



■ Deployment Guide

AX Series for SharePoint 2010



TABLE OF CONTENTS

1 Introduction 5

2 Deployment Guide Overview 5

3 Deployment Guide Prerequisites 6

4 AX Deployment for SharePoint 2010 Server Roles 7

5 Accessing the AX Series Load Balancer 7

6 SharePoint 2010 Recommended Installation Procedures 8

7 Architecture Overview 9

8 Basic AX Configuration For SharePoint 10

 8.1 Server Configuration 11

 8.2 Health Monitor Configuration 12

 8.3 Service Group Configuration 13

 8.4 Virtual Server Configuration 15

 8.5 Source IP Persistence 17

 8.5.1 Create IP Persistence Template 17

 8.5.2 Apply IP Persistence to the VIP 18

 8.6 IP Source NAT 18

 8.6.1 Create IP Source NAT Template 19

 8.6.2 Apply IP Source NAT to the VIP 20

 8.7 Validate Service 21

9 Advanced AX Features for SharePoint 22

 9.1 Preparing the Configuration 22

 9.1.1 Import existing SharePoint webserver SSL cert or create self-signed CA from the AX 22

 9.1.2 Create one client and one server SSL template 26

- 9.1.3 On the virtual server, change the service type of the virtual port from “TCP” to “HTTPS” and apply the new client and server SSL template 27
- 9.2 SSL Offload 29
 - 9.2.1 Change the Port Numbers in the Service Group 30
 - 9.2.2 On the Virtual Server, remove the Server SSL Template 30
 - 9.2.3 Validate the Deployment 31
- 9.3 Compression 32
 - 9.3.1 Create HTTP Compression Template 32
 - 9.3.2 Apply HTTP Compression Template to VIP 34
 - 9.3.3 Validate the Deployment 35
- 9.4 Cookie Persistence 35
 - 9.4.1 Create Cookie Persistence Template 35
 - 9.4.2 Apply Cookie Persistence Template to VIP 36
 - 9.4.3 Validating the Deployment 37
- 9.5 Connection Reuse (TCP Offload) 37
 - 9.5.1 Create Connection Reuse Template 38
 - 9.5.2 Create an IP Source NAT template 38
 - 9.5.3 Apply Connection Reuse and SNAT to VIP 39
 - 9.5.4 Validate the Deployment 40
- 9.6 RAM Caching 40
 - 9.6.1 Create RAM Caching Template 41
 - 9.6.2 Apply RAM Caching Template on VIP 42
 - 9.6.3 Validate the Deployment 42
- 9.7 Securing SharePoint via aFleX 43
 - 9.7.1 Create aFleX Script 43
 - 9.7.2 Configure VIP with HTTP/Port 80 45

9.7.3	Apply AFLEX Script to VIP	45
9.7.4	Validate AFLEX Service	46
10	Summary and Conclusion	47
11	Appendix	48
11.1	AX Series CLI sample configurations:	48

1 INTRODUCTION

Microsoft SharePoint 2010 is the latest web application platform developed by [Microsoft](#) for small to large businesses. Microsoft SharePoint 2010 is designed as a centralized collaboration, content, and file management application software. SharePoint provides many features for clients, such as support for audio, video, and Silverlight applications, making it easy for users to build dynamic web sites. SharePoint 2010 also offers the new ribbon user interface that makes SharePoint easier to deploy, manage and customize. In addition, SharePoint now offers easy-to-deploy templates that range from wikis to workflows. SharePoint is a very scalable solution that can support thousands of customers and it can be deployed in a multi-server environment. The AX Series Application Delivery Controllers (ADCs) provide advanced load balancing services for Microsoft SharePoint 2010.

2 DEPLOYMENT GUIDE OVERVIEW

This document shows how an A10 Networks AX Series device can be deployed with Microsoft SharePoint 2010. The tested solution is based on an AX Series device load balancing two (2) SharePoint Web Front End (WFE) servers. The WFE servers will be referred to as web servers (WS) in the next chapters. Refer to Table 1: AX Deployment for SharePoint 2010 Server Roles, for the details of the server roles within the deployment guide.

The deployment guide is divided into two sections namely: Basic AX configuration and Advanced AX configuration for SharePoint. The Basic AX configuration is a bare minimum configuration that can be used in a SharePoint deployment. To transition configuration from Basic to Advanced there are required configuration to be change. Please refer to the configuration changes required in **Error! Reference source not found.**

This deployment document does not apply to Microsoft SharePoint 2003 or 2007 Servers. This deployment guide only applies to Microsoft SharePoint 2010 installations.

3 DEPLOYMENT GUIDE PREREQUISITES

AX Series Requirements

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

Microsoft SharePoint Requirements

- The Microsoft SharePoint 2010 application was tested and deployed for internal and external users to access the SharePoint service.
- Microsoft SQL Server 2008 R2 is required.
- All Microsoft SharePoint 2010 Server Components are running on Windows 2008 (64-bit) Enterprise Edition Server Operating System.

The deployment guide was tested based on:

- AX Release: 2.6.1
- Clients OS: 64-bit Windows 7 Operating System.
- Client browsers:
 - ◆ Microsoft Internet Explorer Version 8.0
 - ◆ Google Chrome Version 10.0
 - ◆ Mozilla Firefox Version 4.0.1

Note: *If the Virtual IP (VIP) is accessed from an external client, the network topology needs to be deployed on a routed mode. If the SharePoint services are accessed internally, the network has to be deployed on a one-arm mode. If the SharePoint servers are accessed from internal and external clients, the network topology has to be deployed in one-arm mode configuration.*

Note: *For additional deployment modes that the AX Series device can support, please visit the following URL: <http://www.a10networks.com/products/axseries-load-balancing101.php>*

4 AX DEPLOYMENT FOR SHAREPOINT 2010 SERVER ROLES

Figure 1: Provides server description for the test environment:

Server Roles	Role
Web server	This server also known as a Web Front-End server (WFE) hosts all Web pages, Web Parts, and Web services used when your server farm receives a request for processing.
Application server	This server hosts the service applications running in the farm, such as Visio, and Excel Services.
Database server	This server stores most of the data associated with a SharePoint 2010 implementation including configuration settings, administration information, data associated with the service applications, and user content.
Query server	This is an application server feature that is responsible for querying the index, finding the matching content, and then sending the content back to the Web servers for presentation to users.
Crawl server	This is an application server feature that is responsible for accessing and cataloging content sources which then propagate the results to the query servers. The crawl server uses a crawl database to store the URLs of all sources crawled.

Figure 1: SharePoint Server Role Matrix

5 ACCESSING THE AX SERIES LOAD BALANCER

This section describes how to access the AX Series device. The AX 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.

Access information:

- Default Username: “admin”
- Default password is “a10”.
- Default IP Address of the device is “172.31.31.31”

For detailed information how to access the AX Series device, refer to document “A10 Networks AX Series System Configuration and Administration Guide.pdf”

6 SHAREPOINT 2010 RECOMMENDED INSTALLATION PROCEDURES

1. Prepare a list of servers that will be deployed in the topology. The required servers for SharePoint are Application Server (AS), Web Front End (WFE), Database Server (DB), indexing/search server, Active Directory (AD)/Domain Name Servers (DNS) server and optional Network Access Storage (NAS).
2. Install base Windows OS (Windows 2010 64-bit) and install required software prerequisites. Install SQL database and provision a SQL Admin account with the permission level needed to create a database for SharePoint 2010 server.
3. Active Directory (AD) and DNS servers are required for network management and user provisioning.
4. Install SharePoint 2010 server and configure the services based on server roles. This can be done via the SharePoint Web Management GUI.
5. Configure an Alternate Access Mapping (AAM) on the web servers.

Note: For additional information on how to configure AAM refer to:

[http://technet.microsoft.com/en-us/library/cc263208\(office.12\).aspx](http://technet.microsoft.com/en-us/library/cc263208(office.12).aspx)

6. Test the SharePoint site to verify that it is accessible, and then deploy the AX Series device.

Note: If you have an existing SharePoint 2010 Server already installed, you can skip the SharePoint 2010 recommended installation procedure above.

