Deployment Guide

AX Series with Juniper Networks SA Series SSL-VPN Appliances Solution

Table of Contents

DEPLOYMENT GUIDE

AX Series with Juniper Networks SA Series SSL-VPN Appliances Solution

1. Introduction

Juniper Networks SA Series (Juniper SA) allows employees, partners, suppliers and contractors to securely access corporate resources remotely.

Juniper provides three access modes:

- Core – provides access to web-based applications only
- Java-based Secure Application Manager (JSAM) / Windows-based SAM (WSAM) – provides access to other applications in addition to web-based applications
- Network Connect – provides full Layer 3 network access, similar to IPsec

For more information on Juniper SA, visit:
http://www.juniper.net/us/en/products-services/security/sa-series/

Adding the AX Series to your Juniper SA deployment provided the following benefits:

- Higher Scalability – enterprises can provide secured remote access to a very high number of employees, load balancing them among multiple Juniper SA devices in parallel.
- High Availability – secured remote access is guaranteed even if a Juniper SA goes offline.
- Higher Security – protects services from DDoS attacks.

This deployment guide contains configuration procedures for AX Series application delivery controllers and server load balancers, to support a Juniper Networks SA Series SSL VPN Appliances solution.

Prerequisites and Assumptions

- The A10 Networks AX Series device should be running software version 2.2.5 or later.
- It is assumed that readers have some basic configuration familiarity with both the AX Series and Juniper SA.
- Juniper SA screenshots are from Juniper SA release 6.4R1 (build 14063).
- Both IPv4 and IPv6 are supported. The examples in this deployment guide use IPv4.

2. AX deployment for Juniper SA

Juniper SA can be installed in two different modes:

- Juniper-SA in-line mode

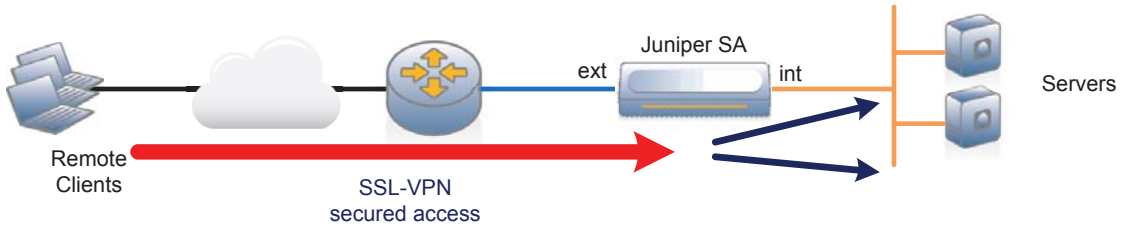


Figure 1: Juniper SA in-line mode deployment

- Juniper-SA one-arm mode

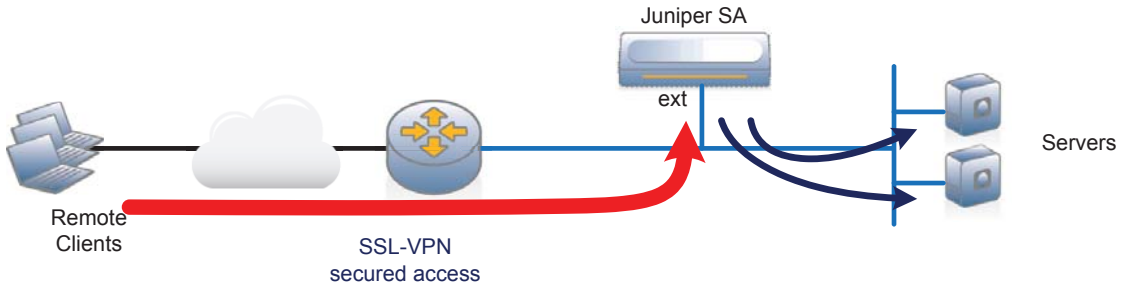


Figure 2: Juniper SA one-arm mode deployment

The AX Series supports each Juniper integration mode and does not require specific configuration depending on mode:

