Implementation Guide

Radware AppDirector and Juniper Networks Secure Access SSL VPN Solution Implementation Guide

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Part Number: 801008-001 August 2008

Table of Contents

Introduction

As enterprises continue to increase the number of employees, partners, suppliers and contractors accessing their corporate resources remotely, it becomes an increasingly critical mandate for IT leaders to provide remote access that is secure, scalable, highly available and cost-effectively deployed. Juniper Networks Secure Access (SA) SSL VPN, combined with Radware's AppDirector application delivery platform, provides a best-in-class SA solution for secure, cost-effective, remote application access.

Scope

This document is intended for end users and technical systems engineers who will be deploying a joint Juniper Networks SA – Radware AppDirector solution. This guide provides detailed configuration and setup information for implementing this joint solution.

Design Considerations

Radware AppDirector Products

- Software: AppDirector Version 1.06.07
- Platform: AppDirector OnDemand Switch 2 (ODS 2)
- Performance: Throughput support from 1 to 4 Gbps with license-based upgrades. OnDemand Switch 2 supports 5 million simultaneous user with a default 2 GB of RAM or 8 million simultaneous users with 4 GB of RAM

Juniper Networks Infranet Controller (IC) Products

- Software: 6.0R3.1 (build 12507)
- Platform: Juniper Networks Secure Access 6000 (SA 6000) SSL VPN
- Performance: 5000 simultaneous users per appliance

Solution Overview

Radware AppDirector, in combination with Juniper Networks SA SSL VPN, is designed to provide a highly scalable and highly available subsystem for deploying SA solutions. The SA 6000 devices are configured in an active-active cluster, with individual components queried for service availability by AppDirector. Using this important health monitoring information, AppDirector can calculate availability. Using existing load information, AppDirector can provide highly granular load distribution both locally and globally, if remote SA clusters are available. AppDirector maintains client sessions for persistency and works in conjunction with SA SSL VPN state replication logic to ensure session survivability through SA SSL VPN failover events. Together the two components help ensure zero loss connectivity, offering a best-in-class solution.

Juniper Networks Secure Access Secure Sockets Layer VPN Overview

Juniper Networks© Secure Access (SA) leads the Secure Sockets Layer (SSL) VPN market with a complete range of remote-access appliances. Juniper Networks SSL VPN security products have a variety of form factors and features that can be combined to meet the needs of companies of all sizes, from small to medium-sized businesses (SMBs) that need VPN access for remote and mobile employees to large global deployments that need to provide secure remote and extranet access for employees, partners, and customers from a single platform. Juniper Networks SSL VPNs are based on the Instant Virtual Extranet (IVE) platform, which uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for client software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper Networks SA SSL VPN appliances combine the overall benefit of a lower total cost of ownership (TCO) than traditional IP Security (IPSec) client solutions with unique end-to-end security features. Enhanced remote access methods enable the enterprise to provision access by purpose for almost any resource, including those that are jitter or latency sensitive.

Radware AppDirector Overview

Radware AppDirector is an intelligent application delivery controller that provides scalability and application-level security for service infrastructure optimization, fault tolerance, and redundancy.

AppDirector combines the power of Radware multi-gigabit application switching hardware with APSolute OS service-smart networking to ensure local and global server availability and accelerated application performance and safeguard services with integrated intrusion prevention and denial of service (DoS) protection for fast, reliable, secure service delivery.

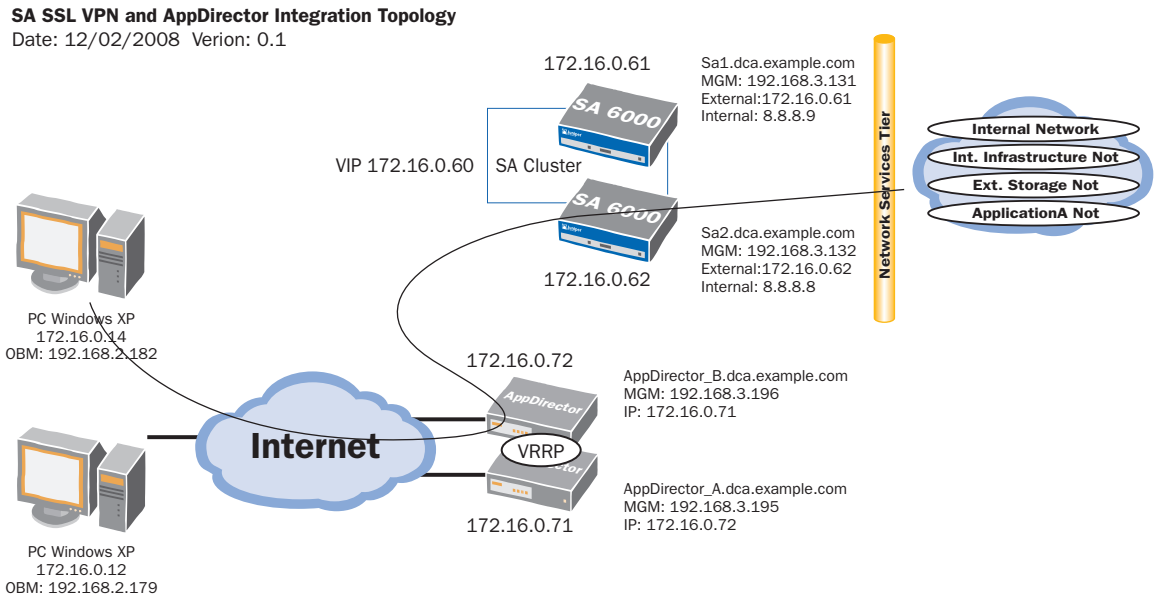
AppDirector uses advanced Layer 4 through 7 policies and granular service intelligence, enabling end-to-end service-smart networking and aligning service infrastructure operations with service front-end requirements to eliminate traffic surges, infrastructure bottlenecks, connectivity disconnects, and downtime for assured service access and full-service continuity and redundancy.

AppDirector enables fine-tuning of service behavior at all critical points, end to end, based on granular service-specific classification of packets to optimize traffic flows for a wide range of services, including support for Hypertext Transfer Protocol (HTTP), HTTP over Secure Sockets Layer (HTTPS), Multipurpose Internet Mail Extensions (MIME), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), voice over IP (VoIP; Session Initiation Protocol, or SIP), streaming media (Real-Time Transfer Protocol, or RTP), RADIUS, Diameter, and secure Lightweight Directory Access Protocol (LDAP) applications.

AppDirector lets you get the most out of your service investments by maximizing the utilization of service infrastructure resources and enabling seamless consolidation and high scalability. Make your network adaptive and more responsive to your dynamic services and business needs with AppDirector fully integrated traffic classification and flow management, health monitoring and failure bypassing, traffic redirection, bandwidth management, intrusion prevention, and DoS protection.

For more information, please visit http://www.radware.com/.

Figure 1. Secure Access SSL VPN and AppDirector Integration Topology



Radware Benefits for Juniper Networks Secure Access SSL VPN Solutions

Juniper and Radware have conducted complete interoperability testing and developed integrated solutions using the Radware AppDirector and Juniper Networks SA SSL VPN products. This strong interoperability and integration provides a solution that delivers industry-leading scalability, security, and performance for those deploying SA solutions.

Radware AppDirector and Juniper Networks Secure Access SSL VPN Local High Availability Interoperability Tests and Configurations

This section describes the interoperability tests performed and presents the steps for configuring AppDirector. There are separate configuration steps to be taken on the primary (active) and backup AppDirector devices, so the configuration discussion is divided into two parts: one for the primary device, and one for the backup device.

Tests Conducted for Local Solution Validation

The tests listed in Table 1 were conducted to ensure that the most appropriate solution was defined and validated. All tests were successfully completed using the AppDirector configurations that follow Table 1.

Table 1. Tests Conducted for Solution Validation

Test Case	Description
AppDirector: Virtual IP and service farm	Verify that the virtual IP address and service farm defined in the load balancer work as expected.
AppDirector: Dispatch algorithm	Verify that a new request follows the least connection policy (configured dispatch method).
AppDirector: Persistency or session affinity	Verify that SSL VPN establishes Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) and Encapsulated Security Payload (ESP) connection with the same server and maintains the selected server throughout the life of a session.
AppDirector HA: Master failover	Verify that the load balancer HA setting prevents a single point of failure (SPOF) and that VRRP fails over properly.
AppDirector HA: Backup assuming master Virtual Router Redundancy Protocol (VRRP) role	Verify that the load balancer maintains a client's sessions during a failover event. This validates the state replication logic between AppDirector controllers, ensuring session survivability through failover.
AppDirector HA: Master failback	Verify that the SSL VPN clients maintain connectivity and that VRRP role exchange occurs as expected.
SA cluster: Failover	Verify that AppDirector detects SA failure and dynamically manages new requests and reconnections to the available SA appliances.
SA cluster: New service	Verify that AppDirector detects new SA service elements without affecting existing sessions.

Primary AppDirector Configuration

This section details the step-by-step AppDirector configuration process, using the Web-based management GUI, for creating the Juniper Networks SA SSL VPN and Radware AppDirector local HA subsystem. Please refer to Figure 1 for topology and addressing information.Primary AppDirector Configuration

Initial Primary AppDirector Configuration

1. Using a serial cable and a terminal emulation program, connect to the AppDirector.

   The default console port settings are:

   - Bits per Second: 19200
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None

2. Enter the following command to assign management IP address 192.168.3.195 / 24 to interface 17 (dedicated management interface) of AppDirector:

```
net ip-interface create 192.168.3.195 255.255.255.0 17
```

Note: Connectivity to AppDirector can be established at this time if the client resides on the same management subnet.

3. Enter the following command line to assign IP address 172.16.0.71 / 23 to interface 1 (production traffic connectivity) of AppDirector:

```
net ip-interface create 172.16.0.71 255.255.254.0 1
```

4. Enter the following command to create a default gateway route entry on AppDirector pointing to 172.16.0.1:

```
net route table create 0.0.0.0 0.0.0.0 172.16.0.1 -i 1
```

5. Using a browser, connect to the management IP address of AppDirector (192.168.3.195) via HTTP or HTTPS. The default username and password are **radware** and **radware**.

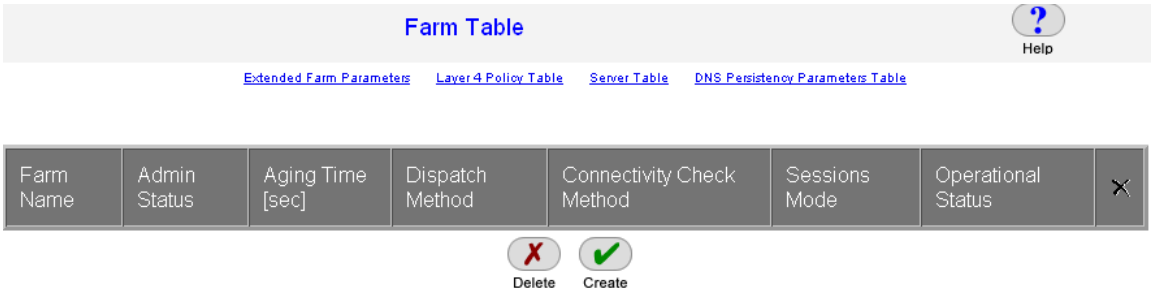
Failure to establish a connection may be due to the following:

- Incorrect IP address in the browser
- Incorrect IP address or default route configuration in AppDirector
- Failure to enable Web-based management or secure Web-based management in AppDirector

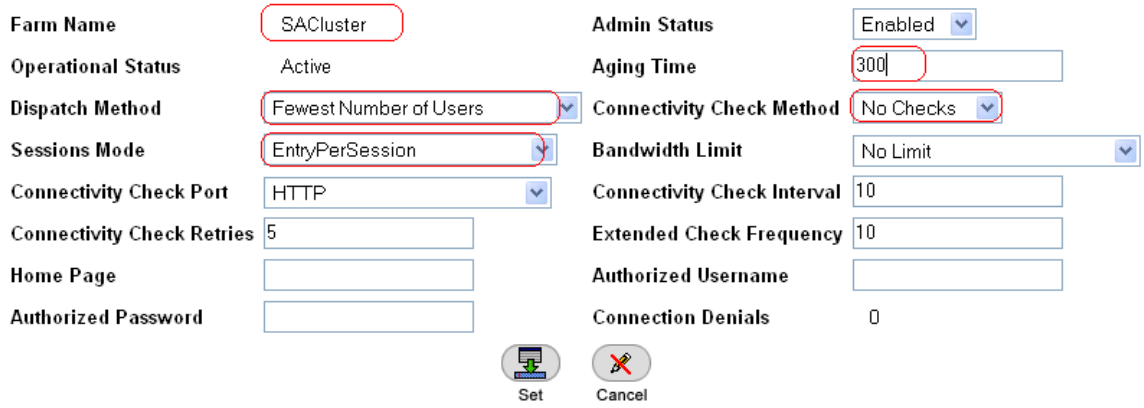
If AppDirector can be successfully pinged, attempt to connect to it via Telnet or SSH. If the pinging or the Telnet or SSH connection is unsuccessful, reconnect to AppDirector via its console port. After you are connected, verify and correct the AppDirector configuration as needed.[1]

Farm Configuration

1. From the menu, choose **AppDirector** > **Farms** > **Farm Table** to display the Farm Table page.



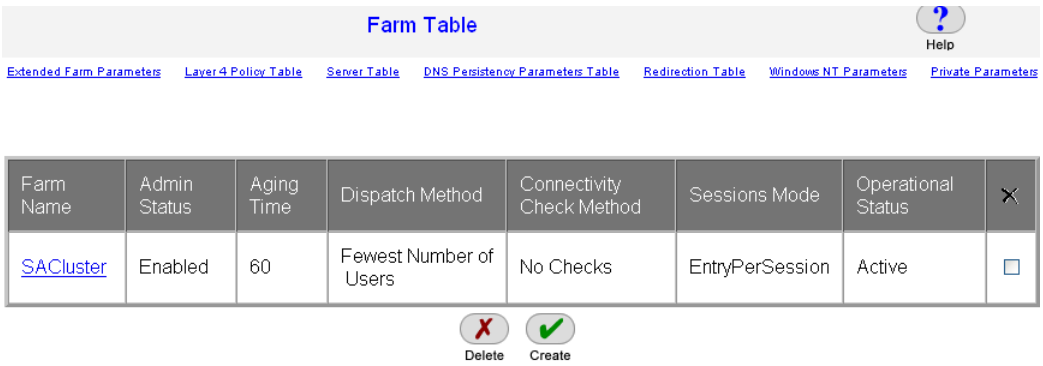
2. Click the **Create** button.
3. On the **Farm Table Create** page, enter the necessary parameters as shown here.[2]



Note: The Aging Time value corresponds to Juniper Networks SA Network Connect remote-access client session timers. The AppDirector Aging timer should be just higher than the highest expected expiration interval between ESP and SSL tunnels. By default, the highest expiration value belongs to the SSL tunnels, with an expiration interval of 270 seconds. These values are configurable, so if you change them, you should also consider the farm Aging Time value (300 seconds is used for the timer in the preceding screenshot).

4. Click the Set button to save the parameters.
5. Verify that the new entry was created on the **Farm Table** page:

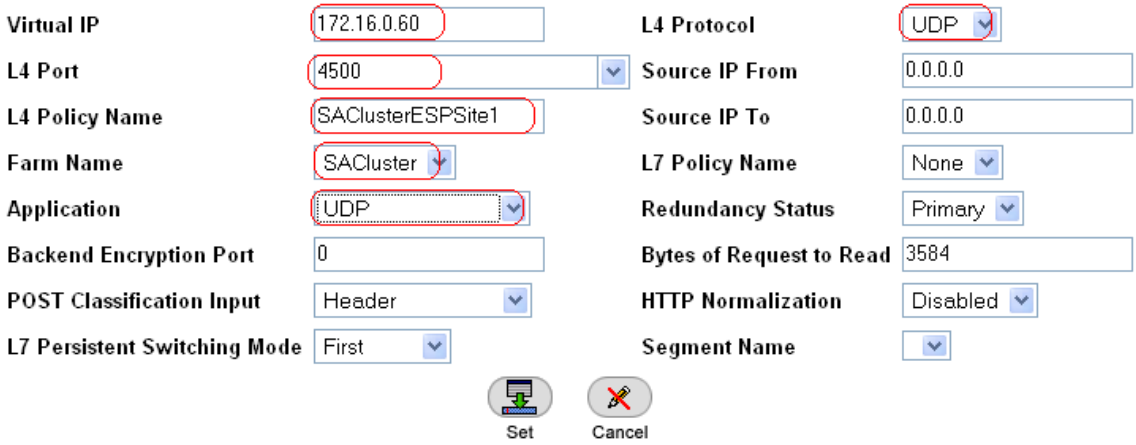
[1]To enable Web-based management from the console command-line interface, enter **manage web status set enable.**
[2]Throughout this guide, items circled in red indicate settings that need to be entered or changed. Items not circled should be left at the default settings.



Layer 4 Policy Configuration

1. From the menu, choose **AppDirector** > **Layer 4 Farm Selection** > **Layer 4 Policy Table** to display the Layer 4 Policy Table page.

2. Click the **Create** button.
3. On the **Layer 4 Policy Table Create** page, enter the necessary parameters as shown here.



Note: This Layer 4 policy is for ESP tunnels.

4. Click the **Set** button to save the parameters.
5. On the **Layer 4 Policy Table**, click the **Create** button.
6. On the **Layer 4 Policy Table Create** page, enter the necessary parameters as shown here.

Virtual IP	172.16.0.60	**L4 Protocol**	TCP
L4 Port	443	**Source IP From**	0.0.0.0
L4 Policy Name	SAClusterSSLSite1	**Source IP To**	0.0.0.0
Farm Name	SACluster	**L7 Policy Name**	None
Application	HTTPS	**Redundancy Status**	Primary
Backend Encryption Port	0	**Bytes of Request to Read**	3584
POST Classification Input	Header	**HTTP Normalization**	Disabled
L7 Persistent Switching Mode	First	**Segment Name**	

Set Cancel

Note: This Layer 4 policy is for SSL tunnels.

