



Security Threat Response Manager

Configuring DSMs

Release_2008.1

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Configuring DSMs
Release 2008.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

31 January 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

CONTENTS

ABOUT THIS GUIDE

1 OVERVIEW

2 3COM 8800 SERIES SWITCH

3 AMBIRON TRUSTWAVE IPANGEL

4 APACHE HTTP SERVER

5 APPLE MAC OS X

6 ARRAY NETWORK SSL VPN

7 F5 NETWORKS BIGIP

8 BLUE COAT SG

9 CHECK POINT FIREWALL-1

10 CHECK POINT PROVIDER-1

11 CISCO ACS

12 CISCO ASA

13 CISCO CATOS FOR CATALYST SWITCHES

14 CISCO CSA

15 CISCO FWSM

16 CISCO IDS/IPS

17 CISCO NAC APPLIANCE

18 CISCO IOS

19 CISCO PIX

20 CISCO VPN 3000 CONCENTRATOR

21 CYBERGUARD FIREWALL/VPN APPLIANCE

22 ENTERASYS DRAGON

23 ENTERASYS MATRIX ROUTER

24 ENTERASYS MATRIX N-SERIES

25 EXTREME NETWORKS EXTREMEWARE

26 FORTINET FORTIGATE

27 UNIVERSAL DSM

28 GENERIC AUTHORIZATION SERVER

29 FORESCOUT COUNTERACT

30 GENERIC FIREWALL

31 IBM AIX 5L

32 ISS PROVENTIA

33 ISS SITEPROTECTOR

-
- 34 JUNIPER NETWORKS DX APPLICATION ACCELERATION PLATFORM**
-
- 35 JUNIPER NETWORKS NETSCREEN IDP**
-
- 36 JUNIPER NETWORKS SECURE ACCESS**
-
- 37 JUNIPER NETWORKS INFRANET CONTROLLER**
-
- 38 JUNIPER NETWORKS NETSCREEN FIREWALL**
-
- 39 JUNIPER NETWORKS NSM**
-
- 40 JUNIPER NETWORKS ROUTER**
-
- 41 JUNIPER NETWORKS STEEL-BELTED RADUIS**
-
- 42 LINUX AUTHORIZATION SERVER**
-
- 43 LINUX DHCP**
-
- 44 LINUX IPTABLES**
-
- 45 MCAFEE INTRUSHIELD**
-
- 46 MCAFEE EPOLICY ORCHESTRATOR**
-
- 47 METAINFO METAIP**
-
- 48 MICROSOFT IIS**
-
- 49 MICROSOFT DHCP SERVER**
-
- 50 MICROSOFT EXCHANGE SERVER**
-
- 51 MICROSOFT WINDOWS SECURITY EVENT LOG**
-
- 52 MICROSOFT IAS SERVER**

53 MICROSOFT IIS SERVER

54 MICROSOFT SQL SERVER

55 NIKSUN

56 NOKIA FIREWALL

57 NORTEL ARN

58 NORTEL APPLICATION SWITCH

59 NORTEL CONTIVITY 5000

60 NORTEL CONTIVITY FIREWALL/VPN

61 NORTEL SWITCHED FIREWALL 5100

62 NORTEL SWITCHED FIREWALL 6000

63 NORTEL VPN GATEWAY

64 OPEN SOURCE SNORT

65 ORACLE AUDIT RECORDS

66 PROFTPD

67 SECURE COMPUTING SIDEWINDER

68 SUN SOLARIS

69 SUN SOLARIS DHCP

70 SONICWALL

71 SUN SOLARIS SENDMAIL

72 SOURCEFIRE INTRUSION SENSOR

73 SQUID WEB PROXY

74 SYMANTEC SGS

75 TIPPING POINT UNITYONE

76 TIPPINGPOINT X505/X506 DEVICE

77 TOPLAYER

78 TREND MICRO INTERSCAN VIRUSWALL

79 TRIPWIRE

80 SYMANTEC SYSTEM CENTER

81 VERICEPT CONTENT 360 DSM

ABOUT THIS GUIDE

This preface provides the following guidelines for using the *Configuring DSMs: Guide*

- [Documentation Feedback](#)
- [Requesting Support](#)

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Support

Open a support case using the Case Management link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

1

OVERVIEW

You can configure STRM to log and correlate events received from external sources such as security equipment (for example, firewalls), and network equipment (for example, switches and routers). Device Support Modules (DSMs) allows you to integrate STRM or STRM SLIM with these external devices.

You can configure the Event Collector to collect security events from various types of security devices in your network. The Event Collector gathers events from local and remote devices. The Event Collector then normalizes and bundles the events and sends the events to the Event Processor.

All events are correlated and security and policy offenses are created based on correlation rules. These offenses are displayed in the Offense Manager. For more information on the Offense Manager interface, see the *STRM Users Guide*.



Note: Before you configure STRM to collect security information from devices, you must set-up your deployment, including off-site sources or targets, using the deployment editor. For more information on the deployment editor, see the *STRM Administration Guide*.

To configure STRM to receive events from devices, you must:

- Step 1** Configure the device to send events to STRM.
- Step 2** Configure STRM to receive events from specific devices. For more information, see the *Managing Sensor Devices Guide*.

2

3COM 8800 SERIES SWITCH

A STRM 3Com 8800 Series Switch DSM accepts events using syslog. STRM records all relevant status and network condition events. Before configuring a 3Com 8800 Series Switch device in STRM, you must configure your device to send syslog events to STRM.

To configure the device to send syslog events to STRM:

Step 1 Log in to the 3Com 8800 Series Switch interface.

Step 2 Enable the information center.

```
info-center enable
```

Step 3 Configure the host with the IP address of your STRM system as the loghost, the severity level threshold value as informational, and the output language to English.

```
info-center loghost <ip_address> facility <severity> language  
english
```

Where:

<ip_address> is the IP address of your STRM system.

<severity> is the facility severity.

Step 4 Configure the ARP and IP information modules to log.

```
info-center source arp channel loghost log level informational  
info-center source ip channel loghost log level informational
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a 3Com 8800 Series Switch, you must select the **3Com 8800 Series Switch** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

3

AMBIRON TRUSTWAVE ipANGEL

A STRM Ambiron TrustWave ipAngel DSM accepts events using syslog. STRM records all Snort-based events from the ipAngel console.

Before you configure STRM to integrate with ipAngel, you must forward your cache and access logs to your STRM system. For information on forwarding device logs to STRM, see your vendor documentation.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a ipAngle device, select **Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

4

APACHE HTTP SERVER

A STRM Apache HTTP Server DSM accepts Apache events using syslog. You can integrate Apache versions 1.3 and above with STRM. STRM records all relevant HTTP status events.



Note: *The procedure in this section applies to Apache DSMs operating on a Unix/Linux platforms only.*

Before you configure STRM to integrate with Apache, you must:

Step 1 Open the Apache configuration file.

Step 2 Add the following below the log format definitions:

```
LogFormat "%h %A %l %u %t \"%r\" %>s %p %b" qradar
```

Step 3 Add the following line below the LogFormat entry to write to syslog:

```
CustomLog "|/usr/bin/logger -t httpd -p <facility>.<priority>" qradar
```

Where:

<facility> is a syslog facility, for example, local0.

<priority> is a syslog priority, for example, info or notice.

For example:

```
CustomLog "|/usr/bin/logger -t httpd -p local1.info" qradar
```



Note: *Verify that the hostname lookups is disabled. To verify, enter `HostnameLookups off`*

Step 4 Open the `syslog.conf` file.

Step 5 Add the following line:

```
<facility>.<priority> <TAB><TAB>@<host>
```

Where:

<facility> is the syslog facility, for example, local0. This value must match the value entered in Step 3.

<priority> is the syslog priority, for example, info or notice. This value must match the value entered in Step 3.

<TAB> indicates you must press the TAB key.

<host> indicates the STRM managed host.

Step 6 Restart syslog:

```
/etc/init.d/syslog restart
```

Step 7 Restart Apache.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Apache device, you must select the **Open Source Apache Webserver** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information on Apache, see <http://www.apache.org/>.

5

APPLE MAC OS X

A STRM Apple Mac OS X DSM accepts events using syslog. STRM records all relevant firewall, web server access, web server error, privilege escalation, and informational events.

Before you configure STRM to integrate with Mac OS X, you must:

Step 1 Log in as a root user.

Step 2 Open the `/etc/syslog.conf` file.

Step 3 Add the following line to the top of the file. Make sure all other lines remain intact:

```
*.*@<IP address>
```

Where `<IP address>` is the IP address of the STRM system.

Step 4 Save and exit the file.

Step 5 Send a hang-up signal to the syslog daemon to make sure all changes are enforced:

```
sudo killall - HUP syslogd
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Mac OS X server, you must select the **Mac OS X** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

See your Mac OS X documentation for more information.

6

ARRAY NETWORK SSL VPN

The STRM Array Networks SSL VPN DSM collects events from an ArrayVPN appliance using syslog. For details of configuring ArrayVPN appliances for remote syslog, please consult Array Networks documentation.

Once you configure syslog to forward events to STRM, you are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Array Networks SSL VPN device, select **Array Networks SSL VPN Access Gateway** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

7

F5 NETWORKS BIGIP

The STRM F5 Networks BigIP DSM collects events from a BigIP load balancer using syslog. For details on configuring remote syslog with the BigIP switch, please consult the vendor documentation.

Once you configure syslog to forward events to STRM, you are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a F5 Network BigIP device, you must select the **F5 Networks BigIP** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

8

BLUE COAT SG

A STRM Blue Coat SG DSM accepts syslog events from a Blue Coat SG Appliance. STRM records all relevant and available information from the event. Before configuring a Blue Coat SG device in STRM, you must configure your device to send syslog to STRM.

For more information regarding your Blue Coat SG Appliance, see your vendor documentation.

To configure your Blue Coat SG device to send syslog to STRM:

- Step 1** Using a web browser, log in to the Blue Coat Management Console.
- Step 2** From the menu, select **Access Logging > General > Default > Default Logging**.
- Step 3** Make sure the **Enable Access Logging** check box is selected.
- Step 4** Select the Protocol you wish to use for logging to STRM. Click **Edit**.
- Step 5** From the Default Logging Policy option, select **Streaming**, which is used for streaming protocols.
- Step 6** Click **Apply**.
- Step 7** From the menu, select **Access Logging > Formats > Streaming**.
- Step 8** Click **Edit**.
- Step 9** Make sure that the W3C Extended File Format (ELFF) string is enabled with the default:

```
c-ip date time c-dns cs-uri-scheme cs-host cs-uri-port
cs-uri-path cs-uri-query c-starttime x-duration c-rate c-status
c-playerid c-playerversion c-playerlanguage cs(User-Agent)
cs(Referer) c-hostexe c-hostexever c-os c-osversion c-cpu
filelength filesize avgbandwidth protocol transport audiocodec
videocodec channelURL sc-bytes c-bytes s-pkts-sent
c-pkts-received c-pkts-lost-client c-pkts-lost-net
c-pkts-lost-cont-net c-resendreqs c-pkts-recovered-ECC
c-pkts-recovered-resent c-buffercount c-totalbuffertime
c-quality s-ip s-dns s-totalclients s-cpu-util x-cache-user
x-cache-info x-client-address
```
- Step 10** Make sure the Multiple-valued header policy option is set to **Log last header**. Click **Ok**.

Step 11 Click **Apply**.

Step 12 Configure the log format:

- a From the menu, select **Access Logging > Logs**.
- b Click the **General Settings** tab.
- c Using the Log: drop-down list box, select **streaming**.
- d Verify the Log Format is set to **squid**.

Step 13 Configure the host you wish to send logs:

- a From the menu, select Access **Logging > Logs**.
- b Click the **Upload Client** tab.
- c Using the Log: drop-down list box, select **streaming**.
- d From the Client type drop-down list box, select **Custom Client**.
- e Click **Settings**.
- f For the host to which you wish to send logs to STRM, configure the host and port. The STRM default for syslog is 514.
- g Click **Ok**.
- h In the Save the log file parameter, make sure the **text file** option is selected.

Step 14 Configure the appropriate access:

- a From the menu, select Access **Logging > Logs**.
- b Click the **Upload Schedule** tab.
- c Using the Log: drop-down list box, select **streaming**.
- d In the Upload the access log parameter, make sure the **continuously** option is selected.
- e Click **Apply**.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Blue Coat SG device, you must select the **Blue Coat SG Appliance** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

9

CHECK POINT FIREWALL-1

You can configure STRM to integrate with a Check Point FireWall-1 device using one of the following methods:

- [Integrating Check Point FireWall-1 Using Syslog](#)
- [Integrating CheckPoint FireWall-1 Using OPSEC](#)



Note: Depending on your Operating System, the procedures for the Check Point FireWall-1 device may vary. The following procedures are based on the Check Point SecurePlatform Operating system.

Integrating Check Point FireWall-1 Using Syslog

This section describes how to ensure that the STRM Check Point FireWall-1 DSMs accepts FireWall-1 events using syslog.



Note: If Check Point SmartCenter is installed on Microsoft Windows, you must use the [Integrating CheckPoint FireWall-1 Using OPSEC](#) method.

Before you configure STRM to integrate with a Check Point FireWall-1 device:

Step 1 Enter the following command to access the Check Point console as an expert user:

```
expert
```

A password prompt appears.

Step 2 Enter your expert console password. Press **Enter**.

Step 3 Open the following file:

```
/etc/rc.d/rc3.d/S99local
```

Step 4 Add the following lines:

```
$FWDIR/bin/fw log -ftn | /usr/bin/logger -p  
<facility>.<priority> > /dev/null 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, `local3`.

<priority> is a Syslog priority, for example, `info`.

For example:

```
$FWDIR/bin/fw log -ftn | /usr/bin/logger -p local3.info >
/dev/null 2>&1 &
```

Step 5 Save and close the file.

Step 6 Open the syslog.conf file.

Step 7 Add the following line:

```
<facility>.<priority> <TAB><TAB>@<host>
```

Where:

<facility> is the syslog facility, for example, `local3`. This value must match the value entered in [Step 4](#).

<priority> is the syslog priority, for example, `info` or `notice`. This value must match the value entered in [Step 4](#).

<TAB> indicates you must press the TAB key.

<host> indicates the STRM managed host.

Step 8 Save and close the file.

Step 9 Depending on your operating system, enter the following command to restart syslog:

In Linux: `service syslog restart`

In Solaris: `/etc/init.d/syslog start`

Step 10 Enter the following command:

```
nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p
<facility>.<priority> > /dev/null 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, `local3`. This value must match the value entered in [Step 4](#).

<priority> is a Syslog priority, for example, `info`. This value must match the value entered in [Step 4](#).

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Check Point Firewall-1 device using syslog, choose one of the following options:

- If you are using STRM 6.0, select **CheckPoint Firewall-1 Devices via Syslog** from the Sensor Device Type drop-down list box.
- If you are using STRM 6.0.1 and above, select **CheckPoint Firewall-1** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding Check Point FireWall-1, see the Check Point FireWall-1 documentation.

Integrating CheckPoint FireWall-1 Using OPSEC



This section describes how to ensure that the STRM Check Point FireWall-1 DSM accepts FireWall-1 events using Open Platform for Security (OPSEC).

Note: The method used for integrating Check Point Firewall-1 into STRM using OPSEC is dependent on the version of STRM you are running.

This section includes the following information:

- [Enabling CheckPoint Firewall-1 and STRM](#)
- [Reconfiguring CheckPoint FireWall-1 SmartCenter](#)

Enabling CheckPoint Firewall-1 and STRM

This section describes how to enable CheckPoint Firewall to integrate with STRM.

