Deployment Guide

AX Series with Microsoft Office SharePoint Server

Table of Contents

DEPLOYMENT GUIDE

AX Series with Microsoft Office SharePoint Server

Introduction

This deployment guide contains detailed procedures to configure AX Series server load balancers to support Microsoft 2003 and 2007 SharePoint Servers.

Microsoft SharePoint is a web-based enterprise application for document management and collaboration, utilizing the HTTP and HTTPS protocols. Organizations have purchased more than 100 million licenses, and more than 17,000 organizations use SharePoint implementations to facilitate and collaborate with information that is critical to businesses. SharePoint is a TCP-based application requiring multiple acknowledgements and secure processing of data, which could slow down server response and degrade responsiveness to users when load increases.

For more information on Microsoft Office SharePoint Server, visit:

http://office.microsoft.com/en-us/sharepointserver/default.aspx

The AX Series with its Advanced Core Operating System (ACOS) has been designed specifically for applications such as SharePoint, providing better robustness in failover situations, offloading security processing, and performing intelligent load balancing.

Prerequisites & Assumptions

- A10's AX platform should be running software version 2.0 or later.
- All of the configuration steps in this document apply to the AX platform. For information on the SharePoint Server, refer to the appropriate SharePoint documentation. http://www.microsoft.com/sharepoint/prodinfo/what.mspx
- The SharePoint Servers should be clustered and use replication or use an external database, which is independent of AX platform.
- It is assumed that users have some basic configuration familiarity with both AX and SharePoint products.
- The AX can be configured in one-armed mode or routed mode.

INTRODUCTION

Configuring the AX for Microsoft SharePoint Server

- AX running OS version 2.0 or later

  Note: The configuration steps in this document are based on AX Series Software Release 2.0.

- Microsoft Windows running SharePoint Server

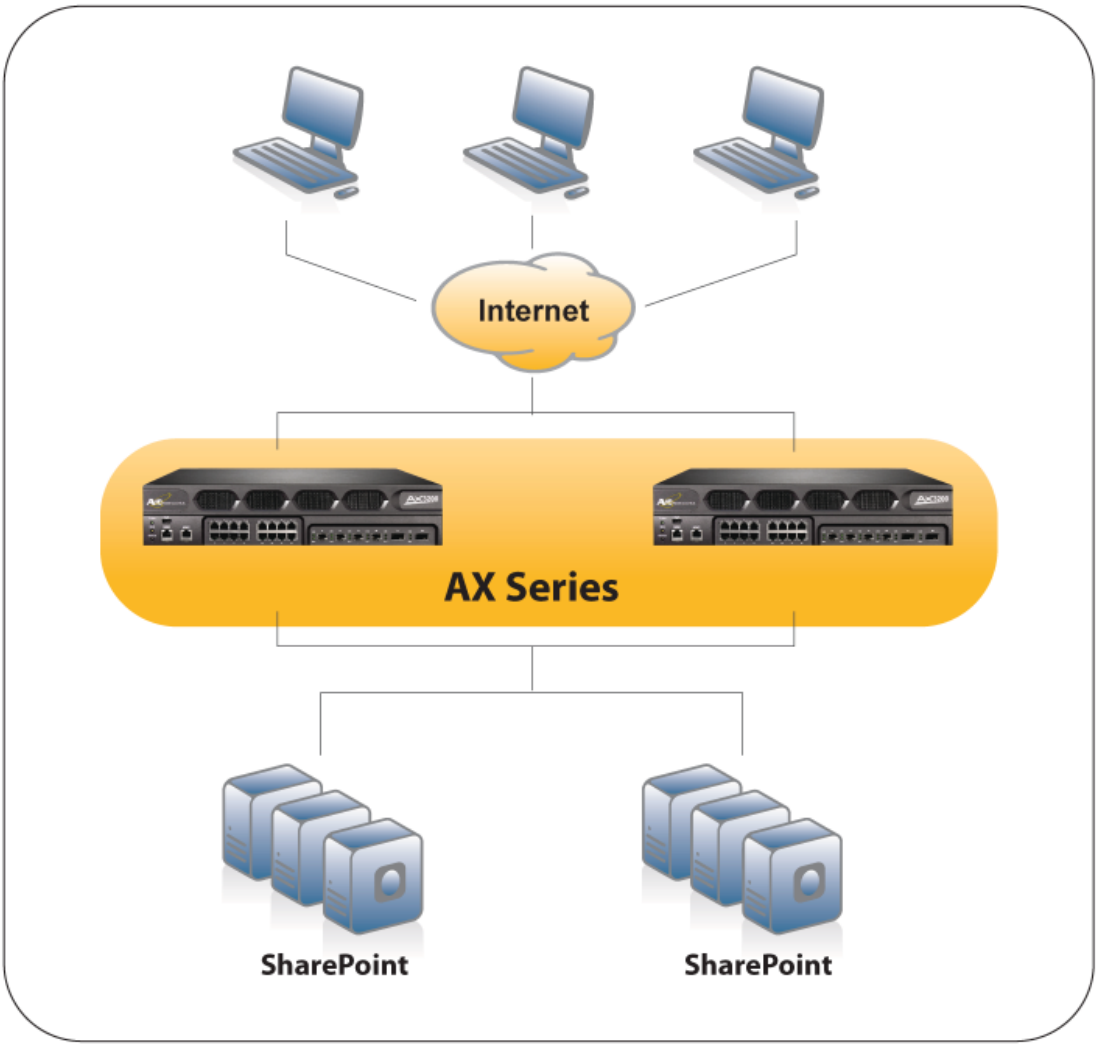

Figure 2.1 Deployment Guide Logical Configuration

Configuring the AX for SharePoint Server Using HTTP

Connect the AX devices to the network that consists of SharePoint Servers and configure the network routing entries if the SharePoint Servers are in a different subnet, then follow the configuration steps below.

Configuration Steps

The configuration steps differ slightly depending on whether the SharePoint Server will be accessed on HTTP or HTTPS (SSL). This deployment guide contains both of the configurations.

To configure the AX device to load balance SharePoint Servers, perform the following steps:

- Configure a HTTP health monitor.
- Configure a real server.
- Configure a service group.
- Configure IP Source NAT.
- Configure templates.
- Configure a HTTP virtual server.

These configuration steps are applicable to HTTP mode. If you are using the AX device as a SSL proxy to connect to the servers over HTTPS, some additional steps are required. These are described in the section “Configuring the AX for SharePoint Server Using SSL.”

Configure HTTP Health Monitor

The AX device can regularly check the health of real servers and service ports. Health checks ensure that client requests are directed only to available servers. You can use default Layer 3 (ping) and Layer 4 health monitors and custom health monitors. You also can use external health monitors implemented using scripts. The configuration in this guide uses default Layer 3 and custom HTTP health monitors.

To configure a HTTP health monitor:

1. Select **Config Mode > Service > Health Monitor**.
2. Click **Add**.
3. On the **Health Monitor** tab, enter a name for the monitor in the name field. In this example, the name “*HTTP*” is used.
4. In the **Method** box, select **HTTP** from the **Type** drop-down list.
5. Configure optional fields as required for your deployment. In this example, the default health monitor settings are used.
6. Click **OK** to finish configuration of the health monitor. The health monitor appears in the health monitor table.