7. Click the **Set** button to save the parameters.
8. Verify that the new entries were created on the **Layer 4 Policy Table** page.

Virtual IP	L4 Protocol	L4 Port	Source IP From	L4 Policy Name	L7 Policy Name	Farm Name	✕
172.16.0.60	TCP	443	0.0.0.0	SAClusterSSLSite1	None	SACluster	☐
172.16.0.60	UDP	4500	0.0.0.0	SAClusterESPSite1	None	SACluster	☐

Delete Create

Client Network Address Translation Configuration

1. From the menu, choose **AppDirector** > **NAT** > **Client NAT** to display the Client NAT Global Parameters page.
2. On the **Client NAT Global Parameters** page, change the parameters as shown here.

Client NAT Global Parameters

Device Tuning Client NAT Intercept Table Client NAT Address Table

Client NAT Enabled

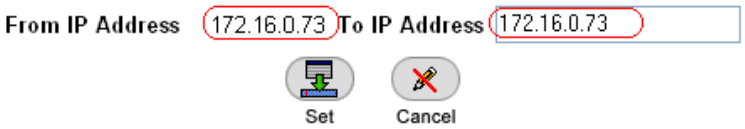
Set

3. Click the **Set** button to save the parameters.
4. Click the **Client NAT Intercept Table** hyperlink at the top of the configuration window.
5. Click the **Create** button.
6. On the **Client NAT Intercept Table Create** page, enter the necessary parameters as shown here.

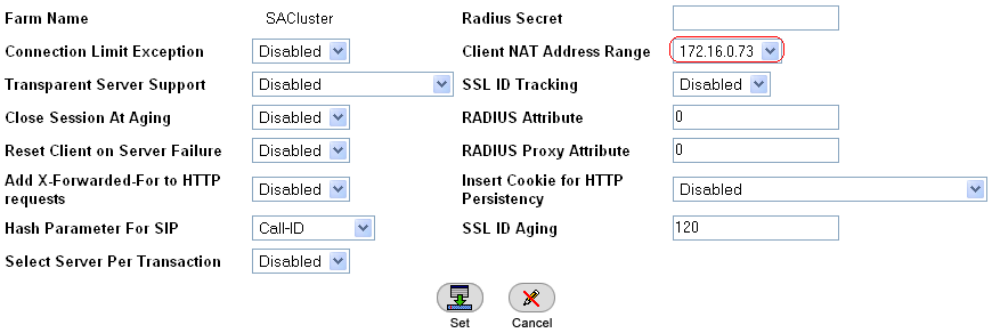
From Client IP 1.1.1.1 **To Client IP** 255.255.255.254

Set Cancel

7. Click the **Set** button to save the parameters.
8. Click the **Client NAT Address Table** hyperlink at the top of the configuration window.
9. Click the **Create** button.
10. On the **Client NAT Address Table Create** page, enter the necessary parameters as shown here.



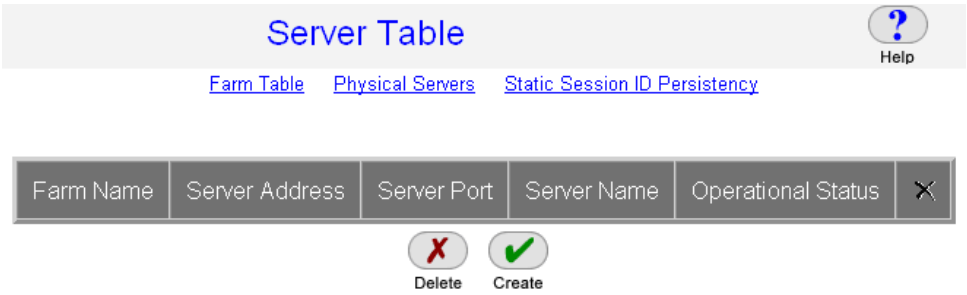
11. Click the **Set** button to save the parameters.
12. From the menu, choose **AppDirector** > **Farms** > **Farm Table** to display the Farm Table page.
13. Click the **Extended Farm Parameters** hyperlink near the top of the page.
14. On the **Extended Farm Parameters** page, click the **SACluster** farm name and enter the necessary parameters as shown here.



15. Click the **Set** button to save parameters.

Adding Servers to the Farm

1. From the menu, choose **AppDirector** > **Servers** > **Application Servers** to display the Server Table page.



2. On the **Server Table** page, click the **Create** button.
3. On the **Server Table Create** page, enter the necessary parameters as shown here.

Farm Name	SACluster	**Server Address**	172.16.0.61
Server Port	None	**Server Name**	SA1
Server Description		**Admin Status**	Enable
Operational Status	Active	**Weight**	1
Operation Mode	Regular	**Type**	Regular
Connection Limit	0	**Response Threshold [ms]**	0
Client NAT	Enabled	**Backup Server Address**	172.16.0.62
Redirect To		**Bandwidth Limit**	No Limit
Backup Preemption	Enable	**Client NAT Address Range**	0.0.0.0
FarmNameForLocalFarm	None		

Set Cancel

4. Click the **Set** button to save parameters.
5. Verify that the new entry was created on the **Server Table** page.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type	Connection Limit	Bandwidth Limit
SACluster	172.16.0.61	None	SA1	Active	Regular	Enable	Regular	0	No Limit

Delete Create

6. Create the second server using the information shown here.

Farm Name	SACluster	**Server Address**	172.16.0.62
Server Port	None	**Server Name**	SA2
Server Description		**Admin Status**	Enable
Operational Status	Active	**Weight**	1
Operation Mode	Regular	**Type**	Regular
Connection Limit	0	**Response Threshold [ms]**	0
Client NAT	Enabled	**Backup Server Address**	172.16.0.61
Redirect To		**Bandwidth Limit**	No Limit
Backup Preemption	Enable	**Client NAT Address Range**	0.0.0.0
FarmNameForLocalFarm	None		

Set Cancel

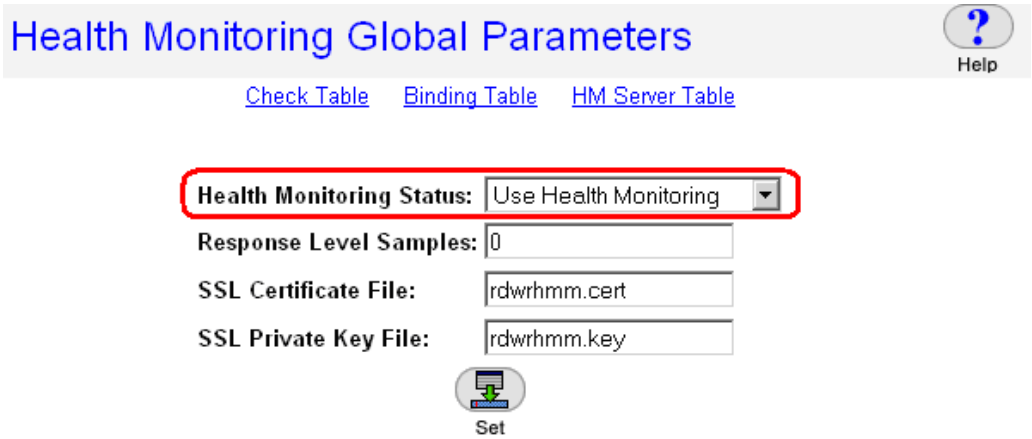
7. Verify that the second server entry was created on the **Server Table** page.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type	Connection Limit	Bandwidth Limit
SACluster	172.16.0.61	None	SA1	Active	Regular	Enable	Regular	0	No Limit
SACluster	172.16.0.62	None	SA2	Active	Regular	Enable	Regular	0	No Limit

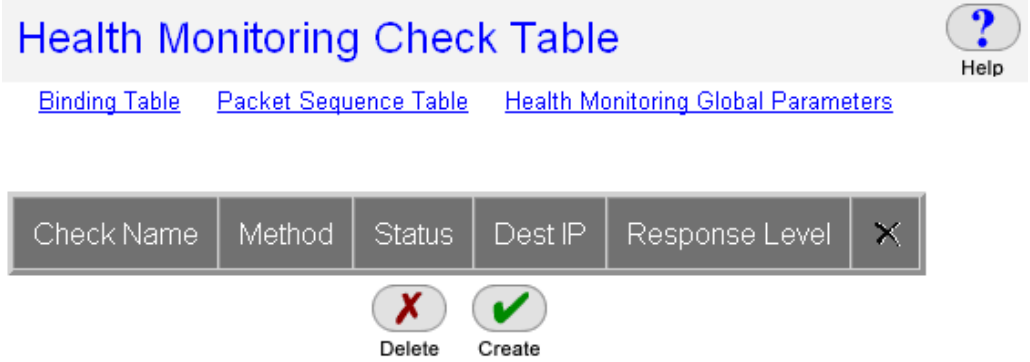
Delete Create

Health Monitoring Configuration

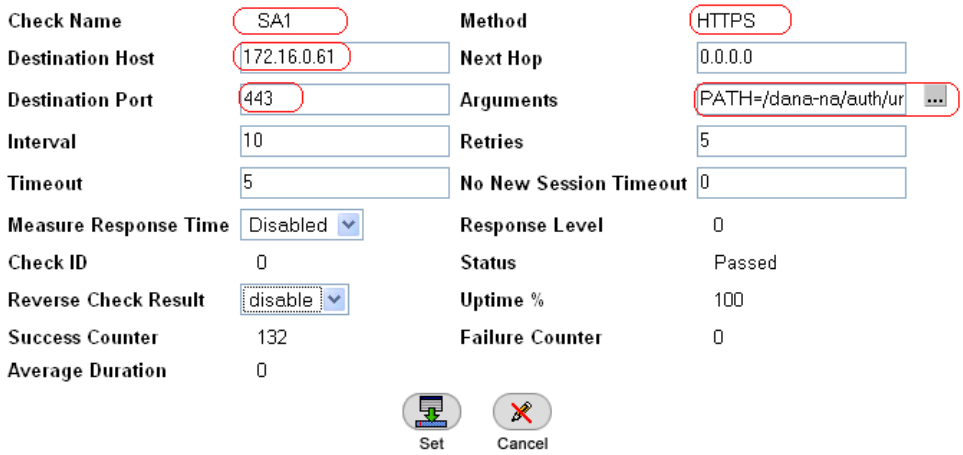
1. From the menu, choose **Health Monitoring > Global Parameters** to display the Health Monitoring Global Parameters page.
2. On the **Health Monitoring Global Parameters** page, change the parameters as shown here.



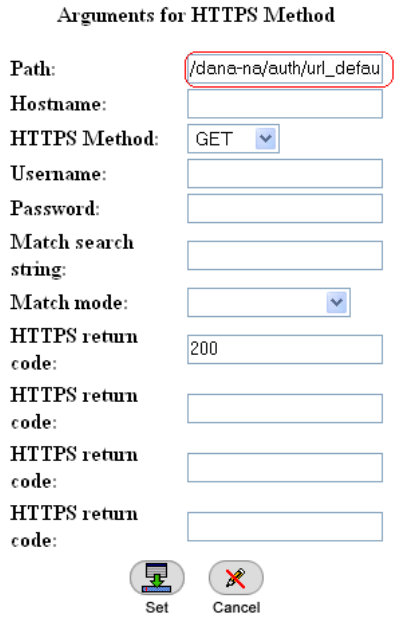
3. Click the **Set** button to save the parameters.
4. From the menu, choose **Health Monitoring > Check Table** to display the Health Monitoring Check Table page.



5. To create the health monitoring check for the first server, click the **Create** button.
6. On the **HM Check Table Create** page, enter the necessary parameters as shown here.



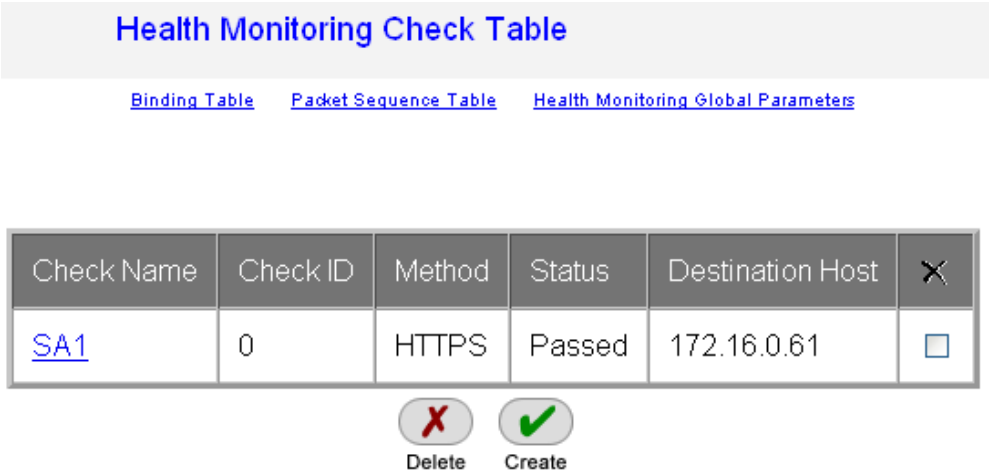
7. Click the button next to **Arguments** ... to populate the specific settings for the rest of this check.
8. Enter the information shown here.



Path = /dana-na/auth/url_default/welcome.cgi

9. Click the **Set** button for the method arguments; then click the **Set** button in the **HM Check Table Create** window.

The Health Monitoring Check Table should have a single entry as shown here.



The status of this check may be listed as Unknown until the server replies successfully to the AppDirector check.

10. Create the health monitoring check for the second server: If the **Health Monitoring Check Table** page is not already displayed from the previous step, choose **Health Monitoring > Check Table** from the menu.
11. Click the **Create** button.
12. On the **HM Check Table Create** page, enter the necessary parameters as shown here.

Check Name	SA2	**Method**	HTTPS
Destination Host	172.16.0.62	**Next Hop**	0.0.0.0
Destination Port	443	**Arguments**	PATH=/dana-na/auth/ur ...
Interval	10	**Retries**	5
Timeout	5	**No New Session Timeout**	0
Measure Response Time	Disabled	**Response Level**	0
Check ID	1	**Status**	Passed
Reverse Check Result	disable	**Uptime %**	100
Success Counter	159	**Failure Counter**	0
Average Duration	0		

Set Cancel

13. Click the button next to **Arguments** ... to configure the specific arguments for this check as shown here.

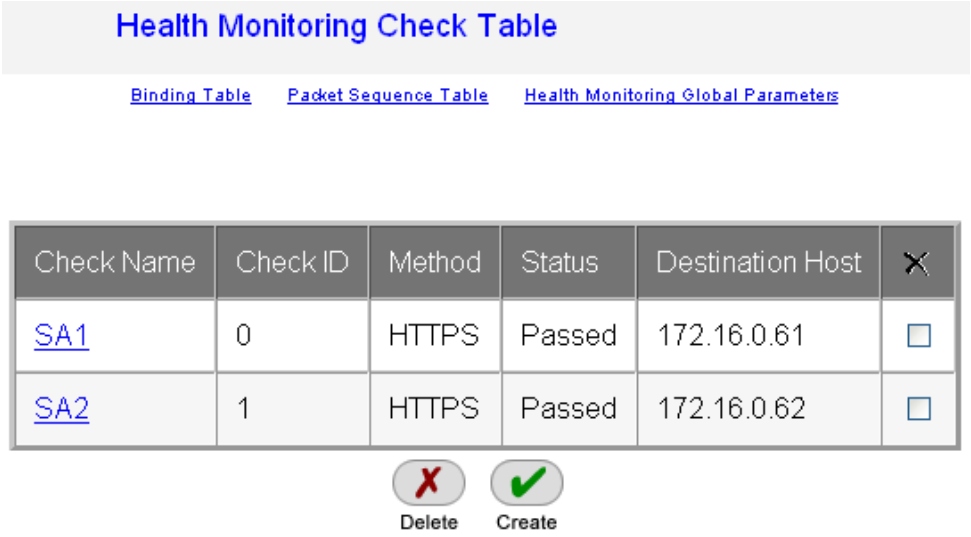
Arguments for HTTPS Method

Path:	/dana-na/auth/url_defau
Hostname:	
HTTPS Method:	GET
Username:	
Password:	
Match search string:	
Match mode:	
HTTPS return code:	200
HTTPS return code:	
HTTPS return code:	
HTTPS return code:	

Set Cancel

Path = /dana-na/auth/url_default/welcome.cgi

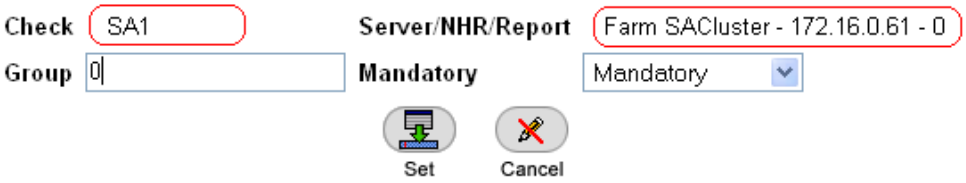
14. Click the **Set** button to save the method argument parameters.
15. Verify that the **Arguments** text box has been populated.
16. Click the **Set** button to save the health check.
17. Verify that the new entry was created on the **Health Monitoring Check Table** page.



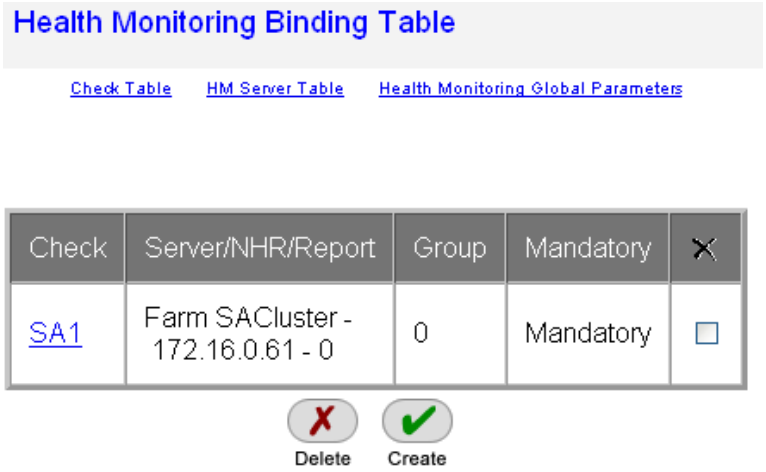
Binding Health Checks to Servers

1. To create the health monitoring binding for the first server, from the menu, choose **Health Monitoring** > **Binding Table** to display the Health Monitoring Binding Table page.

