

REMOTE ACCESS PROTECTION

Best Practices for Implementing Remote Access Protection Using Juniper Networks SA Series SSL VPN Appliances, IDP Series Intrusion Detection and Prevention Appliances and STRM Series Security Threat Response Managers

Table of Contents

Introduction	1
Scope.....	1
Target Audience	1
Design Considerations	1
Requirements and Recommended Devices	2
Authorized Secure Remote Access	2
Traffic Inspection and Coordinated Threat Control	3
Centralized Security Management, Visibility and Control.....	3
Network and Security Devices Generating Events/Logs.....	3
STRM Series Operational Guidelines	4
Monitoring the Dashboard	4
Enterprise Security State	5
Enterprise Vulnerability State	5
Most Severe and Most Recent Offenses	5
Top Attackers and Targets	5
Offense Investigation	5
Implementation Guidelines	6
Configure the IDP Series and SA Series Device	6
1. Creating a One-time Password (OTP) on the IDP Series.....	6
2. Configuring a Route to the SA Series Device	6
3. Configuring IPS Policies for Event Logging	7
4. Configuring IDP Series Sensor on the SA Series Device	7
5. Configuring a Quarantine Role for Restricted Access	8
6. Configuring the Sensor Event Policy	9
7. Enabling the IDP Series and SA Series Connection	11
Troubleshooting Coordinated Threat Control.....	11
Connectivity Issues	11
Failure of Logs to Appear.....	11
Integrating Network and Security Devices with STRM Series	12
1. Adding Sensor Devices on STRM Series.....	12
2. Configuring J-Flow on STRM Series.....	14
3. Configuring NSM Log Export to STRM Series	14
4. Configuring SA Series Device for Log Forwarding to STRM Series.....	14
5. Sending Flow Records to STRM Series from Junos OS Routers	15
Troubleshooting STRM Series Connection.....	16
Summary	16
About Juniper Networks.....	16

Table of Figures

- Figure 1: Sample Reference Network Enforcing Remote Access Protection Requirements 2
- Figure 2: Example of STRM Series Dashboard View 4
- Figure 3: Example of Offensive Investigation 5
- Figure 4: Event Analysis Window 6
- Figure 5: Configure SA Series Routing Table Entry 7
- Figure 6: IDP Policy for Event Logging 7
- Figure 7: Configuring a New Sensor 8
- Figure 8: Setting up the Quarantine User Role 9
- Figure 9: Creating the Sensor Policies 10
- Figure 10: Configuring the Sensor Policies 10
- Figure 11: IDP Series and SA Series Connection 11
- Figure 12: STRM Series Sensor Devices 12
- Figure 13: Protocol Configuration Parameters 13
- Figure 14: Editing a Sensor Device 13
- Figure 15: Configuring SA Series Device 13
- Figure 16: Flow Source Configuration 14
- Figure 17: Device Log Action 14
- Figure 18: SA Series Devices' Syslog Configuration 15

Introduction

Securing and protecting remote access users is a daunting and challenging task for most network administrators and enterprises. Existing security solutions have limited capabilities to adapt, scale and meet changing security landscapes.

Juniper Networks® Adaptive Threat Management Solutions comprise high-performance security platforms that leverage a dynamic cooperative system and network-wide visibility and control in order to adapt to changing risks. Juniper Networks Adaptive Threat Management Solutions provide a responsive and trusted security environment for your high-performance network. By leveraging a cooperative system of tightly integrated security products that include firewall, Juniper Networks SA Series SSL VPN Appliances, IDP Series Intrusion Detection and Prevention Appliances, STRM Series Security Threat Response Managers and Network and Security Manager, this solution adapts and secures the network against constantly evolving threats. The key characteristics of this solution are the following:

- A system of tightly integrated security products that adapt and proactively respond in real time to internal and external threats.
- Support for scalability in network requirements, traffic and applications while maintaining fast, reliable and secure access to applications and network resources, thereby eliminating security/performance tradeoffs.
- A single network-wide view for identification, mitigation and reporting on complex attacks, which eliminates false positives by using a highly advanced correlation system that enables IT and security staff to concentrate on actual security incidents. To effectively secure your network, these solutions deliver centralized management capabilities to help you adaptively protect your perimeter; proactively protect critical resources; and provide secure remote access with confidence.

In this paper, we discuss how to implement an essential part of Juniper Networks Adaptive Threat Management Solutions—namely remote access protection—helping the network administrator gain several major advantages in providing authorized secure remote access, Coordinated Threat Control, and enterprise-wide visibility and control. Furthermore, administrators can accomplish this crucial protection single-handedly through a centrally managed device. In this guide, we discuss how to implement SA Series SSL VPN Appliances, along with IDP Series and STRM Series, to provide the best remote access protection.

Scope

This paper specifically highlights one of the most important aspects of Juniper Networks Adaptive Threat Management Solutions—remote access protection, and it emphasizes best practices around centralized management and integration between Juniper Networks devices. The products discussed in this guide primarily include STRM Series, firewall, SA Series and IDP Series.

Target Audience

- IT managers
- Systems engineers
- Network analysts
- Network administrators.

Design Considerations

This section covers the key design considerations for remote access protection which is an integral part of Juniper Networks Adaptive Threat Management Solutions. For further details regarding these solutions, refer to the *Adaptive Threat Management Reference Architecture* document.

Figure 1 depicts a sample reference network showing Juniper Networks security devices such as Juniper Networks ISG Series Integrated Security Gateways, SA Series, IDP Series, STRM Series and NSM, all of which define remote access protection requirements (see Table 1 for requirements and recommended devices). This sample reference network consists of a small data center that connects to the Internet. The ISG Series acts as the firewall protecting the perimeter. The IDP Series appliance and the SA Series appliance sit behind the ISG Series. The Juniper Networks EX Series Ethernet Switches sit behind the IDP Series connecting to the rest of the LAN network. STRM Series and NSM are the management tools that are connected to the network to monitor and manage the various devices. The remote user connects to the SA Series appliance, gets authenticated, and then accesses the appropriate applications hosted on this network.

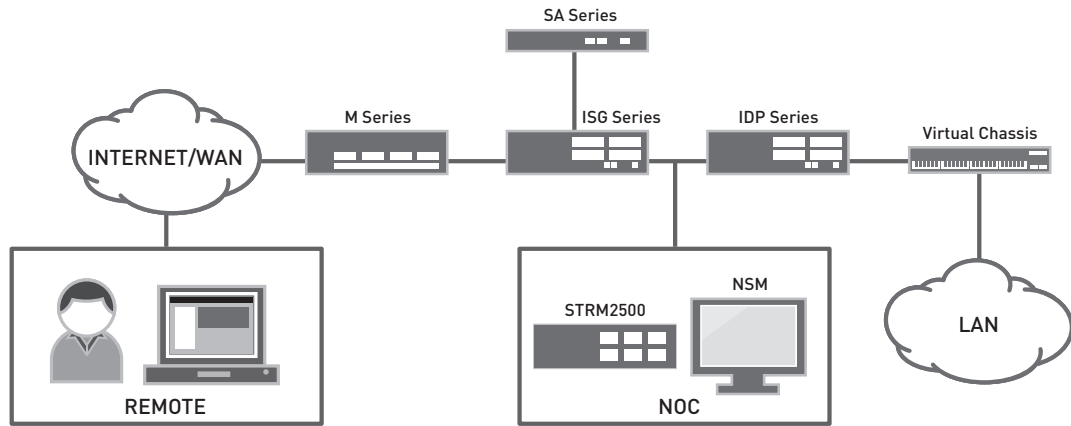


Figure 1: Sample Reference Network Enforcing Remote Access Protection Requirements

