Deployment Guide

AX Series with Citrix XenApp 6.5

TABLE OF CONTENTS

1 INTRODUCTION

Citrix XenApp is a thin client application that enables users to remotely connect to corporate applications. Citrix XenApp is widely used in the enterprise environment.

Note: *Citrix XenApp was formerly known as Citrix MetaFrame, Citrix Presentation Server or Citrix Winframe.*

1 DEPLOYMENT GUIDE OVERVIEW

This deployment guide shows how to install, configure, and optimize the AX Series with Citrix XenApp solution. The AX Series Application Delivery Controller (ADC) offers additional security, reliability and application optimization features; including SSL Offload and TCP Connection Reuse.

This configuration has an AX Series to load balance all the web traffic requests to the XenApp Servers.

2 DEPLOYMENT GUIDE PREREQUISITES

This deployment guide has the following prerequisites.

AX Series Requirement

The A10 Networks AX Series ADC must be running version 2.6.x or higher.

Tested Citrix XenApp Server

- XenApp 6.5
- Server 2008 R2 Standard x64
- 4 GB Memory
- 2 Processors
- 60 GB HDD

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

3 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*.

4 ARCHITECTURE OVERVIEW

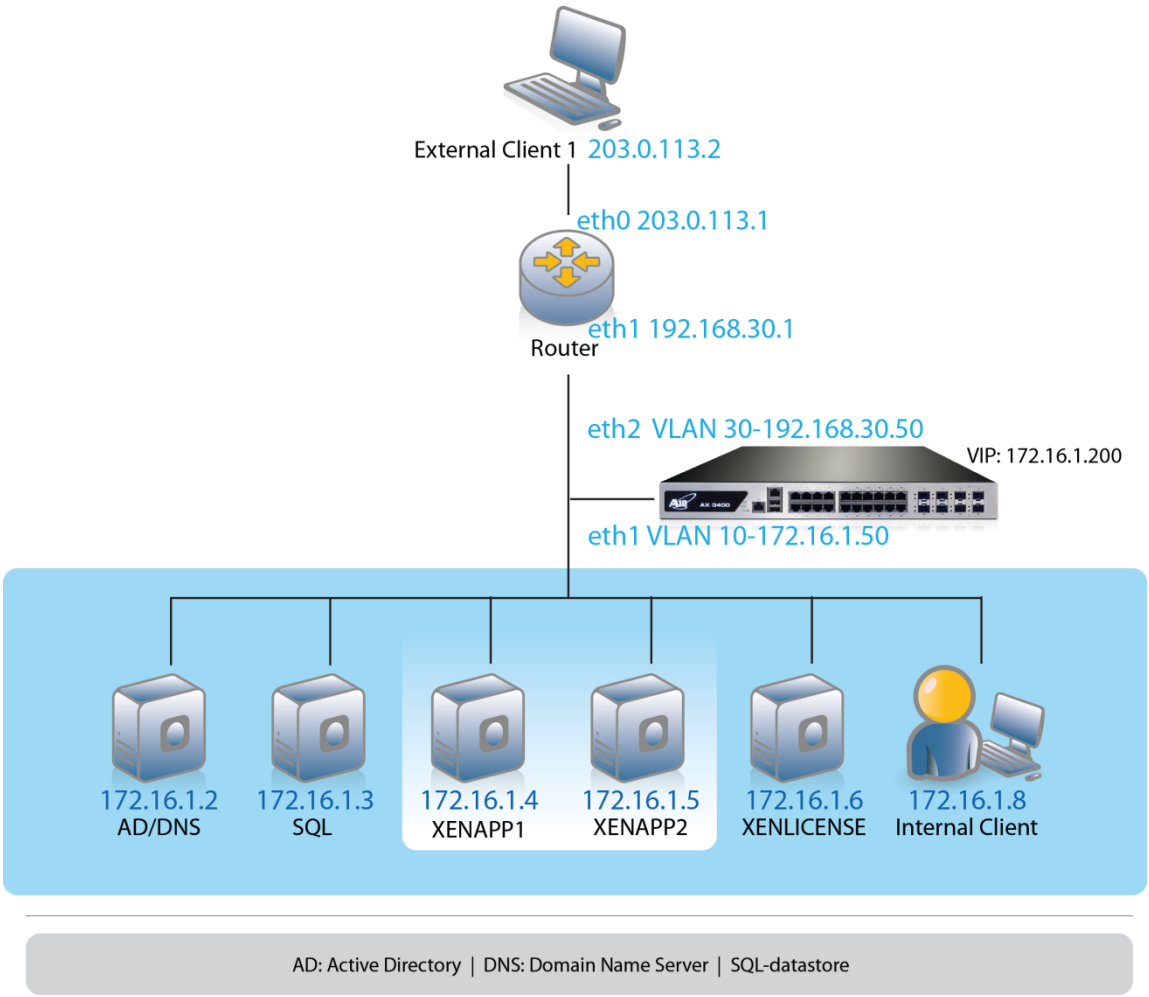

Figure 1: Configuration overview

5 CITRIX XENAPP SERVER ROLES

Citrix servers can be deployed to fulfill the following roles:

- Active Directory (AD) – All Citrix XenApp servers must be joined in a domain and in Active Directory Domain Services (ADDS).
- Data store – Critical component of the Citrix XenApp application. The data store is a central repository for all XenApp configurations such as applications, users, printers and servers.

- XenApp Application Servers – Server pool on which the core XenApp application suite is installed. XenApp allows users to connect to their corporate applications via any network connected device. XenApp can host applications on a central server and allows users to interact with them remotely or stream and deliver them to user devices for local execution. Hosts the published application to which users connect.
- XenLicense – Licensing server that enables features and services within a XenApp solution.

6 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 on-demand 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 request to the same XenApp server based on the source IP address of a packet.

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 “XENAPPHC”.
4. Select **Method** “HTTP”.
5. Click **OK**, and then see the next section to continue with the Service Group configuration.

