Deployment Guide

AX Series with Active Directory Federation Services 2.0 and Office 365

TABLE OF CONTENTS

1 OVERVIEW

Active Directory Federation Services (ADFS) allows the sharing of identity authentication between two trusted partners beyond the boundary of an Active Directory (AD) forest. This feature is available within Windows Servers and provides users with Single Sign-On access to systems and applications across organizational boundaries. ADFS is becoming very popular due to the dramatic shift of enterprise customers towards cloud based services such as Microsoft Office 365.

ADFS enables use of existing AD credentials to access Office 365 or other trusted networks through AD federation. The benefit to users is a single access credential for access to applications. The single access credential works as long as the trust between the AD forests remains established.

2 DEPLOYMENT GUIDE OVERVIEW

This guide describes how to deploy the AX Series Application Delivery Controller (ADC)/Server Load Balancer in ADFS farms. This guide provides sections for the following deployment scenarios: Internal ADFS, and Internal/External ADFS.

3 DEPLOYMENT GUIDE PREREQUISITES

This deployment guide has the following prerequisites.

AX Series Requirements:

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

Tested Microsoft ADFS Server:

- 2.66 Ghz or faster Quad-Core processor CPU
- 4 GB Memory
- 2 Processors
- 100 MB of disk space

Test ADFS Software:

- Windows Server 2008 R2 Operating System with ADFS 2.0 installed.

Note: *For additional informational as to which Windows Servers 2008 and Windows Server 2008 R2* versions *are supported, navigate to Availability and description of Active Directory Federation Services 2.0.*

Before installing ADFS 2.0, make sure that the prerequisite applications and hotfixes are installed. The ADFS wizard attempts to automatically check. For more details, read the Install the ADFS 2.0 Software section in the ADFS 2.0 Deployment Guide.

ADFS Certificates:

- ADFS will be required in order to secure communication between federations' servers, federation server proxies (FSP/External Access), claims-aware applications and web clients. The requirements for the ADFS deployment will vary depending on whether the setup is designed for federation servers or federation server proxies. The certificate must come from a Trusted Root Authority Certificate provider.

Note: *If your ADFS deployment is geared to use multiple domain names, it is recommended to (delete bold) purchase an ADFS certificate that can support Subject Alternative Names (SANs). ADFS certificates are available from third-party SSL providers.*

For additional ADFS requirements, refer to the ADFS 2.0 Design Guide.

Note: *It is strongly recommended to configure the trust relationships across federation servers, services, and applications before you begin the procedures in this guide.*

4 ACCESSING THE AX SERIES APPLICATION 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 covers two layers of traffic load balancing; namely: Internal ADFS load balancing and Internal/External ADFS load balancing. Below is a sample topology. Some components may be consolidated.

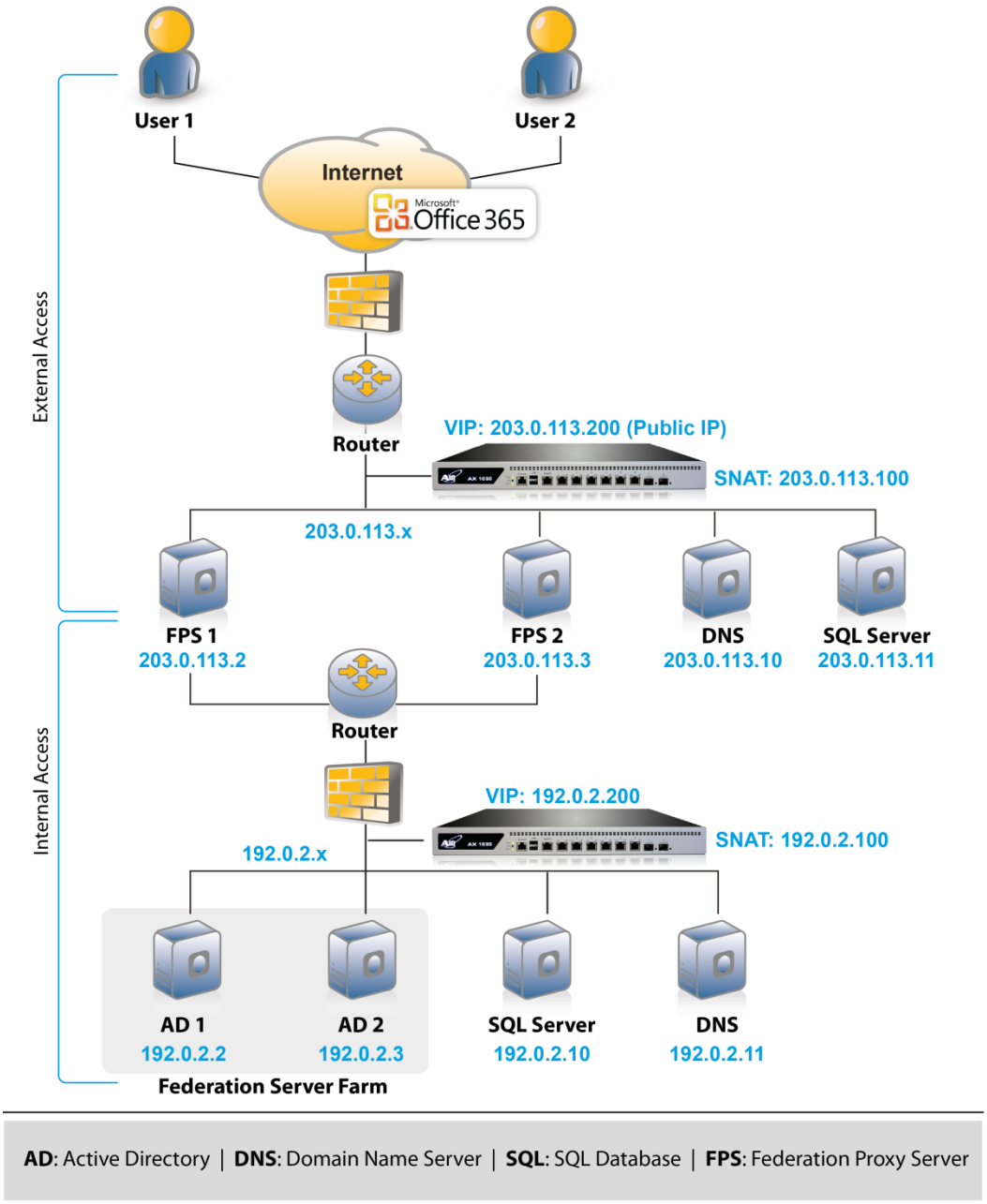

Figure 1: ADFS and FPS deployment overview

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 can support, please visit the following URL:*

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

6 AX SERIES 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 templates:

- Health Monitor: Sends on-demand health checks to configured servers 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.
- SSL Certificate: An SSL certificate is required to provide secure connection to the pool of ADFS servers.

Note: *This certificate is different from the ADFS certificate requirement for Active Directory Federation.*

- Cookie Persistence: Enables a user to direct multiple requests to the same ADFS server based on Cookie Persistence.

