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

Table of Contents

| Introduction |
|---|
| Scope |
| Design Considerations |
| Radware AppDirector Products |
| Juniper Networks Infranet Controller (IC) Products |
| Solution Overview |
| Juniper Networks Secure Access Secure Sockets Layer VPN Overview |
| Radware AppDirector Overview |
| Radware AppDirector and Juniper Networks Secure Access SSL VPN Architecture |
| Radware Benefits for Juniper Networks Secure Access SSL VPN Solutions |
| Radware AppDirector and Juniper Networks Secure Access SSL VPN Local High Availability Interoper- |
| ability Tests and Configurations |
| Tests Conducted for Local Solution Validation |
| Primary AppDirector Configuration |
| Initial Primary AppDirector Configuration |
| Farm Configuration |
| Layer 4 Policy Configuration |
| Adding Servers to the Farm |
| Health Monitoring Configuration |
| Binding Health Checks to Servers 16 |
| Primary AppDirector VRRP Configuration 18 |
| Backup AppDirector Configuration |
| Initial Backup AppDirector Configuration |
| Farm Configuration |
| Layer 4 Policy Configuration |
| Client Network Address Translation Configuration |
| Adding Servers to the Farm |
| Health Monitoring Configuration |
| Binding Health Checks to Servers 29 |
| Backup AppDirector VRRP Configuration |
| Secure Access 6000 SSL VPN Active-Active Configuration |
| License |
| Creating a Cluster in sa6000-c |
| Adding a Cluster Member in sa6000-c |
| Joining a Cluster in sa6000-d |
| Monitoring a Cluster |
| Secure Access Configuration References |
| AppDirector and Secure Access Global Architecture |
| DNS Redirection |

| Radware AppDirector and Juniper Networks Secure Access SSL VPN Global Topology Interopera | bility |
|---|--------|
| Tests and AppDirector Configuration | 40 |
| Tests Conducted for Global Solution Validation | 40 |
| Site 1: AppDirector Global Configuration | 40 |
| DNS Server Configuration | 41 |
| Farm Redirection Configuration | 41 |
| Adding Distributed AppDirector to the Farm | 42 |
| Layer 4 Policy Configuration | 43 |
| DNS Hostname Configuration | 44 |
| Global Load Report Configuration | 45 |
| Proximity Configuration | 45 |
| Adding the DNS Virtual IP to the Existing VRRP Configuration | 46 |
| Configuring the Backup AppDirector | 46 |
| Site 2: AppDirector Global Configuration | 46 |
| DNS Server Configuration | 46 |
| Farm Redirection Configuration | 46 |
| Adding Distributed AppDirector to the Farm | 47 |
| Layer 4 Policy Configuration | 48 |
| DNS Hostname Configuration | 49 |
| Global Load Report Configuration | 49 |
| Proximity Configuration | 50 |
| Adding the DNS Virtual IP to the existing VRRP Configuration | 51 |
| Configuring the Backup AppDirector | 51 |
| Summary | 51 |
| Appendix A | 52 |
| Local High Availability Design Configurations | 52 |
| Master Configuration from OnDemand Switch 2 Platform | 52 |
| Backup Configuration from OnDemand Switch 2 Platform | 54 |
| Appendix B | 57 |
| DNS Server Configurations | 57 |
| Zone Definition | 57 |
| Zone Definition for Reverse DNS | 57 |
| Sample DNS Lookup | 57 |
| About Juniper Networks | 58 |

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-inclass 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 applicationlevel 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 servicespecific 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.

| 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. |

 Table 1.
 Tests Conducted for Solution Validation

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.

| Farm Table | | | | | | ? Help | |
|--------------|-----------------|----------------------|-------------------------|---|----------------------|-----------------------|---|
| | 1 | Extended Farm Parame | ters Laver 4 Policy Tat | ole <u>Server Table</u> <u>DNS Persiste</u> | ncy Parameters Table | | |
| Farm Name | Admin Status | Aging Time [sec] | Dispatch Method | Connectivity Check Method | Sessions Mode | Operational Status | × |
| | | | Delet | e Create | | | |

