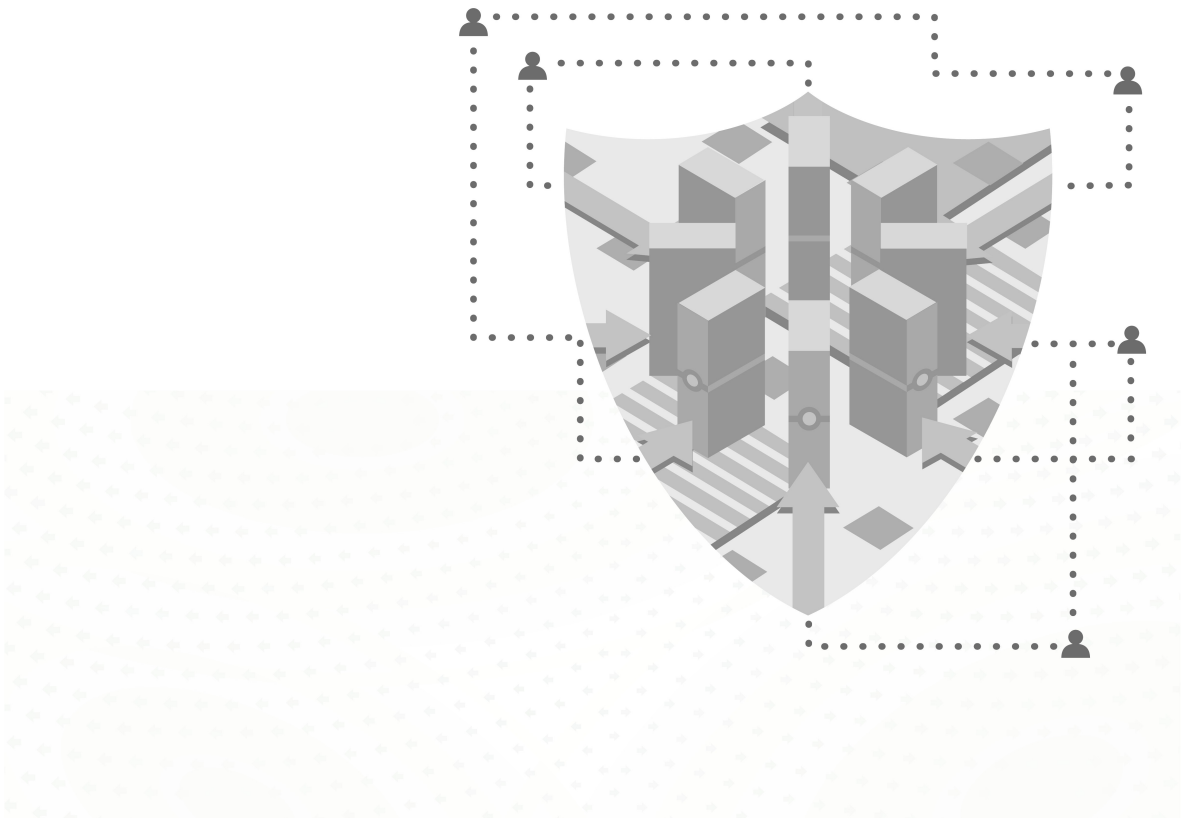
Sourcefire SSL Appliance Getting Started Guide for SSL1500, SSL2000, and SSL8200

Software version: 3.6



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

Table of Contents

Table of Contents

Chapter 1
Introduction to the Sourcefire SSL Appliances

This guide describes how to get started using the Sourcefire SSL Appliance 1500, also called the SSL1500; the Sourcefire SSL Appliance 2000, also called the SSL2000; or the Sourcefire SSL Appliance 8200, also called the SSL8200. It shows how to configure the minimum set of system options and provides basic examples showing how to configure the device to operate in two common modes. The *Sourcefire SSL Appliance Administration and Deployment Guide* provides full details on all of the options available in the SSL appliance and should be consulted for more complex configurations.

Components

Carefully unpack the Sourcefire SSL appliance and compare the actual contents with the Product Checklist to ensure that you have received all ordered components.

Product Checklist

Part	Description	Quantity
Sourcefire SSL1500 and SSL2000 or Sourcefire SSL Appliance 8200	1U rack-mountable device 2U rack-mountable device	1
2 x Power Cords	One for each redundant power supply	2
Rack-mounting rails	Rails to rack mount the device	2
Administration and Deployment Guide	On documentation CD	1
Getting Started Guide	Paper copy and on documentation CD	1
Release Notes	Downloadable PDF Document	1
Safety Notice	Single sheet safety notice	1

Documentation Conventions

The following conventions are used throughout this document.

IMPORTANT! A note provides additional information that may be of interest.

WARNING! A warning provides additional information that you need to pay attention to.

Throughout this document the term SSL is used to mean both SSL and TLS, unless explicitly indicated. Secure Socket Layer (SSL) has been largely replaced by Transport Layer Security (TLS) which is the more up-to-date standard derived

from SSL. Both SSL and TLS traffic are present in networks today and the Sourcefire SSL appliance is capable of inspecting both types of traffic.

IMPORTANT! The embedded software contained within the Sourcefire SSL Appliance 1500, SSL Appliance 2000, and SSL Appliance 8200 is subject to licensing terms and conditions imposed by Sourcefire and third party software providers. You should only use the SSL1500, SSL2000, or SSL8200 if you agree to these licensing conditions. See Licenses and Licensing Terms on page 46 for details of licensing terms and conditions.

IMPORTANT! The act of inspecting SSL traffic may be subject to corporate policy guidelines or national legislation. It is your responsibility to ensure that your use of the SSL appliance is in accordance with any such legal or policy requirements.

Chapter 2
Physical Installation

This section describes the following procedures:

- Installing the Sourcefire SSL appliance as a rack-mounted component.
- Connecting the Sourcefire SSL appliance to the network.

Safety Information

Follow the warnings and cautions listed in the Safety and Information chapter of the *Sourcefire SSL Appliance Administration and Deployment Guide* when installing or working with the SSL appliance.

WARNING! Read all the installation instructions before connecting the appliance to its power source. See the important safeguards in Safety and Information chapter of the *SSL Appliance Administration and Deployment Guide* for information regarding the setup and placement of the SSL appliance.

Requirements Checklist

The following will be required:

Requirements Checklist

SSL Appliance 1500	SSL Appliance 2000	SSL Appliance 8200
At least 1U rack space (deep enough for a 27″ device) – power and management ports at rear	At least 1U rack space (deep enough for a 27″ device) – power and management ports at rear	At least 2U rack space (deep enough for a 27″ device) – power and management ports at rear
Phillips (crosshead) screwdriver	Phillips (crosshead) screwdriver	Phillips (crosshead) screwdriver
Two available power outlets (110 VAC or 220-240 VAC)	Two available power outlets (110 VAC or 220-240 VAC)	Two available power outlets (110 VAC or 220-240 VAC)
Two IEC-320 power cords (that is, standard server / PC power cords) should the supplied power cords not be suitable for your environment	Two IEC-320 power cords (that is, standard server / PC power cords) should the supplied power cords not be suitable for your environment	Two IEC-320 power cords (that is, standard server / PC power cords) should the supplied power cords not be suitable for your environment
Cooling for an appliance with two 450W power supply units	Cooling for an appliance with two 650W power supply units	Cooling for an appliance with two 750W power supply units
One RJ-45 CAT5e/CAT6 Ethernet cable to connect the SSL Appliance 1500 to the management network (or a local notebook / desktop computer which is used to manage the SSL Appliance 1500)	One RJ-45 CAT5e/CAT6 Ethernet cable to connect the SSL Appliance 2000 to the management network (or a local notebook / desktop computer which is used to manage the SSL Appliance 2000)	One RJ-45 CAT5e/CAT6 Ethernet cable to connect the SSL Appliance 8200 to the management network (or a local notebook / desktop computer which is used to manage the SSL Appliance 8200)
Appropriate copper or fiber cables to connect SSL Appliance 1500 to the network and to associated security appliances	Appropriate copper or fiber cables to connect NetMods to the network and to associated security appliances	Appropriate copper or fiber cables to connect NetMods to the network and to associated security appliances

Rack Mounting

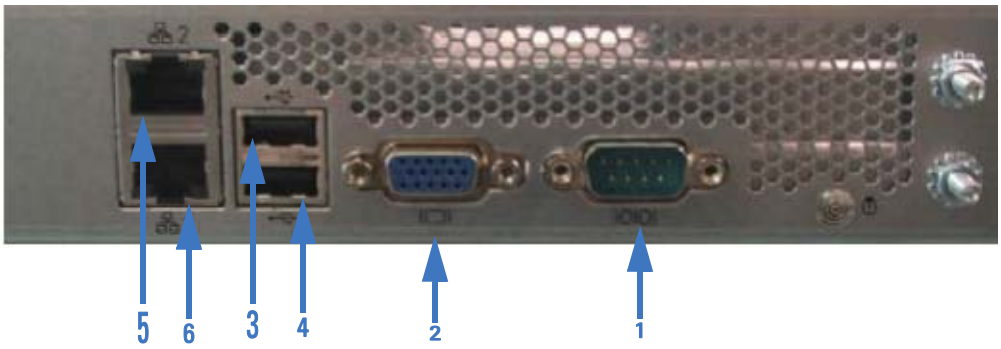
The SSL appliance is equipped with installed rack mount brackets and supplied with rack mount rails allowing easy installation in a rack.