7 ARCHITECTURE OVERVIEW

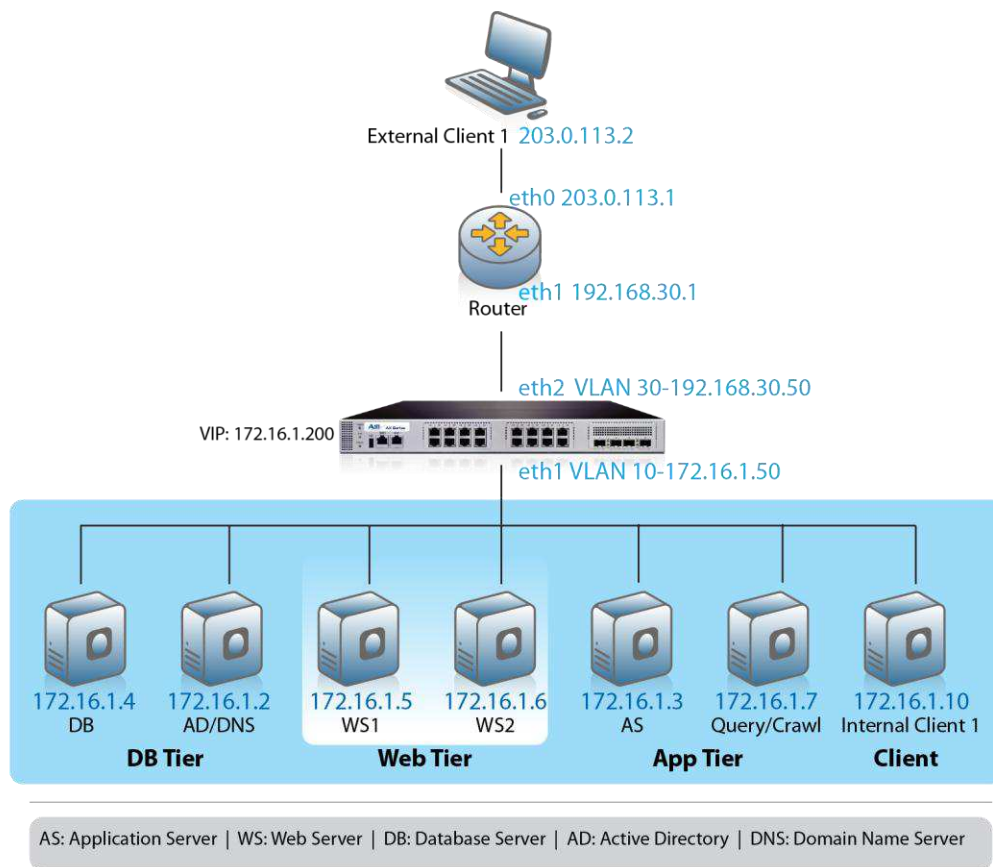


Figure 2: SharePoint 2010 Deployment Topology

8 BASIC AX CONFIGURATION FOR SHAREPOINT

This chapter explains how the AX Series is configured with Microsoft SharePoint 2010 server implementation. This chapter provides instructions for installing the real servers, service group, virtual services, and virtual servers in a basic Microsoft SharePoint configuration with no optimization.

Basic SharePoint Configuration



Figure 3: Basic SharePoint Configuration

The simplest configuration uses the AX series device to load balance SharePoint traffic using a secured HTTPS connection. The WFE are the only servers that are load balanced by the AX. This is because Microsoft SharePoint 2010 has its own built-in redundancy and load balancing mechanism on the backend servers. For detailed information explaining why Applications Servers (AS) and other SharePoint components cannot be load balanced with any load balancer, refer to the following URLs:

<http://social.technet.microsoft.com/Forums/en-CA/sharepoint2010setup/thread/f3ae16b1-8a3b-4ffa-a2e0-e78a48889c71>

<http://blogs.msdn.com/b/spses/archive/2010/01/20/sharepoint-2010-shared-service-architecture-part-1.aspx>

8.1 SERVER CONFIGURATION

This section demonstrates how to configure the SharePoint webservers in the AX Series.

1. Navigate to **Config Mode > SLB > Server**.
2. Click **Add** to add a new server.
3. Within the Server section, enter the following required information.
4. Name: **“WS1”**
5. IP address /Host: **172.16.1.5**

Note: Enter additional servers if necessary.

The screenshot shows the configuration page for a new server in the SLB (Server Load Balancing) section. The page title is "SLB >> Server >> Create". The "General" tab is active. The following fields are visible:

Name: *	WS1
IP Address/Host: *	172.16.1.5 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default)
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume:	
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:	

Figure 4: Real Server Configuration

6. In the **Port** section, enter **Port** and **Protocol** type, then click **Add**.

Port

Port: * 443 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"/>	443	TCP	8000000	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	default	(default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Add, Update, Delete, Enable, Disable

Figure 5: Real Server Port Configuration

7. Click **OK** and then click **Save** to store your configuration changes.

8.2 HEALTH MONITOR CONFIGURATION

The AX series automatically initiate the health status checks of real servers (ICMP) and service ports (TCP Health Check). This provides clients assurance that all request go to functional and available servers. If a server or a port does not respond appropriately to a health check, the server will be temporarily removed from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server will be automatically added back to the list of available servers.

For higher availability Microsoft recommends the test IIS servers with a real http “GET” request.

1. Navigate to **Config Mode > SLB > Server Port > Health Monitor**.
2. Click **Add**.
3. For the health monitor **Name**, enter “**SharePoint HC**”.
4. For the **Type**, select “**HTTP**”.
5. Click **OK** and then continue with the Service Group configuration.

Health Monitor		
Name: *	SharePoint HC	
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:	HTTP
Port:	80
Host:	
URL:	GET /
User:	
Password:	
Expect:	<input type="radio"/> Text <input type="radio"/> Code
Maintenance Code:	

Figure 6: Health Monitor Configuration

8.3 SERVICE GROUP CONFIGURATION

This section demonstrates how to configure the SharePoint webservers in a 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 supports multiple SharePoint real servers as one logical server.

1. Navigate to **Config Mode > SLB > Service Group**.
2. Click **Add** to add a new service group.
3. Within the **Server Group** section, enter the following required information:
 - ◆ Name: Enter "**SharePoint Servers**".
 - ◆ Type: Select "**TCP**" from the drop-down menu.
 - ◆ Algorithm: Select "**Round Robin**" from the drop-down menu.
 - ◆ Health Monitor: Select "**SharePoint HC**" from the drop-down menu.

Service Group	
Name: *	SharePoint Servers
Type:	TCP
Algorithm:	Round Robin
Health Monitor:	SharePoint HC
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 7: Service Group Configuration

4. Navigate to **Config Mode > Service > SLB > Service Group**.
5. In the **Server** section of the window, add one or more servers from the server drop-down list:
 - ◆ Server: Select **“WS1”** from the drop-down menu.
 - ◆ Port: Enter **“443”**.
6. Click **Add** and enter all the available SharePoint web servers.

Figure 8 shows that the server names "WS1" and "WS2" are entered, each with port 443.

