

CONFIGURING AND IMPLEMENTING A10 NETWORKS LOAD BALANCING SOLUTION WITH JUNIPER'S SSL VPN APPLIANCES

Although Juniper Networks has attempted to provide accurate information in this guide, Juniper Networks does not warrant or guarantee the accuracy of the information provided herein. Third party product descriptions and related technical details provided in this document are for information purposes only and such products are not supported by Juniper Networks. All information provided in this guide is provided "as is", with all faults, and without warranty of any kind, either expressed or implied or statutory. Juniper Networks and its suppliers hereby disclaim all warranties related to this guide and the information contained herein, whether expressed or implied of statutory including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement, or arising from a course of dealing, usage, or trade practice.

Table of Contents

Introduction	3
Scope	4
Design Considerations	4
Description and Deployment Scenario	4
Configure AX2	13
SA6500 Active-Active Configuration	15
Creating a Cluster in sa6500-c	15
Adding a Cluster Member in sa6500-c	17
Joining a Cluster in sa6500-d	18
Monitoring a Cluster	19
SA Series Configuration References	20
Summary	20
About A10 Networks	20
About Juniper Networks	20

Table of Figures

Figure 1: Logical topology overview	3
Figure 2: Logical topology overview with the IP addresses used in this example	3
Figure 3: Select the interface	5
Figure 4: Enter the IP address and mask for e1	5
Figure 5: Set up HA	6
Figure 6: Configure the health monitor	8
Figure 7: Add the servers	9
Figure 8: Configure the source NAT pool	10
Figure 9: Enter general settings and click Add to include a virtual port	11
Figure 10: Configure port settings (settings for port 443 shown)	11
Figure 11: Configure the source-IP persistence template	12
Figure 12: Virtual ports configured and listed on the Port tab	12
Figure 13: Set up HA (compare with the setup for AX1)	14
Figure 14: HA Config Sync	14

Introduction

The combined solution of Juniper Networks® SA Series SSL VPN Appliances and the A10 Networks AX Series Advanced Traffic Manager provides an enhanced SSL VPN service. The access and security features of the SA Series are easily extended as needed by deploying AX Series server load-balancing functionality for additional security, availability, and capacity.

AX Series load balancers add the following benefits to an SA Series solution:

- Intelligent, flexible load-balancing algorithms to select the best SA Series node for each session
- Industry-leading connection speed, supporting greater than 500,000 new TCP connections per second
- Customizable health monitors to ensure service availability
- Stickiness options, such as persistence based on client source IP address
- Hardware-based protection against distributed denial of service (DDoS) attacks
- One virtual VPN server to provide a single point of access for all users in all locations
- High availability (HA) AX redundancy with session synchronization to eliminate single point of failure

