REVISED 13 FEBRUARY 2019

PROVIDING SECURE ACCESS TO VMWARE HORIZON 7 WITH THE VMWARE UNIFIED ACCESS GATEWAY

vmware®

Table of Contents

Providing Secure Access to VMware Horizon 7 with the VMware Unified Access Gateway

Introduction

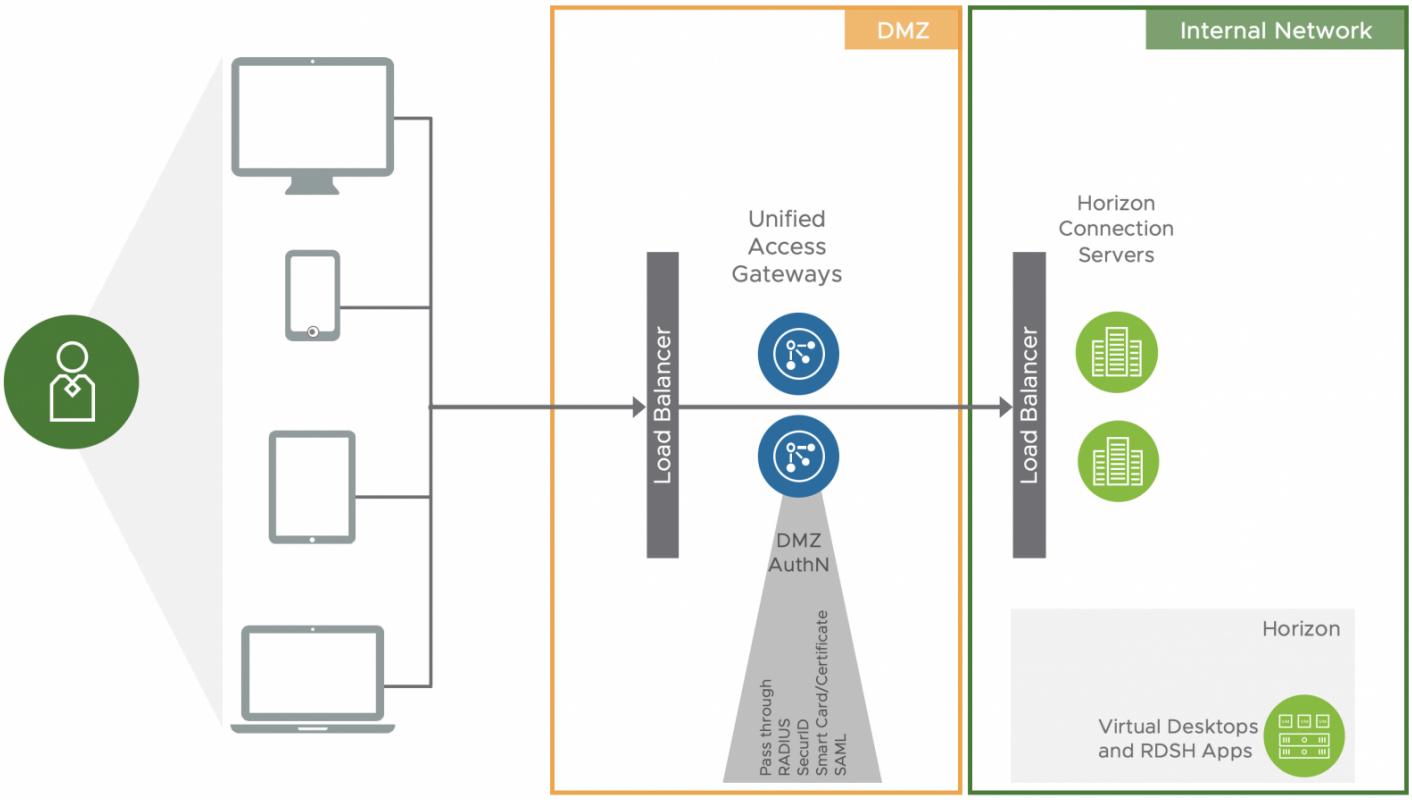
The VMware Unified Access Gateway™ is a platform that provides secure edge services and access to defined resources that reside in the internal network. This allows authorized, external users to access internally located resources in a secure manner.