2. Click the Create button.

3. On the Farm Table Create page, enter the necessary parameters as shown here.²

| Farm Name | SACluster | | Admin Status | Enabled 💌 | |
|----------------------------|------------------------|----------|-----------------------------|-------------|---|
| Operational Status | Active | | Aging Time | 300 |] |
| Dispatch Method | Fewest Number of Users | ; | Connectivity Check Method | No Checks 🕑 | |
| Sessions Mode | EntryPerSession | • | Bandwidth Limit | No Limit | * |
| Connectivity Check Port | HTTP | * | Connectivity Check Interval | 10 |] |
| Connectivity Check Retries | 5 | | Extended Check Frequency | 10 |] |
| Home Page | | | Authorized Username | | |
| Authorized Password | | | Connection Denials | 0 | |
| | | • | × | | |
| | | Set | Cancel | | |

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:

¹To enable Web-based management from the console command-line interface, enter **manage web status set enable**. ²Throughout 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.

| Farm Table | | | | | | Help | |
|--------------------|-------------------|---------------|----------------------------|------------------------------|--------------------------|-----------------------|------------------|
| Extended Farm Para | imeters Laver 4 I | Policy Table | Server Table DNS Persisten | ov Parameters Table Redi | rection Table Windows NT | Parameters Private P. | <u>arameters</u> |
| | | | | | | | |
| Farm Name | Admin Status | Aging Time | Dispatch Method | Connectivity Check Method | Sessions Mode | Operational Status | × |
| SACluster | Enabled | 60 | Fewest Number of Users | No Checks | EntryPerSession | Active | |
| | | | | | | | |

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.

| | Layer 4 F | Policy T | able | | ? Help |
|------------|-------------------|---------------------|------------------------------|-----------------|-----------|
| | <u>Farm Table</u> | <u>Layer 7 Poli</u> | <u>cy Table – Layer 4 Pc</u> | licy Statistics | |
| Virtual IP | L4 Protocol | L4 Port | Source IP From | L4 Policy Name | × |
| | | X | e Create | | |

2. Click the Create button.

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

| Virtual IP | 172.16.0.60 | L4 Protocol | UDP 引 |
|------------------------------|-------------------|--------------------------|------------|
| L4 Port | 4500 | Source IP From | 0.0.0.0 |
| L4 Policy Name | SAClusterESPSite1 | Source IP To | 0.0.0.0 |
| Farm Name | SACluster y | L7 Policy Name | None 💌 |
| Application | UDP | 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 | ~ |
| | 王 × | | |
| | Set Can | cel | |

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 | * |
| | 😨 🔉 | 2 | |
| | Set Can | icel | |

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 | × |
|--------------------|-------------|---------|----------------|-------------------|----------------|-----------|---|
| <u>172.16.0.60</u> | ТСР | 443 | 0.0.0.0 | SAClusterSSLSite1 | None | SACluster | |
| <u>172.16.0.60</u> | 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 Gl | obal Parameters | |
|---------------|----------------------------|--------------------------|
| Device Tuning | Client NAT Intercept Table | Client NAT Address Table |
| | | |
| | | |
| | | |
| | Client NAT Enabled | v) |
| | | |
| | 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.



- 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.

| Farm Name | SACluster | Radius Secret | |] |
|---|------------|---------------------------------------|---------------|---|
| Connection Limit Exception | Disabled 💌 | Client NAT Address Range | 172.16.0.73 💌 | |
| Transparent Server Support | Disabled 🔹 | SSL ID Tracking | Disabled 💌 | |
| Close Session At Aging | Disabled 🚩 | RADIUS Attribute | 0 |] |
| Reset Client on Server Failure | Disabled 🚩 | RADIUS Proxy Attribute | 0 |] |
| Add X-Forwarded-For to HTTP requests | Disabled 💌 | Insert Cookie for HTTP Persistency | Disabled | ~ |
| Hash Parameter For SIP | Call-ID 🖌 | SSL ID Aging | 120 |] |
| Select Server Per Transaction | Disabled 💌 | | | |
| | (| | | |