Note on the "Save" button: Clicking OK adds the health monitor to the AX device's running-configuration, which is the configuration in active memory. At this point, the changes will not be restored if the device is rebooted. For changes to be restored after a reboot, you must save them to the startup-configuration, by clicking the "Save" icon in the upper portion of the GUI window. Make sure to click Save after completing the remaining configuration steps. The icon to the right of the "Save" button will continually flash red when a change has not been saved. See Figure 2.2.1

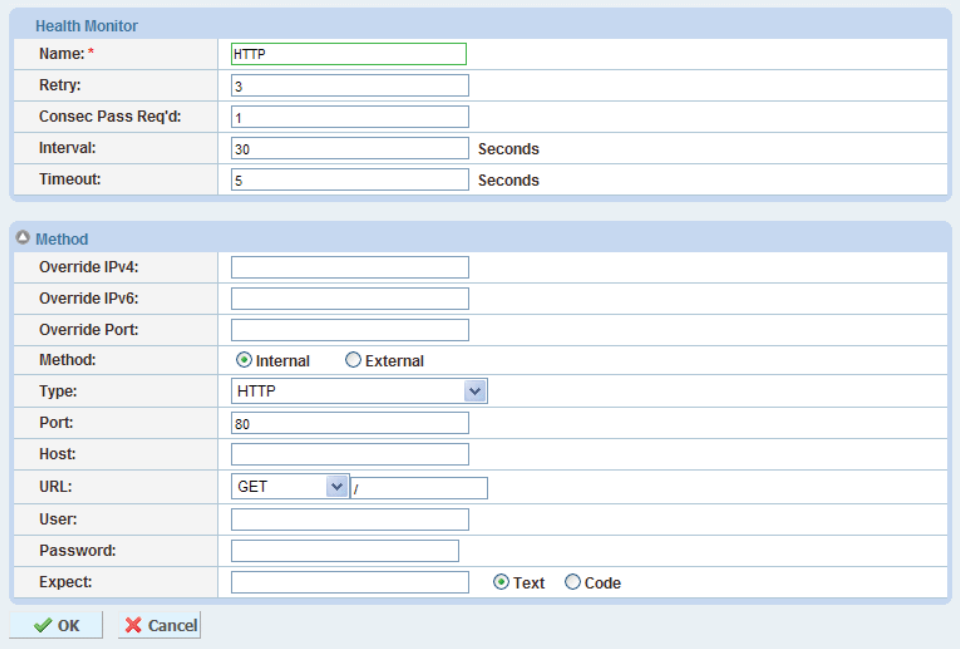

Figure 2.2 Health Monitor Configuration

Figure 2.2.1 "Save" icon flashing Red indicating Running-Config is not saved to Startup-Config

Configure Real Server

In this example, the real server is the SharePoint Server. You need to configure a separate real server on the AX device for each SharePoint Server. On each real server, configure a HTTP port for the server and apply the HTTP health monitor to the port. The AX device will periodically check the health of the server and its HTTP port using the default Layer 3 health monitor and the custom HTTP health monitor.

To configure a real server:

1. Select **Config Mode > Service > SLB**.
2. Select **Server** on the menu bar.
3. Click **Add**. The **General** box appears.
4. In the **Name** field, enter a name for the server. In this example, the name is *"Win2003-SPS"*.
5. In the **IP Address** field, enter the IP address of the server.
6. In the **Health Monitor** drop-down list, leave the default health monitor selected. This drop-down list specifies the Layer 3 health monitor, which will ping the server's IP address.
7. In the **Port** box **Port** field, enter the number of the service port on the real server. In this example, the port number is 80.
8. In the **Health Monitor** (HM) drop-down list for the port, select the previously configured HTTP health monitor *"HTTP"*.
9. Click **Add** to add the port to the port list for the server.
10. Click **OK**. The real server appears in the server table.
11. Repeat this procedure for each of the SharePoint Servers.

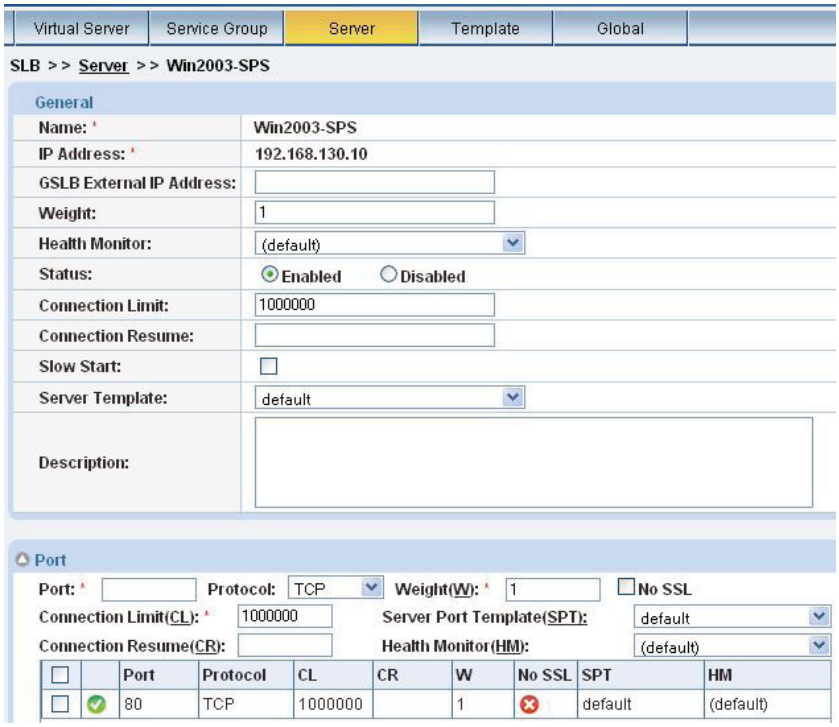

Figure 2.3 Real Server Configuration

Configure Service Group

A service group contains a set of real servers from which the AX device can select to service client requests. A service group allows you to virtually support multiple SharePoint real servers as one logical server. This example uses a service group that contains SharePoint Servers as real servers and the applicable service port 80.

To configure a service group:

1. Select **Config Mode > Service > SLB**.
2. Select **Service Group** on the menu bar.
3. Click **Add**. The **Service Group** box appears.
4. In **Name** field, enter name of service group. In this example, the name is *"HTTP-SPS"*.
5. In the **Algorithm** drop-down list, select the preferred load-balancing method. You can control the load on each server by selecting the appropriate type of load balancing methods. For this configuration, **Round Robin** is used.
6. In the **Server** box, select a previously configured real server from the Server drop-down list. For example *"Win2003-SPS"*.
7. In the **Port** field, enter the service port number (in this example, *"80"*).
8. Click **Add**. Repeat steps 6-8 for each real server.
9. Click **OK**. The new group appears in the service group table.

