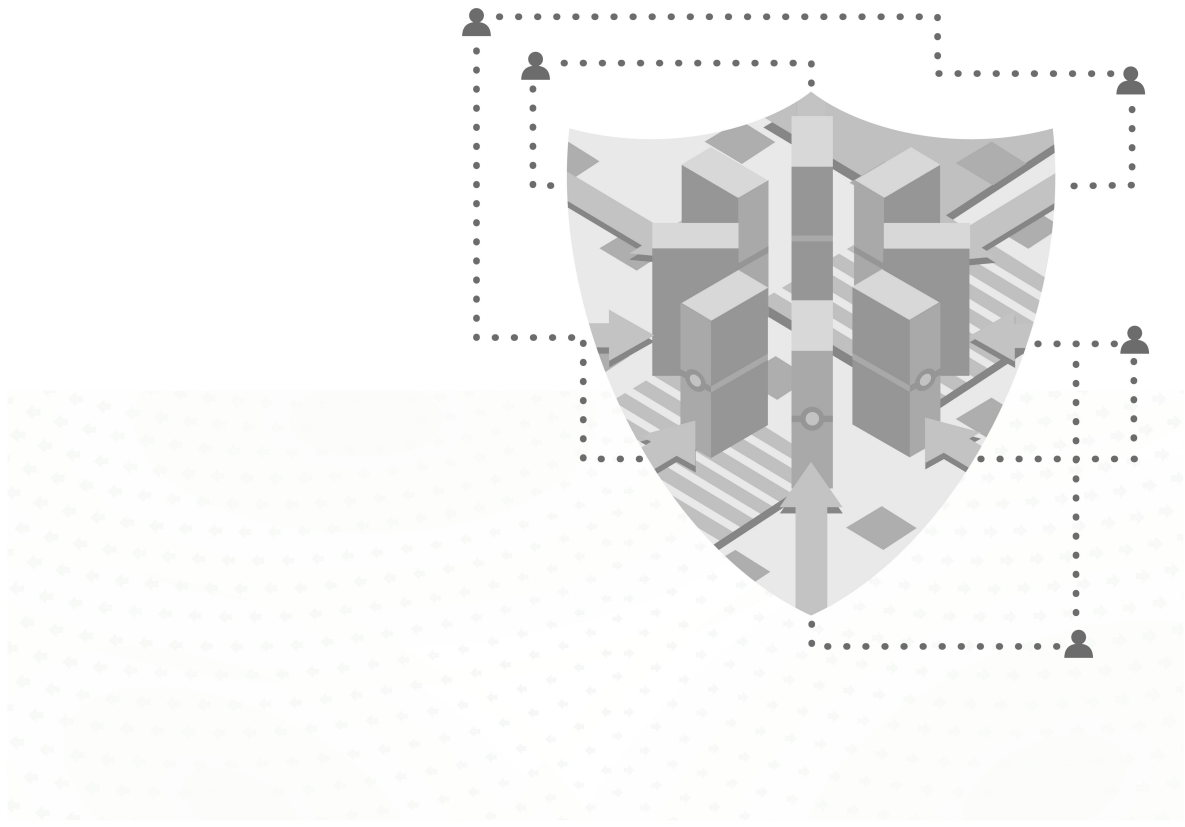
Sourcefire
SSL Appliance 2000/8200
Administration & Deployment Guide

Software version: 3.7.1
Document Revision 04/01/2014



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

Legal Notices

Cisco, the Cisco logo, Sourcefire, the Sourcefire logo, Snort, the Snort and Pig logo, and certain other trademarks and logos are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Cisco or its subsidiaries (collectively, "Cisco") or any Sourcefire-provided or Cisco-provided products. Sourcefire and Cisco products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

The copyright in the Documentation is owned by Cisco and is protected by copyright and other intellectual property laws of the United States and other countries. You may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Cisco's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

No part of the Documentation may be used in a compilation or otherwise incorporated into another work or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of Cisco. Cisco reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms.

© 2004 - 2014 Cisco and/or its affiliates. All rights reserved.

Disclaimers

THE DOCUMENTATION AND ANY INFORMATION AVAILABLE FROM IT MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. CISCO MAY CHANGE THE DOCUMENTATION FROM TIME TO TIME. CISCO MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE ACCURACY OR SUITABILITY OF ANY CISCO-CONTROLLED WEBSITE, THE DOCUMENTATION AND/OR ANY PRODUCT INFORMATION. CISCO-CONTROLLED WEBSITES, THE DOCUMENTATION AND ALL PRODUCT INFORMATION ARE PROVIDED "AS IS" AND CISCO DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL CISCO BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF PROFITS, AND/OR BUSINESS INTERRUPTIONS), ARISING OUT OF OR IN ANY WAY RELATED TO CISCO-CONTROLLED WEBSITES OR THE DOCUMENTATION, NO MATTER HOW CAUSED AND/OR WHETHER BASED ON CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER TORTUOUS ACTIVITY, OR ANY OTHER THEORY OF LIABILITY, EVEN IF CISCO IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Contents

1. Introduction....13
1.1 SSL Inspection Overview....13
1.2 Product Overview....15
1.3 Key Features....17
1.4 Product Specifications....18
1.5 Product Checklist....20
2. System Behavior & Deployment Examples....21
2.1 Transparent SSL Decryption / Encryption....21
2.2 SSL Decryption Methods....22
2.2.1 Known Server Key Method....22
2.2.2 Certificate Resigning Method....25
2.2.3 Self-Signed Server Certificate Handling....27
2.2.4 Decryption Methods in Cooperative Configurations....27
2.2.5 Marking SSL Plaintext....28
2.3 Deployment Modes....28
2.3.1 Passive-Tap Mode....30
2.3.2 Passive-Inline Mode....32
2.3.3 Active-Inline Mode....34
2.4 Policies....35
2.4.1 Segment Policies....36
2.4.2 Ruleset Policies....37
2.4.3 Lists....43
2.4.4 Reset Generation....44
2.5 Failure Modes and High Availability....45
2.5.1 Link Failures....46
2.5.2 Software (Data-Plane) Failures....47
2.6 Example Deployment Configurations....48
2.6.1 Outbound Inspection....48
2.6.2 Inbound Inspection....50
2.6.3 Inbound and Outbound Inspection....51
2.6.4 High Availability Deployment....51
3. Physical Installation....53
3.1 Safety Information....53
3.2 Requirements Checklist....53
3.3 Rack Mounting....54
3.4 Back Panel....54
3.5 Front Panel....55
3.6 Connecting to the Network....59
4. Initial Configuration and Setup....60

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

4.1 Bootstrap Phase....60
4.1.1 Configuring Static IP Address for Management....62
4.1.2 Password Entry....63
4.1.3 Installation Process....67
4.2 Network Connections....69
4.3 Post Bootstrap Configuration....69
4.3.1 Configuring System Date/Time and Timezone....70
4.3.2 Configuring Management Network Settings....72
4.3.3 Configuring Management Users....73
4.3.4 Licensing....74
4.3.5 System Status....77
4.4 Installing a CA for Certificate Resign....77
4.4.1 Creating a CA....78
4.4.2 Importing a CA....81
4.5 Importing Known Server Keys....81
4.6 Example Passive-Tap Mode Inspection....82
4.7 Example Passive-Inline Mode Inspection....91
4.8 Example Active-Inline Mode Inspection....95
5. User Interface Overview....99
5.1 Introduction....99
5.1.1 Configure the Browser....99
5.1.2 Login Process....100
5.1.3 Using the Main Screen....101
5.2 Monitoring the System....103
5.2.1 Dashboard....104
5.2.2 System Log....106
5.2.3 SSL Session Log....107
5.2.4 SSL Statistics....109
5.2.5 Certificates....109
5.2.6 Errors....110
5.2.7 Diagnostics....111
5.2.8 Debug....112
5.3 Configuring Segments and Policies....113
5.3.1 Rulesets....113
5.3.2 Segments....117
5.3.3 Subject/Domain Names List....121
5.3.4 Domain Names List....122
5.3.5 IP Address Lists....123
5.3.6 Cipher Suites List....124
5.3.7 Host Categorization Lists....125
5.4 PKI Management....130
5.4.1 Internal Certificate Authorities....130

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.4.2 External Certificate Authorities....131
5.4.3 Certificate Revocation Lists....132
5.4.4 Trusted Certificates....133
5.4.5 Known Certificates and Keys....134
5.5 Platform Management....135
5.5.1 Information....136
5.5.2 Management Network....137
5.5.3 Remote Logging....138
5.5.4 Date/Time....138
5.5.5 Users....139
5.5.6 TACACS Servers....139
5.5.7 Alerts....141
5.5.8 License....143
5.5.9 Backup/Restore....144
5.5.10 Halt/Reboot....144
5.5.11 Import UI Certificate/Key....145
5.5.12 Update....145
5.5.13 Preferences....146
5.6 User Management....146
5.6.1 Change Password....147
5.6.2 Logout....147
6. Troubleshooting the System....148
6.1 Supported Network Protocols and Frame Encapsulations....148
6.2 Supported SSL/TLS versions....148
6.3 Support for Client Certificates....148
6.4 Supported Cipher Suites....149
6.5 Support for SSL Record Layer Compression....151
6.6 Support for Stateless Session Resumption (RFC5077)....151
6.7 Steps to Troubleshoot SSL Decryption....152
6.7.1 Monitor Network Port Statistics....152
6.7.2 Monitor the SSL Statistics....152
6.7.3 Monitor the SSL Session Log....152
6.7.4 Verify that the Inspection Policy is Set Up Correctly....152
6.8 Known Server vs Trusted Server Certificates....153
6.9 Caveats when Enabling/Disabling SSL Inspection....153
6.10 Generating the Internal CA Certificates....154
6.11 Access to Microsoft Windows Update Denied....154
6.12 Issues with Alerts....155
6.13 Procedure for Reporting an Issue....155
6.14 Preparing for Hardware Diagnostics or Maintenance....155
6.15 Command Line Diagnostics Interface....155
7. Safety Information....158
7.1 Safety Instructions....158

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

7.2 Rack Mounting the Equipment....158
8. Technical Support....159

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

List of Figures

Figure 2.1: Known Server Key Decryption Method - Passive-Tap Mode....23
Figure 2.2: Known Server Key Decryption Method - Passive-Inline mode....24
Figure 2.3: Certificate Resign Decryption Method - Passive-Inline mode....25
Figure 2.4 Certificate Resign Decryption Method in a Cooperative Deployment....28
Figure 2.5: PT-sym....31
Figure 2.6: PT-sym-ag2....31
Figure 2.7: PT-sym-ag3....31
Figure 2.8 Copy Options for Symmetric PT Mode....31
Figure 2.9 PT-asym....32
Figure 2.10 Copy Options for Asymmetric PT Mode....32
Figure 2.11 PI-sym....33
Figure 2.12 Symmetric PI Mode Copy Options....33
Figure 2.13: PI-asym....33
Figure 2.14: Copy options for asymmetric PI mode....33
Figure 2.15: AI-sym FTN....34
Figure 2.16: Al-sym FTA....34
Figure 2.17: Copy Modes for Active-Inline with Symmetric Traffic....34
Figure 2.18: AI-asym FTA....35
Figure 2.19: AI-asym FTN....35
Figure 2.20 Outbound Monitoring with Network Forensic Appliance....49
Figure 2.21 Inbound Monitoring with IDS and Application Performance Monitor....50
Figure 2.22 Inbound and Outbound Inspection with IPS and Network Forensic Appliances....51
Figure 2.23 High Availability Deployment....52
Figure 3.1 SSL2000 Back Panel....54
Figure 3.2: SSL8200 Back Panel....54
Figure 3.3 SSL2000 Front Panel....55
Figure 3.4 SSL8200 Front Panel....56
Figure 3.5 SSL2000 Front Panel Controls....57
Figure 3.6 SSL8200 Front Panel Controls....57
Figure 4.1 Boot up Screens....60
Figure 4.2 Default LCD Display....61
Figure 4.3 Top Level IP Address Configuration....62
Figure 4.4 Configurable IP Address Options....62
Figure 4.5 Initial IP address Configuration....63
Figure 4.6 Editing IP Address....63
Figure 4.7 Edited IP Address....63
Figure 4.8 Apply Command to Change Static IP Address....63
Figure 4.9 PIN Entry, Menu 1: Select Upper or Lower Case....64

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.10 PIN Entry, Menu 2: Character Group Selection....65
Figure 4.11 PIN Entry, Menu 3: Character Sub Group Selection....65
Figure 4.12 PIN Entry, Menu 4: Character Selection....65
Figure 4.13 PIN Entry: First character Entered....65
Figure 4.14 Pin Entry, Menu 2: Character Group Selection....66
Figure 4.15 PIN Entry, Menu 3 : Character Sub Group Selection....66
Figure 4.16 PIN Entry, Menu 4: Character Selection....66
Figure 4.17 PIN Entry, Menu 4: Next Character....66
Figure 4.18 PIN Entry, Menu 1: Space Entered....66
Figure 4.19 PIN Entry, Menu 1: Complete Password Entered....67
Figure 4.20 Bootstrap Master Key Mode....67
Figure 4.21 Bootstrap User Setup....68
Figure 4.22 Initial Access Login....69
Figure 4.23 Status Information on Initial Login....70
Figure 4.24 Management Standard Features....70
Figure 4.25 Edit Date and Time....71
Figure 4.26 Time Settings with Reboot Button....71
Figure 4.27 Management Network Settings with Edit Window....72
Figure 4.28 Management Network Settings with Apply Button....73
Figure 4.29 Current System Users....73
Figure 4.30 Add User....74
Figure 4.31 Change User Password....74
Figure 4.32 Management Dashboard....77
Figure 4.33 Empty Internal Certificate Authority Screen....78
Figure 4.34 Generate Internal Certificate Authority Window....78
Figure 4.35 Internal Certificate Authority Certificate Signing Request....79
Figure 4.36 Internal Certificate Authority with CSR Entry....80
Figure 4.37 Internal Certificate Authority -Import....80
Figure 4.38 Known Server Certificate with Keys Lists....81
Figure 4.39 Known Certificate with Keys Import....82
Figure 4.40 Known Certificate and Keys with Entries....82
Figure 4.41 Adding a Ruleset....83
Figure 4.42 Add Cut Through Rule to Using Known Server Key/Certificate....84
Figure 4.43 Empty Segments Display....85
Figure 4.44 Add Segment....85
Figure 4.45 Selecting Mode of Operation for a Segment....86
Figure 4.46 Example Passive-Tap Segment Configuration....87
Figure 4.47 Passive-Tap Segment Options and Activation....88
Figure 4.48 Activating a Passive-Tap Segment - Step One....89
Figure 4.49 Activating a Passive-Tap Segment - Step 2....90
Figure 4.50 Activating a Passive-Tap Segment - Final Step....90
Figure 4.51 Segment Display with Active Passive-Tap Segment....91

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.52 Create a Passive-Inline Ruleset....92
Figure 4.53 List of Subject/Domain Names....92
Figure 4.54 Rule to Inspect using Certificate Resign and a DN List....93
Figure 4.55 Passive-Inline Ruleset with Two Rules Defined....94
Figure 4.56 Passive-Inline Segment Configuration....95
Figure 4.57 Active Passive-Inline Segment....95
Figure 4.58 Create a Custom List of Known Server Keys/Certificates....96
Figure 4.59 Adding Entries to a Custom List....97
Figure 4.60 Active-Inline Ruleset....97
Figure 4.61 Active-Inline Segment Configuration....98
Figure 5.1 Warning from Chrome Browser....100
Figure 5.2 Warning from Firefox Browser....100
Figure 5.3 SSL2000 and SSL8200 Login....101
Figure 5.4 Basic Management Screen Layout....101
Figure 5.5 Example Information Display Panel....102
Figure 5.6 Example Configuration Edit Panel....102
Figure 5.7 Example of Linked Panels....102
Figure 5.8 Monitor Menu Options....104
Figure 5.9 SSL8200 System Panel....104
Figure 5.10 Dashboard Segment Status Panel....105
Figure 5.11 Dashboard Network Interface Panel....105
Figure 5.12 Dashboard CPU Load %....105
Figure 5.13 Dashboard Fan Speed (RPM)....105
Figure 5.14 Dashboard Temperatures (Degrees °C)....106
Figure 5.15 Dashboard Utilization %....106
Figure 5.16 Dashboard System Log....106
Figure 5.17 System Log....106
Figure 5.18 Filter on Process....107
Figure 5.19 Session Log....107
Figure 5.20 Export Session Log....107
Figure 5.21 Detailed SSL Session Information....108
Figure 5.22 SSL Statistics....109
Figure 5.23 Invalid Certificates Panel....110
Figure 5.24 Invalid Certificates Panel with Self-Signed Certificate Details....110
Figure 5.25 SSL Error Counts....111
Figure 5.26 Diagnostics....111
Figure 5.27 Debug NFE Network Statistics 1....112
Figure 5.28 Debug NFE Network Statistics 2....112
Figure 5.29 Debug NFE Network Statistics 3....112
Figure 5.30 Policies Menu....113
Figure 5.31 Rulesets....114
Figure 5.32 Rulesets Clone....114
Figure 5.33 Ruleset Options....114

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.34 Edit Ruleset Options....115
Figure 5.35 Insert Rule....116
Figure 5.36 Rules Table Positioning....117
Figure 5.37 System Graphic on Segment Screen....117
Figure 5.38 Segment System Options....118
Figure 5.39 Segment Undecryptable Actions....118
Figure 5.40 Certificate Status Actions....119
Figure 5.41 Edit Certificate Status Actions....119
Figure 5.42 Edit Plaintext Marker....120
Figure 5.43 Segment Failure Mode Options....120
Figure 5.44 Subject/Domain Names list for Unsupported Sites....121
Figure 5.45 Add a Subject/Domain Name to a List....122
Figure 5.46 Examples of Subject/Domain Names Formats....122
Figure 5.47 Add a New Domain Name....123
Figure 5.48 IP Address Formats....124
Figure 5.49: Add a Cipher Suite to a Cipher Suites List....124
Figure 5.50 Examples of Cipher Suite Formats....124
Figure 5.51 Host Categorizations....125
Figure 5.52: Edit Host Categorization Settings....126
Figure 5.53 Host List with its Categorizations....127
Figure 5.54: Edit Host Categories....128
Figure 5.55 PKI Menu....130
Figure 5.56 Creating a Custom External Certificate Authorities List....132
Figure 5.57 Clone a List....132
Figure 5.58 Import CRL....133
Figure 5.59 Platform Management Menu....135
Figure 5.60 Platform Information - Software Versions and Chassis Data....136
Figure 5.61 Management Network Panel with Edit Settings....137
Figure 5.62 Editing Remote Logging Settings....138
Figure 5.63 Date/Time Panel....138
Figure 5.64 Managing User Accounts....139
Figure 5.65 TACACS Servers Panel....139
Figure 5.66 WebUI Login when TACACS is Used....140
Figure 5.67 TACACS Server Configuration....140
Figure 5.68 E-mail Configuration for Alert System....141
Figure 5.69 Add Alert to System....142
Figure 5.70 Add a New License....143
Figure 5.71 Backup....144
Figure 5.72 Restore....144
Figure 5.73 Halt/Reboot Option....144
Figure 5.74 Import Certificate for WebUI....145
Figure 5.75 Update the SystemI....145

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.76 WebUI Layout Preferences with Edit Window....146
Figure 5.77 User Menu....146
Figure 5.78 Change Password....147
Figure 6.1 Certificate Status....153

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

List of Tables

Table 1 SSL2000 Specification....19
Table 2 SSL8200 Specification....20
Table 3 SSL2000/SSL8200 Packing List....20
Table 4 Segment Policy Options....37
Table 5 Ruleset Policy Options....38
Table 6 Actions that can be Specified in a Rule....39
Table 7 Decrypt with Known Certificate and Key Rule Format....40
Table 8 Decrypt using Replacement of Key and Certificate Format....41
Table 9 Decrypt using Certificate Resign Format....42
Table 10 Decrypt Anonymous Diffie-Hellman Format....42
Table 11 Rules Not Involving Decryption Format....43
Table 12 Default List Types and Contents....44
Table 13 SSL2000 and SSL8200 Back Panel Components....55
Table 14: SSL2000 Front Panel Components....58
Table 15: SSL2000 System Status Indicators....59
Table 16: Keypad Layout....61
Table 17: SSL2000 Power On Key Sequences....61
Table 18 TACACS Levels to User Roles....141
Table 19 Supported Cipher Suites....151

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

1. Introduction

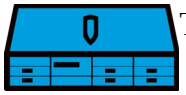
The following conventions are used throughout this document.

Note: This style indicates a "note" providing additional information that the reader may be interested in.

! This symbol indicates a "warning" providing additional information that the reader needs to pay attention to.

Name: This style refers to elements you see on the WebUI (GUI, such as the names of screens, fields, and options.

This icon indicates information that only applies to the SSL2000.


This icon indicates information that only applies to the SSL8200.

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.

! The embedded software contained within the Sourcefire SSL appliance is subject to licensing. See Section 4.3.4 of this document for details on licensing.

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

1.1 SSL Inspection Overview

As organizations become dependent on IP-based applications and services, the demand for secure reliable communications has never been higher. The increase in CPU performance has made client-based encryption a viable solution for enterprise communications. SSL is the dominant client-based encryption protocol and now constitutes a significant and growing percentage of the traffic in enterprise LAN and WAN, as well as throughout service provider networks. SSL is used as a VPN technology to allow users to securely communicate with the enterprise. It is also used for secure communications from inside of the enterprise to Internet-based applications and services (banking, e-commerce, web mail, cloud applications and personal e-mail).

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The privacy benefits provided by SSL can quickly be overshadowed by the risks it brings to the enterprise network. SSL encryption can:

- Mask threats, such as viruses, spam and malware
- Make corporate acceptable use policies less effective
- Increase the likelihood of accidental or intentional leakage of confidential information

SSL Inspection enables existing security and network appliances to access the plaintext within SSL flows thereby enabling the security appliance to do its job, even with SSL encrypted traffic. Unmodified applications running on devices attached to the Sourcefire SSL appliance gain visibility into the content of the SSL traffic. SSL Inspection is a complex and computationally intensive process that can easily become a performance bottleneck unless implemented with appropriate hardware acceleration techniques.

There are two different mechanisms that can be used in order to "inspect" SSL traffic depending on what information is available and how the inspection device is deployed in the network.

- Known server key mechanism relies on the inspecting device having a copy of the servers private key and certificate
- Certificate resign mechanism relies on the inspecting device having a trusted CA certificate that can be used to sign SSL server certificates that have been intercepted and modified

There are three basic connectivity modes that define how the SSL inspecting appliance and the associated security appliance are connected to each other and to the network. These modes are identified as:

- Active-Inline
- Passive-Inline
- Passive-Tap

The Active/Passive designation refers to the associated security appliance and how it behaves while the Inline/Tap designation refers to how the SSL inspecting device is connected to the network. An "Active" associated appliance processes traffic from the SSL inspecting device and then returns the traffic to the device while a "Passive" appliance simply consumes traffic. The SSL Inspecting device can be either "In-line" or can be connected to a network span or tap port.

! SSL Inspection using "certificate resign" and SSL policy enforcement can only be done if the SSL Inspecting device is connected "inline" in the network.

! Only "known server key" mode can be used to inspect SSL traffic when the inspecting device is connected to a network tap. Inspection is not possible if the session uses Diffie-Hellman or Elliptic Curve Diffie-Hellman for key exchange.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

SSL inspection enables the identification and elimination of risks, such as regulatory compliance violations, viruses/malware, and intrusion attempts normally hidden within SSL. The privacy and integrity of SSL encrypted communications are maintained by making the plaintext available only to the directly attached appliance. This requires the environment to be physically secure. Additional privacy for SSL encrypted traffic can be achieved by configuring appropriate policies to control which traffic is inspected and which is not.

> **!** The Sourcefire SSL appliance and the associated security appliance(s) that it is enabled to "inspect" traffic should all be located in a physically secure environment in order to prevent unauthorized access to the decrypted SSL traffic.

1.2 Product Overview

The Sourcefire SSL appliance is a high performance transparent proxy for Secure Socket Layer (SSL) network communications. It enables a variety of applications to access the plaintext (that is, the original unencrypted data) in SSL encrypted connections and has been designed for security and network appliance manufacturers, enterprise IT organizations and system integrators. Without compromising any aspect of enterprise policies or government compliance, the Sourcefire SSL appliance lets network appliances be deployed with highly granular flow analysis while maintaining line rate performance.

The Sourcefire SSL appliance products provide two main functions:

- Enabling other security appliances to see a non-encrypted version of SSL traffic that is crossing the network. This is called SSL Inspection, as the security appliance is able to inspect the decrypted traffic for possible threats: something it cannot do when it sees encrypted traffic.
- Acting as a policy control point enabling explicit control over what SSL traffic is and is not allowed across the network.

The Sourcefire SSL appliance is designed to work alongside existing security devices such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Data Loss Prevention systems (DLP), Network Forensic appliances, etc. It provides a non-encrypted version of SSL traffic to the associated appliance while maintaining an end-to-end SSL connection between the client and server involved in the session.

Unlike most other SSL proxy devices, the Sourcefire SSL appliance does not rely on the TCP destination port number being used by a session to determine if it is using SSL or not. The Sourcefire SSL appliance uses deep packet inspection (DPI) to identify SSL flows. This ensures that it can find and inspect any SSL traffic in the network, even if the traffic is using non-standard port numbers.

The Sourcefire SSL appliance incorporates flow processing hardware and cryptographic acceleration hardware, enabling it to forward non-SSL traffic at multi-Gigabit/s rates,

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

while offering industry-leading transparent proxy performance (that is, decrypting and re-encrypting) for SSL traffic.

The Sourcefire SSL appliance supports two different mechanisms that allow SSL inspection. Each mechanism requires that different information is available to the Sourcefire SSL appliance.

- Known server key mechanism relies on the inspecting device having a copy of the SSL server's private key and certificate
- Certificate resign mechanism relies on the inspecting device having a trusted CA certificate that can be used to sign SSL server certificates that have been intercepted and modified

The mechanism used to inspect an SSL flow can be chosen based on the details related to that flow, so it is possible for the Sourcefire SSL appliance to be configured to use both mechanisms at the same time.

There are three basic connectivity modes that define how the Sourcefire SSL appliance and the associated security appliance are connected to each other and to the network. These modes are identified as:

- Active-Inline
- Passive-Inline
- Passive-Tap

The Active/Passive designation refers to the associated security appliance and how it behaves, while the Inline/Tap designation refers to how the Sourcefire SSL appliance is connected to the network. An "Active" associated appliance processes traffic from the Sourcefire SSL appliance and then returns the traffic to the Sourcefire SSL appliance, while a "Passive" appliance simply consumes traffic. The Sourcefire SSL appliance can be either "In-line" or connected to a network span or tap port.

It is possible to have more than one associated security appliance connected to the Sourcefire SSL appliance and receiving the "inspected" traffic. A typical configuration would be an IPS device attached to the Sourcefire SSL appliance operating in Active-Inline mode, with a network forensic appliance also connected in Passive mode, and receiving the same data that is going through the IPS. The ability to "mirror" the output of the Sourcefire SSL appliance to additional passive appliances is a useful feature that removes the need for an external device to "mirror" traffic to more than one appliance.

The Sourcefire SSL appliance enables the identification and elimination of risks, such as regulatory compliance violations, viruses/malware, and intrusion attempts normally hidden within SSL. The privacy and integrity of SSL encrypted communications are maintained by making the plaintext available only to the attached appliance. This requires the environment to be physically secure. Additional privacy for SSL encrypted traffic can be achieved by configuring appropriate policies to control which traffic is inspected.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

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

1.3 Key Features

The Sourcefire SSL appliance provides a complete solution to the problem of dealing with threats contained within encrypted SSL traffic. A single Sourcefire SSL appliance can be deployed to detect and inspect all SSL traffic that may pose a threat, and can pass the decrypted content to one or more network security appliances which can record or block any threats. The ability to feed "inspected" traffic to more than one associated security appliance ensures that SSL traffic only has to be decrypted and then re-encrypted once as it crosses the network.

- ✔ **Line rate Network Performance for GigE and 10G links**

  All non-SSL traffic flows are "cut through" (forwarded directly from port to port) by the embedded flow processor(s) (NFP-3240), minimizing latency for traffic such as VoIP.

- ✔ **Network Transparency**

  The Sourcefire SSL appliance is deployed as a "bump in the wire" and is completely transparent to both end systems and intermediate networking elements. There is no need for network reconfiguration, IP addressing or topology changes, or modifications to client or server software (for example, changing web proxy settings or client IP addresses).

- ✔ **Compatible with Existing Devices and Applications**

  Intercepted plaintext is delivered to attached devices as a valid regenerated TCP stream via the Sourcefire SSL appliance's network ports. This allows existing security appliances (such as IDS, IPS, firewall, lawful intercept, and compliance monitoring devices) to expand their scope to also provide benefits for SSL encrypted traffic.

