Unified Access Gateway Double DMZ Deployment for Horizon

Technical Note
12 DEC 2019
Unified Access Gateway 3.8

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

Introduction

1

This document describes how VMware Horizon is supported using Unified Access Gateway 3.3 and later in environments that have a double Demilitarized Zone (DMZ).

Unified Access Gateway is a VMware virtual appliance used in support of secure remote access for several VMware End-User Computing enterprise products. One example is to use Unified Access Gateway to support remote access to VMware Horizon for accessing virtual desktops and Remote Desktop hosted applications.

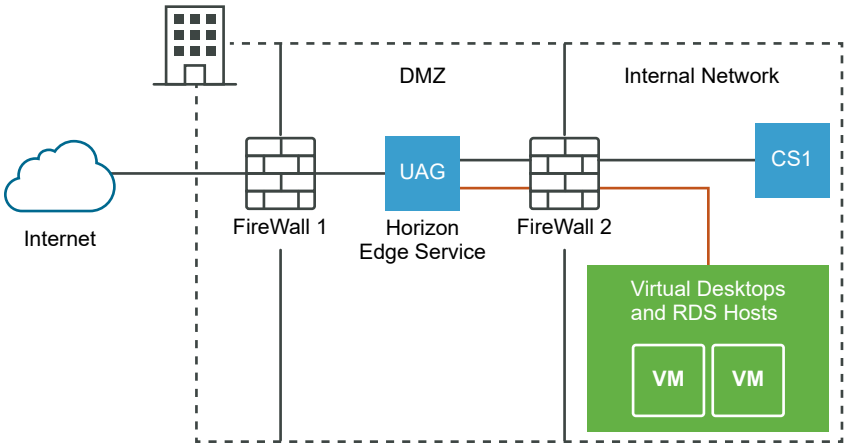
Unified Access Gateway Appliance Deployed in a Single DMZ

2

For on-premises deployment of Horizon within a data center of an organization, it is common to install Unified Access Gateway appliances in a single DMZ which provides a network isolation layer between the internet and the customer data center.

Unified Access Gateway has built-in security mechanisms for all the Horizon protocols to ensure that the only network traffic entering the data center is traffic on behalf of an authenticated user. Any unauthenticated traffic is discarded in the DMZ.

Figure 2-1. Unified Access Gateway appliance deployed in a single DMZ



This is shown in **Figure 2-1**. For a simple setup, it shows just a single Unified Access Gateway appliance in a DMZ although in a production environment supporting high availability and large scale it is common to deploy multiple Unified Access Gateway appliances fronted by a load balancer. Details of configuring a Unified Access Gateway appliance for use in a single DMZ are covered in the standard document *Deploying and Configuring Unified Access Gateway*.

Unified Access Gateway Appliances Deployed in a Double DMZ

3

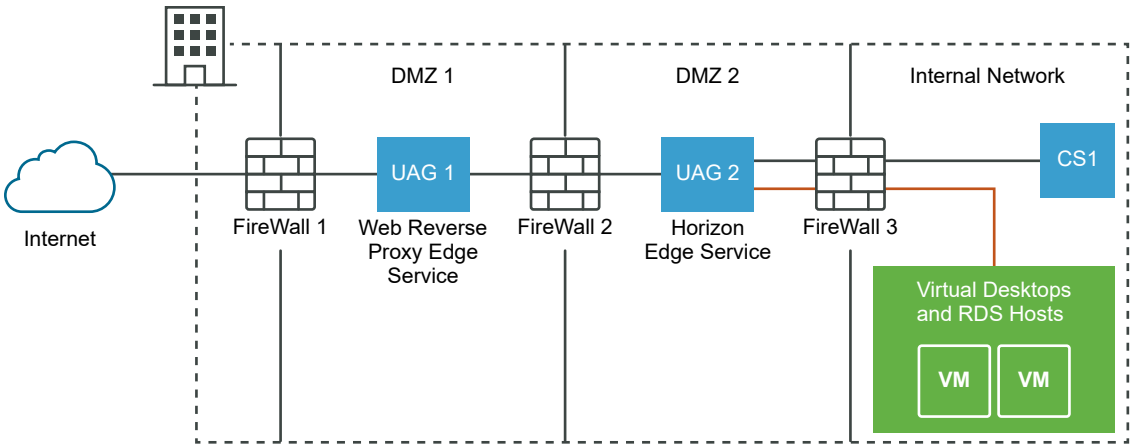
Some organizations have two DMZ. It is often called as a double DMZ or a double-hop DMZ and is sometimes used to provide an extra layer of security protection between the Internet and the internal network.