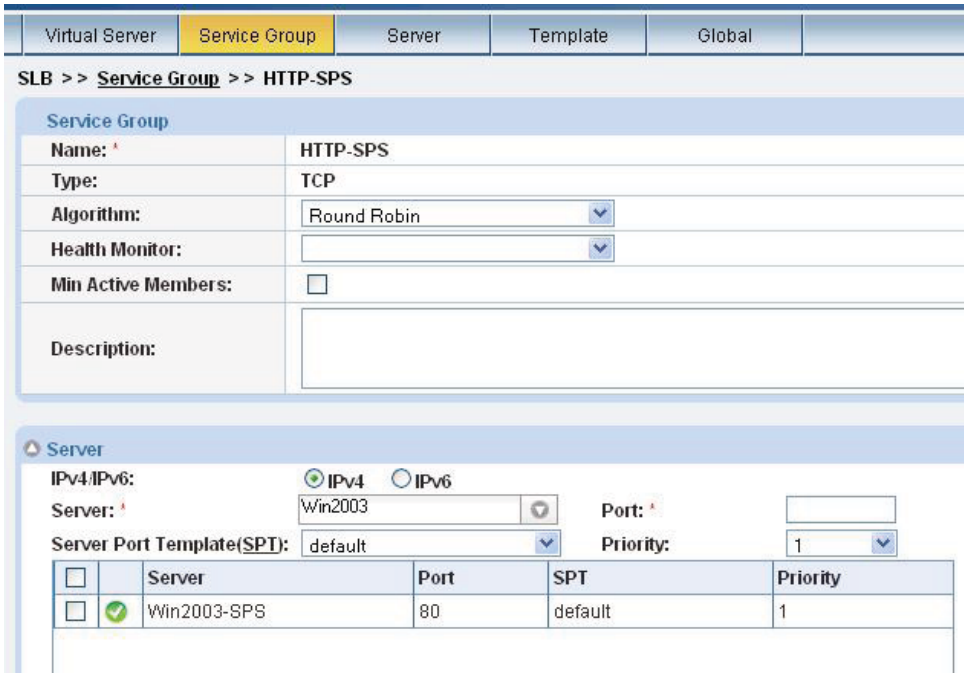

Figure 2.4 Service Group Configuration

Configure IP Source NAT

This step configures the IP address pool to use for IP source Network Address Translation (NAT). This pool assigns IP addresses to clients that connect to the SharePoint Servers. When the AX device performs NAT for a port that is bound to the template, the device selects an IP address from the pool. Note: This step is optional, typically for mapping between external IP addresses and internal IP addresses.

To configure Source NAT:

1. Select **Config Mode > Service > IP Source NAT**.
2. Select **IPv4** Pool on the menu bar.
3. Click **Add**. The **IPv4 Pool** box appears.
4. Enter a **Name** for the pool. In this example, the pool name is *"SPS"*.
5. Enter the single IP or IP addresses for the **Start IP Address** and **End IP Address** fields (the beginning and ending addresses in the range to use for the pool).
6. Enter the network mask in the **Netmask** field.
7. If the AX device is deployed in transparent mode, enter the default gateway if needed in the **Gateway** field to use for the NAT traffic (in this example, the AX device is deployed in route mode, so the field is left blank).
8. To use session synchronization for NAT translations with another AX for high availability configurations, select the high availability (HA) group. This drop down is empty if no HA Groups have been defined.
9. Click **OK**.

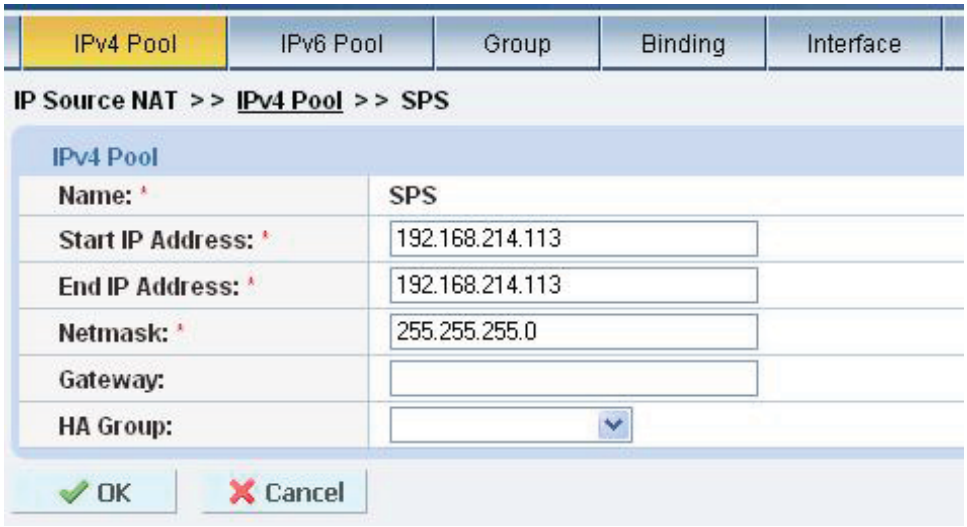

Figure 2.5 IP Source NAT Configuration

Configure Templates

Templates are sets of configuration parameters that apply to specific service types or to servers and service ports. Even though in some cases default templates can be used, it is recommended that you create templates specifically allowing you to change the templates in the future without impacting the default templates, which others may be sharing also.

For this deployment, the following types of templates are used:

- HTTP template
- Cookie-persistence template (optional)
- TCP-proxy template
- RAM Caching template (optional)

To place a template into use, you must bind it to the virtual port on the virtual server. This is covered later in the configuration steps for the virtual server.

Configure HTTP Template

AX HTTP templates have many options, including options to change information in the HTTP header, and select a service group based on the URL requested by the client. By default, all the options in this template are either disabled or not set, so you need to configure these options per your deployment requirements.

To configure a HTTP template:

1. Select **Config Mode > Service > Template**.
2. Select **Application > HTTP** from the drop down menu bar.
3. Click **Add**. The **HTTP > List** box appears.
4. Enter a **Name** for the template (in this example, *"SPS-HTTP-Temp"*).
5. Select or enter values for the template options you want to use. In this example, the default values are used for the remaining options.
6. There are additional options for this tab below, or when finished, click **OK**. The template now appears in the HTTP template list.

