INTEGRATION GUIDE
Load Balancing VMware Unified Access Gateway
## Version History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Description</th>
<th>Compatible Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 2019</td>
<td>2.0</td>
<td>Matt Mabis</td>
<td>Document Updates and IAPP Integration Changes</td>
<td>Unified Access Gateway 2.x and 3.x (2)</td>
</tr>
<tr>
<td>Nov 2017</td>
<td>1.0</td>
<td>Matt Mabis</td>
<td>Initial Document with How-To Configure F5 LTM with VMware Unified Access Gateway (2)</td>
<td>VMware Access Point 2.5.x, 2.7.x, 2.8.x, Unified Access Gateway 2.9.x, 3.0.x (1) (2) (3)</td>
</tr>
</tbody>
</table>

**NOTES:**

1. VMware Access Point was the name given to Unified Access gateway prior to 2.9.x Releases, it was changed after 2.9.0 to Unified Access Gateway and the branding will continue to be called Unified Access Gateway moving forward. This document will refer to Unified Access Gateway but is also applicable to VMware Access Point.

2. Functionality for Blast Extreme UDP is only supported in VMware Unified Access Gateway 3.0.x and above

3. Functionality for Blast Extreme TCP is supported in VMware Access Point 2.8.0 and above and VMware Unified Access Gateway 3.0.x and above
Overview

VMware Unified Access Gateway (UAG), formerly known as VMware Access Point is an appliance that is typically installed in the demilitarized zone (DMZ). UAG is designed to provide safe and secure access to desktop and application resources for remote access. UAG simplifies gateway access and provides tunneled and proxied resources for the following VMware product suites.

- VMware Horizon (Formerly known as Horizon View)
- VMware Horizon Air (Formerly known as DAAS)
- VMware Horizon Air Hybrid Mode
- VMware Workspace One (Cloud and On-Premise)
- AirWatch Tunnel Gateway/Proxy

Typically, UAG is designed to run in the DMZ as the appliance has the following settings:

- Up-to-date Linux Kernel and software patches
- Multiple NIC support for Internet and Intranet traffic
- Disabled SSH
- Disabled FTP, Telnet, Rlogin, or Rsh services
- Disabled unwanted services

F5’s products and solutions bring an improved level of reliability, scalability, and security to UAG deployments. For large Horizon deployments requiring multiple pods or several data centers, F5’s products provide the load balancing and traffic management needed to satisfy the requirements of customers around the world. F5 and VMware continue to work together on providing customers best-of-breed solutions that allow for better and faster deployments as well as being prepared for future needs, requirements, and growth.

F5 and VMware have a long-standing relationship that centers on technology integration and solution development. As a result, customers benefit from leveraging the experience gained by peers from deploying proven, real-world solutions.
VMware Horizon Protocols

When a Horizon Client user connects to a 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.

Primary Horizon Protocol

The user enters a hostname at the Horizon Client which 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 as shown in Figure 1, the load balancer routes this connection to one of the UAG appliances. The load balancer usually selects the appliance based first on availability, and then out of the available appliances routes traffic based on the least number of current sessions. This evenly distributes the traffic from different clients across the available set of UAG appliances.

Secondary Horizon Protocols

After the Horizon Client has established secure communication to one of the UAG 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, MMR/CDR and the client framework channel (TCP 443).
- Blast Extreme display protocol (TCP 8443 and UDP 8443).
- PCoIP display protocol (TCP 4172 and UDP 4172).

These secondary Horizon protocols must be routed to the same UAG appliance to which the primary Horizon protocol was routed. This is so UAG can authorize the secondary protocols based on the authenticated user session. An important security capability of UAG is that it only forwards traffic into the corporate datacenter if the traffic is on behalf of an authenticated user. If the secondary protocols were to be misrouted to a different UAG appliance (different from the one where primary protocols were handled) 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.
The following are prerequisites for this solution and must be complete before proceeding with the configuration. Step-by-step instructions for prerequisites are outside the scope of this document, see the BIG-IP documentation on support.f5.com for specific instructions.

1. F5 recommends running this configuration using BIG-IP LTM version 14.x and 13.x, however it should run on earlier editions of BIG-IP LTM.

2. Create/import an SSL Certificate that contains the load-balanced FQDN that will be used for the Horizon instance.

3. Upload the following to the BIG-IP system:
   - The SSL certificate.
   - The Private Key used for the load balanced FQDN certificate.
   - The Primary CA or Root CA for the SSL Certificate you uploaded to the BIG-IP.

4. Ensure the new FQDN for Horizon is in DNS with both forward and reverse records, and points to the Virtual Server IP address on the BIG-IP that will be used for load balancing the Horizon environment.

5. VMware Horizon deployed and functional within the environment. This includes Horizon Connection Servers, VDI, and Unified Access Gateway Servers.