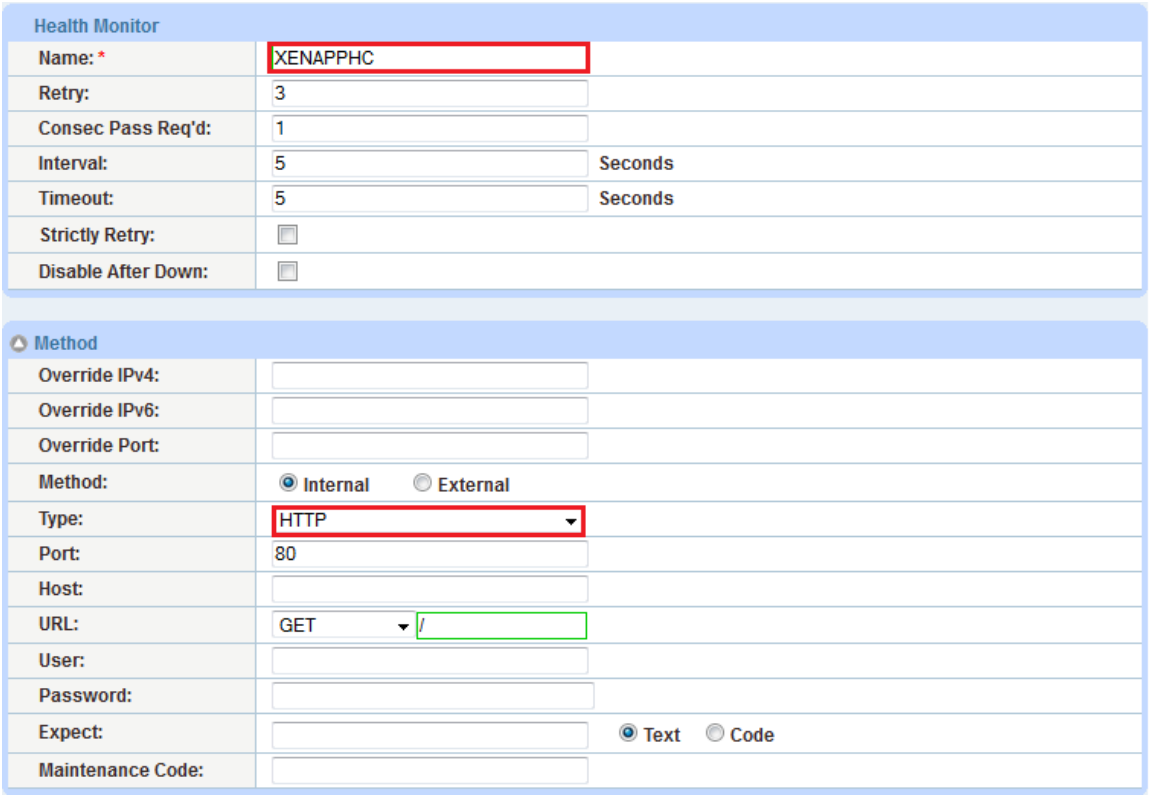

Figure 2: Health monitor configuration

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 an address from a pool of source NAT addresses. 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 Source NAT, 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:

- **NAT:** “SNAT”
- **Start IP Address:** “172.16.1.122”
- **End IP Address:** “172.16.1.122”
- **Netmask:** “255.255.255.0”

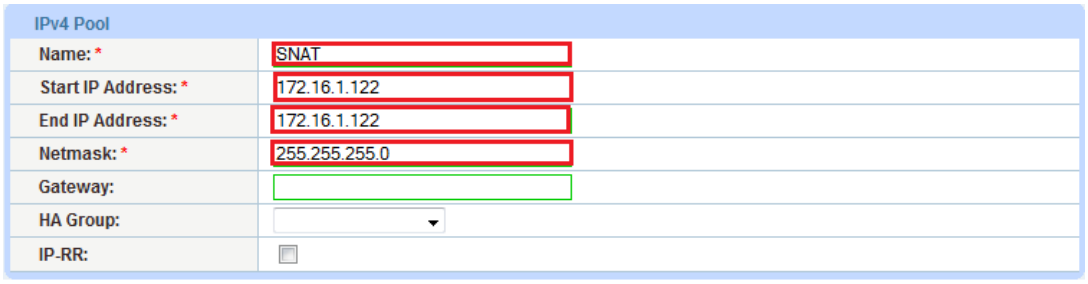

Figure 3: Source NAT pool configuration

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 SOURCE IP PERSISTENCE

The Source IP Persistence feature enables an HTTP 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:

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

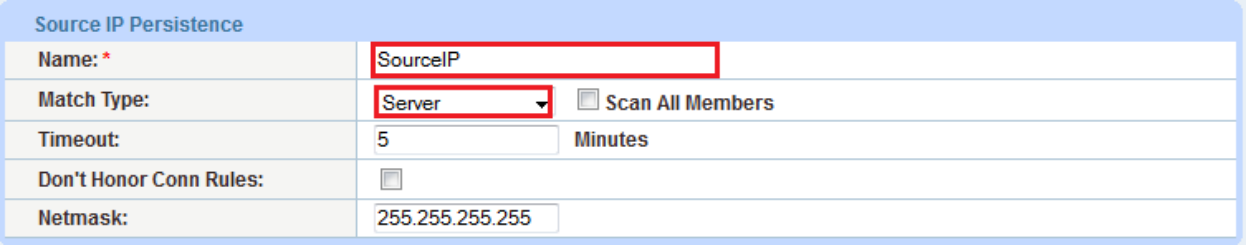

Figure 4: Source IP persistence

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

7 BASIC CONFIGURATION

This section explains how the AX appliance is configured for Citrix XenApp traffic with the TCP VIP type. This section contains detailed instructions on how to install real servers, a service group, virtual services, and virtual services in an AX Series.

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

7.1 SERVER CONFIGURATION

This section demonstrates how to configure the Citrix XenApp web 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:** "XENAPP1"
   - **IP Address/Host:** "172.16.1.4"