- ✔ **Supports Multiple Decryption Methods and Various Encryption Algorithms / Protocols**

  One decryption method supports situations where server keys can be obtained, while another method can decrypt traffic to servers on the Internet, therefore the Sourcefire SSL appliance supports both "inbound" as well as "outbound" SSL traffic. The Sourcefire SSL appliance can accommodate most SSL-encrypted protocols, such as web (HTTPS), e-mail protocols, and most other standard or proprietary protocols. Either SSL 3.0, TLS 1.0, TLS 1.1, or TLS 1.2 can be used.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- ✔ **High Availability Deployment Options**

  Link state mirroring and fail to wire/fiber options allow the Sourcefire SSL appliance to be deployed in configurations that ensure connectivity is maintained even if hardware fails or software is temporarily not fully functional (for example,. because software is being upgraded).

- ✔ **Traffic Mirroring**

  The ability to mirror copies of the traffic on an interface to up to two other interfaces enables multiple network security appliances to receive the "inspected" traffic flows. For example, an IPS may be attached to the Sourcefire SSL appliance, and at the same time a Network forensics appliance could be connected with both appliances receiving the inspected traffic flows.

- ✔ **Traffic Aggregation**

  When the Sourcefire SSL appliance is used in Tap mode (connected to a network TAP rather than in-line) it can be configured to aggregate traffic received on multiple interfaces onto a single logical segment which contains the policies for how the traffic should be processed. This avoids the need to use an external aggregation device when traffic is being collected from multiple network TAPs.

1.4 Product Specifications

This document covers the SSL2000 and SSL8200 products. Where hardware or software features differ between the two models the features for each product will be shown separately. Any features not explicitly identified as relating to only one model apply to both products.

The specifications shown in Table 1 may change over time, any changes will be reflected in new versions of this documentation which may be downloaded from the Sourcefire support site.

Category	Description
Chassis Dimensions	17.2" (W) x 19.2" (D) x 1.73" (H) (433mm x 728mm x 44mm)
Weight	43.5 lbs (19.8 kg)
Processors	2 x Intel Xeon E5620 quad core CPUs
System memory	24GB DDR3
Network Flow Engine (NFE)	1 x NFE-3240 card (NFP-3240 + 4GB DDR3 + PCIe gen2 x8)
Network Module slots (Netmods)	3 x Netmod slots

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Category	Description
Supported Netmod types all Netmods have fail to wire/open capabilities	2 x 10G fiber 4 x 10/100/1000 fiber 4 x 10/100/1000 copper
Management Network interfaces	2 x 10/100/1000 copper interfaces on rear panel
Integrated Display	16 character by 2 line LCD on front panel
Power Supplies	2 x 650W redundant hot swap power supplies
Operating Temperature	0°C to 40°C
Storage Temperature	-10°C to 70°C
Cooling	Generates up to 1725 BTU/hour worst case
Air flow	160 ft^3/min (4.5m^3/min)

Table 1 SSL2000 Specification

The specifications shown in Table 2 may change over time, any changes will be reflected in new versions of this documentation which may be downloaded from the Sourcefire support site.

Category	Description
Chassis Dimensions	17.2" (W) x 19.0" (D) x 3.48" (H) (433mm x 735mm x 88.2mm)
Weight	58 lbs (26.4 kg)
Processors	2 x Intel Xeon E5645 hex core CPUs
System memory	48 GB DDR3
Network Flow Engine (NFE)	2 x NFE-3240 card (NFP-3240 + 4GB DDR3 + PCIe gen2 x8)
Network Module slots (Netmods)	7 x Netmod slots (recommended system limit is a total of 16 interfaces)
Supported Netmod types all Netmods have fail to wire/open capabilities	2 x 10G fiber 4 x 10/100/1000 fiber 4 x 10/100/1000 copper
Management Network interfaces	2 x 10/100/1000 copper interfaces on rear panel
Integrated Display	16 character by 2 line LCD on front panel
Power Supplies	2 x 750W redundant hot swap power supplies
Operating Temperature	0°C to 40°C

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Category	Description
Storage Temperature	-10°C to 70°C
Cooling	Generates up to 2225 BTU/hour worst case
Air flow	210 ft^3/min (6m^3/min)

Table 2 SSL8200 Specification

1.5 Product Checklist

Carefully unpack the Sourcefire SSL appliance and compare the actual contents with Table 3 to ensure that you have received all ordered components. Follow the instructions in Sections 3 to install and initially configure the appliance.

Part	Description	Quantity
Sourcefire SSL2000 Appliance or Sourcefire SSL8200 Appliance	1U rack mountable device 2U rack mountable device	1
2 x Power Cords	One for each redundant supply	2
Rack mounting rails	Rails to rack mount the device	1
	Number of Components	**4**

Table 3 SSL2000/SSL8200 Packing List

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

2. System Behavior & Deployment Examples

This section describes the functions performed by the Sourcefire SSL appliance, its behavior, and its interaction with attached devices. For details on how to setup and configure the SSL2000 and SSL8200 refer to Section 4. and Section 5.

2.1 Transparent SSL Decryption / Encryption

The main function of the Sourcefire SSL appliance is to decrypt SSL traffic to obtain the plaintext sent within the SSL encrypted session. The plaintext information is fed to one or more attached device(s) for processing or analysis. As the plaintext data stream is repackaged as a valid TCP stream, applications that are hosted on the attached device(s) do not need to be modified to process the received plaintext stream.

- The Sourcefire SSL appliance provides SSL Inspection capabilities to existing devices.

The collection of SSL2000 and SSL8200 interfaces that are used to connect to the network carrying the traffic that is being inspected and to the attached appliances that are processing the traffic is called a "segment". Depending on how the SSL2000 or SSL8200 is connected and on how many attached appliances are connected a segment may contain up to 8 interfaces.

When used in Active-Inline (AI) mode or Passive-Inline (PI) mode the Sourcefire SSL appliance acts as a fully transparent proxy: the Ethernet ports used to connect it to the data network do not have IP addresses, and the other devices in the network are unaware that the Sourcefire SSL appliance has been installed. Unlike a non-transparent proxy, which requires that client machines are configured to send traffic to the IP address associated with the proxy, there are no changes required to clients or other network equipment when installing the SSL2000 or SSL8200.

- If used in Active-Inline mode or Passive-Inline mode, the Sourcefire SSL appliance is a Layer 2 "bump-in-the-wire" device and it can be deployed without renumbering the existing IP network. In most cases no network topology changes whatsoever are required.
- If used in Passive-Tap (PT) mode the Sourcefire SSL appliance is no longer a "bump-in-the-wire" on the live network, but rather a "bump-in-the-wire" on the passive link between the network SPAN/tap device and the attached appliance(s).

The Sourcefire SSL appliance can detect SSL traffic within TCP streams whether standard or non-standard TCP ports are used. It is compatible with most protocols layered on SSL, such as HTTP, SMTP, POP3, IMAP, and many other proprietary protocols. The Sourcefire SSL appliance is also compatible with selected protocols which first send non-encrypted requests and responses, followed by the actual SSL

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

protocol setup. The supported protocol variants that behave this way include the HTTP protocol's CONNECT method (used to traverse proxies) and the STARTTLS command used by e-mail protocols (SMTP, POP3 and IMAP).

- The Sourcefire SSL appliance can decrypt most SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2 secured traffic (not just HTTPS traffic).

The Sourcefire SSL appliance decrypts information received from the client, and re-encrypts it before sending it to the server, with the converse being performed for server to client traffic.

- Client and server software does not need to be modified, and security is maintained for the entire path between the client and the server.

2.2 SSL Decryption Methods

The Sourcefire SSL appliance supports two different methods for inspecting SSL. Each method requires that different information is available to the Sourcefire SSL appliance.

- Known server key mechanism relies on the Sourcefire SSL appliance having a copy of the SSL server's private key and certificate.
- Certificate resign mechanism relies on the Sourcefire SSL appliance having a trusted CA certificate that can be used to sign SSL server certificates that have been intercepted and modified.

Both these methods can be used when the Sourcefire SSL appliance is operating in Active-Inline (Section 2.3.3) or Passive-Inline (Section 2.3.2) mode but only the "known server key" method can be used if the Sourcefire SSL appliance is operating in Passive-Tap (Section 2.3.1) mode.

Note: The method used to inspect an SSL flow can be chosen based on the details related to that flow so it is possible for the Sourcefire SSL appliance to be configured to use both mechanisms at the same time.

There are different variations of these two basic mechanisms that are used depending on the type of SSL session being decrypted, the mode of operation of the Sourcefire SSL appliance and the type of certificates/keys available to the system. The different variations are shown in detail in Section 2.4.2.

2.2.1 Known Server Key Method

Figure 2.1 illustrates the use of known server key decryption when the Sourcefire SSL appliance is connected in Passive-Tap mode. When the Sourcefire SSL appliance is deployed, the server certificate and key are installed on the Sourcefire SSL appliance for every server that you want to inspect traffic to. The Sourcefire SSL appliance can use the key/certificate from a specific server to decrypt SSL sessions established with that server. A variant of this method which requires that only the server private key is installed on the Sourcefire SSL appliance is also supported.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Note: If the private-key-only mode is being used, then references to key and certificate in the rest of this section should be taken to mean only the private key.

This method can only be used where the Sourcefire SSL appliance administrator has access to the server private key and certificate information; this is normally only the case if the Sourcefire SSL appliance and the server are managed and operated by the same organization or enterprise, that is, for "inbound" traffic to "your" servers.

The simplest example of known-server-key mode is illustrated in Figure 2.1. You can see that the client is sending "abc" to the server, and this is encrypted to "#$*" before being sent across the network. The server receives "#$*" and decrypts it back to "abc" in order that the communication is successful. The Sourcefire SSL appliance receives a copy of the encrypted traffic "#$*" from the tap device, and using the server key and certificate that have been loaded, it decrypts this to get the plaintext "abc."

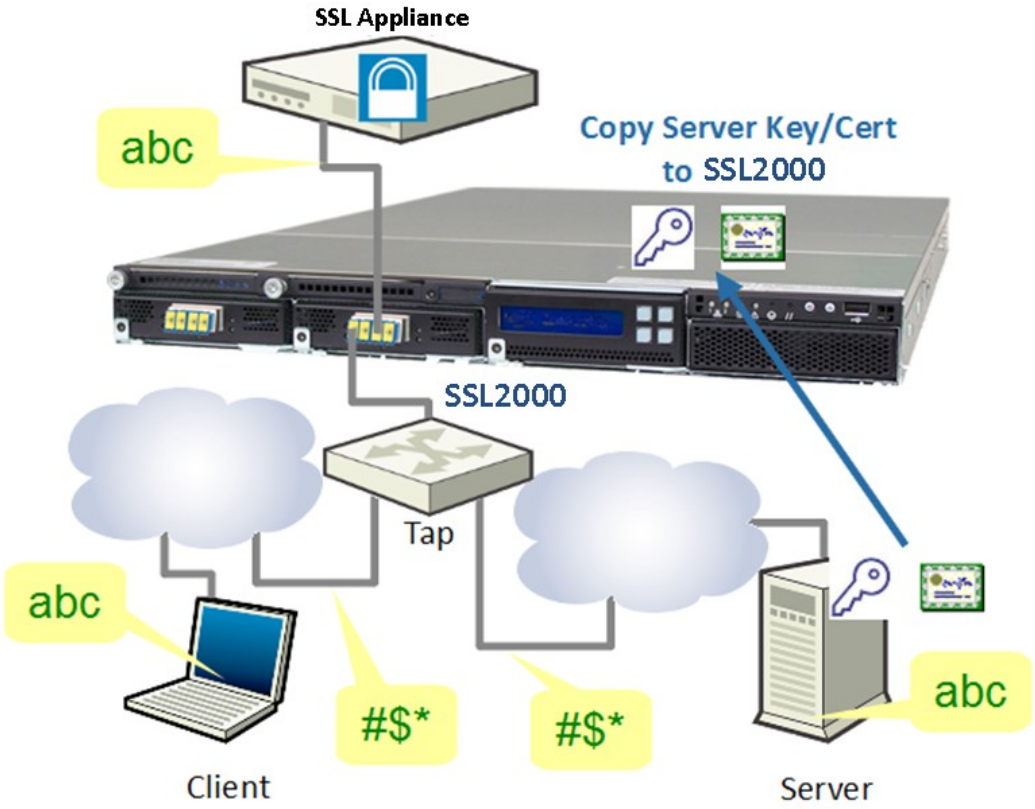


Figure 2.1: Known Server Key Decryption Method - Passive-Tap Mode

In this example, the Sourcefire SSL appliance is not a "Man In The Middle" (MITM) of the SSL session. It is simply receiving a copy of the encrypted data, and decrypting it using the server private key and certificate that it has copies of.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The fact that in Passive-Tap mode the Sourcefire SSL appliance is not a MITM for the SSL session is important, as it means that not all SSL traffic can be decrypted even when the Sourcefire SSL appliance has the relevant servers private key and certificate. If the SSL session handshake makes use of Diffie-Hellman during the key exchange process then it is impossible for the Sourcefire SSL appliance to decrypt the traffic. In order to use known server key decryption to inspect a flow that uses Diffie-Hellman for key exchange the Sourcefire SSL appliance must be a MITM of the SSL session.

Figure 2.2 shows an example of known-server-key decryption when the Sourcefire SSL appliance is installed in Passive-Inline mode. In this case, the Sourcefire SSL appliance is a MITM as the traffic between client and server passes through the Sourcefire SSL appliance.

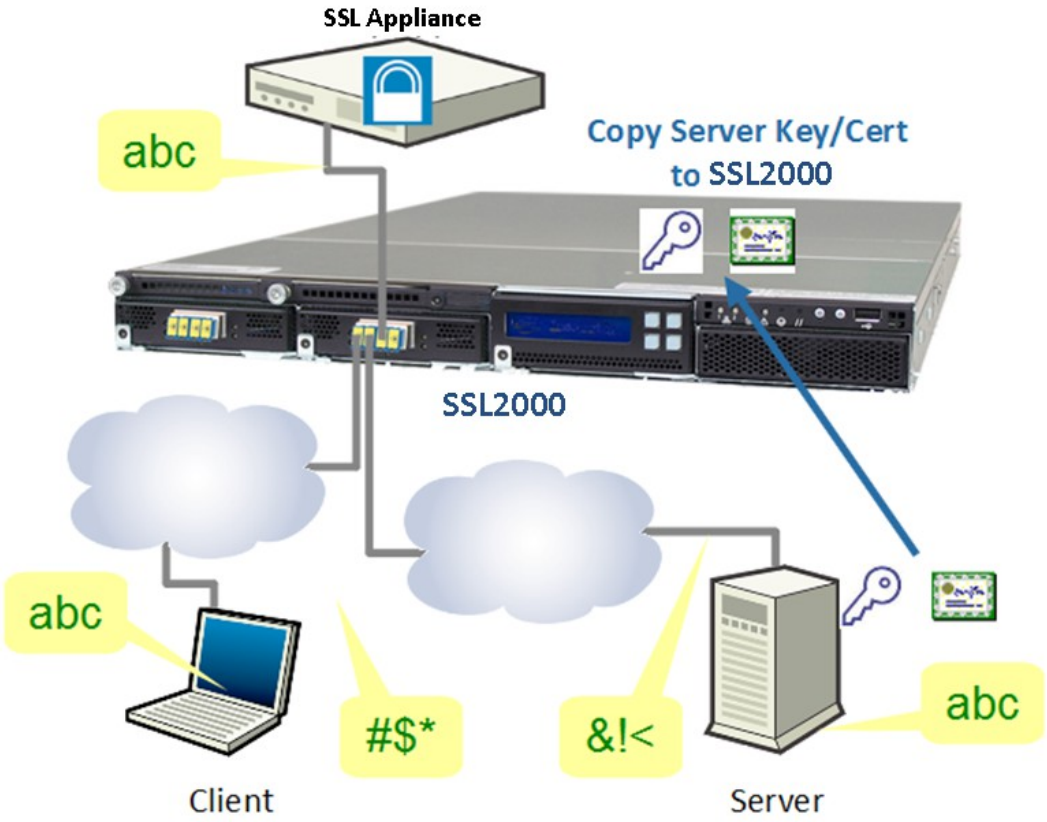


Figure 2.2: Known Server Key Decryption Method - Passive-Inline mode

An important point to note here is that there are now two different encrypted SSL sessions. The Client encrypts "abc" to "#$*" and sends this out over the network. Using its copy of the server private key and certificate, the Sourcefire SSL appliance can decrypt this to access the plaintext "abc." The Sourcefire SSL appliance re-encrypts the plaintext to produce "&!<," and sends this over the network to the server which can decrypt it to access the plaintext "abc".

The encrypted traffic between the client and the Sourcefire SSL appliance and between

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

the Sourcefire SSL appliance and the server is different, because the two SSL sessions have different cryptographic session details. If the session uses Diffie-Hellman for key exchange, the session details will be different for the two SSL sessions. If Diffie-Hellman is not used for key exchange, the session details can be the same, and the Sourcefire SSL appliance can optimize performance by avoiding the need to re-encrypt the plaintext, and simply forwarding the encrypted packet received from the client.

Traffic to many different SSL servers with different SSL server certificates can be inspected by a single Sourcefire SSL appliance.

2.2.2 Certificate Resigning Method

Figure 2.3 shows an example of the certificate resign decryption method.

> **!** In order to use certificate resign the Sourcefire SSL appliance must be a MITM which means this mechanism cannot be used if the Sourcefire SSL appliance is connected in Passive-Tap mode.

Certificate resign is used when it is impossible to obtain a copy of the SSL server's private key and certificate, which is normally the case for any SSL servers not controlled by the organization deploying the Sourcefire SSL appliance. In general any "outgoing" SSL traffic from an organization will need to be inspected using certificate resign.

The way that certificate resign works is shown in Figure 2.3. The client initiates an SSL session to the server and the server responds by sending its SSL server certificate to the client. As all traffic between client and server passes through the Sourcefire SSL appliance it can detect and intercept the server certificate.

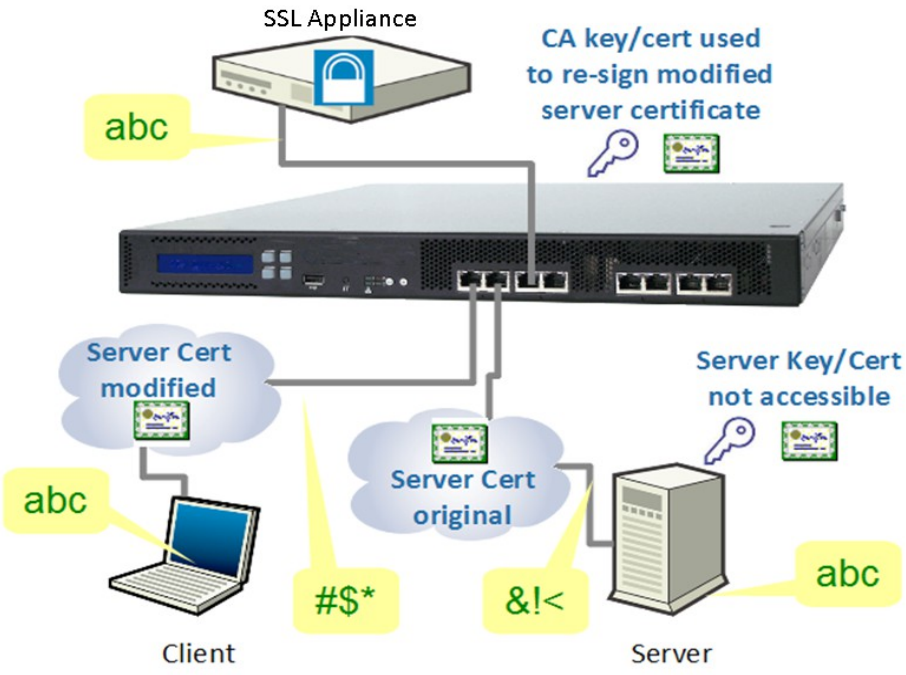


Figure 2.3: Certificate Resign Decryption Method - Passive-Inline mode

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Once the Sourcefire SSL appliance has intercepted the server certificate, it replaces the server's public keys with its own public keys and modifies the Certificate Revocation List (CRL) details in the server certificate. Having modified the server certificate, the Sourcefire SSL appliance then resigns the server certificate using a Certificate Authority (CA) certificate and CA private key that is installed in the Sourcefire SSL appliance.

The resigned server certificate is then sent over the network to the client. If the client trusts the CA that was used to sign the server certificate it receives it will not generate any warnings. As the modified server certificate now contains public keys that are associated with private keys within the Sourcefire SSL appliance, it is possible for the Sourcefire SSL appliance to inspect the traffic.

When certificate resign is used, the two SSL sessions will always have different cryptographic session details and the Sourcefire SSL appliance will have to re-encrypt the plaintext before sending it back to the network.

As noted above, the client must trust the CA used to resign the server certificate; otherwise it will generate warnings indicating that the SSL session should not be trusted. In order to ensure that the client does trust the CA used by the Sourcefire SSL appliance, there are two approaches that can be taken.

1. The Sourcefire SSL appliance can generate a CA certificate and keys internally and use these to resign server certificates. The CA certificate which includes the CA public key can be exported from the Sourcefire SSL appliance, and then imported into the trusted CA store on the client; you only have to do this once.
2. If the Sourcefire SSL appliance is deployed in a network that already has a private public key infrastructure (PKI), this can be used to issue an intermediate CA certificate and keys which can be loaded into the Sourcefire SSL appliance. As the intermediate CA is issued by the enterprise root CA it, will automatically be trusted by all clients in the enterprise, as will all server certificates that are signed by the intermediate CA.

Use of EC-signed Server Certificates

Certificate authorities may sign server certificates with either RSA or EC keys.

If the system tries to use certificate resign to inspect a flow that has a server certificate signed by a CA using Elliptic keys, and it resigns with an internal CA that uses RSA keys, it won't work. The CA used to resign the server certificate must use the same type of key as the original CA.

Hence, the Sourcefire SSL appliance must have two internal CAs on the appliance, one that uses RSA keys, and another using Elliptic keys. You can create or load keys that use either RSA or Elliptic keys for use in resigning server certificates.

In the SSL inspection rules, you can specify an internal CA that uses RSA keys, and another that uses Elliptic keys. If a CA using Elliptic keys is not present, a flow with an EC signed server cert will not match the rule, and will normally be cut through.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

2.2.3 Self-Signed Server Certificate Handling

Some SSL servers have server certificates that are self-signed, meaning the server generated the certificate and keys and then signed the certificate itself, rather than having the certificate signed by a Certificate Authority (CA). Self-signed certificates are inherently less trustworthy than certificates signed by a trusted CA, so some organizations may have a policy of not allowing SSL connections to servers that are using a self-signed certificate. The Sourcefire SSL appliance can be used to enforce such policies (see Section 2.4.2).

If SSL connections to servers using self-signed certificates are allowed, the Sourcefire SSL appliance can inspect the traffic two ways.

- Resign the certificate the same way a none self-signed certificate is resigned; see Section 2.2.2. This method is used if "Decrypt (Resign)" mode is chosen.
- The second method involves the self-signed certificate information (that is, serial number, subject and issuer) not being modified and only the public key and signature in the X.509 structure being replaced, effectively keeping the certificate self-signed. This method is used if "Replace Key Only" mode is used.

If the Sourcefire SSL appliance policy control has been used to block all traffic to servers using self-signed certificates, it is possible to explicitly allow traffic to a specific server using a self-signed certificate by loading a copy of the self-signed certificate into the Trusted Certificates store in the Sourcefire SSL appliance.

2.2.4 Decryption Methods in Cooperative Configurations

In some circumstances the Sourcefire SSL appliance may be deployed in networks that already have an SSL proxy device in place that is inspecting some of the outgoing SSL traffic using certificate resign. The Sourcefire SSL appliance would typically be deployed in order to allow other security appliances to view inspected traffic in addition to the existing proxy device that may not have an ability to pass inspected traffic to other devices. There are two possible ways to address this type of deployment and these are detailed below.

Figure 2.4 shows a cooperative configuration with the Sourcefire SSL appliance deployed in Passive-Inline mode using certificate resign. In this configuration both the existing SSL proxy and the Sourcefire SSL appliance are MITM devices. The existing proxy resigns the original server certificate and then the Sourcefire SSL appliance resigns the modified server certificate it receives. In order for this configuration to work the Sourcefire SSL appliance must trust the CA that the existing proxy uses to resign server certificates and the client must trust the CA used by the Sourcefire SSL appliance. To simplify things it is possible to add the CA used by the existing proxy to the trusted CA store in the Sourcefire SSL appliance and to use the same CA in the Sourcefire SSL appliance for certificate resign which avoids the need for multiple CA certificates and removes the need to add an additional CA to the trust store on the client.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

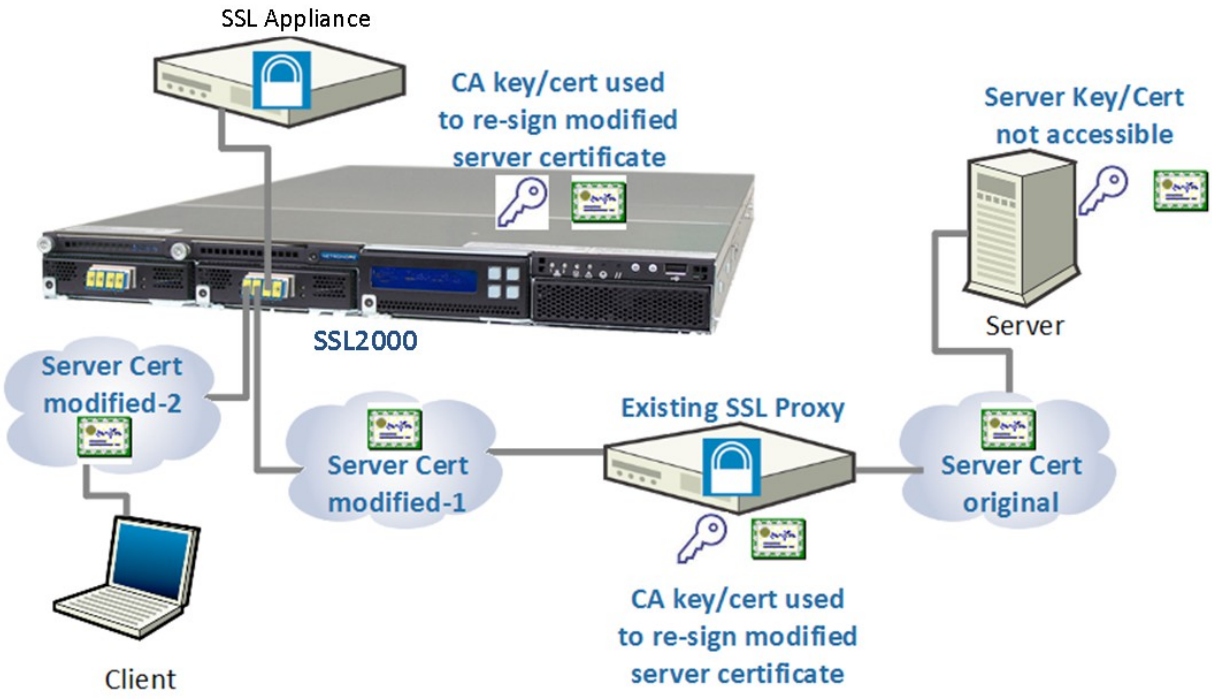


Figure 2.4 Certificate Resign Decryption Method in a Cooperative Deployment

2.2.5 Marking SSL Plaintext

The generated flow containing plaintext obtained from inspected SSL traffic can optionally be marked by the Sourcefire SSL appliance, by modifying the source MAC address or by adding a VLAN tag to allow an attached device to distinguish this traffic from other traffic that was not inspected.

In Active-Inline mode a marking method must be selected, as the Sourcefire SSL appliance needs to be able to distinguish returned plaintext traffic from other forwarded traffic. In Passive-Tap or Passive-Inline mode it is optional to have generated text marked. If modifying the source MAC address is enabled, the source MAC address is always set to 00:15:4D:00:00:D5. The VLAN tag value can be specified as part of the segment configuration if VLAN marking is being used.

2.3 Deployment Modes

This section provides details on how the Sourcefire SSL appliance can be deployed in a network and how it operates in each of the deployment modes. The deployment mode is configured for a segment; each segment will use a number of network interfaces on the Sourcefire SSL appliance. There may be multiple segments configured on a single Sourcefire SSL appliance; each segment is independent of the other segments. A

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

network interface can only be associated with a single segment.

Before looking at the deployment modes in more detail we need to define some terminology that is common to all deployment modes

- Network port: A network interface that is either part of the "bump-in-the wire" or is connected to a network tap device.
- Device port: A network interface that is connected to the primary attached appliance which is dealing with inspected traffic from the Sourcefire SSL appliance.
- Copy port: A network interface connected to a secondary passive appliance that is receiving a copy of the inspected traffic.
- Aggregation port: A network interface providing a connection to an additional network tap, so that a segment can receive traffic from more than one network tap.
- Symmetric traffic: Traffic where packets for both directions of a network flow are seen on the same network interface on the Sourcefire SSL appliance.
- Asymmetric traffic: Traffic where the packets for both directions of a network flow are seen on different network interfaces on the Sourcefire SSL appliance.
- Active-active: An HA deployment scenario where packets on a given flow may be sent over either of the HA network links. From the SSL Inspector's perspective this is equivalent to the Asymmetric traffic scenario, in that packets belonging to a single flow may arrive on either one of two different network interfaces.

