfaces)**에서 **하위 인터페이스 선택 (Select Sub Interfaces)**을 클릭하여 서버로 확장할 하위 인터페이스를 선택합니다.
 - a **개체 선택 (Select Object)**에서 Edge에 대한 트렁크 인터페이스를 선택합니다.
트렁크 vNIC에 구성된 하위 인터페이스가 표시됩니다.
 - b 확장할 하위 인터페이스를 두 번 클릭합니다.
 - c **확인 (OK)**을 클릭합니다.
- 6 설명을 입력합니다.
- 7 **송신 최적화 게이트웨이 주소 (Egress Optimization Gateway Address)**에서 하위 인터페이스의 게이트웨이 IP 주소 또는 트래픽이 터널을 통해 흐르지 않아야 할 IP 주소를 입력합니다.
- 8 (선택 사항) 확장되지 않은 네트워크의 VM이 확장된 네트워크의 L2 VPN 서버 Edge 뒤에 있는 VM과 통신하도록 하려면 **확장되지 않은 네트워크 사용 (Enable Unstretched Networks)** 확인란을 선택합니다. 또한 이 통신이 동일한 L2 VPN 터널을 통해 라우팅되도록 하려면 확장되지 않은 서브넷을 L2 VPN 서버 Edge 또는 L2 VPN 클라이언트 Edge 중 하나의 뒤에 두거나 둘 다의 뒤에 둘 수 있습니다.

예를 들어 NSX L2 VPN 서비스를 사용하여 2개의 데이터 센터 사이트 사이에서 192.168.10.0/24 하위 네트워크를 확장하기 위해 L2 VPN 터널을 생성했다고 가정합니다.

L2 VPN 서버 Edge 뒤에 2개의 추가 서브넷(예: 192.168.20.0/24 및 192.168.30.0/24)을 둡니다. 확장되지 않은 네트워크를 사용하도록 설정한 경우 192.168.20.0/24 및 192.168.30.0/24 서브넷의 VM은 확장된 네트워크의 L2 VPN 서버 Edge 뒤에 있는 VM(192.168.10.0/24)과 통신할 수 있습니다. 이 통신은 동일한 L2 VPN 터널을 통해 라우팅됩니다.

9 확장되지 않은 네트워크를 사용하도록 설정한 경우 확장되지 않은 서브넷이 있는 위치에 따라 다음 단계를 수행합니다.

- 확장되지 않은 서브넷이 L2 VPN 서버 Edge 뒤에 있는 경우 L2 VPN 클라이언트 Edge를 구성하는 동안 확장되지 않은 네트워크의 네트워크 주소를 CIDR 형식으로 입력합니다. 확장되지 않은 다중 네트워크를 입력하려면 네트워크 주소를 쉼표로 구분합니다.
- 확장되지 않은 서브넷이 L2 VPN 클라이언트 Edge 뒤에 있는 경우 **확장되지 않은 네트워크 (Unstretched Networks)** 텍스트 상자를 비워둡니다. 즉, L2 VPN 클라이언트 Edge에 있는 확장되지 않은 네트워크의 네트워크 주소는 입력하지 마십시오.

이전 예제에서는 확장되지 않은 서브넷이 L2 VPN 서버 Edge 뒤에 있으므로 L2 VPN 클라이언트 Edge를 구성하는 동안 확장되지 않은 네트워크를 **192.168.20.0/24, 192.168.30.0/24**로 입력해야 합니다.

10 사용자 세부 정보 (User Details)에서 서버에서 인증할 사용자 자격 증명을 입력합니다.

11 고급 (Advanced) 탭을 클릭합니다.

클라이언트 NSX Edge가 인터넷에 직접 액세스할 수 없지만 프록시 서버를 통해 소스(서버) NSX Edge에 연결해야 하는 경우 **프록시 설정 (Proxy Settings)**을 지정합니다.

12 보안 프록시 연결만 사용하려면 **보안 프록시 사용 (Enable Secure Proxy)**을 선택합니다.

13 프록시 서버 주소, 포트, 사용자 이름 및 암호를 입력합니다.

14 서버 인증서 검증을 사용하도록 설정하려면 **서버 인증서 확인 (Validate Server Certificate)**을 선택한 후 적절한 CA 인증서를 선택합니다.

15 **확인 (OK)**을 클릭하고 **변경 내용 게시 (Publish Changes)**를 클릭합니다.

다음에 수행할 작업

방화벽에 연결되는 인터넷이 L2 VPN Edge에서 인터넷으로 트래픽 흐름을 허용하는지 확인합니다. 대상 포트는 443입니다.

클라이언트에서 L2 VPN 서비스 사용

L2 VPN 클라이언트(소스 NSX Edge)에서 L2 VPN 서비스를 사용하도록 설정해야 합니다.

절차

1 소스 NSX Edge의 경우 **관리(Manage) > VPN > L2 VPN**으로 이동합니다.

2 **L2 VPN 서비스 상태(L2 VPN Service Status)** 옆에 있는 **시작(Start)**을 클릭합니다.

다음에 수행할 작업

- 클라이언트와 서버가 서로 연결할 수 있도록 설정하려면 인터넷 연결 방화벽 측에서 **NAT** 또는 방화벽 규칙을 생성합니다.

- 표준 포트 그룹에서 지원하는 트렁크 vNic를 확장할 경우 다음 단계를 수행하여 L2 VPN 트래픽을 수동으로 사용하도록 설정합니다.

a 무차별 모드(Promiscuous mode)를 수락(Accept)으로 설정합니다.

b 위조 전송(Forged Transmits)을 수락(Accept)으로 설정합니다.

무차별 모드 작업 및 위조 전송에 대한 자세한 내용은 VMware vSphere® 설명서에서 "vSphere Standard 스위치 보안을 참조하십시오.

독립형 Edge를 L2 VPN 클라이언트로 구성

확장할 사이트 중 하나를 NSX에서 지원하지 않을 경우 해당 사이트에서 독립형 Edge를 L2 VPN 클라이언트로 배포할 수 있습니다.

독립 실행형 Edge에 대해 FIPS 모드를 변경하려면 `fips enable` 또는 `fips disable` 명령을 사용하십시오. 자세한 내용은 "NSX 명령줄 인터페이스 참조"를 참조하십시오.

사전 요구 사항

독립형 Edge가 연결되는 트렁크 인터페이스의 트렁크 포트 그룹을 생성했습니다. 이 포트 그룹에는 약간의 수동 구성이 필요합니다.

- 트렁크 포트 그룹이 vSphere 표준 스위치에 있으면 다음 작업을 수행해야 합니다.

- 위조 전송을 사용하도록 설정합니다.

- 비규칙 모드를 사용하도록 설정합니다.

"vSphere 네트워킹 가이드"를 참조하십시오.

- 트렁크 포트 그룹이 vSphere Distributed Switch에 있으면 다음 작업을 수행해야 합니다.

- 위조 전송을 사용하도록 설정합니다. "vSphere 네트워킹 가이드"를 참조하십시오.

- 트렁크 vNic에 대해 싱크 포트를 사용하도록 설정하거나 비규칙 모드를 사용하도록 설정합니다. 싱크 포트를 사용하도록 설정하는 것이 좋습니다.

Edge 트렁크 vNIC에 연결된 포트의 구성을 변경해야 하므로 독립형 Edge를 배포한 후 싱크 포트를 구성해야 합니다.

절차

- 1 vSphere Web Client를 사용하여 비 NSX 환경을 관리하는 vCenter Server에 로그인합니다.
- 2 **호스트 및 클러스터(Hosts and Clusters)**를 선택하고 클러스터를 확장하여 사용 가능한 호스트를 표시합니다.
- 3 독립 실행형 Edge를 설치할 호스트를 마우스 오른쪽 버튼으로 클릭하고 **OVF 템플릿 배포(Deploy OVF Template)**를 선택합니다.
- 4 인터넷에서 OVF 파일을 다운로드하고 설치할 URL을 입력하거나 **찾아보기(Browse)**를 클릭하여 컴퓨터에서 독립 실행형 Edge OVF 파일이 있는 컴퓨터의 폴더를 찾은 후 **다음(Next)**을 클릭합니다.

- 5 [OVF 템플릿 세부 정보] 페이지에서 템플릿 세부 정보를 확인하고 **다음(Next)**을 클릭합니다.
- 6 [이름 및 폴더 선택] 페이지에서 독립형 **Edge** 이름을 입력하고 배포할 폴더 또는 데이터센터를 선택합니다. **다음(Next)**을 클릭합니다.
- 7 [스토리지 선택] 페이지에서 배포한 템플릿의 파일을 저장할 위치를 선택합니다.
- 8 [네트워크 선택] 페이지에서 배포한 템플릿이 사용할 네트워크를 구성합니다. **다음(Next)**을 클릭합니다.
 - 공용 인터페이스는 업링크 인터페이스입니다.
 - 트렁크 인터페이스는 확장할 네트워크의 하위 인터페이스를 생성하는 데 사용됩니다. 이 인터페이스를 생성한 트렁크 포트 그룹에 연결합니다.
- 9 [템플릿 사용자 지정] 페이지에서 다음 값을 지정합니다.
 - a CLI 관리자 암호를 입력하고 한 번 더 입력합니다.
 - b CLI 사용 암호를 입력하고 한 번 더 입력합니다.
 - c CLI 루트 암호를 입력하고 한 번 더 입력합니다.
 - d 업링크 IP 주소와 접두사 길이를 입력하고 필요한 경우 기본 게이트웨이 및 DNS IP 주소를 입력합니다.
 - e 인증에 사용할 암호를 선택합니다. L2VPN 서버에서 사용되는 암호와 일치해야 합니다.
 - f 송신 최적화를 사용하도록 설정하려면 트래픽이 로컬에서 라우팅되거나 트래픽이 터널에서 차단되어야 하는 게이트웨이 IP 주소를 입력합니다.
 - g L2 VPN 서버 주소 및 포트를 입력합니다.
 - h 피어 사이트를 인증할 사용자 이름 및 암호를 입력합니다.
 - i 하위 인터페이스 VLAN(터널 ID)에 확장할 네트워크의 VLAN ID를 입력합니다. VLAN ID를 쉼표로 구분된 목록 또는 범위로 나열할 수 있습니다. 예를 들면, 2,3,10-20입니다.
 네트워크를 독립 실행형 Edge 사이트로 확장하기 전에 네트워크의 VLAN ID를 변경할 경우 네트워크의 VLAN ID를 입력한 다음 괄호 안에 터널 ID를 입력할 수 있습니다. 예를 들면, 2(100),3(200)입니다. 터널 ID를 사용하여 확장할 네트워크를 매핑합니다. 그러나 범위를 사용하여 터널 ID를 지정할 수 없습니다. 따라서 10(100)-14(104)는 허용되지 않습니다. 이를 10(100),11(101),12(102),13(103),14(104) 같이 다시 적성해야 합니다.
 - j 독립 실행형 NSX Edge가 인터넷에 직접 액세스할 수 없지만 프록시 서버를 통해 소스(서버) NSX Edge에 연결해야 하는 경우 프록시 주소, 포트, 사용자 이름 및 암호를 입력합니다.
 - k 루트 CA를 사용할 수 있을 경우 인증서 섹션에 붙여 넣습니다.
 - l **다음(Next)**을 클릭합니다.
- 10 [완료 준비] 페이지에서 독립 실행형 Edge 설정을 검토하고 **완료(Finish)**를 클릭합니다.

다음에 수행할 작업

독립 실행형 Edge 가상 시스템의 전원을 켭니다.

트렁크 vNIC 포트 번호를 기록하고 싱크 포트를 구성합니다. [싱크 포트 구성](#)을 참조하십시오.

독립형 Edge 명령줄 인터페이스를 사용하여 추가 구성을 변경합니다. "NSX 명령줄 인터페이스 참조"를 참조하십시오.

L2 VPN 통계 보기

L2 VPN 서버 및 클라이언트 Edge 둘 다에서 터널 상태, 송신 및 수신된 바이트 및 기타 통계 등의 L2 VPN 터널 통계를 볼 수 있습니다.

절차

- 1 L2 VPN 클라이언트 Edge에 대한 통계를 봅니다.
 - a L2 VPN 클라이언트 모드에서 구성된 NSX Edge를 두 번 클릭합니다.
 - b **관리 > VPN > L2 VPN**으로 이동합니다.
 - c **터널 상태** 섹션을 확장하고 **새로 고침** 아이콘을 클릭하여 터널 통계를 확인합니다.
- 2 L2 VPN 서버 Edge에 대한 통계를 봅니다.
 - a L2 VPN 서버 모드에서 구성된 NSX Edge를 두 번 클릭합니다.
 - b **L2 VPN** 페이지로 이동합니다.
 - c **사이트 구성 세부 정보** 섹션에서 **L2VPN 통계 표시(Show L2VPN Statistics)** 링크를 클릭합니다.

L2 VPN 서버에 구성된 모든 피어 사이트의 통계가 표시됩니다.

다음에 수행할 작업

트렁크 인터페이스에 구성된 네트워크를 보려면, Edge의 **관리(Manage) > 설정(Settings) > 인터페이스(Interfaces)**로 이동하여 유형 열의 **트렁크(Trunk)**를 클릭합니다.

확장된 VLAN 제거

L2VPN은 지리적 사이트에 걸쳐 여러 논리적 네트워크를 확장할 수 있습니다.

확장된 다른 VLAN에 영향을 주지 않고 L2 VPN Edge에서 확장된 VLAN을 제거하려면 먼저 VLAN을 제거하고 L2 VPN 클라이언트(소스 NSX Edge) 및 L2 VPN 서버(대상 NSX Edge)에서 하위 인터페이스를 제거합니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)** 탭을 클릭한 다음 **VPN > L2VPN**으로 이동합니다.

- 4 사이트 구성 세부 정보, 확장된 인터페이스에서 하위 인터페이스와 연결된 VLAN을 제거합니다.
- 5 **L2 VPN 모드(L2 VPN Mode)**를 **클라이언트(Client)**로 설정하고 이 VLAN에 대한 하위 인터페이스를 제거합니다.
- 6 **L2 VPN 모드(L2 VPN Mode)**를 **서버(Server)**로 설정하고 이 VLAN에 대한 하위 인터페이스를 제거합니다.
- 7 변경 내용을 게시합니다.

논리적 로드 밸런서

15

NSX Edge 로드 밸런서를 사용하여고가용성 서비스를 사용할 수 있으며 여러 서버에 네트워크 트래픽 로드를 분산할 수 있습니다. 즉, 로드 분산이 사용자에게 투명하게 진행되도록 들어오는 서비스 요청을 여러 서버 간에 균일하게 분산합니다. 따라서 로드 밸런싱은 리소스 활용도를 최적화하고, 처리량을 극대화하며, 응답 시간을 최소화하고, 오버로드를 방지하는 데 도움이 됩니다. NSX Edge에서는 계층 7까지 로드 밸런싱을 제공합니다.

로드 밸런싱을 위해 외부 또는 공용 IP 주소를 내부 서버 집합에 매핑합니다. 로드 밸런서는 외부 IP 주소에 대한 TCP, UDP, HTTP 또는 HTTPS 요청을 수락하고 사용할 내부 서버를 결정합니다. 포트 80은 HTTP의 기본 포트이고, 포트 443은 HTTPS의 기본 포트입니다.

작동하는 NSX Edge 인스턴스가 있어야 로드 밸런싱을 구성할 수 있습니다. NSX Edge 설정에 대한 자세한 내용은 [NSX Edge 구성](#) 항목을 참조하십시오.

NSX Edge 인증서 구성에 대한 자세한 내용은 [인증서 사용](#) 항목을 참조하십시오.

NSX 로드 밸런싱 기능은 다음과 같습니다.

- 프로토콜: TCP, UDP, HTTP, HTTPS
- 알고리즘: 가중 라운드 로빈, IP 해시, URI, 최소 연결
- AES-NI 가속을 사용한 SSL 종료
- SSL 브리징(클라이언트 측 SSL + 서버 측 SSL)
- SSL 인증서 관리
- 클라이언트 식별을 위한 X 헤더 전달
- L4/L7 투명 모드
- 연결 조절
- 유지 보수를 위해 개별 서버 사용/사용 안 함(풀 멤버)
- 상태 점검 메서드(TCP, UDP, HTTP, HTTPS)
- 향상된 상태 점검 모니터
- 지속성/고정 메서드: SourceIP, MSRD, COOKIE, SSLSESSIONID

- 단일 암 모드
- 인라인 모드
- URL 다시 쓰기 및 리디렉션
- 고급 트래픽 관리를 위한 애플리케이션 규칙
- L7 프록시 로드 밸런싱에 대한 HA 세션 고정 지원
- IPv6 지원
- 문제 해결을 위한 향상된 로드 밸런서 CLI
- 모든 크기의 NSX Edge 서비스 게이트웨이에서 사용 가능하며, 프로덕션 트래픽의 경우에는 대형 또는 초대형이 권장됨

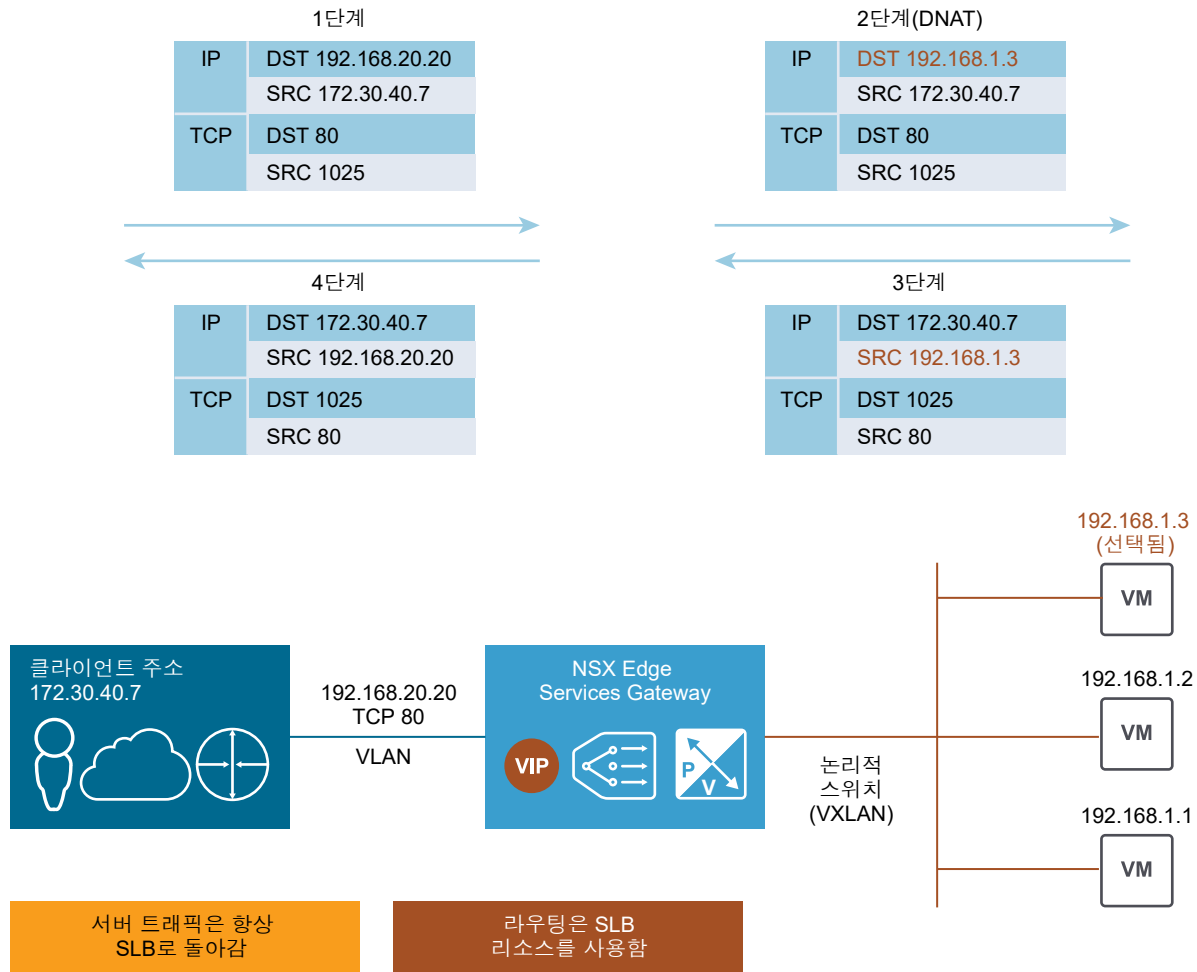
토폴로지

NSX에서 구성하는 로드 밸런싱 서비스에는 2가지 유형이 있습니다. 하나는 프록시 모드로도 알려져 있는 단일 암 모드이고, 다른 하나는 투명 모드로도 알려져 있는 인라인 모드입니다.

NSX 논리적 로드 밸런싱: 인라인 토폴로지

인라인 또는 투명 모드는 서버 팜으로 전달될 트래픽으로 NSX Edge를 인라인으로 배포합니다. 투명 모드 트래픽 흐름은 다음과 같이 처리됩니다.

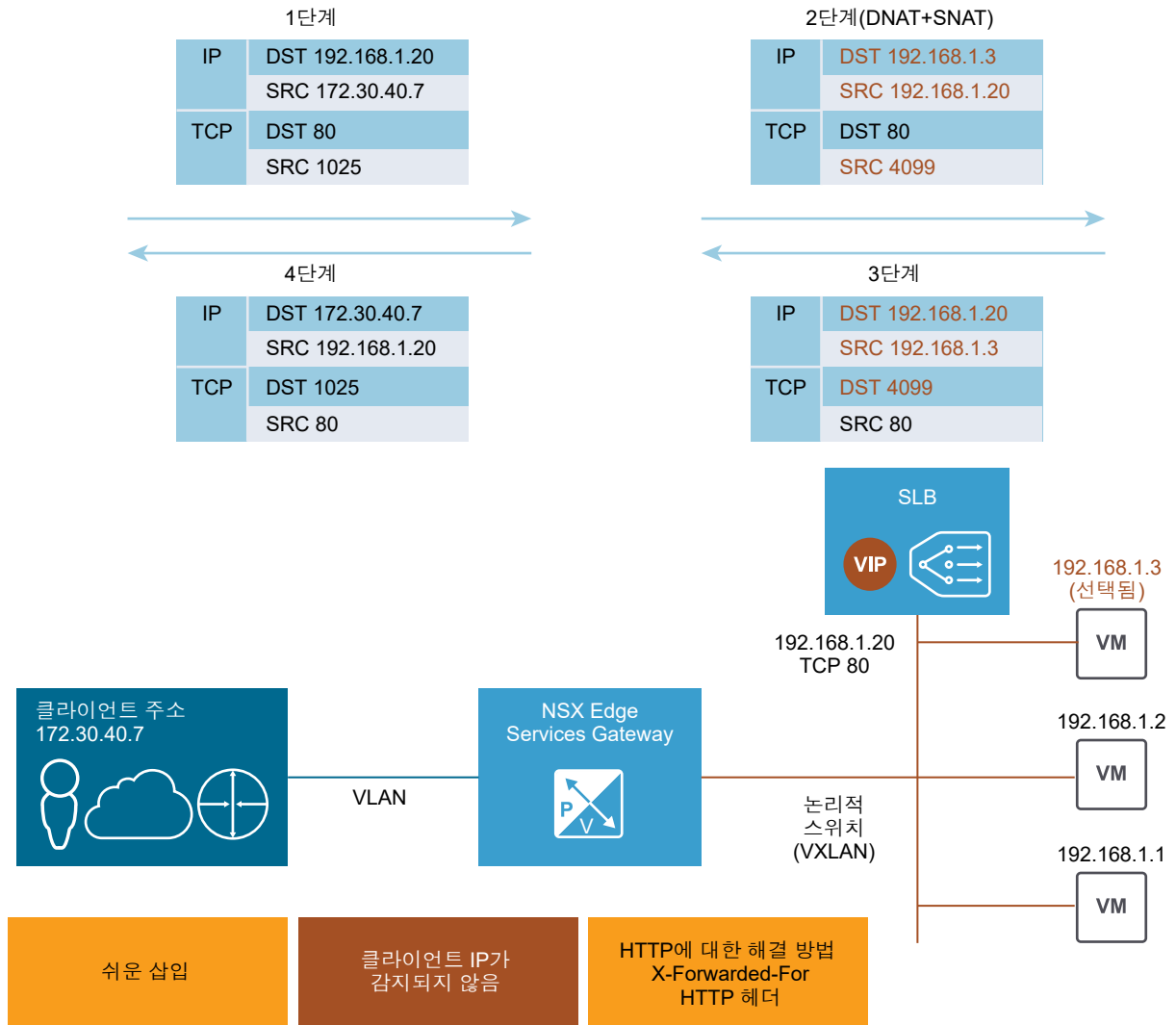
- 외부 클라이언트는 로드 밸런서가 노출하는 VIP(가상 IP 주소)로 트래픽을 전송합니다.
- 중앙 집중식 NSX Edge인 로드 밸런서는 DNAT(대상 NAT)만 수행하여 VIP를 서버 팜에 배포된 서버 중 하나의 IP 주소로 교체합니다.
- 서버 팜의 서버는 원본 클라이언트 IP 주소에 응답합니다. 트래픽은 인라인으로 배포되므로 일반적으로 서버 팜에 대한 기본 게이트웨이로서 로드 밸런서에 다시 수신됩니다.
- 로드 밸런서는 소스 NAT를 수행하여 외부 클라이언트로 트래픽을 전송하고 해당 VIP를 소스 IP 주소로 활용합니다.



NSX 논리적 로드 밸런싱: 단일 암 토폴로지

단일 암 또는 프록시 모드는 로드 밸런싱 서비스가 필요한 논리적 네트워크에 직접 연결된 NSX Edge를 배포하는 과정으로 구성됩니다.

- 외부 클라이언트는 로드 밸런서가 노출하는 VIP(가상 IP 주소)로 트래픽을 전송합니다.
- 로드 밸런서는 클라이언트에서 수신된 원본 패킷에 대해 2가지 주소 변환을 수행합니다. 하나는 서버 팜에 배포된 서버 중 하나의 IP 주소와 VIP를 교체하기 위한 DNAT(대상 NAT)이고, 다른 하나는 클라이언트 IP 주소를 로드 밸런서 자체를 식별하는 IP 주소로 교체하기 위한 SNAT(소스 NAT)입니다. SNAT는 서버 팜에서 클라이언트로의 반환 트래픽이 강제로 로드 밸런서를 통과하도록 하는 데 필요합니다.
- 서버 팜의 서버는 SNAT 기능에 따라 로드 밸런서로 트래픽을 전송하여 응답합니다.
- 로드 밸런서는 다시 소스 및 대상 NAT 서비스를 수행하여 외부 클라이언트로 트래픽을 전송하고 해당 VIP를 소스 IP 주소로 활용합니다.



본 장은 다음 항목을 포함합니다.

- 로드 밸런싱 설정

- 애플리케이션 프로파일 관리
- 서비스 모니터 관리
- 서버 풀 관리
- 가상 서버 관리
- 애플리케이션 규칙 관리
- NTLM 인증을 사용하는 로드 밸런스 웹 서버
- 로드 밸런서 HTTP 연결 모드
- NSX 로드 밸런서 구성 시나리오

로드 밸런싱 설정

NSX Edge 로드 밸런서는 여러 서버에 네트워크 트래픽을 분산시켜 최적의 리소스 사용을 달성하고, 중복성을 제공하고, 리소스 활용률을 분산시킵니다.

NSX 로드 밸런서는 계층 4 및 계층 7 로드 밸런싱 엔진을 지원합니다. 계층 4 로드 밸런서는 패킷 기반으로, 빠른 경로 처리를 제공하고, 계층 7 로드 밸런서는 소켓 기반으로, 백엔드 서비스에 대한 고급 트래픽 조작 및 DDOS 완화를 허용합니다.

패킷 기반의 로드 밸런싱은 TCP 및 UDP 계층에서 구현됩니다. 패킷 기반의 로드 밸런싱은 연결을 중지하거나 전체 요청을 버퍼링하지 않으며, 패킷을 조작한 후에 선택된 서버로 패킷을 직접 전송합니다. TCP 및 UDP 세션은 단일 세션에 대한 패킷이 동일한 서버로 전달되도록 로드 밸런서에서 유지됩니다. 패킷 기반 로드 밸런싱을 사용하도록 설정하기 위해 글로벌 구성 및 해당 가상 서버 구성 둘 다에서 [가속 사용]을 선택할 수 있습니다.

소켓 기반 로드 밸런싱은 소켓 인터페이스 위에서 구현됩니다. 단일 요청에 대해 클라이언트 쪽 연결과 서버 쪽 연결의 두 연결이 설정됩니다. 서버 쪽 연결은 서버를 선택한 후에 설정됩니다. HTTP 소켓 기반 구현의 경우 선택 사항인 L7 조작을 통해 전체 요청이 선택한 서버로 전송되기 전에 수신됩니다. HTTPS 소켓 기반 구현의 경우 클라이언트 쪽 연결 또는 서버 쪽 연결에서 인증 정보가 교환됩니다. 소켓 기반 로드 밸런싱은 TCP, HTTP 및 HTTPS 가상 서버의 기본 모드입니다.

NSX 로드 밸런서의 핵심 개념에는 다음이 포함됩니다.

가상 서버

IP, 포트, 프로토콜 및 애플리케이션 프로파일의 고유 조합(예: TCP 또는 UDP)으로 나타내는 애플리케이션 서비스를 추상화한 것입니다.

서버 풀

백엔드 서버의 그룹입니다.

서버 풀 멤버

백엔드 서버를 풀의 멤버로 나타냅니다.

서비스 모니터

백엔드 서버의 상태를 입증하는 방법을 정의합니다.

애플리케이션 프로파일

지정된 애플리케이션에 대한 TCP, UDP, 지속성 및 인증서 구성을 나타냅니다.

먼저 로드 밸런서에 대한 전역 옵션을 설정하여 시작하고 백엔드 서버 멤버의 서버 풀을 생성한 후 서비스 모니터를 해당 풀에 연결하여 백엔드 서버를 효율적으로 관리하고 공유합니다.

그런 다음 애플리케이션 프로파일을 생성하여 클라이언트 SSL, 서버 SSL, x-forwarded-for 또는 지속성과 같은 로드 밸런서의 일반적인 애플리케이션 동작을 정의합니다. 지속성은 로드 밸런싱 알고리즘을 실행하지 않고 동일한 풀 멤버로 발송되어야 하는 비슷한 특성(예: 소스 IP 또는 쿠키)을 포함하는 후속 요청을 전송합니다. 가상 서버 간에 애플리케이션 프로파일을 다시 사용할 수 있습니다.

그런 다음 트래픽 조작에 대해 요청별로 다른 풀에서 처리될 수 있게 특정 URL 또는 호스트 이름을 일치시키는 것과 같은 애플리케이션별 설정을 구성하는 선택적 애플리케이션 규칙을 생성합니다. 그다음으로 애플리케이션에 관련된 서비스 모니터를 생성하거나 이전에 생성한 서비스 모니터를 사용합니다.

경우에 따라 L7 가상 서버의 고급 기능을 지원하기 위한 애플리케이션 규칙을 생성할 수 있습니다. 애플리케이션 규칙의 일부 사용 사례에는 콘텐츠 스위칭, 헤더 조작, 보안 규칙 및 DOS 보호가 포함됩니다.

마지막으로 서버 풀, 애플리케이션 프로파일 및 잠재적 애플리케이션 규칙을 연결하는 가상 서버를 생성합니다.

가상 서버가 요청을 수신하면 로드 밸런싱 알고리즘에서는 풀 멤버 구성 및 런타임 상태를 고려합니다. 그런 다음 알고리즘에서 해당 풀을 계산하여 하나 이상의 멤버로 구성되는 트래픽을 분산합니다. 풀 멤버 구성에는 가중치, 최대 연결 및 조건 상태와 같은 설정이 포함됩니다. 런타임 상태에는 현재 연결, 응답 시간 및 상태 검사 상태 정보가 포함됩니다. 계산 방법에는 라운드 로빈, 가중 라운드 로빈, 최소 연결, 소스 IP 해시, 가중 최소 연결, URL, URI 또는 HTTP 헤더가 있을 수 있습니다.

각 풀은 연결된 서비스 모니터에 의해 모니터링됩니다. 로드 밸런서가 풀 멤버의 문제를 발견하면 해당 멤버는 [다운] 상태로 표시됩니다. 서버 풀에서 풀 멤버를 선택할 때만 UP 서버가 선택됩니다. 서버 풀이 서비스 모니터로 구성되지 않으면 모든 풀 멤버가 UP로 간주됩니다.

참고 로드 밸런서 문제 해결에 대한 자세한 내용은 "NSX 문제 해결 가이드"를 참조하십시오.

■ 로드 밸런서 서비스 구성

■ 서비스 모니터 생성

특정 유형의 네트워크 트래픽에 대한 상태 점검 매개 변수를 정의하는 서비스 모니터를 생성합니다. 서비스 모니터를 풀에 연결하면 서비스 모니터 매개 변수에 따라 풀 멤버가 모니터링됩니다.

■ 서버 풀 추가

서버 풀을 추가하여 백엔드 서버를 유연하고 효율적으로 관리 및 공유할 수 있습니다. 서버 풀은 로드 밸런서 분산 방법을 관리하고 이 풀에는 상태 점검 매개 변수를 확인하기 위한 서비스 모니터가 연결되어 있습니다.

■ 애플리케이션 프로파일 생성

애플리케이션 프로파일을 사용하여 네트워크 트래픽 관리를 보다 강력하게 제어하고 트래픽 관리 작업을 더 쉽고 효율적으로 수행할 수 있습니다.

■ 애플리케이션 규칙 추가

HAProxy 구문을 사용하여 애플리케이션 트래픽을 조작 및 관리함으로써 애플리케이션 규칙을 작성할 수 있습니다.

■ 가상 서버 추가

NSX Edge 내부 또는 업링크 인터페이스를 가상 서버로 추가합니다.

로드 밸런서 서비스 구성

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage)를 클릭하고 로드 밸런서(Load Balancer) 탭을 클릭합니다.
- 5 편집(Edit)을 클릭합니다.
- 6 사용하도록 설정할 옵션 옆의 확인란을 선택합니다. 글로벌 로드 밸런서 구성 매개 변수를 지정할 수 있습니다.

옵션	설명
로드 밸런서 사용	NSX Edge 로드 밸런서가 로드 밸런싱을 위해 트래픽을 내부 서버로 분산하도록 허용합니다.
가속 사용	<p>사용되지 않도록 설정되면 모든 VIP(가상 IP 주소)가 L7 LB 엔진을 사용합니다.</p> <p>사용하도록 설정되면 가상 IP는 더 빠른 L4 LB 엔진 또는 L7 LB 엔진을 사용합니다 (VIP 구성에 따라).</p> <p>L4 VIP(VIP 구성에서 "가속 사용" 및 쿠키 지속성 또는 SSL-오프로드가 적용된 AppProfile과 같은 L7 설정 없음)는 Edge 방화벽 이전에 처리되므로 VIP에 연결하는데 Edge 방화벽 규칙이 필요하지 않습니다. 그렇지만 VIP가 비투명 모드에서 풀을 사용하는 경우 Edge 방화벽이 사용되도록 설정되어야 합니다(자동으로 생성된 SNAT 규칙을 허용하기 위해).</p> <p>L7 HTTP/HTTPS VIP("가속 사용 안 함" 또는 쿠키 지속성 또는 SSL-오프로드가 적용된 AppProfile과 같은 L7 설정 사용)는 Edge 방화벽 이후에 처리되므로 VIP에 연결하려면 Edge 방화벽 허용 규칙이 필요합니다.</p> <p>참고: NSX 로드 밸런서에서 각 VIP에 대해 사용하는 LB 엔진이 유효한지 확인하려면 NSX Edge CLI(ssh 또는 콘솔)에서 "show service loadbalancer virtual" 명령을 실행하고 "LB PROTOCOL [L4 L7]" 필드를 확인하십시오.</p>

옵션	설명
로깅	<p>NSX Edge 로드 밸런서는 트래픽 로그를 수집합니다.</p> <p>드롭다운 메뉴에서 로그 수준을 선택할 수 있습니다. 로그는 구성된 syslog 서버로 내보내집니다. show log follow 명령을 사용하여 로드 밸런싱 로그를 나열할 수도 있습니다.</p> <p>디버그 및 정보 옵션은 최종 사용자 요청을 로깅합니다. 주의, 오류 및 위험 옵션은 최종 사용자 요청을 로깅하지 않습니다. NSX Edge 제어 수준 로그가 디버그 또는 정보로 설정되어 있으면 로드 밸런서는 1분 간격으로 lb, vip, 풀 및 풀 멤버 통계를 로깅합니다.</p> <p>디버그 또는 정보에서 실행될 경우 CPU 사용량 및 Edge 로그 파티션 공간이 소비되고 최대 트래픽 관리 용량에 약간 영향을 미칠 수 있습니다.</p>
서비스 삽입 사용	<p>로드 밸런서가 타사 벤더 서비스와 함께 작동하도록 허용합니다.</p> <p>타사 벤더 로드 밸런서 서비스가 환경에 배포된 경우 파트너 로드 밸런서 이용 항목을 참조하십시오.</p>

7 확인(OK)을 클릭합니다.

서비스 모니터 생성

특정 유형의 네트워크 트래픽에 대한 상태 점검 매개 변수를 정의하는 서비스 모니터를 생성합니다. 서비스 모니터를 풀에 연결하면 서비스 모니터 매개 변수에 따라 풀 멤버가 모니터링됩니다.

5가지 유형의 모니터 ICMP, TCP, UDP, HTTP, HTTPS가 지원됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage)를 클릭하고 로드 밸런서(Load Balancer) 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 서비스 모니터링(Service Monitoring)을 클릭합니다.
- 6 추가(Add)(+) 아이콘을 클릭합니다.
- 7 서비스 모니터의 이름(Name)을 입력합니다.

간격, 시간 초과 및 최대 재시도 횟수는 모든 유형의 상태 점검에서 공통되는 매개 변수입니다.
- 8 서버를 테스트할 간격(Interval)(초)을 입력합니다.

이 간격은 모니터가 백엔드 서버로 요청을 전송하는 기간(초)입니다.
- 9 시간 초과(Timeout)를 입력합니다. 각 상태 점검에서 시간 초과 값은 서버의 응답이 수신되어야 하는 최대 시간(초)입니다.

- 10 최대 재시도 횟수(Max Retries)**를 입력합니다. 이 값은 다운 상태로 선언되기 전에 서버를 테스트하는 횟수입니다.

예를 들어 **간격(Interval)**을 5초로 설정하고, **시간 초과(Timeout)**를 15초로 설정하고, **최대 재시도 횟수(Max Retries)**를 3으로 설정하면 NSX 로드 밸런서가 5초 간격으로 백엔드 서버를 탐색합니다. 각 탐색에서 예상된 응답이 15초 내에 서버에서 수신되면 상태 결과는 정상입니다. 그렇지 않으면 결과는 위험입니다. 최근 3개의 상태 검사 결과가 모두 다운이면 서버는 다운으로 표시됩니다.

- 11** 서버로 상태 점검 요청을 보낼 방법을 드롭다운 메뉴에서 선택합니다. 5가지 유형의 모니터 ICMP, TCP, UDP, HTTP, HTTPS가 지원됩니다. 미리 정의된 3가지 모니터 `default_tcp_monitor`, `default_http_monitor`, `default_https_monitor`가 시스템에 포함되어 있습니다.

- 12** 모니터 유형으로 **ICMP**를 선택하는 경우 다른 매개 변수를 적용할 수 없습니다. 다른 매개 변수는 비워 두십시오.

13 모니터 유형으로 **TCP**를 선택하는 경우 보내기, 받기 및 확장의 세 가지 매개 변수를 추가로 사용할 수 있습니다.

- a 보내기(옵션) - 연결이 설정된 후에 백엔드 서버로 보낸 문자열입니다.
- b 받기(옵션) - 일치하는지 확인할 문자열을 입력합니다. 이 문자열은 헤더이거나 응답 본문에 있을 수 있습니다. 수신된 문자열이 이 정의와 일치할 때에만 서버가 작동 상태인 것으로 간주됩니다.
- c 확장 -[확장] 섹션에 고급 모니터 매개 변수를 키=값 쌍으로 입력합니다.

샘플 확장 **warning=10**은 서버가 10초 내에 응답하지 않을 경우 상태를 주의(warning)로 설정합니다.

모든 확장 항목을 캐리지 리턴 문자로 구분해야 합니다.

표 15-1. TCP 프로토콜에 대한 확장

모니터 확장	설명
escape	send 또는 quit 문자열에서 \n, \r, \t 또는 \를 사용할 수 있습니다. send 또는 quit 옵션 앞에 와야 합니다. 기본값: send에 아무 것도 추가하지 않고, quit 끝에 \r\n을 추가함.
all	All은 서버 응답에서 발생해야 할 문자열을 예상합니다. 기본값은 any입니다.
quit=STRING	연결 닫기를 시작하기 위해 서버에 전송할 문자열입니다.
refuse=ok warn crit	ok, warn 또는 crit 상태의 TCP 거부를 수락합니다. 기본값은 crit입니다.
mismatch=ok warn crit	ok, warn 또는 crit 상태의 예상되는 문자열 불일치를 수락합니다. 기본값은 warn입니다.
jail	TCP 소켓에서 출력을 숨깁니다.
maxbytes=INTEGER	지정된 수 이상의 바이트를 수신하면 연결을 닫습니다.
delay=INTEGER	문자열 전송과 응답 폴링 간에 대기하는 시간(초)입니다.
certificate=INTEGER[,INTEGER]	인증서가 유효해야 할 최소 일 수입니다. 첫 번째 값은 경고에 대한 일 수이고 두 번째 값은 위험에 대한 일 수입니다(지정하지 않은 경우 0).
warning=DOUBLE	경고 상태를 발생시키는 응답 시간(초)입니다.
critical=DOUBLE	위험 상태를 발생시키는 응답 시간(초)입니다.

14 모니터 유형으로 **HTTP** 또는 **HTTPS**를 선택하는 경우 아래 단계를 수행합니다.

- a 예상(옵션) - [예상] 섹션에 모니터가 HTTP 응답의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다. 이것은 쉼표로 구분된 목록입니다.
예: 200,301,302,401.
- b 메서드(옵션) - 드롭다운 메뉴에서 서버 상태를 검색할 메서드, 즉 GET, OPTIONS 또는 POST를 선택합니다.
- c URL(옵션) - GET 또는 POST에 대한 URL(기본값 "/")을 입력합니다.

- d POST 메서드를 선택하는 경우 전송될 데이터를 **볼드체(Bold)** 섹션에 입력합니다.

- e **받기(Receive)** 섹션의 응답 콘텐츠에서 일치할 문자열을 입력합니다. 이 문자열은 헤더이거나 응답 본문에 있을 수 있습니다.

[예상] 섹션의 문자열이 일치하지 않으면 모니터는 [받기] 콘텐츠와 일치시키려 하지 않습니다.

- f 확장 - [확장] 섹션에 고급 모니터 매개 변수를 키=값 쌍으로 입력합니다.

샘플 확장 **warning=10**은 서버가 10초 내에 응답하지 않을 경우 상태를 주의(warning)로 설정합니다.

모든 확장 항목을 캐리지 리턴 문자로 구분해야 합니다.

표 15-2. HTTP/HTTPS 프로토콜에 대한 확장

모니터 확장	설명
no-body	문서 본문을 기다리지 않습니다. 제목 이후에 읽기를 중지합니다. 그래도 HEAD가 아니라 HTTP GET 또는 POST를 계속 수행합니다.
ssl-version=3	sslv3을 사용하여 SSL 핸드셰이크를 강제로 수행합니다. 기본적으로 sslv3 및 tlsv1은 상태 점검 옵션에서 사용되지 않도록 설정되어 있습니다.
ssl-version=10	tls 1.0을 사용하여 SSL 핸드셰이크를 강제로 수행합니다.
ssl-version=11	tls 1.1을 사용하여 SSL 핸드셰이크를 강제로 수행합니다.
ssl-version=12	tls 1.2를 사용하여 SSL 핸드셰이크를 강제로 수행합니다.
max-age=SECONDS	문서가 SECONDS 이상 오래된 경우 경고합니다. 이 숫자는 분일 경우 10m, 시간일 경우 10h, 일 수일 경우 10d 형식일 수 있습니다.
content-type=STRING	POST 호출에서 Content-Type 헤더 미디어 유형을 지정합니다.
linespan	정규식이 새로운 줄을 걸칠 수 있도록 허용합니다(앞에 -r 또는 -R이 와야 함).
regex=STRING 또는 ereg=STRING	STRING 정규식에 대한 페이지를 검색합니다.
eregi=STRING	대/소문자를 구분하지 않는 STRING 정규식에 대한 페이지를 검색합니다.
invert-regex	있으면 CRITICAL을 반환하고, 없으면 OK를 반환합니다.
proxy-authorization=AUTH_PAIR	기본 인증을 사용하는 프록시 서버의 사용자 이름:암호입니다.
useragent=STRING	HTTP 헤더에서 User Agent로 전송되는 문자열입니다.
header=STRING	HTTP 헤더에서 전송되는 기타 태그입니다. 추가 헤더를 위해 여러 번 사용합니다.
onredirect=ok warning critical follow sticky stickyport	리디렉션된 페이지를 처리하는 방법입니다. sticky는 follow와 유사하지만 지정된 IP 주소에 고정됩니다. stickyport를 사용하면 포트가 항상 동일합니다.
pagesize=INTEGER:INTEGER	필요한 최소 페이지 크기(바이트): 필요한 최대 페이지 크기(바이트)입니다.

표 15-2. HTTP/HTTPS 프로토콜에 대한 확장 (계속)

모니터 확장	설명
warning=DOUBLE	경고 상태를 발생시키는 응답 시간(초)입니다.
critical=DOUBLE	위험 상태를 발생시키는 응답 시간(초)입니다.
expect = <i>STRING</i>	선타로 구분된 문자열 목록입니다. 서버 응답의 첫 번째 (상태) 줄에 이 중 하나 이상의 문자열이 예상됩니다(기본값: HTTP/1). 지정될 경우 다른 모든 상태 줄 논리(예: 3xx, 4xx, 5xx processing)를 건너뜁니다.
string = <i>STRING</i>	컨텐츠에서 예상되는 문자열입니다.
url = PATH	GET 또는 POST에 대한 URL입니다(기본값: /).
post = <i>STRING</i>	http POST 데이터를 인코딩하기 위한 URL입니다.
method = <i>STRING</i>	HTTP 메서드(예: HEAD, OPTIONS, TRACE, PUT, DELETE)를 설정합니다.
timeout = <i>INTEGER</i>	연결이 시간 초과되기 전까지의 시간(초)입니다(기본값 10 초).
header=Host: <i>host_name</i> -H <i>host_name</i> --sni	<i>host_name</i> 은 호스트의 유효한 호스트 이름 또는 FQDN입니다. 각 가상 호스트에 대해 별도의 서비스 모니터를 생성하고 각 서비스 모니터에 SNI(서버 이름 표시) 확장을 추가합니다.

표 15-3. HTTPS 프로토콜에 대한 확장

모니터 확장	설명
certificate= <i>INTEGER</i>	인증서가 유효해야 할 최소 일 수입니다. 포트 기본값이 443으로 설정됩니다. 이 옵션을 사용하면 URL이 선택되지 않습니다.
authorization=AUTH_PAIR	기본 인증을 사용하는 사이트의 사용자 이름:암호입니다.
ciphers=' ECDHE-RSA-AES256-GCM-SHA384'	HTTPS 상태 점검에 사용되는 암호를 표시합니다.

15 모니터 유형으로 **UDP**를 선택하는 경우 아래 단계를 수행합니다.

- a 보내기(필수): 연결이 설정된 후에 백엔드 서버로 보낼 문자열을 입력합니다.
- b 수신(필수): 백엔드 서버에서 수신될 것으로 예상되는 문자열을 입력합니다. 수신된 문자열이 이 정의와 일치할 때에만 서버가 작동 상태인 것으로 간주됩니다.

참고 UDP 모니터에서는 확장을 지원하지 않습니다.

16 확인(OK)을 클릭합니다.

다음에 수행할 작업

서비스 모니터를 풀과 연결합니다.

서버 풀 추가

서버 풀을 추가하여 백엔드 서버를 유연하고 효율적으로 관리 및 공유할 수 있습니다. 서버 풀은 로드 밸런서 분산 방법을 관리하고 이 풀에는 상태 점검 매개 변수를 확인하기 위한 서비스 모니터가 연결되어 있습니다.

절차


- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage)를 클릭하고 로드 밸런서(Load Balancer) 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 풀(Pools)을 클릭합니다.
- 6 추가(Add)(+) 아이콘을 클릭합니다.
- 7 로드 밸런서 풀의 이름과 설명을 입력합니다.
- 8 사용하도록 설정한 각 서비스에 대해 알고리즘 밸런싱 방법을 선택합니다.

옵션	설명
IP-HASH	소스 IP 주소의 해시와 실행 중인 모든 서버의 총 가중치에 따라 서버를 선택합니다. 이 옵션에 대해서는 알고리즘 매개 변수가 사용되지 않도록 설정됩니다.
LEASTCONN	서버에 이미 있는 연결 수를 기반으로 하여 클라이언트 요청을 여러 서버로 분산합니다. 새 연결은 연결 수가 가장 적은 서버로 전송됩니다. 이 옵션에 대해서는 알고리즘 매개 변수가 사용되지 않도록 설정됩니다.
ROUND_ROBIN	각 서버에 할당된 가중치 순서대로 서버가 사용됩니다. 이는 서버의 처리 시간이 고루 분산된 상태를 유지하는 경우 가장 유연하고 공정한 알고리즘입니다. 이 옵션에 대해서는 알고리즘 매개 변수가 사용되지 않도록 설정됩니다.
URI	URI의 왼쪽 부분(물음표 앞부분)을 해시 처리한 후 실행 중인 서버들의 총 가중치로 나눕니다. 결과에 따라 요청을 받는 서버가 지정됩니다. 이 경우 작동이 시작되거나 중단된 서버가 없는 한 URI는 항상 동일한 서버를 가리킵니다. URI 알고리즘 매개 변수에는 uriLength=<len> 및 uriDepth=<dep>의 두 가지 옵션이 있습니다. Length 매개 변수 범위는 1<=len<256입니다. Depth 매개 변수 범위는 1<=dep<10입니다. Length 및 depth 매개 변수 다음에는 양의 정수가 옵니다. 이러한 옵션은 URI 시작 부분에 따라서만 서버 밸런스를 유지합니다. Length 매개 변수는 알고리즘에서 해시 계산을 위해 URI 시작 부분에 정의된 문자만 고려하도록 지정합니다. Depth 매개 변수는 해시 계산에 사용될 최대 디렉토리 깊이를 나타냅니다. 요청의 각 슬래시는 1개의 수준으로 계산됩니다. 두 매개 변수를 모두 지정하면 둘 중 하나에 도달할 때 계산이 중지됩니다.

옵션	설명
HTTPHEADER	<p>HTTP 헤더 이름은 각 HTTP 요청에서 조회됩니다.</p> <p>괄호로 묶인 헤더 이름은 ACL 'hdr()' 함수와 마찬가지로 대/소문자를 구분하지 않습니다. 헤더가 없거나 값을 포함하지 않으면 라운드 로빈 알고리즘이 적용됩니다.</p> <p>HTTPHEADER 알고리즘 매개 변수에는 단일 옵션인 <code>headerName=<name></code>이 있습니다. 예를 들어 <code>host</code>를 HTTPHEADER 알고리즘 매개 변수로 사용할 수 있습니다.</p>
URL	<p>인수에 지정된 URL 매개 변수는 각 HTTP GET 요청의 쿼리 문자열에서 조회됩니다.</p> <p>매개 변수 다음에 등호(=)와 값이 나오면 해당 값은 해시 처리되고 실행 중인 서버의 총 가중치로 나누어집니다. 결과에 따라 요청을 받는 서버가 지정됩니다. 이 프로세스는 요청의 사용자 식별자를 추적하는 데 사용되고, 서버가 켜지거나 꺼지지 않는 한 동일한 사용자 ID가 동일한 서버로 전송되도록 합니다.</p> <p>값이나 매개 변수가 없으면 라운드 로빈 알고리즘이 적용됩니다.</p> <p>URL 알고리즘 매개 변수에는 단일 옵션인 <code>urlParam=<url></code>이 있습니다.</p>

9 (선택 사항) **모니터(Monitors)** 드롭다운 메뉴에서 기존의 기본 모니터 또는 사용자 지정 모니터를 선택합니다.

10 풀에 멤버를 추가합니다.

- a **추가(Add)** 아이콘()을 클릭합니다.
- b 서버 멤버의 이름 및 IP 주소를 입력하거나 **선택(Select)**을 클릭하여 그룹 개체를 할당합니다.

참고 VMware Tools가 각 VM에 설치되어 있거나, IP 주소 대신 그룹 개체를 사용할 때 사용하도록 설정된 IP 검색 방법(DHCP 스누핑이나 ARP 스누핑 또는 둘 다)이 적용되어 있어야 합니다. 자세한 내용은 [가상 시스템에 대한 IP 검색](#)을 참조하십시오.

그룹 개체는 vCenter 또는 NSX일 수 있습니다.

- c 멤버 상태를 **사용(Enable)**, **사용 안 함(Disable)** 또는 **추출(Drain)**로 선택합니다.
 - **추출(Drain)** - 유지 보수를 위해 강제로 서버를 정상 종료합니다. 풀 멤버를 "추출"로 설정하면 로드 밸런싱에서 백엔드 서버가 제거되지만, 지속성이 있는 클라이언트에서 해당 서버로의 연결 및 새 연결을 종료하는 데 사용될 수 있습니다. 추출 상태로 작동하는 지속성 메시드는 소스 IP 지속성, 쿠키 삽입 및 쿠키 접두사입니다.

참고 NSX Edge에서고가용성 구성을 사용하도록 설정한 후 사용하지 않도록 설정하면 소스 IP 지속성 메시지를 통한 지속성 및 추출 상태가 깨질 수 있습니다.

- **사용(Enable)** - 유지 보수 모드에서 서버를 제거하고 다시 작동시킵니다. 풀 멤버 상태는 **추출(Drain)** 또는 **사용 안 함(Disabled)**이어야 합니다.
- **사용 안 함(Disable)** - 서버는 유지 보수 모드를 유지합니다.

참고 풀 멤버 상태를 **사용 안 함(Disabled)**에서 **추출(Drain)**로 변경할 수 없습니다.

d 해당 멤버가 트래픽을 받을 포트와 상태 모니터 ping을 받을 모니터 포트를 각각 입력합니다.

관련 가상 서버가 포트 범위로 구성된 경우 포트 값은 null이어야 합니다.

e [가중치] 섹션에 이 멤버가 처리할 트래픽 비율을 입력합니다.

f 멤버가 처리할 수 있는 최대 동시 연결 수를 입력합니다.

수신 요청이 최대 동시 연결 수보다 더 많을 경우 대기열에 포함되고 연결이 해제되기를 기다립니다.

g 멤버가 항상 허용해야 하는 최소 동시 연결 수를 입력합니다.

h **확인(OK)**을 클릭합니다.

11 클라이언트 IP 주소를 백엔드 서버에 표시하려면 **투명(Transparent)**을 선택합니다. 자세한 내용은 [장 15 논리적 로드 밸런서](#)를 참조하십시오.

[투명]을 선택하지 않을 경우(기본값) 백엔드 서버는 트래픽 소스 IP 주소를 로드 밸런서 내부 IP 주소로 인식합니다. [투명]을 선택할 경우 소스 IP 주소는 실제 클라이언트 IP 주소가 되며 반환 패킷이 NSX Edge 디바이스를 통과할 수 있도록 NSX Edge를 기본 게이트웨이로 설정해야 합니다.

12 **확인(OK)**을 클릭합니다.

애플리케이션 프로파일 생성

애플리케이션 프로파일을 사용하여 네트워크 트래픽 관리를 보다 강력하게 제어하고 트래픽 관리 작업을 더 쉽고 효율적으로 수행할 수 있습니다.

애플리케이션 프로파일을 생성하여 특정 유형 네트워크 트래픽의 동작을 정의할 수 있습니다. 프로파일을 구성한 후 가상 서버에 연결합니다. 그러면 가상 서버에서 프로파일에 지정된 값에 따라 트래픽을 처리합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **애플리케이션 프로파일(Application Profiles)**을 클릭합니다.
- 6 **추가(Add)(+)** 아이콘을 클릭합니다.
- 7 프로파일 이름을 입력하고 드롭다운 메뉴에서 프로파일을 생성할 트래픽 유형을 선택합니다.

트래픽 유형	지원되는 지속성 메서드
TCP	소스 IP, MSRDp
HTTP	쿠키, 소스 IP

트래픽 유형	지원되는 지속성 메서드
HTTPS	쿠키, SSL 세션 ID(SSL 통과 사용), 소스 IP
UDP	소스 IP

8 HTTP 트래픽을 리디렉션할 URL을 입력합니다.

예를 들어 트래픽을 <http://myweb.com>에서 <https://myweb.com>으로 리디렉션할 수 있습니다.

9 드롭다운 메뉴에서 프로파일에 대한 지속성 유형을 지정합니다.

지속성을 통해 클라이언트 요청에 서비스를 지원한 특정 풀 멤버와 같은 세션 데이터를 추적하고 저장합니다. 지속성이 있으면 세션이 실행되는 전체 기간 또는 이후 세션이 실행되는 동안 클라이언트 요청이 동일한 풀 멤버로 이동됩니다.

- **쿠키(Cookie)** 지속성을 선택하여 클라이언트가 사이트에 처음 액세스할 때 세션을 식별하기 위한 고유한 쿠키를 삽입합니다.

이 쿠키는 해당 서버에 대한 연결을 지속하기 위해 후속 요청에서 참조됩니다.

- **소스 IP** 주소를 기준으로 세션을 추적하려면 **소스 IP(Source IP)** 지속성을 선택합니다.

클라이언트가 소스 주소 선호도 지속성을 지원하는 가상 서버에 대한 연결을 요청할 경우 로드 밸런서는 해당 클라이언트가 이전에 연결한 적이 있는지 여부를 확인한 후 연결한 적이 있으면 클라이언트를 동일한 풀 멤버에 할당합니다.

- **Microsoft RDP(원격 데스크톱 프로토콜)** 서비스를 실행하는 서버와 **Windows** 클라이언트 간에 영구 세션을 유지하려면 **MSRDP(Microsoft 원격 데스크톱 프로토콜)** 지속성을 선택합니다.

MSRDP 지속성을 사용하는 권장 시나리오는 **Windows Server 2003** 또는 **Windows Server 2008**을 실행하는 멤버로 구성되어 있고, 모든 멤버가 **Windows** 클러스터에 속해 있고, **Windows** 세션 디렉토리에 참가하도록 지원하는 로드 밸런싱 풀을 생성하기 위한 것입니다.

10 쿠키 이름을 입력하고 쿠키 삽입 모드를 선택합니다.

옵션	설명
삽입	NSX Edge가 쿠키를 전송합니다. 서버가 하나 이상의 쿠키를 전송하면 클라이언트는 하나의 추가 쿠키를 수신합니다 (서버 쿠키 + Edge 쿠키). 서버가 쿠키를 전송하지 않을 경우 클라이언트는 Edge 쿠키를 수신합니다.
접두사	클라이언트에서 둘 이상의 쿠키를 지원하지 않을 경우 이 옵션이 선택됩니다. 참고 모든 브라우저가 다중 쿠키를 지원합니다. 하나의 쿠키만 지원하는 전용 클라이언트를 사용하는 전용 애플리케이션이 있는 경우 웹 서버는 평소대로 쿠키를 전송합니다. NSX Edge는 쿠키 정보를 서버 쿠키 값에 접두사로 넣습니다. NSX Edge가 서버에 쿠키를 전송할 때 이 쿠키 추가 정보가 제거됩니다.
App 세션	서버는 쿠키를 전송하지 않습니다. 대신 사용자 세션 정보를 URL로 전송합니다. 예를 들어 <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD</code> 와 같습니다. 여기서 <code>jsessionid</code> 는 사용자 세션 정보이며 지속성에 사용됩니다. 문제 해결을 위해 App 세션 지속성 테이블을 볼 수 없습니다.

11 지속성 만료 시간(초)을 입력합니다. 지속성의 기본값은 300초(5분)입니다. 지속성 테이블의 크기는 제한되어 있습니다. 시간 초과 값이 크면 트래픽이 과도할 경우 지속성 테이블이 빠르게 채워질 수 있습니다. 지속성 테이블이 채워지면 최신 항목을 수용하기 위해 가장 오래된 항목부터 삭제됩니다.

로드 밸런서 지속성 테이블은 클라이언트 요청이 동일한 풀 멤버로 전송됨을 기록하는 항목을 유지합니다.

- 새 연결 요청이 시간 초과 기간 내에 동일한 클라이언트에서 수신되면 지속성 항목이 만료되어 삭제됩니다.
- 동일한 클라이언트에서의 새 연결 요청이 시간 초과 기간 내에 수신되면 타이머가 재설정되고 클라이언트 요청이 고정 풀 멤버로 전송됩니다.
- 시간 초과 기간이 만료되면 새 연결 요청이 로드 밸런싱 알고리즘에 의해 허용된 풀 멤버로 전송됩니다.

L7 로드 밸런싱 TCP 소스 IP 지속성 시나리오의 경우 기존 연결이 여전히 활성 상태라도 지정된 시간 동안 새 TCP 연결이 설정되지 않으면 지속성 항목은 시간 초과됩니다.

12 (선택 사항) HTTPS 트래픽에 대한 애플리케이션 프로파일을 생성합니다.

지원되는 HTTPS 트래픽 패턴:

- SSL 오프로딩 - 클라이언트 -> HTTPS -> LB(SSL 종료) -> HTTP -> 서버
- SSL 프록시 - 클라이언트 -> HTTPS -> LB(SSL 종료) -> HTTPS -> 서버
- SSL 통과 - 클라이언트 -> HTTPS -> LB(SSL 통과) -> HTTPS -> 서버

■ 클라이언트 -> HTTP-> LB -> HTTP -> 서버

a (선택 사항) 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소를 식별할 수 있도록 **X-Forwarded-For HTTP 헤더 삽입(Insert X-Forwarded-For HTTP header)**을 선택합니다.

b **서비스 인증서 구성(Configure Service Certificate)**을 선택하여 **가상 서버 인증서(Virtual Server Certificates)** 탭에서 로드 밸런서의 클라이언트에서의 HTTPS 트래픽을 종료하는 데 사용되는 해당 서비스 인증서, CA 인증서 및 CRL을 선택합니다.

이 항목은 클라이언트 > LB 연결이 HTTPS일 때만 필요합니다.

c (선택 사항) **풀 측 SSL 사용(Enable Pool Side SSL)**을 선택하여 로드 밸런서와 백엔드 서버 간 HTTPS 통신을 사용하도록 설정합니다.

풀 측 SSL을 사용하여 종단 간 SSL을 구성할 수 있습니다.

d (선택 사항) **서비스 인증서 구성(Configure Service Certificate)**을 선택하여 **풀 인증서(Pool Certificates)** 탭에서 서버 측으로부터 로드 밸런서를 인증하는 데 사용되는 해당 서비스 인증서, CA 인증서 및 CRL을 선택합니다.

이 항목은 클라이언트 -> HTTPS -> LB -> HTTPS -> 서버 패턴에만 필요합니다.

NSX Edge 로드 밸런서에 CA 인증서 및 CRL이 이미 구성되어 있고 백엔드 서버의 서비스 인증서를 확인해야 하는 경우 서비스 인증서를 구성할 수 있습니다. 이 옵션은 백엔드 서버가 로드 밸런서 측 서비스 인증서를 확인해야 하는 경우 백엔드 서버에 로드 밸런서 인증서를 제공하는 데도 사용할 수 있습니다.

13 SSL/TLS 핸드셰이크 중에 협상되는 암호 알고리즘 또는 암호 제품군을 입력합니다. 여러 암호를 콜론(:)으로 구분하여 추가할 수 있습니다. 승인된 암호 그룹에 1024비트보다 크거나 같은 DH 키 길이가 포함되어 있는지 확인하십시오.

아래와 같은 승인된 암호 제품군을 사용할 수 있습니다.

암호 값	암호 이름
DEFAULT	DEFAULT
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDH-ECDSA-AES256-SHA	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
ECDH-RSA-AES256-SHA	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA

14 드롭다운 메뉴에서 클라이언트 인증이 무시될지 또는 반드시 필요한지를 지정합니다.

필수로 설정하면 클라이언트는 요청 또는 핸드셰이크가 중단된 후 인증서를 제공해야 합니다.

15 확인(OK)을 클릭합니다.

애플리케이션 규칙 추가

HAProxy 구문을 사용하여 애플리케이션 트래픽을 조작 및 관리함으로써 애플리케이션 규칙을 작성할 수 있습니다.

애플리케이션 규칙 구문에 대한 내용은 <http://cbonte.github.io/haproxy-dconv/>의 HAProxy 설명서를 참조하십시오.

일반적으로 사용되는 애플리케이션 규칙의 예는 [애플리케이션 규칙 예](#)를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **애플리케이션 규칙(Application Rules)**을 클릭합니다.
- 6 **추가(Add)**(+) 아이콘을 클릭합니다.
- 7 규칙의 이름과 스크립트를 입력합니다.
- 8 **확인(OK)**을 클릭합니다.