The key design considerations for implementing remote access protection consist of the following:

- Authorized secure remote access
- Traffic inspection and Coordinated Threat Control
- Centralized security management and enterprise-wide visibility and control

Requirements and Recommended Devices

Table 1 lists the requirements and recommended devices that define remote access protection. To effectively and efficiently monitor and control threats targeted at remote access users, the enterprise needs to provide preventative and proactive security features such as authorized secure remote access, traffic inspection and Coordinated Threat Control that function throughout the entire network. In addition, allowing remote access devices to integrate with a centralized security management system that provides visibility and control, such as STRM Series/NSM, is crucial to successfully protecting the remote access user. STRM Series/NSM is explained in detail in the following sections.

Table 1: Requirements and Recommended Devices

Requirements	Recommended Devices
Authorized Secure Remote Access	<ul style="list-style-type: none"> • ISG Series • SA Series
Traffic Inspection and Coordinated Threat Control	<ul style="list-style-type: none"> • IDP Series
Centralized Security Management, Visibility and Control	<ul style="list-style-type: none"> • NSM • STRM Series

Authorized Secure Remote Access

Restricting unauthorized access provides the first layer of security (baseline security) and extends the capability to provide access to network resources based on authentication and authorization. This also allows a network administrator to correlate and identify the source of any attack or threat.

- Juniper Networks secure access is capable of authenticating remote users and provides granular resource access control policies. It also provides an encrypted secure connection between remote users and the enterprise network to prevent data theft during transmission. Integrating with an authentication server for user authentication and role assessment allows an administrator to define a granular resource access policy using role mapping and resource profiles.
- The network administrator can use Juniper Networks Host Checker policy to determine a remote client's security posture (antivirus, patch level, firewall, process check, and so on) as defined in the corporate compliance policy, thereby restricting access for non-compliant systems.

- The remote access protection solution easily integrates with Juniper Networks comprehensive Adaptive Threat Management Solutions by leveraging the capability of ISG Series Integrated Security Gateways to create a secure zone (security zones are an important feature of Juniper Networks firewall products) for critical resources and by limiting initial unauthenticated access to the remote access zone. This can be achieved by adding additional zones for the remote user, the untrust zone and the remote access zone that host SA Series devices.
- The network administrator should create a stateful firewall policy to allow traffic from remote users to secure access devices for authentication. Subsequent access to network resources is governed by authentication and authorization of the remote user through secure access devices. Creating stateful firewall policy provides a defense mechanism against any reconnaissance attacks and denial of service (DoS) attacks.
- The ISG Series and SA Series devices provide security events and logs that are analyzed by STRM Series. Note that more detailed information pertaining to STRM Series is covered later in this document.

Traffic Inspection and Coordinated Threat Control

Continuous traffic inspection allows a network administrator to identify attacks, such as those infecting critical resources or inserting worms or harmful traffic into the network. Integrating various security and network devices (to take preventive action when a threat is identified) is critical in preventing any attack from succeeding. This also allows you to provision the security device either manually or automatically to respond to any potential future threats.

- The traffic from authenticated remote users of network resources is inspected using an IDP Series device. Intrusion Detection and Prevention devices use multiple methods to identify malicious traffic. The IDP Series can be installed in sniffer mode to detect the attacks or in transparent mode to not only detect but prevent the attacks. Network administrators can use the system in sniffer mode for fine-tuning the security policy and then deploy it in transparent mode to prevent the threats.
- Juniper Networks IDP Series devices provide a Coordinated Threat Control mechanism by communicating with SA Series devices using adaptive threat messages when any threat is detected from remote users. The SA Series device should be configured to take adaptive action, such as quarantine the user or drop a connection, in order to restrict user access to resources and proactively defend the network from any potential threat.

Centralized Security Management, Visibility and Control

Remote access solution devices should integrate with the enterprise's centralized security management solution. A critical requirement of any security solution that spans the entire enterprise is that it must provide a network-wide perspective of all security events occurring across all locations at any time. Moreover, all aspects of the solution should be managed centrally, and events/logs from multiple devices in the path of traffic (switches, routers, firewalls, intrusion prevention systems), should be managed and correlated to gain a realistic perspective of the security attacks. Further, saving the events/logs for forensic analysis is also a critical requirement.

- Juniper Networks Network and Security Manager (NSM) provides a centralized configuration management and policy deployment capability. NSM can be used to collect logs from the security devices and forward them to STRM Series.
- STRM Series integrates and correlates logs from all network and security devices for centralized monitoring and reporting.

Network and Security Devices Generating Events/Logs

Table 1 lists the network and security devices that generate/trigger events and logs. This table also provides a summary of how STRM Series integrates and correlates events and traffic log information to provide a comprehensive report of network threats and vulnerabilities. For a visual perspective of STRM Series capabilities, see the screen graphics that illustrate STRM Series' dashboard. This dashboard view allows a network administrator to easily see the current health of the network and in particular, provides periodic reports for baseline and trend analysis.

Table 2: Network and Security Devices, Logs and Results

Network and Security Devices	Log Forwarding Types	Results
SA Series appliance	WebTrends Enhanced Log File (WELF) logs	Username, login time, mapped role, role change due to Adaptive Threat Management.
ISG Series/IDP Series	Logs are forwarded to STRM Series via NSM. Types of events/logs to report - Screen Alarm Log - Traffic Log - Deep Inspection Alarm Log	Forwarding logs via NSM reduces CPU utilization on security devices. These logs provide information about malicious traffic, threats like exploits, worm, virus, reconnaissance attacks and unauthorized access attempts.
J Series Services Routers/M Series Multiservice Edge Routers/routers	J-Flow and event logs	Provides traffic details for correlation with network attack and threat status.

STRM Series Operational Guidelines

STRM Series has a rich graphical user interface (GUI) that provides a snapshot of the day-to-day operations giving insight into the current health of the network. Juniper Networks remote access protection integration, an essential component of Adaptive Threat Management Solutions, provides centralized control for automated day-to-day operations. Illustrated below are some of the most important operational tasks that a network administrator should perform to ensure security across his or her enterprise network.

Monitoring the Dashboard

The dashboard allows you to monitor your overall network behavior, security and vulnerability posture, top targeted assets, top attackers, and worst and most recent security offenses—all from one window. Figure 2 is a snapshot of the STRM Series dashboard.