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 💌 | Туре | 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 🔽 | | |
| | (F | | |
| | S | et 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 | Туре | Connection Limit | Bandwidth Limit |
|--------------|-------------------|----------------|----------------|-----------------------|-------------------|-----------------|---------|---------------------|--------------------|
| SACluster | 172.16.0.61 | None | SA1 | Active | Regular | Enable | Regular | 0 | No Limit |
| | | · | | | | - | X | 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 💌 | Туре | 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 💌 | | | |
| | | | | |
| | S | et 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 | Туре | Connection Limit | Bandwidth Limit |
|------------------|-------------------|----------------|----------------|-----------------------|-------------------|-----------------|---------|---------------------|--------------------|
| <u>SACluster</u> | 172.16.0.61 | None | SA1 | Active | Regular | Enable | Regular | 0 | No Limit |
| <u>SACluster</u> | 172.16.0.62 | None | SA2 | Active | Regular | Enable | Regular | 0 | No Limit |
| <u>.</u> | <u></u> | | · | ^ | · | ^ | 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.

| Health Monitoring Global Parameters | | | | | | |
|---|--|--|--|--|--|--|
| Check Table Binding Table HM Server Table | | | | | | |
| | | | | | | |
| Health Monitoring Status: Use Health Monitoring | | | | | | |
| Response Level Samples: 0 | | | | | | |
| SSL Certificate File: rdwrhmm.cert | | | | | | |
| SSL Private Key File: rdwrhmm.key | | | | | | |
| | | | | | | |
| Set | | | | | | |

- 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.

| Health Monitoring Check Table | | | | | | ? Help |
|---|--------|--------|---------|----------------|----------|-----------|
| Binding Table Packet Sequence Table Health Monitoring Global Parameters | | | | | | |
| | | | | | | |
| Check Name | Method | Status | Dest IP | Response Level | \times | |
| \mathbf{X} | | | | | | |

Create

- 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.

Delete

| Check Name | SA1 | Method | нттре | |
|-----------------------|-------------|------------------------|-----------------------|--|
| Check Name | | Method | | |
| Destination Host | 172.16.0.61 | 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 | 0 | Status | Passed | |
| Reverse Check Result | disable 💌 | Uptime % | 100 | |
| Success Counter | 132 | Failure Counter | 0 | |
| Average Duration | 0 | | | |
| | | | | |
| | Set | Cancel | | |

- 7. Click the button next to **Arguments** to populate the specific settings for the rest of this check.
- 8. Enter the information 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 | | | | | |
| coue: HTTPS return | | | | | |
| code: | | | | | |
| æ | | | | | |
| Set | Cancel | | | | |

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.

| Health Monitoring Check Table | | | | | |
|-------------------------------|-----------------------|-------------------------------------|--|--|--|
| Binding Table | Packet Sequence Table | Health Monitoring Global Parameters | | | |

| Check Name | Check ID | Method | Status | Destination Host | × |
|---------------|----------|--------|--------|------------------|---|
| <u>SA1</u> | 0 | HTTPS | Passed | 172.16.0.61 | |
| Delete Create | | | | | |

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 | 200 |
| 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.

| Health Monitoring Check Table | | | | | | | |
|---|----------|--------|--------|------------------|----------|--|--|
| Binding Table Packet Sequence Table Health Monitoring Global Parameters | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Check Name | Check ID | Method | Status | Destination Host | \times | | |
| <u>SA1</u> | 0 | HTTPS | Passed | 172.16.0.61 | | | |
| SA2 1 HTTPS Passed 172.16.0.62 | | | | | | | |
| | | | | | | | |

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.

| | Health Monitoring Binding Table | | | | | |
|----|---|--------|--|--|--|--|
| | Check Table HM Server Table Health Monitoring Global Parameters | | | | | |
| | Check Server/NHR/Report Group Mandatory × | | | | | |
| | | | | | | |
| | | | | | | |
| | Delete Create | | | | | |
| 2. | Click the Create button. | | | | | |
| 3. | On the HM Binding Table Create page, enter the necessary parameters as shown here. | | | | | |
| | Check SA1 Server/NHR/Report Farm SACluster - 172.16.0. Group 이 Mandatory Mandatory マ | 61 - 0 | | | | |
| | Set Cancel | | | | | |
| | | | | | | |

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

| Health Monitoring Binding Table | | | | | | | |
|---|-------------------|-------|-----------|----------|--|--|--|
| Check Table HM Server Table Health Monitoring Global Parameters | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Check | Server/NHR/Report | Group | Mandatory | \times | | | |
| SA1 Farm SACluster - 0 Mandatory | | | | | | | |
| Delete Create | | | | | | | |

- 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.