There are three main deployment modes for the Sourcefire SSL appliance, with many variants within each mode. The following sections describe the way each of the modes operates. For details on how to configure a segment and its mode of operation refer to Sections 4.6, 4.7, 4.8 and 5.3.2.

Note: The actual physical interfaces on the Sourcefire SSL appliance that are used by a particular segment are allocated when the segment is activated. The WebUI allows the user to choose the network interfaces to be used from the set of interfaces that are not currently in use by other, already active, segments.

Segment Elements

The configuration of a segment can be considered to have five elements; not all of these elements will apply to a given segment:

- The network interfaces connecting traffic to the Sourcefire SSL appliance. In a passive-tap mode, the minimum number of such interfaces is one. In an in-line mode, the minimum number will be two, as the Sourcefire SSL appliance is a bump-in-the-wire.
- Whether the traffic being inspected is symmetric or asymmetric. If the traffic is asymmetric, more network interfaces will be required as the Sourcefire SSL appliance must see the packets for both directions of an SSL flow if it is going to be able to inspect the flow.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- Whether there is an active appliance connected to the Sourcefire SSL appliance. An active appliance will require a minimum of two interfaces connecting it to the Sourcefire SSL appliance.
- Whether there are any passive appliances connected to the Sourcefire SSL appliance. A passive appliance will require a minimum of one interface connecting it to the Sourcefire SSL appliance.
- Whether there is more than one passive appliance connected to the Sourcefire SSL appliance. If more than one passive appliance is connected, then decide if all traffic should be copied to each passive appliance, or it it should be load balanced between the passive appliances.

2.3.1 Passive-Tap Mode

This section provides details on all the different Passive-Tap modes of operation supported by the Sourcefire SSL appliance. Passive-Tap mode connectivity options fall into three groups based on:

- Is the Sourcefire SSL appliance connected to a single tap device that provides traffic for both directions of a flow over the single (bi-directional) tap port? This is a symmetric traffic case.
- Is the Sourcefire SSL appliance connected to two tap devices with each tap device providing traffic for one direction of the flow? This is an asymmetric traffic case.
- Is the Sourcefire SSL appliance connected to more than one bi-directional tap port and aggregating traffic from all the tap ports into a single segment? This is an aggregated traffic case.

Only known server key decryption can be used when the Sourcefire SSL appliance is deployed in Passive-Tap mode.

If Diffie-Hellman is used for key exchange then the Sourcefire SSL appliance will be unable to decrypt the flow using the know server key methods when it is connected in Passive-Tap mode.

One common use for Passive-Tap mode is to connect the Sourcefire SSL appliance to the network configured to not inspect any SSL traffic but with the session log enabled. This is a quick way to collect session log data on all of the SSL traffic in the network and does not require access to any certificates or keys. Analysis of the session log provides a detailed picture of the SSL traffic in the network and can be used to plan what traffic needs to be inspected and how the Sourcefire SSL appliance will need connecting to the network in order to achieve this.

The simplest passive-tap modes deal with symmetric traffic being inspected.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

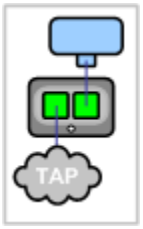


Figure 2.5: PT-sym

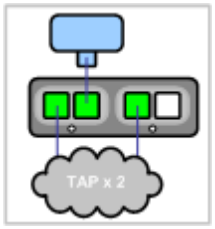


Figure 2.6: PT-sym-ag2

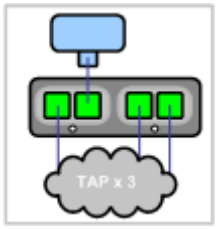


Figure 2.7: PT-sym-ag3

Figure 2.5 shows the simplest passive-tap deployment with the Sourcefire SSL appliance connected to a tap that delivers symmetric traffic to the Sourcefire SSL appliance over a single network interface. The inspected traffic is then sent to a single passive appliance as symmetric traffic over a single network Interface.

Figure 2.6 and Figure 2.7 show deployments that use the aggregation capabilities of the Sourcefire SSL appliance to combine traffic from two or three network taps onto a single Sourcefire SSL appliance segment. In both these examples the inspected traffic is sent to a single attached appliance as symmetric traffic over a single interface (Device port).

> **!** If two tap ports are being used in aggregation mode and are connected to interfaces that share fail-to-wire hardware, then whenever the FTW is active the two taps will be connected to each other. You are advised to ensure that this will not cause problems for the tap ports or the network.

Any of the above modes can be configured to use an additional two interfaces (copy ports) for connection to additional attached passive appliances. If a single copy port is used, it will feed a copy of the symmetric traffic from the Sourcefire SSL appliance to the first passive appliance. If two copy ports are used, then these can be used to either:

- feed a copy of the symmetric traffic to a second and third passive appliance
- feed an asymmetric copy of the traffic to a second passive appliance
- load balance the symmetric traffic to a second and third passive appliance

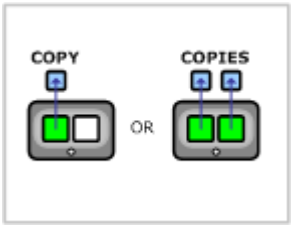


Figure 2.8 Copy Options for Symmetric PT Mode

The copy options for all three of the above operating modes are shown in Figure 2.8.

Passive-tap mode that supports inspection of asymmetric traffic is shown in Figure 2.9, Figure 2.10 shows the copy options available for this mode of operation.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

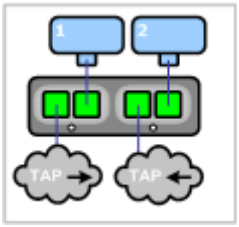


Figure 2.9 PT-asym

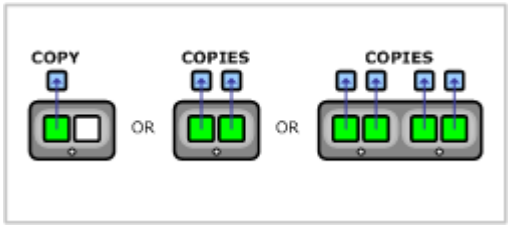


Figure 2.10 Copy Options for Asymmetric PT Mode

If no copy ports are used then a single passive appliance will receive the asymmetric traffic from the Sourcefire SSL appliance over the two device ports.

If a single copy port is used then it will feed a symmetric copy of the asymmetric traffic from the Sourcefire SSL appliance to a second passive appliance. If two interfaces are used then these can be used to either:

- feed a copy of the asymmetric traffic to a second passive appliance
- feed a symmetric copy of the traffic to a second and third passive appliance
- load balance the symmetric traffic to a second and third passive appliance

If four interfaces are used then these can be used to either:

- feed a copy of the asymmetric traffic to a second and third passive appliance
- load balance the asymmetric traffic to a second and third passive appliance

2.3.2 Passive-Inline Mode

This section provides details on all the different Passive-Inline modes of operation supported by the Sourcefire SSL appliance. Passive-Inline mode connectivity options fall into two groups based on:

- Is the Sourcefire SSL appliance connected inline on a network segment that carries traffic for both directions of a flow? This is a symmetric traffic case.
- Is the Sourcefire SSL appliance connected inline on two network segments with packets for a given flow potentially being present on one or other segment? This is an asymmetric traffic case.

Note: If the Sourcefire SSL appliance is being deployed in a network using an active-active HA architecture, this can be treated as an asymmetric traffic case. The Sourcefire SSL appliance can be configured as an in-line device in both active links in the HA network and will treat these as a single Segment internally. It does not matter which packets on a given flow occur on which of the active-active links.

Figure 2.11 shows the simple Passive-Inline configuration. Figure 2.12 shows the copy port options that are available. In Passive-Inline mode there are no device ports configured as part of the initial segment configuration, so all attached appliances are connected to copy ports.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

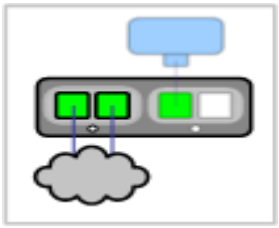


Figure 2.11 PI-sym

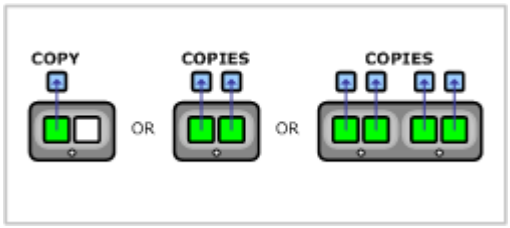


Figure 2.12 Symmetric PI Mode Copy Options

If a single copy port interface is used, it will feed a symmetric copy of the symmetric traffic from the Sourcefire SSL appliance to the first passive appliance. If two interfaces are used, they can either

- feed a copy of the symmetric traffic to the first and second passive appliances
- feed an asymmetric copy of the traffic to the first passive appliance
- load balance the symmetric traffic to the first and second passive appliances

If four interfaces are used, they can be used to either:

- feed an asymmetric copy of the traffic to the first and second passive appliances
- load balance an asymmetric copy of the traffic to the first and second passive appliances
- load balance the asymmetric traffic to a second and third passive appliance

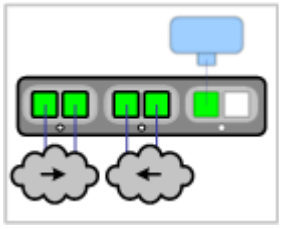


Figure 2.13: PI-asym

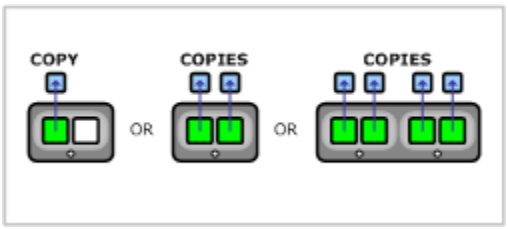


Figure 2.14: Copy options for asymmetric PI mode

Use Passive-Inline mode to inspect asymmetric traffic, as shown in Figure 2.13. The copy port options are shown in Figure 2.14. In Passive-Inline mode there are no device ports configured as part of the initial segment configuration so all attached appliances are connected to copy ports.

If a single copy port interface is used, it will feed a symmetric copy of the symmetric traffic from the Sourcefire SSL appliance to the first passive appliance. If two interfaces are used, they can either:

- feed a copy of the symmetric traffic to the first and second passive appliances
- feed an asymmetric copy of the traffic to the first passive appliance
- load balance the symmetric traffic to the first and second passive appliances

If four interfaces are used, they can be used to either:

- feed an asymmetric copy of the traffic to the first and second passive appliances
- load balance an asymmetric copy of the traffic to the first and second passive

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

appliances

- load balance the asymmetric traffic to a second and third passive appliance

2.3.3 Active-Inline Mode

This section provides details on all the different Active-Inline modes of operation supported by the Sourcefire SSL appliance. Active-Inline mode connectivity options fall into two groups based on:

- Is the Sourcefire SSL appliance connected inline on a network segment that carries traffic for both directions of a flow? This is a symmetric traffic case.
- Is the Sourcefire SSL appliance connected inline on two network segments with packets for a given flow potentially being present on one or other segment? This is an asymmetric traffic case.

Note: If the Sourcefire SSL appliance is being deployed in a network using an active-active HA architecture then this can be treated as an asymmetric traffic case. The Sourcefire SSL appliance can be configured as an in-line device in both active links in the HA network and will treat these as a single Segment internally. It does not matter which packets on a given flow occur on which of the active-active links.

All Active-Inline modes of operation have an active appliance attached to the Sourcefire SSL appliance via the device ports, the way in which the active appliance is connected determines how traffic flows in the event of a failure of the Sourcefire SSL appliance. Fail-To-Appliance (FTA) mode results in traffic flowing through the attached active appliance in the event of failure, while Fail-To-Network (FTN) mode results in traffic bypassing the active appliance in the event of failure.

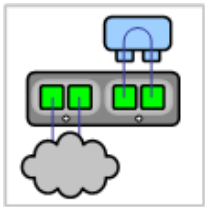


Figure 2.15: AI-sym FTN

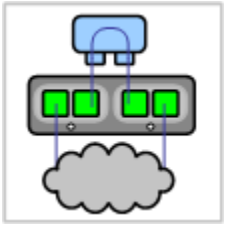


Figure 2.16: AI-sym FTA

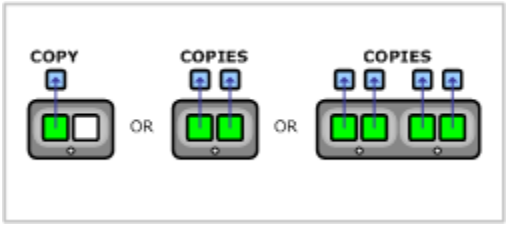


Figure 2.17: Copy Modes for Active-Inline with Symmetric Traffic

Figure 2.15 and Figure 2.16 show Active-inline modes for situations where symmetric traffic is passing through the Sourcefire SSL appliance. Figure 2.17 shows the copy port options available in Active-inline mode.

If a single copy port interface is used, it will feed a symmetric copy of the symmetric traffic from the Sourcefire SSL appliance to the first passive appliance. If two interfaces are used, they can either:

- feed a copy of the symmetric traffic to the first and second passive appliances
- feed an asymmetric copy of the traffic to the first passive appliance

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- load balance the symmetric traffic to the first and second passive appliances

If four interfaces are used, they can be used to either:

- feed an asymmetric copy of the traffic to the first and second passive appliances
- load balance an asymmetric copy of the traffic to the first and second passive appliances
- load balance the asymmetric traffic to a second and third passive appliance

Active-inline mode for dealing with asymmetric traffic is shown in Figure 2.18 and Figure 2.19. Figure 2.17 shows the copy port options.

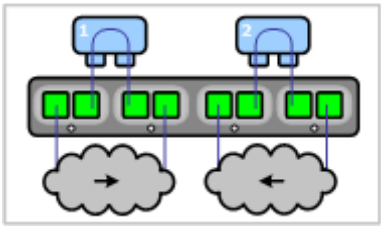


Figure 2.18: AI-asym FTA

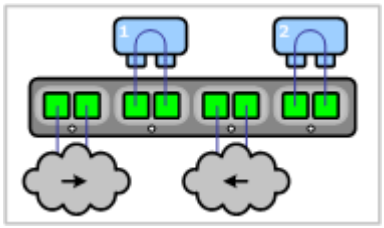


Figure 2.19: AI-asym FTN

If a single copy port interface is used, it will feed a symmetric copy of the symmetric traffic from the Sourcefire SSL appliance to the first passive appliance. If two interfaces are used, they can either:

- feed a copy of the symmetric traffic to the first and second passive appliances
- feed an asymmetric copy of the traffic to the first passive appliance
- load balance the symmetric traffic to the first and second passive appliances

If four interfaces are used, they can be used to either:

- feed an asymmetric copy of the traffic to the first and second passive appliances
- load balance an asymmetric copy of the traffic to the first and second passive appliances
- load balance the asymmetric traffic to a second and third passive appliance

2.4 Policies

Policies in the Sourcefire SSL appliance are composed of three elements:

- Lists
- Segments
- Rulesets

Lists are used to collect multiple items of the same type of information so that a single ruleset can point to the list and will be applied whenever any of the items in the list are true. For example, a list may contain 20 different Subject/Domain Names (S/DN) that occur in the server certificates from 20 different sites. A policy that is configured to

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

"inspect" traffic when it detects a particular Subject/Domain Name can point to the list instead of just indicating a single Domain Name in the policy. This allows a single policy entry to apply to all 20 different sites and means that additional sites can be added (by editing the list) without needing to edit the ruleset.

A segment is a grouping of interfaces that receives a network feed; it tells the Sourcefire SSL appliance which Ruleset to use and in what deployment mode to operate with that network feed, and how to distributed the decrypted SSL and other received traffic. A segment contains some policy information, and is linked to a ruleset that contains the majority of the policy information. Lists are used within rulesets to make it easier to have policies that apply to many different SSL sessions.

The system can have multiple segments defined and can have more than one segment active at any point in time. For example a system could have six rulesets defined (ruleset1 to ruleset6) and might have two active segments each using different ports on the SSL2000 and SSL8200. Segment A could be using ruleset1 and segment 2 ruleset4 or both segments A and B could be using ruleset3. Inactive segments are not associated with physically ports on the SSL2000 and SSL8200 until the point at which they are activated.

A segment is created by selecting one of the Deployment modes, described in Section 2.3. The system will allocate external ports on the Sourcefire SSL appliance that are used by this segment when it is activated. As part of creating the segment a number of default policy actions are defined which apply specifically to the segment. Some of these can be overridden by more explicit policies that are defined in the ruleset associated with this segment.

Policies can be used in the Sourcefire SSL appliance to control the following:

- Which SSL sessions are inspected
- What decryption method is used to inspect a specific session
- Whether an SSL session that is not being inspected is cut through or dropped
- Whether SSL sessions using specific cipher suites are allowed across the network
- How SSL sessions that cannot be decrypted are handled
- How SSL sessions with specific certificate status are handled
- How SSL session to servers using self-signed certificates are handled

2.4.1 Segment Policies

The policies that form part of the segment definition are created with default values which can then be modified. A segment contains policy settings as shown in Table 4.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Item	Default Setting	Notes
Name		Identifies this segment configuration
Comment		Optional descriptive text
Mode		Operating mode for segment chosen from list
Rule set		Name of ruleset used by segment
Session log	Disabled	Enable or disable SSL session log for this segment
Compression	Cut through	The block has policy definitions for how SSL flows that cannot be decrypted are handled on this segment. The cipher suite setting consults a list of cipher suites that cannot be decrypted by the SSL2000 and SSL8200
SSL v2	Cut through	
Diffie-Hellman Passive-Tap mode	Cut through	
Client Certificate	Reject	
Cipher suite	Cut through	
Uncached session	Cut through	
Invalid Issuer		This block has policy definitions that define how to handle specific conditions that occur in the SSL server certificate for a session. The Segment/Rule priority setting determines whether a rule in the ruleset takes priority or is overridden by the segment rule
Invalid Signature		
Expired		
Not yet valid		
Self-signed		
Segment/rule priority	Rule over Segment	

Table 4 Segment Policy Options

2.4.2 Ruleset Policies

A ruleset has a fixed set of operations and a variable number of rules. A rule is used to match against a specific SSL flow or set of flows. The Sourcefire SSL appliance can be very specific in matching a flow using a rule, be more general by using a list of rules, or be “generic” in matching all flows. Modify the parameters of a rule, and the structure of a ruleset to achieve the granularity you want. In the following tables any entry where the Default Setting field is empty means that the default setting is the "nothing is set" option.

The Sourcefire SSL appliance extracts CN, Subject Alternative Name (SAN), and Server Name Indication (SNI) information from intercepted flows in order to deduce the SSL server domain name. The SSL flows are matched against rules using this process:

1. The Sourcefire SSL appliance policy rules support the following subject distinguished name (DN) attributes:
    - CN: Common Name

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- O: Organization
- OU: Organizational Unit
- C: Country

2. Subject/Domain Name and Subject/Domain Name List match field entries without a prefix, as as well as all Domain Name List match field entries, are treated as domain names, and are matched against the domain name deduced from the SSL flow. The rules match fields can contain "*" wild card characters, which will be expanded when matching. For example, a rule match field domain name "*.company.com" will match SSL flows with domain names.
    - The Sourcefire SSL appliance matches the SNI hostname from the SSL flow to the server certificate's subject CN and SAN entries. If a match is found, the SNI hostname is treated as the flow's domain name. If there is no SNI hostname in the flow, or if it does not match any subject CN or SAN entries, the union of all {subject CNS, SAN entries} is considered as possible domain names.
    - The Sourcefire SSL appliance matches the deduced domain name(s) to the domain name match fields in the rule match fields. If a domain name matches, the match field is considered to match.

Table 5 shows the basic set of policy options contained in a ruleset. A single ruleset can have one or more rules. The details relating to rules themselves are shown in more detail later in this section.

Item	Default Setting	Notes
Name		Identifies this ruleset
Default RSA Internal Certificate Authority		Default RSA CA used for certificate resign
Default EC Internal Certificate Authority		Default EC CA used for certificate resign
External Certificate Authorities	All external CAs	Can point to a custom list instead
Certificate Revocation Lists	All CRL lists	Can point to a custom list instead
Trusted Certificates		Optional list
Catch All Action	Cut through	Catch all action: cut, reject or drop
Rules		Rules are of different types (see below) depending on what action they specify
Host Categorization IP Exclude List		IP list used to prevent Host Categorization lookup.

Table 5 Ruleset Policy Options

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

There are six different types of rules that can occur within a ruleset and any type can occur multiple times or not at all in a given ruleset. Each rule contains multiple match fields that can be configured and these fields are compared with the corresponding values in an SSL session to determine if the rule should be applied to the session or not. Any match fields that are left empty are treated as matching any value for that field. The seven different rule types allow for a total of eight possible actions that can be taken if a rule is matched; these are listed in Table 6.

Action	Type ID
Decrypt (Certificate and Key known)	1
Replace Key Only	2
Replace Certificate and Key	3
Decrypt (Resign Certificate)	4
Decrypt (Anonymous Diffie-Hellman)	5
Cut Through	6
Drop	6
Reject	6

Table 6 Actions that can be Specified in a Rule

Some of the match fields can point to lists which allows a single rule entry to be triggered by more than one set of matching criteria. If there is a field to point to a specific item, and another field to point to a list of these items, the fields are mutually exclusive: only one of the fields can be used.

In the following tables mutually exclusive fields are shown by arrows (↓↑) in the default setting column.

Note: The Subject/Domain Name, Subject/Domain Name List, and Domain Name List are mutually exclusive.

If a rule in a ruleset cannot be applied due to the mode of operation of the segment, it will be ignored and a warning will be logged. For example, a rule that specifies decryption using certificate resign cannot be applied if the segment is operating in Passive-Tap mode.

Table 7 shows details for a Decrypt (Certificate and Key known) rule that will trigger decryption using a known server key and certificate if the details in the server certificate for a session match the rule.

Item	Default Setting	Notes
Decrypt (Certificate and Key known)		Decrypt using known key and certificate
Comment		Optional descriptive text
Known Certificate with Key	↓	Pointer to a single certificate/key value

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Item	Default Setting	Notes
Known Certificates with Keys	↑All Known	Name of a list of certificate/key pairs that is checked for a match
Source IP	↓	IP address and mask so can specify subnet
Source IP List	↑	Name of list of source address/masks that is checked for a match
Destination IP	↓	IP address and mask so can specify subnet
Destination IP List	↑	Name of list of destination address/masks that is checked for a match
Destination Port		Destination TCP port number
Host Categorization List		Name of Host Categorization List checked for a match.

Table 7 Decrypt with Known Certificate and Key Rule Format

Table 8 shows details for a Replace Certificate and Key rule that will trigger decryption using a certificate and key replacement method if the details in the server certificate for a session match the rule. Some of the match fields can point to lists, which allows a single rule entry to be triggered by more than one set of matching criteria.

Item	Default Setting	Notes
Replace Certificate and Key		Decrypt using key and certificate replacement
Comment		Optional descriptive text
RSA Known Certificate with Key (to replace with)		Pointer to an RSA certificate and key that will be used to replace the certificate and key in the server certificate
EC Known Certificate with Key (to replace with)		Pointer to an EC certificate and key that will be used to replace the certificate and key in the server certificate
Cipher suite list		List of cipher suites; cannot include Anonymous Diffie-Hellman cipher suites
Trusted Certificate	↓	Trusted certificate that is checked for a match
Trusted Certificates	↑	List of Trusted certificates that are checked for a match
Subject/Domain Name	↓	Subject/Domain names checked for a match; server domain names captured via CN, SAN, SNI fields.
Subject/Domain Name List	↑	List of Subject/Domain names checked for a match; server domain names captured via CN, SAN, SNI fields.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Item	Default Setting	Notes
Domain Name List		List of Domain names checked for a match.
Issuer DN	↓	Issuer Subject/Domain Names checked for a match.
Issuer DN List	↑	List of Issuer Subject/Domain Names checked for a match.
Source IP	↓	IP address and mask so can specify subnet
Source IP List	↑	Name of list of source address/masks that is checked for a match
Destination IP	↓	IP address and mask so can specify subnet
Destination IP List	↑	Name of list of destination address/masks that is checked for a match
Destination Port		Destination TCP port number
Certificate Status		Status of X.509 server certificate
Host Categorization List		Name of Host Categorization List checked for a match.

Table 8 Decrypt using Replacement of Key and Certificate Format

Table 9 shows details for a Decrypt (Resign Certificate) rule that will trigger decryption using certificate resign if the details in the server certificate for a session match the rule. Some of the match fields can point to lists, which allows a single rule entry to be triggered by more than one set of matching criteria.

Item	Default Setting	Notes
Decrypt (Resign Certificate)		Decrypt using certificate resign
Comment		Optional descriptive text
RSA Internal CA		Pointer to the internal RSA CA that is used to resign the server certificate
EC Internal CA		Pointer to the internal EC CA that is used to resign the server certificate
Cipher Suite list		List of cipher suites: can't include Anonymous Diffie-Hellman cipher suites
Trusted Certificate	↓	Trusted certificate that is checked for a match
Trusted Certificates	↑	List of Trusted certificates that are checked for a match
Subject/Domain Name	↓	Subject/Domain names checked for a match; Server domain names captured via CN, SAN, SNI fields.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Item	Default Setting	Notes
Subject/Domain Names List	↑	List of server Subject/Domain names checked for a match.
Domain Name List		List of Domain names checked for a match.
Issuer DN	↓	Issuer Subject/Domain Names checked for a match
Issuer DN List	↑	Issuer Subject/Domain Names checked for a match
Source IP	↓	IP address and mask so can specify subnet
Source IP List	↑	Name of list of source address/masks that is checked for a match
Destination IP	↓	IP address and mask so can specify subnet
Destination IP List	↑	Name of list of destination address/masks that is checked for a match
Destination Port		Destination TCP port number
Certificate Status		Status of X.509 server certificate
Host Categorization List		Name of Host Categorization List checked for a match.

Table 9 Decrypt using Certificate Resign Format

Table 10 shows details for a Decrypt (Anonymous Diffie-Hellman) rule that will trigger decryption if the details in the server certificate for a session match the rule. Some of the match fields can point to lists, which allows a single rule entry to be triggered by more than one set of matching criteria.

Item	Default Setting	Notes
Decrypt (Anonymous Diffie-Hellman)		Decrypt Anonymous Diffie-Hellman session
Comment		Optional descriptive text
Source IP	↓	IP address and mask so can specify subnet
Source IP List	↑	Name of list of source address/masks that is checked for a match
Destination IP	↓	IP address and mask so can specify subnet
Destination IP List	↑	Name of list of destination address/masks that is checked for a match
Destination Port		Destination TCP port number
Host Categorization List		Name of Host Categorization List checked for a match.

Table 10 Decrypt Anonymous Diffie-Hellman Format

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Table 11 shows details for Cut Through/Drop/Reject rules that will trigger actions other than decryption, for example, rules that cut sessions through, reject sessions or drop them if the details in the server certificate for a session match the rule. Some of the match fields can point to lists, which allows a single rule entry to be triggered by more than one set of matching criteria.

Item	Default Setting	Notes
Cut Through/Drop/Reject		Actions are cut, reject or drop
Comment		Optional descriptive text
Cipher Suite List		List of cipher suites: can include Anonymous Diffie-Hellman cipher suites
Trusted Certificate	↓	Certificate that is checked for a match
Trusted Certificates	↑	List of Certificates that are checked for a match
Subject/Domain Name	↓	Subject/Domain names checked for a match; server domain names captured via CN, SAN, SNI fields.
Subject/Domain Name List	↑	List of Subject/Domain names checked for a match; server domain names captured via CN, SAN, SNI fields.
Domain Name List		List of Domain names checked for a match.
Issuer Domain Name	↓	Issuer Subject/Domain Names checked for a match.
Issuer Domain Name List	↑	List of Issuer Subject/Domain Names checked for a match.
Source IP	↓	IP address and mask so can specify subnet
Source IP List	↑	Name of list of source address/masks that is checked for a match
Destination IP	↓	IP address and mask so can specify subnet
Destination IP List	↑	Name of list of destination address/masks that is checked for a match
Destination Port		Destination IP port number
Certificate Status		Status of X.509 server certificate
Host Categorization List		Name of Host Categorization List checked for a match.

Table 11 Rules Not Involving Decryption Format

2.4.3 Lists

Lists can be referenced by rules in rulesets and allow a single rule to be applied to more than one flow, as any flow that matches an entry in the list will trigger the rule action.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

For each type of PKI list the system will create a default list that is read only and includes all items of that type present in the system. The default lists have names that begin with "all-" apart from the list of unsupported sites. User-created custom lists are subsets of the default lists.

Table 12 shows the default set of lists that exist within the SSL2000 and SSL8200.

Name	Contains
all-external-certificate-authorities	All trusted external CAs
all-certificate-revocation-lists	All pointers to Certificate Revocation Lists
all-known-certificates	All known server certificates
all-known-certificates-with-keys	All known server private key/certificates
sslng-unsupported-sites	Sites it is not possible to inspect SSL sessions to

Table 12 Default List Types and Contents

Importing new keys or certificates is always done to the relevant **all** list. Adding entries to a custom list is done by selecting entries from the relevant "all" list.