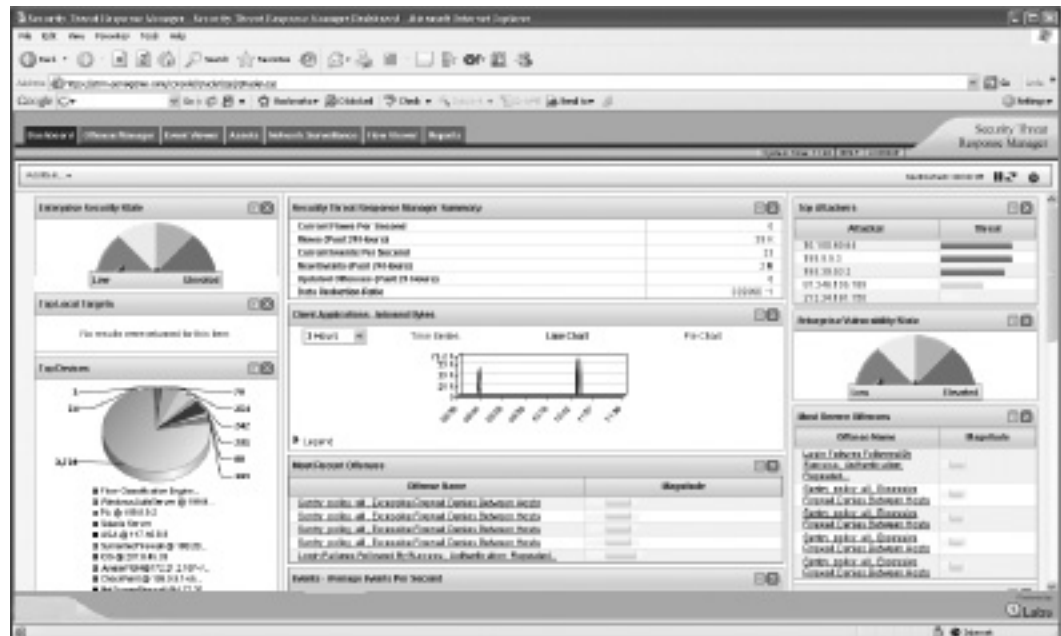


Figure 2: Example of STRM Series Dashboard View

Enterprise Security State

The Enterprise Security State represents your network's current security posture. The security state is formulated from monitoring the security data from flows, external events, and security data to create a single metric that reveals the security health of your network.

Enterprise Vulnerability State

The Enterprise Vulnerability State represents the network's current vulnerability posture. The vulnerability state is formulated from monitoring all vulnerability data across the entire network to create a single "current vulnerability" metric.

Most Severe and Most Recent Offenses

The most recent and severe offenses are identified and classed with a magnitude bar to inform you of the importance of the offense. Point your mouse to the IP address to view detailed information for the particular IP address.

Top Attackers and Targets

The Attackers and Targets option displays the top five attackers or top five local targets. Each target is identified with a magnitude bar to inform you of the importance of the target. Point your mouse to the IP address to view detailed information for a particular IP address.

Offense Investigation

STRM Series allows an administrator to investigate potential threats and attacks by allowing you to save an attack report and then perform a quarantine/analysis investigation.

STRM Series allows you to investigate any reported offense with necessary data from all security devices for forensic analysis. Below are the two steps for offense investigation.

1. From the most *Recent Offenses* or from the *Offense Manager* tab, double click the offense to access a more detailed report. Below is a sample of the offense report (Offense 3) for reference. The offense report provides a summary of such information as attacker source, attacker location, attack target, magnitude of the attack, and primary events.

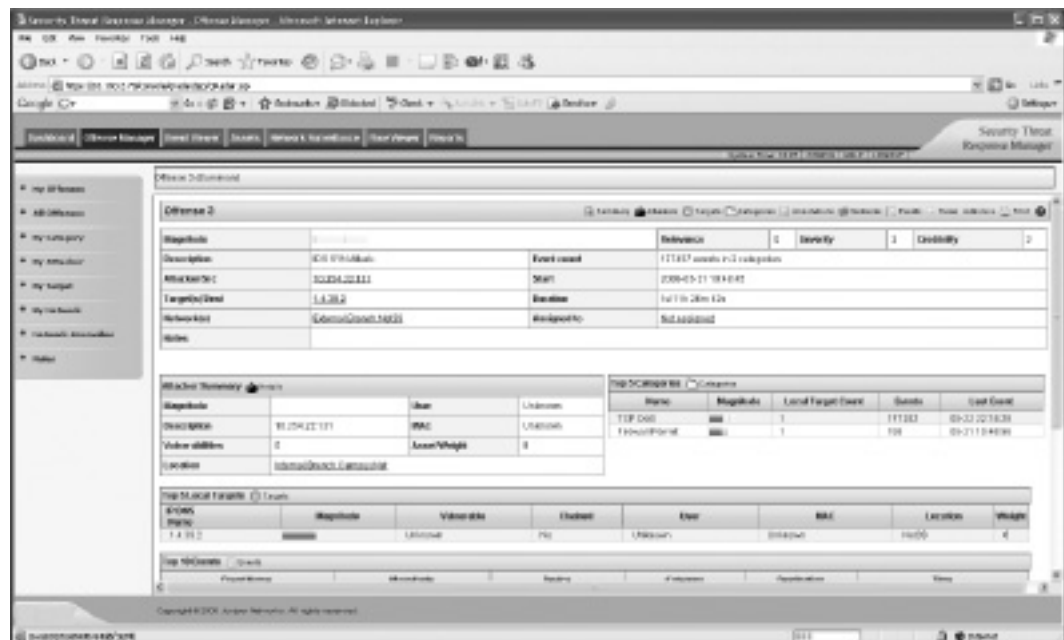


Figure 3: Example of Offensive Investigation

2. The report also provides drill down capability for forensic analysis of the offense. For further analysis, click the Events icon and open an event detail screen to analyze relevant events reported from all security devices. You can further customize the search using different filters and time intervals. Below is a sample screen for event analysis.

Event Name	Device	Event Count	Time	Category	Source IP	Source Port	Destination IP	Destination Port	Decrement	Magnitude
ICB SYN Attack	Adm-NSM	2	22:15	TOP DoS	10.254.22.131	14320	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	2047	22:11	TOP DoS	10.254.22.131	14891	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	1	22:11	TOP DoS	10.254.22.131	4581	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	1	22:09	TOP DoS	10.254.22.131	45315	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	1	22:09	TOP DoS	10.254.22.131	45315	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	2047	21:40	TOP DoS	10.254.22.131	45253	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	1	21:40	TOP DoS	10.254.22.131	35565	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	1	21:40	TOP DoS	10.254.22.131	35895	1.4.28.2	0		■■■■
ICB SYN Attack	Adm-NSM	1	21:45	TOP DoS	10.254.22.131	35895	1.4.28.2	0		■■■■

Figure 4: Event Analysis Window

Now that we've discussed the requirements and design considerations for Adaptive Threat Management Solutions, the next section provides detailed implementation guidelines.

Implementation Guidelines

The primary implementation guidelines discussed in this paper are as follows:

- Configuring the IDP Series and SA Series device
- Integrating network and security devices with STRM Series

Configure the IDP Series and SA Series Device

In order to configure the IDP Series and SA Series devices, perform the following major steps which are described in greater detail below:

1. Create a one-time password on the IDP Series appliance
2. Configure a route to the SA Series device
3. Configure IPS policies for event logging
4. Configure the IDP Series sensor on SA Series device
5. Configure quarantine role for restricted access
6. Configure the sensor event policy
7. Enable the IDP Series and SA Series connection

1. Creating a One-time Password (OTP) on the IDP Series

The following steps help you to create a one-time password on IDP Series:

- a. Launch the IDP Application Configuration Manager (ACM) and in the ACM menu, choose Reconfigure Management Server and IDP Instant Virtual Extranet (IVE) Communication.
- b. To generate an OTP, check the "Reset IVE OTP?" checkbox and click Next Step. The new IVE OTP displays at the top of the Final Configuration page and will be activated once the administrator confirms and applies the changes. For details, refer to the Intrusion Detection and Prevention (IDP) Installers Guide.