   Note: *Enter additional servers if necessary.*

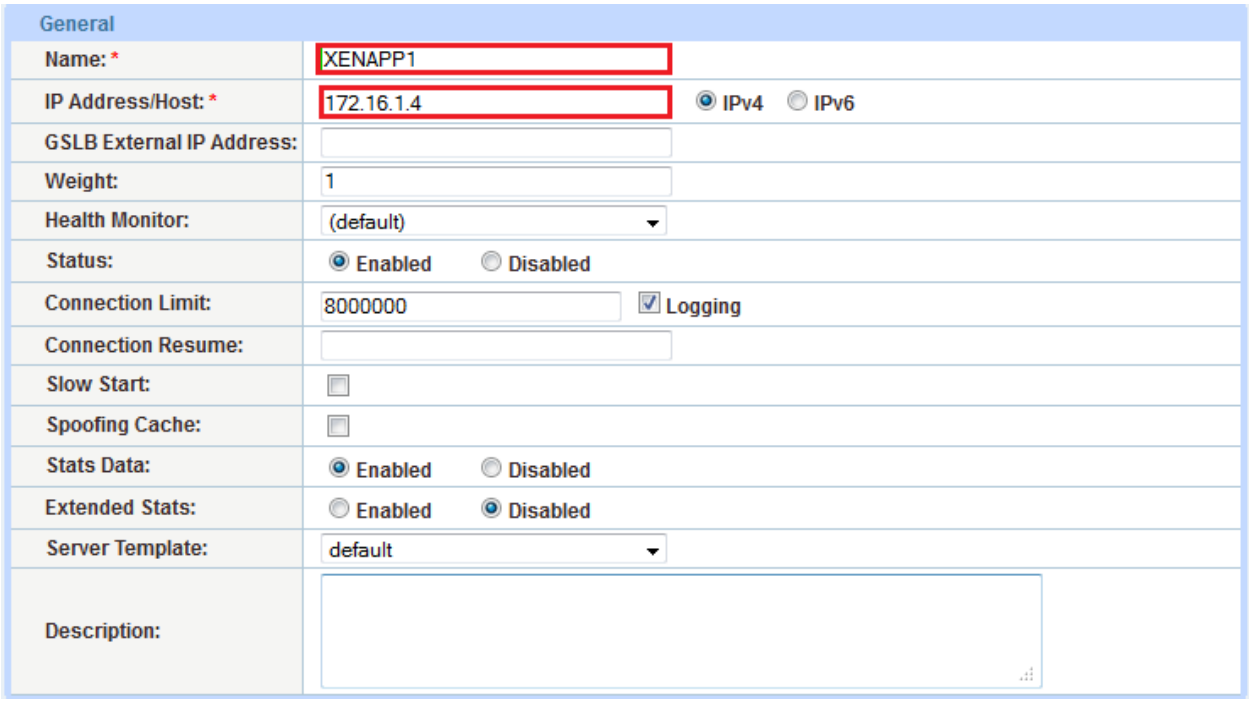

Figure 5: Server configuration

4. To add a port to the server configuration:

    a. Enter the port number in the **Port** field.

    b. Select the **Protocol**.

    c. Click **Add**.

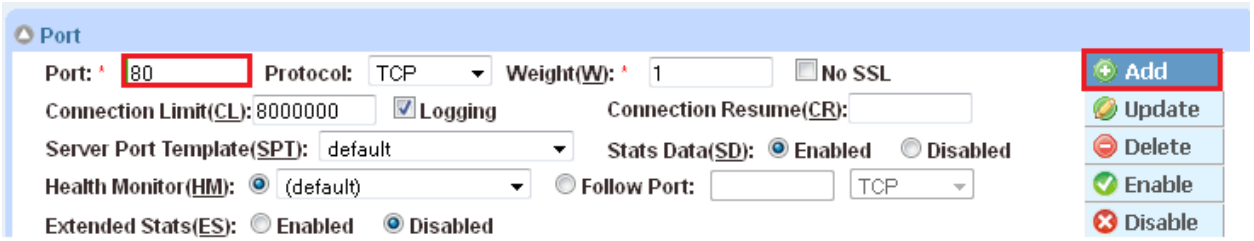

Figure 6: Server port configuration

5. Follow the same steps in this section for the XENAPP2 server.

6. 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:** “XENAPPSG”
   - **Type:** “TCP”
   - **Algorithm:** “Round Robin”
   - **Health Monitor:** “XENAPPHC”
4. In the Server section, select a server from the **Server** drop-down list and enter “80” in the **Port** field.
5. Click **Add**. Repeat for each server.

Figure 7: Service group configuration

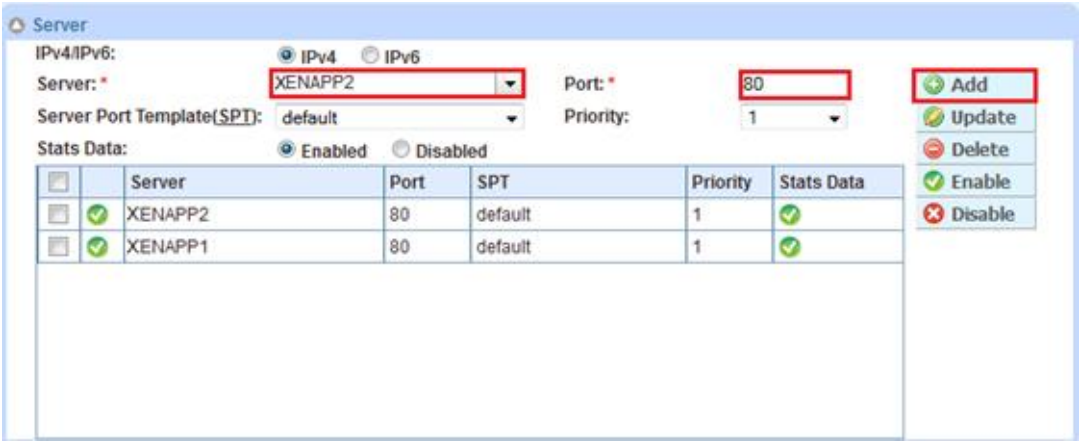

Figure 8: Server configuration

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

7.3 VIRTUAL SERVER CONFIGURATION

This section contains the basic configuration for a Virtual Server. 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:** "XENAPPVIP"
   - **IP Address:** "172.16.1.200"

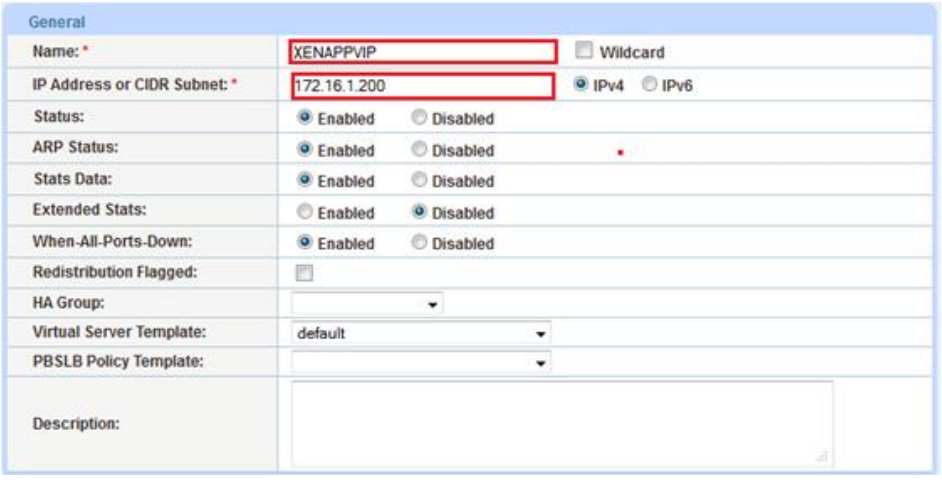

Figure 9: Virtual server configuration

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

   Note: *On the Virtual Service section, the Virtual Service will be pre-populated with a name (Example:_172.16.1.200_TCP_80).*