6. Download the latest F5 iApp templates and extract to an accessible location at https://downloads.f5.com/esd/product.jsp?sw=BIG-IP&pro=iApp_Templates


8. Firewall ports have been configured for External DMZ Access (Front-End Firewall Rules) and firewall ports have been configured from DMZ to Internal Environment/VDI Network (Back-End Firewall Rules) to allow access to the environment as per VMware KB https://kb.vmware.com/kb/1027217. Also newest firewall rules can be referenced in VMware documentation for Unified Access Gateway in https://docs.vmware.com/en/Unified-Access-Gateway

9. For Single Namespace, internal vs external DNS need to be configured correctly for the Zones (Internet) to point at the Unified Access Gateway Servers Virtual IP (VIP) and the Internal DNS (LAN) would typically point at the Connection Servers Virtual IP (VIP).
Importing the iApp Template into BIG-IP

1. Login to the F5 Configuration utility.

![F5 Configuration Utility](image)

2. On the Main tab, click iApps > Templates.

![F5 Main Tab](image)

3. Click the Import button on the right upper side of the window.

![F5 Import Button](image)
4. Click the Choose File button.

5. Browse to the location where you extracted F5 iApp templates. For more information see the Prerequisites section.

6. Once the TMPL file is selected, the file name appears next to the Choose File button. Once that is correct, click Upload.

7. Once the upload is complete ensure the template is available. You can use the search "vmware" to find the template.
Importing a Certificate into BIG-IP

The next task is to import the certificate onto the BIG-IP.

1. Login to the F5 Configuration utility.

2. On the Main tab click System > Certificate Management.

3. Click the Import button on the upper right side of the window.
4. Complete the SSL Certificate/Key Source options. In this use case, we are importing a P12/PFX based file to the BIG-IP:
   a. From the **Import Type** list, select a certificate type.
   b. In the **Name** field, type a unique name for the certificate.
   c. Click the **Choose File** button and then locate your certificate file.
   d. In the **Password** field, type the password to decrypt the key in the file.
   e. Click **Import**.

After the import is completed you see your certificate in the window. Click the certificate to verify all the information in it.

5. **Verify the information in the Certificate/Key.**
Configuring your Horizon Environment for use with Unified Access Gateway.

1. Login to the VMware Horizon Admin using the FQDN or individual broker webpage.

2. In the Horizon Admin Window select a Broker, and then click Edit.
3. Ensure that the Checkboxes for **Use Secure Tunnel connection to machine**, **PCoIP Secure Gateway**, and **Use Blast Secure Gateway for Blast connections to machine** are **UNCHECKED**, as having any of these checked will cause connection issues.

4. In the Horizon Admin Window, edit any additional brokers that will be a part of the pool used to connect to the Unified Access Gateway Servers virtual server, and modify them in the same way as Step 3 (ensuring all boxes are unchecked).
iRule for the Horizon Origin Header

With the release of Horizon 7, a new implementation for accessing the Horizon admin page and HTML5 Blast was added. These changes require an additional implementation done either by the F5 BIG-IP as an iRule, or a configuration that must be done on each Connection Server to allow load balanced configurations to work correctly.

F5 has provided a KB https://support.f5.com/csp/article/K65620682 for resolution of this issue.

VMware has also provided a KB https://kb.vmware.com/kb/2144768 for resolution of this issue.

NOTE: Only one of these two methods are necessary.

Implementing an F5 iRule for Horizon Origin Header

1. Login to the BIG-IP Configuration utility.

2. On the Main tab, click Local Traffic > iRules and then click Create.
3. In the **Name** field, type a unique name for the iRule.

4. In the **Description** field, type or copy/paste the following iRule (found in the KB article referenced above):

   ```
   when HTTP_REQUEST {
       if {
           [HTTP::header "Origin"] ne "" 
       } {
           HTTP::header remove "Origin"
       }
   }
   ```

5. **Click Finished.** Once created you should see your newly created iRule in the list.
Creating/Deploying a Virtual IP for External Connections

As part of the workflow, the configuration has LTM placed in the front and behind the Unified Access Gateway (UAG) Servers. This is because in production scenarios, multiple UAG servers require load balancing. Connection servers that manage the Horizon environment in the datacenter must also be load balanced to prevent Single Points of Failure (SPoF).

A load balanced configuration is recommended, and an FQDN configured in DNS must be setup prior to deploying Unified Access Gateway. This ensures the Unified Access Gateway servers can access the load balanced Connection servers to prevent single points of failure.

Use this section to configure the BIG-IP for the UAG Servers for external use.

NOTE: There must be an internal Virtual IP (VIP) for the Horizon Connection Servers prior to configuring the UAG Servers. See Section Prerequisites for more details.
Using the iApp to Deploy a Virtual Server for UAG’s

Before beginning this task, ensure you have previously imported the iApp Template as described in the Importing iApp Template into BIG-IP section.

Note: F5 Recommends using the latest iApp Available to ensure latest functionality and features are implemented, this build was using iApp Version 1.5.7

1. On the Main tab, click iApps > Application Services > Create.

2. In the Template Selection section of the template, complete the following.
   a. In the Name field, type a unique name.
   b. From the Template list, select the template f5.vmware_view.v1.5.5 (or a newer version if available).