Rear

The rear of the SSL Appliance 1500 is shown below. Ventilation holes on the rear panel must not be blocked because free flow of air is essential for system cooling.

Two M4x15mm lugs are provided on the rear panel to allow connection of the chassis to earth ground.

SSL1500 Back Panel

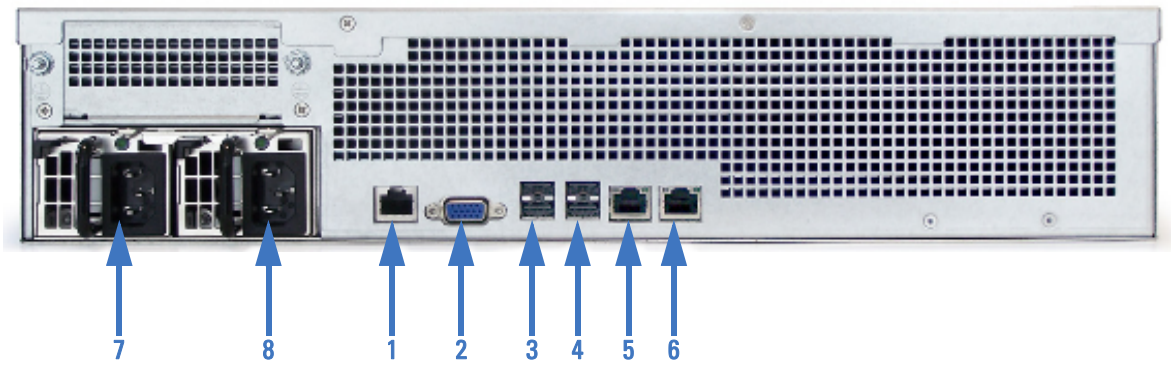


The rear of the SSL Appliance 2000 is shown below. Ventilation holes on the rear panel must not be blocked because free flow of air is essential for system cooling.

SSL2000 Back Panel

The rear of the SSL Appliance 8200 is shown below. Ventilation holes on the rear panel must not be blocked because free flow of air is essential for system cooling.

SSL8200 Back Panel



SSL1500, SSL2000, or SSL8200 Back Panel Components

1	Serial Port	5	Management Ethernet 1
2	VGA Display Connector	6	Management Ethernet 2
3	USB Port	7	Power Supply 1
4	USB Port	8	Power Supply 2

The SSL appliance is equipped with two independent power supply units, either of which can power the appliance. The power supply units feature IEC-320 (that is, standard server / PC style) connectors. Attach both units to an uninterruptible power supply or other power outlet (110 or 220/240 Volt AC).

Power supplies have a bi-color LED indicator. The following table shows the conditions indicated by the LEDS:

Power Supply Status Indicator

Color	State	Meaning
Green	Blink	AC connected but not turned on - Standby
Green	Solid	Powered on and working fine
Red	Blink	AC not connected
Red	Solid	Indicates a fault condition

IMPORTANT! The power supplies are hot-swappable and can be replaced while the SSL appliance is powered on and operating.

WARNING! Use only replacement units supplied by Sourcefire, Inc. Use of other units will void any warranty and may damage the system.

Front Panel

The SSL Appliance 1500 comes configured with eight copper or fiber interfaces.

The SSL Appliance 2000 and SSL Appliance 8200 have modular I/O bays that allow for flexibility in the number of network interfaces and the type of media supported. Network I/O Modules (NetMods) are installed in the bays to configure the desired combination of interfaces. 10Gig and GigE NetMods cannot be mixed in an SSL appliance chassis, so a device may either have GigE NetMods or 10Gig NetMods. There are three front-facing modular I/O bays in the SSL Appliance 2000. There are seven front-facing modular I/O bays in the SSL Appliance 8200. Available NetMod options are listed below; other NetMod types may become available in the future:

- 4 x GigE copper (4 ports of 10/100/1000Base-T with bypass)
- 4 x GigE fiber (4 ports of 10/100/1000Base-SX with bypass)
- 2 x 10Gig fiber (2 ports of 10GBase-SR with bypass)
- 2 x 10Gig fiber (2 ports of 10GBase-LR with bypass)

WARNING! The software supports a maximum of sixteen external interfaces. If 4 x GigE NetMods are used, a maximum of four can be installed in the system.

The image below is of an SSL Appliance 8200 with four NetMods installed, two 4 x GigE fiber interfaces, and two 4 x GigE copper interfaces.

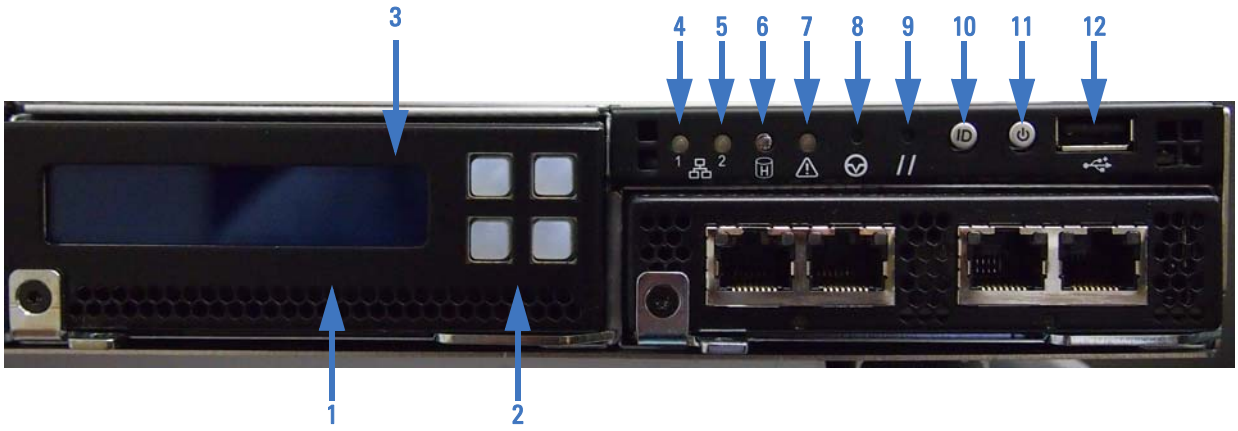
SSL Appliance 8200 Front View

NetMods and the switch module installed in the front facing bays of the SSL appliance are NOT hot-swappable and are not user-replaceable items. **Do not** attempt to remove or insert NetMods or switch modules. Insertion or replacement of NetMods and switch modules should only be carried out by trained service personnel and should only be done when the system is powered off.

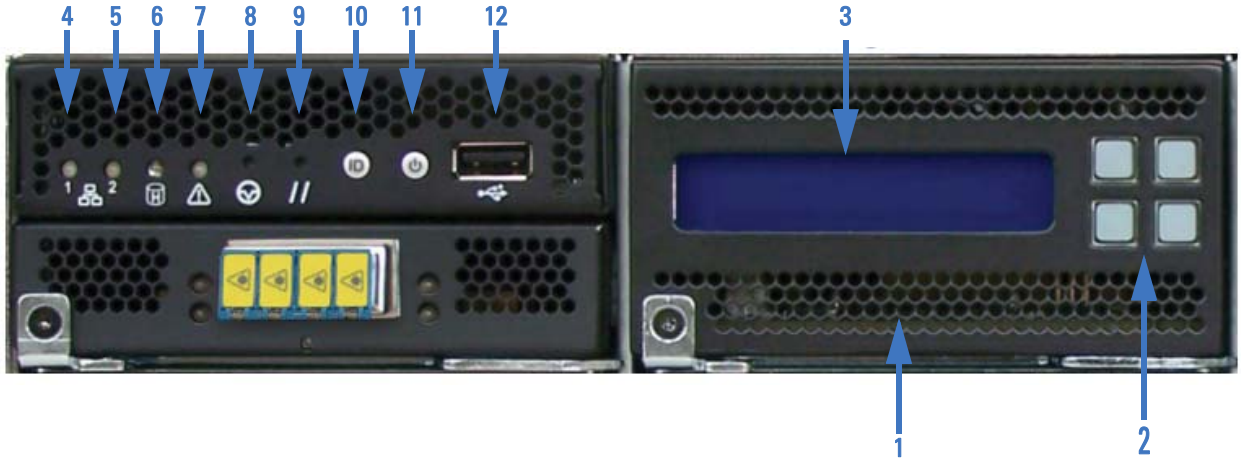
The front panel has indicators, buttons, an LCD display, and a USB port that the administrator can use to configure and diagnose the system. The relevant portion of the front panel is shown in the following illustration and the Front Panel Components table identifies the components.

