Implantação e Configuração do Access Point

Unified Access Gateway 2.8

vmware®

Você pode encontrar a documentação técnica mais atualizada no site da VMware, em:

https://docs.vmware.com/br/

Caso tenha comentários sobre esta documentação, envie seu feedback para:

docfeedback@vmware.com

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

Conteúdo

Implantação e configuração do VMware Access Point 5

1 Preparando-se para implantar o Access Point 6
- Access Point como gateway seguro 6
- Utilizando o Access Point em vez de uma rede virtual privada 7
- Requisitos de sistema e de rede do Access Point 8
- Regras de firewall para appliances do Access Point baseados em DMZ 10
- Topologias do balanceamento de carga do Access Point 11
- Design da DMZ para o Access Point com várias placas de interface de rede 14

2 Implementação do appliance do Access Point 18
- Usando o assistente modelo do OVF para implementar o appliance do Access Point 18
  - Propriedades de implementação do Access Point 19
  - Implementar o Access Point usando o assistente modelo do OVF 20
- Configurando o Access Point a partir das páginas de configuração do administrador 23
  - Definir as configurações de sistema do Access Point 24
- Atualizar certificados assinados de servidor SSL 26

3 Usando o PowerSheel para implementar o Access Point 27
- Requisitos do sistema para a implementação do Access Point usando o PowerShell 27
- Usando o PowerShell para implementar o appliance do Access Point 28

4 Casos de uso de implementação 31
- Implementação do Access Point com o Horizon View e o Horizon Air Hybrid-Mode 31
  - Definir configurações do Horizon 35
- Implementação do Access Point como proxy reverso 37
  - Configurar o proxy reverso para o VMware Identity Manager 39
- Implementação do Access Point com o AirWatch Tunnel 40
  - Implementação do proxy de túnel para o AirWatch 41
  - Implementação de túnel por aplicativo com o AirWatch 41
  - Definir as configurações de túnel por aplicativo e de proxy para o AirWatch 42

5 Configuração do Access Point usando Certificados TLS/SSL 44
- Configurando certificados TLS/SSL para appliances do Access Point 44
  - Selecionando o tipo correto de certificado 44
  - Converter arquivos de certificado para o formato PEM de uma linha 46
  - Substituir o certificado padrão do servidor TLS/SSL pelo Access Point 48

Alterar os protocolos de segurança e os conjuntos de codificação utilizados para a comunicação TLS ou SSL 49

6 Configuração da autenticação em DMZ 51

Configurando a autenticação de certificado ou de cartão inteligente no appliance do Access Point 51

Configurar uma autenticação de certificado no Access Point 52

Obter Certificados de Autoridade de Certificação 54

Configurar a Autenticação RSA SecurID no Access Point 55

Configurando o RADIUS para o Access Point 56

Configurar a autenticação RADIUS 57

Configurando o RSA Adaptive Authentication no Access Point 58

Configurar o RSA Adaptive Authentication no Access Point 59

Gerar metadados SAML do Access Point 61

Criando um autenticador SAML utilizado por outros provedores de serviço 62

Copiar metadados SAML do provedor de serviços para o Access Point 62

7 Resolução de problemas de implementação do Access Point 64

Resolução de erros de implementação 64

Coletando registros do appliance do Access Point 66

Habilitação do modo de depuração 67

Implantação e configuração do VMware Access Point

A *Implantação e Configuração do Access Point* fornece informações sobre a implantação do projeto do VMware Horizon®, do VMware Identity Manager™ e do VMware AirWatch® que utiliza o VMware Access Point™ para acesso externo seguro aos aplicativos de sua organização. Esses aplicativos podem ser aplicativos do Windows, aplicativos de software como um serviço (SaaS) e áreas de trabalho. Este guia também fornece instruções para implementar os appliances virtuais do Access Point e alterar as definições de configuração após a implementação.

Público-alvo

Estas informações são concebidas para qualquer pessoa que deseja implementar e utilizar os appliances do Access Point. As informações foram escritas para administradores de sistema experientes do Linux e do Windows que estejam familiarizados com a tecnologia de máquina virtual e operações de centro de dados.

Preparando-se para implantar o Access Point

1

O Access Pointfunciona como um gateway seguro para usuários que desejam acessar áreas de trabalho e aplicativos remotos fora do firewall corporativo.

Este capítulo inclui os seguintes tópicos:

- Access Point como gateway seguro
- Utilizando o Access Point em vez de uma rede virtual privada
- Requisitos de sistema e de rede do Access Point
- Regras de firewall para appliances doAccess Pointbaseados em DMZ
- Topologias do balanceamento de carga do Access Point
- Design da DMZ para o Access Point com várias placas de interface de rede

Access Point como gateway seguro

O Access Point é um appliance de segurança de 7 camadas normalmente instalado em uma zona desmilitarizada (DMZ). O Access Point é usado para garantir que o único tráfego entrando no centro de dados corporativo seja o tráfego em nome de um usuário remoto fortemente autenticado.

O Access Point direciona solicitações de autenticação ao servidor apropriado e descarta qualquer solicitação não autorizada. Os usuários podem acessar somente os recursos que têm autorização para acessar.

Os appliances virtuais do Access Point também garantem que o tráfego de um usuário autenticado possa ser direcionado somente para os recursos da área de trabalho e aplicativos para os quais o usuário estiver autorizado. Esse nível de proteção envolve a inspeção específica de protocolos de área de trabalho e a coordenação de potenciais endereços de rede e políticas de mudança rápida para controlar o acesso de maneira precisa.

Os appliances do Access Point residem tipicamente dentro de uma DMZ e agem como um host de proxy para conexões no interior da rede confiável da sua empresa. Esse design fornece uma camada extra de segurança ao proteger áreas de trabalho virtuais, hosts de aplicativos e servidores da Internet voltada para o público.

O Access Point é um appliance de segurança protegido projetado especificamente para DMZ. As seguintes configurações de proteção são implementadas.

- Linux Kernel e patches de software atualizados
- Suporte múltiplo de NIC para tráfego de Internet e intranet
- SSH desabilitado
- Serviços desabilitados de FTP, Telnet, Rlogin ou Rsh
- Serviços indesejados desabilitados

Utilizando o Access Point em vez de uma rede virtual privada

O Access Point e as soluções de VPN genéricas são semelhantes, pois ambos garantem que o tráfego seja encaminhado para uma rede internal somente em nome de usuários fortemente autenticados.

As vantagens do Access Point sobre a VPN genérica incluem o seguinte.

- Access Control Manager. O Access Point aplica regras de acesso automaticamente. O Access Point reconhece as qualificações dos usuários e os endereços exigidos para se conectar internamente, o que pode mudar de forma rápida. Uma VPN faz a mesma coisa, porque a maioria das VPNs permite que um administrador configure as regras de conexão de rede para cada usuário ou grupo de usuários individualmente. Primeiro, isso funciona bem com uma VPN, mas exige um esforço administrativo significativo para manter as regras exigidas.
- Interface do Usuário. O Access Point não altera a interface do usuário simples do Horizon Client. Com o Access Point, quando o Horizon Client é iniciado, os usuários autenticados estão no ambiente do View deles e têm acesso controlado aos respectivos aplicativos e áreas de trabalho. Uma VPN exige que você configure o software VPN primeiro e o autentique separadamente antes de iniciar o Horizon Client.
- Desempenho. O Access Point é projetado para maximizar a segurança e o desempenho. Com o Access Point, os protocolos PCoIP, HTML access e WebSocket ficam seguros sem exigir encapsulamento adicional. VPNs são implementadas como VPNs SSL. Essa implementação atende aos requisitos de segurança e com a Segurança de Camada de Transporte (Transport Layer Security, TLS) habilitada são consideradas seguras, mas o protocolo subjacente com SSL/TLS é baseado em TCP. Com protocolos modernos de vídeo remotos explorando transportes baseados em UDP sem conexão, os benefícios de desempenho podem se deteriorar significativamente quando forçados sobre um transporte com base em TCP. Isso não se aplica a todas as tecnologias de VPN, tendo em vista que aqueles que também podem funcionar com DTLS ou IPsec em vez de SSL/TLS podem funcionar bem com protocolos de área de trabalho do View.

Requisitos de sistema e de rede do Access Point

Para implementar o appliance do Access Point, certifique-se de que seu sistema atenda aos requisitos de hardware e software.

Versões de produtos VMware compatíveis

Você deve utilizar versões específicas dos produtos VMware com versões específicas do Access Point. Consulte as notas da versão do produto para obter as informações mais recentes sobre compatibilidade e consulte a Matriz de Interoperabilidade de Produto da VMware em http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. As informações nas notas de versão e na matriz de interoperabilidade substituem as informações neste guia.

O Access Point 2.8 pode ser usado como um gateway seguro com as seguintes ofertas da VMware.

- VMare AirWatch 8.4 e posteriores
- VMware Identity Manager 2.7 e posteriores
- Vmware Horizon 6.2 e posteriores
- VMware Horizon Air Hybrid Mode 1.0 e posteriores
- VMware Horizon Air 15.3 e posteriores

Requisitos de hardware do servidor ESXi

O appliance do Access Point deve ser implementado em uma versão do vSphere que seja a mesma de uma versão suportada para produtos e versões Horizon que esteja utilizando.

Se você planeja utilizar o vSphere Web Client, certifique-se de que o plug-in de integração do cliente esteja instalado. Para obter mais informações, consulte a documentação do vSphere. Se você não instalar esse plug-in antes de iniciar o assistente de implementação, o assistente solicitará a instalação do plug-in. Isso exige o fechamento do navegador e a saída do assistente.

Observação Configure o relógio (UTC) no appliance do Access Point para que ele esteja com a hora correta. Por exemplo, abra uma janela de console na máquina virtual do Access Point e utilize os botões de seta para selecionar o fuso horário correto. Verifique também se o horário do host do ESXi está sincronizado com o servidor NTP e verifique se as VMware Tools, que estão sendo executadas na máquina virtual do appliance, sincronizam o horário na máquina virtual com o horário no host do ESX.

Requisitos do appliance virtual

O pacote OVF para o appliance do Access Point seleciona automaticamente a configuração da máquina virtual que o Access Point exige. Embora você possa alterar estas configurações , a VMware recomenda que não altere o CPU, memória ou espaço em disco para valores inferiores às configurações padrão do OVF.

Certifique-se de que o repositório de dados utilizado para o appliance tenha espaço livre em disco suficiente e atenda aos outros requisitos do sistema.

- O tamanho de download do appliance virtual é de 2,5 GB
- O requisito mínimo de disco com provisionamento dinâmico é de 2,5 GB
- O requisito mínimo de disco com provisionamento estático é de 20 GB

As seguintes informações são necessárias para implementar o appliance virtual

- Endereço IP estático
- Endereço IP do servidor DNS
- Senha para o usuário raiz
- URL da instância do servidor do balanceador de carga para o qual o appliance do Access Point aponta

Requisitos de configuração de rede

Você pode utilizar uma, duas ou três interfaces de rede e o Access Point necessita de um endereço IP estático separado para cada uma. Muitas implementações do DMZ utilizam redes separadas para proteger tipos de tráfego diferentes. Configure o Access Point de acordo com o design da rede do DMZ no qual está implementado.

- Uma interface de rede é apropriada para POCs (prova de conceitos) ou testes. Com um NIC, os tráfegos externo, interno e de gerenciamento estão todos na mesma sub-rede.
- Com duas interfaces de rede, o tráfego externo está em uma sub-rede e o tráfego interno e de gerenciamento estão em outra.
- Utilizar três interfaces de rede é a opção mais segura. Com um terceiro NIC, os tráfegos externo, interno e de gerenciamento têm suas próprias sub-redes.

Importante Verifique se atribuiu um pool de IPs para cada rede. O appliance do Access Point pode então captar a máscara de sub-rede e as configurações do gateway. Para adicionar um pool de IPs, no vCenter Server, se estiver utilizando o vSphere Client nativo, vá até a guia **Pools de IPs** do centro de dados. Alternativamente, se estiver utilizando o vSphere Web Client, você poderá criar um perfil de protocolo de rede. Vá até a guia **Gerenciar** do centro de dados e selecione a guia **Perfis de Protocolo de Rede**. Para obter mais informações, consulte Configurando Perfis de Protocolo para Redes de Máquinas Virtuais.

Requisitos de retenção de registro

Os arquivos de registro são configurados por padrão para utilizar certa quantidade de espaço, que é menor do que o tamanho total do disco no agregado. Os logs para o Access Point são alternados por padrão. Você deve utilizar syslog para preservar estas entradas de registro. Consulte Coletando registros do appliance do Access Point.

Regras de firewall para appliances do Access Point baseados em DMZ

Appliances do Access Pointbaseados em DMZ exigem certas regras de firewall nos firewalls front-end e back-end. Durante a instalação, os serviços do Access Pointsão configurados para ouvir em certas portas de rede por padrão.

A implementação de um appliance do Access Pointbaseado em DMZ normalmente inclui dois firewalls.

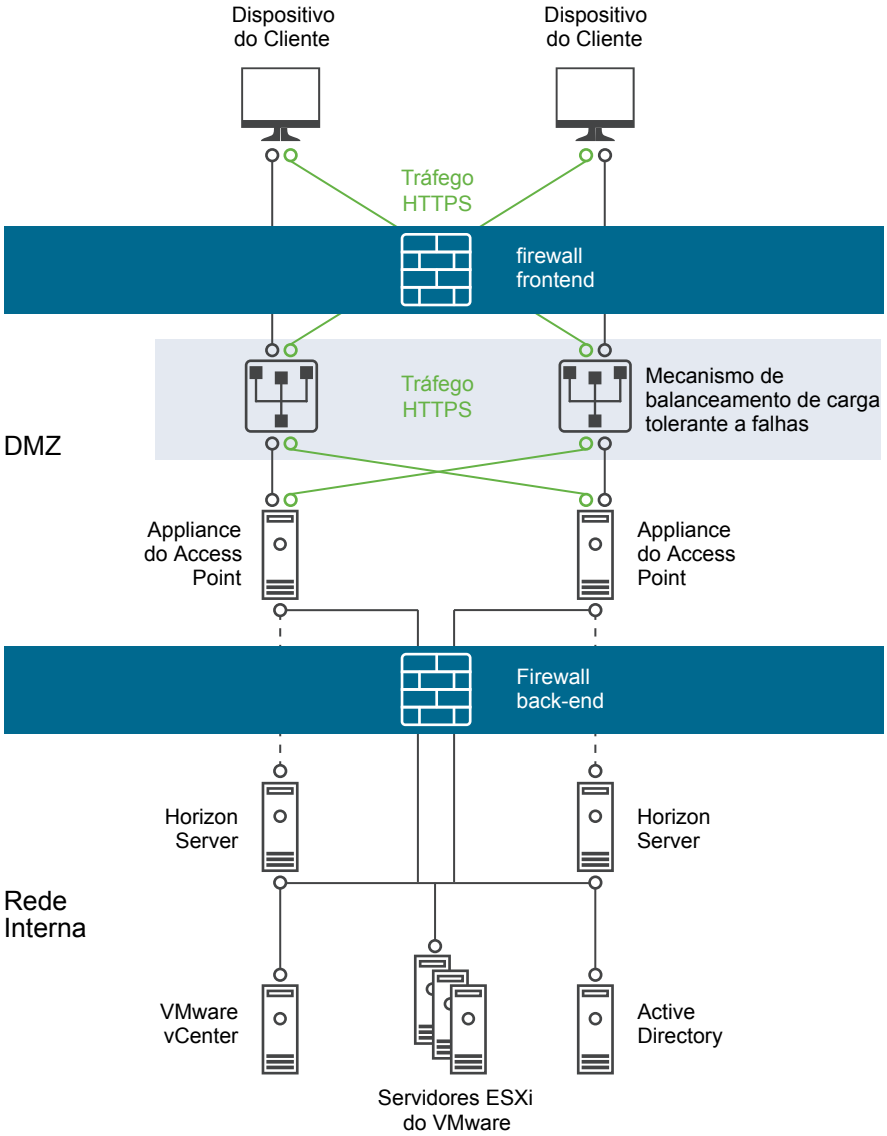
- É necessário um firewall front-end externo voltado para a rede para proteger o DMZ e a rede interna. Configure este firewall para permitir que o tráfego de rede externo chegue até o DMZ.
- É necessário um firewall back-end, entre o DMZ e a rede interna, para fornecer uma segunda camada de segurança. Configure este firewall para aceitar tráfego que se origina somente dos serviços dentro do DMZ.

A política de firewall controla estritamente comunicações de entrada de serviços DMZ, o que reduz amplamente o risco de comprometimento da rede interna.

Para permitir que dispositivos cliente externos se conectem a um appliance do Access Point dentro do DMZ, o firewall front-end deve permitir tráfego em determinadas portas. Por padrão, os dispositivos cliente externos e clientes Web externos (HTML Access) conectam-se a um appliance do Access Point dentro do DMZ na porta TCP 443. Se utilizar o protocolo Blast, a porta 443 deverá ser aberta no firewall. Se utilizar o protocolo PCOIP, a porta 4172 deverá ser aberta no firewall.

A figura a seguir mostra um exemplo de uma configuração que inclui firewalls front-end e back-end.

