Load Balancing Unified Access Gateway for Horizon

Omnissa Horizon

Table of contents

Load Balancing Unified Access Gateway for Horizon

Overview

Omnissa Unified Access Gateway is a virtual appliance designed to protect desktop and application resources to allow remote access from the Internet. For an overview of Unified Access Gateway, see the Unified Access Gateway product page on Tech Zone.

Unified Access Gateway is used with:

- Omnissa Horizon 8
- Omnissa Horizon Cloud Service
- Omnissa Workspace ONE UEM (Tunnel, Content Gateway, Secure Email Gateway)

This document focuses on the Horizon 8 use case for Unified Access Gateway with an external load balancer. Unified Access Gateway also has a built-in high availability feature, although it is outside the scope of this document.

Unified Access Gateway is typically deployed in a demilitarized zone (DMZ). For high availability and scalability requirements in a production deployment, multiple Unified Access Gateway appliances are usually deployed behind a load balancer.

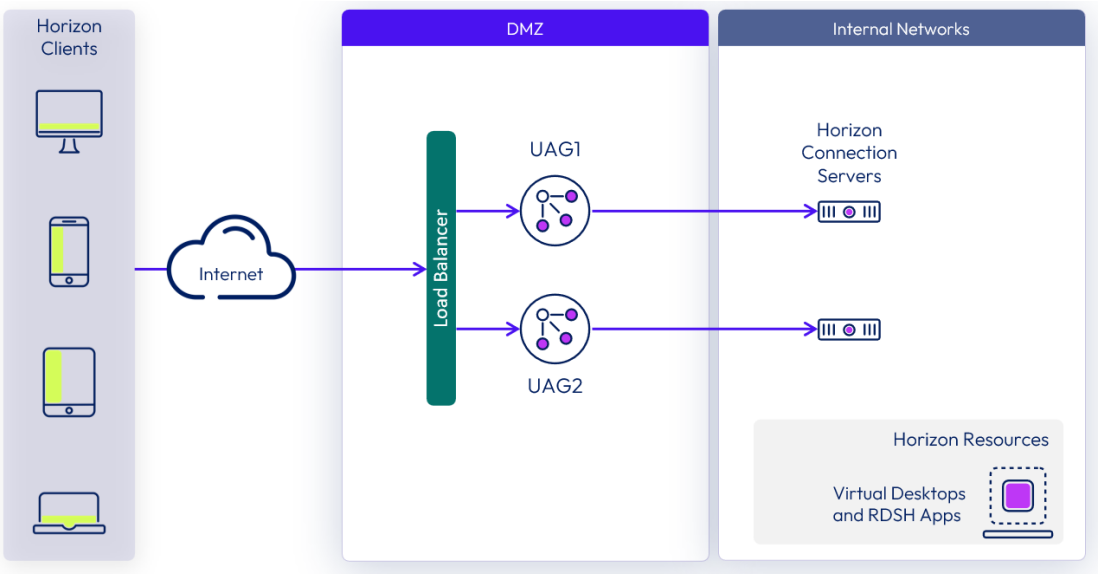

Figure 1: Multiple Unified Access Gateway appliances behind a load balancer

Purpose of this tutorial

This article focuses on the load balancing requirements for the Horizon use cases. It discusses the distinction between the primary and secondary Horizon protocols and describes the three methods for guaranteeing session affinity. The three methods ensure that all protocol traffic from a Horizon client session goes to the same Unified Access Gateway appliance. This article also covers health monitoring and SSL offload/SSL bridging for load balancers.

Transport Layer Security (TLS) and the predecessor Secure Sockets Layer (SSL) are both referred to in this document as just SSL. By default, SSL is disabled on Unified Access Gateway and only TLS 1.2 and TLS 1.3 are enabled.

Note: Updating the security protocols and cipher suites for Blast (8443 port) and PCoIP (4172 port) when not running on port 443 is not supported on Unified Access Gateway,

- With Unified Access Gateway 3.9 and below, both services have TLS 1.1 and 1.2 enabled by default.
- For Unified Access Gateway 3.10 and above, Blast (8443 port) no longer uses TLS 1.1 and only supports TLS 1.2.

Horizon protocols

When an Omnissa Horizon Client user connects to an Omnissa Horizon environment, several different protocols are used. The first connection is always the primary XML-API protocol over HTTPS. Following successful authentication, one or more secondary protocols are also made.

For more information on Horizon primary and secondary protocols, see Understand and Troubleshoot Horizon Connections.