Server

IPv4/IPv6: IPv4 IPv6

Server: * WS2 Port: * 443

Server Port Template(SPT): default Priority: 1

Stats Data: Enabled Disabled

<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data
<input checked="" type="checkbox"/>	WS1	443	default	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	WS2	443	default	1	<input checked="" type="checkbox"/>

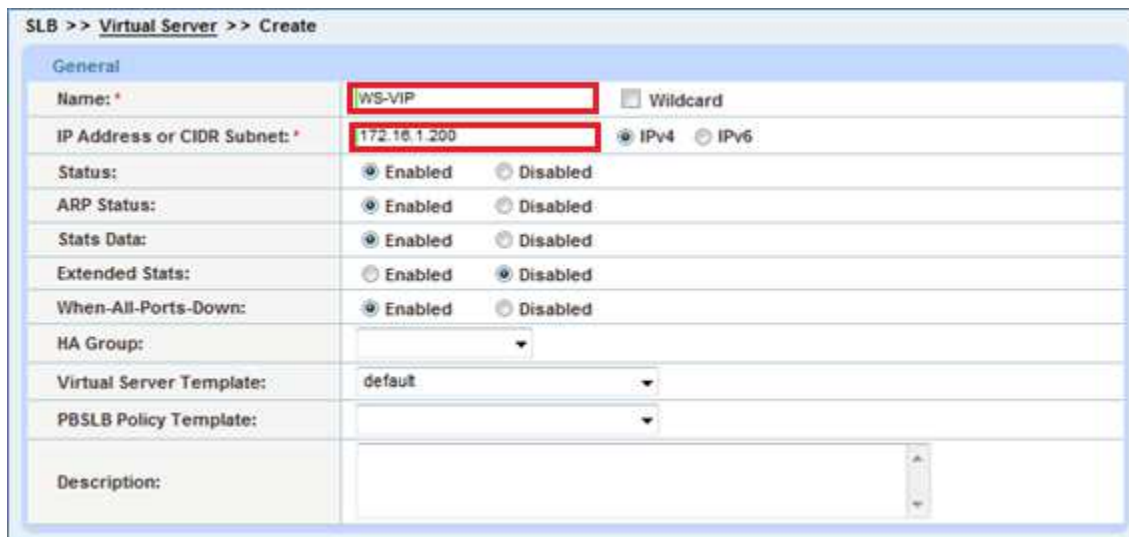
Figure 8: Service Group Server Configuration

7. Click **OK** and then click **Save** to store your configuration changes.

8.4 VIRTUAL SERVER CONFIGURATION

This section demonstrates how to configure the VIP with the AX Series. Adding the virtual server ports within the AX Series will generate a virtual service list based on the protocol type selected.

1. Navigate to **Config Mode > SLB > Virtual Server > General**.
2. Within the **General** section, enter the following required information:
 - ◆ Name: **“WS-VIP”**
 - ◆ IP Address or CIDR Subnet: *172.16.1.200*



The screenshot shows the configuration page for a Virtual Server in the SLB (Server Load Balancing) section. The page title is "SLB >> Virtual Server >> Create". The "General" tab is selected. The form contains the following fields and options:

Name:	WS-VIP	<input type="checkbox"/> Wildcard
IP Address or CIDR Subnet:	172.16.1.200	<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	
HA Group:	▼	
Virtual Server Template:	default ▼	
PBSLB Policy Template:	▼	
Description:		

Figure 9: Virtual Server or VIP Configuration

3. Navigate to **Config Mode > SLB > Virtual Server > Port**.
4. Click **Add**.
5. Enter the **Virtual Server Port** information:
 - ◆ Type: from the drop-down menu, select **“TCP”**.
 - ◆ Port: **“443”**
 - ◆ Service Group: From the drop-down menu, select **“SharePoint Servers”** to bind the virtual server to the real servers.

Virtual Server:	WS-VIP
Type: *	TCP
Port: *	443
Service Group:	SharePoint Servers

Figure 10: Virtual Server Port Configuration

Port					+ Add
<input type="checkbox"/>	Status	Port	Type	Service Group	Edit
<input type="checkbox"/>	✓	443	TCP	SharePoint Servers	- Delete
					✓ Enable
					✗ Disable

Figure 11: Virtual Port Lists

<input type="checkbox"/>	Name	Type	Port	IP Address or CIDR Subnet
<input type="checkbox"/>	_172.16.1.200_TCP_443	TCP	443	172.16.1.200

Select All Unselect All

Figure 12: Virtual Services Overview

- Click **OK** and then click **Save** to store your configuration changes.

8.5 SOURCE IP PERSISTENCE

The AX series can support different modes of persistence; such as Cookie persistence, Destination IP persistence, Source IP persistence, and SSL session ID persistence. The purpose of persistence is to direct traffic from the same client to the same server.

This deployment guide focuses on Source IP Persistence in the basic SharePoint configuration. Cookie persistence configuration will be featured within the Advanced SharePoint section.

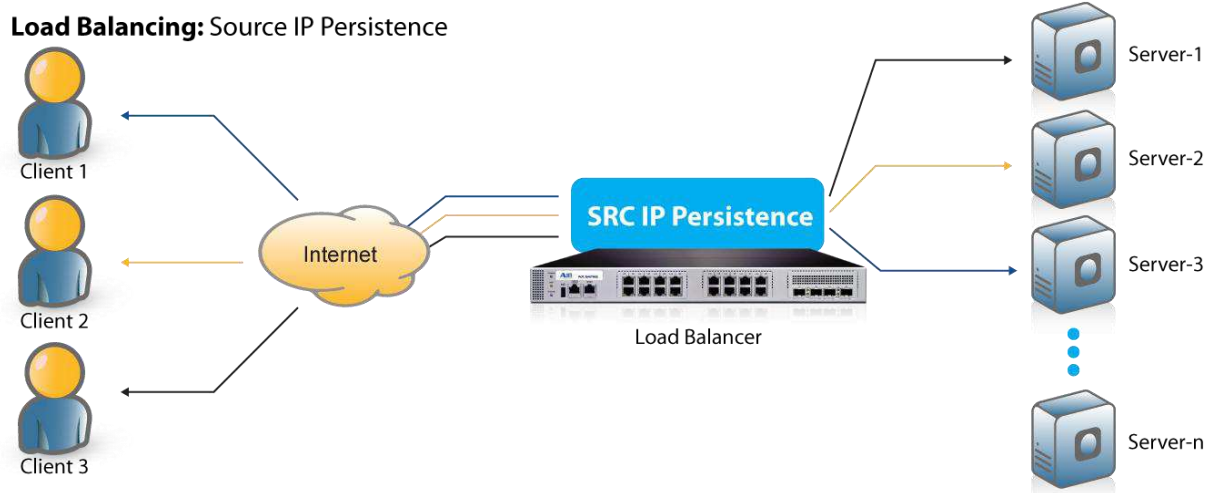


Figure 13: Source IP Persistence

8.5.1 CREATE IP PERSISTENCE TEMPLATE

1. Navigate to **Config Mode > Template > Persistent > Source IP Persistence**.
2. Click **Add**.
3. Enter the Source IP Persistence name.
Example: **"Source IP Persistence"**
4. Click the Match Type drop-down menu and select **"Port"**.
5. Leave the **Timeout** set to 5 minutes (Default).

Source IP Persistence	
Name:	Source IP Persistence
Match Type:	Port
Timeout:	5 Minutes
Don't Honor Conn Rules:	<input type="checkbox"/>
Netmask:	255.255.255.255

Figure 14: Source IP Persistence Overview

- Click **OK** and then click **Save** to store your configuration changes.

8.5.2 APPLY IP PERSISTENCE TO THE VIP

To assign the template to the VIP:

- Navigate to **Config Mode > Service > SLB > Virtual Server Port**.
- From the **Persistence Template Type** drop-down menu, select **Source IP Persistence Template**.
- Select the corresponding template that was created. The name “Source IP Persistence” is used as the template name in the example below.

Persistence Template Type:	Source IP Persistence Template
Source IP Persistence Template:	Source IP Persistence

Figure 15: Persistence Template Configuration

- Click **OK** and then click **Save** to store your configuration changes.

8.6 IP SOURCE NAT

Optional: Only for one-arm deployment.

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: 172.16.1.200), the client requests are “source NAT-ed”, which means that the AX replaces the client’s source IP address based on the configured address pool of the source NAT. 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. The Source NAT template must be applied in the virtual server port for the NAT to take effect.