Figura 1-1. Topologia Dupla de Firewall



Topologias do balanceamento de carga do Access Point

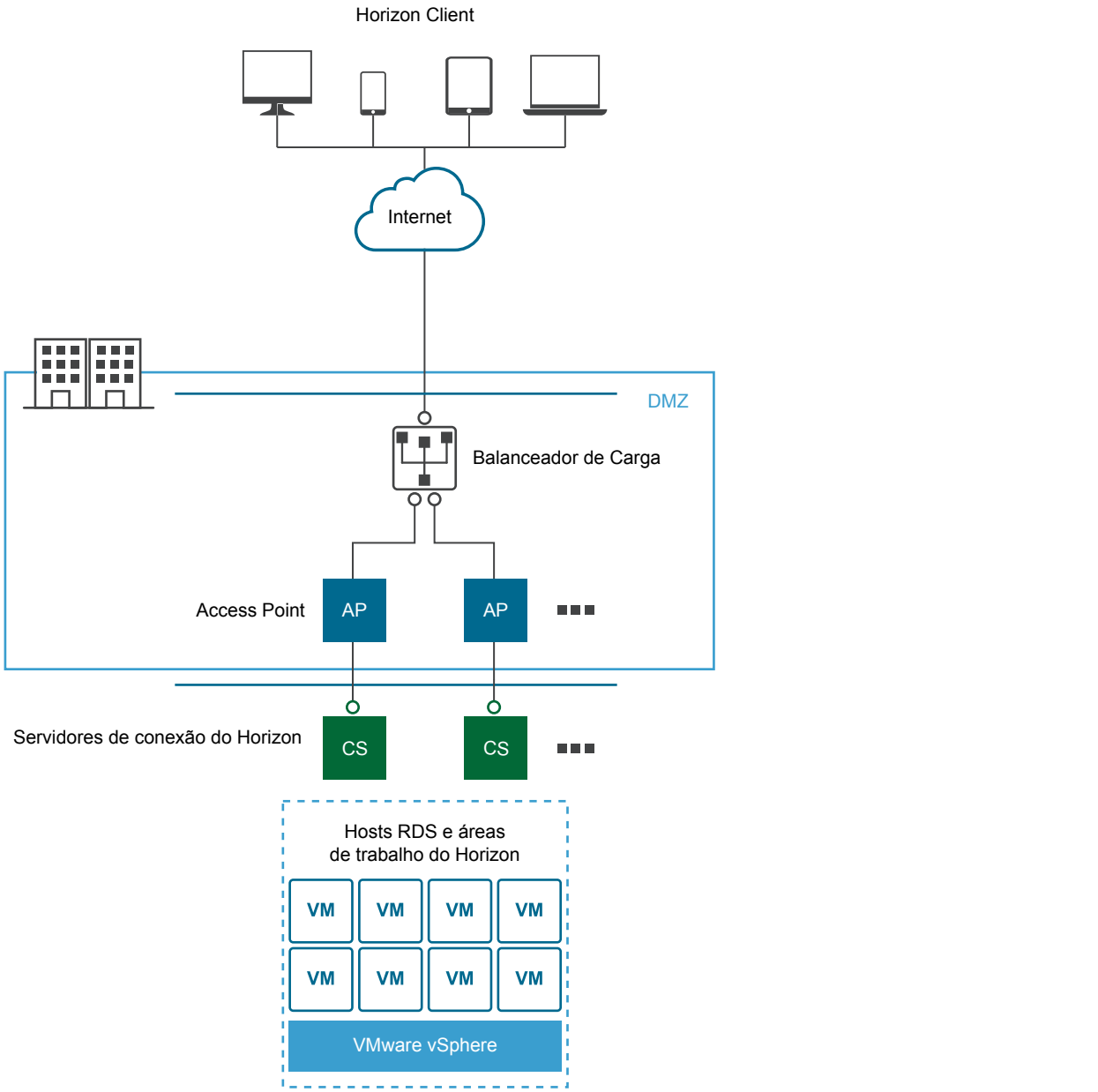
Você pode implementar qualquer uma de várias topologias diferentes.

Um appliance do Access Point no DMZ pode ser configurado para apontar para um servidor ou para um balanceador de carga que vá de encontro com um grupo de servidores. Os appliances do Access Pointfuncionam com soluções de balanceamento de carga padrão de terceiros que são configuradas para HTTPS.

Se o appliance do Access Point apontar para um balanceador de carga na frente de servidores, a seleção da instância do servidor será dinâmica. Por exemplo, o balanceador de carga poderá fazer uma seleção com base na disponibilidade e no conhecimento dele sobre o número de sessões atuais em cada instância do servidor. As instâncias do servidor dentro do firewall corporativo normalmente têm um balanceador de carga para suportar o acesso interno. Com o Access Point, você pode apontar o appliance do Access Point para este mesmo balanceador de carga que está já sendo utilizado com frequência.

Você pode, alternativamente, ter um ou mais appliances doAccess Point apontando para uma instância individual do servidor. Em ambas as abordagens, utilize um balanceador de carga na frente de dois ou mais appliances doAccess Point no DMZ.

Figura 1-2. Vários appliances do Access Point atrás de um balanceador de carga



Protocolos Horizon

Quando um usuário do Horizon Client se conecta a um ambiente Horizon, são utilizados vários protocolos diferentes. A primeira conexão é sempre o protocolo XML-API primário sobre o HTTPS. Após a autenticação bem-sucedida, são criados um ou mais protocolos secundários.

- Protocolo Horizon primário

  O usuário insere um nome do host no Horizon Client e isso inicia o protocolo Horizon primário. Esse é um protocolo de controle para a autorização de autenticação e o gerenciamento de sessão. Utiliza mensagens XML estruturadas sobre o HTTPS (HTTP sobre o SSL). Esse protocolo também é conhecido como protocolo de controle Horizon XML-API. Em um ambiente com carga balanceada como exibido acima na figura Vários appliances do Access Point atrás de um balanceador de carga, o balanceador de carga direciona esta conexão a um dos appliances do Access Point. Em geral, o balanceador de carga seleciona o appliance com base primeiramente na disponibilidade e, em seguida, escolhe a partir dos tráfegos de rotas de appliances disponíveis com base no menor número de sessões atuais. Esta configuração distribui uniformemente o tráfego de diferentes clientes no conjunto disponível de appliances do Access Point

- Protocolos Horizon secundários

  Após o Horizon Client estabelecer a comunicação segura com um dos appliances do Access Point, o usuário faz a autenticação. Se essa tentativa de autenticação for bem-sucedida, uma ou mais conexões secundárias serão feitas do Horizon Client. Essas conexões secundárias podem incluir o seguinte

  - Túnel HTTPS usado para encapsulamento dos protocolos TCP, como o RDP, o MMR/CDR e o canal de estrutura do cliente. (TCP 443).
  - Protocolo de exibição Blast Extreme (TCP 443 e UDP 443).
  - Protocolo de exibição PCoIP (TCP 4172 e UDP 4172).

Esses protocolos Horizon secundários devem ser encaminhados ao mesmo appliance do Access Point ao qual o protocolo Horizon primário foi encaminhado. O Access Point pode então autorizar os protocolos secundários com base na sessão de usuário autenticada. Uma capacidade importante de segurança do Access Point é que ele somente encaminhará o tráfego ao centro de dados corporativo se o tráfego estiver em nome de um usuário autenticado. Se o protocolo secundário for encaminhado erroneamente a um appliance do Access Point diferente do appliance do protocolo primário, ele não será autorizado e será colocado na DMZ. A conexão falha. O encaminhamento incorreto de protocolos secundários será um problema comum se o balanceador de carga não estiver configurado corretamente.

Design da DMZ para o Access Point com várias placas de interface de rede

O Access Point é um appliance de segurança de 7 camadas normalmente instalado em uma Zona Desmilitarizada (Demilitarized Zone, DMZ). O Access Point é usado para garantir que o único tráfego entrando no centro de dados corporativo seja o tráfego em nome de um usuário remoto fortemente autenticado.

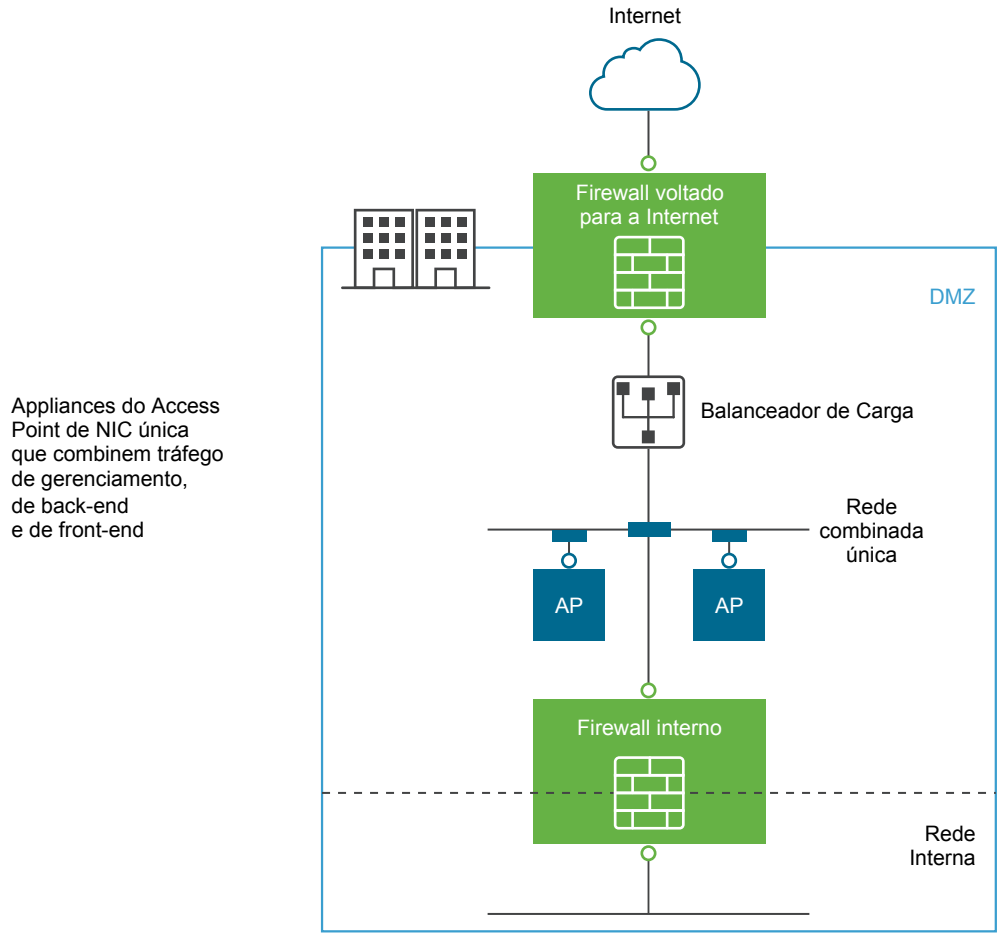
Uma das definições de configuração para o Access Point é o número de Placas de interface de rede (Network Interface Cards, NICs) virtuais a serem utilizadas. Ao implementar o Access Point, você seleciona uma configuração de implementação para sua rede. É possível especificar uma, duas ou três configurações de NICS, especificadas como onenic, twonic ou threenic.

Reduzir o número de portas abertas em cada LAN virtual e separar os tipos diferentes de tráfego de rede pode melhorar a segurança de forma significativa. Os benefícios são principalmente em termos de separação e isolamento dos tipos diferentes de tráfego de rede como parte de uma estratégia de design de segurança da DMZ de defesa em profundidade. Isso pode ser conquistado ao implementar comutadores físicos separados dentro da DMZ, com várias LANs virtuais dentro da DMZ ou como parte de uma DMZ totalmente gerenciada pelo VMware NSX.

Implementação típica da DMZ com NIC única

A implementação mais simples de um Access Point é com uma única NIC, onde todo o tráfego de rede é combinado em uma única rede. O tráfego do firewall voltado para a Internet é direcionado a um dos appliances disponíveis do Access Point. O Access Point então encaminha o tráfego autorizado através do firewall interno aos recursos na rede interna. O Access Point descarta o tráfego não autorizado.

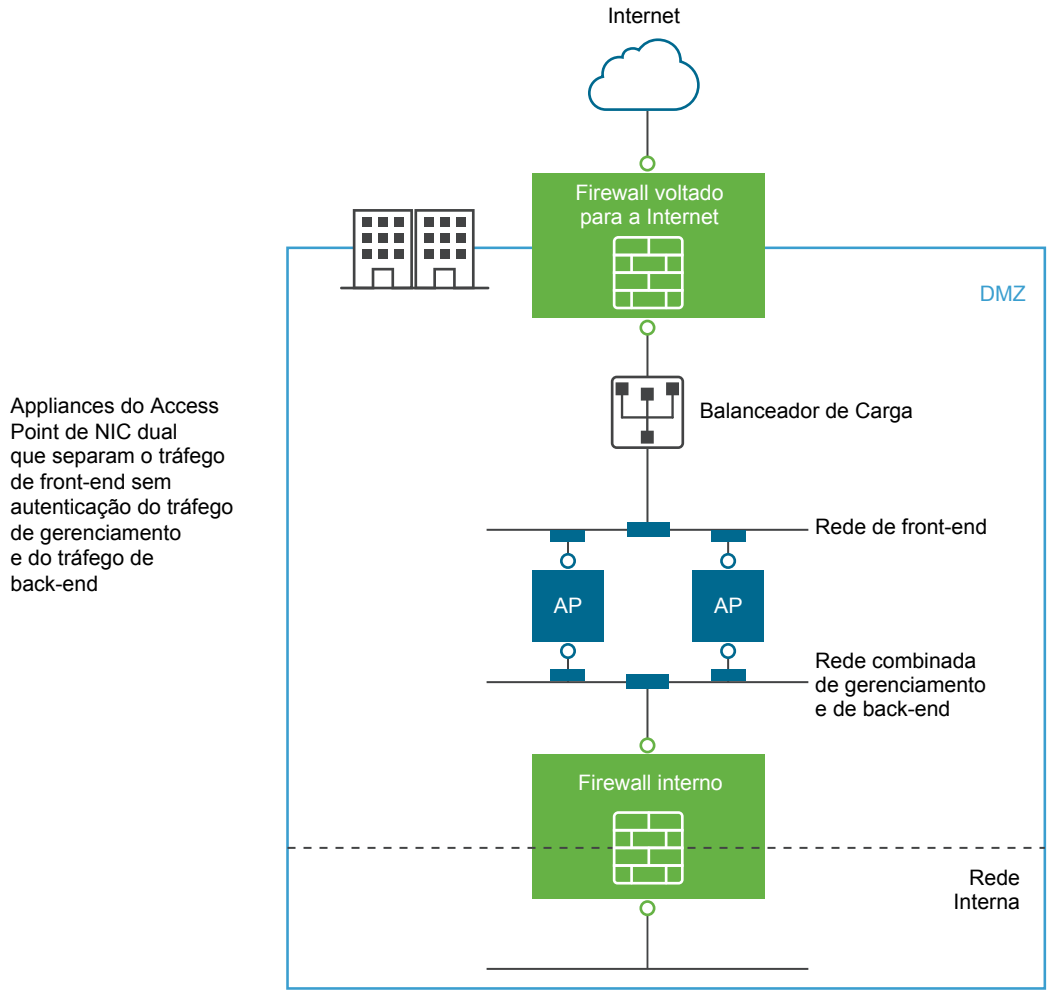
Figura 1-3. Opção de Access Point com NIC única



Separando o tráfego de usuário não autenticado do tráfego de back-end e de gerenciamento

Uma melhoria sobre a implementação de NIC única é especificar duas NICs. A primeira ainda é usada para Internet voltada para o acesso não autenticado, mas o tráfego autenticado de back-end e o tráfego de gerenciamento são separados em uma rede diferente.

Figura 1-4. Opção de Access Point com duas NICs



Em uma implementação com duas NICs, o tráfego que passa pela rede interna por meio do firewall interno deve ser autorizado pelo Access Point. O tráfego não autorizado não está nessa rede de back-end. O tráfego de gerenciamento como o API REST para o Access Point está somente nesta segunda rede

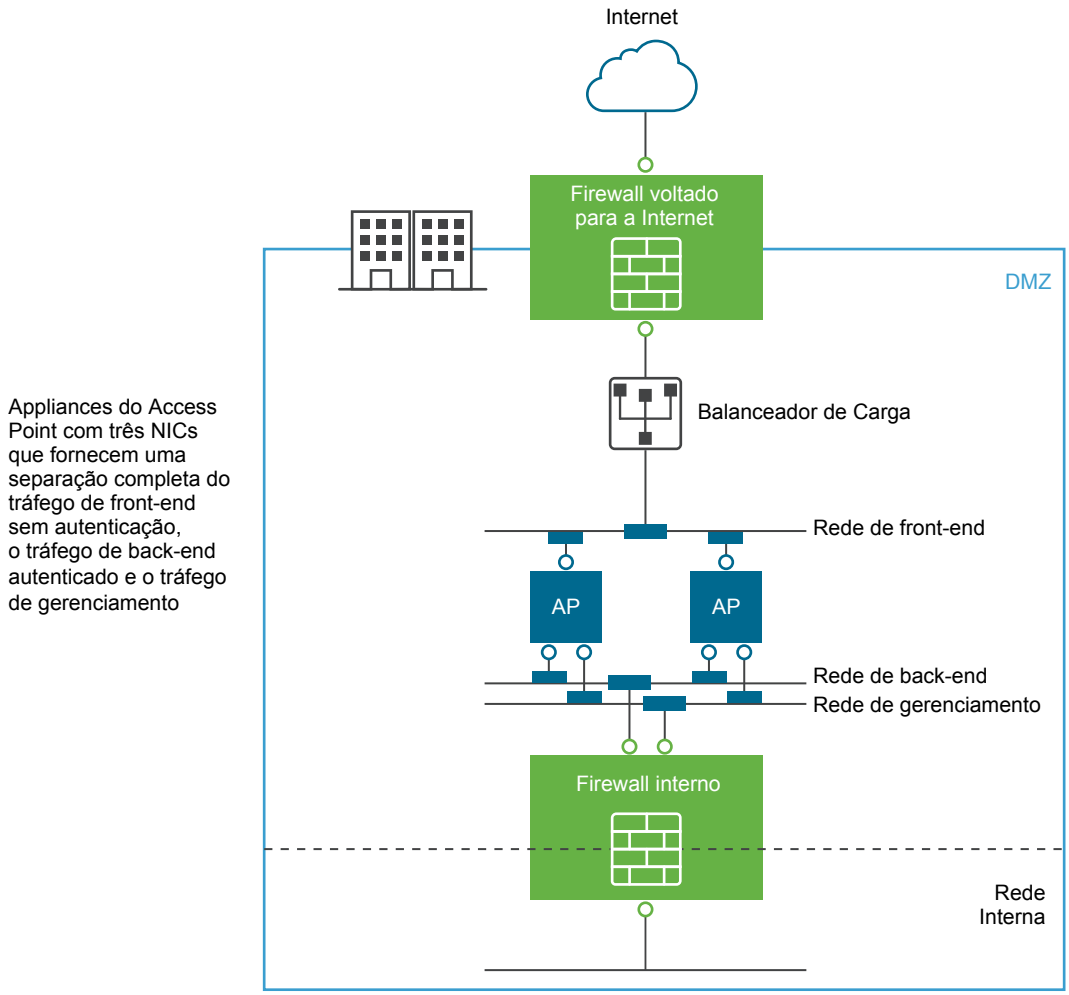
Se um dispositivo na rede de front-end sem autenticação foi comprometido, como o balanceador de carga, então a reconfiguração do dispositivo para ignorar o Access Point não é possível nesta implementação com duas NICs. Ela combina as regras de firewall da camada 4 com a segurança do Access Point da camada 7. De maneira semelhante, se o firewall voltado para a Internet foi configurado de maneira errada para permitir a passagem pela porta 9443 TCP, isso ainda não deixaria o API REST de Gerenciamento do Access Point exposto a usuários da Internet. Um princípio de defesa em profundidade utiliza vários níveis de proteção, como saber que um único erro de configuração ou ataque de sistema não cria necessariamente uma vulnerabilidade geral

Em uma implementação com duas NICs, é comum colocar sistemas de infraestrutura adicionais, como servidores DNS, servidores de Gerenciador de Autenticação do RSA SecurID na rede de back-end dentro da DMZ para que estes servidores não estejam visíveis na rede voltada para a Internet. Colocar sistemas de infraestrutura dentro da DMZ protege contra ataques de camada 2 da LAN voltada para a Internet a partir de um sistema de front-end comprometido e reduz efetivamente a superfície geral de ataque.