In a double DMZ, traffic has to be passed through a specific reverse proxy in each DMZ layer. Traffic cannot simply bypass a DMZ layer.

Note In a Horizon deployment, a double DMZ is not required, but for environments where a double DMZ is mandated, an extra Unified Access Gateway appliance acting as a Web Reverse Proxy can be deployed in the outer DMZ.

This document describes the configuration of Unified Access Gateway appliances for double-DMZ deployment.

Figure 3-1. Unified Access Gateway appliances deployed in a double DMZ



The **Figure 3-1** above shows a network with a double DMZ. In this deployment, **UAG 2** in **DMZ 2** is configured for Horizon edge service in exactly the same way as for a single DMZ described in the previous section. The configuration of the Internet facing **FireWall 1** is the same as for a single DMZ. The required TCP and UDP ports should be allowed and routed **FireWall 1** only to Unified Access Gateway appliances in **DMZ 1**. In terms of TCP and UDP ports for **FireWall 2**, these are the same as for **FireWall 1**

except that the rules should only allow source IP addresses of Unified Access Gateway appliances in **DMZ 1** and should only forward this traffic to Unified Access Gateway appliances in **DMZ 2**. This ensures that the only network traffic entering **DMZ 2** is traffic that has been filtered by a **DMZ 1** Unified Access Gateway appliance.

UAG 1 in **DMZ 1** is configured as a Web Reverse Proxy for Horizon protocols. It terminates the TLS connection from the client and provides specific Horizon URL validation on that traffic prior to forwarding it to **UAG 2** on a new TLS connection between **UAG 1** and **UAG 2**. Any network traffic from the Internet to **UAG 1** that falls outside of the Horizon protocol specification configured on **UAG 1** in terms of port numbers, TLS version, ciphers, and HTTPS URL patterns for Horizon is discarded in **DMZ 1**. Valid Horizon network traffic is forwarded to **UAG 2** in **DMZ 2** for the next layer of security.

In this double DMZ configuration, **UAG 2** is configured as a standard Horizon Edge Server appliance. The Horizon external URLs (`tunnelExternalUrl`,`blastExternalUrl` and the optional `pcoip ExternalUrl`) are used by the clients to connect these protocols to the Unified Access Gateway environment. They must be set to values that route these connections to **UAG 1**.

Note This document does not describe any further configuration needed for **UAG 2** as this is standard Unified Access Gateway Horizon configuration, which is covered in the Horizon sections of the standard Unified Access Gateway document *Deploying and Configuring Unified Access Gateway.*

Configuring Unified Access Gateway as a Web Reverse Proxy for Horizon

4

This section details the configuration of the outer Unified Access Gateway Web Reverse Proxy appliance shown as **UAG 1** in **Figure 3-1**. In this configuration, the Unified Access Gateway Horizon Edge Service is not used as **UAG 1** is acting only as a Web Reverse Proxy supporting Client XML protocol and HTML Access, Horizon Tunnel protocol and Blast Extreme TCP. This section also details a set of optional Horizon protocols that can be enabled with generic TCP and UDP forward rules configured on **UAG 1**.

This chapter includes the following topics:

Minimum Horizon Protocols

The primary requirement for Horizon is to support native Horizon clients and the HTML Access Horizon client with protocol handling for the client XML control protocol, the Horizon HTTPS secure tunnel and the Blast/HTTPS WebSockets protocol.

Client XML, Tunnel and Blast TCP Protocols on TCP Port 443

The primary requirement for Horizon is to support native Horizon clients and the HTML Access Horizon client with protocol handling for the client XML control protocol, the Horizon HTTPS secure tunnel and the Blast/HTTPS WebSockets protocol.

All of these protocols can be supported using HTTPS TCP port 443 and so there is no requirement to allow other ports through the outer **FireWall 1** or through the firewall between the DMZ zones **FireWall 2** as shown in **Figure 3-1**.

