



Deployment Guide

AX Series with Unified Access Gateway 2010



TABLE OF CONTENTS

1	Introduction	4
2	Deployment Guide Overview	4
3	Deployment Guide Prerequisites	4
4	Accessing the AX Series Load Balancer	5
5	Architecture Overview	6
6	Unified Access Gateway Solution Server Roles	7
7	Initial Required Configuration	8
7.1	Health Monitor Configuration	8
7.2	Source NAT Configuration	9
7.3	Source IP Persistence	10
7.4	SSL Certificate	11
7.4.1	Option 1: Generate a Self-Signed Certificate	11
7.4.2	Option 2: Import the Certificate and Key	12
7.4.3	Configure and Apply Client-SSL Template	13
8	Secure Access Layer	15
8.1	Server Configuration	16
8.2	Service Group Configuration	17
8.3	Virtual Server Configuration	18
9	Advanced Access Configuration	20
9.1	Cookie Persistence	21
9.2	TCP Connection Reuse	21
9.3	Apply Optimization and Acceleration Feature Templates To VIP	22
9.4	Enable DDoS Protection	22
10	Application Layer Load Balancing	23

11	Summary and Conclusion	24
A.	CLI Configuration for Secure Access Layer	24

1 INTRODUCTION

Microsoft Unified Access Gateway (UAG) 2010 is part of the Microsoft Forefront security product line. The UAG is a comprehensive remote access software solution that can offer secure unified access to internal corporate systems. The UAG acts as an inbound access control system.

2 DEPLOYMENT GUIDE OVERVIEW

This deployment guide describes how to deploy the AX Series Application Delivery Controller (ADC)/Server Load Balancer to optimize Microsoft Unified Access Gateway. The AX Series offers advanced optimization features such as SSL Offload, Connection Reuse, Cookie Persistence, Source IP Persistence and DDoS Protection.

3 DEPLOYMENT GUIDE PREREQUISITES

This deployment guide has the following prerequisites.

AX Series Requirement:

The A10 Networks AX Series ADC must be running version 2.4.x or higher.

Tested Microsoft Unified Access Gateway Server:

- 2.66 GHz or faster Dual-Core processor CPU
- 4 GB Memory
- 2 Processors
- 40 GB Storage
- Dual network interface card (NIC) adapter for internal (private network) and external (Internet-facing NIC).

Unified Access Gateway Pre-installation Requirements:

- Server 2008 R2 Enterprise 64-bit Operating System
- Windows role and feature requirements:
 - ◆ Network Policy Server
 - ◆ Routing and Remote Access Services

- ◆ Active Directory Lightweight Directory Services Tools
- ◆ Message Queuing Services
- ◆ Web Services (IIS) Tools
- ◆ Network Load Balancing Tools
- ◆ Windows PowerShell

Other Requirements:

- Microsoft .NET Framework 3.5 SP1
- Windows Web Services API
- Windows Update
- Microsoft Windows Installer 4.5
- SQL Server Express 2005
- Forefront TMG is installed as a firewall during Forefront UAG setup. Following setup, Forefront TMG is configured to protect the Forefront UAG server. For information about running Forefront TMG with Forefront UAG, see [Supported Forefront TMG configurations](#).
- The Windows Server 2008 R2 DirectAccess component is automatically installed. For more information, see the [Forefront UAG DirectAccess technical overview](#).

Note: Generally, if the Virtual IP (VIP) is accessed from an external client, the AX device would be deployed in a routed mode. If the web site services are accessed internally, the AX device would be deployed in one-arm mode. If the web server applications are accessed from both internal and external clients, the AX device would be deployed in one-arm mode.

Note: For additional deployment modes the AX Series device can support, please visit the following URL:

<http://www.a10networks.com/products/axseries-load-balancing101.php>

4 ACCESSING THE AX SERIES LOAD BALANCER

This section describes how to access the AX Series device. The AX device can be accessed either from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:

- ◆ Secure protocol – Secure Shell (SSH) version 2
- ◆ Unsecure protocol – Telnet (if enabled)
- GUI – web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using the following protocol:
 - ◆ Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Note: *HTTP requests are redirected to HTTPS by default on the AX device.*

Default Access Information:

- Default username: “admin”
- Default password: “a10”
- Default IP address of the device: “172.31.31.31”

(For detailed information on how to access the AX Series device, refer to the *A10 Networks AX Series System Configuration and Administration Guide*.)