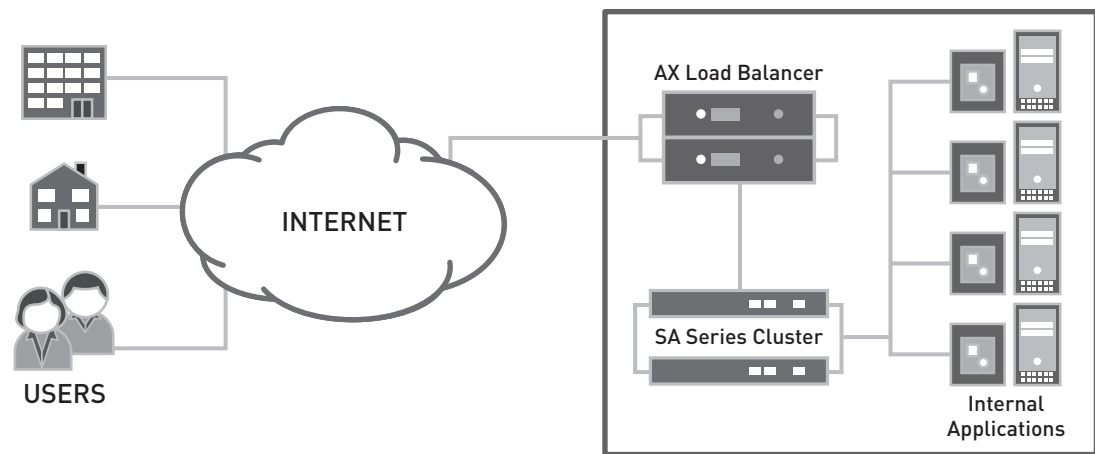


Figure 1: Logical topology overview

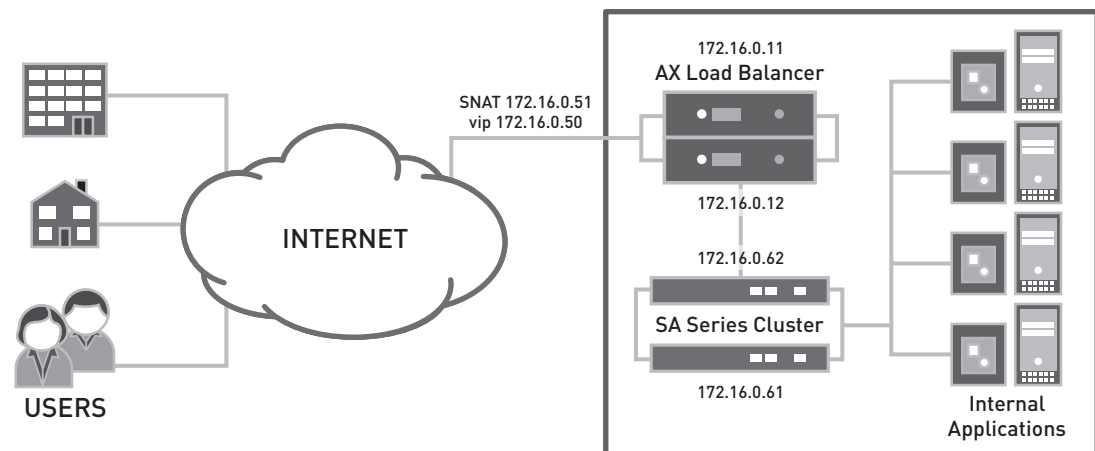


Figure 2: Logical topology overview with the IP addresses used in this example

Scope

The deployment guide is intended to describe the installation steps necessary to implement the A10 Networks AX Series load balancer with the Juniper Networks SA Series SSL VPN Appliances solution. The guide is intended to provide detailed configuration information for organizations' system engineers and technical staff.

Design Considerations

AX Series Appliances

Firmware: AX Series version 2.x or later

Platform: Any

Performance: AX Series appliances are high-performance systems, and characteristics vary by platform.

Performance examples are provided in various third-party performance reports at <http://www.a10networks.com>.

Sample figures:

- >500,000 new connections per second (CPS)
- Millions of concurrent sessions
- 1-9+ million hardware SYN/sec for DDoS
- Multi-Gb throughput

Juniper Networks IC Series Unified Access Control Appliances

- Software: 6.0R3.1 (build 12507) or later
- Platform: Juniper Networks SA6500 SSL VPN Appliance
- Performance: 5,000 simultaneous users per appliance

Description and Deployment Scenario

This section enables solution implementation, detailing device configuration for all relevant protocols and interfaces.

The following procedures show you how to configure a pair of AX load balancers to provide HA and load balancing for a Juniper SA Series cluster. The configuration for the SA Series cluster follows.

Configure AX

First, AX1 will be configured, and then its configuration will be synchronized to AX2.

Add the IP Address to the Interface

1. Select Config Mode > Network > Interface.
2. In the Interface column, click on "e1."
3. Expand the IPv4 tab.
4. Enter the IP address and mask in the IP Address and Mask fields. In this example, enter 172.16.0.11 and 255.255.255.0.
5. Click OK at the bottom of the window. The interface list reappears.