A maior parte do tráfego de rede do Access Point consiste nos protocolos de exibição para Blast e PCoIP. Com uma NIC única, o tráfego de protocolo de exibição de e para a Internet é combinado com tráfego de e para os sistemas de back-end. Quando duas ou mais NICs são utilizadas, o tráfego é espalhado em NICs de front-end e back-end e em redes. Isso reduz o potencial de gargalo de uma NIC única e resulta em benefícios de desempenho.

O Access Point suporta uma separação adicional ao permitir também a separação do tráfego de gerenciamento em uma LAN de gerenciamento específico. O tráfego de gerenciamento HTTPS para a porta 9443 só é possível a partir da LAN de gerenciamento.

Figura 1-5. Opção de Access Point com três NICs



Implementação do appliance do Access Point 2

O Access Point é colocado em um pacote como um OVF e é implementado em um host vSphere ESX ou ESXi como um appliance virtual pré-configurado.

Dois métodos primários podem ser utilizados para instalar o appliance do Access Point.

- O vSphere Client ou o vSphere Web Client podem ser utilizados para implementar o modelo do OVF do Access Point. Você recebe um aviso para configurações básicas, incluindo a configuração de implementação da NIC, endereço IP e senhas da interface de gerenciamento. Após o OVF ser implementado, faça o login na interface de usuário administrador do Access Point para ajustar as configurações de sistema do Access Point, definir os serviços de borda seguros em vários casos de uso e configurar a autenticação na DMZ. Consulte Implementar o Access Point usando o assistente modelo do OVF.
- Os scripts PowerShell podem ser usados para implementar o Access Point e definir serviços de borda seguros em vários casos de uso. Você pode fazer o download do arquivo compactado, configurar o script do PowerShell para o seu ambiente e executar o script para implementar o Access Point. Consulte Usando o PowerShell para implementar o appliance do Access Point.

Este capítulo inclui os seguintes tópicos:

- Usando o assistente modelo do OVF para implementar o appliance do Access Point
- Configurando o Access Point a partir das páginas de configuração do administrador
- Atualizar certificados assinados de servidor SSL

Usando o assistente modelo do OVF para implementar o appliance do Access Point

Para implementar o Access Point, implante o modelo do OVF usando o vSphere Client ou o vSphere Web Client, ative o appliance e defina as configurações.

Após a implementação do Access Point, vá até a interface do usuário (IU) de administração para definir o ambiente do Access Point e configurar os recursos da área de trabalho e do aplicativo e os métodos de autenticação a serem usados na DMZ.

Propriedades de implementação do Access Point

Ao implementar o OVF, você define o número necessário de interfaces de rede (NIC), o endereço IP e a senha do administrador. As outras propriedades de implementação podem ser definidas nas páginas de administração do Access Point.

Tabela 2-1. Opções de Implementação do Access Point

Propriedade de Implementação	Descrição
Configuração da implementação do	Especifica quantas interfaces de rede estão disponíveis na máquina virtual do Access Point. Por padrão, está propriedade não está definida, o que significa que um controlador de interface de rede (network interface controller, NIC) é utilizado.
Endereço IP externo (voltado para a Internet)	(Necessário) Especifica o endereço IPv4 ou IPv6 público utilizado para acessar essa máquina virtual na Internet. **Observação** O nome do computador é definido através de uma consulta ao DNS deste endereço IPv4 ou IPv6 de Internet. Padrão: nenhum.
Endereço IP de rede de gerenciamento	Especifica o endereço IP da interface que está conectada à rede de gerenciamento. Se não estiver configurado, o servidor de administração escutará a interface voltada para a Internet. Padrão: nenhum.
Endereço IP de rede de back-end	Especifica o endereço IP da interface que está conectada à rede de back-end. Se não estiver configurado, o tráfego de rede enviado aos sistemas de back-end será encaminhado através das outras interfaces de rede. Padrão: nenhum.
Endereços de servidor DNS	(Necessário) Especifica um ou mais endereços IPv4 separados por espaço dos servidores de nome de domínio para esta máquina virtual (exemplo: 192.0.2.1 192.0.2.2). É possível especificar até três servidores. Por padrão, esta propriedade não está definida, o que significa que o sistema utiliza o servidor DNS que está associado ao NIC voltado para a Internet. **Cuidado** Se deixar esta opção em branco e se nenhum servidor DNS estiver associado ao NIC voltado para a Internet, o appliance não será implementado corretamente.
Senha para o usuário raiz	(Necessário) Especifica a senha para o usuário raiz desta máquina virtual. A senha deve ser uma senha Linux válida. Padrão: nenhum.
Senha para o usuário administrador	(Obrigatório) Se você não definir essa senha, não poderá acessar o console de administração e o API REST no appliance do Access Point. As senhas devem ter pelo menos 8 caracteres de comprimento, conter pelo menos uma letra maiúscula e uma letra minúscula, um dígito e um caractere especial, que inclui ! @ # $ % * ( ). Padrão: nenhum.

Tabela 2-1. Opções de Implementação do Access Point (Continuação)

Propriedade de Implementação	Descrição
Local a ser utilizado para mensagens localizadas	(Necessário) Especifica o local a ser utilizado ao gerar mensagens de erro. ■ **en_US** para inglês ■ **ja_JP** para japonês ■ **fr_FR** para francês ■ **de_DE** para alemão ■ **zh_CN** para chinês simplificado ■ **zh_TW** para chinês tradicional ■ **ko_KR** para coreano Padrão: en_US.
URL do servidor Syslog	Especifica o servidor Syslog utilizado para registrar eventos do Access Point . Este valor pode ser um URL ou um nome do host ou endereço IP. O esquema e número de porta são opcionais (exemplo: syslog://servidor.exemplo.com:514). Por padrão, esta propriedade não está definida, o que significa que nenhum evento está registrado em um servidor syslog.

Implementar o Access Point usando o assistente modelo do OVF

Você pode implementar o appliance do Access Pointefetuando logon no vCenter Server e utilizando o assistente Implementar Modelo OVF.

Observação Se utilizar o vSphere Web Client para implementar o OVF, será possível também especificar os endereços do servidor DNS, de gateway e de máscara de rede para cada rede. Se você utilizar o vSphere Client nativo, certifique-se de que atribuiu um pool de IPs para cada rede. Para adicionar um pool de IPs no vCenter Server utilizando o vSphere Client original, vá até a guia Pools de IPs do centro de dados. Alternativamente, se estiver utilizando o vSphere Web Client, você poderá criar um perfil de protocolo de rede. Vá até a guia Gerenciar do centro de dados e selecione a guia Perfis de Protocolo de Rede.

Pré-requisitos

- Familiarize-se com as opções de implementação disponíveis no assistente. Consulte Requisitos de sistema e de rede do Access Point.
- Determine quantas interfaces de rede e endereços IP estáticos devem ser configurados para o appliance do Access Point. Consulte Requisitos de configuração de rede.
- Faça o download do arquivo do instalador `.ova` para o appliance do Access Pointno site da VMware em https://my.vmware.com/web/vmware/downloads ou determine o URL a ser utilizado (exemplo: `http://exemplo.com/vapps/euc-access-point-`*Y.Y*`.0.0-`*xxxxxxx*`_OVF10.ova`), onde *Y.Y* é o número da versão e *xxxxxxx* é o número de compilação.

Procedimentos

1 Utilize o vSphere Client nativo ou o vSphere Web Client para efetuar logon em uma instância do vCenter Server.

Para uma rede IPv4, utilize o Cliente vSphere nativo ou o Cliente Web vSphere. Para uma rede IPv6, utilize o cliente Web vSphere.

2 Selecione um comando de menu para iniciar o assistente Implementar Modelo OVF.

Opção	Comando de Menu
vSphere Client	Selecione **Arquivo > Implementar Modelo OVF**.
vSphere Web Client	Selecione um objeto de inventário que seja um objeto parente válido de uma máquina virtual, como um centro de dados, pasta, cluster, pool de recursos ou host e, no menu **Ações**, selecione **Implementar Modelo OVF**.

3 Na página Selecionar Origem do assistente, navegue até a localização do arquivo `.ova` que baixou ou insira um URL e clique em **Avançar**.

Uma página de detalhes é exibida. Revise os detalhes do produto, a versão e os requisitos de tamanho.

4 Siga as indicações do assistente e leve em consideração as seguintes orientações à medida que conclui o assistente.

Opção	Descrição
Selecione uma configuração de implementação	Para uma rede IPv4, você pode utilizar uma, duas ou três interfaces de rede (NICs). Para uma rede IPv6, utilize três NICs. O Access Point exige um endereço IP estático separado para cada NIC. Muitas implementações do DMZ utilizam redes separadas para proteger tipos de tráfego diferentes. Configure o Access Point de acordo com o design da rede do DMZ no qual está implementado.
Formato do disco	Para ambientes de avaliação e teste, selecione o formato de Provisionamento Dinâmico. Para ambientes de produção, selecione um dos formatos de Provisionamento Estático. O Thick Provision Eager Zeroed é um tipo de formato de disco virtual estático que suporta recursos de cluster como tolerância a falhas, mas demora muito mais para ser criado do que outros tipos de discos virtuais.
Política de armazenamento VM	(Somente para vSphere Web Client) Esta opção estará disponível se as políticas de armazenamento estiverem ativadas no recurso de destino.

Opção	Descrição
Configurar Redes/Mapeamento de Rede	Se estiver utilizando o vSphere Web Client, a página Configurar Redes permitirá o mapeamento de cada NIC a uma rede e especifica configurações de protocolo. a Selecione IPv4 ou IPv6 na lista suspensa de **protocolo IP**. b Selecione a primeira linha na tabela **Internet** e, em seguida, clique na seta para baixo para selecionar a rede de destino. Se você selecionar IPv6 como o protocolo IP, será preciso selecionar a rede que possui recursos IPv6. Após selecionar a linha, você pode também inserir os endereços IP para o servidor DNS, o gateway e a máscara de rede na porção inferior da janela. c Se estiver utilizando mais de um NIC, selecione a fileira seguinte **Rede de Gerenciamento**, selecione a rede de destino e, em seguida, poderá inserir os endereços IP para o servidor DNS, gateway e máscara de rede para aquela rede. Se estiver utilizando somente um NIC, todas as linhas serão mapeadas para a mesma rede. d Se possuir um terceiro NIC, selecione também a terceira linha e conclua as configurações. Se estiver utilizando somente dois NICs, para esta terceira linha **Rede Back-end**, selecione a mesma rede que utilizou para **Rede de Gerenciamento**. Com o vSphere Web Client, um perfil de protocolo de rede será criado automaticamente após a conclusão do assistente, se ainda não existir. Se você utiliza o vSphere Client nativo (em vez do Web Client), a página Mapeamento de Rede permite mapear cada NIC a uma rede, mas não há campos para especificar os endereços do servidor DNS, do gateway e da máscara de rede. Como descrito nos pré-requisitos, você precisa ter atribuído um pool de IPs para cada rede ou ter criado um perfil de protocolo de rede.
Personalizar o modelo Propriedades	As caixas de texto na página Propriedades são específicas ao Access Point e podem não ser necessárias para outros tipos de appliance virtuais. O texto na página do assistente explica cada configuração. Se o texto estiver truncado no lado direito do assistente, redimensione a janela arrastando-a partir do canto inferior direito. Você deve inserir valores nas seguintes caixas de texto: ■ **IPMode:STATICV4/STATICV6**. Se digitar STATICV4, será necessário inserir o endereço IPv4 para o NIC. Se digitar STATICV6, será necessário inserir o endereço IPv6 para o NIC. ■ **Lista separada por vírgula das regras de encaminhamento com o formato {tcp|udp}/listening-port-number/destination-ip-address:destination-port-nu** ■ **Endereço IPv4 para o NIC 1 (ETH0)**. Insira o endereço IPv4 para o NIC se digitou STATICV4 para o modo NIC. ■ **Lista separada por vírgula das rotas personalizadas IPv4 para NIC 1 (eth0) com o formato ipv4-network-address/bits.ipv4-gateway-address** ■ **Endereço IPv6**. Insira o endereço IPv6 para o NIC se digitou STATICV6 para o modo NIC. ■ **Endereços de servidor DNS**. Insira os endereços IPv4 ou IPv6 separados por espaço dos servidores do nome de domínio para a VM. ■ **Endereço IP de rede de gerenciamento** se você especificou 2 NICs e **Endereço IP de rede de Back-end** se especificou 3 NICs ■ **Opções de senha**. Insira a senha para o usuário raiz desta VM e a senha para o usuário administrador que acessa o console de administração e ativa o acesso à API REST.

Opção	Descrição
	Todas as outras configurações são opcionais ou já possuem uma configuração padrão inserida. Observe os requisitos de senha listados na página do assistente. Para obter uma descrição de todas as propriedades de implementação, consulte Propriedades de implementação do Access Point.

5 Na página Pronto para Concluir, selecione **Ligar após implementação** e clique em **Concluir**.

Uma tarefa de Implementar Modelo OVF aparece na área de status do vCenter Server para que você possa monitorar a implementação. Você pode também abrir um console na máquina virtual para visualizar as mensagens do console que são exibidas durante a inicialização do sistema. Um registro destas mensagens também está disponível no arquivo `/var/log/boot.msg`.

6 Quando a implementação for concluída, certifique-se de que os usuários finais possam se conectar ao appliance abrindo um navegador e inserindo o seguinte URL:

```
https://FQDN-of-AP-appliance
```

Nesse URL, *FQDN-of-AP-appliance* é o nome de domínio totalmente qualificado do appliance do Access Point que pode ser resolvido por DNS.

Se a implementação for bem-sucedida, você verá a página da Web fornecida pelo servidor para o qual o Access Point estiver apontado. Se a implementação não foi bem sucedida, você pode excluir a máquina virtual do appliance e implementá-lo novamente. O erro mais comum é não inserir as impressões digitais do certificado corretamente.

O appliance do Access Pointé implementado e iniciado automaticamente.

Próximo passo

Faça o login na interface do usuário (IU) do administrador e configure os recursos da área de trabalho e do aplicativo para permitir acesso remoto da Internet por meio do Access Point e os métodos de autenticação a serem usados na DMZ. O URL do console de administração está no formato `https://<mycoAccessPointappliance.com:9443/admin/index.html`.

Configurando o Access Point a partir das páginas de configuração do administrador

Após implantar o OVF e o appliance do Access Point estiver ativado, faça login na Interface do usuário administrador do Access Point para definir as seguintes configurações.

- Configuração de sistema do Access Point e certificado de servidor SSL.
- Configurações de serviço de borda para Horizon, proxy reverso, túnel por aplicativo e configurações de proxy para o AirWatch.
- Configurações de autenticação para o RSA SecurID, RADIUS, Certificado X.509 e RSA Adaptive Authentication.
- Configurações para provedor de identidade SAML e provedor de serviços.

As opções a seguir podem ser acessadas a partir das páginas de configuração.

- Faça o download dos arquivos de registro compactados do Access Point.
- Exporte as configurações do Access Point para recuperar as definições de configuração.
- Importe as configurações do Access Point para criar e atualizar uma configuração inteira do Access Point.

Definir as configurações de sistema do Access Point

É possível configurar os protocolos de segurança e os algoritmos criptográficos usados para criptografar as comunicações entre os clientes e o appliance do Access Point a partir das páginas de configuração do administrador.

O URL da interface do usuário administrador do Access Pointtem o formato `https://<mycoAccessPointappliance.com>:9443/admin/index.html`. Para fazer logon, insira o nome de usuário administrador e a senha que você configurou durante a implantação do OVF.

Pré-requisitos

- Revisar as propriedades de implementação do Access Point. São necessárias as seguintes informações de configurações.
  - Endereço IP estático para o appliance do Access Point
  - Endereço IP do servidor DNS
  - Senha para o console de administração
  - URL da instância do servidor ou balanceador de carga para o qual o appliance do Access Point aponta
  - URL do servidor Syslog para salvar os arquivos de log de evento

Procedimentos

1. Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.
2. Na seção Configurações Avançadas, clique no ícone de engrenagem **Configuração do Sistema**.