To enable Check Point FireWall-1 and STRM integration:

- Step 1** Reconfigure Check Point FireWall-1 SmartCenter. See [Reconfiguring CheckPoint FireWall-1 SmartCenter](#).
- Step 2** Verify and change, if necessary, the OPSEC communication configuration.
- Step 3** In the STRM interface, configure the OPSEC LEA protocol.

To configure STRM to receive events from a Check Point device using OPSEC LEA, you must select the **LEA** option from the Protocol drop-down list box when configuring your protocol configuration. For more information, see Configuring Protocols in *Managing Sensor Devices*.

- Step 4** Configure the sensor device within the STRM interface.

To configure STRM to receive events from an Check Point Firewall-1 device using OPSEC, you must select **CheckPoint Firewall-1** from the Sensor Device Type drop-down list box and **LEA::<protocol_name>** from the Protocol Configuration drop-down list box.

For more information on configuring sensor devices, see *Managing Sensor Devices Guide*.

Reconfiguring CheckPoint FireWall-1 SmartCenter

This section describes how to reconfigure the Check Point FireWall-1 SmartCenter. In the Check Point FireWall-1 SmartCenter, create a host object representing the STRM system. The leapipe is the connection between the Check Point FireWall-1 and STRM.

To reconfigure the Check Point FireWall-1 SmartCenter:

- Step 1** Create a host object:
 - a Open the Check Point SmartDashboard GUI
 - b Select **Manage > Network Objects > New > Node > Host**.
 - c Enter in the appropriate information in the Name, IP Address, and Comment (optional) text fields for your host.
 - d Click **OK**.

e Select **Close**.

Step 2 To create the OPSEC connection:

a Select **Manage > Servers and OPSEC applications > New > OPSEC Application Properties**.

b Enter the appropriate information in the Name and Comment (optional) text fields.



Note: *The name you enter must be different than the name entered in Step 1 c.*

c From the Host drop-down list box, select the host object you created in [Step 1](#).

d From Application Properties drop-down list box, select **User Defined** as the vendor.

e From Client Entries drop-down list box, select **LEA**.

f Click **Communication** to generate a Secure Internal Communication (SIC) certificate.

g Enter an activation key.

h Click **OK**.

i Click **Close**.

Step 3 Select **Policy > Install > OK** to install the Security Policy on your firewall.

Verifying or Changing the OPSEC Communications Configuration

This section describes how to modify your Check Point FireWall-1 configuration to allow OPSEC communications on non-standard ports, and in a clear text, un-authenticated stream.

This section includes the following information:

- [Changing the Default Port on which OPSEC LEA Communicates](#)
- [Configuring OPSEC LEA for Un-Encrypted Communications](#)

Changing the Default Port on which OPSEC LEA Communicates

To change the default port on which OPSEC LEA communicates (that is, port 18184):

Step 1 At the command-line prompt of your Check Point SmartCenter Server, enter the following command to stop the firewall services:

```
cpstop
```

Step 2 Depending on your Check Point SmartCenter Server's operating system, open the following file:

In Linux: `$FWDIR/conf/fwopsec.conf`

In Windows: `%FWDIR%\conf/fwopsec.conf`

The default contents of this file are as follows:

```
# The VPN-1/FireWall-1 default settings are:
#
# sam_server  auth_port  0
# sam_server      port    18183
#
# lea_server  auth_port  18184
# lea_server      port    0
#
# ela_server  auth_port  18187
# ela_server      port    0
#
# cpmi_server auth_port  18190
#
# uaa_server  auth_port  19191
# uaa_server      port    0
#
```

Step 3 Change the default lea_server auth_port from 18184 to another port number.

Step 4 Remove the hash (#) mark from that line.

For example:

```
lea_server  auth_port  18888
# lea_server      port    0
```

Step 5 Save and close the file.

Step 6 Start the firewall services by entering the following command:

```
cpstart
```

Configuring OPSEC LEA for Un-Encrypted Communications

To configure the OPSEC LEA protocol for un-encrypted communications:

Step 1 At the command-line prompt of your Check Point SmartCenter Server, stop the firewall services by entering the following command:

```
cpstop
```

Step 2 Depending on your Check Point SmartCenter Server's operating system, open the following file:

In Linux: **\$FWDIR\conf\fwopsec.conf**

In Windows: **%FWDIR%\conf\fwopsec.conf**

Step 3 Change the default lea_server auth_port from 18184 to 0.

Step 4 Change the default lea_server port from 0 to 18184.

Step 5 Remove the hash (#) marks from both lines.

For example:

```
lea_server  auth_port  0
lea_server      port    18184
```

Step 6 Save and close the file.

Step 7 Start the firewall services by entering the following command:

```
cpstart
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Check Point Firewall-1 device using OPSEC, select CheckPoint Firewall-1 from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see *Managing Sensor Devices Guide*.

For more information on configuring your Check Point Firewall-1, see your vendor documentation.

10

CHECK POINT PROVIDER-1

You can configure STRM to integrate with a Check Point Provider-1 device using one of the following methods:

- [Integrating Check Point Provider-1 Using Syslog](#)
- [Integrating Check Point Provider-1 Using OPSEC](#)



Note: Depending on your Operating System, the procedures for the Check Point Provider-1 device may vary. The following procedures are based on the Check Point SecurePlatform Operating system.

Integrating Check Point Provider-1 Using Syslog

This method ensures the STRM Check Point Provider-1 DSM accepts Check Point Provider-1 events using syslog. STRM records all relevant Check Point Provider-1 events.

Before you configure STRM to integrate with a Check Point Provider-1 device, you must:

Step 1 Enter the following command to access the console as an expert user:

```
expert
```

A password prompt appears.

Step 2 Enter your expert console password. Press **Enter**.

Step 3 Enter the following command:

```
csh
```

Step 4 Select the desired customer logs:

```
mdsensv <customer name>
```

Step 5 Enter the following command:

```
# nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p  
<facility>.<priority> 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, local3.

<priority> is a Syslog priority, for example, info.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Check Point Provider-1 device using syslog, select **CheckPoint Firewall-1** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding Check Point Provider-1, see the Check Point Provider-1 documentation.

Integrating Check Point Provider-1 Using OPSEC

This method ensures the STRM Check Point Provider-1 DSM accepts Check Point Provider-1 events using OPSEC.

To enable Check Point Provider-1 integration, you must:

Step 1 Reconfigure Check Point Provider-1 SmartCenter. See [Reconfiguring Check Point Provider-1 SmartCenter](#).

Step 2 Configure the OPSEC LEA protocol in the STRM interface.

To configure STRM to receive event from a Check Point device using OPSEC LEA, you must select the **LEA** option from the Protocol drop-down list box when configuring your protocol configuration. For more information, see *Configuring Protocols* in the *Managing Sensor Devices Guide*.

Step 3 Configure the sensor device within the STRM interface.

To configure STRM to receive events from an Check Point Provider-1 device using OPSEC, you must select the **CheckPoint Firewall-1 Devices via Syslog** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information, see your vendor documentation.

Reconfiguring Check Point Provider-1 SmartCenter

This section describes how to reconfigure the Check Point Provider-1 SmartCenter. In the Check Point Provider-1 Management Domain GUI (MDG), create a host object representing the STRM system. The leapipe is the connection between the Check Point Provider-1 and STRM.

To reconfigure the Check Point Provider-1 SmartCenter (MDG):

Step 1 To create a host object, open the Check Point SmartDashboard GUI and select **Manage > Network Objects > New > Node > Host**.

Step 2 Enter in the Name, IP Address, and optional Comment for your host.

Step 3 Click **OK**.

Step 4 Select **Close**.

Step 5 To create the OPSEC connection, select **Manage > Servers and OPSEC Applications New > OPSEC Application Properties**.

Step 6 Enter the Name and optional Comment.



Note: The name you enter must be different than the name entered in [Step 2](#).

- Step 7** From the Host drop-down menu, select the STRM host object that you just created.
- Step 8** From Application Properties, select **User Defined** as the Vendor type.
- Step 9** From Client Entries, select **LEA**.
- Step 10** Configure the Secure Internal Communication (SIC) certificate, click **Communication** and enter an activation key.
- Step 11** Select **OK** and then **Close**.
- Step 12** To install the Policy on your firewall, select **Policy > Install > OK**.

11

CISCO ACS

A STRM Cisco Access Control Server (ACS) DSM accepts syslog ACS events using one of the following options:

- A server using the STRM Adaptive Log Exporter (Cisco ACS software version 3.x or later). For more information on the Adaptive Log Exporter, see the *STRM Adaptive Log Exporter Users Guide*.
- Syslog directly from the Cisco ACS device (Cisco ACS software version 4.1 and later).

STRM records all relevant and available information from the event. Before configuring an ACS device in STRM, you must:

Step 1 Configure your device to send syslog to STRM using one of the following options:

- a Configure your Cisco ACS device to directory send syslog to STRM.
- b Using the STRM Adaptive Log Exporter, configure the Cisco ACS device and associated destination. When configuring your Cisco ACS device, you must also configure the **Root Log Directory** parameter, which is the location Cisco ACS stores the logs files. For more information regarding configuring your Cisco ACS device, see the *STRM Adaptive Log Exporter Users Guide*.

Step 2 Configure the sensor device within the STRM interface.

To configure STRM to receive events from a Cisco ACS device, you must select the **Cisco ACS** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding Cisco ACS, see your vendor documentation.

12

CISCO ASA

You can integrate a Cisco Adaptive Security Appliance (ASA) with STRM. A Cisco ASA DSM accepts events using syslog. STRM records all relevant events.

Before you configure STRM to integrate with a CSA server, you must forward all device logs to your STRM system. For more information on forwarding logs to STRM, see your vendor documentation.

To configure STRM to receive events from a Cisco ASA device, select **Cisco Adaptive Security Appliance (ASA)** from the Select sensor device type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

13

CISCO CATOS FOR CATALYST SWITCHES

A STRM Cisco CatOS for Catalyst Switches DSM accepts events using syslog. STRM records all relevant device events. Before configuring a Cisco CatOS device in STRM, you must configure your device to send syslog events to STRM.

To configure the device to send syslog events to STRM:

Step 1 Log in to the Cisco CatOS interface and enter privileged EXEC mode.

Step 2 Configure the system to timestamp messages:

```
set logging timestamp enable
```

Step 3 Specify the IP address of the STRM server:

```
set logging server <IP address>
```

Step 4 Limit messages that are logged by selecting a severity level:

```
set logging server severity <server severity level>
```

Step 5 Specify the facility level that should be used in the message. The default is **local7**.

```
set logging server facility <server facility parameter>
```

Step 6 Enable the switch to send syslog messages to the STRM server.

```
set logging server enable
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Cisco CatOS device, you must select the **Cisco CatOS for Catalyst Switches** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

14

CISCO CSA

You can integrate a Cisco Security Agent (CSA) server with STRM. A CSA DSM accepts events using SNMP. You can integrate CSA versions 4.x and 5.x with STRM. STRM records all relevant events.

Before you configure STRM to integrate with a CSA server, you must:

- Step 1** Open the CSA interface and select **Security Agents**.
- Step 2** Click the **Monitor** tab.
- Step 3** Click **Alerts**.
- Step 4** From the bottom of the window, select **New**.
- Step 5** Enter a name in the Name field and optional description in the description field.
- Step 6** Select the **SNMP** check box.
- Step 7** Enter a Community name (configured on STRM).
- Step 8** Enter the Manager IP address (STRM deployment).
- Step 9** From the drop-down list box, select the events on which you wish to alert.
- Step 10** Click **Save**.

You are now ready to configure the sensor device and SNMP within the STRM interface. For information on configuring SNMP in the STRM interface, see the *Managing Sensor Devices Guide*. To configure STRM to receive events from a Cisco CSA device, select **Cisco Security Agent (CSA)** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

15

CISCO FWSM

You can integrate Cisco Firewall Service Module (FWSM) version 2.2 with STRM. A STRM FWSM DSM accepts FWSM events using syslog. STRM records all relevant Cisco FWSM events.

Before you configure STRM to integrate with Cisco FWSM, you must configure Cisco FWSM to forward logs to STRM:

Step 1 Using a Console connection, telnet, or SSH, log in to the Cisco FWSM.

Step 2 Enable logging:

```
logging on
```

Step 3 Change the logging level:

```
logging trap level (1-7)
```

By default, the logging level is set to 3 (error).

Step 4 Designate STRM as a host to receive the messages:

```
logging host [interface] ip_address [tcp[/port] | udp[/port]]  
[format emblem]
```

For example:

```
logging host dmz1 192.168.1.5
```

Where 192.168.1.5 is the IP address of your STRM system.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Cisco IDS device, select **Cisco Firewall Services Module (FWSM)** from the Sensor Device drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding Cisco FWSM devices, see your Cisco documentation.

16

CISCO IDS/IPS

You can integrate a Cisco IDS/IPS server version 5.x and 6.x with STRM. A Cisco IDS/IPS DSM polls the Cisco IDS/IPS events using the Security Device Event Exchange (SDEE) protocol. SDEE specifies the message format and the protocol used to communicate the events generated by security devices. STRM only supports direct SDEE connections to the device and not the management software, which controls the device.



Note: *You must have security access or web authentication on the device before connecting to STRM.*

You are now ready to configure the SDEE protocol within the STRM interface. For more information, see the *Managing Sensor Devices Guide*. To configure STRM to receive events from a Cisco IDS/IPS device, select **Cisco Intrusion Prevention System (IPS)** from the Sensor Device Type drop-down list box.

For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your Cisco IDS/IPS, see your vendor documentation.

17

CISCO NAC APPLIANCE

A STRM Cisco NAC Appliance DSM accepts events using syslog. STRM records all relevant audit, error, and failure events as well as quarantine and infected system events. Before configuring a Cisco NAC Appliance device in STRM, you must configure your device to send syslog events to STRM.

To configure the device to send syslog events to STRM:

- Step 5** Log in to the Cisco NAC Appliance interface.
- Step 6** In the Monitoring section, select **Event Logs**.
- Step 7** Click the **Syslog Settings** tab.
- Step 8** In the **Syslog Server Address** field, enter the IP address of your STRM system.
- Step 9** In the **Syslog Server Port** field, enter the syslog port. The default is 512.
- Step 10** In the **System Health Log Interval** field, enter the frequency, in minutes, for system statistic log events.
- Step 11** Click **Update**.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Cisco NAC Appliance, you must select the **Cisco NAC** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

18

CISCO IOS

You can integrate a Cisco IOS 12.2, 12.5 and above with STRM. A Cisco IOS DSM accepts Cisco IOS events using syslog. STRM records all relevant events.



Note: Make sure all Access Control Lists (ACLs) are set to LOG.

Before you configure STRM to integrate with a Cisco IOS server, you must:

Step 1 Log in to the router in privileged-exec mode and switch to configuration mode.

```
conf t
```

Step 2 Enter the following series of commands:

```
logging <ip address>
```

```
logging source-interface <interface>
```

Where:

<ip address> is the IP address hosting STRM and the SIM components.

<interface> is the name of the interface, for example, dmz, lan, ethernet0, or ethernet1.

Step 3 Enter the following commands to configure the priority level:

```
logging trap warning
```

```
logging console warning
```

Where **warning** is the priority setting for the logs.

Step 4 Configure the syslog facility:

```
logging facility syslog
```

Step 5 Save and exit the file.

Step 6 Copy running-config to startup-config:

```
copy running-config startup-config
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Cisco IOS device, you must select one of the following options from the Sensor Device Type drop-down list box (depending on your system): **Cisco IOS, Cisco 12000 Series, Cisco 6500 Series Router, Cisco 7600 Series Router, Cisco Carrier Routing Router, or Cisco Integrated**

Services Router. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding your Cisco IOS, see your Cisco IOS documentation.

19

CISCO PIX

You can integrate Cisco Pix versions 5.x and 6.3 with STRM. A Cisco Pix DSM accepts Cisco Pix events using syslog. STRM records all relevant Cisco Pix events.