2. Configuring a Route to the SA Series Device

The connection from the IDP Series appliance to the SA Series device uses port 7103 and the inside address of the SA Series device. Configure a route to the SA Series inside address. The port configuration is within the SA Series configuration (see Figure 5).

Figure 5: Configure SA Series Routing Table Entry

3. Configuring IPS Policies for Event Logging

As an example, the following figure shows configuration policies, their level of severity, and the logging that displays on the NSM console.

No.	Source	Destination	Mar	Look For	Action	Notification
				Attacks		
1	any	any	<input type="checkbox"/>	<ul style="list-style-type: none"> http brute force HTTP: Server Error 404: Object Not Found_copy(1) SSH: Brute Force Login Attempt_copy(1) 	None	<ul style="list-style-type: none"> Logging Alert
2	any	any	<input type="checkbox"/>	<ul style="list-style-type: none"> Anomaly - Critical Response_Critical Signature - Critical 	None	<ul style="list-style-type: none"> Logging Alert Log Packets(10/10)
3	any	any	<input type="checkbox"/>	<ul style="list-style-type: none"> Anomaly - Major Response_Major Signature - Major 	None	<ul style="list-style-type: none"> Logging Alert Log Packets(10/10)
4	any	any	<input type="checkbox"/>	<ul style="list-style-type: none"> Anomaly - Minor Response_Minor 	None	<ul style="list-style-type: none"> Logging Log Packets(10/10)

Figure 6: IDP Policy for Event Logging

4. Configuring IDP Series Sensor on the SA Series Device

- To configure the sensor on the SA Series, select Configure>Sensors.
- Insert the one-time password (configured in Step 1) into the SA Series configuration. In addition, configure the name and IP address of the IDP Series appliance. The port used for communication is 7103. This will have to be open in firewall(s) that are in the path of the SA Series to IDP Series communication.
- Configure the addresses or address range that the remote clients will use and the address of the SA Series. It is these addresses and only these that the IDP Series appliance will use to send a signal to the SA Series device once an attack is triggered by an IPS policy.
- The severity filter determines a threshold of the signal's severity that will be sent to the SA Series device. If medium severity is configured, then all attacks of medium severity and higher are communicated to the SA Series device. You can set the severity level to high, medium or low.

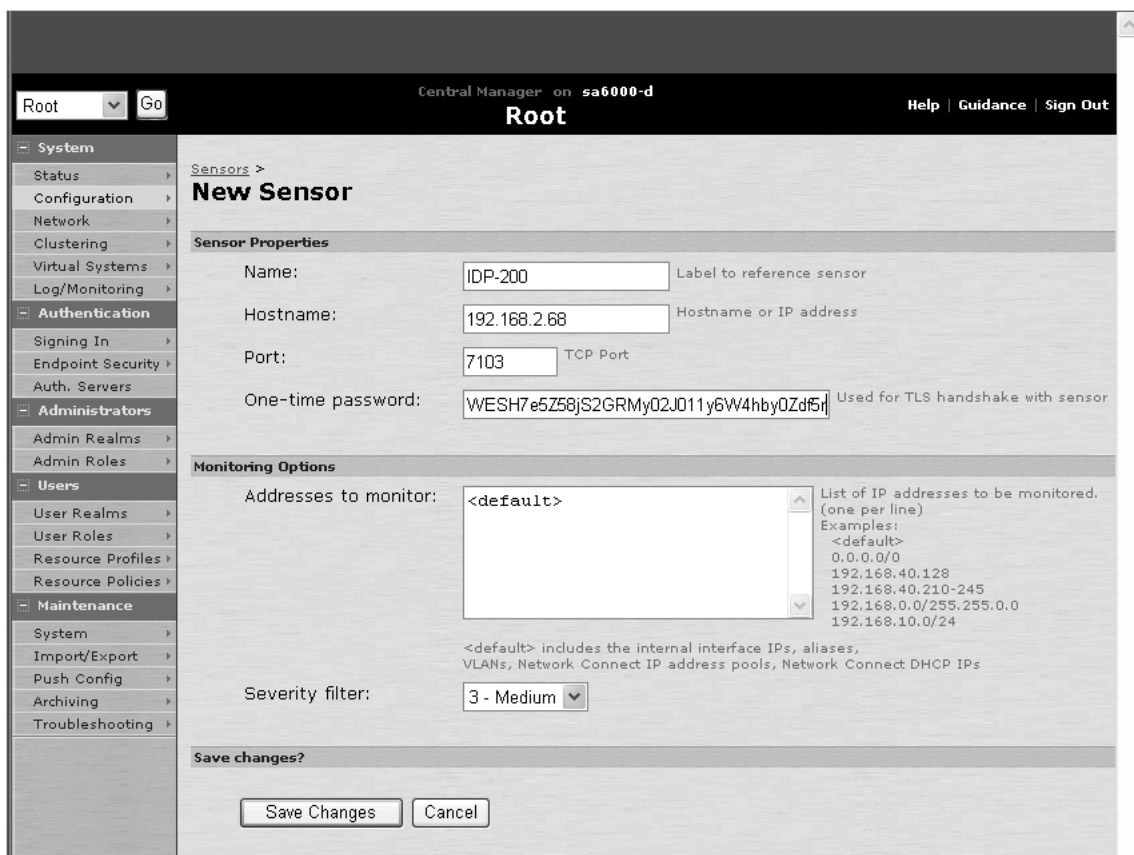


Figure 7: Configuring a New Sensor

5. Configuring a Quarantine Role for Restricted Access

Other than the usable “roles” that have resources assigned to them, create an additional “role” on the SA Series device that has no resources assigned to it. This will be the “quarantine role” that the IDP Series appliance triggers the SA Series to switch to when it signals the SA Series device that an attack has occurred. As shown in the following figure 8, once triggered, the SA Series changes the current user and its original role to the quarantine role.