4. Enter or select the following values:

   - **TYPE:** "TCP"
   - **Port:** "80"
   - **Service Group:** Select **"**XENAPPSG**"** from the drop-down list.
   - **Source NAT Pool:** Select "SNAT" from the drop-down list.
   - **Persistence Template Type:** Select "Source IP Persistence Template".
   - **Source IP Persistence Template:** Select the "SourceIP" template.

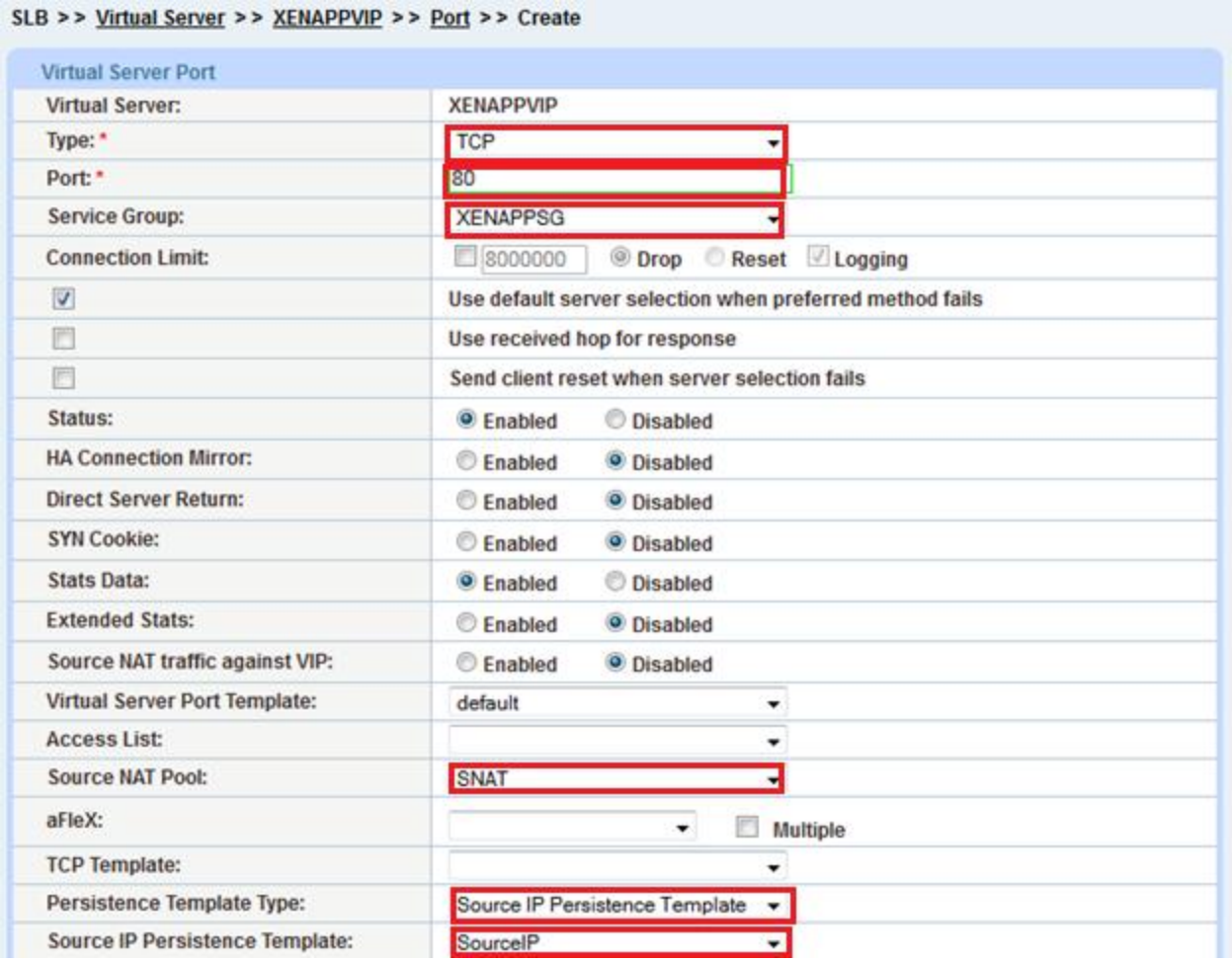

Figure 10: Virtual-server port configuration

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

8 VALIDATING THE CONFIGURATION

This concludes the basic configuration for XenApp. Using a client within the network, you can access the VIP with a browser and type the URL as:

http://172.16.1.200/Citrix/XenApp/auth/login.aspx

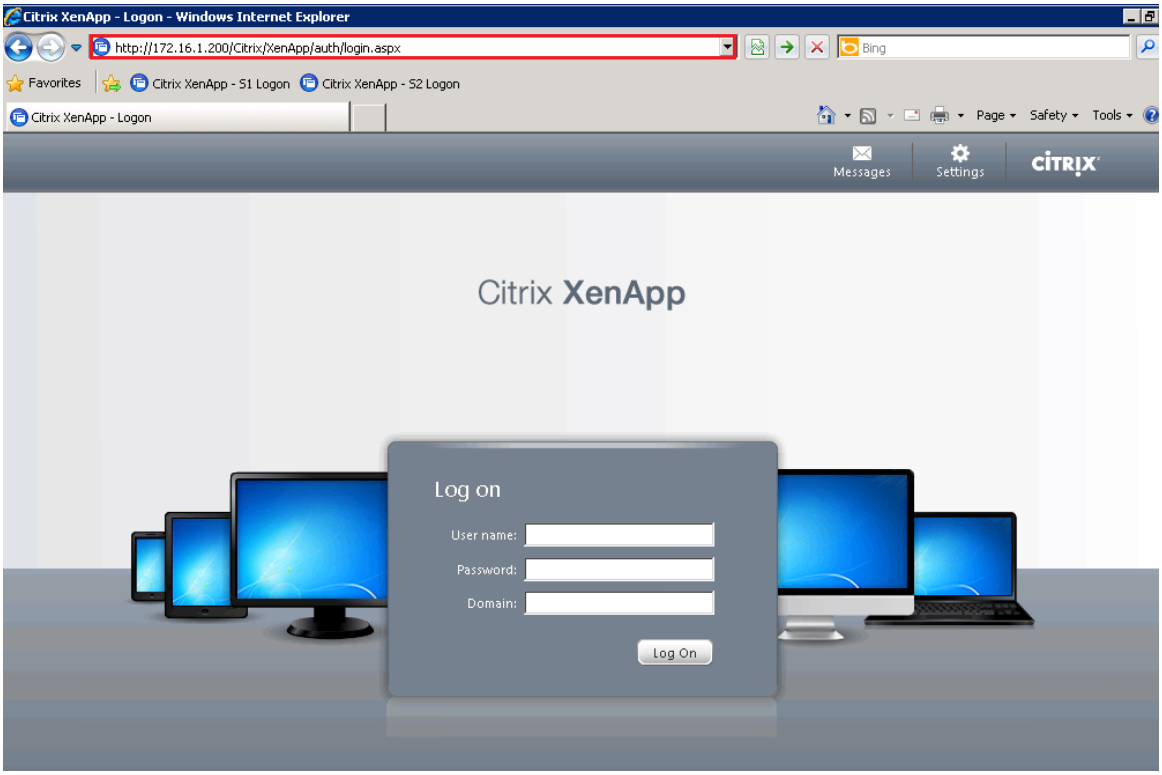

Figure 11: XenApp logon portal

9 ADVANCED CONFIGURATION

This section contains the advanced configuration of the AX Series with Citrix XenApp. The advanced configuration will use the HTTPS VIP type because it offers all the Layer 7 optimization options for enhancing the user experience. The advanced configuration increases server performance with features such as SSL Offload, HTTP Connection Reuse, aFleX redirection scripts, cookie persistence, and DDoS protection.

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 VIP.

Note: *With the assumption that you already understand basic configuration of the server, service group, virtual service and virtual server, this section will move directly to advanced configuration with minimal changes from the basic configuration.*

9.1 VIP TYPE CONVERSION FROM TCP TO HTTPS

To convert the VIP virtual service type from TCP to HTTP:

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. Click on the service name.
3. In the General section, edit the virtual service that was created from the basic configuration. Scroll to the **Type** drop-down list and select “HTTPS”. This option should automatically prefill the port section with "443".

   Note: *For the naming convention on the Virtual Service, if you change the port VIP type, you also should update the Virtual Service name. Example: 172.16.1.100_HTTPS_443*

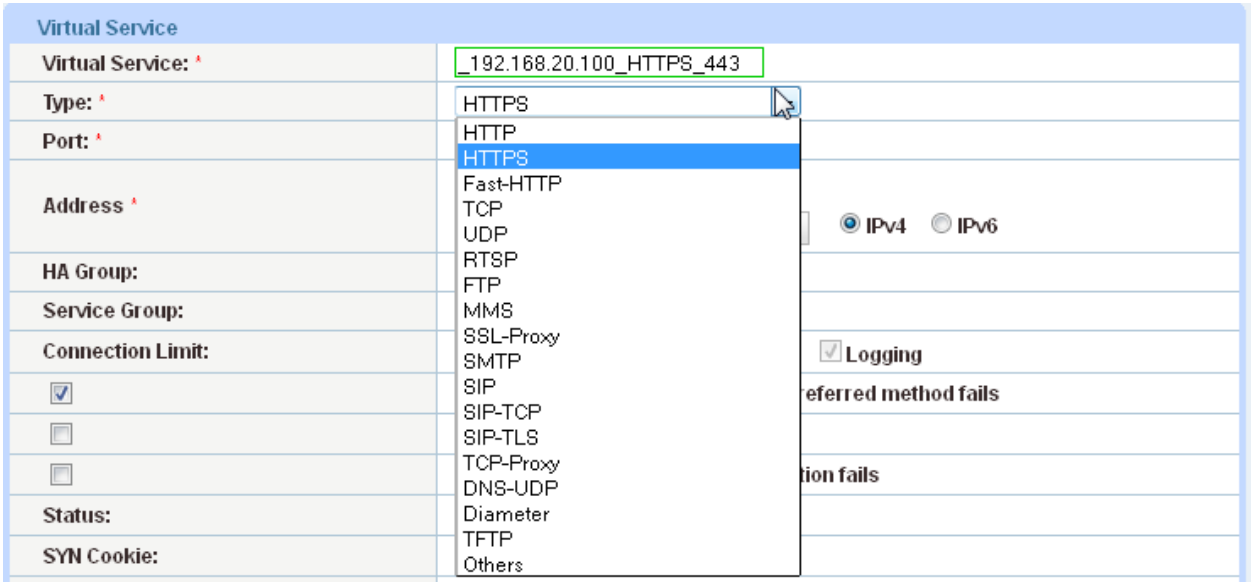

Figure 12: Virtual service

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

9.2 SSL OFFLOAD

SSL Offload mitigates the performance impact that encrypting and decrypting SSL traffic sent via secure SSL can have on a web server application or web server farm. SSL Offload is a performance optimization feature that enables a server to offload the SSL traffic to the AX Series.