Note: *These templates must be configured on the AX appliances located in both the Internal ADFS and External/Internal ADFS segments.*

6.1 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 “ADFSHC”.
4. Select **Method** “HTTPS”.

5. Click **OK**, and then see the next section to continue with the Service Group configuration.

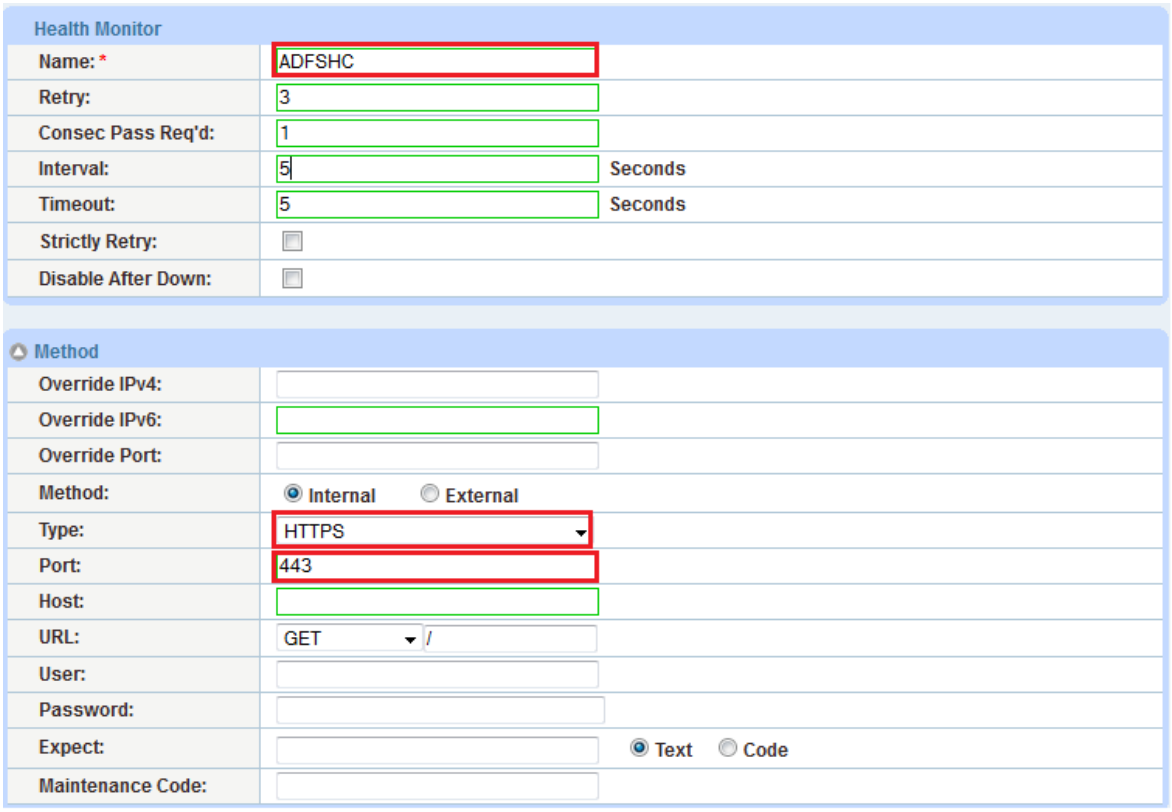

Figure 2: HTTPS health monitor configuration

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

6.2 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**.

3. Enter the following:
   - **Name:** “ADFSSNAT”
   - **Start IP Address:** 192.0.2.100
   - **End IP Address:** 192.0.2.100
   - **Netmask:** 255.255.255.0

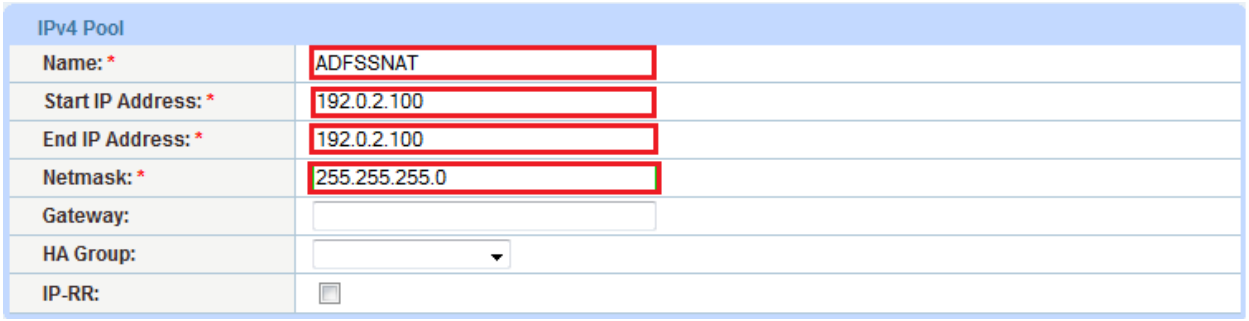

Figure 3: Source NAT pool configuration

4. 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.*

6.3 COOKIE PERSISTENCE CONFIGURATION

Cookie Persistence offers various granularities of persistence such as Port, Server or Service Group. In this deployment, persistence is configured to send each request to the same server. The AX device inserts a cookie into the header of the server reply to the client, to ensure that subsequent requests are sent to the same ADFS server.

To configure Source IP Persistence:

1. Navigate to **Config Mode > Service > Template > Persistence > Cookie Persistence**.
2. Click **Add**.
3. Enter the following:
   - **Name**: “adfscookie”.

- **Expiration:** Select the Expiration checkbox and enter "86400".
- **Cookie Name:** "adfscookie".
- **Domain: “**example.com”.
- **Match Type:** Select “Server” from the drop-down list.
- **Insert Always:** Select the checkbox.

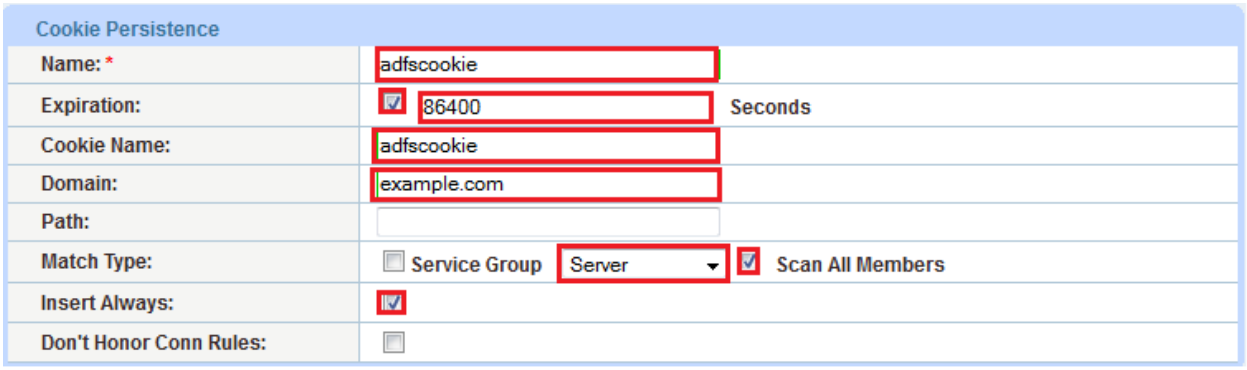

Figure 4: Source-IP persistence

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

6.4 SSL CONFIGURATION

To encrypt and decrypt web traffic from external ADFS users, an SSL certificate is required to secure connections between the AX Series and 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 ADFS 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).