In addition to the above lists, the system can contain lists of:

- **Subject/Domain Names**: Values without explicit distinguished name attribute types are considered domain names; the domain name values are matched against the SNI hostname, the subject Common Names (CNs), and the SAN DNS/IP entries. This includes the **sslng-unsupported-sites** list shown in Table 12.

  Note: Imported pre-3.7 policies using Distinguished Names lists will be converted into Subject/Domain Names lists.

- **Domain Names**: Efficiently match Sourcefire SSL appliance rules against website categories consisting of thousands of Domain Names.

  Note: Imported pre-3.7 policies using Common Names lists will be converted into Domain Names lists.

- Cipher Suites
- IP addresses

The lists of Domain Names and lists of IP addresses are optimized to deal with large numbers of entries in the list as in some circumstances they may be configured with large numbers of entries.

2.4.4 Reset Generation

There are several conditions under which the Sourcefire SSL appliance prematurely terminates TCP connections that pass through it using TCP RST packets. Presently, all of these conditions only apply when the Sourcefire SSL appliance is deployed in Active-Inline or Passive-Inline mode. Thus the device does not terminate connections prematurely in Passive-Tap mode. The appliance generates TCP RST packets when it receives a packet for a flow that triggers a Reject rule, when an undecryptable policy is

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

triggered, or when there is an error in a flow that has been modified so that the remainder of the flow cannot be cut through.

When the Sourcefire SSL appliance determines that it must reject a TCP flow, it releases most of the state associated with that flow and considers the flow terminated. From that point on, the appliance will turn around any packets that it receives and determines to be a part of the original flow into RST packets and transmits them back to the sender.

Thus, if any of the RST packets are lost, packets from the original client or server will trigger RSTs to hang up the connection. An administrator may configure the policy of the appliance to always reject certain flows whenever they arrive. In such a case, the Sourcefire SSL appliance will generate RSTs by turning round packets in flows matching the policy's pattern, but will not spontaneously generate RSTs to send to connection endpoints.

If the Sourcefire SSL appliance rejects a flow, then the appliance also tries to signal both endpoints of the connection about the termination by generating a "spontaneous" TCP RST for each endpoint of the connection. After the initial rejection, any subsequently received packets for the same flow will continue to trigger RSTs back to the sender as described above.

There is one special case for a flow rejection triggered by a TCP SYN. In such a case, there is no server endpoint or state, so the Sourcefire SSL appliance only generates one spontaneous RST to send back to the SYN packet's source. Events that will cause the Sourcefire SSL appliance to generate RST packets are:

- Flows being rejected because of an action configured for dealing with undecryptable flows. For example the presence of a client certificate in a flow that prevents it being inspected.
- Decryption errors on a flow that is modified (where decrypt and re-encrypt are being done). As the flow is modified it cannot simply be cut through after the error.

If the Sourcefire SSL appliance is operating in active-inline mode then the attached inline appliance can also cause the Sourcefire SSL appliance to generate a reset in both directions on an SSL flow that is being inspected. If the inline appliance drops a packet from the generated TCP flow that is carrying the decrypted payload data then the Sourcefire SSL appliance will detect this and generate a RST in both directions on the original SSL flow in order to kill the flow. If the active appliance generates a RST itself on the generated TCP flow then this will be detected by the Sourcefire SSL appliance, and will trigger a RST in each direction on the original SSL flow.

2.5 Failure Modes and High Availability

The Sourcefire SSL appliance can automatically respond to certain types of failures that it detects. The term "failure option" refers to a set of responses that the Sourcefire SSL appliance performs when it detects a particular type of failure.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

There are two types of failures that the Sourcefire SSL appliance can detect and respond to:

- Link failure (interface going down): this is associated with a segment
- Software failure (data-plane):this is associated with the device

A segment is configured to operate in normal mode or High Availability (HA) mode. The failure actions taken by the device will differ depending on whether the segment is configured for HA mode or not. HA mode is not relevant if a segment is operating in Passive-Tap mode so HA mode can only be configured for segments operating in Active-Inline or Passive-Inline mode. The behavior in response to a link failure differs if a segment is operating in HA mode.

In High Availability (HA) mode the failure options are set up to enable the SSL2000 and SSL8200 to propagate failure state to the Ethernet switches that it is connected to in order that the switches can direct traffic to an alternate SSL2000 and SSL8200 system to maintain availability. When not in HA mode link state is not propagated between links on a segment.

Within the system software failures are handled by a failure mode state machine while link failures are handled by a failure mode filter, which is located before the failure mode state machine. If a segment is operating in HA mode then the failure mode filter is active otherwise it is disabled.

The following sections detail how link failures and software failures are dealt with and how segments can be configured to respond to the impact of such failures.

2.5.1 Link Failures

The effect of a link failure on a segment is not configurable, however the segment behavior is different depending on whether it is operating in HA mode or not. Configuring HA mode enables the failure mode filter which is otherwise inactive.

When not operating in HA mode the failure of a link that is one of the links being used by the segment only has the following impact:

- The link state for the affected link will go to down
- The link status LEDs for the affected link will show that the link is down
- The dashboard Network Interfaces status display will show the affected link as down
- The dashboard Segments Status display will show the segment with a yellow background
- The System status indicator will change to red in the status bar at the bottom of the screen
- The Network status indicator will change to red in the status bar at the bottom of the screen
- The event will be logged in the system log

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- If the link is part of the bump in the wire for an in-line segment or is the link to the network tap in PT mode then detection and inspection of SSL traffic will cease
- If the link is a link to an attached passive appliance then SSL detection and inspection will continue even though at least one of the attached passive appliances is no longer receiving the inspected traffic

If the segment is operating in HA mode then the following actions will take place if a link being used by the segment goes down:

- If the segment is Passive-Inline then failure of any segment interface will force all the network facing interfaces in the segment down
- If the segment is Active-Inline then failure of any segment interface, other than those used for mirroring, will force all non-mirrored interfaces in the segment down
- The link state for the affected links will go to down
- The link status LEDs for the affected links will show that the link is down
- The dashboard Network Interfaces status display will show the affected links as down
- The dashboard Segments Status display will show the segment with a red background
- The System status indicator will change to red in the status bar at the bottom of the screen
- The Network status indicator will change to red in the status bar at the bottom of the screen
- The event will be logged in the system log
- Detection and inspection of SSL traffic will cease
- All data-plane failures will be ignored while a segment is in link failure mode
- Recovery from link failure mode is configurable: either by manual reset from the WebUI or by auto recovery when the fault that triggered the failure is removed.

2.5.2 Software (Data-Plane) Failures

Software failures are triggered by one or more checks that are run in the background while the device is operating. These background checks are for the system and not for a specific segment. The subsystem running the checks provides a keep-alive watchdog signal to the failure engine. If the failure engine does not receive the keep alive indication then it triggers the failure mechanism.

The failure mode that becomes active when a failure occurs is configured per segment so a failure may trigger different failure modes for different segments if they are configured differently. Some of the failure modes require manual intervention to exit the mode while others will automatically exit as soon as the condition that caused the

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

failure and any other failure conditions are removed. See Section 5.3.2 for more details.

The various failure modes that can be configured for a segment are:

- Disable Interfaces
- Drop Packets (Auto Recovery)
- Fail-to-wire (Auto Recovery)
- Fail-to-wire (Manual Reset)
- Ignore Failure

Modes that invoke Fail-to-wire cause the hardware mechanisms in the Netmod to activate and connect together pairs of external ports to ensure that traffic continues to flow through the network while the Sourcefire SSL appliance is failed.

During a software failure state any link state changes will be processed as link failures have priority over software failures.

Internally the system generates a recovery event once the issues that caused the software failure have been removed and all run-time tests have succeeded. Automatic recovery will occur once the recovery event occurs as long as the segment is configured to use one of the automatic recovery modes. If a manual recovery mode is in operation then the manual reset will only be accepted after the system has generated a recovery event. Manual recovery is achieved by clicking on the Manually Unfail button on the dashboard. This button will only be enabled if Manual Unfail is allowed and will have an effect; if the condition that triggered the failure has not been resolved then the button will not be active.

2.6 Example Deployment Configurations

This section provides some examples of how the Sourcefire SSL appliance can be deployed alongside other security appliances in order to protect the network against threats carried by SSL traffic.

In all the examples network links shown in red indicate links that are carrying decrypted SSL traffic.

2.6.1 Outbound Inspection

Figure 2.20 shows an outbound monitoring scenario, the monitored web browsers or other SSL clients are located in the private network (intranet), with the monitored servers typically being located in the Internet or in partner's extranets.

For this scenario the Sourcefire SSL appliance is typically deployed adjacent to the firewall or router which leads to the Internet. The Sourcefire SSL appliance needs to be deployed on the public side of the firewall if the firewall itself generates SSL-encrypted traffic which needs to be inspected (for example, if the firewall also includes SSL VPN capabilities) or if the network topology requires deploying the Sourcefire SSL appliance at that location (such as because the firewall also aggregates multiple network

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

segments).

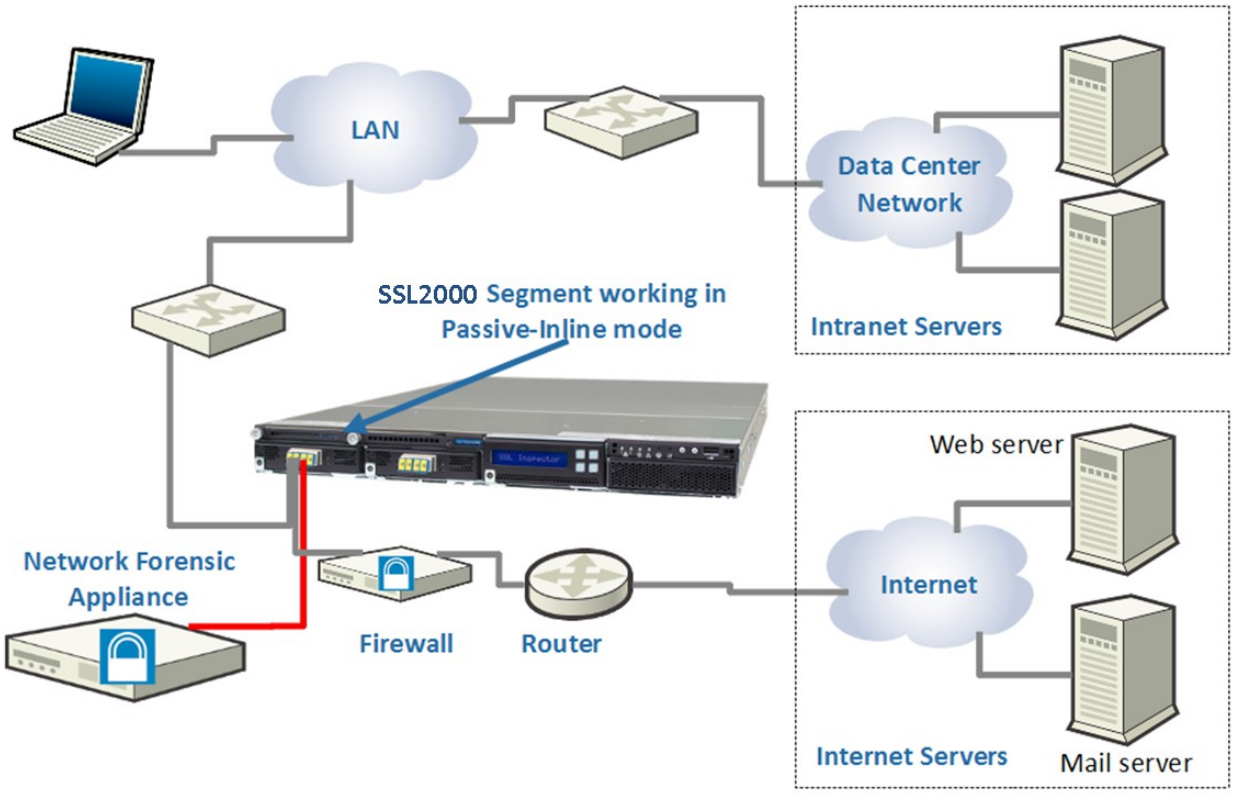


Figure 2.20 Outbound Monitoring with Network Forensic Appliance

For all other cases, deploying the Sourcefire SSL appliance on the private side of the firewall is advisable. In this deployment traffic would be inspected using certificate resign (see Section 2.2.2) as the SSL servers are not under the control of the enterprise deploying the SSL2000 and SSL8200 so it is not possible to obtain copies of the server private key/certificate for these servers. The client systems in this deployment will need to trust the Certificate Authority used by the SSL2000 and SSL8200 to resign server certificates. Figure 2.11 shows the connection mode being used in this example.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

2.6.2 Inbound Inspection

Figure 2.21 shows a deployment where the SSL2000 (alternately, an SSL8200) is connected to a network tap or span port and is delivering decrypted traffic to an Intrusion Detection System and to an Application Performance Monitoring system. The private key and certificate for each of the Intranet servers are loaded into the SSL2000, as it is using known server key mode to decrypt the traffic. Figure 2.5 shows the connection mode being used in this example.

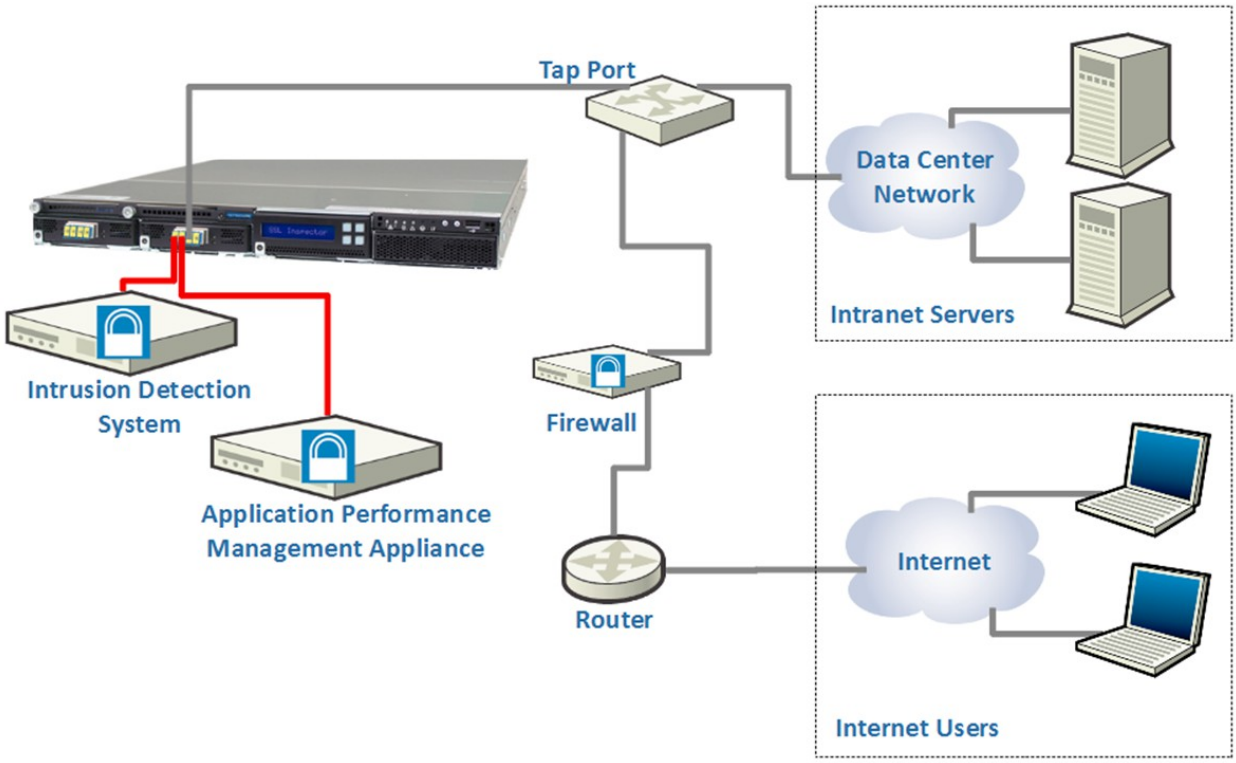


Figure 2.21 Inbound Monitoring with IDS and Application Performance Monitor

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

2.6.3 Inbound and Outbound Inspection

Figure 2.22 shows a deployment where both inbound and outbound traffic are inspected. The IPS in this deployment will be able to detect any threats in inbound sessions heading for the Intranet servers from users on the Internet and at the same time will be able to detect any inbound threats over sessions from users on the LAN to Internet servers. In addition the Network Forensic system will be able to detect and identify any files sent out as webmail attachments by internal users.

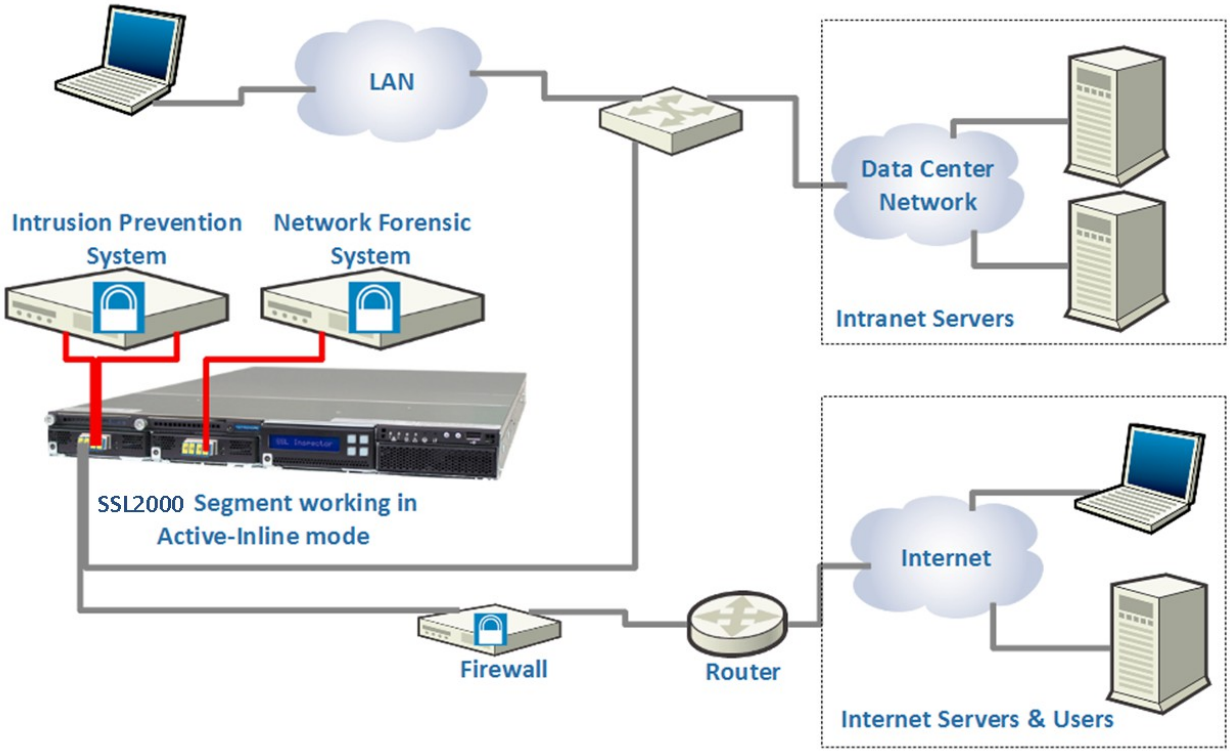


Figure 2.22 Inbound and Outbound Inspection with IPS and Network Forensic Appliances

In this example the SSL2000 will be using both certificate resign and known server key mechanisms to decrypt traffic with the selection of which mode to use being determined by whether an SSL session is incoming or outbound. Figure 2.15 shows the connection mode being used in this example.

2.6.4 High Availability Deployment

Although the Sourcefire SSL appliance segment has fail-to-wire capabilities provided by the Netmod to ensure connectivity, in most scenarios where hardware has failed or software is temporarily not available, some customers prefer to deploy multiple Sourcefire SSL appliances, as this will ensure that in these scenarios traffic continues to be inspected.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

A typical High Availability deployment is depicted in Figure 2.23. Key to this deployment is having the Sourcefire SSL appliance segment configured in HA mode with the software failure mode set to "Disable Interfaces," and with link state mirroring enabled on the Ethernet switch devices.

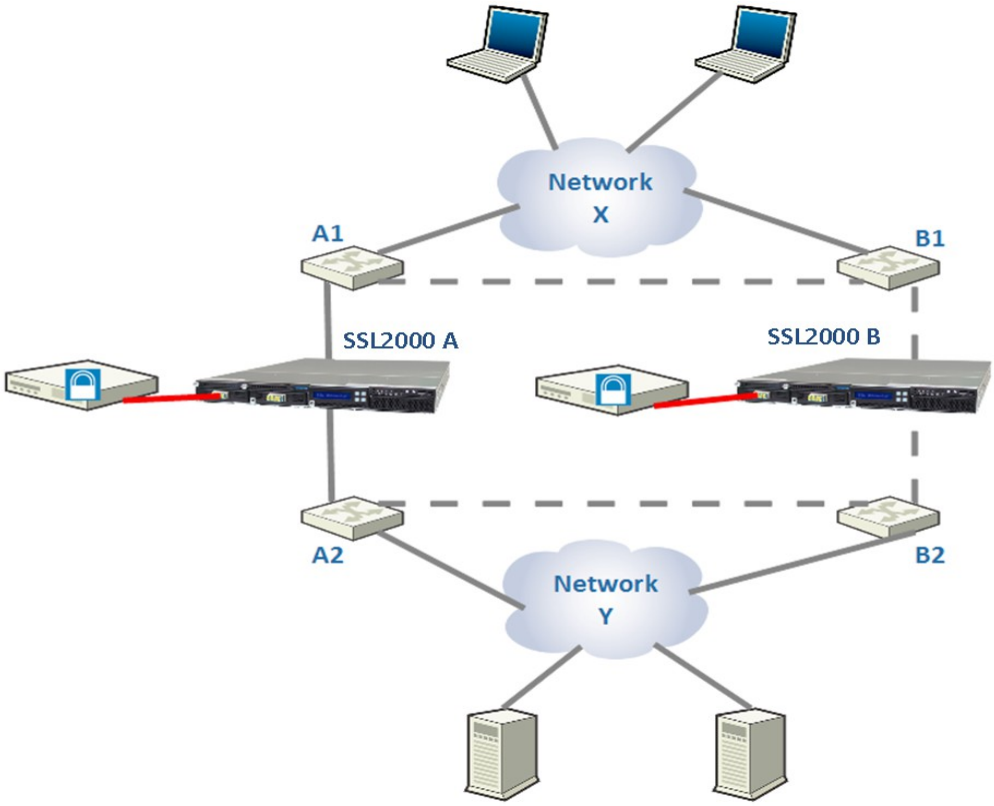


Figure 2.23 High Availability Deployment

Normally switch A1 and A2, Sourcefire SSL appliance A and its attached security appliance(s), will be active. Should any of the links along that path fail, or should the Sourcefire SSL appliance or its attached security appliance or either of the Ethernet switches fail, the link down state will propagate, with standard mechanisms like the Spanning Tree Protocol or the Virtual Router Redundancy Protocol ensuring that traffic is rerouted over the link between switches B1 and B2 that passes through Sourcefire SSL appliance B (dashed line in the figure).

Availability can be further improved by including additional links between switch A1 and B1 and between switch A2 and B2 (shown as dashed lines in Figure 2.23). This ensures that traffic can flow from Network X via A1 to B1, and then through Sourcefire SSL appliance B if required. Depending on the required availability levels and the built-in redundancy features of the switches devices, A1 and B1 may be combined into a single device, with A2 and B2 being similarly combined.

Contact Sourcefire support (support@sourcefire.com) should you require more information with respect to High Availability deployment options.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

3. Physical Installation

This section describes the following procedures:

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

3.1 Safety Information

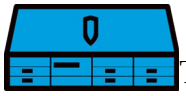
Because this is an electrically powered device, adhere to the warnings and cautions listed in Section 7. when installing or working with the Sourcefire SSL appliance.

> **!** WARNING: Read all the installation instructions before connecting the appliance to its power source. Refer to the important safeguards in Section 7. for information regarding the setup and placement of the Sourcefire SSL appliance.

3.2 Requirements Checklist

The following will be required:

- At least 1U rack space (deep enough for a 27" device):power and management ports at rear
- Phillips (cross-head) screwdriver
- Two available power outlets (110 VAC or 220-240 VAC)
- Two IEC-320 power cords (normal server/PC power cords) should the supplied power cords not be suitable for your environment
- Cooling for an appliance with two 650W power supply units
- One RJ-45 CAT5e/CAT6 Ethernet cable to connect the Sourcefire SSL appliance to the management network (or a local notebook/desktop computer which is used to manage the Sourcefire SSL appliance)
- Appropriate copper or fiber cables to connect Netmods to the network and to associated security appliances



The following will be required:

- At least 2U rack space (deep enough for a 27" device):power and management ports at rear
- Phillips (cross-head) screwdriver
- Two available power outlets (110 VAC or 220-240 VAC)

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- Two IEC-320 power cords (normal server/PC power cords) should the supplied power cords not be suitable for your environment
- Cooling for an appliance with two 750W power supply units
- One RJ-45 CAT5e/CAT6 Ethernet cable to connect the Sourcefire SSL appliance to the management network (or a local notebook/desktop computer which is used to manage the Sourcefire SSL appliance)
- Appropriate copper or fiber cables to connect Netmods to the network and to associated security appliances

3.3 Rack Mounting

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

3.4 Back Panel

The rear of the SSL2000 is shown in3.1, and Table 13 identifies the components. Ventilation holes on the rear panel must not be blocked as free flow of air is essential for system cooling.

Figure 3.1 SSL2000 Back Panel

The rear of the SSL8200 is shown in Figure 3.2 and Table 13 identifies the components. Ventilation holes on the rear panel must not be blocked as free flow of air is essential for system cooling.

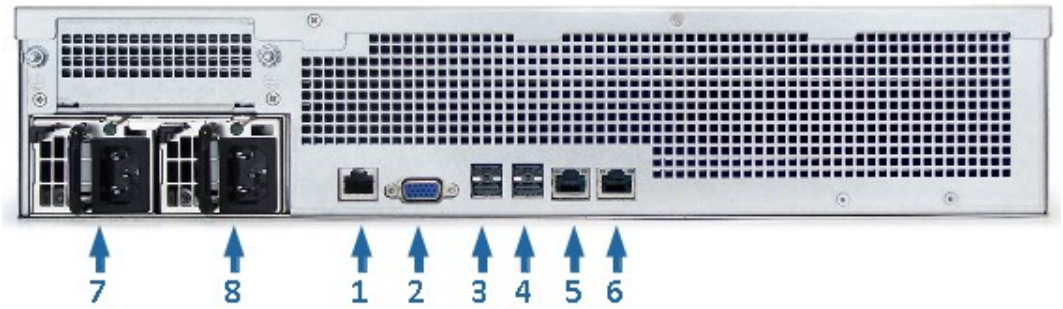


Figure 3.2: SSL8200 Back Panel

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

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*
		*	Not shown in Figure 3.1

Table 13 SSL2000 and SSL8200 Back Panel Components

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

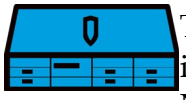
Note: The power supplies are hot swappable and cannot be replaced in while the Sourcefire SSL appliance is powered on and operating.

! Replacement must be done with units supplied by Sourcefire. Use of other units will void any warranty and may damage the system.

3.5 Front Panel

The SSL2000 has three front-facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the three bays to configure the desired combination of interfaces. Figure 3.3 shows an SSL2000 device with three Netmods installed. In this example the Netmods each support 4 x 1Gig copper interfaces.

Figure 3.3 SSL2000 Front Panel



The SSL8200 has 7 front-facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the seven bays to configure the desired combination of interfaces.

! Sourcefire recommends restricting an SSL8200 to supporting a maximum of 16 external interfaces. This means that if 4 x GigE Netmods are used a maximum of four can be installed in the system.

Figure 3.4 shows an SSL8200 device with four Netmods installed. In this example two of the the Netmods each support 4 x GigE fiber interfaces and the other two 4 x GigE copper interfaces.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 3.4 SSL8200 Front Panel

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)
- 2×10G fiber (2 ports of 10GBase-SR with bypass)
- 2 x 10G fiber (2 ports of 10GBase-LR with bypass)

Changing Netmods

! Netmods and the switch module installed in the front-facing bays are NOT hot swappable. Netmods should only be swapped out when the system is powered down.

When the power is off, a Network Module, or the blank plate covering an empty position, may be removed by removing the screw on the front panel (M3×4mm, T8 flat head, black) and pulling the lever out. There is a hole that can be used to pull on the ejector handle.

