Microsoft Forefront Unified Access Gateway Deployment

https://campus.barracuda.com/doc/41113213/

Microsoft Forefront Unified Access Gateway (UAG) provides remote end users access to corporate applications, networks, and internal resources via a Web portal or site.

The Barracuda Load Balancer ADC increases the performance, scalability, and reliability of Forefront UAG. It distributes traffic among the UAG Servers in your deployment for better load distribution and monitors the health of each server.

Terminology

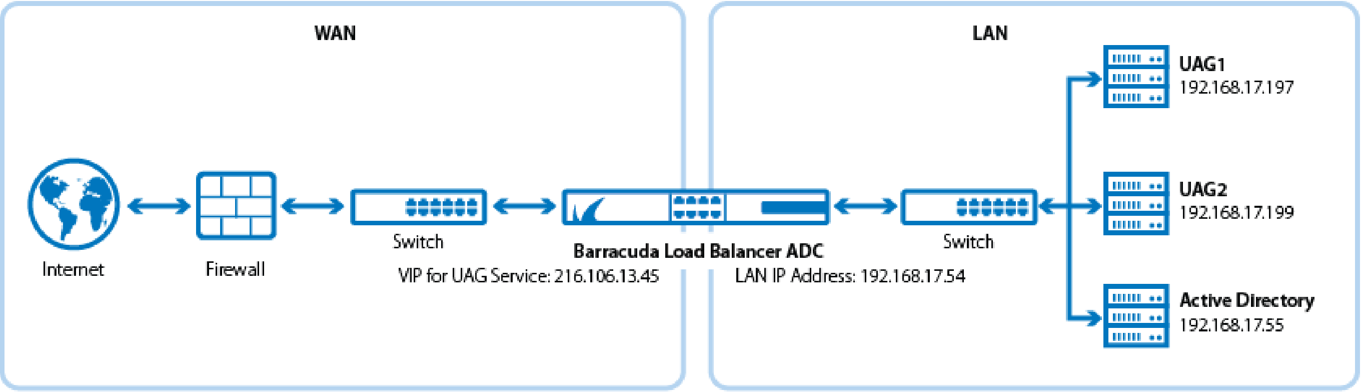
Term	Definition
DNS	Domain Name Server, typically hosted on the Domain Controller
VIP	Virtual IP address. In the ADC deployment, the VIP is added to the service on the Barracuda Load Balancer ADC.
Service	A combination of a virtual IP address and one or more TCP/UDP ports that the Barracuda Load Balancer ADC listens on. Traffic arriving on the specified port(s) is directed to one of the real servers associated with a service.
UAG Array	A combination of two or more Forefront UAG servers existing as a logical unit and which share the same configuration.

Product Versions and Prerequisites

You must have:

- Barracuda Load Balancer ADC version 5.1 or 5.2.
- Microsoft Forefront Unified Access Gateway 2010.
- Installed your Barracuda Load Balancer ADC(s), connected to the web interface, and activated your subscription(s).
- If you want to deploy Microsoft Forefront Unified Access Gateway with high availability, cluster your Barracuda Load Balancer ADCs. For more information, see High Availability.

Deployment Scenario



Barracuda Load Balancer ADC Service Options

On the Barracuda Load Balancer ADC, create services for the types of traffic that are supported by your Microsoft Forefront Unified Access Gateway servers. Depending on the traffic type, you can create HTTP or HTTPS services.

Scenario	Service Options
The UAG servers support traffic over HTTP only.	Create an HTTP service.
The UAG servers support traffic over HTTPS only.	Create an HTTPS service.

Deploy the Barracuda Load Balancer ADC for UAG

To deploy the Barracuda Load Balancer ADC for UAG servers in an array, complete the following steps :

Step 1. Configure your UAG Servers in an array

1. Set up at least two UAG servers with your preferred operating system.
2. Configure the servers in an array.

Step 2. (HTTPS Only) Import UAG Certificates

If you want to create an HTTPS service, import either a certificate from the UAG servers or a CA certificate.

1. Log into the Barracuda Load Balancer ADC as an administrator.
2. Go to the **BASIC > Certificates** page and upload the certificates.
3. If you are using a CA certificate, ensure that you also import it on the UAG servers.

Step 3. Create Services on the Barracuda Load Balancer ADC

On the Barracuda Load Balancer ADC, create services according to the type of traffic supported by your UAG servers.

1. Log into the Barracuda Load Balancer ADC as the administrator.
2. Go to the **BASIC > Services** page.
3. For each type of service that you add from Table 1, click **Add Service** and enter the values in the corresponding fields.

Table 1. Available Services

Name	Type	IP Address	Port	Session Timeout	Certificate	Load Balancing	Server Monitor
UAG_HTTP	HTTP	The VIP address for the UAG service. For example: `10.5.7.193`	80	1800	Not applicable	◦ **Persistence Type**: Source IP ◦ **Persistence Time**: 600	◦ **Testing Method: TCP Port Check** (or) ◦ **Testing Method:** Simple HTTP ◦ **HTTP Method:** GET ◦ **Test Target:** / ◦ **Additional Headers:** Host: adcuag.qa.cudaops.com (Specify the host of the UAG Administration Portal). ◦ **Status Code:** 302 (because the login URL involves redirection)

UAG_HTTPS	HTTPS	The VIP address for the UAG service. For example: `10.5.7.193`	443	1800	Select the certificate that you uploaded for the service.	◦ **Persistence Type**: Source IP ◦ **Persistence Time**: 600	◦ **Testing Method: TCP Port Check** (or) ◦ **Testing Method:** Simple HTTPS ◦ **HTTP Method:** GET ◦ **Test Target:** / ◦ **Additional Headers:** Host: adcuag.qa.cudaops.com (Specify the host of the UAG Administration Portal). ◦ **Status Code:** 302 (because the login URL involves redirection)

4. Click **Create**.

Step 4. Add the Real (UAG) Servers

1. On the **BASIC > Services** page, verify that the correct service for the server is displayed.
2. Click **Add Server**.
3. Enter the IP address and port of the server.
   - If you are adding the server to an HTTP service, use **Port** `80`.
   - If you are adding the server to an HTTPS, use **Port** 443.
4. If the server is part of a cluster, specify whether it is a **Backup server** and enter its **Weight** for the load balancing algorithm.
5. If you are adding the server to an HTTPS service, enable SSL.
   1. Set **Servers uses SSL** to **On**. If you do not enable the server to use SSL, unencrypted traffic is passed to the server because the Barracuda Load Balancer ADC decrypts incoming traffic in order to maintain session persistence using HTTP cookies.
   2. If the certificate for the service is a self-signed or a test certificate, set **Validate Certificate** to **Off**. If the service is using a CA-signed certificate, select **On**.
   3. Select the **Certificate** that you uploaded for the UAG server.
6. Click **Create**.

Step 5. Configure the DNS

Create an A record to point the VIP address that you set on the Barracuda Load Balancer ADC for the UAG service.

For example, if you want to use the name *adcuag* and your domain is *barracuda.com*, your A record would be:

Name	IP Address
adcuag.barracuda.com	10.5.7.193

Verify Your Configuration

To ensure that your setup is fully working, navigate to the UAG Admin site by using the name that you set in the A record and verify that the page displays correctly.

For example: `https://adcuag.barracuda.com`

Figures

1. UAG_deployment_new.png