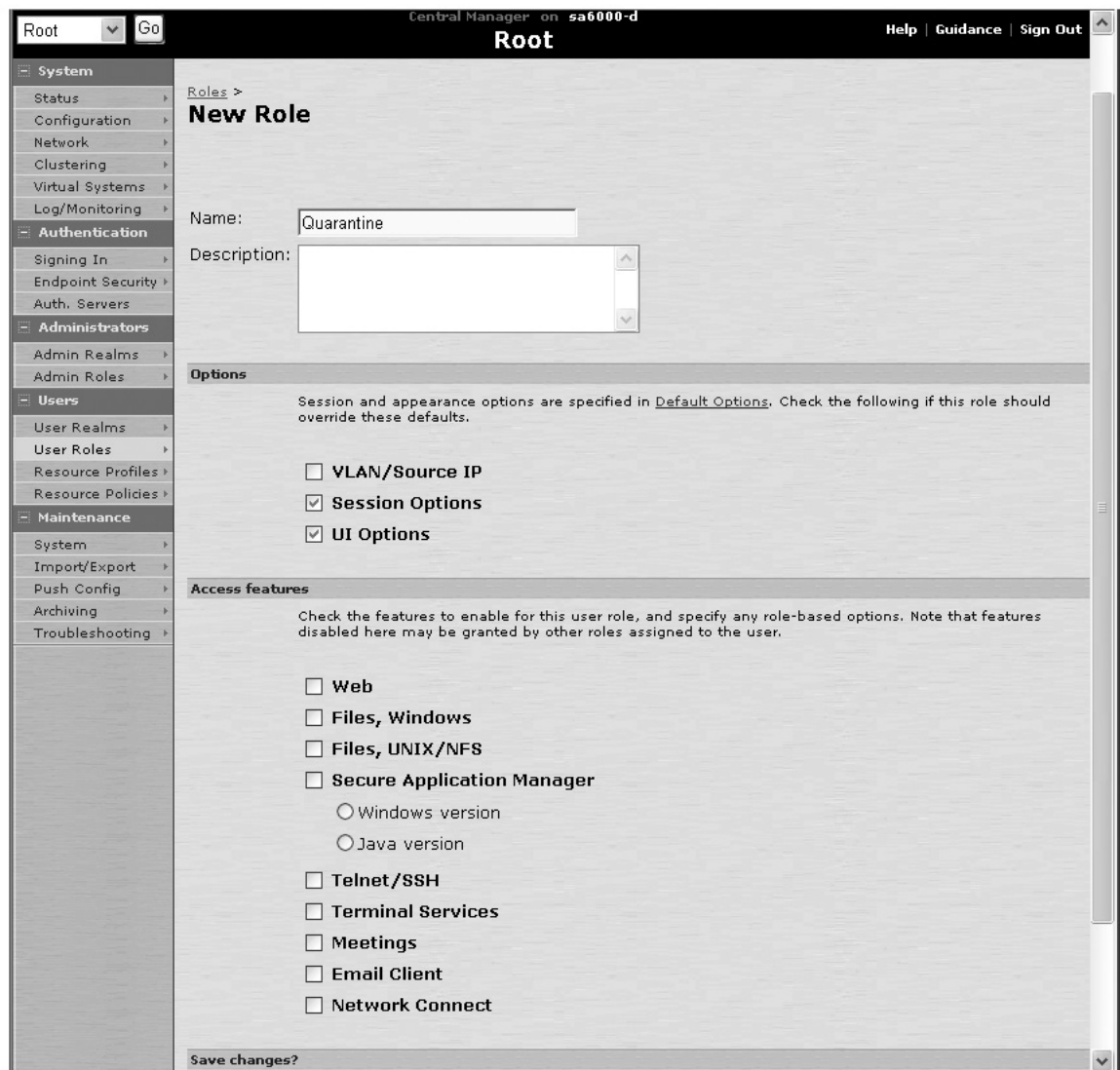


Figure 8: Setting up the Quarantine User Role

6. Configuring the Sensor Event Policy

When performing this task, refer to Figures 9 and 10.

- a. The Event option can be configured to switch or quarantine roles based on a specific sensor signal or event. Juniper Networks recommends that administrators use the default “any event” and an appropriate severity filter at least in the initial setup (see Figure 10).
- b. Initially configure the count to 1. This invokes the role switching with one event. This can be modified once a base has been configured and Coordinated Threat Control has been operating for a period of time.
- c. Configure the signal to replace the role for this session only. This assumes that the quarantine action will be caught and investigated. If the event indeed occurred, the enterprise network has been protected. If the event was benign and becomes a simple matter of educating the user, then this configuration will not prevent the user from trying to access the network in the future.
- d. Apply the rule to all appropriate roles (typically all roles).