6.4.1 OPTION 1: GENERATE A SELF-SIGNED CERTIFICATE

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.

2. Click **Create**.
3. Enter the **File Name** of the certificate, “ADFSSSL”.
4. From the **Issuer** drop-down list, select “Self”.
5. 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”

Note: *The AX Series can support 512-bit, 1028-bit, 2048-bit, and 4096-bit keys. The higher the bit size, the more CPU processing that will be required on the AX device.*

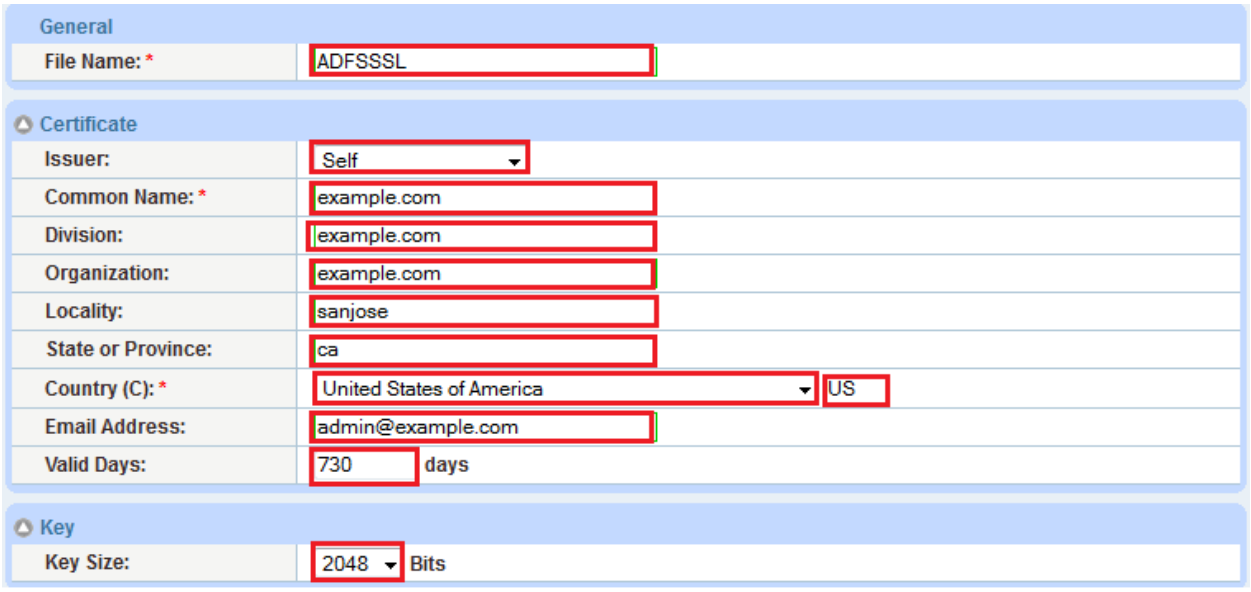

Figure 5: Self-signed certificate configuration

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

6.4.2 OPTION 2: IMPORT THE CERTIFICATE AND KEY

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

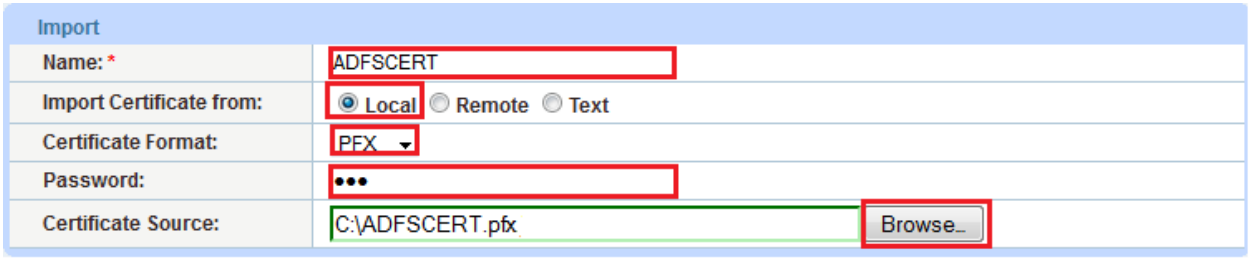

Figure 6: SSL certificate import

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

6.4.3 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:** " ADFSSSL”

- **Key Name:** “ADFSSSL”
- **Pass Phrase:** “a10”
- **Confirm Pass Phrase:** “a10”

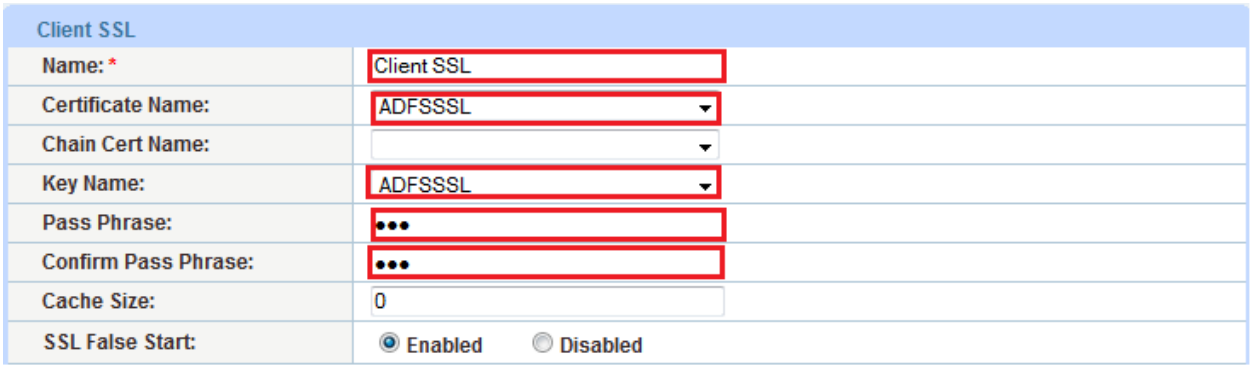

Figure 7: Client-SSL template

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).*

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

7 INTERNAL ADFS DEPLOYMENT

This section demonstrates how to configure Microsoft Internal ADFS load balancing on the AX Series.