Primary Horizon protocol

The user enters a hostname at the Horizon Client, and this starts the primary Horizon protocol. This is a control protocol for authentication, authorization, and session management. It uses XML structured messages over HTTPS (HTTP over SSL). This protocol is sometimes known as the Horizon XML-API control protocol. In a load balanced environment, the load balancer will route this connection to one of the Unified Access Gateway appliances. The load balancer will usually select the appliance based first on availability, and then out of the available appliances will route traffic based on the least number of current sessions. This has the effect of evenly distributing the traffic from different clients across the available set of Unified Access Gateway appliances.

The load balancer affinity timeout should be set to match the session timeout, which by default is 10 hours. This ensures that subsequent connections for XML-API during the whole session will be directed to the same Unified Access Gateway appliance. Affinity to an individual Unified Access Gateway appliance for the XML-API protocol can be ensured with source IP affinity as described below for method 1.

For methods 2 and 3 where source IP affinity is not used, it is common to perform cookie-based affinity by the load balancer. This is either done by tracking the Unified Access Gateway session cookie called "ACCESSPOINTSESSIONID" or can be done with a load balancer inserted cookie.

In all cases, the XML-API protocol must have affinity with the initially selected Unified Access Gateway appliance for the entire session. Specific configuration details for cookie tracking or cookie insert for HTTPS should be obtained from your load balancer vendor.

Secondary Horizon protocols

After the Horizon Client has established secure communication to one of the Unified Access Gateway appliances, the user authenticates. If this authentication attempt is successful, then one or more secondary connections are made from the Horizon client.

These secondary connections can include:

- HTTPS **Tunnel** used for encapsulating TCP protocols such as RDP, multi-media redirection (MMR), client drive redirection (CDR), and the client framework channel. (TCP 443).
- **Blast** Extreme display protocol (TCP 443 and UDP 8443). Note that UDP is optional with Blast.
- **PCoIP** display protocol (TCP 4172 and UDP 4172).

These secondary Horizon protocols must be routed to the same Unified Access Gateway appliance to which the primary Horizon protocol was routed. The reason for this is so that Unified Access Gateway can authorize the secondary protocols based on the authenticated user session.

An important security capability of Unified Access Gateway is that it will only forward traffic into the datacenter if the traffic is on behalf of an authenticated user. If the secondary protocols were to be misrouted to a different Unified Access Gateway appliance to the primary protocol one, they would not be authorized and would therefore be dropped in the DMZ and the connection would fail. Misrouting the secondary protocols is a common problem if the load balancer is not configured correctly.

Session affinity options for secondary protocols

There are three different methods that can be used for a load balancing configuration.

1. Source IP affinity
2. Multiple port number groups
3. Multiple VIPs

Method 1 - source IP affinity

This is the simplest configuration for a load balancer as it uses standard port numbers and a single load balanced virtual IP address (VIP). It relies on the load balancer to route secondary protocols to the same Unified Access Gateway appliance as was selected for the primary Horizon protocol. It can do this on the basis of repeat connections coming from the same Horizon client IP address.

Unfortunately, this method does not work in all situations. For example, with certain Network Service Providers or NAT devices, the source IP address is not available for this affinity configuration. If source IP affinity cannot be used in your environment, then one of the other two methods should be used as they do not rely on source IP affinity.

In this example, the public IP address is 10.20.30.40 (uag.myco.com) and would be translated to 192.168.0.100 (the load balanced VIP DMZ IP address).