5 ARCHITECTURE OVERVIEW

This deployment guide offers two layers of traffic load balancing, namely:

- Secure Access Layer. This layer of the network is where the UAG traffic is load balanced across a pool of UAG Servers.
- Application Layer. This layer of the network is where the internal application within the corporate network is load balanced.

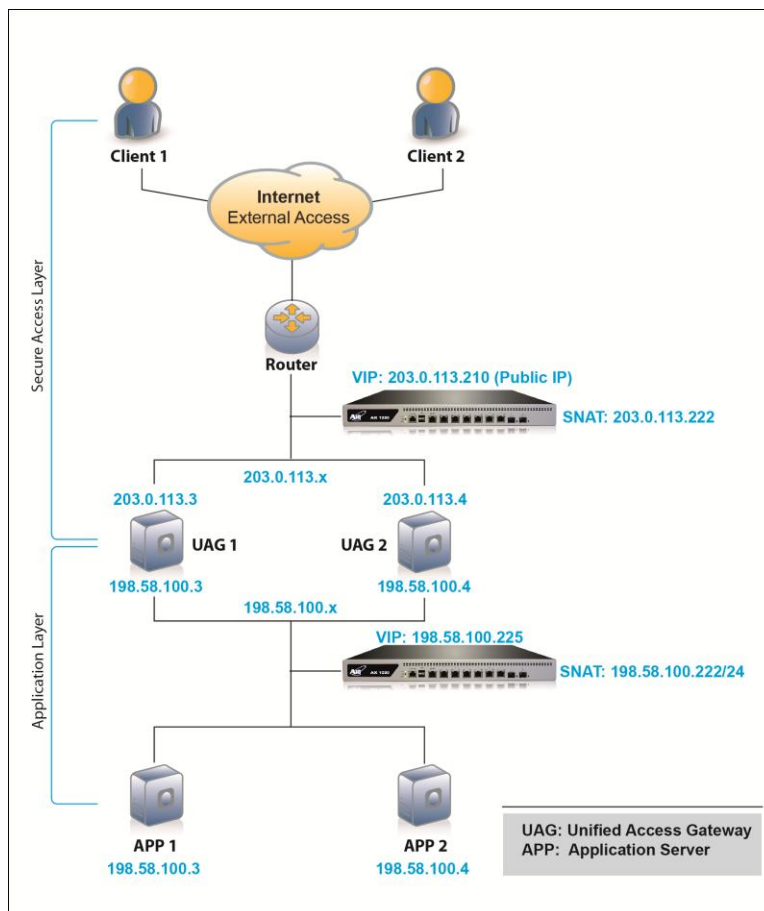


Figure 1: Configuration overview

6 UNIFIED ACCESS GATEWAY SOLUTION SERVER ROLES

Unified Access Gateway required servers and roles:

- Active Directory (AD) – All UAG servers must be joined in a domain and in Active Directory Domain Services (ADDS).
- UAG Servers: This is a pool of UAG servers and responsible to provide reverse proxy and act as a VPN solution that provides secure access to corporate networks.
- Application Servers: This is a pool of servers that resides within the internal corporate network. Application Server is used as a generic term for internal business applications within a corporation such as Microsoft SharePoint, Microsoft Exchange, Oracle applications or web servers.

7 INITIAL REQUIRED CONFIGURATION

This section of the deployment guide details the initial configuration within the AX appliance. The initial requirement is to configure the following items:

- **Health Monitor:** Sends periodic health checks to configured servers and/or all the server members of a service group. The health checks can be configured with different protocol types, health monitor retries, time intervals between each health check, health check timeouts and many other customizable health check options.
- **Source NAT:** Translates internal host addresses into global routable addresses before sending the host's traffic to the Internet. When reply traffic is received, the AX device then retranslates the addresses back into internal addresses before sending the reply to the client.
- **Session Persistence:** Enables a user to direct multiple requests to the same UAG server based on the source IP address.
- **SSL Certificate:** An SSL certificate is required in this deployment guide to provide secure connection to the pool of UAG servers.