- Juniper-SA in-line mode

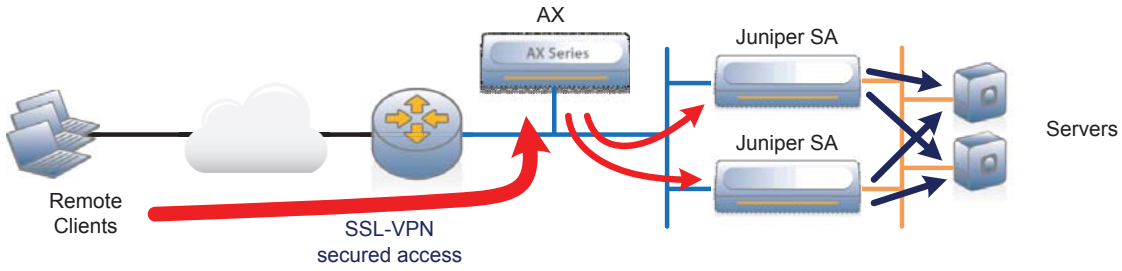


Figure 3: AX one-arm - Juniper SA in-line mode deployment

- Juniper-SA one-arm mode

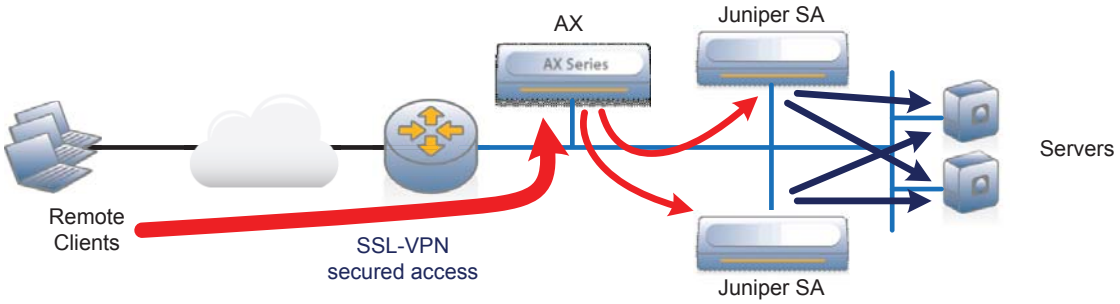


Figure 4: AX one-arm - Juniper SA one-arm mode deployment

Note: The AX Series usually is integrated in one-arm mode (as displayed in the examples above) but can also be installed in routed mode.

2.1 Lab diagram

The following diagram shows the network used for the configuration procedures.

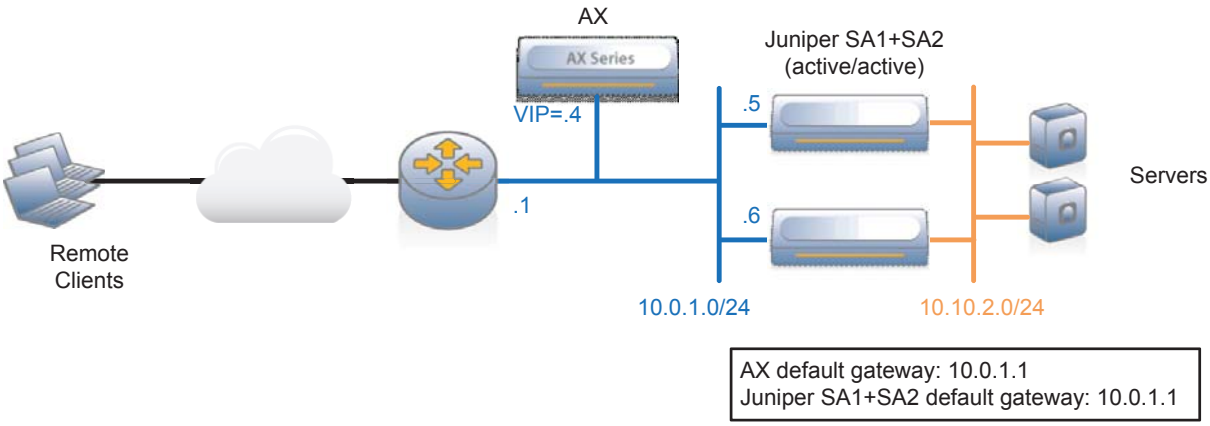


Figure 5: AX – Juniper SA lab diagram

2.2 Juniper SA Active-Active configuration

Note: This example shows only the required Juniper SA options. For information about other options, see the Juniper manuals (http://www.juniper.net/techpubs/software/ive/6.x/6.0).