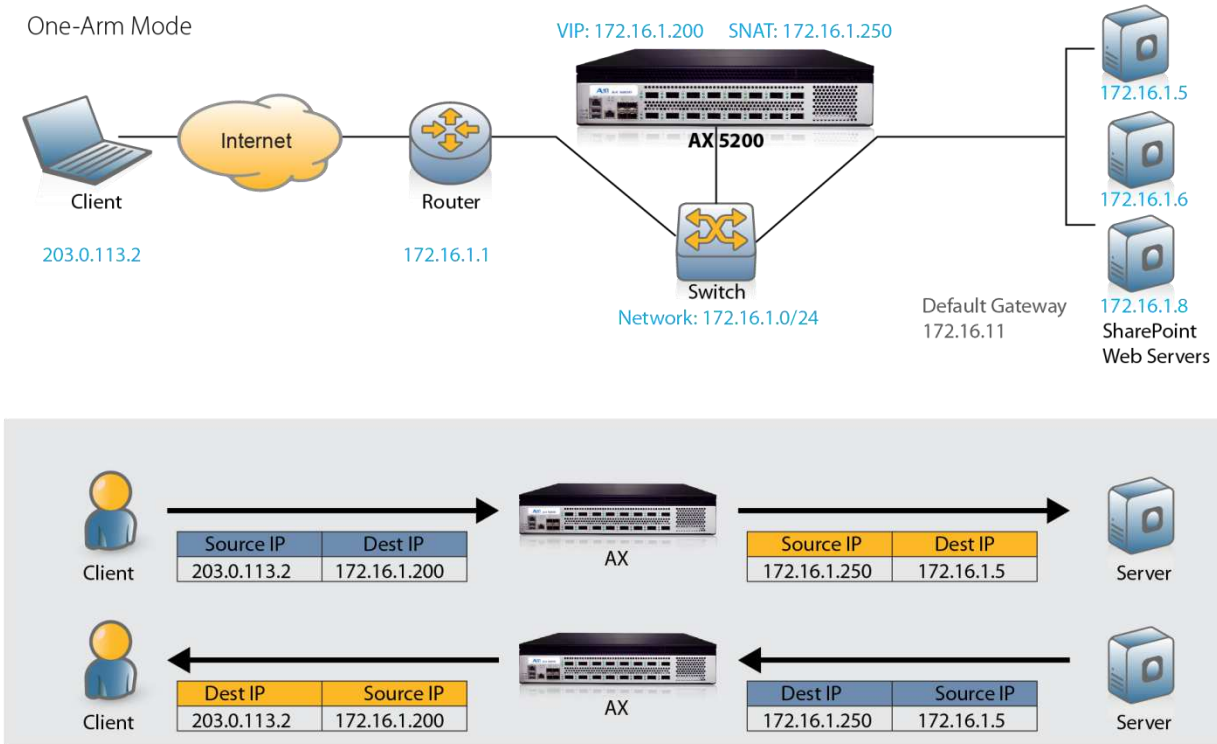


Figure 16: IP Source NAT and traffic flow overview

8.6.1 CREATE IP SOURCE NAT TEMPLATE

1. Navigate to **Config Mode >Service> IP Source NAT**.
2. Click **Add**.
3. Enter IP Source NAT **Name**: "SNAT".
4. Enter **Start IP Address**: 172.16.1.250 (Example)
5. Enter **End IP Address**: 172.16.1.250 (Example)
6. Enter **Netmask**: 255.255.255.0

IPv4 Pool	
Name: *	SNAT
Start IP Address: *	172.16.1.250
End IP Address: *	172.16.1.250
Netmask: *	255.255.255.0
Gateway:	
HA Group:	

Figure 17: IP Source NAT Configuration

7. Click **OK** and then click **Save** to store your configuration changes.

Note: Apply the SNAT template to the Virtual Server Port. If the SharePoint environment will consist of many concurrent users, it is advisable to configure multiple SNAT IP addresses. One IP address can be used for up to 64,000 flows.

8.6.2 APPLY IP SOURCE NAT TO THE VIP

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. Select the **Virtual Server** name “**WS-VIP**”.
3. Select port “**443**” and click **Edit**.
4. From the **Source NAT Pool** drop-down list, select the “**SNAT**” template.


Access List:	
Source NAT Pool:	SNAT

Figure 18: SNAT Binding

5. Click **OK** and then click **Save** to store your configuration changes.

8.7 VALIDATE SERVICE

To validate that the basic configuration is functioning correctly, do the following:

1. Navigate to **Monitor Mode > Service > SLB > Virtual Server**.
2. Check that the **Status** states is green: 









Name	Connections	Connections	
		Current	Total
 WS-VIP/172.16.1.200		0	320
 TCP/443		0	320
 443 (WS1)		0	176
 443 (WS2)		0	176

Figure 19: Virtual Server status

3. Launch one of the approved web browsers from the lists above and navigate to the VIP address. For example, 172.16.1.200 = www.example.com.

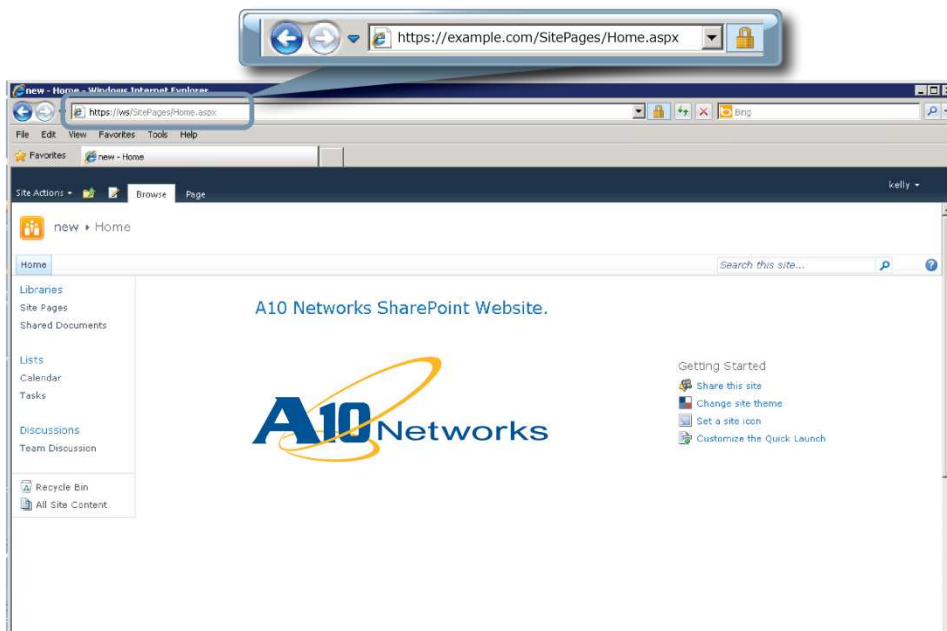


Figure 20: Connection to the Load-Balanced SharePoint Site

9 ADVANCED AX FEATURES FOR SHAREPOINT

This section describes advanced traffic optimization features you can add to your basic SharePoint configuration. These features provide web application acceleration, optimize SharePoint web server performance, and increase scalability.

- SSL Offload
- HTTP/HTTPS Compression
- Cookie Persistence
- Connection Reuse
- RAM Caching

9.1 PREPARING THE CONFIGURATION

To configure any of these advanced features, a few changes to the basic configuration are required:

- Import existing SharePoint webserver SSL cert or create self-signed CA from the AX.
- Create one client and one server SSL template
- On the virtual server, change the service type of the virtual port from “TCP” to “HTTPS” and apply the new client and server SSL template

9.1.1 IMPORT EXISTING SHAREPOINT WEBSERVER SSL CERT OR CREATE SELF-SIGNED CA FROM THE AX

There are two options to configure when installing an SSL template from the AX Series either:

- **Option 1:** Generate a Self-Signed CA from the AX: Self-signed CA is generated from the AX Series.
- **Option 2:** Import an SSL Certificate and Key: Export existing CA certificate from SharePoint webserver and import to AX Series device.

9.1.1.1 OPTION 1: GENERATE A SELF-SIGNED CA FROM THE AX

1. Navigate to **Config Mode > SSL Management > Certificate**.
2. Click **Create** to add a new SSL certificate.
3. Enter the File Name of the certificate: **"WS"**.
4. From the Issuer drop-down menu, select **Self** from the from the drop-down menu, and then enter the following values:
 - ◆ Common Name: **"SharePoint.example.com"**
 - ◆ Division: **"A10"**
 - ◆ Organization: **"A10"**
 - ◆ Locality: **San Jose**
 - ◆ State or Province: **"CA"**
 - ◆ Country: **"USA"**
 - ◆ Email Address: **"spadmin@example.com"**
 - ◆ Valid Days: **"730"** (Default)
 - ◆ Key Size (Bits): **"2048"**

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

5. Click **OK** and then click **Save** to store your configuration changes.

General	
File Name: *	WS

Certificate	
Issuer:	Self
Common Name: *	SharePoint.example.com
Division:	A10
Organization:	A10
Locality:	San Jose
State or Province:	CA
Country (C): *	United States of America
	US
Email Address:	spadmin@example.com
Valid Days:	730 days

Key	
Key Size:	2048 Bits

Figure 21: Client SSL Certificate Creation

9.1.1.2 OPTION 2: IMPORT SSL CERTIFICATE AND KEY

Before beginning this procedure, export your certificate and key from your IIS server on your PC.