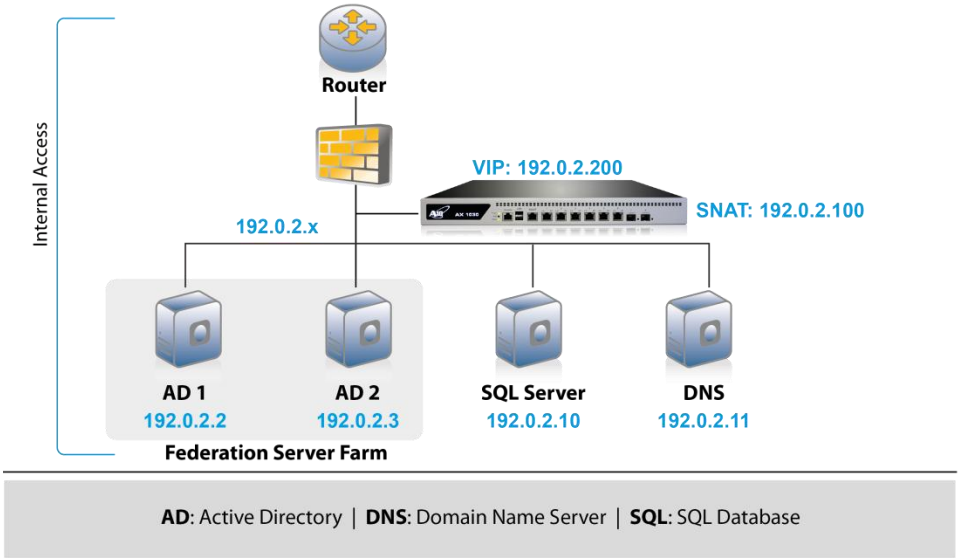

Figure 8: ADFS internal architecture

7.1 SERVER CONFIGURATION

This section describes how to create configurations for the ADFS servers.

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:** "AD1"
   - **IP Address/Host:** "192.0.2.2"

Note: *Enter additional servers if necessary.*

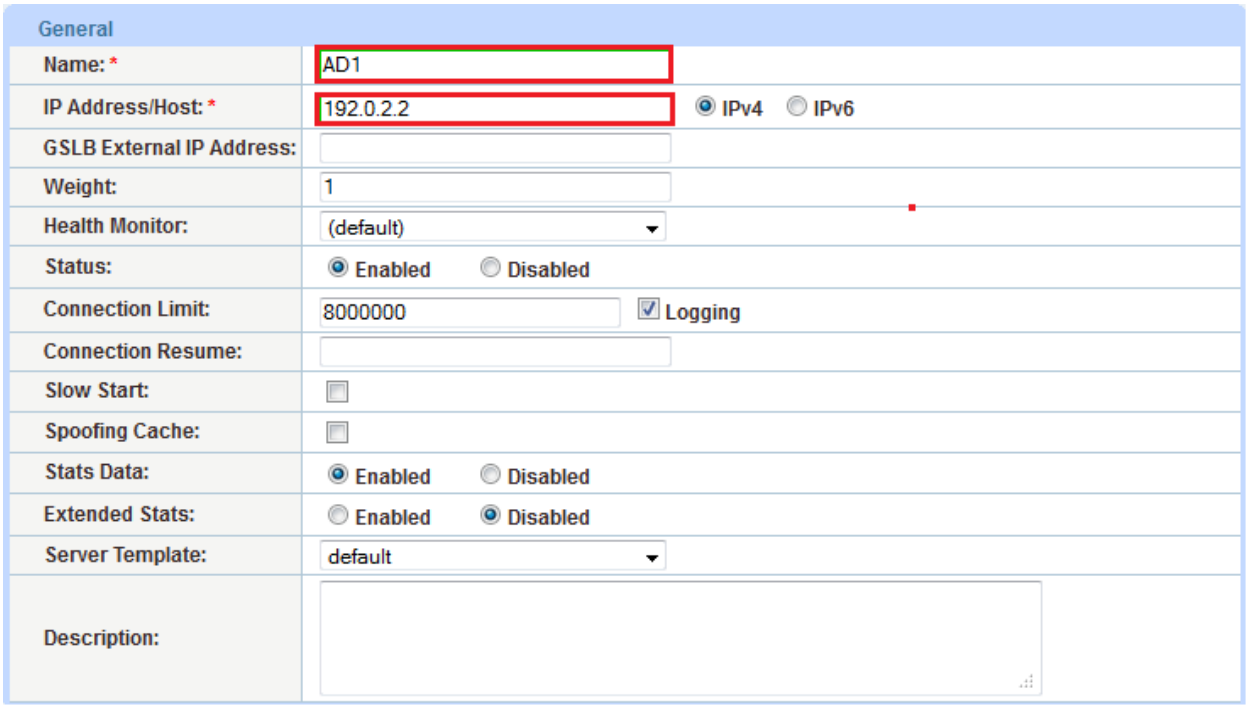

Figure 9: Active Directory Federation Server configuration

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**.

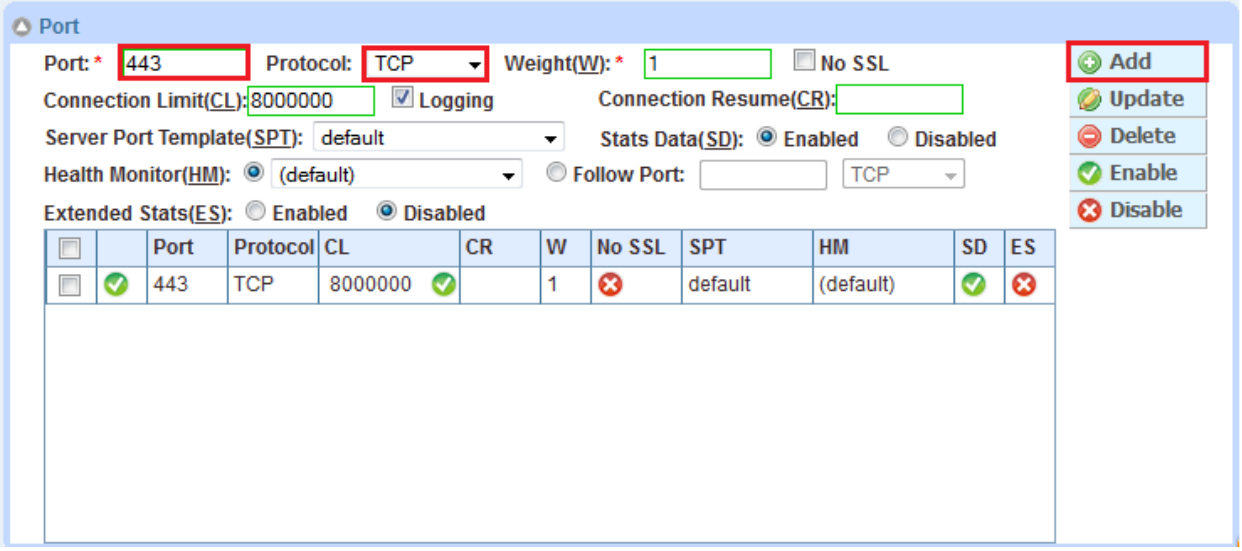

Figure 10: Port configuration

d. Follow the same steps for server “AD2”.

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

7.2 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:** “ADFS443”
   - **Type:** “TCP”
   - **Algorithm:** “Round Robin”
   - **Health Monitor:** “ADFSHC”
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.