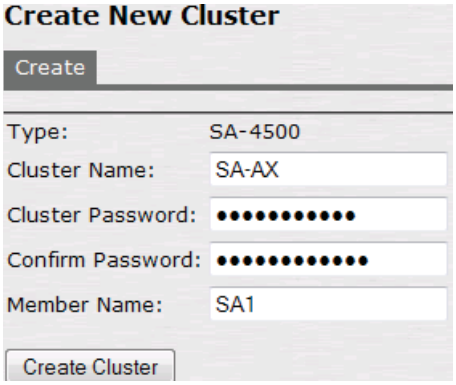
Cluster license validation

Validate Juniper-SA2 has a clustering license (under System > Configuration > Licensing):

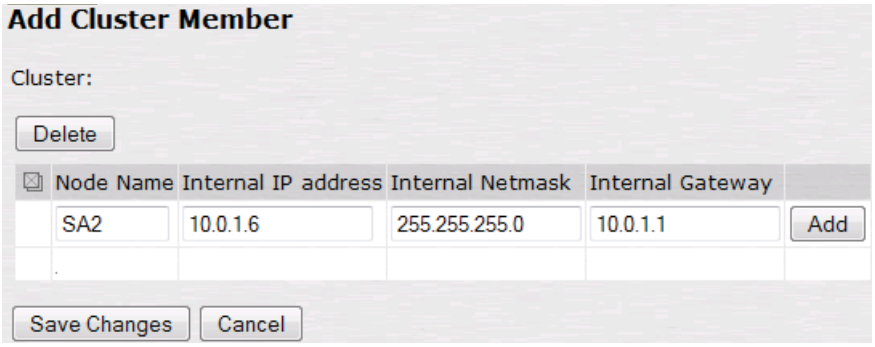
1. **Clustering: Allow 50 additional users to be shared from another SA 4500**
   Key: kiosk bring spruce harp crucial pinwheel vigor

Cluster configuration

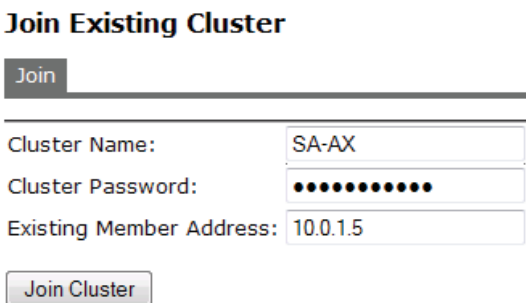
- Create the Cluster on the Juniper SA.
  - On Juniper-SA1:
    - Create a new cluster, “SA-AX” (under System > Clustering).



    - Add member Juniper-SA2 information (under System > Clustering).

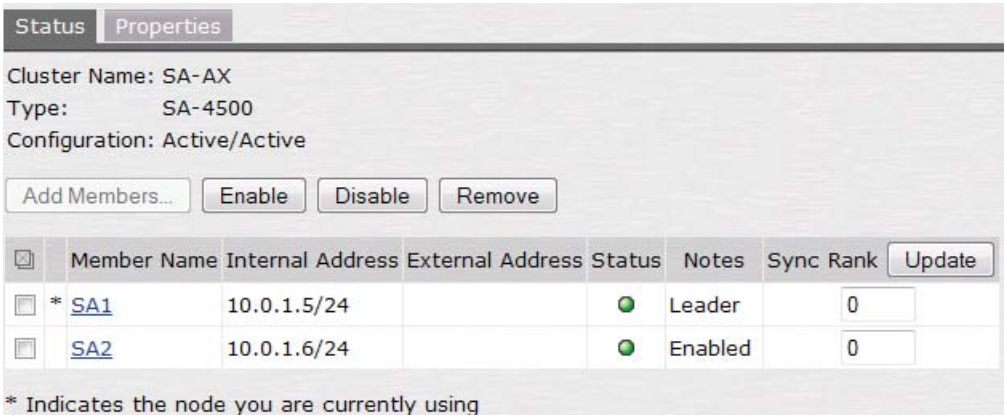


- On Juniper-SA2:
  - Join the new cluster SA-AX (under System > Clustering).



- Validate cluster creation.
  - On Juniper-SA1:
    - Validate that the 2 Juniper SA devices are in the same cluster and in Active/Active mode (under System > Clustering).

Note: Active/Active mode is the default cluster setting.