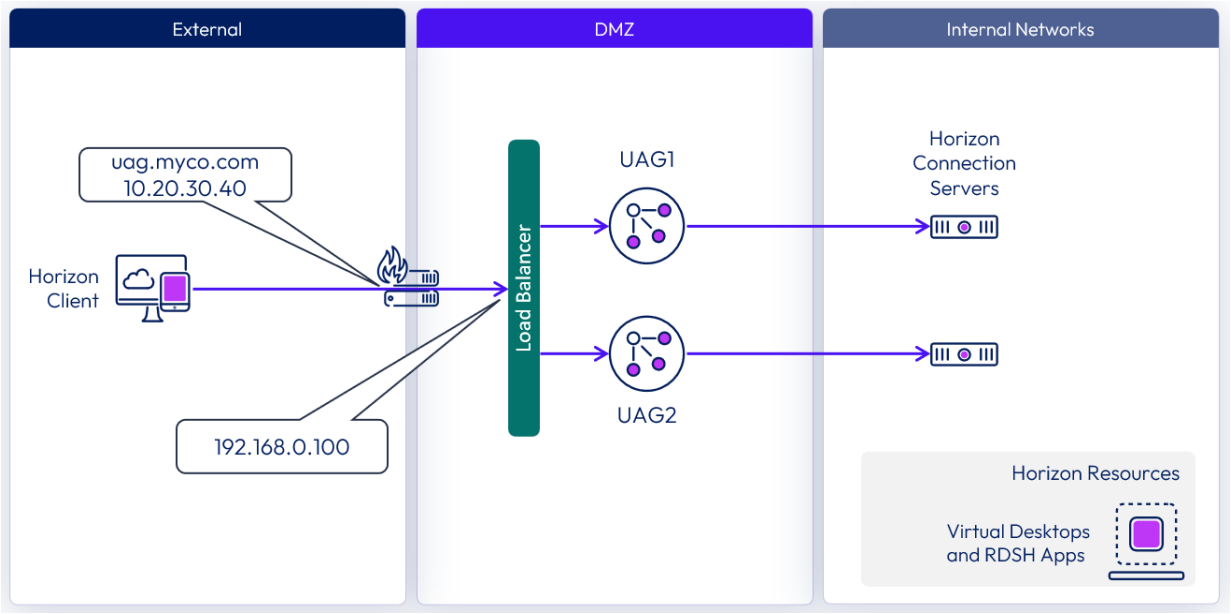

Figure 2: Method 1 - source IP affinity

Unified Access Gateway Configuration for external URLs for this configuration would be as shown in this table.

UAG appliance	Configuration item	Value
UAG01	tunnelExternalURL	https://uag.myco.com:443
UAG01	blastExternalURL	https://uag.myco.com:443
UAG01	pcoipExternalURL	10.20.30.40:4172
UAG02	tunnelExternalURL	https://uag.myco.com:443
UAG02	blastExternalURL	https://uag.myco.com:443
UAG02	pcoipExternalURL	10.20.30.40:4172

Method 1 advantages:

- Uses standard port numbers.
- Does not require multiple public virtual IP addresses.

Method 1 disadvantages:

- Relies on source IP address affinity which is not always possible.

Method 1 is recommended for all environments where source IP address affinity is possible. Where it is not possible, then either method 2 or method 3 should be used.

Method 2 - multiple port number groups

Multiple port group affinity does not rely on source IP address for affinity. Instead, the load balancer is configured to route the secondary Horizon protocols based on unique port numbers assigned to each Unified Access Gateway appliance.

- The primary Horizon protocol on HTTPS port 443 is load balanced to allocate the session to a specific Unified Access Gateway appliance based on health and least loaded.
- The secondary connections would then be routed to the correct Unified Access Gateway appliance based on the load balancer configuration table below.