SSL1500 Front Panel Components

SSL2000 Front Panel Components



SSL8200 Front Panel Components



Front Panel Components

1	Switch Module	7	System Status Indicator
2	Keypad Array	8	NMI Button (recessed)
3	LCD Display	9	Reset Button (recessed)

Front Panel Components (Continued)

4	Management Ethernet 1 Indicator	10	Identify Button
5	Management Ethernet 2 Indicator	11	Power Button
6	Disk Activity Indicator	12	USB socket

The front panel status LEDs for the management Ethernet ports are green when the link is up and flash amber/yellow to indicate traffic flowing over the link. The two LEDs that are part of the Ethernet ports on the rear panel indicate the operating speed of the link and if data is flowing over the link. The left LED viewed from the back of the unit is green if the link is up and flashes to indicate traffic flow. The right LED can be: off, indicating a 10Mbps connection; green, indicating a 100Mbps connection; or amber, indicating a GigE connection.

The disk activity LED is green and flashes when there is any disk activity on a SATA port in the system.

The system status LED is green/amber and the various display options indicated different system states.

The System Status Indicator Meaning for SSL1500 table shows the various system states that can be indicated by the system status LED on the front panel of the SSL Appliance 1500.

System Status Indicator Meaning for SSL1500

Color	State	System Status	Meaning
None	Off	OK	System ready - no errors detected
Red	Solid	Fault	AC power supply failure No AC power cord present Absence of AC power supply module

The System Status Indicator Meaning for SSL2000 and SSL8200 table shows the various system states that can be indicated by the system status LED on the front panel of the unit.

System Status Indicator Meaning for SSL2000 and SSL8200

Color	State	System Status	Meaning
Green	Solid	OK	System ready - no errors detected
Green	Blink	Degraded	Memory, fan, power supply or PCIe failures
Amber	Solid	Fatal	Alarm – system has failed and shut down
Amber	Blink	Non-Fatal	Alarm – system likely to fail – voltage/temp warnings
Green + Amber	Solid	OK	First 30 seconds after AC power connected
None	Off	Power Off	AC or DC power is off

On the SSL Appliance 2000 and SSL Appliance 8200, the NMI and Reset buttons are recessed, requiring the use of a straight thin object to press the button. Pressing the Reset button will cause the system to be reset. The NMI button should not be pressed during normal operation because it may cause the system to halt. If the NMI button is pressed, this fact will be recorded in the system log file.

If you press the ID button, a blue LED on the rear panel to the left of the serial port illuminates. This LED is located behind the back panel and is visible through the ventilation holes. This LED makes it easier to locate a system when it is racked with other systems.

Connecting to the Management Network

The WebUI management interface is accessed via Management Ethernet 1. Plug a cable into the ethernet port identified as Management Ethernet 1 on page 11. Check that the LEDs on the port indicate that the link is up.

Connecting to the Network and Attached Appliance

The SSL Appliance 1500 has eight front facing copper or fiber interfaces. The image below shows an SSL Appliance 1500 with eight copper interfaces.

SSL Appliance 1500 with copper interfaces

Ports are numbered from left to right when facing the front of the device. When a segment is configured and activated the port numbers allocated to that segment are displayed on the management WebUI. The relevant ports will need to be connected to the network and associated security appliance(s) using appropriate copper or fiber cabling.

LEDs at the top of the socket, the left LED indicates link status and the right indicates link activity. The left LED can be: off indicating no connection, green indicating a 1000Mbps connection or amber indicating a GigE connection.

Below each pair of interfaces is a Fail-To-Wire (FTW) status LED that indicates the current FTW status for that pair of interfaces.

Fail-To-Wire Status

Color	State	FTW Status
None	Off	Active State
Green	Solid	Active State with armed watchdog
Amber	Solid	Commanded FTW state change
Amber	Flashing	Forced FTW

The image below shows an SSL Appliance 1500 with eight fiber interfaces.

SSL Appliance 1500 with fiber interfaces

Each fiber interface has two LEDs arranged vertically. The top LED indicates link activity and the bottom LED indicates link state. Link state can be off meaning no link is established or solid green indicating a 1000Mbps link is established.

Each pair of fiber ports has a FTW indicated LED that indicates FTW status as shown above.

IMPORTANT! Pairs of ports share fail-to-wire hardware that is used to directly connect the two ports together whenever the port pair are in Fail-To-Wire (FTW) mode. If the box is powered off then all ports will be in FTW mode so each pair of ports will be connected to each other.

Ports are numbered from left to right when facing the front of the SSL Appliance 2000, and left to right and top to bottom when facing the front of the SSL Appliance 8200. When a segment is configured and activated the port numbers allocated to that segment are displayed on the management WebUI. The relevant ports will need to be connected to the network and associated security appliances using appropriate copper or fiber cabling.

Chapter 3
Power On and Initial Configuration

Ensure that the two power supplies are connected to power using appropriate cabling. To turn the unit on, press the front panel power button which is shown on SSL1500 Front Panel Components on page 13, SSL2000 Front Panel Components on page 14, or SSL8200 Front Panel Components on page 14. If all is well the System Status Indicator will be solid green and, after a minute or so, the LCD display will illuminate and display a message similar to that in the following graphic.

Initial LCD Display after Power On

The initial screen will appear for a while and then the LCD will blank before displaying the message shown in the following graphic.

Power On Message - Detecting HD

Power On Message - Failsafe Indication

After the system has detected the SSD and the Disk on Module, it will boot from the SSD and displays the message shown in the following graphic.

Power On Message - Booting HD

Once the system has booted, the display changes to indicate the keypad is now active and can be used to access menu options. The following graphic shows the display with an arrow at the bottom right of the display indicating that the bottom right button on the keypad is active.

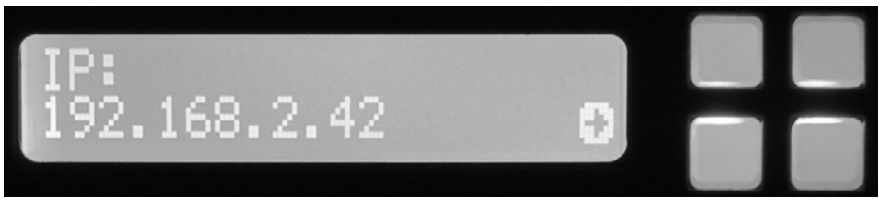
Power On Display - Menu Active

Press the bottom right button to display the IP address of the system. The following graphic shows the message displayed while an address is being acquired with DHCP.

Power On Display - Acquiring IP Address

The following graphic shows the display once the address has been acquired.

Power On Display - IP Address Acquired



Take a note of the IP address as this will be needed to access the WebUI in order to continue setting up the device. Refer to the *Administration Guide* for details of how to configure an IP address if the management network is not using DHCP.

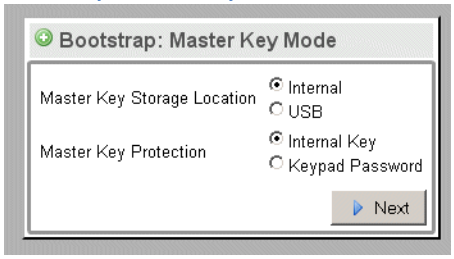
Chapter 4
System Bootstrap Phase

If the basic system information has not been configured the device will enter the *bootstrap* phase when powered on. To enter the minimum necessary information required by the system before it will exit the bootstrap mode, a connection is required to the WebUI. Using a web browser, open a session to the IP address that is being used by the SSL appliance. In this example, the IP address is `192.168.2.42`, so accessing the following URL will connect to the WebUI.

```
https://192.168.2.42
```

The first step is shown in the following graphic and only occurs if the master key mode is not already configured. This allows configuration of where the Master Key for the SSL appliance is to be stored and whether or not it is password protected. In this example the default options are used so there is no password required and the master key is stored internally. Simply click on the Next button to continue configuring the device.

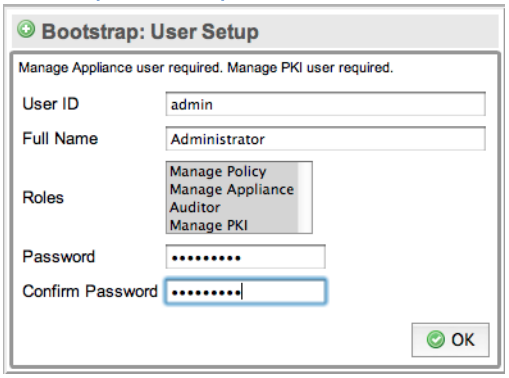
Bootstrap Master Key Mode



The final stage of the bootstrap process is user setup. At least one user with the Manage Appliance role and at least one user with the Manage PKI role must be

created – it can be one user with both roles, or two users. As soon as the users are created, the system will exit bootstrap mode.

Bootstrap User Setup



IMPORTANT! If the system has previously been configured and already has at least one user with the Manage Appliance role and one with the Manage PKI role then this step will be skipped.

Chapter 5
Completing System Configuration

The following common steps are done once the system is out of the bootstrap phase. An HTTPS connection to the IP address assigned to the SSL appliance management interface will produce the standard login box.

IMPORTANT! The SSL appliance uses a self-signed SSL server certificate which may result in a warning message from the browser when connecting to the WebUI. The warning can be prevented by adding this self signed certificate to your browser as a trusted device. Consult your browser documentation for details on how to add the SSL appliance as a trusted device.