Health Monitoring Binding Table

Check Table HM Server Table Health Monitoring Global Parameters

| Check | Server/NHR/Report | Group | Mandatory | × | | |
|---------------|-------------------------------------|-------|-----------|---|--|--|
| <u>SA1</u> | Farm SACluster - 172.16.0.61 - 0 | 0 | Mandatory | | | |
| <u>SA2</u> | Farm SACluster - 172.16.0.62 - 0 | 0 | Mandatory | | | |
| Delete Create | | | | | | |

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.

| lf Index | F-1 💌 | VR ID | 1 |
|--------------|-------------|--------------------|-----------------------|
| Admin Status | down 💌 | Priority | 200 |
| Primary IP | 172.16.0.71 | Auth Type | No Authentication 🛛 👻 |
| Auth Key | | Advertise Interval | 1 |
| Preempt Mode | False 🗸 | Protocol | ip 💌 |
| | . | | |
| | Set | Cancel | |

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

| lf Index | F-1 | * | | VR ID | 1 | ۷ | |
|---------------|---------|------|--------|-------|---|---|--|
| Associated IP | 172.16. | D.60 |) | | | | |
| | | | × | | | | |
| | Se | t | Cancel | | | | |

³For 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.

| Associated IP Addresses | | | | | |
|---|------------|------|---------------|---|--|
| Virtual Router Table Active Device Parameters Backup Device | | | | | |
| | | | | | |
| | lf Index | VRID | Associated IP | × | |
| | <u>F-1</u> | 1 | 172.16.0.60 | | |
| Delete Create | | | | | |

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

| lf Index | F-1 | * | | VR ID | 1 | * |
|-----------------|-----------|----|---------------|-------|---|---|
| Associated IP (| 172.16.0. | 73 | | | | |
| | Set | Ca | R ncel | | | |

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.

| ssociated IP Addresses | | | | | | | |
|----------------------------|---|------|---------------|---|--|--|--|
| Virtu | Virtual Router Table Active Device Parameters Backup Device | | | | | | |
| | | | | | | | |
| | lf Index | VRID | Associated IP | × | | | |
| | <u>F-1</u> | 1 | 172.16.0.60 | | | | |
| <u>F-1</u> 1 172.16.0.73 □ | | | | | | | |
| Delete Create | | | | | | | |

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.

| lf Index | F-1 | VR ID | 1 |
|---------------|--------------|--------------------|-----------------------|
| VR MAC | 00005e000101 | State | initialize |
| Admin Status | up 🔽 | Priority | 200 |
| Address Count | 2 | Master IP | 0.0.0.0 |
| Primary IP | 172.16.0.71 | Auth Type | No Authentication 🛛 👻 |
| Auth Key | | Advertise Interval | 1 |
| Preempt Mode | False 💌 | Up Time | 0 |
| Protocol | ip 💌 | | |
| | | × | |
| | Set | Cancel | |

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.

| Virtual Router Table | | | | | | | |
|--|---------------|-----------|---------------|--------------|----------------------|-----------------|--|
| <u>Configuration</u> | Associated IP | Addresses | Active Device | e Parameters | Backup Device Parame | <u>eters Mi</u> | |
| VRIDs Up/Down No Change 💌 Set Virtual Router Table | | | | | | | |
| If Index | VR ID | VR MA | IC | State | Admin Status | \times | |
| <u>F-1</u> 1 00005e000101 master up □ | | | | | | | |
| Delete Create | | | | | | | |

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

| Dynamic DNS Persistency Table Mirroring | Disabled 🔽 |
|---|------------|
| Client Table Mirroring | enable 💌 |
| Session ld Table Mirroring | disable 💌 |
| Set | |

- 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 | ТСР |
|------------------------------|-------------------|--------------------------|--------------|
| 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 | v | | |
| | E | | |

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.

| | 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 wind |
| 5. | Click the Create button. |
| 6. | On the Client NAT Intercept Table Create page, enter the necessary parameters as |



- 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.

| From IP Address | (172.16.0.73)To IP Address (172.16.0.73 | |
|-----------------|---|--|
| | | |
| | Set Cancel | |