The VMware Unified Access Gateway can be used for multiple use cases including

- Remote access to VMware Horizon® 7 desktops and applications
- Reverse proxying of web servers
- Access to on-premises legacy applications that use Kerberos or header-based authentication with identity bridging from SAML or certificates
- With Workspace ONE® UEM to allow mobile applications secure access to internal services through VMware Tunnel
- Allowing Mobile Content Management access to internal files shares or SharePoint repositories by running the VMware Content Gateway service

A Unified Access Gateway appliance typically resides within a network demilitarized zone (DMZ) and acts as a proxy host for connections inside your organization's trusted network. This design provides an additional layer of security by shielding the internal resources such as internal web servers, virtual desktops, application hosts, and servers from the public-facing Internet.

This article describes how to deploy a single Unified Access Gateway to proxy VMware Horizon 7 traffic.



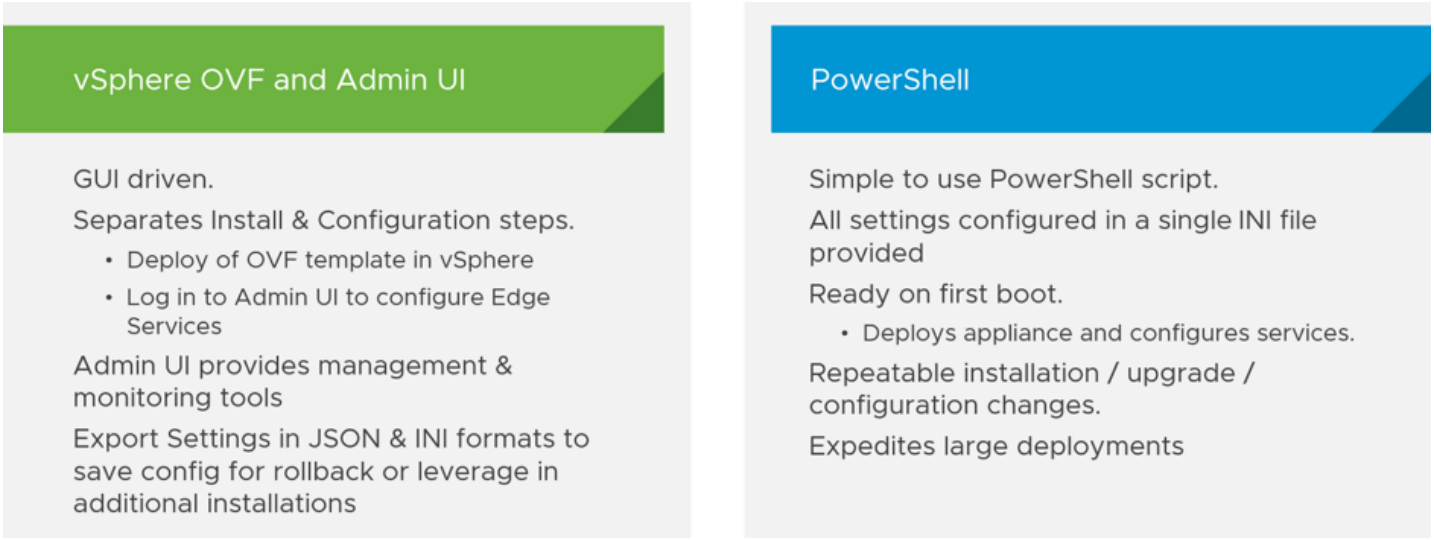
For Horizon 7, Unified Access Gateway provides very similar functionality to the View security server but does not need one-to-one pairing with a Horizon Connection Server. Unified Access Gateway is also capable of proxying sessions to other VMware products and providing more advanced security options, including authentication in DMZ. If you are running View security servers,

take the time to look at replacing them with Unified Access Gateway appliances.

In larger-scale environments, you may still want to have separate Unified Access Gateway appliances for certain edge use cases, to provide scale and operational separation. But in mid-sized to smaller environments, where the load on Unified Access Gateway is not substantial, combining workloads on one set of Unified Access Gateway appliances is convenient.

Deployment Options

Following are two ways to deploy and configure a Unified Access Gateway:



This section walks through using the PowerShell method with the script and the sample INI settings files provided. Do not be put off by the fact that this method uses PowerShell. You will be running a single command that calls an INI file that contains all of your settings. You do not need to know PowerShell.