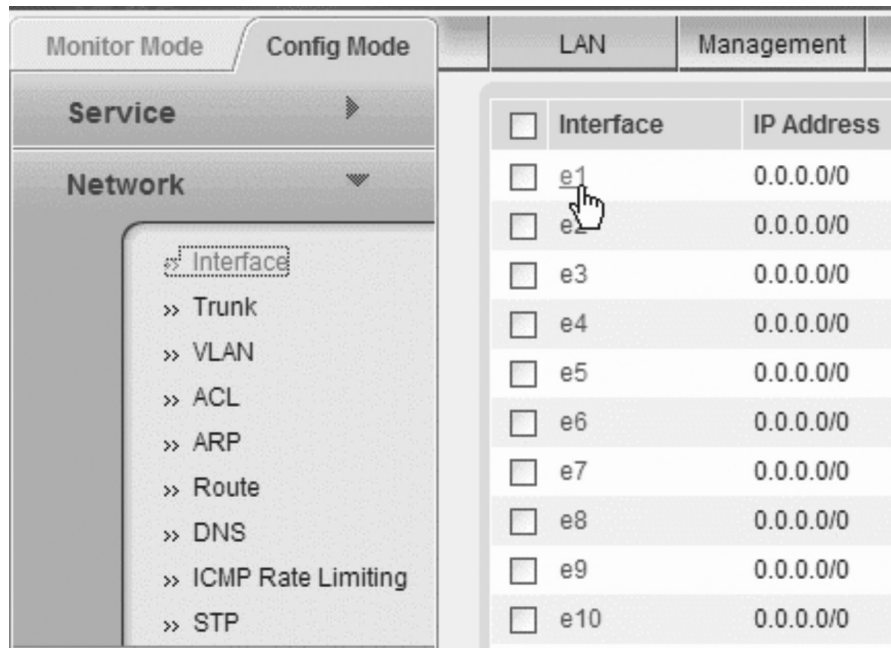


Figure 3: Select the interface



Figure 4: Enter the IP address and mask for e1

Add the Default Gateway

1. Select Config Mode > Network > Route.
2. Click Add.
3. In the IP Address Prefix field, enter 0.0.0.0.
4. In the Netmask field, enter 0.0.0.0.
5. In the Gateway field, enter 172.16.0.1.
6. Click OK. The default route appears in the route table.

Set up HA

1. Select Config Mode > HA > Setting.
2. On the General tab, select "1" from the Identifier drop-down list.
3. Click Enabled next to HA Status.
4. Click Enabled next to Preempt Status.
5. In the HA Mirroring IP Address field, enter the IP address of AX2 (172.16.0.12 in this example).
6. Enter Group parameters:
 - a. Expand the Group tab.
 - b. Select "1" from the Group Name drop-down list.
 - c. In the Priority field, enter 100.
 - d. Click Add.
7. Click OK at the bottom of the page.
8. Enable SSH access on the HA interface:
 - a. Select Config Mode > System > Access Control.
 - b. Select the SSH checkbox in the row for ethernet1.

The screenshot shows the 'Setting >> HA Global' configuration page. It is divided into several sections:

- General:** A table of configuration fields.

Identifier:*	1	Set ID:	
HA Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Preempt Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Time Interval:	2		100ms
HA Mirroring IP Address:	172.16.0.12		
Timeout Retries:	5		Seconds
ARP Retry:	4		
- Group:** A section for managing HA groups.
 - Group Name: 1 (dropdown), Priority: (empty field)
 - Buttons: + Add, - Delete
 - Table:

Group Name	Priority
1	100
- Other sections:** Floating IP Address, Status Check, and an OK button at the bottom.

Click OK.

Figure 5: Set up HA

Set up a Service Group for the SA Series Cluster

1. Select Config Mode > Service > SLB.
2. On the menu bar, select Service Group.
3. Click Add.
4. For the Name, enter "sa_group."
5. For the Type, leave "TCP" selected.
6. For the load-balancing Algorithm, select Least Connection.
7. Configure an HTTPS health monitor:
 - a. In the Health Monitor drop-down list, select "create." The configuration tabs for configuring a health monitor appear.
 - b. In the Name field, enter "sa_monitor."
From the Type drop-down list, select HTTPS.
 - c. Click OK. The service group configuration tabs reappear.
8. Add the SA Series servers:
 - a. On the Server tab, in the Server field, enter the IP address of an SA Series server. (In this example, enter 172.16.0.61.)
 - b. In the Port field, enter 0.
 - c. Click Add.
 - d. Repeat for the second SA Series server, but enter IP address 172.16.0.62.
9. Click OK at the bottom of the page to finish creating the service group.