Note: *These items must be configured on the AX appliances located in both the External and Internal segments (on both the Secure Access Layer and the Application Layer).*

7.1 HEALTH MONITOR CONFIGURATION

The AX Series can automatically initiate health status checks for real servers and service ports. Health checks assure that all requests go to functional and available servers. If a server or a port does not respond appropriately to a health check, the server is temporarily removed from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server is automatically added back to the list of available servers.

1. Navigate to **Config Mode > Service > Health Monitor > Health Monitor**.
2. Click **Add**.
3. In the **Name** field, enter "UAGHC".
4. Select **Method** "HTTPS".
5. Click **OK**, and then see the next section to continue with the Service Group configuration.

Health Monitor		
Name: *	UAGHC	
Retry:	3	
Consec Pass Req'd:	1	
Interval:	5	Seconds
Timeout:	5	Seconds
Strictly Retry:	<input type="checkbox"/>	
Disable After Down:	<input type="checkbox"/>	

Method	
Override IPv4:	
Override IPv6:	
Override Port:	
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External
Type:	HTTPS
Port:	443
Host:	
URL:	GET /
User:	
Password:	
Expect:	<input type="radio"/> Text <input type="radio"/> Code
Maintenance Code:	

Figure 2: HTTPS health monitor configuration

6. Click **OK**, then click **Save** to save the configuration.

7.2 SOURCE NAT CONFIGURATION

This section configures the IP address pool to be used for IP Source Network Address Translation (SNAT). When incoming traffic from a client accesses the VIP address (for example: 10.0.0.200), the client requests are “source NAT-ed”, which means that the AX device replaces the client’s source IP address with a SNAT address. SNAT is required when your network topology is based on “one-arm” deployment and if you have internal clients that reside on the same subnet as the VIP.

To configure SNAT, use this section to configure the address pool. Then, later in this document, a procedure shows how to apply the pool to the VIP.

1. Navigate to **Config Mode > Service > IP Source NAT > IPv4 Pool**.
2. Click **Add**.

- Enter the following:
 - Name:** "UAGSNAT"
 - Start IP Address:** "203.0.113.222"
 - End IP Address:** "203.0.113.222"
 - Netmask:** "255.255.255.0"

IPv4 Pool	
Name: *	<input type="text" value="UAGSNAT"/>
Start IP Address: *	<input type="text" value="203.0.113.222"/>
End IP Address: *	<input type="text" value="230.0.113.222"/>
Netmask: *	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text"/>
HA Group:	<input type="text"/>

Figure 3: Source NAT pool configuration

- Click **OK**, then click **Save** to save the configuration.

Note: When you are in the Virtual Service configuration section, you can apply the SNAT pool to the VIP.

Note: When using the AX device in a High Availability (HA) configuration, an HA Group must be selected. This will prevent duplicate IP addresses from occurring in the SNAT Pool.

7.3 SOURCE IP PERSISTENCE

The Source IP Persistence feature enables an HTTP/S request to be directed to the following destinations: Port, Server or Service Group. In this deployment, we will configure each request to land on the same server.

To configure Source IP Persistence:

- Navigate to **Config Mode > Service > Template > Persistence > Source IP Persistence**.
- Click **Add**.
- Enter the following:
 - Name:** "SourceIP"
 - Match Type:** Select "Server" from the drop-down list.

Source IP Persistence	
Name: *	SourceIP
Match Type:	Server <input type="checkbox"/> Scan All Members
Timeout:	5 Minutes
Don't Honor Conn Rules:	<input type="checkbox"/>
Netmask:	255.255.255.255

Figure 4: Source IP persistence

- Click **OK**, then click **Save** to save the configuration.

7.4 SSL CERTIFICATE

To encrypt and decrypt web traffic from external UAG users, an SSL certificate is required to secure connections between the AX Series and the external clients. This section of the deployment guide provides instructions for either importing a certificate signed by a Certificate Authority (CA), or generating a self-signed certificate.

Since the AX device will act as an HTTPS proxy for the UAG server, the server certificate for each server must be imported onto or generated by the AX device.

There are two options for installing an SSL certificate on the AX Series:

- **Option 1:** Generate a self-signed certificate on the AX device.
- **Option 2:** Import an SSL certificate and key signed by a Certificate Authority (CA).