1. Navigate to **Config Mode > SSL Management > Certificate**.
2. Click **Import** to add a new SSL certificate.
3. Enter a name for the certificate: **"WS"**.
4. Select **Local** next to **Import Certificate from**.
5. Enter the **Certificate Password** (if applicable).
6. Click **Browse** and navigate to the certificate file.

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

Figure 22: Import SSL Certificate

7. Click **OK** and then click **Save** to store your configuration changes.

9.1.2 CREATE ONE CLIENT AND ONE SERVER SSL TEMPLATE

9.1.2.1 CREATE 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 the **Name**: "Client-SSL-WS".
4. Enter the **Certificate Name**: "WS".
5. Enter the **Key Name**: "WS".
6. Enter the **Pass Phrase (If Applicable)**

Client SSL	
Name: *	<input type="text" value="Client-SSL-WS"/>
Certificate Name:	<input type="text" value="WS"/>
Chain Cert Name:	<input type="text"/>
Key Name:	<input type="text" value="WS"/>
Cache Size:	<input type="text" value="0"/>
Pass Phrase:	<input type="text"/>
Confirm Pass Phrase:	<input type="text"/>

Figure 23: Client SSL Template

9.1.2.2 CREATE SERVER SSL TEMPLATE

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

1. Navigate to **Config Mode > Service > Template > SSL > Server SSL**.
2. Click **Add**.
3. Enter the **Name**: “**Server-SSL-WS**”.

Server SSL	
Name: *	<input type="text" value="Server-SSL-WS"/>
Certificate Name:	<input type="text"/>
Key Name:	<input type="text"/>
CA Cert Name:	<input type="text"/>
TLS/SSL Version:	<input type="text"/>

Figure 24: Server SSL Template

9.1.3 ON THE VIRTUAL SERVER, CHANGE THE SERVICE TYPE OF THE VIRTUAL PORT FROM “TCP” TO “HTTPS” AND APPLY THE NEW CLIENT AND SERVER SSL TEMPLATE

9.1.3.1 CHANGE THE SERVICE TYPE OF THE VIRTUAL PORT FROM “TCP” TO “HTTPS”

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. Click on the name of the virtual service created during basic configuration: “_172.16.1.200_TCP_443”
3. Edit the Virtual Service name to “_172.16.1.200_HTTPS_443”.
4. From the **Type** drop-down menu, select “**HTTPS**”.

Figure 25: Update Virtual Service type

5. Click **OK** and then click **Save** to store your configuration changes.

9.1.3.2 APPLY THE NEW CLIENT AND SERVER SSL TEMPLATE

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

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

RAM Caching Template:	<input type="text"/>
Client-SSL Template:	Client-SSL-WS
Server-SSL Template:	Server-SSL-WS
Connection Reuse Template:	<input type="text"/>
TCP-Proxy Template:	<input type="text"/>
Persistence Template Type:	<input type="text"/>
PBSLB Policy Template:	<input type="text"/>

Figure 26: Client and Server SSL Binding

- Click **OK** and then click **Save** to store your configuration changes.

9.2 SSL OFFLOAD

SSL Offload acts as an acceleration feature by removing the burden of processing SSL traffic from the SharePoint web servers. Instead of having the SharePoint servers handling these transactions, the AX Series decrypts traffic and forwards the traffic to the SharePoint Server via (unsecured) HTTP.



Figure 27: SSL Offload Overview

In this configuration, an SSL certificate is configured for the SharePoint HTTPS virtual server.

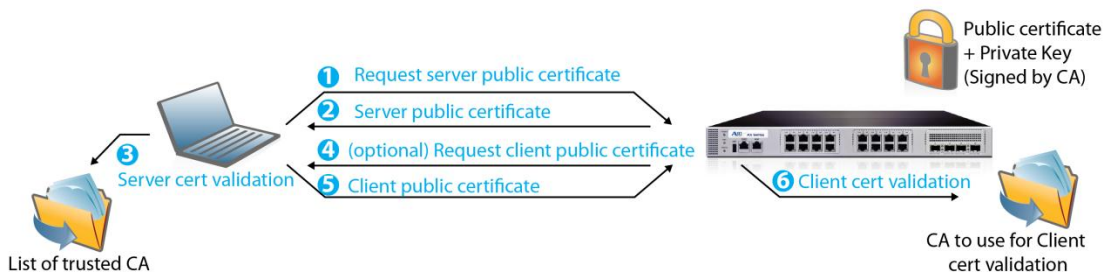


Figure 28: Client SSL Overview

9.2.1 CHANGE THE PORT NUMBERS IN THE SERVICE GROUP

1. Navigate to **Config Mode > Service > SLB > Service Group**.
2. Click the name of the service group created during basic configuration.
3. In the **Server** section:
 - a. Select the checkbox next to a server.
 - b. Edit the Port from “443” to “80”.
 - c. Select **Update**.
4. Repeat for each additional server.



The screenshot shows the 'Server' configuration window. At the top, there are radio buttons for 'IPv4' (selected) and 'IPv6'. Below that, the 'Server' dropdown is set to 'WS2', and the 'Port' is set to '80'. The 'Server Port Template (SPT)' is 'default' and 'Priority' is '1'. There are buttons for 'Add', 'Update', 'Delete', 'Enable', and 'Disable'. Below the form is a table with columns: 'Server', 'Port', 'SPT', 'Priority', and 'Stats Data'. The table contains two rows: 'WS1' and 'WS2', both with port '80', 'default' SPT, and '1' priority. The 'Stats Data' column has a green checkmark for both. There are checkboxes in the first column of the table, and the 'WS2' row's checkbox is highlighted with a red box.

	Server	Port	SPT	Priority	Stats Data
<input checked="" type="checkbox"/>	WS1	80	default	1	✓
<input checked="" type="checkbox"/>	WS2	80	default	1	✓

Figure 29: Server Configuration

5. Click **OK** and then click **Save** to store your configuration changes.

9.2.2 ON THE VIRTUAL SERVER, REMOVE THE SERVER SSL TEMPLATE

1. Navigate to **Config Mode > SLB > Virtual Server**.
2. Click on the Virtual Server name.
3. Select “443” and click **Edit**.
4. Remove the Server SSL template by selecting it from the **Server-SSL Template** drop-down menu.

RAM Caching Template:	<input type="text"/>
Client-SSL Template:	Client-SSL-WS
Server-SSL Template:	<input type="text"/>
Connection Reuse Template:	<input type="text"/>
TCP-Proxy Template:	<input type="text"/>
Persistence Template Type:	<input type="text"/>
PBSLB Policy Template:	<input type="text"/>

Figure 30: Client only SSL Binding

- Click **OK** and then click **Save** to store your configuration changes.

9.2.3 VALIDATE THE DEPLOYMENT

To validate that SSL Offload is working, navigate to **Monitor Mode > Service > Application > SSL**.

Note: Browse to the SharePoint site with HTTPS (443) and validate the statistics for SSL connections and total SSL connections.

Statistics for SSL	
Number of SSL Modules:	1
Current SSL Connections:	1
Total SSL Connections:	1.2M
Failed SSL Handshakes:	0
Failed Crypto operations:	0
SSL Memory Usage:	170.8K Bytes
SSL fail CA verification:	0
No HW Context Memory:	0
HW ring full:	0
SSL Module	1
Number of Enabled Crypto Engines:	22
Number of Available Crypto Engines:	22

Figure 31: SSL Offload Statistics

9.3 COMPRESSION

Compression is a bandwidth optimization feature that condenses the HTTP objects that are requested from a web server. The purpose of compression is to transmit the requested data more efficiently (less data transmitted) and faster response times to the client.