9.2.1 IMPORT OR GENERATE THE SERVER CERTIFICATE

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

9.2.2 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, “XenApp”.
4. From the **Issuer** drop-down list, select “Self”.
5. Enter the following values:
    - **Common Name:** “example”
    - **Division:** “example”
    - **Organization:** “example”
    - **Locality:** “San Jose”
    - **State or Province:** “CA”
    - **Country:** “USA”
    - **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.*

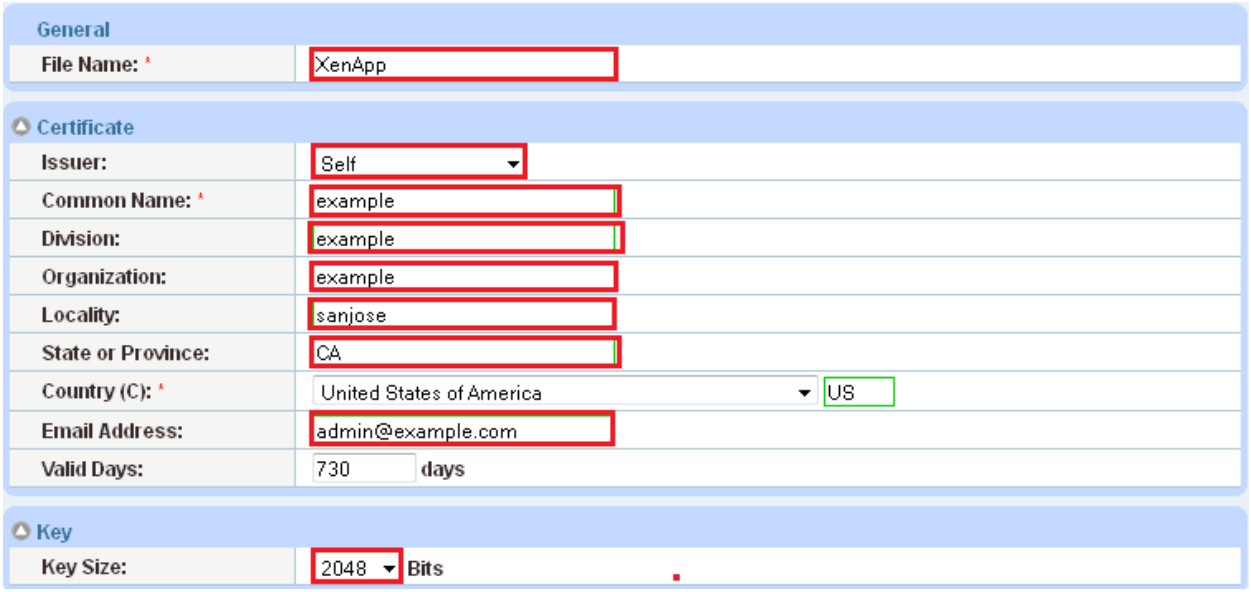

Figure 13: Self-signed certificate configuration

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

9.2.3 OPTION 2: IMPORT THE CERTIFICATE AND KEY

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Import**.
3. Enter the **Name**, “xenapp”.
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.*

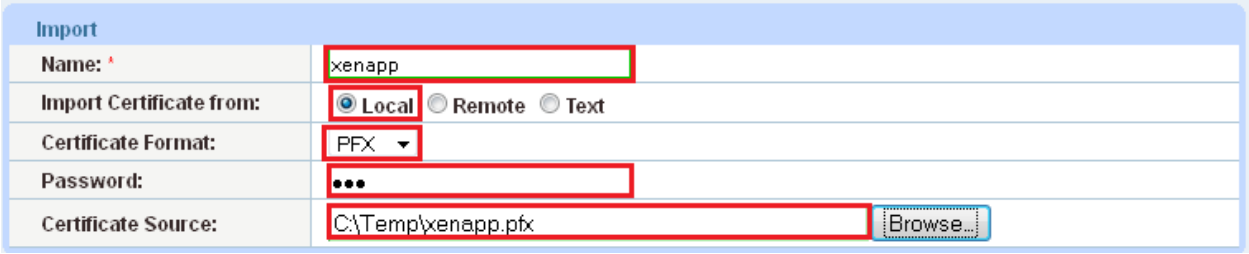

Figure 14: SSL certificate import

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

9.2.4 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:** "XenApp”
   - **Key Name:** “XenApp”
   - **Pass Phrase:** “123”
   - **Confirm Pass Phrase:** “123”

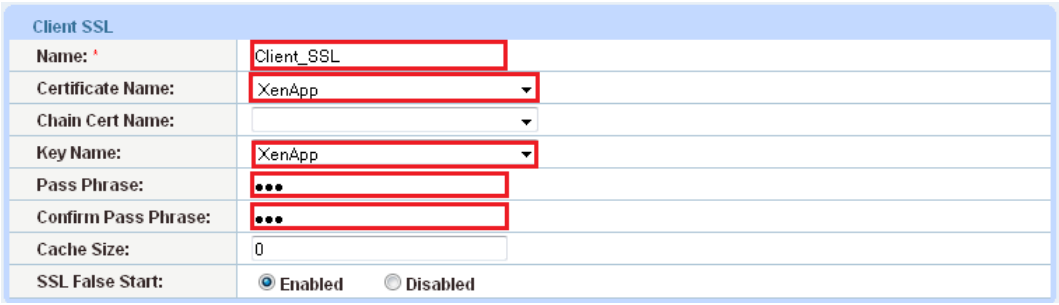

Figure 15: Client SSL template

Once the Client SSL template is completed, you must bind the template to the HTTPS VIP (port 443), as follows:

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. Click on the virtual server name.
3. Select Port “443” and click **Edit**.
4. Apply the Client SSL template created by selecting it from the **Client-SSL Template** drop-down list.

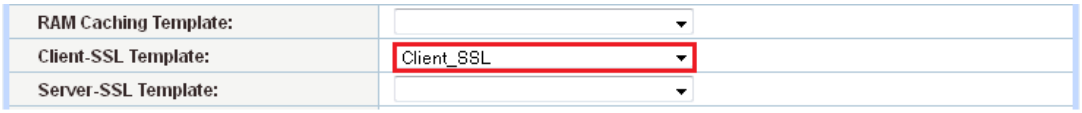

Figure 16: Client SSL template selection

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

9.3 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**, "xenapp_cookie".
4. Check the **Expiration** radio button and enter “86400” in the **Seconds** field.