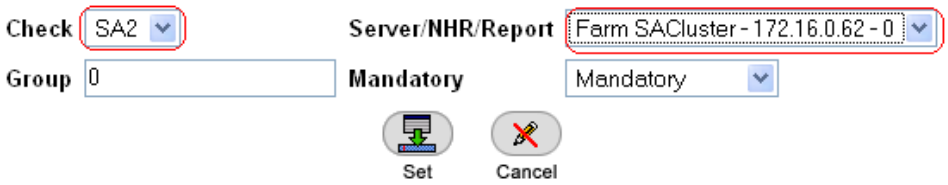
2. Click the **Create** button.
3. On the **HM Binding Table Create** page, enter the necessary parameters as shown here.



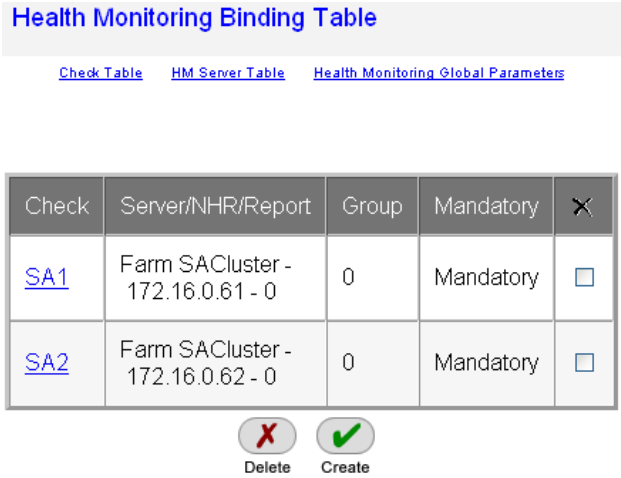
4. Click the **Set** button to save the parameters.
5. Verify that the new entry was created on the **Health Monitoring Table** page.



6. Create the health monitoring binding for the second server: If the **Health Monitoring Binding Table** page is not already displayed from the previous step, choose **Health Monitoring > Binding Table** from the menu.
7. Click the **Create** button.
8. On the **HM Binding Table Create** page, enter the necessary parameters as shown here.



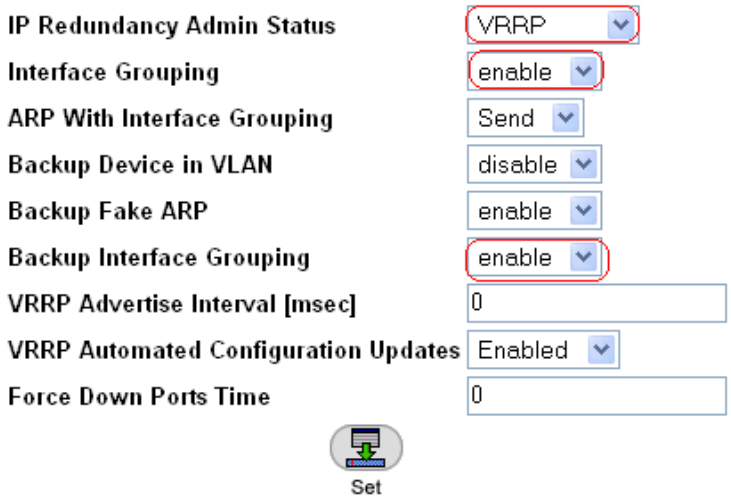
9. Click the **Set** button to save the parameters.
10. Verify that the new entry was created on the **Health Monitoring Binding Table** page.



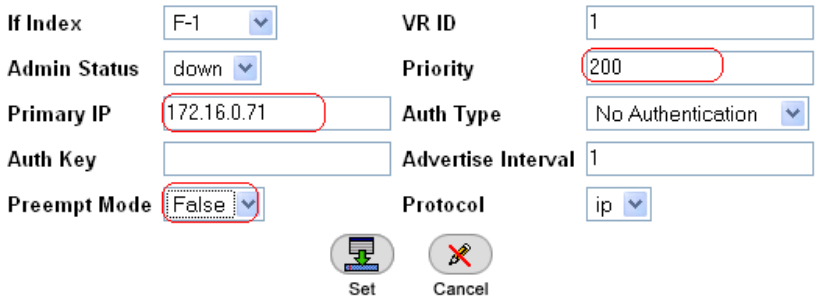
Primary AppDirector VRRP Configuration

Note: Radware offers two means of redundancy and failover between pairs of devices: proprietary and VRRP. Since VRRP is a more commonly used method within the industry, this section presents the steps to configure both AppDirector devices using that method.[3]

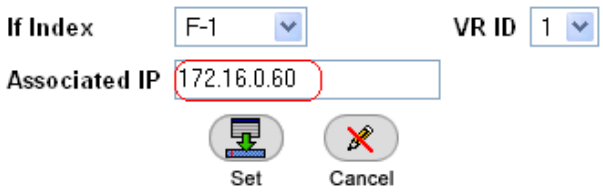
1. From the menu, choose **AppDirector** > **Redundancy** > **Global Configuration** and set the parameters as shown here.



2. Click the **Set** button to save these changes.
3. Choose **AppDirector** > **Redundancy** > **VRRP** > **Virtual Routers** and create a new entry.



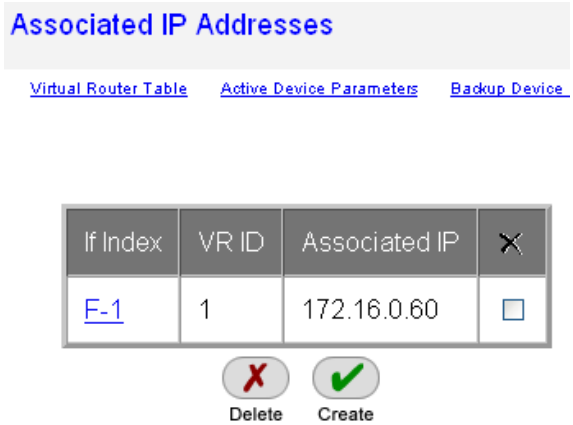
4. Click the **Set** button to save the parameters.
5. Choose **AppDirector** > **Redundancy** > **VRRP** > **Associated IP Addresses** and create a new entry.



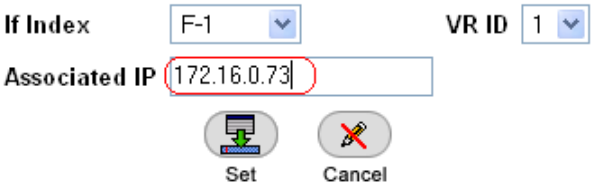
[3]For a detailed discussion of VRRP, see RFC 3768.

6. Click the **Set** button to save the parameters.

   The Associated IP Addresses window should have a single entry as shown here.

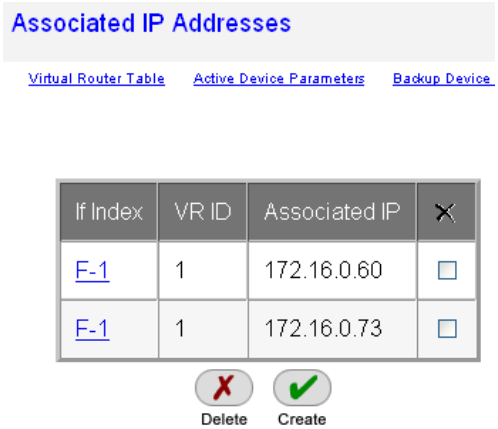


7. Create a second entry in the Associated IP Addresses table as shown here.

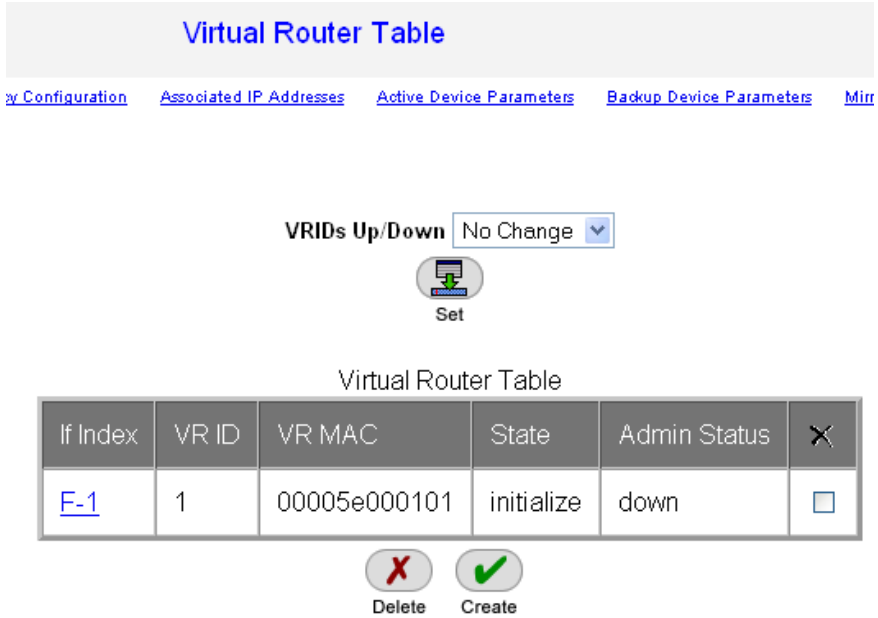


   This is the virtual IP address.

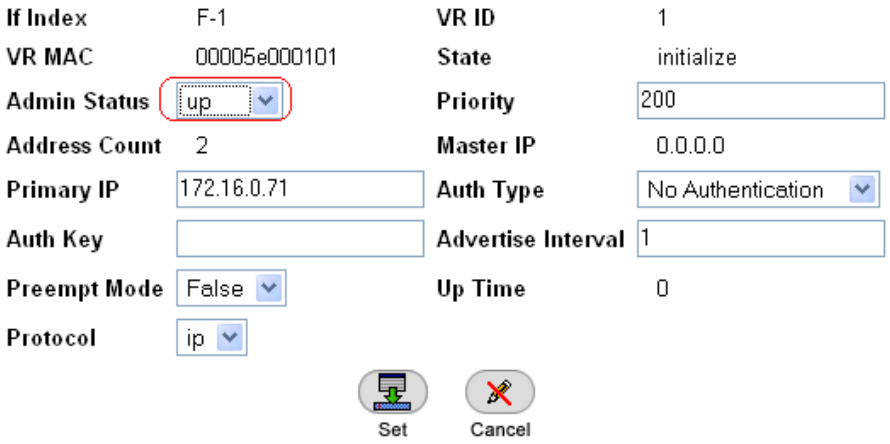
8. Click the **Set** button to save the parameters. You should have two entries in the Associated IP Addresses window as shown here.



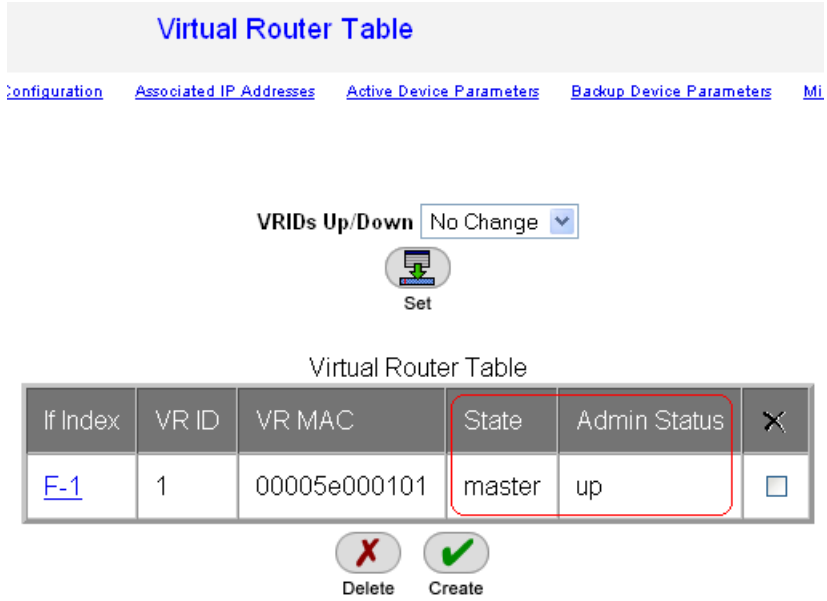
9. Choose **AppDirector** > **Redundancy** > **VRRP** > **Virtual Routers** and click the link to **If IndexF-1**.



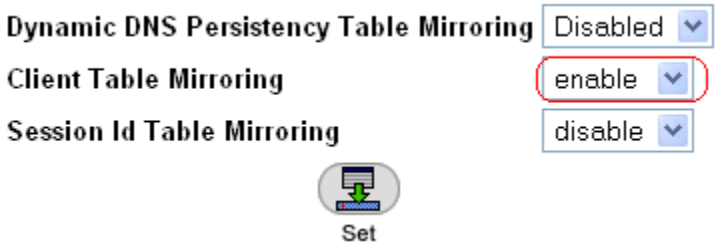
10. Change Admin Status to up, but leave all other settings unchanged as shown here.



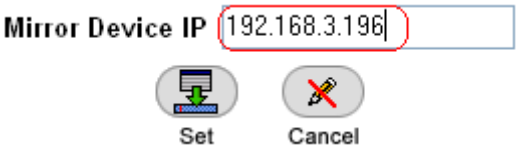
11. Click the **Set** button to save the parameters.
12. On the **Virtual Router Table** page, verify that the **State** setting for this virtual router is **master** as shown here.



13. Choose **AppDirector** > **Redundancy** > **Mirroring** > **Active Device Parameters** and set the **Client Table Mirroring** status to **enable**.



14. Click the **Set** button to save the parameters.
15. Choose **AppDirector** > **Redundancy** > **Mirroring** > **Mirror Device Parameters** and create a new entry.



This sets the backup AppDirector target address used for mirror traffic.

16. Click the **Set** button to save the parameters.

This completes configuration of the primary AppDirector.

Backup AppDirector Configuration

The overall configuration of a backup AppDirector is very similar to that of the primary (active) device.

Initial Backup AppDirector Configuration

1. Using a serial cable and a terminal emulation program, connect to AppDirector.

   The default console port settings are:

   - Bits per Second: 19200
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None

2. Enter the following command to assign management IP address 192.168.3.196 / 24 to interface 17 (dedicated management interface) of AppDirector:

```
net ip-interface create 192.168.3.196 255.255.255.0 17
```

Note: Connectivity can be established to AppDirector at this time if the client resides on the same management subnet.

3. Enter the following command to assign IP address 172.16.0.72 / 23 to interface 1 (production traffic connectivity) of AppDirector:

```
net ip-interface create 172.16.0.72 255.255.254.0 1
```

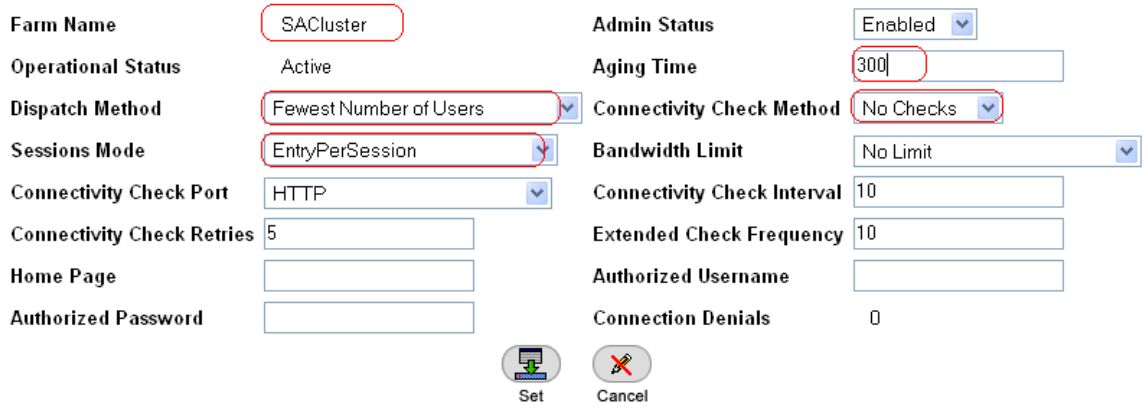
4. Enter the following command to create a default gateway route entry on AppDirector pointing to 172.16.0.1:

```
net route table create 0.0.0.0 0.0.0.0 172.16.0.1 -i 1
```

5. Using a browser, connect to the management IP address of the backup AppDirector (192.168.3.196) via HTTP or HTTPS. The default username and password are **radware** and **radware**.

Farm Configuration

1. Choose AppDirector > Farms > Farm Table and create a new entry as shown here.



Note: The Aging Time value corresponds to Juniper SA Network Connect remote-access client session timers. The AppDirector Aging timer is meant to be just higher than the highest expected expiration interval between ESP and SSL tunnels. By default, the highest expiration value belongs to the SSL tunnels, with an expiration interval of 270 seconds. These values are configurable, so if you changed them, you should also consider the farm Aging Time value.

2. Click the **Set** button to save the parameters.

Layer 4 Policy Configuration

1. Choose **AppDirector** > **Layer 4 Farm Selection** > **Layer 4 Policy Table** and create a new entry as shown here.

Virtual IP	172.16.0.60	**L4 Protocol**	TCP
L4 Port	443	**Source IP From**	0.0.0.0
L4 Policy Name	SAClusterSSLSite1	**Source IP To**	0.0.0.0
Farm Name	SACluster	**L7 Policy Name**	None
Application	HTTPS	**Redundancy Status**	Backup
Backend Encryption Port	0	**Bytes of Request to Read**	3584
POST Classification Input	Header	**HTTP Normalization**	Disabled
L7 Persistent Switching Mode	First	**Policy DefinedBy**	User Defined
Segment Name			

Set Cancel

Note: Redundancy Status for this farm has been set to Backup. This is the SSL tunnel Layer 4 policy.