When the power is off, the Network Modules may be installed as follows:

1. If the Network Module ejector is held in by a screw, remove the screw.
2. Pull out the ejector handle until it is approximately 25mm (1") from the front panel.
3. Insert the Network Module into the empty slot until the protrusion on the right side touches the chassis.
4. Gently press on the ejector handle where the screw normally is, and push the module into the chassis.
5. Make sure the seating plane of the front of the network module is lined up with other modules. It may be necessary to push on the front of the module to fully seat it. If the module cannot be fully seated, try reinserting it, paying attention to the retention mechanism on the right side of the module.
6. Install the screw.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

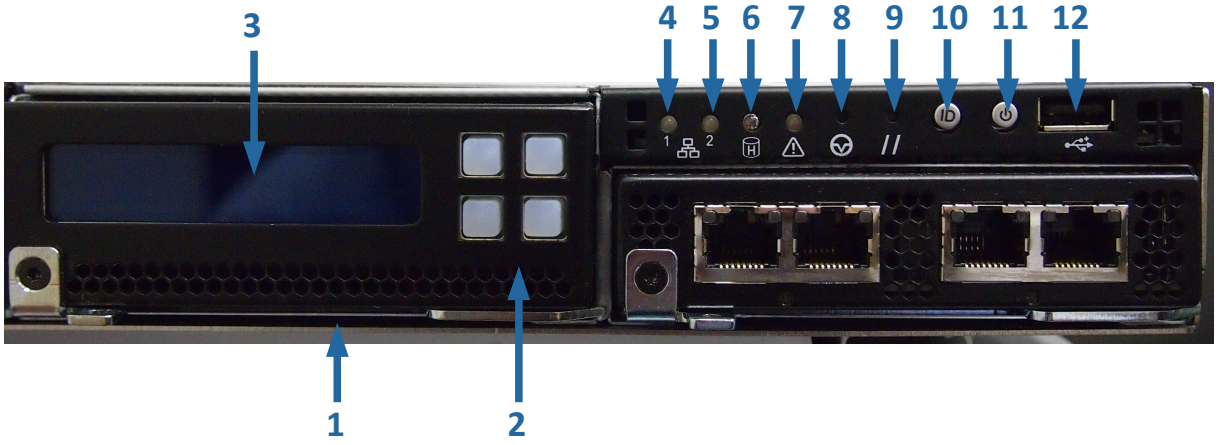


Figure 3.5 SSL2000 Front Panel Controls

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 Figure 3.5 and Table 14 identifies the components. Section 4. provides details on how the front panel components can be used to configure the system. The unit pictured in Figure 3.5 is an SSL2000 and has a 4 x GigE copper Netmod installed in the right hand bay.

The LCD presents license information: the name and expiration date of each licensable component.

Figure 3.6 shows the front panel controls on an SSL8200 and Table 14 identifies the components. Section 4. provides details on how the front panel components can be used to configure the system

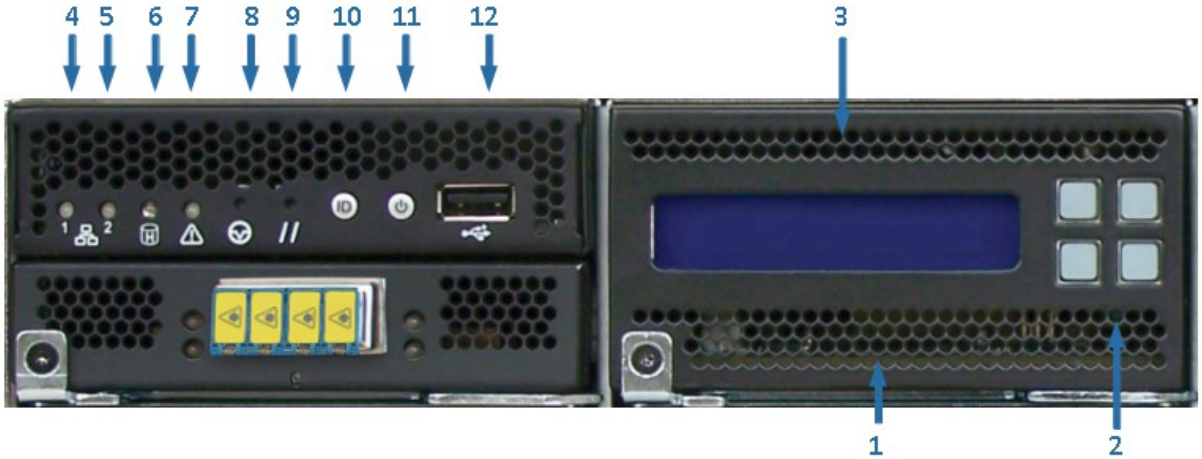


Figure 3.6 SSL8200 Front Panel Controls

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

1	Switch Module	7	System Status Indicator
2	Keypad Array	8	NMI button (recessed)
3	LCD Display	9	Reset button (recessed)
4	Management Ethernet 1 Indicator	10	Identify Button
5	Management Ethernet 2 Indicator	11	Power Button
6	Disk Activity Indicator	12	USB socket

Table 14: SSL2000 Front Panel Components

The front panel status LEDs for the management Ethernets 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 indicate different system states.

Table 15 shows the various system states that can be indicated by the system status LED on the front panel of the unit.

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.

Note: The NMI button should not be pressed during normal operation as it may cause the system to halt.

If the NMI button is pressed this fact will be recorded in the system log file.

The ID button if pressed will cause a blue LED on the rear panel to the left of the serial port to illuminate. This LED is located behind the back panel so it is visible through the ventilation holes. The purpose of this LED is to make it easier to locate a system when it is racked in a stack with other systems.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

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

Table 15: SSL2000 System Status Indicators

3.6 Connecting to the Network

The SSL2000 and SSL8200 products have front facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the bays to configure the desired combination of interfaces. Figure 3.3 shows an SSL2000 device with three Netmods installed. In this example the Netmods each support 4×1Gig copper interfaces. 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 10G fiber (2 ports of 10GBase-SR with bypass)
- 2 x 10G fiber (2 ports of 10GBase-LR with bypass)

! **Netmods and the switch module installed in the front-facing bays are NOT hot swappable.** Netmods should only be swapped out when the system is powered down.

Ports are numbered from left to right and top to bottom in the case of the SSL8200 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.

Note: 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.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

4. Initial Configuration and Setup

The Sourcefire SSL appliance is configured and managed using a Web based User Interface (WebUI) which provides a graphical means to configure the device. The front panel keypad and display can be used to configure the management network settings for the device and are also used during initial bootstrap mode and to unlock the master key during system start up.

Note: The Sourcefire SSL appliance is factory configured to use DHCP to acquire an IP address for the management Ethernet. The front panel keypad and LCD can be used to configure a different fixed IP address.

You will see several start up messages before the appliance boots up. Here is the series:

Figure 4.1 Boot up Screens

4.1 Bootstrap Phase

Every time that the Sourcefire SSL appliance is powered on or re-booted it goes through a number of stages before reaching the fully operational state; these stages are termed the "bootstrap" phase.

As soon as the Sourcefire SSL appliance is powered on it can be forced into one of three states by typing in the correct sequence on the front panel keypad. To enter factory default reset mode the key sequence must be typed within five seconds of seeing the

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

"Appliance Startup Loading" message; key sequences for other states can be typed at any time.

- Enter code on keypad to enter one of three states
  - Factory default reset
  - IP configuration mode
  - PIN entry mode

The front panel keypad shown in Figure 3.5 and Figure 3.6 has the keys arranged in the following layout:

0	1
2	3

Table 16: Keypad Layout

The following key sequences are used to enter one of the three states described above.

Sequence	State Entered
31203	Factory default reset
01320132	IP configuration mode
1230123	PIN entry mode

Table 17: SSL2000 Power On Key Sequences

Factory default reset and IP configuration mode can both be run before the system enters the main bootstrap phase. Factory default reset causes the box to reset and erases all configuration and other data on the system, returning it to exactly the same state as when it was received from the factory.

> **!** The factory default sequence only works after the LCD turns on and says "Loading..." on the second line. You have 5 seconds to enter the sequence at this point.

IP configuration mode lets the management network be configured to use a static IP address. By default the system will attempt to obtain an IP address using DHCP. The IP address settings will then be used during the bootstrap phase and will be saved so it is used after the bootstrap phase is over. Pin entry mode is explained later in this section. Figure 4.2 shows the front panel LCD with the default screen that is displayed in normal operation once the bootstrap phase is complete. The two symbols at the right of the display indicate what the two right most buttons on the keypad do; if all four buttons of the keypad are active then four symbols will be displayed.

Figure 4.2 Default LCD Display

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The main sequence of events during bootstrap is shown below, depending on the initial state of the Sourcefire SSL appliance some of these steps may or may not apply:

- Choose Master Key Mode: this step only occurs if the mode is not already set
- Find or create the master key
  - If master key is password protected then unlock using password
- If there is not at least one user with the Manage Appliance role and one with the Manage PKI role then create them. This step won't occur if there are already users with these roles

All the above steps are managed using a limited version of the WebUI.

4.1.1 Configuring Static IP Address for Management

The easiest way to use the Sourcefire SSL appliance is to allocate it a management IP address using DHCP. However, if a static IP address is required then it can be configured by interrupting the start up sequence using the keypad sequence described in Table 17 and then using the front panel keypad and LCD to configure the desired address. Figure 4.3 shows the initial screen which allows DHCP to be enabled or disabled by pressing the top or bottom rightmost button on the front panel keypad.

Figure 4.3 Top Level IP Address Configuration

To configure a static IP address, use the up and down arrows to move to screens where you can configure the address information. Pressing the down arrow key will display the screen shown in Figure 4.4. Use the up/down arrow key to select the item to be configured and then press the top right button on the keypad to edit that item.

Figure 4.4 Configurable IP Address Options

Configuration Items:

- IP address for the system
- IP Netmask for the system
- Gateway IP address for the system

After selecting an item to edit, use the left and right arrows to move within the configuration item. Use the up arrow to change the value at the point where the cursor is located.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.5 shows the screen to input/edit the static IP address to be used by the system. On entry to this screen the cursor is located under the leftmost digit in the address. The left/right arrow buttons will move the cursor.

Figure 4.5 Initial IP address Configuration

Figure 4.6 shows the screen after the right arrow key has been used to move the cursor to underneath the numeral 6.

Figure 4.6 Editing IP Address

Pressing the up arrow button at this point will cause the number above the cursor to be incremented and the display will then appear as shown in Figure 4.7.

Figure 4.7 Edited IP Address

Once all the changes to the IP address are complete the top right button can be pressed to exit back to the previous level in the menu which allows the other elements such as Netmask to be configured.

Once all the elements have been configured the Apply option needs to be selected, this is the last option in the list of menu items as shown in 4.8.

Figure 4.8 Apply Command to Change Static IP Address

4.1.2 Password Entry

The password used to unlock the master key must be typed in on the front panel keypad after entering the code for PIN entry mode. The password is only required if the master key mode chosen requires a PIN. The password is a minimum of 8 characters long and the user has to select each character from a set of 4 characters that are displayed on the LCD. Passwords can include upper and lower case characters and the space character. The mechanism used to enter a password is described below.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Characters are selected using the buttons on the keypad and four button presses are required to input each character in the password. Each button press narrows down the set of characters that can be selected with the final button press choosing a specific character.

The first menu option allows for selection of upper or lower case for the character being entered. The three remaining menus narrow down the selection of the character to be input. The second menu allows for selection of a character group with the letters "A", "J" or "S" identifying the character group as shown on the grid below.

A	D	G	**J**	M	P	**S**	V	Y
B	E	H	K	N	Q	T	W	Z
C	F	I	L	O	R	U	X	␣

Choosing a character limits future selection options to other characters that are the same color in the grid. The third menu allows the selection of a subset of the character group already selected with the subset being identified by either "ADG" or "JMP" or "SVY" depending on which character was selected from menu 2. This is shown in the grid below.

A	**D**	**G**	**J**	**M**	**P**	**S**	**V**	**Y**
B	E	H	K	N	Q	T	W	Z
C	F	I	L	O	R	U	X	␣

The final menu allows selection of the character to be used in the password from the three characters in the vertical column with the character selected from menu 3 at the top. So, if "A" was chosen from menu 3 then menu 4 will offer the characters "A", "B" and "C".

A	D	G	J	M	P	S	V	Y
B	E	H	K	N	Q	T	W	Z
C	F	I	L	O	R	U	X	␣

The bottom character in the column with "Y" at the top is the space character.

The following sequence of images shows the LCD display at various points during the process of entering the password "Pass word".

Figure 4.9 shows the initial menu display once PIN entry mode is active. The four characters at the right of the display correspond to the four buttons with the two upper buttons being used to select upper or lower case for the character. The lower left button is a backspace key to erase a selection and the lower right button is used to enter the chosen selection.

Figure 4.9 PIN Entry, Menu 1: Select Upper or Lower Case

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.10 shows the second menu in the PIN entry process, which allows selection of the group of characters that will be used. Notice that the characters are shown in upper case as this was the selection chosen on the preceding menu. As the password being entered in the example is "Pass word" the group that needs selecting is "J" as from the grid shown earlier we can see that the character "P" is part of the green block of characters which includes "J" at the top left of the block.

Figure 4.10 PIN Entry, Menu 2: Character Group Selection

Figure 4.11 shows the third menu in the PIN entry process which allows selection of the sub group of characters to be used. In this example the character we want is "P" and this is shown as an option. Note however that selecting "P" in this menu is really choosing the sub group containing the characters "P", "Q" and "R".

Figure 4.11 PIN Entry, Menu 3: Character Sub Group Selection

Figure 4.12 shows the fourth and final menu in the PIN entry process which allows the desired character to be selected. In this example the character "P" is selected by pushing the top left button in the keypad.

Figure 4.12 PIN Entry, Menu 4: Character Selection

Figure 4.13 shows the display after the first character in the password has been entered. The system is now back at menu 1 in the process allowing the choice of upper or lower case to be selected for the next character in the password.

Figure 4.13 PIN Entry: First character Entered

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.14, Figure 4.15 and Figure 4.16 show the steps in the process of entering the second character in the password.

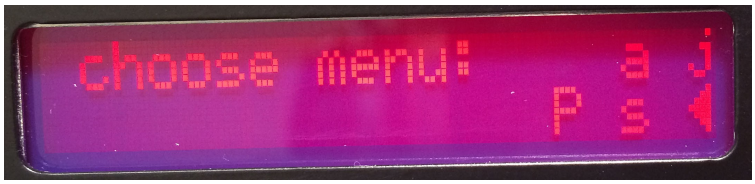


Figure 4.14 Pin Entry, Menu 2: Character Group Selection

Figure 4.15 PIN Entry, Menu 3 : Character Sub Group Selection

Figure 4.16 PIN Entry, Menu 4: Character Selection

To enter a space character into a password, use the bottom left button to select the space character, which is shown as a space on the LCD display.

Figure 4.17 PIN Entry, Menu 4: Next Character

Figure 4.18 shows the space character in the partially entered password.

Figure 4.18 PIN Entry, Menu 1: Space Entered

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.19 shows the final complete password, which is saved by pressing the bottom right button. Once the password has been entered and accepted it is stored in the system and will be used when the appropriate point in the bootstrap sequence is reached.

Figure 4.19 PIN Entry, Menu 1: Complete Password Entered

4.1.3 Installation Process

A typical installation of a new Sourcefire SSL appliance is to:

- Install the system in a rack in the equipment room
- Power it up and use the keypad to enter IP configuration mode and configure a valid address for the device
- Use the keypad to enter PIN entry mode and enter a PIN

For security, part of the Master Key can be stored on an external USB memory device and can be password protected; this means that the USB memory device will need to be present when the device is powered on, and the password must be input on the front panel keypad in order to make the device operational.

Figure 4.20 Bootstrap Master Key Mode

Once the master key mode is configured, the appliance will scan the internal, and if required external persistent storage device, for the master key, and if not found create the master key. If the master key is protected by a password, the user must first enter the password on the keypad before the master key can be unlocked or created. While in this state the GUI will display a screen with a "spinner" and without any buttons or links.

Note: The password can be entered into the device prior to the WebUI bootstrap phase in which case it will be retrieved and used when this point in the bootstrap sequence is reached.

Once the master key is unlocked the secure store can be opened or created.

The final stage of the bootstrap process is user setup. At least one user with the Manage

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Appliance role and at least one user with the Manage PKI role must be created; there may be one user with both roles, or two users.

As soon as the users are created, the GUI will go to the login screen, after which the user can log in with real credentials and configure the appliance. The configuration screen for users with these roles is shown in Figure 4.21.

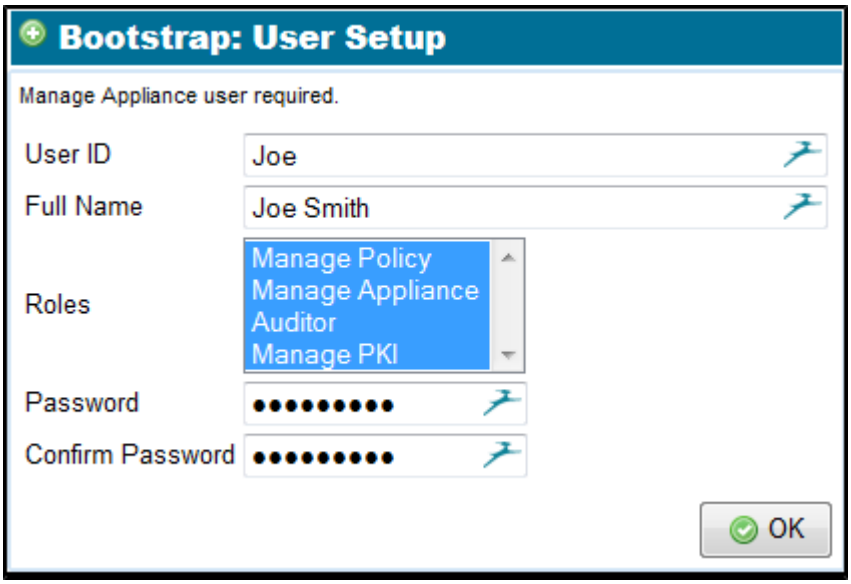


Figure 4.21 Bootstrap User Setup

Note: 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, this step will be skipped.

After creating the necessary user(s), the normal system login screen will appear allowing the user to login, at which point they will have access to the full WebUI (see User Interface Overview) to manage the SSL2000 and SSL8200. At this point a user with the Manage Appliances role can create additional users but cannot give these users the Manage PKI role. Only a user with the Manage PKI role can give this role to a user.

Whenever the Sourcefire SSL appliance is powered on or forced to do a factory default reset, the bootstrap phase will run before the device becomes fully functional. Depending on how the device is configured the administrator may need to provide input to enable the bootstrap phase to complete allowing the device to become operational again.

- If the master key is stored internally and no password is set for the master key then the bootstrap process becomes invisible and the device will start up without any need for input from the administrator.
- If the master key is partly stored on a USB storage device then this will need to be connected to the system before the bootstrap phase can complete.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- If the master key is protected by a password then the password will have to be entered using the front panel keypad before the bootstrap phase can complete.
- If the master key is partly stored on a USB storage device and is protected by a password then the password will have to be entered using the front panel keypad and the USB storage device will have to be connected before the bootstrap phase can complete.

4.2 Network Connections

HTTPS access to the Sourcefire SSL appliance is via the separate management Ethernet interface which should be connected to a secure network used by administrators to manage security appliances. Connect Management Ethernet 1 to the secure management network (see Figure 3.1, Figure 3.2 and Table 13).

By default the Sourcefire SSL appliance uses DHCP to acquire an IP address from the network. The acquired address can be viewed on the front panel LCD. If DHCP is not in use then a static IP address can be configured, see Section 4.1.1.

4.3 Post Bootstrap Configuration

Once the bootstrap phase is complete the full WebUI is available and can be used to configure the system. The WebUI is described in detail in Section 5. this section provides a quick summary of the basic configuration steps. An HTTPS connection to the IP address assigned to the Sourcefire SSL appliance management interface will produce the standard login box.

Note: The Sourcefire 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 Sourcefire SSL appliance as a trusted device.

Figure 4.22 shows the login box which appears in the center of the initial access screen.

Figure 4.22 Initial Access Login

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The bottom of the initial access screen displays additional information on the appliance, as shown in Figure 4.23. This status information allows you to determine what version of software the Sourcefire SSL appliance is running without needing to log on to the system.

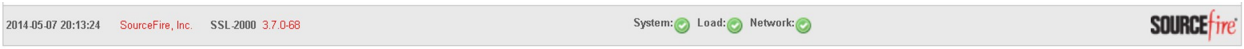


Figure 4.23 Status Information on Initial Login

Figure 4.24 shows the top and bottom of the initial management dashboard screen after the username "support" has logged on. The top of the screen contains menus on both the left and right side. The two menus on the right side have names that depend on the device name and the username.

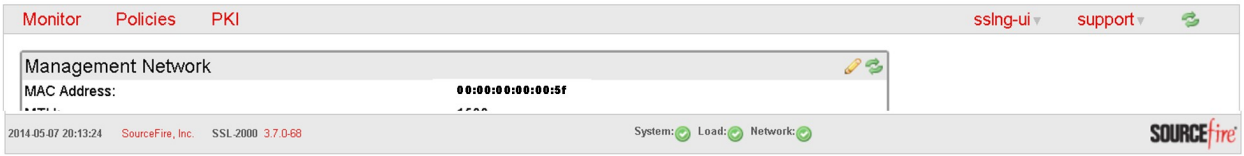


Figure 4.24 Management Standard Features

In this example the appliance has a device name of **sslng-ui** and the username of the connected user is **support**. The bottom of the screen (footer) contains status information on the device and shows:

- current date and time
- version of software running on the device
- status indicators for **System, Load** , and **Network**

The status indicators will change color if there are problems

As part of an initial configuration the following would normally be configured:

- Management network settings
- Time zone and use of NTP
- Additional user accounts with relevant roles assigned to the user

4.3.1 Configuring System Date/Time and Timezone

To configure the system date and time use the **Date/Time** option on the device menu. In the example in Figure 4.24 the device menu is labeled **sslng-ui**, which is the system's name. Click the pencil icon at the top right of the **Date/Time** field (Figure 4.26) to edit these settings. Figure 4.25 shows the edit screen and settings that can be changed.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

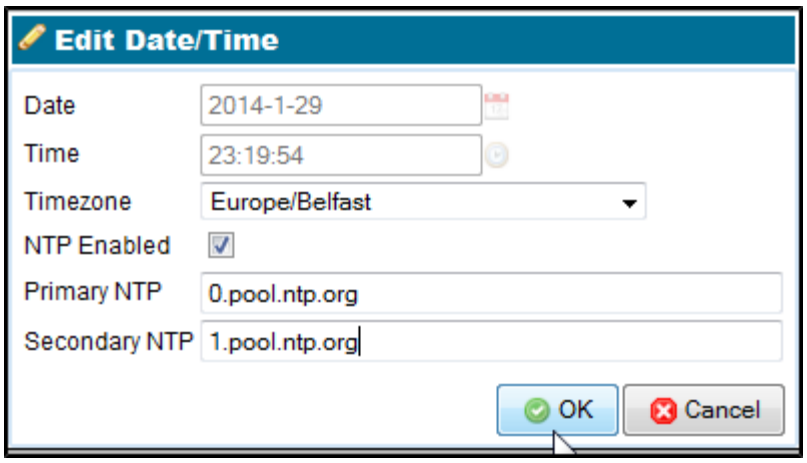


Figure 4.25 Edit Date and Time

Figure 4.26 Time Settings with Reboot Button

If NTP is enabled, as in this example, then the **Date** and **Time** fields will be disabled as these values are being set by the Network Time Protocol (**NTP**). In order for NTP to operate you need to configure a primary NTP server and ideally a secondary NTP server. Once the settings are configured and **OK** is clicked to save the settings the screen will appear as in Figure 4.26. NTP will not be able to resolve NTP server hostnames if there are no nameservers configured (DHCP or manually).

Note: If you have changed the date, time, NTP, or timezone, you must select Apply at the "Platform Config Changes" message which appears at the bottom of the screen.

Finally, click the Reboot button for the time changes take effect; this will reboot the system.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

4.3.2 Configuring Management Network Settings

To configure the management network settings use the **Management Network** menu option on the device menu. Figure 4.27 shows the menu options.

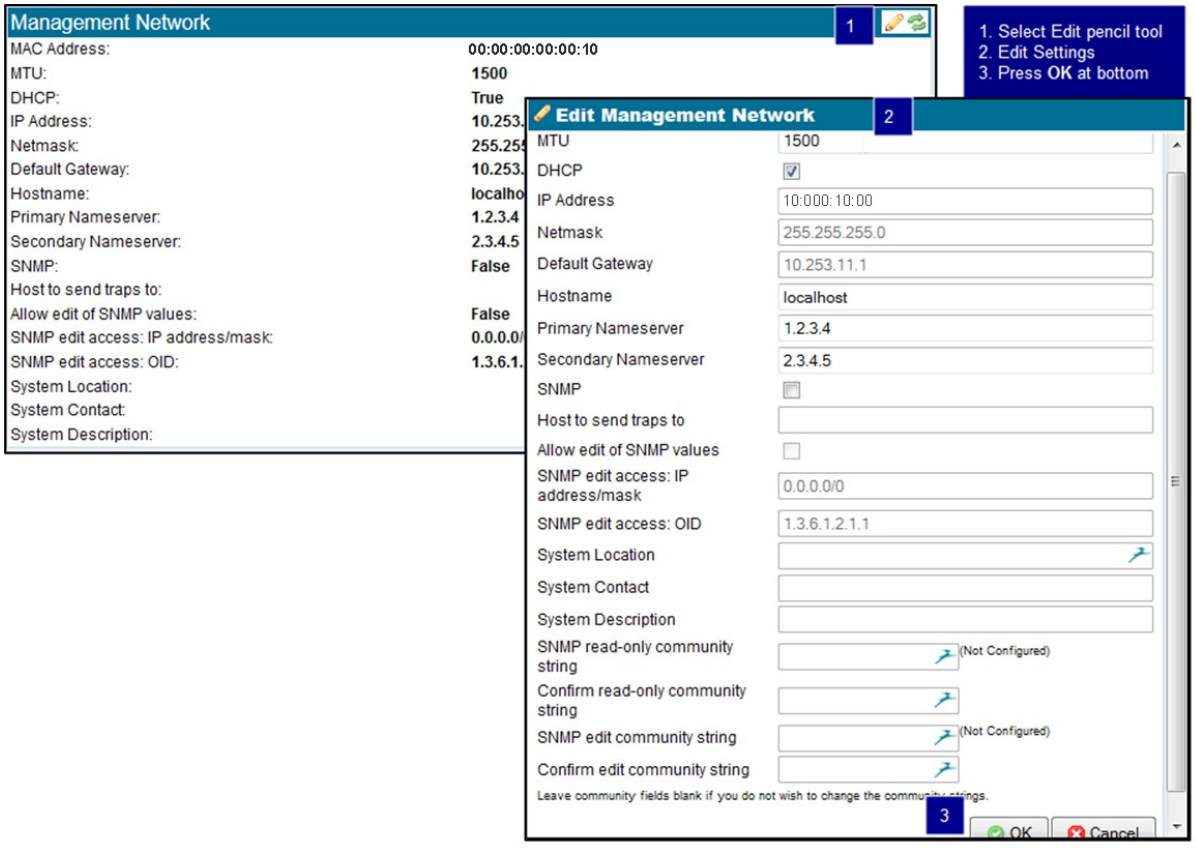


Figure 4.27 Management Network Settings with Edit Window

Click on the pencil icon at the top right to edit these settings. Figure 4.27 also shows the configuration screen and the parameters that can be edited. In this example the system is configured to use a static IP address. If DHCP was being used to obtain an address the IP Address, **Netmask** and Default Gateway fields would be disabled. If DHCP is disabled, these fields will be editable. To configure the management network settings use the **Management Network** menu option on the device menu.

You can also configure **SNMP** parameters and may to enable or disable SNMP management. The SSL2000 and SSL8200 supports the standard SNMP MIB2 tables, and use the SNMP v2c version of the protocol.

To allow SNMP management of the SSL2000 and SSL8200, enable SNMP and configure the SNMP parameters appropriately for your SNMP management system.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

After pressing **OK** to save the settings, the screen will appear as shown in Figure 4.28. Clicking Apply will cause a Reboot button to be displayed and the changes to the network settings will only take place once the reboot has occurred.