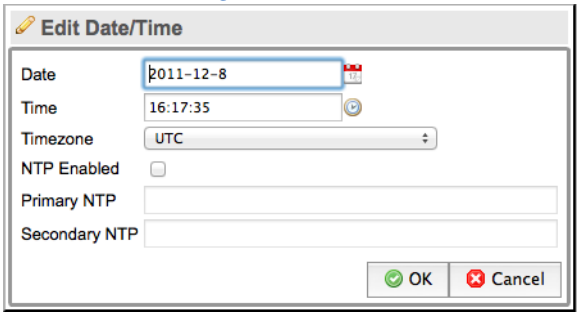
Login Box on the Initial Access Screen

Configuring the Date and Time

To configure the system date and time use the **Date/Time** option on the Device menu. Initially, the Device menu is labeled `localhost.localdomain`. Click the

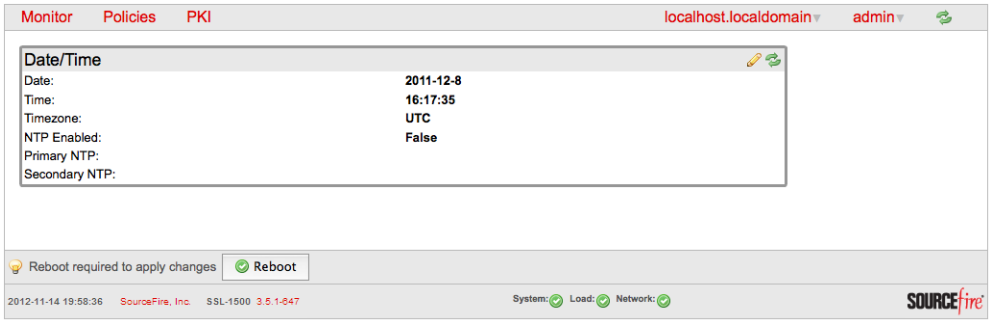
pencil icon at the top right of the Date/Time box to edit these settings. The following graphic shows the edit screen and settings that can be changed.

Date and Time Configuration



If NTP is enabled, as in this example, the Data and Time input boxes will be disabled. These values are set by the Network Time Protocol (NTP). To use NTP to operate, you must configure a primary NTP server and, ideally, a secondary NTP server. After the settings are configured, click **OK** to save the settings. The following graphic shows the updated Date/Time box.

Time Settings with the Reboot Button



To change the time, click **Reboot**. This reboots the system.

Chapter 6
Configuring PKI Details

The two example inspection configurations provided later in the document make use of a known server key and certificate that needs to be loaded into the SSL appliance and use certificate re-sign, which requires that the SSL appliance has a CA certificate. This section details how to set up these certificates on the system. It is assumed that a local SSL server is available and that a copy of the private key and SSL server certificate are available.

Installing a CA for Certificate Re-Sign

Before the SSL appliance can be used to inspect traffic using Certificate Re-sign mechanisms the SSL appliance must have at least one CA certificate and private key installed for the re-signing. A CA can either be created by the SSL appliance (and self-signed or sent off for signing by another CA) or can be imported. If the SSL appliance has more than one CA for re-sign installed, it is possible to use different CAs to re-sign different SSL sessions by choosing the appropriate CA in the policy configuration. Management of Internal Certificate Authorities is done using the menu option on the PKI menu. The following graphic shows the screen when there are no Internal Certificate Authorities in the system.

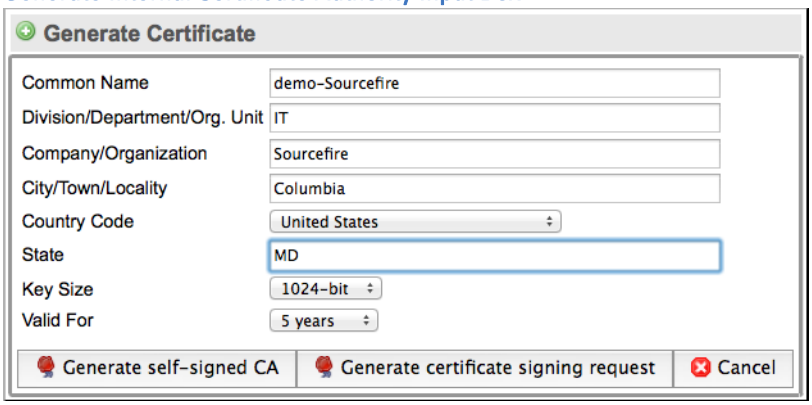
Internal Certificate Authority Screen with no Entries

The icons at the top right allow the user to:

- Generate a new Internal Certificate Authority
- Add an Internal Certificate Authority by importing an existing CA and key

The simplest approach is to generate an internal self signed CA certificate. Clicking on the icon to generate a CA will produce the input form shown in the following graphic.

Generate Internal Certificate Authority Input Box



This allows the basic data required in a CA to be input and the key size and validity period to be specified.

Because this CA is self-signed it will not be trusted by client systems until it has been exported and added to the list of trusted CAs on the client system. When the **OK** button is clicked, the certificate is saved and installed and an entry in the Internal Certificate Authorities table appears with an indication that no CSR has been generated for this certificate. To download the CA certificate so you can install it on the client system, click to select the entry and then click on the export certificate button. Consult your browser documentation for details on how to add this CA to the browsers list of trusted CAs.

Importing Known Server Keys

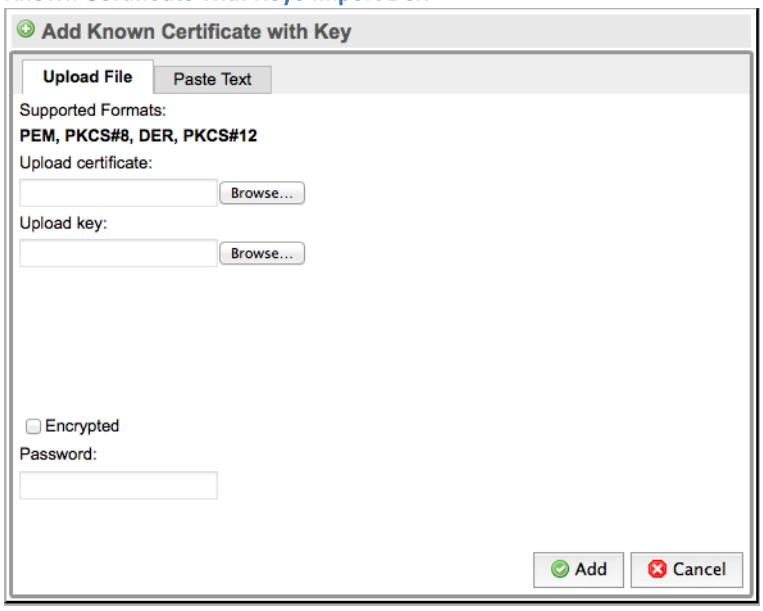
To inspect traffic to an internal SSL server, the easiest approach is to use a known server mode which requires that a copy of the server's SSL certificate and private key, or just the private key, are loaded into the SSL appliance. Known server certificates and keys are imported into the `all-known-certificates-with-keys` list or the `all-known-keys` list and can then be copied to custom lists, if required. Use the **Known Certificates and Keys** option on the **PKI** menu to import new certificates and keys. The **Known Keys List** option on the **PKI** menu is used to import new keys.

There are two input forms provided: one chooses the list that is to be operated on, and the other manipulates the contents of that list. Initially, there is only one list called `all-known-certificates-with-keys`, and it will not contain any certificates. In this example the key/certificate will be added to the `all-known-certificates-with-keys` list. The following graphic shows the initial appearance of the input forms.

Known Certificate with Keys Display

Click to select the **all-known-certificates-with-keys** list and then click **Add**. The following graphic shows the input form that will appear.

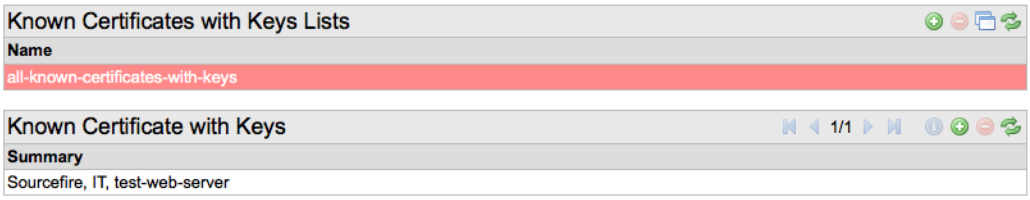
Known Certificate with Keys Import Box



You can either specify the files to import, or paste in the key and certificate details and click **Add**. If the key and certificate are valid, a message confirming that the Certificate has been added appears with a button that allows you to view the details of the imported certificate. The key now appears as a row in the Known Certificate with Keys form.

The following graphic shows the screen after a number of keys have been imported and shows the **Apply** button that needs to be used to save the imported certificates and keys to the secure store.

Known Certificate and Keys Display with Entries



Load the key/certificate for each local SSL server that you wish to inspect traffic to.