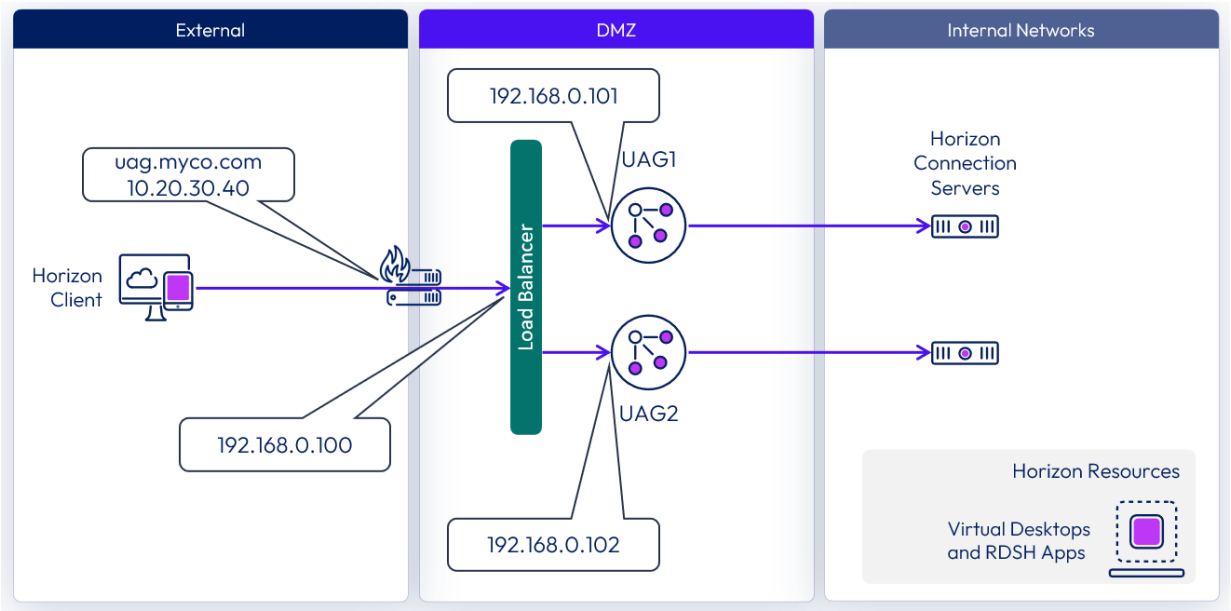

Figure 3: Method 2 - multiple port number groups

Source IP Address	Source Port	Protocol	Target Server	Target Port	Protocol	Name
192.168.0.100	443	TCP	192.168.0.101 192.168.0.102	443 443	Primary	UAGLB - HTTPS
192.168.0.100	10443	TCP	192.168.0.101	443	Secondary	UAG01 - HTTPS
192.168.0.100	10443	UDP	192.168.0.101	8443	Secondary	UAG01 - BLAST-UDP
192.168.0.100	10172	TCP	192.168.0.101	4172	Secondary	UAG01 - PCOIP
192.168.0.100	10172	UDP	192.168.0.101	4172	Secondary	UAG01 - PCOIP-UDP
192.168.0.100	10243	TCP	192.168.0.102	443	Secondary	UAG02 - HTTPS
192.168.0.100	10243	UDP	192.168.0.102	8443	Secondary	UAG02 - BLAST-UDP
192.168.0.100	10272	TCP	192.168.0.102	4172	Secondary	UAG02 - PCOIP
192.168.0.100	10272	UDP	192.168.0.102	4172	Secondary	UAG02 – PCOIP-UDP

The same port mapping scheme can be used for additional Unified Access Gateway appliances from 03 to 99. The virtual IP address for the load balancer might be behind a NAT device. In this example, the public IP address is 10.20.30.40 (uag.myco.com) and would be translated to 192.168.0.100 (the load balanced VIP IP address).

Unified Access Gateway configuration for external URLs for this configuration would be as shown in this table.

UAG Appliance	Configuration Item	Value
UAG01	tunnelExternalURL	https://uag.myco.com:10143
UAG01	blastExternalURL	https://uag.myco.com:10143
UAG01	pcoipExternalURL	10.20.30.40:10172
UAG02	tunnelExternalURL	https://uag.myco.com:10243
UAG02	blastExternalURL	https://uag.myco.com:10243
UAG02	pcoipExternalURL	10.20.30.40:10272

Method 2 advantages:

- Does not rely on source IP affinity.
- Does not require multiple public virtual IP addresses.
- Can be used with the Unified Access Gateway HA feature without a load balancer.

Method 2 disadvantages:

- Uses non-standard port numbers from the Internet although the port numbers on the Unified Access Gateway appliances

themselves are standard.

Method 3 - multiple VIPs

This method is similar to the multiple port groups method except instead of dedicating port number to each Unified Access Gateway appliance it dedicates an individual VIP to each appliance in addition to the primary load balanced VIP. If you have 2 Unified Access Gateway appliances, then you would set up 3 VIPs. The primary Horizon protocol on HTTPS port 443 is load balanced to allocate the session to a specific Unified Access Gateway appliance based on health and least loaded. The secondary connections would then be routed to the correct Unified Access Gateway appliance based on the following load balancer configuration table.

Virtual IP Address	Primary/Secondary	Protocol	Name	Real Servers
192.168.0.100:443	Primary	TCP	UAGLB - HTTPS	192.168.0.101:443 192.168.0.102:443
192.168.0.101:443	Secondary	TCP	UAG01 - HTTPS	192.168.0.101:443
192.168.0.101:8443	Secondary	UDP	UAG01 - BLAST-UDP	192.168.0.101:8443
192.168.0.101:4172	Secondary	TCP	UAG01 - PCOIP	192.168.0.101:4172
192.168.0.101:4172	Secondary	UDP	UAG01 - PCOIP-UDP	192.168.0.101:4172
192.168.0.102:443	Secondary	TCP	UAG02 - HTTPS	192.168.0.102:443
192.168.0.102:8443	Secondary	UDP	UAG02 - BLAST-UDP	192.168.0.102:8443
192.168.0.102:4172	Secondary	TCP	UAG02 - PCOIP	192.168.0.102:4172
192.168.0.102:4172	Secondary	UDP	UAG02 – PCOIP-UDP	192.168.0.102:4172

Note that the secondary protocols do not have to be routed via the load balancer. If required, they can bypass the load balancer.

In this example:

- The first Unified Access Gateway appliance public IP address is 10.20.30.41 (uag1.myco.com) and would be translated to 192.168.0.101.
- The second Unified Access Gateway appliance public IP address is 10.20.30.42 (uag2.myco.com) and would be translated to 192.168.0.102.