Before you configure STRM to integrate with Cisco Pix, you must configure Cisco Pix to forward logs to STRM using the following command:

```
logging host <interface> <ip address>
```

Where:

<interface> is the name of the interface, for example, dmz, lan, ethernet0, or ethernet1.

<ip address> is the IP address hosting STRM and the SIM components.

To integrate Cisco Pix:

Step 1 Log into the Cisco PIX using a console connection, telnet, or SSH.

Step 2 Enter Privileged mode:

```
enable
```

Step 3 Enter Configuration mode:

```
conf t
```

Step 4 Enable logging and timestamp the logs:

```
logging on
```

```
logging timestamp
```

Step 5 Set the log level:

```
logging trap warning
```

Step 6 Configure logging to STRM:

```
logging host <interface> <ip address>
```

Where:

<interface> is the name of the interface, for example, dmz, lan, ethernet0, or ethernet1.

<ip address> is the IP address hosting STRM and the SIM components.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Cisco PIX device, you must select the **Cisco PIX Firewall** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding Cisco Pix devices, see your Cisco documentation.

20

CISCO VPN 3000 CONCENTRATOR

A STRM Cisco VPN 3000 Concentrator DSM accepts Cisco VPN Concentrator events using syslog. You can integrate Original VPN 3000 Concentrator versions VPN 3005 and L.1.7.H with STRM. STRM records all relevant events. Before you configure STRM to integrate with a Cisco VPN concentrator, you must:

Step 1 Log in to the Cisco VPN 3000 Concentrator interface.

Step 2 Enter the following command to add a syslog server to your configuration:

```
set logging server <IP address>
```

Where <IP address> is the IP address of the Event Collector.

Step 3 Enable system message logging to the configured syslog servers:

```
set logging server enable
```

Step 4 Set the facility and severity level for syslog server messages:

```
set logging server facility server_facility_parameter
```

```
set logging server severity server_severity_level
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Cisco VPN Concentrator device, select **Cisco VPN 3000 Series Concentrator** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your Cisco VPN Concentrator, see your vendor documentation.

21

CYBERGUARD FIREWALL/VPN APPLIANCE

A STRM CyberGuard Firewall VPN Appliance DSM accepts CyberGuard events using syslog. STRM records all relevant CyberGuard events. STRM supports the CyberGuard KS series of appliances.

Before you configure STRM to integrate with a CyberGuard device, you must:

- Step 1** Log in to the CyberGuard interface.
- Step 2** Select the Advanced page.
- Step 3** Under the System Log, select **Enable Remote Logging**.
- Step 4** Enter the IP address of the STRM system.
- Step 5** Click **Apply**.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a CyberGuard Firewall VPN device, select **CyberGuard TSP Firewall/VPN** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information on configuring your CyberGuard device, consult your CyberGuard documentation.

22

ENTERASYS DRAGON

You can integrate Enterasys Dragon versions 5.0, 6x, and 7.1 with STRM. A STRM Enterasys Dragon DSM accepts Enterasys Dragon events using syslog and SNMP. STRM records all relevant Enterasys Dragon events.

Before you configure STRM to integrate with Enterasys Dragon, you must:

- Step 1** Log in to the Enterasys Dragon console.
- Step 2** Click the **Alarm Tool** icon.
- Step 3** Configure the Alarm Tool Policy:
 - a In the **Alarm Tool Policy View > Custom Policies** menu tree, use the right mouse button (right-click) and select **Add Alarm Tool Policy**.
The Add Alarm Tool Policy window appears.
 - b In the Add Alarm Tool Policy field, enter the policy name **Q1Labs**. Click **Ok**.
 - c In the menu tree, select the newly created Q1Labs policy.
- Step 4** To configure the Event Group:
 - a Click the **Events Group tab**. Click **New**.
 - b In the Event Group Editor, expand the Event Group Template of All Dragon and move the selected item to the Event Group panel.
The Add Event Group field appears.
 - c Click **Yes**.
The Event Group Editor window appears.
 - d Click **Ok**.
- Step 5** Configure Notification Rules:
 - a Click the **Notification Rules** tab. Click **New**.
 - b In the name field, enter **Q1Labs-Rule**. Click **Ok**.
 - c In the Notification Rules panel, select the newly created **Q1Labs-Rule** item.
 - d Click the **SNMP V3** tab. Click **New**.
The SNMP V3 Editor field appears.
 - e Update values, as necessary:
 - Change the server IP address to that of the Juniper system.

- Do not change the OID.
- **Inform** — Select the check box.
- **Security Name** — Specify the SNMPv3 username.
- **Auth Password** — Specify the appropriate password.
- **Priv Password** — Specify the appropriate password.
- **Message** — Enter the following:

Dragon Event: %DATE%,,%TIME%,,%NAME%,,%SENSOR%,,%PROTO%,,%SIP%,,%DIP%,,%SPORT%,,%DPORT%,,%DIR%,,%DATA%



Note: Verify that the entered security passwords and protocols match data configured in the SNMP configuration.

Step 6 Configure the SNMP options:

- a Click the **Global Options** tab.
- b Click the **SNMP** tab
- c Specify the IP address of the EMS server that you wish to send traps.

Step 7 Configure the alarm information:

- a Click the **Alarms** tab. Click **New**.
- b Enter values for the parameters:
 - **Name** — Enter a name of Juniper-Alarm.
 - **Type** — Select Real Time.
 - **<All-Dragon>** — Select the newly created Event Group.
 - **Notification Rule** — Select the check box for the Juniper-Rule.
- c Click **Ok**.
- d Click **Commit**.

Step 8 Navigate to the Enterprise View.

Step 9 Use the right mouse button (right-click) on Alarm Tool and select **Associate Alarm Tool Policy**.

Step 10 Select the newly created Juniper policy. Click **Ok**.

Step 11 In the Enterprise menu, use the right mouse button (right-click) and select **Deploy**.

You are now ready to configure the sensor device and SNMP within the STRM interface. For information on configuring SNMP in the STRM interface, see the *Managing Sensor Devices Guide*.

To configure STRM to receive events from an Enterasys Dragon device, select **Enterasys Dragon Network IPS** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding Enterasys Dragon, see your Enterasys Dragon documentation.

23

ENTERASYS MATRIX ROUTER

A STRM Enterasys Matrix Router DSM accepts Enterasys Matrix events using SNMP and syslog. You can integrate Enterasys Matrix Router version 3.5 with STRM. STRM records all SNMP events and syslog login, logout, and login failed events. Before you configure STRM to integrate with Enterasys Matrix, you must:

Step 1 Log in to the switch/router as a privileged user.

Step 2 Enter the following command:

```
set logging server <server number> description <description>
facility <facility> ip_addr <ip address> port <port> severity
<severity>
```

Where:

<server number> is the server number 1 to 8.

<description> is a description of the server.

<facility> is a syslog facility, for example, local0.

<ip address> is the IP address of the server you wish to send syslog messages.

<port> is the default UDP port that the client uses to send messages to the server. Use port 514 unless otherwise stated.

<severity> is the server severity level 1 to 9 where 1 indicates an emergency and 8 is debug level.

For example:

```
set logging server 5 description ourlogserver facility local0
ip_addr 1.2.3.4 port 514 severity 8
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Enterasys Matrix device, you must select the **Enterasys Matrix E1 Switch** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information, see your vendor documentation.

24

ENTERASYS MATRIX N-SERIES

A STRM Enterasys Matrix N-Series DSM accepts N-Series events using syslog. STRM records all relevant Matrix N3, N5, N7, and N Standalone device events. Before you configure STRM to integrate with a Matrix N-Series, you must:

Step 1 Log in to the switch/router.

Step 2 Enter the following command:

```
set logging server <index> ip-addr <IP address> facility
<facility> severity <severity> descr <description> port <port>
state <enable | disable>
```

Where:

<index> is the server table index number (1 to 8) for this server.

<ip address> is the IP address of the server you wish to send syslog messages. This is an optional field.

<facility> is a syslog facility. Valid values are `local0` to `local7`. This is an optional field.

<severity> is the server severity level 1 to 8. This is an optional field. Valid values include:

- 1: Emergencies (system is unusable)
- 2: Alerts (immediate action required)
- 3: Critical conditions
- 4: Error conditions
- 5: Warning conditions
- 6: Notifications (significant conditions)
- 7: Informational messages
- 8: Debugging messages

<description> is a description of the server. This is an optional field.

<port> is the default UDP port that the client uses to send messages to the server. Use port 514 unless otherwise stated. This is an optional field.

<enable | disable> enables or disables this facility/server configuration. This is an optional field.

For example, enter the command below if you wish to enable a syslog server configuration for the following:

- Index — 1
- IP address: 134.141.89.113
- Facility: local4
- Severity: Level 3 on port 514

```
set logging server 1 ip-addr 134.141.89.113 facility local4
severity 3 port 514 state enable
```

For more information on configuring the Matrix N-Series, consult your vendor documentation.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Enterasys Matrix N-Series device, select **Enterasys N Series Switch** from the Sensor Device Type drop-down list box.

For information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

25

EXTREME NETWORKS EXTREMEWARE

A STRM ExtremeWare DSM accepts Extreme events using syslog. STRM records all relevant events. Before you configure STRM to integrate with an ExtremeWare device, you must configure syslog within your Extreme device.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from your ExtremeWare device, select **Extreme Networks ExtremeWare Operating System (OS)** from the Sensor Device Type drop-down list box.

For more information on configuring devices, see the *Managing Sensor Devices Guide*. For more information on configuring Extreme, consult your vendor documentation.

26

FORTINET FORTIGATE

A STRM Fortinet FortiGate DSM accepts FortiGate IPS/Firewall events using syslog. STRM records all relevant events. Before you configure STRM to integrate with the device, you must configure syslog within your FortiGate device. For more information on configuring a Fortinet FortiGate device, see your vendor documentation.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from your FortiGate device, select **Fortinet FortiGate Security Gateway** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

27

UNIVERSAL DSM

STRM collects and correlates events from network infrastructure and security devices. Once the events are collected and before the correlation can begin, the individual events from these devices must be properly parsed to determine the event name, IP addresses, protocol, and ports. For common network devices (such as, NetScreen Firewalls) predefined DSMs have been engineered into STRM to properly parse all event messages from the respective devices. Once the events from a device have been parsed by the DSM, STRM can continue to correlate events into offenses.

This chapter includes information on configuring a Universal DSM including:

- [Universal DSM Example](#)
- [Building the Universal DSM XML Configuration File](#)
- [Configuring the Universal DSM within STRM](#)

If an enterprise network has one or more network or security devices that are not officially supported (no specific DSM for the device exists), you can use the Universal DSM. The Universal DSM allows you to forward SNMP, Syslog, or SDEE messages from unsupported devices to STRM for correlation. The Universal DSM is then programmed (using Regular Expressions through an XML definition file) by the administrator to parse and categorize the incoming events providing the exact same functionality as supported DSMs.



Note: *Because the Universal DSM is programmed using Regular Expressions, some additional research may be needed. A basic and functional understanding of Regular Expressions can be found by thoroughly reviewing the following sites: <http://java.sun.com/docs/books/tutorial/extra/regex/> or <http://www.dshield.org/regex.php>*

Additionally, you can use a Regular Expression calculator to verify that a Regular Expression search pattern functions properly against the event string being parsed. A commonly used freeware Windows based Regular Expression calculator can be downloaded from: <http://www.silveragesoftware.com/rxl.html>

Universal DSM Example

This section provides an example of a Universal DSM. This example includes a simple software-based UNIX Firewall. This UNIX firewall creates two critical SYSLOG messages (Firewall Accept and Firewall Deny) suitable for STRM to parse. For example:

```
Firewall Accept example-> Jun 09 16:50:43.813005 rule
669/(match) user="john doe" pass in on em1: 172.16.11.240.1844 >
172.16.53.34.6080: S 2744116838:2744116838(0) win 16384
mss1460,nop,nop,sackOK> 00:01:23:45:67:89 > 01:22:33:44:55:66
```

```
Firewall Deny example -> Mar 26 22:06:16.057139 rule 0/0(match):
block in on r10: 172.16.165.146.53 > 172.16.169.126.1026: 1024
update
```

The Universal DSM supports the parsing of Event Name, Source IP Address, Destination IP Address, Source Port, Destination Port, and Protocol from within event messages. When building a Universal DSM, the first goal is to analyze the available event messages and isolate which of the data fields are actually contained within the messages. In this UNIX Firewall example, the SYSLOG messages contain data for all of the fields except for Protocol as displayed in the table below:

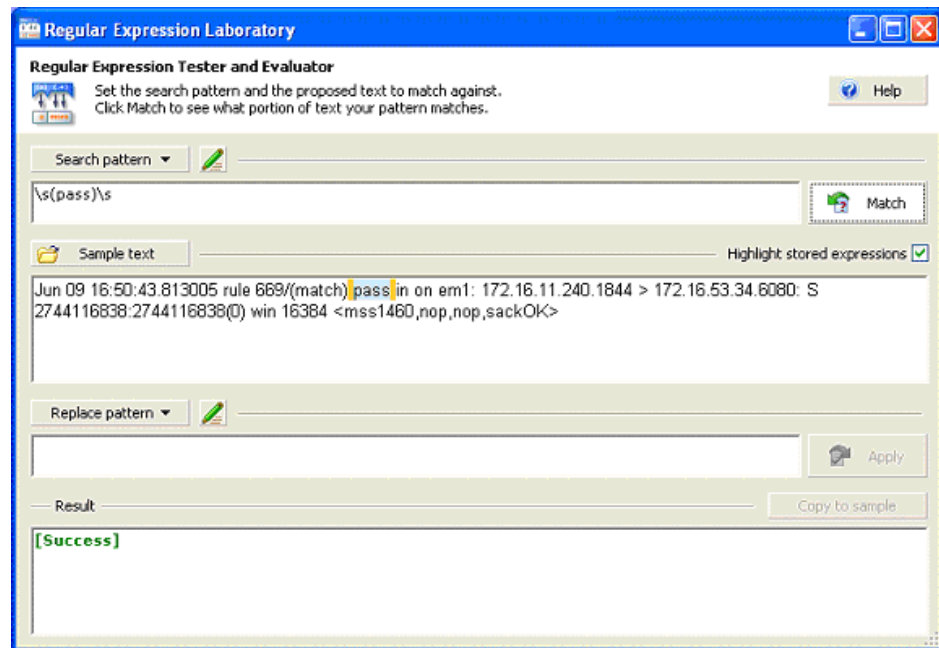
Table 27-1 Example of Messages

	Firewall Accept Record	Firewall Deny Record
Event Name	pass	Block
Source IP Address	172.16.11.240	172.16.165.146
Destination IP Address	172.16.53.34	172.16.169.126
Source Port	1844	53
Destination Port	6080	1026
Protocol	(not available)	(not available)
User Name	John Doe	(not available)
Mac Address	00:01:23:45:67:89	(not available)

Once the available data fields have been visually isolated, build individual Regular Expressions capable of searching and parsing the specific event messages to extract the necessary data field information. You can now use the Regular Expression Calculator to build these individual expressions.

To build individual expressions:

- Step 1** Open the Regular Expressions Calculator.
- Step 2** Paste the example of the Firewall Accept SYSLOG message into the Regular Expression Calculator's string or **Sample text** field.



- Step 3** Once the string field has been populated, create a regular expression search pattern for the event name field, which in this example is the text string **pass**. By using the knowledge from the Regular Expression tutorials, you can create the search pattern in an attempt to isolate the **pass** string.

```
\s(pass)\s
```



Note: The `\s` in the Regular Expression language detects white space while the parentheses controls the exact data being returned in the search.