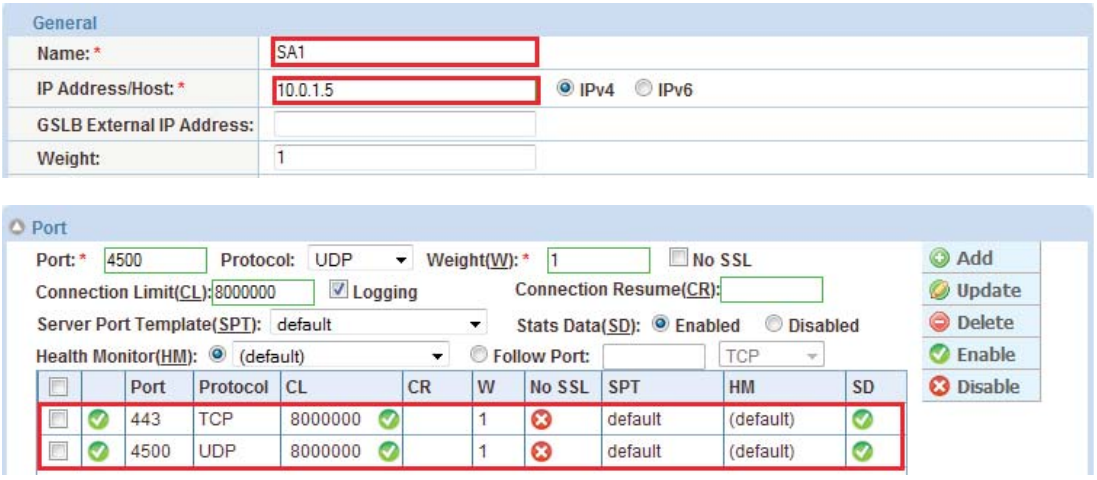


2.3 AX Series configuration

Note: This example shows only the required AX options. For information about other options, see the AX Series Configuration Guide, the AX Series GUI Reference, or the GUI online help.

Create Juniper-SA real servers

- Create a real server for each Juniper-SA. Enter the SA name and IP address, and add the protocol port(s) required for the access modes you plan to allow:
  - TCP 443 – Add TCP port 443 for Core or JSAM/WSAM access.
  - UDP 4500 – Add UDP port 4500 for Network Connect access.
  - Via Web GUI: Config Mode > Service > SLB > Server



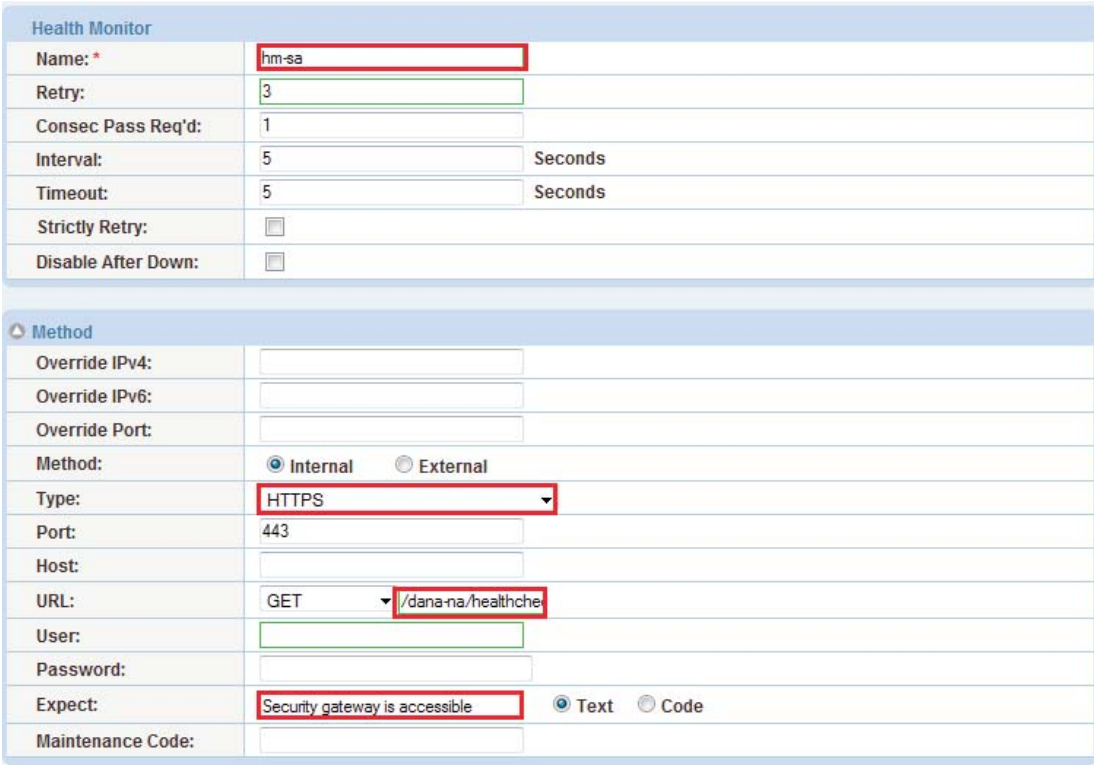
  - Via CLI:

```
AX(config)#slb server SA1 10.0.1.5
AX(config-real server)#port 443 tcp
AX(config-real server)#port 4500 udp
```

Create Juniper-SA health check

- Create a health monitor template to test the availability of the Juniper-SA. Enter the health monitor template name and select type HTTPS. Add URL "/dana-na/healthcheck/healthcheck.cgi" and expected return string "Security gateway is accessible".