2. Click the **Set** button to save the parameters.
3. Choose **AppDirector** > **Layer 4 Farm Selection** > **Layer 4 Policy Table** and create a second entry as shown here.

Virtual IP	172.16.0.60	**L4 Protocol**	UDP
L4 Port	4500	**Source IP From**	0.0.0.0
L4 Policy Name	SAClusterESPSite1	**Source IP To**	0.0.0.0
Farm Name	SACluster	**L7 Policy Name**	None
Application	UDP	**Redundancy Status**	Backup
Backend Encryption Port	0	**Bytes of Request to Read**	3584
POST Classification Input	Header	**HTTP Normalization**	Disabled
L7 Persistent Switching Mode	First	**Policy DefinedBy**	User Defined
Segment Name			

Set Cancel

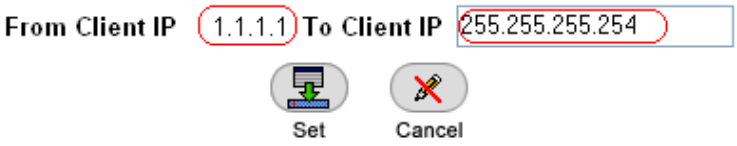
Note: Redundancy Status for this farm has been set to Backup. This is the ESP tunnel Layer 4 policy.

4. Click the **Set** button to save the parameters.

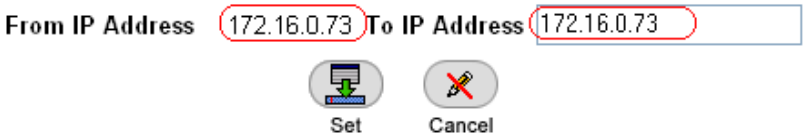
Client Network Address Translation Configuration

1. From the menu, choose **AppDirector** > **NAT** > **Client NAT** to display the Client NAT Global Parameters page.
2. On the **Client NAT Global Parameters** page, change the parameters as shown here.

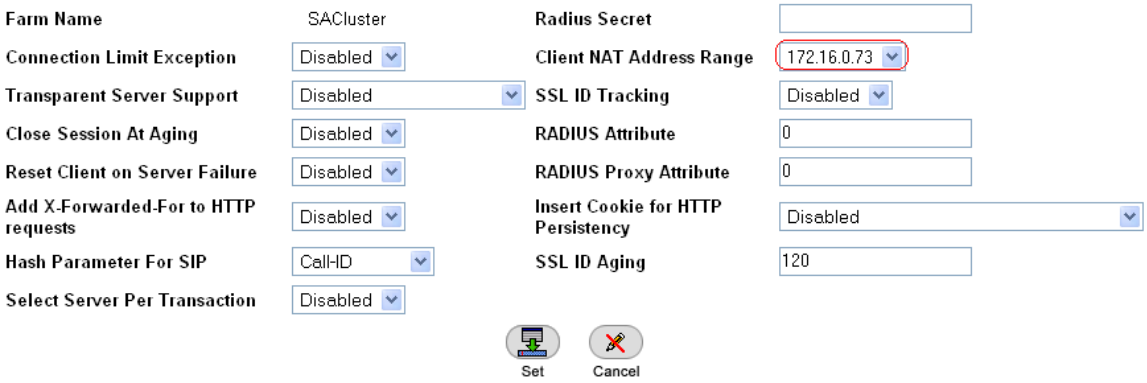
3. Click the **Set** button to save the parameters.
4. Click the **Client NAT Intercept Table hyperlink** at the top of the configuration window.
5. Click the **Create** button.
6. On the **Client NAT Intercept Table Create** page, enter the necessary parameters as shown here.



7. Click the **Set** button to save the parameters.
8. Click the **Client NAT Address Table hyperlink** at the top of the configuration window.
9. Click the **Create** button.
10. On the Client NAT Address Table Create page, enter the necessary parameters as shown here.



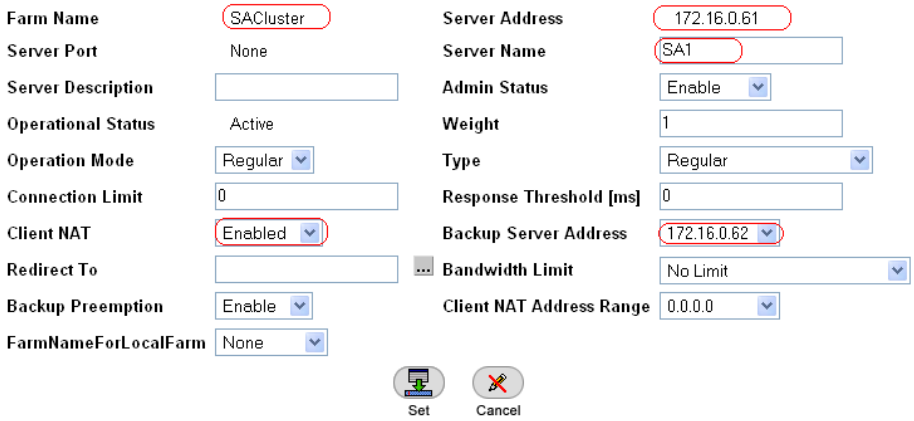
11. Click the Set button to save the parameters.
12. From the menu, select AppDirector > Farms > Farm Table to display the Farm Table page.
13. Click the Extended Farm Parameters hyperlink near the top of the page.
14. On the Extended Farm Parameters page, click the SACluster farm name and enter the necessary parameters as shown here.



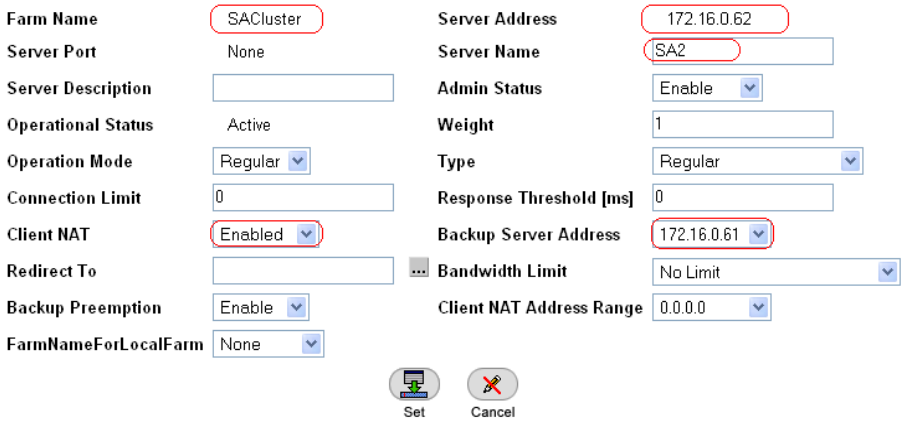
15. Click the **Set** button to save the parameters.

Adding Servers to the Farm

1. From the menu, choose **AppDirector** > **Servers** > **Application Servers** to display the Server Table page.
2. On the **Server Table** page, click the **Create** button.
3. On the **Server Table Create** page, enter the necessary parameters as shown here.



4. Click the **Set** button to save the parameters.
5. Create the second server using the information show here.



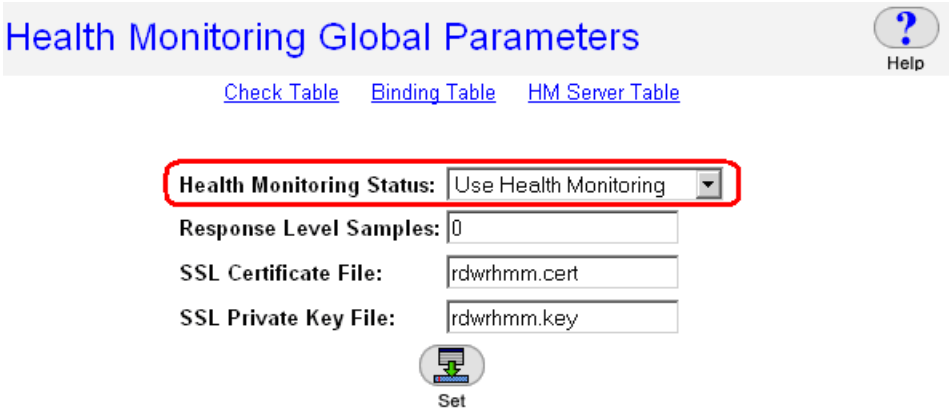
6. Verify that the second server entry was created on the **Server Table** page.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type	Connection Limit	Bandwidth Limit
SACluster	172.16.0.61	None	SA1	Active	Regular	Enable	Regular	0	No Limit
SACluster	172.16.0.62	None	SA2	Active	Regular	Enable	Regular	0	No Limit

Delete Create

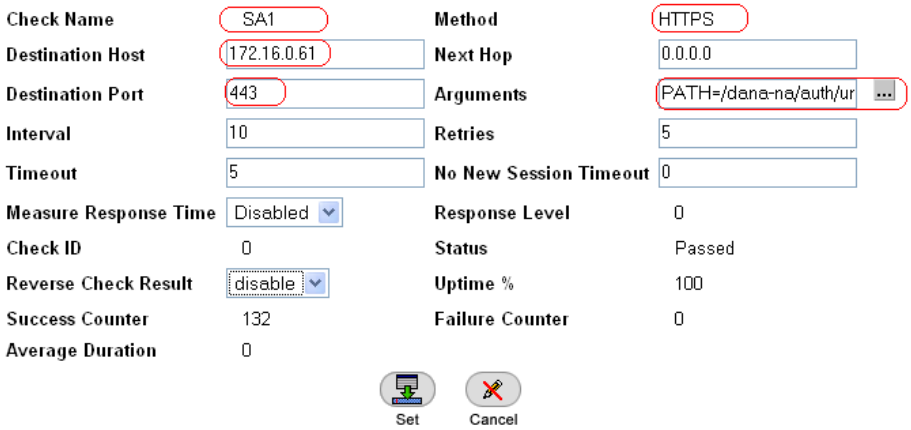
Health Monitoring Configuration

1. From the menu, choose **Health Monitoring > Global Parameters** to display the Health Monitoring Global Parameters page.
2. On the **Health Monitoring Global Parameters** page, change the parameters as shown here.



3. Click the **Set** button to save the parameters.
4. Create the health monitoring check for the first server: From the menu, choose **Health Monitoring > Check Table** to display the Health Monitoring Check Table page.

5. Click the **Create** button.
6. On the **HM Check Table Create** page, enter the necessary parameters as shown here.

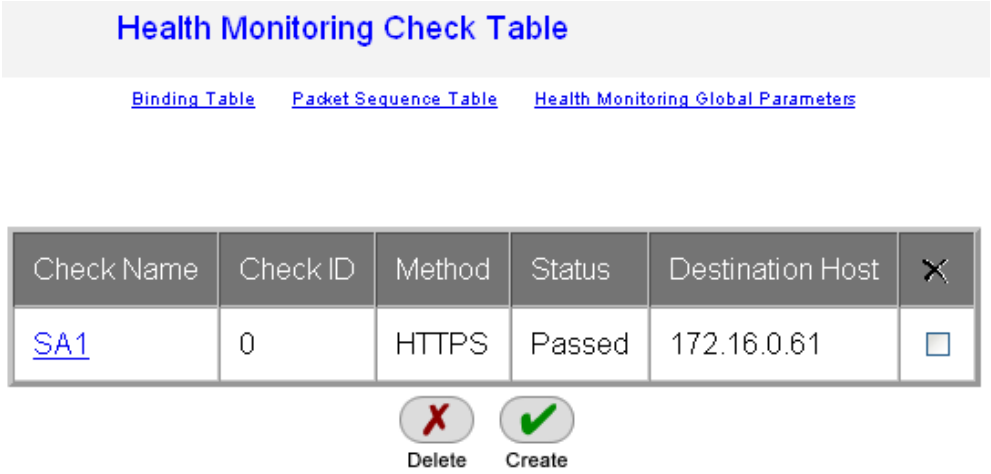


7. Click the button next to **Arguments** ... to populate the specific settings for the rest of this check.
8. Enter the information shown here.

Path = /dana-na/auth/url_default/welcome.cgi

9. Click the **Set** button for the method arguments and then click the **Set** button in the **HM Check Table Create** window.

   The Health Monitoring Check Table should have a single entry as shown here.



   The status of this check may be displayed as Unknown until the server replies successfully to the AppDirector check.

10. Create the health monitoring check for the second server: If the **Health Monitoring Check Table** page is not already displayed from the previous step, choose **Health Monitoring > Check Table** from the menu.
11. Click the **Create** button.
12. On the **HM Check Table Create** page, enter the necessary parameters as shown here.

Check Name	SA2	**Method**	HTTPS
Destination Host	172.16.0.62	**Next Hop**	0.0.0.0
Destination Port	443	**Arguments**	PATH=/dana-na/auth/ur ...
Interval	10	**Retries**	5
Timeout	5	**No New Session Timeout**	0
Measure Response Time	Disabled	**Response Level**	0
Check ID	1	**Status**	Passed
Reverse Check Result	disable	**Uptime %**	100
Success Counter	159	**Failure Counter**	0
Average Duration	0		

Set Cancel

13. Click the button next to **Arguments** ... to configure the specific arguments as shown here.

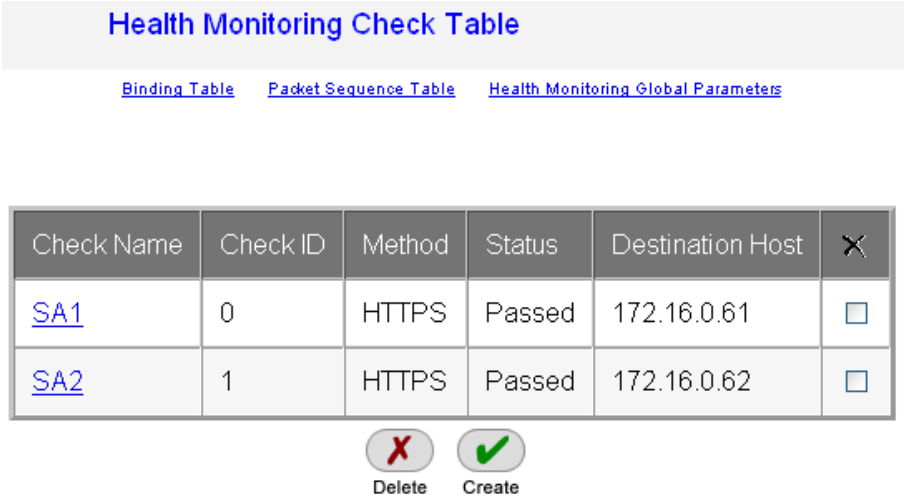
Arguments for HTTPS Method

Path:	/dana-na/auth/url_defau
Hostname:	
HTTPS Method:	GET
Username:	
Password:	
Match search string:	
Match mode:	
HTTPS return code:	200
HTTPS return code:	
HTTPS return code:	
HTTPS return code:	

Set Cancel

Path = /dana-na/auth/url_default/welcome.cgi

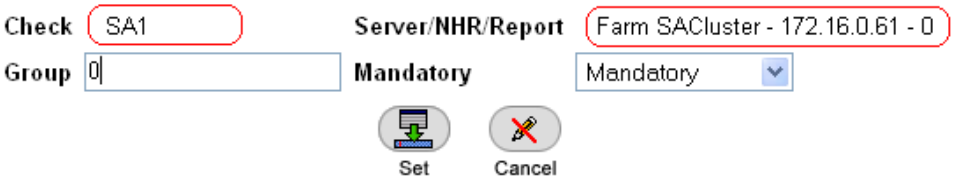
14. Click the **Set** button to save the method argument parameters.
15. Verify that the **Arguments** text box has been populated.
16. Click the **Set** button to save the health check.
17. Verify that the new entry was created on the **Health Monitoring Check Table** page as shown here.



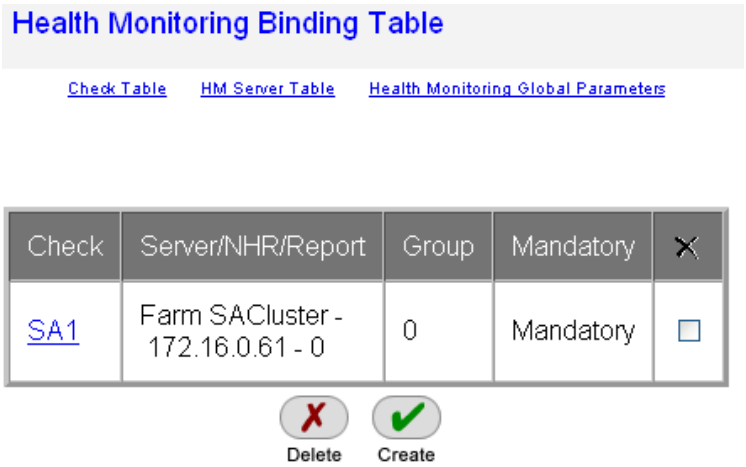
Binding Health Checks to Servers

1. Create the health monitoring binding for the first server: From the menu, choose **Health Monitoring** > **Binding Table** to display the Health Monitoring Binding Table page.

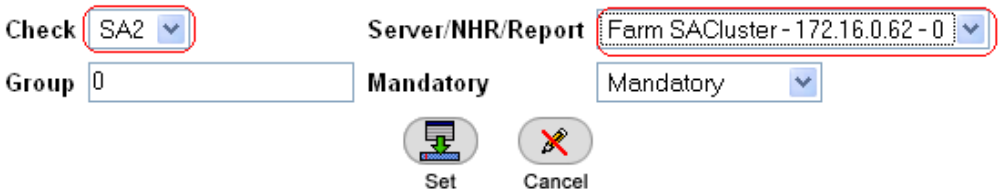
2. Click the **Create** button.
3. On the **HM Binding Table Create** page, enter the necessary parameters as shown here.