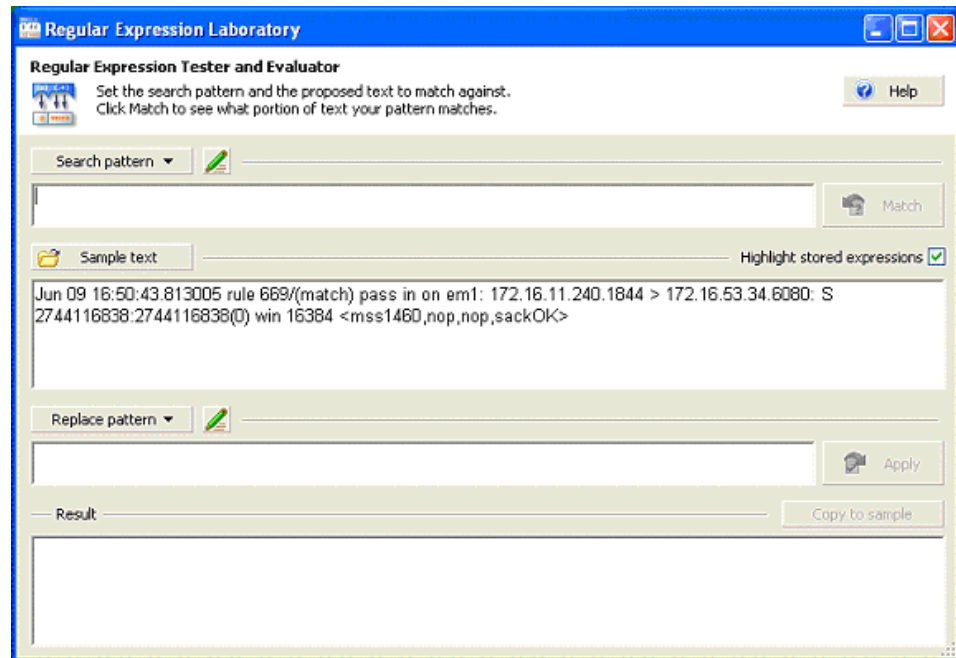
- Step 4** Copy this proposed search pattern for the event name into the Search Pattern field of the Regular Expression calculator.

- Step 5** Click **Match**.

The Regular Expression calculator begins to process the search pattern against the sample text. If the search pattern is successful, the text is highlighted and the result field includes the term Success, as shown below.



Note: The orange highlights mark the white space while the blue highlights contain the exact data to be returned from inside the parentheses.



Each of the Regular Expressions used parse the event message must now be verified within the Regular Expression calculator to verify that it will perform properly when used within STRM.

The table below details the Regular Expression to successfully search and parse the event message for the UNIX Firewall used in this example.

Table 27-2 Regular Expressions

	Firewall Accept Record	Firewall Deny Record	Regular Expressions
Event Name	Pass	Block	<code>\s(pass)\s & \s(block)\s</code>
Source IP Address	172.16.11.240	172.16.165.146	<code>\s(\d+\.\d+\.\d+\.\d+)\.</code>
Destination IP Address	172.16.11.240	172.16.169.126	<code>\>\s(\d+\.\d+\.\d+\.\d+)\.</code>
Source Port	1844	53	<code>\.(\d+)\s>\s</code>
Destination Port	6080	1026	<code>\.(\d+)\:\s</code>
Protocol	(not available)	(not available)	
User Name	John Doe	(not available)	<code>user=\("[^"]+")\"</code>
Mac Address	00:01:23:45:67:89	(not available)	<code>[0-9a-f][0-9a-f]:-[0-9a-f][0-9a-f]:-[0-9a-f][0-9a-f]:-[0-9a-f][0-9a-f]:-[0-9a-f][0-9a-f]</code>

In the above Universal DSM definition, the standard Java regular expression rules apply. Most critically, the use of the Pattern Group field must follow the Java regular expression definition below:

Capturing groups are numbered by counting their opening parentheses from left to right. In the expression ((A)(B(C))), for example, there are four such groups:

((A)(B(C)))

(A)

(B(C))

(C)

Group zero always stands for the entire expression.

Capturing groups are so named because, during a match, each subsequence of the input sequence that matches such a group is saved. The captured subsequence may be used later in the expression, via a back reference, and may also be retrieved from the matcher once the match operation is complete.

The captured input associated with a group is always the subsequence that the group most recently matched. If a group is evaluated a second time because of quantification then its previously-captured value, if any, will be retained if the second evaluation fails. Matching the string "aba" against the expression (a(b)?)+, for example, leaves group two set to "b". All captured input is discarded at the beginning of each match.

Groups beginning with (?) are pure, non-capturing groups that do not capture text and do not count towards the group total."



Note: For additional information regarding regular expressions, go to: <http://java.sun.com/j2se/1.5.0/docs/api/java/util/regex/Pattern.html>

- Step 6** Once you complete the Pattern Group for each field, configure the Order parameter. The Order setting determines the precedence of patterns within a particular Pattern set. Each Pattern within the pattern set for a particular field is used in the Order set here. In the Event Name in the above example, the pass pattern is always attempted before the block pattern. Therefore, it is important to give your more common patterns a higher Order to improve performance.

Configuring the Universal DSM within STRM

Once you configure the GenericDSM.xml file, you must integrate the UNIX Firewall with STRM. This means configuring a Universal DSM Sensor Device using the STRM interface.

To configure the Universal DSM within STRM:

- Step 1** Configure a Universal DSM sensor device:

For more information on configuring a sensor device, see the *Managing Sensor Devices Guide*.

- Step 2** Log in to STRM, using SSH.

- Step 3** Enter the following command:

service ecs restart

Events from the Universal DSM device can now successfully flow into STRM and be parsed by the Universal DSM definition file.

Step 4 To verify the correct parsing is occurring by performing a raw event search against incoming events into STRM, log in to STRM.

Step 5 Click the **Event Viewer** Tab.

Step 6 Click the **Filter/Search** icon.

The Search window appears.

Step 7 In the Filter Area, make sure the only check box selected is the new Universal DSM device.



Note: *If you wish, you can also specify a certain time frame you wish to isolate for incoming events.*

Step 8 Click **Filter**.

The search results appear with the events listed with an Event Name of **Unknown Universal Event** as well as an **Unknown** category.

Step 9 To focus on a single class of events, double-click one of the unknown event entries.

Step 10 To map the unknown event to a specific category, click **Map Event**.

The Device Event window appears.

Step 11 Map the event to a specific category.

For more information on mapping an event, see the *STRM Users Guide*.

Step 12 Click **Ok**.

28

GENERIC AUTHORIZATION SERVER

A STRM generic authorization server DSM accepts events using syslog. STRM records all relevant events. Before you configure STRM to integrate with generic authorization server, you must:

Step 1 Forward all authentication server logs to your STRM system.



Note: For information on forwarding authentication server logs to STRM, see your generic authorization server vendor documentation.

Step 2 Open the following file:

```
/opt/gradar/conf/genericAuthServer.conf
```



Note: Make sure you copy this file to systems hosting the Event Collector and the Console.

Step 3 Restart the Tomcat server:

```
service tomcat restart
```

A message appears indicating that the Tomcat server has restarted.

Step 4 Enable or disable regular expressions in your patterns by setting the `regex_enabled` property accordingly. By default, regular expressions are disabled. For example:

```
regex_enabled=false
```

When you set the `regex_enabled` property to false, the system generates regular expressions (regex's) based on the tags you entered while attempting to retrieve the corresponding data values from the logs.

When you set the `regex_enabled` property to true, you can define custom regex's to control patterns. These regex are directly applied to the logs and the first captured group is returned. When defining custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see the following web site:

<http://java.sun.com/docs/books/tutorial/extra/regex/>

To integrate the generic authorization server with STRM, make sure you specify the classes directly instead of using the predefined classes. For example, the digit class `(/\d/)` becomes `/[0-9]/`. Also, instead of using numeric qualifiers, re-write the expression to use the primitive qualifiers `(/?/,/*/ and /+)`.

Step 5 Review the file to determine a pattern for successful login:

For example, if your authentication server generates the following log message for accepted packets:

```
Jun 27 12:11:21 expo sshd[19926]: Accepted password for root
from 10.100.100.109 port 1727 ssh2
```

The pattern for successful login is `Accepted password`.

Step 6 Add the following entry to the file:

```
login_success_pattern=<login success pattern>
```

Where `<login success pattern>` is the pattern determined in [Step 5](#).

For example:

```
login_success_pattern=Accepted password
```



Note: All entries are case insensitive.

Review the file to determine a pattern for login failures.

For example, if your authentication server generates the following log message for login failures:

```
Jun 27 12:58:33 expo sshd[20627]: Failed password for root from
10.100.100.109 port 1849 ssh2
```

The pattern for login failures is `Failed password`.

Step 7 Add the following to the file:

```
login_failed_pattern=<login failure pattern>
```

Where `<login failure pattern>` is the pattern determined for login failure.

For example:

```
login_failed_pattern=Failed password
```



Note: All entries are case insensitive.

Step 8 Review the file to determine a pattern for logout:

For example, if your authentication server generates the following log message for logout:

```
Jun 27 13:00:01 expo su(pam_unix)[22723]: session closed for
user genuser
```

The pattern for lookout is `session closed`.

Step 9 Add the following to the genericAuthServer.conf file:

```
logout_pattern=<logout pattern>
```

Where `<logout pattern>` is the pattern determined for logout in [Step 8](#).

For example:

```
logout_pattern=session closed
```



Note: All entries are case insensitive.

- Step 10** Review the file to determine a pattern, if present, for source IP address and source port.

For example, if your authentication server generates the following log message:

```
Jun 27 12:11:21 expo sshd[19926]: Accepted password for root
from 10.100.100.109 port 1727 ssh2
```

The pattern for source IP address is `from` and the pattern for source port is `port`.

- Step 11** Add an entry to the file for source IP address and source port:

```
source_ip_pattern=<source IP pattern>
source_port_pattern=<source port pattern>
```

Where `<source IP pattern>` and `<source port pattern>` are the patterns identified in [Step 10](#) for source ip address and source port.

For example:

```
source_ip_pattern=from
source_port_pattern=port
```

- Step 12** Review the file to determine if a pattern exists for username.

For example:

```
Jun 27 12:11:21 expo sshd[19926]: Accepted password for root
from 10.100.100.109 port 1727 ssh2
```

The pattern for username is `for`.

- Step 13** Add an entry to the file for the username pattern:

For example:

```
user_name_pattern=for
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a generic authorization server, you must select the **Configurable Authentication message filter** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding your firewall, see your vendor documentation.

29

FORESCOUT COUNTERACT

A STRM ForeScout CounterACT DSM accepts CounterACT events using syslog. STRM records all relevant and available information from the event. Before configuring a CounterACT device in STRM, you must configure your device to send syslog to your STRM installation. For more information on configuring your CounterACT device, consult your vendor documentation.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a CounterACT device, you must select the **Forescout CounterACT** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

30

GENERIC FIREWALL

A STRM generic firewall server DSM accepts events using syslog. STRM records all relevant events. Before you configure STRM to integrate with generic firewall, you must:

Step 1 Forward all firewall logs to your STRM system.



Note: For information on forwarding firewall logs from your generic firewall to STRM, see your firewall vendor documentation.

Step 2 Open the following file:

```
/opt/gradar/conf/genericFirewall.conf
```



Note: Make sure you copy this file to systems hosting the Event Collector and the Console.

Step 3 Restart the Tomcat server:

```
service tomcat restart
```

A message appears indicating that the Tomcat server has restarted.

Step 4 Enable or disable regular expressions in your patterns by setting the `regex_enabled` property accordingly. By default, regular expressions are disabled. For example:

```
regex_enabled=false
```

When you set the `regex_enabled` property to false, the system generates regular expressions (regex's) based on the tags you entered while attempting to retrieve the corresponding data values from the logs.

When you set the `regex_enabled` property to true, you can define custom regex's to control patterns. These regex are directly applied to the logs and the first captured group is returned. When defining custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see the following web site:

<http://java.sun.com/docs/books/tutorial/extra/regex/>

To integrate a generic firewall with STRM, make sure you specify the classes directly instead of using the predefined classes. For example, the digit class (`/\d/`) becomes `[0-9]`. Also, instead of using numeric qualifiers, re-write the expression to use the primitive qualifiers (`/?`, `/*` and `/+`).

Step 5 Review the file to determine a pattern for accepted packets.

For example, if your device generates the following log messages for accepted packets:

```
Aug. 5, 2005 08:30:00 Packet accepted. Source IP: 192.168.1.1
Source Port: 80 Destination IP: 192.168.1.2 Destination Port: 80
Protocol: tcp
```

The pattern for accepted packets is `Packet accepted`.

Step 6 Add the following to the file:

```
accept_pattern=<accept pattern>
```

Where `<accept pattern>` is the pattern determined in [Step 5](#). For example:

```
accept_pattern=Packet accepted
```



Note: *Patterns are case insensitive.*

Step 7 Review the file to determine a pattern for denied packets.

For example, if your device generates the following log messages for denied packets:

```
Aug. 5, 2005 08:30:00 Packet denied. Source IP: 192.168.1.1
Source Port: 21 Destination IP: 192.168.1.2 Destination Port: 21
Protocol: tcp
```

The pattern for denied packets is `Packet denied`.

Step 8 Add the following to the file:

```
deny_pattern=<deny pattern>
```

Where `<deny pattern>` is the pattern determined in [Step 7](#).



Note: *Patterns are case insensitive.*

Step 9 Review the file to determine a pattern, if present, for the following:

source ip

source port

destination ip

destination port

protocol

For example, if your device generates the following log message:

```
Aug. 5, 2005 08:30:00 Packet accepted. Source IP: 192.168.1.1
Source Port: 80 Destination IP: 192.168.1.2 Destination Port: 80
Protocol: tcp
```

The pattern for source IP is `source IP`.

Step 10 Add the following to the file:

```
source_ip_pattern=<source ip pattern>
```

```
source_port_pattern=<source port pattern>
```

```
destination_ip_pattern=<destination ip pattern>
```

```
destination_port_pattern=<destination port pattern>  
protocol_pattern=<protocol pattern>
```

Where <source ip pattern>, <source port pattern>, <destination ip pattern>, <destination port pattern>, and <protocol pattern> are the corresponding patterns identified in [Step 9](#).



Note: Patterns are case insensitive and you can add multiple patterns. For multiple patterns, separate using a # symbol.

Step 11 Save and exit the file.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a generic firewall, you must select the **Configurable Firewall Filter** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding your firewall, see your vendor documentation.

31

IBM AIX 5L

A STRM IBM AIX 5L DSM accepts events using syslog. STRM records all relevant login, logoff, session opened, session closed, and accepted/failed password events.



Note: *If you are using syslog on a Unix host, we recommend that you upgrade the standard syslog to a more recent version, such as, syslog-ng.*

Before you configure STRM to integrate with IBM AIX, you must:

Step 1 Log in as a root user.

Step 2 Open the `/etc/syslog.conf` file.

Step 3 Forward the system's authentication logs to STRM by adding the following line to the file:

```
auth.*@<IP address>
```

Where `<IP address>` is the IP address of the STRM system.

Step 4 Save and exit the file.

Step 5 Restart syslog:

```
refresh -s syslogd
```

For example, a typical `/etc/syslog.conf` file may resemble the following:

```
##### begin /etc/syslog.conf
```

```
mail.debug /var/adm/maillog
```

```
mail.none /var/adm/maillog
```

```
auth.notice /var/adm/authlog
```

```
lpr.debug /var/adm/lpd-errs
```

```
kern.debug /var/adm/messages
```

```
*.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info  
/var/adm/messages
```

```
auth* @123.234.234.123
```

```
##### end /etc/syslog.conf where 123.456.789.123 is the IP of  
the QRadar system.
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an IBM AIX 5L server, you must select the **IBM AIX Server** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

See your authorization server manufacturer for configuration information.