- Via Web GUI: Config Mode > Service > Health Monitor



- Via CLI:

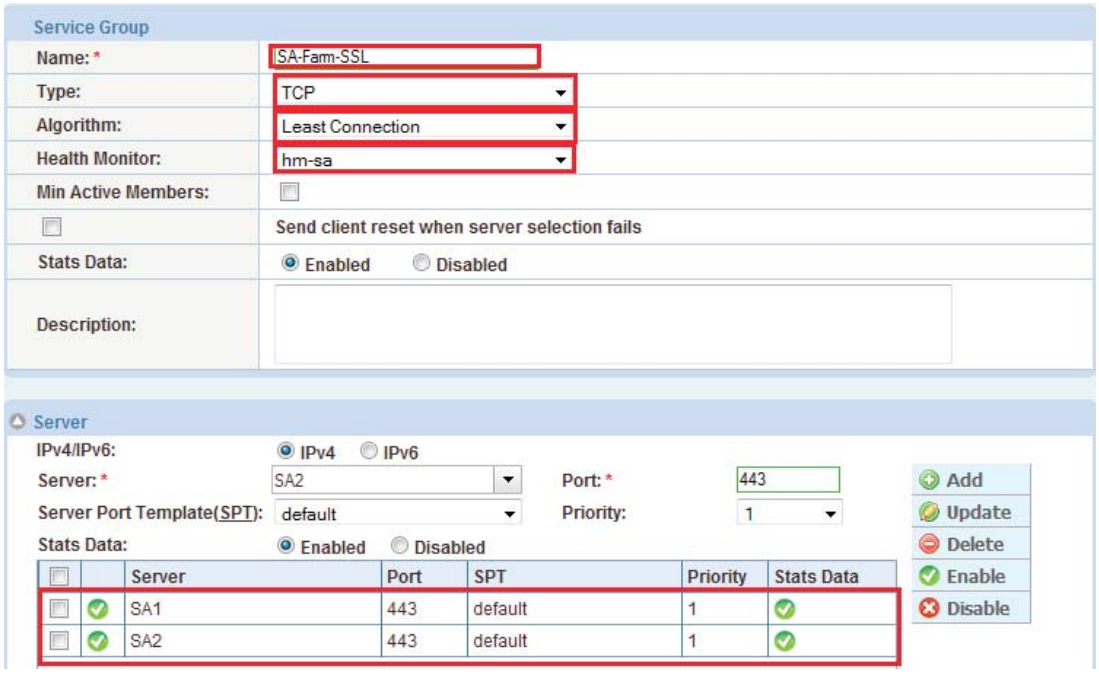
```
AX(config)#health monitor hm-sa
AX(config-health:monitor)#method https url GET /dana-na/
healthcheck/healthcheck.cgi expect "Security gateway is
accessible"
```

Create Juniper-SA service groups

Separate service groups are required. If you plan to allow Core or JSAM/WSAM access, you need a TCP service group. For Network Access mode, you also need a UDP group.

- Create a TCP service group for SSL traffic.
  Enter a name for the service group, select TCP from the Type drop-down list, select the load balancing algorithm least connection, and select the SA health monitor. Assign each Juniper SA to the service group.