To support this minimum set of Horizon protocols with TLS termination and URL filtering, **UAG 1** should be set up as a Web Reverse Proxy by enabling a Reverse Proxy Edge Service with the following Proxy Pattern

```
(/broker/xml(.*)|/xmlapi(.*)|/broker/resources/(.*)|/ice/(.*)|/r/(.*)|/portal(.*)|/)
```

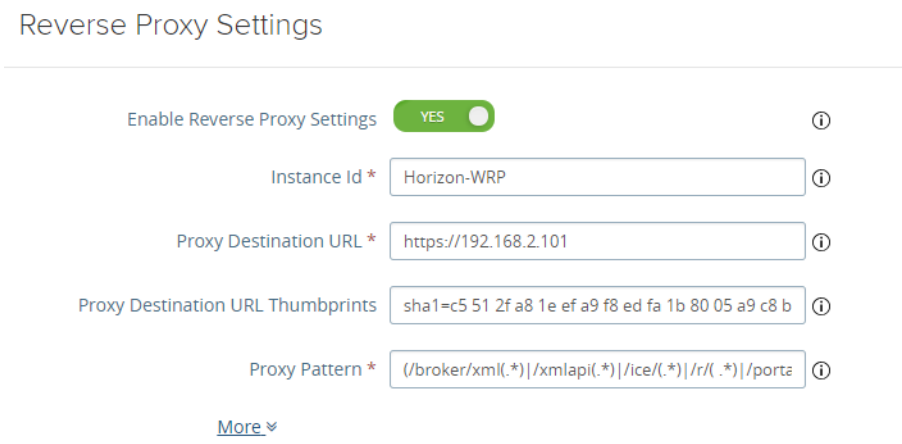
This restricts web traffic as it limits the range of allowed URLs to those conforming to the configured proxy pattern.

To configure this automatically at deploy time with PowerShell, add the following example section to the `UAG.INI` file:

```
[WebReverseProxy1]
instanceId=Horizon-WRP
proxyDestinationUrl=https://192.168.2.101
proxyDestinationUrlThumbprints=sha1=c5 51 2f a8 1e ef a9
f8 ed fa 1b 80 05 a9 c8 bc 6e 2c 64 b1
proxyPattern=(/broker/xml(.*)|/xmlapi(.*)|/broker/resources/(.*)|/ice/(.*)|/r/(.*)|/portal(.*)|/)
```

If using the Unified Access Gateway Admin UI, add a **Reverse Proxy Edge Service** with the following settings.

Figure 4-1. Unified Access Gateway Admin UI Settings for Web Reverse Proxy



Other ports described in the remainder of this section are optional depending on requirements for these additional protocols.

Optional Horizon Protocols

Horizon can be used with the minimum Horizon protocols listed above. There are a set of optional protocols that can are supported and are described below.

In all of the forward rules examples, the IP address used by **UAG 1** to connect to **UAG 2** is 192.168.2.101. If NAT is in use between **DMZ 1** and **DMZ 2**, this will be that NAT'd address used in **DMZ 1**.The forward rules configuration settings for **UAG 1** can either be applied by specifying the rules in the [General] section of the `PowerShell.INI` file or can be specified in the Deploy OVF Template wizard if doing a manual deployment.

Note Multiple forward rules must be specified as a set of comma separated rules on a single line.

For more information on this refer to the standard Unified Access Gateway document *Deploying and Configuring Unified Access Gateway.*

HTTP TCP Port 80

As a convenience for users, Unified Access Gateway supports automatic redirect of port 80 HTTP requests to HTTPS URL on port 443. This can be used so that a user does not need to enter `https://` before the hostname in a browser URL or in the Horizon client. To allow this capability, TCP port 80 must be allowed through **FireWall 1**.There are no additional configuration steps needed on Unified Access Gateway.

Blast Extreme on TCP Port 8443

Blast Extreme TCP can be used on TCP port 8443 as an alternative to TCP port 443. Allow TCP port 8443 through **FireWall 1** and **FireWall 2**. Add a TCP forward rule to **UAG 1** so that TCP connections on port 8443 arriving from the Internet to **UAG 1** will be forwarded to **UAG 2**.

```
forwardrules=tcp/8443/192.168.2.101:8443
```

Blast Extreme on UDP Port 8443

Blast Extreme UDP can be used on UDP port 8443. Allow UDP port 8443 through **FireWall 1** and **FireWall 2**. Add a UDP forward rule to **UAG 1** so that UDP datagrams on port 8443 arriving from the Internet to **UAG 1** will be forwarded to **UAG 2**.

```
forwardrules=udp/8443/192.168.2.101:8443
```

UDP Tunnel on UDP Port 443

Allow UDP port 443 through **FireWall 1** and **FireWall 2**. Add a UDP forward rule to **UAG 1** so that UDP datagrams on port 443 arriving from the Internet to **UAG 1** will be forwarded to **UAG 2**.

```
forwardrules=udp/443/192.168.2.101:443
```

PCoIP on TCP Port 4172 and UDP Port 4172

To support PCoIP

```
forwardrules=tcp/4172/192.168.2.101:4172,udp/4172/192.168.2.101:4172
```

SSL Server Certificates

5

In a double DMZ configuration, it is necessary to install the same SSL server certificate on **UAG 1** and **UAG 2**. This is because Horizon includes a security feature which uses certificate thumbprint calculation to reduce the risk of a malicious man-in-the-middle attack.