32

ISS PROVENTIA

A STRM ISS Proventia DSM accepts ISS Proventia events using SNMP. STRM records all relevant events. You can integrate ISS Proventia version M10 v2.1_2004.1122_15.13.53 with STRM. Before you configure STRM to integrate with ISS Proventia, you must:

- Step 1** In the Proventia Manager interface navigation pane, expand the System node.
- Step 2** Select **System**.
- Step 3** Select **Services**.
The Service Configuration page appears.
- Step 4** Click the **SNMP** tab.
- Step 5** Select **SNMP Traps Enabled**.
- Step 6** In the Trap Receiver field, enter the IP address of your STRM system you wish to monitor incoming SNMP traps.
- Step 7** In the Trap Community field, enter the appropriate community name.
- Step 8** From the Trap Version list, select the trap version.
- Step 9** Click **Save Changes**.

You are now ready to configure STRM to receive SNMP traps. For information on configuring SNMP in the STRM interface, see the *Managing Sensor Devices Guide*.

To configure STRM to receive events from an ISS Proventia device, select **IBM Proventia Management SiteProtector** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your ISS Proventia device, see your vendor documentation.

33

ISS SITEPROTECTOR

A STRM ISS SiteProtector DSM accepts ISS SiteProtector events by polling the ISS SiteProtector database allowing STRM to record the relevant events. You can integrate ISS SiteProtector version 2.0 with STRM. Before you configure STRM to integrate with ISS SiteProtector, you must:

Step 1 Access the ISS SiteProtector console.

Step 2 Add a database user and password.

You must record this username and password for use when configuring the ISS SiteProtector DSM in the STRM user interface. Ensure the defined user has read permissions for the table used to store SiteProtector events. This table is defined in the STRM user interface.



Note: *Ensure no firewall rules are blocking the communication between the ISS SiteProtector console and STRM.*

You are now ready to configure STRM to receive SiteProtector events. For information, see the *Managing Sensor Devices Guide*.

To configure STRM to receive events from an ISS SiteProtector device, select **IBM Proventia Network Intrusion Prevention System (IPS)** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your ISS SiteProtector device, see your vendor documentation.

34

JUNIPER NETWORKS DX APPLICATION ACCELERATION PLATFORM

The Juniper Networks DX Application Acceleration Platforms off-load core networking and I/O responsibilities from web and application servers to improve the performance of web-based applications, increasing productivity of local, remote, and mobile users. A STRM Juniper DX Application Acceleration Platform DSM accepts events using syslog. STRM records all relevant status and network condition events. Before configuring a Juniper DX device in STRM, you must configure your device to send syslog events to STRM.

To configure the device to send syslog events to STRM:

Step 1 Log in to the Juniper DX interface.

Step 2 Browse to the desired cluster configuration (Services – Cluster Name), Logging section.

Step 3 Select the **Enable Logging** check box.

Step 4 Select the desired **Log Format**.



Note: STRM supports Juniper DX logs using the **common** and **perf2** formats only.

Step 5 Specify the desired **Log Delimiter** format.



Note: STRM supports comma delimited logs only.

Step 6 In the **Log Host** section specify the IP address of your STRM system.

Step 7 In the **Log Port** section, specify the UDP port on which you wish to export logs.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Juniper DX Application Acceleration Platform, you must select the **Juniper DX Application Acceleration Platform** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

35

JUNIPER NETWORKS NETSCREEN IDP

A STRM NetScreen IDP DSM accepts NetScreen IDP events using syslog. STRM records all relevant NetScreen IDP events. Before you configure STRM to integrate with NetScreen IDP, you must:

- Step 1** Log in to the NetScreen IDP interface.
- Step 2** In NSM, edit the IDP device.
- Step 3** Select **Report Settings**.
- Step 4** Select **Enable Syslog**.
- Step 5** Click **Ok**.
- Step 6** Apply the changes for the IDP sensors you wish to enable logging.



Note: When creating a STRM custom rule, make sure the *Logging* option is selected as the *Notification method* for any custom rules you wish to report to STRM. For more information, see the *STRM Users Guide*.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a NetScreen IDP device, select **Juniper Networks Intrusion Detection and Prevention (IDP)** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding NetScreen IDP, see the NetScreen IDP documentation.

36

JUNIPER NETWORKS SECURE ACCESS

A STRM Juniper Networks Secure Access DSM accepts login and session information using syslog. You can integrate Secure Access version 5.2 with STRM. Before you configure STRM to integrate with a Secure Access device, you must:

- Step 1** Log in to the Secure Access administration interface.
- Step 2** Select **System > Log/Monitoring > Event Log > Settings**.
- Step 3** In the Syslog Server list, add the IP address of the STRM system.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from Juniper Networks Secure Access device, select **Juniper Networks Secure Access (SA) SSL VPN** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your Juniper Networks device, see your vendor documentation.

37

JUNIPER NETWORKS INFRANET CONTROLLER

A STRM Juniper Networks Infranet Controller DSM accepts DHCP events using syslog. STRM records all relevant events from a Juniper Networks Infranet Controller. Before you configure STRM to integrate with a Juniper Networks Infranet Controller, you must configure syslog within the server. For more information on configuring your Juniper Networks Infranet Controller, consult your vendor documentation.

Once you have configured syslog, you are ready to configure the sensor device within the STRM interface. To configure STRM to receive events from your Juniper Networks Infranet Controller, select **Juniper Networks Infranet Controller** from the Sensor Device Type drop-down list box.

For more information on configuring devices, see the *Managing Sensor Devices Guide*.

38

JUNIPER NETWORKS NETSCREEN FIREWALL

You can integrate NetScreen Firewall version 3.0 with STRM. A STRM NetScreen Firewall DSM accepts NetScreen Firewall events using syslog. STRM records all relevant NetScreen Firewall events. Before you configure STRM to integrate with NetScreen Firewall, you must:

- Step 1** Login to your NetScreen Firewall user interface.
- Step 2** From the menu, select **Configuration > Report Settings > Syslog**.
- Step 3** Select the **enable syslog messages** check box.
- Step 4** Enter the IP address of your STRM system hosting the Event Collector.
- Step 5** Click **Apply**.
- Step 6** Click **Policy**.
- Step 7** Click **Edit**.
- Step 8** Select the Logging check box.
- Step 9** Click **Save**.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a NetScreen Firewall device, select **Juniper Networks NetScreen Firewall** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding NetScreen Firewall, see the NetScreen Firewall documentation.

39

JUNIPER NETWORKS NSM

The STRM Juniper Networks NSM DSM accepts NetScreen events using syslog. STRM records all relevant Juniper Networks NSM events.

Before you configure STRM to integrate with a Juniper Networks NSM device, you must configure syslog within your Juniper Networks NSM device. You must also configure a Juniper Networks NSM pipe to ensure proper communications with STRM.

Juniper NSM is a central management server for many Juniper Networks products including ScreenOS firewalls, ISG, and Juniper IDP. You can configure STRM to either collect and represent all device alerts as coming from a central NSM or to represent the individual Juniper Networks security devices that are generating alerts to the NSM server.

To configure the Juniper NSM DSM:

Step 1 Configure the Juniper NSM protocol in the STRM interface.

To configure STRM to receive event from a Juniper Networks NSM device using OPSEC LEA, you must select the **JuniperNSM** option from the Protocol drop-down list box when configuring your protocol configuration. For more information, see Configuring Protocols in the *Managing Sensor Devices Guide*.

Step 2 Configure the sensor device within the STRM interface.

To configure STRM to receive events from a Juniper NSM device, you must select the **Juniper Netscreen-Security Manager (NSM)** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

40

JUNIPER NETWORKS ROUTER

A STRM Juniper Router DSM accepts events using syslog. STRM records all valid syslog events. The STRM Juniper Router DSM supports all Juniper devices running JunOS. Before you configure STRM to integrate with a Juniper Router, you must forward your syslog logs to your STRM system.

To configure the routing platform to log system messages to STRM:

- Step 1** Log into your Juniper platform using SSH.
- Step 2** Include the following syslog statements at the `edit system` hierarchy level:

```
[edit system]
syslog {
  host (hostname) {
    facility severity;
    explicit-priority;
    match "regular-expression";
  }
  source-address source-address;
}
}
```

[Table 40-1](#) lists and describes the configuration setting variables to be entered in the syslog statement.

Table 40-1 List of syslog Configuration Setting Variables

Parameter	Description
hostname	Specify the IP address or the fully-qualified hostname of your STRM system.

Table 40-1 List of syslog Configuration Setting Variables (continued)

Parameter	Description
Facility severity	<p>Specify the severity of the messages that belong to the named facility with which it is paired. Valid severity levels are:</p> <ul style="list-style-type: none"> • any • none • emergency • alert • critical • error • warning • notice • info <p>Messages with the specified severity level and higher are logged. The levels from emergency through info are in order from highest severity to lowest.</p>
Regular-expression	<p>Specify text string that must (or must not) appear in a message for the message to be logged to a destination.</p> <p>This is an optional configuration setting.</p>
Source-address	<p>Specify a valid IP address configured on one of the router interfaces. For system logging purposes.</p> <p>The source-address is recorded as the source of the message in the messages sent to the remote machine specified in host hostname statement at the edit system syslog hierarchy level; not, however, for messages directed to the other routing engine, or to the TX Matrix platform in a routing matrix.</p>

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from Juniper Router, you must select the **Juniper Networks Routing Platform, Juniper M-Series Multiservice Edge Routing, Juniper MX-Series Ethernet Services Router, or Juniper T-Series Core Platform** option (depending on your Juniper platform) from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding your Juniper device, see your vendor documentation.

41

JUNIPER NETWORKS STEEL-BELTED RADIUS

A STRM Juniper Networks Steel-Belted RADIUS DSM accepts syslog events from a client running the STRM Adaptive Log Exporter utility. STRM records all successful and unsuccessful login attempts. For more information on configuring your Steel-Belted Radius server consult your vendor documentation.

To integrate a Juniper Networks Steel-Belted RADIUS DSM with STRM:

- Step 1** Configure the STRM Adaptive Log Exporter utility for Juniper Networks Steel-Belted Radius.



Note: *The Adaptive Log Exporter must be installed on the same system as your Juniper Networks SBR system.*

When configuring your Juniper Networks Steel-Belted RADIUS device, you must also configure the **Root Log Directory** parameter, which is the location Juniper SBR stores the logs files. For more information regarding configuring your Cisco ACS device, see the *Adaptive Log Exporter Users Guide*.



Note: *You must use the default values for the log file heading in the Juniper Networks Steel-Belted Radius appliance. If the log file headings have been changed from the default values and STRM is not parsing SBR events properly, please contact Juniper Networks Customer Support.*

- Step 2** Configure STRM to receive events from your Juniper Networks Steel-Belted RADIUS server.

You must select the **Juniper Steel-Belted Radius** option from the Sensor Device Type drop-down box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

42

LINUX AUTHORIZATION SERVER

A STRM Linux Authorization Server DSM accepts events using syslog. You can integrate the following Linux Authorization Servers with STRM:

- Open Source Linux Login/Logout Log version 2.4
- Red Hat Login/Logout version 2.4

STRM records all relevant login, logoff, session opened, session closed, and accepted/failed password events.



Note: *If you are using syslog on a Unix host, Juniper recommends that you upgrade the standard syslog to a more recent version, such as, syslog-ng.*

Before you configure STRM to integrate with a Linux Authorization Server, you must:

Step 1 Log in as a root user.

Step 2 Open the `/etc/syslog.conf` file.

Step 3 Forward the system's authentication logs to STRM by adding the following line to the file:

```
auth.* @<IP address>
```

Where `<IP address>` is the IP address of the STRM system.

Step 4 Save and exit the file.

Step 5 Restart syslog:

```
/etc/init.d/syslog restart
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Linux authorization server, you must select the **Linux login messages** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

See your authorization server manufacturer for configuration information.

43

LINUX DHCP

A STRM Linux DHCP Server DSM accepts DHCP events using syslog. STRM records all relevant events from a Linux DHCP Server. Before you configure STRM to integrate with a Linux DHCP Server, you must configure syslog within the server.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from your Linux DHCP Server, you must select the **Linux DHCP Server** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*. For more information on configuring your Linux DHCP Server, consult the man pages or associated documentation for your DHCP daemon.

44

LINUX IPTABLES

A STRM Linux IPtables DSM accepts events using syslog. STRM records all relevant Accept, Drop, or Reject events. You can integrate IPTables version 2.4 with STRM.

Before you configure STRM to integrate with IPtables, you must:

Step 1 Open the `iptables.conf` file.



Note: The file containing IP tables rules varies according to Linux operating system. For a system operating Red Hat Enterprise, the file is located in the `/etc/sysconfig/iptables` directory. Consult the documentation for your Linux operating system for more information on configuring IP tables.

Step 2 Review the file to determine the IP tables rules you wish to log.

For example, if you wish to log the rule defined by the entry:

```
-A INPUT -i eth0 --dport 31337 -j DENY
```

Step 3 Insert a matching rule immediately before each rule you wish to log:

```
-A INPUT -i eth0 --dport 31337 -j DENY
```

```
-A INPUT -i eth0 --dport 31337 -j DENY
```

Step 4 Update the target of the new rule to LOG for each rule you wish to log. For example:

```
-A INPUT -i eth0 --dport 31337 -j LOG
```

```
-A INPUT -i eth0 --dport 31337 -j DENY
```

Step 5 Set the log level of the LOG target to a SYSLOG priority level, such as info or notice:

```
-A INPUT -i eth0 --dport 31337 -j LOG --log-level info
```

```
-A INPUT -i eth0 --dport 31337 -j DENY
```

Step 6 Add a string to the file to identify the rule's subsequent behavior. Set the log prefix parameter to `Q1Target=<rule>`.

Where `<rule>` is one of `fw_accept`, `fw_drop`, or `fw_reject`.

For example, if the rule being logged targets DENY, the log prefix setting should be `Q1Target=fw_deny`.

```
-A INPUT -i eth0 --dport 31337 -j LOG --log-level info --log-prefix "Q1Target=fw_deny "  
-A INPUT -i eth0 --dport 31337 -j DENY
```



Note: The trailing space is required before the closing quotation mark.

Step 7 Save and exit the file.

Step 8 Restart IPTables:

```
/etc/init.d/iptables restart
```

Step 9 Open the `syslog.conf` file.

Step 10 Add the following line:

```
kern.<log level><TAB><TAB>@<IP Address>
```

Where:

<log level> is the previously set log level.

<TAB><TAB> is any chosen amount of space.

<IP Address> is the IP address of the STRM Event Collector.

Step 11 Save and exit the file.

Step 12 Restart the syslog daemon:

```
/etc/init.d/syslog restart
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an IP tables device, you must select the **Linux iptables Firewall** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information on IPTables, see the IPTables documentation.

45

McAFEE INTRUSHIELD

A STRM McAfee Intrushield DSM accepts events using syslog. You can integrate McAfee Intrushield versions 1.5 and 1.8 with STRM. STRM records all relevant events. Before you configure STRM to integrate with a McAfee Intrushield device, you must:

- Step 1** Log in to the McAfee Intrushield Manager.
- Step 2** In the Resource window, access the Manager Node.
- Step 3** Enter the Syslog Server details.
- Step 4** Configure syslog using the following string:

```
| $IV_ALERT_ID$ | $IV_ALERT_TYPE$ | $IV_ATTACK_TIME$ | "$IV_ATTACK_NAM  
E$" | $IV_ATTACK_ID$ | $IV_ATTACK_SEVERITY$ | $IV_ATTACK_SIGNATURE$ | $  
IV_ATTACK_CONFIDENCE$ | $IV_ADMIN_DOMAIN$ | $IV_SENSOR_NAME$ | $IV_IN  
TERFACE$ | $IV_SOURCE_IP$ | $IV_SOURCE_PORT$ | $IV_TARGET_IP$ | $IV_TAR  
GET_PORT$ |
```

- Step 5** From the Root Admin Domain, select **Forwarding > Syslog Forwarder**.
- Step 6** Enable Syslog Forwarder.

