Table of Contents

Component Design: Unified Access Gateway Architecture

– Design Overview
– Network Deployment Options
– Authentication Options
– Deployment Options
– Required Deployment Information

Component Design: Unified Access Gateway Architecture

VMware Unified Access Gateway™ is an extremely useful component in a VMware Workspace ONE® deployment because it allows secure remote access from outside the corporate network to a variety of internally hosted resources.

Unified Access Gateway can be used for multiple use cases, including:

- Deployment of VMware Workspace ONE® Tunnel to allow mobile applications secure access to internal services
- Access from VMware Workspace ONE® Content to internal file shares or SharePoint repositories by running the Content Gateway service
- Reverse proxying of web servers
- Access to on-premises legacy applications that use Kerberos or header-based authentication by providing identity bridging from SAML or certificates
- External access to VMware Horizon® Cloud Service™ on Microsoft Azure desktops and applications
- Secure external access to VMware Horizon® 7 desktops and applications

When providing access to internal resources, Unified Access Gateway is typically deployed within the corporate DMZ and acts as a proxy host for connections to your company’s resources. Unified Access Gateway directs authenticated requests to the appropriate resource and discards any unauthenticated requests.

On Horizon Cloud Service on Microsoft Azure, Unified Access Gateway appliances can be deployed as part of the node’s gateway configuration. See Specify the Node's Gateway Configuration in Getting Started with VMware Horizon Cloud Service on Microsoft Azure.
Design decisions: Unified Access Gateway was deployed as part of Horizon Cloud Service on Microsoft Azure to provide external access for users. Deployment is automated when selected as part of the Horizon Cloud node’s gateway configuration.

Unified Access Gateway was also deployed, separately, to provide Per-App Tunnel components and to run the Content Gateway as part of the VMware Workspace ONE® UEM (powered by AirWatch) service.

Design Overview

A successful deployment of Unified Access Gateway is dependent on good planning and a robust understanding of the platform. The following sections discuss the design options and detail the design decisions that were made to satisfy the design requirements.

Scalability

Unified Access Gateway gives two sizing options during deployment.
To satisfy the requirements that the proposed solution be robust and able to handle failures, we deployed \( n+1 \) appliances.

**Design decisions:** 3 large-sized Unified Access Gateway appliances were deployed to satisfy the requirement for 50,000 devices, using both Content Gateway and Per-App Tunnel (total of 100,000 sessions) and high availability \((n+1)\).

**Load Balancing**

It is strongly recommended that users connect to Unified Access Gateway using a load-balanced virtual IP (VIP). This ensures that user load is evenly distributed across all available Unified Access Gateway appliances. Using a load balancer also facilitates greater flexibility by enabling IT administrators to perform maintenance, upgrades, and configuration changes without impacting users.

For more information on configuring load balancing for Unified Access Gateway, see the following resources:

- *Unified Access Gateway Load Balancing Topologies* in *Deploying and Configuring VMware Unified Access Gateway*
- *Load Balancing across VMware Unified Access Gateway Appliances*

**Service Design**

A Unified Access Gateway appliance is capable of running multiple edge services on the same appliance. In larger environments, as a rule of thumb, be sure to separate Horizon traffic from other services, and have discrete sets of Unified Access Gateway appliances for Horizon and for Workspace ONE UEM services.

**Network Deployment Options**

Unified Access Gateway can be deployed with one, two, or three network interface controllers (NICs). The choice is determined by your network requirements and discussions with the security teams to ensure compliance with company policy.
Single NIC

In a single-NIC deployment, all traffic (Internet, backend, and management) uses the same network interface.

Two NIC

A two-NIC deployment separates the Internet traffic onto its own NIC, while the management and backend network data still share a NIC. This type of deployment is suitable for production environments.

**Figure**: Unified Access Gateway Single-NIC Deployment
Three NIC

A three-NIC deployment separates the Internet traffic onto its own NIC, and separates management and backend network data onto dedicated networks. This type of deployment is suitable for production environments.
Design decision: To meet the requirements of separating Internet traffic from management and backend data, the Unified Access Gateway appliances were deployed in a dual-NIC mode.

Authentication Options

Unified Access Gateway supports multiple authentication options, for example, pass-through, RSA SecurID, RADIUS, certificate, and smart card. Pass-through authentication forwards the request to the internal server or resource. Other authentication types enable authentication at the Unified Access Gateway, before passing authenticated traffic through to the internal resource.

These options are depicted in the following diagrams.
Design decision: Because users will authenticate through Workspace ONE and VMware Identity Manager, Unified Access Gateway was configured to use pass-through authentication.

Deployment Options
In this section, we briefly discuss the two supported methods of deploying Unified Access Gateway and then detail the optimal solution to satisfy the design requirements.

- **VMware vSphere OVF® template and administration console** – With this option, you run the Import OVF (Open Virtualization Format) wizard and respond to various deployment questions. This method requires responses from an IT administrator during deployment. If you use this method, the Unified Access Gateway is not production ready on first boot and requires post-deployment configuration using the administration console. The required configuration tasks can be performed either manually or by importing a configuration file from another Unified Access Gateway appliance.
PowerShell script – The PowerShell method ensures that the Unified Access Gateway virtual appliance is production ready on first boot. This method uses the VMware OVF Tool command-line utility in the background. The IT administrator updates an INI file with the required configuration settings and then deploys the Unified Access Gateway by entering a simple deployment command in PowerShell (.\uagdeploy.ps1 .\<name>.ini).

Design decision: The PowerShell method was used because it satisfies most deployment scenarios and does not require the IT administrator to manually enter settings during the deployment.

More information on using the PowerShell method is available on the Using PowerShell to Deploy VMware Unified Access Gateway community page. The PowerShell script and sample INI files can be downloaded from the Unified Access Gateway product download page.

Required Deployment Information

Before deploying a Unified Access Gateway appliance, you must verify that certain prerequisites are met and provide the following information.

Certificates

TLS/SSL certificates are used to secure communications for the user between the endpoint and the Unified Access Gateway and between the Unified Access Gateway and internal resources. A certificate can also be used on the administrative interface to verify the administrator’s identity.

Although Unified Access Gateway generates default self-signed certificates during deployment, for production use, you should replace the default certificates with certificates that have been signed by a trusted certificate authority (CA-signed certificates). You can replace certificates either during deployment or as part of the initial configuration. The same certificate or separate certificates can be used for the user and the administrative interfaces, as desired.

The following types of certificates are supported:

- Single-server-name certificates, which means using a unique server certificate for each Unified Access Gateway appliance
- Subject alternate name (SAN) certificates
- Wildcard certificates

Certificate files can be provided in either PFX or PEM format.


Passwords

Unified Access Gateway requires the IT administrator to define two passwords during installation: The first secures access to the REST API, and the second secures access to the Unified Access
Gateway appliance console. The passwords must meet the minimum requirements listed in the Unified Access Gateway documentation.

**IP Address and Fully Qualified Domain Name (FQDN)**

As previously discussed, the Unified Access Gateway in this scenario is configured with two NICs:

- Internet-facing IP address and external FQDN
- Backend and management IP address and FQDN