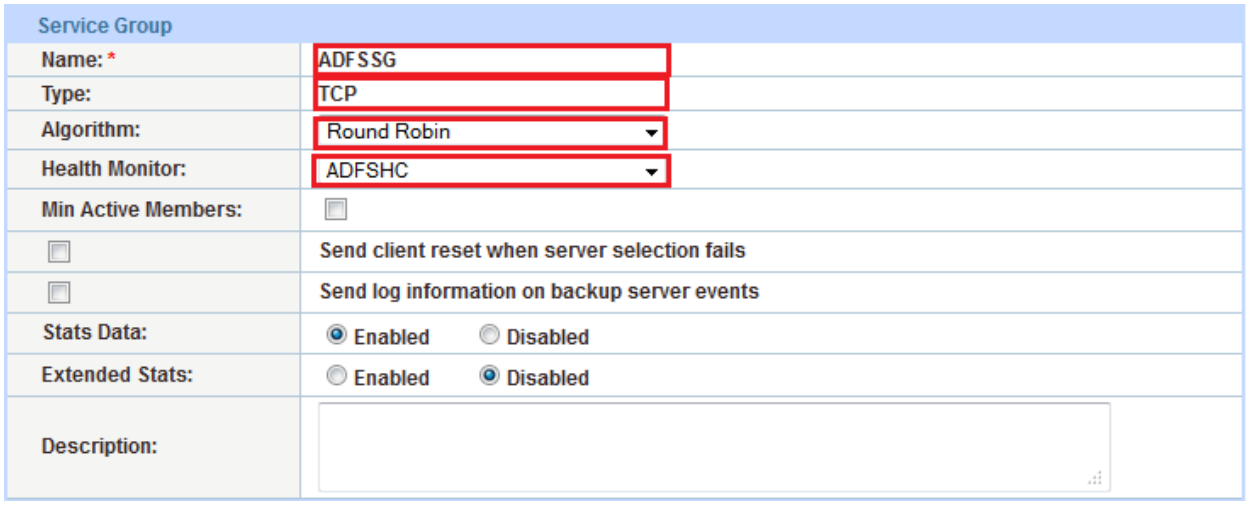

Figure 11: Service-group configuration

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

8 VIRTUAL SERVER CONFIGURATION

This section contains the basic configuration for a Virtual Server. The Virtual Server also is 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:** "ADFSVIP-INTERNAL"
   - **IP Address:** 192.0.2.200

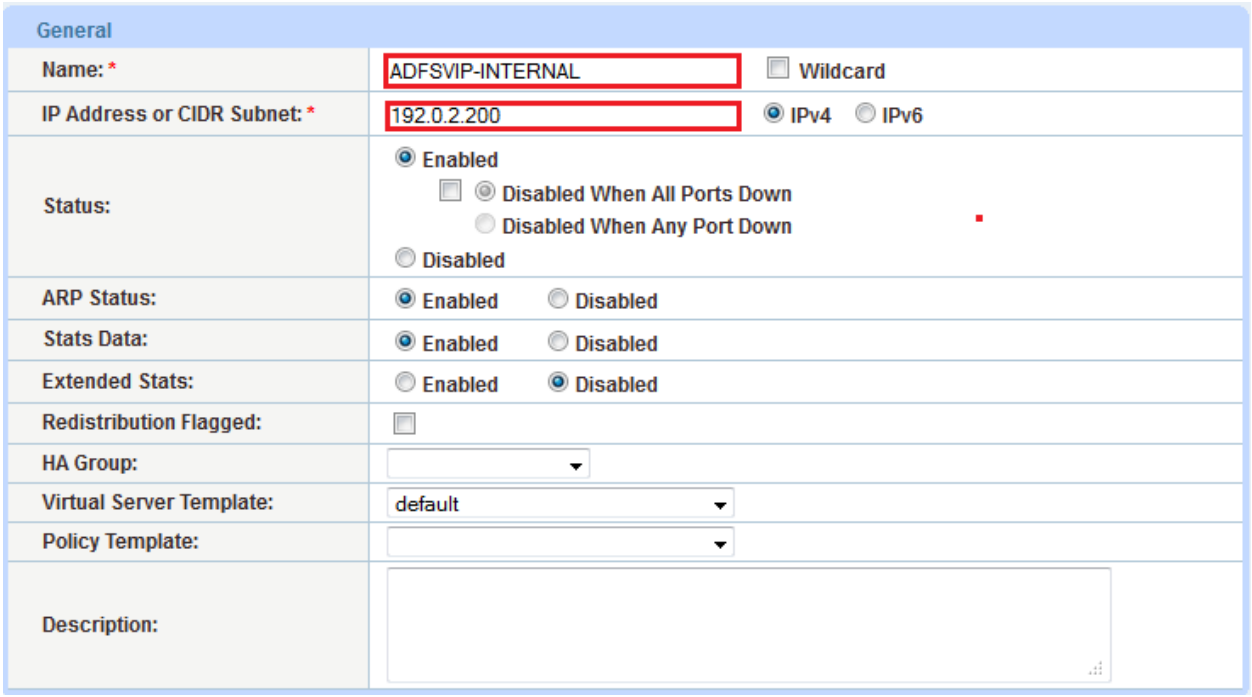

Figure 12: VIP configuration

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:_192.0.2.200_TCP_443).*

4. Enter or select the following values:

- **Type:** "TCP"
- **Port:** "443"
- **Service Group:** Select "**ADFSSG"** from the drop-down menu.
- **Source NAT Pool:** Select "ADFSSNAT" 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 "Cookie Persistence Template".
- **Cookie Persistence Template:** Select the "adfscookie" template.

9 FEDERATION PROXY SERVER DEPLOYMENT

This section of the deployment guide focuses on the external ADFS configuration, also known as Federation Proxy Server (FPS). The FPS is a Windows Server 2008 server that acts as an intermediary proxy server between an external client on the Internet and a Federation Server that is located behind a firewall on an internal network. For Microsoft Office 365 to work, the Federation Server Proxy is required for the applications to work.