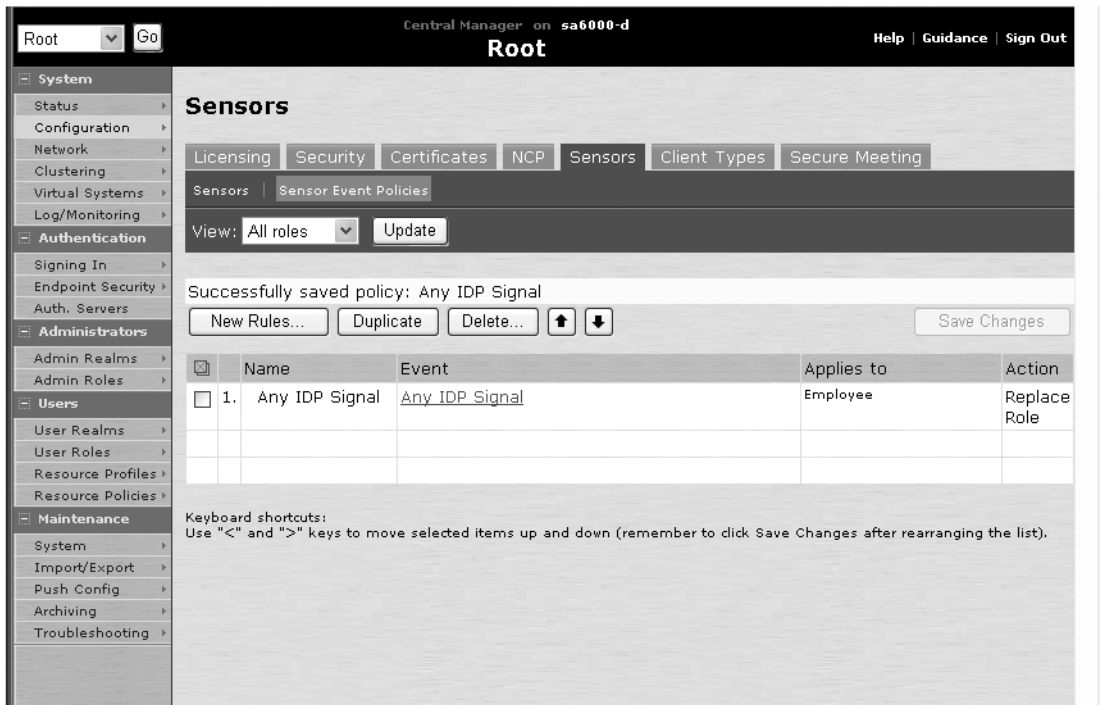


Figure 9: Creating the Sensor Policies

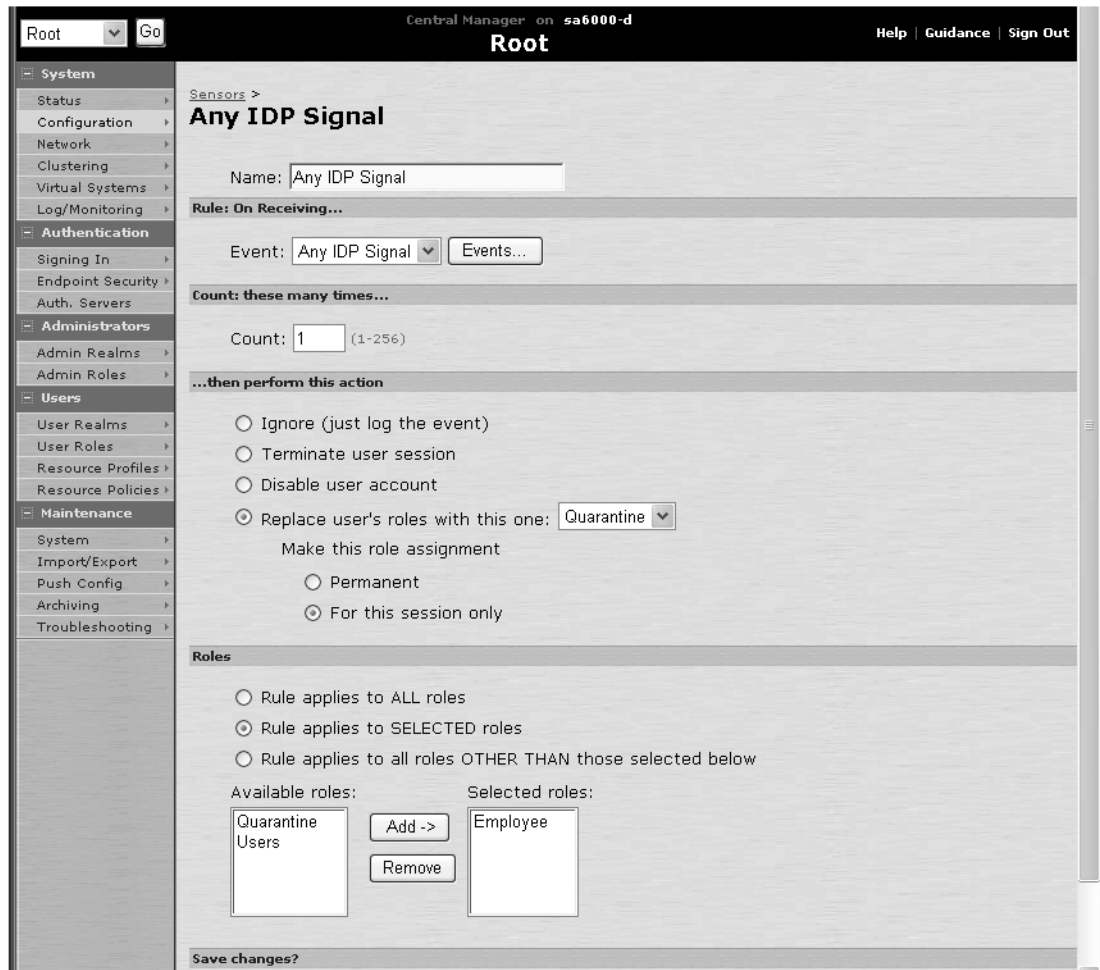


Figure 10: Configuring the Sensor Policies

7. Enabling the IDP Series and SA Series Connection

After SA Series and the IDP Series configurations have been completed, return to the SA Series sensor Configuration screen and enable the IDP Series and SA Series connection.

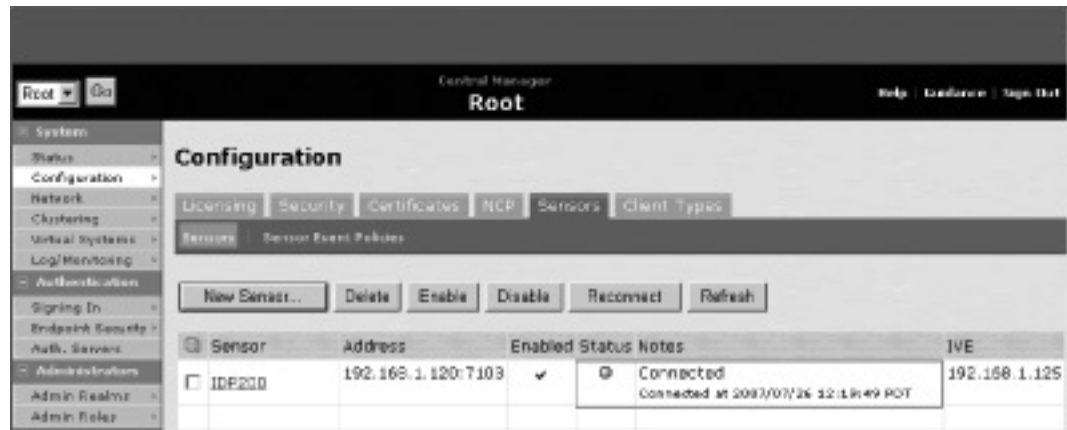


Figure 11: IDP Series and SA Series Connection

Troubleshooting Coordinated Threat Control

The majority of problems in this collaboration typically fall into two areas:

- Connectivity
- Failure of logs to appear

Connectivity Issues

There are many tools for connectivity problems as one would expect from any sophisticated networking device—pinging, traceroute and packet tracing (using ethereal freeware on PCs and laptops, using tcpdump on SA Series and IDP Series). All of these are available in one command form or another on Juniper Networks devices.

Failure of Logs to Appear

Logs may not appear for several reasons due to the Coordinated Threat Control mechanism malfunctioning. One may find that the IDP Series appliance has not signaled as expected, or that it signaled but the SA Series device either did not receive the signal or it did not switch users.

Loss of Signal or Signaling Event Steps

1. Confirm the connectivity between the IDP Series appliance and SA Series device (see the above paragraph for tools).
2. With NSM, confirm that the attacks are configured in the IPS policies. Make sure that the policy or policies contain the attacks the enterprise wants to monitor.
3. With NSM, confirm that logging is enabled on the IPS policy. It is the trigger for the IDP Series to SA Series signaling.
4. Confirm that the proper addresses are configured on the IDP Series appliance. See the first SA Series configuring a new sensor where “interesting” addresses are configured. The IDP Series appliance will only signal on the addresses that are configured in this screen (Configuration>Sensors).
5. Check the configured severity level (Configuration>Sensor>Sensor Events). Make certain that the severity level encompasses the severity of the signal that is configured in the policy.

Roles did not Switch to the Quarantined Role

1. Confirm that an event occurred that would switch roles.
2. Configure the quarantine role to have an idle time long enough to check and investigate, should the attacker or mistaken remote user remain connected to the IVE. You can observe the current user utilizing SSL VPN on the device at **Status>Active Users**.
3. Confirm if an attack occurred by exploring the logs in **NSM/IDP Series (Log Viewer>Predefined> IDP/DI** and the **SSL VPN logs (Log/Monitoring>Sensor)**.
4. Enable logging user access. If the user did switch to the quarantine role, there should be a log record of the switch. First, there should be matching log records in NSM that denote the attack. Second, follow the logging trail. The logical progression is as follows: first, NSM captures the IDP Series attack event in its log; then the SA Series device logs the sensor signal; if the mechanism occurs correctly, the administrator will see the log event where the user's role is switched (on the SA Series device).