Chapter 7
Example Passive-Tap Mode Inspection

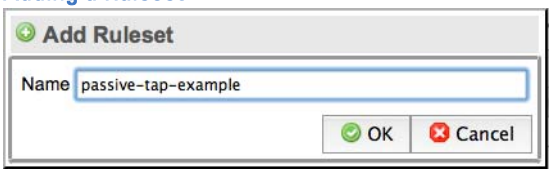
The following example shows the steps needed to configure the SSL appliance to inspect traffic that is intended for a server where you can obtain a copy of the private key and certificate and with the SSL appliance connected in passive-tap mode. The simplest passive-tap configuration is one port on the SSL appliance which receives a copy of network traffic from a network tap device and one port on the SSL appliance that sends traffic to the attached security appliance.

The steps involved are:

1. Load the server key/certificate into the SSL appliance.
2. Create a ruleset that contains a rule to inspect traffic to the server.
3. Create a segment for passive-tap operation.
4. Activate the segment to start inspection.

Creating a ruleset is a two-step process. First, create the ruleset to hold the rule. Next, define the rule itself. The following graphic shows the screen while adding a new ruleset called `passive-tap-example`.

Adding a Ruleset

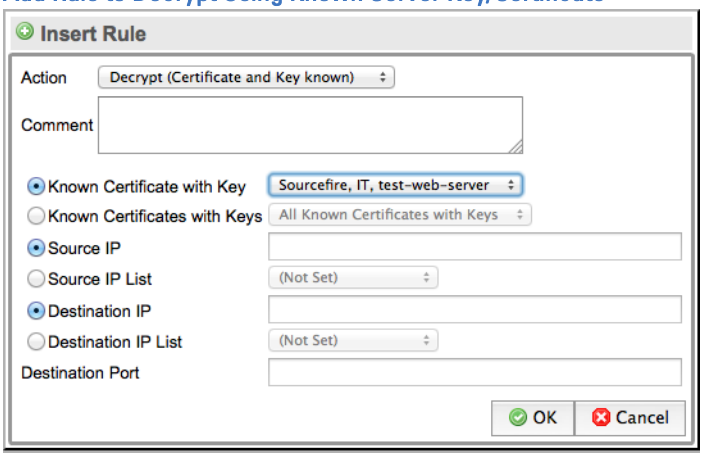


After clicking **OK,** the new entry will appear as a row in the Rulesets grid and is available for use. A Policy Changes notification block with buttons to apply or cancel the change appears at the bottom of the screen. Click **Apply** to complete the process and to save the ruleset to disk.

Now select the `passive-tap-example`. This will cause the Ruleset Options for this ruleset to be displayed. In this example the default settings are fine.

The Rules panel will also appear when the ruleset row is selected. Click **Add** in the Rules grid section to display the Insert Rule form. Selecting **Decrypt (Certificate and Key known)** from the drop-down menu in this form will allow the valid options to be configured for this rule.

Add Rule to Decrypt Using Known Server Key/Certificate



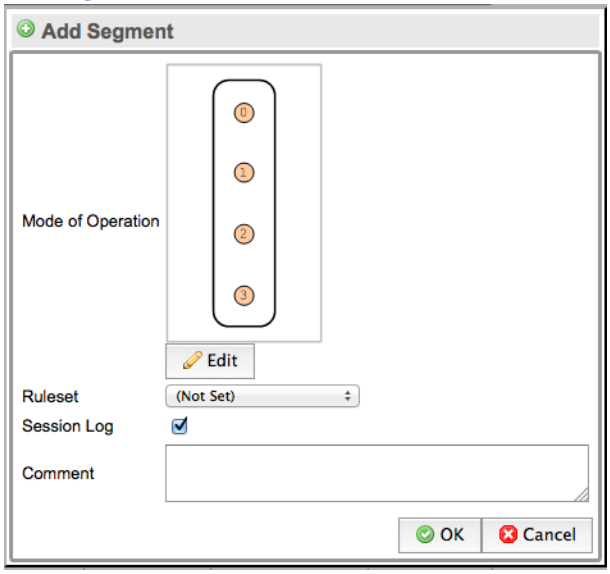
In this example, the rule applies only to a single server for which the certificate and key are known. The **Known Certificate with Key** option is checked and the system with the loaded key is selected from the drop-down menu. You can add a comment to the Comment box, but no other options are used in this rule. Click **Save** to create the rule. At the bottom of the screen is the Policy Changes notification block with buttons to apply or cancel the change. Click **Apply** to complete the process and to save the rule to disk.

The above rule inspects all SSL traffic passing through the appliance. By specifying a particular Subject DN (server Common Name) or a list that contains multiple Subject DNs a rule only inspects traffic going to particular SSL servers. When specifying the Subject DN, you can use a wildcard `*` at the start of the name. For example, a Subject DN value of `*company.com` matches the server certificates from servers such as `mail.company.com`, `server1.company.com`, and so on.

The final part of the process is to create a segment, configure the segment to use the ruleset just created, and then activate the segment. To create a segment, go to the **Policies / Segments** menu option for the Segments information. Initially there

are no segments configured in the system. To create a new segment, click **Add** in the Segments table. The following graphic shows the initial form.

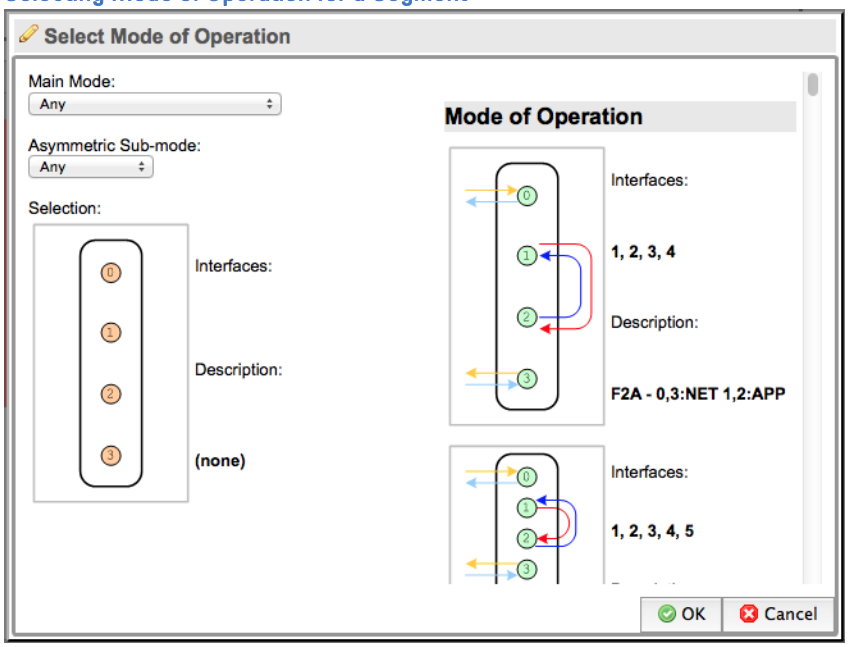
Add Segment Box



Click **Edit** to select the Mode of Operation for the required mode and then choose from the **Select Mode of Operation**. Choose the Ruleset from the drop-down menu.

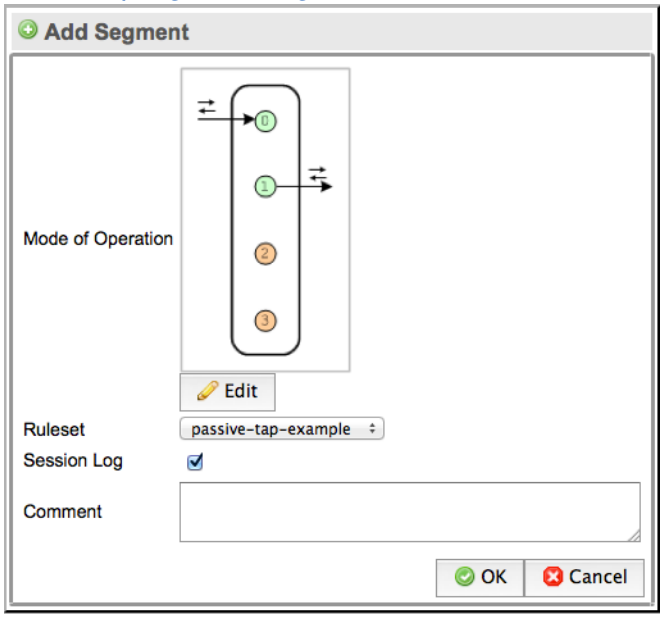
The following graphic shows the form used to select the mode of operation for a segment.

Selecting Mode of Operation for a Segment



The Mode of Operation part of the form has a scroll bar and displays all the different operating modes as images. The **Main Mode** drop-down menu allows the set of operating modes to be narrowed by choosing only `passive-tap` for example. This will reduce the number of options displayed in the Mode of Operations part of the form. The **Asymmetric Sub-Mode** drop-down menu can further narrow the number of modes of operation that are displayed. Click on the image for the desired operating mode to select it and click **Save** to set this as the mode of operation for the segment. The following graphic shows the completed segment details before they are saved.

Passive-Tap Segment Configuration



In this example, the session log has been enabled and the segment is using the `passive-tap-example` ruleset created earlier in the process. The graphic in the input box indicates that this segment will use two ports on the system. The actual ports used are determined when the segment is activated.