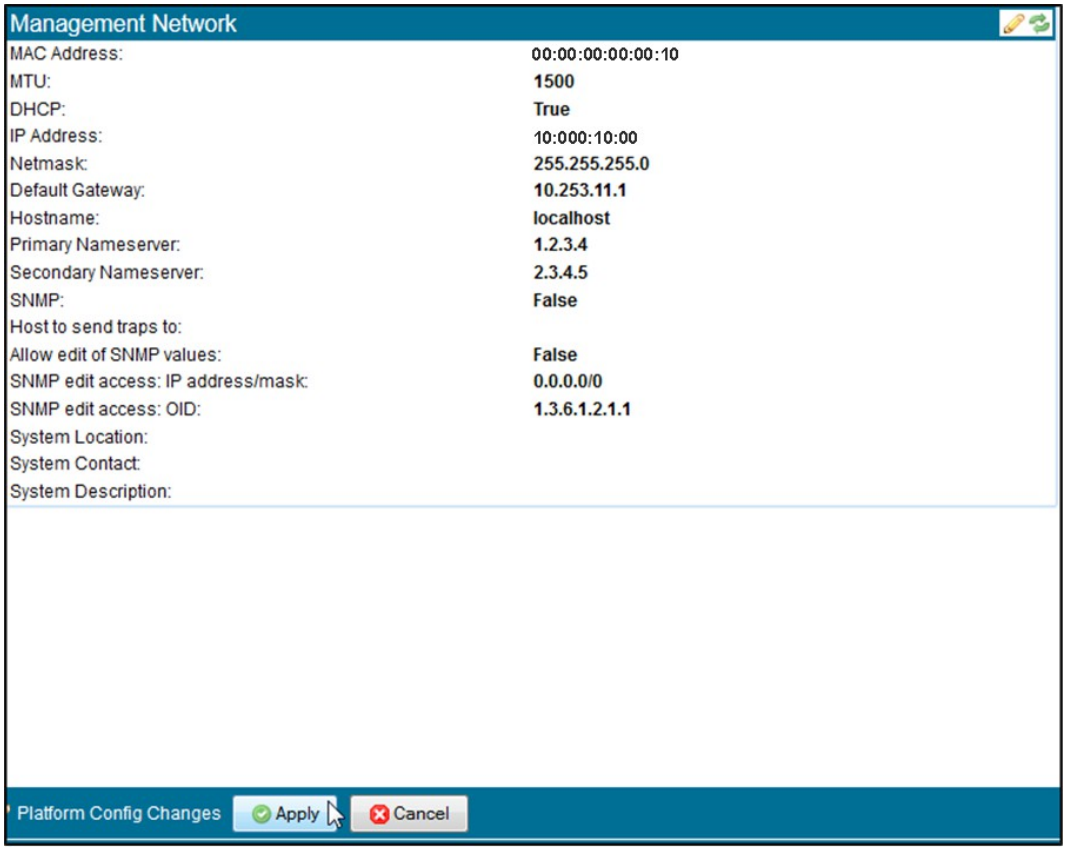


Figure 4.28 Management Network Settings with Apply Button

4.3.3 Configuring Management Users

Create new user accounts on the system using the **Users** option on the platform menu, shown in Figure 4.29. Clicking on the + icon enables a new user to be added to the system.

Figure 4.29 Current System Users

Figure 4.30 shows the **User Management Add** window with the details required to add a user. The **Roles** section lets you assign one or more roles to the user being created.

To assign more than one role click on the first role, which will highlight the role, then hold down the CTRL key (Command key, for Mac users) and click on a second role which will also be highlighted. Repeat this process until all the roles you wish the new user to have are highlighted and then click the Save button.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Click **OK** to create and add the new user to the system.

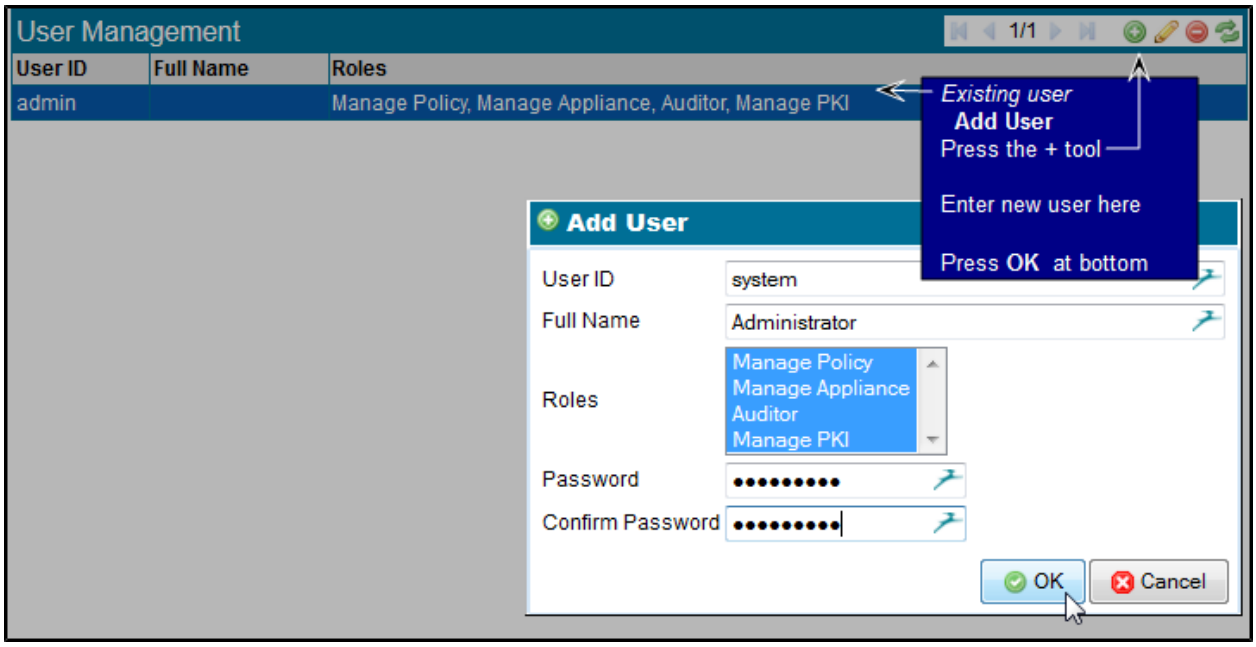


Figure 4.30 Add User

A user can change their own password at any time by logging on to the system and using the **Change Password** option on the **User** menu. The user menu is the menu at the top right of the screen under the user name. A **Change Password** window, as shown in Figure 4.31, allows the user to change their own password.

4.3.4 Licensing

The Host Categorization feature (Section 5.3.7) requires a software license.

Note: See Section 5.5.8 for further information on the **License** feature.

Determining the Type of License

View the license status on the front LCD panel and on the **License** window (see Section 5.5.8).

- **Perpetual:** A license that does not expire.
- **Subscription:** A license that is valid for a set period of time.

License Expiration

At the end of a subscription license period, the license expires. A license expiration notification message is logged in the **System Log** (Section 5.2.2).

When the Sourcefire SSL appliance license expiration is within 30 days, a "Pending License Expiration" message will appear on logging in.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Licensing the Sourcefire SSL Appliance

The Blue Coat Host Categorization service allows policy to be tailored to the destination of an SSL flow. This feature is offered as a subscription service; to use the Host Categorization service on your Sourcefire SSL appliance, you must first purchase a subscription from Blue Coat.

When you purchase a subscription, you will receive subscription details, including an **Activation** code. This code is used to activate the service and to generate the license file for the Sourcefire SSL appliance you want to enable to use Host Categorization. The subscription is per appliance. When generating the license file, you will need to provide the serial number of the Sourcefire SSL appliance; the license file produced will only work on that appliance.

Before You Begin

The Sourcefire SSL appliance requires a license to use the Host Categorization feature. Before you can license your Sourcefire SSL appliance, you must have the following:

- A user with the Manage Appliance authentication role configured on the appliance.
- The serial number of your appliance. To locate the serial number, go to Platform Management > Information. View the serial number under Chassis FRU Info. The serial number can also be found on the front panel LCD screen.
- A BlueTouch Online account. If you need a BlueTouch Online login, go to the BlueTouch Request Login screen (https://bto.bluecoat.com/requestlogin), and follow the registration process.

Download a Blue Coat License

1. Using your BlueTouch Online account, log in to the Blue Coat Licensing Portal (https://services.bluecoat.com/eservice_enu/licensing/register.cgi).
2. At the "Home" page, enter the activation code you received when you ordered the Host Categorization subscription, then click "Next".
3. When prompted, enter the serial number of your appliance, then click Submit.
4. When prompted, accept the End User License Agreement, then click "Next".
5. When the "Software Add-On Activation" page is displayed, save the username and password. You will need them to download the Blue Coat Host Categorization database for your Sourcefire SSL appliance
6. From the menu on the left side, choose "SSL Visibility," then choose "License Download".
7. When prompted, enter the serial number of your appliance, then click Submit.
8. When the license file has been generated, press "Download License File" for the required Sourcefire SSL appliance.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Install a Blue Coat License

1. Select Platform Management > License.
2. Press the Add (plus sign) tool. The Install License window displays.
3. On the Upload File tab, use the Browse button to browse to the file location.
   Or
   On the Paste Text tab, paste in the previously copied license text.
4. Press Add. You will see a confirmation message. The license is now installed.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

4.3.5 System Status

The overall status of the appliance can be viewed by clicking on the **Monitor > Dashboard** menu option. Figure 4.32 shows an example of the dashboard screen providing detail on the system status. Status details shown here feed into the summary status indicators for **System**, **Load**, **Network**, and **License** that appear in the footer at the bottom of the display.

Segments Status

Segment ID	Main Interfaces	Copy Interfaces	Interfaces Down	Main Mode	Failures
A	3, 4, 5, 6			Active-Inline-FTN	

Network Interfaces

Port	Type	Link State	RX Packets/Bytes	TX Packets/Bytes	RX Drops
1	10G	Down	0/0	0/0	0
2	10G	Down	0/0	0/0	0
3	1G	1G	36/6724	199/17844	0
4	1G	1G	196/16812	40/7646	0
5	1G	1G	174/14061	19/3408	0
6	1G	1G	19/3408	174/14061	0

CPU Load %

cpu	cpu0	cpu1	cpu2	cpu3	cpu4	cpu5	cpu6	cpu7	cpu8	cpu9	cpu10	cpu11	cpu12	cpu13	cpu14	cpu15
0.8	11.2	0	1	0	1	0	2	0	0	0	0	0	0	0	0	1

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
11926	10051	11926	9917	7036	12931	13043

Temperatures (Degrees °C)

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
28	21	-45	-41	-51	-57	-68	51	33	38

Thermal margin sensors are reported as negative values which when increased to 0 will cause CPU to throttle down or halt

Utilization %

Disk	Memory
33.0	26.4

System Log

Time	Process	Log
Mar 13 15:59:19	sslmanage[3340]	Login attempt for uid[admin]
Mar 13 15:59:23	sslmanage[3340]	Login attempt for uid[admin]
Mar 13 16:03:18	sshd[7657]	Received disconnect from 10.95.9.14: 11: disconnected by user
Mar 13 16:03:18	sshd[7644]	pam_unix(sshd:session): session closed for user ssldebug
Mar 13 16:03:18	su[7671]	pam_unix(su:session): session closed for user root
Mar 13 16:08:40	sslmanage[3340]	Login attempt for uid[admin]
Mar 13 17:49:57	sslmanage[3340]	Login attempt for uid[admin]

Figure 4.32 Management Dashboard

4.4 Installing a CA for Certificate Resign

Before the Sourcefire SSL appliance can be used to inspect traffic using Certificate Resign mechanisms it must have at least one CA certificate and private key installed which can be used to do the resigning. A CA can either be created by the Sourcefire SSL appliance (and self signed or sent off for signing by another CA) or can be imported. If

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

the Sourcefire SSL appliance has more than one CA for resign installed then it is possible to use different CAs to resign 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.

If the Sourcefire SSL appliance is operating in an environment where SSL server certificates signed by the CA using an EC key are present, you must create or load one or more internal CAs which use EC keys. When creating a self-signed CA on the appliance, you can specify if the CA should use RSA or EC keys. The type of key being used by an internal CA is shown on the WebUI.

Figure 4.33 shows the screen when there are no Internal Certificate Authorities in the system. 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

Figure 4.33 Empty Internal Certificate Authority Screen

The following subsections consider each of these ways of adding an Internal Certificate Authority.

4.4.1 Creating a CA

Clicking on the icon to generate a CA will produce the **Generate Certificate** window shown in Figure 4.34. Enter the basic data required in a CA, and the key size and validity period to be specified. Once the data is input there are two options:

- Generate a self-signed CA
- Generate a certificate signing request (CSR)

Figure 4.34 Generate Internal Certificate Authority Window

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

If you select the **Generate a self-signed CA** option, there are no further steps. The CA is generated and added to the set of Internal Certificate Authorities in the system. As 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. See Section 5.4 for details on how to do this. When **OK** 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.

If you select **Generate a CSR**, a PEM format CSR is generated. It needs to be sent to the Certificate Authority that is going to sign it. Figure 4.35shows an example CSR.

The text in the CSR box should be copied into a file. The file then must be communicated to the CA that will sign the final Internal Certificate Authority certificate. When **OK** is clicked, the certificate details are saved, and an entry in the **Internal Certificate Authorities** table appears with an indication that a CSR has been generated for this certificate. At this point the certificate is not installed in the system, as the signed Internal CA has not been received back from the CA that is signing it. When an entry in the table shows CSR True, the icon for installing a certificate is active. When used, you will prompted to provide the signed CA so it can be installed in the system.

Figure 4.35 Internal Certificate Authority Certificate Signing Request

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

> **!** It is important to understand that the CSR is for a Certificate Authority and not for a normal SSL server certificate. The CA that will be used to sign this certificate will in almost all cases be the root CA of a private PKI domain and NOT a public CA. If the organization has a private PKI domain and client machines in the organization are configured to trust the private root CA then the CSR should be presented to the private root CA and the private root CA should sign this to create a private Intermediate CA which can then be loaded onto the Sourcefire SSL appliance and which the client machines will trust as it is signed by the private root CA that they already trust.

> **!** Public Certificate Authorities will sign CA CSR requests to create Intermediate CAs that are publicly trusted but there are onerous conditions and significant costs involved in doing this.

After the CSR has been generated the **Internal Certificate Authority** screen will appear as in Figure 4.36. At this point the CA cannot be used as the signed certificate from the CA that the CSR was sent to has not been loaded. Once the signed certificate is available, it can be loaded by selecting the entry in the **Internal Certificate Authority** window and clicking the icon. This will produce a window similar to Figure 4.37 allowing the signed certificate to be imported into the system.

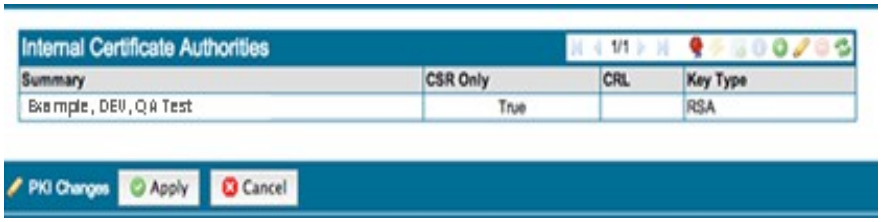


Figure 4.36 Internal Certificate Authority with CSR Entry

Figure 4.37 Internal Certificate Authority -Import

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

4.4.2 Importing a CA

If you already have a CA that you want to use as an Internal Certificate Authority in the Sourcefire SSL appliance you can import this and install it in the system. You will need both the CA certificate and the private key for the CA in order to install it on the system. Clicking Add (⊕) will generate a form where you can either select the files containing the certificate and private key or paste in the certificate and private key directly. Figure 4.37 shows the window used to import a CA.

If the certificate and key being imported have been encrypted and protected with a password then you will need to check **Encrypted** then type the password in the **Password** field.

4.5 Importing Known Server Keys

In order 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 Sourcefire SSL appliance. Known server certificates and keys are imported into the **all-known-certificates-with-keys** list, and can then be copied to custom lists if required. The **Known Certificates and Keys** option on the **PKI** menu is used to import new certificates and keys.

There are two input forms provided, one to choose the list that is to be operated on and the other to manipulate the contents of that list. Initially there will only be one list, called all-known-certificates-with-keys, and it will have no certificates in it. Figure 4.38 shows the initial appearance of the input forms.

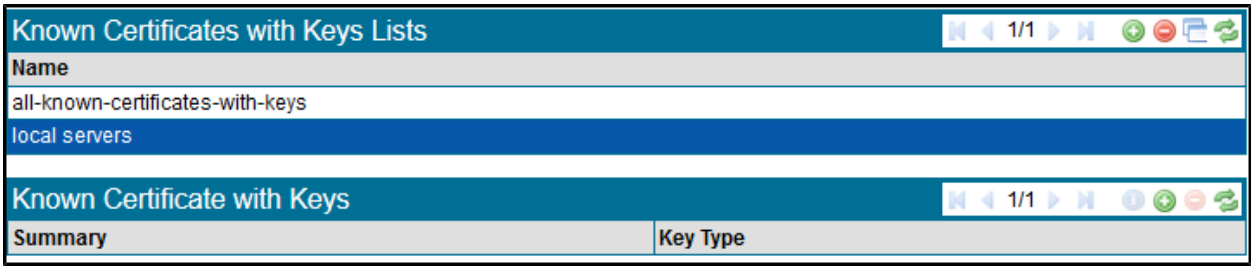


Figure 4.38 Known Server Certificate with Keys Lists

In order to import the first known server key and certificate, click the **all-known-certificates-with-keys** entry in the **Known Certificates with Keys List** window, then click **Add**.

Figure 4.39 shows the input form that will appear. You can then either specify the files to import or paste in the key and certificate details and click the Add button. If the key and certificate are valid then a message confirming that the Certificate has been added will appear with a View Details button. You will see that the key now appears as a row in the **Known Certificate with Keys** form.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

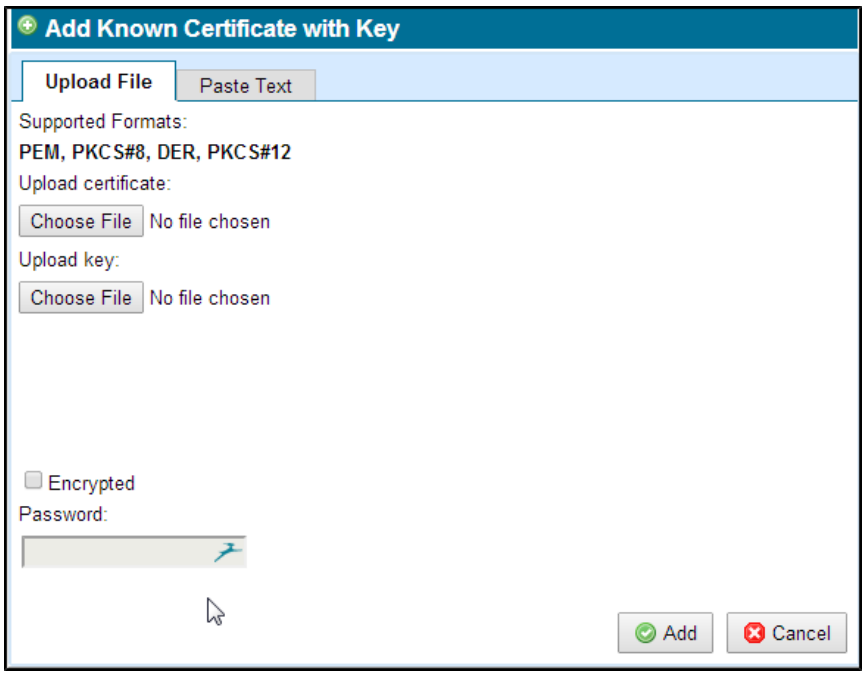


Figure 4.39 Known Certificate with Keys Import

Figure 4.40 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.

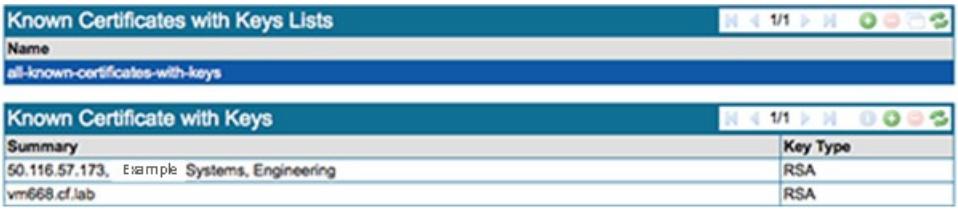


Figure 4.40 Known Certificate and Keys with Entries

Section 5.4 explains how to create custom lists of Certificates and Keys in more detail.

4.6 Example Passive-Tap Mode Inspection

The following example shows the steps needed to configure the Sourcefire SSL appliance to inspect traffic that is destined for a server that you can obtain a copy of the private key and certificate from. In this example the Sourcefire SSL appliance is deployed in passive-tap mode with an additional copy port as described in Section 2.3.1. The known server certificates and keys used in this example are those shown in Figure 4.40.

The steps involved are:

- Load the server key/certificate into the Sourcefire SSL appliance (see section 4.5)
- Create a ruleset that contains a rule to inspect traffic to the server

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- Create a segment for passive-tap operation
- Activate the segment to start inspection

In this example the certificate and key for viola.example.com is used to allow inspection of traffic going to that server. As this certificate/key is already loaded into the system, we can proceed to the next step, which is to create a ruleset that contains a rule specifying that traffic to viola.example.com should be inspected.

This is a two-step process, first creating the ruleset to hold the rule, then defining the rule itself. Figure 4.41 shows the screen while adding a new ruleset called passive-tap-example. After clicking OK, the new entry will appear as a row in the **Rulesets** grid, and is available for use. 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.

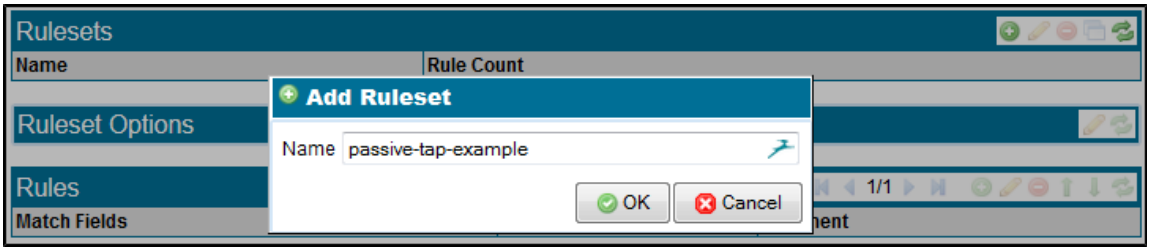


Figure 4.41 Adding a Ruleset

Now click on the passive-tap-example row to select it. This will display the **Ruleset Options** for this ruleset. In this example the default settings are fine and are explained below:

- No Internal Certificate Authority as we are not doing certificate resigning
- All External Certificate Authorities and CRLs are used when checking an SSL session
- There are no trusted certificate being used for systems that either have self-signed certificates or certificates signed by untrusted Certificate Authorities. If there were trusted certificates loaded into the system then the default setting would be to use All Trusted Certificates.
- Any SSL sessions that don't match a rule in this ruleset will be cut through to the attached security appliance without being decrypted

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Clicking on the add button in the **Rules** grid section will open the **Insert Rule** form. Selecting **Cut Through** on the drop-down menu in this form will allow the valid options to be configured for this rule. Figure 4.42 shows this form with the data entered.

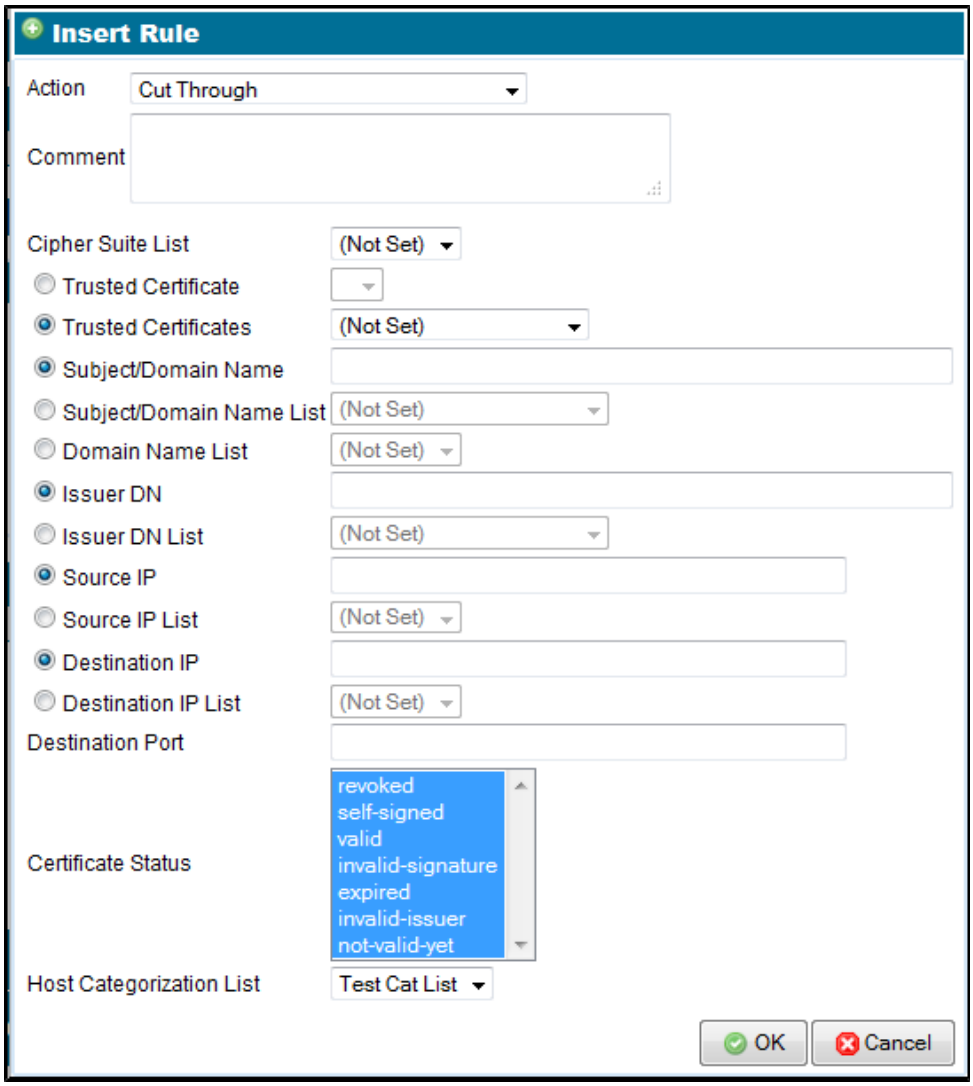


Figure 4.42 Add Cut Through Rule to Using Known Server Key/Certificate

In this example the rule only applies to a single server for which the certificate and key are known, so the **Known Certificate with Key** option is checked and the system for which we loaded the key is selected from the drop-down menu. Apart from adding a comment to the Comment box no other options are used in this rule, so click **Save** to create the rule. At the bottom of the screen is a **Policy Changes** notification area. 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 then to activate it. To create a Segment go to the **Policies / Segments** menu option and you will see the Segments information. Figure 4.43 shows the segment screen when no segments currently exist on the system. In this case the device is an

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

SSL2000 as can be seen from the graphic at the top of the screen. The ports that show green on the graphic indicate that the links on these ports are up.

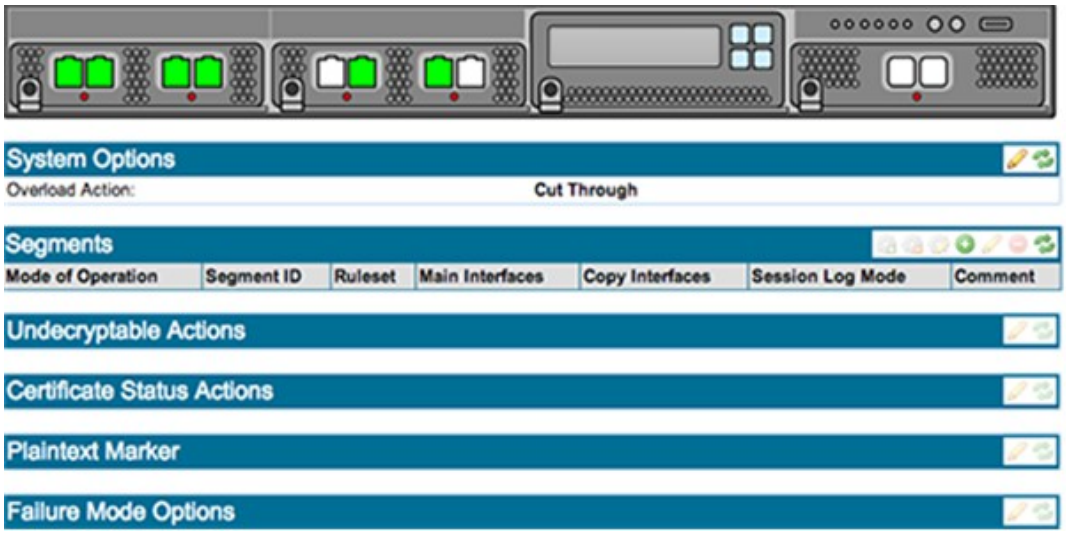


Figure 4.43 Empty Segments Display

Initially there will be no segments configured in the system. To create a new segment click Add in the **Segments** table. Figure 4.44 shows the initial form. The **Mode of Operation** is selected by clicking on the edit button and then choosing from the Select **Mode of Operation** from the required mode. The **Ruleset** is chosen from the drop-down menu.