◦ Via Web GUI: Config Mode > Service > SLB > Service Group

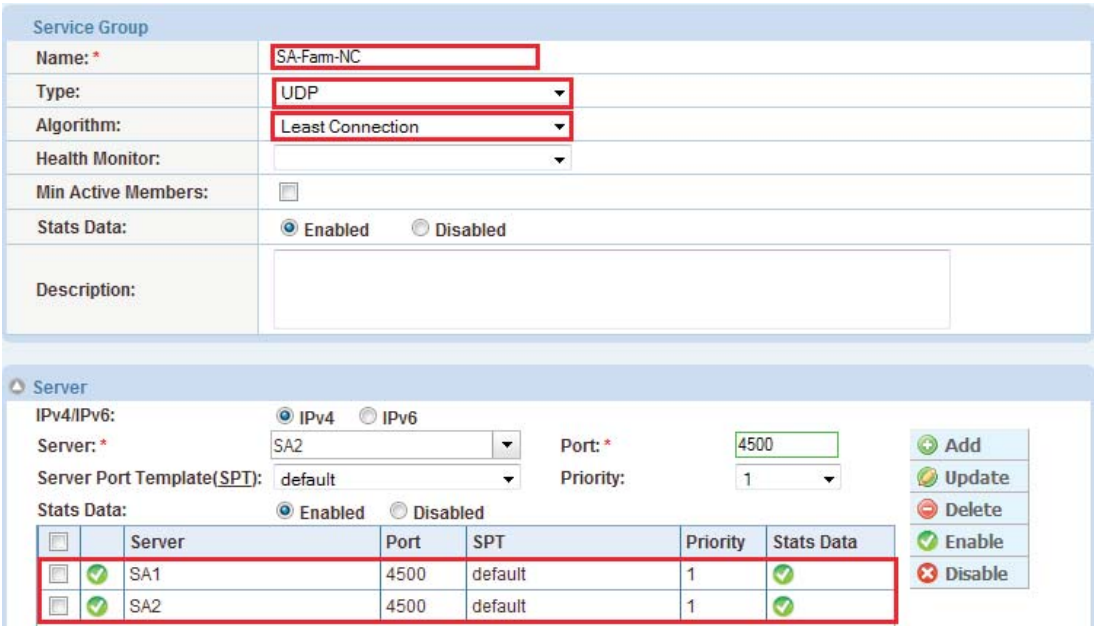


◦ Via CLI:

```
AX(config)#slb service-group SA-Farm-SSL tcp
AX(config-slb svc group)#method least-connection
AX(config-slb svc group)#health-check hm-sa
AX(config-slb svc group)#member SA1:443
AX(config-slb svc group)#member SA2:443
```

- Create a UDP service group for UDP traffic (Network Connect).
  Enter a name for the service group, select UDP from the Type drop-down list, and select the load balancing algorithm least connection. Assign each Juniper SA to the service group.

- Via Web GUI: Config Mode > Service > SLB > Service Group



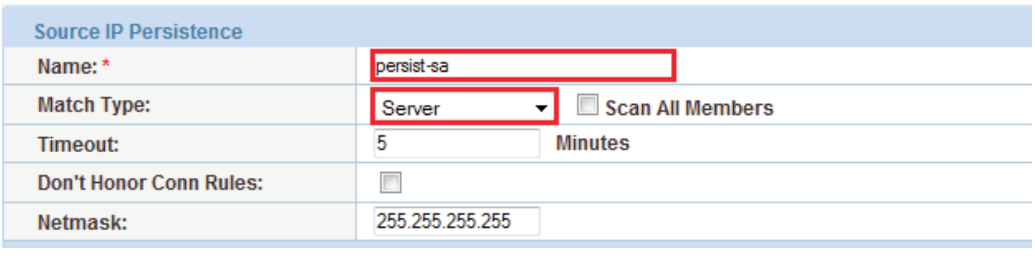
- Via CLI:

```
AX(config)#slb service-group SA-Farm-NC udp
AX(config-slb svc group)#method least-connection
AX(config-slb svc group)#member SA1:4500
AX(config-slb svc group)#member SA2:4500
```

Create Juniper-SA persistency

- Create a source IP persistence template to guarantee each end user will always go to the same Juniper-SA. This is required regardless of the access modes supported (Core, JSAM/WSAM, Network Connect). Enter the persistence template name and select match type server.

  - Via Web GUI: Config Mode > Service > Template > Persistent > Source IP Persistence

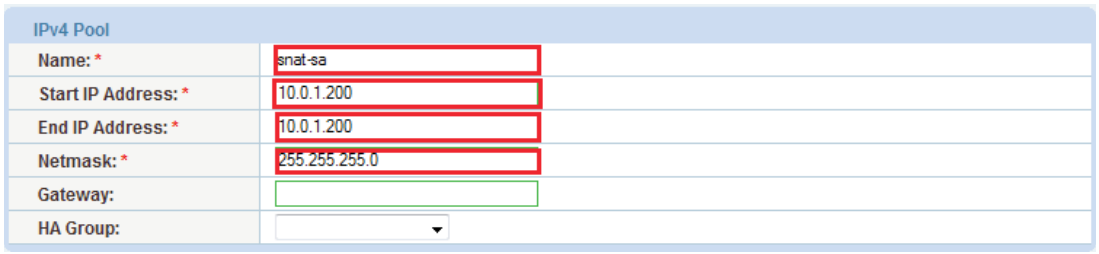


  - Via CLI:

```
AX(config)#slb template persist source-ip persist-sa
AX(config- source ip persist)#match-type server
```