If the Syslog Forwarder is enabled and the syslog server is not receiving any syslog messages, open the `$IntruShield/Config/tms_trace.properties` file and, in the Syslog section, uncomment (remove the #) the three lines within this section. Also, if the McAfee Intrushield Manager and the syslog server are communicating through a firewall, make sure UDP port 514 is not blocked on your firewall.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a McAfee IntruShield device, you must select the **McAfee IntruShield Network IPS Appliance** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information on McAfee Intrushield, see your vendor documentation.

46

McAFEE ePOLICY ORCHESTRATOR

A STRM McAfee ePolicy Orchestrator DSM accepts events using SNMP. STRM records all relevant AntiVirus events. Before configuring a McAfee ePolicy Orchestrator device in STRM, you must configure your device to send SNMP traps to STRM.

To configure the device to send SNMP traps to STRM:

Step 1 Log in to the ePolicy Orchestrator 3.x Console.

Step 2 In the Console tree, click **Notifications**.

Step 3 In the details pane, select the **Configuration | SNMP Servers** tab.

Step 4 Add a name and the IP address of your STRM server. Click **OK**.

Step 5 Click the **Rules** tab.

Step 6 Click **Add Rule**.

The Add or Edit Notification Rule wizard appears.

Step 7 In the **Describe Rule** window, make sure the default (**Directory**) for the **Defined At** text box is configured. You may define rules for the Directory or any site within the Directory.

Step 8 Provide a name for the rule in the **Rule Name** text box. For example, Virus Detected.

Step 9 In the Description field, enter a description. For example, Viruses detected by VirusScan Enterprise. Click **Next**.

Step 10 In the **Set Filters** window:

- a Make sure all **Operating systems** check boxes are selected.
- b Under Products, select **VirusScan**.
- c Under Categories, select **Any category** above the list.
- d Click **Next**.

Step 11 Make sure the **Send a notification for every event** option is selected. Click **Next**.

Step 12 In the Add or Edit Notification Rule window, click **Add SNMP Trap**.

Step 13 In the **SNMP server** list, select the SNMP server that represents your STRM server.

Step 14 Ensure that all boxes are enabled. Click **Save**.

Step 15 Click **Next**.

Step 16 Verify your configuration in n the View Summary page.

Step 17 Click **Finish**.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a McAfee ePolicy Orchestrator device, you must select the **McAfee ePolicy Orchestrator** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

47

METAINFO METAIP

A STRM MetaInfo MetaIP DSM accepts MetaIP events using syslog. STRM records all relevant and available information from the event. Before configuring a MetaIP device in STRM, you must configure your device to send syslog to STRM. For more information regarding your MetaInfo MetaIP device, see your vendor documentation.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a MetaInfo MetaIP device, you must select the **MetaInfo MetaIP** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

48

MICROSOFT IIS

You can integrate a Microsoft Internet Information Services (IIS) 5.x or 6.x server with STRM. A STRM IIS DSM accepts IIS server events using syslog. STRM records all HTTP status code events. Before you configure STRM to integrate with an IIS server, you must:

Step 1 Open the IIS console.

Step 2 From the login options, select **W3C Extended** format.

Step 3 Select the following options:

- Date
- Time
- Client IP
- User Name
- Server IP Address
- Server Port
- Method
- URI Stem
- URI Query
- Protocol Status
- User Agent

Step 4 Install open source Snare Agent for IIS.



Note: To download a Snare Agent, see the following web site:
<http://www.intersectalliance.com/projects/index.html>

Step 5 In the Snare Agent interface, select **Audit Configuration**.

The Audit Service Configuration window appears.

Step 6 In the Target Host field, enter the IP address of your STRM installation.

Step 7 In the Destination option, select **Syslog**.

Step 8 In the Delimiter option, select **TAB**.

Step 9 Select the Display IIS Header Information check box.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an IIS device, you must select the **Microsoft IIS Webserver Logs** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding IIS, see your vendor documentation.

49

MICROSOFT DHCP SERVER

A STRM Microsoft DHCP Server DSM accepts DHCP events using the STRM Adaptive Log Exporter. You can integrate Windows DHCP Server versions 2000/2003 with STRM using the Adaptive Log Exporter Windows DHCP devices. For more information on the Adaptive Log Exporter, see the *STRM Adaptive Log Exporter Users Guide*.

To configure the Microsoft DHCP Server to send syslog to STRM:

- Step 1** Log in to the DHCP Server Administration Tool.
- Step 2** From the DHCP Administration Tool, use the right-mouse button (right-click) on the DHCP server and select **Properties**.
The Properties window appears.
- Step 3** Click the **General** tab.
The General panel appears.
- Step 4** Click **Enable DHCP Audit Logging**.
The log file %WINDIR%\system32\dhcp\DhcpSrvLog-xxx.log is created.
- Step 5** Restart the DHCP service.

To integrate Windows DHCP Server versions 2000/2003 with STRM using the Adaptive Log Exporter Windows DHCP devices, see the *STRM Adaptive Log Exporter Users Guide*.

To configure STRM to receive events from a Microsoft Windows DHCP Server, you must select the **Microsoft DHCP Server** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your server, see your vendor documentation.

50

MICROSOFT EXCHANGE SERVER

A STRM Microsoft Exchange Server DSM accepts Exchange mail and security events using syslog. You can integrate Microsoft Exchange 2003 with STRM using the STRM Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

To configure STRM to receive events from a Microsoft Exchange Server, you must select the **Microsoft Exchange Server** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your server, see your vendor documentation.

51

MICROSOFT WINDOWS SECURITY EVENT LOG

A STRM Microsoft Windows Security Event Log DSM accepts events using syslog from relevant authentication and authorization events. You can integrate Windows server versions 2000/XP with STRM using one of the following methods:

- Use the STRM Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.
- Set-up the Snare Agent to forward windows security event logs to STRM.

To set-up the Snare Agent to forward windows security event logs to STRM:

Step 1 Download and install the Snare Agent.



Note: To download a Snare Agent, see the following web site:
www.intersectalliance.com/projects/index.html

Step 2 In the Snare Agent interface, select **Audit Configuration**.



Note: If you are using the web interface, select **Network Configuration**.

Step 3 In the Enter the remote IP or DNS address field, enter the IP address of the STRM system.



Note: If you are using the web interface, you must enter the IP address of the STRM system in the Destination Snare Server address field.

Step 4 Make sure the Enable Syslog Header check box is selected.

Step 5 Click **Objectives Configuration**.

Step 6 Select the check boxes to determine which Windows events you wish to forward to STRM.

Step 7 From the menu, select **Activity > Apply and restart Audit**.



Note: The value entered in the override host name detection with field must match the IP address or hostname assigned to the device configured in the STRM setup.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Windows security event log, you must select the **Microsoft Security Event Log** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your server, see your vendor documentation.

52

MICROSOFT IAS SERVER

A STRM Microsoft IAS Server DSM accepts RADIUS events using syslog. You can integrate Windows 2000/2003 Server IAS logs with STRM using the STRM Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

To configure STRM to receive events from a Microsoft Windows IAS Server, you must select the **Microsoft IAS Server** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your server, see your vendor documentation.

53

MICROSOFT IIS SERVER

A STRM Microsoft Internet Information Services (IIS) Server DSM accepts IIS FTP, Web, and SMTP events using syslog. You can integrate a Microsoft IIS device with STRM using the STRM Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

To configure STRM to receive events from a Microsoft IIS Server, you must select the **Microsoft IIS** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your server, see your vendor documentation.

54

MICROSOFT SQL SERVER

A STRM Microsoft SQL Server DSM accepts Exchange mail and security events using syslog. You can integrate Microsoft SQL Server 2000/2005 with STRM using the Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

To configure STRM to receive events from a Microsoft SQL Server, you must select the **Microsoft SQL Server** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your server, see your vendor documentation.

55

NIKSUN

A STRM Nixsun DSM accepts Nixsun events using syslog. STRM records all relevant Nixsun events. You can integrate NetDetector/NetVCR2005, version 3.2.1sp1_2 with STRM. Before you configure STRM to integrate with a Nixsun device, you must configure syslog within your Nixsun device. For more information on configuring Nixsun, consult your Nixsun documentation.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Nixsun device, you must select the **Nixsun 2005 v3.5** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

56

NOKIA FIREWALL

A STRM Nokia Firewall DSM accepts events using the following methods:

- [Integrating Nokia Firewall Using Syslog](#)
- [Integrating Nokia Firewall Using OPSEC](#)

You can integrate Nokia Firewall version NG AI R55 with STRM.

Integrating Nokia Firewall Using Syslog

This method ensures the STRM Nokia Firewall DSM accepts Nokia events using syslog. Before you configure STRM to integrate with a Nokia Firewall device, you must:

- Step 1** Login to the Nokia Voyager interface.
- Step 2** Click **Config**.
- Step 3** Below the System Configuration heading, click **System Logging**.
- Step 4** In the Add new remote IP address to log to field, enter the IP address of your STRM system.
- Step 5** Click **Apply**.
- Step 6** Click **Save**.
- Step 7** Using SSH, or a direct console connection, log in to the Nokia device as an administrative user.



Note: If the SSH terminal is disabled, you must enable it through the Nokia Voyager web interface. See your Nokia Voyager documentation.

- Step 8** Open the `/var/etc/rc.local` file.



Note: If the file does not exist, you must create the file.

- Step 9** Add the following to the file:

```
$FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
```

- Step 10** At the terminal prompt, enter the following command:

```
nohup $FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Nokia Firewall device using syslog, select **CheckPoint Firewall-1** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

Integrating Nokia Firewall Using OPSEC


This method ensures the STRM Check Point FireWall-1 DSMs accepts FireWall-1 events using OPSEC. Before you configure STRM to integrate with a Nokia Firewall device, you must:

- Step 1** Reconfigure Nokia Firewall using OPSEC, see [Reconfiguring Nokia Firewall Using OPSEC](#).
- Step 2** Configure the OPSEC LEA protocol in the STRM interface.
To configure STRM to receive event from a Check Point device using OPSEC LEA, you must select the **LEA** option from the Protocol drop-down list box when configuring your protocol configuration. For more information, see *Configuring Protocols* in the *Managing Sensor Devices Guide*.
- Step 3** Configure the sensor device within the STRM interface.
To configure STRM to receive events from an Check Point Provider-1 device using OPSEC, you must select the **CheckPoint Firewall-1 Devices via Syslog** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information, see your vendor documentation.

Reconfiguring Nokia Firewall Using OPSEC

To reconfigure Nokia Firewall using OPSEC:

- Step 1** To create a host object for your STRM system, open up the Check Point SmartDashboard GUI and select **Manage > Network Objects > New > Node > Host**.
 - Step 2** Enter in the Name, IP Address, and optional Comment for your STRM host
 - Step 3** Click **OK**.
 - Step 4** Select **Close**.
 - Step 5** To create the OPSEC connection, select **Manage > Servers and OPSEC Applications > New > OPSEC Application Properties**.
 - Step 6** Enter the Name and optional Comment.
-  **Note:** The name you enter must be different than the name entered in [Step 2](#).
- Step 7** From the Host drop-down menu, select the STRM host object that you created.
 - Step 8** From Application Properties, select **User Defined** as the Vendor Type.
 - Step 9** From Client Entries, select **LEA**.

Step 10 Select **Communication** and enter an activation key to configure the Secure Internal Communication (SIC) certificate.

Step 11 Select **OK** and then select **Close**.

Step 12 To install the policy on your firewall, select **Policy > Install > OK**.

57

NORTEL ARN

A STRM Nortel ARN DSM accepts Nortel ARN events using syslog. STRM records all relevant events. Before you configure STRM to integrate with a Nortel ARN device, you must:

- Step 1** Open Site Manager.
- Step 2** In the tools menu, select **Configuration Manager > Dynamic**.
- Step 3** In the Configuration Manager window, select **Platform > Syslog > Syslog Host Table**.
- Step 4** In the new Syslog Host List window, click **Add**.
- Step 5** In the Syslog Remote Host Configuration window, enter the STRM Console IP address in the Destination Host field.
- Step 6** Click **Ok**.
- Step 7** In the Syslog Host List, click **Done**.
- Step 8** Exit the Configuration Manager

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Nortel ARN device, you must select the **Nortel BayRS 15.x** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding Nortel ARN, see your vendor documentation.

58

NORTEL APPLICATION SWITCH

Nortel Application Switches integrate routing and switching by forwarding traffic at layer 2 speed using layer 4-7 information. A STRM Nortel Application Switch DSM accepts events using syslog. STRM records all relevant status and network condition events. Before configuring a Nortel Application Switch device in STRM, you must configure your device to send syslog events to STRM.

To configure the device to send syslog events to STRM:

Step 1 Log in to the Nortel Application Switch interface.

Step 2 Set the IP address of the first syslog host:

```
host <ip_address>
```

Where <ip_address> is the IP address of your STRM system.

Step 3 Set the IP address of the first syslog host:

```
sever <severity>
```

Where <severity> sets the severity level (0 to 7) of the first syslog host displayed. The default is 7, which means you wish to log all the seven severity levels.

Step 4 Set the facility level of the first syslog host displayed. The default is 0:

```
facil <facility>
```

Where <facility> sets the facility level (0 to 7) of the first syslog host displayed. The default is 0.

Step 5 Enable/disable syslog on device features:

```
log <feature|all> <enable|disable>
```

Where:

<feature|all> displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as vlans, gslb, filter), or enable/disable syslog on all available features.

<enable|disable> enables or disables the log features.

The seven levels of severity includes:

- **0: Emergency** — Indicates that the system is unusable.
- **1: Alert** — Indicates that corrective action must be taken immediately.

- **2: Critical** — Indicates that the condition of the system is critical.
- **3: Error** — Indicates that the system has errors that should be corrected.
- **4: Warning** — Indicates that the system is issuing a warning.
- **5: Notice** — Indicates that the condition of the system is normal but with significant conditions that need attention.
- **6: Informational** — Indicates that the system is functioning but sending information regarding certain unfavorable conditions.
- **7. Debug** — Indicates that the system is sending debug-level messages.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Nortel Application Switch, you must select the **Nortel Application Switch** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

59

NORTEL CONTIVITY 5000

A STRM Nortel Contivity DSM accepts Contivity events using syslog. STRM records all relevant Contivity events. You can integrate Nortel Contivity Firewall/VPN version 5000 V04_85.160 with STRM. Before you configure STRM to integrate with a Contivity device, you must configure syslog within your Contivity device. For more information on configuring Contivity, consult your vendor documentation.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Contivity device, you must select the **Nortel Contivity 5000** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

60

NORTEL CONTIVITY FIREWALL/VPN

A STRM Nortel Contivity DSM accepts Nortel Contivity events using syslog. STRM records all relevant events. Before you configure STRM to integrate with a Nortel Contivity device, you must:

- Step 1** Log in to the Nortel Contivity interface.
- Step 2** From the menu, select **Admin > Config**.
- Step 3** Select the option to allow the switch to send system messages to a specific machine.
- Step 4** Enter the IP address of the STRM system to which you wish to send logs.
- Step 5** In the Message Level section, specify the information you wish to send to the STRM system. The options are:
 - **Urgent events** — Indicates events that may pose security or access problems and you wish to be notified immediately.
 - **Normal events** — Indicates the event for users and system interactions that allow you to review switch activity.
 - **Detailed events** — Indicates events for Nortel Networks Customer Support personnel only.
 - **All Section** — Indicates events for Nortel Networks Customer Support personnel only.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Nortel Contivity device, you must select the **Nortel Contivity VPN Switch** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding your Nortel Contivity device, see your vendor documentation.

61

NORTEL SWITCHED FIREWALL 5100

A STRM Nortel Switched Firewall 5100 DSM accepts Check Point FireWall-1 events from a Check Point SmartCenter Server, which is managed by the Nortel Switched Firewall. STRM records all relevant events. Before configuring a Nortel Switched Firewall device in STRM, you must configure your Check Point SmartCenter Server to send events to STRM.

You can configure STRM to integrate with a Nortel Switched Firewall 5100 using one of the following methods:

- [Integrating Nortel Switched Firewall Using Syslog](#)
- [Integrating Nortel Switched Firewall Using OPSEC](#)



Note: Depending on your Operating System, the procedures for the Check Point SmartCenter Server may vary. The following procedures are based on the Check Point SecurePlatform Operating system.

Integrating Nortel Switched Firewall Using Syslog

This method ensures the STRM Nortel Switched Firewall 5100 DSM accepts Check Point FireWall-1 events using syslog. Before you configure STRM to integrate with a Check Point FireWall-1 SmartCenter Server, you must:



Note: If Check Point SmartCenter Server is installed on Microsoft Windows, you must use the OPSEC method.

Step 1 Enter the following command to access the Check Point SmartCenter Server console as an expert user:

```
expert
```

A password prompt appears.

Step 2 Enter your expert console password. Press **Enter**.

Step 3 Open the following file:

```
/etc/rc.d/rc3.d/s99local
```

Step 4 Add the following lines:

```
$FWDIR/bin/fw log -ftn | /usr/bin/logger -p  
<facility>.<priority> > /dev/null 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, local3.