SLB >> Service Group >> Create

Service Group

Name:	sa_group
Type:	TCP
Algorithm:	Least Connection
Health Monitor:	
Min Active Members:	ping
Description:	create ...

Service Group >> Health Monitor

Health Monitor

Name:	sa_monitor	
Retry:	3	
Consec Pass Req'd:	1	
Interval:	30	Seconds
Timeout:	5	Seconds

Method

Override IPv4:	
Override IPv6:	
Override Port:	
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External
Type:	HTTPS
Port:	443
Host:	
URL:	GET /
User:	
Password:	
Expect:	<input checked="" type="radio"/> Text <input type="radio"/> Code

Figure 6: Configure the health monitor

SLB >> Service Group >> Create

Service Group

Name: *	<input type="text" value="sa_group"/>		
Type:	TCP ▼		
Algorithm:	Least Connection ▼		
Health Monitor:	sa_monitor ▼		
Min Active Members:	<input type="checkbox"/>		
Description:	<div style="border: 1px solid gray; height: 20px;"></div>		

Server

IPv4/IPv6: IPv4 IPv6

Server: * ▼ Port: *

Server Port Template(SPT): ▼ Priority: ▼

		Server	Port	SPT	Priority	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	172.16.0.61	0	default	1	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	172.16.0.62	0	default	1	

Figure 7: Add the servers

Set up the Source NAT Pool

1. Select Config Mode > Service > SNAT.
2. Click Add.
3. In the Name field, enter "sa_snat."
4. In both IP Address fields, enter 172.16.0.51.
5. In the Netmask field, enter 255.255.255.0.
6. From the HA Group drop-down list, select "1."
7. Click OK.

IP Source NAT >> IPv4 Pool >> Create

IPv4 Pool	
Name: *	sa_snat
Start IP Address: *	172.16.0.51
End IP Address: *	172.16.0.51
Netmask: *	255.255.255.0
Gateway:	
HA Group:	1

Figure 8: Configure the source NAT pool

Set up the Virtual Server

1. Select Config Mode > Service > SLB.
2. On the menu bar, select Virtual Server.
3. Click Add.
4. In the Name field, enter "sa_vip."
5. In the IP Address field, enter the IP address at which clients will request the SA Series service. This is the IP address that DNS should send when replying to client queries for the SA Series service. In this example, enter 172.16.0.50.
6. From the HA Group drop-down list, select the HA group configured previously (group ID "1").
7. Configure a virtual port:
 - a. On the Port tab, click Add. The Virtual Server Port tab appears.
 - b. From the Type drop-down list, select TCP if not already selected.
 - c. In the Port field, enter "443."
 - d. From the Service Group drop-down list, select "sa_group."
 - e. Select Enabled next to HA Connection Mirror.
 - f. From the Source NAT Pool drop-down list, select "sa_snat."
 - g. From the Persistence Template Type drop-down list, select Source IP Persistence Template.
 - h. From the Source IP Persistence Template field, select "create." The configuration tab for the template appears.
 - i. In the Name field, enter "sa_source."
 - j. In the Timeout, change the value to 20.
 - k. Click OK to return to the Virtual Server Port tab. The port appears on the Port tab.
8. Click Add again to configure another virtual port. For this port, use the following settings:
 - Type – Others
 - Port – 0
 - Service Group – sa_group
 - Source NAT Pool - sa_snat
 - Source IP Persistence Template – sa_source
9. Click OK.
10. Click OK again to finish creating the virtual server.

SLB >> Virtual Server >> Create

General

Name: *	sa_vip	<input type="checkbox"/> Wildcard
IP Address: *	172.16.0.50	<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	
HA Group:	1	<input type="checkbox"/> Dynamic Server Weight
Virtual Server Template:	default	
Description:		

Port

<input type="checkbox"/>	Status	Port	Type	Service Group	
					<input checked="" type="button" value="Add"/> <input checked="" type="button" value="Edit"/> <input checked="" type="button" value="Delete"/> <input checked="" type="button" value="Enable"/> <input checked="" type="button" value="Disable"/>