Preparation

First, download the latest version of the Unified Access Gateway OVA file and the PowerShell script with it accompanying sample INI settings files.

1. From the Downloads page for Unified Access Gateway, download the appliance OVA file.

2. Download the latest version of the PowerShell Scripts ZIP files and extract the contents. (At time of writing, this is uagdeploy-3.7.1.0-14660734.zip).
3. Additionally, visit the community page Using PowerShell to Deploy VMware Unified Access Gateway for additional detail on the process and information about the settings.

Configuration

From the downloaded ZIP file, use the sample INI settings files to create your own settings file.

1. Make a copy of the `uag2-advanced.ini` file and edit it.
2. As with any deployment, go through and enter your information as required for the General and SSLCert sections.

   Leave all other lines as they are. In the following example, spaces and comment lines have been removed to conserve space.

   ```
   [General]

   name=uag1
   ```

```
source=S:\euc-unified-access-gateway-3.7.1.0-14660734_OVF10.ova

target=vi://administrator@vsphere.local:PASSWORD@192.
168.3.12/Datacenter/host/Cluster/

ds=vsanDatastore

netInternet=DMZ

netManagementNetwork=DMZ

netBackendNetwork=DMZ

deploymentOption=onenic

ip0=192.168.2.36

dns=192.168.3.10

[SSLCert]

pfxCerts=sslcertificate.pfx
```

Depending on your network topology, you may need to use a `twonic` or `threenic` deployment. Uncomment the lines for your choice and add the required networking information as necessary.

SSL Certificates can also be provided in PEM format. Comment out the `pfxcerts` line and uncomment the following two `pemCerts` lines and complete if using PEM format.

```
pemCerts=sslcertificate.pem

pemPrivKey=private.key
```

3. Next, add in a Horizon section by copying that section from the `uag2-advanced.ini` file and paste it into your first file (your copy of `uag2-advanced.ini`) at the end, on a new line after the `authCookie` line.

4. Complete the Horizon section and enter the following relevant values for your environment.

```
[Horizon]

proxyDestinationUrl=https://cs.domain.com

tunnelExternalUrl=https://horizon.domain.com:443

blastExternalUrl=https://horizon.domain.com:443

pcoipExternalUrl=88.100.100.100:4172
```

In the example above:

- `cs.domain.com` is the internal address of the Connection Server (or the internal load balancer address if you have more than one Connection Server).
- `horizon.domain.com` is the external address used for Horizon 7 connections.
- `88.100.100.100` is the external IP address for `horizon.domain.com`.

Deployment

Now you are ready to deploy the Unified Access Gateway appliance.

1. Open a PowerShell prompt and change to the directory where the scripts are located.
2. Run `./uagdeploy.psl ./<filename>.ini`, follow the prompts, and enter the passwords.
3. After the process is complete, wait a few minutes for the Unified Access Gateway appliance to boot completely.

You can monitor this process in VMware vCenter Server to see when the assigned IP address is reported on the Summary page for the VM.

If you have all the settings in the INI file completed correctly, and your certificates are in order, you will have a fully operational Unified Access Gateway that will proxy connections to both your Horizon Connection Server. You can also login to the administrative console to confirm settings and change if required using `https://FQDN` or IP address of `UAG:9443/admin`.

Summary

Of course, this configuration of Unified Access Gateway works with multiple components (Unified Access Gateway appliances, Connection Servers) and load balancers. To understand how to deploy multiple components with load balancers, see the VMware Workspace ONE and VMware Horizon Reference Architecture.

You can create PowerShell scripts that quickly deploy the appliance and provide secure edge services to multiple use cases including Horizon Connection Server, Workspace ONE UEM components such as the Content Gateway, VMware Tunnel, and Secure Email Gateway to provide identity bridging. Try the deployment instructions in this article and use this as an opportunity to make the move to Unified Access Gateway. You can also mix and match the deployment approaches and use the administrative UI on a running Unified Gateway appliance to modify or add new edge services.

Learn more about use cases and deploying Unified Access Gateway by following the activity path on Tech Zone: https://techzone.vmware.com/mastering-unified-access-gateway.

About the Author

This article was written by:

- Graeme Gordon, Senior Staff End-User-Computing Architect, EUC Technical Marketing, VMware

To comment on this article, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com