애플리케이션 규칙 예

일반적으로 사용되는 애플리케이션 규칙입니다.

조건 기반 HTTP/HTTPS 리디렉션

애플리케이션 프로파일을 사용하면 HTTP/HTTPS 리디렉션을 지정하여 요청 URL에 관계없이 항상 트래픽을 리디렉션할 수 있습니다. HTTP/HTTPS 트래픽의 리디렉션 조건도 유연하게 지정할 수 있습니다.

```
move the login URL only to HTTPS.
acl clear dst_port 80
acl secure dst_port 8080
acl login_page url_beg /login
acl logout url_beg /logout
acl uid_given url_reg /login?userid=[^&]+
acl cookie_set hdr_sub(cookie) SEEN=1
redirect prefix https://mysite.com set-cookie SEEN=1 if !cookie_set
redirect prefix https://mysite.com if login_page !secure
redirect prefix http://mysite.com drop-query if login_page !uid_given
redirect location http://mysite.com/ if !login_page secure
redirect location / clear-cookie USERID= if logout
```

도메인 이름 기준 라우팅

도메인 이름에 따라 요청을 특정 로드 밸런서 풀로 향하게 하는 애플리케이션 규칙을 생성할 수 있습니다. 다음 규칙은 **foo.com**으로 들어오는 요청을 **pool_1**로, **bar.com**으로 들어오는 요청을 **pool_2**로 향하게 합니다.

```
acl is_foo hdr_dom(host) -i foo
acl is_bar hdr_dom(host) -i bar
use_backend pool_1 if is_foo
use_backend pool_2 if is_bar
```

Microsoft RDP 로드 밸런싱 및 보호

다음 샘플 시나리오에서는 로드 밸런서가 새 사용자를 로드가 더 적은 서버로 보내고 끊어진 세션을 재개합니다. 이 시나리오에서 **NSX Edge** 내부 인터페이스 IP 주소는 **10.0.0.18**이고, 내부 인터페이스 IP 주소는 **192.168.1.1**이며, 가상 서버는 **192.168.1.100**, **192.168.1.101** 및 **192.168.1.102**입니다.

- 1 **MSRDP** 지속성을 사용하여 **TCP** 트래픽에 대한 애플리케이션 프로파일을 생성합니다.
- 2 **TCP** 상태 모니터(**tcp_monitor**)를 생성합니다.
- 3 **192.168.1.100:3389**, **192.168.1.101:3389** 및 **192.168.1.102:3389**가 멤버로 속한 풀(이름은 **rdp-pool**)을 생성합니다.
- 4 **tcp_monitor**를 **rdp-pool**에 연결합니다.
- 5 다음 애플리케이션 규칙을 생성합니다.

```
tcp-request content track-sc1 rdp_cookie(msthash) table rdp-pool
tcp-request content track-sc2 src table ipv4_ip_table

# each single IP can have up to 2 connections on the VDI infrastructure
tcp-request content reject if { sc2_conn_cur ge 2 }

# each single IP can try up to 5 connections in a single minute
tcp-request content reject if { sc2_conn_rate ge 10 }

# Each user is supposed to get a single active connection at a time, block the second one
tcp-request content reject if { sc1_conn_cur ge 2 }

# if a user tried to get connected at least 10 times over the last minute,
# it could be a brute force
tcp-request content reject if { sc1_conn_rate ge 10 }
```

- 6 가상 서버(named **rdp-vs**)를 생성합니다.
- 7 애플리케이션 프로파일을 이 가상 서버에 연결하고 4단계에서 생성한 애플리케이션 규칙을 추가합니다.

가상 서버에 새로 적용된 애플리케이션 규칙이 **RDP** 서버를 보호합니다.

고급 로깅

기본적으로 **NSX** 로드 밸런서는 기본 로깅을 지원합니다. 다음과 같은 애플리케이션 규칙을 생성하여 문제 해결에 유용한 더 자세한 로깅 메시지를 볼 수 있습니다.

```
# log the name of the virtual server
capture request header Host len 32

# log the amount of data uploaded during a POST
capture request header Content-Length len 10
# log the beginning of the referrer
capture request header Referer len 20

# server name (useful for outgoing proxies only)
capture response header Server len 20

# logging the content-length is useful with "option logasap"
capture response header Content-Length len 10

# log the expected cache behaviour on the response
capture response header Cache-Control len 8

# the Via header will report the next proxy's name
capture response header Via len 20

# log the URL location during a redirection
capture response header Location len 20
```

애플리케이션 규칙을 가상 서버에 연결하면 로그에 다음 예와 같은 자세한 메시지가 포함됩니다.

```
2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 -- [25/Apr/
2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51656 856 "vip-http-complete"
"pool-http-complete" "m2" 145 0 1 26 172 --NI 1 1 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""

2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 -- [25/Apr/
2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51657 856 "vip-http-complete"
"pool-http-complete" "m2" 412 0 0 2 414 --NI 0 0 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""
```

HTTPS 트래픽 문제를 해결하려면 규칙을 더 추가해야 할 수도 있습니다. 대부분의 웹 애플리케이션은 클라이언트를 페이지로 향하게 하는 위치 헤더와 함께 **301/302** 응답을 사용하며(대부분의 경우 로그인 또는 **POST** 호출 후) 애플리케이션 쿠키를 요구합니다. 따라서 애플리케이션 서버가 클라이언트 연결 정보를 파악하는 데 어려움이 있을 수 있으며 올바른 응답을 제공하지 못할 수도 있습니다. 애플리케이션의 작동이 중지될 수도 있습니다.

웹 애플리케이션이 **SSL** 오프로드를 지원하도록 허용하려면 다음 규칙을 추가하십시오.

```
# See clearly in the log if the application is setting up response for HTTP or HTTPS
capture response header Location len 32
capture response header Set-Cookie len 32

# Provide client side connection info to application server over HTTP header
http-request set-header X-Forwarded-Proto https if { ssl_fc }
http-request set-header X-Forwarded-Proto http if !{ ssl_fc }
```

SSL을 통해 연결이 설정되면 로드 밸런서가 다음 헤더를 삽입합니다.

```
X-Forwarded-Proto: https
```

HTTP를 통해 연결이 설정되면 로드 밸런서가 다음 헤더를 삽입합니다.

```
X-Forwarded-Proto: http
```

특정 URL 차단

URL에 특정 키워드가 포함된 요청을 차단할 수 있습니다. 다음 샘플 규칙은 요청이 **/private** 또는 **/finance**로 시작하는지 확인하고 해당 용어가 포함된 요청을 차단합니다.

```
# Check if the request starts with "/private" or "/finance" (case insensitive)
acl block_url_list path_beg -i /private /finance

# If the request is part of the list forbidden urls,reply "Forbidden"(HTTP response code 403)
block if block_url_list
```

쿠키가 없는 경우 인증 **HTTP** 리디렉션

쿠키가 없는 클라이언트 요청을 리디렉션하여 인증을 받을 수 있습니다. 다음 샘플 규칙은 **HTTP** 요청이 진짜인지와 헤더에 쿠키가 있는지 확인합니다. 요청에 쿠키가 없으면 규칙은 인증을 위해 요청을 **/authentic.php**로 리디렉션합니다.

```
acl authentic_url url /authentic.php
acl cookie_present hdr_sub(cookie) cookie1=
redirect prefix /authentic.php if !authentic_url !cookie_present
```

기본 페이지 리디렉션

클라이언트 요청 **/**를 기본 페이지로 리디렉션할 수 있습니다. 다음 샘플 규칙은 **HTTP** 요청이 **/**인지 확인하고 요청을 기본 로그인 페이지로 리디렉션합니다.

```
acl default_url url /
redirect location /login.php if default_url
```

유지 보수 사이트로 리디렉션

기본 풀이 다운되면 유지 보수 서버 풀을 사용하고 URL을 유지 보수 웹 사이트로 리디렉션할 수 있습니다.

```
redirect location http://maitenance.xyz.com/maintenance.htm
```

NTLM(NT LAN Manager) 인증

기본적으로 서버 측 NSX는 각 요청 후에 TCP 연결을 닫습니다. 각 요청 후에 서버 세션을 닫지 않으려면 서버 세션을 활성 상태로 두고 NTLM 프로토콜로 보호할 수 있습니다.

```
no option http-server-close
```

기본적으로 클라이언트 측 NSX는 요청 간에 TCP 연결이 설정된 상태를 유지합니다. 그렇지만 "X-Forwarded-For" 옵션을 사용하면 각 요청 후에 세션이 닫힙니다. 다음 옵션은 XFF가 구성된 경우에도 요청 간에 클라이언트 연결을 열린 상태로 유지합니다.

```
no option httpclose
```

서버 헤더 교체

기본 응답 서버 헤더를 삭제하고 다른 서버로 교체할 수 있습니다. 다음 샘플 규칙은 서버 헤더를 삭제하고 HTTP, HTTPS, SMTP, POP3 및 IMAP 프로토콜, HTTP 캐시 및 로드 밸런서에 대한 역방향 프록시 서버 역할을 할 수 있는 NGINX 웹 서버로 바꿉니다.

```
rspidel Server
rspadd Server:\ nginx
```

다시 쓰기 리디렉션

위치 헤더를 HTTP에서 HTTPS로 다시 쓸 수 있습니다. 다음 샘플 규칙은 위치 헤더를 식별한 후 HTTP를 HTTPS로 바꿉니다.

```
rspirep ^Location:\ http://(.*) Location:\ https://\1
```

호스트 기반 특정 풀 선택

특정 호스트가 있는 요청을 정의된 풀로 리디렉션할 수 있습니다. 다음 샘플 규칙은 특정 호스트 app1.xyz.com, app2.xyz.com 및 host_any_app3에 대한 요청을 확인하고 이러한 요청을 각각 정의된 풀 pool_app1, pool_app2 및 pool_app3으로 리디렉션합니다. 다른 모든 요청은 가상 서버에 정의된 기존 풀로 리디렉션됩니다.

```
acl host_app1 hdr(Host) -i app1.xyz.com
acl host_app2 hdr(Host) -i app2.xyz.com
acl host_any_app3 hdr_beg(host) -i app3
```

각 호스트 이름에 대해 특정 풀을 사용합니다.

```
use_backend pool_app1 if host_app1
use_backend pool_app2 if host_app2
use_backend pool_app3 if host_any_app3
```

URL 기반 특정 풀 선택

URL 키워드가 있는 요청을 특정 풀로 리디렉션할 수 있습니다. 다음 샘플 규칙은 요청이 `/private` 또는 `/finance`로 시작하는지 확인하고 이러한 요청을 정의된 풀, `pool_private` 또는 `pool_finance`로 리디렉션합니다. 다른 모든 요청은 가상 서버에 정의된 기존 풀로 리디렉션됩니다.

```
acl site_private path_beg -i /private
acl site_finance path_beg -i /finance
use_backend pool_private if site_private
use_backend pool_finance if site_finance
```

기본 풀이 다운될 때 리디렉션

기본 풀의 서버가 다운되면 보조 풀의 서버를 사용하도록 사용자를 리디렉션할 수 있습니다. 다음 샘플 규칙은 `pool_production`이 다운되었는지 확인하고 사용자를 `pool_sorry_server`로 전송합니다.

```
acl pool_production_down nbsrv(pool_production) eq 0
use_backend pool_sorry_server if pool_production_down
```

화이트리스트 TCP 연결

클라이언트 IP 주소가 서버에 액세스하지 못하게 차단할 수 있습니다. 다음 샘플 규칙은 정의된 IP 주소를 차단하고 클라이언트 IP 주소가 화이트리스트에 없으면 연결을 재설정합니다.

```
acl whitelist src 10.10.10.0 20.20.20.0
tcp-request connection reject if !whitelist
```

ssl3 및 tls1 사용

ssl3 및 tls1 서비스 모니터 확장은 기본적으로 사용하지 않도록 설정됩니다. 다음 애플리케이션 규칙을 사용하여 이를 사용하도록 설정할 수 있습니다.

```
ssl3 enable
tls1 enable
```

클라이언트 세션 시간 초과 구성

세션 시간 초과는 클라이언트 측의 최대 연결 비활성 시간입니다. 클라이언트가 데이터를 확인하거나 전송해야 할 때 비활성 시간 초과가 적용됩니다. HTTP 모드에서는 클라이언트가 요청을 보내는 첫 번째 단계와 클라이언트가 서버에서 전송된 데이터를 읽는 응답 시간 동안 이 시간 초과를 특히 중요하게 고려해야 합니다. 기본 시간 초과 값은 5분입니다.

다음 샘플 규칙은 시간 초과 기간을 100초로 설정합니다.

```
timeout client 100s
```

시간은 밀리초, 초, 분, 시간 또는 일 단위의 정수로 설정할 수 있습니다.

HTTPS 사이트로 리디렉션

HTTP로 오는 클라이언트를 HTTPS의 동일한 페이지로 리디렉션할 수 있습니다.

```
# Redirect all HTTP requests to same URI but HTTPS redirect scheme
https if ![ ssl_fc ]
```

기타 옵션은 다음과 같습니다.

```
rspirep ^Location:\ http://(.*) Location:\ https://^1
```

비인증 클라이언트 리디렉션

쿠키가 없는 경우 클라이언트 요청을 "/authentic.php"로 리디렉션합니다.

```
# Check the HTTP request if request is "/authentic.php"
acl authentic_url url /authentic.php
# Check the cookie "cookie1" is present
acl cookie_present hdr_sub(cookie) cookie1=
# If the request is NOT "/authentic.php" and there is no cookie, then redirect to "/authentic.php"
redirect prefix /authentic.php if !authentic_url !cookie_present
```

HTTP 응답 헤더 다시 쓰기

응답 서버 헤더 "Server"를 값 "nginx"로 바꿉니다.

```
# Delete the existing Response Server header "Server"
rspidel Server
# Add the Response Server header "Server" with the value "nginx"
rspadd Server:\ nginx
```

장애 대비 서버

기본 풀의 서버가 모두 비활성 상태이면 보조 풀의 서버를 사용합니다.

```
# detect if pool "pool_production" is still up
acl pool_production_down nbsrv(pool_production) eq 0
# use pool "pool_sorry_server" if "pool_production" is dead
use_backend pool_sorry_server if pool_production_down
# Option 1: # Redirect everything to maintenance site
redirect location http://maintenance.xyz.com/maintenance.htm
# Option 2: #Use a specific maintenance server pool and rewrite all URLs to maintenance.php
acl match_all always_true
use_backend maint_pool if match_all
reqirep ^GET\(.*)\HTTP\(.*) GET\ /maintenance.php\ HTTP/\2
```


가상 서버 추가

NSX Edge 내부 또는 업링크 인터페이스를 가상 서버로 추가합니다.

사전 요구 사항

- 애플리케이션 프로파일을 사용할 수 있는지 확인합니다. [애플리케이션 프로파일 생성](#)를 참조하십시오.
- 애플리케이션 규칙을 가상 서버에 연결하려는 경우 [애플리케이션 프로파일 생성](#)를 참조하십시오.
- 더 빠른 로드 밸런서를 사용하기 위해 가속을 사용하도록 설정하는 경우 로드 밸런서를 구성할 때 가속을 사용하도록 설정해야 합니다. [로드 밸런서 서비스 구성](#)를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **가상 서버(Virtual Servers)**를 클릭합니다.
- 6 **추가(Add)**(+) 아이콘을 클릭합니다.
- 7 **가상 서버 사용(Enable Virtual Server)**을 선택하여 이 가상 서버를 사용할 수 있게 합니다.
- 8 (선택 사항) NSX Edge 로드 밸런서에서 L7 로드 밸런서 엔진보다 더 빠른 L4 로드 밸런서 엔진을 사용하려면 **가속 사용(Enable Acceleration)**을 선택합니다.

참고 이 구성을 사용하려면 Edge에서 방화벽이 사용되도록 설정되어야 합니다.

애플리케이션 규칙, HTTP 유형 또는 쿠키 지속성과 같은 가상 서버 구성에서 L7 로드 밸런서 엔진을 사용하는 경우 가속 사용 여부와 관계없이 L7 로드 밸런서 엔진이 사용됩니다. [글로벌 구성]에서 **가속 사용(Acceleration Enabled)** 옵션을 선택해야 합니다.

show service loadbalancer virtual CLI 명령을 사용하여 사용 중인 로드 밸런서 엔진을 확인할 수 있습니다.

- 9 가상 서버와 연결할 애플리케이션 프로파일을 선택합니다.

추가할 가상 서버와 프로토콜이 동일한 애플리케이션 프로파일만 연결할 수 있습니다. 선택한 풀에서 지원되는 서비스가 나타납니다.

- 10 가상 서버의 설명과 이름을 입력합니다.

11 IP 주소 선택(Select IP Address)을 클릭하여 로드 밸런서가 수신하는 IP 주소를 설정하고 가상 서버가 처리하는 프로토콜을 입력합니다.

[IP 주소 선택] 대화상자에는 기본 IP 주소만 표시됩니다. 보조 IP 주소를 사용하여 VIP를 생성할 경우 수동으로 입력하십시오.

12 드롭다운 메뉴에서 가상 서버가 처리하는 프로토콜을 선택합니다.

13 로드 밸런서가 수신하는 포트 번호를 입력합니다.

서버 풀, 애플리케이션 프로파일 및 애플리케이션 규칙과 같은 가상 서버 구성을 공유하기 위한 포트 범위(예: 80,8001-8004,443)를 설정할 수도 있습니다.

FTP를 사용하려면 TCP 프로토콜에 포트 21이 할당되어야 합니다.

14 애플리케이션 규칙을 선택합니다.

15 [연결 제한] 섹션에서 가상 서버가 처리할 수 있는 최대 동시 연결 수를 입력합니다.

16 [연결 속도 제한] 섹션에서 초당 수신되는 최대 새 연결 요청 수를 입력합니다.

17 (선택 사항) 고급(Advanced) 탭을 클릭하고 애플리케이션 규칙을 추가하여 가상 서버에 연결합니다.

18 확인(OK)을 클릭합니다.

애플리케이션 프로파일 관리

애플리케이션 프로파일을 생성하고 이를 가상 서버에 연결한 후에는 기존 프로파일을 업데이트하거나 삭제하여 시스템 리소스를 절약할 수 있습니다.

애플리케이션 프로파일 편집

애플리케이션 프로파일을 편집할 수 있습니다.

절차

1 vSphere Web Client에 로그인합니다.

2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.

3 NSX Edge를 두 번 클릭합니다.

4 관리(Manage) 탭을 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.

5 왼쪽 탐색 패널에서 **애플리케이션 프로파일(Application Profiles)**을 클릭합니다.

6 프로파일을 선택하고 **편집(Edit)**() 아이콘을 클릭합니다.

7 트래픽, 지속성, 인증서 또는 암호 구성을 적절히 변경하고 **완료(Finish)**를 클릭합니다.

로드 밸런서에 대한 SSL 종료 구성

SSL 종료를 구성하지 않으면 HTTP 요청이 검사되지 않습니다. 로드 밸런서는 소스 및 대상 IP 주소와 암호화된 데이터를 확인합니다. HTTP 요청을 조사하려는 경우 로드 밸런서에서 SSL 세션을 종료한 다음 셀 풀에 대한 새 SSL 세션을 생성할 수 있습니다.

사전 요구 사항

관리 > 설정 > 인증서(Manage > Settings > Certificates)로 이동하여 유효한 인증서가 있는지 확인합니다. 다음과 같이 로드 밸런서에 대한 인증서를 업로드할 수 있습니다.

- PEM 형식으로 또는
- CSR 생성 또는
- 자체 서명된 인증서 생성

절차

- 1 애플리케이션 프로파일의 **관리 > 로드 밸런서 > 애플리케이션 프로파일(Manage > Load Balancer > Application Profiles)**에서 다음을 수행합니다.
- 2 드롭다운 메뉴에서 **HTTPS** 유형을 선택합니다.
- 3 **SSL 통과 사용(Enable SSL Passthrough)**이 선택 취소되어 있는지 확인합니다.
- 4 **서비스 인증서 구성(Configure Service Certificate)**이 선택되어 있는지 확인합니다.

- 5 목록에서 해당 인증서를 선택합니다.

Edit Profile

Name:

Type:

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates **Pool Certificates**

Service Certificates **CA Certificates** **CRL**

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

애플리케이션 프로파일 삭제

애플리케이션 프로파일을 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **애플리케이션 프로파일(Application Profiles)**을 클릭합니다.
- 6 프로파일을 선택하고 **삭제(Delete)** 아이콘을 클릭합니다.

서비스 모니터 관리

서비스 모니터는 로드 밸런서에 대한 상태 점검 매개 변수를 정의합니다.

HA(고가용성)에서 로드 밸런서 서비스 모니터를 사용하는 경우 전용 인터페이스에서 HA를 사용하도록 설정해야 합니다.

서비스 모니터를 생성하고 풀에 연결한 후에 기존 서비스 모니터를 업데이트하거나 삭제하여 시스템 리소스를 절약할 수 있습니다.

서비스 모니터에 대한 자세한 내용은 [서비스 모니터 생성](#)을 참조하십시오.

서비스 모니터 편집

서비스 모니터를 편집할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **서비스 모니터링(Service Monitoring)**을 클릭합니다.
- 6 서비스 모니터를 선택하고 **편집(Edit)** 아이콘을 클릭합니다.
- 7 필요한 내용을 변경하고 **확인(OK)**을 클릭합니다.

서비스 모니터 삭제

서비스 모니터를 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **서비스 모니터링(Service Monitoring)**을 클릭합니다.
- 6 서비스 모니터를 선택하고 **삭제>Delete)** 아이콘을 클릭합니다.


서버 풀 관리

로드 밸런서 분산을 관리하기 위해 서버 풀을 추가한 후에는 기존 풀을 업데이트하거나 삭제하여 시스템 리소스를 절약할 수 있습니다.

서버 풀 편집

서버 풀을 편집할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭하고 로드 밸런서(Load Balancer) 탭을 클릭합니다.
- 5 풀 탭으로 이동합니다.
- 6 편집할 풀을 선택합니다.
- 7 편집(Edit)() 아이콘을 클릭합니다.
- 8 필요한 내용을 변경하고 확인(OK)을 클릭합니다.

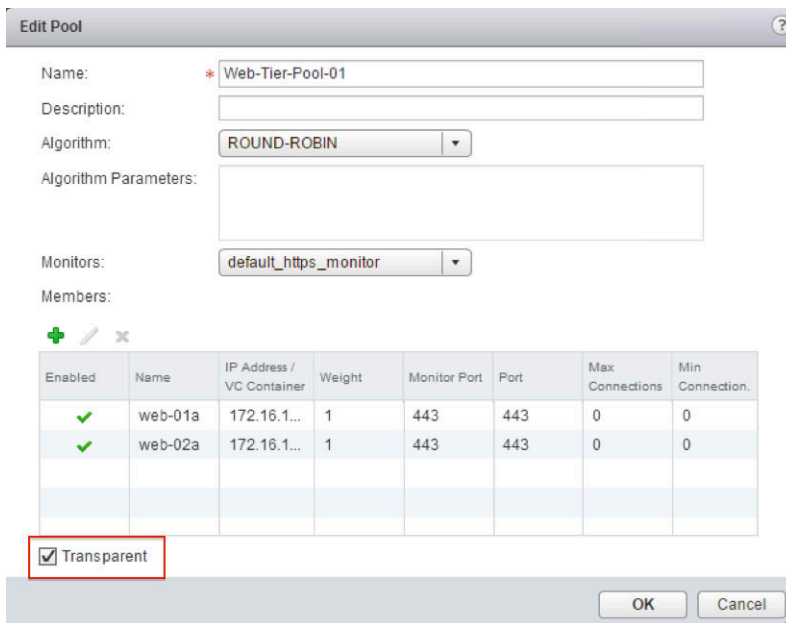
투명 모드를 사용하도록 로드 밸런서 구성

[투명]은 클라이언트 IP 주소를 백엔드 서버에 표시할지 여부를 나타냅니다. [투명]을 선택하지 않을 경우 (기본값) 백엔드 서버는 트래픽 소스 IP를 로드 밸런서 내부 IP로 인식합니다. [투명]을 선택하는 경우 소스 IP는 실제 클라이언트 IP이고 NSX Edge는 서버 응답 경로에 있어야 합니다. 일반적인 설계는 서버 기본 게이트웨이를 NSX Edge로 사용하는 것입니다.

자세한 내용은 [장 15 논리적 로드 밸런서](#)를 참조하십시오.

절차

- ◆ 서버 풀 구성의 관리 > 로드 밸런서 > 풀(Manage > Load Balancer > Pools)에서 투명 모드를 사용하도록 설정합니다.



Edit Pool

Name: * Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_https_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	web-01a	172.16.1...	1	443	443	0	0
✓	web-02a	172.16.1...	1	443	443	0	0

☒ Transparent

OK Cancel

서버 풀 삭제

서버 풀을 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 풀 탭으로 이동합니다.
- 6 삭제할 풀을 선택합니다.
- 7 **삭제>Delete)(X)** 아이콘을 클릭합니다.

풀 통계 표시

풀 및 연결된 풀 멤버의 최신 상태를 볼 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **풀(Pools)**을 클릭합니다.
- 6 필요한 풀을 선택하고 **풀 통계 표시(Show Pool Statistics)** 링크를 클릭합니다.

풀 상태는 [UP] 또는 [DOWN]일 수 있습니다. 풀의 모든 멤버가 DOWN 상태면 풀이 [DOWN]으로 표시되고, 그렇지 않으면 [UP]으로 표시됩니다.

멤버 상태는 다음 중 하나일 수 있습니다.

- **UP:** 멤버가 사용되도록 설정되어 있고 멤버 상태는 UP입니다. 또는 풀에서 모니터가 정의되어 있지 않습니다.
- **DOWN:** 멤버가 사용되도록 설정되어 있고 멤버 상태는 DOWN입니다.
- **MAINT:** 멤버가 사용되지 않도록 설정되어 있습니다.
- **DRAIN:** 멤버가 추출 상태입니다.


가상 서버 관리

가상 서버를 추가한 후에는 기존 가상 서버 구성을 업데이트하거나 삭제할 수 있습니다.

가상 서버 편집

가상 서버를 편집할 수 있습니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭하고 로드 밸런서(Load Balancer) 탭을 클릭합니다.
- 5 가상 서버(Virtual Servers) 탭을 클릭합니다.
- 6 편집할 가상 서버를 선택합니다.
- 7 편집(Edit)() 아이콘을 클릭합니다.
- 8 필요한 내용을 변경하고 완료(Finish)를 클릭합니다.

가상 서버 삭제

가상 서버를 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭하고 로드 밸런서(Load Balancer) 탭을 클릭합니다.
- 5 가상 서버(Virtual Servers) 탭을 클릭합니다.
- 6 삭제할 가상 서버를 선택합니다.
- 7 삭제>Delete)() 아이콘을 클릭합니다.

애플리케이션 규칙 관리

애플리케이션 규칙을 생성하여 애플리케이션 트래픽을 구성한 후에는 기존 규칙을 편집하거나 제거할 수 있습니다.

애플리케이션 규칙 편집

HAProxy 구문을 사용하여 애플리케이션 트래픽을 조작하기 위한 애플리케이션 규칙을 추가하거나 편집합니다.

애플리케이션 규칙 구문에 대한 내용은 <http://cbonte.github.io/haproxy-dconv/>의 HAProxy 설명서를 참조하십시오.

일반적으로 사용되는 애플리케이션 규칙의 예는 [애플리케이션 규칙 예](#)를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **애플리케이션 규칙(Application Rules)**을 클릭합니다.
- 6 규칙을 선택하고 **편집(Edit)** 아이콘을 클릭합니다.
- 7 필요한 내용을 변경하고 **확인(OK)**을 클릭합니다.

애플리케이션 규칙 삭제

애플리케이션 규칙을 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 5 왼쪽 탐색 패널에서 **애플리케이션 프로파일(Application Profiles)**을 클릭합니다.
- 6 프로파일을 선택하고 **삭제>Delete)** 아이콘을 클릭합니다.

NTLM 인증을 사용하는 로드 밸런스 웹 서버

NSX 로드 밸런서 및 NTLM 인증에는 서버 연결이 유지되어야 합니다.

기본적으로 NSX 로드 밸런서는 각 클라이언트 요청 이후에 서버 TCP 연결을 닫지만 Windows NTLM(NT LAN Manager) 인증을 위해서는 인증된 요청의 수명 동안 같은 연결이 필요하며 요청이 지속되는 동안 연결이 유지되어야 합니다.

요청 간에 서버 연결이 열려 있으려면 NTLM 인증을 사용하는 웹 서버의 가상 IP 로드 밸런싱에 대한 다음 애플리케이션 규칙을 추가합니다.

```
add # NTLM authentication and keep the server connection open between requests
no option http-server-close
```

로드 밸런서 HTTP 연결 모드

NSX 6.1.5 이상에서 **x-forwarded-for**를 사용하도록 설정하는 경우 HTTP 연결 모드가 수동 닫기(option **httpclose**)에서 기본 HTTP 서버 닫기(option **http-server-close**) 모드로 변경됩니다. 이 경우 서버에서 응답을 받은 후에 서버 쪽 연결은 닫히지만 클라이언트 쪽 연결은 열린 상태를 유지합니다. NSX 6.1.5 이전 버전에서는 NSX 로드 밸런서가 연결을 미리 닫지 않았지만 양방향에서 **"Connection:close"** 헤더를 삽입하여 클라이언트 또는 서버에 연결을 닫도록 지시했습니다. NSX 6.1.5 이상으로 업그레이드한 후에 NSX 로드 밸런서에서 HTTP/HTTPS 트랜잭션이 실패하면 스크립트 option **httpclose**를 사용하여 애플리케이션 규칙을 추가하고 더 이상 작동하지 않는 가상 서버에 연결합니다.

HTTP 서버 닫기(기본값) - 서버 쪽 연결은 응답 끝이 수신되면 닫히고 클라이언트 쪽 연결은 열린 상태를 유지합니다. HTTP 서버 닫기는 클라이언트 측에 지연 시간(느린 네트워크)을, 서버 측에 가장 빠른 세션 재사용을 제공하여 서버 리소스를 절약합니다. 또한 연결을 유지할 수 없는 서버가 클라이언트 측면에서 연결 유지하도록 합니다. 이 모드는 가장 일반적인 사용 사례에 적합합니다. 특히 느린 클라이언트 쪽 네트워크 및 빠른 서버 쪽 네트워크에 적합합니다.

HTTP 연결 유지 - 모든 요청 및 응답이 처리되고 연결은 열린 상태를 유지하지만 응답과 새 요청 간은 유휴 상태가 됩니다. 장점은 트랜잭션 간 지연 시간이 줄어들고 서버 측에 필요한 처리 능력이 줄어듭니다. 활성 세션 수를 수용하도록 메모리 요구 사항이 늘어나며, 각 요청 후에 더 이상 연결이 닫히지 않으므로 메모리 요구 사항이 더 높아집니다. 클라이언트 쪽 유휴 시간 초과는 애플리케이션 규칙 **"timeout http-keep-alive [time]"** 을 통해 구성할 수 있습니다. 기본적으로 유휴 시간 초과는 1초입니다. 이 모드는 애플리케이션이 NTLM 인증을 요구할 때 필수입니다.

HTTP 터널 - 첫 번째 요청 및 응답만 처리되고 클라이언트와 서버 간에 터널이 설정되므로 HTTP 프로토콜의 추가 분석 없이도 소통할 수 있습니다. 설정된 연결은 클라이언트 및 서버 양 측에서 유지됩니다. 이 모드를 사용하도록 설정하려면 수동-닫기 모드, 서버-닫기 모드, 강제-닫기 모드 중 어떤 옵션도 설정하지 않아야 합니다.

HTTP 터널 모드는 다음 기능에 영향을 미치며 세션의 첫 번째 요청 및 응답에만 적용됩니다.

- 로그가 생성되지 않음
- HTTP 헤더 구문 분석
- HTTP 헤더 조작
- 쿠키 처리
- 콘텐츠 전환
- X-Forwarded-For 헤더 삽입

HTTP 수동 닫기 - 터널 모드와 동일하지만 클라이언트 및 서버 방향 둘 다로 **"Connection: close"** 헤더가 추가됩니다. 첫 번째 요청 및 응답이 교환된 후에 양쪽 끝이 닫힙니다. **"option httpclose"**가 설정되면 NSX 로드 밸런서는 HTTP 터널 모드에서 작동하고 각 방향으로 **"Connection: close"** 헤더가 있는지 확인합니다. 이 헤더가 없으면 **"Connection: close"** 헤더가 추가됩니다. 그러면 각 끝에서 각 전송 후에 TCP 연결이 능동적으로 닫히고 HTTP 닫기 모드로 전환됩니다. **"close"** 이외의 모든 연결 헤더는 제거됩니다. NSX 로드 밸런서에 의해 삽입된 후 클라이언트의 다음 요청에 의해 다시 운반되는 쿠키 같은 두 번째 및 후속 요청을 제대로 처리할 수 없는 애플리케이션은 터널 모드 또는 수동 닫기 모드를 사용할 수 있습니다.

일부 HTTP 서버는 "option httpclose"로 설정된 "Connection: close"를 수신할 때 반드시 연결을 닫지는 않을 수 있습니다. 또한 클라이언트가 연결을 닫지 않으면 시간 초과가 만료될 때까지 연결은 열린 상태를 유지합니다. 이로 인해 서버에서 많은 수의 동시 연결이 발생하고 로그에는 높은 전역 세션 시간이 표시됩니다. 이러한 이유로 이전 HTTP 1.0 브라우저와 호환되지 않습니다. 이 경우 "option forceclose"를 사용합니다. 그러면 서버가 응답할 경우 요청 연결이 능동적으로 닫힙니다. Option "forceclose"는 클라이언트의 승인을 대기할 필요가 없으므로 서버 연결이 더 빠르게 해제됩니다.

HTTP 강제 닫기 - 응답이 끝난 후에 클라이언트 및 서버 연결 둘다 NSX 로드 밸런서에 의해 능동적으로 닫힙니다. 일부 HTTP 서버는 "option httpclose"로 설정된 "Connection: close"를 수신할 때 반드시 연결을 닫지는 않을 수 있습니다. 또한 클라이언트가 연결을 닫지 않으면 시간 초과가 만료될 때까지 연결은 열린 상태를 유지합니다. 이로 인해 서버에서 많은 수의 동시 연결이 발생하고 로그에는 높은 전역 세션 시간이 표시됩니다. 이 경우 "option forceclose"는 서버가 응답을 끝내는 즉시 송신 서버 채널을 능동적으로 닫고 "option httpclose"를 사용할 때보다 더 빠르게 일부 리소스를 해제합니다.

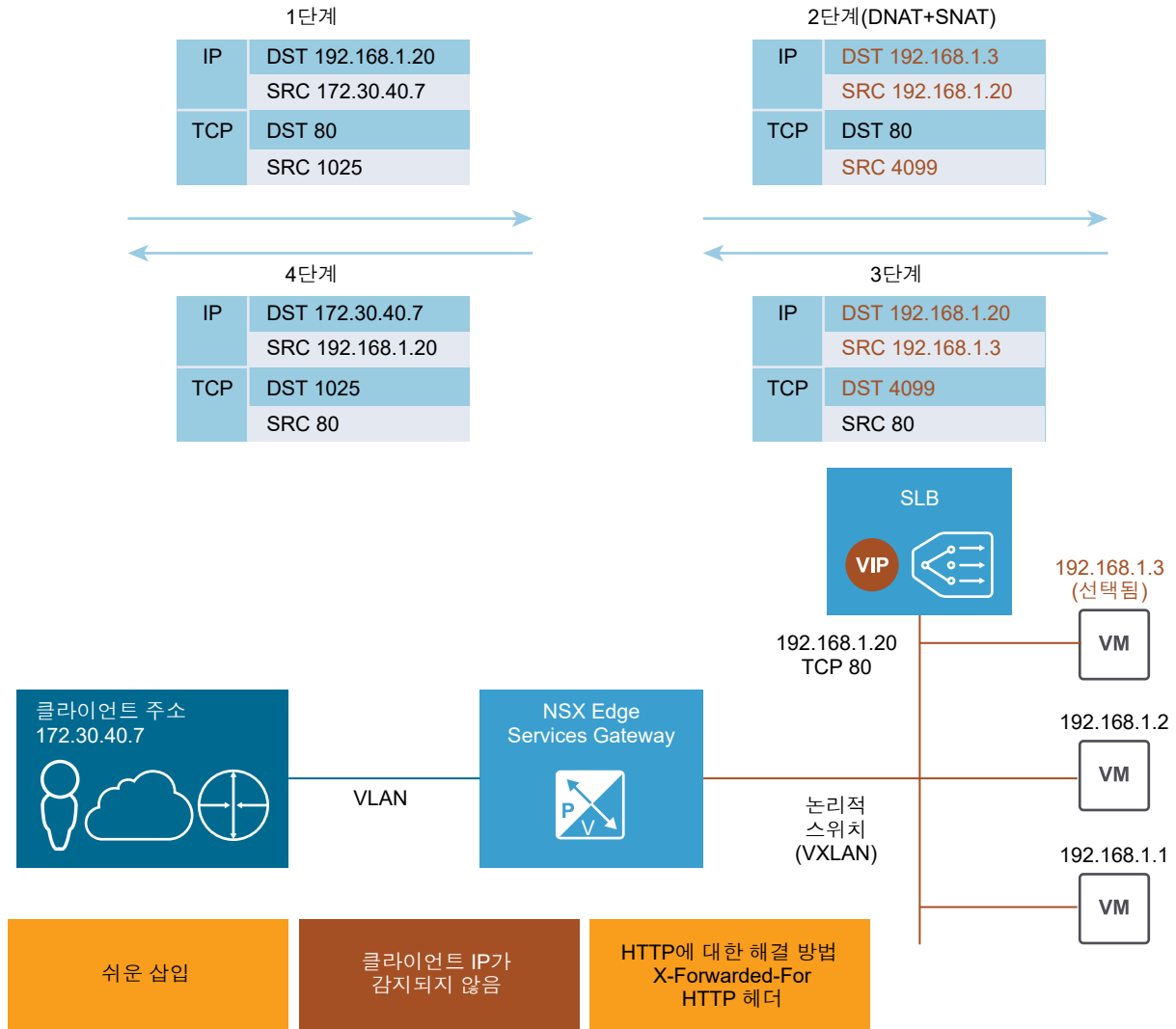
NSX	기본 연결 모드	X-Forwarded-For가 사용하도록 설정된 경우의 연결 모드	연결 모드를 전환하는 데 사용할 수 있는 애플리케이션 규칙
6.0.x, 6.1.0, 6.1.1	HTTP 서버 닫기	HAProxy 문서에 지정된 대로 각 요청에 강제로 xff가 추가되도록 "option httpclose"가 가상 서버에 자동으로 추가됩니다. 클라이언트에서 백엔드 서버에 각 요청이 발송될 때 각 요청에 xff 헤더가 추가됩니다.	아니요
6.1.2 - 6.1.4	HTTP 서버 닫기	HTTP 수동 닫기(가상 서버에 "option httpclose"가 자동으로 추가됨)	"no option http-server-close" "option httpclose" "no option httpclose"
6.1.5 - 6.1.x 6.2.0 - 6.2.2	HTTP 서버 닫기	클라이언트에서 백엔드 서버에 각 요청이 발송될 때 각 요청에 HTTP Server Close xff 헤더가 추가됩니다.	"no option http-server-close" "option httpclose" "no option httpclose"
6.2.3-6.2.5	HTTP 서버 닫기	클라이언트에서 백엔드 서버에 각 요청이 발송될 때 각 요청에 HTTP Server Close xff 헤더가 추가됩니다.	"no option http-server-close" "option httpclose" "no option httpclose"
6.2.3-6.2.5	HTTP 서버 닫기	클라이언트에서 백엔드 서버에 각 요청이 발송될 때 각 요청에 HTTP Server Close xff 헤더가 추가됩니다.	"no option http-server-close" "no option httpclose" "option httpclose"
6.2.5 - 6.2.x	HTTP 서버 닫기	클라이언트에서 백엔드 서버에 각 요청이 발송될 때 각 요청에 HTTP Server Close xff 헤더가 추가됩니다.	"no option http-server-close" "option http-keep-alive" "option http-tunnel" "option httpclose" "option forceclose"

NSX 로드 밸런서 구성 시나리오

NSX 로드 밸런서 구성 시나리오를 사용하여 요청된 중단 간 워크플로를 이해할 수 있습니다.

단일 암 로드 밸런서 구성

ESG(Edge Services Gateway)는 수신 클라이언트 트래픽에 대한 프록시로 간주될 수 있습니다.



프록시 모드에서 로드 밸런서는 자체 IP 주소를 소스 주소로 사용하여 백엔드 서버로 요청을 전송합니다. 백엔드 서버는 로드 밸런서에서 전송되는 모든 트래픽을 확인하고 응답을 로드 밸런서로 직접 보냅니다. 이 모드는 **SNAT** 모드 또는 비투명 모드라고도 합니다. 자세한 내용은 "**NSX 관리 가이드**"를 참조하십시오.

일반적인 **NSX** 단일 암 로드 밸런서는 논리적 라우터와는 별도로 해당 백엔드 서버가 있는 동일한 서브넷에 배포됩니다. **NSX** 로드 밸런서 가상 서버는 클라이언트의 수신 요청을 가상 IP에서 수신하고 해당 요청을 백엔드 서버로 발송합니다. 반환 트래픽의 경우 소스 IP 주소를 백엔드 서버에서 **VIP**(가상 IP) 주소로 변경한 다음 가상 IP 주소를 클라이언트로 보내기 위해 역방향 **NAT**가 필요합니다. 이 작업이 없으면 클라이언트의 연결이 끊어질 수 있습니다.

ESG는 트래픽을 수신하면 두 가지 작업을 수행합니다. 하나는 **VIP** 주소를 로드 밸런싱된 시스템 중 하나의 IP 주소로 변경하기 위한 **DNAT**(대상 네트워크 주소 변환)이고 다른 하나는 클라이언트 IP 주소를 **ESG** IP 주소와 교환하기 위한 **SNAT**(소스 네트워크 주소 변환)입니다.

그런 다음 **ESG** 서버는 로드 밸런싱된 서버로 트래픽을 전송하며, 로드 밸런싱된 서버는 응답을 **ESG**로 보낸 후 클라이언트로 다시 보냅니다. 이 옵션은 인라인 모드보다 구성하기가 훨씬 더 쉽지만 두 가지 잠재적인 문제가 있습니다. 첫째는 이 모드에는 전용 **ESG** 서버가 필요하다는 것이고 둘째는 로드 밸런서 서버가 원래 클라이언트 IP 주소를 알지 못한다는 것입니다. **HTTP/HTTPS** 애플리케이션에 대한 한 가지 해결 방법은 클라이언트 IP 주소가 요청의 **X-Forwarded-For** HTTP 헤더를 통해 백엔드 서버로 전달되도록 **HTTP** 애플리케이션 프로파일에서 **[X-Forwarded-Forheader 삽입]**을 사용하도록 설정하는 것입니다.

HTTP/HTTPS 이외의 애플리케이션에 대한 백엔드 서버에 클라이언트 IP 주소 가시성이 필요한 경우 IP 풀을 투명하게 구성할 수 있습니다. 클라이언트가 백엔드 서버와 동일한 서브넷에 있지 않은 경우 인라인 모드가 권장됩니다. 그렇지 않은 경우 백엔드 서버의 기본 게이트웨이로 로드 밸런서 IP 주소를 사용해야 합니다.

참고 일반적으로 연결 무결성을 보장하는 방법에는 다음 세 가지가 있습니다.

- 인라인/투명 모드
- **SNAT**/프록시/비투명 모드(위에 설명됨)
- **DSR**(직접 서버 반환) - 현재 지원되지 않습니다.

DSR 모드에서 백엔드 서버는 클라이언트에 직접 응답합니다. 현재 **NSX** 로드 밸런서는 **DSR**을 지원하지 않습니다.

절차

- 1 예를 들어 **SSL** 오프로드를 사용하여 단일 암 가상 서버를 구성해보겠습니다. **Edge**를 두 번 클릭한 다음 **관리 > 설정 > 인증서(Manage > Settings > Certificate)**를 선택하여 인증서를 생성합니다.

2 관리 > 로드 밸런서 > 글로벌 구성 > 편집(Manage > Load Balancer > Global Configuration > Edit)

을 선택하여 로드 밸런서 서비스를 사용하도록 설정합니다.

Edit Load balancer global configuration

☒ Enable Load Balancer

☐ Enable Acceleration

☐ Logging

Log Level: **Info** ▼

☐ Enable Service Insertion

Service Definition:

Service Configuration:

Deployment Specification:

3 관리 > 로드 밸런서 > 애플리케이션 프로파일(Manage > Load Balancer > Application Profiles)을

선택하여 HTTPS 애플리케이션 프로파일을 생성합니다.

New Profile ?

Name:

Type: **HTTPS** ▼

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: **None** ▼

Cookie Name:

Mode: ▼

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certifica... Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

참고 위의 스크린샷은 문서 용도로만 자체 서명된 인증서를 사용합니다.

4 필요한 경우 관리 > 로드 밸런서 > 서비스 모니터링(Manage > Load Balancer > Service Monitoring)

을 클릭하고 기본 서비스 모니터링을 편집하여 기본 HTTP/HTTPS에서 특정 URL/URI로 변경합니다.

5 관리 > 로드 밸런서 > 풀(Manage > Load Balancer > Pools)을 선택하여 서버 풀을 생성합니다.

SNAT 모드를 사용하려면 풀 구성에서 **투명(Transparent)** 확인란을 선택 취소된 상태로 둡니다.

Edit Pool

Name: * Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_https_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	web-01a	172.16.10.11	1	443	443	0	0
✓	web-02a	172.16.10.12	1	443	443	0	0

☐ Transparent

OK Cancel

VM이 나열되고 사용되도록 설정되어 있는지 확인합니다.

6 필요한 경우 **관리 > 로드 밸런서 > 풀 > 풀 통계 표시(Manage > Load Balancer > Pools > Show Pool Statistics)**를 클릭하여 상태를 확인합니다.

멤버 상태가 [UP]인지 확인합니다.

7 관리 > 로드 밸런서 > 가상 서버(Manage > Load Balancer > Virtual Servers)를 선택하여 가상 서버를 생성합니다.

UDP 또는 고성능 TCP에 대해 L4 로드 밸런서를 사용하려면 **가속 사용(Enable Acceleration)**을 선택합니다. **가속 사용(Enable Acceleration)**을 선택하는 경우 L4 SNAT에서 방화벽이 필요하므로 로드 밸런서 NSX Edge에서 방화벽 상태가 **사용(Enabled)**인지 확인합니다.

General Advanced

☒ Enable Virtual Server
☐ Enable Acceleration

Application Profile: * OneArmWeb-01 ▼

Name: * Web-Tier-VIP-01

Description:

IP Address: * 172.16.10.10 ✕ Select IP Address

Protocol: HTTPS ▼

Port: * 443

Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

IP 주소가 서버 풀에 연결되어 있는지 확인합니다.

- 8 필요한 경우 애플리케이션 규칙을 사용하고 있으면 **관리 > 로드 밸런서 > 애플리케이션 규칙(Manage > Load Balancer > Application Rules)**에서 구성을 확인합니다.

Add Application Rule ?

Name: App-Rule-1

Script: # A sample application rule to log the name of the virtual server
capture request header Host len 32

- 9 애플리케이션 규칙을 사용하는 경우 **관리 > 로드 밸런서 > 가상 서버 > 고급(Manage > Load Balancer > Virtual Servers > Advanced)**에서 애플리케이션 규칙이 가상 서버에 연결되어 있는지 확인합니다.

지원되는 예제를 보려면 <https://communities.vmware.com/docs/DOC-31772>를 참조하십시오.

Edit Virtual Server ?

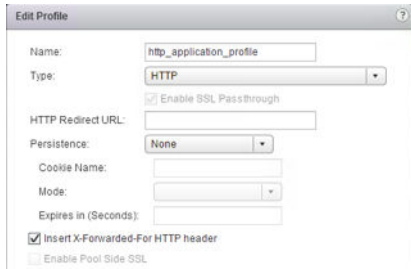
General **Advanced**

Application Rules:

+ ✕ ⇅ ⇅ Filter

Rule Id	Name	Script
applicationRule-1	App-rule-1	capture request he...

비투명 모드에서 백엔드 서버는 클라이언트 IP를 볼 수 없으나 로드 밸런서 내부 IP 주소를 볼 수 있습니다. HTTP/HTTPS 트래픽에 대한 해결 방법으로 **X-Forwarded-For HTTP 헤더 삽입(Insert X-Forwarded-For HTTP header)**을 선택합니다. 이 옵션을 선택하면 Edge 로드 밸런서는 클라이언트 소스 IP 주소 값과 함께 "X-Forwarded-For" 헤더를 추가합니다.



시나리오: Platform Services Controller에 대한 NSX 로드 밸런서 구성

PSC(Platform Services Controller)는 vCenter Single Sign-On, 라이선싱, 인증서 관리 및 서버 예약과 같은 인프라 보안 기능을 제공합니다.

NSX 로드 밸런서를 구성한 후에 vCenter Single Sign-On에 대한 NSX Edge 디바이스 업링크 인터페이스 IP 주소를 제공할 수 있습니다.

사전 요구 사항

- 기술 자료에 나열된 PSC 고가용성 준비 작업을 수행합니다. <http://kb.vmware.com/kb/2113315>를 참조하십시오.
- 첫 번째 PSC 노드의 /ha/lb.crt 및 /ha/lb_rsa.key를 저장하여 인증서를 구성합니다.
- NSX Edge 디바이스가 구성되어 있는지 확인합니다.
- VIP를 구성하기 위한 하나 이상의 업링크가 있는지와 내부 논리적 스위치에 인터페이스 하나가 연결되어 있는지 확인합니다.

절차

- 1 NSX Edge에 PSC CA 인증서를 추가합니다.
 - a PSC root.cer 및 인증서, OpenSSL 명령에서 생성한 RSA 및 암호를 저장합니다.
 - b Edge를 두 번 클릭하고 **관리(Manage) > 설정(Settings) > 인증서(Certificate)**를 선택합니다.
 - c 저장된 내용 root.cer 파일을 CA 인증서 내용에 추가합니다.
 - d 저장된 암호를 개인 키 섹션에 추가합니다.
- 2 로드 밸런서 서비스를 사용하도록 설정합니다.
 - a **관리(Manage) > 로드 밸런서(Load Balancer) > 편집(Edit)**을 선택합니다.
 - b **로드 밸런싱 사용(Enable Load Balancing)** 및 **로깅(Logging)** 옵션을 선택합니다.

3 TCP 및 HTTPS 프로토콜을 사용하여 애플리케이션 프로파일을 생성합니다.

- a 관리(Manage) > 로드 밸런서(Load Balancer) > 애플리케이션 프로파일(Application Profiles)을 선택합니다.
- b TCP 애플리케이션 프로파일을 생성합니다.

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso_tcp_profile
- Type:** TCP
- Enable SSL Passthrough:** ☐
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- Insert X-Forwarded-For HTTP header:** ☐
- Enable Pool Side SSL:** ☐
- Certificates:** Virtual Server Certificates (selected), Pool Certificates
- Service Certificates:** (selected), CA Certificates, CRL
- Configure Service Certificate:** ☐

Common Name	Issuer	Validity
NSX-ESG-1-0.system	CA	Thu Jul 30 2015 - Thu
- Cipher:** (empty)
- Client Authentication:** Ignore

Buttons: OK, Cancel

- c HTTPS 애플리케이션 프로파일을 생성합니다.

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso_https_profile
- Type:** HTTPS
- Enable SSL Passthrough:** ☐
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- Insert X-Forwarded-For HTTP header:** ☐
- Enable Pool Side SSL:** ☒
- Certificates:** Virtual Server Certificates (selected), Pool Certificates
- Service Certificates:** (selected), CA Certificates, CRL
- Configure Service Certificate:** ☒

Common Name	Issuer	Validity
NSX-ESG-1-0.system	CA	Thu Jul 30 2015 - Thu
- Cipher:** (empty)
- Client Authentication:** Ignore

Buttons: OK, Cancel

4 애플리케이션 풀을 생성하여 멤버 PSC 노드를 추가합니다.

- a 관리(Manage) > 로드 밸런서(Load Balancer) > 풀(Pools)을 선택합니다.
- b 모니터 포트 443이 있는 두 애플리케이션 풀을 생성합니다.

PSC 노드 IP 주소를 사용합니다.

Edit Pool

Name: * sso_tcp_pool1

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168....	1	443		0	0
✓	PSC02	192.168....	1	443		0	0

☐ Transparent

OK Cancel

- c 모니터 포트 389가 있는 두 애플리케이션 풀을 생성합니다.

PSC 노드 IP 주소를 사용합니다.

New Pool

Name: * sso_tcp_pool2

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168....	1	389		0	0
✓	PSC02	192.168....	1	389		0	0

☐ Transparent

OK Cancel

5 TCP 및 HTTPS 프로토콜에 대한 가상 서버를 생성합니다.

- a 관리(Manage) > 로드 밸런서(Load Balancer) > 가상 서버(Virtual Servers)를 선택합니다.
- b TCP VIP에 대한 가상 서버를 생성합니다.

The 'New Virtual Server' dialog box is shown with the 'General' tab selected. The 'Enable Virtual Server' checkbox is checked. The 'Application Profile' is set to 'sso_tcp_profile'. The 'Name' is 'sso_tcp_vip'. The 'IP Address' is '10.156.209.158' with a 'Select IP Address' link. The 'Protocol' is 'TCP'. The 'Port' is '389,636,2012,2014,2020'. The 'Default Pool' is 'sso_tcp_pool2'. The 'Connection Limit' and 'Connection Rate Limit' fields are empty.

- c HTTPS VIP에 대한 가상 서버를 생성합니다.

The 'New Virtual Server' dialog box is shown with the 'General' tab selected. The 'Enable Virtual Server' checkbox is checked. The 'Application Profile' is set to 'sso_https_profile'. The 'Name' is 'sso_https_vip'. The 'IP Address' is '10.156.209.158' with a 'Select IP Address' link. The 'Protocol' is 'HTTPS'. The 'Port' is '443'. The 'Default Pool' is 'sso_tcp_pool1'. The 'Connection Limit' and 'Connection Rate Limit' fields are empty.

시나리오: SSL 오프로딩

Edge는 클라이언트 HTTPS(SSL 세션)를 종료합니다. Edge는 서버에 대한 HTTP의 클라이언트 로드를 밸런싱합니다. L7 애플리케이션 규칙을 적용할 수 있습니다.

절차

- 1 웹 서버 인증서를 가져옵니다.
 - a vSphere Web Client에 로그인합니다.
 - b **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
 - c NSX Edge를 두 번 클릭합니다.
 - d **관리(Manage)**를 클릭하고 **설정(Settings)** 탭을 클릭합니다.
 - e 왼쪽 탐색 패널에서 **인증서(Certificates)**를 클릭합니다.
 - f **추가(Add)(+)** 아이콘을 클릭하고 **인증서(Certificate)**를 선택합니다. 자세한 내용은 [인증서 사용](#)을 참조하십시오.

- g 인증서 콘텐츠를 복사하여 **인증서 콘텐츠(Certificate Contents)** 텍스트 상자에 붙여 넣습니다. 텍스트에는 "-----BEGIN xxx-----" 및 "-----END xxx-----"가 포함되어야 합니다.

체인 인증서(서버 인증서 및 중간 또는 루트 CA 인증서)에 대해 **인증서(Certificate)** 옵션을 선택합니다. 다음은 체인 인증서 콘텐츠 예입니다.

```
-----BEGIN CERTIFICATE-----
    Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Root cert
-----END CERTIFICATE-----
```

- h 개인 키 콘텐츠를 복사하여 **개인 키(Private Key)** 텍스트 상자에 붙여 넣습니다.

다음은 개인 키 콘텐츠의 예입니다.

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END RSA PRIVATE KEY-----
```

인증서 콘텐츠(인증서 또는 개인 키의 PEM)에는 다음 문자열 중 하나를 접두사로 붙여야 합니다.

```
-----BEGIN PUBLIC KEY-----
-----BEGIN RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
-----BEGIN NEW CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
-----BEGIN PKCS7-----
-----BEGIN X509 CERTIFICATE-----
-----BEGIN X509 CRL-----
-----BEGIN ATTRIBUTE CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN DSA PRIVATE KEY-----
-----BEGIN EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
```

인증서 및 개인 키의 전체 예를 보려면 [예: 인증서 및 개인 키](#) 항목을 참조하십시오.

참고 다음 접두사는 NSX Manager에서 지원되지 않습니다.

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

2 HTTPS 애플리케이션 프로파일을 생성합니다.

- a vSphere Web Client에 로그인합니다.
- b **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.

- c NSX Edge를 두 번 클릭합니다.
 - d **관리(Manage)**를 클릭한 다음 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
 - e 왼쪽 탐색 패널에서 **애플리케이션 프로파일(Application Profile)**을 클릭합니다. 자세한 내용은 [애플리케이션 프로파일 관리](#)를 참조하십시오.
 - f 다음 매개 변수를 사용하여 새 애플리케이션 프로파일을 생성합니다.
 - 목록에서 유형으로 **HTTPS**를 선택합니다.
 - **서비스 인증서 구성(Configure Service Certificates)** 확인란을 선택합니다.
 - 1단계에서 구성한 서비스 인증서를 선택합니다.
- 3** 가상 서버를 생성합니다.
- a vSphere Web Client에 로그인합니다.
 - b **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
 - c NSX Edge를 두 번 클릭합니다.
 - d **관리(Manage)**를 클릭한 다음 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
 - e 왼쪽 탐색 패널에서 **가상 서버(Virtual Servers)**를 클릭합니다. 자세한 내용은 [가상 서버 관리](#) 항목을 참조하십시오.
 - f 다음 매개 변수를 사용하여 새 가상 서버를 생성합니다.
 - **가상 서버 사용(Enable Virtual Server)** 확인란을 선택하여 가상 서버를 사용할 수 있게 설정합니다.
 - 프로토콜로 **HTTPS**를 선택합니다.
 - HTTP 서버(HTTPS 서버 아님)로 구성된 기본 풀을 선택합니다.
 - 2단계에서 구성한 애플리케이션 프로파일을 선택합니다.

예: 인증서 및 개인 키

다음은 인증서 및 개인 키의 예입니다.

웹 서버 인증서

```
-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjET
MBEGA1UECAwKU29tZS1TdG9ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp
bWkxDTALBgNVBAMBE5TQlUxEDA0BgNVBAMMB0RpbWkgQ00ExGZAZBgkqhkiG9w0B
CQEWDRpbw1AZGltS5mcjAeFw0xNDAMjgyMDM2NTVaFw0yNDAMjYyMDM2NTVa
MFsxZCZAJBgNVBAYTAKZSMRMwEQYDVQQIDApTb211LVN0YXRIMSEwHwYDVQQKDBHJ
bnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxZDASBgNVBAMMC3d3dy5kaW1pLmZyMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpnaPKLIKdvx98KW68Lz8pGa
RRcYersNGqPjpi fMVjjE8LuCoXgPU0HePnNTUjpShBnynKCvrtWhN+haKbSp+QWX
SxiTrw99HBfA11MDQyWcukoEb9Cw6INctVUN4iRvkn9T8E6q174RbcnwA/7yTc7p
1NCvw+6B/aAN9l1G2pQXgRdYC/+G6o1IZEHtWhqzE97nY5QKNuUVD0V09dc5CDYB
```

```
aKjgetwvw6DFk/GRd0SEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os6Dau
ZkChSRyc/Whvurx6o85D6qpywo8xwNaLZHxTQPgcIA5su9ZIytv9LH2E+lSwwID
AQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQFfH1PcGVuU1NMIEdlbmVy
YXR1ZCBBDXJ0aWZpY2F0ZTAuBgNVHQ4EFgQU+tugFtyN+cXe1wxUqeA7X+yS3bgw
HwYDVR0jBBgwFoAUhMwqkbBrGp87HxfvvgPnlgGVR64wDQYJKoZIhvcNAQEFBQAD
ggEBAIEEmqqhEzeXZ4CKhE5UM9vCKzkj5Iv9TFs/a9CcQuepzplT7YVmevBFN0c0
+1ZyR4tXgi4+5MHGzhYCIvHo4hKqYm+J+o5mwQInflqoAHu07CLD3WNa1sKcVUV
vepIxc/1aHzRg+dPeEHt0MDF0w13YdUc2FH6AqEdcEL4aV5PXq2eYR8hR4zKbc1
fBtuqUsvA8NWSIyzQ16fyGve+ANf6vXvUizyvwDrPrv/kfvLNa3ZPnLMMxU98Mvh
PXy3PkB8++6U4Y3vdk2Ni2WYYLIls8yqbM4327IKmkDc2TimS8u60CT47mKU7aDY
cbTV5RDkrLaYwm5yqlTIglvCv7o=
-----END CERTIFICATE-----
```

체인이 있는 웹 서버 인증서(루트 CA 포함)

```
-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjET
MBEGA1UECAwKU29tZS1tdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp
bWkxDTALBgNVBASMBE5TQlUxEDA0BgNVBAMMB0RpbWkgQ0ExGzAZBgkqhkiG9w0B
CQEWdGRpbWlAZGltas5mcjAeFw0xNDAMjgyMDM2NTVaFw0yNDAMjYyMDM2NTVa
MFsxZCZAJBgNVBAYTAkZSMRMwEQYDVQQIDApTb211LVN0YXRlMSEwHwYDVQQKBHJ
bnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxZDASBgNVBAMMC3d3dy5kaW1pLmZyMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpnaPKLIKdvx98KW681z8pGa
RRcYersNGqPjpiFMVjje8LuCoXgPU0HePnNTUjPshBnynKCvrtWhN+haKbSp+QWX
SxiTrw99HBfAl1MDQyWcukoEb9Cw6INctVUN4iRvkn9T8E6q174RbcnwA/7yTc7p
1NCvw+6B/aAN91G2pQXgRdYC/+G6o1IEHtWhqzE97nY5QKNUUVD0V09dc5CDYB
aKjgetwvw6DFk/GRd0SEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os6Dau
ZkChSRyc/Whvurx6o85D6qpywo8xwNaLZHxTQPgcIA5su9ZIytv9LH2E+lSwwID
AQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQFfH1PcGVuU1NMIEdlbmVy
YXR1ZCBBDXJ0aWZpY2F0ZTAuBgNVHQ4EFgQU+tugFtyN+cXe1wxUqeA7X+yS3bgw
HwYDVR0jBBgwFoAUhMwqkbBrGp87HxfvvgPnlgGVR64wDQYJKoZIhvcNAQEFBQAD
ggEBAIEEmqqhEzeXZ4CKhE5UM9vCKzkj5Iv9TFs/a9CcQuepzplT7YVmevBFN0c0
+1ZyR4tXgi4+5MHGzhYCIvHo4hKqYm+J+o5mwQInflqoAHu07CLD3WNa1sKcVUV
vepIxc/1aHzRg+dPeEHt0MDF0w13YdUc2FH6AqEdcEL4aV5PXq2eYR8hR4zKbc1
fBtuqUsvA8NWSIyzQ16fyGve+ANf6vXvUizyvwDrPrv/kfvLNa3ZPnLMMxU98Mvh
PXy3PkB8++6U4Y3vdk2Ni2WYYLIls8yqbM4327IKmkDc2TimS8u60CT47mKU7aDY
cbTV5RDkrLaYwm5yqlTIglvCv7o=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDyTCCArGgAwIBAgIBADANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjET
MBEGA1UECAwKU29tZS1tdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp
bWkxDTALBgNVBASMBE5TQlUxEDA0BgNVBAMMB0RpbWkgQ0ExGzAZBgkqhkiG9w0B
CQEWdGRpbWlAZGltas5mcjAeFw0xNDAMjgyMDI2NDRaFw0yNDAMjYyMDI2NDRa
MH8xCzAJBgNVBAYTAkZSMRMwEQYDVQQIDApTb211LVN0YXRlMQ4wDAYDVQQHDAVQ
YXJpczENMAsGA1UECgwERGltaTENMAsGA1UECwwETlNCVTEQMA4GA1UEAwwHRGlta
aSBDbQTEbMBkGCSqGSIb3DQEJARYMZGltUBkaW1pLmZyMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEauxuG4QeBIGXj/AB/YRLLtpgpTpGnDntVlgsycZrL
3qqyOdBNlwnvbc9etfY5iWzjeq7YZRr6i0dIV4sFNBR2NoK+YvdD9j1TRi7njZg0
d6zth0x1s0hCsDlV/YCL1CTcYDlKA/QiKeIQa7GU3Rh0t/KnAkr6mwoDbdKBQX1
D5HgQuXjiFdh5XRebxF1ZB3gH+0kCEaEZPrjFDApk0XNxEARZdpBLpbvQljtVXtj
HMsvrI0c7QqUSOU3GcbBMSHjT8cgg8ss492Go3bDQkIzTROz9QgDHaqDqTC9Hoe
vLIpTS+q/3BCY5AGWKL3CCR6dDyK6honn0R/8srezaN4PwIDAQABo1AwTjAdBgNV
HQ4EFgQUhMwqkbBrGp87HxfvvgPnlgGVR64wHwYDVR0jBBgwFoAUhMwqkbBrGp87
HxfvvgPnlgGVR64wDAYDVR0TBAlUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAyq
vhm5wAEKmvRkXRjeb5kiEIp7oZAFkYp6sKODuZ1VdkjMDD4wv46iqAe1QIIsfGwd
```



```
Dmv0oqSl+iPPy24ATMSZQBLO5K64Hw7Q8KPos0yD8gHSg2d4S0ukj+FD2IjAH17
a8auMw7TTHu6976JprQQktPADRcfodGd5UFiz/6ZgLzUE23cktJMc2Bt18B90ZII
J9ef2PZxZirJg10qF2KssDLJP5EC09K3EmovC5M5Aly++s8ayjBnNivtklYL1V0T
ZrpPgcndTHUA5KS/DuF40dXm0snCxLAKNP28pMowDLSYc6IjVrD4+qqw3f1b7yGb
bJcFgxKDeg5YecQ0Sg==
-----END CERTIFICATE-----
```

개인 키(암호 없음)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEEwIBAAKCAQEAwpnaPKLIKdvx98KW681z8pGaRRcYersNGqPjpiFMVjjE8LuC
oXgPU0HePnTUjPShBnynKCvrtWhN+haKbSp+QWXSxiTrW99HBfAl1MDQyWcukoE
b9Cw6INctVUN4iRvkn9T8E6q174RbcnwA/7yTc7p1NCvw+6B/aAN9l1G2pQXgRdY
C/+G6o1IIEHtWhqzE97nY5QKNuUVD0V09dc5CDYBaKjgetwwv6DFk/GRd0SEd/6b
W+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os6DauZkChSRyc/Whvurx6o85D6qpz
ywo8xwNaLZHxTQPgcIA5su9ZIyvtv9LH2E+lSwwIDAQABAoIBAFm18cD9a5pMqLW3
f9btTQz1sRL4Fvp7CmHSHxhvsjeHwhHckEe0ObkWTRsgkTsm1XLu5W8IITn0+1
iNr+78eB+rRGngdAXh8di0dkEy+8/Cee8tFI3jyutKdRlxMbwiKsouVviumoq3fx
OGQYwQ0Z2l/PvCwy/Y82ffq3ysC5gAJsbBYsCrg14bQo44ulrELE4SDws5HCjKYb
EI2b8c0MucqZS0txg9niLN/je2bo/I2HGSawibgc0dBms8k6TvsSrZMr3kJ506J+
77LGwKH37brVgbVYvbq6nWPL0xLG7dUv+7LWEo5qQaPy6aXb/zbckqLqu6/Ej0Ve
ydG5JQECgYEA9kKFTZD/WEVAreA0dzfeJRu8vlnwoagL7cJaoDxqXos4mcr5mPDT
kbWgFkLFFH/AyUnPB1K6BcJp1XK67B13ETUa3i9Q5t1WuZEobiKKBLFm9DDQJt43
uKZWJxBKFGSvFrYPtGZst719mZVcPct2CzPjEgN3Hlpt6fyw3e0rnoECgYEAxi0u
jwXC0muGaB7+0W2tR0PGEzbvVLEgdkAJ6TC/HoKM1A8r2u4hLTEJJCrLLTfw++4I
ddHE2dLeR4Q7058SfLphwgPmLDezN7WRLGr7Vyfuv7VmaHjGuC3Gv9aghnWD1A2Q
gBG9/R9oVfL0Dc7CgJgLeUtItCYC31bGT3yhV0McgYEA4k3DG4L+RN4PXDpHvK9I
pA1jXAJHEifeHnaw1d3vWkbSkvJmgVf+9U5VeV+OwRHN1qzPZV4suRI6M/8lK8rA
Gr4UnM4aqK4K/qkY4G05LKrik9Ev2CgqSLQDRA7CJQ+Jn3Nb50qg6hFnFPafN+J7
7juWln08wFYV4Atpdd+9XQECgYBxizkZFL+9Iqkf0cONvWAZGo+Dq1N0L3J4iTIk
w56CKWxyj88d4qB4eUU3yJ4uB4S9miaW/eLEwKZIBWpUPFAn0db7i6h3ZmP5ZL8Q
qS3nQCb9DULmU2/tU641eRUKAmIoka1g9sndKAZuWo+o6fdkIb1Rg0bk9XNn8R4r
psv+aQKBgB+CicExR30vycv5bnZN9EFIXNkaeMJUrYCXcRQNVrnUIUBvA08+jAe
CdLygS5RtgOLZib0IVERqWsp3EI1ACGuLts0vQ9GFLQGaN1SaMS40C9kvns1mLDu
LhIhYpJ8UsCVt5snWo2N+M+6ANh5tpWdQnEK6zILh4tRbuzaiHgB
-----END RSA PRIVATE KEY-----
```

시나리오: SSL 인증서 가져오기

SSL 종단 간: NSX Edge는 클라이언트 HTTPS(SSL 세션)를 종료합니다. Edge는 서버에 대한 새 HTTPS 연결에서 클라이언트를 로드 밸런싱합니다. L7 애플리케이션 규칙을 적용할 수 있습니다.