7.4.1 OPTION 1: GENERATE A SELF-SIGNED CERTIFICATE

- Navigate to **Config Mode > Service > SSL Management > Certificate**.
- Click **Create**.
- Enter the **File Name** of the certificate, "UAGSSL".
- From the **Issuer** drop-down list, select "Self".
- Enter the following values:
 - ◆ **Common Name:** "example.com"
 - ◆ **Division:** "example.com"
 - ◆ **Organization:** "example.com"

- ◆ **Locality:** "sanjose"
- ◆ **State or Province:** "CA"
- ◆ **Country:** "United States of America"
- ◆ **Email Address:** "admin@example.com"
- ◆ **Valid Days:** "730" (Default)
- ◆ **Key Size (Bits):** "2048"

General	
File Name: *	UAGSSL
Certificate	
Issuer:	Self
Common Name: *	example.com
Division:	example.com
Organization:	example.com
Locality:	sanjose
State or Province:	CA
Country (C): *	United States of America US
Email Address:	admin@example.com
Valid Days:	730 days
Key	
Key Size:	2048 Bits

Figure 5: Self-signed certificate configuration

6. Click **OK**, then click **Save** to save the configuration.

7.4.2 OPTION 2: IMPORT THE CERTIFICATE AND KEY

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Import**.
3. Enter the **Name**, "UAGCERT".
4. Select "Local" or "Remote", depending on the file location.
5. Enter the certificate **Password** (if applicable).

6. Enter or select file location and access settings.
7. Click **OK**.

Note: If you are importing a CA-signed certificate for which you used the AX device to generate the CSR, you do not need to import the key. The key is automatically generated on the AX device when you generate the CSR.

Import	
Name:*	UAGCERT
Import Certificate from:	<input checked="" type="radio"/> Local <input type="radio"/> Remote <input type="radio"/> Text
Certificate Format:	PFX
Password:	•••
Certificate Source:	C:\UAGCERT.pfx <input type="button" value="Browse..."/>

Figure 6: SSL certificate import

8. Click **OK**, then click **Save** to save the configuration.

7.4.3 CONFIGURE AND APPLY CLIENT-SSL TEMPLATE

This section describes how to configure a client-SSL template and apply it to the VIP.

1. Navigate to **Config Mode > Service > Template > SSL > Client SSL**.
2. Click **Add**.
3. Enter or select the following values:
 - ◆ **Name:** "Client SSL"
 - ◆ **Certificate Name:** " UAGSSL"
 - ◆ **Key Name:** "UAGSSL"
 - ◆ **Pass Phrase:** "a10"
 - ◆ **Confirm Pass Phrase:** "a10"

Client SSL	
Name: *	Client SSL
Certificate Name:	UAGSSL
Chain Cert Name:	
Key Name:	UAGSSL
Pass Phrase:	...
Confirm Pass Phrase:	...
Cache Size:	0
SSL False Start:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Figure 7: Client-SSL template

Note: The template that was created above will be used to implement SSL Offload by binding the Client SSL template to a HTTP VIP (port 443).

8 SECURE ACCESS LAYER

This section explains how the AX appliance is configured to be a load balanced Microsoft Unified Access Gateway with the HTTPS VIP type. This section contains detailed instructions on how to configure the servers, add them to a service group, and bind them to the HTTPS virtual port on the VIP.