Figure 9: Enter general settings and click Add to include a virtual port

SLB >> Virtual Server >> Port >> Create

Virtual Server Port

Name:	sa_vip
Type: *	TCP
Port: *	443
Service Group:	sa_group
Connection Limit:	<input type="checkbox"/> 1000000 <input checked="" type="radio"/> Drop <input type="radio"/> Reset
<input checked="" type="checkbox"/>	Use default server selection when preferred method fails
<input type="checkbox"/>	Use received hop for response
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HA Connection Mirror:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Direct Server Return:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SYN Cookie:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	sa_snat
aFlEx:	
TCP Template:	
Persistence Template Type:	Source IP Persistence Template
Source IP Persistence Template:	sa_source
Policy Template:	

ACL-SNAT Binding:

Access List:	1	<input checked="" type="button" value="Add"/>
Source NAT Pool:	sa_snat	<input checked="" type="button" value="Update"/>
<input type="checkbox"/> Access List	Source NAT Pool	<input checked="" type="button" value="Delete"/>

Figure 10: Configure port settings (settings for port 443 shown)

Virtual Server Port >> Template >> Source IP Persistence

Source IP Persistence

Name: *	sa_source	
Match Type:	Port	
Timeout:	20	Minutes
Don't Honor Conn Rules:	<input type="checkbox"/>	
Netmask:		

OK Cancel

Figure 11: Configure the source-IP persistence template

SLB >> Virtual Server >> sa_vip

General

Name: *	sa_vip		
IP Address: *	172.16.0.50		
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
ARP Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
HA Group:	1	<input type="checkbox"/> Dynamic Server Weight	
Virtual Server Template:	default		
Description:			

Port

<input type="checkbox"/>	Status	Port	Type	Service Group	
<input checked="" type="checkbox"/>	✓	443	TCP	sa_group	<input checked="" type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Disable
<input checked="" type="checkbox"/>	✓	0	Others	sa_group	

OK Cancel

Figure 12: Virtual ports configured and listed on the Port tab

Configure AX2

Add the IP Address to the Interface

1. Select Config Mode > Network > Interface.
2. In the Interface column, click on "e1."
3. Expand the IPv4 tab.
4. Enter the IP address and mask in the IP Address and Mask fields. In this example, enter 172.16.0.12 and 255.255.255.0.
5. Click OK at the bottom of the window. The interface list reappears.

Add the Default Gateway

1. Select Config Mode > Network > Route.
2. Click Add.
3. In the IP Address Prefix field, enter 0.0.0.0.
4. In the Netmask field, enter 0.0.0.0.
5. In the Gateway field, enter 172.16.0.1.
6. Click OK. The default route appears in the route table.

Set up HA

1. Select Config Mode > HA > Setting.
2. On the General tab, select "2" from the Identifier drop-down list.
3. Click Enabled next to HA Status.
4. Click Enabled next to Preempt Status.
5. In the HA Mirroring IP Address field, enter the IP address of AX1 (172.16.0.11 in this example).
6. Enter Group parameters:
 - a. Expand the Group tab.
 - b. Select "1" from the Group Name drop-down list.
 - c. In the Priority field, enter 90.
 - d. Click Add.
7. Click OK at the bottom of the page.
8. Enable SSH access on the HA interface:
 - a. Select Config Mode > System > Access Control.
 - b. Select the SSH checkbox in the row for ethernet2.
 - c. Click OK.

Setting >> HA Global

General

Identifier:*	2 <input type="button" value="v"/> Set ID: <input type="text"/>
HA Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Preempt Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Time Interval:	2 <input type="text"/> 100ms
HA Mirroring IP Address:	172.16.0.11 <input type="text"/>
Timeout Retries:	5 <input type="text"/> Seconds
ARP Retry:	4 <input type="text"/>

Group

Group Name: 1 Priority:

Group Name	Priority
1	90

Floating IP Address

Status Check

Figure 13: Set up HA (compare with the setup for AX1)

Synchronize the Load-Balancing Configuration from AX1 to AX2

1. Select Config Mode > HA > Config Sync.
2. Enter the admin username and password required for Enable access to AX1 (in this example, "admin" and "a10").
3. Click OK.