Note: *The FPS is used to redirect client authentication from external users to the Federation Server pool or VIP. The FPS is a required component of Office 365 if you want your users to be able to roam among work computers, use home or public computers to log in to a domain, use smart phone access to Office 365 applications such as Microsoft Exchange Online, or use Microsoft Outlook or other email clients for IMAP or POP access.*

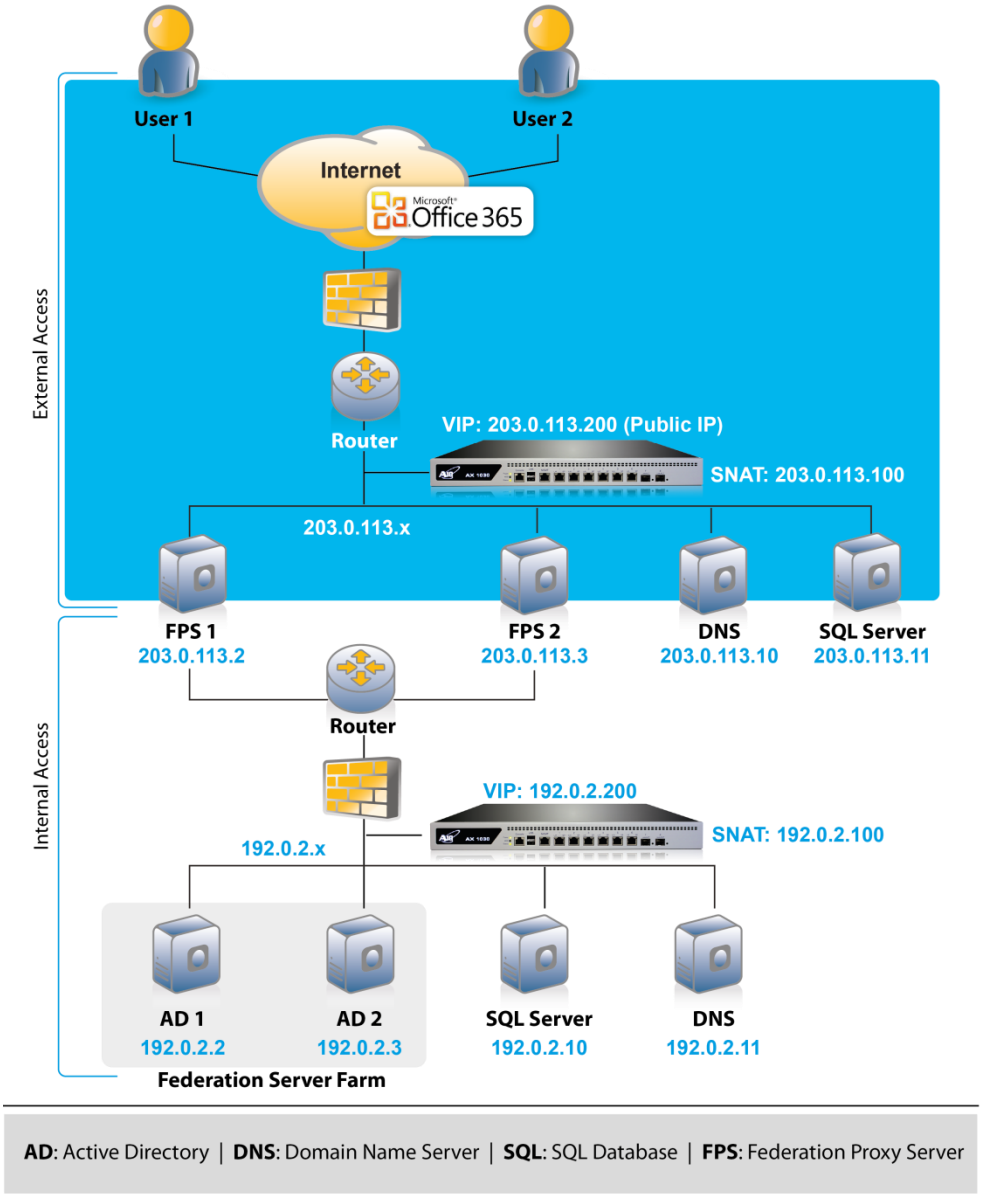

Figure 13: Federation Proxy Server overview

9.1 FPS SERVER CONFIGURATION

This section of the deployment guide describes how to provision the FPS within the External 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:** “FPS1”
   - **IP Address/Host:** 203.0.113.2

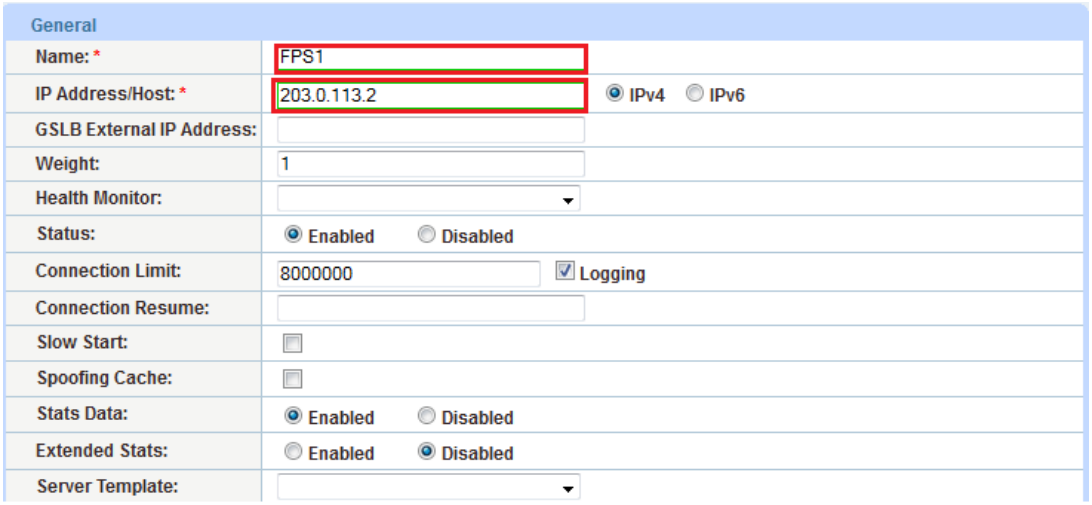

Figure 14: FPS AX Series configuration

Note: *Enter additional servers if necessary.*

4. To add a port to the server configuration:
5. Enter the port number (443) in the **Port** field.
6. Select the **Protocol**, “TCP”.
7. Click **Add**.

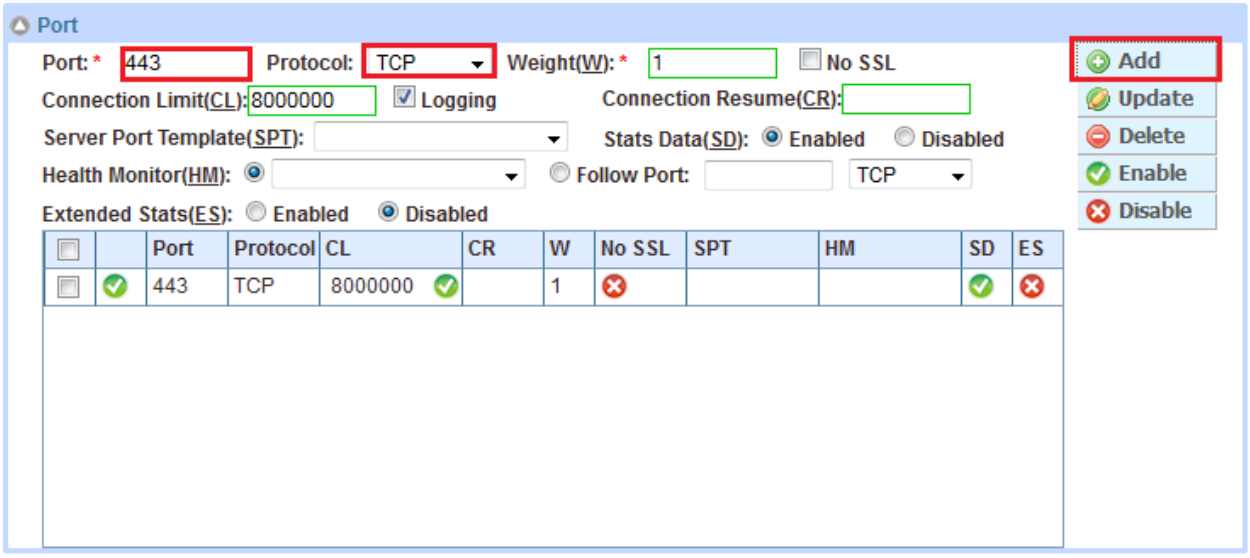

Figure 15: Port configuration

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

9.2 FPS SERVER GROUP CONFIGURATION

This section of the deployment guide explains how the FPS can be configured in a Server Group within the AX Series.