- 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.

| Farm Name | SACluster | | Radius Secret | | |
|---|------------|---|---------------------------------------|---------------|---|
| Connection Limit Exception | Disabled 💌 | | Client NAT Address Range | 172.16.0.73 💌 | |
| Transparent Server Support | Disabled | ~ | SSL ID Tracking | Disabled 💌 | |
| Close Session At Aging | Disabled 💌 | | RADIUS Attribute | 0 | |
| Reset Client on Server Failure | Disabled 💌 | | RADIUS Proxy Attribute | 0 | |
| Add X-Forwarded-For to HTTP requests | Disabled 💌 | | Insert Cookie for HTTP Persistency | Disabled | ~ |
| Hash Parameter For SIP | Call-ID 💌 | | SSL ID Aging | 120 | |
| Select Server Per Transaction | Disabled 💌 | | | | |
| | | ļ | z × | | |

Set

Cancel

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.

| 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 💌 | | Туре | 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 the parameters.
- 5. Create the second server using the information show 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 💌 | Туре | 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

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 | Туре | 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 |
| - | | | | · | | | X | Create | |

Cancel

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.

| Health Monitoring Global Parameters | ? Help |
|---|-----------|
| Check Table Binding Table HM Server Table | |
| | |
| | |
| Health Monitoring Status: Use Health Monitoring | • |
| Response Level Samples: 0 | |
| SSL Certificate File: rdwrhmm.cert | |
| SSL Private Key File: rdwrhmm.key | |
| Set | |
| Set | |

- 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.

| Health Monitoring Check Table | | | | | |
|---|--|---|--|---|--|
| Binding Table Packet Sequence Table Health Monitoring Global Parameters | | | | | |
| | | | | | |
| Method | Status | Dest IP | Response Level | \times | |
| | × | | | | |
| | nitoring Packet Sequ Method | nitoring Chec Packet Sequence Table Method Status | nitoring Check Table Packet Sequence Table Method Status Dest IP | nitoring Check Table Packet Sequence Table Method Status Dest IP Response Level | nitoring Check Table Health Monitoring Global Parameters Packet Sequence Table Health Monitoring Global Parameters Method Status Dest IP Response Level X Image: Comparison of the second status Image: Comparison of the second status Image: Comparison of the secon |

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

| Check Name | SA1 | Method | HTTPS | |
|-----------------------|-------------|------------------------|-----------------------|---|
| Destination Host | 172.16.0.61 | 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 | 0 | Status | Passed | |
| Reverse Check Result | disable 🖌 | Uptime % | 100 | |
| Success Counter | 132 | Failure Counter | 0 | |
| Average Duration | 0 | | | |
| | | | | |
| | Set | Cancel | | |

7. Click the button next to Arguments

to populate the specific settings for the rest of this check.

8. Enter the information shown here.

| Arguments for | r 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: | |
| E Sat | |

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 | | |
| | . | | |

13. Click the button next to Arguments

to configure the specific arguments as shown here.

Arguments for HTTPS Method

Cancel

Set

| /dana-na/auth/url_defau |
|-------------------------|
| |
| GET 💌 |
| |
| |
| |
| ~ |
| 200 |
| |
| |
| |
| 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.

| Health Monitoring Check Table | | | | | |
|---|----------|--------|--------|------------------|---|
| Binding Table Packet Sequence Table Health Monitoring Global Parameters | | | | | |
| | | | | | |
| | | | | | |
| Check Name | Check ID | Method | Status | Destination Host | × |
| <u>SA1</u> | 0 | HTTPS | Passed | 172.16.0.61 | |
| <u>SA2</u> | 1 | HTTPS | Passed | 172.16.0.62 | |
| | | Delete | Create | | |

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.

| | Health Monitoring Binding Table | | |
|----|--|--------|--|
| | Check Table HM Server Table Health Monitoring Global Parameters | | |
| | Check Server/NHR/Report Group Mandatory 🗙 | | |
| | Delete Create | | |
| 2. | Click the Create button. | | |
| 3. | On the HM Binding Table Create page, enter the necessary parameters as shown here. | | |
| | CheckSA1Server/NHR/ReportFarm SACluster - 172.16.0.6Group0Mandatory | 61 - 0 | |
| | Set Cancel | | |

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

| Check Table HM Server Table Health Monitoring Global Parameters | | | | |
|---|-------------------------------------|--------|-----------|---|
| Check | Server/NHR/Report | Group | Mandatory | × |
| <u>SA1</u> | Farm SACluster - 172.16.0.61 - 0 | 0 | Mandatory | |
| | Delete (| Create | | |

- 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.