<priority> is a Syslog priority, for example, info.

For example:

```
$FWDIR/bin/fw log -ftn | /usr/bin/logger -p local3.info >
/dev/null 2>&1 &
```

Step 5 Save and exit the file.

Step 6 Open the syslog.conf file and add the following:

```
<facility>.<priority> <TAB><TAB>@<host>
```

Where:

<facility> is the syslog facility, for example, local3. This value must match the value entered in [Step 4](#).

<priority> is the syslog priority, for example, info or notice. This value must match the value entered in [Step 4](#).

<TAB> indicates you must press the TAB key.

<host> indicates the STRM managed host.

Step 7 Save and exit the file.

Step 8 Restart syslog.

Step 9 Enter the following command:

```
# nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p
<facility>.<priority> > /dev/null 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, local3. This value must match the value entered in [Step 4](#).

<priority> is a Syslog priority, for example, info. This value must match the value entered in [Step 4](#).

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Nortel Switched Firewall 5100 using syslog, you must select the **Nortel Switched Firewall 5100** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information, see your vendor documentation.

Integrating Nortel Switched Firewall Using OPSEC

This method ensures the STRM Nortel Switched Firewall 5100 DSM accepts CheckPoint FireWall-1 events using OPSEC. To enable Nortel Switched Firewall and STRM integration, you must:


- Step 1** Reconfigure Check Point SmartCenter Server. See [Reconfiguring Check Point SmartCenter Server](#).
- Step 2** Configure the OPSEC LEA protocol in the STRM interface.
To configure STRM to receive event from a Check Point SmartCenter Server using OPSEC LEA, you must select the **LEA** option from the Protocol drop-down list box when configuring your protocol configuration. For more information, see *Configuring Protocols* in the *Managing Sensor Devices Guide*.
- Step 3** Configure the sensor device within the STRM interface.
To configure STRM to receive events from a Nortel Switched Firewall 5100 device using OPSEC, you must select the **Nortel Switched Firewall 5100** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information, see your vendor documentation.

Reconfiguring Check Point SmartCenter Server

This section describes how to reconfigure the Check Point SmartCenter Server. In the Check Point SmartCenter Server, create a host object representing the STRM system. The leapipe is the connection between the Check Point SmartCenter Server and STRM.

To reconfigure the Check Point SmartCenter Server:

- Step 1** To create a host object, open the Check Point SmartDashboard GUI and select **Manage > Network Objects > New > Node > Host**.
- Step 2** Enter in the Name, IP Address, and optional Comment for your host.
- Step 3** Click **OK**.
- Step 4** Select **Close**.
- Step 5** To create the OPSEC connection, select **Manage > Servers and OPSEC applications > New > OPSEC Application Properties**.
- Step 6** Enter the Name and optional Comment.
 **Note:** The name you enter must be different than the name entered in [Step 2](#).
- Step 7** From the Host drop-down menu, select the host object you have created in [Step 1](#).
- Step 8** From Application Properties, select **User Defined** as the vendor.
- Step 9** From Client Entries, select **LEA**.
- Step 10** Click **Communication** to generate a Secure Internal Communication (SIC) certificate and enter an activation key.

Step 11 Click **OK** and then click **Close**.

Step 12 To install the Security Policy on your firewall, select **Policy > Install > OK**.

62

NORTEL SWITCHED FIREWALL 6000

A STRM Nortel Switched Firewall 6000 DSM accepts Check Point FireWall-1 events from a Check Point SmartCenter Server, which is managed by the Nortel Switched Firewall. STRM records all relevant events. Before configuring a Nortel Switched Firewall device in STRM, you must configure your Check Point SmartCenter Server to send events to STRM.

You can configure STRM to integrate with a Nortel Switched Firewall 6000 using one of the following methods:

- [Integrating Nortel Switched Firewall Using Syslog](#)
- [Integrating Nortel Switched Firewall Using OPSEC](#)



Note: Depending on your Operating System, the procedures for the Check Point SmartCenter Server may vary. The following procedures are based on the Check Point SecurePlatform Operating system.

Integrating Nortel Switched Firewall Using Syslog

This method ensures the STRM Nortel Switched Firewall 6000 DSM accepts Check Point FireWall-1 events using syslog. Before you configure STRM to integrate with a Check Point FireWall-1 SmartCenter Server, you must:



Note: If Check Point SmartCenter Server is installed on Microsoft Windows, you must use the OPSEC method.

Step 1 Enter the following command to access the Check Point SmartCenter Server console as an expert user:

```
expert
```

A password prompt appears.

Step 2 Enter your expert console password. Press **Enter**.

Step 3 Open the following file:

```
/etc/rc.d/rc3.d/s99local
```

Step 4 Add the following lines:

```
$FWDIR/bin/fw log -ftn | /usr/bin/logger -p  
<facility>.<priority> > /dev/null 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, local3.

<priority> is a Syslog priority, for example, info.

For example:

```
$FWDIR/bin/fw log -ftn | /usr/bin/logger -p local3.info >
/dev/null 2>&1 &
```

Step 5 Save and exit the file.

Step 6 Open the syslog.conf file and add the following:

```
<facility>.<priority> <TAB><TAB>@<host>
```

Where:

<facility> is the syslog facility, for example, local3. This value must match the value entered in [Step 4](#).

<priority> is the syslog priority, for example, info or notice. This value must match the value entered in [Step 4](#).

<TAB> indicates you must press the TAB key.

<host> indicates the STRM managed host.

Step 7 Save and exit the file.

Step 8 Restart syslog.

Step 9 Enter the following command:

```
# nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p
<facility>.<priority> > /dev/null 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, local3. This value must match the value entered in [Step 4](#).

<priority> is a Syslog priority, for example, info. This value must match the value entered in [Step 4](#).

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an Nortel Switched Firewall 6000 using syslog, you must select the **Nortel Switched Firewall 6000** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information, see your vendor documentation.

Integrating Nortel Switched Firewall Using OPSEC

This method ensures the STRM Nortel Switched Firewall 6000 DSM accepts CheckPoint FireWall-1 events using OPSEC. To enable Nortel Switched Firewall and STRM integration, you must:


- Step 1** Reconfigure Check Point SmartCenter Server. See [Reconfiguring Check Point SmartCenter Server](#).
- Step 2** Configure the OPSEC LEA protocol in the STRM interface.
To configure STRM to receive event from a Check Point SmartCenter Server using OPSEC LEA, you must select the **LEA** option from the Protocol drop-down list box when configuring your protocol configuration. For more information, see *Configuring Protocols* in the *Managing Sensor Devices Guide*.
- Step 3** Configure the sensor device within the STRM interface.
To configure STRM to receive events from a Nortel Switched Firewall 6000 device using OPSEC, you must select the **Nortel Switched Firewall 6000** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information, see your vendor documentation.

Reconfiguring Check Point SmartCenter Server

This section describes how to reconfigure the Check Point SmartCenter Server. In the Check Point SmartCenter Server, create a host object representing the STRM system. The leapipe is the connection between the Check Point SmartCenter Server and STRM.

To reconfigure the Check Point SmartCenter Server:

- Step 1** To create a host object, open the Check Point SmartDashboard GUI and select **Manage > Network Objects > New > Node > Host**.
- Step 2** Enter in the Name, IP Address, and optional Comment for your host.
- Step 3** Click **OK**.
- Step 4** Select **Close**.
- Step 5** To create the OPSEC connection, select **Manage > Servers and OPSEC applications > New > OPSEC Application Properties**.
- Step 6** Enter the Name and optional Comment.
 **Note:** The name you enter must be different than the name entered in [Step 2](#).
- Step 7** From the Host drop-down menu, select the host object you have created in [Step 1](#).
- Step 8** From Application Properties, select **User Defined** as the vendor.
- Step 9** From Client Entries, select **LEA**.
- Step 10** Click **Communication** to generate a Secure Internal Communication (SIC) certificate and enter an activation key.

Step 11 Click **OK** and then click **Close**.

Step 12 To install the Security Policy on your firewall, select **Policy > Install > OK**.

63

NORTEL VPN GATEWAY

A STRM Nortel VPN Gateway DSM accepts events using syslog. STRM records all relevant operating system (OS), system control, traffic processing, startup, configuration reload, AAA, and IPsec events. Before configuring a Nortel VPN Gateway device in STRM, you must configure your device to send syslog events to STRM.

To configure the device to send syslog events to STRM:

Step 1 Log in to the Nortel VPN Gateway interface.

Step 2 Configure the device to send syslog events log to STRM:

```
add <ip_address> <local_facility_number>
```

Where:

<ip_address> is the IP address of your STRM system.

<local_facility_number> is the local facility number.



Note: When adding a syslog server, a prompt appears requesting the IP address and the local facility number. The local facility number can be used to uniquely identify syslog entries. For more information, see the manual page for `syslog.conf` under UNIX.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Nortel VPN Gateway device, you must select the **Nortel VPN Gateway** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

64

OPEN SOURCE SNORT

A STRM Open Source SNORT DSM accepts SNORT events using syslog. You can integrate SNORT version 2.x with STRM. STRM records all relevant SNORT events.



Note: *The below procedure applies to a system operating Red Hat Enterprise. The procedures below may vary for other operating systems.*

Before you configure STRM to integrate with a SNORT device, you must:

Step 1 Configure SNORT on a remote system.

Step 2 Open the `snort.conf` file.

Step 3 Uncomment the following line:

```
output alert_syslog:LOG_AUTH LOG_INFO
```

Step 4 Save and exit the file.

Step 5 Open the following file:

```
/etc/init.d/snortd
```

Step 6 Add an `-s` to the following lines, as shown in the example below:

```
daemon /usr/sbin/snort $ALERTMODE $BINARY_LOG $NO_PACKET_LOG
$DUMP_APP -D $PRINT_INTERFACE -i $i -s -u $USER -g $GROUP $CONF
-i $LOGDIR/$i $PASS_FIRST

daemon /usr/sbin/snort $ALERTMODE $BINARY_LOG $NO_PACKET_LOG
$DUMP_APP -D $PRINT_INTERFACE $INTERFACE -s -u $USER -g $GROUP
$CONF -i $LOGDIR
```

Step 7 Save and exit the file.

Step 8 Restart SNORT:

```
/etc/init.d/snortd restart
```

Step 9 Open the `syslog.conf` file.

Step 10 Update the file to reflect the following:

```
auth.info @<IP Address>
```

Where `<IP Address>` is the system to which you want logs sent.

Step 11 Save and exit the file.

Step 12 Restart syslog:

```
/etc/init.d/syslog restart
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a SNORT device, you must select the **Snort Open Source IDS** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding SNORT, see <http://www.snort.org/docs/>.

65

ORACLE AUDIT RECORDS

Oracle databases track auditing events, such as, user login and logouts, permission changes, table creation, and deletion and database inserts. STRM can collect these events for correlation and reporting purposes through the use of the Oracle Audit DSM. For more, see your Oracle documentation.



Note: Oracle provides two modes of audit logs. STRM does not support fine grained auditing.



Note: The information in this document is specific to Oracle RDBMS running on Linux. These procedures should be considered guidelines only. Juniper recommends that you have experience with Oracle DBA before performing the procedures in this document. Other UNIX host operating systems may also work to send audit records, however, Microsoft Windows hosts are not supported. For more information, see your vendor documentation.

Before STRM can collect Oracle Audit events from an Oracle RDBMS instance, that instance must be configured to write audit records to either syslog or the database audit tables. For complete details and instructions for configuring auditing, see your vendor documentation.



Note: Only Oracle version 10g can sent audit records through syslog. Therefore, you must use Oracle v9i to configure database auditing.

To configure the device to write audit logs to syslog:

- Step 1** Log in to the Enterprise Manager (EM) console as sysdba.
- Step 2** Click the **Administration** tab.
- Step 3** From the Database Configuration section, click **All Initialization Parameters** link.
- Step 4** Click the **SPFile** tab.
- Step 5** Sort the parameters by name (click on the Name column header) so that the parameters starting with "a" are shown first.
- Step 6** From the audit_trail drop-down list box, select one of the following options:
 - a For syslog-based events, select **OS**. Click **Apply**. Go to Step [Step 8](#).
 - b For JDBC-based events, select **DB**. Click **Apply**. A prompt appears from the EM to restart the database. The DB must be restarted for auditing configuration to take effect.

Step 7 Apply the change using the button at the top right of the page and log out of the EM.

Step 8 Since one of the following configuration parameters is not available through the Enterprise Management console (EM), both the EM and the database instance must be shutdown:

a Log in to the server using SSH or Telnet as the Oracle user.

b Shutdown the EM:

```
emctl stop dbconsole
```

c Stop the database by first connecting to the idle instance:

```
sqlplus / as sysdba
```

d Stop the database:

```
shutdown
```

e Create a text version of the spfile:

```
create pfile from spfile;
```

f Close sqlplus:

```
quit
```

Step 9 Open the init.ora file:

```
$ORACLE_HOME/dbs/init<instance-name>.ora
```

Where <instance name> is the instance of Oracle you wish to configure.

Step 10 Verify the audit_trail parameter is set to **OS**. Add the **audit_syslog_level** parameter and set it to the desired syslog facility and severity.

For example:

```
*.audit_trail='OS'
```

```
*.audit_syslog_level='local0.info'
```

Step 11 Open the /etc/syslog.conf and edit to direct the audit messages to the STRM host:

```
# oracle audit logs
```

```
local0.* @<host>
```

Where <host> is the IP address of the STRM Event Collector.

Step 12 Restart syslogd:

```
service syslog restart
```

Step 13 Re-create the spfile with the changes and start the database:

```
sqlplus / as sysdba
```

```
create spfile from pfile;
```

```
startup
```

```
quit
```

Step 14 Start EM:

```
emctl start dbconsole
```

Step 15 If you are using Oracle v9i, you must create a view, using SQLplus, to support STRM as follows:

```
CREATE VIEW qradar_audit_view AS SELECT
CAST(dba_audit_trail.timestamp AS TIMESTAMP) AS qradar_time,
dba_audit_trail.* FROM dba_audit_trail;
```

You are now ready to configure the sensor device within the STRM interface. If you are using the JDBC protocol, see the *Managing Sensor Devices Guide* for more information on configuring the JDBC protocol. When configuring the JDBC protocol within STRM (see the *Managing Sensor Devices Guide*), use the following specific parameters:

Table 65-2 Configuring Sensor Device Parameters

Parameter Name	Oracle v9i Value	Oracle v10g Value
Table Name	qradar_audit_view	dba_audit_trail
Select List	*	*
Compare Field	qradar_time	extended_timestamp



Note: Make sure that database user that STRM will use to query events from the audit log table has the appropriate permissions for the Table Name object.