Click **OK** to create the segment. A Policy Changes notification block with buttons to apply or cancel the change will appear at the bottom of the screen. Click **Apply** to complete the process and to save the rule to disk.

The created segment is displayed in the Segments table and, as shown in the following graphic. Click on the segment to select it.

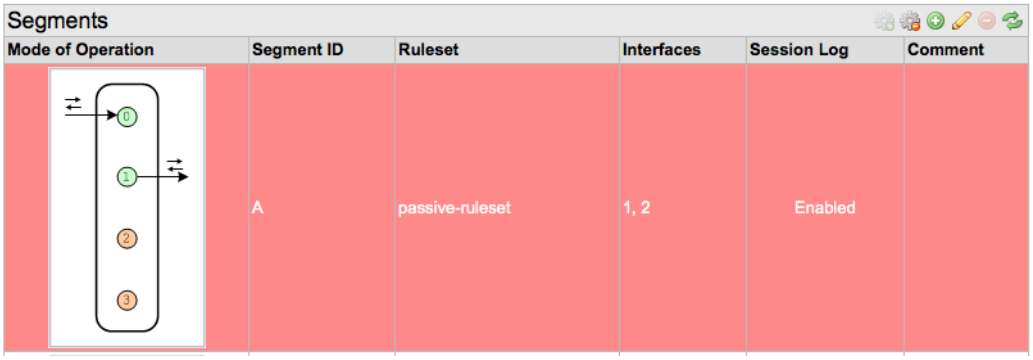
Passive-Tap Segment Options and Activations

There are three panels below the Segment panel in this table, each of which allows different types of actions to be configured for the selected segment. In this example, the default values are OK, so there is no need for further editing.

The Interface column in the Segment does not shows interface numbers. These are allocated when the segment is activated. Activation is done by clicking Activate for the segment, which is in the tool block at the top right of the segment panel. During the activation process you can select the ports that for the segment, any copy ports, and the modes for the copy ports.

The following graphic shows these interface numbers which indicate how the device should be wired up to the network.

Passive-Tap Segment Activated



In this example:

- Port 1 connects to the network tap device that is feeding traffic to the SSL appliance
- Port 2 connects to the first passive security appliance

The red background indicates that the segment is not activated. If there is SSL traffic to the server then the SSL session log and SSL statistics screens should show this.

Chapter 8
Example Active-Inline Mode Inspection

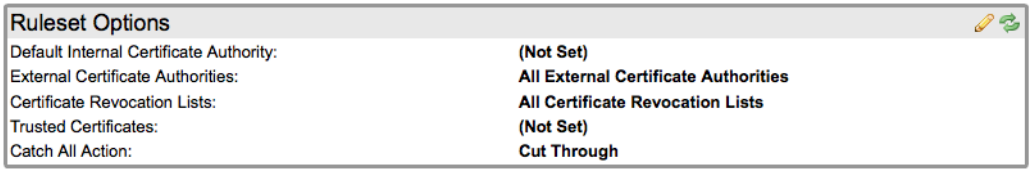
The following example shows the steps needed to configure the SSL appliance to inspect traffic and to pass the inspected traffic through an active-inline security appliance. In this example, the SSL appliance is deployed in active-inline mode and has an inline security appliance such as an IPS attached. The configuration described below uses four network ports on the SSL appliance. The steps involved are:

1. Create or load an Internal CA certificate and key into the SSL appliance.
2. Create a ruleset that contains a rule to inspect traffic using certificate re-sign.
3. Add a segment for active-inline operation.
4. Activate the segment to start inspection.

Creating a ruleset is a two-step process and is explained in Adding a Ruleset on page 30. In this example, the ruleset is called `active-inline-example`. After creating the ruleset name, click **OK**, and the new entry will appear as a row in the Rulesets panel. At the bottom of the screen is a Policy Changes notification block with buttons to apply or cancel the change. Click **Apply** to complete the process and to save the ruleset to disk.

Now click on the `active-inline-example` row to select it. This will display the Ruleset Options, as shown in the following graphic.

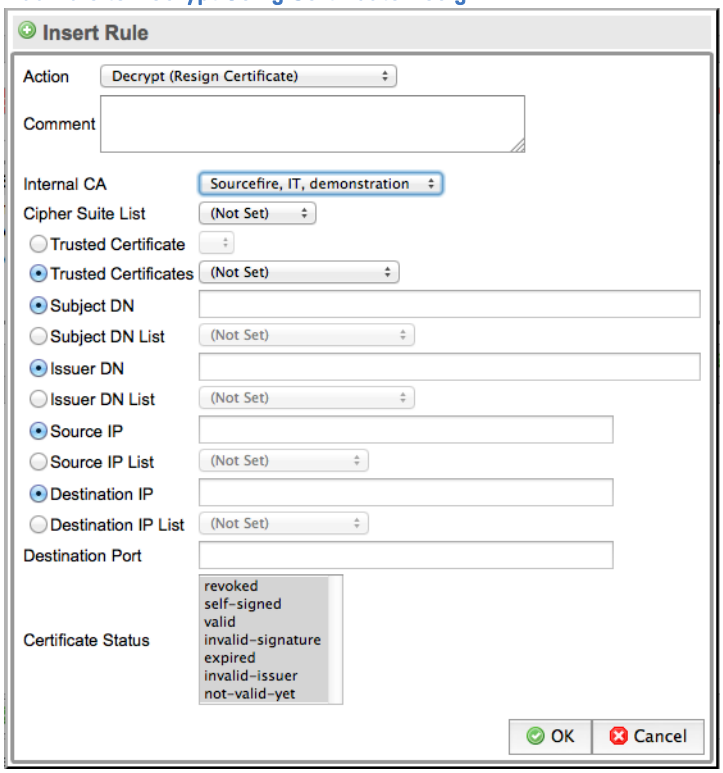
Active-Inline Ruleset Options



Click the edit tool and change the Trusted Certificates setting to All Trusted Certificates.

The Rules panel will also appear when the ruleset row is selected. Clicking on the **Add** button will cause the Insert Rule form to appear.

Add Rule to Decrypt Using Certificate Resign



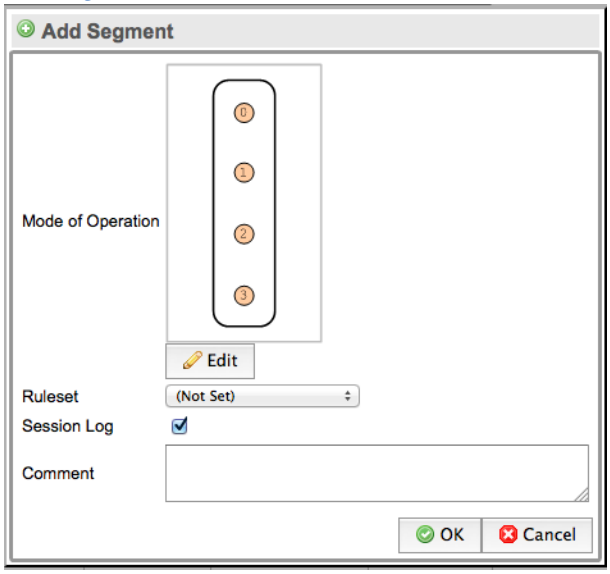
Select **Decrypt (Resign Certificate)** on the drop-down menu in this form to configure a rule. In this example the rule applies to all SSL sessions that pass through the SSL appliance. The *Administration Guide* provides more details on the options available when creating a rule and how they can be used to create specific rules that only apply to traffic to particular destinations.

Apart from adding a comment to the Comment box no other options are used in this rule so click the **Save** button to create the rule. At the bottom of the screen is a Policy Changes notification block with buttons to apply or cancel the change. Click **Apply** to complete the process and to save the rule to disk.

The final part of the process is to create a segment, configure it to use the ruleset just created, and activate it. To create a segment go to the **Policies / Segments** menu option and you will see the Segments panel. Initially there will be no

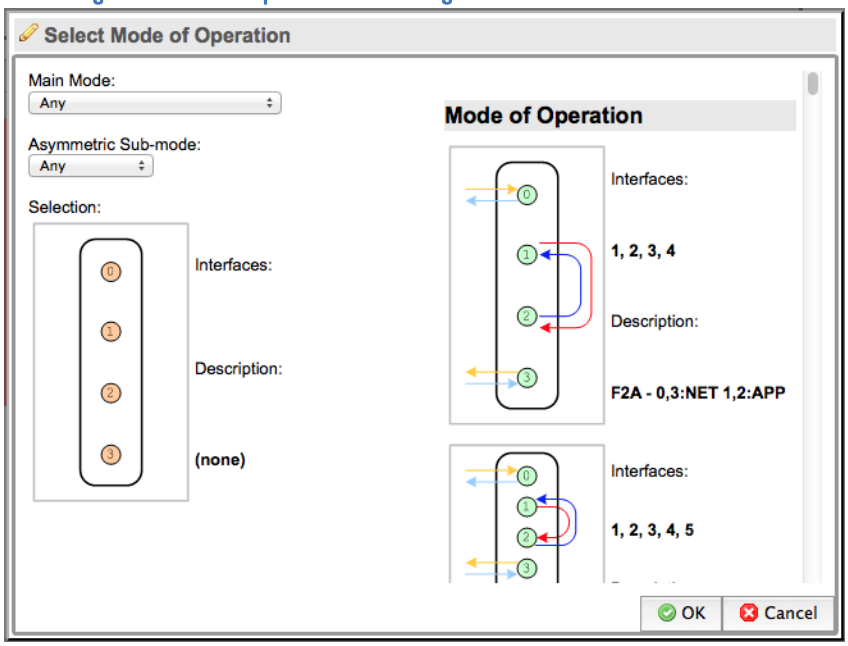
segments configured in the system. Click **Add** in the Segments panel to create a new segment. The following graphic shows the initial form.