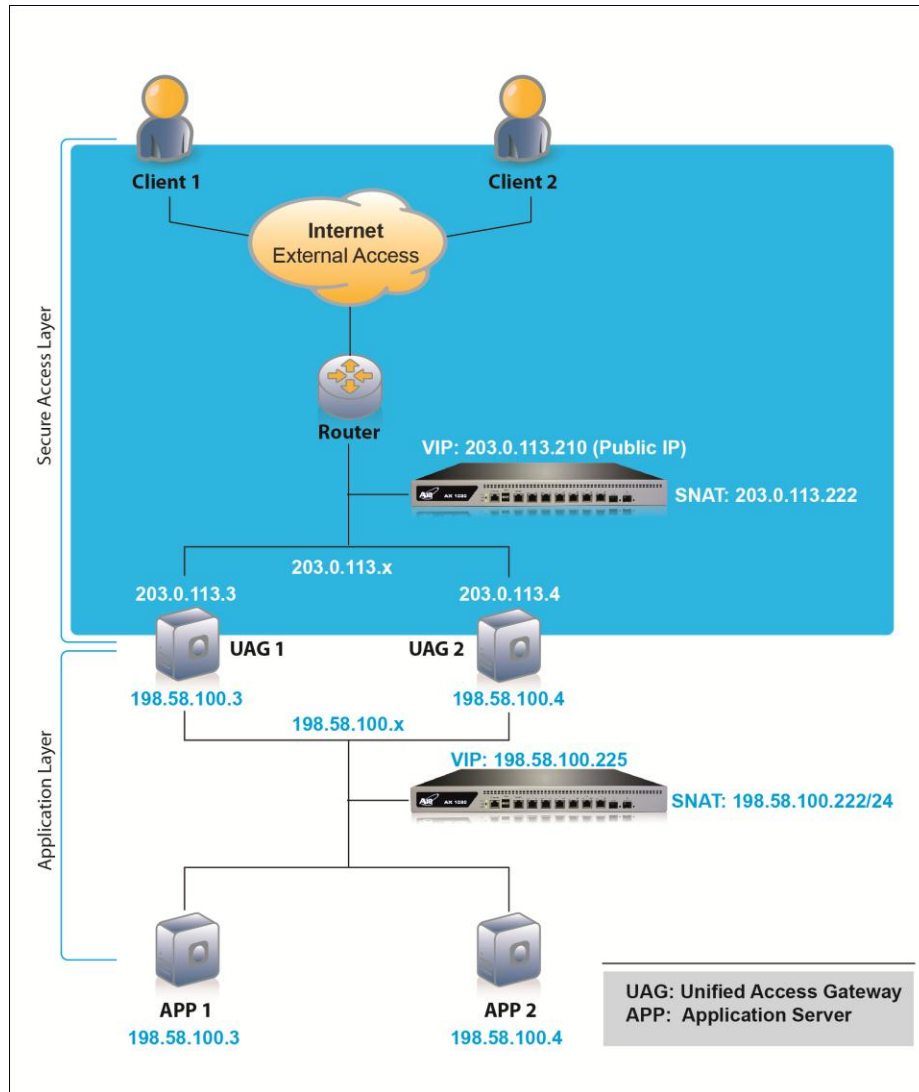


Figure 8: Secure access layer

Note: The Virtual Server is also known as the "Virtual IP" ("VIP") that a client accesses during an initial request.

8.1 SERVER CONFIGURATION

This section demonstrates how to configure the Microsoft UAG servers on the AX Series.

1. Navigate to **Config Mode > Service > SLB > Server**.
2. Click **Add** to add a new server.
3. Within the Server section, enter the following required information:
 - ◆ **Name:** "UAG1"
 - ◆ **IP Address/Host:** "203.0.113.3"

Note: Enter additional servers if necessary.

General	
Name: *	<input type="text" value="UAG1"/>
IP Address/Host: *	<input type="text" value="203.0.113.3"/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	<input type="text"/>
Weight:	<input type="text" value="1"/>
Health Monitor:	(default) ▼
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	<input type="text" value="8000000"/> <input checked="" type="checkbox"/> Logging
Connection Resume:	<input type="text"/>
Slow Start:	<input type="checkbox"/>
Spoofing Cache:	<input type="checkbox"/>
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server Template:	default ▼
Description:	<input type="text"/>

Figure 9: Server configuration

4. To add a port to the server configuration:
 - a. Enter the port number (443) in the **Port** field.
 - b. Select the **Protocol**, "TCP".
 - c. Click **Add**.

Port configuration window showing the following settings:

- Port: 80
- Protocol: TCP
- Weight(W): 1
- No SSL:
- Connection Limit(CL): 8000000
- Logging:
- Connection Resume(CR):
- Server Port Template(SPT): default
- Stats Data(SD): Enabled Disabled
- Health Monitor(HM): (default)
- Follow Port: TCP
- Extended Stats(ES): Enabled Disabled

<input type="checkbox"/>	Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD	ES
<input checked="" type="checkbox"/>	80	TCP	8000000	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	default	(default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 10: Server port configuration

5. Follow the same steps in this section for server “UAG2”.
6. Click **OK**, then click **Save** to save the configuration.

8.2 SERVICE GROUP CONFIGURATION

This section contains the basic configuration for a service group.