3. In the Template Options section, from the configuration mode question, select Advanced – configure advanced options.

4. In the BIG-IP Access Policy Manager section, select No, do not deploy BIG-IP Access Policy Manager.

5. In the SSL Encryption section, complete the following.
a. From the *How should the BIG-IP system handle encrypted traffic?* question, select **Terminate SSL for clients, re-encrypt to View Servers (SSL Bridging)**.

b. From the *Which Client SSL profile do you want to use?* question, select **Create a new Client SSL profile**.

c. From the *Which SSL certificate do you want to use?* and *Which SSL private key do you want to use?* questions, select the SSL certificate and key you imported in **Importing a Certificate into BIG-IP**.

d. (Optional) If using an Internal CA, we recommend you select an intermediate certificate.

<table>
<thead>
<tr>
<th>SSL Encryption</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How should the BIG-IP system handle encrypted traffic?</strong></td>
<td>Terminate SSL for clients, re-encrypt to View servers (SSL bridging)</td>
</tr>
<tr>
<td><strong>Which Client SSL profile do you want to use?</strong></td>
<td>Create a new Client SSL profile</td>
</tr>
<tr>
<td><strong>Which SSL certificate do you want to use?</strong></td>
<td>Wildcard</td>
</tr>
<tr>
<td><strong>Which SSL private key do you want to use?</strong></td>
<td>Wildcard</td>
</tr>
</tbody>
</table>
| **NOTE:** | Select the associated SSL key.

*Do you want to redirect inbound HTTP traffic to HTTPS?* | Redirect HTTP to HTTPS |

*From which port should HTTP traffic be redirected?* | 80 |
6. In the PC Over IP section, complete the following.
   a. From the **Should PCoIP connections go through the BIG-IP system?** question, select **Yes, PCoIP connection should go through the BIG-IP system.**
   b. From the **Will PCoIP connections be proxied by the VMware UAGs?** question, select **Yes, PCoIP connections are proxied by the VMware UAGs.**
   c. From the **Should Blast connections go through the BIG-IP system?** question, select **Yes, Blast connection should go through the BIG-IP system.**
   d. From the **Will Blast connections be proxied by the VMware UAGs?** question, select **Yes, Blast connections are proxied by the VMware UAGs.**

   ![PC Over IP Configuration](image)

7. In the Virtual Servers and Pools section, complete the following.
   a. Type the IP address for the virtual server.
   b. Type the FQDN to which external clients will connect with the Horizon Client.
   c. If a longer persistence is required due to longer global timeouts it is recommended to create a persistence profile and modify the setting. If using a default configuration leave the default recommended persistence profile.

   ![Virtual Servers and Pools Configuration](image)
8. Virtual Servers and Pools configuration continued.
   a. In the *Which servers should be included in this pool* section, type the IP addresses of the nodes for
      the Unified Access Gateway Servers, and ensure that port 443 is automatically set (if it is set to port
      80, then check previous step #3 and make sure **SSL Bridging** is selected and not **SSL Offload**).
      Click **Add** to include more servers.
   b. For the next two questions, select the options based on your environment.
   c. From the *Should the BIG-IP system insert the X-Forwarded-For header?* question, ensure **Yes**,
      **Insert the X-Forwarded-For HTTP header** is selected.

<table>
<thead>
<tr>
<th>Which servers should be included in this pool?</th>
<th>Node IP address</th>
<th>Node IP address</th>
<th>Port</th>
<th>Conn lim</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.105.185.100</td>
<td>10.105.185.101</td>
<td>443</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>10.105.185.102</td>
<td>10.105.185.103</td>
<td>443</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Where will the virtual servers be in relation to the view servers?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BIG-I P virtual server IP and View servers are an different subnet</strong></td>
</tr>
</tbody>
</table>

It is important to ensure that responses to client requests made using the BIG-I P virtual server address are returned through the BIG-I P system. If the client receives a response directly from the View server, the connection is dropped.

For environments in which the virtual server IP address is on a subnet different from the View servers, select **BIG-I P virtual server IP and View servers are on different subnets**.

For environments in which the virtual server IP address is on the same subnet as the View servers in the associated pool, select **BIG-I P virtual server IP and View servers are on the same subnet**. This enables Secure Network Address Translation (SNAT Auto Map). This configuration results in the BIG-I P system replacing the client IP address of an incoming connection with the IP address (using floating addresses when available) ensuring the server response returns through the BIG-I P system.

<table>
<thead>
<tr>
<th>How have you configured routing on your View servers?</th>
</tr>
</thead>
<tbody>
<tr>
<td>View servers do not have a route to clients through the BIG-I P</td>
</tr>
</tbody>
</table>

For environments in which the virtual server IP address is on a subnet different from the View servers, information regarding the IP setting of the View servers is required to ensure the correct BIG-I P system configuration.

If the View servers use the BIG-I P system as their default gateway, View servers will have a route for clients through the BIG-I P. In this scenario, no configuration is needed to support your environment to ensure correct server response handling.