Health Monitoring Binding Table

Check Table HM Server Table Health Monitoring Global Parameters

| Check | Server/NHR/Report | Group | Mandatory | × |
|------------|-------------------------------------|--------|-----------|---|
| <u>SA1</u> | Farm SACluster - 172.16.0.61 - 0 | 0 | Mandatory | |
| <u>SA2</u> | Farm SACluster - 172.16.0.62 - 0 | 0 | Mandatory | |
| | Delete 0 | Create | | |

Backup AppDirector VRRP Configuration

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

| IP Redundancy Admin Status | VRRP 🕑 |
|--------------------------------------|-----------|
| Interface Grouping | enable 💌 |
| ARP With Interface Grouping | Send 💌 |
| Backup Device in VLAN | disable 💌 |
| Backup Fake ARP | enable 💌 |
| Backup Interface Grouping | enable 💌 |
| VRRP Advertise Interval [msec] | 0 |
| VRRP Automated Configuration Updates | Enabled 💌 |
| Force Down Ports Time | 0 |
| | |
| Set | |

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

| lf Index | F-1 💌 | VR ID | 1 |
|----------------|------------|--------------------|-----------------------|
| Admin Status | down 💌 | Priority | 100 |
| Primary IP 🛛 [| 72.16.0.72 | Auth Type | No Authentication 🛛 💌 |
| Auth Key | | Advertise Interval | 1 |
| Preempt Mode 🌔 | False 🕑 | Protocol | ip 💌 |
| | Ŧ | × | |
| | Set | Cancel | |

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.



| F-1 | VR ID | 1 |
|--------------|---|---|
| 00005e000101 | State | initialize |
| up 💌 | Priority | 100 |
| 2 | Master IP | 0.0.0.0 |
| 172.16.0.72 | Auth Type | No Authentication 🛛 👻 |
| | Advertise Interval | 1 |
| False 💌 | Up Time | 0 |
| ip 💌 | | |
| Set | Cancel | |
| | F-1 00005e000101 up v 2 172.16.0.72 False v ip v Set | F-1 VR ID 00005e000101 State up V Priority 2 Master IP 172.16.0.72 Auth Type Advertise Interval False V Up Time ip V Set Cancel |

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

- Virtual Router Table Associated IP Addresses Active Device Parameters nfiguration Backup Device Parameters Mi VRIDs Up/Down | No Change 💌 Set Virtual Router Table VR ID **VR MAC** Admin Status F-1 1 00005e000101 backup up х Delete Create
- 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 | License for total concurrent users |
| | Enables Juniper Networks Secure Applica- tion Manager and Network Connect for SA 6000 | |
| 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...

Create New Cluster

| Create | | | | |
|-------------------|-------------|---|--|--|
| Туре: | SA-6000 | | | |
| Cluster Name: | sa-dcb | Name of the cluster to create. Must be alphanumeric, "-", or "_"; and must start with a letter. | | |
| Cluster Password: | sololololol | Shared secret among the nodes in the cluster. Must be at least 6 characters long | | |
| Confirm Password: | sekekekek | Shared secret among the nodes in the cluster. Must match the password you typed in the previous line | | |
| Member Name: | sa6000-c | 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 <i>sa6000-c</i> to the cluster. Click Cancel if you do not want to create a cluster. |
| Create |
| |

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 |
| |
| Cluster Name: sa-dcb |
| Cluster Password: Velecence |
| Confirm Password: Westerer |
| Configuration Settings |
| C 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: |
| External VIP: |
| |
| Active/Active configuration |
| i his mode requires an external load-balancer. |
| Synchronization Settings |
| Protocol: Ounicast OMulticast OBroadcast |
| 🗖 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 |
| |

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.