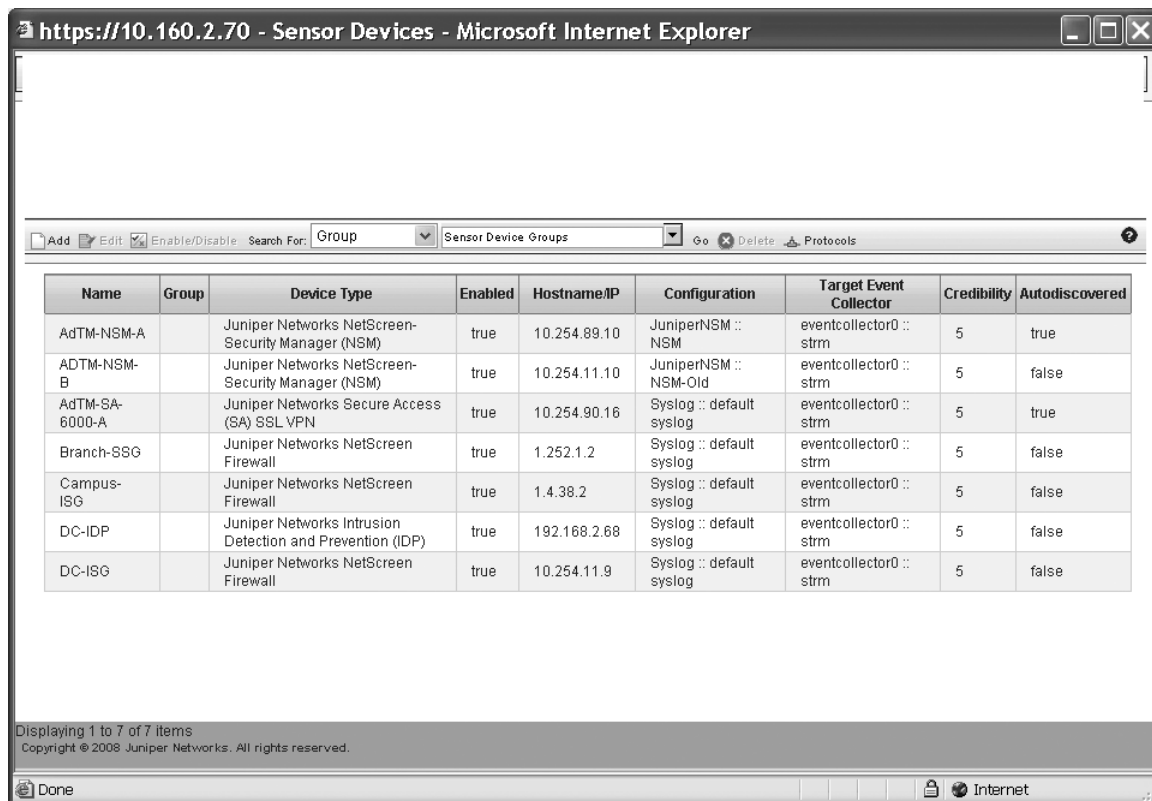
Integrating Network and Security Devices with STRM Series

Another important task is to integrate events and flow information with STRM Series for centralized monitoring and reporting. Below are the major steps to attain integration.

1. Adding sensor devices on STRM Series
2. Adding Flow Sources on STRM Series
3. Configuring NSM for Log Forwarding to STRM Series
4. Configuring SA Series device for Log Forwarding to STRM Series
5. Configuring Juniper Networks Junos® operating system for sending flow records to STRM Series

1. Adding Sensor Devices on STRM Series

- a. At the Administration Console, select **CONFIG>SIM Configuration>Sensor Device**.
- b. Click **Add**. The following window displays.



Name	Group	Device Type	Enabled	Hostname/IP	Configuration	Target Event Collector	Credibility	Autodiscovered
AdTM-NSM-A		Juniper Networks NetScreen-Security Manager (NSM)	true	10.254.89.10	JuniperNSM :: NSM	eventcollector0 :: strm	5	true
ADTM-NSM-B		Juniper Networks NetScreen-Security Manager (NSM)	true	10.254.11.10	JuniperNSM :: NSM-Old	eventcollector0 :: strm	5	false
AdTM-SA-6000-A		Juniper Networks Secure Access (SA) SSLVPN	true	10.254.90.16	Syslog :: default syslog	eventcollector0 :: strm	5	true
Branch-SSG		Juniper Networks NetScreen Firewall	true	1.252.1.2	Syslog :: default syslog	eventcollector0 :: strm	5	false
Campus-ISG		Juniper Networks NetScreen Firewall	true	1.4.38.2	Syslog :: default syslog	eventcollector0 :: strm	5	false
DC-IDP		Juniper Networks Intrusion Detection and Prevention (IDP)	true	192.168.2.68	Syslog :: default syslog	eventcollector0 :: strm	5	false
DC-ISG		Juniper Networks NetScreen Firewall	true	10.254.11.9	Syslog :: default syslog	eventcollector0 :: strm	5	false

Displaying 1 to 7 of 7 items
Copyright © 2008 Juniper Networks. All rights reserved.

Figure 12: STRM Series Sensor Devices

The following graphic illustrates an NSM sample configuration. NSM is a predefined DSM which means that STRM Series will recognize the log formats that are sent. Note that NSM is also given a credibility of 5. This number is a confidence level used to refine and consolidate the log messages from all devices and sensors. The default is 5; the range is 1 through 10. The STRM Series can also auto discover the sensor devices. STRM series needs at least 200 log messages from the device for it to discover it automatically.

Figure 13: Protocol Configuration Parameters

- c. Click **Configure >SIM Configuration >Protocol Configuration** to display the Juniper Networks NSM Configuration window. This configuration defines the ports and the IP addresses that STRM Series expects as source addresses for this sensor’s log events (see Figure 14). The IP address matches the additional configuration under sensors.

The following graphic illustrates an NSM sensor configuration example. The **Sensor Device Type**—Network-Security Manager (NSM) is predefined. The **Credibility** factor ranges from 1 to 10.

Figure 14: Editing a Sensor Device

The SA Series sensor configuration is similar to the NSM configuration. When adding a device from the Sensor menu, there is a predefined Juniper Networks SA Series device. Its protocol and thus its fields are prescribed by the syslog specification. Log events have a credibility of 5.

Figure 15: Configuring SA Series Device

2. Configuring J-Flow on STRM Series

You can configure flow collectors (J-Flow) from the Administrator Console. The configurations for Juniper Networks routers display on two configuration screens. The flow sources are used to designate that this flow collector is J-Flow, and the interface on which STRM Series expects to get flow reports, and the UDP port that is used in the messages.

Basically, Flow Source defines the flow type. In Adaptive Threat Management Solutions, we are using J-Flow generated from Juniper Networks routers. Flow Source Alias cross references an IP address to the Flow Source.

Edit Flow source ?

Flow Source Details

Flow Source Name	Campus-RTR-Jflow
Target Flow Collector	qflow0 :: strm
Flow Source Type	JFlow
<input type="checkbox"/> Enable Asymmetric Flows	

JFlow Configuration

Monitoring Interface	Any
Monitoring Port	9995
<input type="checkbox"/> Enable Flow Forwarding	

Figure 16: Flow Source Configuration

3. Configuring NSM Log Export to STRM Series

- From the Action Manager, select the NSM configuration. Configure the address of the syslog server (STRM Series) and the logging facility desired. Device log action defines the attack on a granular level and the severity that is reported in syslog.