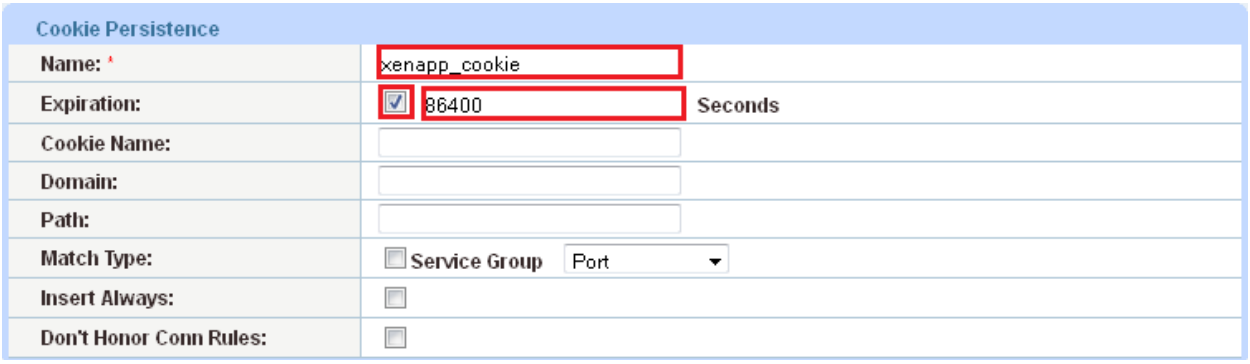

Figure 17: Cookie persistence template

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

9.4 TCP CONNECTION REUSE

1. Navigate to **Config Mode > Service > Template > Connection Reuse**.
2. Click **Add**.
3. Enter **Name**: “xenapp_cr”.

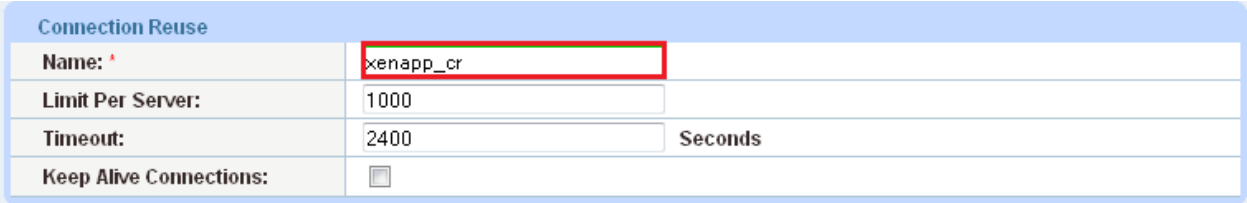

Figure 18: TCP Connection Reuse template

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

9.5 HTTP-TO-HTTPS REDIRECT

This section explains how to redirect XenApp web traffic that is destined from HTTP (port 80) to HTTPS (port 443) using aFleX scripts. aFleX is based on a standard scripting language, TCL, and enables the AX device to perform Layer 7 deep-packet inspection (DPI). For examples of aFleX scripts, please refer to the following URL:

http://www.a10networks.com/products/axseries-aflex_advanced_scripting.php

As an example, one of the most commonly used aFleX scripts is the “HTTP redirect to HTTPS traffic” script. You can download additional aFleX script examples from the URL listed above.

To configure transparent HTTPS redirect using aFleX:

1. Create the aFleX script:
    a. Navigate to **Config Mode > Service > aFleX**.
    b. Enter a **Name** for the script.
    c. Type or copy-and-paste the script into the **Definition** field.
    d. Click **OK**, then click **Save** to save the configuration.

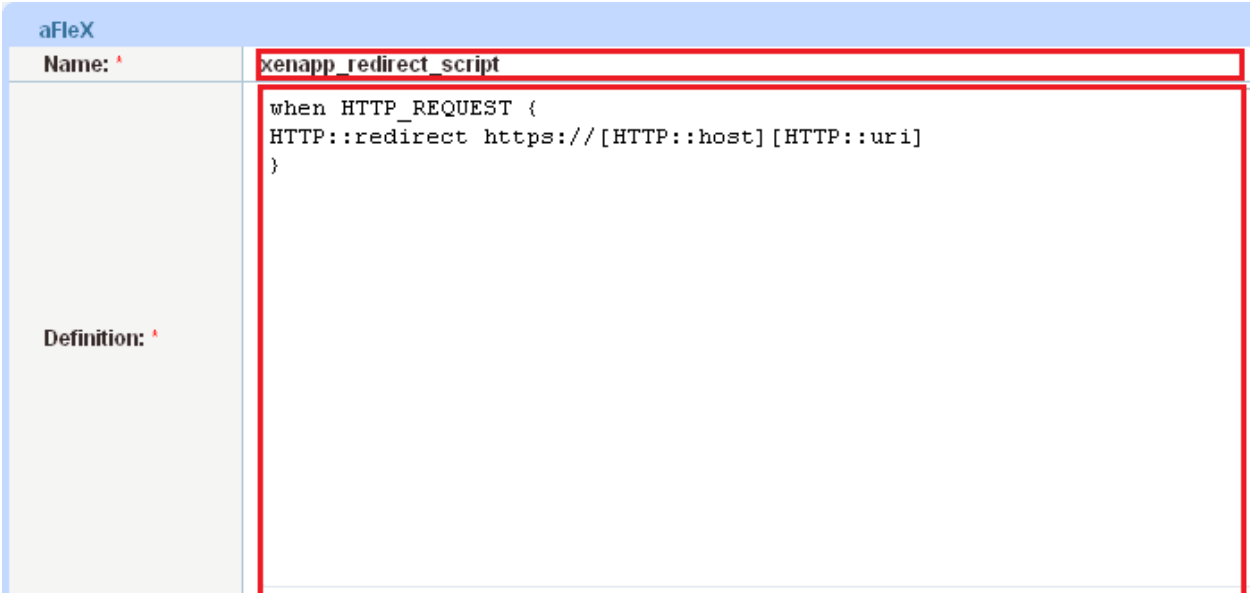

Figure 19: aFleX redirect script

2. Apply the aFleX script to the virtual port on the VIP:
    a. Navigate to **Service > SLB > Virtual Server**.
    b. Select the virtual port and click **Edit**.
    c. Select the script from the **aFleX** drop-down list.
    d. Click **OK**.
    e. Click **OK**, then click **Save** to save the configuration.