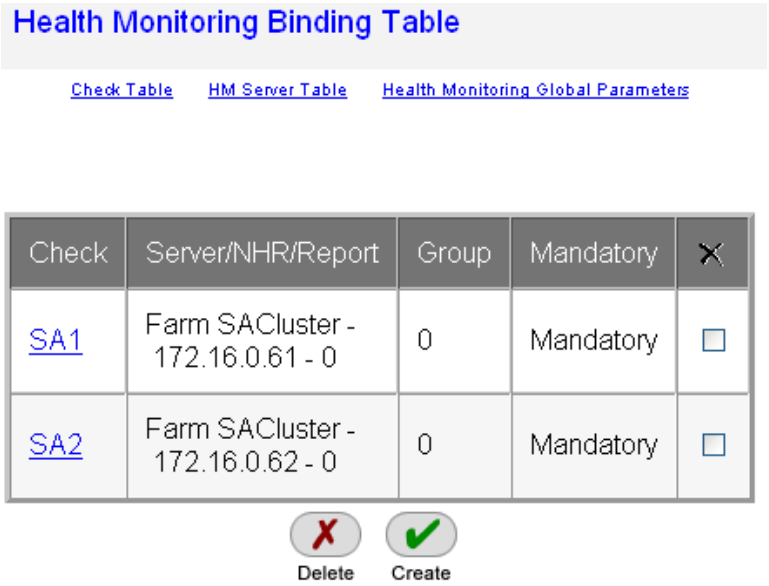
4. Click the **Set** button to save the parameters.
5. Verify that the new entry was created on the **Health Monitoring Table** page.



6. Create the health monitoring binding for the second server: If the **Health Monitoring Binding Table** page is not already displayed from the previous step, choose **Health Monitoring > Binding Table** from the menu.
7. Click the **Create** button.
8. On the **HM Binding Table Create** page, enter the necessary parameters as shown here.

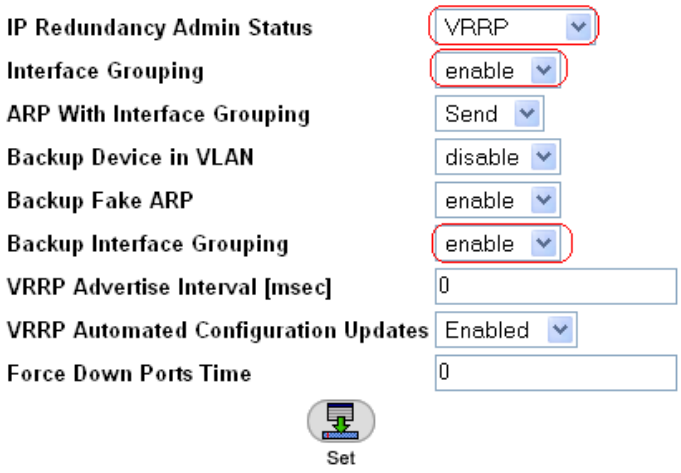


9. Click the **Set** button to save the parameters.
10. Verify that the new entry was created on the **Health Monitoring Binding Table** page.

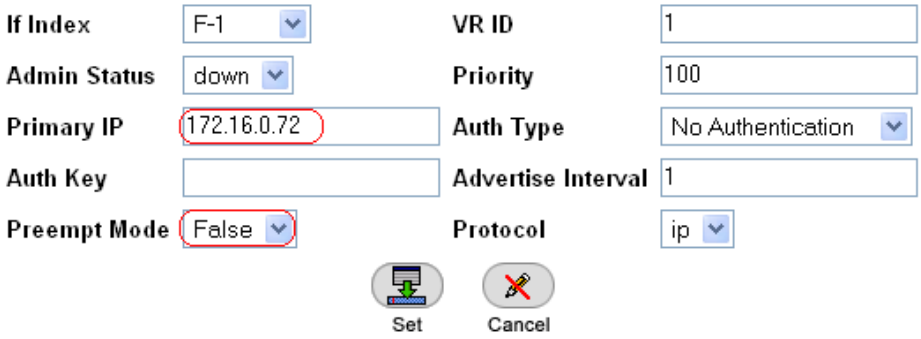


Backup AppDirector VRRP Configuration

1. On the backup **AppDirector, choose AppDirector** > **Redundancy** > **Global Configuration** and change the settings as shown here.

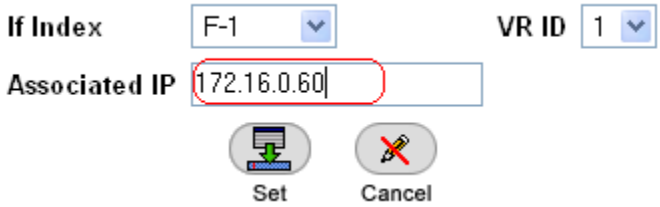


2. Click the **Set** button to save the parameters.
3. Choose **AppDirector** > **Redundancy** > **VRRP** > **Virtual Routers** and create a new entry as shown here.



Note: The Priority value on the backup AppDirector is set to 100, while on the primary device, this value was set to 200. The device with the higher priority value will be the master of this virtual router.

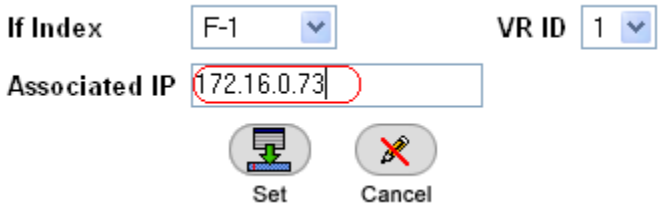
4. Click the **Set** button to save the parameters.
5. Choose **AppDirector** > **Redundancy** > **VRRP** > **Associated IP Addresses** and create a new entry as shown here.



This is the virtual IP address.

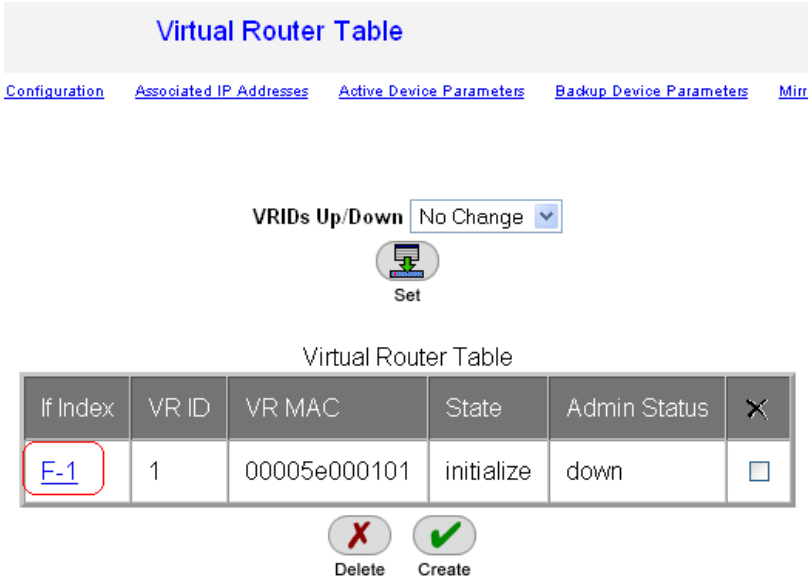
6. Click the **Set** button to save the parameters.

7. Create a second entry in the **Associated IP Addresses** table as shown here.

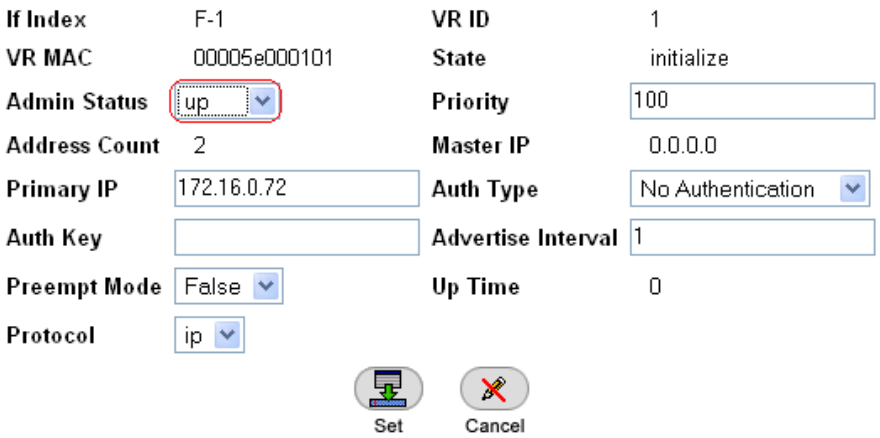


This is the client NAT IP address.

8. Click the **Set** button to save the parameters.
9. Choose **AppDirector** > **Redundancy** > **VRRP** > **Virtual Routers** and edit the existing entry by clicking the link.

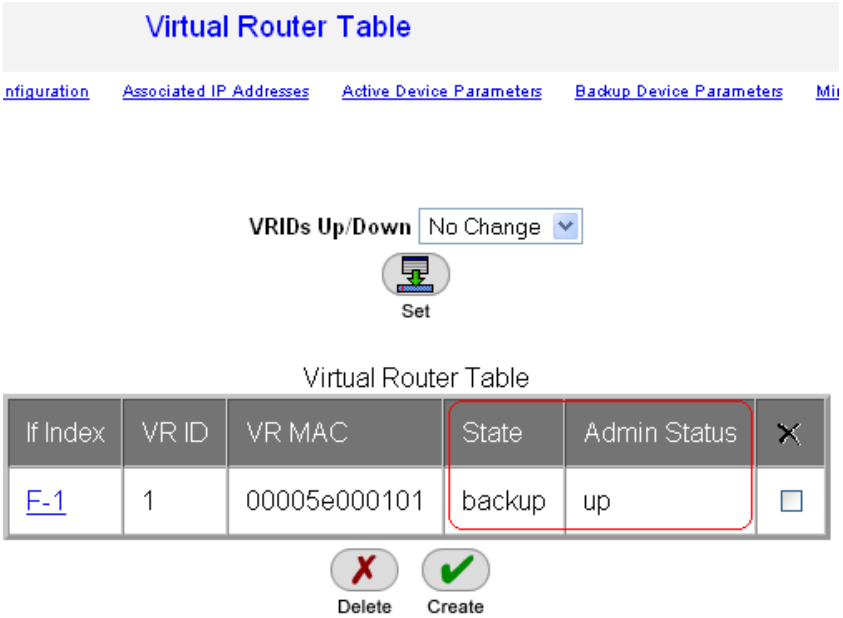


10. Change **Admin Status** to **up**:



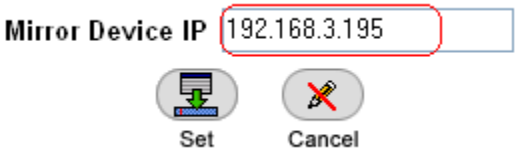
11. Click the **Set** button to save the parameters.

12. Verify that the state of the backup device for this virtual router is **backup**.



13. Choose **AppDirector** > **Redundancy** > **Mirroring** > **Backup Device Parameters** and set the mirroring status to **enable**.

14. Click the **Set** button to save the parameters.
15. Choose **AppDirector** > **Redundancy** > **Mirroring** > **Mirror Device Parameters** and create a new entry as shown here.



This sets the master AppDirector target address used for mirror traffic.

16. Click the **Set** button to save the parameters.

This concludes the configuration of the backup AppDirector and the local HA solution. See Appendix A for actual configurations.

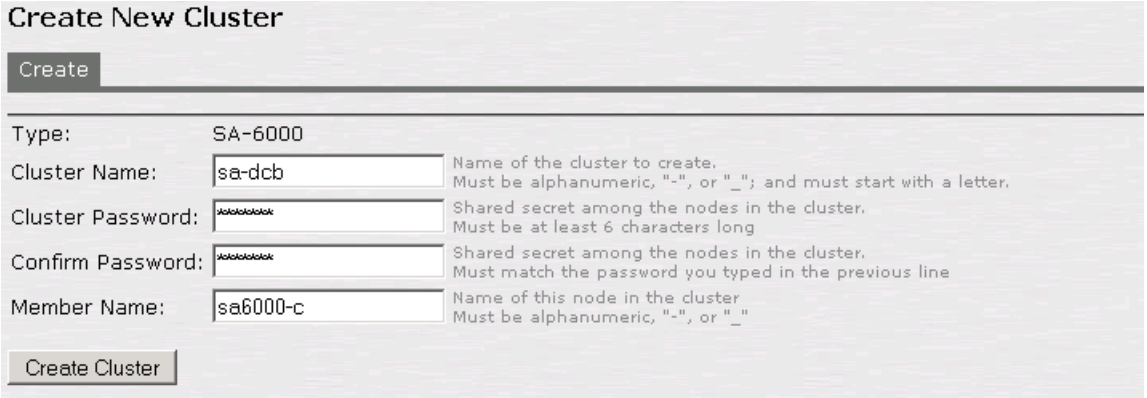
Secure Access 6000 SSL VPN Active-Active Configuration

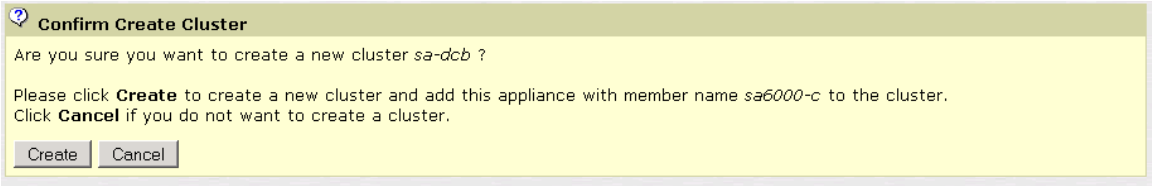
License

Node	License	Comment
sa6000-c	• Enables 5000 simultaneous users of SA 6000 • Enables Juniper Networks Secure Application Manager and Network Connect for SA 6000	• License for total concurrent users • License to use Network Connect
sa600-d	• Enables clustering: Allows 5000 additional users to be shared from another SA 6000	• Clustering license for second node

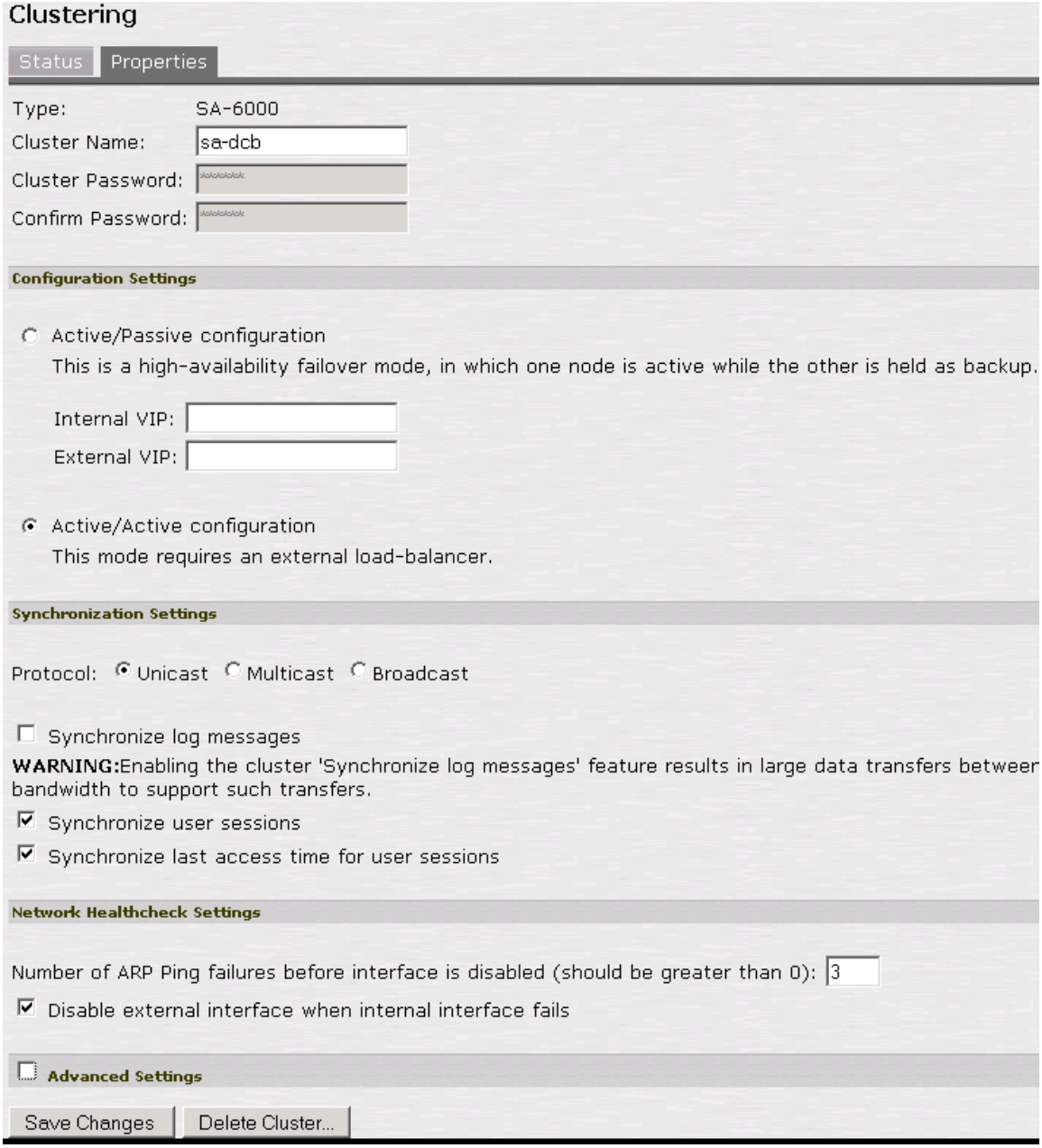
Creating a Cluster in sa6000-c

1. To create a new cluster, choose…





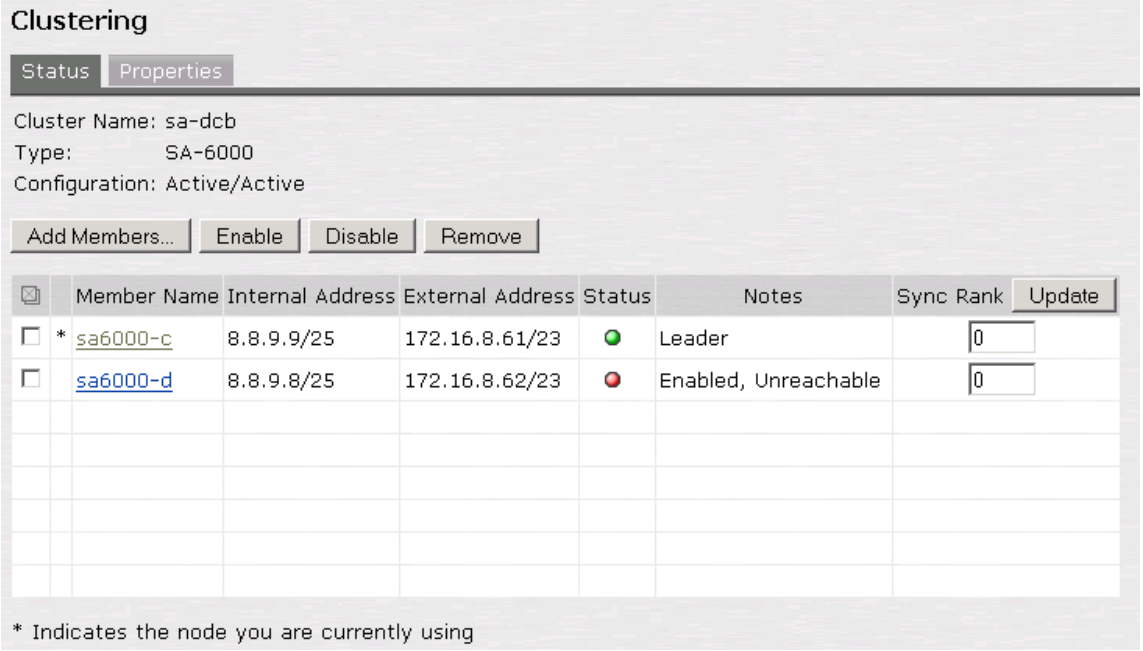
2. By default, a cluster is created in the active-active configuration. To modify the settings, choose **Clustering > Properties**. Then make your changes: for instance, you can select **disable external interface when internal interface fails** as shown here.