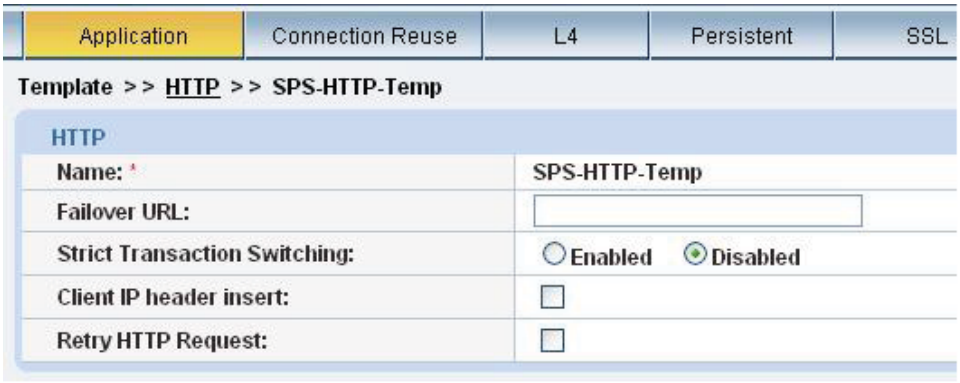

Figure 2.6 HTTP Template Configuration

Optionally, continue on the same configuration to add compression with the default compression level:

1. Click on **Compression** box to expand it.
2. Click **Enabled** on the **Compression** radio button.
3. To keep the Accept-Encoding field in client requests, select the **Enabled** radio button next to **Keep Accept Encoding**. Otherwise, to remove the field, leave this option disabled.
4. To specify the minimum content length that is eligible for compression, check the **Min Content Length** check box, then enter the minimum number of bytes the content must be in the field that is now visible. In our example we type *"1024"*.
5. To add more content types to be compressed:
   a. Click the **Content Type** then **Type** field.
   b. In the **Type** field, enter the string for a content type to compress. In this example first we type "*pdf*".
   c. Click **Add**.
   d. Repeat step b and step c for each type of content to compress.
6. Additonal options to **Exclude Content Type** and **Exclude URI** can be set on this screen as needed.
7. Click **OK**.

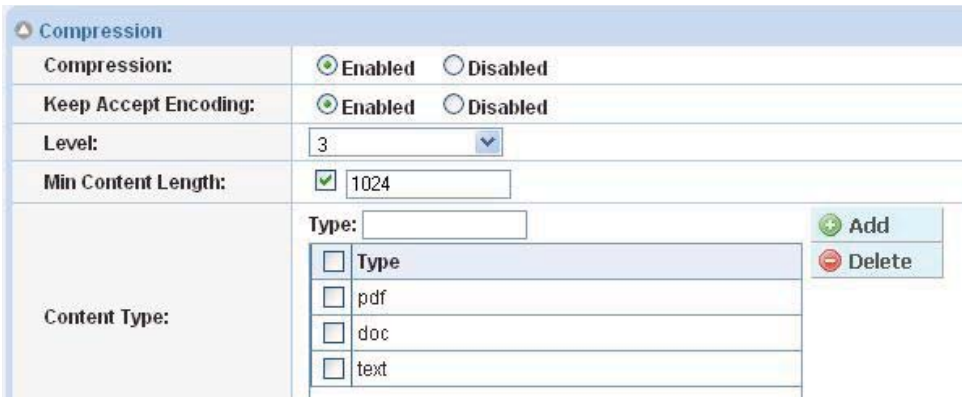

Figure 2.6.1 HTTP Template Configuration – Compression Option Content Types

Configure Cookie Persistence Template

Cookie persistence inserts a cookie in the HTTP header of a server reply before sending the reply to the client. The cookie ensures that subsequent requests from the client for the same virtual server and virtual port are directed to the same service group, real server, or real service port for a specified time configured in the expiration field below.

To configure Cookie Persistence:

1. Select **Config Mode > Service > Template**.
2. Select **Persistent > Cookie Persistence** from the drop down menu bar.
3. Click **Add** to create a new template.
4. In the **Name** field, type the name of the template. In this example, the name is *"SPS-Per_Cookie"*.
5. Check the **Expiration** box and in the field enter a time. We used the expiration time of "*604800*" seconds, which is seven days. The maximum configurable expiration is one year.
6. In the **Cookie Name** field type "*sps-cookie*".
7. Click **OK**. The template appears in the **Template > Cookie Persistence > List**.

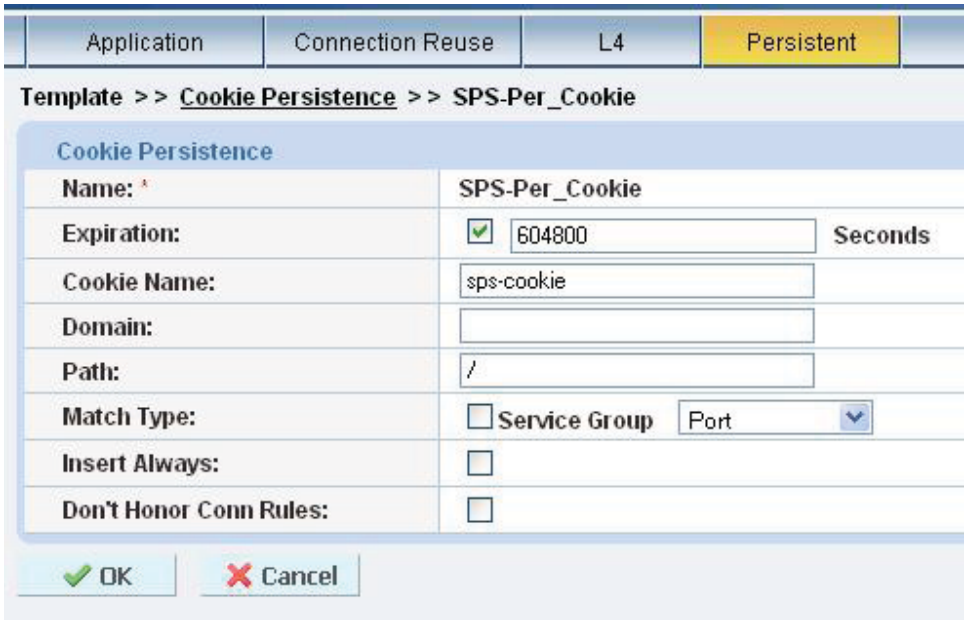

Figure 2.7 Cookie Persistence Configuration

Configure TCP-Proxy Template

TCP-proxy templates control TCP stack settings such as the idle timeout for TCP connections. Unless you need to change the setting for a TCP/IP stack parameter, you can use the default TCP-proxy template for the service type that uses it.

To configure a TCP-proxy template:

1. Select **Config Mode > Service > Template**.
2. Click **TCP Proxy** on the top menu bar.
3. Click **Add**.
4. In the **Name** field, enter a name for new template. In this example, the name is *"SPS-TCP-Proxy"*.
5. In the **Idle Timeout** field, the default value is 600 seconds. The defaults for this setting and the other settings are used in this example.
6. Click **OK**.