1. Navigate to **Config Mode > Service > SLB > Service Group**.
2. Click **Add**.
3. Enter or select the following values:
 - ◆ **Name:** “UAGSG80”
 - ◆ **Type:** “TCP”
 - ◆ **Algorithm:** “Round Robin”
 - ◆ **Health Monitor:** “UAGHC”
4. In the Server section, select a server from the **Server** drop-down list and enter “443” in the **Port** field.
5. Click **Add**. Repeat for each server.

Service Group	
Name: *	UAGSG80
Type:	TCP
Algorithm:	Round Robin
Health Monitor:	UAGHC
Min Active Members:	<input type="checkbox"/>
<input type="checkbox"/>	Send client reset when server selection fails
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Description:	<input type="text"/>

Figure 11: Service group configuration

Server						
IPv4/IPv6:		<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6				
Server: *	UAG2	Port: *	80			
Server Port Template(SPT):	default	Priority:	1			
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled					
<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data	
<input type="checkbox"/>	UAG1	80	default	1	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	UAG2	80	default	1	<input checked="" type="checkbox"/>	

Figure 12: Server configuration

6. Click **OK**, then click **Save** to save the configuration.

8.3 VIRTUAL SERVER CONFIGURATION

This section contains the basic configuration for a Virtual Server. As previously mentioned, the Virtual Server is also known as the “Virtual IP” (“VIP”) that a client accesses during an initial request.

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. In the General section, enter the name of the VIP and its IP address:

- ◆ **Name:** "UAGVIP"
- ◆ **IP Address:** "203.0.113.210"

General	
Name: *	<input type="text" value="UAGVIP"/> <input type="checkbox"/> Wildcard
IP Address or CIDR Subnet: *	<input type="text" value="203.0.113.210"/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ARP Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
When-All-Ports-Down:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Redistribution Flagged:	<input type="checkbox"/>
HA Group:	<input type="text"/>
Virtual Server Template:	<input type="text" value="default"/>
PBSLB Policy Template:	<input type="text"/>
Description:	<input type="text"/>

Figure 13: Virtual server configuration

3. In the Port section, click **Add**.

Note: On the Virtual Service page of the GUI, the Virtual Service will be pre-populated with a name (example: `_203.0.113.210_TCP_443`).

4. Enter or select the following values:

- ◆ **Type:** "TCP"
- ◆ **Port:** "443"
- ◆ **Service Group:** Select "UAGSG80" from the drop-down menu.
- ◆ **Source NAT Pool:** Select "UAGSNAT" from the drop-down menu.
- ◆ **Client-SSL Template:** Select "Client SSL" from the drop-down menu.

Note: Selecting this template enables the SSL Offload feature within the AX Series.

- ◆ **Persistence Template Type:** Select "Source IP Persistence Template".
- ◆ **Source IP Persistence Template:** Select the "SourceIP" template.

Virtual Server Port	
Virtual Server:	UAGVIP
Type: *	HTTPS
Port: *	443
Service Group:	UAGSG80
Connection Limit:	<input type="checkbox"/> 8000000 <input checked="" type="radio"/> Drop <input type="radio"/> Reset <input checked="" type="checkbox"/> Logging
<input checked="" type="checkbox"/>	Use default server selection when preferred method fails
<input type="checkbox"/>	Use received hop for response
<input type="checkbox"/>	Send client reset when server selection fails
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SYN Cookie:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Source NAT traffic against VIP:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	UAGSNAT
aFlx:	<input type="checkbox"/> Multiple
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	Client SSL
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	
Persistence Template Type:	Source IP Persistence Template
Source IP Persistence Template:	SourceIP
PBSLB Policy Template:	

Figure 14: Virtual-server port configuration

5. Click **OK**, then click **Save** to save the configuration.

9 ADVANCED ACCESS CONFIGURATION

This section contains the advanced configuration of the AX Series with Unified Access Gateway. The advanced Layer 7 optimizations can enhance the user experience, by increasing server performance with features such as HTTP Connection Reuse, cookie persistence, and protection against distributed denial-of-service (DDoS) attacks.

The first step in the advanced configuration is to predefine all the optimization and performance features in configuration templates. Once all the performance features are defined in the templates, you can bind the features to the “UAGIP” VIP.

9.1 COOKIE PERSISTENCE

To enable cookie persistence, the template must be created first, as follows:

1. Navigate to **Config Mode > Service > Template > Cookie Persistence**.
2. Click **Add** to add a new cookie persistence template.
3. Enter the **Name**, "UAG_COOKIE".
4. Check the **Expiration** radio button and enter "86400" in the **Seconds** field.