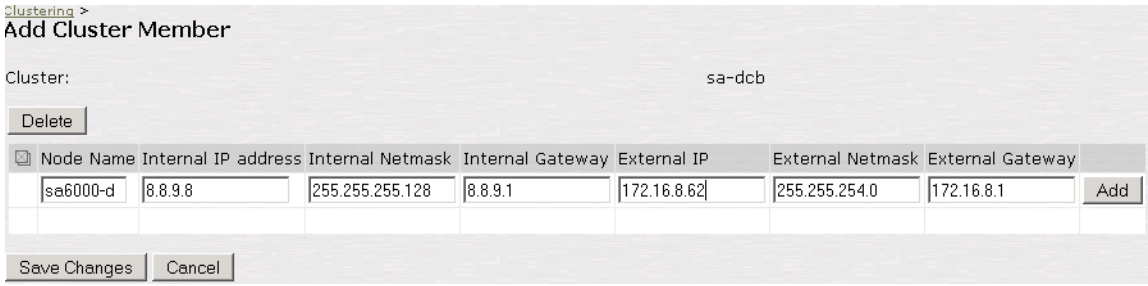
3. When you are finished making changes, click the **Save Changes** button.

Adding a Cluster Member in sa6000-c

4. Before a cluster member can join a cluster, you need to define it. Choose **Clustering > Status**. Two cluster members, sa6000-c and sa6000-d, are defined in the following screenshot.



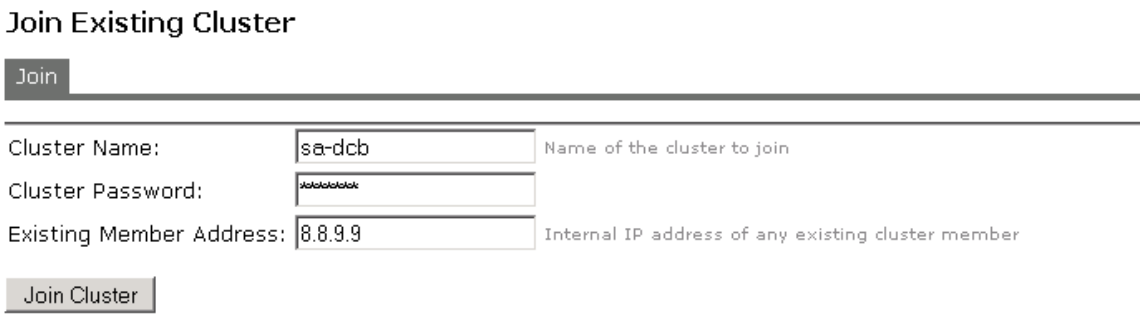
5. To add a member to the cluster, on the **Status** tab select the cluster.
6. Click the **Add Members** button. The following screenshot shows how to add sa6000-d as a cluster member.

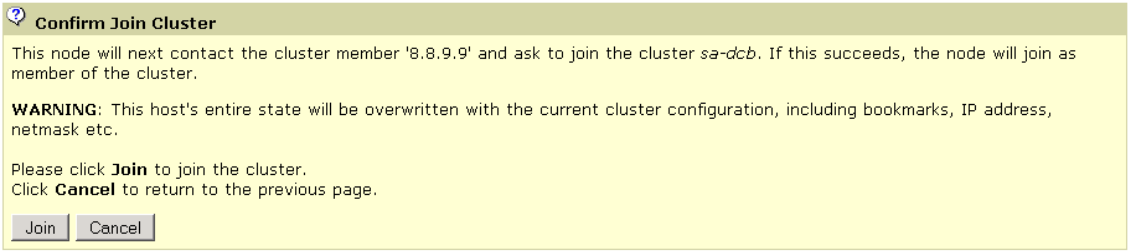


7. Click the **Add** button to add the cluster member.

Joining a Cluster in sa6000-d

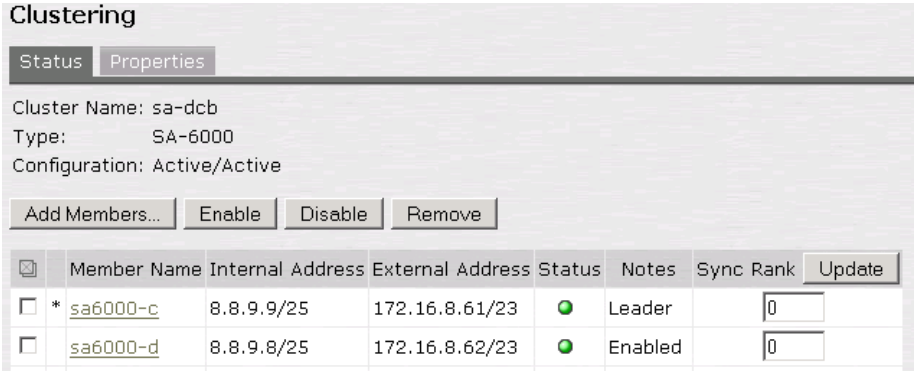
1. After cluster information has been defined for sa6000-c, it is time for sa6000-d to join the cluster. Log in sa6000-d admin URL and choose **Cluster > Join**. Enter the cluster name, cluster password, and existing member address (for example, the internal address of sa6000-c).



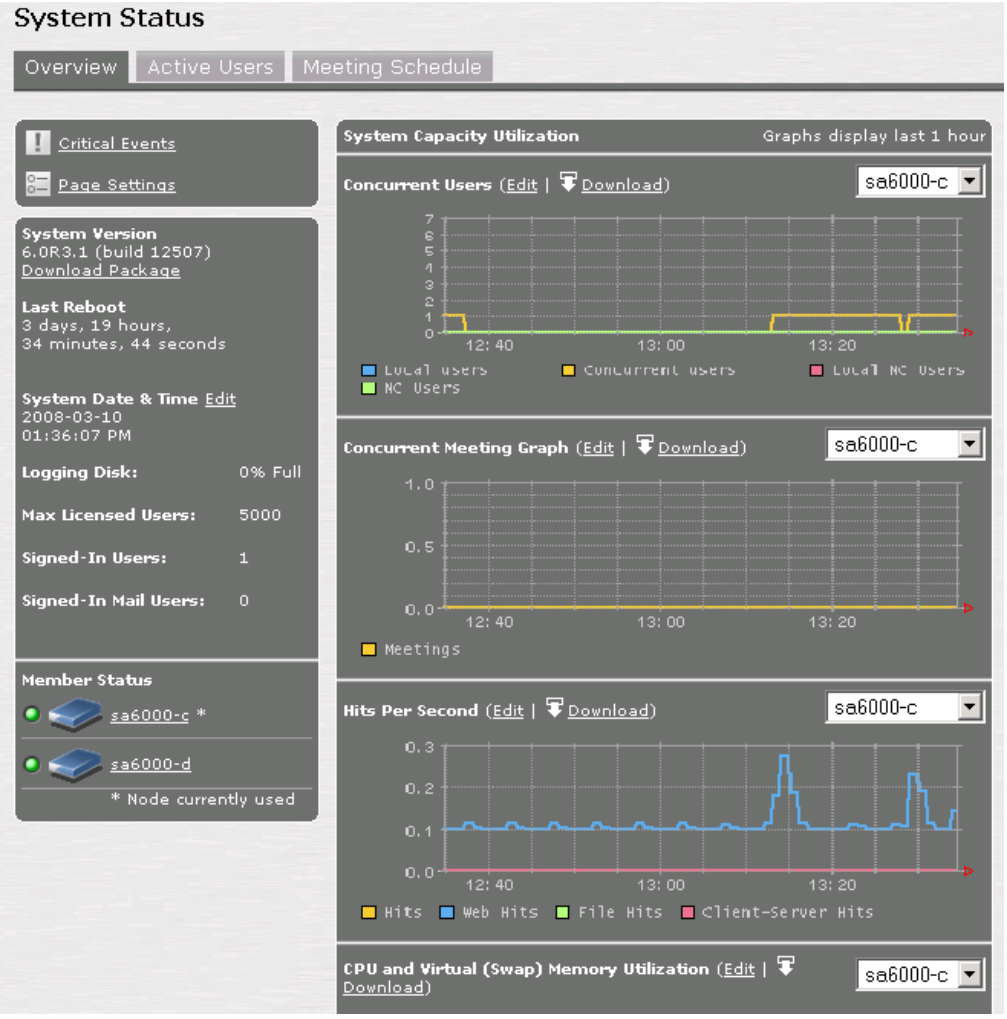


Monitoring a Cluster

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



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



Secure Access Configuration References

- Secure Access system software downloads: http://www.juniper.net/techpubs/software/ive/
- Juniper Networks knowledgebase: http://kb.juniper.net/
- SSL VPN (IVE) Version 6.0 technical document: http://www.juniper.net/techpubs/software/ive/6.x/6.0/

AppDirector and Secure Access Global Architecture

Figure 2 shows a common two Datacenter deployment model. Clients are represented in three geographic locations to demonstrate mobile and regional clients. AppDirectors share Availability, Load and Proximity information to ensure the best resource allocation decision per client to ensure the best user experience possible.

DNS Redirection

DNS sends requests to the AppDirector IP interface address or DNS virtual IP interface address to resolve a host name to an IP address. AppDirector responds with the IP address of the most available farm or of a standalone server that is part of this policy. AppDirector can also respond with the virtual IP address of the closest available AppDirector to the asking DNS machine. All the network proximity calculations and measurements are made between the address from which the DNS request is sent and the AppDirector IP interface address to which the request is destined.

The DNS redirection process follows these steps:

1. The DNS request to resolve a host name to an IP address reaches the AppDirector physical IP interface or DNS virtual IP Interface from a DNS server. See Appendix B for the DNS server changes required for authoritative role exchange with AppDirector.

2. The client table is not searched. AppDirector searches the static proximity table for a range that fits the asking DNS server. If a match is made, the top-priority server from the active servers that is not overloaded is selected. AppDirector resolves the name to the IP address of the chosen server, which can be a local Layer 4 virtual IP or a virtual IP configured on a remote AppDirector.

   Note: DNS queries must be sent to a device physical IP interface address or the virtual IP interface address, and not to the address of the virtual IP defined for production traffic. Traffic to the virtual IP defined for production traffic is load balanced by AppDirector.

3. If there is no match in the static proximity table, the dynamic proximity table is searched. If there is a match, AppDirector resolves the request to the Layer 4 virtual IP address of the highest-priority site (that is active and not overloaded), taking into account the hops weight, latency weight, and load weight variables.
4. If there is no match in the dynamic proximity table, AppDirector resolves the request to the IP address of the least-loaded site, while calculating proximity information for the querying DNS server (if proximity is enabled). Then AppDirector sends proximity reporting protocol requests to other AppDirector devices to do the same.
5. AppDirector resolves the query to the IP address of the least-loaded site.

   Note: DNS answers are made with a DNS time to live (TTL) of 0 (default) to reduce Internet caching and to keep the system dynamic. You can set DNS TTL to a higher value, and you can set different DNS TTL values for different farms.

Using AppDirector, DNS redirection works best if DNS servers from all over the Internet make queries to AppDirector. If the DNS servers local to AppDirector are responsible for the super-domain and make queries to AppDirector, their proximity calculations result in inaccurate data. AppDirector allows you to configure up to two DNS servers with requests that are resolved to the least-loaded site; no proximity calculations are made if a request comes from either of these two DNS servers. See the discussions of proximity configuration later in this guide for specific configuration details.

Radware AppDirector and Juniper Networks Secure Access SSL VPN Global Topology Interoperability Tests and AppDirector Configuration

Tests Conducted for Global Solution Validation

The following tests were conducted to ensure that the most appropriate global solution was defined and validated. All tests were successfully completed using the AppDirector configurations following Table 2.

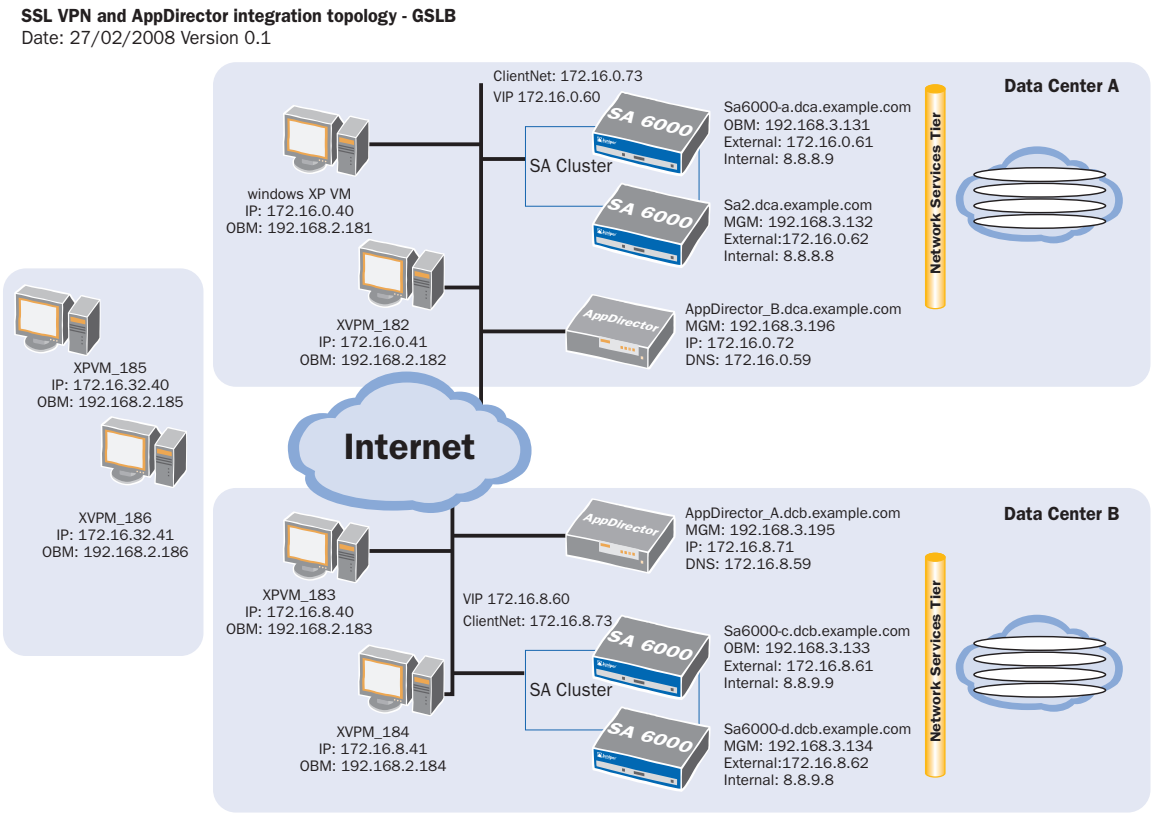
Table 2. Tests Conducted for Global Solution Validation

Test Case	Description
AppDirector: Virtual IP and service farm	Verify that the virtual IP address and service farm defined in the load balancer work as expected.
AppDirector: Dispatch algorithm	Verify that a new request follows the least connection policy (configured dispatch method).
AppDirector: Persistency or session affinity	Verify that SSL VPN establishes HTTPS and ESP connection with the same server and maintains the selected site and server throughout the life of a session.
AppDirector site recovery: Site 1 failover	Verify that the load balancer Site 1 setting prevents an SPOF and that Site 1 fails over properly to Site 2.
AppDirector site recovery: Site 2 failover	Verify that the load balancer Site 2 setting prevents an SPOF and that Site 2 fails over properly to Site 1.
SA cluster: Failover	Verify that AppDirector detects SA failure and dynamically manages new requests and reconnections to the available site and SA appliances.