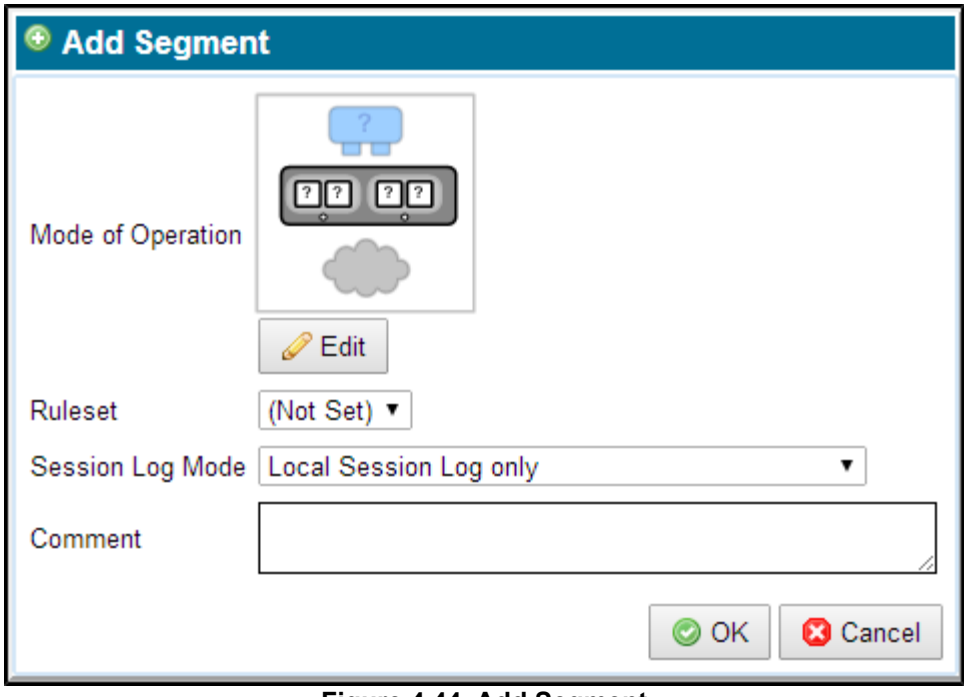


Figure 4.44 Add Segment

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.45 shows the form used to select the mode of operation for a segment. The **Mode of Operation** area has a scroll bar and displays all the different operating modes as images. Narrow the set of operating modes using the **Main Mode** drop-down menu by choosing only Passive Tap for example, this will reduce the number of options displayed in the **Mode of Operations** area. The **Asymmetric Sub-mode** drop-down menu can be used to further narrow the number of modes of operation that are displayed. Click the image of the desired operating mode selects it and click Save to set this as the mode of operation for the segment.

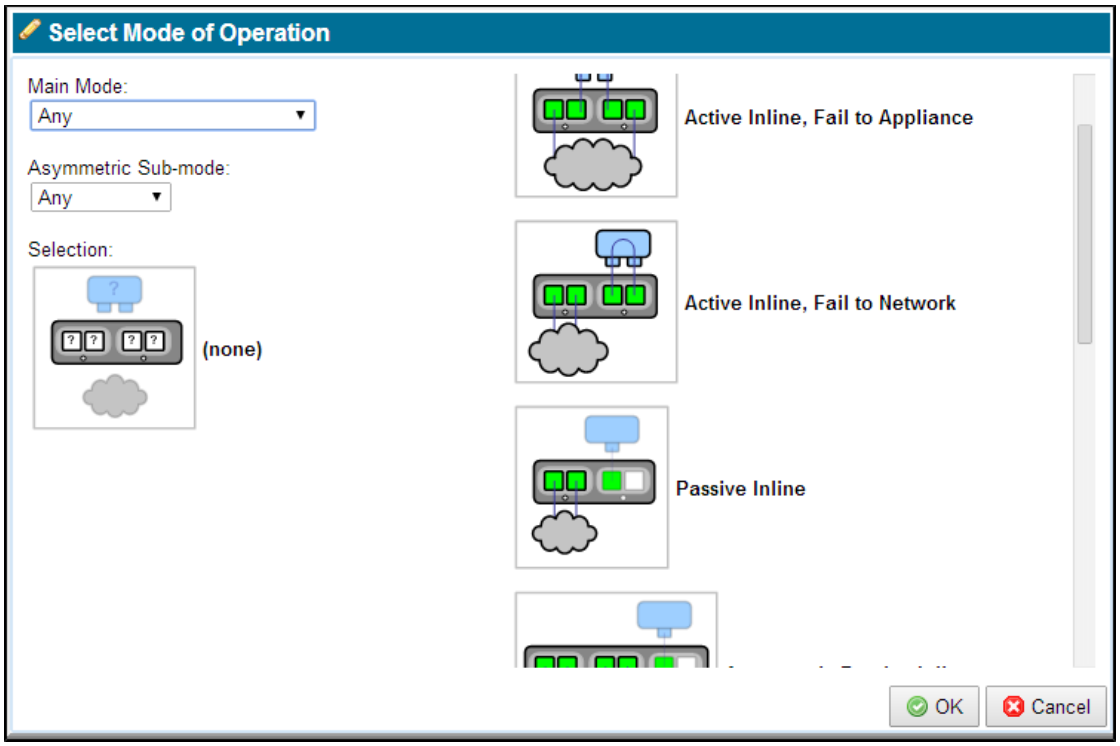


Figure 4.45 Selecting Mode of Operation for a Segment

Select the Rule set as required.

Logs can be saved locally, and you can send errors or session logs to remote servers, at the **Session Log Mode** field. Make sure to follow up with the **Remote Logging** menu item (Section 5.5.3) to actually transmit the logs remotely.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.46 shows the completed segment details before they are saved. In this example, the local session log has been enabled. The graphic in the input window indicates that this segment will make use of two ports on the system; the actual port numbers to be used are not known at this point, they are determined when the segment is actually activated.

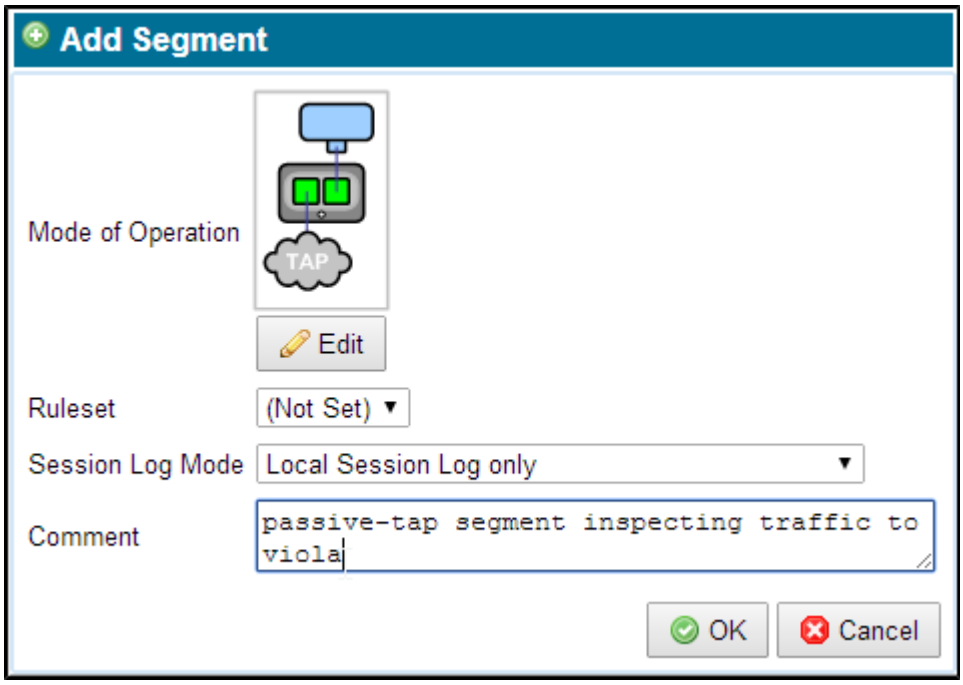


Figure 4.46 Example Passive-Tap Segment Configuration

Clicking OK in Figure 4.46 will 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 to save the rule to disk.

Once created, the segment can be seen in the **Segments** table, and can be selected by clicking on it, as shown in Figure 4.47. There are three panels below the **Segment** panel in this table, each of which allow different types of actions to be configured for the selected segment. These are explained below. To change any of the settings in the **Undecryptable Actions**, **Certificate Status Actions** or **Plaintext Marker** panels, click the Edit button for that panel.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

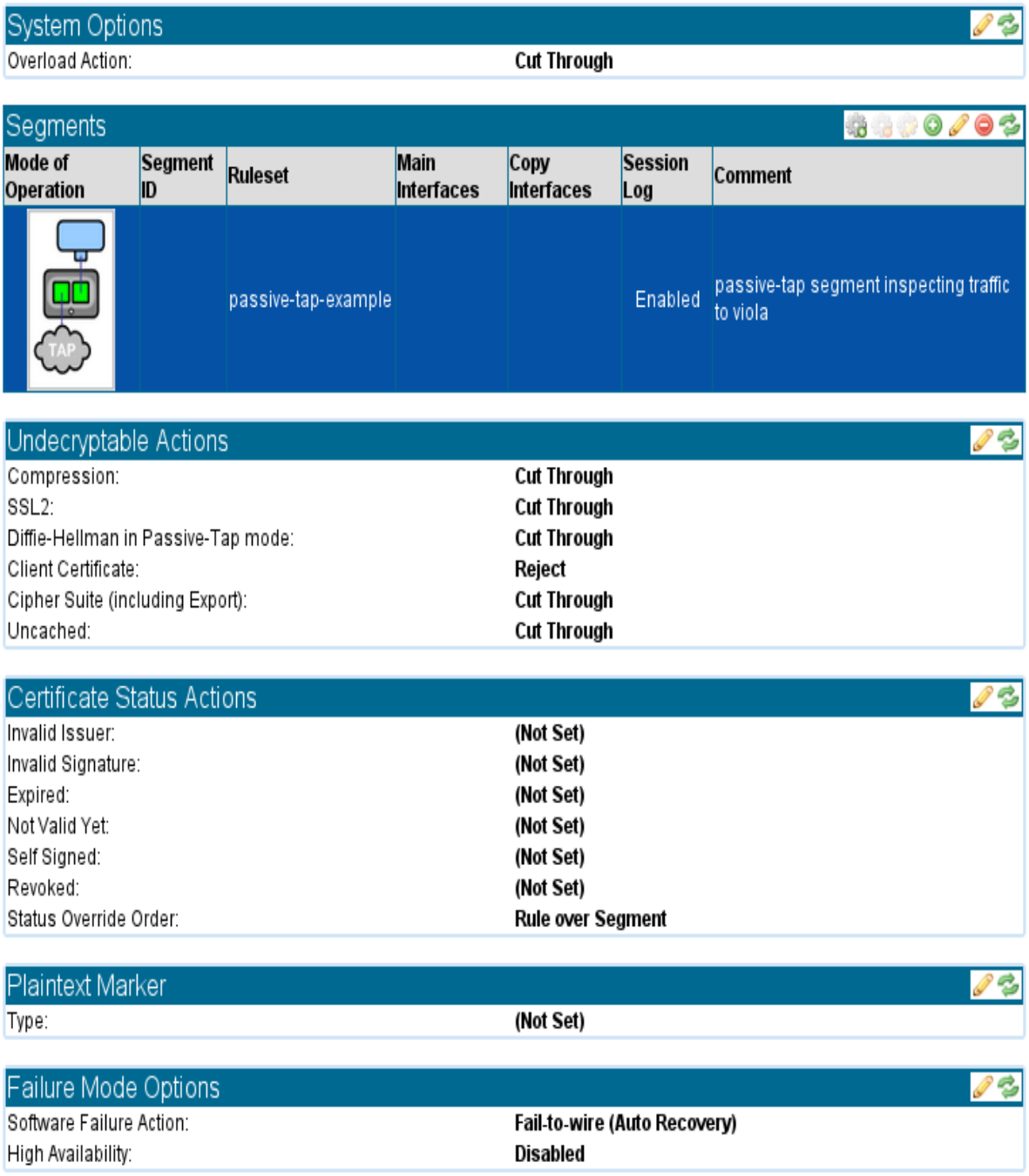


Figure 4.47 Passive-Tap Segment Options and Activation

The **Undecryptable Actions** panel gives you control over what will happen to an SSL session that cannot be decrypted by the Sourcefire SSL appliance. Different actions can be configured depending on the reason why decryption is not possible. In the example in Figure 4.47 the action is to cut through the session except in the case where client certificates are used when the SSL session will be rejected.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The **Certificate Status Actions** panel gives you control over what will happen if the server certificate used by the SSL session has particular errors in it. In this example, the action is to cut through the session for all error conditions. Use **Status Override Order** to configure which Certificate Status actions have priority—those configured for the segment, or those configured in a rule in the ruleset being used by this segment.

In the case of a rule to inspect using a known server Certificate and Key, there is no option to specify **Certificate Status Actions**, so the override setting and segment default actions have no effect.

The **Plaintext Marker** panel lets you control how the generated flow with the decrypted payload is marked, of if it is marked at all. The options are to have these flows be marked with:

- VLAN tag; the VLAN ID used is configurable
- Modified source MAC address
- No marking

As this example is a passive-tap segment all three options are available. In the case of an active-inline segment the no marking option is not available as generated flows must be marked in order that the Sourcefire SSL appliance can identify them when they are sent back to it by the attached security appliance.

In the example shown in Figure 4.47, the generated flows will be sent out with no marking.

Notice that the **Interface** columns in the **Segment** do not shows interface numbers; these are allocated when the segment is activated. Click Activate for the segment to activate it, which is in the tool block at the top right of the segment panel, then click Apply.

During the activation process a series of screens appear for you to select the ports to use for the segment, and to select any copy ports and the modes that the copy ports will operate in. The initial screen shown in Figure 4.48 indicates which interfaces on the device are available for use and which are already in use by other segments. In this example no other interfaces are in use.

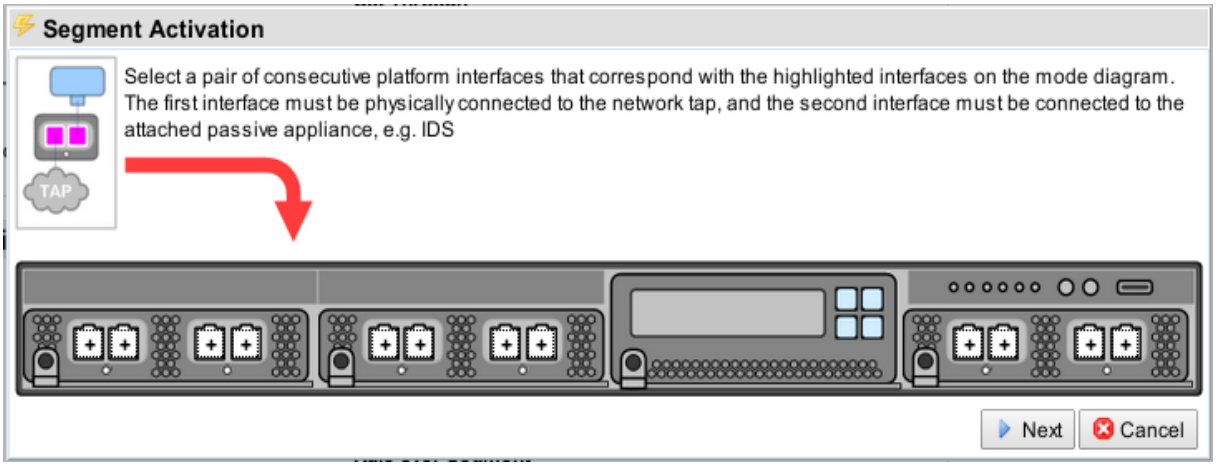


Figure 4.48 Activating a Passive-Tap Segment - Step One

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.49 shows that ports 5 and 6 have been selected as the two primary ports for this segment. Clicking **Next** will move on to the next step in the process.

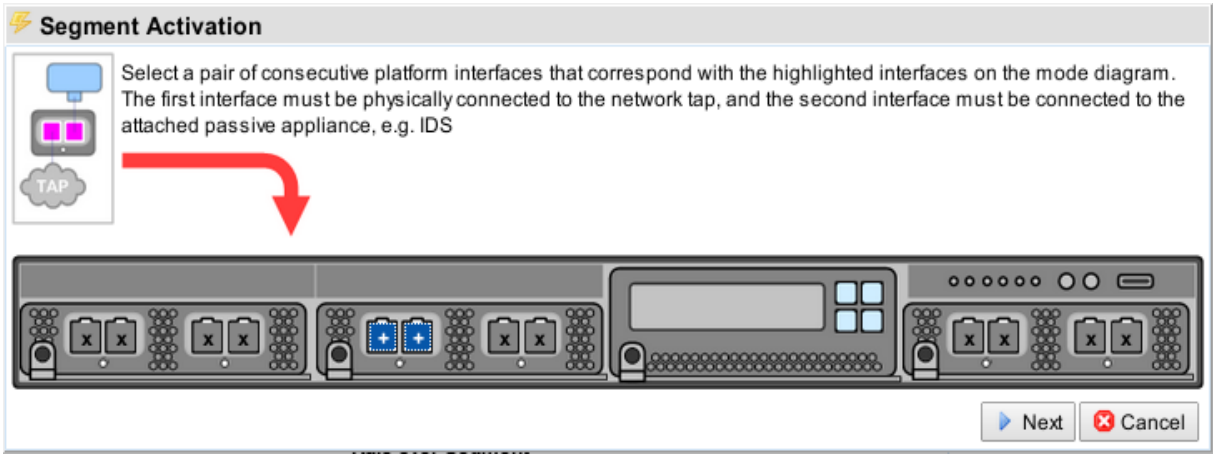


Figure 4.49 Activating a Passive-Tap Segment - Step 2

Figure 4.50 shows that one or two mirror ports can be configured for this passive tap segment, indicated by the images in the box at top left. One mirror port has been selected in this case. If two mirror ports had been selected then the options allowing

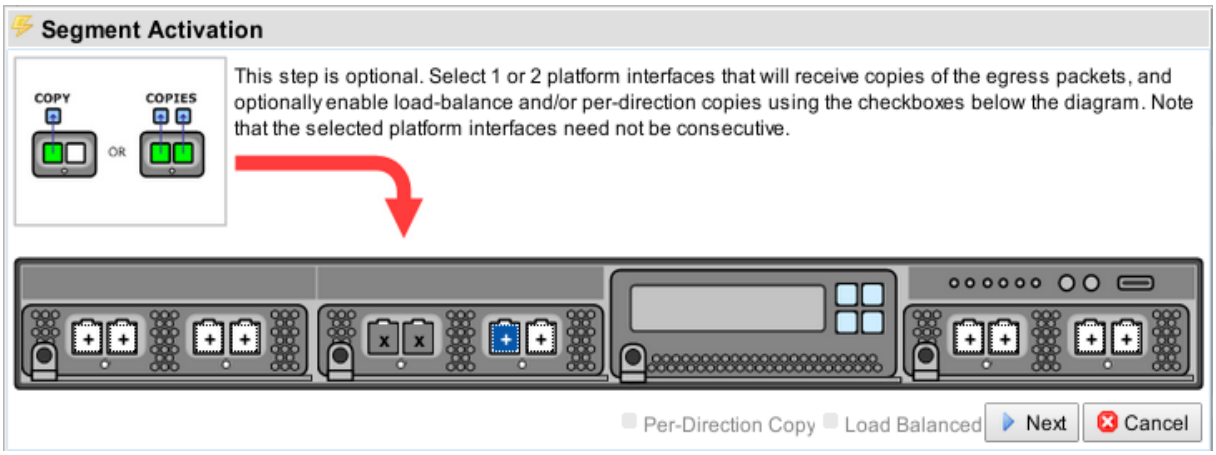


Figure 4.50 Activating a Passive-Tap Segment - Final Step

selection of per-direction copy or load balancing would be active allowing selection of these capabilities if required. Click Next then Apply to finish the activation process.

Once the segment is active the **Segment** screen will show an entry for the new segment and the graphic at the top of the screen will indicated the ports being used by the segment; see Figure 4.51. In this example the segment is identified as Segment A and the three ports being used all show the letter A.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

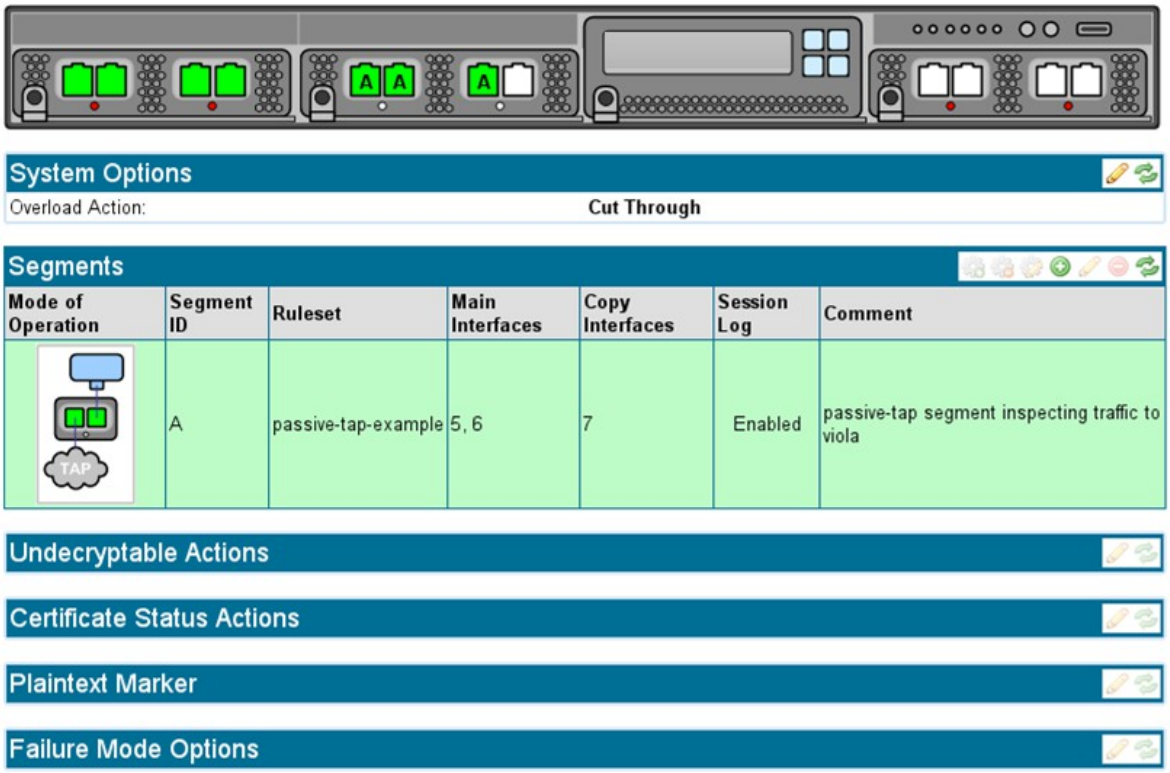


Figure 4.51 Segment Display with Active Passive-Tap Segment

The green background indicates that this segment is activated. If there is SSL traffic to the server then the SSL session log and SSL statistics screens should show this. See Section 5.2 for details on the session log and other monitoring tools.

4.7 Example Passive-Inline Mode Inspection

The following example shows the steps for configuring the Sourcefire SSL appliance to inspect traffic that is destined for a number of SSL servers that you cannot obtain a copy of the private key and certificate for. In this example the Sourcefire SSL appliance is deployed in passive-inline mode as described in Section 2.3.2. This example illustrates the use of certificate resign to inspect traffic and also how to use custom lists to enable a single rule to apply to traffic going to multiple destinations and how to apply policy to SSL traffic that is not being inspected. The Internal CA used in this example is shown in Figure 4.34.

The steps involved are:

- Create or load an Internal CA certificate and key into the Sourcefire SSL appliance (see section 4.4.1)
- Create a ruleset that contains rules to inspect traffic going to specific destinations
  - Create a list of destinations for use by a single rule
- Create a segment for passive-inline operation
- Activate the segment to start inspection

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 4.52 shows the edit options screen for a ruleset called passive-Inline-example that has already been added to the rulesets on the system. The internal CA created above is selected as the default Internal Certificate Authority.

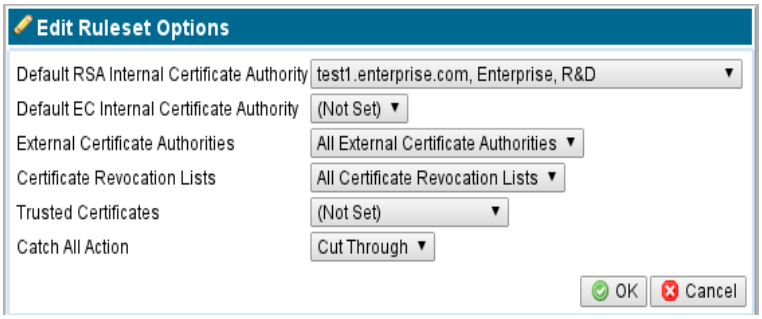


Figure 4.52 Create a Passive-Inline Ruleset

Before adding any rules to this ruleset we will create a list of **Domain Names (DN)** that will allow a single rule to apply to SSL sessions to multiple destinations.

Figure 4.53shows the list that we are going to use in this example. The list was created by clicking on the icon in the **Subject/Domain Names List** area and giving the new list the name "webmail destinations". After creation the empty list it was selected in the **Subject/Domain Names List** area and then the icon was clicked in the **Domain Names List** area allowing a name to be added to the list. Two Domain Names have been added to the list. 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 new list to disk.

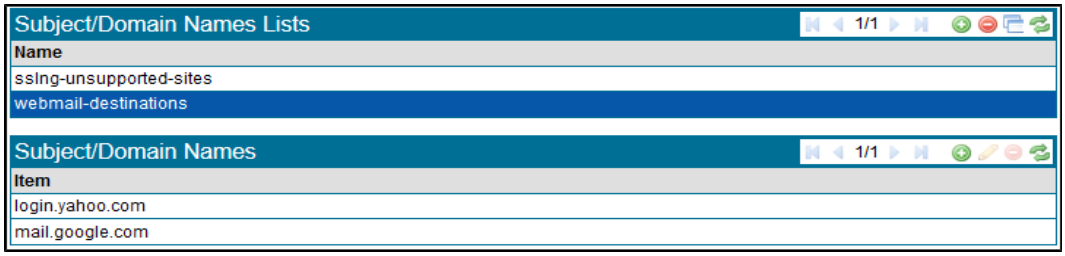


Figure 4.53 List of Subject/Domain Names

Now that the list exists we can go back to the ruleset and add a rule to use this list. Figure 4.54 shows the rule creation box with the relevant parameters configured. The radio button beside **Subject DN List** is checked and **webmail destinations** has been selected from the drop-down menu. In this example we have also configured the **Destination Port** to be 443. The effect of this rule will be to inspect any traffic going to a server that has a DN which is in the **webmail destinations** list and where the destination port number is 443. If there was any traffic to one of the servers on the list that had a destination port number other than port 443 then this rule would not be triggered.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

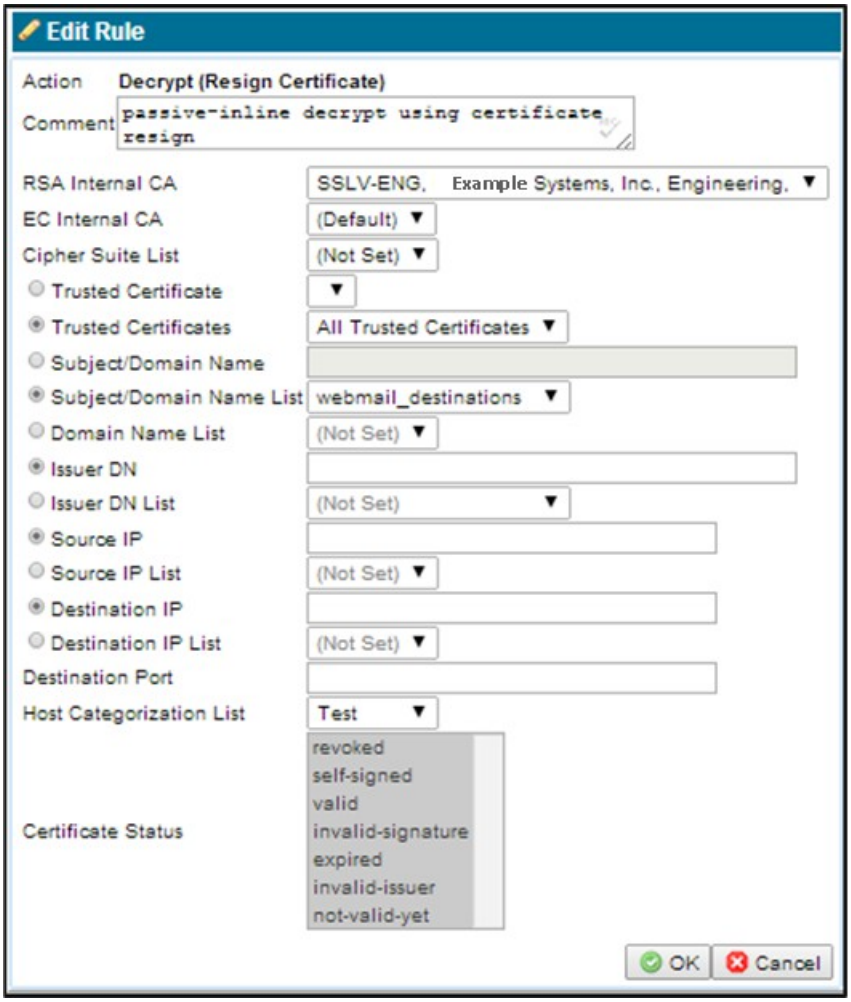


Figure 4.54 Rule to Inspect using Certificate Resign and a DN List

Note: In this example the entries added to the list are all Domain Names, and were simply typed into the add to list window. It is possible to include other elements of the x509 certificate in a list by specifying what the item is when it is added. If the type of item being added is not specified then it is assumed to be a Common Name. More details on how to include other elements of the X.509 certificate in a list are given later in this document.