Figure 32: HTTP Compression Overview

9.3.1 CREATE HTTP COMPRESSION TEMPLATE

1. Navigate to **Config Mode > Template > Application > HTTP**.
2. Click **Add**.
3. Enter the Name: **"HTTP Compression"**.

Note: Compression is disabled by default. When compression is enabled, the following options will have these default values:

HTTP	
Name: *	HTTP Compression
Failover URL:	
Strict Transaction Switching:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Client IP Header Insert:	<input type="checkbox"/>
Retry HTTP Request:	<input type="checkbox"/>
<input type="checkbox"/>	Terminate HTTP 1.1 client when request has Connecton: close

Figure 33: HTTP Compression Template

4. Click **Compression** to enter compression options:
 - ◆ **Compression:** Enabled
 - ◆ **Level:** "1"

Note: The AX device offers various compression levels, ranging from levels 1 to 9. Level 1 is the recommended compression setting.

The screenshot shows a 'Compression' configuration dialog box. It has several sections:

- Compression:** Radio buttons for 'Enabled' (selected and highlighted with a red box) and 'Disabled'.
- Keep Accept Encoding:** Radio buttons for 'Enabled' and 'Disabled' (selected).
- Level:** A dropdown menu showing '1 (least compression, fastest)', which is also highlighted with a red box.
- Min Content Length:** A checkbox checked and the value '120'.
- Content Type:** A section with a 'Type' input field, an 'Add' button, and a 'Delete' button. A table below shows one entry with 'Type' in the 'Type' column.
- Exclude Content Type:** A section with a 'Type' input field, an 'Add' button, and a 'Delete' button. A table below shows one entry with 'Type' in the 'Type' column.
- Exclude URI:** A section with a 'URI' input field, an 'Add' button, and a 'Delete' button. A table below shows one entry with 'URI' in the 'URI' column.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 34: Compression Configuration Column

5. Click **OK** and then click **Save** to store your configuration changes.

9.3.2 APPLY HTTP COMPRESSION TEMPLATE TO VIP

To apply the compression template within the Virtual Server Port,

1. Navigate to **Config Mode > SLB > Virtual Server**.
2. Click on the Virtual Server name.
3. Select “**443**” and click **Edit**.
4. Locate the **HTTP Template** drop-down menu, and select “**HTTP Compression**” to apply the compression feature to the virtual server port.

HTTP Template:	HTTP Compression ▼
RAM Caching Template:	▼
Client-SSL Template:	▼
Server-SSL Template:	▼
Connection Reuse Template:	▼
TCP-Proxy Template:	▼

Figure 35: HTTP Compression Template

5. Click **OK** and then click **Save** to store your configuration changes.

9.3.3 VALIDATE THE DEPLOYMENT

You can validate that the AX Series device is compressing the data by navigating to **Monitor Mode > Service > Application > HTTP**.

	Control CPU	Data CPU1	Data CPU2	Data CPU3	Data CPU4	Data CPU5	Data CPU6	Data CPU7	Total
Curr Proxy Conns	0	0	0	0	0	0	0	0	0
Total Proxy Conns	0	132.9K	259.1K	570.8K	393.0K	5.4K	10.6K	60.2K	1.4M
HTTP Requests	0	132.9K	274.6K	787.5K	595.3K	5.4K	10.6K	60.2K	1.8M
HTTP Requests(succ)	0	132.9K	274.6K	787.5K	595.3K	5.4K	10.6K	60.2K	1.8M
HTTP Requests(cache succ)	0	0	0	0	0	0	0	0	0
No Proxy Error	0	0	0	0	0	0	0	0	0
Client RST	0	44.6K	86.3K	189.5K	130.7K	1.8K	3.6K	20.2K	476.7K
Server RST	0	0	0	0	0	0	0	0	0
No Tuple Error	0	0	0	0	0	0	0	0	0
Parse Req Fail	0	0	0	0	0	0	0	0	0
Server Selection Fail	0	0	0	0	0	0	0	0	0
Fwd Req Fail	0	0	0	0	0	0	0	0	0
Fwd Req Data Fail	0	0	0	0	0	0	0	0	0
Req Retransmit	0	0	0	0	0	0	0	0	0
Req Pkt Out-of-Order	0	0	0	0	0	0	0	0	0
Server Reselection	0	0	0	0	0	0	0	0	0
Server Premature Close	0	0	0	0	0	0	0	0	0
Server Conn Made	0	83.5K	164.6K	384.8K	271.3K	3.9K	7.1K	37.9K	953.0K
Source NAT Failure	0	0	0	0	0	0	0	0	0
Data Before Compression	0	276.0M	686.6M	2.5G	2.0G	9.8M	18.8M	128.4M	5.6G
Data After Compression	0	4.4M	11.0M	40.8M	32.8M	161.8K	308.6K	2.1M	91.6M
Request Over Limit	0	0	0	0	0	0	0	0	0
Request Rate Over Limit	0	0	0	0	0	0	0	0	0

Figure 36: Compression Statistics (Before and After)

9.4 COOKIE PERSISTENCE

Cookie persistence provides granularity in comparison to Source IP persistence. With cookie persistence, the session data is kept within the user’s browser.

9.4.1 CREATE COOKIE PERSISTENCE TEMPLATE

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 Name: **“SharePoint Cookie”**

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

Figure 37: Cookie Persistence Template

4. Click **OK** and then click **Save** to store your configuration changes.

Once you have finished configuring the template, the template appears in Cookie Persistence template list.

9.4.2 APPLY COOKIE PERSISTENCE TEMPLATE TO VIP

To apply cookie persistence to the VIP:

1. Navigate to **Config Mode > SLB > Virtual Server**.
2. Click on the Virtual Server name.
3. Select “**443**” and click **Edit**.
4. From the list of AX features, navigate to the “**Cookie Persistence Template**” section.
5. From the drop-down menu under “**Cookie Persistence Template**”, select the “**SharePoint Cookie**” template that was just created.

Persistence Template Type:	Cookie Persistence Template
Cookie Persistence Template:	SharePoint Cookie

Figure 38: Cookie Persistence Template

6. Click **OK** and then click **Save** to store your configuration changes.

9.4.3 VALIDATING THE DEPLOYMENT

To validate that the cookie persistence is installed, navigate to **Monitor Mode >Service > Application > Persistent**.

	Control CPU	Data CPU1	Data CPU2	Data CPU3	Data CPU4	Data CPU5	Data CPU6	Data CPU7	Total
URL Hash Persistent OK(primary)	0	19.7K	6.1K	2.3K	1.0K	461	206	15.5K	45.2K
URL Hash Persistent OK(secondary)	0	0	0	0	0	0	0	0	0
URL Hash Persistent Fails	0	0	0	0	0	0	0	0	0
Source IP Persistent OK	0	239.2K	103.6K	44.8K	19.4K	8.6K	3.9K	168.5K	588.0K
Source IP Persistent Fails	0	0	0	0	0	0	0	0	0
SSL SID Persistent OK	0	0	0	0	0	0	0	0	0
SSL SID Persistent Fails	0	0	0	0	0	0	0	0	0
Cookie Persistent OK	0	213.7K	91.3K	36.6K	14.4K	6.4K	2.8K	149.6K	514.7K
Cookie Persistent Fails	0	0	0	0	0	0	0	0	0
Persistent Cookie Not Found	0	121.6K	30.8K	12.6K	4.5K	1.6K	732	100.1K	272.0K

Figure 39: Cookie Persistent Monitor

9.5 CONNECTION REUSE (TCP OFFLOAD)

The AX Series Connection Reuse feature reduces the overhead associated with TCP connection setup by establishing TCP connections with SharePoint web servers and then reusing those connections for multiple client requests. This reduces the total number of TCP connections to each SharePoint WFE server.

The advantage of reusing connections is to off-load the server TCP stack in order to provide faster response times and to increase server scalability. If connection reuse is enabled, Source NAT must be enabled. Refer to Source NAT for configuration information. Figure 13 below is a sample diagram of a non-connection reuse configuration. Figure 32 depicts how connection reuse is deployed.

Note: Connection reuse is not supported if NTLM authentication is configured on the SharePoint servers.