Site 1: AppDirector Global Configuration

This section details the step-by-step AppDirector configuration process, using the Web-based management GUI, for creating the Juniper Networks SA SSL VPN and Radware AppDirector global solution. The configuration steps presented here are an extension of the local HA subsystem configuration and build on the steps presented in the previous part of this document. The global configuration focuses on the primary AppDirector in each of two locations. The same configuration process should be repeated on the backup AppDirector. Please refer to Figure 2 for topology and addressing information.

Figure 2. Secure Access SSL VPN and AppDirector Global Integration Topology



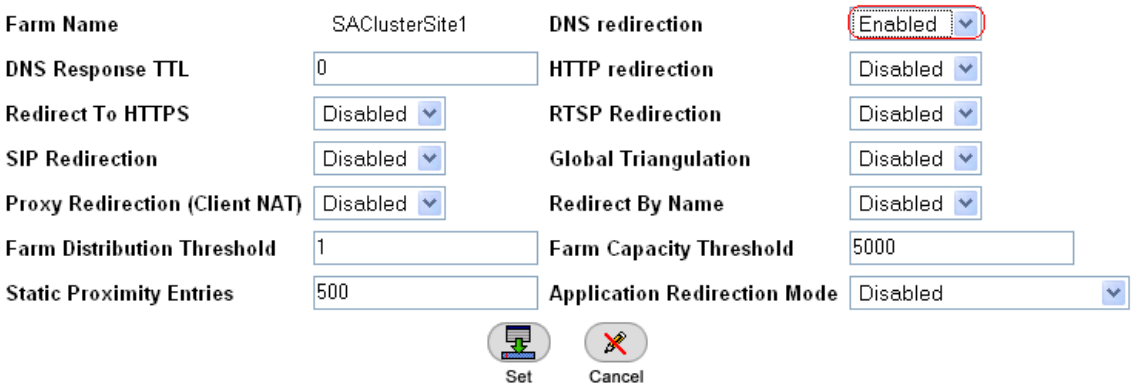
DNS Server Configuration

1. From the menu, choose **AppDirector > DNS > Server** to display the DNS Server Parameters page.
2. On the **DNS Server Parameters** page, change the parameters as shown here.

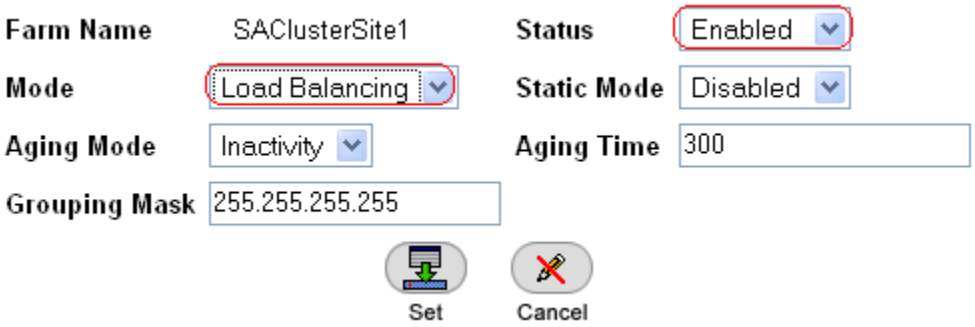
3. Click the **Set** button to save the parameters.

Farm Redirection Configuration

1. From the menu, choose **AppDirector > Farms > Redirection** to display the Redirection Table page.
2. Click the name of the existing farm in the **Farm Name** entry.
3. On the **Redirection Table Update** page, enter the necessary parameters as shown here.



4. Click the **Set** button to save the parameters.
5. From the menu, choose **AppDirector** > **Farms** > **DNS Persistency Parameters** to display the DNS Persistency Parameters Table page.
6. Click the name of the existing farm in the **Farm Name** entry.
7. On the **DNS Persistency Parameters Update** page, enter the necessary parameters as shown here.



8. Click the **Set** button to save the parameters.

Adding Distributed AppDirector to the Farm

1. From the menu, choose **AppDirector** > **Servers** > **Application Servers** to display the Server Table page as shown here.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type
SAClusterSite1	172.16.0.61	None	SAClusterServer1	Active	Regular	Enable	Regular
SAClusterSite1	172.16.0.62	None	SAClusterServer2	Active	Regular	Enable	Regular

Delete Create

2. Click the **Create** button to display the Server Table Create page.
3. On the **Server Table Create** page, enter the necessary parameters as shown here.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type
SAClusterSite1	172.16.0.61	None	SAClusterServer1	Active	Regular	Enable	Regular
SAClusterSite1	172.16.0.62	None	SAClusterServer2	Active	Regular	Enable	Regular

Delete Create

4. Click the Set button to save the parameters.
5. Verify that the new entry was created on the Server Table page.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type
SAClusterSite1	172.16.0.61	None	SAClusterServer1	Active	Regular	Enable	Regular
SAClusterSite1	172.16.0.62	None	SAClusterServer2	Active	Regular	Enable	Regular
SAClusterSite1	172.16.8.60	None	RemoteAD	Active	Regular	Enable	Distributed AppDirector

Delete Create

Layer 4 Policy Configuration

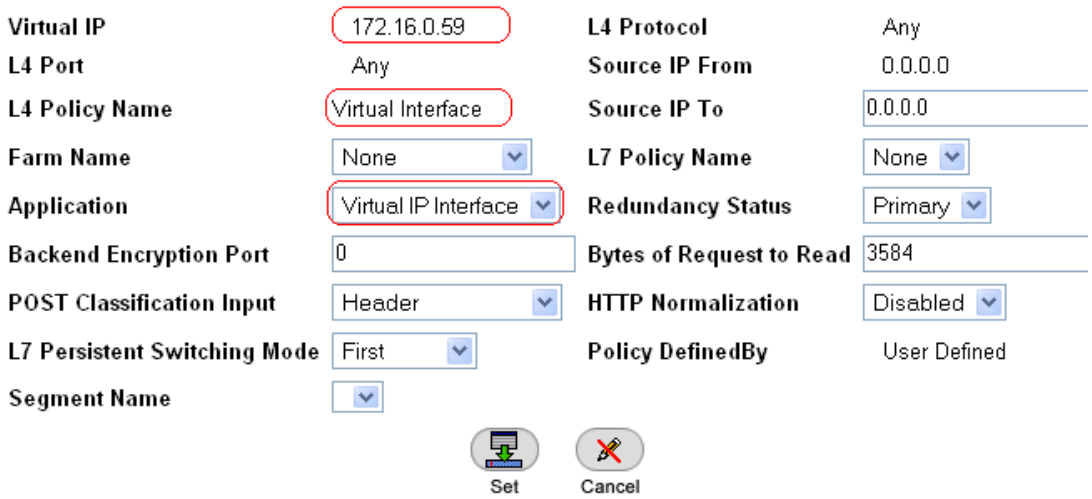
1. From the menu, choose **AppDirector > Layer 4 Farm Selection > Layer 4 Policy Table** to display the Layer 4 Policy Table page as shown here.

Virtual IP	L4 Protocol	L4 Port	Source IP From	L4 Policy Name	L7 Policy Name	Farm Name	✕
172.16.0.60	TCP	443	0.0.0.0	SASite1Policy	None	SAClusterSite1	☐
172.16.0.60	UDP	4500	0.0.0.0	SAESPSite1Policy	None	SAClusterSite1	☐

Delete Create

2. Click the **Create** button.
3. On the **Layer 4 Policy Table Create** page, enter the necessary parameters as shown here.

Note: This virtual IP is the destination address for DNS queries. The address is shared as a highly available address to receive DNS authoritative requests for the local HA subsystem (primary and backup AppDirector devices).



4. Click the **Set** button to save the parameters.
5. Verify that the new entry was created on the **Layer 4 Policy Table** page.

Virtual IP	L4 Protocol	L4 Port	Source IP From	L4 Policy Name	L7 Policy Name	Farm Name	✕
172.16.0.59	Any	Any	0.0.0.0	Virtual Interface	None	None	☐
172.16.0.60	TCP	443	0.0.0.0	SASite1Policy	None	SAClusterSite1	☐
172.16.0.60	UDP	4500	0.0.0.0	SAESPSite1Policy	None	SAClusterSite1	☐

Delete Create

DNS Hostname Configuration

1. From the menu, choose **AppDirector** > **DNS** > **Hostnames** to display the Hostname page.
2. On the **DNS Hostname** page, select the **Host Name** entry and click the **Create** button and then change the parameters as shown here.

Note: Several options are available for Preferred Resolve IP:

- 0.0.0.0 (default): The host name is resolved to the best available IP (either a local virtual IP or a virtual IP of a distributed site that is part of the local farm). This mode ignores the servers' operation mode in the Layer 4 policy farm.
- Layer 4 policy virtual IP defined for this host name: In this case, if a local server is available, the device responds with the Layer 4 policy virtual IP; otherwise, it selects the IP of one of the remote and distributed server's IPs according to availability, load, and proximity. This is the selection shown in the example here.
- IP of a distributed AppDirector server or a remote server in the farm: If the specified farm server is unavailable, the local Layer 4 policy virtual IP or the distributed or remote server's IP in the farm is selected according to availability, load, and proximity.

3. Click the **Set** button to save the parameters.

Global Load Report Configuration

1. From the menu, choose **AppDirector** > **Distributed System** > **Report Configuration** to display the Load Report page.
2. On the **Load Report** page, click the **Create** button and change the parameters as shown here.

Distributed Farm Name	SAClusterSite2	**Distributed Server**	172.16.0.60
Farm Name	SAClusterSite1	**L4 Policy Name**	SASite1Policy
Triangulation VIP	0.0.0.0	**Triangulation VIP NAT**	0.0.0.0
Original VIP	0.0.0.0	**Health Monitoring ID**	
Destination Address	172.16.8.59	**Redundant Destination Address**	0.0.0.0

Set Cancel

3. Click the **Set** button to save the parameters.

Proximity Configuration

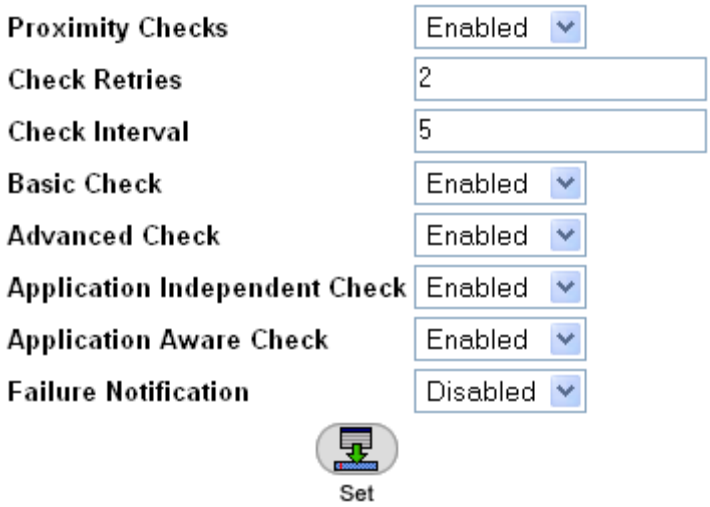
1. From the menu, choose **AppDirector** > **Proximity** > **Parameters** > **General** to display the Proximity Parameters page.
2. On the **Proximity Parameters** page, change the parameters as shown here.

Proximity Mode	Full Proximity
Main DNS Address	0.0.0.0
Backup DNS Address	0.0.0.0
Proximity Aging Period [min]	2880
Hops Weight	1
Latency Weight	1
Load Weight	1
Proximity Table Cleanup [min]	0

If local DNS servers exist which proximity calculations should not be made, please enter them here.
Hops, Latency and Load can be defined to have different influences on the outcome. Those weights would also be defined here.

Set

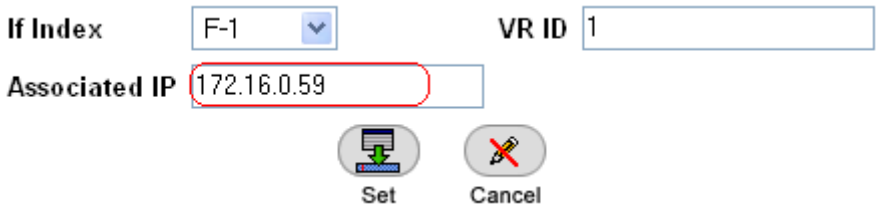
3. Click the **Set** button to save the parameters.
4. From the menu, choose **AppDirector** > **Proximity** > **Parameters** > **Proximity Checks** to display the Proximity Checks page.
5. On the **Proximity Checks** page, verify that the parameters are set as shown here.



6. Click the **Set** button to save the parameters.

Adding the DNS Virtual IP to the Existing VRRP Configuration

1. From the menu, choose **AppDirector** > **Redundancy** > **VRRP** > **Associated IP Addresses** to display the Associated IP Addresses page. Click **Create** and add the entry shown here.



Note: This is the DNS virtual IP address.

2. Click the **Set** button to save the parameters.

Configuring the Backup AppDirector

Repeat the preceding configuration steps on the backup AppDirector.

Site 2: AppDirector Global Configuration

DNS Server Configuration

1. From the menu, choose **AppDirector** > **DNS** > **Server** to display the DNS Server Parameter page.
2. On the **DNS Server Parameters** page, change the parameters as shown here.

3. Click the **Set** button to save the parameters.

Farm Redirection Configuration

1. From the menu, choose **AppDirector** > **Farms** > **Redirection** to display the Redirection Table.
2. Click the name of the existing farm in the **Farm Name** entry.

3. On the **Redirection Table Update** page, enter the necessary parameters as shown here.

Farm Name	SAClusterSite2	**DNS redirection**	Enabled
DNS Response TTL	0	**HTTP redirection**	Disabled
Redirect To HTTPS	Disabled	**RTSP Redirection**	Disabled
SIP Redirection	Disabled	**Global Triangulation**	Disabled
Proxy Redirection (Client NAT)	Disabled	**Redirect By Name**	Disabled
Farm Distribution Threshold	1	**Farm Capacity Threshold**	5000
Static Proximity Entries	500	**Application Redirection Mode**	Disabled

Set Cancel

4. Click the **Set** button to save the parameters.
5. From the menu, choose **AppDirector** > **Farms** > **DNS Persistency Parameters** to display the DNS Persistency Parameters Table page.
6. Click the name of the existing farm in the **Farm Name** entry.
7. On the **DNS Persistency Parameters Update** page, enter the necessary parameters as shown here.

Farm Name	SAClusterSite2	**Status**	Enabled
Mode	Load Balancing	**Static Mode**	Disabled
Aging Mode	Inactivity	**Aging Time**	300
Grouping Mask	255.255.255.255		

Set Cancel

8. Click the **Set** button to save the parameters.

Adding Distributed AppDirector to the Farm

1. From the menu, choose **AppDirector** > **Servers** > **Application Servers** to display the Server Table as shown here.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type
SAClusterSite2	172.16.8.61	None	SAClusterServer1	Not In Service	Regular	Enable	Regular
SAClusterSite2	172.16.8.62	None	SAClusterServer2	Not In Service	Regular	Enable	Regular

Delete Create

2. Click the **Create** button to display the Server Table Create page.
3. On the **Server Table Create** page, enter the necessary parameters as shown here.

Farm Name	SAClusterSite2	**Server Address**	172.16.0.60
Server Port	None	**Server Name**	RemoteAD
Server Description		**Admin Status**	Enable
Operational Status	Active	**Weight**	2
Operation Mode	Regular	**Type**	Distributed AppDirector
Connection Limit	0	**Response Threshold [ms]**	0
Client NAT	Disabled	**Backup Server Address**	0.0.0.0
Redirect To		**Bandwidth Limit**	No Limit
Backup Preemption	Enable	**Client NAT Address Range**	0.0.0.0
FarmNameForLocalFarm	None		

Set Cancel

4. Click the **Set** button to save the parameters.
5. Verify that the new entry was created on the **Server Table** page.

Farm Name	Server Address	Server Port	Server Name	Operational Status	Operation Mode	Admin Status	Type
SAClusterSite2	172.16.0.60	None	RemoteAD	Not In Service	Regular	Enable	Distributed AppDirector
SAClusterSite2	172.16.8.61	None	SAClusterServer1	Not In Service	Regular	Enable	Regular
SAClusterSite2	172.16.8.62	None	SAClusterServer2	Not In Service	Regular	Enable	Regular

Delete Create

Layer 4 Policy Configuration

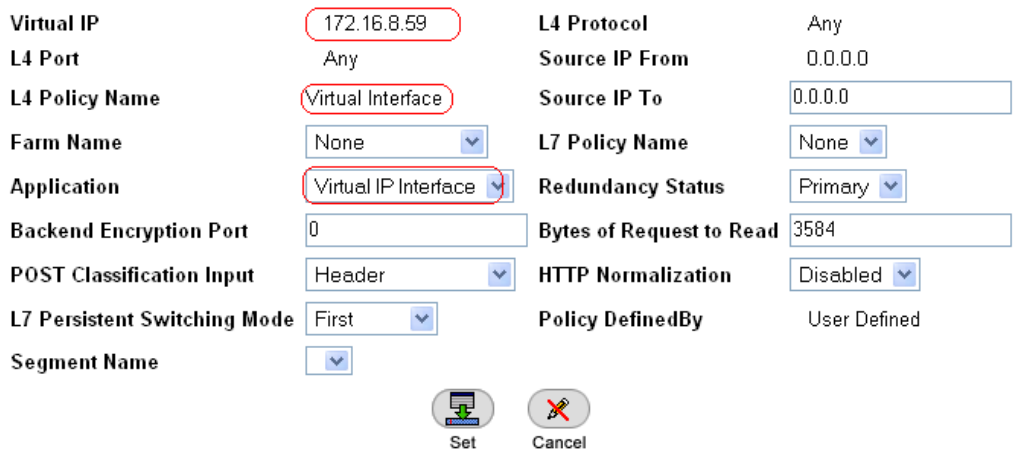
1. From the menu, choose AppDirector > Layer 4 Farm Selection > Layer 4 Policy Table to display the Layer 4 Policy Table page as shown here.