3 Edite os seguintes valores de configuração do appliance do Access Point.

Opção	Valor padrão e descrição
Localidade	Especifica o local a ser utilizado ao gerar mensagens de erro. ■ **en_US** para inglês ■ **ja_JP** para japonês ■ **fr_FR** para francês ■ **de_DE** para alemão ■ **zh_CN** para chinês simplificado ■ **zh_TW** para chinês tradicional ■ **ko_KR** para coreano
Senha do administrador	Esta senha foi definida quando você implementou o appliance. É possível redefini-la. As senhas devem ter pelo menos 8 caracteres de comprimento, conter pelo menos uma letra maiúscula e uma letra minúscula, um dígito e um caractere especial, que inclui ! @ # $ % * ( ).
Conjuntos de criptografia	Na maioria dos casos, as configurações padrão não precisam ser alteradas. Estes são os algoritmos criptográficos usados para criptografar as comunicações entre os clientes e o appliance do Access Point. As configurações de criptografia são usadas para ativar vários protocolos de segurança.
Obedecer ordem de criptografia	O padrão é NÃO. Selecione **SIM** para ativar o controle de ordem da lista de criptografia TLS.
SSL 3.0 ativado	O padrão é NÃO. Selecione **SIM** para ativar o protocolo de segurança SSL 3.0.
TLS 1.0 ativado	O padrão é NÃO. Selecione **SIM** para ativar o protocolo de segurança TLS 1.0.
TLS 1.1 ativado	O padrão é SIM. O protocolo de segurança TLS 1.1 está ativado.
TLS 1.2 ativado	O padrão é SIM. O protocolo de segurança TLS 1.2 está ativado.
URL do Syslog	Insira o URL do servidor Syslog utilizado para registrar eventos do Access Point. Este valor pode ser um URL ou um nome do host ou endereço IP. Se você não definir o URL do servidor syslog, nenhum evento será registrado. Digite como `syslog://server.example.com:514`.
URL de verificação de integridade	Insira um URL pelo qual o balanceador de carga se conecta e verifica a integridade do Access Point
Cookies a serem armazenados em cache	O conjunto de cookies que o Access Point armazena em cache. O padrão é nenhum.
Modo do IP	Selecione modo do IP estático, STATICV4 OU STATICV6.
Tempo limite da sessão	O valor padrão é **36000000** milissegundos.
Modo fechar para novas sessões	Ative **SIM** para pausar o appliance do Access Point a fim de alcançar um estado consistente para realizar tarefas de manutenção
Intervalo do monitor	O valor padrão é **60**.

4 Clique em **Salvar**.

Próximo passo

Defina as configurações do serviço de borda para os componentes com os quais o Access Point é implementado. Após definir as configurações de borda, defina as configurações de autenticação.

Atualizar certificados assinados de servidor SSL

É possível substituir os certificados assinados após a expiração.

Para ambientes de produção, a VMware recomenda enfaticamente a substituição do certificado padrão o mais rápido possível. O certificado padrão do servidor TLS/SSL gerado ao implementar um appliance do Access Point não é assinado por uma Autoridade de Certificação confiável.

Pré-requisitos

- Novo certificado assinado e chave privada salvos em um computador que possa ser acessado
- Converta o certificado em arquivos de formato PEM e converta os arquivos .pem no formato de uma linha. Consulte Converter arquivos de certificado para o formato PEM de uma linha.

Procedimentos

1. No console de administração, clique em **Selecionar**.
2. Na seção Configurações Avançadas, clique no ícone de engrenagem Configurações do Certificado do Servidor SSL.
3. Na linha Chave Privada, clique em **Selecionar** e navegue até o arquivo da chave privada.
4. Clique em **Abrir** para carregar o arquivo.
5. Na linha Cadeia de certificados, clique em Selecionar e navegue até o arquivo da cadeia de certificados.
6. Clique em **Abrir** para carregar o arquivo.
7. Clique em **Salvar**.

Próximo passo

Se a CA que assinou o certificado não tiver reputação renomada, configure os clientes para confiar nos certificados raiz e intermediário.

Usando o PowerSheel para implementar o Access Point

3

Um script do PowerSheel pode ser usado para implementar o Access Point. O script do PowerShell é entregue como um script de amostra que pode ser adaptado às necessidades específicas do ambiente.

Ao usar o script do PowerShell script para implementar o Access Point, o script chama o comando da OVF Tool e valida as configurações para construir automaticamente a sintaxe de linha de comando correta. Esse método também permite configurações avançadas, como a configuração do certificado do servidor TLS/SSL a ser aplicado no momento da implementação.

Este capítulo inclui os seguintes tópicos:

- Requisitos do sistema para a implementação do Access Point usando o PowerShell
- Usando o PowerShell para implementar o appliance do Access Point

Requisitos do sistema para a implementação do Access Point usando o PowerShell

Para implementar o Access Point usando script do PowerShell, você deve usar versões específicas dos produtos VMware.

- Host do vSphere ESX com um vCenter Server.
- O script do PowerShell é executado em máquinas com Windows 8.1 ou versões posteriores ou no Windows Server 2008 R2 ou versões posteriores.

  A máquina também pode ser um vCenter Server executado no Windows ou em uma máquina separada do Windows.
- A máquina com Windows que executar o script deve ter um comando de VMware OVF Tool instalado.

  Você deve instalar o OVF Tool 4.0.1 ou versão posterior do https://www.vmware.com/support/developer/ovf/.

Você deve selecionar a rede e o repositório de dados do vSphere a serem usados.

Um Perfil do Protocolo de Rede do vSphere deve ser associado a cada nome de rede de referência. Esse Perfil de Protocolo de Rede especifica as configurações de rede, como máscara de sub-rede IPv4, gateway etc. A implementação do Access Point usa esses valores, então verifique se os valores estão corretos.

Usando o PowerShell para implementar o appliance do Access Point

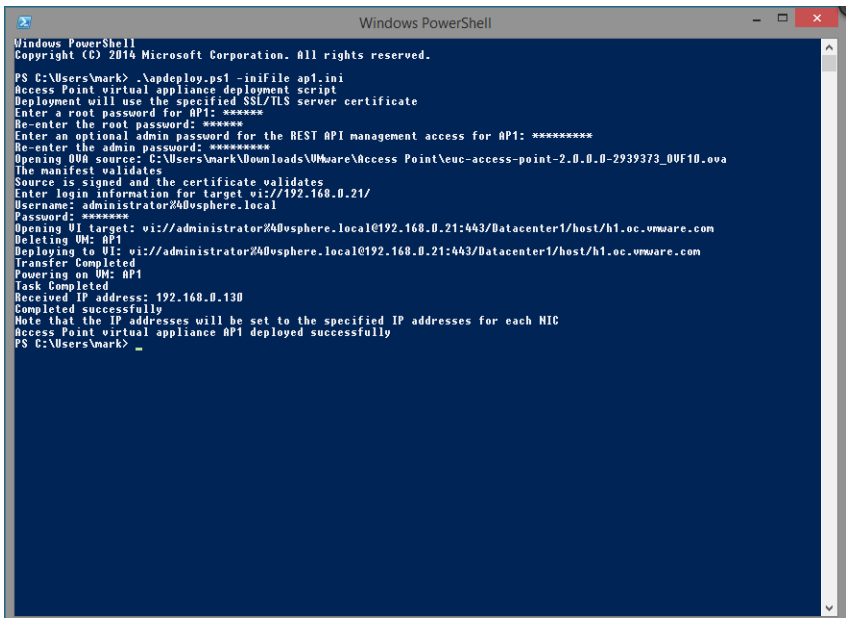
Os scripts do PowerShell preparam seu ambiente com todas as definições de configuração. Ao executar o script do PowerShell para implementar o Access Point, a solução está pronta para produção na primeira inicialização do sistema.

Pré-requisitos

- Verifique se os requisitos do sistema são apropriados e se estão disponíveis para uso.

  Este é um script de amostra para implementar o Access Point no seu ambiente.

  Figura 3-1. Script de amostra do PowerShell



Procedimentos

1. Faça o download do OVA do Access Point no My VMware para sua máquina Windows.
2. Faça o download dos arquivos ap-deploy-XXX.zip em uma pasta na máquina Windows.

   Os arquivos zip estão disponíveis em https://communities.vmware.com/docs/DOC-30835.
3. Abra um script do PowerShell e modifique o diretório do local do seu script.

4 Crie um arquivo de configuração .INI para o appliance virtual do Access Point.

Por exemplo: implemente um novo appliance AP1 do Access Point. O arquivo de configuração é nomeado como ap1.ini. Esse arquivo contém todas as definições de configuração para AP1. É possível usar os arquivos .INI de amostra no arquivo apdeploy .ZIP para criar o arquivo .INI e modificar as configurações adequadamente.

Observação Você pode ter arquivos .INI exclusivos para várias implementações do Access Point no seu ambiente. Você deve alterar os Endereços IP e os parâmetros de nome no arquivo .INI adequadamente para implantar vários appliances.

Exemplo do arquivo .INI a ser modificado.

```
name=AP1
source=C:\APs\euc-access-point-2.8.0.0-000000000_OVF10.ova
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esx1.myco.int
ds=Local Disk 1
netInternet=VM Network
netManagementNetwork=VM Network
netBackendNetwork=VM Network

[Horizon/WebReverseProxy/AirwatchTunnel]
proxyDestinationUrl=https://192.168.0.209

# For IPv4, proxydestinationURL=https://192.168.0.209
# For IPv6, proxyDEstinationUrl=[fc00:10:112:54::220]
```

5 Para assegurar que a execução do script seja bem-sucedida, digite o comando set-executionpolicy do PowerShell.

```
set-executionpolicy -scope currentuser unrestricted
```

Você deve executar esse comando uma vez e somente se ele estiver restrito no momento.

Se houver um aviso para o script, execute o comando para desbloquear o aviso:

```
unblock-file -path .\apdeploy.ps1
```

6 Execute o comando para iniciar a implementação. Se você não especificar o arquivo .INI, o script será padronizado para ap.ini.

```
.\apdeploy.ps1 -iniFile ap1.ini
```

7 Insira as credenciais quando receber o aviso e conclua o script.

Observação Se você receber um aviso para adicionar a impressão digital da máquina de destino, digite **sim**.

O appliance do Access Point está implementado e disponível para produção.

Para obter mais informações sobre scripts do PowerShell, consulte https://communities.vmware.com/docs/DOC-30835.

Casos de uso de implementação 4

Os cenários de implementação descritos neste capítulo podem auxiliar a identificar e organizar a implementação do Access Point em seu ambiente.

Você pode implementar o Access Point com o Horizon View, o Horizon Air Hybrid-Mode, o VMware Identity Manager e o VMware AirWatch.

Este capítulo inclui os seguintes tópicos:

- Implementação do Access Point com o Horizon View e o Horizon Air Hybrid-Mode
- Implementação do Access Point como proxy reverso
- Implementação do Access Point com o AirWatch Tunnel

Implementação do Access Point com o Horizon View e o Horizon Air Hybrid-Mode

Você pode implementar o Access Point com o Horizon View e o Modo Híbrido do Horizon Air. Para o componente View do VMware Horizon, os appliances do Access Point cumprem a mesma função que foi anteriormente desempenhada pelos servidores de segurança do View.

Cenário de implementação

O Access Point fornece acesso remoto seguro a áreas de trabalho e aplicativos virtuais no local em um centro de dados do cliente. Isso funciona com uma implementação local do Horizon View ou Horizon Air Hybrid-Mode para o gerenciamento unificado.

O Access Point fornece à empresa uma garantia de preservação da identidade do usuário e controla de forma precisa o acesso às áreas de trabalho e aplicativos autorizados.

Os appliances virtuais do Access Point são implementados, geralmente, em uma zona desmilitarizada (DMZ) da rede. A implementação na DMZ assegura que todo o tráfego entrando no centro de dados para os recursos da área de trabalho e do aplicativo é tráfego em nome de um usuário fortemente autenticado. Os appliances virtuais do Access Point também garantem que o tráfego de um usuário autenticado possa ser direcionado somente para os recursos da área de trabalho e de aplicativos para os quais o usuário estiver autorizado. Esse nível de proteção envolve a inspeção específica de protocolos de área de trabalho e a coordenação de potenciais endereços de rede e políticas de mudança rápida para controlar o acesso de maneira precisa.

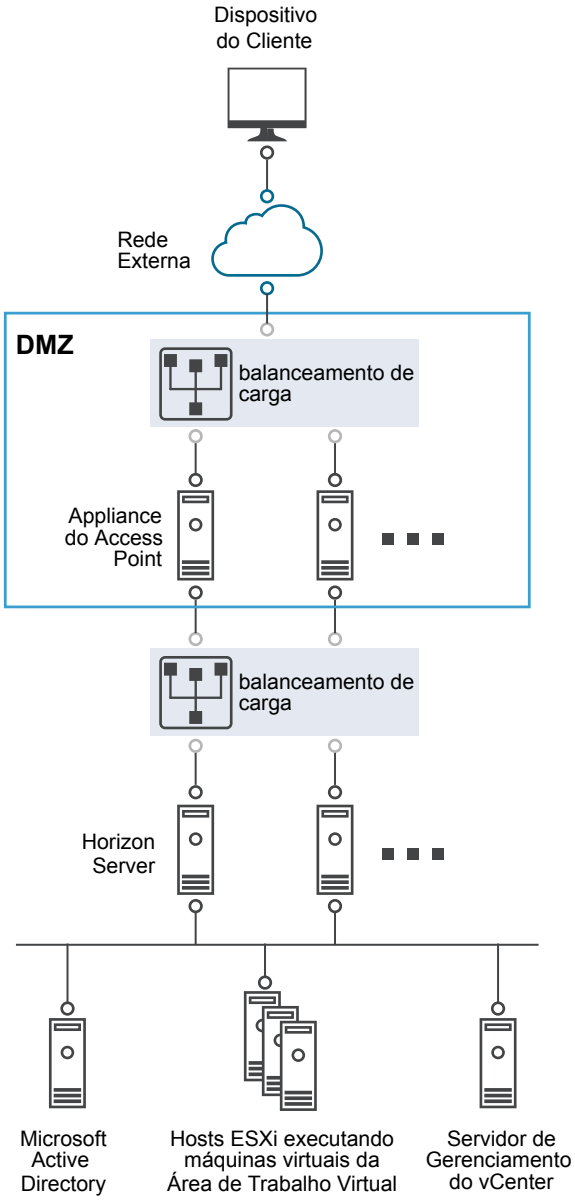
Você deve verificar os requisitos para a implementação contínua do Access Point com o Horizon.

- Se o appliance do Access Point apontar para um balanceador de carga na parte frontal dos servidores Horizon, a seleção da instância do servidor será dinâmica.
- O Access Point substitui o servidor de segurança Horizon.
- A Porta 443 deve estar disponível para Blast TCP/UDP.
- O Gateway seguro Blast e o Gateway seguro PCoIP devem ser habilitados quando o Access Point estiver implementado com o Horizon. Isso garante que os protocolos de exibição possam servir como proxies automaticamente por meio do Access Point. As configurações do BlastExternalURL e pcoipExternalURL especificam endereços de conexão usados pelos clientes do Horizon para encaminhar essas conexões de protocolo de exibição por meio dos gateways apropriados no Access Point. Isso oferece uma segurança melhorada, tendo em vista que esses gateways garantem que o tráfego do protocolo de exibição seja controlado em nome de um usuário autenticado. O tráfego do protocolo de exibição não autorizado é desconsiderado pelo Access Point.
- Desabilite os gateways seguros nas instâncias do Servidor de Conexão do View e habilite estes gateways nos appliances do Access Point.

A principal diferença do servidor de segurança do View é que o Access Point apresenta-se como segue.

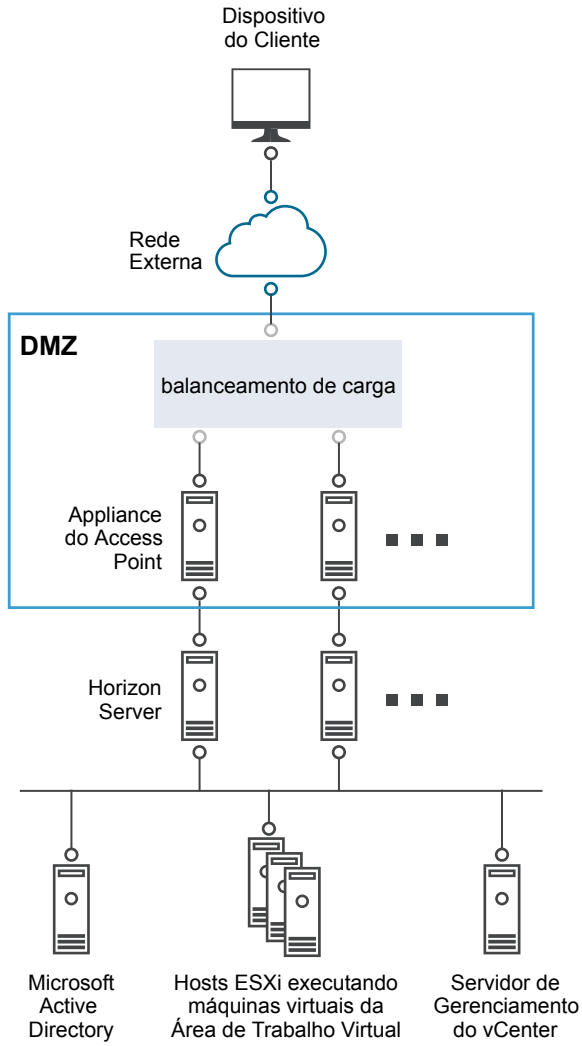
- Implementação segura. O Access Point é implementado como uma máquina virtual pré-configurada, protegida e bloqueada, baseada em Linux.
- Escalável. Você pode conectar o Access Point com um Servidor de Conexão do View individual, ou você pode conectá-lo por meio de um balanceador de carga na frente de vários Servidores de Conexão do View, oferecendo alta disponibilidade aprimorada. Ele age como uma camada entre o Horizon Clients e os Servidores de Conexão do View de back-end. Como a implementação é rápida, ele pode rapidamente ser ampliado ou reduzido para atender as demandas de empresas em constante mudança.