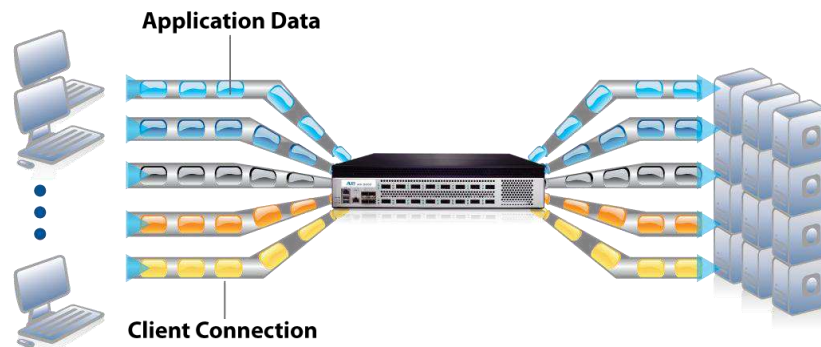


Figure 40: Non-Connection Reuse setup

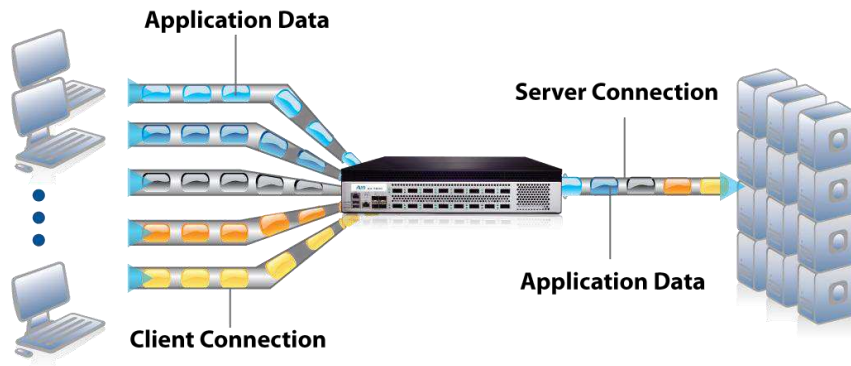


Figure 41: Connection Reuse Setup

9.5.1 CREATE CONNECTION REUSE TEMPLATE

1. Navigate to **Config Mode > Template > Connection Reuse**.
2. Click **Add**.
3. Enter the **Name**: “**SharePoint Connection**”.
4. Click **OK** and then click **Save** to store your configuration changes.

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

Figure 42: Connection Reuse Overview

9.5.2 CREATE AN IP SOURCE NAT TEMPLATE

If not already done in step “8.6, IP Source NAT” because you’re in one-arm mode, create one IP Source NAT.

See configuration steps in “8.6, IP Source NAT”.

9.5.3 APPLY CONNECTION REUSE AND SNAT TO VIP

To apply connection reuse within the VIP:

1. Navigate to **Config Mode > SLB > Virtual Server**.
2. Click on the Virtual Server name.
3. Select “**443**” and click **Edit**.
4. Locate the **Connection Reuse Template** drop-down list and select “**SharePoint Connection**” to apply the connection reuse feature to the virtual server port.

HTTP Template:	<input type="text"/>
RAM Caching Template:	<input type="text"/>
Client-SSL Template:	<input type="text"/>
Server-SSL Template:	<input type="text"/>
Connection Reuse Template:	SharePoint Connection
TCP-Proxy Template:	<input type="text"/>
Persistence Template Type:	<input type="text"/>

Figure 43: Connection Reuse Template

5. Locate the **Connection Reuse Template** drop-down list and select “**SharePoint Connection**” to apply the connection reuse feature to the virtual server port.

Access List:	<input type="text"/>
Source NAT Pool:	SNAT
aFleX:	<input type="text"/> <input type="checkbox"/> Multiple

Figure 44: SNAT Template

6. Click **OK** and then click **Save** to store your configuration changes.

9.5.4 VALIDATE THE DEPLOYMENT

To validate that connection reuse is working, navigate to **Monitor Mode >Service > SLB > Virtual Server**

	Name	Connections	
		Current	Total
	WS/-VIP 172.16.1.200	223	429
	HTTPS/443	223	429
	80(WS1)	9	201
	80(WS2)	10	201

Figure 45: Connection Reuse Monitor

Note: To see the benefits of the connection reuse feature, you must have multiple concurrent users connecting to the SharePoint servers. To verify connection reuse is working properly, compare the total current connections of the VIP to the real servers' current connections. The real server's current connections will be less than the current connections to the VIP if working correctly. See the example above in Figure 45.

9.6 RAM CACHING

Cacheable data is cached within the AX Series device, thus reducing overhead on each WFE servers, and increasing the capacity of the SharePoint servers. RAM caching reduces the number of connections and server requests that need to be processed.



Figure 46: RAM Caching Template

9.6.1 CREATE RAM CACHING TEMPLATE

1. Navigate to **Config Mode> Service> Template > Application > RAM Caching**.
2. Click **Add**.
3. Enter the **Name**: “**SharePoint RAM Caching**”.
4. Leave the **Age** set to 3600 seconds.
5. Enter the following values:
 - ◆ **Max Cache Size: 512 MB**
 - ◆ **Min Content Size: 10 Bytes**
 - ◆ **Max Content Size: 4194303 Bytes**
6. Click **OK** and then click **Save** to store your configuration changes.

Note: The RAM caching policy option is not required unless you have specific data that requires caching, no caching or invalidate. These policy options can be configured in the policy form of the RAM Caching template. For additional information on RAM caching policy, please refer to the AX Series System Configuration and Administration Guide.

RAM Caching	
Name: *	SharePoint RAM Caching
Age:	3600 Seconds
Max Cache Size:	512 MB
Min Content Size:	10 Bytes
Max Content Size:	4194303 Bytes
Replacement Policy: *	Least Frequently Used
Accept Reload Request:	<input type="checkbox"/>
Verify Host:	<input type="checkbox"/>
Default Policy No-Cache:	<input type="checkbox"/>
Insert Age:	<input checked="" type="checkbox"/>
Insert Via:	<input checked="" type="checkbox"/>

Figure 47: RAM Caching Overview

9.6.2 APPLY RAM CACHING TEMPLATE ON VIP

To apply the RAM caching template within the Virtual Server Port:

1. Navigate to **Config Mode > SLB > Virtual Server**.
2. Click on the Virtual Server name.
3. Select “443” and click **Edit**.
4. Locate the **RAM Caching Template** drop-down list and select “**SharePoint RAM Caching**” to apply the RAM caching to the virtual server port.

HTTP Template:	<input type="text"/>
RAM Caching Template:	SharePoint RAM Caching
Client-SSL Template:	<input type="text"/>
Server-SSL Template:	<input type="text"/>
Connection Reuse Template:	<input type="text"/>
TCP-Proxy Template:	<input type="text"/>
Persistence Template Type:	<input type="text"/>

Figure 48: RAM Caching Template

5. Click **OK** and then click **Save** to store your configuration changes.

9.6.3 VALIDATE THE DEPLOYMENT

To validate that RAM caching is working, navigate to **Monitor Mode > Service > Application > RAM Caching > Details**.

Statistics for Cache Details

Virtual Server: All Port: 1 Minute Refresh Clear

Cache Hits	484	Total number of objects found in the cache and served from the cache
Cache Misses	50	
Memory Used	1121920	
Bytes Served	13376410	
Entries Cached	49	Total number of cache objects
Entries Replaced	0	
Entries Aged Out	0	
Entries Cleaned	0	
Total Requests	685	
Cacheable Requests	534	
No-cache Requests	44	
No-cache Responses	85	

Figure 49: RAM Caching Monitor

9.7 SECURING SHAREPOINT VIA AFLEX

This section of the deployment guide explains how to redirect SharePoint traffic that comes from HTTP to HTTPS using the AX aFlex scripts. aFlex is based on a standard scripting language, TCL, and it enables the load balancer to perform Layer 7 deep-packet inspection (DPI). For examples of aFlex scripts, please refer to the following URL below:

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



Figure 50: Redirect Overview

As an example, one of the most common aFlex scripts that can be used with SharePoint 2010 server is the “HTTP redirect to HTTPS traffic”. You can download additional aFlex script examples from the following URL:

To configure a transparent HTTPS redirect using aFlex script:

Step 1. Create aFlex Script

Step 2. Configure VIP with HTTP/Port 80

Step 3: Apply aFlex to VIP

9.7.1 CREATE AFLEX SCRIPT

1. Navigate to **Config Mode > Service > aFlex**.
2. Click **Add**.
3. Within the **Definition** box, enter the TCL code.
4. Click **OK** and then click **Save** to store your configuration changes.