| Clus | Clustering | | | | | | | |
|--|--|------------------|------------------|--------|----------------------|------------------|--|--|
| Stat | Status Properties | | | | | | | |
| Cluster Name: sa-dcb Type: SA-6000 Configuration: Active/Active Add Members Enable Disable Remove | | | | | | | | |
| | Member Name | Internal Address | External Address | Status | Notes | Sync Rank Update | | |
| □ * | * <u>sa6000-c</u> | 8.8.9.9/25 | 172.16.8.61/23 | ٩ | Leader | 0 | | |
| | <u>sa6000-d</u> | 8.8.9.8/25 | 172.16.8.62/23 | 0 | Enabled, Unreachable | 0 | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| * Ind | * Indicates the node you are currently using | | | | | | | |

- 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.

| Add Cluster Member | | | | | | | |
|---------------------------------------|-----------------|------------------|-------------|------------------|------------------|-----|--|
| Cluster: | | | | | | | |
| Delete | | | | | | | |
| 🖾 Node Name Internal IP address Inter | ernal Netmask I | Internal Gateway | External IP | External Netmask | External Gateway | | |
| sa6000-d 8.8.9.8 255.3 | .255.255.128 | 8.8.9.1 | 172.16.8.62 | 255.255.254.0 | 172.16.8.1 | Add | |
| | | | | | | | |
| Save Changes Cancel | | | | | | | |

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

Joining a Cluster in sa6000-d

Clusterina >

1-1-

 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).

Join Existing Cluster

| Cluster Name: | sa-dcb | Name of the cluster to join |
|--------------------------|-------------|--|
| Cluster Password: | kololololok | |
| Existing Member Address: | 8.8.9.9 | 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.

| Clus | Clustering | | | | | | | | |
|---|-----------------------------------|------------------|------------------|--------|---------|--------------|-------|--|--|
| Stat | Status Properties | | | | | | | | |
| Cluster Name: sa-dcb Type: SA-6000 Configuration: Active/Active | | | | | | | | | |
| Add | Add Members Enable Disable Remove | | | | | | | | |
| | Member Name | Internal Address | External Address | Status | Notes | Sync Rank Up | odate | | |
| □ * | <u>sa6000-c</u> | 8.8.9.9/25 | 172.16.8.61/23 | ٩ | Leader | 0 | | | |
| | <u>sa6000-d</u> | 8.8.9.8/25 | 172.16.8.62/23 | ٩ | Enabled | 0 | | | |

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.

| Farm Name | SAClusterSite1 | 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 | ~ | | | |
| | | | | | | | |

- 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 | Туре |
|----------------|-------------------|----------------|------------------|-----------------------|-------------------|-----------------|---------|
| SAClusterSite1 | 172.16.0.61 | None | SAClusterServer1 | Active | Regular | Enable | Regular |
| SAClusterSite1 | 172.16.0.62 | None | SAClusterServer2 | Active | Regular | Enable | Regular |
| | · | | ^ | · | | | |



- 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.

| SAClusterSite1 172.16.0.61 None SAClusterServer1 Active Regular Enable | Regular |
|--|---------|
| SAClusterSite1 172.16.0.62 None SAClusterServer2 Active Regular Enable | Regular |



- 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 | Туре | |
|----------------|-------------------|----------------|------------------|-----------------------|-------------------|-----------------|---|--|
| 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 | |
| | | | | | | De | K 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 | × | |
|--------------------|-------------|---------|----------------|------------------|----------------|----------------|---|--|
| <u>172.16.0.60</u> | ТСР | 443 | 0.0.0.0 | SASite1Policy | None | SAClusterSite1 | | |
| <u>172.16.0.60</u> | 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).

| Virtual IP | 172.16.0.59 | L4 Protocol | Any |
|------------------------------|------------------------|--------------------------|--------------|
| L4 Port | Any | Source IP From | 0.0.0.0 |
| L4 Policy Name | Virtual Interface | Source IP To | 0.0.0.0 |
| Farm Name | None 💌 | L7 Policy Name | None 💌 |
| Application | Virtual IP Interface 💌 | 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 💌 | Policy DefinedBy | User Defined |
| Segment Name | ~ | | |
| | Ŧ | × | |
| | Set | Cancel | |