Create IP Source-NAT Pool

- Create a source NAT pool to guarantee the Juniper-SA traffic back to the end users will go through the AX device. Enter the source NAT template name, select the first and last IP addresses used to SNAT the traffic (one IP address can be used for up to 64 k flows), and select the subnet of that SNAT pool.
  - Via Web GUI: Config Mode > Service > IP Source NAT



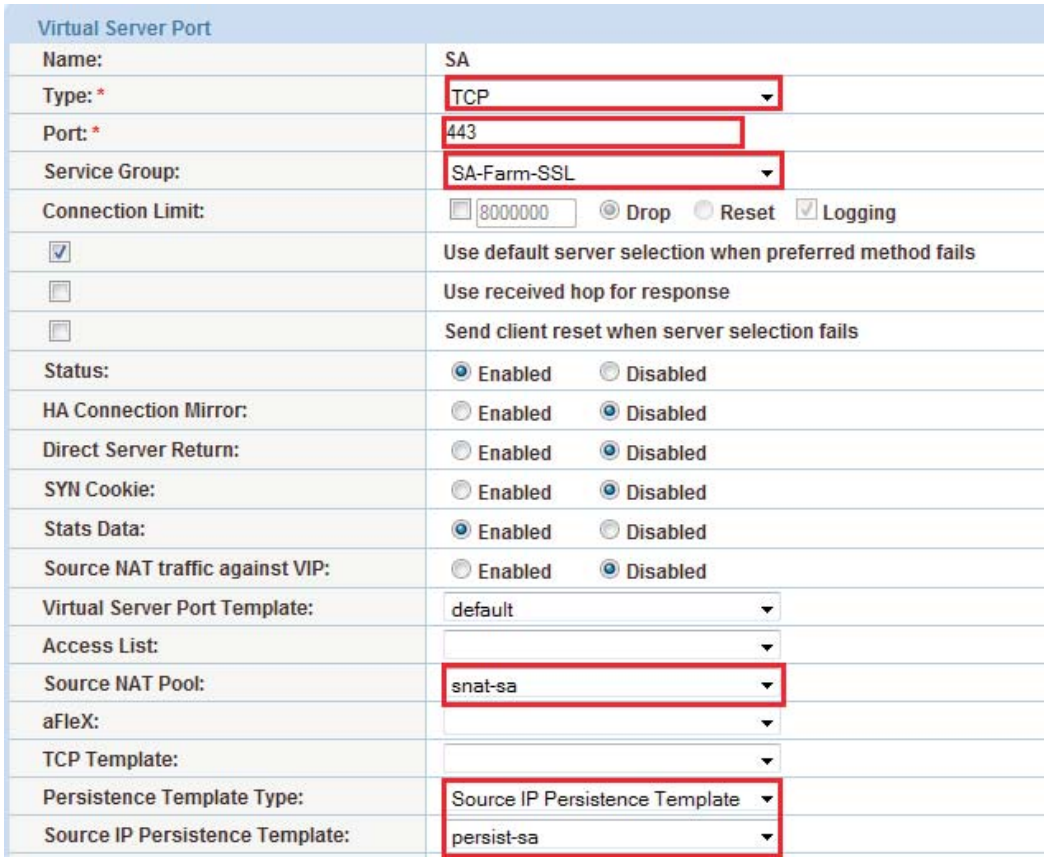
  - Via CLI: `AX(config)# ip nat pool snat-sa 10.0.1.200 10.0.1.200 netmask /24`

Create Juniper-SA VIP

- Create the virtual IP address (VIP), which is the IP address that end users will access.
  - Enter a name for the VIP, and enter the IP address.
    - Via Web GUI: Config Mode > Service > SLB > Virtual Server