Figure 51: aFleX Redirect Configuration

Redirect Script Copy and Paste:

```
when HTTP_REQUEST {  
  HTTP::redirect https://[HTTP::host][HTTP::uri]  
}
```

The aFleX script must be bound to Virtual Server Port 80.

9.7.2 CONFIGURE VIP WITH HTTP/PORT 80

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. “Select” VIP Name and click “edit”.
3. In the port section, click “**Add**”
4. Select Type: “**HTTP**”
5. Port: “**80**”

Virtual Server Port	
Virtual Server:	WS-VIP
Type: *	HTTP
Port: *	80
Service Group:	SharePoint Servers

Figure 52: VIP Configuration

6. Click **OK** and then click **Save** to store your configuration changes.

9.7.3 APPLY AFLEX SCRIPT TO VIP

7. Navigate to **Config Mode > SLB > Virtual Server**.
8. **Click on the VIP name WS-VIP**.
9. In the **Port** section, select “**80**” and click **Edit**.
10. From the **aFlex** drop-down list, select “**Redirect**”.
11. Click **OK** and then click **Save** to store your configuration changes.

Source IAT Pool:	
aFlex:	Redirect <input type="checkbox"/> Multiple
HTTP Template:	
RAM Caching Template:	

Figure 53: aFlex Configuration

9.7.4 VALIDATE AFLEX SERVICE

To verify that the aFlex script is working, open a web browser and navigate to “http://example.com”. The browser will accept the URL request and client URL address will change from “http://example.com” to “https://example.com”.

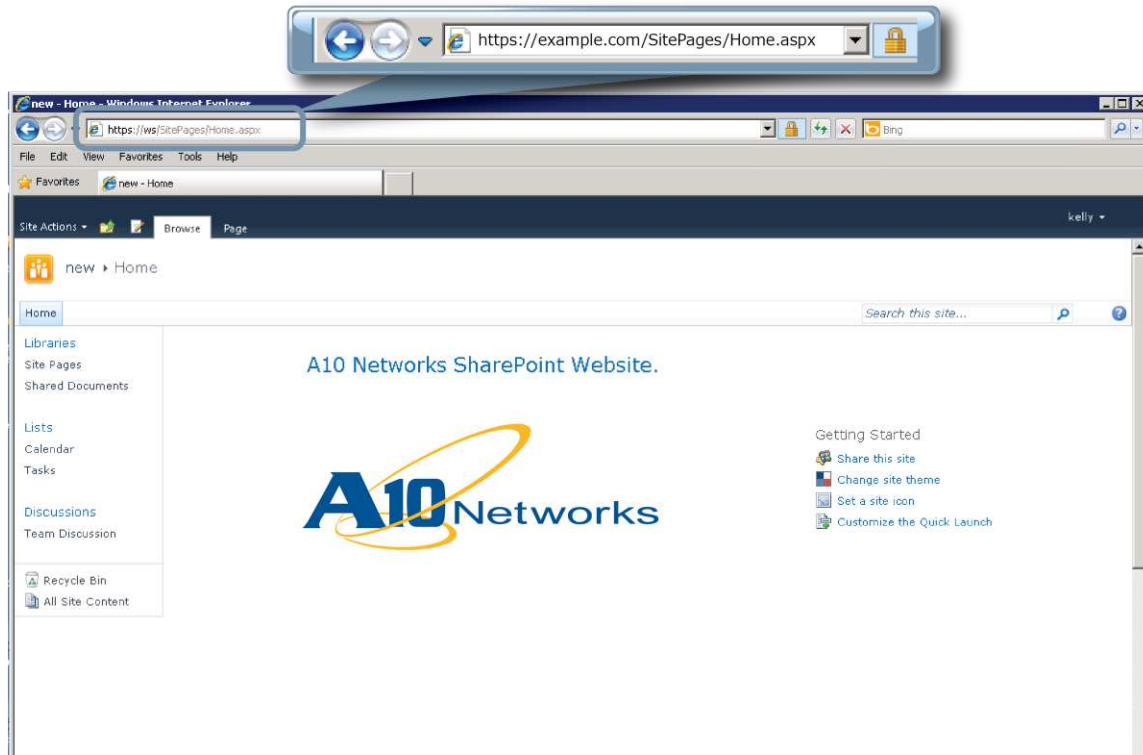


Figure 54: SharePoint Website Sample

10 SUMMARY AND CONCLUSION

The configuration steps described above show how to set up the AX for Microsoft SharePoint 2010 Server. By using the AX device to load balance SharePoint Web Front End (WFE) Servers, the following key advantages are achieved:

- Obtain high availability for SharePoint Servers to prevent website failure, meaning there is no adverse impact on how users can access the applications.
- Distribute client traffic seamlessly across multiple SharePoint WFE Servers for site scalability.
- Higher connection throughput, faster end user responsiveness and reduce WFE CPU utilization by initiating SSL offload, HTTP Compression, RAM Caching and Connection Reuse.
- Improve site performance and reliability to end users

By using the AX Series Advanced Traffic Manager, significant benefits are achieved for all Microsoft SharePoint 2010 users. For more information about AX Series products, please refer to the following URLs:

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

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

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

11 APPENDIX

11.1 AX SERIES CLI SAMPLE CONFIGURATIONS:

SharePoint Basic Configuration in “one-arm mode”:

```
basicconfig-ax1#show run
interfaces management
  enable
hostname basicconfig-ax1
clock timezone Europe/Dublin
interface management
  ip address 192.168.18.41 255.255.255.0
ip nat pool SNAT 172.16.1.250 172.16.1.250 netmask /24
health monitor "SharePoint HC"
  method http
slb server WS1 172.16.1.5
  port 443 tcp
slb server WS2 172.16.1.6
  port 443 tcp
slb service-group "SharePoint Servers" tcp
  health-check "SharePoint HC"
  member WS1:443
  member WS2:443
slb template persist source-ip "IP Persistence"
  timeout 10
slb virtual-server WS-VIP 172.16.1.200
  port 443 https
```



```
name _172.16.1.200_TCP_443
source-nat pool SNAT
service-group "SharePoint Servers"
template persist source-ip "IP Persistence"
end
```

SharePoint configuration with all advanced options in “one-arm mode”

```
advconfig-ax2#show run
interfaces management
enable
hostname advconfig-ax2
clock timezone Europe/Dublin
interface management
ip address 192.168.18.41 255.255.255.0
ip nat pool SNAT 172.16.1.250 172.16.1.250 netmask /24
health monitor "SharePoint HC"
method http
slb server WS1 172.16.1.5
port 80 tcp
slb server WS2 172.16.1.6
port 80 tcp
slb service-group "SharePoint Servers" tcp
health-check "SharePoint HC"
member WS1:80
member WS2:80
```

```
slb template connection-reuse "SharePoint Connection"

slb template cache "SharePoint RAM Caching"
    max-content-size 4194303
    min-content-size 10

slb template http HTTP Compression
    compression enable
    compression minimum-content-length 120

slb template client-ssl Client-SSL-WS
    cert WS
    key WS

slb template persist cookie "SharePoint Cookie"

slb virtual-server WS-VIP 172.16.1.200
    port 443 https
        name _172.16.1.200_HTTPS_443
        source-nat pool SNAT
        service-group "SharePoint Servers"
        template http "HTTP Compression"
        template cache "SharePoint RAM Caching"
        template client-ssl Client-SSL-WS
        template connection-reuse "SharePoint Connection"
        template persist cookie "SharePoint Cookie"

    port 80 http
        name _172.16.1.200_HTTP_80
        aflex Redirect

end
```