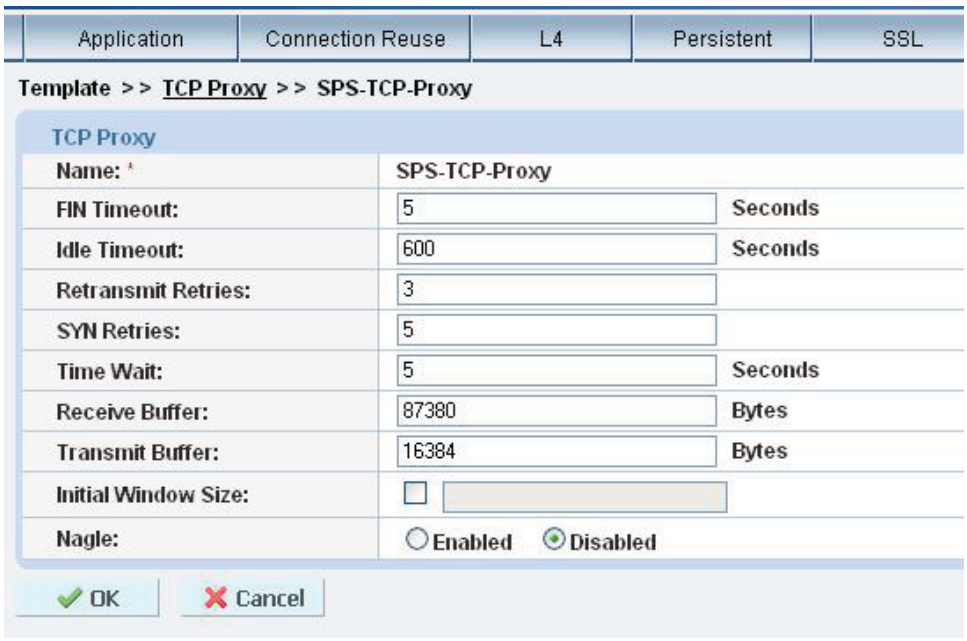

Figure 2.8 TCP Proxy Template Configuration

Configure RAM Caching Template

RAM Caching directly serves content that is cached on the AX and only sends requests to the web server for content that is not cached. RAM Caching can be used with compression on the same virtual port. In this case, compressed objects are cached and served to clients. The RAM Cache can store a variety of static and dynamic content and serve this content instantly and efficiently to a large number of users.

Caching of HTTP content reduces the number of web server transactions and hence the load on the servers. Caching of dynamic content reduces the latency and the computation cost of generating dynamic pages by application servers and database servers. Caching can also result in significant reduction in page download time and in bandwidth utilization.

RAM Caching is especially useful for high-demand objects on a website, for static content such as images, and when used in conjunction with compression to store compressed responses, eliminating unnecessary overhead.

RAM Caching is configured using a TCP-proxy template:

1. Select **Config Mode > Service > Template**.
2. On the top menu bar, select **Application** then **RAM Caching** from the drop down menu.
3. Click **Add** to create a new one.
4. Enter a **Name** for the template, if you are creating a new one. In this example name is *"SPS-RAM".*

5. Enter or change any settings for which you do not want to use the default settings. Here we changed **Age (aging) value** to *7200* seconds.
6. To configure dynamic caching polices, use the applicable set of steps below.
   To configure a cache policy use the **Policy** box:
   a. In the **URI** field, enter the portion of the URI string to match, which in this configuration is "*apps/docs/*".
   b. Select **Cache** from the **Action** drop-down list. The **Duration** field appears.
   c. By default, the content is cached for the number of seconds specified in the **Age** field of the **RAM Caching** box. To override the aging period, specify the number of seconds in the **Duration** field. We have used 3600 for this.
   d. Click **Add**.
7. Click **OK**.

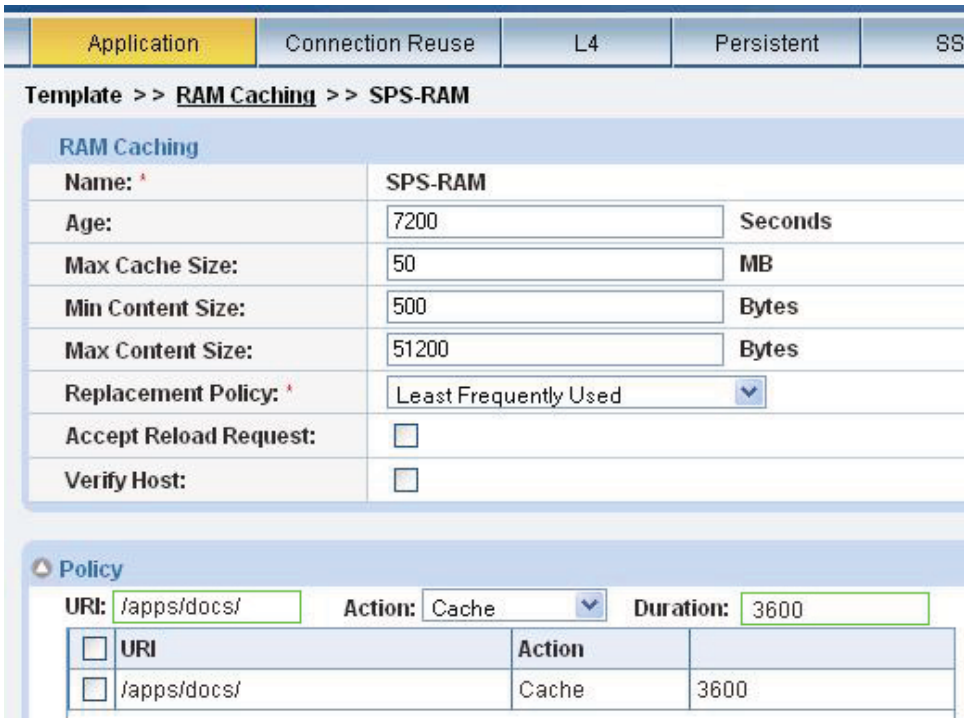

Figure 2.9 RAM Caching Configuration

Configure HTTP Virtual Server

When you configure a virtual server, you add a virtual service port to it for each of the load-balanced services. When adding a virtual service port, you specify the protocol port number for the port, and the service type. In this example, the service type is HTTP. Virtual port configuration also includes binding the service group and the templates to the port.

To configure a virtual server for the HTTP service:

1. Select **Config Mode > Service > SLB**.
2. Select **Virtual Server** on the top menu bar.
3. Click **Add**. The General box appears.
4. In the **Name** field, enter a name for the virtual server. In this example, the name is *"http-sps"*.
5. In the **IP Address** field, enter the IP address that clients will request. In this example, the address is *192.168.214.114*.

Figure 2.10 Virtual Server Configuration

6. In the **Port** box, click **Add**. The **SLB >> Virtual Server >> Port >> Create** screen appears.
7. In the **Type** drop-down list, select the service type. In this example, select "*HTTP*".
8. In the **Port** field, enter the service port number. In this example, it will automatically pre-populate with "*80*".
9. In the **Service Group** drop-down list, select the service group. In this example, select service group "*HTTP_SPS*".