절차

- 1 웹 서버 인증서를 가져옵니다.
 - a vSphere Web Client에 로그인합니다.
 - b 네트워킹 및 보안(Networking & Security)를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
 - c NSX Edge를 두 번 클릭합니다.
 - d **관리(Manage)**를 클릭하고 **설정(Settings)** 탭을 클릭합니다.

- e 왼쪽 탐색 패널에서 **인증서(Certificates)**를 클릭합니다.
- f **추가(Add)(+)** 아이콘을 클릭하고 **인증서(Certificate)**를 선택합니다. 자세한 내용은 [인증서 사용](#)을 참조하십시오.
- g 인증서 콘텐츠를 복사하여 **인증서 콘텐츠(Certificate Contents)** 텍스트 상자에 붙여 넣습니다. 텍스트에는 "-----BEGIN xxx-----" 및 "-----END xxx-----"가 포함되어야 합니다.

체인 인증서(서버 인증서 및 중간 또는 루트 CA 인증서)에 대해 **인증서(Certificate)** 옵션을 선택합니다. 다음은 체인 인증서 콘텐츠 예입니다.

```
-----BEGIN CERTIFICATE-----
    Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Root cert
-----END CERTIFICATE-----
```

- h 개인 키 콘텐츠를 복사하여 **개인 키(Private Key)** 텍스트 상자에 붙여 넣습니다.

다음은 개인 키 콘텐츠의 예입니다.

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END RSA PRIVATE KEY-----
```

인증서 콘텐츠(인증서 또는 개인 키의 PEM)에는 다음 문자열 중 하나를 접두사로 붙여야 합니다.

```
-----BEGIN PUBLIC KEY-----
-----BEGIN RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
-----BEGIN NEW CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
-----BEGIN PKCS7-----
-----BEGIN X509 CERTIFICATE-----
-----BEGIN X509 CRL-----
-----BEGIN ATTRIBUTE CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN DSA PRIVATE KEY-----
-----BEGIN EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
```

인증서 및 개인 키의 전체 예를 보려면 [예: 인증서 및 개인 키](#) 항목을 참조하십시오.

참고 다음 접두사는 NSX Manager에서 지원되지 않습니다.

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

2 HTTPS 애플리케이션 프로파일을 생성합니다.

- a vSphere Web Client에 로그인합니다.
- b **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- c NSX Edge를 두 번 클릭합니다.
- d **관리(Manage)**를 클릭한 다음 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- e 왼쪽 탐색 패널에서 **애플리케이션 프로파일(Application Profile)**을 클릭합니다. 자세한 내용은 [애플리케이션 프로파일 관리](#)를 참조하십시오.
- f 다음 매개 변수를 사용하여 새 애플리케이션 프로파일을 생성합니다.
 - 목록에서 유형으로 **HTTPS**를 선택합니다.
 - **풀 측 SSL 사용(Enable Pool Side SSL)** 확인란을 선택합니다.
 - **서비스 인증서 구성(Configure Service Certificates)** 확인란을 선택합니다.
 - 1단계에서 구성한 서비스 인증서를 선택합니다.

3 가상 서버를 생성합니다.

- a vSphere Web Client에 로그인합니다.
- b **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- c NSX Edge를 두 번 클릭합니다.
- d **관리(Manage)**를 클릭한 다음 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- e 왼쪽 탐색 패널에서 **가상 서버(Virtual Servers)**를 클릭합니다. 자세한 내용은 [가상 서버 관리](#)를 참조하십시오.
- f 다음 매개 변수를 사용하여 새 가상 서버를 생성합니다.
 - **가상 서버 사용(Enable Virtual Server)** 확인란을 선택하여 가상 서버를 사용할 수 있게 설정합니다.
 - 프로토콜로 **HTTPS**를 선택합니다.
 - HTTPS 서버로 구성된 기본 풀을 선택합니다.
 - 2단계에서 구성한 애플리케이션 프로파일을 선택합니다.

시나리오: SSL 패스스루

Edge는 클라이언트 HTTPS(SSL 세션)를 종료하지 않습니다. Edge는 서버에 TCP 세션 로드를 밸런싱합니다. Edge가 아닌 서버에 대한 클라이언트 SSL 세션이 종료됩니다. L7 애플리케이션 규칙을 적용할 수 없습니다.

사전 요구 사항

참고 HTTPS 패스스루 시나리오에는 인증서가 필요하지 않습니다.

절차

1 HTTPS 애플리케이션 프로파일을 생성합니다.

- a vSphere Web Client에 로그인합니다.
- b **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- c NSX Edge를 두 번 클릭합니다.
- d **관리(Manage)**를 클릭한 다음 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- e 왼쪽 탐색 패널에서 **애플리케이션 프로파일(Application Profile)**을 클릭합니다. 자세한 내용은 [애플리케이션 프로파일 관리](#)를 참조하십시오.
- f 다음 매개 변수를 사용하여 새 애플리케이션 프로파일을 생성합니다.
 - 목록에서 유형으로 **HTTPS**를 선택합니다.
 - **SSL 패스스루 사용(Enable SSL Passthrough)** 확인란을 선택합니다.
 - 지속성으로 **없음(None)**을 선택합니다.

참고 HTTPS 패스스루 시나리오에는 인증서가 필요하지 않습니다.

2 가상 서버를 생성합니다.

- a vSphere Web Client에 로그인합니다.
- b **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- c NSX Edge를 두 번 클릭합니다.
- d **관리(Manage)**를 클릭한 다음 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- e 왼쪽 탐색 패널에서 **가상 서버(Virtual Servers)**를 클릭합니다. 자세한 내용은 [가상 서버 관리](#)를 참조하십시오.
- f 다음 매개 변수를 사용하여 새 가상 서버를 생성합니다.
 - **가상 서버 사용(Enable Virtual Server)** 확인란을 선택하여 가상 서버를 사용할 수 있게 설정합니다.
 - 프로토콜로 **HTTPS**를 선택합니다.
 - HTTPS 서버로 구성된 기본 풀을 선택합니다.
 - 1단계에서 구성한 애플리케이션 프로파일을 선택합니다.

참고 **가속 사용(Enable Acceleration)** 확인란이 선택되고 L7 관련 구성이 없으면 Edge에서 세션을 종료하지 않습니다.

가속 사용(Enable Acceleration) 확인란을 선택하지 않으면 세션은 L7 TCP 모드로 취급되고 Edge는 두 세션으로 종료합니다.

시나리오: SSL 클라이언트 및 서버 인증

SSL 클라이언트 및 서버 인증

클라이언트 인증

클라이언트는 HTTPS를 통해 웹 애플리케이션에 액세스합니다. HTTPS는 Edge VIP에서 종료되고 클라이언트 인증서를 요청합니다.

- 1 루트 CA와 함께 웹 서버 인증서를 가져옵니다. 자세한 내용은 [시나리오: SSL 인증서 가져오기](#)를 참조하십시오.
- 2 다음 매개 변수를 사용하여 HTTPS 애플리케이션 프로파일을 생성합니다.
 - a 목록에서 유형으로 **HTTPS**를 선택합니다.
 - b **가상 서버 인증서(Virtual Server Certificates)** 탭을 선택하고 **CA 인증서(CA Certificates)** 탭을 선택합니다. CA는 클라이언트 인증서를 확인하는 데 사용됩니다.
 - c 1단계에서 구성한 서비스 인증서를 선택합니다.
 - d 목록에서 클라이언트 인증을 **필수(Required)**로 선택합니다.

참고 클라이언트 인증(Client Authentication) 옵션이 **무시(Ignore)**로 설정되면 로드 밸런서는 클라이언트 인증서 인증을 무시합니다.

- 3 가상 서버를 생성합니다. 자세한 내용은 [시나리오: SSL 인증서 가져오기](#)를 참조하십시오.

참고 애플리케이션 프로파일에서 **풀 측 SSL 사용(Enable Pool Side SSL)** 옵션을 사용하지 않도록 설정하면 선택한 풀이 HTTP 서버로 구성됩니다. 애플리케이션 프로파일에서 **풀 측 SSL 사용(Enable Pool Side SSL)** 옵션을 사용하도록 설정하면 선택한 풀이 HTTPS 서버로 구성됩니다.

- 4 브라우저에서 루트 CA가 서명한 클라이언트 인증서를 가져옵니다.
- 5
 - a <https://www.sslshopper.com/ssl-converter.html> 웹 사이트로 이동합니다.
 - b 인증서 및 개인 키를 **pfx** 파일로 변환합니다. 인증서 및 개인 키의 전체 예를 보려면 [예: 인증서 및 개인 키](#) 항목을 참조하십시오.

Certificate File to Convert: Choose File client.crt

Private Key File: Choose File client.key

Chain Certificate File (optional): Choose File Dimi-CA.crt

Chain Certificate File 2 (optional): Choose File No file chosen

Type of Current Certificate: Standard PEM Detected type from file extension

Type To Convert To: PFX/PKCS#12

PFX Password:

- c 브라우저에서 **pfx** 파일을 가져옵니다.

서버 인증

클라이언트는 HTTPS를 통해 웹 애플리케이션에 액세스합니다. HTTPS가 Edge VIP에서 종료됩니다. Edge는 서버에 대한 새 HTTPS 연결을 설정하고, 서버 인증서를 요청한 후 확인합니다.

Edge에서 특정 암호만 수락됩니다.

- 1 서버 인증서 인증을 위해 웹 서버 인증서 및 루트 CA 인증서를 가져옵니다. 자세한 내용은 [시나리오: SSL 인증서 가져오기](#)을 참조하십시오.
- 2 다음 매개 변수를 사용하여 HTTPS 애플리케이션 프로파일을 생성합니다.
 - a 목록에서 유형으로 **HTTPS**를 선택합니다.
 - b **풀 측 SSL 사용(Enable Pool Side SSL)** 확인란을 선택합니다.
 - c **풀 인증서(Pool Certificates)** 탭을 선택하고 **CA 인증서(CA Certificates)** 탭을 선택합니다. CA는 백엔드 HTTPS 서버에서 클라이언트 인증서를 확인하는 데 사용됩니다.
 - d **서버 인증(Server Authentication)** 확인란을 선택합니다.
 - e 1단계에서 구성한 CA 인증서를 선택합니다.
 - f **암호(Ciphers)** 목록에서 필요한 암호를 선택합니다.

참고 암호가 승인된 암호 제품군에 없으면 기본값으로 다시 설정됩니다.

이전 버전에서 업그레이드한 후에 암호가 null/비어 있거나 이전 버전에서 승인된 암호 제품군에 포함되지 않았으면 기본값으로 다시 설정됩니다.

- 3 가상 서버를 생성합니다. 자세한 내용은 [시나리오: SSL 인증서 가져오기](#)을 참조하십시오.

참고 애플리케이션 프로파일에서 **풀 측 SSL 사용(Enable Pool Side SSL)** 옵션을 사용하지 않도록 설정하면 선택한 풀이 HTTP 서버로 구성됩니다. 애플리케이션 프로파일에서 **풀 측 SSL 사용(Enable Pool Side SSL)** 옵션을 사용하도록 설정하면 선택한 풀이 HTTPS 서버로 구성됩니다.

NSX Services 게이트웨이는 IP 주소 풀링, 일대일 정적 IP 주소 할당 및 외부 DNS 서버 구성을 제공합니다.

작동하는 NSX Edge 인스턴스가 있어야 위의 서비스를 사용할 수 있습니다. NSX Edge 설정에 대한 자세한 내용은 [NSX Edge 구성](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [DHCP 서비스 관리](#)
- [DHCP 릴레이 구성](#)
- [DNS 서버 구성](#)

DHCP 서비스 관리

NSX Edge는 IP 주소 풀링 및 일대일 정적 IP 주소 할당을 지원합니다. 정적 IP 주소 바인딩은 요청 클라이언트의 vCenter 관리 개체 ID 및 인터페이스 ID를 기반으로 합니다.

NSX Edge DHCP 서비스는 다음과 같은 지침을 따릅니다.

- DHCP 검색을 위해 NSX Edge 내부 인터페이스를 수신합니다.
- NSX Edge에서 내부 인터페이스의 IP 주소를 모든 클라이언트에 대한 기본 게이트웨이 주소로 사용하고(풀에 직접 연결하지 않는 경우는 제외), 컨테이너 네트워크에 대한 내부 인터페이스의 브로드캐스트 및 서브넷 마스크 값을 사용합니다.

다음과 같은 경우 클라이언트 가상 시스템에서 DHCP 서비스를 다시 시작해야 합니다.

- DHCP 풀, 기본 게이트웨이 또는 DNS 서버를 변경하거나 삭제한 경우
- NSX Edge 인스턴스의 내부 IP 주소를 변경한 경우

DHCP IP 풀 추가

DHCP 서비스에는 IP 주소 풀이 필요합니다.

IP 풀은 네트워크 내에 있는 순차적인 IP 주소 범위입니다. NSX Edge로 보호되고 주소가 바인딩되지 않은 가상 시스템에는 이 풀에서 IP 주소가 할당됩니다. IP 풀의 범위는 서로 교차할 수 없으므로 한 IP 주소는 한 IP 풀에만 속할 수 있습니다.

절차


- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭하고 **DHCP**를 클릭합니다.
- 5 **추가(Add)(+)** 아이콘을 클릭합니다.
- 6 [일반] 탭에서 풀을 구성합니다.

옵션	작업
DNS 자동 구성(Auto Configure DNS)	DHCP 바인딩에 DNS 서비스 구성을 사용하도록 선택합니다.
리스가 만료되지 않음(Lease never expires)	주소를 가상 시스템의 MAC 주소에 영구적으로 바인딩하도록 선택합니다. 이 옵션을 선택하면 리스 시간(Lease Time) 이 사용되지 않도록 설정됩니다.
시작 IP(Start IP)	풀의 시작 IP 주소를 입력합니다.
종료 IP(End IP)	풀의 종료 IP 주소를 입력합니다.
도메인 이름(Domain Name)	DNS 서버의 도메인 이름을 입력합니다. 이는 선택 사항입니다.
기본 이름 서버(Primary Name Server)	DNS 자동 구성(Auto Configure DNS) 을 선택하지 않은 경우 DNS 서비스에 대한 기본 이름 서버(Primary Nameserver) 를 입력합니다. 호스트 이름 대 IP 주소를 확인하려면 DNS 서버의 IP 주소를 입력해야 합니다. 이는 선택 사항입니다.
보조 이름 서버(Secondary Name Server)	DNS 자동 구성(Auto Configure DNS) 을 선택하지 않은 경우 DNS 서비스에 대한 보조 이름 서버(Secondary Nameserver) 를 입력합니다. 호스트 이름 대 IP 주소를 확인하려면 DNS 서버의 IP 주소를 입력해야 합니다. 이는 선택 사항입니다.
기본 게이트웨이(Default Gateway)	기본 게이트웨이 주소를 입력합니다. 기본 게이트웨이 IP 주소를 지정하지 않으면 NSX Edge 인스턴스의 내부 인터페이스가 기본 게이트웨이로 지정됩니다. 이는 선택 사항입니다.
서브넷 마스크(Subnet Mask)	서브넷 마스크를 지정합니다. 분산 라우터의 경우 서브넷 마스크가 Edge 인터페이스 또는 DHCP 릴레이의 서브넷 마스크와 동일해야 합니다.
리스 시간(Lease Time)	주소를 기본 시간(1일) 동안 클라이언트에 리스하도록 선택하거나, 값을 초 단위로 입력합니다. 리스가 만료되지 않음(Lease never expires) 을 선택한 경우 리스 시간을 지정할 수 없습니다. 이는 선택 사항입니다.

- 7 (선택 사항) [DHCP 옵션] 탭에서 DHCP 옵션을 구성합니다.

NSX 6.2.5 이상에서는 Edge Services Gateway에서 클래스 없는 정적 경로와 기본 게이트웨이를 둘 다 사용하여 DHCP 풀을 구성하는 경우 기본 게이트웨이가 클래스 없는 정적 경로로 추가됩니다.

옵션	작업
다음 서버(Next Server)	PXE boot 또는 bootp에 사용되는 다음 부팅 TFTP 서버입니다.
TFTP 서버 이름(옵션 66)(TFTP server name (option 66))	디바이스에서 부트 파일 이름에 지정된 파일을 다운로드하는 데 사용해야 하는 유니캐스트 IPv4 주소 또는 호스트 이름을 입력합니다(옵션 67).

옵션	작업
TFTP 서버 주소(옵션 150)(TFTP server address (option 150))	하나 이상의 TFTP 서버 IPv4 주소를 입력합니다.
부트 파일 이름(옵션 67)(Bootfile name (option 67))	TFTP 서버 이름에 지정된 서버에서 다운로드할 부트 파일의 파일 이름을 입력합니다(옵션 66).
인터페이스 MTU(옵션 26)(Interface MTU (option 26))	MTU(최대 전송 단위)는 조작화 없이 두 호스트 간에 전송될 수 있는 최대 프레임 크기입니다. 이 옵션은 인터페이스에서 사용할 MTU 크기를 지정합니다. 각 폴 및 정적 바인딩에 대해 하나의 MTU 크기(바이트)를 설정할 수 있습니다. MTU 최소값은 68 바이트이고 최대값은 65535바이트입니다. 인터페이스 MTU가 DHCP 서버에서 설정되지 않으면 DHCP 클라이언트는 인터페이스 MTU의 OS 기본 설정을 유지합니다.
클래스 없는 정적 경로(옵션 121)(Classless static route (option 121))	<p>각 클래스 없는 정적 경로 옵션에는 같은 대상의 여러 경로가 있을 수 있습니다. 각 경로에는 대상 서브넷, 서브넷 마스크, 다음 홉 라우터가 포함됩니다. 0.0.0.0/0은 정적 경로의 유효하지 않은 서브넷입니다. 클래스 없는 정적 경로 및 옵션 121에 대한 자세한 내용은 RFC 3442를 참조하십시오.</p> <p>a 추가(Add)( 아이콘을 클릭합니다.</p> <p>b 대상 및 다음 홉 라우터 IP 주소를 입력합니다.</p>

8 **확인(OK)**을 클릭합니다.

DHCP 서비스 사용

DHCP 서비스를 사용하도록 설정하여 NSX Edge에서 IP 주소가 정의된 IP 풀에서 가상 시스템으로 자동 할당되도록 허용할 수 있습니다.

사전 요구 사항

DHCP IP 풀이 추가되어 있어야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **DHCP** 탭을 클릭합니다.
- 5 **사용(Enable)**을 클릭합니다.
- 6 필요한 경우 **로깅 사용(Enable logging)**을 선택하고 로그 수준을 선택합니다.
- 7 **변경 내용 게시(Publish Changes)**를 클릭합니다.

결과

참고 악의적인 사용자가 잘못된 DHCP 서버를 도입하지 못하게 하려면 방화벽 규칙을 생성하는 것이 좋습니다. 이렇게 하려면 트래픽이 올바른 DHCP 서버 IP 주소에서 송수신될 때 포트 67 및 68에서만 UDP 트래픽을 허용하는 방화벽 규칙을 추가하십시오. 자세한 내용은 [방화벽 규칙 사용](#)을 참조하십시오.

다음에 수행할 작업

IP 풀 및 바인딩을 생성합니다.

DHCP IP 풀 편집

DHCP IP 풀을 편집하여 IP 주소를 추가하거나 제거할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 DHCP 탭을 클릭합니다.
- 5 DHCP 풀을 선택하고 편집(Edit) 아이콘을 클릭합니다.
- 6 필요한 내용을 변경하고 확인(OK)을 클릭합니다.

DHCP 정적 바인딩 추가

가상 시스템에서 실행 중인 서비스가 있는 경우 IP 주소를 변경하지 않으려면 IP 주소를 가상 시스템의 MAC 주소에 바인딩하면 됩니다. 바인딩하는 IP 주소는 IP 풀과 겹치면 안 됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 DHCP 탭을 클릭합니다.
- 5 왼쪽 패널에서 바인딩(Bindings)을 선택합니다.
- 6 추가(Add)(+) 아이콘을 클릭합니다.
- 7 바인딩을 구성합니다.

옵션	작업
DNS 자동 구성(Auto Configure DNS)	DHCP 바인딩에 DNS 서비스 구성을 사용하도록 선택합니다.
리스가 만료되지 않음(Lease never expires)	주소를 가상 시스템의 MAC 주소에 영구적으로 바인딩하도록 선택합니다.

옵션	작업
인터페이스(Interface)	바인딩할 NSX Edge 인터페이스를 선택합니다.
VM 이름(VM Name)	바인딩할 가상 시스템을 선택합니다.
VM vNIC 색인(VM vNIC Index)	IP 주소에 바인딩할 가상 시스템 NIC를 선택합니다.
호스트 이름(Host Name)	DHCP 클라이언트 가상 시스템의 호스트 이름을 입력합니다.
IP 주소(IP Address)	선택한 가상 시스템의 MAC 주소에 바인딩할 주소를 입력합니다.
서브넷 마스크(Subnet Mask)	서브넷 마스크를 지정합니다. 분산 라우터의 경우 서브넷 마스크가 Edge 인터페이스 또는 DHCP 릴레이의 서브넷 마스크와 동일해야 합니다.
도메인 이름(Domain Name)	DNS 서버의 도메인 이름을 입력합니다.
기본 이름 서버(Primary Name Server)	DNS 자동 구성(Auto Configure DNS)을 선택하지 않은 경우 DNS 서비스에 대한 기본 이름 서버(Primary Nameserver)를 입력합니다. 호스트 이름 대 IP 주소를 확인하려면 DNS 서버의 IP 주소를 입력해야 합니다.
보조 이름 서버(Secondary Name Server)	DNS 자동 구성(Auto Configure DNS)을 선택하지 않은 경우 DNS 서비스에 대한 보조 이름 서버(Secondary Nameserver)를 입력합니다. 호스트 이름 대 IP 주소를 확인하려면 DNS 서버의 IP 주소를 입력해야 합니다.
기본 게이트웨이(Default Gateway)	기본 게이트웨이 주소를 입력합니다. 기본 게이트웨이 IP 주소를 지정하지 않으면 NSX Edge 인스턴스의 내부 인터페이스가 기본 게이트웨이로 지정됩니다.
리스 시간(Lease Time)	리스가 만료되지 않음(Lease never expires)을 선택하지 않은 경우 주소를 기본 시간(1일) 동안 클라이언트에 리스하도록 선택하거나, 값을 초 단위로 입력합니다.

8 추가(Add)를 클릭합니다.

9 변경 내용 게시(Publish Changes)를 클릭합니다.

DHCP 바인딩 편집

가상 시스템의 MAC 주소에 바인딩된 다른 정적 IP 주소를 할당합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)를 클릭한 다음 NSX Edge(NSX Edges)를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 관리(Manage) 탭을 클릭한 후 DHCP 탭을 클릭합니다.
- 5 왼쪽 패널에서 바인딩(Bindings)을 선택하고 편집할 바인딩을 클릭합니다.
- 6 [편집] 아이콘을 클릭합니다.
- 7 필요한 내용을 변경하고 확인(OK)을 클릭합니다.

DHCP 릴레이 구성

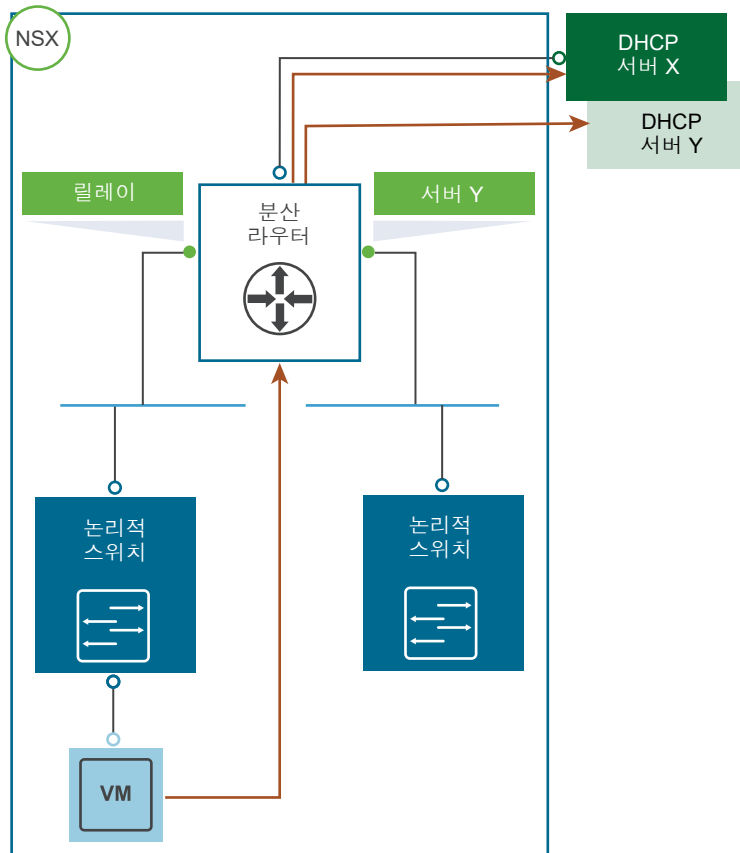
DHCP(Dynamic Host Configuration Protocol) 릴레이를 사용하면 환경의 IP 주소 관리를 중단하지 않고도 NSX 내에서 기존 DHCP 인프라를 활용할 수 있습니다. 가상 시스템에서 물리적 환경의 지정된 DHCP 서버로 DHCP 메시지가 릴레이됩니다. 이를 통해 NSX내 IP 주소가 다른 환경의 IP 주소와 계속 동기화될 수 있습니다.

DHCP 구성은 논리적 라우터 포트에 적용되고 일부 DHCP 서버를 나열합니다. 나열된 모든 서버에 요청이 전송됩니다. 클라이언트에서 DHCP 요청을 릴레이하는 동안, 게이트웨이 IP 주소가 요청에 추가됩니다. 외부 DHCP 서버는 이 게이트웨이 주소를 사용하여 풀을 비교하고 요청에 대한 IP 주소를 할당합니다. 게이트웨이 주소는 릴레이가 실행되는 NSX 포트의 서브넷에 속해야 합니다.

논리적 스위치마다 다른 DHCP 서버를 지정할 수 있고 논리적 라우터마다 여러 DHCP 서버를 구성하여 다중 IP 도메인에 대한 지원을 제공할 수 있습니다.

참고 DHCP 제공에 논리적 인터페이스(LIF)와 일치하지 않는 IP 주소가 포함될 경우 DLR은 VM으로 다시 릴레이하지 않습니다. 패킷은 삭제됩니다.

DHCP 서버에 풀 및 바인딩을 구성할 때 릴레이된 쿼리에 대한 풀/바인딩의 서브넷 마스크와 DHCP 릴레이의 인터페이스가 동일하도록 설정해야 합니다. DLR이 DHCP 서비스를 제공하는 Edge와 VM 사이에서 DHCP 릴레이로 작동하는 동안 서브넷 마스크 정보가 API에 제공되어야 합니다. 이 서브넷 마스크는 DLR의 VM에 대한 게이트웨이 인터페이스에 구성된 서브넷 마스크와 일치해야 합니다.



참고

- DHCP 릴레이에서는 IP 주소 공간의 겹침을 지원하지 않습니다(옵션 82).
- DHCP 릴레이 및 DHCP 서비스를 포트/vNic에서 동시에 실행할 수 없습니다. 포트에 릴레이 에이전트가 구성된 경우 이 포트의 서브넷에 DHCP 풀을 구성할 수 없습니다.


DHCP 릴레이 서버 추가

DHCP 메시지를 릴레이할 외부 릴레이 서버를 추가합니다. 릴레이 서버는 IP 집합, IP 주소 블록, 도메인 또는 이들 모두의 조합일 수 있습니다. 나열된 각 DHCP 서버에 메시지가 릴레이됩니다.

사전 요구 사항

- DHCP 릴레이에서는 IP 주소 공간의 겹침을 지원하지 않습니다(옵션 82).
- DHCP 릴레이 및 DHCP 서비스를 포트/vNic에서 동시에 실행할 수 없습니다. 포트에 릴레이 에이전트가 구성된 경우 이 포트의 서브넷에 DHCP 풀을 구성할 수 없습니다.
- DHCP 제공에 논리적 인터페이스(LIF)와 일치하지 않는 IP 주소가 포함될 경우 DLR은 VM으로 다시 릴레이하지 않습니다. 패킷은 삭제됩니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 해당하는 Edge를 두 번 클릭하고 **관리(Manage) > DHCP** 탭에 있는지 확인합니다.
- 3 **DHCP 릴레이 글로벌 구성(DHCP Relay Global Configuration)** 옆에 있는 **편집(Edit)**을 클릭합니다.
- 4 IP 집합을 서버로 추가하려면
 - a **추가(Add)** 아이콘을 클릭하고 IP 집합을 선택합니다.
 - b  아이콘을 클릭하여 선택한 IP 집합을 선택한 개체 목록으로 이동합니다.
 - c **확인(OK)**을 클릭합니다.
- 5 IP 주소 또는 도메인 이름을 추가하려면 해당 영역에 주소 또는 이름을 입력합니다.
- 6 **확인(OK)**을 클릭합니다.

릴레이 에이전트 추가

DHCP 메시지가 외부 DHCP 릴레이 서버로 릴레이되는 Edge 인터페이스를 추가합니다.

절차

- 1 **DHCP 릴레이 에이전트(DHCP Relay Agents)** 영역에서 **추가(Add)** 아이콘을 클릭합니다.
- 2 **vNIC**에서 내부 vNIC가 선택되었는지 확인합니다.
게이트웨이 IP 주소(Gateway IP Address)에 선택된 vNic의 기본 IP 주소가 표시됩니다.
- 3 **확인(OK)**을 클릭합니다.

DNS 서버 구성

NSX Edge에서 외부 DNS 서버를 구성할 수 있습니다. Edge는 클라이언트 애플리케이션에서 DNS 서버로 DNS 요청을 전달하여 네트워크 이름을 확인합니다. Edge는 DNS 서버에서 수신하는 응답을 캐시할 수도 있습니다. DNS 서비스는 크로스 vCenter NSX 환경의 Edge 서비스 게이트웨이, DLR 및 UDLR에서 지원됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다.
- 5 **DNS 구성(DNS Configuration)** 패널에서 **변경(Change)**을 클릭합니다.

- 6 DNS 서비스 사용(Enable DNS Service)**을 클릭하여 DNS 서비스를 사용하도록 설정합니다.
- 7** 두 DNS 서버 모두의 IP 주소를 입력합니다.
- 8** 필요한 경우 기본 캐시 크기를 변경합니다.
- 9 로깅 사용(Enable Logging)**을 클릭하여 DNS 트래픽을 로그하고 로그 수준을 선택합니다.
생성된 로그는 Syslog 서버로 전송됩니다.
- 10 확인(Ok)**을 클릭합니다.

Service Composer는 네트워크 및 보안 서비스를 가상 인프라의 애플리케이션에 프로비저닝하고 할당하는데 도움이 됩니다. 이러한 서비스를 보안 그룹에 매핑하면 보안 그룹의 가상 시스템에 서비스가 적용됩니다.

보안 그룹

먼저 보안 그룹을 생성하여 보호할 자산을 정의합니다. 보안 그룹은 정적(특정 가상 시스템 포함) 또는 동적일 수 있으며 멤버 자격은 다음 방법 중 하나 이상을 사용하여 정의될 수 있습니다.

- vCenter 컨테이너(클러스터, 포트 그룹 또는 데이터센터)
- 보안 태그, IPset, MACset 또는 다른 보안 그룹. 예를 들어 특정 보안 태그(예: AntiVirus.virusFound)로 태그 지정된 멤버를 모두 보안 그룹에 추가하는 조건을 포함할 수 있습니다.
- 디렉토리 그룹(NSX Manager가 Active Directory에 등록된 경우)
- 이름이 VM1인 가상 시스템과 같은 정규식

보안 그룹 멤버 자격은 지속적으로 바뀐다는 점을 유의하십시오. 예를 들어 AntiVirus.virusFound 태그가 지정된 가상 시스템은 차단 보안 그룹으로 이동됩니다. 바이러스가 제거되어 가상 시스템에서 이 태그가 제거되면 다시 차단 보안 그룹 밖으로 이동합니다.

보안 정책

보안 정책은 다음과 같은 서비스 구성의 모음입니다.

표 17-1. 보안 정책에 포함된 보안 서비스

서비스	설명	적용 대상
방화벽 규칙	보안 그룹으로 들어오거나, 보안 그룹에서 나가거나, 보안 그룹 내에서 이동하는 것이 허용되는 트래픽을 정의하는 규칙입니다.	vNIC
Endpoint 서비스	바이러스 백신이나 취약성 관리 서비스와 같은 타사 솔루션 제공자 서비스입니다.	가상 시스템
네트워크 검사 서비스	IPS와 같은 네트워크를 모니터링하는 서비스입니다.	가상 시스템

NSX에서 서비스가 배포되는 동안 타사 벤더가 배포되고 있는 서비스의 서비스 범주를 선택합니다. 각 벤더 템플릿에 대해 기본 서비스 프로파일이 생성됩니다.

타사 벤더 서비스가 **NSX 6.1**로 업그레이드되면 업그레이드된 벤더 템플릿에 대해 기본 서비스 프로파일이 생성됩니다. 게스트 검사 규칙을 포함하는 기존 서비스 정책이 업그레이드되는 동안 생성된 서비스 프로파일을 참조하도록 업데이트됩니다.

보안 정책을 보안 그룹에 매핑

보안 정책(예: **SP1**)을 보안 그룹(예: **SG1**)에 매핑합니다. **SP1**에 대해 구성된 서비스는 **SG1**의 멤버인 모든 가상 시스템에 적용됩니다.

참고 동일한 보안 정책을 연결해야 하는 보안 그룹이 많을 때에는 이러한 모든 하위 보안 그룹을 포함하는 포괄 보안 그룹을 생성하고 포괄 보안 그룹에 공통 보안 정책을 적용합니다. 이렇게 하면 **NSX** 분산 방화벽이 **ESXi** 호스트 메모리를 효율적으로 이용합니다.

그림 17-1. Service Composer 개요



가상 시스템이 둘 이상의 보안 그룹에 속한 경우 가상 시스템에 적용되는 서비스는 보안 그룹에 매핑된 보안 정책의 우선 순위에 따라 달라집니다.

Service Composer 프로파일을 백업이나 다른 환경에 사용할 목적으로 내보내거나 가져올 수 있습니다. 이런 방법으로 네트워크 및 보안 서비스를 관리하면 작업 가능하고 반복 가능한 보안 정책 관리에 도움이 됩니다.

본 장은 다음 항목을 포함합니다.

- [Service Composer 사용](#)
- [Service Composer 캔버스](#)
- [보안 태그 사용](#)
- [유효한 서비스 보기](#)
- [보안 정책 사용](#)
- [Service Composer 시나리오](#)
- [보안 정책 구성 가져오기 및 내보내기](#)

Service Composer 사용

Service Composer를 통해 보안 서비스를 쉽게 사용할 수 있습니다.

Service Composer가 네트워크 전체를 보호하는 데 어떻게 도움이 되는지 예제를 통해 살펴보겠습니다. 사용자 환경에 다음의 보안 정책이 정의되어 있다고 가정하겠습니다.

- 취약성 검사 서비스가 포함된 초기 상태 보안 정책(InitStatePolicy)
- 방화벽 규칙 및 바이러스 백신 서비스 이외에 네트워크 IPS 서비스가 포함된 업데이트 적용 보안 정책(RemPolicy)

RemPolicy가 InitStatePolicy보다 가중치(우선 순위)가 높은지 확인합니다.

또한 다음의 보안 그룹이 있어야 합니다.

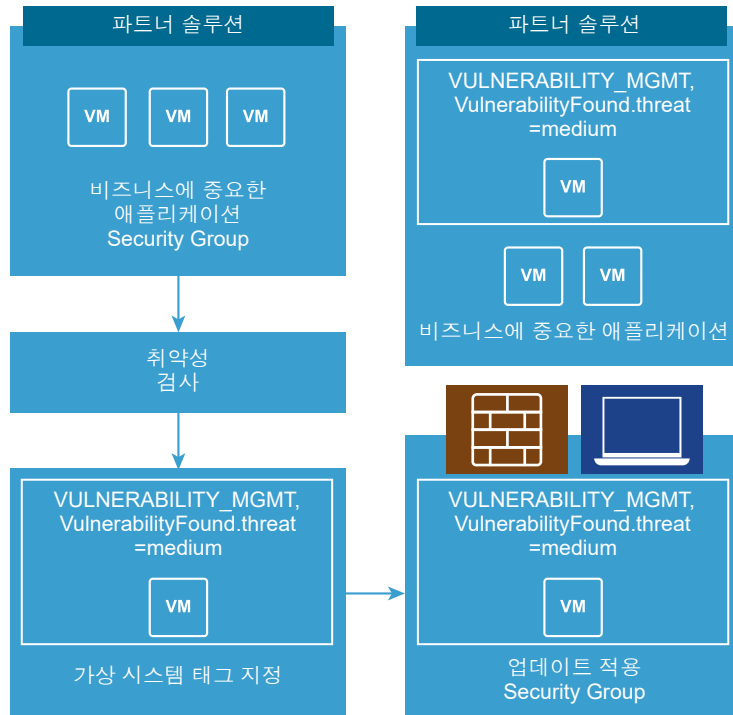
- 사용자 환경에서 비즈니스에 중요한 애플리케이션을 포함하는 애플리케이션 자산 그룹(AssetGroup)
- 가상 시스템이 취약함을 알리는 태그
(VULNERABILITY_MGMT.VulnerabilityFound.threat=medium)에 의해 정의된 업데이트 적용 보안 그룹(RemGroup)

이제 사용자 환경에서 비즈니스에 중요한 모든 애플리케이션을 보호하기 위해 InitStatePolicy를 AssetGroup에 매핑합니다. 또한 취약한 가상 시스템을 보호하기 위해 RemPolicy를 RemGroup에 매핑합니다.

취약성 검사를 시작하면 AssetGroup의 모든 가상 시스템이 검사됩니다. 검사 중 취약성이 있는 가상 시스템이 식별되면 VULNERABILITY_MGMT.VulnerabilityFound.threat=medium 태그를 가상 시스템에 적용합니다.

Service Composer는 이 태그 지정된 가상 시스템을 즉시 RemGroup에 추가하며, 이 그룹에는 이 취약한 가상 시스템을 보호하기 위한 네트워크 IPS 솔루션이 이미 적용되어 있습니다.

그림 17-2. Service Composer 작동



이제 이 항목에서는 Service Composer가 제공하는 보안 서비스를 사용하는 데 필요한 단계를 안내합니다.

절차

1 Service Composer에서 보안 그룹 생성

보안 그룹은 NSX Manager 수준에서 생성할 수 있습니다.

2 보안 정책 생성

보안 정책은 보안 그룹에 적용할 수 있는 Guest Introspection, 방화벽 및 네트워크 검사 서비스의 집합입니다. 보안 정책이 표시되는 순서는 정책과 연결된 가중치에 의해 결정됩니다. 기본적으로 새 정책은 테이블의 맨 위에 나타나도록 가장 높은 가중치가 할당됩니다. 하지만 기본 제안 가중치를 수정하여 새 정책에 할당된 순서를 변경할 수 있습니다.

3 보안 그룹에 보안 정책 적용

보안 그룹에 보안 정책을 적용하여 가상 데스크톱, 비즈니스에 중요한 애플리케이션 및 이들 간의 연결에 보안을 유지할 수 있습니다. 또한 적용되지 않은 서비스의 목록과 적용하지 못한 이유도 볼 수 있습니다.

Service Composer에서 보안 그룹 생성

보안 그룹은 NSX Manager 수준에서 생성할 수 있습니다.

절차

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 그룹(Security Groups)** 탭을 클릭하고 **보안 그룹 추가(Add Security Group)** 아이콘을 클릭합니다.
- 4 보안 그룹의 이름 및 설명을 입력하고 **다음(Next)**을 클릭합니다.
- 5 생성할 보안 그룹에 추가하려면 개체가 충족해야 하는 조건을 [동적 멤버 자격] 페이지에서 정의합니다.

예를 들어 특정 보안 태그(예: `AntiVirus.virusFound`)로 태그 지정된 멤버를 모두 보안 그룹에 추가하는 조건을 포함할 수 있습니다.

또는 이름 `w2008`을 포함하는 모든 가상 시스템과 논리적 스위치 `global_wire`에 있는 가상 시스템을 보안 그룹에 추가할 수 있습니다.

보안 태그는 대/소문자를 구분합니다.

참고 특정 보안 태그가 적용된 가상 시스템에서 보안 그룹을 정의하면 동적 또는 조건부 워크플로우를 생성할 수 있습니다. 태그가 가상 시스템에 적용되는 순간 가상 시스템이 자동으로 해당 보안 그룹에 추가됩니다.

- 6 **다음(Next)**을 클릭합니다.
- 7 [포함할 개체 선택] 페이지의 드롭다운에서 개체 유형을 선택합니다.
- 8 포함 목록에 추가할 개체를 두 번 클릭합니다. 다음 개체를 보안 그룹에 포함할 수 있습니다.
 - 생성할 보안 그룹 안에 중첩될 다른 보안 그룹
 - 클러스터
 - 논리적 스위치
 - 네트워크
 - 가상 장치
 - 데이터센터
 - IP 집합
 - AD 그룹

참고 NSX 보안 그룹에 대한 AD 구성은 vSphere SSO에 대한 AD 구성과 다릅니다. NSX AD 그룹 구성은 게스트 가상 시스템에 액세스하는 최종 사용자를 위한 것이며 vSphere SSO는 vSphere 및 NSX를 사용하는 관리자를 위한 것입니다.

■ MAC 집합

참고 Service Composer는 정책 구성에 MAC 집합이 포함된 보안 그룹을 사용하도록 허용하지만 Service Composer에서 해당 특정 MAC 집합에 대해 규칙을 적용하지 못합니다. Service Composer는 계층 3에서 작동하고 계층 2 구성을 지원하지 않습니다.

- 보안 태그
- vNIC
- 가상 시스템
- 리소스 풀
- 분산 가상 포트 그룹

여기에서 선택하는 개체는 동적 조건의 충족 여부에 상관없이 항상 보안 그룹에 포함됩니다.

보안 그룹에 리소스를 추가하면 연결된 모든 리소스가 자동으로 추가됩니다. 예를 들어 가상 시스템을 선택하면 연결된 vNIC가 자동으로 보안 그룹에 추가됩니다.

9 다음(Next)을 클릭하고 보안 그룹에서 제외할 개체를 두 번 클릭합니다.

여기에서 선택하는 개체는 동적 조건을 충족하거나 포함 목록에 선택된 경우에도 항상 보안 그룹에서 제외됩니다.

10 완료(Finish)를 클릭합니다.

예

보안 그룹의 멤버 자격은 다음과 같이 결정됩니다.

{표현식 결과(단계 4단계에서 파생됨) + 포함(단계 7단계에 지정됨)} - 제외(단계 8단계에 지정됨)

이는 포함 항목이 표현식 결과에 먼저 추가됨을 의미합니다. 그런 다음 조합된 결과에서 제외 항목을 뺍니다.

보안 정책 생성

보안 정책은 보안 그룹에 적용할 수 있는 Guest Introspection, 방화벽 및 네트워크 검사 서비스의 집합입니다. 보안 정책이 표시되는 순서는 정책과 연결된 가중치에 의해 결정됩니다. 기본적으로 새 정책은 테이블의 맨 위에 나타나도록 가장 높은 가중치가 할당됩니다. 하지만 기본 제안 가중치를 수정하여 새 정책에 할당된 순서를 변경할 수 있습니다.

사전 요구 사항

다음 사항을 충족하는지 확인하십시오.

- 분산 방화벽 및 Guest Introspection과 같은 필수 VMware 기본 제공 서비스가 설치되어 있습니다.
- 필수 파트너 서비스가 NSX Manager에 등록되어 있습니다.
- Service Composer 방화벽 규칙에 대해 원하는 기본값이 설정되어 있습니다. [Service Composer 방화벽 적용 대상 설정 편집](#)를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 정책(Security Policies)** 탭을 클릭합니다.

- 4 **보안 정책 생성(Create Security Policy)**() 아이콘을 클릭합니다.

- 5 보안 정책 추가 대화상자에서 보안 정책의 이름을 입력합니다.

- 6 보안 정책에 대한 설명을 입력합니다.


NSX는 정책에 기본 가중치(가장 높은 가중치 + 1000)를 할당합니다. 예를 들어 기존 정책 중 가장 높은 가중치가 1200이면 새 정책에는 2200의 가중치가 할당됩니다.

보안 정책은 해당 가중치에 따라 적용됩니다. 즉, 가중치가 높은 정책이 가중치가 낮은 정책보다 우선 적용됩니다.

- 7 생성 중인 정책이 다른 보안 정책에서 서비스를 받도록 하려면 **지정된 정책에서 보안 정책 상속(Inherit security policy from specified policy)**을 선택합니다. 상위 정책을 선택합니다.

상위 정책의 모든 서비스가 새 정책에 상속됩니다.

- 8 **다음(Next)**을 클릭합니다.

- 9 [Guest Introspection 서비스] 페이지에서 **Guest Introspection 서비스 추가(Add Guest Introspection Service)**() 아이콘을 클릭합니다.

- a [Guest Introspection 서비스 추가] 대화상자에서 서비스의 이름과 설명을 입력합니다.

- b 서비스를 적용할지 또는 차단할지 여부를 지정합니다.

보안 정책을 상속할 때는 상위 정책의 서비스를 차단하도록 선택할 수 있습니다.

서비스를 적용할 경우 서비스 및 서비스 프로파일을 선택해야 합니다. 서비스를 차단할 경우 차단할 서비스 유형을 선택해야 합니다.

- c 서비스 차단을 선택한 경우 서비스 유형을 선택합니다.

- d **Guest Introspection** 서비스 적용을 선택한 경우 에서 서비스 이름을 선택합니다.

선택한 서비스의 기본 서비스 프로파일이 표시되고, 여기에는 연결된 벤더 템플릿에서 지원하는 서비스 기능 유형에 대한 정보가 포함됩니다.

- e **상태(State)**에서는 선택한 **Guest Introspection** 서비스를 사용하도록 설정할지 여부를 지정합니다.


Guest Introspection 서비스를 나중에 사용하도록 설정할 서비스에 대한 자리 표시자로 추가할 수 있습니다. 이 방법은 필요에 따라 서비스를 적용해야 하는 경우(예: 새 애플리케이션)에 특히 유용합니다.

- f **Guest Introspection** 서비스를 강제 적용(즉, 재정의할 수 없음)할지 여부를 선택합니다. 선택한 서비스 프로파일에서 여러 서비스 기능 유형을 지원할 경우 기본적으로 **강제 적용(Enforce)**으로 설정되어 있고 변경할 수 없습니다.

보안 정책에서 **Guest Introspection** 서비스를 강제 적용하는 경우 이 보안 정책을 상속하는 다른 정책에서는 나머지 하위 정책보다 먼저 이 정책을 적용해야 합니다. 이 서비스를 강제 적용하지 않으면 상속 선택에서 하위 정책이 적용된 후에 상위 정책이 추가됩니다.

- g **확인(OK)**을 클릭합니다.

위의 단계를 수행하여 다른 **Guest Introspection** 서비스를 추가할 수 있습니다. 서비스 테이블 위의 아이콘을 통해 **Guest Introspection** 서비스를 관리할 수 있습니다.

[**Guest Introspection** 서비스] 페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 서비스를 내보내거나 복사할 수 있습니다.

10 다음(Next)을 클릭합니다.

11 [방화벽] 페이지에서 **방화벽 규칙 추가(Add Firewall Rule)(+)** 아이콘을 클릭합니다.

여기에서는 이 보안 정책이 적용될 보안 그룹에 대한 방화벽 규칙을 정의합니다.

- 추가 중인 방화벽 규칙에 대한 이름과 설명을 입력합니다.
- 허용(Allow)** 또는 **차단(Block)**을 선택하여 규칙이 선택된 대상으로의 트래픽을 허용할지 아니면 차단할지를 지정합니다.
- 규칙의 소스를 선택합니다. 기본적으로 규칙은 이 정책이 적용되는 보안 그룹에서 오는 트래픽에 적용됩니다. 기본 소스를 변경하려면 **변경(Change)**을 클릭하고 적절한 보안 그룹을 선택합니다.
- 규칙의 대상을 선택합니다.


참고 소스 또는 대상(또는 둘 모두)은 이 정책이 적용되는 보안 그룹이어야 합니다.

기본 소스가 있는 규칙을 생성하고 대상을 **Payroll**로 지정하고 **대상 부정(Negate Destination)**을 선택했다고 가정하겠습니다. 그런 다음 이 보안 정책을 보안 그룹 **Engineering**에 적용합니다. 이렇게 하면 **Engineering**은 **Payroll** 서버를 제외한 모든 항목에 액세스할 수 있습니다.

- 규칙이 적용될 서비스 및/또는 서비스 그룹을 선택합니다.
- 사용(Enabled)** 또는 **사용 안 함(Disabled)**을 선택하여 규칙 상태를 지정합니다.
- 이 규칙과 일치하는 세션을 로깅하려면 **로그(Log)**를 선택합니다.
로깅을 사용하도록 설정하면 성능에 영향을 줄 수 있습니다.

- h **확인(OK)**을 클릭합니다.

위의 단계를 수행하여 다른 방화벽 규칙을 추가할 수 있습니다. 방화벽 테이블 위의 아이콘을 통해 방화벽 규칙을 관리할 수 있습니다.

[방화벽] 페이지 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 규칙을 내보내거나 복사할 수 있습니다.

여기에서 추가하는 방화벽 규칙은 방화벽 테이블에 표시됩니다. 방화벽 테이블에서 **Service Composer** 규칙은 편집하지 않는 것이 좋습니다. 긴급 문제 해결을 위해 편집해야 하는 경우에는 보안 정책 탭의 **작업(Actions)** 메뉴에서 **방화벽 규칙 동기화(Synchronize Firewall Rules)**를 선택하여 Service Composer 규칙을 방화벽 규칙과 다시 동기화해야 합니다.

12 다음(Next)을 클릭합니다.

[네트워크 검사 서비스] 페이지에는 VMware 가상 환경에 통합된 NetX 서비스가 표시됩니다.


13 네트워크 검사 서비스 추가(Add Network Introspection Service)(+) 아이콘을 클릭합니다.

- a [네트워크 검사 서비스 추가] 대화상자에서 추가할 서비스의 이름과 설명을 입력합니다.
- b 서비스로 리디렉션할지 여부를 선택합니다.
- c 서비스 이름과 프로파일을 선택합니다.
- d 소스와 대상을 선택합니다.
- e 추가할 네트워크 서비스를 선택합니다.

선택한 서비스를 기반으로 추가 항목을 선택할 수 있습니다.

- f 서비스를 사용하도록 설정할지 여부를 선택합니다.
- g 이 규칙과 일치하는 세션을 로깅하려면 로그를 선택합니다.
- h **확인(OK)**을 클릭합니다.

위의 단계를 수행하여 다른 네트워크 검사 서비스를 추가할 수 있습니다. 서비스 테이블 위의 아이콘을 통해 네트워크 검사 서비스를 관리할 수 있습니다.

[네트워크 검사 서비스] 페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 서비스를 내보내거나 복사할 수 있습니다.

참고 Service Composer 정책에서 사용된 서비스 프로파일에 대해 수동으로 생성된 바인딩을 덮어씁니다.

14 완료(Finish)를 클릭합니다.

보안 정책이 정책 테이블에 추가됩니다. 정책 이름을 클릭하고 적절한 탭을 선택하면 정책과 연결된 서비스의 요약을 보거나 서비스 오류를 보거나 서비스를 편집할 수 있습니다.

다음에 수행할 작업

보안 정책을 보안 그룹에 매핑합니다.

Service Composer 방화벽 적용 대상 설정 편집

Service Composer를 통해 생성된 모든 방화벽 규칙에 대한 적용 대상 설정을 [분산 방화벽] 또는 [정책의 보안 그룹]으로 설정할 수 있습니다. 기본적으로 적용 대상은 [분산 방화벽]으로 설정되어 있습니다.

Service Composer 방화벽 규칙의 적용 대상이 [분산 방화벽]으로 설정되어 있으면 [분산 방화벽]이 설치된 모든 클러스터에 규칙이 적용됩니다. 방화벽 규칙의 적용 대상이 [정책의 보안 그룹]으로 설정되어 있으면 방화벽 규칙을 보다 미세하게 제어할 수 있지만 원하는 결과를 얻기 위해 여러 보안 정책 또는 방화벽 규칙이 필요할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **Service Composer, 보안 정책(Security Policies)** 탭을 차례로 클릭합니다.
- 3 **작업(Actions) > 방화벽 정책 설정 편집(Edit Firewall Policy Settings)**을 클릭합니다. 적용 대상에 대해 기본 설정을 선택하고 [확인]을 클릭합니다.

옵션	설명
분산 방화벽	방화벽 규칙이 [분산 방화벽]이 설치된 모든 클러스터에 적용됩니다.
정책의 보안 그룹	방화벽 규칙이 보안 정책이 적용된 보안 그룹에 적용됩니다.

API를 통해 기본 적용 대상 설정을 보고 변경할 수도 있습니다. "NSX API 가이드"를 참조하십시오.

예제: 적용 대상 동작

이 예제 시나리오에서 기본 방화벽 규칙 작업은 [차단]으로 설정되어 있습니다. 두 가지 보안 그룹인 **web-servers** 및 **app-servers**가 있습니다(VM 포함). 다음 방화벽 규칙을 포함하는 보안 정책, **allow-ssh-from-web**을 생성한 후 보안 그룹 **app-servers**에 적용합니다.

- 이름: **allow-ssh-from-web**
- 소스: **web-servers**
- 대상: 정책의 보안 그룹
- 서비스: **ssh**
- 작업: 허용

방화벽 규칙이 [분산 방화벽]에 적용되는 경우 보안 그룹 **web-servers**의 VM에서 보안 그룹 **app-servers**의 VM으로 **ssh**를 수행할 수 있습니다.


방화벽 규칙이 [정책의 보안 그룹]에 적용되는 경우 트래픽이 애플리케이션 서버에 도달될 수 없게 차단되므로 **ssh**가 가능하지 않게 됩니다. 애플리케이션 서버에 대한 **ssh**를 허용하기 위한 추가 보안 정책을 생성하고 이 정책을 보안 그룹 **web-servers**에 적용해야 합니다.

- 이름: **allow-ssh-to-app**
- 소스: 정책의 보안 그룹
- 대상: **app-servers**
- 서비스: **ssh**
- 작업: 허용

보안 그룹에 보안 정책 적용

보안 그룹에 보안 정책을 적용하여 가상 데스크톱, 비즈니스에 중요한 애플리케이션 및 이들 간의 연결에 보안을 유지할 수 있습니다. 또한 적용되지 않은 서비스의 목록과 적용하지 못한 이유도 볼 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 정책(Security Policy)** 탭을 클릭합니다.
- 4 보안 정책을 선택하고 **보안 정책 적용(Apply Security Policy)**() 아이콘을 클릭합니다.
- 5 정책을 적용할 보안 그룹을 선택합니다.
특정 보안 태그가 적용된 가상 시스템에서 정의된 보안 그룹을 선택하면 동적 또는 조건부 워크플로우를 생성할 수 있습니다. 태그가 가상 시스템에 적용되는 순간 가상 시스템이 자동으로 해당 보안 그룹에 추가됩니다.
정책과 연관된 네트워크 검사 규칙 및 끝점 규칙은 IPSet 및/또는 MacSet 구성원이 포함된 보안 그룹에 영향을 미치지 않습니다.
- 6 선택된 보안 그룹에 적용할 수 없는 서비스와 실패 이유를 보려면 **서비스 상태 미리 보기(Preview Service Status)** 아이콘을 클릭하십시오.
예를 들어 정책 서비스 중 하나가 설치되지 않은 클러스터에 속하는 가상 시스템이 보안 그룹에 포함될 수 있습니다. 보안 정책이 의도대로 작동하려면 적절한 클러스터에 해당 서비스를 설치해야 합니다.
- 7 **확인(OK)**를 클릭합니다.

Service Composer 캔버스

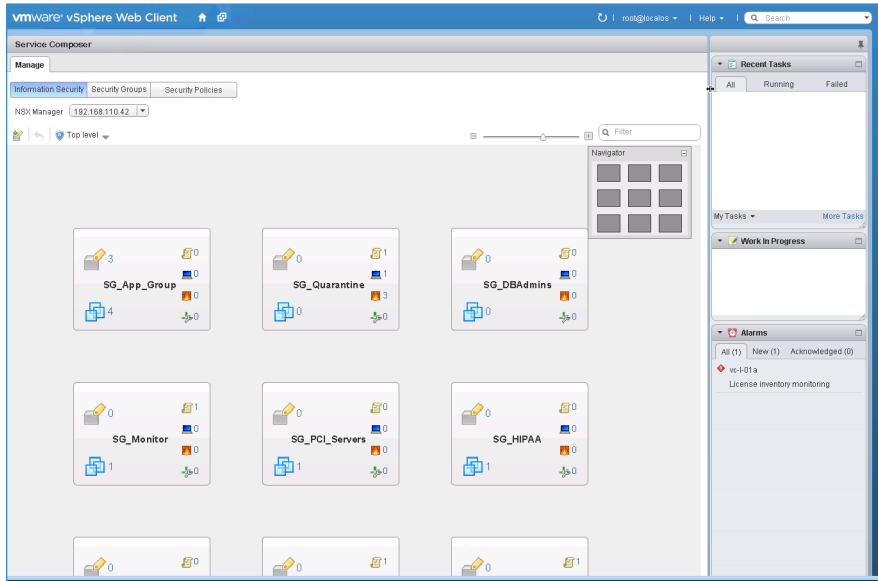
Service Composer 캔버스 탭은 선택한 NSX Manager 내의 모든 보안 그룹이 표시되는 그래픽 보기를 제공합니다. 이 보기에는 각 보안 그룹의 멤버와 여기에 적용된 보안 정책과 같은 세부 정보도 표시됩니다.

이 항목에서는 보안 그룹과 보안 정책 개체 간의 매핑을 캔버스 보기에서 상위 수준으로 살펴볼 수 있도록, 부분적으로 구성된 시스템을 단계별로 안내하는 방식으로 **Service Composer**를 소개합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **캔버스(Canvas)** 탭을 클릭합니다.
선택한 NSX Manager 내에서 다른 보안 그룹에 속하지 않는 모든 보안 그룹이 해당 그룹에 적용된 정책과 함께 표시됩니다. **NSX Manager** 드롭다운 목록에는 현재 로그인한 사용자에게 역할이 할당된 모든 NSX Manager가 나열됩니다.

그림 17-3. Service Composer 캔버스 최상위 수준 보기




결과

캔버스의 각 사각형 상자는 보안 그룹을 나타내며 상자 내의 아이콘은 보안 그룹 멤버와 보안 그룹에 매핑된 보안 정책에 대한 세부 정보를 나타냅니다.

그림 17-4. 보안 그룹



각 아이콘 옆의 숫자는 인스턴스의 수를 나타냅니다. 예를 들어  1은 해당 보안 그룹에 1개의 보안 정책이 매핑되었음을 의미합니다.

아이

콘 클릭하면 표시되는 항목




기본 보안 그룹 내에 중첩된 보안 그룹




현재 기본 보안 그룹 및 중첩된 보안 그룹의 일부인 가상 시스템. 오류 탭을 클릭하면 서비스 오류가 있는 가상 시스템이 표시됩니다.



보안 그룹에 매핑된 유효한 보안 정책

- **보안 정책 생성(Security Policy)**() 아이콘을 클릭하여 새 보안 정책을 생성할 수 있습니다. 새로 생성된 보안 정책 개체는 자동으로 보안 그룹에 매핑됩니다.

- 추가적인 보안 정책을 보안 그룹에 매핑하려면 **보안 정책 적용(Apply Security Policy)**() 아이콘을 클릭합니다.

아이**콘 클릭하면 표시되는 항목**

보안 그룹에 매핑된 보안 정책과 연결된 유효한 **Endpoint** 서비스. 보안 그룹에 두 개의 정책이 적용되어 있으며 둘 모두에 동일한 범주 **Endpoint** 서비스가 구성되어 있다고 가정하겠습니다. 이 경우 우선 순위가 두 번째로 낮은 서비스는 재정의되므로 유효한 서비스 수는 1입니다.

Endpoint 서비스 오류가 있는 경우에는 경고 아이콘으로 표시됩니다. 아이콘을 클릭하면 오류가 표시됩니다.



보안 그룹에 매핑된 보안 정책과 연결된 유효한 방화벽 규칙.

서비스 오류가 있는 경우에는 경고 아이콘으로 표시됩니다. 아이콘을 클릭하면 오류가 표시됩니다.



보안 그룹에 매핑된 보안 정책과 연결된 유효한 네트워크 검사 서비스.

서비스 오류가 있는 경우에는 경고 아이콘으로 표시됩니다. 아이콘을 클릭하면 오류가 표시됩니다.

아이콘을 클릭하면 적절한 세부 정보가 있는 대화상자가 표시됩니다.

그림 17-5. 보안 그룹에서 아이콘을 클릭할 때 표시되는 세부 정보

No.	Name	Source	Destination	Service	Action	Security
1	f1	Policy's S...	Any	Any	Allow	Sec...
2	f2	Policy's S...	Any	Any	Allow	Sec...

이름으로 보안 그룹을 검색할 수 있습니다. 예를 들어 캔버스 보기 오른쪽 위에 있는 검색 필드에 **PCI**를 입력하면 이름에 **PCI**가 있는 보안 그룹만 표시됩니다.

보안 그룹 계층을 보려면 창의 왼쪽 위에 있는 **최상위 수준(Top Level)**(▼) 아이콘을 클릭하고 표시할 보안 그룹을 선택합니다. 보안 그룹에 다른 보안 그룹이 중첩된 경우 ▶을 클릭하면 중첩된 그룹이 표시됩니다. 맨 위의 막대에는 상위 보안 그룹의 이름이 표시되고 막대의 아이콘에는 보안 정책, **Endpoint** 서비스, 방화벽 서비스 및 상위 그룹에 적용 가능한 네트워크 검사 서비스의 총 개수가 표시됩니다. 창의 왼쪽 위에서 **한 수준 위로 이동(Go up one level)**(↶) 아이콘을 클릭하면 다시 최상위 수준으로 이동할 수 있습니다.

창의 오른쪽 위에 있는 확대/축소 슬라이더를 움직여서 캔버스 보기를 매끄럽게 확대하거나 축소할 수 있습니다. 탐색기 상자에는 전체 캔버스의 축소된 보기가 표시됩니다. 캔버스가 너무 커서 화면에 맞지 않는 경우에는 실제 보이는 영역 주위에 상자가 표시되며, 이 상자를 움직여서 현재 표시되는 캔버스 부분을 변경할 수 있습니다.

다음에 수행할 작업

지금까지 보안 그룹 및 보안 정책 간의 매핑이 작동하는 방식을 살펴보았으므로 이제 보안 정책을 생성하여 보안 그룹에 적용할 보안 서비스를 정의할 수 있습니다.

보안 그룹을 보안 정책에 매핑

선택한 보안 그룹을 보안 정책에 매핑할 수 있습니다.

절차

- 1 보안 그룹에 적용할 보안 정책을 선택합니다.
- 2 새 정책을 생성하려면 새 보안 그룹을 선택합니다.

[보안 정책 생성](#)를 참조하십시오.

- 3 **저장(Save)**을 클릭합니다.

보안 태그 사용

가상 시스템에 적용된 보안 태그를 확인하거나 사용자 정의 보안 태그를 생성할 수 있습니다.

보안 태그는 VM(가상 시스템)과 연결될 수 있는 레이블입니다. 특정 워크로드를 식별하기 위해 다양한 보안 태그를 생성할 수 있습니다. 보안 그룹의 일치 조건은 보안 태그일 수 있으며, 태그가 지정된 워크로드는 보안 그룹에 자동으로 배치될 수 있습니다.

VM에 대한 보안 태그는 바이러스 백신 또는 취약성 검색 및 침입 방지 시스템과 같은 다양한 조건에 대한 응답으로 동적으로 추가되거나 삭제될 수 있습니다. 또한 관리자가 수동으로 태그를 추가하고 제거할 수 있습니다.

크로스 vCenter NSX 환경에서는 기본 NSX Manager에서 범용 보안 태그가 생성되고 보조 NSX Manager와 범용 동기화되도록 표시됩니다. 범용 보안 태그는 고유한 ID 선택에 따라 VM에 정적으로 할당될 수 있습니다.

고유한 ID 선택

고유한 ID 선택 조건은 활성화 대기 배포의 가상 시스템에 태그를 할당할 때 사용됩니다.

고유한 ID는 VM(가상 시스템)이 대기 상태에서 활성화 배포로 전환될 때 NSX Manager에서 사용됩니다. 고유한 ID는 VM 인스턴스 UUID, VM BIOS UUID 또는 VM 이름이나 이러한 옵션의 조합을 기준으로 할 수 있습니다. 범용 보안 태그가 생성되고 VM에 연결된 후 조건이 변경되면(예: VM 이름 변경) 보안 태그를 분리했다가 VM에 다시 연결해야 합니다.

절차

- 1 vSphere Web Client에서 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)**로 이동하고 **[관리]** 탭을 선택합니다.
- 2 기본 NSX Manager를 클릭합니다. 그런 다음 **작업 > 고유한 ID 선택 조건(Actions > Unique ID Selection Criteria.)**을 선택합니다.
- 3 다음 고유한 ID 옵션 중 하나 이상을 선택합니다.
 - 가상 시스템 인스턴스 UUID 사용(권장) - VM 인스턴스 UUID는 일반적으로 VC 도메인 내에서 고유하지만 스냅샷을 통해 배포가 수행되는 경우처럼 예외도 있습니다. VM 인스턴스 UUID가 고유하지 않으면 VM 이름과 VM BIOS UUID를 함께 사용하는 것이 좋습니다.

- 가상 시스템 BIOS UUID 사용 - BIOS UUID는 VC 도메인 내에서 고유하다고 보장할 수 없으나 재해가 발생하더라도 항상 보존됩니다. VM 이름과 BIOS UUID를 함께 사용하는 것이 좋습니다.
- 가상 시스템 이름 사용 - 환경의 모든 VM 이름이 고유한 경우 VM 이름을 사용하여 vCenter에서 VM을 식별할 수 있습니다. VM BIOS UUID와 VM 이름을 함께 사용하는 것이 좋습니다.

4 확인(OK)을 클릭합니다.

다음에 수행할 작업

그런 다음 보안 태그를 생성합니다.

적용된 보안 태그 보기

사용자 환경의 가상 시스템에 적용된 보안 태그를 볼 수 있습니다.

사전 요구 사항

바이러스 백신 검사를 실행하고 적절한 가상 시스템에 태그를 적용해야 합니다.

참고 타사 솔루션에 의해 적용되는 태그에 대한 자세한 내용은 해당 솔루션의 설명서를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 **이름(Name)** 열의 NSX Manager를 클릭한 후 **관리(Manage)** 탭을 클릭합니다.
- 4 **보안 태그(Security Tags)** 탭을 클릭합니다.

사용자 환경에서 적용된 태그의 목록이 해당 태그가 적용된 가상 시스템에 대한 세부 정보와 함께 표시됩니다. 특정 태그가 있는 가상 시스템을 포함하는 보안 그룹을 추가할 계획이라면 정확한 태그 이름을 기록해 두십시오.

- 5 **VM 수(VM Count)** 열의 숫자를 클릭하면 해당 행의 태그가 적용된 가상 시스템을 볼 수 있습니다.

보안 태그 생성

보안 태그를 생성하고 가상 시스템에 적용할 수 있습니다. 크로스-vCenter 환경에서 보안 태그는 기본 및 보조 NSX Manager 간에 동기화됩니다.

사전 요구 사항

활성 대기 배포 시나리오에서 범용 보안 태그를 생성하는 경우 먼저 기본 NSX Manager에서 고유한 ID 선택 조건을 설정합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.

- 3 **이름(Name)** 열의 NSX Manager를 클릭한 후 **관리(Manage)** 탭을 클릭합니다.
- 4 **보안 태그(Security Tags)** 탭을 클릭합니다.
- 5 **새 보안 태그(New Security Tag)** 아이콘을 클릭합니다.
- 6 (선택 사항) 크로스 vCenter NSX 환경에서 사용할 범용 보안 태그를 생성하려면 **이 개체를 범용 동기화에 대해 표시(Mark this object for universal synchronization)**를 선택합니다.
- 7 태그의 이름과 설명을 입력하고 **확인(OK)**을 클릭합니다.

다음에 수행할 작업

보안 태그에 가상 시스템을 할당합니다.

보안 태그 할당

동적 멤버 자격 기반 보안 태그를 사용하여 조건부 워크플로우를 생성하는 것 외에도 보안 태그를 가상 시스템에 수동으로 할당할 수 있습니다.

보안 태그를 보안 그룹에서 일치하는 조건으로 사용할 수 있습니다. 크로스-vCenter 환경에서 보안 태그는 기본 및 보조 NSX Manager 간에 동기화됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 **이름(Name)** 열의 NSX Manager를 클릭한 후 **관리(Manage)** 탭을 클릭합니다.
- 4 **보안 태그(Security Tags)** 탭을 클릭합니다.
- 5 보안 태그를 마우스 오른쪽 버튼으로 클릭하고 **보안 태그 할당(Assign Security Tag)**을 선택합니다.
사용 가능한 VM으로 채워진 **가상 시스템에 보안 태그 할당(Assign Security Tag to Virtual Machine)** 창이 나타납니다.
- 6 하나 이상의 가상 시스템을 두 번 클릭하여 **선택한 개체(Selected Objects)** 열로 이동합니다. **확인(OK)**을 클릭합니다.
보안 태그의 VM 수가 업데이트된 상태로 **보안 태그(Security Tags)** 탭이 나타납니다.

보안 태그 편집

사용자 정의 보안 태그를 편집할 수 있습니다. 편집하려는 태그가 보안 그룹에 사용되고 있는 경우에는 태그 변경 사항이 보안 그룹 멤버 자격에 영향을 줄 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 **이름(Name)** 열의 NSX Manager를 클릭한 후 **관리(Manage)** 탭을 클릭합니다.

4 **보안 태그(Security Tags)** 탭을 클릭합니다.

5 보안 태그를 마우스 오른쪽 버튼으로 클릭하고 **보안 태그 편집(Edit Security Tag)**을 선택합니다.

6 필요한 내용을 변경하고 **확인(OK)**을 클릭합니다.

보안 태그 삭제

사용자 정의 보안 태그를 삭제할 수 있습니다. 삭제하려는 태그가 보안 그룹에 사용되고 있는 경우에는 태그 변경 사항이 보안 그룹 멤버 자격에 영향을 줄 수 있습니다.

절차

1 vSphere Web Client에 로그인합니다.

2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.

3 **이름(Name)** 열의 NSX Manager를 클릭한 후 **관리(Manage)** 탭을 클릭합니다.

4 **보안 태그(Security Tags)** 탭을 클릭합니다.

5 보안 태그를 선택하고 **보안 태그 삭제>Delete Security Tag**() 아이콘을 클릭합니다.

유효한 서비스 보기

보안 정책 개체 또는 가상 시스템에서 유효한 서비스를 볼 수 있습니다.

보안 정책에 유효한 서비스 보기

상위 정책에서 상속된 서비스를 포함하여 보안 정책에 유효한 서비스를 볼 수 있습니다.

절차

1 vSphere Web Client에 로그인합니다.

2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.

3 **보안 정책(Security Policies)** 탭을 클릭합니다.

4 **이름(Name)** 열에서 보안 정책을 클릭합니다.

5 **관리(Manage) > 정보 보안(Information Security)** 탭으로 이동합니다.

결과

세 개의 각 탭(**Endpoint 서비스(Endpoint Services)**, **방화벽(Firewall)**, **네트워크 검사 서비스(Network Introspection Services)**)에는 보안 정책에 해당하는 서비스가 표시됩니다.

유효하지 않은 서비스는 회색으로 표시됩니다. **재정의됨(Overridden)** 열에는 실제로 보안 정책에 적용되는 서비스가 표시되고 **다음에서 상속됨(Inherited from)** 열에는 서비스가 상속된 보안 정책이 표시됩니다.

보안 정책의 서비스 오류 확인

정책에 매핑된 보안 그룹에 보안 정책을 적용하지 못한 경우 해당 보안 정책에 연결된 서비스를 확인할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 정책(Security Policies)** 탭을 클릭합니다.
- 4 **이름(Name)** 열에서 보안 정책을 클릭합니다.
- 5 **모니터(Monitor) > 서비스 오류(Service Errors)** 탭으로 이동합니다.

실행 상태(Status) 열의 링크를 클릭하면 서비스 오류를 해결할 수 있는 서비스 배포 페이지로 이동합니다.

가상 시스템에 유효한 서비스 보기

가상 시스템에 적용되는 유효한 서비스를 볼 수 있습니다. 가상 시스템에 여러 보안 정책이 적용되는 경우, 즉 정책이 매핑되는 여러 보안 그룹의 일부가 가상 시스템인 경우에는 이 보기에 이러한 모든 정책의 유효한 서비스가 적용되는 순서대로 모두 나열됩니다. 서비스 상태 열에는 각 서비스의 상태가 표시됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **vCenter**를 클릭한 후 **가상 시스템(Virtual Machines)**을 클릭합니다.
- 3 **이름(Name)** 열에서 가상 시스템을 클릭합니다.
- 4 **모니터(Monitor) > Service Composer** 탭으로 이동합니다.

보안 정책 사용

보안 정책은 네트워크 및 보안 서비스 그룹입니다.

다음의 네트워크 및 보안 서비스를 보안 정책으로 그룹화할 수 있습니다.




- 끝점 서비스 - 바이러스 백신 및 취약성 관리
- 분산 방화벽 규칙
- 네트워크 검사 서비스 - 네트워크 IPS 및 네트워크 포렌식

보안 정책 우선 순위 관리

보안 정책은 가중치에 따라 적용됩니다. 가중치가 높은 보안 정책이 우선 순위가 더 높습니다. 테이블에서 정책을 위아래로 이동하면 이에 따라 가중치가 조정됩니다.

가상 시스템을 포함하는 보안 그룹이 여러 정책과 연결되어 있거나 가상 시스템이 서로 다른 정책과 연결된 여러 보안 그룹에 속해 있기 때문에 가상 시스템에 여러 보안 정책이 적용될 수 있습니다. 각 정책과 함께 그룹화된 서비스 간에 충돌이 있는 경우 정책의 가중치에 따라 가상 시스템에 적용될 서비스가 결정됩니다. 예를 들어 정책 1은 인터넷 액세스를 차단하고 가중치 값이 1000인 반면 정책 2는 인터넷 액세스를 허용하고 가중치 값이 2000인 경우, 정책 2의 가중치가 더 높으므로 가상 시스템에서 인터넷 액세스가 허용됩니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 정책(Security Policies)** 탭을 클릭합니다.
- 4 **우선 순위 관리(Manage Precedence)**() 아이콘을 클릭합니다.
- 5 우선 순위 관리 대화상자에서 우선 순위를 변경할 보안 정책을 선택하고 **위로 이동(Move Up)**() 또는 **아래로 이동(Move Down)**() 아이콘을 클릭합니다.
- 6 **확인(OK)**을 클릭합니다.

보안 정책 편집

보안 정책의 이름이나 설명 외에 관련 서비스와 규칙도 편집할 수 있습니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 정책(Security Policies)** 탭을 클릭합니다.
- 4 편집할 보안 정책을 선택하고 **보안 정책 편집(Edit Security Policy)**() 아이콘을 클릭합니다.
- 5 보안 정책 편집 대화상자에서 필요한 내용을 변경하고 **완료(Finish)**를 클릭합니다.

보안 정책 삭제

보안 정책을 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 정책(Security Policies)** 탭을 클릭합니다.
- 4 삭제할 보안 정책을 선택하고 **보안 정책 삭제>Delete Security Policy**() 아이콘을 클릭합니다.

Service Composer 시나리오

이 섹션에서는 Service Composer에 대한 가설 시나리오 몇 가지를 소개합니다. 여기서는 보안 관리자 역할을 생성하여 각 사용 사례마다 관리자에게 할당한 것으로 가정합니다.

감염된 시스템 차단 시나리오

Service Composer는 타사 바이러스 백신 솔루션으로 네트워크에서 감염된 시스템을 식별하고 이를 차단하여 추가적인 전파를 방지할 수 있습니다.

VMware의 샘플 시나리오에서는 데스크톱을 전반적으로 보호하는 방법을 보여 줍니다.

그림 17-6. Service Composer 구성

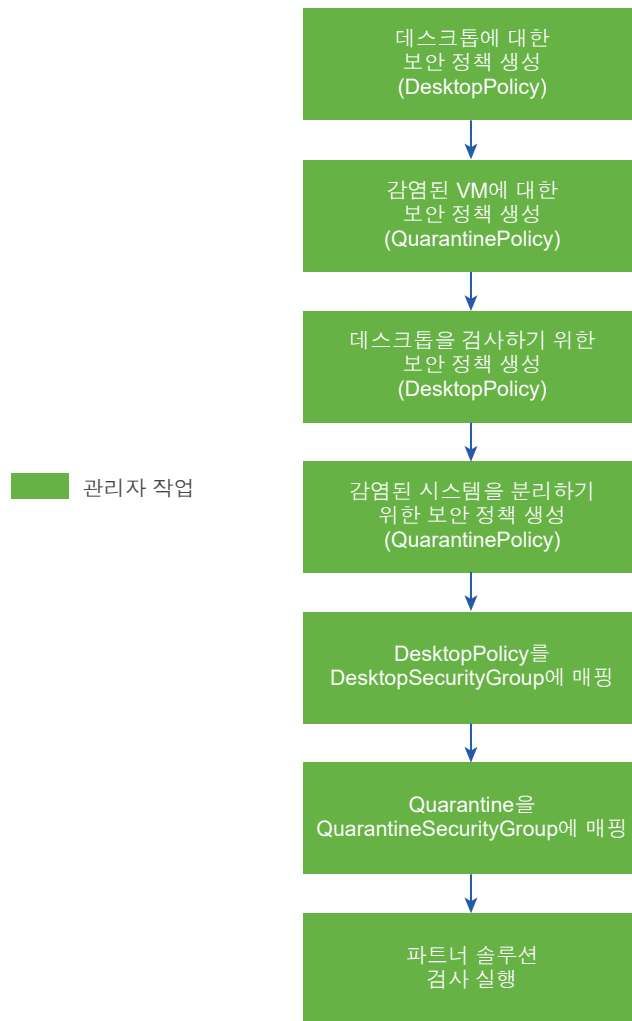
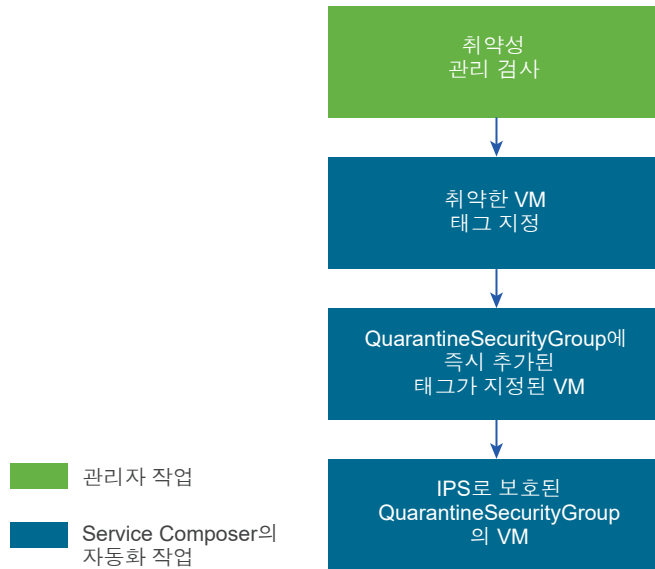


그림 17-7. Service Composer 조건부 워크플로우




사전 요구 사항

Symantec의 경우 감염된 가상 시스템에 **AntiVirus.virusFound** 태그를 지정합니다.

절차

- 1 Symantec Antimalware 솔루션을 설치, 등록 및 배포합니다.
- 2 데스크톱에 대한 보안 정책을 생성합니다.
 - a **보안 정책(Security Policies)** 탭을 클릭하고 **보안 정책 추가(Add Security Policy)** 아이콘을 클릭합니다.
 - b **이름(Name)**에 **DesktopPolicy**를 입력합니다.
 - c **설명(Description)**에 **모든 데스크톱에 대한 바이러스 백신 검사**를 입력합니다.
 - d 가중치를 51,000으로 변경합니다. 다른 모든 정책보다 우선 적용되도록 정책 우선 순위가 매우 높게 설정됩니다.
 - e **다음(Next)**을 클릭합니다.

- f Endpoint 서비스 추가 페이지에서 를 클릭하고 다음 값을 입력합니다.

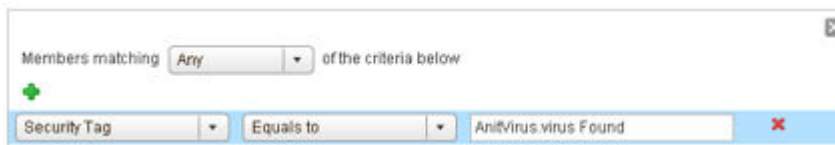
옵션	값
작업(Action)	기본값을 수정하지 않음
서비스 유형(Service Type)	Anti Virus
서비스 이름(Service Name)	Symantec Antimalware
서비스 구성(Service Configuration)	Silver
상태(State)	기본값을 수정하지 않음
적용(Enforce)	기본값을 수정하지 않음
이름(Name)	Desktop AV
설명(Description)	모든 데스크톱에서 적용할 필수 정책

- g **확인(OK)**을 클릭합니다.
- h 방화벽이나 네트워크 검사 서비스를 추가하지 않고 **완료(Finish)**를 클릭합니다.
- 3 감염된 가상 시스템에 대한 보안 정책을 생성합니다.
- a **보안 정책(Security Policies)** 탭을 클릭하고 **보안 정책 추가(Add Security Policy)** 아이콘을 클릭합니다.
- b 이름에 **QuarantinePolicy**를 입력합니다.
- c 설명에 **모든 감염된 시스템에 적용할 정책**을 입력합니다.
- d 기본 가중치를 변경하지 마십시오.
- e **다음(Next)**을 클릭합니다.
- f Endpoint 서비스 추가 페이지에서 아무 작업도 하지 않고 **다음(Next)**을 클릭합니다.
- g 방화벽에서 송신 트래픽을 모두 차단하는 규칙, 그룹으로 모든 트래픽을 차단하는 규칙 및 업데이트 적용 도구에서 들어오는 트래픽만 허용하는 규칙, 이 세 가지 규칙을 추가합니다.
- h 네트워크 검사 서비스를 추가하지 않고 **완료(Finish)**를 클릭합니다.
- 4 **QuarantinePolicy**를 다른 모든 정책보다 우선 적용할 수 있도록 보안 정책 테이블의 맨 위로 이동합니다.
- a **우선 순위 관리(Manage Priority)** 아이콘을 클릭합니다.
- b **QuarantinePolicy**를 선택하고 **위로 이동(Move Up)** 아이콘을 클릭합니다.
- 5 환경 내 모든 데스크톱에 대한 보안 그룹을 생성합니다.
- a vSphere Web Client에 로그인합니다.
- b **네트워킹 및 보안(Networking & Security)**를 클릭한 후 **Service Composer**를 클릭합니다.
- c **보안 그룹(Security Groups)** 탭을 클릭하고 **보안 그룹 추가(Add Security Group)** 아이콘을 클릭합니다.

- d 이름에 **DesktopSecurityGroup**을 입력합니다.
- e 설명에 **모든 데스크톱**을 입력합니다.
- f 이후의 일부 페이지에서 **다음(Next)**을 클릭합니다.
- g [완료 준비] 페이지에서 선택 항목을 검토하고 **완료(Finish)**를 클릭합니다.


6 감염된 가상 시스템을 배치할 차단 보안 그룹을 생성합니다.

- a **보안 그룹(Security Groups)** 탭을 클릭하고 **보안 그룹 추가(Add Security Group)** 아이콘을 클릭합니다.
- b **이름(Name)**에 **QuarantineSecurityGroup**을 입력합니다.
- c **설명(Description)**에 **바이러스 백신 검사로 식별된 감염된 VM에 기반한 동적 그룹 멤버 자격**을 입력합니다.
- d 멤버 자격 조건 정의 페이지에서 **+**를 클릭하고 다음 조건을 추가합니다.



- e 포함할 개체 선택 또는 제외할 개체 선택 페이지에서 아무 작업도 하지 않고 **다음(Next)**을 클릭합니다.
- f [완료 준비] 페이지에서 선택 항목을 검토하고 **완료(Finish)**를 클릭합니다.


7 DesktopPolicy 정책을 DesktopSecurityGroup 보안 그룹에 매핑합니다.

- a 보안 정책 탭에서 **DesktopPolicy** 정책이 선택되어 있는지 확인합니다.
- b **보안 정책 적용(Apply Security Policy)**() 아이콘을 클릭하고 **SG_Desktops** 그룹을 선택합니다.
- c **확인(OK)**을 클릭합니다.

이렇게 매핑하면 바이러스 백신 검사가 트리거되었을 때 모든 데스크톱(**DesktopSecurityGroup**의 일부)을 검사할 수 있습니다.

8 캔버스 보기로 이동하여 QuarantineSecurityGroup에 아직 가상 시스템이 포함되지 않았는지 확인합니다.

- a **정보 보안(Information Security)** 탭을 클릭합니다.

- b 그룹()에서 가상 시스템이 0개인지 확인합니다.

9 QuarantinePolicy를 QuarantineSecurityGroup에 매핑합니다.

이렇게 매핑하면 트래픽이 감염된 시스템으로 이동하지 않습니다.

10 Symantec Antimalware 콘솔에서 네트워크 검사를 트리거합니다.

검사 중 감염된 가상 시스템이 발견되고 보안 태그 **AntiVirus.virusFound**로 태그가 지정됩니다. 태그 지정된 가상 시스템은 즉시 **QuarantineSecurityGroup**에 추가됩니다. **QuarantinePolicy**가 감염된 시스템의 송신 및 수신 트래픽을 허용하지 않습니다.

보안 구성 백업

Service Composer는 보안 구성을 백업하고 나중에 이를 복원할 때 효과적으로 사용할 수 있습니다.

절차

- 1 Rapid 7 취약성 관리 솔루션을 설치, 등록 및 배포합니다.
- 2 Share Point 애플리케이션의 첫 번째 계층인 웹 서버에 대한 보안 그룹을 생성합니다.
 - a vSphere Web Client에 로그인합니다.
 - b **네트워킹 및 보안(Networking & Security)**를 클릭한 후 **Service Composer**를 클릭합니다.
 - c **보안 그룹(Security Groups)** 탭을 클릭하고 **보안 그룹 추가(Add Security Group)** 아이콘을 클릭합니다.
 - d **이름(Name)**에 **SG_Web**을 입력합니다.
 - e **설명(Description)**에서 **애플리케이션 계층에 대한 보안 그룹**을 입력합니다.
 - f **[멤버 자격 조건 정의]** 페이지에서 아무 작업도 하지 않고 **다음(Next)**을 클릭합니다.
 - g **[포함할 개체 선택]** 페이지에서 웹 서버 가상 시스템을 선택합니다.
 - h **[제외할 개체 선택]** 페이지에서 아무 작업도 하지 않고 **다음(Next)**을 클릭합니다.
 - i **[완료 준비]** 페이지에서 선택 항목을 검토하고 **완료(Finish)**를 클릭합니다.
- 3 이제 데이터베이스 및 공유 지점 서버에 대한 보안 그룹을 생성하고 이름을 각각 **SG_Database** 및 **SG_Server_SharePoint**로 지정합니다. 각 그룹에 적절한 개체를 포함시킵니다.
- 4 애플리케이션 계층에 대한 최상위 수준 보안 그룹을 생성하고 이름을 **SG_App_Group**으로 지정합니다. **SG_Web**, **SG_Database** 및 **SG_Server_SharePoint**를 이 그룹에 추가합니다.
- 5 웹 서버에 대한 보안 정책을 생성합니다.
 - a **[보안 정책]** 탭을 클릭하고 **[보안 정책 추가]** 아이콘을 클릭합니다.
 - b 이름에서 **SP_App**를 입력합니다.
 - c 설명에서 **애플리케이션 웹 서버에 대한 SP**를 입력합니다.
 - d 가중치를 50,000으로 변경합니다. 대부분의 다른 정책(차단 제외)보다 우선 적용되도록 정책 우선 순위가 매우 높게 설정됩니다.
 - e **[다음]**을 클릭합니다.

- f [Endpoint Service] 페이지에서 를 클릭하고 다음 값을 입력합니다.


옵션	값
작업(Action)	기본값을 수정하지 않음
서비스 유형(Service Type)	취약성 관리
서비스 이름(Service Name)	Rapid 7
서비스 구성(Service Configuration)	Silver
상태(State)	기본값을 수정하지 않음
적용(Enforce)	기본값을 수정하지 않음

- g 방화벽이나 네트워크 검사 서비스를 추가하지 않고 **완료(Finish)**를 클릭합니다.


- 6 SP_App을 SG_App_Group에 매핑합니다.

- 7 캔버스 보기로 이동하여 SP_App이 SG_App_Group으로 매핑되었는지 확인합니다.

- a [정보 보안] 탭을 클릭합니다.

- b  아이콘 옆의 숫자를 클릭하여 SP_App이 매핑되었는지 확인합니다.

- 8 SP_App 정책을 내보냅니다.

- a [보안 정책] 탭을 클릭하고 **Blueprint 내보내기(Export Blueprint)**() 아이콘을 클릭합니다.

- b **이름(Name)**에 **Template_ App_**를 입력하고 **접두사(Prefix)**에 **FromAppArchitect**를 입력합니다.

- c [다음]을 클릭합니다.

- d SP_App 정책을 선택하고 [다음]을 클릭합니다.

- e 선택 항목을 검토하고 [완료]를 클릭합니다.

- f 내보낸 파일을 다운로드할 컴퓨터에서 디렉토리를 선택하고 [저장]을 클릭합니다.

그러면 보안 정책과 이 정책이 적용된 모든 보안 그룹(이 경우 애플리케이션 보안 그룹과 이 그룹 안에 중첩된 세 개의 보안 그룹)이 내보내집니다.

- 9 내보낸 정책이 어떻게 작동하는지 확인하려면 SP_App 정책을 삭제합니다.

- 10 이제 7단계에서 내보낸 **Template_ App_ DevTest** 정책을 복원하겠습니다.

- a **작업(Actions)**을 클릭하고 **서비스 구성 가져오기(Import Service Configuration)** 아이콘을 클릭합니다.

- b 7단계에서 데스크톱에 저장한 **FromAppArchitect_Template_App** 파일을 선택합니다.

- c **다음(Next)**을 클릭합니다.

- d [완료 준비] 페이지에 가져올 보안 정책 및 연결된 개체(정책이 적용된 보안 그룹과 Endpoint 서비스, 방화벽 규칙 및 네트워크 검사 서비스)가 표시됩니다.
- e **완료(Finish)**를 클릭합니다.

그러면 구성 및 연결된 개체를 vCenter 인벤토리로 가져와서 캔버스 보기에 표시할 수 있습니다.

보안 정책 구성 가져오기 및 내보내기

Service Composer를 사용하여 보안 정책 구성을 한 NSX Manager에서 특정 파일 형식으로 내보내고 내보낸 구성을 다른 NSX Manager로 가져올 수 있습니다.

Service Composer에서는 보안 그룹을 직접 내보낼 수 없습니다. 먼저 보안 정책이 보안 그룹에 할당되었는지 확인한 다음, 해당 보안 정책을 내보내야 합니다. 보안 정책의 모든 콘텐츠(예: DFW 규칙, Guest Introspection 규칙, 네트워크 검사 규칙, 보안 정책에 바인딩된 보안 그룹)를 내보냅니다.

컨테이너 보안 그룹에 중첩된 보안 그룹이 포함되어 있으면 중첩된 보안 그룹은 내보내지 않습니다. 내보내는 동안 정책에 접두사를 추가할 수 있습니다. 접두사는 정책 이름, 정책 작업 이름 및 보안 그룹 이름에 적용됩니다.

구성을 다른 NSX Manager로 가져오는 경우 접미사를 지정할 수 있습니다. 접미사는 정책 이름, 정책 작업 이름 및 보안 그룹 이름에 적용됩니다. 가져오기가 수행되는 NSX Manager에 동일한 이름의 보안 그룹 또는 보안 정책이 있는 경우 보안 정책 구성 가져오기가 실패합니다.

보안 정책 구성 내보내기

보안 정책 구성을 내보낸 후 데스크톱에 저장할 수 있습니다. 정책 구성을 실수로 삭제한 경우 저장해 둔 구성을 백업으로 사용하거나 내보내 다른 NSX Manager 환경에서 사용할 수도 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **보안 정책(Security Policies)** 탭을 클릭합니다.
- 4 내보낼 보안 정책을 선택합니다.
- 5 **작업(Actions)**을 클릭한 후 **구성 내보내기(Export Configuration)**를 클릭합니다.
- 6 내보낼 구성의 이름과 설명을 입력합니다.
- 7 필요한 경우 내보낼 보안 정책 및 보안 그룹에 추가할 접두사를 입력합니다.
접두사를 지정하면 대상 보안 정책 이름에 해당 접두사가 추가되어 고유한 이름이 생성됩니다.
- 8 **다음(Next)**을 클릭합니다.
- 9 **보안 정책 선택** 페이지에서 내보낼 보안 정책을 선택하고 **다음(Next)**을 클릭합니다.

10 완료 준비 페이지에서는 내보낼 보안 정책, 끝점 서비스, 방화벽 규칙 및 네트워크 검사 서비스를 표시합니다.

이 페이지에는 보안 정책이 적용되는 보안 그룹도 표시됩니다.

11 완료(Finish)를 클릭합니다.

12 내보낸 **Blueprint**를 다운로드할 컴퓨터에서 디렉토리를 선택하고 **저장(Save)**을 클릭합니다.

지정한 위치에 보안 정책 구성 파일이 저장됩니다.

보안 정책 구성 가져오기

저장한 보안 정책 구성을 백업으로 가져오거나 다른 **NSX Manager**에서 비슷한 구성을 복원할 수 있습니다.

구성을 가져올 때 빈 보안 그룹이 생성됩니다. 모든 서비스, 서비스 프로파일, 애플리케이션 및 애플리케이션 그룹은 대상 환경에 있어야 합니다. 그렇지 않으면 가져오기가 실패합니다.

절차

1 vSphere Web Client에 로그인합니다.

2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.

3 **보안 정책(Security Policies)** 탭을 클릭합니다.

4 **작업(Actions)**을 클릭하고 **서비스 구성 가져오기(Import Service Configuration)** 아이콘을 클릭합니다.

5 가져올 구성 파일을 선택합니다.

6 필요한 경우 가져올 보안 정책 및 보안 그룹에 추가할 접미사를 입력합니다.

접미사를 지정하면 가져올 보안 정책 이름에 해당 접미사가 추가되어 고유한 이름이 생성됩니다.

7 **다음(Next)**를 클릭합니다.

Service Composer는 구성에서 참조되는 모든 서비스가 대상 환경에서 사용 가능한지 확인합니다. 그렇지 않은 경우 누락된 서비스를 사용 가능한 대상 서비스에 매핑할 수 있는 **누락된 서비스 관리** 페이지가 표시됩니다.

완료 준비 페이지에서는 가져올 보안 정책, 끝점 서비스, 방화벽 규칙 및 네트워크 검사 서비스를 표시합니다. 이 페이지에는 보안 정책이 적용되는 보안 그룹도 표시됩니다.

8 **완료(Finish)**를 클릭합니다.

가져온 보안 정책 구성은 대상 **NSX Manager**에서 보안 정책 테이블의 맨 위(기존 정책 위)에 추가됩니다. 보안 정책에서 가져온 규칙 및 보안 서비스의 원래 순서가 유지됩니다.

Guest Introspection은 바이러스 백신 및 멀웨어 방지 에이전트 처리 작업을 VMware 파트너가 제공하는 전용 보안 가상 장치로 오프로드합니다. 게스트 가상 시스템과 달리 보안 가상 장치는 오프라인 상태로 전환되지 않으므로 바이러스 백신 서명을 지속적으로 업데이트하여 호스트의 가상 시스템을 중단 없이 보호할 수 있습니다. 또한 새로운 가상 시스템이나 오프라인 상태로 전환된 기존 가상 시스템은 온라인 상태가 되면 최신 바이러스 백신 서명을 통해 즉시 보호됩니다.

Guest Introspection 상태는 vCenter Server 콘솔에서 빨간색으로 표시되는 경보를 통해 전달됩니다. 또한 이벤트 로그를 확인하여 상태 정보를 추가로 수집할 수 있습니다.

중요 작업 환경이 Guest Introspection 보안을 유지할 수 있도록 올바르게 구성되어 있어야 합니다.

- Guest Introspection을 적용할 수 있도록 보호되는 가상 시스템을 포함하는 리소스 풀의 모든 호스트를 준비해야 합니다. 그래야 가상 시스템이 vMotion을 통해 리소스 풀 내의 ESXi 호스트 간에 이동될 때 계속 보호됩니다.
- 가상 시스템이 Guest Introspection 보안 솔루션으로 보호되려면 Guest Introspection Thin Agent가 설치되어 있어야 합니다. 모든 게스트 운영 체제가 지원되는 것은 아닙니다. 지원되지 않는 운영 체제가 설치된 가상 시스템은 보안 솔루션을 통해 보호되지 않습니다.

본 장은 다음 항목을 포함합니다.

- [호스트 클러스터에 Guest Introspection 설치](#)
- [Windows 가상 시스템에서 Guest Introspection Thin Agent 설치](#)
- [Linux 가상 시스템에서 Guest Introspection Thin Agent 설치](#)
- [Guest Introspection 상태 보기](#)
- [Guest Introspection 감사 메시지](#)
- [Guest Introspection 문제 해결 데이터 수집](#)
- [Guest Introspection 모듈 제거](#)

호스트 클러스터에 Guest Introspection 설치

Guest Introspection을 설치하면 클러스터의 각 호스트에 새 VIB 및 서비스 가상 시스템이 자동으로 설치됩니다. Activity Monitoring, 여러 타사 보안 솔루션을 사용하려면 Guest Introspection이 필요합니다.

참고 vMotion/SvMotion을 사용하여 SVM(서비스 VM)을 마이그레이션할 수 없습니다. SVM이 올바르게 작동하려면 배포된 호스트에 유지되어야 합니다.

사전 요구 사항

수행할 설치 지침에서는 사용자가 다음 시스템을 갖추고 있는 것으로 간주합니다.

- 지원되는 버전의 vCenter Server 및 ESXi가 클러스터의 각 호스트에 설치되어 있는 데이터센터.
- 클러스터의 호스트가 vCenter Server 버전 5.0에서 5.5로 업그레이드된 경우 해당 호스트에서 포트 80 및 443을 열어야 합니다.
- Guest Introspection을 설치하려는 클러스터의 호스트는 NSX 준비가 완료되어 있습니다. "NSX 설치 가이드"에서 "NSX에 대한 호스트 클러스터 준비"를 참조하십시오. 독립형 호스트에는 Guest Introspection을 설치할 수 없습니다. 바이러스 백신 오프로드 기능 전용 Guest Introspection을 배포 및 관리하기 위해 NSX를 사용하는 경우에는 NSX를 위해 호스트를 준비할 필요가 없습니다. NSX for vShield Endpoint 라이선스에서 허용하지 않기 때문입니다.
- NSX Manager가 설치되어 실행되고 있습니다.
- NSX Manager 및 Guest Introspection 서비스를 실행할 준비된 호스트가 동일한 NTP 서버에 연결되었고 시간이 동기화되었는지 확인합니다. 확인하지 않으면 클러스터의 상태가 Guest Introspection 및 타사 서비스에 대해 녹색으로 표시되어도 VM이 바이러스 백신 서비스로 보호되지 않을 수 있습니다.

NTP 서버가 추가되면 Guest Introspection 및 타사 서비스를 다시 배포하는 것이 좋습니다.

NSX Guest Introspection 서비스 가상 시스템에 IP 풀의 IP 주소를 할당하려면 NSX Guest Introspection을 설치하기 전에 IP 풀을 생성합니다. "NSX 관리 가이드"에서 IP 풀 사용을 참조하십시오.

vSphere Fault Tolerance가 Guest Introspection에서는 작동하지 않습니다.

절차

- 1 **설치(Installation)** 탭에서 **서비스 배포(Service Deployments)**를 클릭합니다.
- 2 **새 서비스 배포(New Service Deployment)**() 아이콘을 클릭합니다.
- 3 네트워크 및 보안 서비스 배포 대화상자에서 **Guest Introspection**을 선택합니다.
- 4 대화상자 아래쪽의 **스케줄 지정(Specify schedule)**에서 **지금 배포(Deploy now)**를 선택하여 Guest Introspection을 설치 즉시 배포하거나 배포 날짜 및 시간을 선택합니다.
- 5 **다음(Next)**을 클릭합니다.
- 6 Guest Introspection을 설치할 데이터센터 및 클러스터를 선택하고 **다음(Next)**을 클릭합니다.

- 7 [스토리지 및 관리 네트워크 선택] 페이지에서 서비스 가상 시스템 스토리지를 추가할 데이터스토어를 선택하거나 **지정된 호스트(Specified on host)**를 선택합니다. "지정된 호스트" 대신 공유 데이터스토어 및 네트워크를 사용하여 배포 워크플로우를 자동화하는 것이 좋습니다.

선택한 데이터스토어는 선택한 클러스터의 모든 호스트에서 사용할 수 있어야 합니다.

지정된 호스트(Specified on host)를 선택했을 경우 클러스터의 각 호스트에 대해 아래의 단계를 수행합니다.

- a vSphere Web Client 홈 페이지에서 **vCenter**를 클릭하고 **호스트(Hosts)**를 클릭합니다.
 - b **이름(Name)** 열에서 호스트를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
 - c **에이전트 VM(Agent VMs)**을 클릭하고 **편집(Edit)**을 클릭합니다.
 - d 데이터스토어를 선택하고 **확인(OK)**을 클릭합니다.
- 8 관리 인터페이스를 호스팅할 분산 가상 포트 그룹을 선택합니다. 데이터스토어가 **지정된 호스트(Specified on host)**로 설정된 경우 네트워크도 **지정된 호스트(Specified on host)**로 설정해야 합니다.

선택한 포트 그룹이 NSX Manager의 포트 그룹에 액세스할 수 있어야 하고 선택한 클러스터의 모든 호스트에서 사용 가능해야 합니다.

지정된 호스트(Specified on host)를 선택했을 경우 7단계의 하위 단계를 수행하여 호스트의 네트워크를 선택합니다. 호스트(또는 다중 호스트)를 클러스터에 추가할 경우 호스트가 클러스터에 추가되기 전에 데이터스토어와 네트워크를 설정해야 합니다.

- 9 IP 할당에서 다음 중 하나를 선택합니다.

선택	수행되는 작업
DHCP	DHCP(Dynamic Host Configuration Protocol)를 통해 IP 주소를 NSX Guest Introspection 서비스 가상 시스템에 할당합니다. 호스트가 다른 서브넷에 있는 경우 이 옵션을 선택합니다.
IP 풀	선택한 IP 풀의 IP 주소를 NSX Guest Introspection 서비스 가상 시스템에 할당합니다.

- 10 **다음(Next)**을 클릭한 후 [완료 준비] 페이지에서 **완료(Finish)**를 클릭합니다.
- 11 **설치 상태(Installation Status)** 열이 **성공(Succeeded)**으로 표시될 때까지 배포를 모니터링합니다.
- 12 **설치 상태(Installation Status)** 열에 **실패(Failed)**가 표시되면 실패 옆의 아이콘을 클릭합니다. 그러면 모든 배포 오류가 표시됩니다. **해결(Resolve)**을 클릭하여 오류를 해결합니다. 경우에 따라 오류를 해결하면 다른 오류가 표시됩니다. 필요한 조치를 취하고 **해결(Resolve)**을 다시 클릭합니다.

Windows 가상 시스템에서 Guest Introspection Thin Agent 설치

Guest Introspection 보안 솔루션을 사용하여 VM을 보호하려면 VM에 Guest Introspection 드라이버라고도 하는 Guest Introspection Thin Agent를 설치해야 합니다. Guest Introspection 드라이버는 Windows용 VMware Tools에 포함되어 있으나 기본 설치의 일부는 아닙니다. Windows VM에 Guest Introspection을 설치하려면 사용자 지정 설치를 수행하고 해당 드라이버를 선택해야 합니다.

- vSphere 5.5 또는 6.0을 사용하는 경우 다음의 VMware Tools 설치 지침을 참조하십시오. http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html.
- vSphere 6.5를 사용하는 경우 다음의 VMware Tools 설치 지침을 참조하십시오. <https://www.vmware.com/support/pubs/vmware-tools-pubs.html>.

Guest Introspection 드라이버가 설치된 Windows 가상 시스템은 보안 솔루션이 설치된 ESXi 호스트에서 시작될 때마다 자동으로 보호됩니다. 보호된 가상 시스템은 보안 솔루션이 설치된 다른 ESXi 호스트로 vMotion이 이동한 후에도 종료할 때부터 다시 시작할 때까지 보안 상태를 유지합니다.

Linux 지침에 대해서는 [Linux 가상 시스템에서 Guest Introspection Thin Agent 설치](#)를 참조하십시오.

사전 요구 사항

게스트 가상 시스템에 지원되는 Windows 버전이 설치되어 있는지 확인하십시오. NSX Guest Introspection에서는 다음 Windows 운영 체제가 지원됩니다.

- Windows XP SP3 이상(32비트)
- Windows Vista(32비트)
- Windows 7(32/64비트)
- Windows 8(32/64비트) -- vSphere 5.5만 해당
- Windows 8.1(32/64) -- vSphere 5.5 패치 2 이상
- Windows 10
- Windows 2003 SP2 이상(32/64비트)
- Windows 2003 R2(32/64비트)
- Windows 2008(32/64비트)
- Windows 2008 R2(64비트)
- Win2012(64) -- vSphere 5.5만 해당
- Win2012 R2(64) -- vSphere 5.5 패치 2 이상

절차

- 1 VMware Tools 설치를 시작하고 사용 중인 vSphere 버전의 지침을 따릅니다. **사용자 지정(Custom)** 설치를 선택합니다.

2 VMCI 드라이버(VMCI Driver) 섹션을 확장합니다.

사용 가능한 옵션은 VMware Tools 버전에 따라 다릅니다.

드라이버	설명
vShield Endpoint 드라이버	파일 자체 검사(vsepfilt) 및 네트워크 자체 검사(vnetflt) 드라이버를 설치합니다.
Guest Introspection 드라이버	파일 자체 검사(vsepfilt) 및 네트워크 자체 검사(vnetflt) 드라이버를 설치합니다.
NSX 파일 자체 검사 드라이버 및 NSX 네트워크 자체 검사 드라이버	<p>[NSX 파일 자체 검사 드라이버]를 선택하여 vsepfilt을 설치합니다.</p> <p>필요에 따라 [NSX 네트워크 자체 검사 드라이버]를 선택하여 vnetflt(Windows 10에서는 vnetWFP)를 설치합니다.</p> <p>참고 ID 방화벽 또는 끝점 모니터링 기능을 사용하는 경우에만 [NSX 네트워크 자체 검사 드라이버]를 선택합니다.</p>

3 추가하려는 드라이버 옆의 드롭다운 메뉴에서 **이 기능은 로컬 하드 드라이브에 설치됩니다.(This feature will be installed on the local hard drive)**를 선택합니다.

4 절차의 나머지 단계를 수행합니다.

다음에 수행할 작업

Thin Agent가 관리 권한의 fltmc 명령을 사용하여 실행되고 있는지 확인합니다. 출력의 [파일 이름] 열에는 vsepfilt 항목이 있는 Thin Agent가 나열됩니다.

Linux 가상 시스템에서 Guest Introspection Thin Agent 설치

Guest Introspection은 바이러스 백신 용도로만 Linux에서 파일 검사를 지원합니다. Guest Introspection 보안 솔루션을 사용하여 Linux VM을 보호하려면 Guest Introspection Thin Agent를 설치해야 합니다.

GI Thin Agent는 VMware Tools OSP(운영 체제별 패키지)의 일부로 사용할 수 있습니다. VMware Tools는 설치하지 않아도 됩니다. GI Thin Agent 설치 및 업그레이드는 NSX 설치 및 업그레이드에 연결되지 않습니다. 또한 엔터프라이즈 또는 보안 관리자(비 NSX 관리자)는 NSX 외부의 게스트 VM에 이 에이전트를 설치할 수 있습니다.

RHEL 또는 SLES 시스템에 GI Thin Agent를 설치하려면 RPM 패키지를 사용하십시오. Ubuntu Linux 시스템에 GI Thin Agent를 설치하려면 DEB 패키지를 사용하십시오.

Windows 지침에 대해서는 [Windows 가상 시스템에서 Guest Introspection Thin Agent 설치](#)를 참조하십시오.

사전 요구 사항

- 게스트 가상 시스템에 지원되는 Linux 버전이 설치되어 있는지 확인하십시오.
 - RHEL(Red Hat Enterprise Linux) 7 GA(64비트)
 - SLES(SUSE Linux Enterprise Server) 12 GA(64비트)

- Ubuntu 14.04 LTS(64비트)
- Linux VM에 GLib 2.0이 설치되어 있는지 확인합니다.
- VMware 패키지 저장소 <https://packages.vmware.com/packages/index.html>을 방문하여 GI Thin Agent 패키지(vmware-nsx-gi-file)를 다운로드합니다.

절차

- ◆ Linux 운영 체제에 따라 루트 권한을 사용하여 다음 단계를 수행하십시오.

- Ubuntu 시스템:

- a 다음 명령을 사용하여 VMware 패키징 공용 키를 가져옵니다.