Redirect Script Copy and Paste:

```
when HTTP_REQUEST {

HTTP::redirect https://[HTTP::host][HTTP::uri]

}
```

***Note:** The aFleX script must be bound to virtual service type HTTP and virtual server port 80. Otherwise, if you use the basic configuration using TCP, the aFleX redirect script will not apply to the VIP.*

9.6 APPLY OPTIMIZATION AND ACCELERATION FEATURE TEMPLATES ON 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.

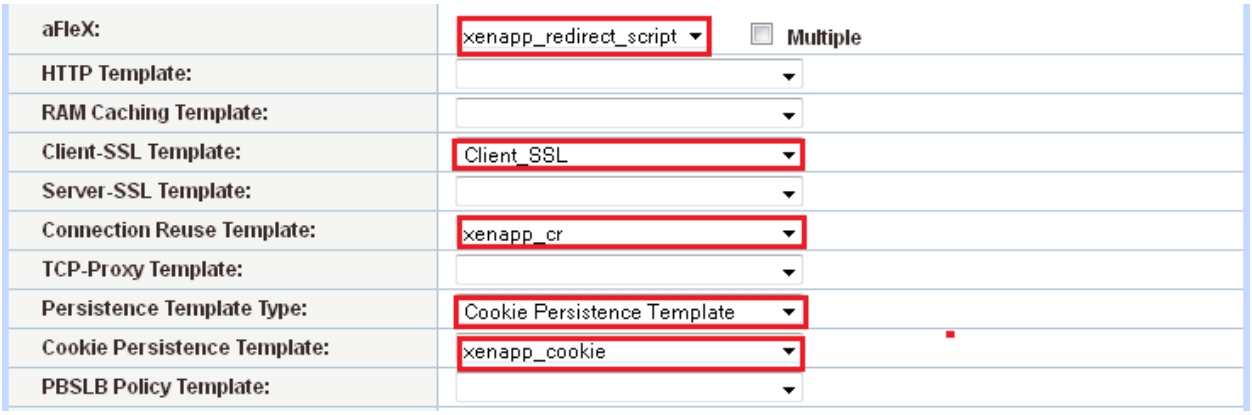

Figure 20: Applying features

Note: *To review, the aFleX redirect script is used to redirect all HTTP requests to be sent to a HTTPS/Secure XenApp portal. The client SSL template is used for SSL Offload to secure and offload the backend XenApp servers from processing SSL requests. Connection Reuse uses the same TCP connection to send and receive multiple requests/responses. Cookie persistence stores HTTP cookies to a client's device and allows the client to reconnect to the same server previously visited at a website.*

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

9.7 OPTIONAL SECURITY FEATURES

The AX Series offers additional security features against distributed denial-of-service (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.

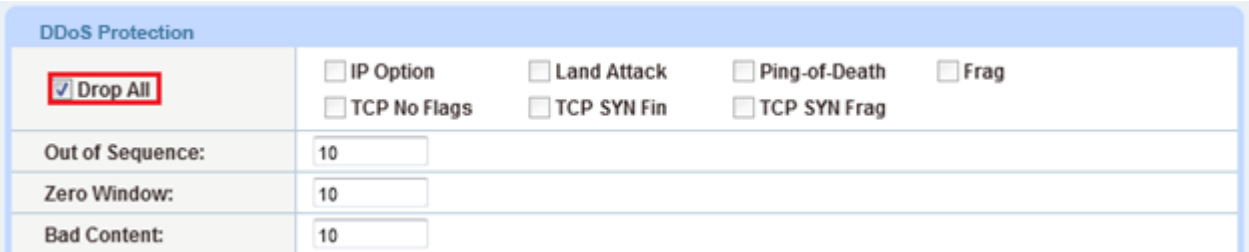

Figure 21: DDoS protection

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 SUMMARY AND CONCLUSION

The sections above show how to deploy the AX device for optimization of Citrix's XenApp solution. By using the AX device to load balance a pool of XenApp web servers, the following key advantages are achieved:

- High availability for XenApp web servers to prevent web site failure, with no adverse impact on user access to applications
- Seamless distribution of client traffic across multiple XenApp web servers for site scalability
- Higher connection counts, faster end-user responsiveness, and reduced XenApp 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 XenApp application 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 COMMANDS FOR SAMPLE BASIC CONFIGURATION

This section shows the CLI commands for implementing the sample basic configuration described above.

```
CitrixXenAppLB#show run
Current configuration: 1114 bytes
Configuration last updated at 02:41:15 IST Fri Apr 27 2012
Configuration last saved at 03:09:19 IST Fri Apr 27 2012
version 2.6.1-P2-SP1, build 8 (Nov-11-2011,14:44)
hostname CitrixXenAppLB
clock timezone Europe/Dublin
ip nat pool SNAT 172.16.1.122 172.16.1.122 netmask /24
health monitor XENAPPHC
 method http
slb server XENAPP1 172.16.1.3
   health-check XENAPPHC
   port 80  tcp
slb server XENAPP2 172.16.1.4
   health-check XENAPPHC
   port 80  tcp
slb service-group XENAPPSG tcp
    health-check XENAPPHC
    member XENAPP1:80
    member XENAPP2:80
slb virtual-server XENAPPVIP 172.16.1.100
   port 80  tcp
      name _172.16.1.100_HTTP_80
```

```
      source-nat pool SNAT
      service-group XENAPPSG
web-service timeout-policy idle 0
end
CitrixXenAppLB#
```

B. CLI COMMANDS FOR SAMPLE ADVANCED CONFIGURATION

This section shows the CLI commands for implementing the sample advanced configuration described above.

```
CitrixXenAppLBAdv#show run
Current configuration: 1723 bytes
Configuration last updated at 22:12:54 IST Fri Apr 27 2012
Configuration last saved at 22:12:56 IST Fri Apr 27 2012
version 2.6.1-P2-SP1, build 8 (Nov-11-2011,14:44)
hostname CitrixXenAppLBAdv
ip nat pool SNAT 172.16.1.122 172.16.1.122 netmask /24
health monitor XENAPPHC
 method http
ip anomaly-drop drop-all
slb server XENAPP1 172.16.1.3
   health-check XENAPPHC
   port 80  tcp
slb server XENAPP2 172.16.1.4
   health-check XENAPPHC
   port 80  tcp
slb service-group XENAPPSG tcp
    health-check XENAPPHC
    member XENAPP1:80
    member XENAPP2:80
slb template connection-reuse xenapp_cr
```

```
slb template client-ssl Client_SSL
   cert XenApp
   key XenApp pass-phrase encrypted
37O48xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb template persist cookie xenapp_cookie
   expire 86400
slb template persist source-ip SourceIP
   netmask6 0
   match-type server
slb virtual-server XENAPPVIP 172.16.1.100
   port 443  https
      name _172.16.1.100_HTTPS_80
      source-nat pool SNAT
      service-group XENAPPSG
      template client-ssl Client_SSL
      template connection-reuse xenapp_cr
      template persist cookie xenapp_cookie
   port 80  http
      name _172.16.1.100_HTTP_80
      service-group XENAPPSG
      aflex xenapp_redirect_script
web-service timeout-policy idle 0
end
CitrixXenAppLBAdv#
```