<table>
<thead>
<tr>
<th>Should the BIG-I P system insert the X-Forwarded-For header?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, insert the X-Forwarded-For HTTP header</td>
</tr>
</tbody>
</table>

If the View servers do not have a route through the BIG-I P system, View servers do not have a route for clients through the BIG-I P. This enables Secure Network Address Translation (SNAT Auto Map). This configuration results in the BIG-I P system replacing the client IP address of an incoming connection with the View server IP address (using floating addresses when available) ensuring the server response returns through the BIG-I P system.

9. In the Client and Server Optimization sections, leave all settings at the defaults.

### Client Optimization

<table>
<thead>
<tr>
<th>Which Web Acceleration profile do you want to use for caching?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use a Web Acceleration profile</td>
</tr>
</tbody>
</table>

Caching is the local storage of data for re-use. Once an item is cached on the BIG-I P, the same data are served from local storage. This can improve client request response scalability by reducing load associated with processing subsequent requests.

Use a custom Web Acceleration profile only if you need to define specific URLs that should be cached.

<table>
<thead>
<tr>
<th>Which HTTP compression profile do you want to use?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not compress HTTP responses</td>
</tr>
</tbody>
</table>

Compression improves performance and end user experience for Web applications by reducing the amount of data sent to the client.

<table>
<thead>
<tr>
<th>How do you want to optimize client-side connections?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use P/S recommended optimizations for Wi-Fi clients</td>
</tr>
</tbody>
</table>

The client-side TCP profile optimizes the communication between the BIG-I P system and the client by reducing the number of connection attempts and improving connection reliability.

### Server Optimization

<table>
<thead>
<tr>
<th>Which OneConnect profile do you want to use?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use a OneConnect profile</td>
</tr>
</tbody>
</table>

OneConnect (connection pooling or multiplexing) improves server scalability by allowing concurrent connections and connections to move to servers. When enabled, a OneConnect connection to each View server is used to send requests from multiple clients.

<table>
<thead>
<tr>
<th>How do you want to optimize server-side connections?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use P/S recommended optimizations for the LAN</td>
</tr>
</tbody>
</table>

The server-side TCP profile optimizes the communication between the BIG-I P system and the server by reducing the number of connection attempts and improving connection reliability.
10. In the Application Health section, Select “Create a simple health monitor” as the Advanced monitor does NOT work with UAG Servers.

![Application Health](image)

How many seconds should pass between health checks?

- **30**

   This is the duration, in seconds, of a single monitor cycle. At this interval, the application instance on each View server configured in the View server pool will be monitored.

11. If you created the iRule in **iRule for the Horizon Origin Header**, from the Options list, select the iRule you created and click the Add (<<) button to move it to the Selected list. Using the iRule removes the need to disable the origin header within the servers' locked.properties.

   **Note:** If you used the VMware Origin Header method, skip this step.

   ![iRules](image)

   **Do you want to add any custom iRules to the virtual server used by remote clients?**

   ![Options](image)

12. In the Statistics and Logging section, leave the defaults and then click the **Finished** button.

   ![Statistics and Logging](image)

   **Which HTTP request logging profile do you want to use?**

   ![Additional Steps](image)

   - **Do not enable HTTP request logging**

   ![Additional Steps](image)

   **Modifying your DNS Settings**

   You must configure a DNS entry with the fully qualified host name that clients will use to access the View environment. The DNS record must resolve to the IP address you configured for the BIG-IP network access virtual server.

   ![Additional Steps](image)

   **Configuring SSL settings on the servers**

   Depending on your service and application software, you may have to perform additional steps on your application to enable SSL Offloading. If you are performing SSL offload on the BIG-IP system, you may need to configure your servers not to expect SSL to avoid certificate errors and unnecessary redirects. Also, the server software may need to be configured to handle any HTTP/1.1 HEAD requests if you specified handle HEADs during monitor creation.

   ![Additional Steps](image)

   **Configuring the View Servers**

   You must configure the External URL setting on each View Server to use the IP address (or DNS name) of the BIG-IP virtual server (the address you specified) as the IP address of the BIG-IP virtual server (the address you specified) that View clients will use to access the View deployment. For specific instructions, see the View 5 Deployment Guide: [http://www.vmware.com/pdf/deployment-guide/vmware-view-5-app-dg.pdf](http://www.vmware.com/pdf/deployment-guide/vmware-view-5-app-dg.pdf)

   ![Additional Steps](image)

   **Apply Access Policy**

   If using BIG-IP ARP, you may need to click the ‘Apply Access Policy’ link (in the upper left corner of the Configuration Edit form) to the right of the F5 logo after running the URL template:

   ![Additional Steps](image)

   **Troubleshooting**

   If you have deployed ARP for secure network access and are unable to login, ensure a subdomain of the domain name is entered correctly and your DNS Search Domain List entries are properly populated.