- 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 | × |
|--------------------|-------------|---------|----------------|-------------------|----------------|----------------|---|
| <u>172.16.0.59</u> | Any | Any | 0.0.0.0 | Virtual Interface | None | None | |
| <u>172.16.0.60</u> | TCP | 443 | 0.0.0.0 | SASite1Policy | None | SAClusterSite1 | |
| <u>172.16.0.60</u> | UDP | 4500 | 0.0.0.0 | SAESPSite1Policy | None | SAClusterSite1 | |
| | | | | | | | |



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 |
| | S | E X 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 | If local DNS servers exist which provimity |
| Backup DNS Address | 0.0.0.0 | calculations should not |
| Proximity Aging Period [min] | 2880 | be made, please enter |
| Hops Weight | 1 | Hops, Latency and Load |
| Latency Weight | 1 | can be defined to have |
| Load Weight | 1 | the outcome. Those |
| Proximity Table Cleanup [min] | 0 | weights would also be |
| Ŧ | | 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.

| 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.

| lf Index | F-1 | * | VR ID | 1 |
|---------------|----------|-----|--------|---|
| Associated IP | 172.16.0 | .59 |) | |
| | | Set | Cancel | |

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 💌 |
| | Ţ | | |
| | 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.



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 | Туре |
|----------------|-------------------|----------------|------------------|-----------------------|-------------------|-----------------|---------|
| 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.

| F | 01010400340 | | Common Adding on | 470.40.0.00 |
|----------------------|------------------|-----|--------------------------|---------------------------|
| Farm Name | (SACIUSTERSITEZ) | | 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 💌 | | Туре | 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 💌 | | | |
| | | Ŧ | | |
| | | 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 | Туре |
|----------------|-------------------|----------------|------------------|-----------------------|-------------------|-----------------|----------------------------|
| 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 |



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 | × |
|--------------------|-------------|---------|----------------|------------------|----------------|----------------|---|
| <u>172.16.8.60</u> | ТСР | 443 | 0.0.0.0 | SASite2Policy | None | SAClusterSite2 | |
| <u>172.16.8.60</u> | UDP | 4500 | 0.0.0.0 | SAESPSite2Policy | None | SAClusterSite2 | |
| × v | | | | | | | |

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).

Delete

| Virtual IP | (172.16.8.59) | L4 Protocol | Any |
|------------------------------|------------------------|--------------------------|--------------|
| L4 Port | Any | Source IP From | 0.0.0.0 |
| L4 Policy Name | Virtual Interface | Source IP To | 0.0.0.0 |
| Farm Name | None 💌 | L7 Policy Name | None 💌 |
| Application | Virtual IP Interface 🛐 | 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 💌 | Policy DefinedBy | User Defined |
| Segment Name | * | | |
| | | × | |
| | Set | Cancel | |

- 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 | × | |
|--------------------|-------------|---------|----------------|-------------------|----------------|----------------|---|--|
| <u>172.16.8.59</u> | Any | Any | 0.0.0.0 | Virtual Interface | None | None | | |
| <u>172.16.8.60</u> | ТСР | 443 | 0.0.0.0 | SASite2Policy | None | SAClusterSite2 | | |
| <u>172.16.8.60</u> | UDP | 4500 | 0.0.0.0 | SAESPSite2Policy | None | SAClusterSite2 | | |
| 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 change the parameters as shown here.

| Host Name global. | example.com Externa | al NAT Address | 0.0.0.0 |
|-----------------------|---------------------|----------------|---------------|
| L4 Policy Name SASite | 2Policy 🗹 Preferr | ed Resolve IP | 172.16.8.60 💌 |
| Farm Name SAClus | terSite2 💌 | | |
| | | × | |
| | Set C | Cancel | |

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 | | |
| | | | | | |
| | Se | et 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 14-policy table create 172.16.0.60 TCP 443 0.0.0.0 \
SAClusterSSLSite1 -fn SACluster -ta HTTPS
appdirector 14-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 \backslash
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 12-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

IDevice Configuration
IDate: 14-02-2008 20:39:08
IDeviceDescription: AppDirector
IBase MAC Address: 00:03:b2:3d:41:c0
ISoftware Version: 1.06.07 (Build date Feb 13 2008, 23:50:02,Build#50)
IAPSolute OS Version: 10.31-01.01(26):2.06.06
I
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 14-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

Copyright 2008 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. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

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