The client TLS connection has to connect to a server that has the same certificate as the Unified Access Gateway appliance running the Horizon Edge service (**UAG 2**). As the client TLS connection is being made to **UAG 1**, if a different certificate was presented, then the connection would fail due to a mismatched certificate thumbprint. Similarly, if a load balancer is used in **DMZ 1** in front of multiple Unified Access Gateway appliances, then if that load balancer is also terminating TLS (TLS bridging), then the same certificate must be present on **UAG 2** and the load balancer so that the thumbprint validation succeeds.

Multiple Unified Access Gateway Appliances for Scale and High Availability

6

For simplicity, this document has described a deployment with just a single Unified Access Gateway appliance in **DMZ 1** and **DMZ 2**. In production environments designed for scale and high availability it is recommended that multiple Unified Access Gateway appliances are deployed with load balancing.

The configuration of each Web Reverse Proxy Unified Access Gateway in **DMZ 1** is the same except that it will reference the specific IP address for its corresponding Unified Access Gateway appliance in **DMZ 2**.

Figure 6-1. Multiple Unified Access Gateway appliances deployed in a double DMZ

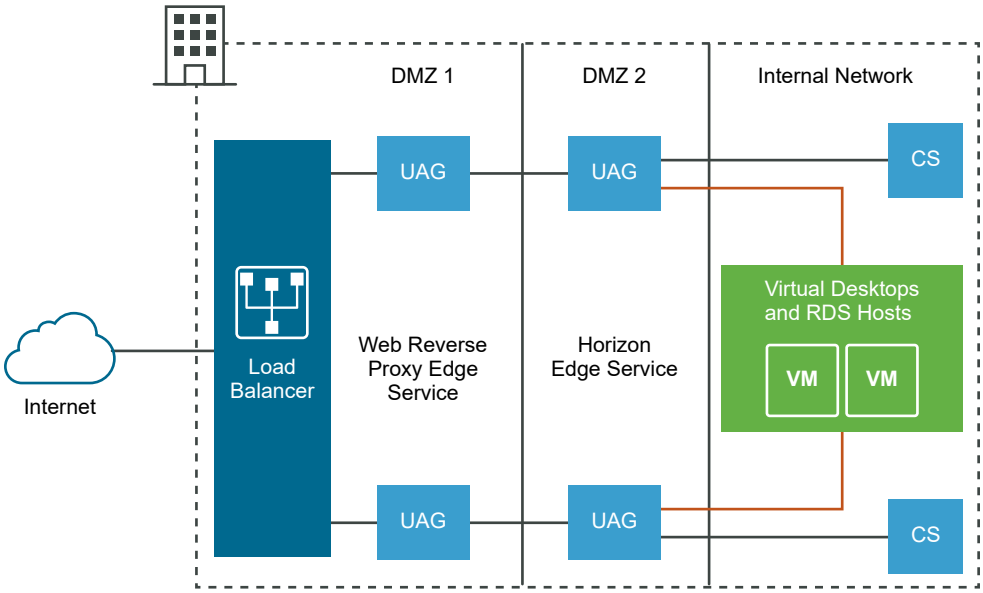


Figure 6-1 shows an example deployment of multiple Unified Access Gateway appliances with load balancing performed in **DMZ 1**.

Smart Card Support

7

Smart Card authentication in Horizon uses certificate negotiation within the client TLS connection. This requires that the first client TLS termination point is a server or appliance configured for Horizon.

Smart Card authentication in Horizon uses certificate negotiation within the client TLS connection. This requires that the first client TLS termination point is a server or appliance configured for Horizon. If there is any intermediate server in between such as a load balancer configured for SSL bridging or a TLS terminating Web Reverse Proxy, then Smart Card authentication cannot be performed. The Unified Access Gateway Web Reverse Proxy configuration for **DMZ 1** described in this document cannot be used for Smart Card authentication. One option is to instead configure **UAG 1** with a generic forward rule for TCP port 443 so that client connections are directly forwarded to **UAG 2** for filtering and Smart Card authentication support on **UAG 2**. The firewall rules don't change for this, but the **UAG 1** Web Reverse Proxy Edge Service should not be enabled.