Add Segment Box



Select the Mode of Operation by clicking on **Edit** button and then choosing from the Select Mode of Operation from the required mode. Chose the Ruleset from the drop-down menu. The following graphic shows the form used to select the mode of operation for a segment.

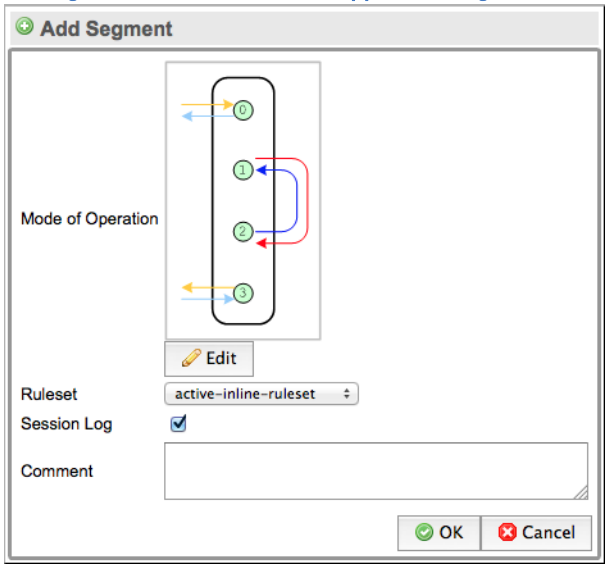
Selecting the Mode of Operation for a Segment



The Mode of Operation part of the form has a scroll bar and displays all the different operating modes as images. The Main Mode drop-down menu allows the set of operating modes to be narrowed by choosing only `Active-Inline`. This will reduce the number of options displayed in the Mode of Operations part of the form. Click on the image for the desired operating mode to select it, and click **Save** to set this as the mode of operation for the segment.

The following graphic shows the completed segment details before they are saved.

Adding an Active-Inline Fail To Appliance Segment



In this example, the session log is enabled and the segment is using the `active-inline-example` ruleset created earlier. The graphic in the input box indicates that this segment uses four ports on the system. The actual port numbers are determined when the segment is activated.

Click **OK** to create the segment. At the bottom of the screen is a Policy Changes notification block with buttons to apply or cancel the change. Click **Apply** to complete the process and save the configuration to disk.

Select the segment in the Segments table. There are three panels below the Segment panel in this table, each of which allow different types of actions for the selected segment. In this example the default values are OK so there is no need for further editing.

The Interface column in the Segment does not shows interface numbers. These are allocated when the segment is activated. Click the **Activate** button for the segment, which is in the tool block at the top right of the segment panel to activate the segment.

The following graphic shows these interface numbers which indicate how the device should be wired up to the network.

Active-Inline Segment Activated

In this example:

- Port 3 connects to the network where the SSL appliance is a bump-in-the-wire.
- Port 4 connects to the active security appliance.
- Port 5 connects to the active security appliance.
- Port 6 connects to the network where the SSL appliance is a bump-in-the-wire.

The red background indicates that the segment is not activated. If there is SSL traffic to the server, then the SSL session log and SSL statistics screens will show this. Both of these options are under the **Monitor** menu.

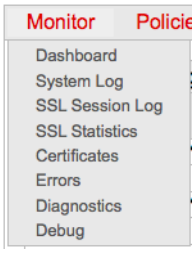
Chapter 9
Monitoring the System

The Monitor menu contains eight options that provide details on the operation of the system and that allow the collection of diagnostic and debug information. Only the Dashboard, SSL Session Log, and SSL Statistics are described in this document. For more details on monitoring options consult the *Administration Guide*.

TIP! The session log can be enabled on a per segment basis. Make sure that it is enabled on the segment for which you are trying to see details.

The following graphic shows the menu options that appear when the pointer is moved over the Monitor menu title.

Monitor Menu Options



The Dashboard, SSL Session Log, and SSL Statistics options are described below.

Dashboard

The dashboard display contains seven panels, described below.

The following graphic shows the segment status panel which displays the status of currently active segments.

Dashboard Segment Status Panel

Segments Status

Segment ID	Interfaces Used	Interfaces Down	Main Mode	Failures
A	1, 2		Passive Tap	

The Segment ID is a unique identifier that distinguishes this segment from other segments in the system. The Interface numbers identify the physical ports used by this segment. If any of the interfaces used by the segment are down then the interface numbers will show in the Interfaces Down column. Main Mode indicates the operating mode of the segment and the Failures column records failure details. The Manually Unfail button is normally available if the segment is in a failure mode that requires manual intervention to clear the failure.

The following graphic shows the Network Interfaces panel which contains a row for every interface that is installed in the system. The maximum number of rows in an SSL Appliance 1500 is 8, an SSL Appliance 2000 is 12, and 16 for an SSL Appliance 8200. The link state column shows the link speed for 1G NetMods.

Dashboard Network Interfaces

Network Interfaces

Port	Type	Link State	RX Packets/Bytes	TX Packets/Bytes	RX Drops
1	1G	1G	776/116320	0/0	0
2	1G	1G	0/0	776/116320	0
3	1G	Down	0/0	0/0	0
4	1G	Down	0/0	0/0	0

Each row shows the interface type and the speed it is operating at along with transmit and receive statistics. The only tool provided for this panel is the refresh button.

The following graphic shows the current CPU utilization as a percentage of the total capacity of the CPU. The only tool provided for this panel is the refresh button.

Dashboard CPU Load %

CPU Load %

cpu	cpu0	cpu1	cpu2	cpu3	cpu4	cpu5	cpu6	cpu7	cpu8	cpu9	cpu10	cpu11	cpu12	cpu13	cpu14	cpu15
3.1	40.7	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1

The following graphic shows the Fan Speed panel which has the current speed values for the various fans in the system. The only tool provided for this panel is the refresh button.

Dashboard Fan Speed (RPM)

Fan Speed (RPM)

Fan Mod 1 Inlet	Fan Mod 1 Outlet	Fan Mod 2 Inlet	Fan Mod 2 Outlet	Fan Mods 3 to 5	Left Power Supply Fan	Right Power Supply Fan
18226	16148	18226	16550	7304	5882	16129

The following graphic shows the Temperatures panel which includes details of temperatures and thermal margins for components within the system. The only tool provided for this panel is the refresh button.

Dashboard Temperatures (Degrees °C)

Temperatures (Degrees ºC)

Baseboard Temp	Front Panel Temp	IOH Therm Margin	Mem P1 Thrm Mrgn	Mem P2 Thrm Mrgn	P1 Therm Margin	P2 Therm Margin	NFP0 Temp	Left Power Supply Temp	Right Power Supply Temp
35	29	-37	-28	-44	-54	-45	57	39	44

The following graphic shows the Utilization panel which shows the percentage utilization of system memory and disk space. The only tool provided for this panel is the refresh button.

Dashboard Utilization %

Utilization %

Disk	Memory
2.0	24.3

The following graphic shows the System Log panel that contains the most recently generated system log entries, this panel automatically refreshes.

System Log

System Log

Time	Process	Log
Jul 24 15:17:46	sslmanage[4831]	Store update detected: Policy
Jul 24 15:17:46	ssldata[4834]	Activation request received. Activation pending
Jul 24 15:17:46	sslmanage[4831]	Activation request sent to data-plane

SSL Session Log

The System Log screen contains a single multi-page panel enabling all entries in the system log to be viewed.

Session Log Panel

SSL Session Log 1/2

Start Time	Segment ID	SrcIP:Port	DstIP:Port	Subject	Certificate Status	Cipher Suite	Action	Status
Dec 08 14:49:17.406 *	A	192.168.0.121:49217	192.168.0.80:443	--unknown--		TLS_RSA_WITH_AES_128_CBC_SHA	Cut Through	Master key invalid
Dec 08 14:49:17.406	A	192.168.0.121:49217	192.168.0.80:443	--unknown--		TLS_RSA_WITH_AES_128_CBC_SHA	Invalid	Master key invalid
Dec 08 14:49:17.406 *	A	192.168.0.121:49215	192.168.0.80:443	--unknown--		TLS_RSA_WITH_AES_128_CBC_SHA	Cut Through	Master key invalid

The panel has the normal multi-page navigation buttons in addition to the refresh button and a **View Details** button an **Export** button, and two filter buttons. The **Export** button brings up a dialog box that allows the range of SSL session log entries that are to be exported to be specified.