Figura 4-1. Appliance do Access Point apontando para um balanceador de carga



De modo alternativo, é possível ter um ou mais appliances do Access Point apontando para uma instância do servidor individual. Em ambas as abordagens, utilize um balanceador de carga na frente de dois ou mais appliances do Access Point no DMZ.

Figura 4-2. Appliance do Access Point apontando para uma instância do servidor Horizon



Autenticação

A autenticação do usuário é muito similar ao servidor de segurança View. Os métodos compatíveis de autenticação do usuário no Access Point incluem o seguinte.

- O nome de usuário e a senha do Active Directory
- Modo Kiosk. Para obter mais detalhes sobre o modo Kiosk, consulte a documentação do Horizon.
- Autenticação de dois fatores do RSA SecurID, formalmente certificada pela RSA para SecurID
- RADIUS por meio de várias soluções de fornecedores de segurança de dois fatores e de terceiros
- Cartão inteligente, CAC ou certificados de usuário PIV X.509
- SAML

Esses métodos de autenticação são compatíveis em combinação com o Servidor de Conexão do View. Não é obrigatório que o Access Point tenha comunicação direta com o Active Directory. Essa comunicação serve como um proxy por meio do Servidor de Conexão do View, que pode acessar diretamente o Active Directory. Após a sessão do usuário ser autenticada de acordo com a política de autenticação, o Access Point pode encaminhar as solicitações para informações de qualificação, e a área de trabalho e o aplicativo iniciam solicitações para o Servidor de Conexão do View. O Access Point também gerencia a área de trabalho e os manipuladores do protocolo de aplicação para permitir que encaminhem somente tráfego de protocolo autorizado.

O Access Point manipula sozinho a autenticação do cartão inteligente. Isso inclui opções para que o Access Point se comunique com os servidores do Protocolo de Status do Certificado On-Line (OCSP) e para verificar a revogação do certificado X.509, e assim por diante.

Definir configurações do Horizon

É possível implementar o Access Point a partir do Horizon View e do Horizon Air Hybrid-Mode. Para o componente do View do VMware Horizon, o appliance do Access Point cumpre a mesma função que foi anteriormente desempenhada pelo servidor de segurança do View.

Procedimentos

1. Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.
2. Nas Configurações Gerais > Configurações de Serviços de Borda, clique em **Mostrar**.
3. Clique no ícone de engrenagem **Configurações do Horizon**.
4. Na página Configurações do Horizon, altere o NÃO para **SIM** para ativar o Horizon
5. Defina os seguintes recursos de configurações do serviço de borda para o Horizon

Opção	Descrição
Identificador	Definido como padrão para o View. O Access Point pode se comunicar com servidores que utilizem o protocolo View XML, como o Servidor de Conexão do View, o Horizon Air e o Horizon Air Hybrid-Mode.
URL do servidor de conexão	Insira o endereço do servidor Horizon ou do balanceador de carga. Insira-o como https://00.00.00.00
Impressões digitais do URL de destino do proxy	Insira a lista de impressões digitais do servidor do Horizon Se você não fornecer uma lista das impressões digitais, os certificados do servidor deverão ser emitidos por uma CA confiável. Insira os dígitos da impressão digital hexadecimal. Por exemplo, sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3

6 Para configurar a regra do método de autenticação e outras configurações avançadas, clique em **Mais**.

Opção	Descrição
Métodos de autenticação	Selecione os métodos de autenticação a serem utilizados. O padrão é utilizar a autenticação de passagem do nome de usuário e senha. Os métodos de autenticação configurados no Access Point estão listados nos menus suspensos. Para configurar uma autenticação que inclui aplicar um segundo método de autenticação caso a primeira tentativa de autenticação não seja bem-sucedida. a Selecione um método de autenticação no primeiro menu suspenso. b Clique no **+** e selecione E ou OU. c Selecione o segundo método de autenticação no terceiro menu suspenso. Para exigir que os usuários façam a autenticação através de dois métodos de autenticação, altere OU para E no menu suspenso.
URL de verificação de integridade	Se um balanceador de carga estiver configurado, insira o URL que o balanceador de carga utiliza para se conectar e verifique a integridade do appliance do Access Point.
SAML SP	Insira o nome do provedor de serviços SAML para o agente do View XMLAPI. Esse nome deve corresponder ao nome de um metadado de um provedor de serviços configurado ou ser o valor especial DEMO.
PCOIP ativado	Altere NÃO para **SIM** para especificar se o Gateway seguro PCoIP está ativado.
URL externo do proxy	Insira o URL externo do appliance do Access Point. Os clientes utilizam esse URL para conexões seguras por meio do Gateway seguro PCoIP. Esta conexão é utilizada para o tráfego PCoIP. O padrão é o endereço IP do Access Point e porta 4172.
Aviso de dica do cartão inteligente	Altere o NÃO para **SIM** para ativar o appliance do Access Point para suportar o recurso de sugestões de nome de usuário de cartão inteligente. Com o recurso de sugestões de cartão inteligente, o certificado de cartão inteligente de um usuário pode mapear várias contas de usuário do domínio Active Directory.
Blast ativado	Para usar o Gateway seguro Blast, altere o NÃO para **SIM**.
URL externo de Blast	Insira o URL do FQDN do appliance do Access Point que os usuários utilizam para fazer uma conexão segura a partir dos navegadores da web através do Gateway seguro Blast. Insira-o como https://exampleappliance:443
Túnel ativado	Se o túnel seguro do View for utilizado, altere NÃO para **SIM**. O Client utiliza o URL externo para conexões de túnel através do Gateway seguro do View. O túnel é utilizado para tráfego RDP, USB e de redirecionamento de multimídia (multimedia redirection, MMR).
URL externo do túnel	Insira o URL externo do appliance do Access Point. O valor padrão do Access Point padrão será utilizado se não for definido.
Corresponder nome do usuário do Windows	Altere o NÃO para **SIM** para corresponder ao RSA SecurID e ao nome do usuário Windows. Quando definido para SIM, o securID-auth está definido como verdadeiro e a correspondência de nomes de usuário SecurID e Windows é aplicada.

Opção	Descrição
Localização do gateway	Altere o NÃO para **SIM** para ativar a localização de onde as solicitações se originam. O servidor de segurança e o Access Point definem a localização do gateway. O local pode ser externo ou interno.
Windows SSO ativado	Altere o NÃO para **SIM** para ativar a autenticação RADIUS. O login do Windows utiliza as credenciais utilizadas na primeira solicitação de acesso RADIUS bem-sucedida.

7 Clique em **Salvar**.

Implementação do Access Point como proxy reverso

O Access Point pode ser usado como um proxy reverso da web e pode agir como um proxy reverso comum ou como um proxy reverso de autenticação na DMZ.

Cenário de implementação

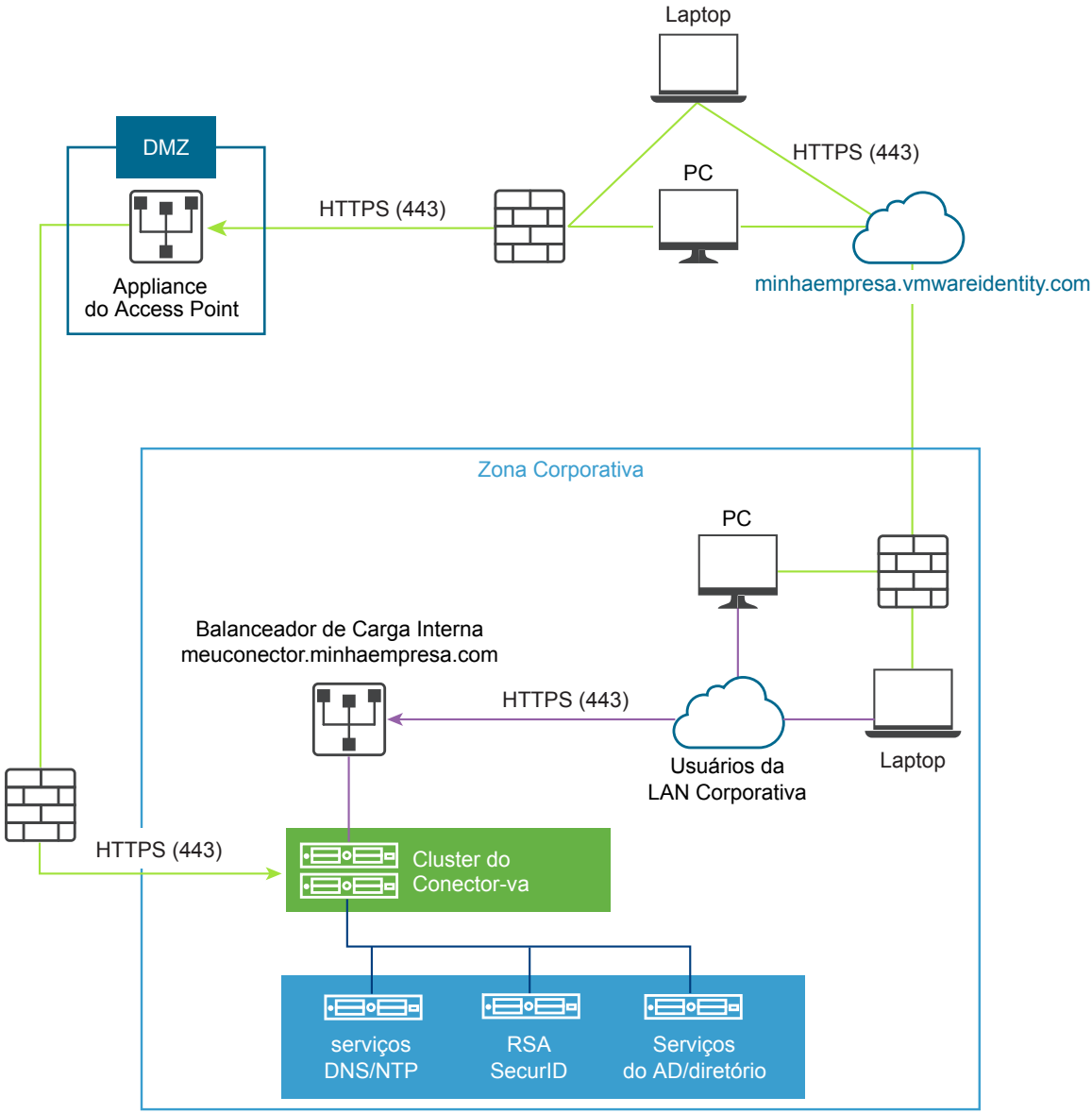
O Access Point fornece acesso remoto para implementação no local do VMware Identity Manager. Os appliances do Access Point são implementados, geralmente, em uma zona de rede desmilitarizada (DMZ). Com o VMware Identity Manager, o appliance do Access Point opera como um proxy reverso da web entre um navegador do usuário e o serviço VMware Identity Manager no centro de dados. O Access Point também ativa o acesso remoto ao catálogo do VMware Identity Manager para iniciar aplicativos do Horizon.

Requisitos para a implementação do Access Point com o VMware Identity Manager

- DNS dividido
- O appliance do VMware Identity Manager deve ter um nome de domínio totalmente qualificado (fully qualified domain name, FQDN) como nome do host.

- O Access Point deve utilizar um DNS interno. Isso significa que o URL de destino de proxy deve usar um FQDN.

Figura 4-3. Appliance do Access Point apontado para o conector



Entendendo o proxy reverso

O Access Point, como uma solução, fornece acesso ao portal de aplicativos para usuários remotos para Single Sign-On e acesso aos recursos. Você ativa o proxy reverso de autenticação em um Service Manager de borda. Atualmente, os métodos de autenticação do RSA SecureID e RADIUS são compatíveis.

Observação Você deve gerar metadados do provedor de identidade antes de habilitar a autenticação no proxy reverso da web.

O Access Point fornece acesso remoto ao VMware Identity Manager e aos aplicativos da web com ou sem autenticação do cliente baseado no navegador e, em seguida, inicia a área de trabalho do Horizon.

- Os clientes baseados em navegadores são suportados usando o RADIUS e o RSA SecurID como os métodos de autenticação.

A compatibilidade do proxy reverso é limitada com a versão 2.8 do Access Point para o VMware Identity Manager e os recursos internos da web, como confluência e WIKI. No futuro, a lista de recursos será ampliada.

Observação As propriedades do `authCookie` e do `unSecurePattern` não são válidas para proxy reverso de autenticação. Você deve usar a propriedade `authMethods` para definir o método de autenticação.

Configurar o proxy reverso para o VMware Identity Manager

É possível configurar o serviço de Proxy Reverso da Web para utilizar o Access Point com o VMware Identity Manager.

Pré-requisitos

Requisitos para a implementação do Access Point com o VMware Identity Manager.

- DNS dividido
- O serviço do VMware Identity Manager deve ter um nome de domínio totalmente qualificado (fully qualified domain name, FQDN) como o nome do host.
- O Access Point deve utilizar um DNS interno. Isso significa que o URL de destino de proxy deve usar um FQDN.

Procedimentos

1. Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.
2. Nas Configurações Gerais > Configurações de Serviços de Borda, clique em **Mostrar**.
3. Clique no ícone de engrenagem **Configurações de Proxy Reverso**.
4. Na página Configurações de Proxy Reverso, altere o NÃO para **SIM** para ativar o proxy reverso.
5. Defina os seguintes recursos de configurações do serviço de borda para o Horizon.

Opção	Descrição
Identificador	O identificador do serviço de borda esta definido como WEB_REVERSE_PROXY.
URL de destino do proxy	Insira o endereço do servidor do VMware Identity Manager. Por exemplo, insira como **`https://vmwareidentitymgr.example.com`**.

Opção	Descrição
Impressões digitais do URL de destino do proxy	Insira uma lista das impressões digitais do certificado do servidor SSL aceitáveis para o URL de destino do proxy. Se você incluir um curinga*, qualquer certificado será permitido. Uma impressão digital tem o formato [alg=]xx:xx, onde alg pode ser sha1, o padrão ou md5. Os 'xx' são dígitos hexadecimais. Por exemplo, sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3 Se você não configurar as impressões digitais, os certificados do servidor deverão ser emitidos por uma Autoridade de Certificação (Certificate Authority, CA) confiável.
Padrão de proxy	Insira os caminhos de URI correspondentes que encaminham para o URL de destino. Por exemplo, insira como `(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`.

6 Para definir outras configurações avançadas, clique em **Mais**.

Opção	Descrição
Métodos de autenticação	O padrão é utilizar a autenticação de passagem do nome de usuário e senha. Os métodos de autenticação configurados no Access Point estão listados nos menus suspensos. Os métodos de autenticação configurados no Access Point estão listados no menu suspenso.
URL de verificação de integridade	Se um balanceador de carga estiver configurado, insira o URL que o balanceador de carga utiliza para se conectar e verifique a integridade do appliance do Access Point.
SAML SP	Insira o nome do provedor de serviços SAML para o agente do View XML API. Esse nome deve corresponder ao nome de um metadado de um provedor de serviços configurado ou ser o valor especial `DEMO`.
Código de ativação	Insira o código de ativação gerado pelo serviço do VMware Identity Manager e importado no Access Point para configurar a confiança entre o VMware Identity Manager e o Access Point.
URL externo	O valor padrão é o URL do host do Access Point e a porta 443. É possível inserir um outro URL externo. Digite como `https://<host:port>`.

7 Clique em **Salvar**.

Implementação do Access Point com o AirWatch Tunnel

O appliance do Access Point é implementado no DMZ. A implementação envolve a instalação de componentes do Access Point e de componentes do AirWatch, como serviços do Agent e do Proxy de túnel

A implementação do Túnel do AirWatch no seu ambiente AirWatch envolve o ajuste do hardware inicial, a configuração das informações do servidor e as configurações do aplicativo no console administrador do AirWatch, além do download de um arquivo de instalação e da execução desse instalador no seu servidor de Túnel do AirWatch.

Você pode configurar manualmente cada um dos serviços de borda após a instalação do OVF ser concluída e os valores serem alterados.

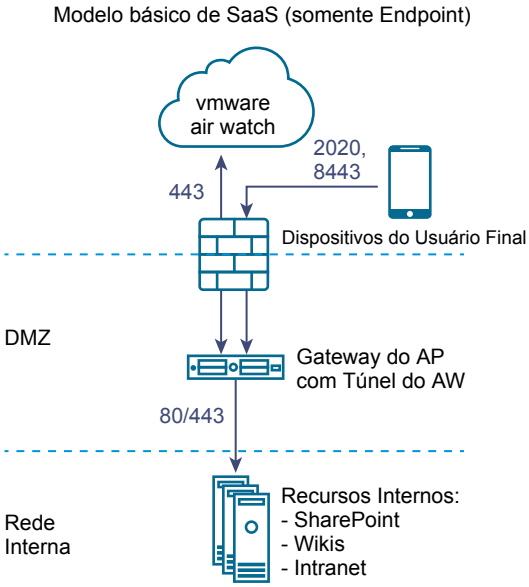
Para obter mais informações sobre a implementação do Access Point com o AirWatch, consulte https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy .

Implementação do proxy de túnel para o AirWatch

A implementação do proxy de túnel garante o tráfego de rede entre um dispositivo de usuário final e um site por meio do aplicativo móvel do Navegador do VMware a partir do AirWatch.

O aplicativo móvel cria uma conexão HTTPS com o servidor do proxy de túnel e protege os dados confidenciais. Para usar um aplicativo interno com o proxy AirWatch Tunnel, verifique se o AirWatch SDK está incorporado em seu aplicativo, o que lhe oferece capacidades de encapsulamento com este componente.