Unified Access Gateway configuration for External URLs for this configuration would be as shown in this table.

UAG Appliance	Configuration Item	Value
UAG01	tunnelExternalURL	https://uag1.myco.com:443
UAG01	blastExternalURL	https://uag1.myco.com:443
UAG01	pcoipExternalURL	10.20.30.41:4172
UAG02	tunnelExternalURL	https://uag2.myco.com:443
UAG02	blastExternalURL	https://uag2.myco.com:443
UAG02	pcoipExternalURL	10.20.30.42:4172

Method 3 advantages:

- Does not rely on source IP affinity.
- Uses standard port numbers.
- Can be used with the Unified Access Gateway HA feature without a load balancer.

Method 3 disadvantages:

- Requires an additional public facing VIP for each Unified Access Gateway appliance in addition to the primary load balanced VIP.

Health monitoring

A load balancer monitors the health of each Unified Access Gateway appliance by periodically sending an HTTPS GET /favicon.ico request (e.g., https://uag1.myco-dmz.com/favicon.ico). This monitoring is configured on the load balancer.

It will perform this HTTPS GET and expect a "HTTP/1.1 200 OK" response from Unified Access Gateway to know that it is "healthy". If it gets a response other than "HTTP/1.1 200 OK" response or does not get any response, it will mark the particular Unified Access Gateway appliance as down and will not attempt to route client requests to it. It will continue to poll so that it can detect when it is available again. A response of 200 from Unified Access Gateway indicates the health of Unified Access Gateway itself as well as the Horizon services and the health of the Connection Server(s) used.

An interval of 30 seconds is a good guide for the polling frequency.

Unified Access Gateway can be put into "quiesce" mode after which it will not respond to the load balancer health monitoring request with a "HTTP/1.1 200 OK" response. Instead, it will respond with "HTTP/1.1 503" to indicate that the Unified Access Gateway service is temporarily unavailable. This setting is often used prior to scheduled maintenance, planned reconfiguration, or planned upgrade of a Unified Access Gateway appliance.

In this mode, the load balancer will not direct new sessions to this appliance because it will be marked as unavailable but can allow existing sessions to continue until the user disconnects or the maximum session time is reached. Consequently, this operation will not disrupt existing user sessions. The appliance will then be available for maintenance after a maximum of the overall session timer, which is typically 10 hours. This capability can be used to perform a rolling upgrade of a set of Unified Access Gateway appliances in a strategy resulting in zero user downtime for the service.

SSL offloading or bridging

Many load balancers have the capability of SSL offloading where the SSL connection terminates at the load balancer. This can be useful for managing SSL server certificates and ciphers etc. at the load balancer. Note that in cases where client certificate authentication is used, the load balancer must not terminate TLS and so SSL bridging cannot be used. In client certificate authentication cases a layer-4 TCP load balancing configuration is needed.

In order for the client connection to be secure right to Unified Access Gateway, if the load balancer is configured to terminate SSL, then it is necessary to re-encrypt SSL traffic for communication between the load balancer and Unified Access Gateway. This is often known as SSL bridging as nothing is actually offloaded from Unified Access Gateway. SSL bridging is not necessary, but it is supported. If SSL bridging is used, then it is important to install the same SSL server certificate on Unified Access Gateway as is on the load balancer. This is because when a Horizon Tunnel and Blast connection is made by the client, it is expecting the same certificate at the point where TLS is terminated. It does this to detect a malicious man in the middle (MITM) attack. In other words, Unified Access Gateway and the load balancer must have the same certificate.

It is possible to use a different certificate on the load balancer and Unified Access Gateway in which case you can configure the public load balancer certificate for the Tunnel and Blast sessions so that the thumbprint mismatch will not occur.

Unified Access Gateway supports load balancers that use SSL bridging and load balancers that pass through the SSL communication for termination at Unified Access Gateway.

Summary and additional resources

Additional resources

For more information about Omnissa Unified Access Gateway, you can explore the following resources:

- Unified Access Gateway product page
- Unified Access Gateway documentation
- Network ports in Horizon 8
- Understand and troubleshoot Horizon connections

Changelog

The following updates were made to this guide:

Date	Description of Changes
2025-01-15	
2024-05-16	
2022-08-09	

About the author and contributors

The content in this document is based on an article created by Mark Benson, Alumni.

The following people reviewed and updated the content:

- Andreano Lanusse, Staff Architect, Omnissa
- Graeme Gordon, Senior Staff Architect, Omnissa

Feedback

Your feedback is valuable. To comment on this paper, either use the feedback button or contact us at tech_content_feedback@omnissa.com.