1. Navigate to **Config Mode > Service > SLB > Service Group**.
2. Click **Add**.
3. Enter or select the following values:
   - **Name:** “FPSSG”
   - **Type:** “TCP”
   - **Algorithm:** “Round Robin”

- **Health Monitor:** "FPSHC"

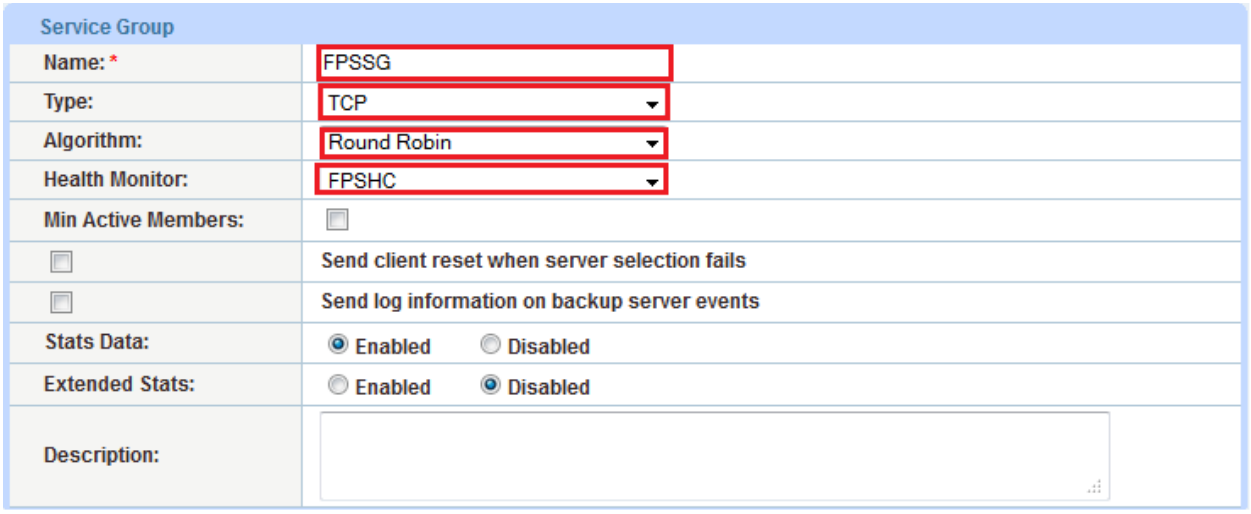

Figure 16: FPS health check

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.

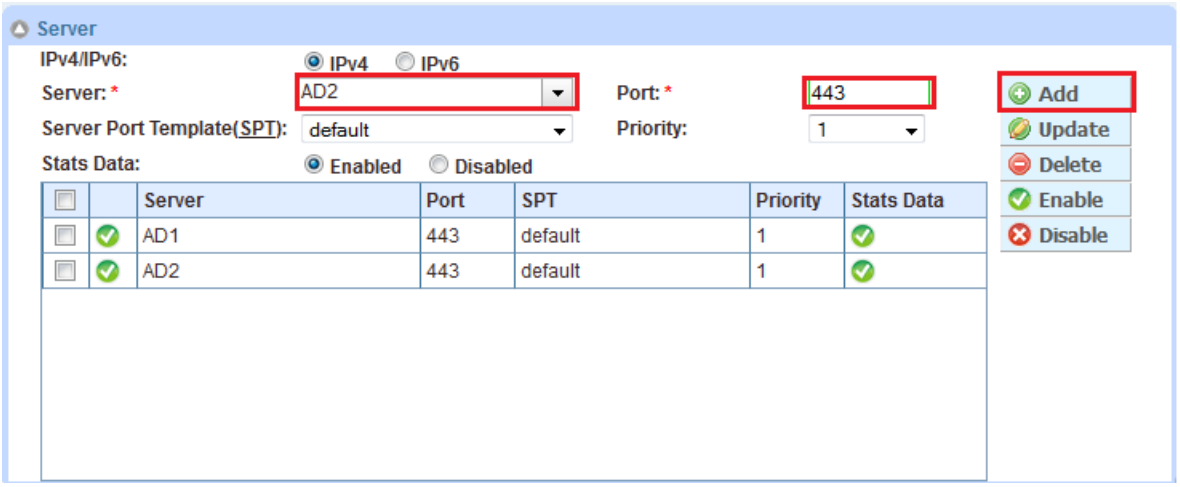

Figure 17: Service-group configuration

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

9.3 FPS VIRTUAL SERVER CONFIGURATION

This section of the deployment guide is where the external Federation Proxy Server VIP (Virtual IP) is configured.