    - Via CLI: `AX(config)#slb virtual-server SA 10.0.1.4`

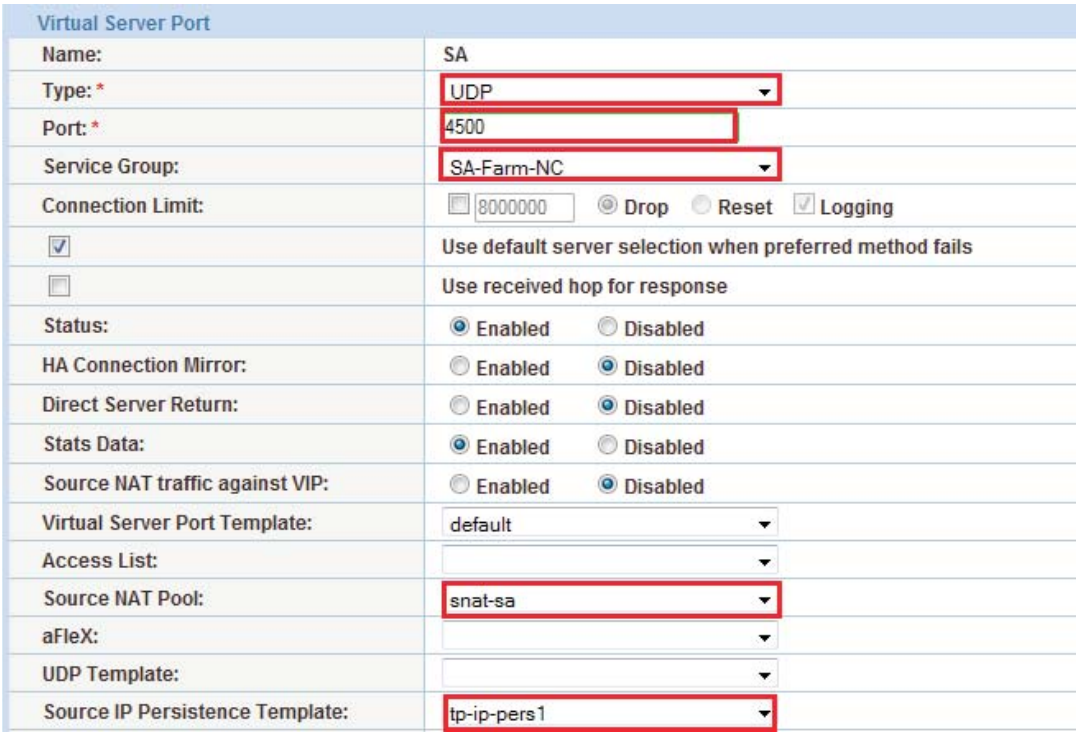
- For Core or JSAM/WSAM access, add TCP port 443 and select the service group, SNAT pool, and persistence template.
  - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port



  - Via CLI:

```
AX(config-slb vserver)#port 443 tcp
AX2(config-slb vserver-vport)#service-group SA-Farm-SSL
AX2(config-slb vserver-vport)#source-nat pool snat-sa
AX2(config-slb vserver-vport)#template persist source-ip
persist-sa
```

- For Network Connect access, add UDP port 4500 and select the service group, SNAT pool, and persistence template.
  - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port



  - Via CLI:

```
AX(config-slb vserver)#port 4500 udp
AX2(config-slb vserver-vport)#service-group SA-Farm-NC
AX2(config-slb vserver-vport)#source-nat pool snat-sa
AX2(config-slb vserver-vport)#template persist source-ip
persist-sa
```

2.4 Validate AX configuration

Display the status of the VIP and its members.

- Via Web GUI: Config Mode > Service > SLB > Virtual Server

		Name	Connections		Packets		Bytes		
			Current	Total	Forward	Reverse	Forward	Reverse	
		SA/10.0.1.4	0	0	0	0	0	0	
		TCP/443	0	0	0	0	0	0	
		443 (SA1)	0	0	0	0	0	0	
		443 (SA2)	0	0	0	0	0	0	
		UDP/4500	0	0	0	0	0	0	
		4500 (SA1)	0	0	0	0	0	0	
		4500 (SA2)	0	0	0	0	0	0	

- Via CLI:
```
AX#show slb virtual-server SA
AX#show slb service-group [SA-Farm-SSL | SA-Farm-NC]
AX#show slb server [SA1 | SA2]
```

2.5 AX / Juniper SA deployment validation

To validate the AX deployment:

- Verify that clients can access the Juniper SA farm using the access modes authorized through the VIP:
  - Core
  - JSAM/WSAM
  - Network Connect

- Validate both the Juniper SA devices receive traffic from different clients.

  Note: You must have multiple end users concurrently connected.

3. Summary and Conclusion

The AX Series Advanced Traffic Manager enhances Juniper SA load balancing by providing:

- High availability
- High scalability
- High flexibility
- High performance
- High security

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 and centers of excellence around the globe. 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

A10 Networks