Sync Operation

User: *	admin <input type="text"/>
Password : *	••• <input type="text"/>
Sync All Partitions :	<input type="checkbox"/>
Operation:	<input checked="" type="radio"/> All <input type="radio"/> Data Files <input type="radio"/> Running-config <input type="radio"/> Startup-config
Peer Option:	<input checked="" type="radio"/> To running-config <input type="radio"/> To startup-config <input checked="" type="checkbox"/> With Reload

Figure 14: HA Config Sync

SA6500 Active-Active Configuration

Table 1: License

NODE	LICENSE	COMMENT
sa6500-c	<ul style="list-style-type: none"> Enables 5,000 simultaneous users of SA6500 Enables Juniper Networks Secure Application Manager and Network Connect for SA6500 	<ul style="list-style-type: none"> License for total concurrent users License to use Network Connect
sa6500-d	<ul style="list-style-type: none"> Enables clustering: Allows 5,000 additional users to be shared from another SA6500 	<ul style="list-style-type: none"> Clustering license for second node

Creating a Cluster in sa6500-c

- To create a new cluster, choose...

Create New Cluster

Create

Type: SA-6500

Cluster Name: Name of the cluster to create. Must be alphanumeric, "-", or "_"; and must start with a letter.

Cluster Password: Shared secret among the nodes in the cluster. Must be at least 6 characters long

Confirm Password: Shared secret among the nodes in the cluster. Must match the password you typed in the previous line

Member Name: Name of this node in the cluster. Must be alphanumeric, "-", or "_"

Create Cluster

Confirm Create Cluster

Are you sure you want to create a new cluster *sa-dcb* ?

Please click **Create** to create a new cluster and add this appliance with member name *sa6500-c* to the cluster. Click **Cancel** if you do not want to create a cluster.

Create Cancel

- By default, a cluster is created in the active-active configuration. To modify the settings, choose **Clustering > Properties**. Then make your changes. For instance, you can select **disable external interface when internal interface fails** as shown here.

Clustering

Status Properties

Type: SA-6500

Cluster Name: sa-dcb

Cluster Password: [password field]

Confirm Password: [password field]

Configuration Settings

Active/Passive configuration
This is a high-availability failover mode, in which one node is active while the other is held as backup.

Internal VIP: [text field]

External VIP: [text field]

Active/Active configuration
This mode requires an external load-balancer.

Synchronization Settings

Protocol: Unicast Multicast Broadcast

Synchronize log messages
WARNING:Enabling the cluster 'Synchronize log messages' feature results in large data transfers between bandwidth to support such transfers.

Synchronize user sessions

Synchronize last access time for user sessions

Network Healthcheck Settings

Number of ARP Ping failures before interface is disabled (should be greater than 0): 3

Disable external interface when internal interface fails

Advanced Settings

Save Changes Delete Cluster...

- When you are finished making changes, click the **Save Changes** button.

Adding a Cluster Member in sa6500-c

4. Before a cluster member can join a cluster, you need to define it. Choose **Clustering > Status**. Two cluster members, sa6500-c and sa6500-d, are defined in the following screenshot.

The screenshot shows the Clustering Status page for a cluster named 'sa-dcb'. The page includes tabs for 'Status' and 'Properties'. Below the cluster name, it shows 'Type: SA-6500' and 'Configuration: Active/Active'. There are buttons for 'Add Members...', 'Enable', 'Disable', and 'Remove'. A table lists the cluster members:

<input type="checkbox"/>	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
<input checked="" type="checkbox"/>	* sa6500-c	8.8.9.9/25	172.16.8.61/23	●	Leader	0	
<input type="checkbox"/>	sa6500-d	8.8.9.8/25	172.16.8.62/23	●	Enabled, Unreachable	0	

* Indicates the node you are currently using

5. To add a member to the cluster, select the cluster on the **Status** tab.

The screenshot shows the Clustering Status page for a cluster named 'sa-dcb'. The page includes tabs for 'Status' and 'Properties'. Below the cluster name, it shows 'Type: SA-6500' and 'Configuration: Active/Active'. There are buttons for 'Add Members...', 'Enable', 'Disable', and 'Remove'. A table lists the cluster members:

<input type="checkbox"/>	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
--------------------------	-------------	------------------	------------------	--------	-------	-----------	--------

6. Click the **Add Members** button. The following screenshot shows how to add sa6500-d as a cluster member.
7. Click the **Add** button to include the cluster member.