   ![Additional Steps](image)

13. After clicking Finished, the summary screen appears. You should see all monitored items with a green Available icon if configured correctly.
Final Configuration

Once completed, you should the iApp (1.5.7) will create the below configuration for F5 LTM with VMware Horizon Unified Access Gateway (UAG) for PCoIP and Blast Extreme TCP/UDP with BEAT (Blast Extreme Adaptive Transport).
Manually Creating a Virtual Server for UAG’s

This Section is for customers who wish to manually configure the Virtual Servers for integrating a VMware UAG with F5

Note: If you previously created an iAPP deployment with the information in previous sections you do NOT need to follow these steps.

Creating Monitors

HTTPS - Monitor

1. Create a simple HTTPS monitor using the following guidance.
   a. On the Main tab, click Local Traffic > Monitors > Create.
   b. In the Name field, type a unique name.
   c. From the Type list, select HTTPS.
   d. Ensure the Parent Monitor is https.
   e. In the Interval field, type 30.
   f. In the Timeout field, type 91.
   g. In the Send String field, type (or copy and paste): {FQDN} is replaced by FQDN for VIP:
      GET /broker/xml/ HTTP/1.1
      Host: {FQDN}
      Connection: Close
   h. In the Receive String field, type clientlaunch-default.
   i. Leave all other settings at the default and then click Finished.
1. Create a simple HTTPS monitor using the following guidance.
   a. On the Main tab, click Local Traffic > Monitors > Create.
   b. In the Name field, type a unique name (different from the first).
   c. From the Type list, select HTTPS.
   d. Ensure the Parent Monitor is https.
   e. In the Interval field, type 30.
   f. In the Timeout field, type 91.
   g. In the Send String field, type (or copy and paste):
      ```
      GET /favicon.ico HTTP/1.1
      Host: 
      Connection: Close
      ```
   h. In the Receive String field, type 200
   i. In the Receive Disable String field, type 503
   j. Leave all other settings at the default and then click Finished.
TCP (PCoIP/Blast) - Monitor

1. Create a simple monitor for TCP (PCoIP/Blast) using the following guidance.
   a. On the Main tab, click **Local Traffic > Monitors > Create**.
   b. In the **Name** field, type a unique name.
   c. From the **Type** list, select **TCP**.
   d. Ensure the Parent Monitor is **tcp**.
   e. In the **Interval** field, type **30**.
   f. In the **Timeout** field, type **91**.
   g. Leave all other settings at the default and then click **Finished**.

![Monitor Configuration Screen](image)
**UDP (PCoIP/Blast) - Monitor**

1. Create a simple monitor for UDP (PCoIP/Blast) using the following guidance.
   a. On the Main tab, click **Local Traffic > Monitors > Create**.
   b. In the **Name** field, type a unique name.
   c. From the **Type** list, select **UDP**.
   d. Ensure the Parent Monitor is **udp**.
   e. In the **Interval** field, type **30**.
   f. In the **Timeout** field, type **91**.
   g. In the **Send String** field, type (or copy and paste):
      
      `default send string`
      
   h. Leave all other settings at the default and then click **Finished**.

### Local Traffic > Monitors > Create Monitor

**General Properties**

- **Name**: MyHZN-LTM-4P_udp
- **Description**: 
- **Type**: UDP
- **Parent Monitor**: udp

**Configuration**: Basic

- **Interval**: 30 seconds
- **Timeout**: 91 seconds
- **Send String**: default send string
Creating Pools

Port 443 - Pool

1. Create a pool of servers for Port 443, using the following guidance.
   a. On the Main tab, click **Local Traffic > Pools > Create**.
   b. In the **Name** field, type a unique name.
   c. In the **Health Monitors** area, select all of the monitors created previously (https, uag_maintenance) and then click the Add (<<) button to move them to Active.
   d. From the **Load Balancing Method** list, select **Least Connections (member)**.
   e. In the **New Members** area, complete the following.
      i. Click the **New Node** button.
      ii. (Optional) In the **Node Name** field, type a name for the node.
      iii. In the **Address** field, type the IP address of a Unified Access Gateway Server.
      iv. In the **Service Port** field, type the port of the Unified Access Gateway Server (443).
      v. Click the **Add** button.
   f. Click **Finished**.
Port 8443 - Pool

1. Create a pool of servers for Port 8443 using the following guidance.
   a. On the Main tab, click Local Traffic > Pools > Create.
   b. In the Name field, type a unique name.
   c. In the Health Monitors area, select the TCP and UDP monitor you created previously and then click the Add (<<) button to move it to Active.
   d. From the Load Balancing Method list, select Least Connections (member).
   e. In the New Members area, complete the following.
      i. Click the New Node button.
      ii. (Optional) In the Node Name field, type a name for the node.
      iii. In the Address field, type the IP address of a Unified Access Gateway Server.
      iv. In the Service Port field, type the port of the Unified Access Gateway Server (8443).
      v. Click the Add button.
   f. Click Finished.
Port 4172 - Pool

1. Create a Pool of servers for Port 4172 using the following guidance.
   a. On the Main tab, click Local Traffic > Pools > Create.
   b. In the Name field, type a unique name.
   c. In the Health Monitors area, select the TCP and UDP monitor you created previously and then click the Add (<>) button to move it to Active.
   d. From the Load Balancing Method list, select Least Connections (member).
   e. In the New Members area, complete the following.
      i. Click the New Node button.
      ii. (Optional) In the Node Name field, type a name for the node.
      iii. In the Address field, type the IP address of a Unified Access Gateway Server.
      iv. In the Service Port field, type the port of the Unified Access Gateway Server (4172).
      v. Click the Add button.
   f. Click Finished.