The Session Log includes the following details for each SSL session that is recorded in the log:

- Start date and time
- Segment ID for the segment the SSL session occurred on
- IP source and destination address and port number
- Subject details from the server certificate used during the session
- Status of the server certificate

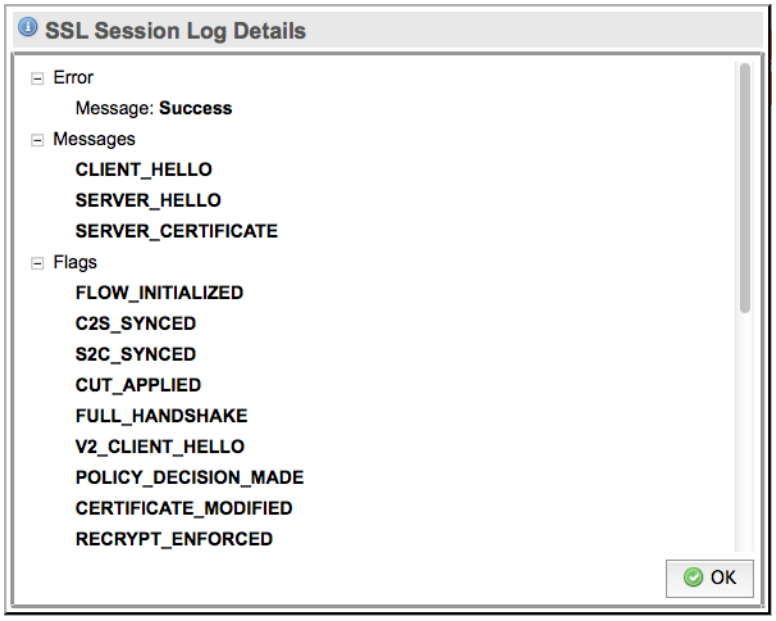
- Cipher Suite that was used for the session
- Action taken by the SSL appliance for this session
- Status for the session

Entries in the session log are ordered from most recent to oldest. So, the first row on page 1 is the most recent entry and the last row on page 64 is the oldest entry.

The filter on error button causes the session log to only display entries for flows with an inspection error. The no filter button causes the session log to display all entries.

The **View Details** button is only active when a row in the SSL Session Log panel has been selected. Click on the **View Details** button to open up a dialog box showing more details about the selected session. The following graphic shows an example of the detail available for a successful session.

SSL Session Detailed Information



SSL Statistics

The SSL Session Log screen contains a single multi-page panel enabling all entries in the last 64 pages of the SSL Statistics log to be viewed. The panel has

the normal multi-page navigation buttons and a clear statistics button. The following graphic displays an example of available statistics information.

SSL Statistics

SSL Statistics 1/64

Timestamp	#Detected	#Done	#Ignored	#Decrypt	#Decrypt Done	#Error	Detected	Decrypt
Dec 08 16:13:19	16	16	12	0	0	16	0	0
Dec 08 16:13:18	16	16	12	0	0	16	0	0
Dec 08 16:13:17	16	16	12	0	0	16	0	0
Dec 08 16:13:16	16	16	12	0	0	16	0	0
Dec 08 16:13:15	16	16	12	0	0	16	0	0
Dec 08 16:13:14	16	16	12	0	0	16	0	0
Dec 08 16:13:13	16	16	12	0	0	16	0	0
Dec 08 16:13:12	16	16	12	0	0	16	0	0
Dec 08 16:13:11	16	16	12	0	0	16	0	0
Dec 08 16:13:10	16	16	12	0	0	16	0	0
Dec 08 16:13:09	16	16	12	0	0	16	0	0
Dec 08 16:13:08	16	16	12	0	0	16	0	0
Dec 08 16:13:07	16	16	12	0	0	16	0	0
Dec 08 16:13:06	16	16	12	0	0	16	0	0
Dec 08 16:13:05	16	16	12	0	0	16	0	0
Dec 08 16:13:04	16	16	12	0	0	16	0	0

Statistics are collected every second and each row in the table holds the data for a collection interval. All the counts are cumulative except for the Detected and Decrypted columns. The Detected and Decrypted columns show the instantaneous number of sessions in each category at the point the data was collected. This is not the total number of sessions that may have been in that category over the one second period.

Entries in the Statistics panel are ordered from most recent to oldest. The first row on page 1 is the most recent entry and the last row on page 64 is the oldest entry.

Chapter 10
Licenses and Licensing Terms

The following sections include details of license terms and conditions that apply to the Netronome SSL Inspector as well as licenses details for third party software that is included in the product.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the

software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any

warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you

cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact `openssl-core@openssl.org`.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL' appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (`eay@cryptsoft.com`).

This product includes software written by Tim Hudson (`tjh@cryptsoft.com`).

Copyright Statement

COPYRIGHT

No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative work by any means including but not limited to by translation, transformation or adaptation without permission from Netronome Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice.

Limited Warranty

WARRANTY

Netronome warrants that any media on which this documentation is provided will be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of shipment. If a defect in any such media should occur during this 90-day period, the media may be returned to Netronome for a replacement.

NETRONOME DOES NOT WARRANT THAT THE DOCUMENTATION SHALL BE ERROR-FREE. THIS LIMITED WARRANTY SHALL NOT APPLY IF THE DOCUMENTATION OR MEDIA HAS BEEN (I) ALTERED OR MODIFIED; (II) SUBJECTED TO NEGLIGENCE, COMPUTER OR ELECTRICAL MALFUNCTION;

OR (III) USED, ADJUSTED, OR INSTALLED OTHER THAN IN ACCORDANCE WITH INSTRUCTIONS FURNISHED BY NETRONOME OR IN AN ENVIRONMENT OTHER THAN THAT INTENDED OR RECOMMENDED BY NETRONOME. EXCEPT FOR WARRANTIES SPECIFICALLY STATED IN THIS SECTION, NETRONOME HEREBY DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to some users of this documentation. This limited warranty gives users of this documentation, specific legal rights, and users of this documentation may also have other rights which vary from jurisdiction to jurisdiction.

Liability

Regardless of the form of any claim or action, Netronome's total liability to any user of this documentation for all occurrences combined, for claims, costs, damages or liability based on any cause whatsoever and arising from or in connection with this documentation shall not exceed the purchase price (without interest) paid by such user.

IN NO EVENT SHALL NETRONOME OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SSL INSPECTOR APPLIANCE BE LIABLE FOR ANY LOSS OF DATA, LOSS OF PROFITS OR LOSS OF USE OF THE SSL INSPECTOR APPLIANCE OR FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, MULTIPLE OR OTHER DAMAGES, ARISING FROM OR IN CONNECTION WITH THE SSL INSPECTOR APPLIANCE EVEN IF NETRONOME HAS BEEN MADE AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT SHALL NETRONOME OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SSL INSPECTOR APPLIANCE BE LIABLE TO ANYONE FOR ANY CLAIMS, COSTS, DAMAGES OR LIABILITIES CAUSED BY IMPROPER USE OF THE SSL INSPECTOR APPLIANCE OR USE WHERE ANY PARTY HAS SUBSTITUTED PROCEDURES NOT SPECIFIED BY NETRONOME.

Disclaimer of Damages

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS

ESSENTIAL PURPOSE, IN NO EVENT WILL NETRONOME OR ITS LICENSORS OR PARTNERS, BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE APPLIANCE, EVEN IF NETRONOME HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL NETRONOME'S OR ITS LICENSORS OR PARTNER'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE.

THE DISCLAIMES AND LIMITATIONS SET FORTH ABOVE WILL APPLY REGARDLESS OF WHETHER YOU ACCEPT THE APPLIANCE OR ITS ASSOCIATED SOFTWARE.

Export Regulations

You agree to comply strictly with all applicable export control regulations and laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses as required to export, re-export or import the Appliance. Export or re-export of the Appliance to the following countries is prohibited: Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan.

General

If you are located in North America or Latin America, this Agreement will be governed by the laws of the state of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License module is the entire between you and Netronome Systems, Inc. relating to the Appliance and (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter, and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgement or similar communications between the parties. This agreement may only be modified by a License Module or by a written document which has been signed by both you and Netronome. This agreement shall terminate upon Your breach of any term contained herein and You shall cease use of the Appliance and its associated software and shall return the Appliance to Netronome. The disclaimers of warranties and damages and limitations on liabilities shall survive termination. Should you have any questions concerning this agreement, please write:

Netronome Customer Service

144 Emeryville Drive, Suite 230

Cranberry Township, PA 16066-5015

USA

Excluded Software

The excluded software consists of the open source code software known as Linux included in the Appliance. All Excluded Software is licensed under the GNU General Public License, Version 2, June 1991, a copy of which is included in this document. The license entitles You to receive a copy of the source code for the Linux only upon request at a nominal charge. If you are interested in obtaining a copy of such source code, please contact Netronome Systems, Inc. for further information.

Chapter 11
Technical Support

To obtain additional information or to provide feedback, please email support@sourcefire.com or contact the nearest Sourcefire technical support representative.

Visit https://support.sourcefire.com to download the latest documentation and software, access the knowledge base, or log a support ticket.