```
curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

- b /etc/apt/sources.list.d에 새 파일 *vm.list*를 생성합니다.

- c 다음 내용으로 파일을 편집합니다.

```
vi /etc/apt/sources.list.d/vm.list
deb https://packages.vmware.com/packages/ubuntu/ trusty main
```

- d 이제 다음과 같이 패키지를 설치합니다.

```
apt-get update
apt-get install vmware-nsx-gi-file
```

- RHEL7 시스템:

- a 다음 명령을 사용하여 VMware 패키징 공용 키를 가져옵니다.

```
curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

- b /etc/yum.repos.d에 새 파일 *vm.repo*를 생성합니다.

- c 다음 내용으로 파일을 편집합니다.

```
vi /etc/yum.repos.d/vm.repo
[vm]
name = VMware
baseurl = https://packages.vmware.com/packages/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```


- d 이제 다음과 같이 패키지를 설치합니다.

```
yum install vmware-nsx-gi-file
```

◆ SLES 시스템:

- a 다음 명령을 사용하여 VMware 패키징 공용 키를 가져옵니다.

```
curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub  
  
rpm --import VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

- b 다음 저장소를 추가합니다.

```
zypper ar -f "https://packages.vmware.com/packages/sle12/x86_64/" VMware
```

- c 이제 다음과 같이 패키지를 설치합니다.