Validate Pools Online

After a few minutes ensure all the statuses are green on the Pool Objects with the monitors to ensure that the Unified Access Gateway (UAG) Servers are online and functioning appropriately.
Creating Profiles

Creating a HTTP Profile

1. Create an HTTP profile using the following guidance.
   a. On the Main tab, click Local Traffic > Profiles > Services > HTTP > Create.
   b. In the Name field, type a unique name.
   c. From the Parent Profile list, ensure http is selected.
   d. From the Redirect Rewrite row, click the Custom checkbox on the right, and then select Matching from the list.
   e. From the Insert X-Forwarded-For row, click the Custom box and then select Enabled.
   f. Leave all other settings at the default and then click Finished.

<table>
<thead>
<tr>
<th>General Properties</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>MyLocalLTM-AP_H</td>
</tr>
<tr>
<td>Proxy Mode</td>
<td>Reverse</td>
</tr>
<tr>
<td>Parent Profile</td>
<td>http</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Auth Realm</td>
<td></td>
</tr>
<tr>
<td>Fallback Host</td>
<td></td>
</tr>
<tr>
<td>Fallback on Error Codes</td>
<td></td>
</tr>
<tr>
<td>Request Header Erase</td>
<td></td>
</tr>
<tr>
<td>Request Header Insert</td>
<td></td>
</tr>
<tr>
<td>Response Headers Allowed</td>
<td></td>
</tr>
<tr>
<td>Request Chaining</td>
<td></td>
</tr>
<tr>
<td>Response Chaining</td>
<td></td>
</tr>
<tr>
<td>OneConnected Transformations</td>
<td></td>
</tr>
<tr>
<td>Redirect Rewrite</td>
<td></td>
</tr>
<tr>
<td>Encrypt Cookies</td>
<td></td>
</tr>
<tr>
<td>Cookie Encryption Passphrase</td>
<td></td>
</tr>
<tr>
<td>Confirm Cookie Encryption Passphrase</td>
<td></td>
</tr>
<tr>
<td>Insert X-Forwarded-For</td>
<td></td>
</tr>
<tr>
<td>URI Maximum Columns</td>
<td></td>
</tr>
<tr>
<td>URI Separator</td>
<td></td>
</tr>
<tr>
<td>Maximum Requests</td>
<td></td>
</tr>
<tr>
<td>Send Proxy Via Header In Request</td>
<td></td>
</tr>
<tr>
<td>Send Proxy Via Header In Response</td>
<td></td>
</tr>
<tr>
<td>Accept OFF</td>
<td></td>
</tr>
<tr>
<td>XFF Alternative Names</td>
<td></td>
</tr>
<tr>
<td>Server Agent Name</td>
<td></td>
</tr>
</tbody>
</table>

* Cancel | Repeat | Finished
Creating a UDP Protocol Profile

1. Create an UDP profile using the following guidance.
   b. In the Name field, type a unique name.
   c. From the Parent Profile list, ensure udp is selected.
   d. Leave all other settings at the default and then click Finished.
Creating a TCP-WAN-Optimized Profiles

1. Create a TCP profile using the following guidance.
   b. In the Name field, type a unique name.
   c. From the Parent Profile list, ensure tcp-wan-optimized is selected.
   d. In Data Transfer section in the Nagle’s Algorithm row, click the Custom checkbox on the right, and then select Enable from the list.
   e. Leave all other settings at the default and then click Finished.

Creating a TCP-LAN-Optimized Profiles

1. Create a TCP profile using the following guidance.
   b. In the Name field, type a unique name.
   c. From the Parent Profile list, ensure tcp-lan-optimized is selected.
   d. Leave all other settings at the default and then click Finished.
Creating a Persistence Profile

1. Creating a Persistence profile using the following guidance.
   a. On the Main tab, click Local Traffic > Profiles > Persistence > Create.
   b. In the Name field, type a unique name.
   c. From the Persistence Type list, select Source Address Affinity.
   d. From the Parent Profile list, ensure source_addr is selected.
   e. If you have deployed a redundant pair of BIG-IP systems only:
      - From the Mirror Persistence row, click the Custom checkbox on the right, and then click the checkbox to enable persistence mirroring.
   f. From the Match Across Services row, click the Custom checkbox, and then click the checkbox to enable matching across services.
   g. From the Match Across Virtual Servers row, ensure the Match Across Virtual Servers box is UNCHECKED.
   h. (Optional) Timeout can be increased for environments who increase in Horizon the “Global Session Timeout” variable (when increased the heartbeats in Horizon are lengthened and its recommended to increase the Timeout variable to accommodate)
   i. Click Finished.
Creating a Client SSL Profile