Figura 4-4. Implementação de proxy de túnel

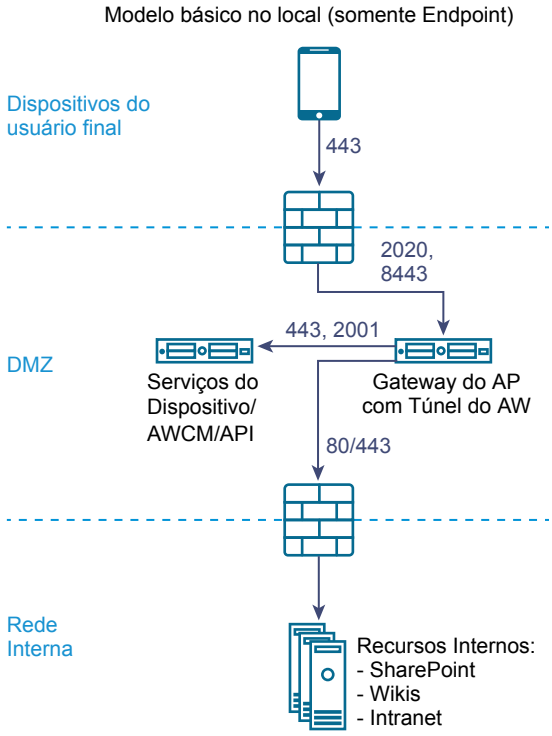


Implementação de túnel por aplicativo com o AirWatch

A Implementação de túnel por aplicativo permite que os aplicativos internos e públicos acessem com segurança recursos corporativos residentes em sua rede interna segura.

Utiliza capacidades por aplicativo oferecidas pelos sistemas operacionais, como o iOS 7 e superior ou o Android 5.0 e superior. Esses sistemas operacionais permitem que aplicativos específicos aprovados pelos administradores de mobilidade acessem recursos internos em uma base de aplicativo por aplicativo. A vantagem de usar essa solução é que nenhuma alteração de código é necessária para os aplicativos móveis. O suporte do sistema operacional oferece uma experiência contínua ao usuário e segurança adicional diferentes de qualquer outra solução personalizada.

Figura 4-5. Implementação de túnel por aplicativo



Definir as configurações de túnel por aplicativo e de proxy para o AirWatch

A implementação do proxy de túnel garante o tráfego de rede entre um dispositivo de usuário final e um site por meio do aplicativo móvel do Navegador do VMware.

Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Nas Configurações Gerais > Configurações de Serviços de Borda, clique em **Mostrar**.

3 Clique no ícone de engrenagem **Configurações de túnel por aplicativo e de proxy**.

4 Altere o NÃO para **SIM** para ativar o proxy de túnel.

5 Defina os seguintes recursos de configurações do serviço de borda.

Opção	Descrição
Identificador	Definido como padrão para o View. O Access Point pode se comunicar com servidores que utilizem o protocolo View XML, como o Servidor de Conexão do View, o Horizon Air e o Horizon Air Hybrid-Mode.
URL do servidor da API	Insira o URL do servidor da API do AirWatch. Por exemplo, insira como https://example.com:<port>.
Nome de usuário do servidor da API	Insira a nome de usuário para fazer login no servidor da API.
Senha do servidor da API	Insira a senha para fazer login no servidor da API.

Opção	Descrição
Código do grupo de organização	Insira a organização do usuário.
Nome do host do servidor AirWatch	Insira o nome do host do servidor AirWatch.

6 Para definir outras configurações avançadas, clique em **Mais**.

Opção	Descrição
Proxy de saída do AirWatch	Altere o NÃO para **SIM** para inicializar o serviço de Proxy de Túnel.
HOST do proxy de saída	Insira o nome do host onde o proxy de saída está instalado. **Observação** Este não é o Proxy de Túnel.
PORTA do proxy de saída	Insira o número da porta do proxy de saída.
Nome de usuário do proxy de saída	Insira a nome de usuário para fazer login no proxy de saída.
Senha do proxy de saída	Insira a senha para fazer login no proxy de saída.
Autenticação NTLM	Altere o NÃO para **SIM** para especificar que a solicitação de proxy de saída exige a autenticação NTLM.
Usar para o proxy do AirWatch Tunnel	Altere o NÃO para **SIM** para utilizar este proxy como um proxy de saída para o AirWatch Tunnel. Se não estiver habilitado, o Access Point utilizará esse proxy para a chamada da API inicial a fim de obter a configuração do console de administração do AirWatch.

7 Clique em **Salvar**.

Configuração do Access Point usando Certificados TLS/SSL

5

Você deve configurar os Certificados TLS/SSL para os appliances do Access Point.

Observação A configuração dos certificados TLS/SSL para o appliance do Access Point aplica-se somente ao Horizon View, ao Horizon Air Hybrid-Mode e ao proxy reverso da web.

Configurando certificados TLS/SSL para appliances do Access Point

O TLS/SSL é necessário para conexões de clientes aos appliances do Access Point. Appliances do Access Pointe servidores intermediários voltados para o cliente que terminam conexões TLS/SSL necessitam de certificados de servidor TLS/SSL.

Certificados de servidor TLS/SSL são assinados por uma Autoridade de Certificação (CA). Uma CA é uma entidade confiável que garante a identidade do certificado e de seu criador. Quando um certificado é assinado por uma CA confiável, os usuários passam a não receber mensagens pedindo a verificação do certificado e os dispositivos cliente leves podem se conectar sem necessitar de configurações adicionais.

Um certificado de servidor TLS/SSL padrão é gerado ao implementar um appliance do Access Point. Para ambientes de produção, a VMware recomenda a substituição do certificado padrão o mais rápido possível. O certificado padrão não é assinado por uma CA confiável. Utilize o certificado padrão somente em um ambiente que não é de produção.

Selecionando o tipo correto de certificado

Você pode utilizar vários tipos de certificados TLS/SSL com o Access Point. É crucial selecionar o tipo de certificado correto para a sua implementação. Tipos diferentes de certificado variam em termos de custo, dependendo do número de servidores nos quais podem ser utilizados.

Siga as recomendações de segurança da VMware utilizando nomes de domínio totalmente qualificados (FQDNs) para os certificados, independentemente do tipo selecionado. Não utilize um nome de servidor ou endereço IP simples, mesmo para comunicações dentro de seu domínio interno.

Certificado de nome único de servidor

Você pode gerar um certificado com um nome da entidade para um servidor específico. Por exemplo: `dept.exemplo.com`.

Este tipo de certificado será útil se, por exemplo, apenas um appliance do Access Pointprecisar de um certificado.

Ao enviar uma solicitação de assinatura de certificado a uma Autoridade de Certificação, você fornece o nome de servidor que estará associado com o certificado. Certifique-se de que o appliance do Access Pointpossa resolver o nome de servidor fornecido para que ele corresponda ao nome associado com o certificado.

Nomes Alternativos da Entidade

Um Nome Alternativo da Entidade (Subject Alternative Name, SAN) é um atributo que pode ser adicionado a um certificado quando ele está sendo emitido. Você utiliza este atributo para adicionar nomes de entidade (URLs) a um certificado para que ele possa validar mais de um servidor

Por exemplo, três certificados podem ser emitidos para os appliances do Access Pointque estejam atrás de um balanceador de carga: `ap1.exemplo.com`, `ap2.exemplo.com` e `ap3.exemplo.com`. Ao adicionar um Nome Alternativo da Entidade que representa o nome de host do balanceador de carga, como `horizon.exemplo.com` neste exemplo, o certificado será válido, pois será correspondente ao nome de host especificado pelo cliente.

Certificado Curinga

Um certificado curinga é gerado para que possa ser utilizado para vários serviços. Por exemplo: `*.exemplo.com`.

Um curinga será útil se muitos servidores precisarem de um certificado. Se outros aplicativos no ambiente além dos appliances do Access Pointprecisarem de certificados TLS/SSL, você também poderá utilizar um certificado curinga para estes servidores. No entanto, se você utilizar um certificado curinga que esteja compartilhado com outros serviços, a segurança do produtoVMware Horizontambém dependerá da segurança destes outros serviços.

Observação Você pode utilizar um certificado curinga somente em um nível único de domínio. Por exemplo, um certificado curinga com o nome de entidade `*.exemplo.com` pode ser utilizado para o subdomínio `dept.exemplo.com` mas não para `dept.it.exemplo.com`.

Os certificados importados para o appliance do Access Pointdevem ser confiáveis para as máquinas clientes e também devem ser aplicáveis a todas as instâncias do Access Pointe de qualquer balanceador de carga, utilizando curingas ou utilizando certificados de Nome Alternativo de Entidade (SAN).

Converter arquivos de certificado para o formato PEM de uma linha

Para utilizar a API REST do Access Pointpara configurar definições de certificado ou para utilizar os scripts do PowerShell, você deve converter o certificado em arquivos de formato PEM para a cadeia de certificados e a chave privada, e deve converter os arquivos `.pem` em um formato de uma linha que inclua caracteres newline integrados.

Ao configurar o Access Point, há três tipos possíveis de tipos de certificados que talvez seja preciso converter.

- Você deve sempre instalar e configurar um certificado de servidor TLS/SSL para o appliance do Access Point.
- Se planeja utilizar a autenticação com cartão inteligente, você deve instalar e configurar o certificado do emissor de CA confiável para o certificado que será colocado no cartão inteligente.
- Se planeja utilizar a autenticação com cartão inteligente, a VMware recomenda a instalação e configuração de um certificado raiz para o certificado de autoridade de certificação de assinatura do certificado de servidor SAML que está instalado no appliance do Access Point.

Para todos estes tipos de certificados, realize o mesmo procedimento para converter o certificado para o arquivo de formato PEM que contém a cadeia de certificados. Para os certificados de servidor TSL/SSL e certificados raiz, também é possível converter cada arquivo para o arquivo PEM que contém a chave privada. Você deve converter cada arquivo `.pem` para um formato de uma linha que possa ser passado em uma cadeia de caracteres de JSON à API REST do Access Point.

Pré-requisitos

- Verifique se possui o arquivo do certificado. O arquivo pode estar no formato PKCS#12 (`.p12` ou `.pfx`) ou no formato Java JKS ou JCEKS.
- Familiarize-se com a ferramenta de linha de comando do `openssl` que você usará para converter o certificado. Consulte https://www.openssl.org/docs/apps/openssl.html.
- Se o certificado estiver no formato Java JKS ou JCEKS, familiarize-se com a ferramenta de linha de comando `keytool` do Java para converter o certificado primeiramente para o formato `.p12` ou `.pks` antes de convertê-lo para arquivos `.pem`.

Procedimentos

1 Se seu certificado estiver no formato Java JKS ou JCEKS, utilize o `keytool` para converter o certificado para o formato `.p12` ou `.pks`.

Importante Utilize a mesma senha de origem e destino durante essa conversão.

2 Se seu certificado estiver no formato PKCS#12 (`.p12` ou `.pfx`) ou após o certificado ser convertido para o formato PKCS#12, utilize o `openssl` para converter o certificado para arquivos `.pem`.

   Por exemplo, se o nome do certificado é `mycaservercert.pfx`, utilize os seguintes comandos para converter o certificado:

   ```
   openssl pkcs12 –in mycaservercert.pfx –nokeys –out mycaservercert.pem
   openssl pkcs12 –in mycaservercert.pfx –nodes –nocerts –out mycaservercert.pem
   openssl rsa –in mycaservercertkey.pem –check –out mycaservercertkeyrsa.pem
   ```

3 Edite `mycaservercert.pem` e remova quaisquer entradas de certificado desnecessárias. Ele deve conter o certificado de servidor SSL seguido por quaisquer certificados de autoridade de certificação intermediários necessários e o certificado de autoridade de certificação raiz.

4 Utilize o seguinte comando UNIX para converter cada arquivo `.pem` para um valor que possa ser passado em uma cadeia de caracteres de JSON à API REST do Access Point:

   ```
   awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' cert–name.pem
   ```

   Neste exemplo, *`cert–name`*`.pem` é o nome do arquivo do certificado.

   O novo formato coloca todas as informações do certificado em uma única linha com caracteres integrados de nova linha. Se você possui um certificado intermediário, esse certificado deve também estar no formato de uma linha e adicionar-se ao primeiro certificado para que ambos os certificados estejam na mesma linha.

Você pode agora configurar certificados para o Access Pointutilizando estes arquivos `.pem` com os scripts do PowerShell anexados à publicação do blog "Utilizando o PowerShell para Implementar o VMware Access Point", disponível em https://communities.vmware.com/docs/DOC-30835. De forma alternativa, você pode criar e utilizar uma solicitação JSON para configurar o certificado.

Próximo passo

Se você converteu um certificado de servidor TLS/SSL, consulte Substituir o certificado padrão do servidor TLS/SSL pelo Access Point. Para certificados de cartão inteligente, consulte Configurando a autenticação de certificado ou de cartão inteligente no appliance do Access Point.

Substituir o certificado padrão do servidor TLS/SSL pelo Access Point

Para armazenar um certificado de servidor TLS/SSL assinado pela CA no appliance do Access Pointvocê deve converter o certificado para o formato correto e utilizar scripts do PowerShell ou a API REST do Access Pointpara configurar o certificado.

Para ambientes de produção, a VMware recomenda enfaticamente a substituição do certificado padrão o mais rápido possível. O certificado padrão do servidor TLS/SSL que é gerado ao implementar um appliance do Access Pointnão é assinado por uma Autoridade de Certificação Confiável.

Importante Utilize também este procedimento para a substituição periódica de um certificado que foi assinado por uma CA confiável antes da expiração do certificado, o que pode acontecer a cada dois anos.

Esse procedimento descreve como utilizar a API REST para substituir o certificado. Uma alternativa mais simples pode ser a utilização de scripts do PowerShell anexados à publicação do blog "Utilizando o PowerShell para Implementar o VMware Access Point," disponível em https://communities.vmware.com/docs/DOC-30835. Se você já implementou um appliance chamado Access Point, executar o script novamente desligará o appliance. Exclua-o e implemente-o novamente com as configurações atuais que especificar.

Pré-requisitos

- A menos que já possua um certificado de servidor TLS/SSL válido e sua chave privada, obtenha um novo certificado assinado de uma Autoridade de Certificação. Ao gerar uma solicitação de assinatura de certificado (certificate signing request, CSR) para obter um certificado, certifique-se de que também seja gerada uma chave privada. Não gere certificados para servidores utilizando um valor KeyLength inferior a 1024.

  Para gerar o CSR, é preciso conhecer o nome de domínio totalmente qualificado (FQDN) que os dispositivos cliente utilizam para se conectar ao appliance do Access Pointe a unidade organizacional, organização, cidade, estado e país para preencher o nome da Entidade.
- Converta o certificado para arquivos de formato PEM-e converta os arquivos `.pem` para o formato de uma linha. Consulte Converter arquivos de certificado para o formato PEM de uma linha.
- Familiarize-se com a API REST doAccess Point. A especificação para esta API está disponível no seguinte URL na máquina virtual onde o Access Point está instalado: `https://access-point-appliance.exemplo.com:9443/rest/swagger.yaml`.

Procedimentos

1 Crie uma solicitação JSON para enviar o certificado ao appliance do Access Point.

```
{
  "privateKeyPem": "string",
  "certChainPem": "string"
}
```

Neste exemplo, os valores de *string* são os valores PEM JSON de uma linha que você criou conforme descrito nos pré-requisitos.

2 Utilize um cliente REST, como o `curl` ou o `postman`, para utilizar a solicitação JSON para invocar a API REST do Access Point e armazene o certificado e chave no appliance do Access Point.

O seguinte exemplo utiliza um comando do `curl`. No exemplo, *access-point-appliance.exemplo.com* é o nome de domínio totalmente qualificado do appliance do Access Point e *certificado*.json é a solicitação JSON que você criou na etapa anterior.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-
appliance.exemplo.com:9443/rest/v1/config/certs/ssl < ~/cert.json
```

Próximo passo

Se a CA que assinou o certificado não tiver reputação renomada, configure clientes para confiar nos certificados raiz e intermediário.

Alterar os protocolos de segurança e os conjuntos de codificação utilizados para a comunicação TLS ou SSL

Embora na maioria dos casos, as configurações padrão não precisem ser alteradas, você pode configurar protocolos de segurança e algoritmos de criptografia que são utilizados para codificar as comunicações entre clientes e o appliance doAccess Point.

A configuração padrão inclui conjuntos de criptografia que utilizam a Criptografia AES de 128 ou 256 bits, exceto para algoritmos DH anônimos e os classifica por força. Por padrão, o TLS v.1.1 e o TLS v1.2 estão ativados. O TLS v1.0 e o SSL v3.0 estão desativados.

Pré-requisitos

- Familiarize-se com a API REST doAccess Point. A especificação para esta API está disponível no seguinte URL na máquina virtual onde o Access Point está instalado: `https://access-point-appliance.exemplo.com:9443/rest/swagger.yaml`.
- Familiarize-se com as propriedades específicas para configurar os protocolos e conjuntos de criptografia: `cipherSuites`, `ssl30Enabled`, `tls10Enabled`, `tls11Enabled` e `tls12Enabled`.

Procedimentos

1 Crie uma solicitação JSON para especificar os protocolos e conjuntos de criptografia a serem utilizados.

O exemplo a seguir possui as configurações padrão.

```
{
"cipherSuites":
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "true",
  "tls12Enabled": "true"
}
```

2 Utilize um cliente REST, como o `curl` ou o `postman`, para utilizar a solicitação JSON invocar a API REST do Access Point e configurar os protocolos e conjuntos de criptografia.

No exemplo, *access-point-appliance.exemplo.com* é o nome de domínio totalmente qualificado do appliance do Access Point .