Cookie Persistence	
Name: *	UAG_COOKIE
Expiration:	<input checked="" type="checkbox"/> 86400 Seconds
Cookie Name:	
Domain:	
Path:	
Match Type:	<input type="checkbox"/> Service Group <input type="checkbox"/> Port
Insert Always:	<input type="checkbox"/>
Don't Honor Conn Rules:	<input type="checkbox"/>

Figure 15: Cookie persistence template

5. Click **OK**, then click **Save** to save the configuration.

9.2 TCP CONNECTION REUSE

1. Navigate to **Config Mode > Service > Template > Connection Reuse**.
2. Click **Add**.
3. Enter **Name**: "UAG_CR".

Connection Reuse	
Name: *	UAG_CR
Limit Per Server:	1000
Timeout:	2400 Seconds
Keep Alive Connections:	<input type="checkbox"/>

Figure 16: TCP Connection Reuse template

4. Click **OK**, then click **Save** to save the configuration.

9.3 APPLY OPTIMIZATION AND ACCELERATION FEATURE TEMPLATES TO VIP

After configuring the optimization and acceleration features, you must bind them to the virtual port on the VIP to place them into effect.

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. Click on the virtual service name.
3. Apply the features by selecting the templates from the applicable drop-down lists.

Connection Reuse Template:	UAG_CR
TCP-Proxy Template:	
Persistence Template Type:	Cookie Persistence Template
Cookie Persistence Template:	UAG_COOKIE

Figure 17: Applying features

4. Click **OK**, then click **Save** to save the configuration.

Note: In the Basic Access Configuration, source IP persistence was bound to the VIP. So to apply cookie persistence, you must remove the source IP persistence first within the Virtual Service before you can apply the cookie persistence template.

9.4 ENABLE DDOS PROTECTION

The AX Series offers additional security features against DDoS attacks. The DDoS protection options within the AX Series provide an additional layer of protection from unwanted attacks. To enable DDoS protection within the AX series:

1. Navigate to **Config Mode > Service > SLB > Global > DDoS protection**.
2. Check **Drop All**.
3. Click **OK**, then click **Save** to save the configuration.

DDoS Protection	
<input checked="" type="checkbox"/> Drop All	<input type="checkbox"/> IP Option <input type="checkbox"/> Land Attack <input type="checkbox"/> Ping-of-Death <input type="checkbox"/> Frag <input type="checkbox"/> TCP No Flags <input type="checkbox"/> TCP SYN Fin <input type="checkbox"/> TCP SYN Frag
Out of Sequence:	10
Zero Window:	10
Bad Content:	10

Figure 18: DDoS protection

Note: Checking "Drop All" means that all DDoS attacks with IP Option, Land Attack, Ping-of-Death, Frag, TCP No Flags, TCP SYN Fin or TCP Syn Frag will be dropped when a request is sent to the AX device. For more information about the DDoS attacks, see the AX Series System Configuration and Administration Guide.

10 APPLICATION LAYER LOAD BALANCING

This section of the deployment guide is where the application load balancing occurs. The AX Series can accept any incoming traffic regardless of the protocol and the AX Series can load balance the traffic across a pool of application servers.