```
zypper install vmware-nsx-gi-file
```

다음에 수행할 작업

Thin Agent가 관리 권한의 `service vsep` `status` 명령을 사용하여 실행되고 있는지 확인합니다. 상태는 실행 중이어야 합니다.

Guest Introspection 상태 보기

Guest Introspection 인스턴스 모니터링에는 SVM(보안 가상 시스템), ESXi 호스트-상주 Guest Introspection 모듈 및 보호되는 가상 시스템-상주 Thin Agent 등의 Guest Introspection 구성 요소에서 비롯되는 상태의 점검이 포함됩니다.

절차

- 1 vSphere Web Client에서 **vCenter 인벤토리 목록(vCenter Inventory Lists)**을 클릭한 후 **데이터 센터(Datacenters)**를 클릭합니다.
- 2 **이름(Name)** 열에서 데이터 센터를 클릭합니다.
- 3 **모니터(Monitor)**를 클릭하고 **Guest Introspection**을 클릭합니다.

Guest Introspection 상태 및 정보 페이지에서는 선택한 데이터 센터에 있는 개체의 상태와 활성 경로를 보여 줍니다. 상태 변경 사항은 변경을 유발한 이벤트가 실제 발생한 시점으로부터 1분 이내에 반영됩니다.

Guest Introspection 감사 메시지

감사 메시지는 치명적인 오류와 그 외 중요한 감사 메시지를 포함하며 `vmware.log`에 로깅됩니다.

다음 상황은 감사 메시지로 로깅됩니다.

- Thin Agent 초기화 성공(및 버전 번호)

- Thin Agent 초기화 실패
- SVM과의 첫 번째 통신이 설정됨
- SVM과의 통신을 설정하지 못함(해당 실패가 처음 발생한 경우)

생성된 로그 메시지 중 각 로그 메시지의 시작 부분 근처에 다음과 같은 하위 문자열이 있습니다. **vf-AUDIT**, **vf-ERROR**, **vf-WARN**, **vf-INFO**, **vf-DEBUG**.

Guest Introspection 문제 해결 데이터 수집

VMware 기술 지원은 지원 요청이 처리될 때 진단 정보 또는 지원 번들을 주기적으로 요청합니다. 이 진단 정보에는 가상 시스템에 대한 로그 및 구성 파일이 포함되어 있습니다.

ID 방화벽 문제 해결 데이터

ID 기반 방화벽 환경이 Guest Introspection을 사용하는 경우 "NSX 문제 해결 가이드" 및 "NSX 로깅 및 시스템 이벤트"에서 진단 정보를 찾을 수 있습니다.

Guest Introspection 모듈 제거

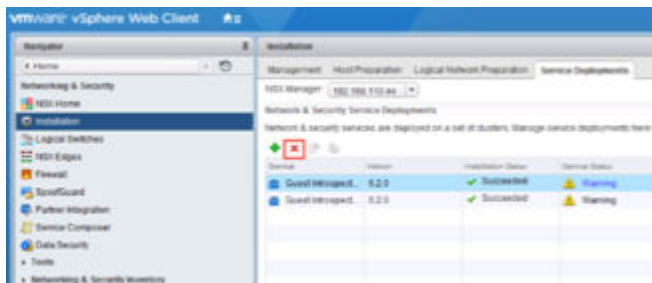
Guest Introspection을 제거하면 클러스터 내의 호스트에서 VIB가 제거되며 클러스터 내의 각 호스트에서 서비스 가상 시스템이 제거됩니다. ID 방화벽, 끝점 모니터링, 여러 타사 보안 솔루션을 사용하려면 Guest Introspection이 필요합니다. Guest Introspection 모듈 제거는 폭넓은 영향을 미칠 수 있습니다.

경고 클러스터에서 Guest Introspection 모듈을 제거하기 전에 해당 클러스터의 호스트에서 Guest Introspection을 사용하는 모든 타사 제품을 제거해야 합니다. 솔루션 제공자의 지침을 따르십시오.

NSX 클러스터의 VM에 대한 보호가 손실됩니다. 제거하기 전에 클러스터의 VM에 대해 vMotion을 수행해야 합니다.

Guest Introspection을 제거하기 위해서는,

- 1 vCenter에서 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)**로 이동하고 **서비스 배포(Service Deployments)** 탭을 선택합니다.
- 2 Guest Introspection 인스턴스를 선택하고 삭제 아이콘을 클릭합니다.
- 3 지금 삭제하거나 추후 삭제를 예약합니다.



Linux용 Guest Introspection 제거

게스트 가상 시스템에서 Guest Introspection용 Linux Thin Agent를 제거할 수 있습니다.

사전 요구 사항

Linux용 Guest Introspection이 설치됩니다. Linux 시스템에 대해 루트 권한이 있습니다.

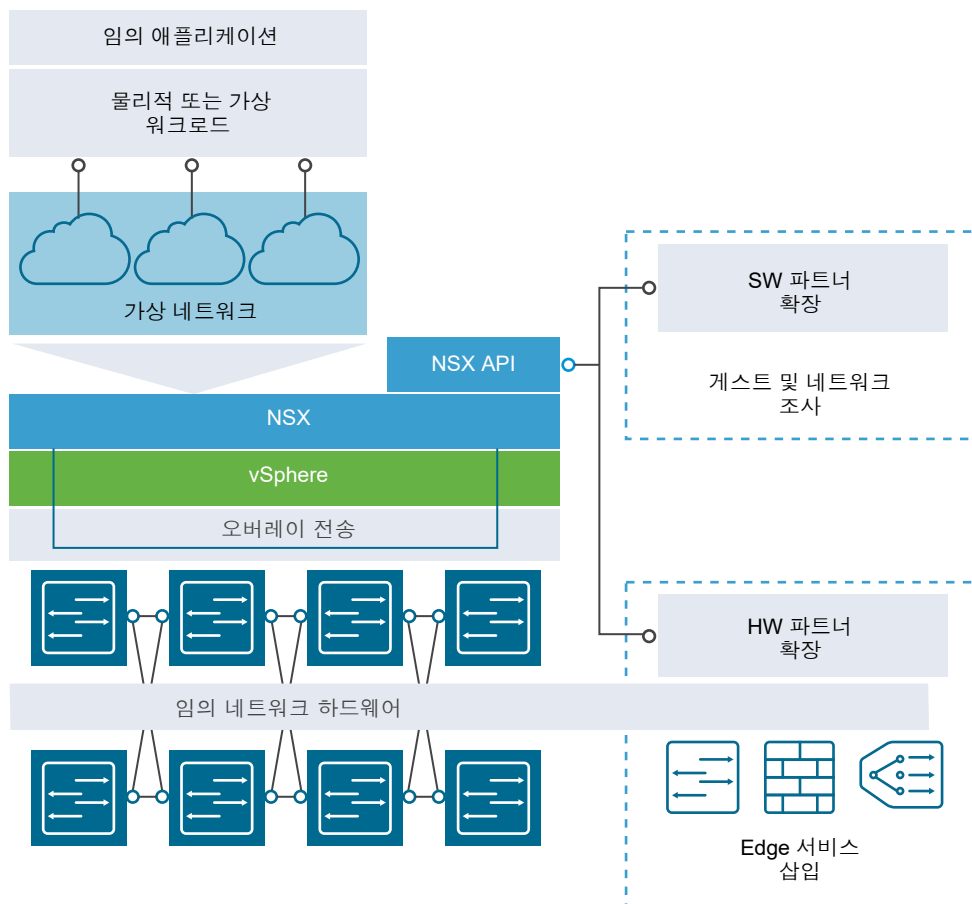
절차

- ◆ Ubuntu 시스템에서 패키지를 제거할 때는 `apt-get remove vmware-nsx-gi-file` 명령을 실행합니다.
- ◆ RHEL7 시스템에서 패키지를 제거할 때는 `yum remove vmware-nsx-gi-file` 명령을 실행합니다.
- ◆ SLES 시스템에서 패키지를 제거할 때는 `zypper remove vmware-nsx-gi-file` 명령을 실행합니다.

결과

Linux 가상 시스템에 설치된 Thin Agent가 제거됩니다.

일반적으로 데이터센터 네트워크에는 스위칭, 라우팅, 방화벽 기능, 로드 밸런싱 등을 포함한 다양한 네트워크 서비스가 포함되어 있습니다. 대부분의 경우 서로 다른 벤더들이 이 서비스를 제공합니다. 물리적 환경에서는 이런 서비스를 네트워크에서 연결하는 것이 물리적 네트워크 디바이스의 랙 및 스택 작업, 물리적인 연결 설정, 서비스의 별도 관리 작업이 포함된 복잡한 업무가 될 수 있습니다. **NSX**는 적절한 서비스를 적절한 트래픽 경로에서 연결하는 작업을 단순화함으로써 단일 **ESX Server** 호스트 또는 다중 **ESX Server** 호스트에서 프로덕션, 테스트 및 개발을 위해 복잡한 네트워크를 구축할 수 있도록 도와줄 수 있습니다.



타사 서비스를 **NSX**에 삽입하는 다양한 배포 방법이 있습니다.

본 장은 다음 항목을 포함합니다.

- 분산 서비스 삽입
- **Edge** 기반 서비스 삽입
- 타사 서비스 통합
- 파트너 서비스 배포
- **Service Composer**를 통한 벤더 서비스 이용
- 논리적 방화벽을 통해 벤더 솔루션으로 트래픽 리디렉션
- 파트너 로드 밸런서 이용
- 타사 통합 제거

분산 서비스 삽입

분산 서비스 삽입에서 단일 호스트는 단일 물리적 시스템에 모든 서비스 모듈, 커널 모듈 및 가상 시스템 구현을 보유하고 있습니다. 시스템의 모든 구성 요소는 물리적 호스트 내 구성 요소와 상호 작용합니다. 이를 통해 모듈 간의 통신이 더 빨라지고 배포 모델이 소형화됩니다. 네트워크의 물리적 시스템에 동일한 구성을 복제하여 확장할 수 있는 반면, 서비스 모듈과 **vmkernel** 간의 제어부 및 데이터부 트래픽은 동일한 물리적 시스템에서 유지됩니다. 보호된 가상 시스템의 **vMotion** 중에 파트너 보안 시스템이 가상 시스템 상태를 소스에서 대상 호스트로 이동합니다.

이런 유형의 서비스 삽입을 사용하는 벤더 솔루션에는 **IPS(Intrusion Prevention Service)/IDS(Intrusion Detection Service)**, **Firewall**, **Anti Virus**, **FIM(File Identity Monitoring)** 및 취약성 관리가 포함됩니다.

Edge 기반 서비스 삽입

NSX Edge는 다른 네트워크 서비스와 함께 **Edge Services Cluster**에서 가상 시스템으로 배포됩니다. **NSX Edge**에는 특정 트래픽을 타사 네트워크 서비스로 리디렉션할 수 있는 기능이 있습니다.

이런 유형의 서비스 삽입을 이용하는 벤더 솔루션에는 **ADC/로드 밸런서** 디바이스가 포함됩니다.

타사 서비스 통합

타사 서비스를 **NSX** 플랫폼에 삽입하기 위한 일반적인 높은 수준의 워크플로우입니다.

절차

- 1 벤더의 콘솔에서 타사 서비스를 **NSX Manager**에 등록합니다.

서비스를 등록하려면 **NSX** 로그인 자격 증명이 필요합니다. 자세한 내용은 벤더 설명서를 참조하십시오.

- 2 **NSX**에서 서비스를 배포합니다. **파트너 서비스 배포**를 참조하십시오.

배포되면 타사 서비스가 **NSX** 서비스 정의 창에 표시되고 사용할 준비가 됩니다. **NSX**에서 서비스를 사용하는 절차는 삽입된 서비스 유형에 따라 달라집니다.

예를 들어, **Service Composer**에서 보안 정책을 생성하거나 트래픽을 서비스로 리디렉션하는 방화벽 규칙을 생성하여 호스트 기반 방화벽 서비스를 사용하도록 설정할 수 있습니다. **Service Composer**를 통한 **벤더 서비스 이용** 또는 **논리적 방화벽을 통해 벤더 솔루션으로 트래픽 리디렉션**을 참조하십시오. Edge 기반 서비스 사용에 대한 자세한 내용은 **파트너 로드 밸런서 이용** 항목을 참조하십시오.

파트너 서비스 배포


파트너 솔루션에 호스트 상주 가상 장치가 포함된 경우 솔루션을 **NSX Manager**에 등록한 후 서비스를 배포할 수 있습니다.

사전 요구 사항

다음 사항을 충족하는지 확인하십시오.

- 파트너 솔루션이 **NSX Manager**에 등록되어 있는지 확인합니다.
- **NSX Manager**가 파트너 솔루션의 관리 콘솔에 액세스할 수 있는지 확인합니다.
- 필요한 라이선스 버전이 할당되었습니다. <https://kb.vmware.com/kb/2145269>를 참조하십시오.

절차

- 1 **Networking & Security**를 클릭하고 **설치(Installation)**를 클릭합니다.
- 2 **서비스 배포(Service Deployments)** 탭을 클릭하고 **새 서비스 배포(New Service Deployment)**() 아이콘을 클릭합니다.
- 3 네트워크 및 보안 서비스 배포 대화상자에서 해당 솔루션을 선택합니다.
- 4 대화상자 아래쪽의 **스케줄 지정(Specify schedule)**에서 **지금 배포(Deploy now)**를 선택하여 솔루션을 즉시 배포하거나 배포 날짜 및 시간을 선택합니다.
- 5 **다음(Next)**을 클릭합니다.
- 6 솔루션을 배포할 데이터센터 및 클러스터를 선택하고 **다음(Next)**을 클릭합니다.
- 7 솔루션 서비스 가상 시스템 스토리지를 추가할 데이터스토어를 선택하거나 **지정된 호스트(Specified on host)**를 선택합니다.

선택한 데이터스토어는 선택한 클러스터의 모든 호스트에서 사용할 수 있어야 합니다.

지정된 호스트(Specified on host)를 선택한 경우 ESX 호스트를 클러스터에 추가하기 전에 해당 ESX 호스트의 데이터스토어를 호스트의 **에이전트 VM 설정(AgentVM Settings)**에 지정해야 합니다. 자세한 내용은 "vSphere API/SDK 설명서"를 참조하십시오.

- 8 관리 인터페이스를 호스팅할 분산 가상 포트 그룹을 선택합니다. 이 포트 그룹은 **NSX Manager**의 포트 그룹에 연결할 수 있어야 합니다.

네트워크를 **지정된 호스트(Specified on host)**로 설정한 경우 클러스터에 있는 각 호스트의 **에이전트 VM 설정 > 네트워크(Agent VM Settings > Network)** 속성에 사용할 네트워크를 지정해야 합니다. 자세한 내용은 "vSphere API/SDK 설명서"를 참조하십시오.

호스트를 클러스터에 추가하기 전에 호스트에 대해 에이전트 VM 네트워크 속성을 설정해야 합니다.

관리(Manage) > 설정(Settings) > 에이전트 VM 설정(Agent VM Settings) > 네트워크(Network)로 이동하고 **편집(Edit)**을 클릭하여 에이전트 VM 네트워크를 설정합니다.

선택한 포트 그룹은 선택한 클러스터의 모든 호스트에서 사용할 수 있어야 합니다.

9 IP 할당에서 다음 중 하나를 선택합니다.

선택	수행되는 작업
DHCP	DHCP(Dynamic Host Configuration Protocol)를 통해 IP 주소를 서비스 가상 시스템에 할당합니다.
IP 풀	선택한 IP 풀의 IP 주소를 서비스 가상 시스템에 할당합니다.

10 **다음(Next)**을 클릭한 후 [완료 준비] 페이지에서 **완료(Finish)**를 클릭합니다.

11 **설치 상태(Installation Status)**가 [성공]으로 표시될 때까지 배포를 모니터링합니다. 상태가 [실패]로 표시되면 [실패] 옆에 있는 아이콘을 클릭하고 오류를 해결할 조치를 취합니다.

다음에 수행할 작업

이제 NSX UI 또는 NSX API를 통해 파트너 서비스를 사용할 수 있습니다.

Service Composer를 통한 벤더 서비스 이용

타사 벤더 서비스는 트래픽 리디렉션, 로드 밸런서 및 데이터 손실 방지, 바이러스 백신 등을 포함한 게스트 보안 서비스를 포함합니다. Service Composer를 사용하여 이러한 서비스를 vCenter 개체의 집합에 적용할 수 있습니다.

보안 그룹은 클러스터, 가상 시스템, vNICs 및 논리적 스위치와 같은 vCenter 개체의 집합입니다. 보안 정책은 Guest Introspection 서비스, 방화벽 규칙, 네트워크 검사 서비스의 집합입니다.

보안 정책을 보안 그룹에 매핑할 때 리디렉션 규칙이 적절한 타사 벤더 서비스 프로파일에 생성됩니다. 해당 보안 그룹에 속하는 가상 시스템에서 트래픽이 발생하기 때문에 트래픽 처리 방법을 지정하는 등록된 타사 벤더 서비스로 트래픽이 리디렉션됩니다. Service Composer에 대한 자세한 내용은 [Service Composer 사용](#) 항목을 참조하십시오.

논리적 방화벽을 통해 벤더 솔루션으로 트래픽 리디렉션

등록된 벤더 솔루션으로 트래픽 리디렉션하기 위해 방화벽 규칙을 추가할 수 있습니다. 그러면 벤더 서비스가 트래픽 리디렉션을 처리합니다.

사전 요구 사항

- 타사 서비스는 반드시 NSX Manager에 등록되어야 하며 NSX 내에서 배포되어야 합니다.
- 기본 방화벽 규칙 작업이 차단하도록 설정되어 있는 경우 트래픽이 리디렉션될 수 있는 규칙을 추가해야 합니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > 방화벽(Firewall)**으로 이동합니다.
- 2 **파트너 보안 서비스(Partner security services)** 탭을 클릭합니다.
- 3 규칙을 추가할 섹션에서 **규칙 추가(Add rule)(+)** 아이콘을 클릭합니다.
새로 생성한 규칙은 섹션의 맨 위에 추가됩니다.
- 4 새 규칙의 **이름(Name)** 셀을 가리키고 **+**을 클릭합니다. 그리고 규칙의 이름을 입력합니다.
- 5 규칙의 **소스(Source)**, **대상(Destination)** 및 **서비스(Service)** 를 지정합니다. 자세한 내용은 [분산 방화벽 규칙 추가](#) 항목을 참조하십시오.
- 6 새 규칙의 **작업(Action)** 셀을 가리키고 **+**을 클릭합니다.
 - a **작업(Action)**에서, **리디렉션(Redirect.)**을 선택합니다.
 - b **리디렉션 대상(Redirect To)**에서 서비스 프로파일에 바인딩하려는 논리적 스위치 또는 보안 그룹을 선택합니다.
서비스 프로파일이 선택된 논리적 스위치 또는 보안 그룹에 연결되었거나 포함된 가상 시스템에 적용됩니다.
 - c 트래픽 리디렉션의 기록 여부를 지정하고 필요한 경우 주석을 입력합니다.
 - d **확인(OK)**을 클릭합니다.
선택된 서비스 프로파일이 **작업(Action)** 열에 링크로 표시됩니다. 서비스 프로파일 링크를 클릭하면 서비스 프로파일 바인딩이 표시됩니다.
- 7 **변경 내용 게시(Publish Changes)**를 클릭합니다.

파트너 로드 밸런서 이용

특정 NSX Edge에 대한 트래픽 밸런싱을 위해 타사 로드 밸런서를 사용할 수 있습니다.

사전 요구 사항

타사 로드 밸런서는 반드시 NSX Manager에 등록되어야 하며 NSX 내에서 배포되어야 합니다.

절차

- 1 vSphere Web Client에서 **네트워킹 및 보안(Networking & Security) > NSX Edge(NSX Edges)**로 이동합니다.
- 2 NSX Edge를 두 번 클릭합니다.
- 3 **관리(Manage)**를 클릭하고 **로드 밸런서(Load Balancer)** 탭을 클릭합니다.
- 4 로드 밸런서 글로벌 구성 옆에 있는 **편집(Edit)**을 클릭합니다.

- 5 로드 밸런서 사용(Enable Load Balancer) 및 서비스 삽입 사용(Enable Service Insertion)을 선택합니다.
- 6 서비스 정의(Service Definition)에서 적절한 파트너 로드 밸런서를 선택합니다.
- 7 서비스 구성(Service Configuration)에서 적절한 서비스 구성을 선택합니다.
- 8 남은 필드를 완성하고 서비스 모니터, 서버 풀, 애플리케이션 프로파일, 애플리케이션 규칙 및 가상 서버를 추가하여 로드 밸런서를 설정합니다. 가상 서버를 추가할 때 벤더 제공 템플릿을 선택합니다. 자세한 내용은 [로드 밸런싱 설정](#) 항목을 참조하십시오.

결과

특정 Edge의 트래픽은 타사 벤더의 관리 콘솔에 의해 로드 밸런싱됩니다.

타사 통합 제거

이 예에서는 NSX에서 타사 통합 솔루션을 제거하는 방법을 설명합니다.

타사 소프트웨어 솔루션을 제거할 때는 올바른 제거 순서가 있습니다. 이 순서를 따르지 않고, 특히 NSX Manager에서 타사 솔루션이 등록 해제되기 전에 해당 솔루션을 제거하거나 삭제하면 제거 작업이 실패합니다. 이 문제 해결 방법에 대한 자세한 내용은 <https://kb.vmware.com/kb/2126678>을 참조하십시오.

절차

- 1 vSphere Web Client에서 **Networking & Security > Service Composer**로 이동한 다음 트래픽을 타사 솔루션으로 리디렉션하는 규칙(또는 보안 정책)을 삭제합니다.
- 2 서비스 정의(Service Definitions)로 이동한 다음 타사 솔루션의 이름을 두 번 클릭합니다.
- 3 관련 개체(Related Objects)를 클릭하고 관련 개체를 삭제합니다.
- 4 설치 > 서비스 배포(Installation > Service Deployments)로 이동한 다음 타사 배포를 삭제합니다.
이 작업을 수행하면 연결된 VM이 제거됩니다.
- 5 서비스 정의(Service Definitions)로 돌아간 다음 정의의 하위 구성 요소를 모두 삭제합니다.
- 6 서비스 인스턴스에서 서비스 프로파일을 삭제합니다.
- 7 서비스 인스턴스를 삭제합니다.
- 8 서비스 정의를 삭제합니다.

결과

타사 통합 솔루션이 NSX에서 제거됩니다.

다음에 수행할 작업

구성 설정을 기록한 다음 NSX를 타사 솔루션에서 제거합니다. 예를 들어 다른 개체를 참조하는 규칙을 삭제한 다음 해당 개체를 삭제해야 할 수 있습니다.

많은 조직에서 네트워킹 및 보안 작업은 다른 팀 또는 구성원이 처리합니다. 이러한 조직에는 특정 작업을 특정 사용자에게 제한하는 방법이 필요합니다. 이 항목에서는 이와 같은 액세스 제어를 구성하기 위해 NSX에서 제공하는 옵션을 설명합니다.

NSX는 Active Directory, NIS, LDAP 등의 다른 ID 서비스에서 사용자를 인증할 수 있도록 SSO(Single Sign On)도 지원합니다.

vSphere Web Client의 사용자 관리 작업은 NSX 구성 요소의 CLI에서 수행하는 사용자 관리 작업과는 별개입니다.

본 장은 다음 항목을 포함합니다.

- NSX 사용자 및 기능별 사용 권한
- Single Sign On 구성
- 사용자 권한 관리
- 기본 사용자 계정 관리
- vCenter 사용자에게 역할 할당
- CLI를 사용하여 웹 인터페이스 액세스 권한이 있는 사용자 생성
- 사용자 계정 편집
- 사용자 역할 변경
- 사용자 계정 사용 또는 사용 안 함
- 사용자 계정 삭제

NSX 사용자 및 기능별 사용 권한

NSX를 배포하고 관리하려면 특정 vCenter 사용 권한이 필요합니다. NSX는 다양한 사용자 및 역할에 대한 광범위한 읽기 및 쓰기/쓰기 사용 권한을 제공합니다.

역할 및 사용 권한을 포함하는 기능 목록

기능	설명	역할			
		감사자	보안 관리자	NSX 관리자	엔터프라이즈 관리자
관리자 (Administrator)					
구성	NSX로 vCenter 및 SSO 구성	R	R	R, W	R, W
업데이트		액세스 권한 없음	액세스 권한 없음	R, W	R, W
시스템 이벤트	시스템 이벤트	R	R, W	R, W	R, W
감사 로그	감사 로그	R	R	R	R
URM(사용자 계정 관리) (User Account Management (URM))					
사용자 계정 관리	사용자 관리	액세스 권한 없음	액세스 권한 없음	R	R, W
개체 액세스 제어		액세스 권한 없음	액세스 권한 없음	R	R
기능 액세스 제어		액세스 권한 없음	액세스 권한 없음	R	R
Edge					
시스템	시스템은 일반 시스템 매개 변수를 나타냄	R	R	R, W	R, W
장치	NSX Edge의 다양한 폼 팩터(소형/대형/초대형/4배 대형)	R	R	R, W	R, W
고가용성		R	R	R, W	R, W
vNic	NSX Edge의 인터페이스 구성	R	R, W	R, W	R, W
DNS		R	R, W	R	R, W
SSH	NSX Edge의 SSH 구성	R	R, W	R, W	R, W
자동 연결		R	R, W	R	R, W
통계		R	R	R	R, W
NAT	NSX Edge의 NAT 구성	R	R, W	R	R, W
DHCP		R	R, W	R	R, W
로드 밸런싱		R	R, W	R	R, W
VPN		R	R, W	R	R, W
Syslog	NSX Edge의 Syslog 구성	R	R, W	R, W	R, W
지원		액세스 권한 없음	R, W	R, W	R, W
라우팅	NSX Edge의 모든 라우팅 정적 및 동적 라우팅(BGP/OSPF)	R	R, W	R	R, W
방화벽	NSX Edge의 방화벽 구성	R	R, W	R	R, W

기능	설명	역할			
		감사자	보안 관리자	NSX 관리자	엔터프라이즈 관리자
브리징		R	R, W	R	R, W
인증서		R	R, W	R	R, W
시스템 제어	시스템 제어는 최대 제한, IP 전달, 네트워킹 및 시스템 설정과 같은 시스템 커널 매개 변수를 나타냅니다. 예: ysctl.net.ipv4.conf.vNic_1.rp_filter sysctl.net.netfilter.nf_conntrack_tcp_timeout_established	R	R, W	R, W	R, W
분산 방화벽(Distributed Firewall)					
방화벽 구성	계층 3(일반) 및 계층 2(이더넷) 방화벽 규칙	R	R, W	액세스 권한 없음	R, W
흐름	Flow Monitoring은 시스템의 트래픽 흐름을 모니터링하기 위한 기능입니다. 라이브 흐름도 모니터링할 수 있습니다.	R	R, W	액세스 권한 없음	R, W
IPFix 구성	IPFix 사용/사용 안 함 및 수집기 할당	R	R, W	액세스 권한 없음	R, W
강제 동기화	강제 동기화는 설치 > 호스트 준비(Installation > Host Preparation) 페이지에서 전체 동기화를 수행합니다.	R	R	액세스 권한 없음	R, W
DFW 설치(호스트 준비)	클러스터에 VIBS 설치	R	R	R, W	R, W
저장된 구성(초안)	게시할 때마다 기존 DFW 구성이 자동으로 초안으로 저장됩니다.	R	R, W	액세스 권한 없음	R, W
제외 목록	DFW에서 보호하지 않을 VM을 제외 목록에 추가한 후 제거합니다.	R	R, W	액세스 권한 없음	R, W
DFW 기술 지원	호스트에서 DFW 기술 지원 번들 수집(NSX 구성 셀만 해당)	액세스 권한 없음	R, W	액세스 권한 없음	R, W
DFW 세션 타이머	TCP/UDP/기타 프로토콜 연결 시간 초과 구성 설정	R	R, W	액세스 권한 없음	R, W
IP 검색(DHCP/ARP 스누핑)	VMware Tools가 게스트 VM에서 실행되고 있지 않을 때 IP 검색	R	R, W	액세스 권한 없음	R, W
애플리케이션 규칙 관리자	선택한 애플리케이션 집합에 대해 흐름이 수집됩니다. 그런 다음 수집된 흐름에 따라 방화벽 규칙이 생성됩니다.	R	R, W	액세스 권한 없음	R, W
네임스페이스(NameSpace)					

기능	설명	역할			
		감사자	보안 관리자	NSX 관리자	엔터프라이즈 관리자
구성		R	R	R, W	R, W
SpoofGuard					
구성	TOFU 또는 수동 모드에서 SpoofGuard 게시	R	R, W	액세스 권한 없음	R, W
끝점 보안(EPSEC)(Endpoint Security (EPSEC))					
보고서		R	R	R, W	R, W
등록	솔루션 관리[등록, 등록 취소, 등록된 솔루션 쿼리, 활성화]	R	액세스 권한 없음	R, W	R, W
상태 모니터링	VM, SVM의 상태를 NSX Manager로 검색	액세스 권한 없음	R	R	R
정책	보안 정책 관리[생성, 읽기, 업데이트, 삭제]	R	R, W	R, W	R, W
검색 예약		R	액세스 권한 없음	R, W	R, W
라이브러리(Library)					
호스트 준비	클러스터에 대한 호스트 준비 작업	액세스 권한 없음	액세스 권한 없음	R, W	R, W
그룹화	IP 집합, MAC 집합, Security Group, 서비스, 서비스 그룹	R	R, W	R	R, W
태그 표시	보안 태그(예: VM 연결 또는 분리)	R	R, W	R	R, W
설치(Install)					
애플리케이션		액세스 권한 없음	R	R, W	R, W
EPSEC		액세스 권한 없음	R	R, W	R, W
DLP		액세스 권한 없음	R	R, W	R, W
VDN					
NSM 구성	Network Security Manager 구성	R	R	R, W	R, W
프로비저닝		R	R	R, W	R, W
EAM(ESX Agent Manager)(ESX Agent Manager (EAM))					
설치	ESX Agent Manager	액세스 권한 없음	R	R, W	R, W
서비스 삽입(Service Insertion)					
서비스		R	R, W	R, W	R, W

기능	설명	역할			
		감사자	보안 관리자	NSX 관리자	엔터프라이즈 관리자
서비스 프로파일		R	R	R, W	R, W
신뢰 저장소(Trust Store)					
trustentity_management	NSX 인증서 관리	R	R, W	R, W	R, W
IPAM(IP 주소 관리)(IP Address Management (IPAM))					
구성	IP 풀 구성	R	R, W	R, W	R, W
IP 할당	IP 할당 및 릴리스	R	R, W	R, W	R, W
보안 패브릭(Security Fabric)					
배포	서비스 배포(Service Deployment) 페이지를 사용하여 클러스터에 서비스 또는 보안 VM 배포	R	R	R, W	R, W
경보	서비스 배포(Service Deployment) 페이지에서 보안 VM에서 생성된 경보를 관리합니다.	R	R	R, W	R, W
에이전트 상태	주로 파트너 VM에서 사용되는 REST 호출에 대한 에이전트 상태 정보 관리	R	R, W	R, W	R, W
메시징(Messaging)					
메시징	NSX Edge 및 Guest Introspection에서 NSX Manager와 통신하는 데 사용하는 메시징 프레임워크	R	R, W	R, W	R, W
Replicator(보조 NSX Manager를 사용한 다중 vCenter 설정) (Replicator (Multi vCenter setup with secondary NSX Manager))					
구성	NSX Manager에 대한 기본 역할 선택 또는 선택 취소, 보조 NSX Manager 제거	R	R	R, W	R, W
보안 정책(Security Policy)					
구성	보안 정책을 구성하여 생성, 업데이트, 편집 또는 삭제	R	R, W	액세스 권한 없음	R, W
Security Group 바인딩	Security Group을 보안 정책에 연결	R	R, W	액세스 권한 없음	R, W

Single Sign On 구성

SSO를 사용하면 각 구성 요소가 사용자를 개별적으로 인증할 필요 없이 다양한 구성 요소가 보안 토큰 교환 메커니즘을 통해 서로 통신할 수 있어 vSphere와 NSX의 보안이 한층 강화됩니다.

NSX Manager에서 Lookup Service를 구성하고 SSO 관리자 자격 증명을 제공하여 NSX 관리 서비스를 SSO 사용자로 등록할 수 있습니다. SSO(Single Sign On) 서비스를 NSX와 통합하면 vCenter 사용자의 사용자 인증 보안이 강화되며 NSX가 AD, NIS, LDAP 등 다른 ID 서비스의 사용자를 인증할 수 있습니다. SSO를 사용하면 NSX가 REST API 호출을 통해 신뢰할 수 있는 소스의 인증된 SAML(Security Assertion Markup Language) 토큰을 사용하여 인증을 지원합니다. 또한 NSX Manager는 다른 VMware 솔루션에 사용할 인증 SAML 토큰을 획득할 수도 있습니다.

NSX는 SSO 사용자를 위한 그룹 정보를 캐시합니다. 그룹 멤버 자격에 대한 변경 사항이 ID 제공자(예: Active Directory)에서 NSX로 전파되는 데 최대 60분이 걸립니다.

사전 요구 사항

- NSX Manager에서 SSO(Single Sign-On)를 사용하려면 vCenter Server 5.5 이상을 사용하고 vCenter Server에 SSO 인증 서비스가 설치되어 있어야 합니다. 이는 내장된 SSO에 해당하는 요건입니다. 대신 해당 배포 환경에서 외부 중앙 SSO 서버를 사용 중일 수 있습니다.

vSphere에서 제공되는 SSO 서비스에 대한 자세한 내용은 <http://kb.vmware.com/kb/2072435> 및 <http://kb.vmware.com/kb/2113115> 항목을 참조하십시오.

- SSO 서버 시간과 NSX Manager 시간이 동기화되도록 NTP 서버를 지정해야 합니다.

예:

Time Settings [Unconfigure NTP Servers] [Edit]

Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.

NTP Server	192.168.110.10
Timezone	UTC
Date/Time	12/28/2016 21:31:49

절차

- 1 NSX Manager 가상 장치에 로그인합니다.

웹 브라우저에서 <https://<nsx-manager-ip>> 또는 <https://<nsx-manager-hostname>>의 NSX Manager 장치 GUI로 이동하여 NSX Manager 설치 중에 설정한 암호를 사용하여 admin 권한으로 로그인합니다.

- 2 NSX Manager 가상 장치에 로그인합니다.

- 3 홈 페이지에서 **장치 설정 관리(Manage Appliance Settings) > NSX 관리 서비스(NSX Management Service)**를 클릭합니다.

- 4 [Lookup Service URL] 섹션에서 **편집(Edit)**을 클릭합니다.

- 5 Lookup Service가 있는 호스트의 이름 또는 IP 주소를 입력합니다.

6 포트 번호를 입력합니다.

vSphere 6.0을 사용하는 경우 포트 443을 입력합니다. vSphere 5.5의 경우 포트 번호 7444를 사용합니다.

지정된 호스트 및 포트를 기준으로 Lookup Service URL이 표시됩니다.

7 SSO 관리자 사용자 이름 및 암호를 입력하고 **확인(OK)**을 클릭합니다.



SSO 서버의 인증서 지문이 표시됩니다.

8 인증서 지문이 SSO 서버의 인증서와 일치하는지 확인합니다.

CA 서버에 CA 서명된 인증서를 설치한 경우 CA 서명된 인증서의 지문이 제공됩니다. 그렇지 않은 경우 자체 서명된 인증서가 제공됩니다.

9 Lookup Service 상태가 **연결됨(Connected)**인지 확인합니다.

예:

Lookup Service URL:	https://psc-01a.corp.local:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Status:	 Connected 

다음에 수행할 작업

"NSX 관리 가이드"에서 vCenter 사용자에게 역할 할당을 참조하십시오.

사용자 권한 관리

사용자 역할은 지정된 리소스에 대해 사용자가 수행할 수 있는 작업을 정의합니다. 사용자 역할은 지정된 리소스에 대해 사용자에게 권한을 부여할 작업을 결정하여 사용자가 해당 작업을 완료하는 데 필요한 기능에만 액세스하도록 제한합니다. 따라서 특정 리소스에 대한 도메인 제어가 가능하며, 권한에 제한이 없는 경우에는 시스템 전체 제어도 가능합니다.

다음과 같은 규칙이 적용됩니다.

- 각 사용자에게는 한 가지 역할만 부여될 수 있습니다.
- 사용자에게 역할을 추가하거나 사용자에게 할당된 역할을 제거할 수 없습니다. 하지만 사용자에게 할당된 역할을 변경할 수는 있습니다.

표 20-1. NSX Manager 사용자 역할

오른쪽	사용 권한
엔터프라이즈 관리자	NSX 작업 및 보안
NSX 관리자	NSX 작업만(예: 가상 장치 설치, 포트 그룹 구성)
보안 관리자	NSX 보안만: 예) 분산 방화벽 규칙을 정의하고 NAT 및 로드 밸런서 서비스를 구성합니다.
감사자	읽기 전용

엔터프라이즈 관리자 및 NSX 관리자 역할은 vCenter 사용자에게만 할당할 수 있습니다.

기본 사용자 계정 관리

NSX Manager 사용자 인터페이스에는 모든 리소스에 대한 액세스 권한을 보유한 사용자 계정이 포함되어 있습니다. 이 사용자의 권한을 편집하거나 이 사용자를 삭제할 수는 없습니다. 기본 사용자 이름은 **admin** 이고 기본 암호는 **default** 또는 NSX Manager를 설치할 때 지정한 암호입니다.

NSX Manager 장치의 **admin** 사용자는 CLI 명령을 통해서만 관리할 수 있습니다.

vCenter 사용자에게 역할 할당

SSO 사용자에게 역할을 할당하는 경우 vCenter는 SSO 서버에 구성된 ID 서비스를 통해 해당 사용자를 인증합니다. SSO 서버가 구성되어 있지 않거나 사용할 수 없는 경우에는 vCenter 구성에 따라 로컬로 인증되거나 Active Directory로 인증됩니다.

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 이름 열에서 NSX Manager를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
- 4 **사용자(Users)**를 클릭합니다.
- 5 **추가(Add)**를 클릭합니다.
역할 할당 창이 열립니다.
- 6 **vCenter 사용자 지정(Specify a vCenter user)** 또는 **vCenter 그룹 지정(Specify a vCenter group)**을 클릭합니다.
- 7 사용자의 vCenter **사용자(User)** 또는 **그룹(Group)** 이름을 입력합니다.
자세한 내용은 아래 예제를 참조하십시오.
도메인 이름: corp.vmware.com
별칭: corp
그룹 이름: group1@corp.vmware.com
사용자 이름: user1@corp.vmware.com
NSX Manager에서 그룹에 역할이 할당되면 해당 그룹의 사용자는 NSX Manager 사용자 인터페이스에 로그인될 수 있습니다.
사용자에게 역할을 할당할 경우 사용자 별칭을 입력하십시오. 예를 들어, user1@corp입니다.
- 8 **다음(Next)**을 클릭합니다.
- 9 사용자의 역할을 선택하고 **다음(Next)**을 클릭합니다. 사용 가능한 역할에 대한 자세한 내용은 [사용자 권한 관리](#) 항목을 참조하십시오.

10 완료(Finish)를 클릭합니다.

사용자 계정이 사용자 테이블에 나타납니다.

그룹 기반 역할 할당 이해

조직에서는 사용자를 적절히 관리하기 위해 사용자 그룹을 생성합니다. SSO와 통합된 NSX Manager는 사용자가 속한 그룹의 세부 정보를 가져올 수 있습니다. 같은 그룹에 속한 개별 사용자에게 역할을 할당하는 대신 NSX Manager가 그룹에 역할을 할당할 수 있습니다. 다음 시나리오에서는 NSX Manager가 역할을 할당하는 방법을 보여 줍니다.

예제: 역할 기반 액세스 제어(RBAC) 시나리오

이 시나리오에서는 다음 환경에서 IT 네트워크 엔지니어(Sally Moore)가 NSX 구성 요소에 액세스합니다.

AD 도메인: corp.local, vCenter 그룹: neteng@corp.local, 사용자 이름: smoore@corp.local

사전 요구 사항: vCenter Server가 NSX Manager에 등록되어 있고 SSO가 구성되어 있어야 합니다. SSO는 그룹에만 필요합니다.

1 Sally에 역할을 할당합니다.

- a vSphere Web Client에 로그인합니다.
- b **Networking & Security**를 클릭하고 **NSX Manager(NSX Managers)**를 클릭합니다.
- c 이름 열에서 NSX Manager를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
- d **사용자(Users)** 및 **추가(Add)**를 차례로 클릭합니다.
역할 할당 창이 열립니다.
- e **vCenter 그룹 지정(Specify a vCenter group)**을 클릭하고 **그룹(Group)**에 neteng@corp.local을 입력합니다.
- f **다음(Next)**을 클릭합니다.
- g [역할 선택]에서 **NSX 관리자(NSX Administrator)**를 클릭한 후 **다음(Next)**을 클릭합니다.

2 Sally에게 데이터센터에 대한 권한을 부여합니다.

- a [홈] 아이콘을 클릭한 다음 **vCenter 홈(vCenter Home)** > **데이터센터(Datacenters)**를 클릭합니다.
- b 데이터센터를 선택하고 **작업(Actions)** > **모든 vCenter 작업(All vCenter Actions)** > **사용 권한 추가(Add Permission)**를 클릭합니다.
- c **추가(Add)**를 클릭하고 CORP 도메인을 선택합니다.
- d **사용자 및 그룹(Users and Groups)**에서 **그룹 먼저 표시(Show Groups First)**를 선택합니다.
- e NetEng를 선택하고 **확인(OK)**을 클릭합니다.
- f **할당된 역할(Assigned Role)**에서 **읽기 전용(Read-only)**을 선택하고 하위 항목으로 전파(**Propagate to children**)를 선택 해제한 다음, **확인(OK)**을 클릭합니다.

3 vSphere Web Client에서 로그아웃한 다음 `smoore@corp.local`로 다시 로그인합니다.

Sally는 NSX 작업만 수행할 수 있습니다. 예를 들어, 가상 장치 설치, 논리적 스위치 생성 등의 작업을 수행할 수 있습니다.

예제: 사용자 그룹 멤버 자격을 통한 권한 상속 시나리오

그룹 옵션	값
이름	G1
할당된 역할	감사자(읽기 전용)
리소스	글로벌 루트

사용자 옵션	값
이름	John
소속 그룹	G1
할당된 역할	없음

John은 감사자 역할이 할당된 G1 그룹에 속해 있습니다. John은 이 그룹의 역할 및 리소스 권한을 상속합니다.

예제: 여러 그룹에 속한 사용자 멤버 시나리오

그룹 옵션	값
이름	G1
할당된 역할	감사자(읽기 전용)
리소스	글로벌 루트

그룹 옵션	값
이름	G2
할당된 역할	보안 관리자(읽기 및 쓰기)
리소스	Datacenter1

사용자 옵션	값
이름	Joseph
소속 그룹	G1, G2
할당된 역할	없음

Joseph는 G1 및 G2 그룹에 속하며, 감사자 및 보안 관리자 역할이 조합된 권한을 상속합니다. 예를 들어 John의 권한은 다음과 같습니다.

- Datacenter1에 대한 읽기, 쓰기(보안 관리자 역할) 권한
- 글로벌 루트에 대한 읽기 전용(감사자 역할) 권한

예제: 여러 역할이 할당된 사용자 멤버 시나리오

그룹 옵션	값
이름	G1
할당된 역할	엔터프라이즈 관리자
리소스	글로벌 루트

사용자 옵션	값
이름	Bob
소속 그룹	G1
할당된 역할	보안 관리자(읽기 및 쓰기)
리소스	Datacenter1

Bob은 보안 관리자 역할을 할당받았으므로 그룹 역할 권한을 상속하지 않습니다. Bob의 권한은 다음과 같습니다.

- Datacenter1 및 해당 하위 리소스에 대한 읽기, 쓰기(보안 관리자 역할) 권한
- Datacenter1에 대한 엔터프라이즈 관리자 역할

CLI를 사용하여 웹 인터페이스 액세스 권한이 있는 사용자 생성

CLI를 사용하여 웹 인터페이스 액세스 권한이 있는 NSX 사용자를 생성할 수 있습니다. 이 사용자 계정을 사용하여 다른 플러그인을 액세스하고 작동하거나 감사 용도로 사용할 수 있습니다.

절차

- 1 CLI 사용자 계정을 생성합니다. 각 NSX 가상 장치에 대한 CLI 사용자 계정을 생성할 수 있습니다. CLI 사용자 계정을 생성하려면 다음 단계를 수행하십시오.
 - a vSphere Web Client에 로그인하고 NSX Manager 가상 장치를 선택합니다.
 - b 콘솔(Console) 탭을 클릭하여 CLI 세션을 엽니다.
 - c NSX Manager를 설치할 때 지정한 관리자 계정 및 암호를 사용하여 CLI 세션에 로그인합니다. 예를 들면 다음과 같습니다.

```
nsx-mgr> enable
Password:
nsx-mgr>
```

- d 다음과 같이 enable 명령을 사용하여 기본 모드에서 권한 모드로 전환합니다.

```
nsx-mgr> enable
Password:
nsx-mgr#
```

- e 다음과 같이 `configure terminal` 명령을 사용하여 권한 모드에서 구성 모드로 전환합니다.

```
nsx-mgr# configure terminal
nsx-mgr(config)#
```

- f `user username password (hash | plaintext) password` 명령을 사용하여 CLI 사용자 계정을 추가합니다. 예를 들면 다음과 같습니다.

```
nsx-mgr(config)# user cliuser password plaintext abcd1234
```

참고 대문자 사용자 이름은 허용되지 않습니다.

- g 다음과 같이 구성을 저장합니다.

```
nsx-mgr(config)# write memory
Configuration saved
[OK]
```

- 2 이제 사용자가 NSX Manager 가상 장치에 로그인할 수 있도록 하고 다음과 같이 장치 관리 REST API의 실행을 허용하는 웹 인터페이스 권한을 제공합니다.

- a 다음과 같이 구성 모드인지 확인합니다.

```
nsx-mgr# configure terminal
nsx-mgr(config)#
```

- b `user username privilege web-interface` 명령을 사용하여 생성된 CLI 사용자가 REST API 호출을 실행할 수 있도록 합니다. 예:

```
nsx-mgr(config)# user userName privilege web-interface

nsx-mgr(config)# user cliuser privilege web-interface
```

- 3 (선택 사항) 다음과 같이 실행 중인 구성을 확인할 수 있습니다.

```
nsx-mgr# show running-config
Building configuration...

Current configuration:
!
user cliuser
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr-01a
!
interface mgmt
ip address 192.168.110.15/24
```

```
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager
```

- 4 CLI 세션에서 종료합니다.

```
nsx-mgr#(config)# exit
nsx-mgr# exit
```

생성된 사용자가 **Networking & Security > NSX Managers “NSX Manager 선택”** (**“Select your NSX Manager”**) > **관리(Manage)** > **사용자(Users)** 탭에 표시되지 않습니다. 또한 사용자에게 할당된 역할도 없습니다.

- 5 REST API를 사용하여 사용자에게 필요한 역할을 할당합니다. 다음과 같이 **auditor**(감사자), **security_admin**(보안 관리자) 또는 **super_user**(시스템 관리자) 역할을 할당할 수 있습니다.

```
POST - https://<NSX-IP>/api/2.0/services/usermgmt/role/<username>?isCli=true
<accessControlEntry>
<role>auditor</role> # Enter the required role #
<resource>
<resourceId>globalroot-0</resourceId>
</resource>
</accessControlEntry>
```

결과

NSX CLI 사용자는 웹 인터페이스 액세스를 사용하여 생성됩니다.

다음에 수행할 작업

사용자를 생성하는 동안 제공된 자격 증명을 사용하여 vSphere Web Client에 로그인할 수 있습니다.

CLI에 대한 자세한 내용은 "NSX 명령줄 인터페이스 참조"를 참조하십시오.

API에 대한 자세한 내용은 "NSX API 가이드"를 참조하십시오.

사용자 계정 편집

사용자 계정을 편집하여 역할 또는 범위를 변경할 수 있습니다. **admin** 계정은 편집할 수 없습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열에서 NSX Manager를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
- 4 **사용자(Users)**를 클릭합니다.
- 5 편집할 사용자를 선택합니다.

- 6 **편집(Edit)**을 클릭합니다.
- 7 필요한 내용을 변경합니다.
- 8 **완료(Finish)**를 클릭하여 변경 내용을 저장합니다.

사용자 역할 변경

admin 사용자를 제외한 모든 사용자에게 할당된 역할을 변경할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열에서 **NSX Manager**를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
- 4 **사용자(Users)**를 클릭합니다.
- 5 역할을 변경할 사용자를 선택합니다.
- 6 **역할 변경(Change Role)**을 클릭합니다.
- 7 필요한 내용을 변경합니다.
- 8 **완료(Finish)**를 클릭하여 변경 내용을 저장합니다.

사용자 계정 사용 또는 사용 안 함

사용자 계정을 사용하지 않도록 설정하면 해당 사용자가 **NSX Manager**에 로그인하는 것을 차단할 수 있습니다. **admin** 사용자 또는 현재 **NSX Manager**에 로그인되어 있는 사용자는 사용하지 않도록 설정할 수 없습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열에서 **NSX Manager**를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
- 4 **사용자(Users)**를 클릭합니다.
- 5 사용자 계정을 선택합니다.
- 6 **사용(Enable)** 또는 **사용 안 함(Disable)** 아이콘을 클릭합니다.

사용자 계정 삭제

생성한 사용자 계정을 삭제할 수 있습니다. 단, **admin** 계정은 삭제할 수 없습니다. 삭제된 사용자에 대한 감사 레코드는 데이터베이스에 유지되며 감사 로그 보고서에서 참조할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열에서 **NSX Manager**를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
- 4 **사용자(Users)**를 클릭합니다.
- 5 사용자 계정을 선택합니다.
- 6 **삭제>Delete**를 클릭합니다.
- 7 **확인(OK)**을 클릭하여 삭제를 확인합니다.

vCenter 사용자 계정을 삭제하는 경우 **NSX Manager**에 대한 역할 할당만 삭제되며, vCenter의 사용자 계정은 삭제되지 않습니다.

네트워크 및 보안 개체

21

이 섹션에서는 사용자 지정 네트워크 및 보안 컨테이너에 대해 설명합니다. 분산 방화벽 및 **Service Composer**에서 이 컨테이너를 사용할 수 있습니다. 크로스 vCenter NSX 환경에서 범용 분산 방화벽 규칙에서 사용할 범용 네트워크 및 보안 컨테이너를 생성할 수 있습니다. 범용 네트워크 및 보안 개체는 **Service Composer**에서 사용할 수 없습니다.

참고 범용 범위로 그룹을 생성할 때 중복된 이름이 허용됩니다. 다음 그룹을 생성하는 동안 **이 개체를 범용 동기화에 대해 표시(Mark this object for Universal Synchronization)** 옵션을 선택하여 중복된 이름을 제공할 수 있습니다.

- IP 주소 그룹
- MAC 주소 그룹
- 보안 그룹
- 서비스 및 서비스 그룹

본 장은 다음 항목을 포함합니다.

- IP 주소 그룹 사용
- MAC 주소 그룹 사용
- IP 풀 사용
- 보안 그룹 사용
- 서비스 및 서비스 그룹 사용

IP 주소 그룹 사용

IP 주소 그룹 생성

IP 주소 그룹을 생성한 후 방화벽 규칙에 이 그룹을 소스 또는 대상으로 추가할 수 있습니다. 이러한 규칙은 물리적 시스템을 가상 시스템으로부터 보호하거나, 가상 시스템을 물리적 시스템으로부터 보호하는 데 도움이 될 수 있습니다.

사전 요구 사항

VMware Tools가 각 VM에 설치되어 있거나, IP 주소 대신 그룹 개체를 사용할 때 사용하도록 설정된 IP 검색 방법(DHCP 스누핑이나 ARP 스누핑 또는 둘 다)이 적용되어 있어야 합니다. 자세한 내용은 [가상 시스템에 대한 IP 검색](#)를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 IP 주소 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **IP 집합(IP Sets)**을 클릭합니다.
- 5 **추가(+)** 아이콘을 클릭합니다.
- 6 주소 그룹의 이름을 입력합니다.
- 7 (선택 사항) 주소 그룹에 대한 설명을 입력합니다.
- 8 그룹에 포함할 IP 주소 또는 IP 주소 범위를 입력합니다.


경고 IP 집합에 IPv6 주소 범위를 입력하는 동안 주소 범위를 /64로 구분했는지 확인합니다. 그렇지 않으면 방화벽 규칙을 게시하지 못합니다.

- 9 (선택 사항) 기본 범위에서 볼 수 있도록 **상속 사용**을 선택합니다.
- 10 (선택 사항) 이 개체를 **범용 동기화하도록 표시**를 선택하여 범용 IP 주소 그룹을 생성합니다.
- 11 **확인(OK)**을 클릭합니다.

IP 주소 그룹 편집

사전 요구 사항

절차


- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 IP 주소 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체** 탭을 클릭하고 **IP 집합**을 클릭합니다.
- 5 편집할 그룹을 선택한 다음 **편집(Edit)**() 아이콘을 클릭합니다.

6 [IP 집합 편집] 대화상자에서 필요한 내용을 변경합니다.

7 **확인(OK)**을 클릭합니다.

IP 주소 그룹 삭제

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 IP 주소 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **IP 집합(IP Sets)**을 클릭합니다.
- 5 삭제할 그룹을 선택한 다음 **삭제(Delete)**() 아이콘을 클릭합니다.

MAC 주소 그룹 사용

MAC 주소 그룹 생성

MAC 주소 범위로 구성된 MAC 주소 그룹을 생성한 후 분산 방화벽 규칙에서 이 그룹을 소스 또는 대상으로 추가할 수 있습니다. 이러한 규칙은 물리적 시스템을 가상 시스템으로부터 보호하거나, 가상 시스템을 물리적 시스템으로부터 보호하는 데 도움이 될 수 있습니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 MAC 주소 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **MAC 집합(MAC Sets)**을 클릭합니다.
- 5 **추가(+)** 아이콘을 클릭합니다.
- 6 주소 그룹의 이름을 입력합니다.
- 7 (선택 사항) 주소 그룹에 대한 설명을 입력합니다.
- 8 그룹에 포함할 MAC 주소를 입력합니다.
- 9 (선택 사항) 기본 범위에서 볼 수 있도록 **상속 사용**을 선택합니다.
- 10 (선택 사항) 이 개체를 범용 동기화하도록 표시를 선택하여 범용 MAC 주소 그룹을 생성합니다.

11 **확인(OK)**을 클릭합니다.


MAC 주소 그룹 편집

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 MAC 주소 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **MAC 집합(MAC Sets)**을 클릭합니다.
- 5 편집할 그룹을 선택한 다음 **편집(Edit)**() 아이콘을 클릭합니다.
- 6 MAC 집합 편집 대화상자에서 필요한 내용을 변경합니다.
- 7 **확인(OK)**을 클릭합니다.

MAC 주소 그룹 삭제

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 MAC 주소 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **MAC 집합(MAC Sets)**을 클릭합니다.
- 5 삭제할 그룹을 선택한 다음 **삭제(Delete)**() 아이콘을 클릭합니다.

IP 풀 사용

IP 풀을 생성하여 IP 주소 범위를 지정할 수 있습니다.

IP 풀 생성

절차

- 1 vSphere Web Client에 로그인합니다.

- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭한 후 **IP 풀(IP Pool)**을 클릭합니다.
- 5 **새 IP 풀 추가(Add New IP Pool)** 아이콘을 클릭합니다.
- 6 IP 풀의 이름을 입력하고 기본 게이트웨이 및 접두사 길이를 입력합니다.
- 7 (선택 사항) 기본 및 보조 DNS와 DNS 접미사를 입력합니다.
- 8 풀에 포함할 IP 주소 범위를 입력하고 **확인(OK)**을 클릭합니다.

IP 풀 편집

IP 풀은 편집할 수 있고, CIDR 및 게이트웨이는 편집할 수 없습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭한 후 **IP 풀(IP Pools)**을 클릭합니다.
- 5 IP 풀을 선택하고 **편집(Edit)** 아이콘을 클릭합니다.
- 6 필요한 내용을 변경하고 **확인(OK)**을 클릭합니다.

IP 풀 삭제

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭한 후 **IP 풀(IP Pool)**을 클릭합니다.
- 5 삭제할 IP 풀을 선택한 다음 **삭제>Delete)** 아이콘을 클릭합니다.

보안 그룹 사용

보안 그룹은 vSphere 인벤토리에 있는 자산 또는 그룹 개체의 모음입니다.

보안 그룹은 논리적 스위치, vNIC, IPset 및 VM(가상 시스템)을 포함하는 여러 개체 유형을 포함할 수 있는 컨테이너입니다. 보안 그룹에는 보안 태그, VM 이름 또는 논리적 스위치 이름에 따라 동적 멤버 자격 조건을 지정할 수 있습니다. 예를 들어 보안 태그 "web"을 갖는 모든 VM은 웹 서버를 대상으로 하는 특정 보안 그룹에 자동으로 추가됩니다. 보안 그룹을 생성한 후에는 해당 그룹에 보안 정책이 적용됩니다.

크로스 vCenter NSX 환경에서는 기본 NSX Manager에서 범용 보안 그룹이 정의되고 보조 NSX Manager와 범용 동기화되도록 표시됩니다. 범용 보안 그룹은 활성 대기 배포 시나리오에서 사용하도록 표시된 경우에만 동적 멤버 자격 조건이 정의될 수 있습니다.

활성 대기 배포 시나리오가 있는 크로스 vCenter NSX 환경에서는 SRM은 활성 사이트의 보호된 VM당 하나의 위치 지정자 VM을 복구 사이트에 생성합니다. 위치 지정자 VM은 활성 상태가 아니므로 대기 모드를 유지합니다. 보호된 VM이 중단되면 복구 사이트에 있는 위치 지정자 VM의 전원이 켜지고 보호된 VM의 작업을 인계받습니다. 사용자는 활성 사이트에서 범용 보안 태그를 포함하는 범용 보안 그룹으로 분산 방화벽 규칙을 생성합니다. NSX Manager는 위치 지정자 VM에서 범용 보안 태그를 포함하는 범용 보안 그룹으로 분산 방화벽 규칙을 복제하고, 위치 지정자 VM의 전원이 켜지면 범용 보안 그룹 및 범용 보안 태그를 갖는 복제된 방화벽 규칙이 올바르게 적용됩니다.

참고

- 6.3 이전에 생성된 범용 보안 그룹은 활성 대기 배포에서 사용하기 위해 편집할 수 없습니다.

보안 그룹 생성

보안 그룹은 NSX Manager 수준에서 생성할 수 있습니다.

범용 보안 그룹은 두 가지 유형의 배포에서 사용됩니다. 하나는 활성 활성 크로스 vCenter NSX 환경이고, 다른 하나는 한 사이트가 지정된 시간에 라이브 상태이고 나머지는 대기 상태를 유지하는 활성 대기 크로스 vCenter NSX 환경입니다.

- 활성 활성 환경의 범용 보안 그룹은 포함된 개체로 보안 그룹, IP 집합, MAC 집합만 포함할 수 있습니다. 동적 멤버 자격 또는 제외된 개체는 구성할 수 없습니다.
- 활성 대기 환경의 범용 보안 그룹은 포함된 개체로 보안 그룹, IP 집합, MAC 집합, 범용 보안 태그를 포함할 수 있습니다. 또한 VM 이름만 사용해서 동적 멤버 자격을 구성할 수도 있습니다. 제외된 개체는 구성할 수 없습니다.

참고 6.3 이전에 생성된 범용 보안 그룹은 활성 대기 배포에서 사용하기 위해 편집할 수 없습니다.

사전 요구 사항

Active Directory 그룹 개체를 기반으로 보안 그룹을 생성할 경우 NSX Manager에 하나 이상의 도메인이 등록되어 있는지 확인하십시오. NSX Manager는 등록된 각 도메인에서 그룹 및 사용자 정보와 서로 간의 관계를 가져옵니다. NSX Manager에 Windows 도메인 등록을 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.

- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 보안 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **보안 그룹(Security Group)**을 클릭한 다음 **보안 그룹 추가(Add Security Group)** 아이콘을 클릭합니다.
- 5 보안 그룹의 이름과 설명(선택 사항)을 입력합니다.
- 6 (선택 사항) 범용 보안 그룹을 생성하는 경우 이 개체를 범용 동기화에 대해 표시(Mark this object for universal synchronization)를 선택합니다.
- 7 (선택 사항) 활성 대기 배포에서 사용할 범용 보안 그룹을 생성하는 경우 이 개체를 범용 동기화에 대해 표시(Mark this object for universal synchronization) 및 활성 대기 배포에 사용합니다(Use for active standby deployments)를 둘 다 선택합니다. 활성 대기 배포의 범용 보안 그룹에 대한 동적 멤버 자격은 가상 시스템 이름을 기준으로 합니다.
- 8 **다음(Next)**을 클릭합니다.
- 9 생성할 보안 그룹에 추가하려면 개체가 충족해야 하는 조건을 [동적 멤버 자격] 페이지에서 정의합니다. 이렇게 하면 검색 기준과 일치하기 위해 지원되는 여러 매개 변수를 사용하여 필터 조건을 정의함으로써 가상 시스템을 포함할 수 있습니다.

참고 범용 보안 그룹을 생성할 경우 활성 활성 배포에서 동적 멤버 자격 정의(Define dynamic membership) 단계를 사용할 수 없습니다. 활성 대기 배포에서는 가상 시스템 이름에 따라서만 사용할 수 있습니다.

예를 들어 특정 보안 태그(예: AntiVirus.virusFound)로 태그 지정된 가상 시스템을 모두 보안 그룹에 추가하는 조건을 포함할 수 있습니다. 보안 태그는 대/소문자를 구분합니다.

또는 이름 W2008을 포함하는 모든 가상 시스템과 논리적 스위치 global_wire에 있는 가상 시스템을 보안 그룹에 추가할 수 있습니다.

New Security Group

- ✓ 1 Name and description
- ✓ 2 Define dynamic membership
- ✓ 3 Select objects to include
- ✓ 4 Select objects to exclude
- ✓ 5 Ready to complete

Define dynamic membership

Specify dynamic membership criteria that objects must meet to be part of this security group.

Members matching **All** of the criteria below

Computer Name	Contains	W2008	✗
Entity	Belongs to	global_wire	✗

- 10 **다음(Next)**을 클릭합니다.

- 11** [포함할 개체 선택] 페이지에서 추가할 리소스에 대한 탭을 선택하고 보안 그룹에 추가할 하나 이상의 리소스를 선택합니다. 다음 개체를 보안 그룹에 포함할 수 있습니다.

표 21-1. 보안 그룹 및 범용 보안 그룹에 포함될 수 있는 개체.

보안 그룹	범용 보안 그룹
<ul style="list-style-type: none"> ■ 생성할 보안 그룹 안에 중첩될 다른 보안 그룹 ■ 클러스터 ■ 논리적 스위치 ■ 네트워크 ■ 가상 장치 ■ 데이터센터 ■ IP 집합 ■ 디렉토리 그룹 	<ul style="list-style-type: none"> ■ 생성할 범용 보안 그룹 안에 중첩될 다른 범용 보안 그룹. ■ 범용 IP 집합 ■ 범용 MAC 집합 ■ 범용 보안 태그(활성 대기 배포만 해당)
<p>참고 NSX 보안 그룹에 대한 Active Directory 구성은 vSphere SSO에 대한 AD 구성과 다릅니다. NSX AD 그룹 구성은 게스트 가상 시스템에 액세스하는 최종 사용자를 위한 것이며 vSphere SSO는 vSphere 및 NSX를 사용하는 관리자를 위한 것입니다. 이러한 디렉토리 그룹을 사용하려면 Active Directory와 동기화해야 합니다. 장 11 ID 방화벽 개요를 참조하십시오.</p>	
<ul style="list-style-type: none"> ■ MAC 집합 ■ 보안 태그 ■ vNIC ■ 가상 시스템 ■ 리소스 풀 ■ 분산 가상 포트 그룹 	

여기에서 선택하는 개체는 [단계 8단계](#)의 조건 충족 여부에 상관없이 항상 보안 그룹에 포함됩니다.

보안 그룹에 리소스를 추가하면 연결된 모든 리소스가 자동으로 추가됩니다. 예를 들어 가상 시스템을 선택하면 연결된 vNIC가 자동으로 보안 그룹에 추가됩니다.

- 12** 다음(Next)을 클릭하고 보안 그룹에서 제외할 개체를 선택합니다.

참고 범용 보안 그룹을 생성할 경우 **제외할 개체 선택** 단계를 사용할 수 없습니다.

여기에서 선택하는 개체는 동적 조건의 충족 여부에 상관없이 항상 보안 그룹에서 제외됩니다.

- 13** 다음(Next)을 클릭합니다.

보안 그룹 요약과 함께 **완료 준비(Ready to Complete)** 창이 나타납니다.

- 14** 완료(Finish)를 클릭합니다.

예

보안 그룹의 멤버 자격은 다음과 같이 결정됩니다.


{포현식 결과(동적 멤버 자격 정의(Define dynamic membership)에서 파생됨) + 포함(포함할 개체 선택(Select objects to include)에 지정됨) - 제외(제외할 개체 선택(Select objects to exclude)에 지정됨)}

이는 포함 항목이 표현식 결과에 먼저 추가됨을 의미합니다. 그런 다음 조합된 결과에서 제외 항목을 뺍니다.

보안 그룹 편집

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 보안 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭한 후 **보안 그룹(Security Group)**을 클릭합니다.

6.3 이전에 생성된 범용 보안 그룹은 활성 대기 배포에서 사용하기 위해 편집할 수 없습니다.
- 5 편집할 그룹을 선택한 다음 **편집(Edit)**() 아이콘을 클릭합니다.
- 6 보안 그룹 편집 대화상자에서 필요한 내용을 변경합니다.
- 7 **확인(OK)**을 클릭합니다.

보안 그룹 삭제

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 보안 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭한 후 **보안 그룹(Security Group)**을 클릭합니다.
- 5 삭제할 그룹을 선택한 다음 **삭제>Delete)**() 아이콘을 클릭합니다.

서비스 및 서비스 그룹 사용

서비스는 프로토콜-포트 조합이며 서비스 그룹은 서비스 또는 다른 서비스 그룹으로 구성된 그룹입니다.

서비스 생성

서비스를 생성한 후 해당 서비스에 대한 규칙을 정의할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 서비스를 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭한 후 **서비스(Service)**를 클릭합니다.
- 5 **추가(+)** 아이콘을 클릭합니다.
- 6 서비스를 식별할 **이름(Name)**을 입력합니다.
- 7 (선택 사항) 서비스에 대한 **설명(Description)**을 입력합니다.
- 8 **프로토콜(Protocol)**을 선택합니다.
 - a 선택한 프로토콜에 따라 대상 포트 같은 추가 정보를 입력하라는 메시지가 표시될 수 있습니다.
- 9 (선택 사항) **기본 범위에서 볼 수 있도록 상속 사용**을 선택합니다.
- 10 (선택 사항) **이 개체를 범용 동기화하도록 표시**를 선택하여 범용 서비스를 선택합니다.
- 11 **확인(OK)**을 클릭합니다.

결과

서비스가 서비스 테이블에 나타납니다.

서비스 그룹 생성

서비스 그룹을 생성한 후 해당 서비스 그룹에 대한 규칙을 정의할 수 있습니다.

절차


- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 서비스 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭한 후 **서비스 그룹(Service Groups)**을 클릭합니다.
- 5 **추가(Add)** 아이콘을 클릭합니다.
- 6 서비스 그룹을 식별할 **이름(Name)**을 입력합니다.
- 7 (선택 사항) 서비스 그룹에 대한 **설명(Description)**을 입력합니다.
- 8 (선택 사항) **이 개체를 범용 동기화하도록 표시**를 선택하여 범용 서비스 그룹을 선택합니다.

- 9 멤버에서 그룹에 추가할 서비스 또는 서비스 그룹을 선택합니다.
- 10 (선택 사항) 기본 범위에서 볼 수 있도록 상속 사용을 선택합니다.
- 11 확인(OK)을 클릭합니다.

서비스 또는 서비스 그룹 편집

서비스 및 서비스 그룹을 편집할 수 있습니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 서비스 또는 서비스 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **서비스(Service)** 또는 **서비스 그룹(Service Groups)**을 클릭합니다.
- 5 사용자 지정 서비스 또는 서비스 그룹을 선택하고 **편집(Edit)**() 아이콘을 클릭합니다.
- 6 필요한 내용을 변경합니다.
- 7 **확인(OK)**을 클릭합니다.

서비스 또는 서비스 그룹 삭제

서비스 또는 서비스 그룹을 삭제할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **관리** 탭을 클릭합니다.
 - ◆ 범용 서비스 또는 서비스 그룹을 관리해야 하는 경우에는 기본 NSX Manager를 선택해야 합니다.
- 4 **그룹 개체(Grouping Objects)** 탭을 클릭하고 **서비스(Service)** 또는 **서비스 그룹(Service Groups)**을 클릭합니다.
- 5 사용자 지정 서비스 또는 서비스 그룹을 선택하고 **삭제(Delete)**() 아이콘을 클릭합니다.
- 6 **예(Yes)**를 클릭합니다.

서비스 또는 서비스 그룹이 삭제됩니다.

본 장은 다음 항목을 포함합니다.

- [NSX 대시보드 사용](#)
- [통신 채널 상태 확인](#)
- [NSX Controller](#)
- [VXLAN 포트 변경](#)
- [고객 환경 향상 프로그램](#)
- [NSX 로그 정보](#)
- [감사 로그](#)
- [시스템 이벤트](#)
- [관리 시스템 설정](#)
- [NSX 백업 및 복원](#)
- [Flow Monitoring](#)
- [애플리케이션 규칙 관리자](#)
- [Activity Monitoring](#)
- [끝점 모니터링 데이터 수집](#)
- [Traceflow](#)

NSX 대시보드 사용

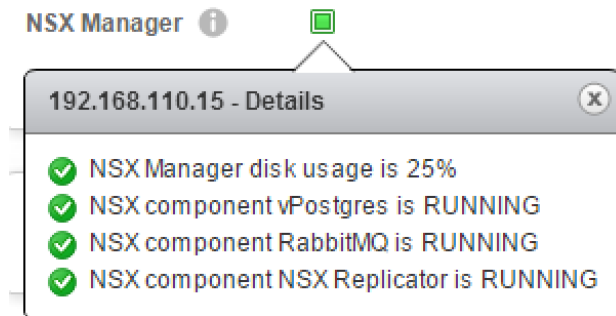
NSX 대시보드는 하나의 중앙 보기에서 NSX 구성 요소의 전반적인 상태에 대한 가시성을 제공합니다. NSX 대시보드는 NSX Manager, 컨트롤러, 논리적 스위치, 호스트 준비, 서비스 배포, 백업뿐만 아니라 Edge 알림과 같은 여러 다른 NSX 구성 요소의 상태를 표시하여 문제 해결을 단순화합니다.

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **대시보드(Dashboard)**를 클릭합니다. [대시보드] 페이지가 표시됩니다.

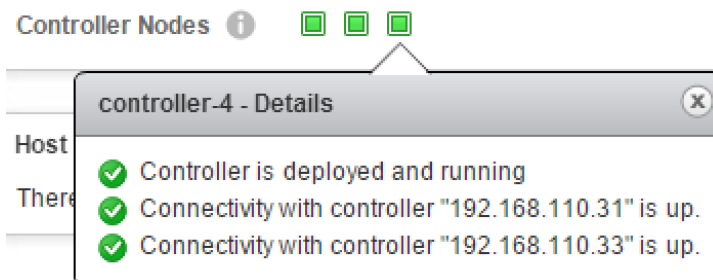
3 크로스 vCenter NSX 환경에서 기본 역할 또는 보조 역할을 갖는 NSX Manager를 선택합니다.

대시보드는 다음 정보를 제공합니다.

- NSX 인프라 — 다음 서비스에 대한 NSX Manager 구성 요소 상태가 모니터링됩니다.
 - 데이터베이스 서비스(vPostgres)
 - 메시지 버스 서비스(RabbitMQ)
 - Replicator 서비스 — 복제 오류도 모니터링합니다(크로스 vCenter NSX가 사용되도록 설정된 경우).
 - NSX Manager 디스크 사용량:
 - 노란색은 디스크 사용량이 80%보다 많음을 나타냅니다.
 - 빨간색은 디스크 사용량이 90%보다 많음을 나타냅니다.



- NSX 인프라—NSX Controller 상태:
 - 컨트롤러 노드 상태(작동/다운/실행 중/배포 중/제거 중/실패/알 수 없음)
 - 컨트롤러 피어 연결 상태가 표시됩니다. 컨트롤러가 다운되어 빨간색으로 표시되면 피어 컨트롤러는 노란색으로 표시됩니다.
 - 컨트롤러 VM 상태(전원 꺼짐/삭제됨)
 - 컨트롤러 디스크 지연 시간 경고



- NSX Manager 백업 상태:
 - 백업 일정
 - 마지막 백업 상태(실패/성공/예약되지 않음과 날짜 및 시간)

- 마지막 백업 시도(날짜 및 시간과 세부 정보)
- 마지막 성공 백업(날짜 및 시간과 세부 정보)

Backup Status ⓘ

Backup schedule:	✓ Daily at 14:50 hrs
Last backup status:	✗ Failed
Last backup attempt:	✗ 10/18/2016 10:53:48 PM
Latest successful backup:	✓ 10/18/2016 8:24:23 AM

Backup Status ⓘ

Backup schedule:	⚠ Not scheduled
Last backup status:	✓ Successful
Last backup attempt:	✓ 10/18/2016 2:19:40 AM

- NSX 인프라 — 다음 서비스에 대한 호스트 상태가 모니터링됩니다.
 - 배포 관련:
 - 설치 실패 상태의 클러스터 수
 - 업그레이드가 필요한 클러스터 수
 - 설치가 진행 중인 클러스터 수
 - 준비되지 않은 클러스터 수
 - 방화벽:
 - 방화벽이 사용되지 않도록 설정된 클러스터 수
 - 방화벽 상태가 노란색/빨간색인 클러스터 수:
 - 노란색은 분산 방화벽이 클러스터에서 사용되지 않도록 설정됨을 나타냅니다.
 - 빨간색은 분산 방화벽이 호스트/클러스터에서 설치될 수 없음을 나타냅니다.
 - VXLAN:
 - VXLAN이 구성되지 않은 클라이언트 수
 - VXLAN 상태가 녹색/노란색/빨간색인 클러스터 수:
 - 녹색은 기능이 성공적으로 구성되었음을 나타냅니다.
 - 노란색은 VXLAN 구성이 진행 중임을 의미합니다.

- 빨간색(오류)은 VTEP 생성이 실패했거나, VTEP에서 IP 주소를 찾을 수 없거나, VTEP에 *LinkLocal* IP 주소가 할당된 경우 등을 나타냅니다.

■ NSX 인프라—서비스 배포 상태

- 배포 실패—실패한 배포에 대한 설치 상태
- 서비스 상태—실패한 모든 서비스에 해당

■ NSX 인프라 —NSX Edge 알림

Edge 알림 대시보드에는 특정 서비스에 대해 활성 상태인 경보를 강조 표시합니다. 아래 나열된 중요 이벤트 목록을 모니터링하고 문제가 해결될 때까지 계속 추적합니다. 경보는 복구 이벤트가 보고되거나, Edge가 강제로 동기화되거나, 재배포되거나, 업그레이드될 때 자동으로 해결됩니다.

- 로드 밸런서(Edge 로드 밸런서 서버 상태):
 - Edge 로드 밸런서 백엔드 서버가 다운됨
 - Edge 로드 밸런서 백엔드 서버 경고 상태
- VPN(IPSec 터널/IPSec 채널 상태):
 - Edge IPSec 채널이 다운됨
 - Edge IPSec 터널이 다운됨
- 장치(Edge VM, Edge Gateway, Edge 파일 시스템, NSX Manager 및 Edge Services Gateway 보고서 상태):
 - Edge Services Gateway에 상태 검사 펄스가 누락됨
 - Edge VM의 전원이 꺼짐
 - Edge VM의 상태 검사 펄스가 누락됨
 - NSX Edge에서 잘못된 상태를 보고함
 - Edge Services Gateway가 잘못된 상태라는 NSX Manager 보고서
 - Edge VM이 VC 인벤토리에 없음

■ HA 분할 브레인 이 감지됨

참고 로드 밸런서 및 VPN 정보가 구성 업데이트 동안 자동으로 지워지지 않습니다. 문제가 해결되면 `alarm-id` 명령을 사용하여 API를 통해 경보를 수동으로 지워야 합니다. 다음은 경보를 지우기 위해 사용할 수 있는 API의 예입니다. 자세한 내용은 "NSX API 가이드"를 참조하십시오.

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{source-Id}
POST https://<<NSX-IP>>/api/2.0/services/alarms?action=resolve

GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

■ NSX Services—방화벽 게시 상태:

- 방화벽 게시 상태가 실패인 호스트 수. 호스트가 게시된 분산 방화벽 구성을 성공적으로 적용하지 못할 경우 상태가 빨간색입니다.

■ NSX Services—논리적 네트워킹 상태:


- 상태가 오류 또는 경고인 논리적 스위치 수
- 지원되는 분산 가상 포트 그룹이 vCenter Server에서 삭제될 경우 플래그 지정

통신 채널 상태 확인

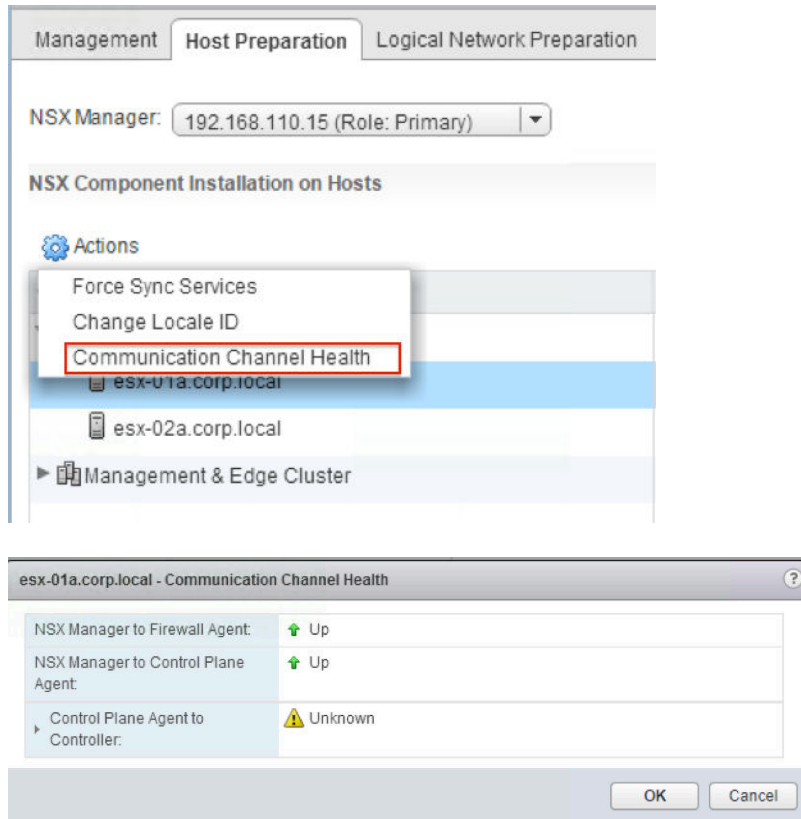
NSX는 NSX Manager와 방화벽 에이전트 사이, NSX Manager와 제어부 에이전트 사이 및 제어부 에이전트와 컨트롤러 사이의 통신 상태를 확인합니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 설치(Installation) > 호스트 준비(Host Preparation)**로 이동합니다.

- 클러스터를 선택하거나 클러스터를 확장하고 호스트를 선택합니다. **작업(Actions)**()을 클릭한 후 **통신 채널 상태(Communication Channel Health)**를 클릭합니다.

통신 채널 상태 정보가 표시됩니다.



NSX Controller

NSX Controller 인스턴스를 관리할 수 있습니다.

컨트롤러를 안전하게 삭제하는 방법을 비롯하여 컨트롤러 클러스터 문제 해결에 대한 자세한 내용은 "NSX 문제 해결 가이드"의 "NSX Controller" 섹션을 참조하십시오.

컨트롤러 암호 변경

보안을 보장하기 위해 NSX 컨트롤러의 암호를 변경할 수 있습니다.

절차

- vSphere Web Client에 로그인합니다.
- Networking & Security**를 클릭하고 **설치(Installation)**를 클릭합니다.
- [관리]에서 암호를 변경할 컨트롤러를 선택합니다.
- 작업(Actions)**을 클릭하고 **컨트롤러 클러스터 암호 변경(Change Controller Cluster Password)**을 클릭합니다.

- 5 새 암호를 입력하고 **확인(OK)**을 클릭합니다.

컨트롤러 암호가 변경됩니다.

NSX Controller용 기술 지원 로그 다운로드

각 NSX Controller 인스턴스에 대한 기술 지원 로그를 다운로드할 수 있습니다. 이러한 제품별 로그에는 분석을 위한 진단 정보가 포함되어 있습니다.

NSX Controller 로그를 수집하려면:

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **설치**를 클릭합니다.
- 3 **관리**에서 로그를 다운로드하려는 컨트롤러를 선택합니다.
- 4 **기술 지원 로그 다운로드**를 클릭합니다.
- 5 **다운로드**를 클릭합니다.

NSX Manager는 NSX Controller 로그 다운로드를 시작하고 잠금을 획득합니다.

참고 한 번에 NSX Controller 로그를 하나씩 다운로드합니다. 첫 번째 로그 다운로드가 완료되면 다른 로그 다운로드를 시작합니다. 여러 컨트롤러에서 동시에 로그를 다운로드하면 오류가 발생할 수 있습니다.

- 6 로그를 다운로드할 준비가 되면 **저장**을 클릭하여 로그를 데스크톱에 다운로드합니다.

로그가 압축되고 .gz 파일 확장명이 붙습니다.

결과

이제 다운로드한 로그를 분석할 수 있습니다.

다음에 수행할 작업

VMware 기술 지원에 대한 진단 정보를 업로드하려면 [기술 지원 문서 2070100](#)을 참조하십시오.

NSX Controller용 Syslog 서버 구성

NSX Controller용 Syslog 서버를 구성할 경우 NSX Manager는 모든 감사 로그 및 시스템 이벤트를 Syslog 서버로 보냅니다. Syslog 데이터는 설치와 구성 작업 중의 문제 해결과 기록된 데이터 검토에 유용합니다. NSX Controller에서 syslog 서버를 구성할 때는 NSX API를 사용하는 방법만 지원됩니다. VMware에서는 syslog의 프로토콜로 UDP를 사용하는 것을 권장합니다.

절차

- 1 NSX Controller에서 syslog를 사용하도록 설정하려면 다음 NSX API를 사용하십시오. 이 API는 컨트롤러 syslog 내보내기를 추가하고 지정된 컨트롤러 노드에서 syslog 내보내기를 구성합니다.