Device Log Action Criteria - Juniper Networks - NSM - AdTM : current

File View Devices Tools Help

AdTM

- Log Viewer
- Report Manager
- Log Investigator
- Device Manager
- Policy Manager
 - Security Policies
 - Predefined IDP Policies
 - Domain Policies
- VPN Manager
- Object Manager
- Server Manager
- Realtime Monitor
- Security Monitor
- Job Manager
- Audit Log Viewer
- Action Manager
 - Action Parameters
 - Device Log Action Criteria**

Device Log Action Criteria

Type	Category	Subcategory	Severity	Actions
▶ domainba...	SCREEN	ICMP MTU Too Small	Info	syslog
		IDS IP Option SSRR	Warning	
		Block IP fragment traffic	Minor	
▶ domainba...	INFO		Info	syslog
▶ domainba...	ALARM	Device Dead	Info	syslog
		RIP Packet Flood	Not Set	
		CPU TIMEOUT FAIR to SHARE	Warning	
▶ domainba...	SIGNATURE	TCP: Options Error Dangerous O...	Info	syslog
		ICMP: Flood	Not Set	
		TCP: S2C Info ACK in LASTACK ...	Warning	
▶ domainba...	TRAFFIC	IP Action Close	Minor	syslog
		ARP Target HW Mismatch	Warning	
		Oversized TCP Segment	Major	

Figure 17: Device Log Action

4. Configuring SA Series Device for Log Forwarding to STRM Series

To access the SA Series device's syslog configuration, select **Log/Monitoring>Events>Settings**. The syslog server configuration is located at the bottom of the screen, as shown in Figure 18. The configurable parameters include the IP address of STRM Series, the syslog facility setting, and the filter which allows the user to set customizable messages. STRM Series supports syslogs in WELF format.

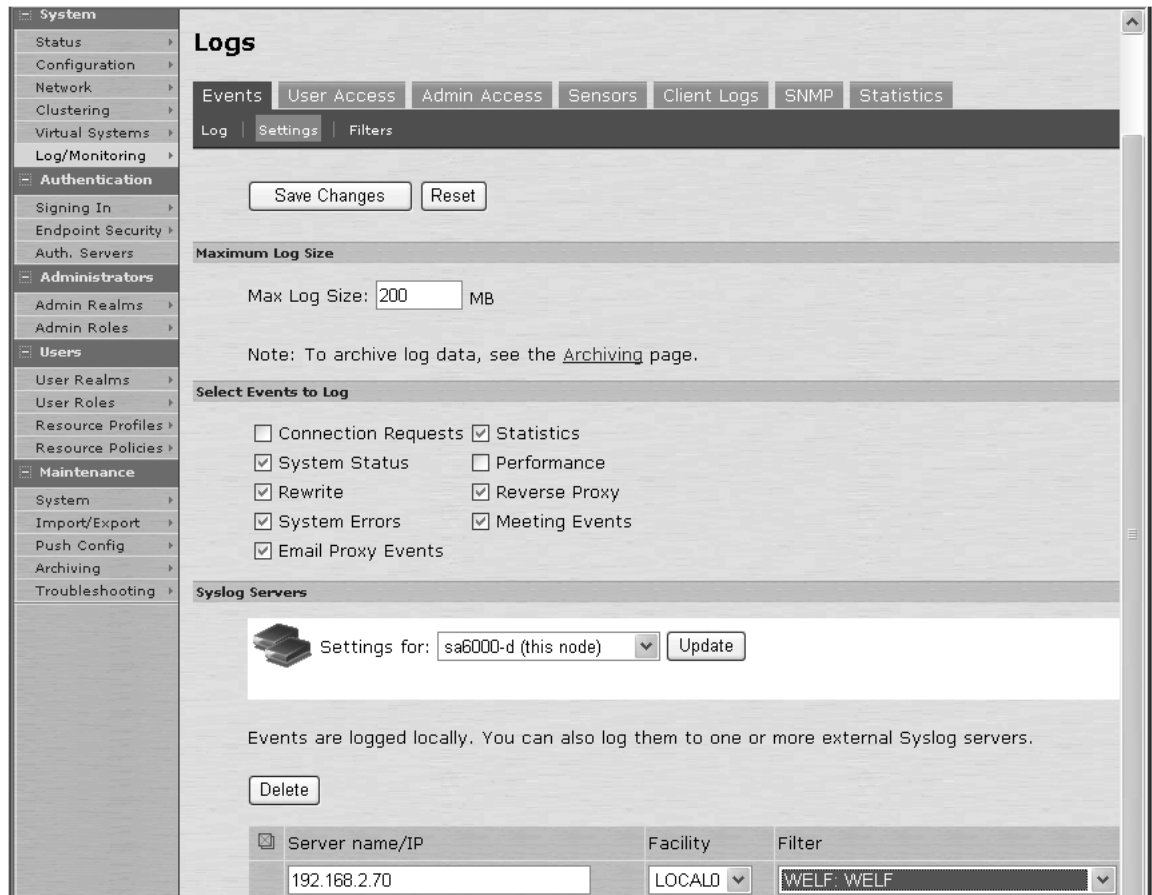


Figure 18: SA Series Devices' Syslog Configuration

5. Sending Flow Records to STRM Series from Junos OS Routers

The Junos OS configuration for J-Flow is as follows:

```

.....
forwarding-options {
  sampling {
    input {
      family inet {
        rate 1;
        run-length 1;
      }
    }
    output {
      cflowd 1.4.39.11 {
        port 9995;
        source-address 1.4.39.1;
        version 5;
      }
    }
  }
}

services {
  flow-monitoring;
}
.....

```

Troubleshooting STRM Series Connection

Similar to Coordinated threat Control, STRM Series connectivity is one of the primary reasons for errors. The following tools: ping, traceroute, tcpdump and packet analyzing are available for troubleshooting connectivity.

```
root@STRM /# tcpdump -s 0 -i <interface> host <dsm_ip> -w <filename>
```

The second critical reason for errors is the variance in ports used by various devices. Most devices use syslog (514/tcp/udp). Naturally the ports and flows between the sensors and flow collectors must be opened by firewalls. Confirm this in the firewall policies.

Summary

To effectively protect today's enterprise, network administrators, IT managers and network security specialists must have insight into the multiple types and levels of evolving threats that impact the integral elements of their networks, including perimeter, critical resources and remote access. Juniper Networks Adaptive Threat Management Solutions are dynamic and high-performance security solutions that adapt to changing risks. By leveraging a cooperative system of tightly integrated security products, these solutions provide network-wide visibility and control that adapts and secures the network against constantly evolving threats. By providing centralized security management and enterprise-wide visibility and control with multi-layered security, these industry-leading security solutions enable network administrators to protect their perimeter, critical resources, and remote access by users and devices to prevent threats from compromising their organization's revenue, reputation and intellectual property.

Remote access protection is a critical part of Juniper Networks Adaptive Threat Management Solutions that enables enterprises to solve major security issues such as securing and authorizing remote access, inspecting malicious traffic and protecting the enterprise from remote attacks. This solution leverages features built into Juniper Networks products such as security zones on firewalls, intrusion prevention and Coordinated Threat Control capabilities of the SA Series appliance and IDP Series, and the centralized security management capabilities of NSM and STRM Series—all working together to provide network-wide protection. The best practices discussed in this paper provide a highly adaptive solution that enables network and security administrators to truly implement a high-performance, comprehensive threat protection solution across the enterprise.

About Juniper Networks

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

Corporate and Sales Headquarters

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

APAC Headquarters

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

EMEA Headquarters

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

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

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