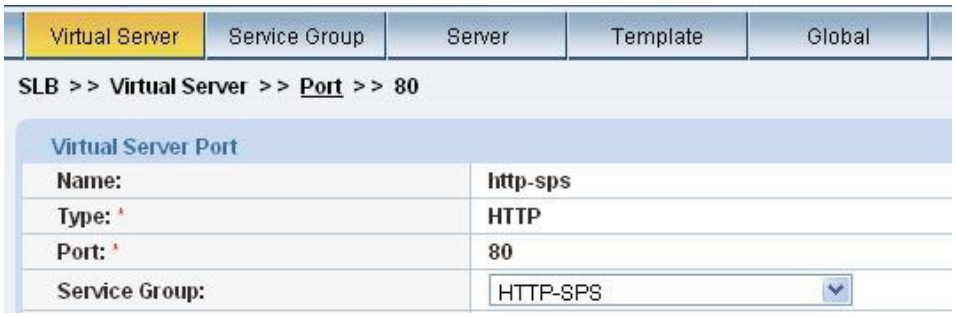

Figure 2.11 Virtual Server Port Configuration

10. The default **Virtual Server Port Template** is used for the service port, so leave "*default*" selected.
11. In the **Source NAT Pool** drop-down list, select the pool (in this example, "*SPS*").
12. In the **HTTP Template** drop-down list, select the HTTP (in this example, "*SPS-HTTP-Temp*").
13. In the **RAM Caching Template** drop-down list, select the RAM Caching template (in this example "*SPS-RAM*").
14. In the **TCP-Proxy Template** drop-down list, select the TCP-proxy template (in this example, "*SPS-TCP-Proxy*").
15. In the **Persistence Template Type** select **Cookie Persistence Template** from the drop-down list. The **Cookie Persistence Template** field appears below, from the drop down select the template. (in this example, "*SPS-Per_Cookie*").

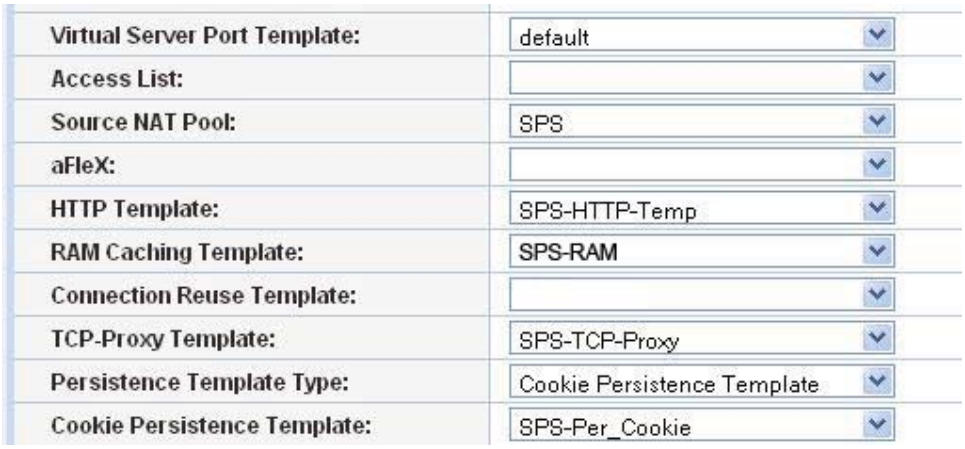

Figure 2.12 Virtual Server Port Configuration (Continuation)

16. Click **OK**. The port appears in the **Port** list of the **Port** box.

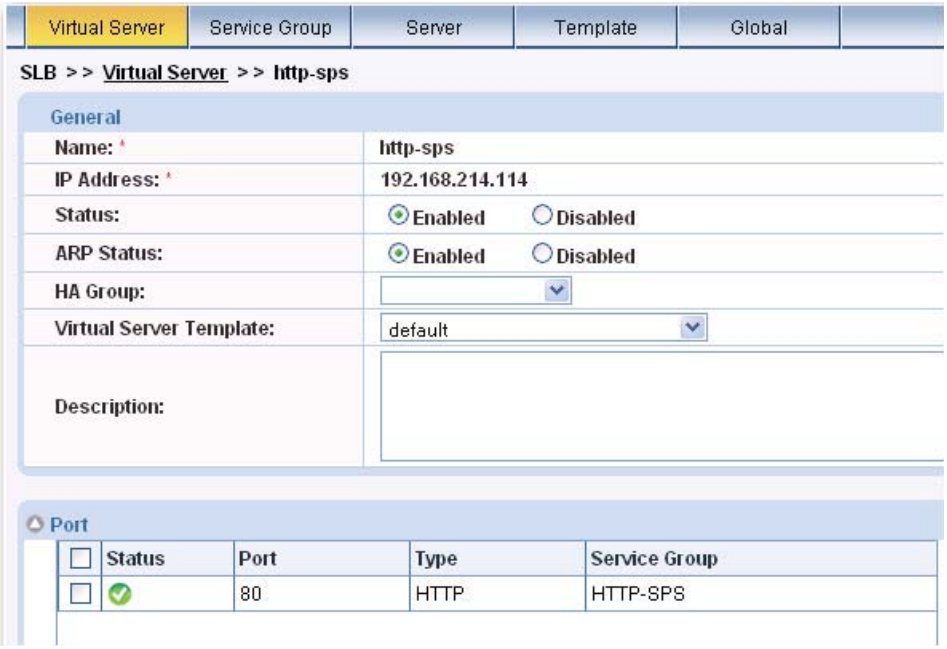

Figure 2.13 Virtual Server Port Configuration (Continuation)

17. Click **OK**. The virtual server appears in the virtual server table.
18. Click **Save** to save the configuration changes to the startup-config.

Note:

- As the configuration is hierarchical, you need to click the **OK** button up to the top level of configuration elements so that all the changes are always applied.
- **NOTE**: Connection Re-use option should not be selected for NTLM authentication.

Configuring the AX for SharePoint Server Using SSL

This section describes how to configure the AX device to load balance Microsoft SharePoint Servers using SSL to securely encrypt communication from the client to the AX. Utilizing SSL for encryption on the load balancer reduces web server CPU utilization and simplifies management with a single place to manage site certificates.

Configuration Steps

To configure the AX device to load balance SharePoint Servers over SSL, use the steps described in the previous section, but on the virtual server, use service type HTTPS instead of HTTP.

Before configuring the virtual server, the following additional steps also are required:

- Configure or import SSL certificate.
- Configure SSL server template.

Configure SSL Certificate

You can import or create certificates for SSL clients. In this example, a certificate and key are created.

1. Select **Config Mode > Service > SSL Management**.
2. Click **Create**. The **SSL Management >> Certificate >> Create** screen appears.
3. In the **File Name** field, type the name for the SSL certificate. In this example, the name is "*SPS-SSL-Cert*".
4. In the **Certificate** box Issuer drop-down list, use the default option of **Self**.
   In the **Common Name** field, enter a name for the certificate (in this example, "*sps-ssl-cert*").
5. Fill in any additional required data (recommended, see Figure 3.1 below). In the Key box select the **Key Size**. The default is *1024* bits.
6. Click **OK**.