Joining a Cluster in sa6500-d

1. After cluster information has been defined for sa6500-c, it is time for sa6500-d to join the cluster. Log in to sa6500-d admin URL and choose **Cluster > Join**. Enter the cluster name, cluster password, and existing member address (for example, the internal address of sa6500-c).

Join Existing Cluster

Join

Cluster Name: Name of the cluster to join

Cluster Password:

Existing Member Address: Internal IP address of any existing cluster member

Join Cluster

Confirm Join Cluster

This node will next contact the cluster member '8.8.9.9' and ask to join the cluster sa-dcb. If this succeeds, the node will join as member of the cluster.

WARNING: This host's entire state will be overwritten with the current cluster configuration, including bookmarks, IP address, netmask etc.

Please click **Join** to join the cluster.
Click **Cancel** to return to the previous page.

Join **Cancel**

Monitoring a Cluster

1. To display the status of the current cluster, choose Clustering > Status.

Clustering

Status Properties

Cluster Name: sa-dcb
 Type: SA-6500
 Configuration: Active/Active

Add Members... Enable Disable Remove

<input type="checkbox"/>	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
<input type="checkbox"/>	* sa6500-c	8.8.9.9/25	172.16.8.61/23	●	Leader	0	<input type="text"/>
<input type="checkbox"/>	sa6500-d	8.8.9.8/25	172.16.8.62/23	●	Enabled	0	<input type="text"/>

2. To display a dashboard showing the system status for all cluster members, choose System > Status.

System Status

Overview Active Users Meeting Schedule

Critical Events
 Page Settings

System Version
 6.0R3.1 (build 12507)
[Download Package](#)

Last Reboot
 3 days, 19 hours, 34 minutes, 44 seconds

System Date & Time [Edit](#)
 2009-03-10
 01:36:07 PM

Logging Disk: 0% Full

Max Licensed Users: 5000

Signed-In Users: 1

Signed-In Mail Users: 0

Member Status

- sa6500-c *
- sa6500-d

* Node currently used

System Capacity Utilization Graphs display last 1 hour

Concurrent Users (Edit | Download) sa6500-c

Local users Concurrent users Local MC Users MC Users

Concurrent Meeting Graph (Edit | Download) sa6500-c

Meetings

Hits Per Second (Edit | Download) sa6500-c

Hits Web Hits File Hits Client-Server Hits

CPU and Virtual (Swap) Memory Utilization (Edit | Download) sa6500-c

SA Series Configuration References

- SA Series system software downloads: <http://www.juniper.net/techpubs/software/ive/>
- Juniper Networks Knowledge Base: <http://kb.juniper.net/>
- SSL VPN (IVE) Version 6.0 technical documents: <http://www.juniper.net/techpubs/software/ive/6.x/6.0/>

Summary

The SSL VPN solution consisting of Juniper Networks SA Series SSL VPN Appliances and A10 Networks AX Series provides one of the most reliable and scalable secure access solutions. New and existing SSL VPN deployments alike can benefit from AX Series features including configurable health monitors, flexible load balancing, and persistence (“stickiness”) options—and HA. hardware-based DDoS protection detects and drops unfriendly TCP traffic while allowing legitimate user traffic to the SA Series nodes. HA eliminates service interruption due to AX or link unavailability. GSLB provides additional flexibility and ease of use, enabling a single-user access experience across multiple sites—regardless of user location—while transparently directing the user to the best site based on site health, user location, and other configurable metrics.

AX Series server load balancers allow SA Series deployments to scale in support of today’s mobile workforce. Tomorrow’s ever-increasing numbers of users—running increasingly bandwidth-intensive applications—continue to enjoy fast, reliable secured access without the need to manage and utilize multiple URLs due to user location or network load. For additional AX Series information, please visit www.a10networks.com.

About A10 Networks

A10 Networks was founded in Q4 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, EMEA, Japan, China, Korea and Taiwan. For more information, visit www.a10networks.com.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King’s Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.