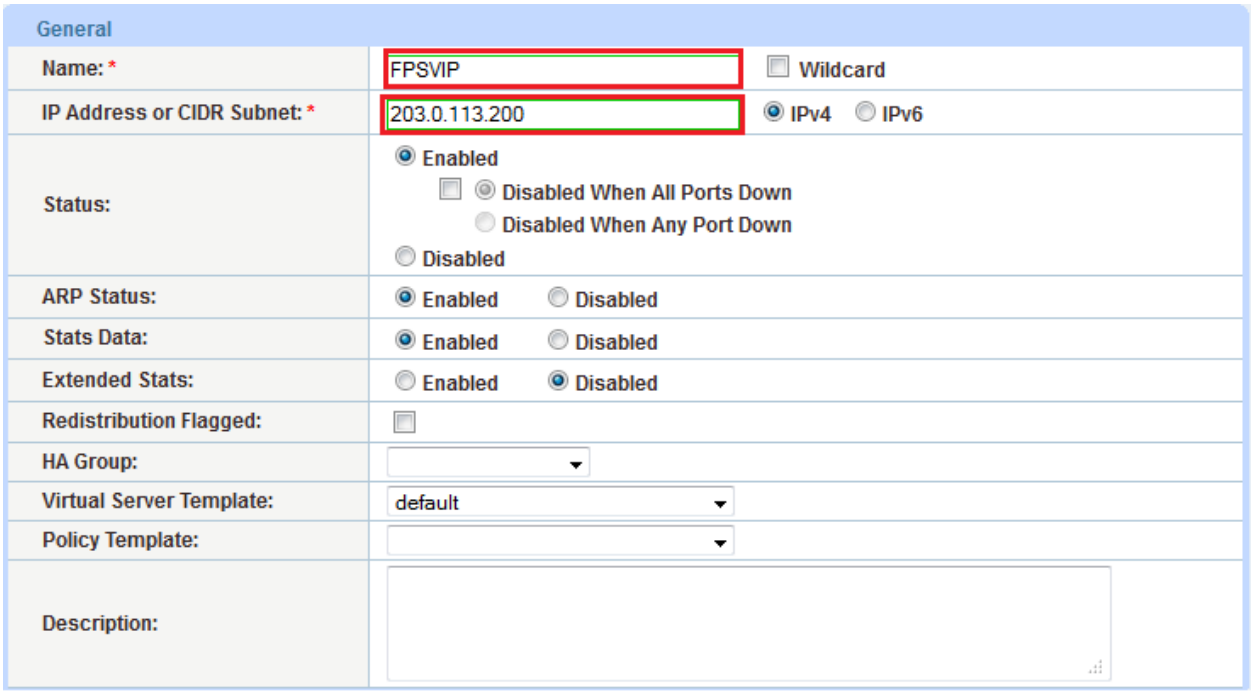

Figure 18: FPS VIP configuration

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:** “FPSVIP”
   - **IP Address:** 203.0.113.200
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:_203.0.113.200_TCP_443).*

4. Enter or select the following values:
   - **Type:** “TCP”.

- **Port:** “443”.
- **Service Group:** Select "FPSSG" from the drop-down menu.
- **Source NAT Pool:** Select “FPSSNAT” from the drop-down menu.
- **Client-SSL Template:** Select “ESSL” from the drop-down menu.

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

- **Persistence Template Type:** Select “Cookie Persistence Template”.
- **Cookie Persistence Template:** Select the “fpscookie” template.

Note: *For information about configuring the Virtual Service options, see the ADFS configuration section for these features. If you are using the same load balancer for ADFS (internal) and FPS (external), it is strongly recommended to use template names that make it easy to identify which templates are for ADFS and which templates are for FPS.*

5. Once completed, click **OK** and **Save** configuration.

10 OPTIONAL: ENABLE DDOS PROTECTION

The AX Series offers additional security features, including protection against Directed Denial-of-Service (DDoS) attacks. The DDoS protection options within the AX Series provide an additional layer of security from unwanted attacks. To enable DDoS protection within the AX Series:

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

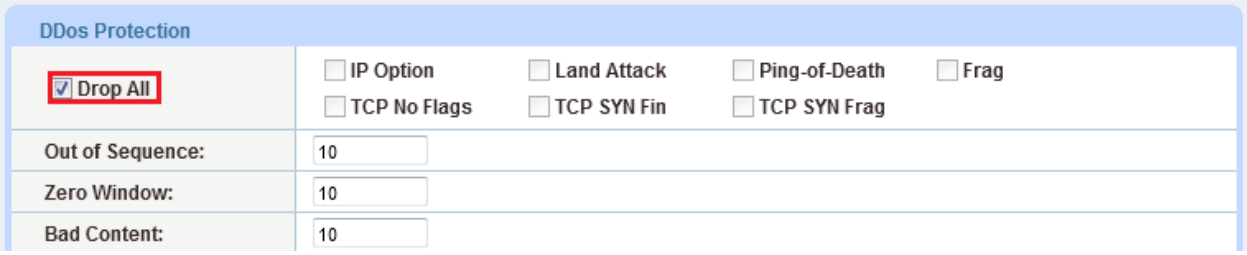

Figure 19: DDoS protection

Note: *Selecting "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 DDoS protection, see the AX Series System Configuration and Administration Guide.

11 SUMMARY AND CONCLUSION

The AX Series Application Delivery Controller enhances Microsoft Active Directory Federation Service (ADFS) by providing:

- High availability for ADFS servers to prevent downtime and access failure, with no adverse impact on user access to internal applications or Office 365 applications
- Provide seamless integration of Internal and External ADFS servers by load balancing requests, resulting in higher connection counts, faster end-user responsiveness and reduced ADFS application CPU utilization
- Seamless distribution of client traffic across multiple ADFS servers for site scalability
- Improved site performance and availability to end-users
- Higher Security with protection against DDoS attacks and other threats

By using the AX Series Application Delivery Controller (ADC), significant benefits are achieved for all ADFS 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

For more information about ADFS 2.0, refer to the following URLs:

http://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides%28v=ws.10%29.aspx

http://www.microsoft.com/en-us/download/details.aspx?id=10909

http://technet.microsoft.com/en-us/library/dd807067%28v=ws.10%29.aspx

12 SAMPLE CONFIGURATIONS

This section shows sample configuration files for the internal and external AX devices.

12.1 INTERNAL AX SERIES ADFS CONFIGURATION

```
!Sample configuration for AX Series for ADFS Load Balancing
hostname AX2500-ADFS
clock timezone Europe/Dublin
ip nat pool ADFSSNAT 192.0.2.100 192.0.2.100 netmask /24
health monitor ADFSHC
 method https
slb server AD1 192.0.2.2
   health-check ADFSHC
   port 443  tcp
slb server AD2 192.0.2.3
   health-check ADFSHC
   port 443  tcp
slb service-group ADFSSG tcp
    member AD1:443
    member AD2:443
slb template client-ssl "Client SSL"
   cert ADFSSSL
   key ADFSSSL pass-phrase encrypted
37O48xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb template persist cookie adfscookie
   name adfscookie
   domain example.com
   expire 86400
   insert-always
   match-type server
slb virtual-server ADFSVIP-INTERNAL 192.0.2.200
   port 443  https
      name _192.0.2.200_HTTPS_443
      source-nat pool ADFSSNAT
      service-group ADFSSG
      template client-ssl "Client SSL"
      template persist cookie adfscookie
```

12.2 EXTERNAL AX SERIES FEDERATION PROXY SERVER CONFIGURATION

```
!Sample configuration for FPS Load Balancing
hostname AX2500-FPS
```

```
clock timezone Europe/Dublin
ip nat pool FPSSNAT 203.0.113.100 203.0.113.100 netmask /24
health monitor FPSHC
 method https
slb server FPS1 203.0.113.2
   health-check FPSHC
   port 443  tcp
slb server FPS2 203.0.113.3
   health-check FPSHC
   port 443  tcp
slb service-group FPSSG tcp
    member FPS1:443
    member FPS2:443
slb template client-ssl "ESSL"
   cert FPSSSL
   key FPSSSL pass-phrase encrypted
37O48xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb template persist cookie fpscookie
   name fpscookie
   domain example.com
   expire 86400
   insert-always
   match-type server
slb virtual-server FPSVIP-EXTERNAL 203.0.113.200
   port 443  https
      name _203.0.113.200_HTTPS_443
      source-nat pool FPSSNAT
      service-group FPSSG
      template client-ssl " ESSL"
      template persist cookie fpscookie
```