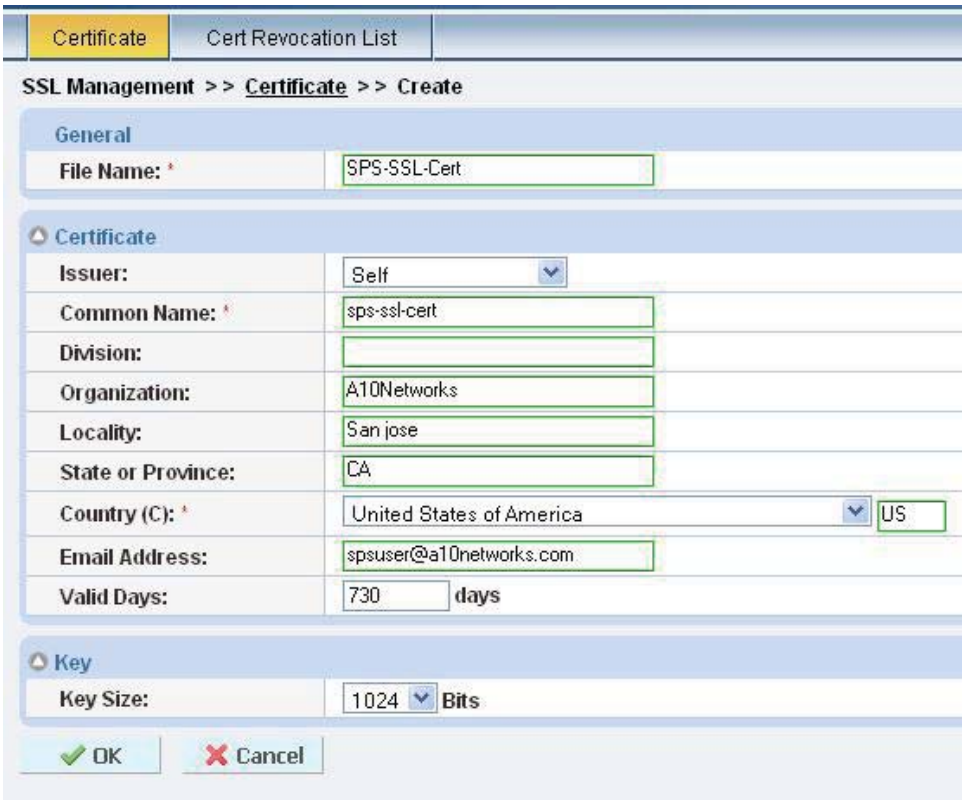

Figure 3.1 SSL Certificate Configuration

Configure SSL Server Template

In this step, a SSL server template is configured for the real server.

To configure a Server SSL template:

1. Select **Config Mode > Service > Template**.
2. Select **SSL > Server SSL** from the menu bar and drop down.
3. Click **Add**. The **Template >> Server SSL >> Create** screen appears.
4. In the **Name** field, enter a name for the template. In this example, the name is "*sps-server*".
5. In the **CA Cert Name** drop-down list, select the certificate configured above "*sps-ssl-cert*".
6. Click **OK**. The new template appears in the Server SSL template table.

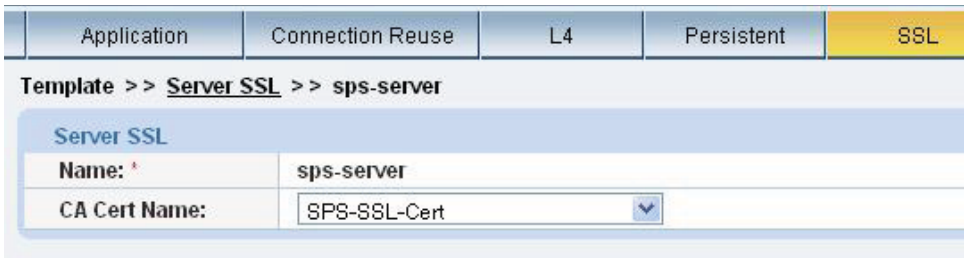

Figure 3.2 Server SSL Template Configuration

Configure SSL Client Template

In this step, a SSL client template is configured for the HTTPS virtual server. The SSL certificate and key configured in the previous step are used here. Later, during configuration of the virtual server, the template will be bound to the HTTPS virtual service port.

To configure a client SSL template:

1. Select **Config Mode > Service > Template**.
2. Select **SSL > Client SSL** from the top menu bar and drop down.
3. Click **Add**. The **Template >> Client SSL >> Create** screen appears.
4. In the **Name** field, enter a name for the template. In this example, the name is "*sps-ssl-temp*".
5. In the **Certificate Name** drop-down list, select the certificate configured above. In this example, the name is also "*sps-ssl-cert*".
6. In the **Key Name** field, select the key configured above. In this example, the name is also "*sps-ssl-cert*".
7. Click **OK**. The new template appears in the Client SSL template list.

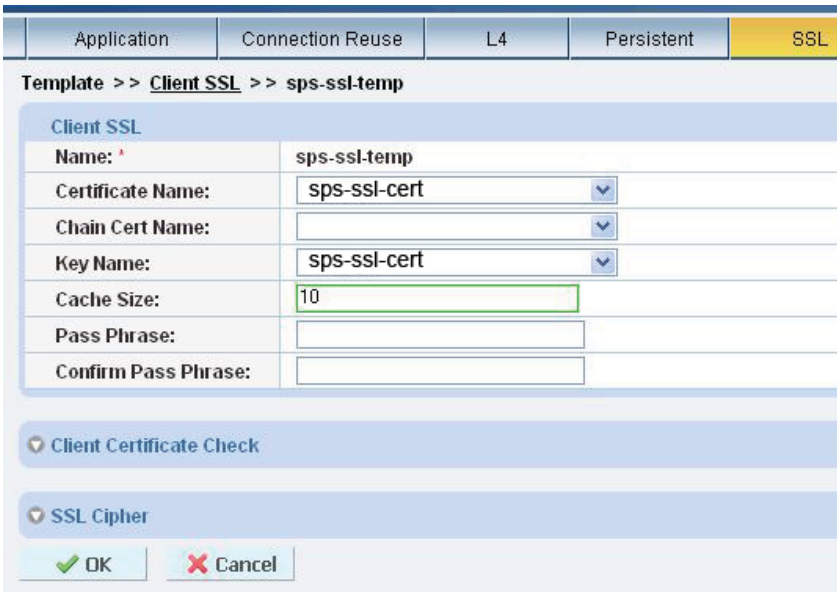

Figure 3.3 Client SSL Template Configuration

Configure HTTPS Virtual Server

In this step, a virtual server with a SSL virtual service port is configured.

1. Select **Config Mode > Service > SLB**.
2. Select **Virtual Serve**r on the top menu bar.
3. Click **Add**. The **SLB >> Virtual Server >> Create** screen appears.
4. In the **Name** field, enter a name for the virtual server. In this example, the name is "*https-sps*".
5. In the **IP Address** field, enter the IP address that clients will request. In this example, the IP address is "*192.168.214.115*".