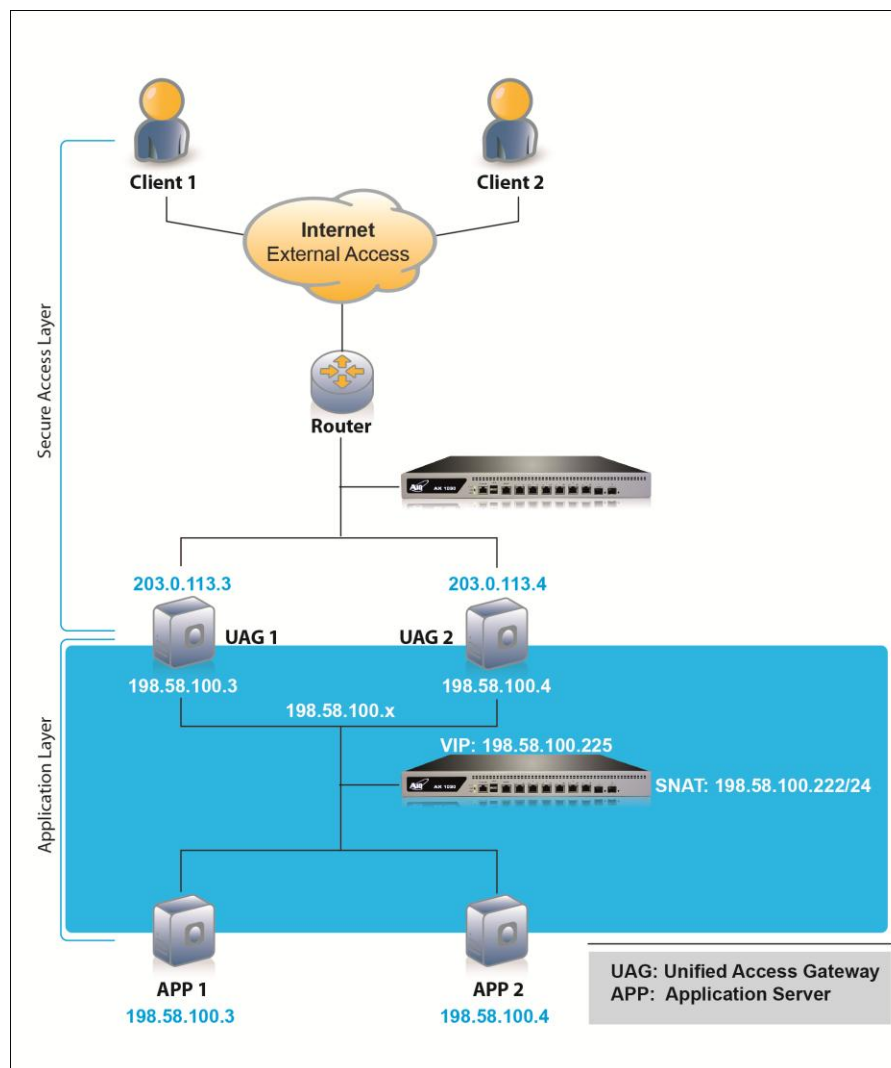


Figure 19: Application layer load balancing

A10 Networks has an extensive selection of deployment guides for enterprise and corporate applications. The deployment guides can be downloaded at:

http://www.a10networks.com/resources/deployment_guides.php

11 SUMMARY AND CONCLUSION

The sections above show how to deploy the AX device for optimization of the Microsoft Unified Access Gateway solution. By using the AX device to load balance a pool of UAG servers, the following key advantages are achieved:

- High-availability for UAG servers to prevent downtime and access failure, with no adverse impact on user access to applications
- Seamless distribution of client traffic across multiple UAG servers for site scalability
- Higher connection counts, faster end-user responsiveness, and reduced UAG application CPU utilization by initiating SSL Offload and Connection Reuse
- Improved site performance and availability to end users

By using the AX Series Advanced Traffic Manager, significant benefits are achieved for all UAG access users. For more information about AX Series products, please refer to the following URLs:

<http://www.a10networks.com/products/axseries.php>

<http://www.a10networks.com/resources/solutionsheets.php>

<http://www.a10networks.com/resources/casestudies.php>

A. CLI CONFIGURATION FOR SECURE ACCESS LAYER

```
UAGLB#show running-config
ip nat pool UAGSNAT 192.168.10.199 192.168.10.199 netmask /24
health monitor UAGHC
  method https
slb server UAG1 203.0.113.3
  port 80 tcp
slb server UAG2 203.0.113.4
  port 80 tcp
```



```
slb service-group UAGSG80 tcp
    health-check UAGHC
    member UAG1:80
    member UAG2:80
slb template connection-reuse UAG_CR
slb template client-ssl "Client SSL"
    cert UAGSSL
    key UAGSSL pass-phrase encrypted
37048xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb template persist cookie UAG_COOKIE
    expire 86400
slb template persist source-ip SourceIP
    netmask6 0
    match-type server
slb virtual-server UAGVIP 203.0.113.210
    port 443 https
    name _203.0.113.210_HTTPS_443
    source-nat pool UAGSNAT
    service-group UAGSG80
    template client-ssl "Client SSL"
    template connection-reuse UAG_CR
    template persist cookie UAG_COOKIE
end
UAGLB#
```