```
curl –k –d @– –u 'admin' –H "Content–Type: application/json" –X PUT https://access–point–
appliance.exemplo.com:9443/rest/v1/config/system < ~/ciphers.json
```

ciphers.json é a solicitação JSON criada nada etapa anterior.

São utilizados os conjuntos e protocolos de criptografia que você especificou.

Configuração da autenticação em DMZ

6

Ao implementar o VMware Access Point inicialmente, a autenticação da senha do Active Directory está definida como o padrão. Os usuários inserem o nome de usuário e a senha do Active Directory e essas credenciais são enviadas por um sistema de back-end para autenticação.

É possível configurar o serviço do Access Point para realizar a autenticação de Certificado/Cartão Inteligente, autenticação do RSA SecurID, autenticação RADIUS e RSA Adaptive Authentication.

Observação A autenticação da senha com o Active Directory é o único método de autenticação que pode ser usado com uma implementação do AirWatch.

Este capítulo inclui os seguintes tópicos:

- Configurando a autenticação de certificado ou de cartão inteligente no appliance do Access Point
- Configurar a Autenticação RSA SecurID no Access Point
- Configurando o RADIUS para o Access Point
- Configurando o RSA Adaptive Authentication no Access Point
- Gerar metadados SAML do Access Point

Configurando a autenticação de certificado ou de cartão inteligente no appliance do Access Point

É possível configurar a autenticação de certificado x509 no Access Point para permitir que os clientes façam a autenticação com certificados em sua área de trabalho ou dispositivos móveis ou usem um adaptador de cartão inteligente para autenticação.

A autenticação com base no certificado é baseada no que o usuário tem (a chave privada ou o cartão inteligente) e no que a pessoa sabe (a senha para a chave privada ou o PIN do cartão inteligente). A autenticação de cartão inteligente fornece a autenticação de dois fatores verificando o que a pessoa possui (o cartão inteligente) e o que a pessoa sabe (o PIN). Os usuários finais podem utilizar os cartões inteligentes para efetuar logon em um sistema operacional de área de trabalho remota do View e para acessar aplicativos ativados por cartão inteligente, como um aplicativo de e-mail que utiliza o certificado para assinar e-mails e provar a identidade do remetente.

Com este recurso, a autenticação de certificado de cartão inteligente é realizada em oposição ao serviço do Access Point. O Access Point usa a asserção SAML para comunicar informações sobre o certificado X.509 de usuário final e o PIN do cartão inteligente ao servidor Horizon.

É possível configurar a verificação de revogação de certificado para evitar que os usuários com certificados de usuário revogados façam a autenticação. Os certificados são frequentemente revogados quando um usuário deixa uma organização, perde um cartão inteligente ou muda de um departamento para outro. Há suporte para a verificação de revogação de certificados com as listas de certificados revogados (certificate revocation lists, CRLs) e com o Protocolo de status de certificado on-line (Online Certificate Status Protocol, OCSP). Uma CRL é uma lista de certificados revogados publicados pela CA que emitiu os certificados. O OCSP é um protocolo de validação de certificado utilizado para obter o status de revogação de um certificado.

É possível definir ambos CRL e OCSP na mesma configuração do adaptador de autenticação de certificado. Ao configurar os dois tipos de verificação de revogação de certificado e a caixa de seleção Usar CRL em caso de falha do OCSP for habilitada, o OCSP será verificado primeiro e, se o OCSP falhar, a verificação de revogação fará fallback para a CRL. A revogação de verificação não utilizará o OCSP se a CRL falhar.

Você também pode configurar a autenticação, de modo que o Access Point exija a autenticação do cartão inteligente, mas, então, a autenticação também passará pelo servidor, exigindo a autenticação do Active Directory.

Observação Para o VMware Identity Manager, a autenticação é sempre passada através do Access Point ao serviço do VMware Identity Manager. Será possível configurar a autenticação do cartão inteligente para que seja realizada no appliance do Access Point somente se o Access Point estiver sendo utilizado com o Horizon 7.

Configurar uma autenticação de certificado no Access Point

Você habilita e configura a autenticação de certificado a partir do console de administração do Access Point.

Pré-requisitos

- Obtenha o certificado raiz e os certificados intermediários da Autoridade de Certificação (Certificate Authority, CA) que assinou os certificados apresentados por seus usuários. Consulte Obter Certificados de Autoridade de Certificação
- Verifique se os metadados do Access Point SAML estão adicionados no provedor de serviços e se os metadados SAML do provedor de serviço são copiados ao appliance do Access Point.
- (Opcional) Lista de Identificadores de Objeto (Object Identifier, OID) das políticas de certificado válidas para a autenticação de certificado.
- Para a verificação de revogação, a localização do arquivo da CRL e o URL do servidor OCSP.
- (Opcional) Localização do arquivo de certificado de assinatura de resposta OCSP.

- Conteúdo do formulário de consentimento se aparecer um formulário de consentimento antes da autenticação.

Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.

3 Clique na engrenagem na linha do Certificado X.509.

4 Configure o formulário do Certificado X.509.

Um asterisco indica uma caixa de texto obrigatória. Todas as outras caixas de texto são opcionais.

Opção	Descrição
Ativar Certificado X.509	Altere o NÃO para **SIM** para ativar a autenticação do certificado.
***Nome**	Nomeie este método de autenticação.
***Certificados de CA raiz e intermediária**	Clique em **Selecionar** para selecionar os arquivos de certificado a serem carregados. É possível selecionar vários certificados de CA intermediária e de CA raiz codificados como DER ou PEM.
Tamanho do cache CRL	Insira o tamanho do cache da lista de revogação de certificado. O padrão é 100.
Ativar revogação de certificado	Altere o NÃO para **SIM** para ativar a verificação de revogação de certificado. A verificação de revogação impede a autenticação dos usuários que têm certificados de usuário revogados.
Usar CRL dos certificados	Marque a caixa de seleção para usar a lista de revogação de certificados (certificate revocation list, CRL) publicada pela CA que emitiu os certificados para validar o status de um certificado revogado ou não revogado.
Local da CRL	Digite o caminho do arquivo do servidor ou o caminho do arquivo local a partir do qual recupera-se a CRL.
Ativar a revogação do OCSP	Marque a caixa de seleção para usar o protocolo de validação de certificado do Protocolo de status de certificado on-line (Online Certificate Status Protocol, OCSP) a fim de obter o status de revogação de um certificado.
Usar a CRL em caso de falha do OCSP	Se você configurar a CRL e o OCSP, poderá marcar esta caixa para fazer fallback ao uso da CRL se a verificação do OCSP não estiver disponível.
Enviar nonce do OCSP	Marque esta caixa de seleção se deseja que o identificador único da solicitação do OCSP seja enviado na resposta.
URL do OCSP	Se você ativou a revogação do OCSP, digite o endereço do servidor do OCSP para a verificação de revogação.
Certificado de assinatura do respondente do OCSP	Insira o caminho ao certificado OCSP para o respondente, */path/to/file.cer*.
Ativar formulário de consentimento antes da autenticação	Marque esta caixa de seleção para incluir uma página do formulário de consentimento que aparecerá antes de os usuários fazerem login no Workspace Portal ONE usando a autenticação de certificado.
Conteúdo do formulário de consentimento	Digite aqui o texto que será exibido no formulário de consentimento.

5 Clique em **Salvar**.

Próximo passo

Quando a autenticação do Certificado X.509 é definida e o appliance do Access Point é configurado atrás de um balanceador de carga, certifique-se de que o Access Point esteja configurado com uma passagem do SSL no balanceador de carga e não esteja configurado para encerrar o SSL no balanceador de carga. Essa configuração assegura que o handshake do SSL esteja entre o Access Point e o cliente para passar o certificado ao Access Point.

Obter Certificados de Autoridade de Certificação

Você deve obter todos os certificados de CA (autoridade de certificação) para todos os certificados de usuários confiáveis nos cartões inteligentes apresentados por seus usuários e administradores. Esses certificados incluem certificados raiz e podem incluir certificados intermediários, se o certificado de cartão inteligente do usuário foi emitido por uma autoridade de certificado intermediária.

Se você não possui o certificado raiz ou intermediário da CA que assinou os certificados nos cartões inteligente apresentados por seus usuários e administradores, é possível exportar os certificados de um certificado de usuário assinado pela CA ou de um cartão inteligente que contenha um certificado assinado pela CA. Consulte Obter o certificado de CA do Windows.

Procedimentos

- Obtenha os certificados CA de uma das seguintes origens.
  - Um servidor Microsoft IIS que esteja executando Serviços de Certificado da Microsoft. Consulte o site da Microsoft TechNet para obter informações sobre como instalar o Microsoft IIS, emitir certificados e distribuí-los em sua organização.
  - O certificado raiz público de uma CA confiável. Esta é a origem mais comum de um certificado raiz em ambientes que já possuem uma infraestrutura de cartão inteligente e uma abordagem padronizada para a distribuição e autenticação de cartões inteligentes.

Obter o certificado de CA do Windows

Se você possui um certificado de usuário assinado por uma autoridade de certificação ou um cartão inteligente que contém um certificado assinado por uma autoridade de certificação e o Windows confia no certificado raiz, é possível exportar o certificado raiz do Windows. Se o emissor do certificado de usuário é uma autoridade de certificação intermediária, é possível exportar este certificado.

Procedimentos

1. Se um certificado de usuário está em um cartão inteligente, insira o cartão inteligente em um leitor para adicionar o certificado de usuário ao seu armazenamento pessoal.

   Se o certificado de usuário não aparecer em seu armazenamento pessoal, utilize o software de leitura para exportá-lo para um arquivo. Este arquivo é usado na Etapa 4 deste procedimento.
2. No Internet Explorer, selecione **Ferramentas > Opções de Internet**.
3. Na guia **Conteúdo**, clique em **Certificados**.

4 Na guia **Pessoal**, selecione o certificado que deseja utilizar e clique em **Visualizar**.

Se o certificado de usuário não aparecer na lista, clique em **Importar** para importá-lo manualmente de um arquivo. Após o certificado ser importado, você pode selecioná-lo na lista.

5 Na guia **Caminho de Certificação**, selecione o certificado no topo da árvore e clique em **Visualizar Certificado**.

Se o certificado de usuário estiver assinado como parte de uma hierarquia de confiança, o certificado assinado poderá ser assinado por outro certificado de nível superior. Selecione o certificado de parente (aquele que assinou o certificado de usuário) como seu certificado raiz. Em alguns casos, o emissor pode ser uma autoridade de certificação intermediária.

6 Na guia **Detalhes**, clique em **Copiar para Arquivo**.

O **Assistente de Exportação de Certificado** aparece.

7 Clique em **Avançar > Avançar** e digite um nome e localização para o arquivo que deseja exportar.

8 Clique em **Avançar** para salvar o arquivo como um certificado raiz em um local especificado.

Configurar a Autenticação RSA SecurID no Access Point

Após o appliance do Access Point ser configurado como o agente de autenticação no servidor RSA SecurID, é necessário adicionar as informações de configuração do RSA SecurID no appliance do Access Point.

Pré-requisitos

- Verifique se o Gerenciador da Autenticação RSA (o servidor RSA SecurID) está instalado e adequadamente configurado.
- Faça o download do arquivo compactado sdconf.rec a partir do servidor RSA SecurID e extraia o arquivo de configuração do servidor.

Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.

3 Clique na engrenagem na linha do RSA SecurID.

4 Configure a página do RSA SecurID.

As informações usadas e os arquivos gerados no servidor do RSA SecurID são necessários ao configurar a página do SecurID.

Opção	Ação
Ativar RSA SecurID	Altere o NÃO para **SIM** para ativar a autenticação do SecurID.
*Nome	O nome é securid-auth.

Opção	Ação
*Número de iterações	Insira o número de tentativas de autenticação permitidas. Este é o número máximo de tentativas de login com falha ao usar o token do RSA SecurID. O padrão é de 5 tentativas. **Observação** Quando mais de um diretório é configurado e você implementa a autenticação do RSA SecurID com diretórios adicionais, configure o **Número de tentativas de autenticação permitidas** com o mesmo valor para cada configuração do RSA SecurID. Se o valor não for o mesmo, haverá falha na autenticação do SecurID.
*Nome do HOST externo	Informe o endereço IP da instância do Access Point. O valor inserido deve corresponder ao valor usado quando você adicionou o appliance do Access Point como um agente de autenticação ao servidor do RSA SecurID.
*Nome do HOST interno	Digite o valor atribuído ao prompt do **Endereço IP** no servidor do RSA SecurID.
*Configuração do servidor	Clique em Alterar para carregar o arquivo de configuração do servidor do RSA SecurID. Primeiro, você deve baixar o arquivo compactado do servidor do RSA SecurID e extrair o arquivo de configuração do servidor, que, por padrão, é denominado `sdconf.rec`.
*Sufixo da ID do nome	Insira o nameId que permite que o View forneça a experiência TrueSSO.

Configurando o RADIUS para o Access Point

É possível configurar o Access Point para que os usuários sejam obrigados a usar a autenticação RADIUS. Você configura as informações do servidor RADIUS no appliance do Access Point.

O suporte do RADIUS oferece uma ampla gama de opções de autenticação alternativa de dois fatores baseada em token. Como soluções de autenticação de dois fatores, como o RADIUS, trabalham com gerenciadores de autenticação instalados em servidores separados, é necessário ter o servidor RADIUS configurado e acessível ao serviço do gerenciador de identidade

Quando os usuários fazem o login e a autenticação RADIUS é habilitada, uma caixa de diálogo de login especial aparece no navegador. Os usuários inserem seu nome de usuário e senha da autenticação RADIUS na caixa de diálogo de login. Se o servidor RADIUS emitir um desafio de acesso, o Access Point exibirá uma caixa de diálogo solicitando uma segunda senha. Atualmente, o suporte para desafios do RADIUS é limitado à solicitação para inserção de texto.

Após os usuários inserirem as credenciais na caixa de diálogo, o servidor RADIUS pode enviar uma mensagem de texto SMS ou e-mail ou texto utilizando algum outro mecanismo de banda externa ao telefone celular do usuário com um código. O usuário pode inserir este texto e código na caixa de diálogo de login para concluir a autenticação.

Se o servidor RADIUS fornecer a habilidade de importar usuários do Active Directory, os usuários finais poderão primeiramente ser solicitados a fornecer as credenciais do Active Directory antes da solicitação do nome de usuário e senha de autenticação RADIUS.

Configurar a autenticação RADIUS

No appliance do Access Point, deve-se ativar a autenticação RADIUS, inserir as definições de configuração do servidor RADIUS e alterar o tipo de autenticação para a autenticação RADIUS.

Pré-requisitos

- Verifique se o servidor a ser utilizado como o servidor do gerenciador da autenticação possui o software RADIUS instalado e configurado. Defina o servidor RADIUS e, em seguida, configure as solicitações do RADIUS a partir do Access Point. Consulte as guias de configuração do fornecedor do RADIUS para obter mais informações sobre como configurar o servidor RADIUS.

São necessárias as seguintes informações do servidor RADIUS.

- Endereço IP ou nome DNS do servidor RADIUS.
- Números das portas de autenticação. A porta de autenticação é normalmente 1812.
- Tipo de autenticação. Os tipos de autenticação incluem PAP, Password Authentication Protocol (Protocolo de autenticação de senha), CHAP, Challenge Handshake Authentication Protocol (Protocolo de autenticação por desafios de identidade), MSCHAP1, MSCHAP2, Microsoft Challenge Handshake Authentication Protocol versões 1 e 2 (Protocolo de autenticação por desafios de identidade).
- Segredo compartilhado do RADIUS utilizado para criptografia e descriptografia nas mensagens do protocolo do RADIUS.
- Tempo limite específico e valores de novas tentativas necessários para a autenticação RADIUS

Procedimentos

1. Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.
2. Nas Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.
3. Clique na engrenagem na linha do RADIUS.

Opção	Ação
Ativar RADIUS	Altere o NÃO para **SIM** para ativar a autenticação RADIUS.
Nome*	O nome é radius-auth
Tipo de autenticação*	Insira o protocolo de autenticação suportado pelo servidor RADIUS. PAP, CHAP, MSCHAP1 OU MSCHAP2.
Segredo compartilhado*	Insira o segredo compartilhado do RADIUS.
Número de tentativas de Autenticação permitidas *	Digite o número máximo de tentativas de login falhas ao usar o RADIUS para fazer o login. O padrão é de três tentativas.

Opção	Ação
Número de tentativas para o servidor RADIUS*	Insira o número total de novas tentativas. Se o servidor primário não responder, o serviço aguardará o tempo configurado antes de tentar novamente.
Tempo limite do servidor em segundos*	Insira o tempo limite do servidor RADIUS em segundos. Depois disso, uma nova tentativa será enviada se o servidor RADIUS não responder.
Nome do host do servidor Radius *	Insira o nome do host ou o endereço IP do servidor RADIUS.
Porta de autenticação*	Insira o número da porta de autenticação do Radius. A porta é normalmente 1812.
Prefixo de território	(Opcional) A localização da conta do usuário é chamada território. Se você especificar uma cadeia de prefixo de território, a cadeia de caracteres será colocada no começo do nome de usuário quando o nome for enviado ao servidor RADIUS. Por exemplo, se o nome de usuário for inserido como jdoe e o prefixo de território DOMAIN-A\ for especificado, o nome de usuário DOMAIN-A\jdoe será enviado ao servidor RADIUS. Se você não configurar esses campos, somente o nome de usuário inserido será enviado.
Sufixo de território	(Opcional) Se você configurar um sufixo de território, a cadeia de caracteres será colocada no final do nome de usuário. Por exemplo, se o sufixo for @myco.com, o nome de usuário jdoe@myco.com será enviado ao servidor RADIUS.
Sufixo da ID do nome	Insira o nameId que permite que o View forneça a experiência True SSO.
Dica de senha da página de logon	Insira a cadeia de caracteres de texto a ser exibida na mensagem na página de logon do usuário para direcioná-los a inserir a senha Radius correta. Por exemplo, se este campo estivesse configurado com a **senha AD primeiro e, em seguida, a senha SMS**, a mensagem da página de logon seria **Insira sua senha AD primeiro e, em seguida, a senha SMS.** A cadeia de caracteres de texto padrão é **Senha RADIUS**.
Ativar servidor secundário	Altere o NÃO para **SIM** para configurar um servidor RADIUS secundário para alta disponibilidade. Configure as informações de servidor secundário conforme descrito na etapa 3.

4 Clique em **Salvar**.

Configurando o RSA Adaptive Authentication no Access Point

O RSA Adaptive Authentication pode ser implementado para fornecer uma autenticação multifator mais forte do que apenas a autenticação de nome de usuário e senha em relação ao Active Directory. O Adaptive Authentication monitora e autentica as tentativas de login do usuário com base em níveis e políticas de risco.

Quando o Adaptive Authentication está habilitado, os indicadores de risco especificados nas políticas de risco estabelecidas no aplicativo de Gerenciamento da Política da RSA e na configuração do Access Point da autenticação adaptativa são usados para determinar se um usuário é autenticado com o nome de usuário e a senha ou se são necessárias informações adicionais para autenticar o usuário.

Métodos de autenticação do RSA Adaptive Authentication suportados

Os métodos de autenticação forte do RSA Adaptive Authentication suportados no Access Point são a autenticação de banda externa via telefone, e-mail ou mensagem de texto SMS e perguntas de desafio. Você habilita no serviço os métodos do RSA Adaptive Authentication que podem ser fornecidos. As políticas do RSA Adaptive Authentication determinam o método de autenticação secundário a ser usado.

A autenticação de banda externa é um processo que exige o envio de verificação adicional em conjunto com o nome de usuário e senha. Quando os usuários se inscrevem no servidor do RSA Adaptive Authentication, fornecem um endereço de e-mail, um número de telefone ou ambos, dependendo da configuração do servidor. Se for necessária alguma verificação adicional, o servidor de autenticação adaptativa da RSA enviará um código de acesso de uso único por meio do canal fornecido. Os usuários digitam esse código de acesso junto com o nome de usuário e a senha.

As perguntas de desafio exigem que o usuário responda a uma série de perguntas quando se inscreve no servidor do RSA Adaptive Authentication. É possível configurar quantas perguntas de inscrição serão feitas e quantas perguntas de desafio serão apresentadas na página de login.

Inscrevendo usuários no servidor do RSA Adaptive Authentication

Os usuários devem ser provisionados no banco de dados do RSA Adaptive Authentication para utilizar a autenticação adaptativa para autenticação. Os usuários serão adicionados ao banco de dados do RSA Adaptive Authentication quando fizerem o login pela primeira vez com seu nome de usuário e senha. Dependendo de como você configurou o RSA Adaptive Authentication no serviço, quando os usuários fazem o login, podem ser solicitados a fornecer o endereço de e-mail, o número de telefone e o número do serviço de envio de mensagens (SMS) deles ou podem ser solicitados a configurar respostas para as perguntas de desafio.

Observação O RSA Adaptive Authentication não permite caracteres internacionais nos nomes de usuário. Se você pretende permitir caracteres de vários bytes nos nomes de usuário, entre em contato com o suporte da RSA para configurar o RSA Adaptive Authentication e o RSA Authentication Manager.

Configurar o RSA Adaptive Authentication no Access Point

Para configurar o RSA Adaptive Authentication no serviço, habilite o RSA Adaptive Authentication, selecione os métodos de autenticação adaptativa a serem aplicados e adicione as informações de conexão do Active Directory e o certificado.

Pré-requisitos

- RSA Adaptive Authentication configurado corretamente com os métodos de autenticação a serem usados para autenticação secundária.
- Detalhes sobre o endereço de endpoint do SOAP e o nome de usuário do SOAP.
- Informações de configuração do Active Directory e certificado SSL disponível do Active Directory.

Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.

3 Clique na engrenagem na linha do RSA Adaptive Authentication.

4 Selecione as configurações apropriadas para o seu ambiente.

Observação Um asterisco indica um campo obrigatório. Os outros campos são opcionais.

Opção	Descrição
Habilitar o RSA AA Adapter	Altere o NÃO para **SIM** para ativar o RSA Adaptive Authentication.
Nome*	O nome é rsaaa-auth.
Endpoint do SOAP*	Insira o endereço do endpoint do SOAP para integração entre o adaptador do RSA Adaptive Authentication e o serviço.
Nome do usuário do SOAP*	Insira o nome de usuário e a senha utilizados para assinar mensagens do SOAP.
Senha do SOAP*	Insira a senha da SOAP API do RSA Adaptive Authentication.
Domínio RSA	Insira o endereço de domínio do servidor Adaptive Authentication.
Habilitar e-mail para OOB	Selecione SIM para habilitar a autenticação de banda externa que envia uma senha única ao usuário final por uma mensagem de e-mail.
Habilitar SMS para OOB	Selecione SIM para habilitar a autenticação de banda externa que envia uma senha única ao usuário final por uma mensagem de texto SMS.
Ativar o SecurID	Selecione SIM para ativar o SecurID. Os usuários são solicitados a inserir seu token e senha RSA.
Habilitar pergunta secreta	Selecione SIM se você estiver usando as perguntas de inscrição e de desafio para autenticação.
Número de perguntas de inscrição*	Insira o número de perguntas que o usuário precisará configurar ao se inscrever no servidor Authentication Adapter.
Número de perguntas de desafio*	Insira o número de perguntas de desafio que os usuários devem responder corretamente ao fazer login.
Número de tentativas de autenticação permitidas*	Insira o número de vezes para exibir as perguntas de desafio a um usuário que tenta fazer login antes que a autenticação falhe.
Tipo de diretório*	O único diretório suportado é o Active Directory.
Usar SSL	Selecione SIM se utilizar o SSL para sua conexão de diretório. Você adiciona o certificado SSL do Active Directory no campo Certificado de Diretório.
Host do servidor*	Insira o nome do host do Active Directory.
Porta do servidor	Insira o número da porta do Active Directory.
Usar localização do serviço DNS	Marque SIM se a localização do serviço DNS for usada para conexão de diretório.
DN Base	Insira o DN do qual se deseja iniciar as pesquisas de conta. Por exemplo, OU=myUnit,DC=myCorp,DC=com.
Vincular DN*	Insira a conta que pode procurar usuários. Por exemplo, CN=binduser,OU=myUnit,DC=myCorp,DC=com
Senha de associação	Insira a senha para a conta de DN de associação.
Atributo de pesquisa	Insira o atributo de conta que contém o nome de usuário.

Opção	Descrição
Certificado do diretório	Para estabelecer conexões SSL seguras, adicione o certificado do servidor de diretório à caixa de texto. No caso de vários servidores, adicione o certificado raiz da autoridade de certificação.
Usar STARTTLS	Altere o NÃO para **SIM** para usar STARTTLS.

5 Clique em **Salvar**.

Gerar metadados SAML do Access Point

Você deve gerar os metadados SAML no appliance do Access Point e trocar metadados com o servidor para estabelecer a confiança mútua necessária para a autenticação de cartão inteligente.

A Security Assertion Markup Language (SAML) é um padrão baseado em XML que é utilizado para descrever e trocar informações de autenticação e autorização entre domínios de segurança diferentes. SAML passa informações sobre usuários entre fornecedores de identidade e fornecedores de serviço em documento chamados de asserções SAML. Neste cenário, o Access Point é o fornecedor de identidade e o servidor no provedor de serviços.

Pré-requisitos

- Configure o relógio (UTC) no appliance doAccess Pointpara que ele esteja com a hora correta. Por exemplo, abra uma janela de console na máquina virtual do Access Point e utilize os botões de seta para selecionar o fuso horário correto. Verifique também se o horário do host ESXi está sincronizado com um servidor NTP. Verifique se as VMware Tools, executadas na máquina virtual do appliance, sincronizam o horário na máquina virtual com o horário no host ESXi.

  Importante Se o relógio do appliance do Access Point não corresponder ao relógio do host do servidor, a autenticação de cartão inteligente poderá não funcionar.

- Obtenha um certificado de autenticação SAML que possa utilizar para assinar os metadados do Access Point.

  Observação A VMware recomenda a criação e utilização de um certificado de autenticação SAML específico quando há mais de um appliance doAccess Pointem sua configuração. Neste caso, todos os appliances devem estar configurados com o mesmo certificado de autenticação para que o servidor possa aceitar as asserções de qualquer um dos appliances do Access Point. Com um certificado de autenticação SAML específico, os metadados SAML de todos os appliances são os mesmos.

- Se você ainda não o fez, converta o certificado de autenticação SAML para arquivos de formato PEM e converta os arquivos `.pem` para o formato de uma linha. Consulte Converter arquivos de certificado para o formato PEM de uma linha.

Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Avançadas, clique no ícone de engrenagem **Configurações do Provedor de Identidade SAML**.

3 Selecione a caixa de seleção **Fornecer Certificado**.

4 Para adicionar um arquivo de Chave privada, clique em **Selecionar** e navegue até o arquivo da chave privada para o certificado.

5 Para adicionar o arquivo de Cadeia de certificados, clique em **Selecionar** e navegue até o arquivo da cadeia de certificados.

6 Clique em **Salvar**.

7 Na caixa de texto Nome do Host, insira o nome do host e faça o download das configurações do provedor de identidade.

Criando um autenticador SAML utilizado por outros provedores de serviço

Após gerar os metadados SAML no appliance do Access Point, você pode copiar estes dados para o provedor de serviços de back-end. Copiar estes dados no provedor de serviços é parte do processo de criação de um autenticador SAML para que o Access Pointpossa ser utilizado como um fornecedor de identidade.

Para um servidor de Horizon Air Hybrid-Mode, consulte a documentação do produto para obter instruções específicas.

Copiar metadados SAML do provedor de serviços para o Access Point

Após criar e ativar o autenticador SAML para que o Access Pointpossa ser utilizado como um fornecedor de identidade, você pode gerar metadados SAML nesse sistema de back-end e utilizar os metadados para criar um provedor de serviços no appliance do Access Point. Esta troca de dados estabelece confiança entre o fornecedor de identidade (Access Point) e o provedor de serviços de back-end, como o Servidor de Conexão do View.

Pré-requisitos

Verifique se você criou um autenticador SAML para o Access Point no servidor do provedor de serviços de back-end.

Procedimentos

1 Recupere os metadados SAML do provedor de serviços, que estão geralmente na forma de um arquivo XML.

Para obter instruções, consulte a documentação para o provedor de serviços.

Provedores de serviços diferentes têm procedimentos diferentes. Por exemplo, você deve abrir um navegador e digitar um URL, como: https://*connection-server.example.com*/SAML/metadata/sp.xml

Você pode então utilizar um comando **Salvar como** para salvar a página da Web em um arquivo XML. O conteúdo deste arquivo começa com o seguinte texto:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

2 Na seção Configurar Manualmente a IU do administrador do Access Point, clique em **Selecionar**.

3 Na seção Configurações Avançadas, clique no ícone de engrenagem **Configurações do Provedor do Servidor SAML**.

4 Na caixa de texto Nome do Provedor de Serviços, insira o nome do provedor de serviços.

5 Na caixa de texto XML de Metadados, cole o arquivo de metadados criado na etapa 1.

6 Clique em **Salvar**.

O Access Pointe o provedor de serviços podem agora trocar informações de autenticação e autorização.

Resolução de problemas de implementação do Access Point 7

Você pode usar vários procedimentos para diagnosticar e corrigir problemas encontrados durante a implementação do Access Point no seu ambiente.

Você pode usar os procedimentos de resolução de problemas para investigar as causas de tais problemas e tentar corrigi-los sozinho, ou você pode obter assistência do Suporte Técnico da VMware.

Este capítulo inclui os seguintes tópicos:

- Resolução de erros de implementação
- Coletando registros do appliance do Access Point
- Habilitação do modo de depuração

Resolução de erros de implementação

Você pode enfrentar dificuldades ao implementar o Access Point no seu ambiente. Você pode usar vários procedimentos para diagnosticar e corrigir problemas da sua implementação.

Aviso de segurança ao executar scripts baixados da Internet

Verifique se o script do PowerShell é o script que você deseja executar e, em seguida, no console do PowerShell, execute o seguinte comando:

```
unblock-file .\apdeploy.ps1
```

comando ovftool não encontrado

Verifique se você instalou o software OVF Tool no Windows e se ele está instalado no local esperado pelo script.

Rede inválida na netmask1 da propriedade

- A mensagem pode indicar netmask0, netmask1 ou netmask2. Verifique se o valor foi definido no arquivo .INI para cada uma das três redes, como netInternet, netManagementNetwork e netBackendNetwork.

- Verifique se um Perfil do Protocolo de Rede do vSphere foi associado a cada nome de rede de referência. Isso especifica as configurações de rede, como máscara de sub-rede IPv4, gateway e assim por diante. Verifique se o Perfil do Protocolo de Rede associado tem valores corretos para cada uma das configurações.

Mensagem de aviso sobre o identificador do sistema operacional não compatível

A mensagem de aviso exibe se o identificador do sistema operacional especificado SUSE Linux Enterprise Server 12.0 64-bit (id:85) não é compatível com o host selecionado. Ele é mapeado com o seguinte identificador de SO: Outro Linux (64-bit).

Ignore esta mensagem de aviso. Ele é mapeado automaticamente para um sistema operacional compatível.

Configuração do Access Point para autenticação do RSA SecurID

Adicione as seguintes linhas à seção do Horizon do arquivo .INI.

```
authMethods=securid-auth && sp-auth
matchWindowsUserName=true
```

Adicione uma nova seção no final do seu arquivo .INI.

```
[SecurIDAuth]
serverConfigFile=C:\temp\sdconf.rec
externalHostName=192.168.0.90
internalHostName=192.168.0.90
```

Os endereços IP devem ser configurados com o endereço IP do Access Point. O arquivo sdconf.rec é obtido a partir de um Gerenciador de Autenticações RSA que deve estar totalmente configurado. Verifique se você está usando o Access Point 2.5 ou uma versão mais recente e se o servidor do Gerenciador de Autenticações RSA é acessível na rede do Access Point. Execute novamente o comando de implementação do Powershell para implementar novamente seu Access Point configurado para RSA SecurID.

O localizador não se refere a um erro de objeto

O erro notifica se o valor de destino que é usado pelo vSphere OVF Tool não está correto para o seu ambiente vCenter. Use a tabela listada em https://communities.vmware.com/docs/DOC-30835 para ver exemplos de formato de destino usado para consultar um host ou cluster do vCenter. O objeto de nível superior é especificado a seguir:

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/
```

O objeto agora lista os nomes possíveis a serem usados no próximo nível.

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

Os nomes da pasta, nomes do host e nomes do cluster usados no destino diferenciam letras maiúsculas e minúsculas.

Coletando registros do appliance do Access Point

Você pode digitar um URL em um navegador para obter um arquivo ZIP que contenha registros do appliance do Access Point>.

Use o seguinte URL para coletar registros do appliance do Access Point.

```
https://access-point-appliance.exemplo.com:9443/rest/v1/monitor/support-archive
```

Neste exemplo, *access-point-appliance. exemplo.com* é o nome de domínio totalmente qualificado do appliance do Access Point .

Estes arquivos de registro são coletados do diretório `/opt/vmware/gateway/logs` no appliance.

As tabelas a seguir contêm descrições dos vários arquivos inclusos no arquivo ZIP.

Tabela 7-1. Arquivos que contêm informações de sistema para auxiliar na resolução de problemas

Nome do Arquivo	Descrição
`df.log`	Contém informações sobre a utilização do espaço em disco.
`netstat.log`	Contém informações sobre conexões de rede.
`ap_config.json`	Contém as definições de configurações atuais para o appliance do Access Point>.
`ps.log`	Inclui a lista de processos.
`ifconfig.log`	Contém informações sobre interfaces de rede.
`free.log`	Contém informações sobre a utilização da memória.

Tabela 7-2. Arquivos de Registro para o Access Point

Nome do Arquivo	Descrição
`esmanager.log`	Contém mensagens de registro do processo do Edge Service Manager, que escuta as portas 443 e 80.
`authbroker.log`	Contém mensagens de registros do processo AuthBroker, que manipula adaptadores de autenticação.
`admin.log`	Contém mensagens de registros do processo que fornece a API REST do Access Point na porta 9443.

Tabela 7-2. Arquivos de Registro para o Access Point (Continuação)

Nome do Arquivo	Descrição
`admin-zookeeper.log`	Contém mensagens de registros relacionadas à camada de dados que é utilizada para armazenar as informações de configuração do Access Point .
`tunnel.log`	Contém mensagens de registros do processo de túnel que é utilizado como parte do processamento da XML API.
`bsg.log`	Contém mensagens de registro do Gateway Seguro Blast.
`SecurityGateway_*.log`	Contém mensagens de registro do Gateway Seguro PCoIP.

Os arquivos de registro que terminam em “-std-out.log”`-std-out.log` contêm informações escritas para o `stdout` de vários processos e são normalmente arquivos vazios.

Arquivos de registro do Access Point para o AirWatch

- `/var/log/airwatch/tunnel/vpnd`

  O tunnel-init.log e o tunnel.log são capturados neste diretório.

- `/var/log.airwatch/proxy`

  O proxy.log é capturado neste diretório.

- `/var/log/airwatch/appliance-agent`

  O appliance-agent.log é capturado neste diretório.

Habilitação do modo de depuração

Você pode habilitar o modo de depuração para um appliance do Access Point para visualizar ou manipular o estado interno do appliance. O modo de depuração permite testar o cenário de implementação no seu ambiente.

Pré-requisitos

- Verifique se o appliance do Access Point não está sendo usado.

  Observação É útil coletar informações de registro em um appliance do Access Point que não esteja funcionando. Os registros podem ser obtidos de uma maneira típica.

Procedimentos

1. Faça login na máquina do Access Point.
2. Insira o seguinte comando na interface da linha de comando.

   ```
   cd /opt/vmare/gateway/conf
   ```

3. Visualize o arquivo de propriedades do registro.

   ```
   vi log4j-esmanager.properties
   ```

4 Localize a seguinte linha no arquivo de propriedades e edite-a. Substitua as informações por depuração.

```
log4j.logger.com.vmware=info,default
```

5 Insira o comando para alterar a configuração de registro a partir de qualquer caminho.

```
supervisorctl restart esmanager
```