Virtual IP	L4 Protocol	L4 Port	Source IP From	L4 Policy Name	L7 Policy Name	Farm Name	✕
172.16.8.60	TCP	443	0.0.0.0	SASite2Policy	None	SAClusterSite2	☐
172.16.8.60	UDP	4500	0.0.0.0	SAESPSite2Policy	None	SAClusterSite2	☐

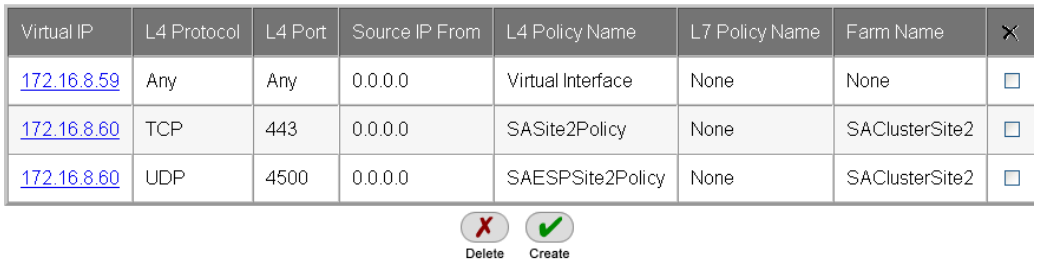
Delete Create

2. Click the **Create** button.
3. On the **Layer 4 Policy Table Create** page, enter the necessary parameters as shown here.

Note: This virtual IP is the destination address for DNS queries. The address is shared as a highly available address to receive DNS authoritative requests for the local HA subsystem (primary and backup AppDirector devices).



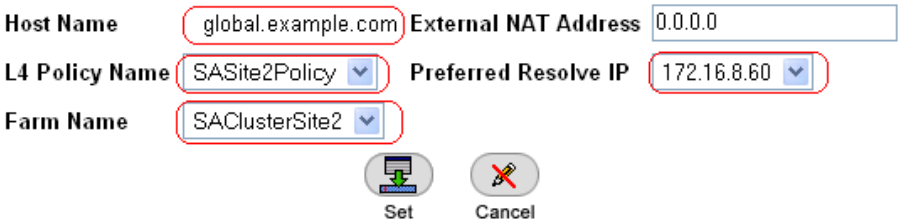
4. Click the **Set** button to save the parameters.
5. Verify that the new entry was created on the **Layer 4 Policy Table** page.



Virtual IP	L4 Protocol	L4 Port	Source IP From	L4 Policy Name	L7 Policy Name	Farm Name	✕
172.16.8.59	Any	Any	0.0.0.0	Virtual Interface	None	None	☐
172.16.8.60	TCP	443	0.0.0.0	SASite2Policy	None	SAClusterSite2	☐
172.16.8.60	UDP	4500	0.0.0.0	SAESPSite2Policy	None	SAClusterSite2	☐

DNS Hostname Configuration

1. From the menu, choose **AppDirector** > **DNS** > **Hostnames** to display the Hostname page.
2. On the **DNS Hostname** page, select the **Host Name** entry and click the **Create** button and change the parameters as shown here.



3. Click the **Set** button to save the parameters.

Global Load Report Configuration

1. From the menu, choose **AppDirector** > **Distributed System** > **Report Configuration** to display the Load Report page.
2. On the **Load Report** page, click the **Create** button and change the parameters as shown here.

Distributed Farm Name	SAClusterSite1	**Distributed Server**	172.16.8.60
Farm Name	SAClusterSite2	**L4 Policy Name**	SASite2Policy
Triangulation VIP	0.0.0.0	**Triangulation VIP NAT**	0.0.0.0
Original VIP	0.0.0.0	**Health Monitoring ID**	
Destination Address	172.16.0.59	**Redundant Destination Address**	0.0.0.0

Set Cancel

3. Click the **Set** button to save the parameters.

Proximity Configuration

1. From the menu, choose **AppDirector** > **Proximity** > **Parameters** > **General** to display the Proximity Parameters page.
2. On the **Proximity Parameters** page, change the parameters as shown here.

Proximity Mode	Full Proximity
Main DNS Address	0.0.0.0
Backup DNS Address	0.0.0.0
Proximity Aging Period [min]	2880
Hops Weight	1
Latency Weight	1
Load Weight	1
Proximity Table Cleanup [min]	0

Set

3. Click the **Set** button to save the parameters.
4. From the menu, choose **AppDirector** > **Proximity** > **Parameters** > **Proximity Checks** to display the Proximity Checks page.
5. On the **Proximity Checks** page, verify that the parameters are set as shown here.

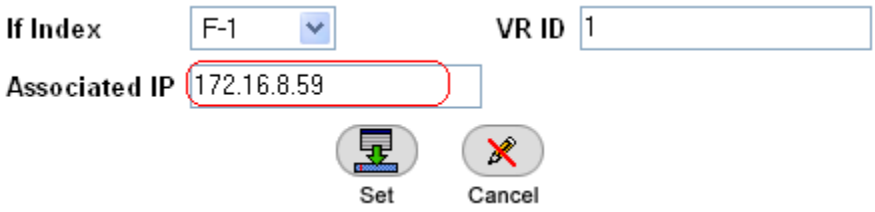
Proximity Checks	Enabled
Check Retries	2
Check Interval	5
Basic Check	Enabled
Advanced Check	Enabled
Application Independent Check	Enabled
Application Aware Check	Enabled
Failure Notification	Disabled

Set

6. Click the **Set** button to save the parameters.

Adding the DNS Virtual IP to the existing VRRP Configuration

1. From the menu, choose AppDirector > Redundancy > VRRP > Associated IP Addresses to display the Associated IP Addresses page. Click Create and add the entry shown here.



Note: This is the DNS virtual IP address.

2. Click the **Set** button to save the parameters.

Configuring the Backup AppDirector

Repeat the preceding configuration steps on the backup AppDirector.

Summary

The Juniper Networks Secure Access SSL VPN solution, in combination with Radware's Application Delivery platform, provides a superior Secure Access (SA) infrastructure for supporting remote application access with a highly available, scalable and secure networking environment. Juniper Networks Secure Access (SA) leads the SSL VPN market with a complete range of remote-access appliances and security products that have a variety of form factors and features that can be combined to meet the needs of companies of all sizes. Radware AppDirector is an intelligent application delivery controller that provides scalability and application-level security for service infrastructure optimization, fault tolerance and redundancy. Together, the two components help ensure zero loss connectivity, offering a best-in-class solution.

Appendix A

Local High Availability Design Configurations

Master Configuration from OnDemand Switch 2 Platform

```
!Device Configuration
!Date: 14-02-2008 20:36:36
!DeviceDescription: AppDirector
!Base MAC Address: 00:03:b2:3d:38:c0
!Software Version: 1.06.07 (Build date Feb 13 2008, 23:50:02,Build#50)
!APSolute OS Version: 10.31-01.01(26):2.06.06

net ip-interface create 192.168.3.195 255.255.255.0 17
net ip-interface create 172.16.0.71 255.255.254.0 1 -f disable
net route table create 0.0.0.0 0.0.0.0 172.16.0.1 -i 1
redundancy mode set VRRP
appdirector farm table setCreate SACluster -as Enabled -at 300 -dm \
“Fewest Number of Users” -cm “No Checks”
appdirector farm server table create SACluster 172.16.0.61 None -sn SA1 \
-id 1 -cn Enabled -ba 172.16.0.62
appdirector farm server table create SACluster 172.16.0.62 None -sn SA2 \
-id 2 -cn Enabled -ba 172.16.0.61
redundancy interface-group set enable
redundancy mirror backup status set disable
redundancy mirror main client-status set enable
redundancy mirror address setCreate 192.168.3.196
appdirector farm connectivity-check httpcode setCreate SACluster \ “200 - OK”
net next-hop-router setCreate 172.16.0.1 -fl 0
appdirector farm nhr setCreate 0.0.0.0 -ip 172.16.0.1 -fl 0
appdirector farm extended-params set SACluster -nr 172.16.0.73
appdirector nat client address-range setCreate 172.16.0.73 -t \ 172.16.0.73
appdirector nat client range-to-nat setCreate 1.1.1.1 -t 255.255.255.254
redundancy backup-interface-group set enable
appdirector segmentation nhr-table setCreate DefaultNHR -ip 172.16.0.1 \ -fl 0
appdirector l4-policy table create 172.16.0.60 TCP 443 0.0.0.0 \
SAClusterSSLSite1 -fn SACluster -ta HTTPS
appdirector l4-policy table create 172.16.0.60 UDP 4500 0.0.0.0 \
SAClusterESPSite1 -fn SAClusterSite1 -ta UDP
health-monitoring check create SA1 -id 0 -m HTTPS -p 443 -a \
PATH=/dana-na/auth/url_default/welcome.cgi|MTD=G|C1=200| -d 172.16.0.61
health-monitoring check create SA2 -id 1 -m HTTPS -p 443 -a \
```

```
PATH=/dana-na/auth/url_default/welcome.cgi|MTD=G|C1=200| -d 172.16.0.62
health-monitoring binding create 0 1
health-monitoring binding create 1 2
health-monitoring status set enable
health-monitoring response-level-samples set 0
redundancy vrrp virtual-routers create 1 1 -as up -p 200 -pip \
172.16.0.71 -pm False
redundancy vrrp associated-ip create 1 1 172.16.0.60
redundancy vrrp associated-ip create 1 1 172.16.0.73
manage user table create radware -pw GndridF04zNWSGOrZjKFV78REiEra/Qm
manage telnet status set enable
manage telnet server-port set 23
manage web status set enable
manage ssh status set enable
manage secure-web status set enable
redundancy arp-interface-group set Send
net l2-interface set 100001 -ad up
manage terminal prompt set AppDirector_A
manage snmp groups create SNMPv1 public -gn initial
manage snmp groups create SNMPv1 ReadOnlySecurity -gn InitialReadOnly
manage snmp groups create SNMPv2c public -gn initial
manage snmp groups create SNMPv2c ReadOnlySecurity -gn InitialReadOnly
manage snmp groups create UserBased radware -gn initial
manage snmp groups create UserBased ReadOnlySecurity -gn InitialReadOnly
manage snmp access create initial SNMPv1 noAuthNoPriv -rvn iso -wvn iso \
-nvn iso
manage snmp access create InitialReadOnly SNMPv1 noAuthNoPriv -rvn \
ReadOnlyView
manage snmp access create initial SNMPv2c noAuthNoPriv -rvn iso -wvn iso \
-nvn iso
manage snmp access create InitialReadOnly SNMPv2c noAuthNoPriv -rvn \
ReadOnlyView
manage snmp access create initial UserBased authPriv -rvn iso -wvn iso \
-nvn iso
manage snmp access create InitialReadOnly UserBased authPriv -rvn \ ReadOnlyView
manage snmp views create iso 1
manage snmp views create ReadOnlyView 1
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.2.7.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.18.1.1 -cm excluded
```

```
manage snmp views create ReadOnlyView 1.3.6.1.6.3.15.1.2.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.35.1.61 -cm \ excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.4 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.5 -cm excluded
manage snmp notify create allTraps -ta v3Traps
manage snmp users create radware -cf 0.0 -ap MD5 -akc \
aa4f37f460702d1faee44b7bc81408c7 -pp DES -pkc \ aa4f37f460702d1faee44b7bc81408c7
manage snmp target-address create v3MngStations -tl v3Traps -p \
radware-authPriv
manage snmp target-parameters create public-v1 -d SNMPv1 -sm SNMPv1 -sn \
public -sl noAuthNoPriv
manage snmp target-parameters create public-v2 -d SNMPv2c -sm SNMPv2c \
-sn public -sl noAuthNoPriv
manage snmp target-parameters create radware-authPriv -d SNMPv3 -sm \
UserBased -sn radware -sl authPriv
manage snmp community create public -n public -sn public
manage telnet session-timeout set 5
manage telnet auth-timeout set 30
appdirector global connectivity-check tcp-timeout set 3
```

Backup Configuration from OnDemand Switch 2 Platform

```
!Device Configuration
!Date: 14-02-2008 20:39:08
!DeviceDescription: AppDirector
!Base MAC Address: 00:03:b2:3d:41:c0
!Software Version: 1.06.07 (Build date Feb 13 2008, 23:50:02,Build#50)
!APSolute OS Version: 10.31-01.01(26):2.06.06
!

net ip-interface create 192.168.3.196 255.255.255.0 17
net ip-interface create 172.16.0.72 255.255.254.0 1 -f disable
net route table create 0.0.0.0 0.0.0.0 172.16.0.1 -i 1
redundancy mode set VRRP
appdirector farm table setCreate SACluster -as Enabled -at 300 -dm \
“Fewest Number of Users” -cm “No Checks”
appdirector farm server table create SACluster 172.16.0.61 None -sn SA1 \ -id 1 -cn Enabled -ba 172.16.0.62
appdirector farm server table create SACluster 172.16.0.62 None -sn SA2 \ -id 2 -cn Enabled -ba 172.16.0.61
```

```
redundancy interface-group set enable
redundancy mirror backup status set enable
redundancy mirror address setCreate 192.168.3.195
appdirector farm connectivity-check httpcode setCreate SACluster \ “200 - OK”
net next-hop-router setCreate 172.16.0.1 -fl 0
appdirector farm nhr setCreate 0.0.0.0 -ip 172.16.0.1 -fl 0
appdirector farm extended-params set SACluster -nr 172.16.0.73
appdirector nat client address-range setCreate 172.16.0.73 -t \ 172.16.0.73
appdirector nat client range-to-nat setCreate 1.1.1.1 -t 255.255.255.254
redundancy backup-interface-group set enable
appdirector segmentation nhr-table setCreate DefaultNHR -ip 172.16.0.1 \ -fl 0
appdirector l4-policy table create 172.16.0.60 TCP 443 0.0.0.0 \
SAClusterSSLSite1 -fn SACluster -ta HTTPS -rs Backup
appdirector l4-policy table create 172.16.0.60 UDP 4500 0.0.0.0 \
SAClusterESPSite1 -fn SAClusterSite1 -ta UDP -rs Backup
health-monitoring check create SA1 -id 0 -m HTTPS -p 443 -a \
PATH = /dana-na/auth/url_default/welcome.cgi|MTD = G|C1 = 200| -d 172.16.0.61
health-monitoring check create SA2 -id 1 -m HTTPS -p 443 -a \
PATH = /dana-na/auth/url_default/welcome.cgi|MTD = G|C1 = 200| -d 172.16.0.62
health-monitoring binding create 0 1
health-monitoring binding create 1 2
health-monitoring status set enable
health-monitoring response-level-samples set 0
redundancy vrrp virtual-routers create 1 1 -as up -pip 172.16.0.72 -pm \ False
redundancy vrrp associated-ip create 1 1 172.16.0.60
redundancy vrrp associated-ip create 1 1 172.16.0.73
manage user table create radware -pw GndridF04zNWSGOrZjKFV78REiEra/Qm
manage telnet status set enable
manage telnet server-port set 23
manage web status set enable
manage ssh status set enable
manage secure-web status set enable
redundancy arp-interface-group set Send
net l2-interface set 100001 -ad up
manage terminal prompt set AppDirector_B
manage snmp groups create SNMPv1 public -gn initial
manage snmp groups create SNMPv1 ReadOnlySecurity -gn InitialReadOnly
```

```
manage snmp groups create SNMPv2c public -gn initial
manage snmp groups create SNMPv2c ReadOnlySecurity -gn InitialReadOnly
manage snmp groups create UserBased radware -gn initial
manage snmp groups create UserBased ReadOnlySecurity -gn InitialReadOnly
manage snmp access create initial SNMPv1 noAuthNoPriv -rvn iso -wvn iso \ -nvn iso
manage snmp access create InitialReadOnly SNMPv1 noAuthNoPriv -rvn \ ReadOnlyView
manage snmp access create initial SNMPv2c noAuthNoPriv -rvn iso -wvn iso \ -nvn iso
manage snmp access create InitialReadOnly SNMPv2c noAuthNoPriv -rvn \ ReadOnlyView
manage snmp access create initial UserBased authPriv -rvn iso -wvn iso \ -nvn iso
manage snmp access create InitialReadOnly UserBased authPriv -rvn \ ReadOnlyView
manage snmp views create iso 1
manage snmp views create ReadOnlyView 1
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.2.7.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.18.1.1 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.15.1.2.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.35.1.61 -cm \ excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.4 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.5 -cm excluded
manage snmp notify create allTraps -ta v3Traps
manage snmp users create radware -cf 0.0 -ap MD5 -akc \
aa4f37f460702d1faee44b7bc81408c7 -pp DES -pkc \
aa4f37f460702d1faee44b7bc81408c7
manage snmp target-address create v3MngStations -tl v3Traps -p \ radware-authPriv
manage snmp target-parameters create public-v1 -d SNMPv1 -sm SNMPv1 -sn \ public -sl noAuthNoPriv
manage snmp target-parameters create public-v2 -d SNMPv2c -sm SNMPv2c \ -sn public -sl noAuthNoPriv
manage snmp target-parameters create radware-authPriv -d SNMPv3 -sm \ UserBased -sn radware -sl authPriv
manage snmp community create public -n public -sn public
manage telnet session-timeout set 5
manage telnet auth-timeout set 30
appdirector global connectivity-check tcp-timeout set 3
```

Appendix B

DNS Server Configurations

Zone Definition

```
zone "example.com" IN {
        type forward;
        forwarders {172.16.0.59; 172.16.8.59;};
};
zone "global.example.com" {
type master;
file "/etc/bind/zones/global.example.com";
};
```

Zone Definition for Reverse DNS

```
zone "0.16.172.in-addr.arpa" {
type master;
file "/etc/bind/zones/db.0.16.172";
};
zone "8.16.172.in-addr.arpa" {
type master;
file "/etc/bind/zones/db.8.16.172";
};
```

Sample DNS Lookup

```
root@dns1:/etc/bind/zones# nslookup global.example.com
Server:         172.16.8.15
Address:        172.16.8.15#53

Non-authoritative answer:
Name:   global.example.com
Address: 172.16.0.60
```

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
Fax: 35.31.8903.601

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