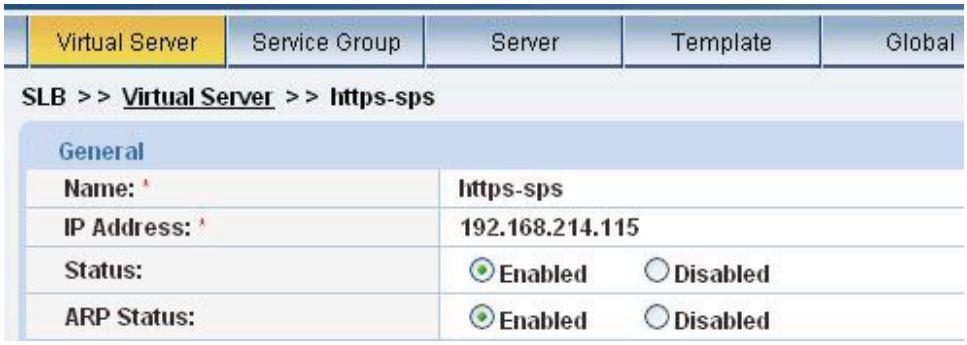

Figure 3.4 HTTPS Virtual Server Configuration

6. In the **Port** box, click Add. The **SLB >> Virtual Server >> Port >> Create** screen appears.
7. In the **Type** drop-down list, select the service type. In this example, select "*HTTPS*".
8. In the **Port** field, the service port number defaults to **443**.
9. In the **Service Group** drop-down list, select the service group (in this example, "*HTTP-SPS*").

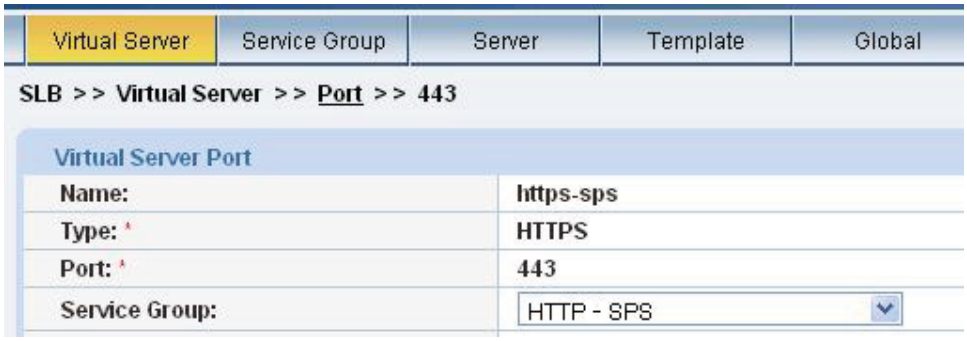

Figure 3.5 HTTPS Virtual Server Port Configuration

10. In the **Source NAT Pool** drop-down list, select the pool configured above (in this example, "*SPS*").
11. In the **HTTP Template** drop-down list, select the HTTP configured above (in this example, "*SPS-HTTP-Temp*").

12. In the **RAM Caching Template** drop-down list, select the RAM Caching template configured above (in this example "*SPS-RAM*").
13. In the **Client-SSL Template** drop-down list, select the configured client-SSL template configured above (in his example, "*sps-ssl-cert*").
14. In the **Server-SSL Template** drop-down list, select the configured server-SSL template (in this example, "*sps-server*").
15. In the **TCP-Proxy Template** field, select the "SPS-TCP-Proxy" template configured above.
16. In the **Persistence Template Type** field select Cookie Persistence Template drop-down list, then in the **Cookie Persistence Template** field below select the cookie-persistence template (in this example, *SPS-Per_Cookie*).

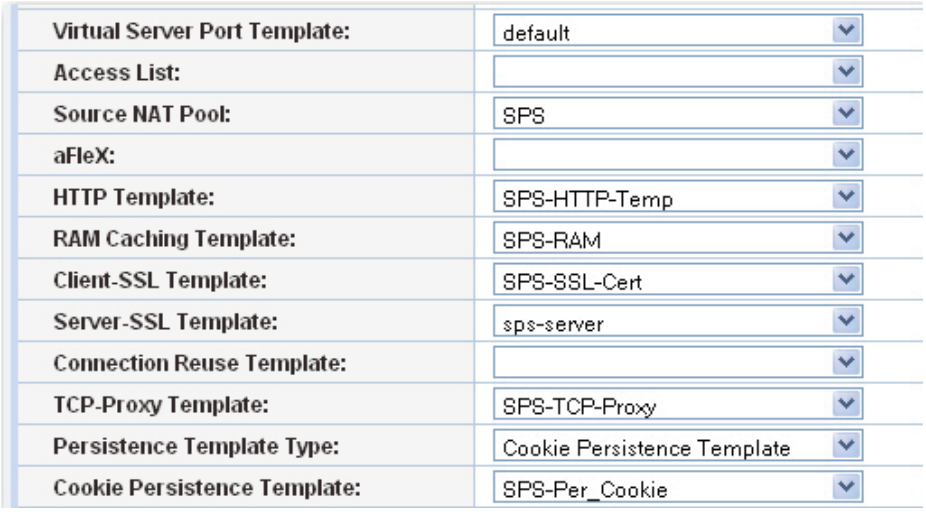

Figure 3.6 HTTPS Virtual Server Port Configuration (Continuation)

17. Click **OK**. The port appears in the **Port** box list.
18. Click **OK**.
19. Click **Save** to save the configuration changes to the startup-config.

Summary and Conclusion

The configuration steps described above show how to set up the AX device for Microsoft SharePoint Servers. By using the AX device to load balance SharePoint, the following key advantages can be achieved:

- Transparent SharePoint application load sharing
  - Multiple SharePoint Servers can be pooled together without any changes to how users access the applications.
- Availability of SharePoint applications
  - Obtain higher availability when SharePoint Servers fail so that there is no direct impact to how users access the applications.
- Performance of SharePoint applications
  - Achieve higher connection throughput and faster end user responsiveness by acceleration techniques and offloading security processing to the AX device.
  - Please visit www.a10networks.com for third party performance reports detailing performance benefits.

The AX Series Advanced Traffic Manager provides significant benefits for all users of Microsoft SharePoint applications. For more information about AX Series products, refer to:

http://a10networks.com/products/axseries.php
http://a10networks.com/resources/solutionsheets.php
http://a10networks.com/resources/casestudies.php

About A10 Networks

A10 Networks was founded in 2004 with a mission to provide innovative networking and security solutions. A10 Networks makes high-performance products that help organizations accelerate, optimize and secure their applications. A10 Networks is headquartered in Silicon Valley with offices in the United States, Europe, Japan, China, Korea and Taiwan. For more information, visit www.a10networks.com.

Performance by Design

To learn more about the AX Series Advanced Traffic Manager and how to improve application performance up to 8 times faster while enhancing reliability and security, visit A10 Networks' website at:
www.a10networks.com
Or call and talk to an A10 sales representative:

Corporate Headquarters

A10 Networks, Inc.
2309 Bering Drive
San Jose, CA 95131
Tel: +1 408 325-8668
Fax: +1 408 325-8666

North America Sales:
+1 888 A10-6363
+1 408 325-8616

Europe, Middle East & Africa Sales:
+31 70 799-9143

Asia Pacific Sales:

China, Beijing Office:
+86 10 8515-0698

China, Shanghai Office:
+86 21 6137-7850

Japan Sales:
+81-3-3291-0091

Korea Office:
+82-2-6007-2150
+82-2-6007-2151

Taiwan Office:
+886-2-2657-3198