```
Request
POST https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Request Body:
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

- 2 다음 NSX API를 사용하여 컨트롤러 syslog 내보내기를 쿼리하고 지정된 컨트롤러 노드의 구성된 syslog 내보내기에 대한 세부 정보를 검색할 수 있습니다.

```
Request
GET https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Response Body:
<?xml version="1.0" encoding="UTF-8"?>
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

- 3 필요하지 않은 경우 다음 NSX API를 사용하여 지정된 컨트롤러 노드에서 컨트롤러 syslog 내보내기를 삭제할 수 있습니다.

```
Request
DELETE https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
```

다음에 수행할 작업

API에 대한 자세한 내용은 "NSX API 가이드"를 참조하십시오.

VXLAN 포트 변경

VXLAN 트래픽에 사용되는 포트를 변경할 수 있습니다.

NSX 6.2.3 이상에서 기본 VXLAN 포트는 IANA에서 할당한 표준 포트인 4789입니다. NSX 6.2.3이 나오기 전에는 기본 VXLAN UDP 포트 번호가 8472였습니다.

새로운 NSX 설치에서는 VXLAN에 UDP 포트 4789를 사용합니다.

NSX 6.2.2 이전에서 NSX 6.2.3 이상으로 업그레이드할 때 이전의 설치에서 기존 기본값(8472)이나 사용자 지정 포트 번호(예: 8888)를 사용한 경우에는 변경 단계를 수행하지 않는 한 업그레이드 후에도 계속 같은 포트를 사용합니다.

업그레이드한 설치에서 VTEP 게이트웨이(ToR 게이트웨이)를 사용하고 있거나 사용할 예정인 경우에는 VXLAN 포트 4789로 전환해야 합니다.

크로스 vCenter NSX에서는 VXLAN 포트에 4789를 사용할 필요가 없지만, 크로스 vCenter NSX 환경에 있는 모든 호스트가 같은 VXLAN 포트를 사용하도록 구성되어 있어야 합니다. 포트 4789로 전환하면 크로스 vCenter NSX 환경에 새로 추가되는 모든 NSX 설치에서 기존 NSX 배포와 같은 포트를 사용하도록 할 수 있습니다.

VXLAN 포트 변경은 세 가지 단계 프로세스로 수행되며 VXLAN 트래픽은 중단되지 않습니다.

- 1 NSX Manager는 모든 호스트가 이전 및 새 포트에서 VXLAN 트래픽을 수신하도록 구성합니다. 호스트는 이전 포트에서 VXLAN 트래픽을 계속 전송합니다.
- 2 NSX Manager는 새 포트에서 트래픽을 전송하도록 모든 호스트를 구성합니다.
- 3 NSX Manager는 모든 호스트가 이전 포트에서의 수신을 중지하도록 구성하며, 모든 트래픽이 새 포트에서 송수신됩니다.

크로스 vCenter NSX 환경에서는 기본 NSX Manager에서 포트 변경을 시작해야 합니다. 다음 단계를 계속 진행하기 전에 각 단계에서 크로스 vCenter NSX 환경의 모든 호스트에서 구성이 변경됩니다.

사전 요구 사항

- VXLAN에 사용하려는 포트가 방화벽에 의해 차단되지 않았는지 확인합니다.
- 호스트 준비가 실행되는 동안 VXLAN 포트가 변경되고 있지는 않은지 확인합니다.

절차

- 1 **논리적 네트워크 준비(Logical Network Preparation)** 탭을 클릭하고 **VXLAN 전송(VXLAN Transport)**을 클릭합니다.
- 2 VXLAN 포트 패널에서 **변경(Change)** 버튼을 클릭합니다. 전환하려는 포트를 입력합니다. 4789는 IANA에서 VXLAN에 할당하는 포트입니다.

포트 변경 내용은 모든 호스트로 빠르게 전파됩니다.

- 3 (선택 사항) GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus API 요청에 따른 포트 변경 진행 상태를 확인하십시오.

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TWO</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

고객 환경 향상 프로그램

NSX는 VMware의 CEIP(고객 환경 향상 프로그램)에 참여합니다.

CEIP를 통해 수집되는 데이터에 대한 세부 정보와 VMware에서 해당 정보를 사용하는 목적은 신뢰 및 보장 센터(<https://www.vmware.com/solutions/trustvmware/ceip.html>)에 명시되어 있습니다.

NSX에 대한 CEIP에 참여하거나 그만두려는 경우 또는 프로그램 설정을 편집하려는 경우에는 [고객 환경 향상 프로그램 옵션 편집](#)을 참조하십시오.

고객 환경 향상 프로그램 옵션 편집

NSX Manager를 설치하거나 업그레이드할 때 CEIP에 참여하도록 선택할 수 있습니다. 나중에 CEIP에 참여하거나 CEIP를 그만둘 수 있습니다. 정보 수집 빈도 및 기간(일)을 정의할 수도 있습니다.

사전 요구 사항

- NSX Manager가 연결되어 있는지와 vCenter Server와 동기화될 수 있는지 확인합니다.
- DNS가 NSX Manager에서 구성되어 있는지 확인합니다.
- NSX가 데이터 업로드를 위해 공용 네트워크에 연결되어 있는지 확인합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 선택합니다.
- 3 [Networking & Security 인벤토리]에서 **NSX Manager(NSX Managers)**를 선택합니다.
- 4 수정하려는 NSX Manager를 두 번 클릭합니다.
- 5 **요약(Summary)** 탭을 클릭합니다.
- 6 [고객 환경 향상 프로그램] 대화상자에서 **편집(Edit)**을 클릭합니다.
- 7 **VMware 고객 환경 향상 프로그램 참여(Join the VMware Customer Experience Improvement Program)** 옵션을 선택하거나 선택 취소합니다.
- 8 (선택 사항) 되풀이 설정을 구성합니다.
- 9 **확인(OK)**을 클릭합니다.

NSX 로그 정보

syslog 서버를 구성하고 각 NSX 구성 요소에 대한 기술 지원 로그를 확인할 수 있습니다. 관리부 로그는 NSX Manager를 통해 제공되고 데이터부 로그는 vCenter Server를 통해 제공됩니다. 따라서 syslog 서버의 로그를 확인할 때 완전한 정보를 파악할 수 있도록 NSX 구성 요소 및 vCenter Server에 대해 동일한 syslog 서버를 지정하는 것이 좋습니다.

vCenter Server에서 관리되는 호스트에 대해 syslog 서버를 구성하는 방법에 대한 자세한 내용은 <https://docs.vmware.com>에서 적절한 vSphere 설명서 버전을 참조하십시오.

참고 로그를 수집하고 NSX DLR(논리적 분산 라우터) 제어 VM에 액세스하는 데 사용되는 Syslog 또는 점프 서버는 해당 DLR의 논리적 인터페이스에 직접 연결되는 논리적 스위치에 있을 수 없습니다.

표 22-1. NSX 로그

구성 요소	설명
ESXi 로그	이러한 로그는 vCenter Server에서 생성된 VM 지원 번들의 일부로 수집됩니다. ESXi 로그 파일에 대한 자세한 내용은 vSphere 설명서를 참조하십시오.
NSX Edge 로그	NSX Edge CLI에서 <code>show log [follow reverse]</code> 명령을 사용합니다. NSX Edge UI를 통해 기술 지원 로그 번들을 다운로드합니다.
NSX Manager 로그	NSX Manager CLI에서 <code>show log CLI</code> 명령을 사용합니다. NSX Manager 가상 장치 UI를 통해 기술 지원 로그 번들을 다운로드합니다.
라우팅 로그	"NSX 로깅 및 시스템 이벤트" 가이드를 참조하십시오.
Firewall 로그	"NSX 로깅 및 시스템 이벤트" 가이드를 참조하십시오.
Guest Introspection 로그	"NSX 로깅 및 시스템 이벤트" 가이드를 참조하십시오.

NSX Manager

syslog 서버를 지정하려면 [NSX Manager에 대한 Syslog 서버 구성](#) 항목을 참조하십시오.

기술 지원 로그를 다운로드하려면 [NSX용 기술 지원 로그 다운로드](#) 항목을 참조하십시오.

NSX Edge

syslog 서버를 지정하려면 [NSX Edge에 대한 Syslog 서버 구성](#) 항목을 참조하십시오.

기술 지원 로그를 다운로드하려면 [NSX Edge에 대한 기술 지원 로그 다운로드](#) 항목을 참조하십시오.

NSX Controller

syslog 서버를 지정하려면 [NSX Controller용 Syslog 서버 구성](#) 항목을 참조하십시오.

기술 지원 로그를 다운로드하려면 [NSX Controller용 기술 지원 로그 다운로드](#) 항목을 참조하십시오.

방화벽

자세한 내용은 [Firewall 로그](#)를 참조하십시오.

감사 로그

티켓으로 추적된 작업에 대한 감사 로그에는 티켓 ID가 포함됩니다. NSX 티켓 로거 기능을 사용하여 티켓 ID로 변경 사항을 추적할 수 있습니다.

NSX 티켓 로거 사용

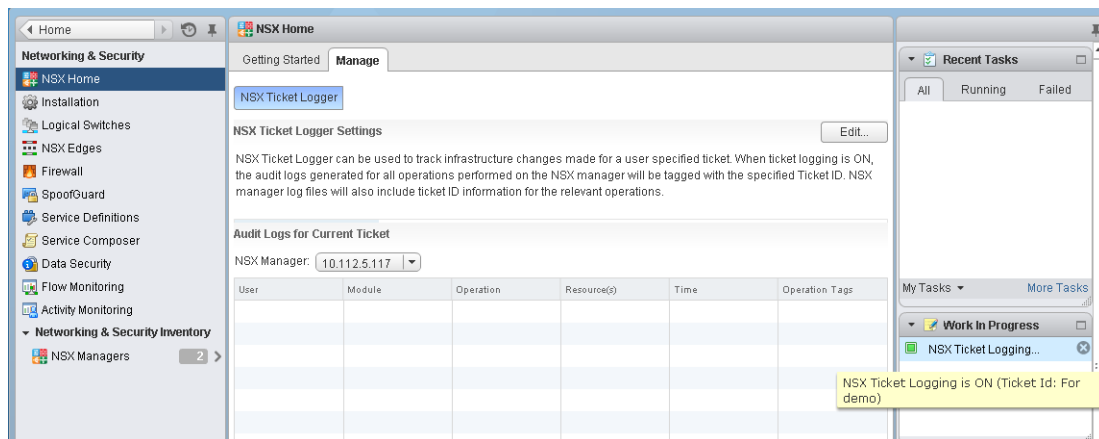
NSX 티켓 로거를 사용하면 수행한 인프라 변경 내용을 추적할 수 있습니다. 모든 작업은 지정한 티켓 ID로 태그가 지정되며 작업의 감사 로그에 티켓 ID가 포함됩니다. 작업의 로그 파일도 동일한 티켓 ID로 태그가 지정됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **관리 탭(Manage)**을 클릭합니다.
- 3 **NSX 티켓 로거 설정(NSX Ticket Logger Settings)** 옆의 **편집(Edit)**을 클릭합니다.
- 4 티켓 ID를 입력하고 **설정(Turn On)**을 클릭합니다.

vSphere Web Client 창 오른쪽에 NSX 티켓 로깅 창이 표시됩니다. 현재 UI 세션에서 수행한 작업에 대한 감사 로그는 **작업 태그(Operation Tags)** 옆의 티켓 ID를 포함합니다.

그림 22-1. NSX 티켓 로거 창



vSphere Web Client가 여러 vCenter Server를 관리하는 경우 해당하는 모든 NSX Manager에서 로깅을 위해 해당 티켓 ID가 사용됩니다.

다음에 수행할 작업

티켓 로깅은 세션 기반입니다. 티켓 로깅이 켜진 상태에서 로그아웃하거나 세션이 끊어진 경우, UI에 다시 로그인하면 티켓 로깅이 기본적으로 해제되어 있습니다. 티켓의 작업이 완료되면 2단계와 3단계를 반복하고 **해제(Turn Off)**를 클릭하여 로깅을 해제합니다.

감사 로그 보기

감사 로그 탭에서는 모든 NSX Manager 사용자가 수행한 작업을 보여 줍니다. NSX Manager는 최대 10만 개의 감사 로그를 보관합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열에서 NSX 서버를 클릭한 후, **모니터** 탭을 클릭합니다.
- 4 **감사 로그** 탭을 클릭합니다.
- 5 감사 로그에 대한 세부 정보가 있을 경우 해당 로그의 **작업** 열에서 텍스트를 클릭할 수 있습니다. 감사 로그 세부 정보를 보려면 **작업** 열의 텍스트를 클릭합니다.
- 6 **감사 로그 변경 세부 정보**에서 **변경된 행**을 선택하면 이 감사 로그 작업에서 값이 변경된 속성만 표시됩니다.

시스템 이벤트

시스템 이벤트는 NSX 작업과 관련된 이벤트입니다. 이러한 이벤트가 발생하면 모든 작동 이벤트의 세부 정보가 제공됩니다. 이벤트는 기본 작업과 관련된 정보 메시지가거나 심각한 오류와 관련된 위험 수준의 메시지가 될 수 있습니다.

시스템 이벤트 보고서 보기

vSphere Web Client에서 NSX Manager를 통해 관리되는 모든 구성 요소에 대한 시스템 이벤트를 볼 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **모니터** 탭을 클릭합니다.
- 4 **시스템 이벤트** 탭을 클릭합니다.

열 머리글의 화살표를 클릭하여 이벤트를 정렬하거나 **필터** 텍스트 상자를 사용하여 이벤트를 필터링할 수 있습니다.

시스템 이벤트 형식

Syslog 서버를 지정할 경우 NSX Manager에서는 모든 시스템 이벤트를 Syslog 서버로 보냅니다.

이러한 메시지는 아래 표시된 메시지와 비슷한 형식을 갖습니다.

```
Jan 8 04:35:00 NSXMGR 2017-01-08 04:35:00.422 GMT+00:00
INFO TaskFrameworkExecutor-18 SystemEventDaoImpl:133 -
[SystemEvent] Time:'Tue Nov 08 04:35:00.410 GMT+00:00 2016',
Severity:'High', Event Source:'Security Fabric', Code:'250024',
Event Message:'The backing EAM agency for this deployment could not be found.
It is possible that the VC services may still be initializing.
Please try to resolve the alarm to check existence of the agency.
In case you have deleted the agency manually, please delete the deployment
entry from NSX.', Module:'Security Fabric', Universal Object:'false'
```

시스템 이벤트는 다음 정보를 포함합니다.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Event Message: Text containing detailed information about the event.
Module: Event component. May be the same as event source.
Universal Object: Value displayed is True or False.
```

경보

경보는 이벤트, 일련의 조건 또는 개체의 상태에 대한 응답으로 활성화되는 알림입니다. 다른 경고와 함께 경보가 NSX 대시보드 및 vSphere Web Client UI의 다른 화면에 표시됩니다.

GET `api/2.0/services/systemalarms` API를 사용하여 NSX 개체에 대한 경보를 볼 수 있습니다.

NSX는 경보에 대해 다음 2가지 방법을 지원합니다.

- 경보는 시스템 이벤트에 해당하며, 연결된 해결 기능이 경보를 트리거하는 문제를 해결하려고 합니다. 이 접근법은 네트워크 및 보안 패브릭 배포(예: EAM, 메시지 버스, 배포 플러그인)용으로 설계되었으며 Service Composer에서도 지원됩니다. 이러한 경보는 이벤트 코드를 경보 코드로 사용합니다. 자세한 내용은 *NSX 로깅 및 시스템 이벤트* 문서를 참조하십시오.
- Edge 알림 경보는 트리거 및 해결 정보 쌍으로 구성됩니다. 이 방법은 IPSec VPN, 로드 밸런서, 고가용성, 상태 점검, Edge 파일 시스템 및 리소스 예약을 비롯한 몇 가지 Edge 기능에서 지원됩니다. 이러한 경보는 이벤트 코드와는 다른 고유한 경보 코드를 사용합니다. 자세한 내용은 *NSX 로깅 및 시스템 이벤트* 문서를 참조하십시오.

일반적으로 경보는 오류 조건이 수정되면 시스템에서 자동으로 삭제됩니다. 일부 경보는 구성 업데이트 시 자동으로 지워지지 않습니다. 문제가 해결되면 경보를 수동으로 지워야 합니다.

다음은 경보를 지우기 위해 사용할 수 있는 API의 예입니다.

특정 소스(예: 클러스터, 호스트, 리소스 풀, 보안 그룹 또는 NSX Edge)에 대한 경보가 발생할 수 있습니다. `sourceId`별로 소스에 대한 경보를 봅니다.

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}
```

sourceId별로 소스에 대한 모든 정보를 해결합니다.

```
POST https://<NSX-IP>/api/2.0/services/alarms/{sourceId}?action=resolve
```

메시지 버스, 배포 플러그인, Service Composer 및 Edge 정보를 비롯한 NSX 정보를 볼 수 있습니다.

```
GET https://<NSX-IP>/api/2.0/services/systemalarms
```

alarmId별로 특정 NSX 정보를 볼 수 있습니다.

```
GET https://<NSX-IP>/api/2.0/services/systemalarms/<alarmId>
```

alarmId별로 특정 NSX 정보를 해결할 수 있습니다.

```
POST https://<NSX-IP>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

API에 대한 자세한 내용은 "NSX API 가이드"를 참조하십시오.

경보 형식

API를 통해 경보 형식을 볼 수 있습니다.

경보 형식에는 다음 정보가 포함됩니다.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Message: Text containing detailed information about the event.
Alarm ID: ID of an alarm.
Alarm Code: Event code which uniquely identifies the system alarm.
Alarm Source: Source where you should look to resolve the reported event.
```

SNMP 트랩 사용

NSX Manager는 예를 들어 NSX Edge 및 하이퍼바이저에서 정보, 주의 및 위험에 해당하는 시스템 이벤트를 수신합니다. SNMP 에이전트는 OID가 있는 SNMP 트랩을 SNMP 수신기로 전달합니다.

SNMP 트랩은 SNMPv2c 버전이어야 합니다. SNMP 수신기가 OID(개체 식별자)가 있는 트랩을 처리할 수 있도록 트랩을 MIB(관리 정보 기반)에 연결해야 합니다.

기본적으로 SNMP 트랩 메커니즘은 사용되지 않도록 설정됩니다. SNMP 트랩을 사용하도록 설정하면 SNMP 관리자가 많은 양의 알림 때문에 곤란해지지 않도록 위험 및 높은 심각도 알림만 활성화됩니다. IP 주소 또는 호스트 이름은 트랩 대상을 정의합니다. 호스트 이름을 트랩 대상에 사용하려면 디바이스는 DNS(Domain Name System) 서버를 쿼리하도록 설정되어야 합니다.

SNMP 서비스를 사용하도록 설정하면 OID가 1.3.6.1.6.3.1.1.5.1인 coldStart 트랩이 최초로 전송됩니다. OID가 1.3.6.1.6.3.1.1.5.2인 warmStart 트랩은 나중에 중지-시작이 있을 때마다 구성된 SNMP 수신기로 전송됩니다.

SNMP 서비스가 사용되도록 설정되어 있으면 OID가 1.3.6.1.4.1.6876.4.190.0.401인 하트비트 트랩 vmwHbHeartbeat가 5분 간격으로 전송됩니다. 서비스를 사용하지 않도록 설정하면 OID가 1.3.6.1.4.1.6876.90.1.2.1.0.1인 vmwNsxMSnmpDisabled 트랩이 전송됩니다. 이 프로세스는 vmwHbHeartbeat 트랩이 실행되지 않도록 하고 서비스를 사용되지 않도록 설정합니다.

SNMP 수신기 값을 추가, 수정 또는 삭제하면 OID가 1.3.6.1.6.3.1.1.5.2인 warmStart 트랩과 OID가 1.3.6.1.4.1.6876.90.1.2.1.0.2인 vmwNsxMSnmpManagerConfigUpdated 트랩이 업데이트되거나 새로운 SNMP 수신기 집합으로 전송됩니다.

참고 SNMP 폴링은 지원되지 않습니다.

SNMP 설정 구성

SNMP 설정을 사용하도록 설정하고 위험, 높음 또는 정보에 해당하는 트랩을 전송하도록 대상 수신기를 구성할 수 있습니다.

사전 요구 사항

- SNMP 트랩 메커니즘을 숙지합니다. [SNMP 트랩 사용](#)을 참조하십시오.
- SNMP 수신기가 구성되어 있는지 확인합니다.
- SNMP 수신기가 OID가 있는 트랩을 처리할 수 있도록 NSX Manager에 대한 MIB 모듈을 다운로드한 후 설치합니다. <http://kb.vmware.com/kb/1013445>를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security > Networking & Security 인벤토리(Networking & Security Inventory) > NSX Manager**를 선택합니다.
- 3 NSX Manager IP 주소를 선택합니다.
- 4 **관리(Manage) > 시스템 이벤트(System Events)** 탭을 선택합니다.

5 편집(Edit)을 클릭하여 SNMP 설정을 구성합니다.

옵션	설명
서비스	SNMP 트랩을 전송합니다. 기본적으로 이 옵션은 사용하도록 설정되어 있지 않습니다.
그룹 알림	발생하는 이벤트를 집계하는 데 사용되는 일부 시스템 이벤트에 대해 미리 정의된 그룹 집합입니다. 기본적으로 이 옵션은 사용하도록 설정되어 있습니다. 예를 들어 시스템 이벤트가 그룹에 속하는 경우 이러한 그룹화된 이벤트에 대한 트랩은 보류됩니다. 5분 간격으로 NSX Manager에서 수신된 시스템 이벤트 수를 자세히 나타내는 트랩이 전송됩니다. 더 적은 수의 트랩이 전송되면 SNMP 수신기 리소스가 절감됩니다.
수신기	트랩이 전송될 수신기를 최대 4개 구성합니다. SNMP 수신기를 추가할 때 다음 섹션을 완료해야 합니다. 수신기 주소 - 수신기 호스트의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다. 수신기 포트 - SNMP 수신기 기본 UDP 포트는 162입니다. 커뮤니티 문자열 - 알림 트랩의 일부로 전송되는 정보입니다. 사용 - 이 수신기가 트랩을 전송하고 있는지 여부를 나타냅니다.

6 확인(OK)을 클릭합니다.

결과

SNMP 서비스가 사용되도록 설정되고 트랩이 수신기로 전송됩니다.

다음에 수행할 작업

SNMP 구성이 제대로 작동하는지 여부를 확인합니다. [SNMP 트랩 구성 확인](#)를 참조하십시오.

SNMP 트랩 구성 확인

기존 시스템 트랩을 편집하기 전에 새로 사용하도록 설정된 SNMP 서비스 또는 업데이트된 SNMP가 제대로 작동하는지 확인해야 합니다.

사전 요구 사항

SNMP가 구성되어 있는지 확인합니다. [SNMP 설정 구성](#)를 참조하십시오.

절차

1 SNMP 구성 및 수신기 연결을 확인합니다.

- a **관리(Manage) > 시스템 이벤트(System Events)** 탭을 선택합니다.
- b **편집(Edit)**을 클릭하여 SNMP 설정을 구성합니다.
대화상자에서 설정을 변경하지 마십시오.
- c **확인(OK)**을 클릭합니다.

OID가 1.3.6.1.6.3.1.1.5.2인 warmStart 트랩이 모든 SNMP 수신기로 전송됩니다.

2 SNMP 구성 또는 수신기 문제를 디버깅합니다.

- a SNMP 수신기가 트랩을 수신하지 못하면 해당 SNMP 수신기가 구성된 포트에서 실행되고 있는지 확인합니다.
- b [SNMP 설정] 섹션에서 수신기 세부 사항이 정확한지 확인합니다.
- c SNMP 수신기가 5분마다 OID 1.3.6.1.4.1.6876.4.190.0.401의 vmwHbHeartbeat 트랩 수신을 중지하면 NSX Manager 장치 또는 NSX Manager SNMP 에이전트가 작동하는지 확인합니다.
- d 하트비트 트랩이 중지되면 SNMP 서비스가 사용되지 않도록 설정되어 있는지 확인하거나 NSX Manager 및 SNMP 수신기 사이의 네트워크 연결이 작동하는지 테스트합니다.

시스템 트랩 편집

시스템 트랩을 편집하여 트랩이 수신기로 전송되거나 보류되도록 트랩의 심각도 및 사용 권한을 늘리거나 줄일 수 있습니다.

모듈, SNMP OID 또는 SNMP 트랩 사용 열 값이 --로 나타나면 해당 이벤트에 트랩 OID가 할당되지 않았음을 의미합니다. 따라서 이러한 이벤트에 대한 트랩은 전송되지 않습니다.

시스템 트랩에는 시스템 이벤트의 다양한 측면을 나열하는 몇 개의 열이 있습니다.





옵션	설명
이벤트 코드	이벤트와 연관된 정적 이벤트 코드입니다.
설명	이벤트를 설명하는 요약입니다.
모듈	이벤트를 트리거하는 하위 구성 요소입니다.
심각도	이벤트 수준은 정보, 낮음, 중간, 심각, 위험 또는 높음일 수 있습니다. 기본적으로 SNMP 서비스가 사용되도록 설정되면 즉각적인 주의가 필요한 트랩만 강조하도록 위험 및 높음 심각도 이벤트의 경우에만 트랩이 전송됩니다.
SNMP OID	시스템 이벤트가 발생할 때 개별 OID 및 이 OID가 전송됨을 나타냅니다. 그룹 알림은 기본적으로 사용되도록 설정되어 있습니다. 그룹 알림이 사용되도록 설정되면 이 그룹의 이벤트 또는 트랩이 해당 이벤트나 트랩이 속하는 그룹의 OID를 표시합니다. 예를 들어 구성 그룹 아래에 범주화된 그룹 알림 OID는 OID 1.3.6.1.4.1.6876.90.1.2.0.1.0.1입니다.
SNMP 트랩 사용	이 이벤트에 대한 트랩 전송을 사용하도록 설정할지 또는 사용하지 않도록 설정할지를 표시합니다. 아이콘을 전환하여 이벤트 또는 트랩 사용을 개별적으로 허가할 수 있습니다. 그룹 알림이 사용되도록 설정되면 트랩 사용 권한 설정/해제를 전환할 수 없습니다.
필터	항목을 검색하여 시스템 트랩을 필터링합니다.

사전 요구 사항

SNMP 설정을 사용할 수 있는지 확인합니다. [SNMP 설정 구성](#)를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security > Networking & Security 인벤토리(Networking & Security Inventory) > NSX Manager(NSX Managers)**를 선택합니다.

- 3 NSX Manager IP 주소를 선택합니다.
- 4 **관리(Manage) > 시스템 이벤트(System Events)** 탭을 선택합니다.
- 5 [시스템 트랩] 섹션에서 시스템 이벤트를 선택합니다.
- 6 **편집(Edit)**() 아이콘을 클릭합니다.
그룹 알림이 사용되도록 설정되어 있으면 트랩 사용 권한 편집이 허용되지 않습니다. 그룹에 속하지 않는 트랩의 사용 권한은 변경할 수 있습니다.
- 7 드롭다운 메뉴에서 시스템 이벤트의 심각도를 변경합니다.
- 8 심각도를 [정보]에서 [위험]으로 변경하는 경우 **SNMP 트랩으로 사용(Enable as SNMP Trap)** 확인란을 선택합니다.
- 9 **확인(OK)**을 클릭합니다.
- 10 (선택 사항) 헤더의 **사용(Enable)**() 아이콘 또는 **사용 안 함(Disable)**() 아이콘을 클릭하여 시스템 트랩 전송을 사용하거나 사용하지 않도록 설정합니다.
- 11 (선택 사항) **복사(Copy)**() 아이콘을 클릭하여 하나 이상의 이벤트 행을 클립보드에 복사합니다.

관리 시스템 설정

처음 로그인할 때 지정한 vCenter Server, DNS 및 NTP 서버 및 Lookup 서버를 편집할 수 있습니다. NSX Manager는 VMware Infrastructure 인벤토리에 대한 세부 정보를 제공하기 위해 vCenter Server 및 서비스(예: DNS, NTP 등)와 통신해야 합니다.

NSX Manager 가상 장치에 로그인

NSX Manager 가상 시스템을 설치하여 구성한 후 NSX Manager 가상 장치에 로그인하여 설치 중 지정된 설정을 검토합니다.

절차

- 1 웹 브라우저 창을 열고 NSX Manager에 할당된 IP 주소를 입력합니다. 예를 들어 **https://192.168.110.42** 같은 주소를 입력합니다.
NSX Manager 사용자 인터페이스가 SSL을 사용하여 웹 브라우저 창에서 열립니다.
- 2 보안 인증서를 수락합니다.

참고 SSL 인증서를 사용하여 인증할 수 있습니다.

NSX Manager 로그인 화면이 표시됩니다.

- 3 사용자 이름 **admin**과 설치 중에 설정한 암호를 사용하여 NSX Manager 가상 장치에 로그인합니다.
- 4 **로그인(Log In)**을 클릭합니다.

NSX Manager 가상 장치 이벤트

다음 이벤트는 NSX Manager 가상 장치에만 해당합니다.

표 22-2. NSX Manager 가상 장치 이벤트

	전원 끄기	전원 켜기	인터페이스 중지	인터페이스 작동
로컬 CLI	show log follow 명령을 실행합니다.	show log follow 명령을 실행합니다.	show log follow 명령을 실행합니다.	show log follow 명령을 실행합니다.
GUI	해당 없음	해당 없음	해당 없음	해당 없음

표 22-3. NSX Manager 가상 장치 이벤트

	CPU	메모리	스토리지
로컬 CLI	show process monitor 명령을 실행합니다.	show system memory 명령을 실행합니다.	show filesystem 명령을 실행합니다.
GUI	해당 없음	해당 없음	해당 없음

NSX Manager 날짜 및 시간 편집

처음 로그인할 때 지정한 NTP 서버를 변경할 수 있습니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 장치 관리(Appliance Management)에서 장치 설정 관리(Manage Appliance Settings)를 클릭합니다.
- 3 시간 설정(Time Settings) 옆의 편집(Edit)을 클릭합니다.
- 4 필요한 내용을 변경합니다.
- 5 확인(OK)을 클릭합니다.
- 6 NSX Manager를 재부팅합니다.

NSX Manager에 대한 Syslog 서버 구성

Syslog 서버를 지정할 경우 NSX Manager는 모든 감사 로그 및 시스템 이벤트를 Syslog 서버로 보냅니다.

Syslog 데이터는 설치와 구성 작업 중의 문제 해결과 기록된 데이터 검토에 유용합니다.

NSX Edge는 2개의 Syslog 서버를 지원합니다. NSX Manager 및 NSX Controller는 하나의 Syslog 서버를 지원합니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.

웹 브라우저에서 <https://<nxs-manager-ip>> 또는 <https://<nxs-manager-hostname>>의 NSX Manager 장치 GUI로 이동하여 NSX Manager 설치 중에 설정한 암호를 사용하여 admin 권한으로 로그인합니다.

- 2 홈 페이지에서 **장치 설정 관리(Manage Appliance Settings) > 일반(General)**을 클릭합니다.
- 3 **Syslog 서버(Syslog Server)** 옆의 **편집(Edit)**을 클릭합니다.
- 4 syslog 서버의 IP 주소 또는 호스트 이름, 포트 및 프로토콜을 입력합니다.

예:

- 5 **확인(OK)**을 클릭합니다.

결과

NSX Manager 원격 로깅은 사용하도록 설정되어 있고, 로그는 독립형 syslog 서버에 저장되어 있습니다.

NSX Manager에서 FIPS 모드 및 TLS 설정 변경

FIPS 모드를 사용하도록 설정하면 NSX Manager와의 모든 보안 통신은 미국 FIPS(연방 정부 처리 표준)에서 허용하는 암호화 알고리즘 및 프로토콜을 사용하게 됩니다.

- 크로스 vCenter NSX 환경에서 각 NSX Manager에 대해 별도로 FIPS 모드를 사용하도록 설정해야 합니다.
- NSX Manager 중 하나가 FIPS용으로 구성되어 있지 않으면 여전히 FIPS 표준을 준수하는 보안 통신 방법을 사용하는지 확인해야 합니다.
- 범용 동기화가 제대로 작동하려면 기본 및 보조 NSX Manager 둘 다 동일한 TLS 버전에 있어야 합니다.

중요 FIPS 모드를 변경하면 NSX Manager 가상 장치가 재부팅됩니다.

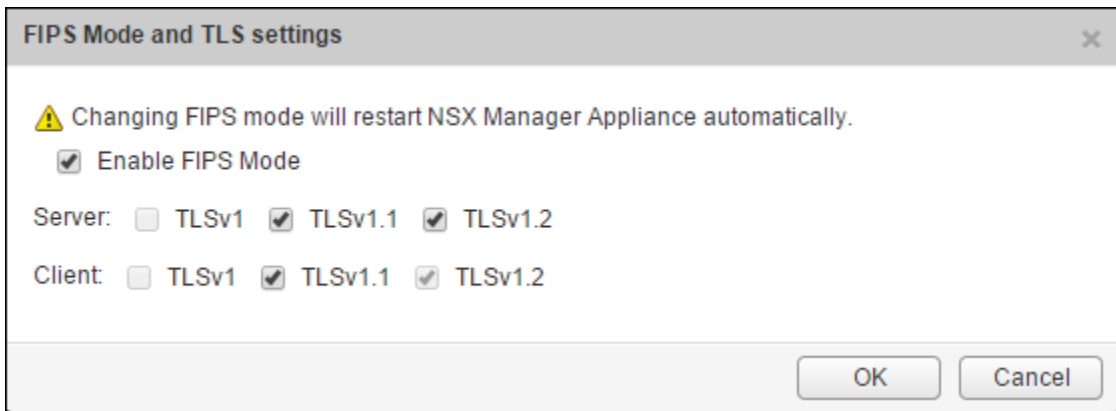
사전 요구 사항

- 파트너 솔루션이 인증된 FIPS 모드인지 확인합니다. 자세한 내용은 VMware 호환성 가이드(<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>)를 참조하십시오.
- 이전 버전의 NSX에서 업그레이드한 경우 NSX 6.3.0으로 업그레이드될 때까지 FIPS 모드를 사용하도록 설정하지 마십시오. "NSX 업그레이드 가이드"에서 "FIPS 모드 및 NSX 업그레이드 이해"를 참조하십시오.

- NSX Manager가 NSX 6.3.0 이상인지 확인하십시오.
- NSX Controller 클러스터가 NSX 6.3.0 이상인지 확인하십시오.
- NSX 워크로드가 실행되는 모든 호스트 클러스터가 NSX 6.3.0 이상으로 준비되어 있는지 확인하십시오.
- 모든 NSX Edge 장치가 버전 6.3.0 이상인지와 필요한 NSX Edge 장치에서 FIPS 모드가 사용되도록 설정되어 있는지 확인하십시오. [NSX Edge에서 FIPS 모드 변경](#)를 참조하십시오.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 **장치 관리(Appliance Management)**에서 **장치 설정 관리(Manage Appliance Settings)**를 클릭합니다.
- 3 설정 패널에서 **일반(General)**을 클릭합니다.
- 4 **FIPS 모드 및 TLS 설정(FIPS Mode and TLS settings)** 옆에 있는 **편집(Edit)**을 클릭합니다.



- 5 FIPS 모드를 사용하도록 설정하려면 **FIPS 모드 사용(Enable FIPS Mode)** 확인란을 선택합니다.
- 6 서버 및 클라이언트에 대해 필수 TLS 프로토콜 버전에 대한 확인란을 선택합니다.

참고 FIPS 모드가 사용되도록 설정되면 NSX Manager는 FIPS 표준과 호환되지 않는 TLS 프로토콜을 사용하지 않도록 설정합니다.

- 7 **확인(OK)**을 클릭합니다.

NSX Manager 장치가 재부팅되고 FIPS가 사용되도록 설정됩니다.

DNS 서버 편집

Manager를 설치할 때 지정한 DNS 서버를 변경할 수 있습니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.

- 2 **장치 관리(Appliance Management)**에서 **장치 설정 관리(Manage Appliance Settings)**를 클릭합니다.
- 3 설정 패널에서 **네트워크(Network)**를 클릭합니다.
- 4 **DNS 서버(DNS Servers)** 옆의 **편집(Edit)**을 클릭합니다.
- 5 필요한 내용을 변경합니다.
- 6 **확인(OK)**을 클릭합니다.

Lookup Service 세부 정보 편집

처음 로그인할 때 지정한 Lookup Service 세부 정보를 변경할 수 있습니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 **장치 관리(Appliance Management)**에서 **장치 설정 관리(Manage Appliance Settings)**를 클릭합니다.
- 3 설정 패널에서 **NSX 관리 서비스(NSX Management Service)**를 클릭합니다.
- 4 **Lookup Service(Edit)** 옆의 **편집(Lookup Service)**을 클릭합니다.
- 5 필요한 내용을 변경합니다.
- 6 **확인(OK)**을 클릭합니다.

vCenter Server 편집

NSX Manager를 설치하는 동안 NSX Manager를 등록한 vCenter Server를 변경할 수 있습니다. 현재 vCenter Server의 IP 주소를 변경하는 경우에만 이 작업을 수행해야 합니다.


절차

- 1 vSphere Web Client에 로그인되어 있으면 로그아웃합니다.
- 2 NSX Manager 가상 장치에 로그인합니다.
- 3 **장치 관리(Appliance Management)**에서 **장치 설정 관리(Manage Appliance Settings)**를 클릭합니다.
- 4 설정 패널에서 **NSX 관리 서비스(NSX Management Service)**를 클릭합니다.
- 5 **vCenter Server** 옆의 **편집(Edit)**을 클릭합니다.
- 6 필요한 내용을 변경합니다.
- 7 **확인(OK)**을 클릭합니다.

NSX용 기술 지원 로그 다운로드

NSX Manager 시스템 로그 및 Web Manager 로그를 데스크톱에 다운로드할 수 있습니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 장치 관리에서 **장치 설정 관리**를 클릭합니다.
- 3 을 클릭하고 **기술 지원 로그 다운로드**를 클릭합니다.
- 4 **다운로드**를 클릭합니다.
- 5 로그를 다운로드할 준비가 되면 **저장**을 클릭하여 로그를 데스크톱에 다운로드합니다.
로그가 압축되고 파일 확장명 **.gz**가 붙습니다.

다음에 수행할 작업

파일을 저장한 디렉토리에서 **모든 파일**을 찾아보고 압축 해제 유틸리티를 사용해 로그를 열 수 있습니다.

NSX Manager SSL 인증

NSX Manager가 NSX Manager 웹 서비스의 ID를 인증하고 NSX Manager 웹 서버로 전송되는 정보를 암호화하려면 서명된 인증서가 필요합니다. 이 프로세스에는 **CSR(인증서 서명 요청)**을 생성하고 **CA**에서 서명한 인증서를 가져오고 서명된 **SSL** 인증서를 NSX Manager로 가져오는 작업이 포함됩니다. 인증서 생성 옵션을 사용하여 개인 키 및 공용 키를 생성하는 것이 보안을 유지하는 가장 좋은 방법입니다. 여기서 개인 키는 NSX Manager에 저장됩니다.

NSX Manager의 기본 제공 CSR 생성기를 사용하거나 OpenSSL과 같은 다른 도구를 사용하여 NSX Manager 인증서를 가져올 수 있습니다.

NSX Manager의 기본 제공 CSR 생성기를 사용하여 생성된 CSR은 **SAN(주체 대체 이름)**과 같은 확장 특성을 포함할 수 없습니다. 확장 특성을 포함하려면 다른 CSR 생성 도구를 사용해야 합니다. OpenSSL과 같은 다른 도구를 사용하여 CSR을 생성할 경우 프로세스는 1) CSR 생성, 2) 인증서에 서명, 3) **NSX Manager 인증서 파일을 PKCS 12 형식으로 변환** 섹션으로 진행 순서로 수행해야 합니다.

기본 제공 CSR 생성기 사용

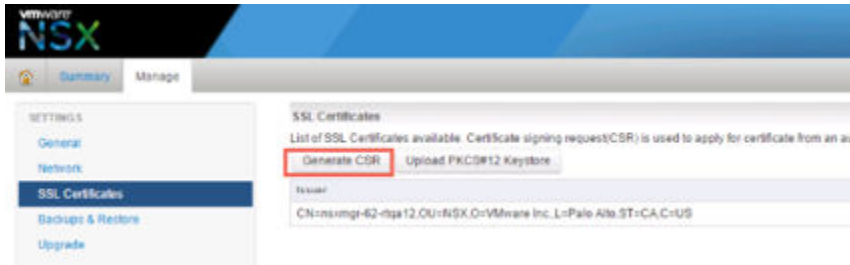
NSX Manager용 SSL 인증서를 얻는 한 가지 방법은 기본 제공 CSR 생성기를 사용하는 것입니다.

이 방법을 사용할 경우 CSR은 **SAN(주체 대체 이름)**과 같은 확장 특성을 포함할 수 없다는 제한이 따릅니다. 확장 특성을 포함하려면 다른 CSR 생성 도구를 사용해야 합니다. 다른 CSR 생성 도구를 사용할 경우 이 절차를 건너뛰십시오.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 **장치 설정 관리(Manage Appliance Settings)**를 클릭합니다.
- 3 [설정] 패널에서 **SSL 인증서(SSL Certificates)**를 클릭합니다.

4 CSR 생성(Generate CSR)을 클릭합니다.



5 다음 필드를 채워 양식을 작성합니다.

옵션	작업
키 크기(Key Size)	선택한 알고리즘에 사용되는 키 길이를 선택합니다.
일반 이름(Common Name)	NSX Manager의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다. FQDN을 입력하는 것이 좋습니다.
조직 구성 단위(Organization Unit)	인증서를 요청한 회사의 부서를 입력합니다.
회사 이름(Organization Name)	회사의 전체 법인명을 입력합니다.
구/군/시 이름(City Name)	회사가 위치한 구/군/시의 전체 이름을 입력합니다.
시/도 이름(State Name)	회사가 위치한 시/도의 전체 이름을 입력합니다.
국가 코드(Country Code)	거주 국가를 나타내는 두 자리 코드를 입력합니다. 예를 들어 미국은 US 입니다.

6 확인(OK)을 클릭합니다.

7 서명을 위해 CSR을 CA로 전송합니다.

a CSR 다운로드(Download CSR)를 클릭하여 생성된 요청을 다운로드합니다.

이 방법을 사용할 경우 개인 키가 항상 NSX Manager에 유지됩니다.

b 이 요청을 CA에 제출합니다.

c 서명된 인증서와 루트 CA, 그리고 PEM 형식의 모든 중간 CA 인증서를 가져옵니다.

d CER/DER 형식 인증서를 PEM으로 변환하려면 다음 OpenSSL 명령을 사용합니다.

```
openssl x509 -inform der -in Cert.cer -out 4-nsx_signed.pem
```

e 모든 인증서(서버 인증서, 중간 인증서 및 루트 인증서)를 하나의 텍스트 파일에 병합합니다.

f NSX Manager UI에서 가져오기(Import)를 클릭하고 모든 인증서가 포함된 텍스트 파일을 찾습니다.

g 가져오기가 성공적으로 완료되면 서버 인증서 및 모든 CA 인증서가 [SSL 인증서] 페이지에 표시됩니다.

다음에 수행할 작업

서명된 SSL 인증서를 NSX Manager로 가져옵니다.

NSX Manager 인증서 파일을 PKCS 12 형식으로 변환

OpenSSL과 같은 다른 도구를 사용하여 NSX Manager 인증서를 사용할 경우 인증서와 개인 키가 PKCS 12 형식이어야 합니다. NSX Manager 인증서 및 개인 키가 PKCS 12 형식이 아닌 경우에는 PKCS 12 형식으로 변환한 다음, PKCS 12 인증서 파일을 NSX Manager로 가져와야 합니다.

사전 요구 사항

- 시스템에 OpenSSL이 설치되어 있는지 확인합니다. <http://www.openssl.org>에서 OpenSSL을 다운로드할 수 있습니다.
- 공용 및 개인 키 쌍을 생성합니다. 예를 들어 다음 OpenSSL 명령을 실행합니다.

```
openssl req -x509 -days [number of days] -newkey rsa:2048 -keyout my-key.pem -out my-cert.pem
```

절차

- ◆ 권한 있는 서명 기관에서 서명된 인증서를 받은 후 OpenSSL 명령을 실행하여 공용 인증서 파일 및 개인 키에서 PKCS 12(.pfx 또는 .p12) Keystore 파일을 생성합니다.

예:

```
openssl pkcs12 -export -in my-cert.pem -inkey my-key.pem -out nsx-manager.p12
```

여기서 다음이 적용됩니다.

- my-cert.pem은 서명된 인증서입니다.
- my-key.pem은 개인 키입니다.
- nsx-manager.p12는 PKCS 12 형식으로 변환한 후 생성된 출력 파일의 이름입니다.

다음에 수행할 작업

PKCS 12 인증서 파일을 NSX Manager로 가져옵니다.

SSL 인증서 가져오기

기존 또는 CA 서명된 SSL 인증서를 가져와 NSX Manager에서 사용할 수 있습니다.

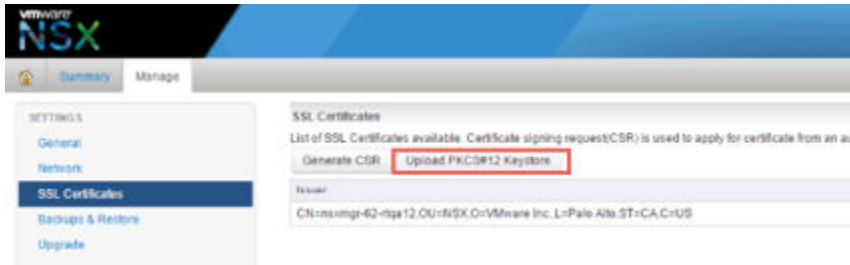
사전 요구 사항

NSX Manager에 인증서를 설치할 때는 PKCS#12 Keystore 형식만 지원되며 인증서에 단일 개인 키와 해당 서명된 인증서 또는 인증서 체인이 포함되어 있어야 합니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 장치 설정 관리(Manage Appliance Settings)를 클릭합니다.
- 3 [설정] 패널에서 SSL 인증서(SSL Certificates)를 클릭합니다.

4 PKCS#12 Keystore 업로드(Upload PKCS#12 Keystore)를 클릭합니다.



5 파일 선택(Choose File)을 클릭하여 파일을 찾습니다.

6 가져오기(Import)를 클릭합니다.

7 인증서를 적용하려면 NSX Manager 장치를 재부팅합니다.

결과

인증서가 NSX Manager에 저장됩니다.

NSX 백업 및 복원

모든 NSX 구성 요소를 올바르게 백업해야 장애 발생 시 시스템을 작동 상태로 복원할 수 있습니다.

NSX Manager 백업에는 컨트롤러, 논리적 스위칭 및 라우팅 항목, 보안, 방화벽 규칙 및 NSX Manager UI 나 API 내에서 구성하는 모든 항목을 포함하는 모든 NSX 구성이 포함되어 있습니다. vCenter 데이터베이스 및 관련 요소(예: 가상 스위치)는 별도로 백업해야 합니다.

NSX Manager와 vCenter는 정기적으로 백업하는 것이 좋습니다. 백업 빈도와 예약은 비즈니스 요구 사항 및 작동 절차에 따라 달라질 수 있습니다. 구성 변경을 자주 수행하는 시기에는 NSX를 자주 백업하는 것이 좋습니다.

NSX Manager 백업은 필요시 수행하거나 매시간, 매일 또는 매주 수행할 수 있습니다.

다음과 같은 경우 백업을 수행하는 것이 좋습니다.

- NSX 또는 vCenter 업그레이드 전
- NSX 또는 vCenter 업그레이드 후
- NSX 구성 요소의 데이터 제로(Day Zero) 배포 및 초기 구성이 완료된 후(예: NSX Controller, 논리적 스위치, 논리적 라우터, Edge Services Gateway, 보안 및 방화벽 정책 생성 후)
- 인프라 또는 토폴로지 변경 후
- 주요 데이터 2(Day 2) 변경 후

롤백하려는 특정 시점의 전체 시스템 상태를 제공할 수 있도록 NSX 구성 요소 백업(예: NSX Manager)을 상호 작용 중인 다른 구성 요소(예: vCenter, 클라우드 관리 시스템, 운영 도구 등)의 백업 예약과 동기화하는 것이 좋습니다.

NSX Manager 백업 및 복원

NSX Manager 가상 장치 웹 인터페이스에서 또는 NSX Manager API를 통해 NSX Manager 백업 및 복원을 구성할 수 있습니다. 매시간, 매일, 매주 단위로 백업을 예약할 수 있습니다.

백업 파일은 NSX Manager가 액세스할 수 있는 원격 FTP 또는 SFTP 위치에 저장됩니다. NSX Manager 데이터에는 구성, 이벤트 및 감사 로그 테이블이 포함됩니다. 구성 테이블은 모든 백업에 포함됩니다.

복원은 백업 버전과 동일한 NSX Manager 버전에서만 지원됩니다. 이러한 이유로 NSX 업그레이드를 수행하기 전과 후에 백업 파일(이전 버전에 대한 백업 하나와 새 버전에 대한 백업 하나)을 생성해야 합니다.

NSX Manager 데이터 백업

요청 시 백업 또는 예약된 백업을 수행하여 NSX Manager 데이터를 백업할 수 있습니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 **백업 및 복원(Backup & Restore)**을 클릭합니다.
- 3 백업 위치를 지정하려면 FTP 서버 설정 옆의 **변경(Change)**을 클릭합니다.
 - a 백업 시스템의 IP 주소 또는 호스트 이름을 입력합니다.
 - b **전송 프로토콜(Transfer Protocol)** 드롭다운 메뉴에서 대상 시스템이 지원하는 프로토콜에 따라 **SFTP** 또는 **FTP**를 선택합니다.
 - c 필요한 경우 기본 포트를 편집합니다.
 - d 백업 시스템에 로그인하는 데 필요한 사용자 이름과 암호를 입력합니다.

- e **백업 디렉토리(Backup Directory)** 텍스트 상자에 백업을 저장할 절대 경로를 입력합니다.

참고 백업 디렉토리를 제공하지 않으면 백업이 **FTP 서버의 기본 디렉토리(홈 디렉토리)**에 저장됩니다.

절대 경로를 확인하려면 **FTP 서버에 로그인하고 사용할 디렉토리로 이동한 다음, 현재 작업 디렉토리 명령(pwd)을 실행합니다.** 예:

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

- f **파일 이름 접두사(Filename Prefix)**에 텍스트 문자열을 입력합니다.

이 텍스트는 백업 시스템에서 파일을 쉽게 인식할 수 있도록 각 백업 파일 이름 앞에 표시됩니다. 예를 들어 **ppdb**를 입력하면 백업 파일 이름은 **ppdbHH_MM_SS_YYYY_Mon_Day**로 지정됩니다.

참고 백업 디렉토리의 파일 수를 **100**으로 제한해야 합니다. 디렉토리의 파일 수가 이 제한을 초과하는 경우 주의 메시지가 표시됩니다.

- g 백업을 보호하려면 암호를 입력합니다.

암호는 백업을 복원할 때 필요합니다.

- h **확인(OK)**을 클릭합니다.

예:

옵션	예
IP/호스트 이름	192.168.110.60
전송 프로토콜	FTP
포트	21
사용자 이름	admin
암호	*****

옵션	예
백업 디렉토리	/datastore-01
파일 이름 접두사	nsxmgr-backup
암호	*****

- 4 요청 시 백업의 경우 **백업(Backup)**을 클릭합니다.

백업 기록(Backup History) 아래에 새 파일이 추가됩니다.

- 5 (필수 사항) 예약된 백업의 경우 [스케줄링] 옆의 **변경(Change)**을 클릭합니다.

- 백업 빈도(Backup Frequency)** 드롭다운 메뉴에서 **매시간(Hourly)**, **매일(Daily)** 또는 **매주(Weekly)**를 선택합니다. 요일, 시간 및 분 드롭다운 메뉴는 선택한 빈도에 따라 사용하지 않도록 설정됩니다. 예를 들어 매일을 선택하는 경우 매일 빈도에 적용되지 않는 요일 드롭다운 메뉴는 사용하지 않도록 설정됩니다.
- 매주 백업을 선택한 경우 데이터가 백업되는 요일을 선택합니다.
- 매주 또는 매일 백업을 선택한 경우 백업이 시작되는 시간을 선택합니다.
- 시작할 분을 선택하고 **스케줄(Schedule)**을 클릭합니다.

옵션	예
백업 빈도	매주
요일	금요일
시간	15
분	45

- 6 로그 데이터 및 흐름 데이터를 백업에서 제외하려면 제외 옆의 **변경(Change)**을 클릭합니다.

- 백업에서 제외할 항목을 선택합니다.
- 확인(OK)**을 클릭합니다.

- 7 FTP 서버 IP/호스트 이름, 자격 증명, 디렉토리 세부 정보 및 암호를 저장합니다. 이 정보는 백업을 복원할 때 필요합니다.

NSX Manager 백업 복원

NSX Manager를 복원하면 백업 파일이 NSX Manager 장치에 로드됩니다. NSX Manager가 액세스할 수 있는 원격 FTP 또는 SFTP 위치에 백업 파일을 저장해야 합니다. NSX Manager 데이터에는 구성, 이벤트 및 감사 로그 테이블이 포함됩니다.

중요 백업 파일을 복원하기 전에 현재 데이터를 백업하십시오.

사전 요구 사항

NSX Manager 데이터를 복원하기 전에 NSX Manager 장치를 다시 설치하는 것이 좋습니다. 기존 NSX Manager 장치에서 복원 작업을 실행할 수도 있지만 지원되는 방법은 아닙니다. 복원 작업에서는 기존 NSX Manager에 오류가 발생하여 새 NSX Manager 장치를 배포한다고 가정합니다.

이전 NSX Manager 장치의 현재 설정을 기록해 두었다가 새로 배포한 NSX Manager 장치에 대한 IP 정보 및 백업 위치 정보를 지정할 때 사용하는 것이 좋습니다.

절차

- 1 기존 NSX Manager 장치의 모든 설정을 적어둡니다. 또한 FTP 서버 설정도 기록해둡니다.
- 2 새 NSX Manager 장치를 배포합니다.
백업한 NSX Manager 장치와 버전이 동일해야 합니다.
- 3 새 NSX Manager 장치에 로그인합니다.
- 4 장치 관리에서 **백업 및 복원(Backups & Restore)**을 클릭합니다.
- 5 [FTP 서버 설정]에서 **변경(Change)**을 클릭하고 FTP 서버 설정을 추가합니다.

[백업 위치] 화면의 **호스트 IP 주소(Host IP Address)**, **사용자 이름(User Name)**, **암호>Password**, **백업 디렉토리(Backup Directory)**, **파일 이름 접두사(Filename Prefix)** 및 **암호(Pass Phrase)** 필드는 복원할 백업의 위치를 식별해야 합니다.

백업 기록(Backup History) 섹션에 백업 폴더가 표시됩니다.

참고 백업 폴더가 **백업 기록(Backup History)** 섹션에 나타나지 않으면 FTP 서버 설정을 확인합니다. FTP 서버에 연결할 수 있는지와 백업 폴더를 볼 수 있는지 확인합니다.

- 6 **백업 기록(Backup History)** 섹션에서 복원할 필수 백업 폴더를 선택하고 **복원(Restore)**을 클릭합니다.

NSX Manager 데이터 복원이 시작됩니다.

결과


NSX 구성이 NSX Manager로 복원됩니다.

경고 NSX Manager 백업을 복원한 후에 추가 작업을 수행하여 NSX Edge 장치 및 논리적 스위치가 제대로 작동하는지 확인해야 할 수 있습니다. **NSX Edge 복원 및 논리적 스위치에 대한 동기화되지 않음 오류 해결**을 참조하십시오.

NSX Edge 복원

모든 NSX Edge 구성(논리적 라우터 및 Edge Services Gateway)은 NSX Manager 데이터 백업의 일부로 백업됩니다.

개별 NSX Edge 백업을 수행하는 것은 지원되지 않습니다.

원래 상태의 NSX Manager 구성이 있을 경우 vSphere Web Client에서 **NSX Edge 다시 배포**  (Redeploy **NSX Edge**)를 클릭하고 NSX Edge를 다시 배포하여 연결할 수 없거나 장애가 발생한 Edge Appliance VM을 다시 생성할 수 있습니다. "NSX 관리 가이드"의 "NSX Edge 다시 배포"를 참조하십시오.

경고 NSX Manager 백업을 복원한 후에 추가 작업을 수행하여 NSX Edge 장치가 제대로 작동하는지 확인해야 할 수 있습니다.

- 마지막 백업 이후에 생성된 Edge 장치는 복원 중에 제거되지 않습니다. VM을 수동으로 삭제해야 합니다.
- 마지막 백업 후에 삭제된 Edge 장치는 다시 배포되지 않으면 복원되지 않습니다.
- 백업이 복원될 때 백업에 저장된 NSX Edge 장치의 구성된 위치 및 현재 위치가 더 이상 존재하지 않으면 다시 배포, 마이그레이션, HA를 사용하거나 사용하지 않도록 설정하는 것과 같은 작업이 실패합니다. 장치 구성을 편집하고 올바른 위치 정보를 제공해야 합니다. PUT /api/4.0/edges/{edgeId}/appliances를 사용하여 장치 위치 구성(필요에 따라 resourcePoolId, datastoreId, hostId 및 vmFolderId)을 편집합니다. "NSX API 가이드"의 "NSX Edge 장치 구성 사용"을 참조하십시오.

마지막 NSX Manager 백업 이후에 다음 변경이 발생하면 복원된 NSX Manager 구성 및 NSX Edge 장치에 존재하는 구성이 달라집니다. NSX Edge를 **강제로 동기화(Force Sync)**하여 장치의 이러한 변경 사항을 되돌리고 NSX Edge가 올바르게 작동하는지 확인해야 합니다. "NSX 관리 가이드"의 "NSX Edge를 NSX Manager와 강제 동기화"를 참조하십시오.

- NSX Edge 방화벽의 preRules에 대해 분산 방화벽을 통해 수행된 변경
- 그룹 개체 멤버 자격의 변경

마지막 NSX Manager 백업 이후에 다음 변경이 발생하면 복원된 NSX Manager 구성 및 NSX Edge 장치에 존재하는 구성이 달라집니다. NSX Edge를 **다시 배포(Redeploy)**하여 장치의 이러한 변경 사항을 되돌리고 NSX Edge가 올바르게 작동하는지 확인해야 합니다. "NSX 관리 가이드"의 "NSX Edge 다시 배포"를 참조하십시오.

- Edge 장치 설정 변경 사항:
 - HA 사용 또는 사용 안 함
 - 장치가 배포 상태에서 배포 해제 상태로 전환
 - 장치가 배포 해제 상태에서 배포 상태로 전환
 - 리소스 예약 설정이 변경됨
- Edge 장치 vNIC 설정 변경 사항:
 - vNIC 추가, 제거 또는 연결 해제
 - 포트 그룹
 - 트렁크 포트
 - Fence 매개 변수
 - 조절 정책

논리적 스위치에 대한 동기화되지 않음 오류 해결

NSX Manager 백업을 작성하고 백업을 복원하는 중간에 논리적 스위치가 변경되면 논리적 스위치는 동기화되지 않음 상태를 보고할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security) > 논리적 스위치(Logical Switches)로 이동합니다.
- 3 있는 경우 [상태] 열에서 동기화되지 않음(Out of sync) 링크를 클릭하여 오류 정보를 표시합니다.
- 4 해결(Resolve)을 클릭하여 논리적 스위치에 대한 누락된 지원 포트 그룹을 다시 생성합니다.

vSphere Distributed Switch 백업

vSphere Distributed Switch 및 분산 포트 그룹 구성을 파일로 내보낼 수 있습니다.

파일에는 유효한 네트워크 구성이 유지되므로 이러한 구성을 다른 배포로 분배할 수 있습니다.

vSphere Distributed Switch 설정 및 포트 그룹 설정은 가져오기 작업의 일부로 가져오게 됩니다.

VXLAN에 사용할 수 있도록 클러스터를 준비하기 전에 vSphere Distributed Switch 구성을 내보내는 것이 좋습니다. 자세한 내용은 <http://kb.vmware.com/kb/2034602> 항목을 참조하십시오.

vCenter 백업

NSX 배포를 보호하려면 vCenter 데이터베이스를 백업하고 VM의 스냅샷을 생성해야 합니다.

vCenter 백업 및 복원 절차와 모범 사례는 사용 중인 vCenter 버전의 vCenter 설명서를 참조하십시오.

VM 스냅샷에 대한 자세한 내용은 <http://kb.vmware.com/kb/1015180> 항목을 참조하십시오.

vCenter 5.5에 유용한 링크:

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

vCenter 6.0에 유용한 링크:

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

Flow Monitoring

Flow Monitoring은 보호된 가상 시스템으로 들어가거나 보호된 가상 시스템에서 나오는 트래픽을 자세히 보여 주는 트래픽 분석 도구입니다. Flow Monitoring을 사용하도록 설정하면 Flow Monitoring 출력에는 어떤 시스템이 어떤 애플리케이션을 통해 데이터를 교환하고 있는지가 명시됩니다. 세션 수와 세션당 전송된

패킷 수도 이 데이터에 포함됩니다. 세션 세부 정보에는 소스, 대상, 애플리케이션, 사용 중인 포트 등이 포함됩니다. 세션 세부 정보를 사용하여 방화벽 허용 또는 차단 규칙을 생성할 수 있습니다.

TCP, UDP, ARP, ICMP 등 다양한 프로토콜 유형에 대한 흐름 데이터를 볼 수 있습니다. 선택한 vNIC로 들어가거나 vNIC에서 나오는 TCP 및 UDP 연결을 실시간으로 모니터링할 수 있습니다. 필터를 지정하여 흐름을 제외할 수도 있습니다.

따라서 **Flow Monitoring**은 악성 서비스를 감지하고 아웃바운드 세션을 검토하는 포렌식 도구로 사용될 수 있습니다.

Flow Monitoring 데이터 보기

지정된 기간 동안의 가상 시스템 트래픽 세션을 볼 수 있습니다. 최근 **24시간**의 데이터가 기본적으로 표시되며 최소 기간은 **1시간**, 최대 기간은 **2주**입니다.

사전 요구 사항

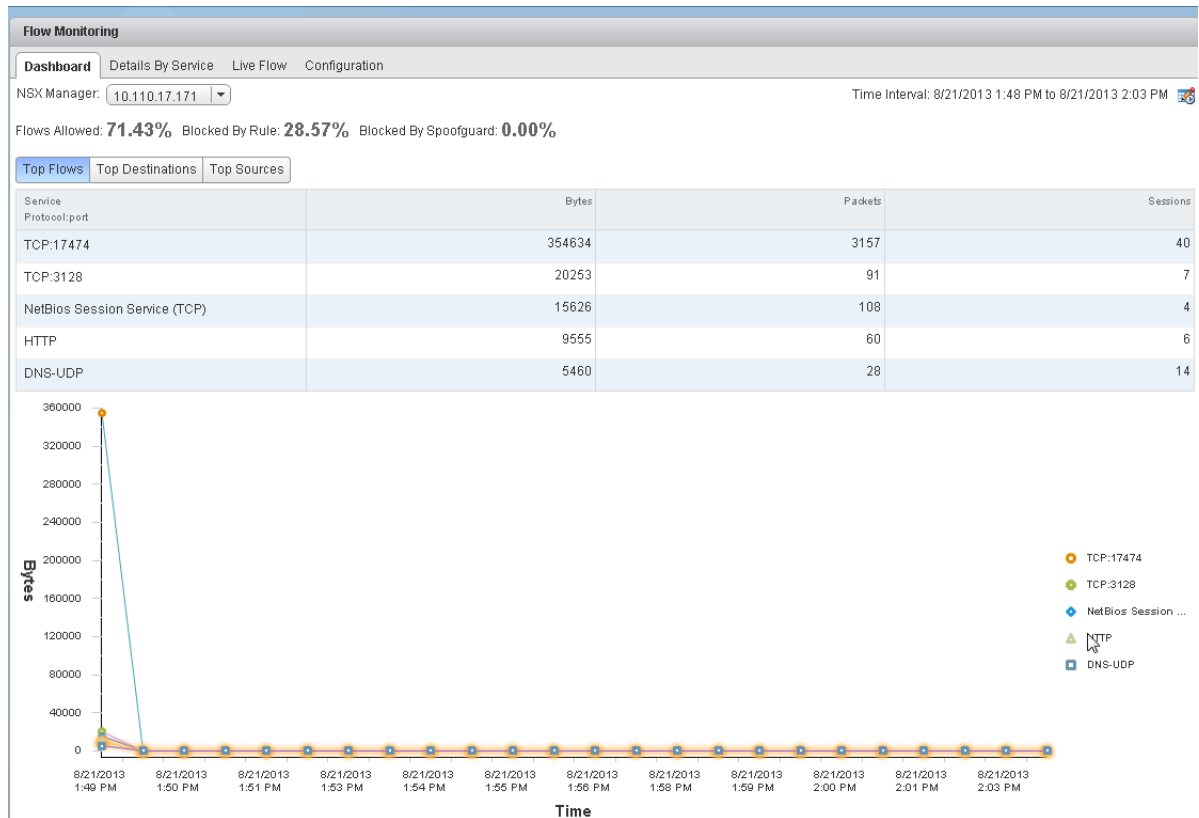
Flow Monitoring 데이터는 네트워크 가상화 구성 요소가 설치되어 있고 방화벽을 사용하는 클러스터에 있는 가상 시스템에만 사용할 수 있습니다. "**NSX 설치 가이드**"를 참조하십시오.

절차

- 1** vSphere Web Client에 로그인합니다.
- 2** 왼쪽 탐색 창에서 **Networking & Security**를 선택하고 **Flow Monitoring**을 선택합니다.
- 3** **대시보드(Dashboard)** 탭으로 이동합니다.

4 Flow Monitoring을 클릭합니다.

페이지가 로드되는 데 몇 초가 걸릴 수 있습니다. 페이지 맨 위에 허용된 트래픽, 방화벽 규칙에 따라 차단된 트래픽 및 SpoofGuard에 의해 차단된 트래픽의 백분율이 표시됩니다. 여러 선형 그래프에는 환경에서 실행되는 각 서비스의 데이터 흐름이 표시됩니다. 범례 영역에서 서비스를 가리키면 해당 서비스에 대한 차트가 강조 표시됩니다.



트래픽 통계는 세 개의 탭에 표시됩니다.

- **상위 흐름(Top Flows)**에는 지정된 기간 동안의 들어오고 나가는 서비스당 총 트래픽이 총 바이트 값 기준으로 표시됩니다(세션/패킷 기준이 아님). 상위 5개 서비스가 표시됩니다. 차단된 흐름은 상위 흐름을 계산할 때 고려되지 않습니다.
- **상위 대상(Top Destinations)**에는 지정된 기간 동안의 대상별 들어오는 트래픽이 표시됩니다. 상위 5개 대상이 표시됩니다.
- **상위 소스(Top Sources)**에는 지정된 기간 동안의 소스별 나가는 트래픽이 표시됩니다. 상위 5개 소스가 표시됩니다.

5 서비스별 세부 정보(Details by Service) 탭을 클릭합니다.

선택한 서비스의 모든 트래픽에 대한 세부 정보가 표시됩니다. **허용된 흐름(Allowed Flows)** 탭에는 허용된 트래픽 세션이 표시되고, **차단된 흐름(Blocked Flows)** 탭에는 차단된 트래픽이 표시됩니다.

서비스 이름을 검색할 수 있습니다.

Flow Monitoring

Dashboard **Details By Service** Live Flow Configuration

NSX Manager: 10.110.17.171 Time Interval: 8/23/2013 6:10 AM to 8/23/2013 6:25 AM

Allowed Flows Blocked Flows

Type	Service	Bytes	Sessions
UDP	DHCP-Server	4954	6
TCP	TCP:17474	2224	1
OTHER	IPv6-ICMP:0	1872	18
OTHER	ARP	1196	26
OTHER	0xffff	162	2
UDP	NTP Time Server	152	1

Find 6 items

Rule Id	Time Stamp	Source	Source User(s)	Destination	Packets	Actions
1021	8/23/2013 6:15 AM	10.112.243.233	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:15 AM	DB_server	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:15 AM	win32rdclone	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:14 AM	10.112.243.214	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:12 AM	win32rdclone	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:11 AM	10.112.243.229	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:13 AM	win32rdclone	Unknown	10.113.60.150	12	Add Rule Edit Rule


6 테이블에 있는 항목을 클릭하면 해당 트래픽 흐름에 대해 허용되거나 차단된 규칙이 표시됩니다.

7 규칙 세부 정보를 표시하려면 규칙의 **규칙 ID(Rule Id)**를 클릭합니다.

Flow Monitoring 차트의 날짜 범위 변경

대시보드 및 세부 정보 탭에 표시되는 Flow Monitoring 데이터의 날짜 범위를 변경할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 왼쪽 탐색 창에서 **Networking & Security**를 선택하고 **Flow Monitoring**을 선택합니다.
- 3 **시간 간격(Time interval)** 옆의 를 클릭합니다.
- 4 기간을 선택하거나, 새 시작 날짜 및 종료 날짜를 입력합니다.
최대 지난 2주간의 트래픽 흐름 데이터를 볼 수 있습니다.
- 5 **확인(OK)**을 클릭합니다.

Flow Monitoring 보고서에서 방화벽 규칙 추가 또는 편집

트래픽 데이터로 드릴다운하면 리소스 사용을 평가하고 분산 방화벽으로 세션 정보를 보내 원하는 수준으로 새 허용 또는 차단 규칙을 생성할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 왼쪽 탐색 창에서 **Networking & Security**를 선택하고 **Flow Monitoring**을 선택합니다.
- 3 **서비스별 세부 정보(Details by Service)** 탭을 클릭합니다.
- 4 트래픽 흐름을 볼 서비스를 클릭합니다.

선택한 탭에 따라 해당 서비스에 대해 트래픽을 허용하거나 거부한 규칙이 표시됩니다.

- 5 규칙 세부 정보를 보려면 규칙 ID를 클릭합니다.
- 6 다음 중 하나를 수행합니다.

- 규칙을 편집하려면

- 1 **작업(Edit Rule)** 열에서 **규칙 편집(Actions)**을 클릭합니다.
- 2 규칙의 이름, 작업 또는 주석을 변경합니다.
- 3 **[확인]**을 클릭합니다.

- 규칙을 추가하려면

- 1 **작업(Add Rule)** 열에서 **규칙 추가(Actions)**를 클릭합니다.
- 2 양식을 작성하고 규칙을 추가합니다. 방화벽 규칙 양식을 작성하는 방법에 대한 자세한 내용은 [분산 방화벽 규칙 추가](#) 항목을 참조하십시오.
- 3 **확인(OK)**을 클릭합니다.

규칙이 방화벽 규칙 섹션의 맨 위에 추가됩니다.

라이브 흐름 보기

선택한 vNIC로 들어가거나 vNIC에서 나오는 TCP 및 UDP 연결을 볼 수 있습니다. 두 가상 시스템 간의 트래픽을 보려는 경우 한 컴퓨터에서 한 가상 시스템의 라이브 트래픽을 본 후 두 번째 컴퓨터에서 다른 가상 시스템의 라이브 트래픽을 보면 됩니다. 호스트당 최대 2개의 vNIC와 인프라당 최대 5개의 vNIC의 트래픽을 볼 수 있습니다.

라이브 흐름을 보는 작업은 NSX Manager와 해당 가상 시스템의 성능에 영향을 줄 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 왼쪽 탐색 창에서 **Networking & Security**를 선택하고 **Flow Monitoring**을 선택합니다.
- 3 **라이브 흐름(Live Flow)** 탭을 클릭합니다.
- 4 **찾아보기(Browse)**를 클릭하고 vNIC를 선택합니다.

5 시작(Start)을 클릭하여 라이브 흐름 보기를 시작합니다.

페이지 새로 고침 간격은 **5초**입니다. **새로 고침 속도(Refresh Rate)** 드롭다운에서 다른 빈도를 선택할 수 있습니다.

RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	state	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets
1026	OUT	Active	TCP	172.16.40.121	49099	172.16.40.131	3306	FINWAIT2	747	11	2077	9
1026	OUT	Inactive	TCP	172.16.40.121	49098	172.16.40.131	3306	FINWAIT2	747	11	2077	9

6 NSX Manager나 선택한 가상 시스템의 성능에 영향을 주지 않도록 디버깅이나 문제 해결이 완료되면 중지(Stop)를 클릭합니다.

Flow Monitoring 데이터 수집 구성

수집할 Flow Monitoring 데이터를 보고 필터링한 후 데이터 수집을 구성할 수 있습니다. 제외 조건을 지정하여 필터링한 데이터만 표시되도록 할 수 있습니다. 예를 들어 프록시 서버를 제외하여 중복 흐름이 표시되지 않도록 할 수 있습니다. 또는 인벤토리의 가상 시스템에서 Nessus 검사를 실행 중인 경우에는 검사 흐름이 수집 대상에 포함되도록 할 수 있습니다. 특정 흐름에 대한 정보가 방화벽에서 흐름 수집기로 직접 보내지도록 IPFix를 구성할 수 있습니다. Flow Monitoring 그래프에는 IPFix 흐름이 포함되지 않습니다. 이 흐름은 IPFix 수집기의 인터페이스에 표시됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 왼쪽 탐색 창에서 **Networking & Security**를 선택하고 **Flow Monitoring**을 선택합니다.
- 3 **구성(Configuration)** 탭을 선택합니다.
- 4 **글로벌 흐름 수집 상태(Global Flow Collection Status)**가 **사용(Enabled)**으로 설정되어 있는지 확인합니다.

제외 설정(Exclusion Settings)에 지정된 개체를 제외하고 인벤토리 전체에서 모든 방화벽 관련 흐름이 수집됩니다.

5 필터링 조건을 지정하려면 **흐름 제외(Flow Exclusion)**를 클릭하고 아래 단계를 수행합니다.

a 제외할 흐름에 해당하는 탭을 클릭합니다.

Flow Monitoring

Dashboard Details By Service Live Flow **Configuration**

NSX Manager: 10.110.8.93

Global Flow Collection Status: **Enabled** Disable

Flow Exclusion IPFix

Exclusion Settings
System will not collect flows that match the specified condition

Filter	
Collect Blocked Flows	Yes
Collect Layer2 Flows	Yes
Source	
Destination	system-generated-broadcast-macset, 224.0.0.0/24, 255.255.255.255
Destination ports	138,137
Service	

System is configured to collect all firewall related flows except those that match the conditions specified below

Detail Collection Policy: (Click Save to commit changes to settings)

Collect Blocked Flows:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Collect Layer2 Flows:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Save

b 필요한 정보를 지정합니다.

다음을 선택한 경우	다음 정보 지정
차단된 흐름 수집	차단된 흐름을 제외하려면 아니요를 선택합니다.
계층 2 흐름 수집	계층 2 흐름을 제외하려면 아니요를 선택합니다.
소스	지정한 소스에 대해 흐름이 수집되지 않습니다. <ol style="list-style-type: none"> 1 추가(Add) 아이콘을 클릭합니다. 2 보기에서 적절한 컨테이너를 선택합니다. 3 제외할 개체를 선택합니다.
대상	지정한 대상에 대해 흐름이 수집되지 않습니다. <ol style="list-style-type: none"> 1 추가(Add) 아이콘을 클릭합니다. 2 보기에서 적절한 컨테이너를 선택합니다. 3 제외할 개체를 선택합니다.
대상 포트	지정한 포트에 가는 흐름을 제외합니다. 제외할 포트 번호를 입력합니다.
서비스	지정한 서비스 및 서비스 그룹에 대한 흐름을 제외합니다. <ol style="list-style-type: none"> 1 추가(Add) 아이콘을 클릭합니다. 2 적절한 서비스 및/또는 서비스 그룹을 선택합니다.

c 저장(Save)을 클릭합니다.

6 흐름 수집을 구성하려면 **IPFix**를 클릭하고 **분산 방화벽에 대한 IPFIX**에 설명된 단계를 수행합니다.

7 변경 내용 게시(Publish Changes)를 클릭합니다.

IPFIX 구성

IPFIX(Internet Protocol Flow Information Export)는 최종 디바이스에서 모니터링 시스템으로 흐름 정보를 내보내기 위한 표준을 정의하는 IETF 프로토콜입니다. NSX는 IP 흐름 정보를 수집기로 내보내기 위해 IPFIX를 지원합니다.

다음에서 IPFIX를 사용하도록 설정할 수 있습니다.

- VDS(vSphere Distributed Switch)
- DFW(분산 방화벽)

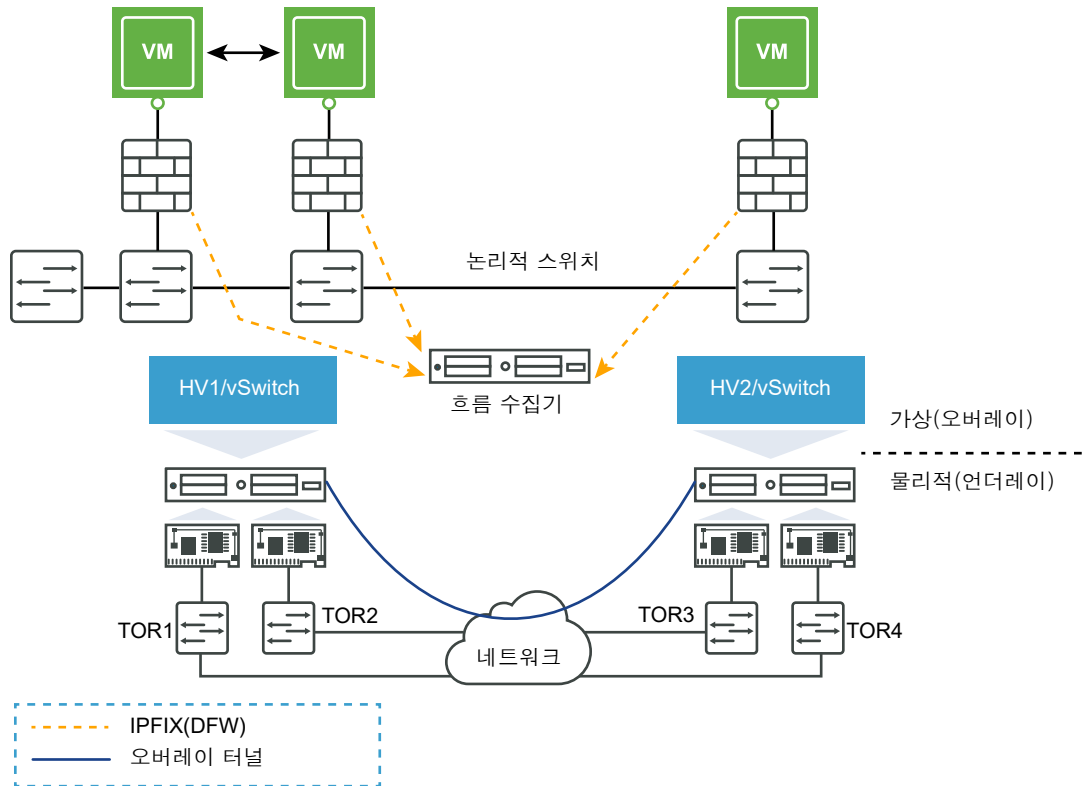
vSphere 환경에서 vSphere Distributed Switch는 내보내기이고, 수집기는 네트워킹 벤더의 모니터링 도구입니다.

IPFIX 표준은 IP 흐름 정보가 제공되고 내보내기에서 수집기로 전송되는 방식을 지정합니다.

vSphere Distributed Switch에서 IPFIX를 사용하도록 설정하면 수집기 도구로 메시지가 주기적으로 전송됩니다. 이러한 메시지의 콘텐츠는 템플릿을 사용하여 정의됩니다. 템플릿에 대한 자세한 내용은 [IPFIX 템플릿](#)을 참조하십시오.

분산 방화벽에 대한 IPFIX

분산 방화벽에 대해 IPFIX를 사용하도록 설정할 수 있습니다. 분산 방화벽은 흐름의 상태 저장 추적을 구현하며, 추적된 흐름은 일련의 상태 변경을 겪습니다. IPFIX는 흐름의 상태에 대한 데이터를 내보내는 데 사용될 수 있습니다. 추적된 이벤트에는 흐름 생성, 흐름 거부, 흐름 업데이트 및 흐름 해체가 포함됩니다.



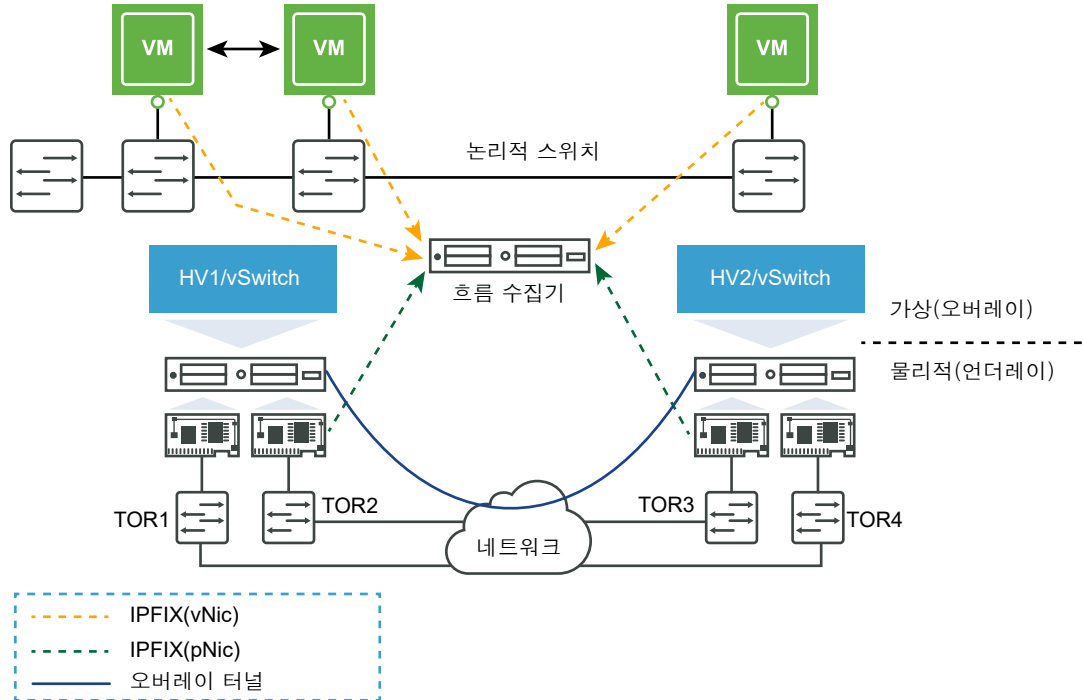
다음과 같이 분산 방화벽에서 IPFIX에 대한 흐름 내보내기를 사용하도록 설정할 수 있습니다.

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **도구(Tools)** 아래에서 **Flow Monitoring**을 클릭합니다.
- 3 **구성(Configuration)** 탭을 선택합니다.
- 4 **글로벌 흐름 수집 상태(Global Flow Collection Status)**가 **사용(Enabled)**으로 설정되어 있는지 확인합니다.
- 5 흐름 수집을 구성하려면 **IPFix**를 클릭하고 다음 단계를 수행합니다.
 - a IPFix 구성 옆에 있는 **편집(Edit)**을 클릭하고 **IPFix 구성 사용(Enable IPFix Configuration)**을 클릭합니다.
 - b 관찰 **DomainID(Observation DomainID)**에서 흐름 수집기에 대한 방화벽 내보내기를 식별하는 32비트 식별자를 입력합니다. 유효한 범위는 0-65535입니다.
 - c **활성화된 흐름 내보내기 시간 초과(Active Flow Export Timeout)**에서 활성화된 흐름을 흐름 수집기로 내보내게 되는 시간 초과(분)를 입력합니다. 기본값은 5입니다. 예를 들어, 흐름이 30분 동안 활성 상태이고 내보내기 시간 초과가 5분일 경우 흐름은 지속 시간 동안 7번 내보내집니다. 여기에는 각 생성 및 삭제에 대해 한 번, 활성 기간 동안 5번이 포함됩니다.
 - d **수집기 IP(Collector IPs)**에서 추가(추가) 아이콘을 클릭하고 흐름 수집기의 IP 주소 및 UDP 포트를 입력합니다. 포트 번호를 확인하려면 **NetFlow** 수집기 설명서를 참조하십시오.
 - e **확인(OK)**을 클릭합니다.

6 변경 내용 게시(Publish Changes)를 클릭합니다.

논리적 스위치에 대한 IPFIX

vSphere Distributed Switch에서 IPFIX를 사용하도록 설정할 수 있습니다.



논리적 스위치에 대한 IPFIX는 다음과 같이 사용하도록 설정할 수 있습니다.

- 1 NSX 전송 영역(논리적 스위치)을 지원하는 vSphere Distributed Switch에서 NetFlow 수집기를 구성합니다. NetFlow 수집기를 구성하는 방법에 대한 자세한 내용은 vSphere 네트워킹 가이드에서 "vSphere Distributed Switch의 NetFlow 설정 구성" 항목을 참조하십시오.
- 2 논리적 스위치에 해당하는 분산 포트 그룹에서 NetFlow 모니터링을 사용하도록 설정할 수 있습니다. NSX 전송 영역이 여러 VDS(vSphere Distributed Switch)에 걸쳐 있는 경우 각 VDS/분산 포트 그룹에 대해 이러한 단계를 반복합니다. NetFlow 모니터링을 사용하도록 설정하는 방법에 대한 자세한 내용은 vSphere 설명서에서 "분산 포트 그룹 또는 분산 포트에서 NetFlow 모니터링을 사용하거나 사용하지 않도록 설정"을 참조하십시오.

NSX 환경에서 ESXi의 NSX 업링크를 탐색하는 논리적 스위치의 가상 시스템 데이터 트래픽은 VXLAN으로 캡슐화됩니다. 호스트 업링크에서 NetFlow를 사용하도록 설정하면 사용자 지정 IPFIX 흐름 레코드 템플릿을 사용하여 IP 흐름 레코드가 내보내집니다. 템플릿에는 외부 VXLAN UDP/IP 헤더 정보와 캡슐화된 내부 IP 패킷의 정보가 포함되어 있습니다. 따라서 이러한 흐름 레코드는 패킷(외부 헤더)을 캡슐화하는 VTEP에 대한 가시성과 NSX 논리 스위치(VXLAN)에서 호스트 간 트래픽(내부 헤더)를 생성한 가상 시스템의 세부 정보를 제공합니다.

vSphere Distributed Switch의 IPFIX 템플릿에 대한 자세한 내용은 [IPFIX 템플릿](#)을 참조하십시오.

IPFIX 템플릿

IPFIX 템플릿은 VXLAN 및 비 VXLAN 흐름에 대한 가시성을 제공합니다. 템플릿에는 캡슐화된 트래픽에 대한 자세한 정보를 제공하는 추가 매개 변수가 있습니다.

템플릿은 vSphere Distributed Switch(내보내기)에서 지원됩니다. vSphere Distributed Switch에 대한 IPFIX 지원은 가상 시스템 흐름 및 VXLAN 흐름에 대한 필수 가시성을 제공합니다. 다른 타사 수집기 도구를 이용하는 경우, 템플릿에서 사용할 수 있는 추가 정보를 사용하여 내부 및 외부 흐름 간 상관 관계와 포트 연결을 제공할 수 있습니다.

IPv4 템플릿

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv4 VXLAN 템플릿

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_VXLAN)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
```

```

IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_END()

```

IPv4 ICMP VXLAN 템플릿

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_VXLAN)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv4 ICMP 템플릿

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)

```



```

IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

IPv6 ICMP VXLAN 템플릿

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_VXLAN)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//VXLAN Specific
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv6 ICMP 템플릿

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)

```

```

IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

IPv6 템플릿

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv6 VXLAN 템플릿

```

IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)

```

```

IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//VXLAN specific
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_END()

```

추가 매개 변수

다음은 추가 매개 변수입니다.

- 1 VXLAN 특정 매개 변수: 테넌트 특정 필드는 내부 흐름 IP, 포트 및 프로토콜 정보입니다.

- tenantSourceIPv4
- tenantSourceIPv6
- tenantDestIPv4
- tenantDestIPv6
- tenantSourcePort
- tenantDestPort
- tenantProtocol
- 인터페이스 포트 매개 변수

- 2 인터페이스 포트 매개 변수: 이러한 매개 변수는 VXLAN 및 비 VXLAN 템플릿 둘 다에서 사용할 수 있습니다.

- ingressInterfaceAttr
- egressInterfaceAttr
- vxlanExportRole

수신 및 송신 인터페이스 특성은 포트 유형을 기준으로 다음 값을 사용할 수 있습니다.

- IPFIX_UPLINK_PORT 0X01

- IPFIX_ACCESS_PORT 0x02
- IPFIX_VXLAN_TUNNEL_PORT 0x03

*vxlanExportRole*은 내보내기가 ESXi 호스트인지 또는 기타 네트워크 디바이스인지 정의합니다.

*IPFIX_END_POINT 0x01*은 호스트에서 데이터를 내보내고 있음을 의미합니다. 다른 디바이스가 IPFIX 템플릿을 내보낼 경우 이 필드는 다른 값을 가질 수 있습니다(아직 정의되지 않음).

vSphere Distributed Switch용 IPFIX에서 모니터링되는 흐름

위 다이어그램에서는 2개의 다른 호스트에서 실행되는 2개의 VM 간 통신과 vSphere Distributed Switch의 IPFIX 기능에 의해 모니터링되는 흐름을 보여 줍니다.

그림 22-2. 호스트 1의 흐름

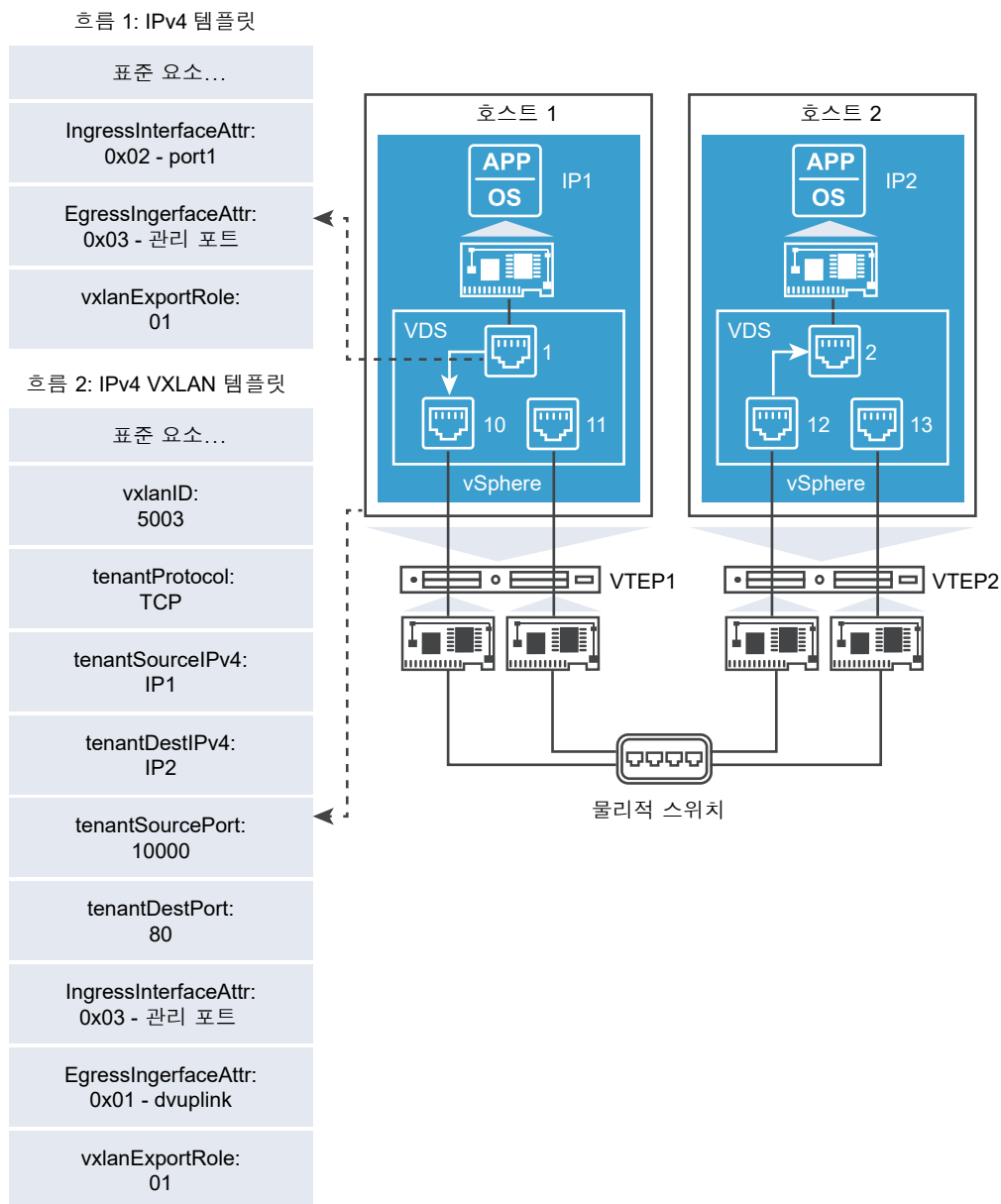


그림 22-2. 호스트 1의 흐름은 호스트 1에서 수집된 흐름을 보여 줍니다. IPv4 템플릿에는 수신 및 송신 포트와 표준 요소에 대한 추가 정보가 포함되어 있습니다.

ingressInterfaceAttr 텍스트 상자 0x02는 가상 시스템이 연결된 액세스 포트임을 나타냅니다. 액세스 포트 번호는 템플릿의 *ingressInterface* 매개 변수에 할당됩니다.

0x03의 *egressInterfaceAttr* 값은 VXLAN 터널 포트라는 사실과 연결된 포트 번호가 관리 VMKNic 포트임을 나타냅니다. 이 포트 번호는 템플릿의 *egressInterface* 매개 변수에 할당됩니다.

IPv4 VXLAN 템플릿에는 VXLAN ID, 내부 소스 및 대상 IP/포트 및 프로토콜에 대한 추가 정보가 포함되어 있습니다. 수신 및 송신 인터페이스는 각각 *VXLAN 터널 포트* 및 *dvuplink* 포트입니다.

그림 22-3. 호스트 2의 흐름

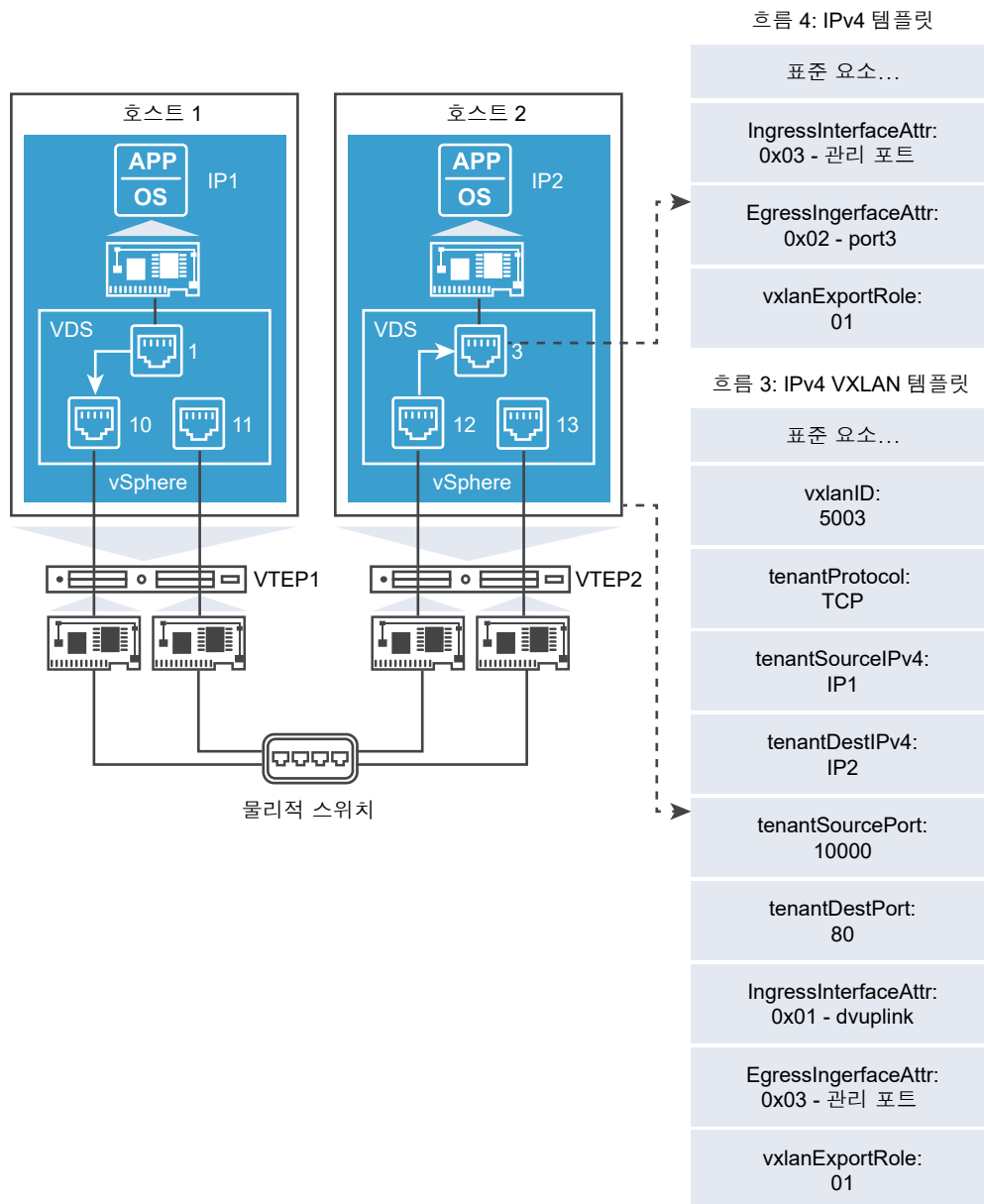


그림 22-2. 호스트 1의 흐름은 호스트 2에서 나타나는 흐름을 보여 줍니다.

그림 22-2. 호스트 1의 흐름 템플릿은 수신 및 송신 특성과 포트 번호에서만 그림 22-2. 호스트 1의 흐름과 다릅니다.

이 템플릿을 통해 제공하는 추가 정보는 수집기 도구 벤더가 외부 VXLAN 흐름과 내부 가상 시스템 흐름 간의 상관 관계를 파악하는 데 도움이 됩니다.

수집기 도구 벤더에 대한 정보

vSphere Distributed Switch에 대한 IPFIX 지원은 가상 시스템 흐름 및 VXLAN 흐름에 대한 필수 가시성을 제공합니다. 다른 타사 수집기 도구를 이용하는 경우, 템플릿에서 사용할 수 있는 추가 정보를 사용하여 내부 및 외부 흐름 간 상관 관계와 포트 연결을 제공할 수 있습니다.

다음 섹션에서는 VXLAN 템플릿에 추가된 새 매개 변수를 디코딩하는 방법에 대한 세부 정보를 제공합니다. IANA는 IPFIX 정보 요소 및 해당 요소 ID를 정의합니다. <http://www.iana.org/assignments/ipfix/ipfix.xml>에서 표준 요소 ID 목록을 찾을 수 있습니다.

VXLAN 템플릿의 일부로 정의된 모든 새 요소는 해당 새 요소 ID를 갖습니다.

이러한 사용자 지정 매개 변수 또는 요소는 VXLAN 및 내부 흐름에 대한 추가 정보를 제공합니다. 다음은 새 요소 및 해당 ID입니다.

표 22-4. 사용자 지정 매개 변수

요소 ID	매개 변수 이름	데이터 유형	단위
880	tenantProtocol	unsigned8	1바이트
881	tenantSourceIPv4	ipv4Address	4바이트
882	tenantDestIPv4	ipv4Address	4바이트
883	tenantSourceIPv6	ipv6Address	16바이트
884	tenantDestIPv6	ipv6Address	16바이트
886	tenantSourcePort	unsigned16	2바이트
887	tenantDestPort	unsigned16	2바이트
888	egressInterfaceAttr	unsigned16	2바이트
889	vxlanExportRole	unsigned8	1byte
890	ingressInterfaceAttr	unsigned16	2바이트

참고 엔터프라이즈 ID는 위에 정의된 모든 사용자 지정 요소에 추가됩니다. VMware의 엔터프라이즈 ID는 6876입니다.

다음 표에서는 요소의 전체 ID 목록 예를 보여 줍니다. <http://www.iana.org/assignments/ipfix/ipfix.xml>에서 표준 요소 ID에 대한 데이터 유형 및 단위를 찾을 수 있습니다.

요소 ID	매개 변수 이름
1	octetDeltaCount
2	packetDeltaCount

요소 ID	매개 변수 이름
4	protocolIdentifier
5	IPv4TOS
5	IPv6TOS
6	tcpFlags
7	sourceTransportPort
8	sourceIPv4Address
10	ingressInterface
11	destinationTransportPort
12	destinationIPv4Address
14	egressInterface
15	nextHopIPv4
27	sourceIPv6Address
28	destinationIPv6Address
53	maxTTL
61	flowDir
136	flowEndReason
152	flowStartSysUpTime
153	flowEndSysUpTime
210	paddingOctets
351	vxlanId
880	tenantProtocol
881	tenantSourceIPv4
882	tenantDestIPv4
883	tenantSourceIPv6
884	tenantDestIPv6
886	tenantSourcePort
887	tenantDestPort
888	egressInterfaceAttr
889	vxlanExportRole
890	ingressInterfaceAttr

애플리케이션 규칙 관리자

애플리케이션 규칙 관리자 도구는 기존 애플리케이션에 대해 보안 그룹 및 방화벽 규칙을 생성하여 응용 프로그램을 세분화하는 프로세스를 간소화합니다.

Flow Monitoring은 시스템 전반에서 장기적인 데이터 수집에 사용되지만 애플리케이션 규칙 관리자는 애플리케이션에 대한 목표 모델링에 사용됩니다.

애플리케이션 규칙 관리자 워크플로에는 다음 3단계가 있습니다.

- 1 애플리케이션을 형성하고 모니터링해야 하는 **VM(가상 시스템)**을 선택합니다. 일단 구성되면, **VM**의 정의된 **VNIC(Virtualized Network Interface Cards)** 집합에 대한 모든 수신 및 송신 흐름이 모니터링됩니다. 한 번에 흐름을 수집하는 세션이 **5개**까지 가능합니다.
- 2 흐름 테이블을 생성하려면 모니터링을 중지합니다. 흐름이 분석되고 **VM** 간 상호 작용이 확인됩니다. 흐름 레코드가 제한된 작업 집합으로 이동되도록 흐름을 필터링할 수 있습니다.
- 3 흐름 테이블을 사용하여 보안 그룹, **IP** 집합, 서비스 및 서비스 그룹, 방화벽 규칙과 같은 그룹화 개체를 생성합니다.

모니터링 세션 생성

모니터링 세션은 지정된 세션에서 최대 **30개**의 **vNIC**에 대해 모든 수신 및 송신 흐름을 수집합니다.

사전 요구 사항

모니터링 세션을 시작하기 전에 모니터링해야 하는 **VM** 및 **vNIC**를 정의해야 합니다.

VMware Tools가 **Windows** 데스크톱 **VM**에서 실행 중이고 최신 상태여야 합니다.

선택한 **VM**은 방화벽이 사용하도록 설정된(제외 목록에 포함할 수 없음) 클러스터에 있어야 합니다.

선택한 **vNIC**에 적용되는 기본 방화벽 규칙인 "허용"이 모니터링 세션 기간에 생성되므로 **vNIC**에서 송수신되는 흐름이 다른 방화벽 규칙에 의해 삭제되지 않습니다.

절차

- 1 vSphere Web Client에 로그인한 다음 왼쪽 탐색 창에서 **[Networking & Security]**를 선택합니다.
- 2 **Flow Monitoring**을 선택합니다.
- 3 **애플리케이션 규칙 관리자(Application Rule Manager)** 탭을 선택합니다.
- 4 **새 세션 시작(Start New Session)**을 클릭합니다.
- 5 **새 세션 시작(Start New Session)** 대화 상자에서 세션의 이름을 입력합니다.
- 6 **vNIC** 또는 **VM**을 개체 유형으로 선택합니다.

사용 가능한 개체(Available Objects) 열이 사용 가능한 개체로 채워집니다.

- 7 모니터링하려는 **vNIC** 또는 **VM**을 두 번 클릭합니다. 선택한 **vNIC** 또는 **VM**이 **선택한 개체(Selected Objects)** 열로 이동됩니다.
- 8 **확인(OK)**을 클릭하여 흐름 수집을 시작합니다.
상태는 이제 **데이터 수집 중(Collecting Data)**이 됩니다. 수집되는 최신 흐름 집합이 흐름 테이블에 표시됩니다.
- 9 흐름 수집을 종료하려면 **중지(Stop)**를 클릭합니다.

결과

선택한 vNIC 및 VM에 대해 Flow Monitoring 세션이 생성되었습니다.

다음에 수행할 작업

흐름이 수집된 후에 흐름을 분석하십시오.

흐름 분석

Flow Monitoring 세션이 수집되면 결과가 분석되고, 개체 및 방화벽 규칙의 그룹화에 사용하도록 결과를 필터링할 수 있습니다.

분석된 흐름을 필터링하여 작업 집합의 흐름 수를 제한할 수 있습니다. 필터 옵션 아이콘은 오른쪽의 [처리된 보기] 드롭다운 메뉴 옆에 표시됩니다.

사전 요구 사항

분석하려면 먼저 Flow Monitoring 세션이 선택한 vNIC 또는 VM에서 수집되어 있어야 합니다.

절차

- 1 흐름이 수집되면 **분석(Analyze)**을 클릭합니다.

정의된 서비스가 확인되면 VM으로의 IP 주소 변환이 시작되고 중복된 항목은 제거됩니다.

- 2 분석이 완료되면 흐름에 대해 다음 데이터가 제공됩니다.

필드	옵션
방향	IN - 흐름이 입력 시드의 일부로 선택된 VM 및 vNIC 중 하나로 들어옵니다. OUT - 흐름이 입력 시드의 일부로 선택된 VM 및 vNIC 중 하나에서 생성됩니다. INTRA- 흐름이 입력 시드의 일부로 선택된 VM 및 vNIC 사이에 있습니다.
소스	VM 이름(흐름 레코드의 소스 IP 주소가 NSX 인벤토리의 한 VM으로 확인되는 경우). VM Tools가 해당 VM에서 사용되도록 설정된 경우에만 IP 주소를 VM으로 확인할 수 있습니다. 원시 IP(NSX 인벤토리에서 이 소스 IP 주소에 대해 발견된 VM이 없는 경우). 멀티캐스트 및 브로드캐스트 IP 주소는 VM으로 확인되지 않습니다. VM 수(예: 2개의 가상 시스템)(IP 주소가 다른 네트워크의 여러 VM에 매핑된 겹치는 IP 주소인 경우 사용자는 가상 시스템을 이 흐름 레코드와 관련된 올바른 가상 시스템으로 확인해야 함).
대상	소스 필드와 같은 값.
서비스	프로토콜/포트에 대한 NSX 정의의 서비스. 원시 프로토콜/포트(NSX Manager에 정의된 서비스가 없는 경우) 서비스의 수 (동일한 프로토콜/포트에 둘 이상의 서비스가 매핑되어 있고 사용자가 이를 흐름 레코드에 적용 가능한 하나의 서비스로 확인해야 하는 경우).

다음에 수행할 작업

분석된 흐름을 수정해서 추가로 사용자 지정할 수 있습니다. 그런 다음 분석된 흐름을 사용하여 방화벽 규칙을 생성합니다.

흐름 통합 및 사용자 지정

시스템 분석이 완료되면 분석된 흐름 테이블을 **처리된 보기(Processed View)**에서 사용할 수 있습니다. 사용자는 소스, 대상 및 서비스 필드를 변경하여 흐름을 추가로 통합할 수 있습니다. [흐름 레코드에서 서비스 사용자 지정](#) 및 [흐름 레코드에서 소스 및 대상 사용자 지정](#) 를 참조하십시오.

참고 처리된 보기

통합된 흐름이 다음 열이 있는 테이블에 표시됩니다.

필드	옵션
방향	<p>IN - 흐름이 입력 시드의 일부로 선택된 VM 및 vNIC 중 하나로 들어옵니다.</p> <p>OUT - 흐름이 입력 시드의 일부로 선택된 VM 및 vNIC 중 하나에서 생성됩니다.</p> <p>INTRA- 흐름이 입력 시드의 일부로 선택된 VM 또는 vNIC 사이에 있습니다.</p>
소스	<p>VM 이름(흐름 레코드의 소스 IP 주소가 NSX 인벤토리의 한 VM으로 확인되는 경우).</p> <p>원시 IP(NSX 인벤토리에서 이 소스 IP 주소에 대해 발견된 VM이 없는 경우). 멀티캐스트 및 브로드캐스트 IP는 VM으로 확인되지 않습니다.</p> <p>VM 수(IP 주소가 다른 네트워크의 여러 VM에 매핑된 겹치는 IP 주소인 경우 사용자는 여러 VM을 이 흐름 레코드와 관련된 단일 VM으로 확인해야 함).</p>
대상	소스 필드와 같은 값.
서비스	<p>프로토콜/포트에 대한 NSX 정의 서비스.</p> <p>원시 프로토콜/포트(NSX Manager에 정의된 서비스가 없는 경우)</p> <p>서비스의 수 (동일한 프로토콜/포트에 둘 이상의 서비스가 매핑되어 있고 사용자가 이를 흐름 레코드에 적용 가능한 하나의 서비스로 확인해야 하는 경우).</p>

보다 쉬운 규칙 생성을 위해 흐름 테이블을 편집하고 흐름을 통합할 수 있습니다. 예를 들어 소스 필드를 ANY로 바꿀 수 있습니다. HTTP 및 HTTPS를 사용하여 흐름을 수신하는 여러 VM을 HTTP 및 HTTPS 서비스를 모두 포함하는 “WEB-Service” 서비스 그룹으로 바꿀 수 있습니다. 이렇게 하여 여러 흐름이 비슷해 보이고, 방화벽 규칙으로 쉽게 변환될 수 있는 흐름 패턴이 나타날 수 있습니다.

흐름 테이블의 각 셀을 수정할 수 있지만 셀이 자동으로 채워지지는 않습니다. 예를 들어 IP 주소 196.1.1.1이 DHCP-서버 IPSet에 추가된 후에 해당 IP가 나올 때마다 DHCP-서버 그룹을 표시하도록 자동으로 채워지지는 않습니다. IP 주소의 모든 인스턴스를 IPSet으로 바꿀지 묻는 메시지가 표시됩니다. 이렇게 하면 해당 IP를 여러 IPSet 그룹의 부분으로 유연하게 지정할 수 있습니다.

참고 통합된 보기

통합된 보기는 오른쪽 모서리의 드롭다운 목록에서 액세스할 수 있습니다. 통합된 보기는 중복된 흐름을 제거하고 최소 흐름 수를 표시합니다. 이 보기는 방화벽 규칙을 생성하는 데 사용될 수 있습니다.

[방향] 열 왼쪽 구석의 화살표를 클릭하면 다음과 같은 해당 관련 원시 흐름 정보가 표시됩니다.

- 내부 흐름의 경우 원시 데이터가 있는 해당 IN 및 OUT 흐름이 표시됩니다.
- 레코드로 통합된 모든 원시 흐름의 원본 소스 IP, 대상 IP, 포트 및 프로토콜 정보
- ALG 흐름의 경우 제어 흐름의 해당 데이터가 표시됩니다.

흐름 레코드에서 서비스 사용자 지정

서비스 흐름 셀은 사용자별로 개별 셀에 사용자 지정할 수 있습니다.

흐름 분석 후에 사용자는 정의되지 않은 프로토콜/포트 조합을 연결하고 서비스를 생성할 수 있습니다. 수집된 흐름에 나열된 서비스에 대해 서비스 그룹을 생성할 수 있습니다. 흐름 레코드 수정에 대한 자세한 내용은 [흐름 통합 및 사용자 지정](#)을 참조하십시오.

사전 요구 사항

흐름 데이터는 vNIC 및 VM 집합에서 수집되어 있어야 합니다. [모니터링 세션 생성](#)를 참조하십시오.

절차

- ◆ 흐름 상태가 **분석 완료(Analysis Completed)**이면 흐름 테이블은 **처리된 보기(Processed View)**에서 데이터로 채워집니다. 셀 데이터를 사용자 지정하려면 셀 위로 커서를 가져갑니다. 셀의 오른쪽 모서리에 톱니 바퀴 아이콘이 나타납니다. **서비스(Service)** 열에서 톱니 바퀴 아이콘을 클릭하고 다음 옵션 중 하나를 선택합니다.

옵션	설명
서비스 확인	포트 및 프로토콜이 여러 서비스로 변환된 경우 이 옵션을 사용하여 올바른 서비스를 선택합니다.
서비스 생성 및 바꾸기	<p>서비스를 추가하려면:</p> <ul style="list-style-type: none"> a 서비스의 이름(name)을 입력합니다. b 드롭다운 목록에서 프로토콜을 선택합니다. c 서비스의 대상 포트를 입력합니다. d 고급 옵션(Advanced options)을 클릭하여 서비스의 소스 포트를 입력합니다. 소스 포트는 새 수신 연결 및 데이터 스트림을 추적하는 데 사용됩니다. e 옵션 - 기본 범위에서 볼 수 있도록 상속 사용(Enable inheritance to allow visibility at underlying scopes)을 선택하여 일반 그룹을 생성하거나, 개별 Edge 수준에서 조건을 재사용할 수 있습니다. f 확인(OK)을 클릭하면 새 서비스가 생성된 후 [서비스] 열에서 채워집니다. 정의되지 않은 동일한 포트 및 프로토콜 조합을 갖는 다른 흐름 레코드가 있는 경우 이러한 레코드를 모두 새로 생성된 서비스로 바꿀지 묻는 메시지가 표시됩니다. 이 메시지는 분석 단계에서 발견된 정의되지 않은 서비스의 흐름에만 표시됩니다.
서비스 그룹 생성 및 바꾸기	<p>포함된 흐름에서 해당 서비스가 있는 새 서비스 그룹을 생성할 수 있습니다. 생성한 후에는 새 서비스 그룹이 서비스를 대체합니다. 서비스 그룹을 추가하려면:</p> <ul style="list-style-type: none"> a 서비스 그룹의 이름(name)을 입력합니다. b 선택 사항 - 서비스 그룹에 대한 설명을 입력합니다. c 개체 유형(Object type)을 선택합니다. d 서비스 그룹에 추가하려는 사용 가능한 개체를 선택하고 화살표를 클릭하여 개체를 [선택한 개체] 열로 이동합니다. e 새 서비스 그룹이 생성되고 [서비스] 열에 채워집니다.
서비스를 임의의 서비스로 바꾸기	특정 서비스를 임의의 서비스로 바꿉니다.

옵션	설명
서비스를 서비스 그룹으로 바꾸기	<p>선택한 서비스가 여러 서비스 그룹의 멤버인 경우 적용할 특정 서비스 그룹을 선택합니다.</p> <p>a 사용 가능한 개체 목록에서 원하는 서비스 그룹을 클릭합니다.</p> <p>b 확인(OK)을 클릭합니다.</p>
프로토콜 및 포트 되돌리기	모든 셀 수정 내용을 원래 데이터로 되돌립니다.

결과

변경된 흐름 레코드의 측면에는 분홍색 표시줄이 있습니다. 커서를 수정된 셀 위로 가져가면 녹색 확인 표시가 나타납니다. 확인 표시를 클릭하면 해당 셀에 대해 이전 및 새 값이 포함된 팝업 창이 표시됩니다. 수정된 흐름 레코드는 방화벽 규칙으로 더 쉽게 변환됩니다.

다음에 수행할 작업

그런 다음 흐름 레코드를 사용하여 방화벽 규칙을 생성할 수 있습니다.

흐름이 수정된 후에는 흐름을 추가로 그룹화하여 최소 단위의 고유 작업 집합을 만들 수 있습니다. **처리된 보기(Processed View)**는 서비스 그룹 및 IPSet을 생성하고 흐름을 수정하는 데 사용됩니다. **통합된 보기(Consolidated view)**는 이러한 수정된 흐름을 추가로 압축하여 방화벽 규칙을 더 쉽게 만들 수 있게 합니다.

흐름 레코드에서 소스 및 대상 사용자 지정

소스 및 대상 흐름 셀은 사용자별로 개별 셀에 사용자 지정할 수 있습니다.

흐름 분석이 완료되면 사용자는 흐름 셀을 사용자 지정할 수 있습니다.

사전 요구 사항

흐름 데이터는 vNIC 및 VM 집합에서 수집되어 있어야 합니다. [모니터링 세션 생성](#) 항목을 참조하십시오.

절차

- ◆ 흐름 상태가 **분석 완료(Analysis Completed)**이면 흐름 테이블이 데이터로 채워집니다. 셀 데이터를 사용자 지정하려면 셀 위로 커서를 가져갑니다. 셀의 오른쪽 모서리에 톱니 바퀴 아이콘이 나타납니다. **소스(Source)** 또는 **대상(Destination)** 열에서 톱니 바퀴 아이콘을 클릭하고 다음 옵션 중 하나를 선택합니다.

옵션	설명
VM 확인	여러 VM이 동일한 IP 주소를 가질 경우 이 옵션을 사용할 수 있습니다. 이 옵션은 흐름 레코드의 해당 VM 이름을 선택하는 데 사용됩니다.
임의 항목으로 바꾸기	소스에 누구나 액세스할 수 있게 하려면 임의의 소스 IP 주소를 사용할 수 있습니다. 다른 모든 경우에는 소스 주소를 지정해야 합니다. 대상 IP 주소의 대상 값을 구성하는 것은 바람직하지 않습니다.
멤버 자격으로 바꾸기	VM이 보안 그룹에 속할 경우 보안 그룹이 여기에 표시되며 VM 이름 대신 사용될 수 있습니다.

옵션	설명
보안 그룹 생성	<p>a 보안 그룹의 이름(선택 사항) 및 설명을 입력합니다.</p> <p>b 다음(Next)을 클릭합니다.</p> <p>c 생성할 보안 그룹에 추가되기 위해 개체가 충족해야 하는 조건을 정의합니다. 이렇게 하면 검색 기준과 일치하기 위해 지원되는 여러 매개 변수를 사용하여 필터 조건을 정의함으로써 가상 시스템을 포함할 수 있습니다.</p> <p>d 보안 그룹에 추가할 하나 이상의 리소스를 선택합니다. 보안 그룹에 리소스를 추가하면 연결된 모든 리소스가 자동으로 추가됩니다. 예를 들어 가상 시스템을 선택하면 연결된 vNIC가 자동으로 보안 그룹에 추가됩니다. 다음 개체를 보안 그룹에 포함할 수 있습니다.</p> <p>클러스터</p> <p>논리적 스위치</p> <p>레거시 포트 그룹</p> <p>vApp</p> <p>데이터센터</p> <p>e 다음(Next)을 클릭합니다.</p> <p>f 보안 그룹에서 제외할 개체를 선택합니다. 여기에서 선택하는 개체는 동적 조건의 충족 여부에 상관없이 항상 보안 그룹에서 제외됩니다.</p> <p>g 다음(Next)을 클릭합니다.</p> <p>h 완료 준비(Ready to complete) 창에서 보안 그룹 세부 정보를 검토합니다. 완료(Finish)를 클릭합니다.</p>
기존 보안 그룹에 추가 및 바꾸기	<p>VM의 경우 선택한 VM이 여러 보안 그룹의 멤버인 경우 적용하려는 특정 보안 그룹을 선택합니다. 소스 또는 대상 필드에 IP 주소가 있으면 이 옵션을 사용할 수 없습니다. 원시 IP 주소의 경우 [기존 IPset에 추가 및 바꾸기] 옵션을 사용합니다.</p> <p>a 사용 가능한 개체 목록에서 원하는 서비스 그룹을 클릭합니다.</p> <p>b 확인(OK)을 클릭합니다.</p>
IPSet 생성 및 바꾸기	<p>IPset을 사용하면 한꺼번에 전체 IP 주소 집합에 방화벽 규칙을 적용할 수 있습니다.</p> <p>a IPSet의 이름을 입력합니다.</p> <p>b 선택 사항 - 설명을 입력합니다.</p> <p>c 새 IP 집합의 IP 주소 또는 주소 범위를 입력합니다.</p> <p>d 확인(OK)을 클릭합니다.</p>
기존 IPSet에 추가 및 바꾸기	<p>하나의 IP 주소가 여러 IPset의 일부일 수 있습니다. 표시되는 IP 주소를 다른 IP 주소로 바꾸려면 이 옵션을 사용합니다.</p> <p>a 사용 가능한 개체에서 원하는 IPset을 선택합니다.</p> <p>b 확인(OK)을 클릭합니다.</p>
초기 데이터로 되돌리기	모든 셀 수정 내용을 원래 데이터로 되돌립니다.

다음에 수행할 작업

Flow Monitoring에 따라 방화벽 규칙을 생성합니다.

애플리케이션 규칙 관리자에서 방화벽 규칙 생성

방화벽 규칙은 애플리케이션 규칙 관리자의 일부로 편집 및 삭제하고, 위아래로 이동할 수 있습니다.

사전 요구 사항

흐름 레코드가 분석된 후에 방화벽 규칙을 생성할 수 있습니다.

절차

- 1 흐름 세션을 엽니다. **처리된 보기(Processed View)**에 있는 경우 단일 흐름 셀을 마우스 오른쪽 버튼으로 클릭하거나 **shift+첫 번째 셀 > 마지막 셀**을 클릭한 후 마우스 오른쪽 버튼을 클릭합니다. **통합된 보기(Consolidated View)**에 있는 경우 흐름 셀을 선택하고 **작업(Action)** 아이콘을 클릭합니다. **방화벽 규칙 생성(Create Firewall rule)**을 선택합니다.

선택한 행 데이터에 따라 모든 셀이 채워진 **새 방화벽 규칙(New Firewall Rule)** 팝업 창이 나타납니다. 여러 셀을 선택한 경우 모든 소스, 대상, 서비스 개체가 규칙의 해당 필드에 추가됩니다.

- 2 새 규칙의 이름을 입력합니다.
- 3 (선택 사항) 다른 소스 또는 대상을 선택하려면 [소스] 또는 [대상] 상자 옆에 있는 **선택(Select)**을 클릭합니다. 사용 가능한 개체에서 새 소스 또는 대상을 지정하고 **확인(OK)**을 클릭합니다.
- 4 (선택 사항) 다른 서비스를 선택하려면 [서비스] 상자의 **선택(Select)**을 클릭합니다. 분산 방화벽은 FTP, CIFS, ORACLE TNS, MS-RPC 및 SUN-RPC 프로토콜에 대해 ALG(Application Level Gateway)를 지원합니다. Edge는 FTP에 대해서만 ALG를 지원합니다. 사용 가능한 개체에서 새 서비스를 지정하고 **확인(OK)**을 클릭합니다.
- 5 (선택 사항) 규칙을 다른 범위에 적용하려면 [적용 대상] 상자 옆에 있는 **선택(Select)**을 클릭합니다. 아래 표에서 설명한 대로 적절하게 선택하고 **확인(OK)**을 클릭하십시오. 기본적으로 해당 규칙은 처음에 마우스 오른쪽 버튼을 클릭한 VNIC에 적용됩니다.

규칙 적용 대상	작업
사용자 환경에서 준비된 모든 클러스터	이 규칙을 분산 방화벽이 설치된 모든 클러스터에 적용합니다 (Apply this rule on all clusters on which Distributed Firewall is enabled)를 선택하십시오. 확인(OK) 을 클릭하면 이 규칙에 대한 적용 대상 열에 분산 방화벽(Distributed Firewall) 이 표시됩니다.
하나 이상의 클러스터, 데이터센터, 분산 가상 포트 그룹, NSX Edge, 네트워크, 가상 시스템, vNIC 또는 논리적 스위치	<ol style="list-style-type: none"> 1 컨테이너 유형(Container type)에서 해당하는 개체를 선택하십시오. 2 사용 가능(Available) 목록에서 하나 이상의 개체를 선택하고 를 클릭하십시오.

규칙의 소스 및 대상 필드에 가상 시스템 및 vNIC가 있는 경우 규칙이 제대로 작동하려면 소스 및 대상 가상 시스템 및 vNIC를 **적용 대상(Applied To)**에 추가해야 합니다.

6 아래 표에 설명된 **작업(Action)**을 선택합니다.

작업	결과
허용	지정된 소스, 대상 및 서비스와의 트래픽을 허용합니다.
차단	지정된 소스, 대상 및 서비스와의 트래픽을 차단합니다.
거부	허용되지 않는 패킷에 대해 거부 메시지를 전송합니다. TCP 연결에 대해 RST 패킷이 전송됩니다. UDP, ICMP 및 기타 IP 연결에 대해 관리 목적으로 금지된 코드가 포함된 ICMP 메시지가 전송됩니다.

7 드롭다운 화살표를 클릭하여 규칙의 규칙 **방향(Direction)**을 지정합니다.

8 **확인(OK)**을 클릭합니다.

다음에 수행할 작업

방화벽 규칙을 게시합니다. [애플리케이션 규칙 관리자에서 방화벽 규칙 게시 및 관리](#)를 참조하십시오.

애플리케이션 규칙 관리자에서 방화벽 규칙 게시 및 관리

방화벽 규칙은 편집할 수 있으며, 애플리케이션 규칙 관리자에서 게시할 수 있습니다.

방화벽 규칙이 생성된 후에는 애플리케이션 규칙 관리자의 **방화벽 규칙(Firewall Rules)** 탭에서 관리할 수 있습니다.

사전 요구 사항

Flow Monitoring 세션에서 방화벽 규칙을 생성합니다.

절차

- ◆ Flow Monitoring 세션에서 방화벽 규칙을 생성한 후에 **방화벽 규칙(Firewall Rules)** 탭에 표시됩니다. 다음 옵션 중 하나를 선택합니다.

옵션	설명
게시	<ul style="list-style-type: none"> a 게시(Publish)를 클릭하여 생성된 방화벽 규칙을 게시합니다. 이 규칙은 새 섹션으로 게시됩니다. b 방화벽 규칙의 섹션 이름(Section Name)을 입력합니다. c 새 방화벽 섹션이 기존 방화벽 구성에 삽입될지 여부를 선택합니다. d 확인(OK)을 클릭합니다.
편집	방화벽 규칙을 편집하려면 연필 아이콘을 선택합니다.
삭제	방화벽 규칙을 삭제하려면 빨간색 X 아이콘을 선택합니다.