1. Create a Client SSL profile using the following guidance.
   a. On the Main tab, click **Local Traffic > Profiles > SSL > Client > Create**.
   b. In the **Name** field, type a unique name.

c. From the **Configuration** list, select **Advanced**
d. From the **Certificate Key Chain** area, click the **Custom** checkbox and then click the **Add** button.

e. In the **Edit SSL Certificate to Key Chain** box, complete the following.
   i. From the **Certificate** list, select the certificate you imported in *Importing a Certificate into BIG-IP*.
   ii. From the **Key** list, select the key you imported in *Importing a Certificate into BIG-IP*.
   iii. (Optional) If you imported a chain certificate, select the Intermediate/Root Chain you imported in *Importing a Certificate into BIG-IP*.
   iv. (Optional) If your key is highly encrypted, in the **Passphrase** box, type the passphrase.
   v. Click **ADD**.
f. In the Ciphers area, click the Custom box, and then click the Cipher String button.

g. In the Ciphers field, type DEFAULT:!RC4:!MEDIUM:@STRENGTH

h. In the Options field, click the Custom box (leave defaults)

i. In the Handshake Timeout field, click the Custom box, and specify 10 seconds

j. From the Client Certificate row, click the Custom checkbox and then select Ignore from the list.

k. From the Trusted Certificate Authorities row, click the Custom checkbox and then select None from the list.

l. From the Advertised Certificate Authorities row, click the Custom checkbox and then select None from the list.

m. Scroll to the bottom and click Finished.
Creating a Server SSL Profile

1. Create a Server SSL profile using the following guidance.
   n. On the Main tab, click **Local Traffic > Profiles > SSL > Server > Create**.
   o. In the **Name** field, type a unique name.
   p. From the **Parent Profile** list, ensure **serverssl** is selected.

   ![Local Traffic > Profiles > SSL > Server > Create](image)

   q. From the **Configuration** list, select **Advanced**.
   r. In the **Ciphers** area, click the **Custom** box, and then click the **Cipher String** button.
   s. In the **Ciphers** field, type **DEFAULT:!DHE:@STRENGTH**
   t. Leave all other settings at the defaults and then click **Finished**.

![Configuration](image)
Creating Virtual Servers

HTTP Redirect - Virtual Server

1. Create an HTTP Redirect virtual server using the following guidance.
   a. On the Main tab, click Local Traffic > Virtual Servers > Create
   b. In the Name field, type a unique name.
   c. From the Type list, ensure Standard is selected.
   d. In the Destination Address/Mask field, type the IP Address for the virtual server.
   e. In the Service Port field, type 80 or select HTTP from the list.
   f. From the Protocol list, select TCP.
   g. From the Protocol Profile (Client) list, select the TCP-WAN-Optimized profile previously created.
   h. From the Protocol Profile (Server) list, select the TCP-LAN-Optimized profile previously created.
   i. From the HTTP Profile list, select the HTTP profile previously created.
   j. From the Source Address Translation list, select Auto Map.
k. In the iRules area, from the Available list, select _sys_https_redirect and then click the Add (<<) button.

l. Leave all other settings at the defaults and then click Finished.
**Port 443 TCP - Virtual Server**

1. Create the main virtual server (Port 443 TCP) using the following guidance.
   a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
   b. In the **Name** field, type a unique name.
   c. From the **Type** list, ensure **Standard** is selected.
   d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
   e. In the **Service Port** field, type 443 or select **HTTPS** from the list.
   
   ![Virtual Server Configuration](image)

   f. From the **Protocol** list, select **TCP**.
   g. From the **Protocol Profile (Client)** list, select the **tcp-wan-optimized** profile you created previously.
   h. From the **Protocol Profile (Server)** list, select the **tcp-lan-optimized** profile you created previously.
   i. From the **HTTP Profile** list, select the **HTTP** profile you created previously.
   j. From the **SSL Profile (Client)** list, select the **clientssl** profile you created previously and click the **Add (<<)** button to move it to the Selected list.
   k. From the **SSL Profile (Server)** list, select the **serverssl** profile you created previously and click the **Add (<<)** button to move it to the Selected list.
   l. From the **Source Address Translation** list, select **Auto Map**.

![Configuration Details](image)
m. If you created the iRule for the Horizon Origin Header only: In the **iRules** area, select the iRule you created in **iRule for the Horizon Origin Header** and then click the Add (<<) button.