To configure STRM to receive events from an Oracle Database, you must select the **Oracle RDBMS 9i/10g Audit Records** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

66

PROFTPD

STRM can collect events from a ProFTP server through syslog. By default, ProFTPD logs authentication related messages to the local syslog using the auth (or authpriv) facility. All other logging is done using the daemon facility. To log ProFTPD messages to STRM, use the SyslogFacility directive to change the default facility.

Before you configure STRM to integrate with a ProFTPD device, you must:

Step 1 Open the `/etc/proftd.conf` file.

Step 2 Below the LogFormat directives add the following:

```
SyslogFacility <facility>
```

Where `<facility>` is one of the following options: AUTH (or AUTHPRIV), CRON, DAEMON, KERN, LPR, MAIL, NEWS, USER, UUCP, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, or LOCAL7.

Step 3 Save the file and exit.

Step 4 Open the `/etc/syslog.conf` file

Step 5 Add the following line at the end of the file:

```
<facility> @<Host>
```

Where:

`<facility>` matches the facility chosen in [Step 2](#) (except in lower case).

`<Host>` is the IP address of the STRM Event Collector.

Step 6 Restart syslog and ProFTPD:

```
/etc/init.d/syslog restart
```

```
/etc/init.d/proftpd restart
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from an ProFTPD device, you must select the **ProFTPD server** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding ProFTPD, see your vendor documentation.

67

SECURE COMPUTING SIDEWINDER

A STRM Sidewinder DSM accepts Sidewinder events using syslog. STRM records and processes all Sidewinder events. Before you configure STRM to integrate with a Sidewinder device, you must configure syslog within your Sidewinder device. For more information on configuring Sidewinder, see your vendor documentation.



Note: When configuring the Sidewinder device to forward syslog to STRM, make sure that the logs are exported in **sef** format.

Once you configure syslog to forward events to STRM, you are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Sidewinder device, select **Sidewinder G2 Security Appliance** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

A STRM Sun Solaris DSM accepts Solaris authentication events using syslog. You can integrate Solaris version 5.8 with STRM. STRM records all relevant events. Before you configure STRM to integrate with a Solaris server, you must:

Step 1 Log in as root user.

Step 2 Open the `/etc/syslog.conf` file.

Step 3 Forward the system's authentication logs to STRM by adding the following line to the file:

```
*.err;auth.notice;auth.info @<IP address>
```

Where `<IP address>` is the IP address of the STRM system. Use tabs instead of spaces to format the line.



Note: Depending on the version of Solaris you are running, you may need to add additional log types to the file. Contact your system administrator for more information.

Step 4 Save and exit the file.

Step 5 Enter the following command:

```
kill -HUP `cat /etc/syslog.pid`
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Solaris device, select **Solaris Operating System Authentication Messages** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your Solaris, see your vendor documentation.

69

SUN SOLARIS DHCP

A STRM Sun Solaris DHCP DSM accepts Solaris DHCP events using syslog. STRM records all relevant events. Before you configure STRM to integrate with Solaris DHCP, you must:

Step 1 Log in as root.

Step 2 Open the `/etc/default/dhcp` file.

Step 3 Enable logging of DHCP transactions to syslog by adding the following line:

```
LOGGING_FACILITY=X
```

Where `x` is the number corresponding to a local syslog facility, for example, a number from 0 to 7.

Step 4 Save and exit the file.

Step 5 Open the `/etc/syslog.conf` file.

Step 6 Forward the system's authentication logs to STRM by adding the following line to the file:

```
localX.notice @<IP address>
```

Where:

`x` is the number chosen in [Step 3](#)

`<IP address>` is the IP address of the STRM system. Use tabs instead of spaces to format the line.

Step 7 Save and exit the file.

Step 8 Enter the following command:

```
kill -HUP `cat /etc/syslog.pid`
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Solaris device, select **Solaris Operating System DHCP Logs** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding Solaris, see your vendor documentation.

70

SONICWALL

A STRM SonicWALL UTM/Firewall/VPN Appliance DSM accepts events using syslog. STRM records all relevant events from SonicOS software. Before you configure STRM to integrate with a SonicWALL UTM/Firewall/VPN device, you must configure syslog within the appliance. For more information on configuring SonicWall, see your vendor documentation.

Once you configure syslog to forward events to STRM, you are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from your SonicWALL appliance, you must select the **SonicWALL UTM/Firewall/VPN Appliance** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

SUN SOLARIS SENDMAIL

A STRM Sun Solaris Sendmail DSM accepts Solaris authentication events using syslog. You can integrate Solaris Sendmail version 2.x with STRM. STRM records all relevant events. Before you configure STRM to integrate with Solaris Sendmail, you must:

Step 1 Log in as root user.

Step 2 Open the `/etc/syslog.conf` file.

Step 3 Forward the system's authentication logs to STRM by adding the following line to the file:

```
mail.*; @<IP address>
```

Where `<IP address>` is the IP address of the STRM system. Use tabs instead of spaces to format the line.



Note: Depending on the version of Solaris you are running, you may need to add additional log types to the file. Contact your system administrator for more information.

Step 4 Save and exit the file.

Step 5 Enter the following command:

```
kill -HUP `cat /etc/syslog.pid`
```

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Solaris device, select **Solaris Operating System Sendmail Logs** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your Solaris, see your vendor documentation.

SOURCEFIRE INTRUSION SENSOR

A STRM Sourcefire Intrusion Sensor DSM accepts Sourcefire events using syslog. You can integrate Sourcefire versions IS 500, 2.x, and 3.x with STRM. STRM records all relevant Sourcefire events. Before you configure STRM to integrate with a Sourcefire device, you must:

- Step 1** Log in to your Sourcefire interface.
- Step 2** In the main navigation menu, expand **Detection**.
- Step 3** Under Policy, click **Edit**.
- Step 4** In the list, select your active policy. Click **Edit**.
- Step 5** Click **Alerting**.
The selected policy settings appear.
- Step 6** For the State parameter, select the **On** option.
- Step 7** In the Logging Host field, enter the IP address of the STRM system hosting the Event Collector.
- Step 8** Click **Save**.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Sourcefire device, you must select the **Snort Open Source IDS** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

For more information regarding Sourcefire, see the Sourcefire documentation, see <http://www.sourcefire.com>

73

SQUID WEB PROXY

A STRM Squid Web Proxy DSM accepts events using syslog. STRM records all cache and access log events. Before you configure STRM to integrate with Squid Web Proxy, you must forward your cache and access logs to STRM.

To configure Squid to forward your logs using syslog:

Step 1 Log into the Squid device.

Step 2 Open the following file:

```
/etc/sysconfig/squid.conf
```

Step 3 Change the access_log configuration from:

```
access_log /usr/local/squid/var/logs/access.log
```

to

Squid Version Access Log Configuration

2.6.STABLE14 and earlier	<pre>access_log /usr/local/squid/var/logs/access.log syslog LOG_<FACILITY> LOG_<PRIORITY> squid</pre>
-----------------------------	---

Where:

FACILITY is any valid syslog facility (such as, AUTHPRIV, DAEMON, LOCAL0 to LOCAL7, or USER) written in uppercase.

PRIORITY any valid priority (such as, ERR, WARNING, NOTICE, INFO, DEBUG) written in uppercase.

For example:

```
access_log /usr/local/squid/var/logs/access.log  
syslog LOG_LOCAL4|LOG_INFO squid
```

Squid Version	Access Log Configuration
2.6.STABLE15 and later	<pre>access_log /usr/local/squid/var/logs/access.log syslog:<facility>:<priority> squid</pre> <p>Where:</p> <p>facility is any valid syslog facility (such as, authpriv, daemon, local0 to local7, or user)</p> <p>priority is any valid priority (such as, err, warning, notice, info, debug)</p> <p>For example:</p> <pre>access_log /usr/local/squid/var/logs/access.log syslog:local4:info squid</pre>

Step 4 Save and close the file.

Step 5 Enter the following command to restart the Squid daemon:

```
/etc/init.d/squid restart
```

Step 6 Open the following file:

```
/etc/syslog.conf
```

Step 7 Add the following line to send the logs to the STRM appliance:

```
<priority>.<facility> @<STRM_IP_address>
```

Where:

<priority> is the priority of your Squid messages

<facility> is the facility of your Squid messages

<STRM_IP_address> is the IP address or hostname of your STRM system

For example:

```
info.local4 @172.16.210.50
```

Step 8 Save the file

Step 9 Enter the following command to restart the syslog daemon:

```
/etc/init.d/syslog restart
```

For more information on configuring Squid Web Proxy, consult your vendor documentation.

Once you forward your cache and access logs to STRM, you are able to configure the sensor device within the STRM interface. To configure STRM to receive events from a Squid Web Proxy device, you must select the **Squid WebProxy** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

74

SYMANTEC SGS

A STRM Symantec Gateway Security (SGS) Appliance DSM accepts SGS events using syslog. STRM records all relevant events from SGS. Before you configure STRM to integrate with an SGS, you must configure syslog within your SGS appliance. For more information on Symantec SGS, see your vendor documentation.

Once you configure syslog to forward events to STRM, you are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from your SGS appliance, you must select the **Symantec Gateway Security (SGS) Appliance** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

75

TIPPING POINT UNITYONE

A STRM Tipping Point UnityOne DSM accepts Tipping Point events using syslog. STRM records all relevant events. Before you configure STRM to integrate with Tipping Point, you must:

- Step 1** Log in to the Tipping Point system.
- Step 2** In the Action Sets interface, **Open > Notification Contacts**.
- Step 3** Click **Remote System Log**.
- Step 4** In the Details/Edit window, enter the IP address and facility you wish to use.
- Step 5** Click **Add to table**.
- Step 6** Click **Save**.
- Step 7** Select tab as the delimiter.
- Step 8** Click **Apply**.

You must now select the actions for this device.

- Step 9** Click **Action Sets**.
- Step 10** Select the actions you wish this device to perform. Options include:
 - Block
 - Block, notify
 - Block, notify, trace
 - Notify, trace
 - Permit, notify
- Step 11** Select the check box to enable Remote System Log for each action you have selected.

This enables communication with STRM.

- Step 12** Click **Save**.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Tipping Point device, select

TippingPoint Intrusion Prevention System (IPS) from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your Tipping Point device, see your vendor documentation.

76

TIPPINGPOINT X505/X506 DEVICE

A STRM TippingPoint X505/X506 DSM accepts events using syslog. All information logged by the DSM can be delivered to a STRM server. Before configuring a TippingPoint X505/X506 device in STRM, you must configure your TippingPoint device to send syslog events to STRM. To configure the device to send system, audit, VPN, and firewall session log events to STRM:

- Step 1** Log into the Tipping Point X505/X506 device.
- Step 2** From the LSM menu, select **System > Configuration > Syslog Servers**.
The Syslog Servers window appears.
- Step 3** For each log type you want to deliver to STRM, select the check box and specify the IP address of your STRM system.



Note: Make sure that the TippingPoint X505/X506 can communicate with the STRM server on your network. If the server is on a different subnet than the IPS management port, you may have to add static routes. For more information, see the *X-Series Local Security Manager User Guide*.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a TippingPoint X505/X506 device, you must select the **TippingPoint X Series** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*.

77

TOPLAYER

A STRM Top Layer IPS DSM accepts Top Layer IPS events using syslog. STRM records and processes Top Layer events. Before you configure STRM to integrate with a Top Layer device, you must configure syslog within your Top Layer IPS device. For more information on configuring Top Layer, see your Top Layer documentation.

Once you configure syslog to forward events to STRM, you are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Top Layer IPS device, select **TopLayer Intrusion Prevention System (IPS)** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your Tipping Point device, see your vendor documentation.

78

TREND MICRO INTERSCAN VIRUSWALL

A STRM Trend Micro InterScan VirusWall DSM accepts events using syslog. You can integrate InterScan VirusWall logs with STRM using the STRM Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

To configure STRM to receive events from an InterScan VirusWall device, you must select the **Trend InterScan VirusWall** option from the Sensor Device Type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

For more information regarding your Trend Micro InterScan VirusWall device, see your vendor documentation.

79

TRIPWIRE

A STRM Tripwire DSM accepts resource additions, removal, and modification events using syslog. You can integrate Tripwire version 5.2 with STRM. Before you configure STRM to integrate with Tripwire, you must:

- Step 1** Log in to the Tripwire interface.
- Step 2** On the left-side of the window, click **Actions**.
- Step 3** Click **New Action**.
A wizard appears allowing you to configure the syslog action.
- Step 4** Configure the new action.
- Step 5** Select **Rules** and click on the desired rule you wish to monitor.
- Step 6** Select the **Actions** tab.
- Step 7** Make sure the new action is selected.
- Step 8** Click **Ok**.
- Step 9** Repeat Steps 5 to 8 for each rule you wish to monitor.

You are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from Tripwire device, select **Tripwire Enterprise** from the Sensor Device Type drop-down list box.

For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. For more information regarding your Tripwire device, see your vendor documentation.

A STRM Symantec System Center (SSC) DSM retrieves events from a SSC database using a custom STRM view. STRM records all SSC events. You must configure the SSC database with a user that has read and write privileges for the custom STRM view, which reports the correct information to STRM.

To integrate a SSC DSM with STRM, you must:

Step 1 In the SSC device, configure a custom default view to support STRM:



Note: *The database name must not contain any spaces.*

```
CREATE VIEW dbo.vw_qradar AS SELECT
    dbo.alerts.Idx AS idx,
    dbo.inventory.IP_Address AS ip,
    dbo.inventory.Computer AS computer_name,
    dbo.virus.Virusname AS virus_name,
    dbo.alerts.Filepath AS filepath,
    dbo.alerts.NoOfViruses AS no_of_virus,
    dbo.actualaction.Actualaction AS [action],
    dbo.alerts.Alertdatetime AS [date] FROM
    dbo.alerts INNER JOIN
    dbo.virus ON dbo.alerts.Virusname_Idx =
    dbo.virus.Virusname_Idx INNER JOIN
    dbo.inventory ON dbo.alerts.Computer_Idx =
    dbo.inventory.Computer_Idx INNER JOIN
    dbo.actualaction ON
    dbo.alerts.Actualaction_Idx =
    dbo.actualaction.Actualaction_Idx
```

Step 2 In the STRM interface, configure the JDBC protocol to interact with the created STRM custom view. The below window shows an example of the JDBC configuration in STRM.

For information on configuring the JDBC protocol, see the *Managing Sensor Devices Guide*.

Step 3 In the STRM interface, configure the sensor device.

To configure STRM to receive events from a SSC device, you must select the **Symantec System Center** option from the Sensor Device Type drop-down list box. For more information on configuring sensor devices, see the *Managing Sensor Devices Guide*. Make sure you select the JDBC source you created in [Step 2](#) when you configure the sensor device.

81

VERICEPT CONTENT 360 DSM

A STRM Vericept Content 360 DSM accepts Vericept events using syslog. STRM records all relevant and available information from the event. Before configuring a Vericept device in STRM, you must configure your device to send syslog to STRM. For more information on configuring your Vericept device, consult your vendor documentation.

Once you configure syslog to forward events to STRM, you are now ready to configure the sensor device within the STRM interface. To configure STRM to receive events from a Vericept device, you must select the **Vericept Content 360** option from the sensor device type drop-down list box. For more information on configuring devices, see the *Managing Sensor Devices Guide*.