옵션	설명
아래쪽 화살표	규칙을 아래로 이동하려면 아래쪽 화살표 아이콘을 선택합니다.
위쪽 화살표	규칙을 위로 이동하려면 위쪽 화살표 아이콘을 선택합니다.

참고 방화벽 규칙이 **애플리케이션 규칙 관리자(Application Rule Manager)**에서 게시되면 섹션 이름이 **게시(Publish)** 버튼에 추가됩니다. 이후에 **애플리케이션 규칙 관리자(Application Rule Manager)**에서 게시될 때마다 **애플리케이션 규칙 관리자(Application Rule Manager)**에서 현재 사용 가능한 규칙으로 방화벽 구성의 기존 섹션을 재정의합니다.

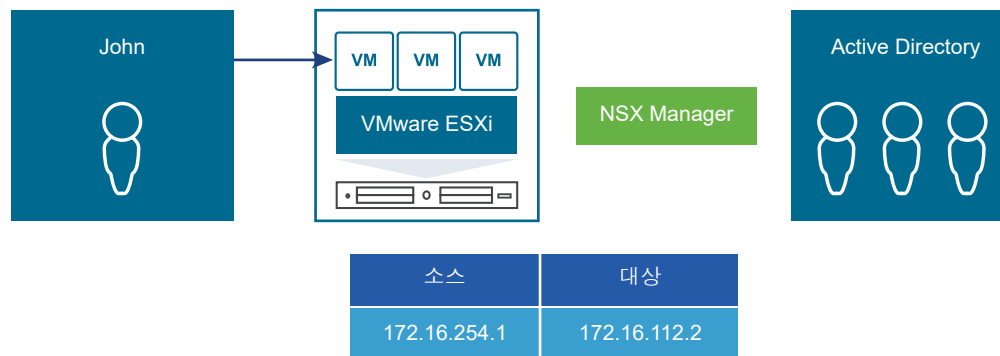
Activity Monitoring

Activity Monitoring을 사용하면 vCenter가 관리하는 Windows 데스크톱 가상 시스템에서 사용 중인 애플리케이션을 시각적으로 파악할 수 있습니다. 이러한 시각화 기능은 조직의 보안 정책이 올바르게 적용되고 있는지 확인할 수 있도록 지원합니다.

참고 NSX 6.3.0부터 NSX Activity Monitoring 기능이 더 이상 지원되지 않습니다. 사용자의 재량에 따라 이 기능을 계속 사용할 수 있지만 향후 릴리스에서는 NSX에서 이 기능이 제거될 것임을 유의하십시오. 6.3.0부터는 Activity Monitoring 대신 끝점 모니터링을 사용하는 것이 좋습니다.

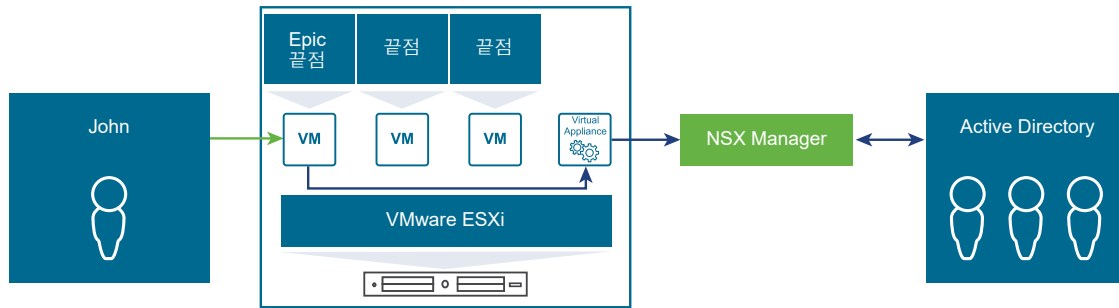
보안 정책은 어떤 사용자에게 어떤 애플리케이션에 대한 액세스 권한이 제공되는지를 명시합니다. 클라우드 관리자는 Activity Monitoring 보고서를 생성하여 자신이 설정한 IP 기반 방화벽 규칙이 의도한 대로 작동하는지 확인할 수 있습니다. Activity Monitoring은 사용자 및 애플리케이션 수준의 세부 정보를 제공함으로써 높은 수준의 보안 정책을 낮은 수준의 IP 주소 및 네트워크 기반 구현으로 변환합니다.

그림 22-4. 현재의 가상 환경



Activity Monitoring의 데이터 수집을 사용하도록 설정하면 보고서를 실행하여 인바운드 트래픽(사용자가 액세스하고 있는 가상 시스템 등) 및 아웃바운드 트래픽(리소스 활용도, 인벤토리 컨테이너 간 상호 작용, 서버에 액세스한 AD 그룹 등)을 볼 수 있습니다.

그림 22-5. Activity Monitoring을 사용하는 가상 환경



사용자	AD 그룹	App 이름	원본 VM 이름	대상 VM 이름	소스 IP	대상 IP
John	Doctors	Epic.exe	DoctorsWS13	EpicSVR3	172.16.254.1	172.16.112.2

중요 Linux VM에서는 Activity Monitoring이 지원되지 않습니다.

Activity Monitoring 설정

Activity Monitoring이 작동하려면 Guest Introspection 드라이버 설치, Guest Introspection VM 설치, NSX Activity Monitoring을 사용하도록 설정 등과 같은 여러 가지 필요한 절차를 수행해야 합니다. 필요한 경우 Service Composer를 사용하여 모니터링할 VM을 제어할 수 있습니다.

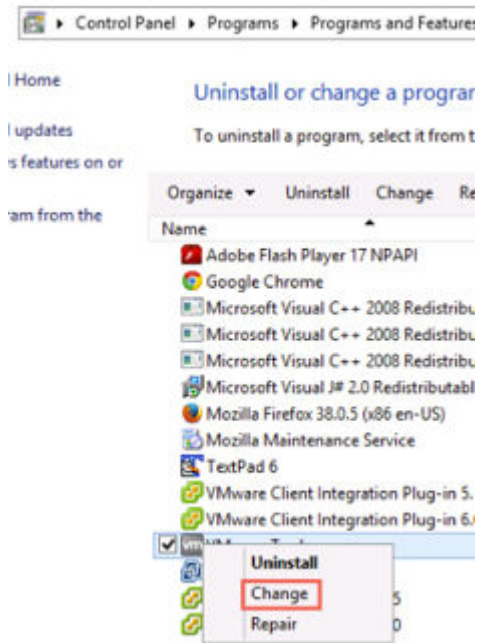
사전 요구 사항

- NSX가 설치되어 작동 중이어야 합니다.
- NSX Manager가 AD 서버에 연결되어 있어야 합니다. NSX Manager는 AD 서버에서 Windows VM 사용자와 일치하는 그룹을 가져옵니다.
- vCenter 인벤토리에 하나 이상의 Windows 데스크톱 VM이 포함되어 있어야 합니다.
- VMware Tools가 Windows 데스크톱 VM에서 실행 중이고 최신 상태여야 합니다.

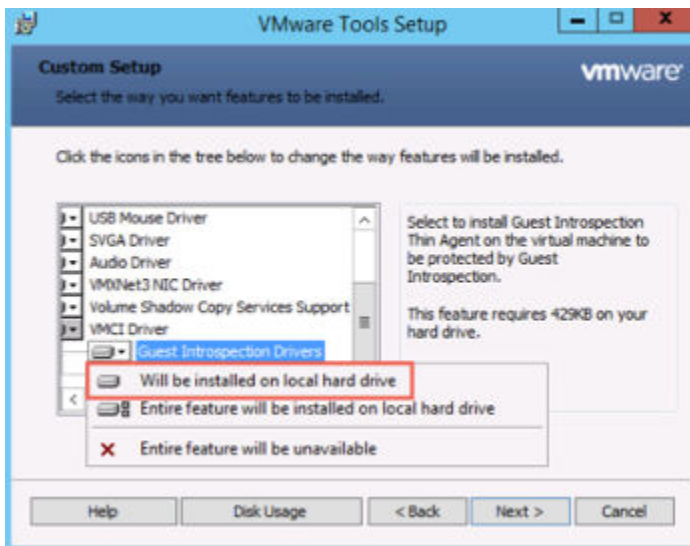
절차

- 1 vCenter 인벤토리의 Windows VM에 Guest Introspection 드라이버가 아직 설치되어 있지 않으면 설치합니다.

- a 제어판\프로그램\프로그램 및 기능(Control Panel\Programs\Programs and Features)으로 이동하고 **VMware Tools**를 마우스 오른쪽 버튼으로 클릭한 다음 **변경(Change)**을 선택합니다.



- b 수정(Modify)을 선택합니다.
- c **VMCI 드라이버(VMCI Driver)**에서 **Guest Introspection 드라이버 (Guest Introspection Drivers) > 로컬 하드 드라이브에 설치됩니다(Will be installed on local hard drive)**를 클릭합니다.



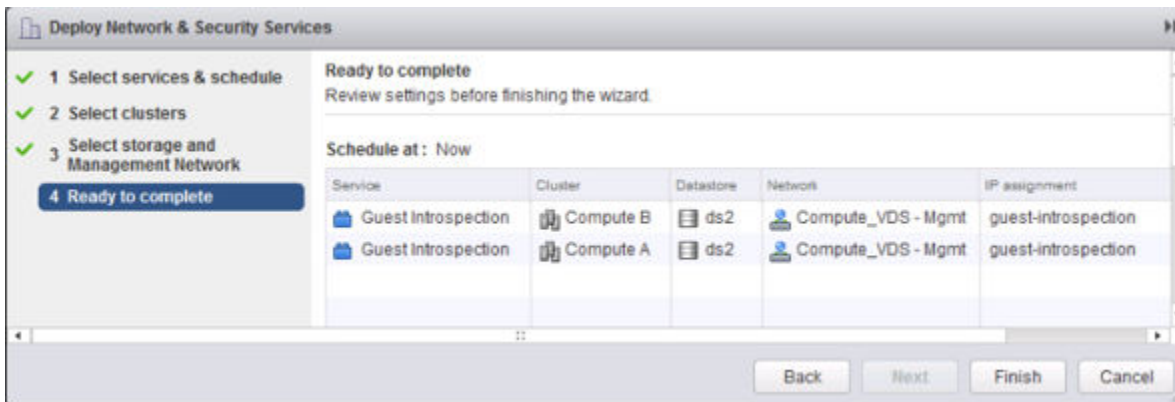
Guest Introspection 드라이버는 각 Windows VM에서 실행 중인 애플리케이션을 검색하고 해당 정보를 Guest Introspection VM으로 전송합니다.

2 Guest Introspection VM을 설치합니다.

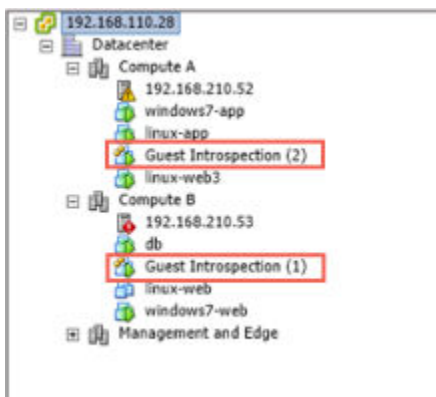
VMware Tools 설치를 처음 실행하는 경우 **사용자 지정(Custom)** 옵션을 선택합니다. VMCI 폴더에서 **Guest Introspection 드라이버(Guest Introspection Driver)**를 선택합니다. 드라이버는 기본적으로 선택되지 않습니다.

VMware Tools를 설치한 후 드라이버를 추가하려면:

- a vSphere Web Client에서 **네트워킹 및 보안 (Networking & Security) > 설치(Installation) > 서비스 배포(Service Deployments)**로 이동합니다.
- b 새 서비스 배포를 추가합니다.
- c **Guest Introspection**을 선택합니다.
- d Windows VM이 포함된 호스트 클러스터를 선택합니다.
- e 적절한 데이터스토어, 네트워크 및 IP 주소 지정 메커니즘을 선택합니다. Guest Introspection VM에 DHCP를 사용 중이지 않은 경우 IP 풀을 생성하여 할당합니다.

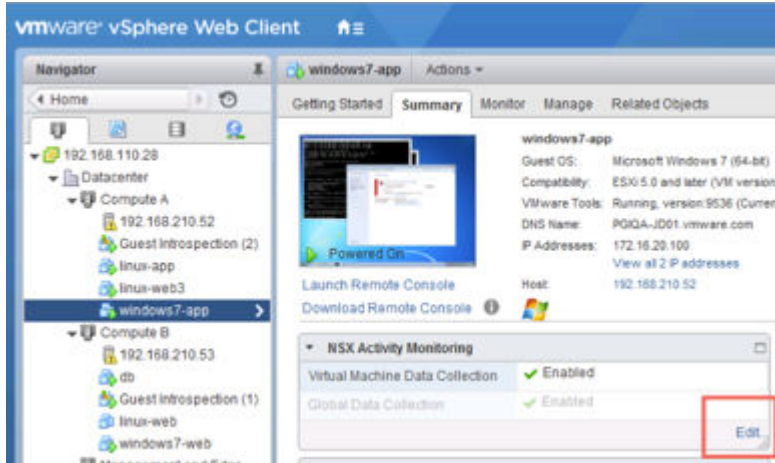


각 클러스터 내의 각 호스트에 하나씩 모두 두 개의 Guest Introspection VM이 설치됩니다.



3 Windows VM에서 Activity Monitoring을 사용하도록 설정합니다.

- a **호스트 및 클러스터(Hosts and Clusters)** 보기에서 Windows VM을 선택하고 **요약(Summary)** 탭을 선택합니다.
- b NSX Activity Monitoring에서 **편집(Edit)**을 클릭하고 **예(Yes)**를 클릭합니다.



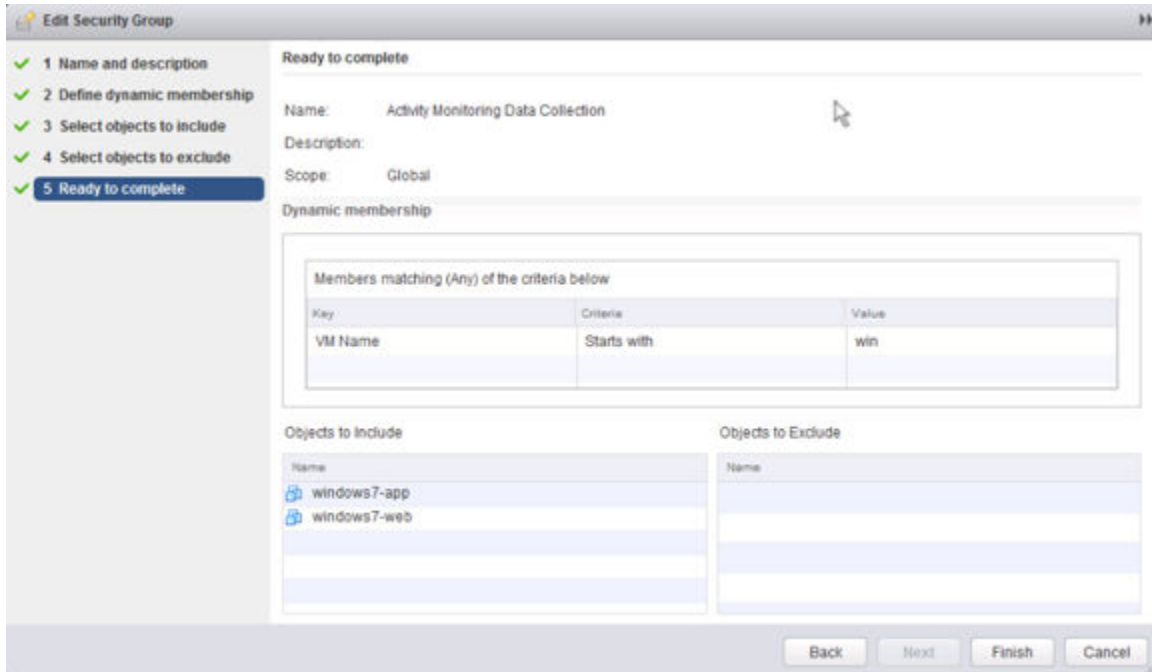
모니터링할 모든 Windows VM에 대해 이 단계를 반복합니다.

4 (선택 사항) 모니터링할 vCenter 개체 목록을 수정하거나 동적 멤버 자격 규칙을 정의합니다.

- a vSphere Web Client에서 **네트워킹 및 보안 (Networking & Security) > Service Composer**로 이동합니다.
- b **Activity Monitoring 데이터 수집(Activity Monitoring Data Collection) Security Group**을 편집합니다.
- c 새 Windows VM이 클러스터에 추가되도록 동적 멤버 자격 규칙을 정의합니다. 그러면 VM이 자동으로 모니터링됩니다..
- d Activity Monitoring Security Group에서 포함하거나 제외할 vCenter 개체를 선택합니다.

Activity Monitoring을 사용하도록 설정한 VM은 Activity Monitoring Security Group에 자동으로 포함됩니다.

이 예에서는 이름이 "win"으로 시작하는 모든 VM이 Activity Monitoring Security Group에 자동으로 추가됩니다. 즉, 해당 VM에서는 Activity Monitoring이 사용하도록 자동으로 설정됩니다.



Activity Monitoring 시나리오

이 섹션에서는 Activity Monitoring에 대한 가설 시나리오 몇 가지를 설명합니다.

애플리케이션에 대한 사용자 액세스

ACME Enterprise라는 가상의 회사는 승인된 사용자만 회사 자산의 특정 애플리케이션에 액세스할 수 있도록 허용합니다.

이 회사의 보안 정책에서 요구하는 사항은 다음과 같습니다.

- 권한이 있는 사용자만 비즈니스에 중요한 애플리케이션에 액세스할 수 있습니다.
- 권한 있는 애플리케이션만 회사 서버에 설치할 수 있습니다.
- 특정 네트워크에서 필요한 포트에만 액세스할 수 있습니다.

이 회사는 위의 정책에 따라 직원의 사용자 ID를 기반으로 한 액세스 제어를 통해 회사 자산을 보호해야 합니다. 우선 ACME Enterprise의 보안 작업자가 MS SQL 서버에 대해 관리자 액세스만 허용되는지를 확인할 수 있어야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)을 클릭한 후 Activity Monitoring을 클릭합니다.
- 3 인바운드 작업(Inbound Activity) 탭을 클릭합니다.
- 4 모든 직원의 액세스 권한을 보려면 아웃바운드 위치(Outbound from) 값을 검색된 모든 AD 그룹(All Observed AD Groups)으로 둡니다.

- 5 대상 가상 시스템(Where destination virtual machine)에서 포함(includes)을 선택하고 검색된 모든 대상 가상 시스템(all observed destination virtual machines)을 원래 선택된 상태로 둡니다.
- 6 대상 애플리케이션(And where destination application)에서 포함(includes)을 선택하고 검색된 모든 대상 애플리케이션(all observed destination applications)을 클릭한 다음 MS SQL Server를 선택합니다.
- 7 검색(Search)을 클릭합니다.
검색 결과에 관리 사용자만 MS SQL 서버에 액세스하는 것으로 나타납니다. Finance나 HR과 같은 다른 그룹은 이 서버에 액세스하지 않는 것을 확인할 수 있습니다.
- 8 이제 아웃바운드 위치(Outbound from) 값을 HR 및 Finance AD 그룹으로 설정하여 이 쿼리를 반대로 바꿀 수 있습니다.
- 9 검색(Search)을 클릭합니다.
레코드가 표시되지 않으며 따라서 HR 및 Finance AD 그룹의 사용자는 MS SQL 서버에 액세스할 수 없음을 알 수 있습니다.

데이터센터의 애플리케이션

ACME Enterprise는 회사 보안 정책에 따라 모든 데이터센터 애플리케이션을 볼 수 있어야 합니다. 이렇게 하면 기밀 정보를 캡처하거나 중요한 데이터를 외부로 빼돌리는 악성 애플리케이션을 쉽게 식별할 수 있습니다.

ACME Enterprise의 클라우드 관리자인 John은 Internet Explorer를 통해서만 SharePoint 서버에 액세스할 수 있고 FTP 또는 RDP를 사용하는 악성 애플리케이션은 서버에 액세스할 수 없도록 하려고 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)을 클릭한 후 Activity Monitoring을 클릭합니다.
- 3 VM 작업(VM Activity) 탭을 클릭합니다.
- 4 소스 VM 위치(Where source VM)에서 포함(includes)을 선택하고 검색된 모든 가상 시스템(All observed virtual machines)을 선택된 상태로 유지하여 데이터 센터의 모든 가상 시스템에서 들어오는 트래픽을 캡처합니다.
- 5 대상 VM(Where destination VM)에서 포함(includes)을 선택하고 검색된 모든 가상 시스템(All observed virtual machines)을 클릭한 다음 SharePoint 서버를 선택합니다.
- 6 검색(Search)을 클릭합니다.

결과

검색 결과에서 아웃바운드 App 제품 이름(Outbound App Product Name) 열을 보면 SharePoint 서버에 대한 모든 액세스는 Internet Explorer를 통해서만 이루어진 것으로 나타납니다. 상대적으로 유사한 검색 결과를 보면 다른 모든 액세스 방법을 차단하는 방화벽 규칙이 이 SharePoint 서버에 적용된 것으로 나타납니다.

또한 검색 결과에는 소스 그룹 대신 검색된 트래픽의 소스 사용자가 표시됩니다. 검색 결과에서 화살표를 클릭하면 사용자가 속한 **AD** 그룹과 같은 소스 사용자에 대한 세부 정보가 표시됩니다.

열려 있는 포트 확인

관리자 John이 권한이 있는 애플리케이션만 **ACME Enterprise**의 공유 지점 서버에 액세스하고 있음을 확인한다면, 회사에서 필요한 포트만 개방을 허용하도록 구성했음을 확인할 수 있습니다.

사전 요구 사항

데이터센터의 애플리케이션 시나리오에서 관리자 John은 **ACME Enterprise** 공유 지점 서버로 들어오는 트래픽을 확인했습니다. 이제 John은 공유 지점 서버에서 **MSSQL** 서버로 액세스할 때 항상 예상 프로토콜과 애플리케이션을 통과하는지 확인하려고 합니다.


절차

- 1 **홈으로 이동(Go Home)** 아이콘을 클릭합니다.
- 2 **vCenter 홈(vCenter Home)**을 클릭한 후 **가상 시스템(Virtual Machines)**을 클릭합니다.
- 3 **win_sharepoint**를 선택하고 **모니터(Monitor)** 탭을 클릭합니다.
- 4 **Activity Monitoring**을 클릭합니다.
- 5 **대상 위치(Where destination)**에서 **win2K-MSSQL**을 선택합니다.
- 6 **검색(Search)**을 클릭합니다.

결과

검색 결과에 공유 지점 서버에서 **MSSQL** 서버로 가는 트래픽이 나타납니다. **사용자(User)** 및 **아웃바운드 App(Outbound App)** 열에 시스템 프로세스만 **MSSQL** 서버에 연결하고 있음이 나타나며 이는 John이 예상한 바와 같습니다.

인바운드 포트(Inbound Port) 및 **애플리케이션(App)** 열에 모든 액세스가 대상 서버에서 실행되는 **MSSQL** 서버에 대한 액세스임이 표시됩니다.

검색 결과의 레코드 수가 너무 많아 웹 브라우저에서 모두 분석할 수 없으므로 John은 페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 전체 결과 집합을 내보내고 **CSV** 형식으로 파일을 저장할 수 있습니다.

데이터 수집 사용

Activity Monitoring 보고서를 실행하기 전에 **vCenter Server**에서 하나 이상의 가상 시스템에 대해 데이터 수집을 사용하도록 설정해야 합니다. 보고서를 실행하기 전에 먼저 사용하도록 설정된 가상 시스템이 활성화되었으며 네트워크 트래픽을 생성하고 있는지 확인하십시오.

또한 **NSX Manager**를 AD 도메인 컨트롤러에 등록해야 합니다. **NSX Manager**에 **Windows** 도메인 등록 항목을 참조하십시오.

활성 연결만 **Activity Monitoring**에 의해 추적됩니다. vNIC 수준에서 방화벽 규칙에 따라 차단된 가상 시스템 트래픽은 보고서에 반영되지 않습니다.

단일 가상 시스템에서 데이터 수집을 사용하도록 설정

Activity Monitoring 보고서를 실행하기 최소 5분 전에 데이터 수집을 사용하도록 설정해야 합니다.

사전 요구 사항

절차


- 1 vSphere Web Client에 로그인합니다.
- 2 vCenter를 클릭하고 **VM 및 템플릿(VMs and Templates)**을 클릭합니다.
- 3 왼쪽 인벤토리 패널에서 가상 시스템을 선택합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다.
- 5 왼쪽 패널에서 **NSX Activity Monitoring**을 클릭합니다.
- 6 **편집(Edit)**을 클릭합니다.
- 7 NSX Activity Monitoring 데이터 수집 설정 편집 대화상자에서 **예(Yes)**를 클릭합니다.

여러 가상 시스템에 대해 데이터 수집을 사용하도록 설정

Activity Monitoring 데이터 수집 Security Group은 미리 정의된 Security Group입니다. 한 번에 여러 개의 가상 시스템을 이 Security Group에 추가할 수 있으며 이러한 가상 시스템에서 모두 데이터 수집이 사용되도록 설정됩니다.

Activity Monitoring 보고서를 실행하기 최소 5분 전에 데이터 수집을 사용하도록 설정해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 후 **Service Composer**를 클릭합니다.
- 3 **Security Group(Security Groups)** 탭을 클릭합니다.
- 4 Activity Monitoring 데이터 수집 Security Group을 선택하고 **편집(Edit)**() 아이콘을 클릭합니다.
- 5 마법사에 따라 Security Group에 가상 시스템을 추가합니다.

이 Security Group에 추가한 모든 가상 시스템에서 데이터 수집이 사용되도록 설정되며 Security Group에서 제외된 가상 시스템에서는 사용되지 않도록 설정됩니다.

가상 시스템 작업 보고서 보기


사용 중인 환경에서 개별 가상 시스템이나 여러 가상 시스템의 송신 또는 수신 트래픽을 확인할 수 있습니다.

검색(Search)을 클릭하여 기본 검색 조건으로 빠르게 쿼리하거나, 사용자의 요구 사항에 따라 쿼리를 조정할 수 있습니다.

사전 요구 사항


- Guest Introspection이 운영 환경에 설치되어 있어야 합니다.
- NSX Manager에 도메인이 등록되어 있어야 합니다. 도메인 등록에 대한 정보는 [NSX Manager에 Windows 도메인 등록](#) 항목을 참조하십시오.
- 하나 이상의 가상 시스템에서 데이터 수집을 사용하도록 설정해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**을 클릭한 후 **Activity Monitoring**을 클릭합니다.
- 3 **VM 작업(VM Activity)** 탭을 클릭합니다.
- 4 **소스(Where source)** 옆의 링크를 클릭합니다. 아웃바운드 트래픽을 확인할 가상 시스템을 선택합니다. 선택한 가상 시스템을 보고서에 포함할지, 아니면 제외할지를 지정합니다.
- 5 **대상(Where destination)** 옆의 링크를 클릭합니다. 인바운드 트래픽을 확인할 가상 시스템을 선택합니다. 선택한 가상 시스템을 보고서에 포함할지, 아니면 제외할지를 지정합니다.
- 6 **기간(During period)**() 아이콘을 클릭하고 검색할 기간을 선택합니다.
- 7 **검색(Search)**을 클릭합니다.

결과

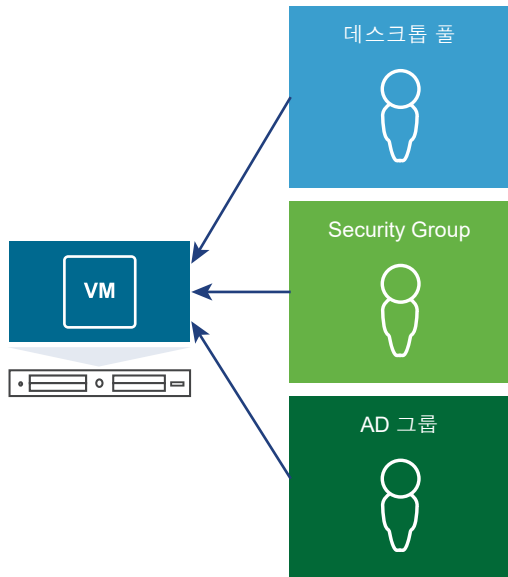
지정한 조건으로 필터링된 검색 결과가 표시됩니다. 행을 클릭하여 해당 행의 사용자에 대한 자세한 정보를 확인합니다.

페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 특정 레코드 또는 모든 레코드를 내보낸 후 디렉토리에 .csv 형식으로 저장할 수 있습니다.

인바운드 작업 보기

서버에 대한 모든 인바운드 작업을 데스크톱 풀, Security Group 또는 AD 그룹별로 볼 수 있습니다.

그림 22-6. 인바운드 작업 보기




검색(Search)을 클릭하여 기본 검색 조건으로 빠르게 쿼리하거나, 사용자의 요구 사항에 따라 쿼리를 조정할 수 있습니다.

사전 요구 사항

- Guest Introspection이 운영 환경에 설치되어 있어야 합니다.
- NSX Manager에 도메인이 등록되어 있어야 합니다. 도메인 등록에 대한 정보는 [NSX Manager에 Windows 도메인 등록](#) 항목을 참조하십시오.
- 하나 이상의 가상 시스템에서 데이터 수집을 사용하도록 설정해야 합니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**을 클릭한 후 **Activity Monitoring**을 클릭합니다.
- 3 **인바운드 작업(Inbound Activity)** 탭을 클릭합니다.
- 4 **원본 위치(Originating from)** 옆의 링크를 클릭합니다.
- 5 작업을 볼 사용자 그룹의 유형을 선택합니다.
- 6 **필터 유형(Filter type)**에서 그룹을 하나 이상 선택하고 확인을 클릭합니다.
- 7 **대상 가상 시스템(Where destination virtual machine)**에서 **포함(includes)** 또는 **제외(excludes)**를 선택하여 선택한 가상 시스템을 검색에 포함할지, 아니면 제외할지를 지정합니다.
- 8 **대상 가상 시스템(And where destination virtual machine)** 옆의 링크를 클릭합니다.
- 9 가상 시스템을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.

- 10 대상 애플리케이션(And where destination application)에서 포함(includes) 또는 제외(excludes)를 선택하여 선택한 애플리케이션을 검색에 포함할지, 아니면 제외할지를 지정합니다.
- 11 대상 애플리케이션(And where destination application) 옆의 링크를 클릭합니다.
- 12 애플리케이션을 하나 이상 선택하고 확인(OK)을 클릭합니다.
- 13 기간(During period)() 아이콘을 클릭하고 검색할 기간을 선택합니다.
- 14 검색(Search)을 클릭합니다.

결과

지정한 조건으로 필터링된 검색 결과가 표시됩니다. 결과 테이블 안에서 아무 곳이나 클릭하여 지정한 가상 시스템 및 애플리케이션에 액세스한 사용자 관련 정보를 봅니다.

페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 특정 레코드 또는 모든 레코드를 내보낸 후 디렉토리에 .csv 형식으로 저장할 수 있습니다.

아웃바운드 작업 보기

Security Group 또는 데스크톱 풀에서 실행 중인 애플리케이션을 확인한 후 보고서로 드릴다운하여 특정 사용자 그룹별로 아웃바운드에 연결한 클라이언트 애플리케이션을 확인할 수 있습니다. 또한 특정 애플리케이션에 액세스 중인 모든 사용자 그룹 및 사용자를 검색하여 사용 환경에서 ID 기반 방화벽을 조정해야 할지 여부를 결정할 수 있습니다.

그림 22-7. 아웃바운드 작업 보기




사전 요구 사항

- Guest Introspection이 운영 환경에 설치되어 있어야 합니다.
- NSX Manager에 도메인이 등록되어 있어야 합니다. 도메인 등록에 대한 정보는 [NSX Manager에 Windows 도메인 등록](#) 항목을 참조하십시오.
- 하나 이상의 가상 시스템에서 데이터 수집을 사용하도록 설정해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 네트워킹 및 보안(Networking & Security)을 클릭한 후 Activity Monitoring을 클릭합니다.
- 3 왼쪽 창에서 아웃바운드 작업(Outbound Activity) 탭을 선택합니다.
- 4 원본 위치(Originating from) 옆의 링크를 클릭합니다.


Guest Introspection을 통해 검색된 모든 그룹이 표시됩니다.

- 5 리소스 활용도를 표시할 사용자 그룹 유형을 선택합니다.
- 6 **필터(Filter)**에서 그룹을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.
- 7 **애플리케이션(Where application)**에서 **포함(includes)** 또는 **제외(excludes)**를 선택하여 선택한 애플리케이션을 검색에 포함할지, 아니면 제외할지를 지정합니다.
- 8 **애플리케이션(Where application)** 옆의 링크를 클릭합니다.
- 9 애플리케이션을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.
- 10 **대상(And where destination)**에서 **포함(includes)** 또는 **제외(excludes)**를 선택하여 선택한 가상 시스템을 검색에 포함할지, 아니면 제외할지를 지정합니다.
- 11 **대상(And where destination)** 옆의 링크를 클릭합니다.
- 12 가상 시스템을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.
- 13 **기간(During period)**() 아이콘을 클릭하고 검색할 기간을 선택합니다.
- 14 **검색(Search)**을 클릭합니다.

표시된 모든 정보를 보려면 오른쪽으로 스크롤하십시오.

결과

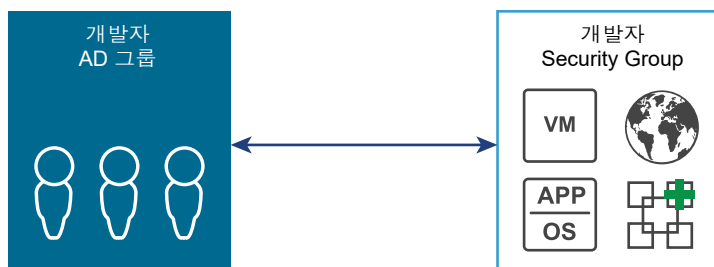
지정한 조건으로 필터링된 검색 결과가 표시됩니다. 행을 클릭하면 해당 AD 그룹 내에서 지정된 애플리케이션을 사용하여 지정된 가상 시스템에 액세스한 사용자에 대한 정보를 볼 수 있습니다.

페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 특정 레코드 또는 모든 레코드를 내보낸 후 디렉토리에 .csv 형식으로 저장할 수 있습니다.

인벤토리 컨테이너 간 상호 작용 보기

AD 그룹, Security Group 및/또는 데스크톱 풀과 같은 정의된 컨테이너 간에 전달되는 트래픽을 볼 수 있습니다. 이를 통해 공유 서비스에 대한 액세스를 식별 및 구성하고 인벤토리 컨테이너 정의, 데스크톱 풀 및 AD 그룹 간에 잘못된 구성된 관계를 해결할 수 있습니다.

그림 22-8. 컨테이너 간 상호 작용




검색(Search)을 클릭하여 기본 검색 조건으로 빠르게 쿼리하거나, 사용자의 요구 사항에 따라 쿼리를 조정할 수 있습니다.

사전 요구 사항


- Guest Introspection이 운영 환경에 설치되어 있어야 합니다.
- NSX Manager에 도메인이 등록되어 있어야 합니다. 도메인 등록에 대한 정보는 [NSX Manager에 Windows 도메인 등록](#) 항목을 참조하십시오.
- 하나 이상의 가상 시스템에서 데이터 수집을 사용하도록 설정해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**을 클릭한 후 **Activity Monitoring**을 클릭합니다.
- 3 왼쪽 창에서 **컨테이너 간 상호 작용(Inter Container Interaction)** 탭을 선택합니다.
- 4 **원본 위치(Originating from)** 옆의 링크를 클릭합니다.
Guest Introspection을 통해 검색된 모든 그룹이 표시됩니다.
- 5 리소스 활용도를 표시할 사용자 그룹 유형을 선택합니다.
- 6 **필터(Filter)**에서 그룹을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.
- 7 **대상(Where the destination is)**에서 **같음(is)** 또는 **같지 않음(is not)**을 선택하여 선택한 그룹을 검색에 포함할지, 아니면 제외할지를 지정합니다.
- 8 **대상(Where the destination is)** 옆의 링크를 클릭합니다.
- 9 그룹 유형을 선택합니다.
- 10 **필터(Filter)**에서 그룹을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.
- 11 **기간(During period)**() 아이콘을 클릭하고 검색할 기간을 선택합니다.
- 12 **검색(Search)**을 클릭합니다.

결과

지정한 조건으로 필터링된 검색 결과가 표시됩니다. 행을 하나 클릭하여 지정한 컨테이너에 액세스한 사용자 관련 정보를 봅니다.

페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 특정 레코드 또는 모든 레코드를 내보낸 후 디렉토리에 .csv 형식으로 저장할 수 있습니다.

예제: 인벤토리 컨테이너 간 상호 작용 쿼리

- 허용되는 통신 확인
vCenter 인벤토리에 컨테이너를 정의하고 해당 컨테이너 간의 통신을 허용하는 규칙을 추가한 경우 **원본 위치(Originating from)** 및 **대상(Where the destination is)** 필드에 지정된 두 컨테이너에서 이 쿼리를 실행하여 규칙이 작동하는지 확인할 수 있습니다.
- 거부된 통신 확인

vCenter 인벤토리에 컨테이너를 정의하고 해당 컨테이너 간의 통신을 거부하는 규칙을 추가한 경우 **원본 위치(Originating from)** 및 **대상(Where the destination is)** 필드에 지정된 두 컨테이너에서 이 쿼리를 실행하여 규칙이 작동하는지 확인할 수 있습니다.

■ 거부된 컨테이너 내부 통신 확인

컨테이너의 멤버가 같은 컨테이너의 다른 멤버와 통신하는 것을 허용하지 않는 정책을 구현한 경우 이 쿼리를 실행하여 해당 정책이 작동하는지 확인할 수 있습니다. **원본 위치(Originating from)** 및 **대상(Where the destination is)** 필드 모두에서 해당 컨테이너를 선택합니다.

■ 불필요한 액세스 제거

vCenter 인벤토리에 컨테이너를 정의하고 이러한 컨테이너 간의 통신을 허용하는 규칙을 추가했다고 가정해 보겠습니다. 두 컨테이너에는 다른 컨테이너와 전혀 상호 작용하지 않는 멤버가 있을 수 있습니다. 그러면 이러한 멤버를 적절한 컨테이너에서 제거하여 보안 제어 성능을 최적화할 수 있습니다. 이러한 목록을 검색하려면 **원본 위치(Originating from)** 및 **대상(Where the destination is)** 필드 모두에서 적절한 컨테이너를 선택합니다. **대상(Where the destination is)** 필드 옆의 **같지 않음(is not)**을 선택합니다.

아웃바운드 AD 그룹 작업 보기

정의된 Active Directory 그룹 멤버 간의 트래픽을 보고 이 데이터를 사용하여 방화벽 규칙을 미세 조정할 수 있습니다.


검색(Search)을 클릭하여 기본 검색 조건으로 빠르게 쿼리하거나, 사용자의 요구 사항에 따라 쿼리를 조정할 수 있습니다.

사전 요구 사항

- Guest Introspection이 운영 환경에 설치되어 있어야 합니다.
- NSX Manager에 도메인이 등록되어 있어야 합니다. 도메인 등록에 대한 정보는 [NSX Manager에 Windows 도메인 등록](#) 항목을 참조하십시오.
- 하나 이상의 가상 시스템에서 데이터 수집을 사용하도록 설정해야 합니다.


절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**을 클릭한 후 **Activity Monitoring**을 클릭합니다.
- 3 왼쪽 창에서 **AD 그룹 및 컨테이너(AD Groups & Containers)** 탭을 선택합니다.
- 4 **원본 위치(Originating from)** 옆의 링크를 클릭합니다.
Guest Introspection을 통해 검색된 모든 그룹이 표시됩니다.
- 5 검색에 포함하려는 사용자 그룹의 유형을 선택합니다.
- 6 **필터(Filter)**에서 그룹을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.

- 7 **AD 그룹(Where AD Group)**에서 **포함(includes)** 또는 **제외(excludes)**를 선택하여 선택한 AD 그룹을 검색에 포함할지, 아니면 제외할지를 지정합니다.
- 8 **AD 그룹(Where AD Group)** 옆의 링크를 클릭합니다.
- 9 AD 그룹을 하나 이상 선택하고 **확인(OK)**을 클릭합니다.
- 10 **기간(During period)**() 아이콘을 클릭하고 검색할 기간을 선택합니다.
- 11 **검색(Search)**을 클릭합니다.

결과

지정한 조건으로 필터링된 검색 결과가 표시됩니다. 행을 클릭하여 지정된 **Security Group** 또는 데스크톱 풀 내에서 네트워크 리소스에 액세스하는 지정된 **AD 그룹**의 멤버에 대한 정보를 봅니다.

페이지의 오른쪽 아래에 있는  아이콘을 클릭하여 이 페이지의 특정 레코드 또는 모든 레코드를 내보낸 후 디렉토리에 **.csv** 형식으로 저장할 수 있습니다.

데이터 수집 재정의

네트워크 오버로드와 같은 긴급 상황에서는 글로벌 수준에서 데이터 수집을 해제할 수 있습니다. 이 경우 다른 모든 데이터 수집 설정이 재정의됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **네트워킹 및 보안(Networking & Security)**을 클릭한 후 **Activity Monitoring**을 클릭합니다.
- 3 **설정(Settings)** 탭을 클릭합니다.
- 4 데이터 수집을 덮어쓰도록 설정할 **vCenter Server**를 선택합니다.
- 5 **편집(Edit)**을 클릭합니다.
- 6 **보고 데이터 수집(Collect reporting data)**을 선택 취소합니다.
- 7 **확인(OK)**을 클릭합니다.

끝점 모니터링 데이터 수집

끝점 모니터링을 사용하여 게스트 OS 내의 특정 프로세스를 프로세스에서 사용 중인 네트워크 연결에 매핑할 수 있습니다.

참고 데이터가 수집된 후에는 매일 오전 2시에 지워집니다. 데이터를 지우는 동안 모든 세션 전반에서 합한 흐름 레코드 수가 확인되고 2천만 개(또는 ~4GB) 이상의 모든 레코드가 삭제됩니다. 가장 오래된 세션부터 삭제되며 데이터베이스의 흐름 레코드 수가 1천 5백만 개 레코드 미만이 될 때까지 계속 삭제됩니다. 데이터를 지우는 동안 세션이 진행 중이면 일부 레코드가 유실될 수 있습니다.

사전 요구 사항

- 끝점 모니터링은 다음 Windows 운영 체제에서 지원됩니다.
Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 2008, Windows 2008 R2, Windows 2012, Windows 10, Windows 2016. Linux에서는 지원되지 않습니다.
- VM(가상 시스템)에 Guest introspection이 설치되어 있어야 합니다.
- VMware Tools가 Windows 데스크톱 VM에서 실행 중이고 최신 상태여야 합니다.
- 끝점 모니터링을 시작하려면 먼저 데이터 수집을 위해 VM이 20개 이하인 보안 그룹이 필요합니다. 자세한 내용은 [보안 그룹 생성](#) 항목을 참조하십시오.
- 끝점 모니터링 보고서를 실행하려면 vCenter Server의 하나 이상의 가상 시스템에 대해 데이터 수집을 사용하도록 설정해야 합니다. 보고서를 실행하기 전에 먼저 사용하도록 설정된 가상 시스템이 활성화되었으며 네트워크 트래픽을 생성하고 있는지 확인하십시오.

절차

- 1 vSphere Web Client에 로그인한 다음 왼쪽 탐색 창에서 **Networking & Security**를 선택합니다.
- 2 **끝점 모니터링(Endpoint Monitoring)**을 선택합니다.
- 3 [요약] 탭에서 **데이터 수집 시작(Start Collecting Data)**을 클릭합니다.
- 4 [보안 그룹에 대한 데이터 수집 시작] 팝업 창에서 데이터를 수집하려는 보안 그룹을 선택합니다. **확인(OK)**을 클릭합니다.
VM이 필드 상자에 표시됩니다.
- 5 데이터 수집을 **켄니다(ON)**.
- 6 **확인(OK)**을 클릭합니다.
주 끝점 모니터링 화면이 표시됩니다. 왼쪽 모서리에 상태가 [데이터 수집 중]으로 표시됩니다.
- 7 데이터 수집을 끝내려면 **데이터 수집 중지(Stop Collecting Data)**를 클릭합니다.
[끝점 모니터링] 화면의 [요약] 탭에 데이터가 채워져 표시됩니다.

끝점 모니터링

끝점 모니터링을 사용하여 특정 애플리케이션 프로세스 및 해당 관련 네트워크 연결을 표시할 수 있습니다.

.

요약 탭

데이터 수집이 완료되면 요약 화면에 NSX Manager의 세부 정보, 보안 그룹 및 수집된 데이터의 시간 슬롯이 표시됩니다. 실행 중인 VM(가상 시스템)의 수 및 트래픽을 생성하는 전체 프로세스 수가 첫 번째 상자에 표시됩니다. 실행 중인 가상 시스템 수를 클릭하면 아래에 설명된 [VM 흐름] 탭으로 이동됩니다. 트래픽을 생성하는 프로세스 수를 클릭하면 아래에 설명된 [프로세스 흐름] 탭으로 이동됩니다.

두 번째 상자에는 총 흐름 수가 있는 도넛형 차트가 표시됩니다. 흐름은 해당 패킷 유형, 소스 및 대상 IP, 포트 식별되는 네트워크 트래픽의 고유한 스트림입니다. 각 섹션 위에 커서를 놓으면 보안 그룹 내부 또는 외부의 흐름 수가 표시됩니다.

VM 흐름 탭

이 화면에는 다음을 포함하여 VM 내 흐름의 세부 정보가 표시됩니다.

- VM 이름 - 모니터링되는 VM의 이름
- 보안 그룹 내부 흐름 - 소스 또는 대상이 모니터링되는 보안 그룹 내부에 있는 경우 VM 간을 흐르는 트래픽
- 보안 그룹 외부 흐름 - 소스 또는 대상이 모니터링되는 보안 그룹 외부에 있는 경우 VM 간을 흐르는 트래픽
- 보안 그룹 외부 공유 서비스 흐름 - 모니터링되는 보안 그룹 외부의 DHCP, LDAP, DNS 또는 NTP 같은 공유 서비스 흐름
- 보안 그룹 내부 공유 서비스 흐름 - 모니터링되는 보안 그룹 내부의 DHCP, LDAP, DNS 또는 NTP 같은 공유 서비스

테이블의 특정 VM 이름을 클릭하면 다음을 나타내는 거품형 그래프가 표시됩니다.

- 동일한 보안 그룹에 있는 VM 간 흐름
- 공유 서비스를 포함하는 흐름
- 다른 보안 그룹 간 흐름

VM의 세부 정보를 보려면 거품을 클릭합니다. 자세한 흐름 보기에는 프로세스 이름, 각 프로세스에서 생성되는 흐름의 버전 및 수가 포함됩니다. 공유 서비스가 포함되어 있는 경우 특수 아이콘이 표시됩니다. 두 개의 VM 거품 사이의 선을 클릭하면 다음을 포함하여 두 VM 간 흐름의 프로세스 흐름 세부 정보가 표시됩니다.

- 소스 프로세스 - 트래픽을 생성하고 흐름을 시작하는 애플리케이션/exe의 이름
- 소스 버전 - 소스의 파일 버전
- 프로토콜 - TCP
- 대상 프로세스 - 흐름의 대상이 되는 프로세스의 서버 애플리케이션/exe의 이름
- 대상 포트 - 대상의 포트 번호

프로세스 흐름 탭

이 화면에는 흐름을 생성하는 모든 애플리케이션 목록이 표시됩니다. 테이블에는 다음이 표시됩니다.

- 프로세스 이름 - 트래픽을 생성하는 애플리케이션의 이름
- VM 이름
- 보안 그룹 내부 흐름 - 소스 또는 대상이 모니터링되는 보안 그룹 내부에 있는 경우 VM 간을 흐르는 트래픽

- 보안 그룹 외부 흐름 - 소스 또는 대상이 모니터링되는 보안 그룹 외부에 있는 경우 VM 간을 흐르는 트래픽
- 보안 그룹 내부 공유 흐름 - 모니터링되는 보안 그룹 내부의 공유 흐름
- 보안 그룹 외부 공유 흐름 - 모니터링되는 보안 그룹 외부의 공유 흐름

거품형 그래프는 선택된 VM의 프로세스 또는 애플리케이션에서 발생하는 흐름을 닷 모양으로 표시합니다. 프로세스 이름 및 버전을 표시하려면 아무 거품이나 클릭합니다. 선을 클릭하면 다음이 표시됩니다.

- 소스 VM - 클라이언트 프로세스를 호스팅하는 클라이언트 VM의 이름
- 소스 IP - 흐름의 IP 주소
- 프로토콜 - TCP
- 대상 VM - 서버 프로세스를 호스팅하는 서버 VM의 이름
- 대상 IP- 대상의 IP 주소
- 대상 포트 - 대상의 포트 번호

Traceflow

Traceflow는 패킷을 투입하고 패킷이 물리적 및 논리적 네트워크를 통과하는 동안 패킷의 위치를 관찰할 수 있게 해주는 문제 해결 도구입니다. 이러한 관찰을 통해 중지된 노드 식별 또는 대상의 패킷 수신을 차단하는 방화벽 규칙과 같은 네트워크에 대한 정보를 파악할 수 있습니다.

Traceflow 정보

Traceflow는 VDS(vSphere Distributed Switch) 포트에 패킷을 삽입하고 오버레이 및 언더레이 네트워크에서 물리적/논리적 엔티티(예: ESXi 호스트, 논리적 스위치 및 논리적 라우터)를 이동할 때 패킷 경로와 함께 다양한 관찰 지점을 제공합니다. 이를 통해 패킷이 대상에 도달하기까지의 경로 또는 반대로 도중에 패킷이 삭제되는 지점을 식별할 수 있습니다. 각 엔티티는 입력 및 출력에서의 패킷 처리를 보고하므로 패킷을 받을 때 또는 패킷을 전달할 때 문제가 발생하는지 확인할 수 있습니다.

Traceflow는 게스트 VM 스택 간을 이동하는 ping 요청/응답과는 다릅니다. Traceflow는 오버레이 네트워크를 탐색할 때 표시된 패킷을 관찰하는 일을 수행합니다. 각 패킷은 대상 게스트 VM에 도달하고 전달 가능해질 때까지 오버레이 네트워크를 이동할 때 모니터링됩니다. 하지만 삽입된 Traceflow 패킷은 실제로는 대상 게스트 VM에 절대로 전달되지 않습니다. 따라서 게스트 VM의 전원이 꺼져 있어도 Traceflow가 성공할 수 있습니다.

Traceflow에서는 다음 트래픽 유형을 지원합니다.

- 계층 2 유니캐스트
- 계층 3 유니캐스트
- 계층 2 브로드캐스트
- 계층 2 멀티캐스트

사용자 지정 헤더 필드 및 패킷 크기를 사용하여 패킷을 구성할 수 있습니다. **Traceflow**의 소스는 항상 가상 시스템 **vNIC**(가상 **NIC**)입니다. 대상 끝점은 **NSX** 오버레이 또는 언더레이의 임의 디바이스일 수 있습니다. 그렇지만 **NSX ESG**(Edge Services Gateway)의 상위(**north**)에 있는 대상은 선택할 수 없습니다. 대상은 동일한 서브넷에 있거나 **NSX** 논리적 분산 라우터를 통해 연결할 수 있어야 합니다.

소스 및 대상 **vNIC**가 동일한 계층 2 도메인에 있는 경우 **Traceflow** 작업이 계층 2로 간주됩니다. **NSX**에서 이는 소스 및 대상 **vNIC**가 동일한 **VXLAN** 네트워크 식별자(**VNI** 또는 세그먼트 **ID**)에 있음을 의미합니다. 예를 들어, 2개의 **VM**이 동일한 논리적 스위치에 연결된 경우 이런 상황이 발생합니다.

NSX 브리징이 구성되면 알 수 없는 계층 2 패킷이 항상 브리지로 전송됩니다. 일반적으로 브리지에서 이러한 패킷을 **VLAN**에 전달하고 해당 **Traceflow** 패킷을 전달됨으로 보고합니다. 패킷이 전달된 것으로 보고되었다고 해서 추적 패킷이 지정된 대상으로 전달되었음을 의미하는 것은 아닙니다.

계층 3 **Traceflow** 유니캐스트 트래픽의 경우 2개의 끝점이 서로 다른 논리적 스위치에 있고 다른 **VNI**를 갖고 있으며, **DLR**(논리적 분산 라우터)에 연결되어 있습니다.

멀티캐스트 트래픽의 경우 소스는 **VM vNIC**이고 대상은 멀티캐스트 그룹 주소입니다.

Traceflow 관찰에는 브로드캐스트된 **Traceflow** 패킷의 관찰이 포함될 수 있습니다. **ESXi** 호스트는 대상 호스트의 **MAC** 주소를 모를 경우 **Traceflow** 패킷을 브로드캐스트합니다. 브로드캐스트 트래픽의 경우 소스는 **VM vNIC**입니다. 브로드캐스트 트래픽의 계층 2 대상 **MAC** 주소는 **FF:FF:FF:FF:FF:FF**입니다. 방화벽 검사를 위한 올바른 패킷을 생성하기 위해 브로드캐스트 **Traceflow** 작업에 서브넷 접두사 길이가 필요합니다. 서브넷 마스크를 통해 **NSX**에서 패킷에 대한 **IP** 네트워크 주소를 계산할 수 있습니다.

경고 배포의 논리적 포트 수에 따라 멀티캐스트 및 브로드캐스트 **Traceflow** 작업에서 높은 트래픽 볼륨을 생성할 수 있습니다.

Traceflow를 사용하는 두 가지 방법은 **API** 또는 **GUI**를 통하는 것입니다. **API**는 **GUI**에서 사용하는 **API**와 동일하지만 예외로 **API**는 패킷 내에 정확한 설정을 지정할 수 있는 반면 **GUI**는 제한된 설정만 지정할 수 있습니다.

GUI를 사용하여 다음 값을 설정할 수 있습니다.

- 프로토콜---TCP, UDP, ICMP.
- TTL(Time-to-live). 기본값은 64 홉입니다.
- TCP 및 UDP 소스/대상 포트 번호. 기본값은 0입니다.
- TCP 플래그.
- ICMP ID 및 일련 번호. 둘 다 기본값은 0입니다.
- **Traceflow** 작업에 대한 만료 시간 초과(밀리초). 기본값은 10,000ms입니다.
- 이더넷 프레임 크기. 기본값은 프레임당 128바이트입니다. 최대 프레임 크기는 프레임당 1,000바이트입니다.
- 페이로드 인코딩. 기본값은 Base64입니다.
- 페이로드 값.

Traceflow를 사용하여 문제 해결

Traceflow를 유용하게 사용하는 여러 가지 시나리오가 있습니다.

Traceflow는 다음과 같은 시나리오에서 유용합니다.

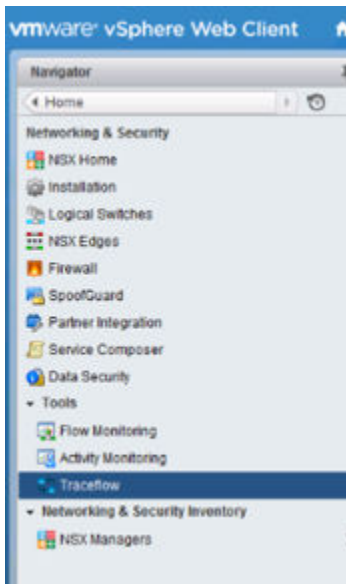
- 트래픽이 취하는 정확한 경로를 보기 위한 네트워크 실패 문제 해결
- 링크 활용도를 보기 위한 성능 모니터링
- 운영 환경에서 네트워크가 어떻게 작동하는지 보기 위한 네트워크 계획

사전 요구 사항

- Traceflow 작업을 위해서는 vCenter, NSX Manager, NSX Controller 클러스터 및 호스트의 netcpa user world 에이전트 간에 통신이 필요합니다.
- Traceflow가 예상대로 작동하려면 컨트롤러 클러스터가 연결되어 있고 정상 상태인지 확인해야 합니다.

절차

- 1 vCenter 웹 클라이언트에서 **홈 > Networking & Security > Traceflow(Home > Networking & Security > Traceflow)**로 이동합니다.



- 2 유니캐스트, 브로드캐스트, 멀티캐스트 중 트래픽 유형을 선택합니다.
- 3 소스 VM vNIC를 선택합니다.

VM이 Traceflow가 실행되는 동일한 vCenter Server에서 관리되는 경우, 목록에서 VM과 vNIC를 선택할 수 있습니다.

4 유니캐스트 Traceflow의 경우 대상 vNIC 정보를 입력합니다.

대상은 호스트, VM, 논리적 라우터, 또는 Edge Services Gateway 등 NSX 오버레이 또는 언더레이 내의 모든 장치의 vNIC가 될 수 있습니다. 대상이 VMware Tools를 실행하는 VM이고 Traceflow가 실행되는 동일한 vCenter Server에서 관리되는 경우, 목록에서 VM과 vNIC를 선택할 수 있습니다.

또는 대상 IP 주소(및 유니캐스트 계층 2 Traceflow의 경우 MAC 주소)를 입력해야 합니다. 이 정보는 장치 자체에서 장치 콘솔 또는 SSH 세션을 통해 얻을 수 있습니다. 예를 들어 Linux VM의 경우, Linux 터미널에서 `ifconfig` 명령을 실행하여 IP 및 MAC 주소를 얻을 수 있습니다. 논리적 라우터 또는 Edge Services Gateway의 경우, `show interface` CLI 명령에서 정보를 얻을 수 있습니다.

5 계층 2 브로드캐스트 Traceflow의 경우, 서브넷 접두사 길이를 입력합니다.

패킷은 MAC 주소만을 기준으로 변경됩니다. 대상 MAC 주소는 FF:FF:FF:FF:FF:FF입니다.

방화벽 검사에 대해 IP 패킷이 유효하려면 소스 및 대상 IP 주소가 모두 필요합니다.

6 계층 2 멀티캐스트 Traceflow의 경우, 멀티캐스트 그룹 주소를 입력합니다.

패킷은 MAC 주소만을 기준으로 변경됩니다.

IP 패킷이 유효하려면 소스 및 대상 IP 주소가 모두 필요합니다. 멀티캐스트의 경우, MAC 주소는 IP 주소에서 추정됩니다.

7 기타 필수 및 선택 설정을 구성합니다.

8 추적(Trace)을 클릭합니다.

예제: 시나리오

다음의 예는 단일 ESXi 호스트에서 실행되는 VM 2개를 포함하는 레이어 2 Traceflow를 보여줍니다. 두 개의 VM은 하나의 논리적 스위치에 연결되어 있습니다.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * web-02a - Network adapter 1 Change...
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Advanced Options

Protocol: TCP

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Received	esx-01a.corp.local	Firewall	Firewall
4	Forwarded	esx-01a.corp.local	Firewall	Firewall
5	Delivered	esx-01a.corp.local	vNIC	vNIC

다음의 예는 두 개의 서로 다른 ESXi 호스트에서 실행되는 VM 2개를 포함하는 레이어 2 Traceflow를 보여줍니다. 두 개의 VM은 하나의 논리적 스위치에 연결되어 있습니다.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **Unicast**

Source: web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: web-03a - Network adapter 1 Change...
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▼ Advanced Options

Protocol: **TCP**

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5	Received	esx-02a.corp.local	Firewall	Firewall
6	Forwarded	esx-02a.corp.local	Firewall	Firewall
7	Delivered	esx-02a.corp.local	vNIC	vNIC

다음의 예는 계층 3 Traceflow를 보여줍니다. 두 개의 VM은 논리적 라우터에 의해 분리된 두 개의 서로 다른 논리적 스위치에 연결되어 있습니다.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d4:2b

▶ Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
4		Received	esx-01a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-01a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-01a.corp.local	Logical Switch	DB-Tier-01
7		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
9		Received	esx-02a.corp.local	Firewall	Firewall
10		Forwarded	esx-02a.corp.local	Firewall	Firewall
11		Delivered	esx-02a.corp.local	vNIC	vNIC

다음 예는 단일 논리적 스위치에 연결된 VM 3개를 포함하는 배포에서 브로드캐스트 Traceflow를 보여줍니다. VM 중 두 개는 호스트 esx-01a에 있고, 세 번째 VM은 다른 호스트 esx-02a에 있습니다. 브로드캐스트는 호스트 192.168.210.53에 있는 VM 중 하나에서 전송됩니다.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **L2 Broadcast** ⚠ High volume of traffic may get generated for this traffic type.

Source: * web-01a - Network adapter 1 [Change...](#) Subnet Prefix Length: * **24**

IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 172.16.10.255, MAC: FF:FF:FF:FF:FF:FF

▶ Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

3 Delivered


Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
3		Received	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Forwarded	esx-01a.corp.local	Firewall	Firewall
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Delivered	esxmgt-02a.corp.local	vNIC	vNIC
5		Delivered	esx-01a.corp.local	vNIC	vNIC
5		Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5		Received	esx-02a.corp.local	Firewall	Firewall
6		Forwarded	esx-02a.corp.local	Firewall	Firewall
7		Delivered	esx-02a.corp.local	vNIC	vNIC



다음 예는 멀티캐스트가 구성된 배포에서 멀티캐스트 트래픽이 전송되는 경우 발생하는 현상을 보여줍니다.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: L2 Multicast  High volume of traffic may get generated for this traffic type.

Source:  web-01a - Network adapter 1 [Change...](#) Destination IP:  239.0.0.1 e.g. 239.0.0.1























































IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 239.0.0.1, MAC: 01:00:5e:00:00:01

▶ Advanced Options

[Trace](#)

Trace Result: Traceflow delivered observation(s) reported

3 Delivered

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	 esx-01a.corp.local	vNIC	 vNIC
1		Received	 esx-01a.corp.local	Firewall	 Firewall
2		Forwarded	 esx-01a.corp.local	Firewall	 Firewall
3		Received	 esx-01a.corp.local	Firewall	 Firewall
3		Forwarded	 esx-01a.corp.local	Physical	 esx-01a.corp.local
3		Forwarded	 esx-01a.corp.local	Physical	 esx-01a.corp.local
4		Received	 esxmgt-02a.corp.local	Physical	 esxmgt-02a.corp.local
4		Received	 esxmgt-02a.corp.local	Physical	 esxmgt-02a.corp.local
4		Received	 esxmgt-02a.corp.local	Physical	 esxmgt-02a.corp.local
4		Received	 esxmgt-02a.corp.local	Physical	 esxmgt-02a.corp.local
4		Forwarded	 esx-01a.corp.local	Firewall	 Firewall
4		Received	 esx-02a.corp.local	Physical	 esx-02a.corp.local
4		Received	 esx-02a.corp.local	Physical	 esx-02a.corp.local
5		Delivered	 esxmgt-02a.corp.local	vNIC	 vNIC
5		Delivered	 esx-01a.corp.local	vNIC	 vNIC
5		Received	 esx-02a.corp.local	Firewall	 Firewall
6		Forwarded	 esx-02a.corp.local	Firewall	 Firewall
7		Delivered	 esx-02a.corp.local	vNIC	 vNIC

다음 예는 분산 방화벽 규칙이 대상 주소로 보내진 ICMP트래픽을 차단하여 Traceflow가 손실된 경우 발생하는 현상을 보여줍니다. 대상 VM이 다른 호스트에 있다 하더라도 트래픽은 원래 호스트를 떠나지 않습니다.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-02a - Network adapter 1 Change...
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Destination: * web-03a - Network adapter 1 Change...
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▶ Advanced Options

Trace

Trace Result: Traceflow dropped observation(s) reported

1 Dropped

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Dropped	esx-01a.corp.local	Firewall	Firewall (Rule - 1013)

다음 예는 Traceflow 대상이 Edge Services Gateway의 다른 쪽에 있을 경우(예를 들어 인터넷 상의 IP 주소 또는 Edge Services Gateway를 통해 라우팅되어야 하는 내부 대상) 발생하는 현상을 보여줍니다.

Traceflow는 동일한 서브넷에 있거나 DLR(논리적 분산 라우터)을 통해 도달할 수 있는 대상에 대해 지원되므로 허용되지 않도록 설계되었습니다.

Select Traceflow Destination

Destination IP address should be on the same subnet or should be reachable via the Distributed Logical Router

IP Address: * 40.1.2.3

☐ Select Destination vNIC

Selected: web-03a - Network adapter 1

Q Filter

Available Objects

- app-01a
- db-01a
- web-01a
- web-02a

5 items

OK Cancel

다음 예는 Traceflow 대상이 다른 서브넷에 있으며 전원이 꺼져 있는 VM인 경우 발생하는 현상을 보여줍니다.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * app-01a - Network adapter 1 Change...
IP: 172.16.20.11, MAC: 00:50:56:ae:23:b9

Destination: * db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d...

► Advanced Options

Trace

Trace Result: No delivered or dropped observations reported

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-02a.corp.local	vNIC	vNIC
1		Received	esx-02a.corp.local	Firewall	Firewall
2		Forwarded	esx-02a.corp.local	Firewall	Firewall
3		Forwarded	esx-02a.corp.local	Logical Switch	App-Tier-01
4		Received	esx-02a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-02a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-02a.corp.local	Logical Switch	DB-Tier-01