   **Note:** If VMware Origin Header method was used skip this step.

n. From the **Default Pool** list, select the pool you created in **Port 443 - Pool**.

o. From the **Default Persistence Profile** list, select the profile you created previously.

p. Click **Finished**.
**Port 443 UDP - Virtual Server**

1. Create the main virtual server (Port 443 UDP) using the following guidance.
   a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
   b. In the **Name** field, type a unique name.
   c. From the **Type** list, ensure **Standard** is selected.
   d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
   e. In the **Service Port** field, type **443** or select **HTTPS** from the list.
   f. From the **Protocol** list, select **UDP**.
   g. From the **Protocol Profile (Client)** list, select the **udp profile** you created previously.
   h. From the **Protocol Profile (Server)** list, select **(Use Client Profile)**.
   i. From the **Source Address Translation** list, select **Auto Map**.
Creating the main virtual server (continued)

j. From the **Default Pool** list, select the pool you created in **Port 443 - Pool**.
k. From the **Default Persistence Profile** list, select the profile you created previously.
l. Click **Finished**.
Port 8443 TCP - Virtual Server

1. Creating the main virtual server for Port 8443 TCP
   a. On the Main tab, click Local Traffic > Virtual Servers > Create
   b. In the Name field, type a unique name.
   c. From the Type list, ensure Standard is selected.
   d. In the Destination Address/Mask field, type the IP Address for the virtual server.
   e. In the Service Port field, type 8443.
   f. From the Protocol list, select TCP.
   g. From the Protocol Profile (Client) list, select the tcp-wan-optimized profile you created previously.
   h. From the Protocol Profile (Server) list, select the tcp-lan-optimized profile you created previously.
   i. From the Source Address Translation list, select Auto Map.
j. From the **Default Pool** list, select the pool you created in [Port 8443 - Pool](#).
k. From the **Default Persistence Profile** list, select the profile you created in [Creating a Persistence Profile](#).
l. Click **Finished**.
Port 8443 UDP - Virtual Server

1. Creating the main virtual server for Port 8443 UDP
   a. On the Main tab, click Local Traffic > Virtual Servers > Create
   b. In the Name field, type a unique name.
   c. From the Type list, ensure Standard is selected.
   d. In the Destination Address/Mask field, type the IP Address for the virtual server.
   e. In the Service Port field, type 8443.

   ![Virtual Server Configuration](image1)

   f. From the Protocol list, select UDP.
   g. From the Protocol Profile (Client) list, select UDP profile you created previously.
   h. From the Source Address Translation list, select Auto Map.

   ![Protocol and Address Configuration](image2)
i. From the **Default Pool** list, select the pool you created in Port 8443 - Pool.

j. From the **Default Persistence Profile** list, select the profile you created in Creating a Persistence Profile.

k. Click **Finished**.
**Port 4172 TCP - Virtual Server**

1. Create the main virtual server (Port 4172 TCP) using the following guidance.
   a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
   b. In the **Name** field, type a unique name.
   c. From the **Type** list, ensure **Standard** is selected.
   d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
   e. In the **Service Port** field, type **4172**.
   f. From the **Protocol** list, select TCP profile you created previously.
   g. From the **Protocol Profile (Client)** list, select **tcp-wan-optimized**.
   h. From the **Protocol Profile (Server)** list, select **tcp-lan-optimized**.
   i. From the **Source Address Translation** list, select **Auto Map**.
j. From the **Default Pool** list, select the pool you created in Port 4172 – Pool.

k. From the **Default Persistence Profile** list, select the profile you created in Creating a Persistence Profile.

l. Click **Finished**.
Port 4172 UDP - Virtual Server

1. Create the main virtual server (Port 4172 UDP) using the following guidance.
   a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
   b. In the **Name** field, type a unique name.
   c. From the **Type** list, ensure **Standard** is selected.
   d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
   e. In the **Service Port** field, type **4172**.

   ![Virtual Server Configuration](image)

   f. From the **Protocol** list, select **UDP**.
   g. From the **Protocol Profile (Client)** list, select UDP profile you created previously.
   h. From the **Source Address Translation** list, select **Auto Map**.
i. From the Default Pool list, select the pool you created in PCoIP - Pool.

j. From the Default Persistence Profile list, select the profile you created in Creating a Persistence Profile.

k. Click Finished.
**Final Configuration**

Once completed you should see the full configuration for F5 LTM with VMware Horizon Unified Access Gateway (UAG) for PCoIP and Blast Extreme TCP/UDP with BEAT (Blast Extreme Adaptive Transport).
Testing the VMware Horizon Connection

After setting up the Virtual IPs (VIPs) for the Unified Access Gateways, you can use the following methods validate that the External VIP is connecting and working properly. In this case, you are now using the new FQDN site name to connect to the Horizon Environment.

NOTE: This connection test should be done from an external computer on the Internet.

1. In a browser, type the FQDN for the VIP you previously created (for example, https://myhzn.bd.f5.com).

You should see the VMware Horizon Client/HTML5 Page. This confirms that your servers are working through the newly created virtual server.
2. You can also test the VMware Horizon Client to ensure accessibility to the Horizon Environment. After logging in you should see the apps/desktops associated with the user that logged on.

Select a Pool to validate connectivity and ensure that you can access a desktop. Once the connection is validated the environment is correctly setup for LTM with the Horizon servers.
References

Load Balancing across VMware Unified Access Gateway Appliances (formerly known as Access Point) – Mark Benson & Vish Kalsi
https://communities.vmware.com/docs/DOC-32792