Having created the rule and clicked on OK as the default action for this ruleset is "cut-through" any SSL traffic which does not match the rule will be cut through and will not be inspected. If we wanted to prevent traffic to a specific SSL site then another rule could be added to the ruleset that matched on the specific Domain Name for that site and had an action to drop the traffic.

Figure 4.55 shows how the ruleset appears after a second rule has been added that will prevent any SSL traffic going to www.example.com.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

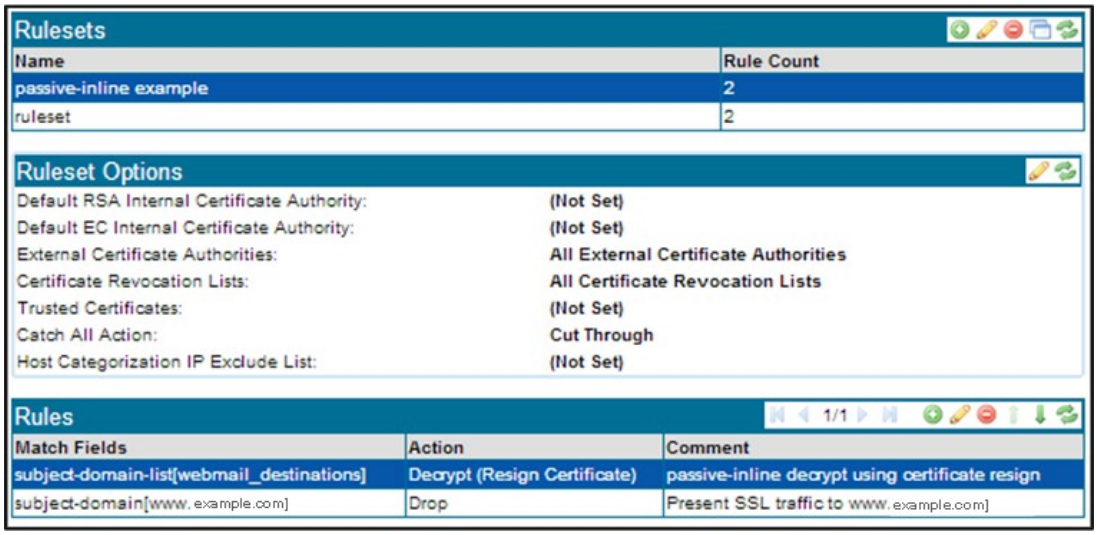


Figure 4.55 Passive-Inline Ruleset with Two Rules Defined

Having created the second rule, click Apply at the bottom of the screen. You will be able to see that the rules are now part of the ruleset.

The final part of the process is to create a segment, configure it to use the ruleset just created and then to activate it.

To create a Segment, go to the **Policies/Segments** menu option. You will see the Segments information. To create a new segment, click on the button in the Segments table and follow the same process as in the earlier example but choosing a Passive-Inline segment type. At the bottom of the screen is a Policy Changes notification block with Apply and Cancel to Apply or Cancel the change. Click Apply to complete the process and to save the CA to disk. Figure 4.56 shows the segment after it has been completed, saved and activated. Notice that:

- The ruleset created above is configured as the ruleset to be used for this segment.
- The session log has been turned on for this segment
- Interfaces 9, 10 and 11 used by this segment and are all currently down
- The segment ID is B

Figure 4.57 shows the segment status once it is active and the interface numbers which indicate how the device should be wired up to the network. In this example:

- Interfaces 9 and 10 connect to the network making the SSL2000 a bump-in-the-wire
- Interface 11 connects to the attached passive security appliance

The green background indicates that the segment is active. If there is SSL traffic to the server then the SSL session log and SSL statistics screens should show this. See Section 5.2 for details on the session log and other monitoring tools. The details for the passive-inline segment configured in an earlier example (segment A) are also shown on this screen.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

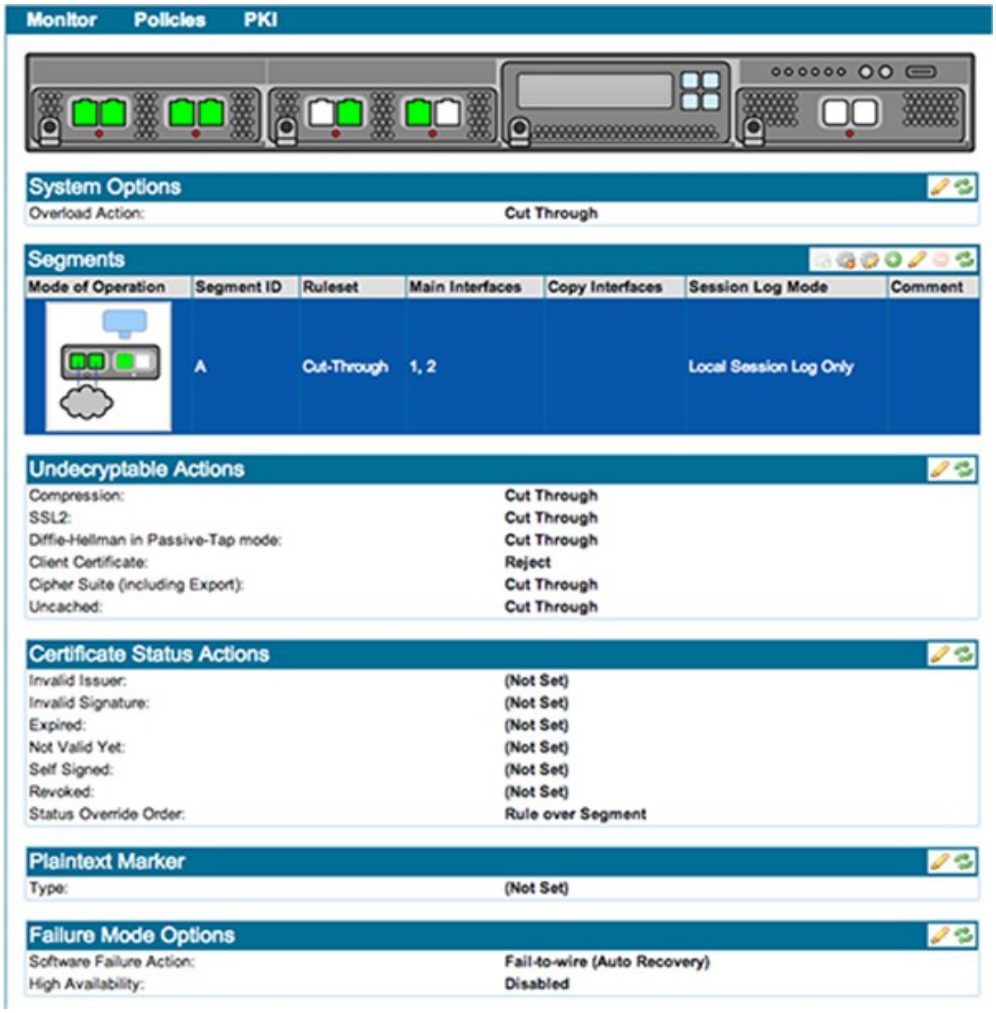


Figure 4.56 Passive-Inline Segment Configuration

Segments Status

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

Figure 4.57 Active Passive-Inline Segment

4.8 Example Active-Inline Mode Inspection

The following example shows the steps needed to configure the Sourcefire SSL appliance to inspect traffic and to pass the inspected traffic through an Active-Inline security appliance. In this example the Sourcefire SSL appliance is deployed in active-inline mode as described in Section 2.3.3. This example illustrates the use of both

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

certificate resign and known server key mechanisms to inspect traffic. It also illustrates the use of custom lists and how to apply policy to SSL traffic that is not being inspected.

The steps involved are:

- Create or load an Internal CA certificate and key into the Sourcefire SSL appliance
- Load one or more server certificates and keys into the Sourcefire SSL appliance
- Create a ruleset that contains rules to inspect traffic going to specific destinations
  - Create a list of destinations for use by a single rule
  - Create a list of local servers for which keys/certs are available
- Create a segment for active-inline operation
- Activate the segment to start inspection

The only steps in this process that have not already been covered in earlier examples are:

- Creation of a list of known server key/certificates
- Creation of a ruleset that includes both known server key inspection and certificate resign inspection
- Creation of an inline-active segment

These steps are shown below.

Figure 4.58 Create a Custom List of Known Server Keys/Certificates

Figure 4.58 shows the **Known Certificates with Keys List** window after a list called "local servers" has been added and saved. Initially this custom list has no entries as can be seen by the fact there are no entries in the **Known Certificates with Keys** area. To add entries to the list highlight the local-servers list and then click on the icon in the **Known Certificate with Keys** section.

To add keys/certs to the custom list, copy them from the **all-known-certificates-with-keys** list. Figure 4.59 shows the mechanism used to copy the desired keys/certs to the custom list. The top section of the box lists all the keys/certs that are present in the all-known-certificates-with-keys list. Clicking on an item will highlight it and clicking on the **Add to Custom List** button will copy the item into the customer list. In Figure 4.59 the key/certificate for viola.example.com has already been copied across. Once all the keys/certs that need to be included in the custom list have been copied, press OK. At

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

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 CA to disk.

Figure 4.59 Adding Entries to a Custom List

The ruleset for this example is shown in Figure 4.60 and includes five rules.

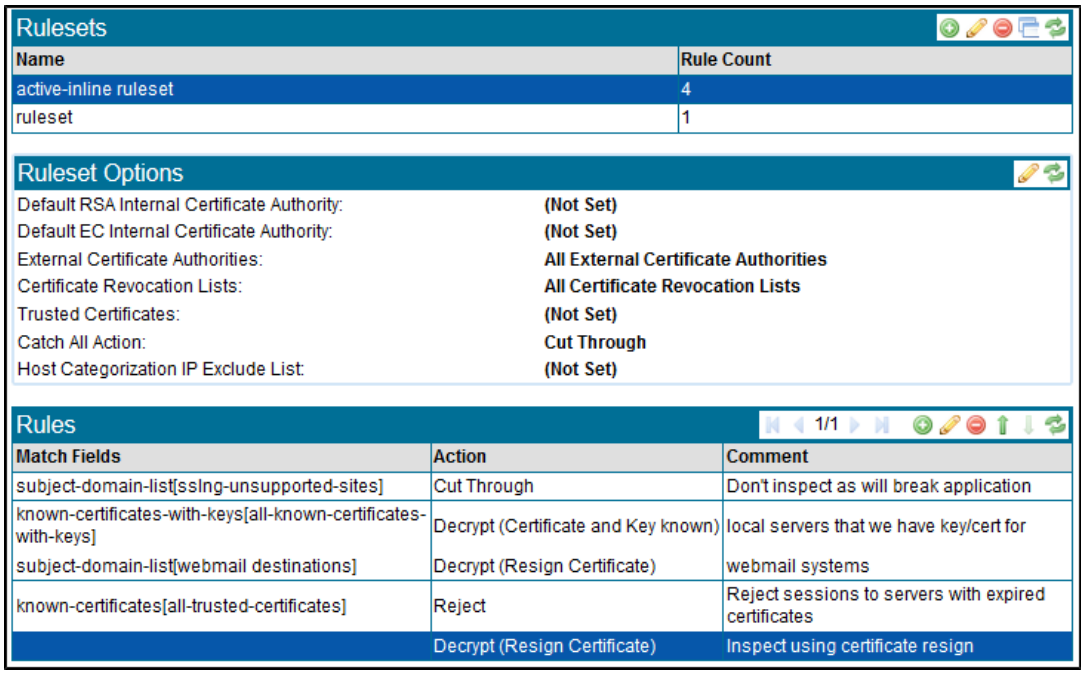


Figure 4.60 Active-Inline Ruleset

The first rule uses the default **sslng-unsupported-sites** list to cut through traffic to any destinations that are in this list. Trying to inspect traffic to these sites will cause the application to break so the cut through rule is needed to prevent this.

The second rule uses the local-servers list to inspect traffic using known server key/certificate mechanisms. The third rule uses the webmail systems list to inspect traffic to webmail systems using certificate resign.

The fourth rule causes any SSL sessions to servers that have an expired server certificate to be rejected. The fifth rule is a "catch all" rule that means any SSL traffic that has not matched one of the preceding rules will be inspected using certificate resign.

> **!** Position of rules in the table matters as the list is processed from top to bottom. As shown the rule relating to expired certificates will not apply to servers in the local-servers list as this will be processed first. The up and down arrows can be used to alter the position of a rule in the Rules block.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

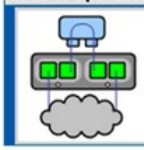
The final part of the process is to create a segment, configure it to use the ruleset above and then to activate it. To create a Segment go to the **Policies > Segments** menu option to see the Segments information. To create a new segment click Add in the **Segments** table. Figure 4.61 shows the segment configuration after it has been saved and activated. In this example you can see:

- The configuration allows the connection of an active security appliance, such as an IPS
- The configuration is a "Fail To Appliance" mode so in the event of failure of the Sourcefire SSL appliance traffic will still flow through the active security appliance
- The session log is enabled for this segment
- The configuration allows the connection of one passive security appliance which receives a copy of the traffic being sent to the active appliance
- Generated flows containing decrypted traffic are marked by changing the src MAC address to the value indicated.

System Options

Overload Action:	**Cut Through**

Segments

Mode of Operation	Segment ID	Ruleset	Main Interfaces	Copy Interfaces	Session Log	Comment
	A	active-inline-example	1, 2, 3, 4	5	Enabled	Active-inline example

Undecryptable Actions

Compression:	**Cut Through**
SSL2:	**Cut Through**
Diffie-Hellman in Passive-Tap mode:	**Cut Through**
Client Certificate:	**Reject**
Cipher Suite (including Export):	**Cut Through**
Uncached:	**Cut Through**

Certificate Status Actions

Invalid Issuer:	**(Not Set)**
Invalid Signature:	**(Not Set)**
Expired:	**(Not Set)**
Not Valid Yet:	**(Not Set)**
Self Signed:	**(Not Set)**
Revoked:	**(Not Set)**
Status Override Order:	**Rule over Segment**

Plaintext Marker

Type:	**Source MAC**
MAC Address:	**00:15:4D:00:00:D5**

Failure Mode Options

Software Failure Action:	**Fail-to-wire (Auto Recovery)**
High Availability:	**Disabled**

Figure 4.61 Active-Inline Segment Configuration

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5. User Interface Overview

5.1 Introduction

This chapter provides details of all the facilities provided by the web-based user interface (WebUI) on the SSL2000 and SSL8200 device. Each top level menu option is covered by a specific section that details all the features available and how they are used.

To connect to the web interface on the Sourcefire SSL appliance, start a web browser (Sourcefire recommends Internet Explorer and Chrome) and enter the hostname or IP address of the appliance in the address bar. The current IP address and hostname of the appliance can be viewed on the front panel LCD screen by pressing the bottom right button on the keypad until the Network option is displayed and then pressing the top left button. If the hostname has not been set yet, or if the hostname does not map to the IP address, the IP address must be used.

5.1.1 Configure the Browser

Accessing the web interface without the correct certificate installed in the web browser will cause the browser to display a warning dialog box or message. This is the normal and correct behavior for the web browser. To prevent the warning message being displayed the browser needs to be configured to trust the certificate being used by the web server in the SSL2000 and SSL8200.

There are two ways that the browser can be made to trust the SSL2000 and SSL8200 certificate. An SSL server certificate that is issued by a trusted CA can be loaded into the SSL2000 and SSL8200, this will be used by the internal web server and as it is issued by a CA that the browser trusts the browser will no longer generate a warning message.

The other method is to configure the browser to trust the "self-signed" server certificate that the SSL2000 and SSL8200 uses by default.

Details on how to import an SSL server certificate to the SSL2000 and SSL8200 are given in Section 5.5.11. If the browser generates warnings then you should consult your browser documentation for instructions on how to add the SSL2000 and SSL8200 certificate to the set of trusted certificates stored in the browser.

Figure 5.1 shows the warning produced by Chrome when accessing an SSL2000 and SSL8200 for the first time and Figure 5.2 shows the warning produced by Firefox. In both these examples the SSL2000 and SSL8200 had a management IP address of 192.168.2.42. In the case of Chrome clicking **Proceed anyway** allows the browser to connect to the SSL2000 and SSL8200. In the case of Firefox, click "**I understand the risks**" to access to screens that allow the certificate from the SSL2000 and SSL8200 to be added to the set of trusted certificates within Firefox.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

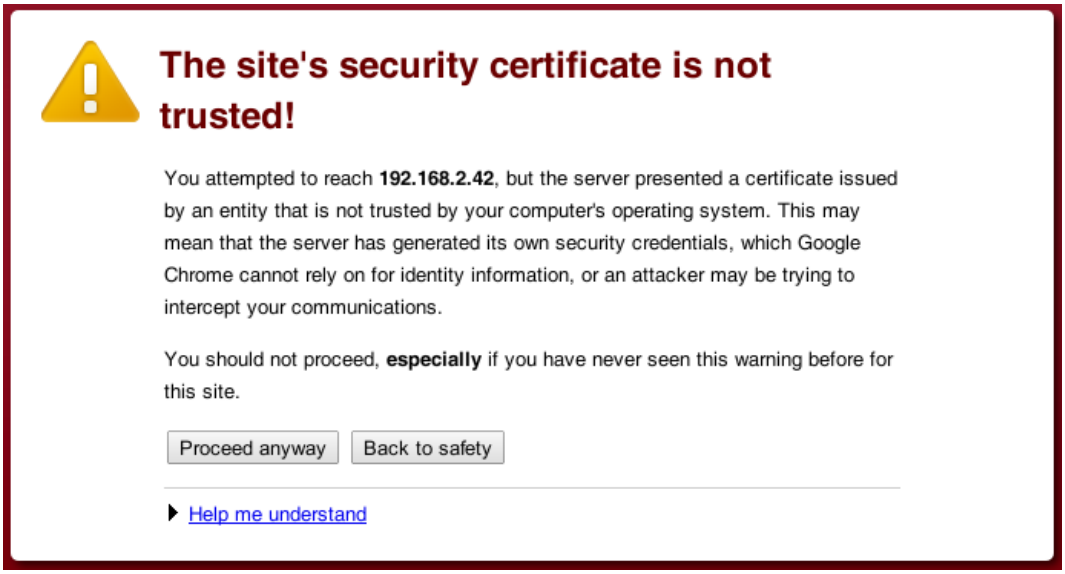


Figure 5.1 Warning from Chrome Browser

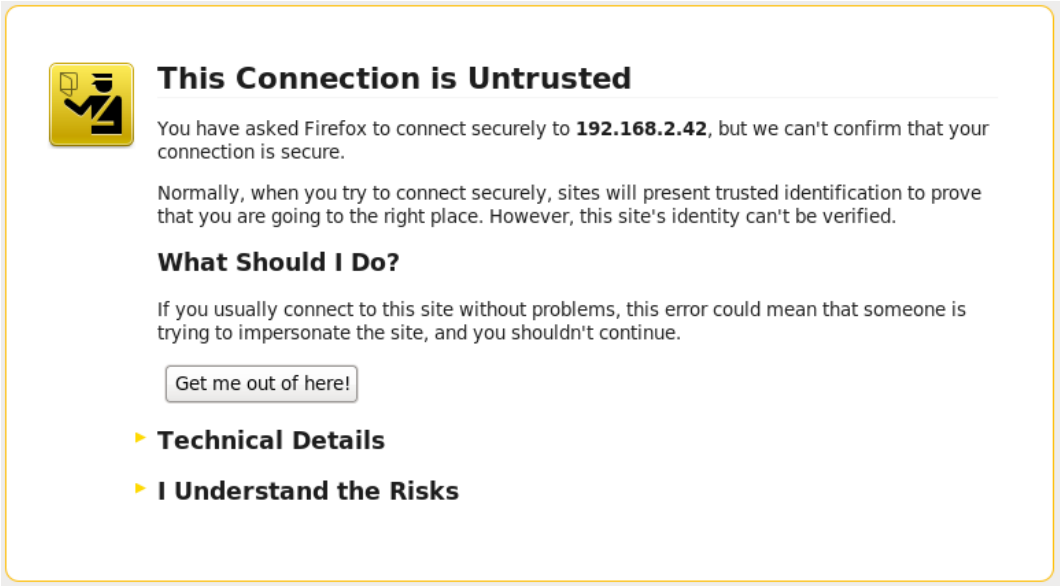


Figure 5.2 Warning from Firefox Browser

5.1.2 Login Process

The SSL2000 and SSL8200 does not have a default username and password when it is shipped from the factory. During the initial bootstrap configuration a user name and password are created and can then be used to log on to the system once the bootstrap phase is complete. See section 4.1.3 for details of the bootstrap process. Additional user names and passwords can be created on the system using the WebUI. Multiple users can be logged on to the system at the same time. The system will rate limit login attempts to prevent attacks. The system will also timeout a session and then prompt the user for their password before allowing access again.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.3 shows the standard login window presented by the WebUI. You may inspect the EULA and software attributions without logging in.

Figure 5.3 SSL2000 and SSL8200 Login

5.1.3 Using the Main Screen

The management interface screens are laid out in such a way that different types of information are displayed in specific areas on the screen, no matter which screen is being viewed. The basic organization of the management screens is described below.

Figure 5.4 shows information that is present at the top and bottom of every screen. The top of the screen contains five menus, a Refresh button and, when a refresh is occurring, a spinner to indicate this fact. The menu items are explained in detail in later sections.

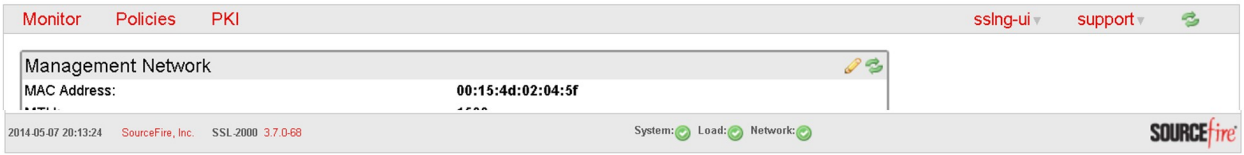


Figure 5.4 Basic Management Screen Layout

The bottom of the screen shows a status bar that is always present. It displays the following information:

- Current date in YYYY-MM-DD format
- Current time in HH:MM:SS format
- Copyright notice
- Sourcefire SSL appliance Model Number: SSL2000 or SSL8200
- Software version currently running on the system
- Icons showing current status for the **System**, **Load**, and **Network**

  The **System, Load, and Network** icons appearance varies as follows:

  - An error is present
  - A warning is present
  - Everything is fine

The active window or panel appears between the top and bottom bars, and is organized into panels; Figure 5.4 shows the **Management Network** window. Each panel of the window

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

has a title bar at the top and a set of tool icons at the right hand side.

The set of tools available varies by panel. Some the tools may be unavailable and grayed out, depending on how the panel is being used. Panels may also be empty, in which case only the title bar will be visible.

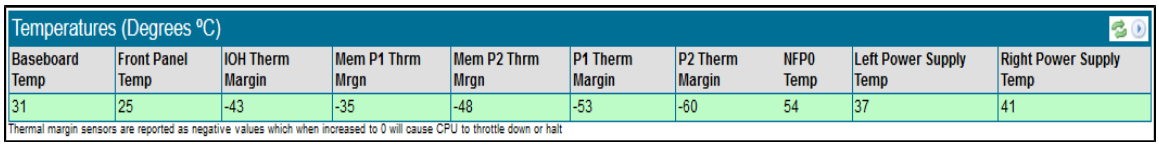


Figure 5.5 Example Information Display Panel

A display-only panel will have the Refresh tool, and may have the toggle Auto Refresh tool. The Refresh tool refreshes the data in the panel, while the toggle Auto Refresh tool turns on or off auto refresh. Figure 5.5 shows an example of a display-only panel.

Some panels contain configuration data that can be edited; in this case there is an Edit tool in addition to the Refresh tool. Figure 5.6 is an example of an editable panel that displays configuration data.

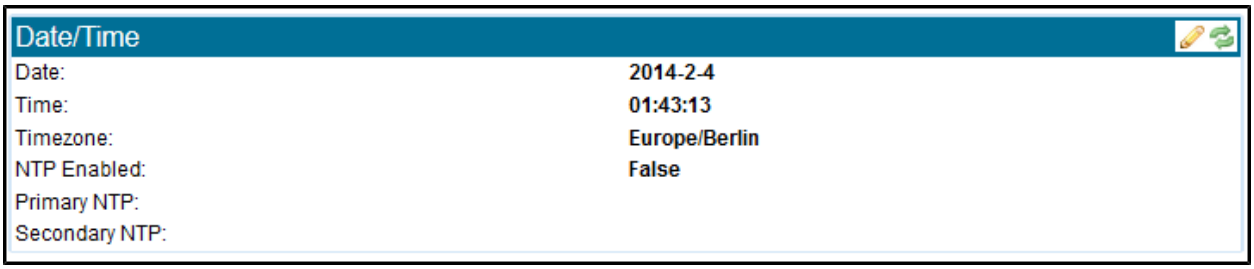


Figure 5.6 Example Configuration Edit Panel

Panels may also be linked to other panels, so that an action taken in one panel will affect the related panel. Figure 5.7 shows an example of two linked panels. The top **Subject/Domain Names Lists** panel contains details of lists that are stored in the system and has tool icons allowing the following actions in addition to the Refresh action and multipage tools:

- Add a new list
- Delete an existing list
- Clone an existing list

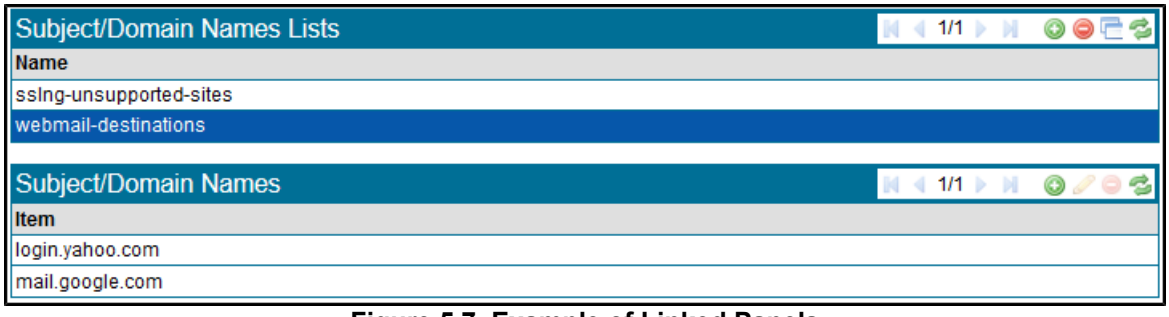


Figure 5.7 Example of Linked Panels

When a row in the top **Subject/Domain Names Lists** panel is selected the lower **Subject/Domain**

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Names panel will show the names contained in the list that has been selected and provides tools icons for you to:

- Add a name
- Edit a name (this is grayed out unless a name has been selected)
- Delete a name (this is grayed out unless a name has been selected)

One other feature that appears in some panels is an indication of which page from a number of pages of data the panel is currently displaying along with multipage tools that help you move between pages within the panel, as explained below.

- Jump to first page
- Jump to last page
- Move forward one page
- Move backward one page

You can also move directly to a particular page by clicking on the numbers between the and tool icons and then typing in the number of the required page.

Note: multipage panels have a built-in multiplier that is used in conjunction with the number of rows value that is configured as the default (see Section 5.5.13). For example, the SSL Statistics panel has a multiplier of 1.6, so with the default row setting of 10 this will mean there are 16 rows displayed in the SSL statistics panel. If the default row count was set to 20 then the SSL Statistics panel would have 32 rows.

Multipage panels are configured to display a maximum number of rows so the maximum number of pages that the panel supports is determined by the page size that is configured (see Section 5.5.13). For example, the SSL Session log holds 1024 entries which with the default row setting of 10 will mean there are maximum of 64 pages.

This covers the basic types of panel that are used by the system. Details on the specific panels used on different menus are covered in later sections of this document.

5.2 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.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

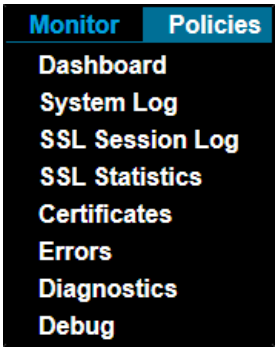


Figure 5.8 Monitor Menu Options

Figure 5.8 shows the menu options. These options are described in detail below in the order in which they appear on the menu.

5.2.1 Dashboard

The dashboard display contains seven panels containing different types of information; these panels are described below. In addition the top of the dashboard display shows a graphical representation of the system that identifies which interfaces are being used by which segment, and indicates if the interface is active or not. The image represents the physical configuration of the system so the number and types of Netmods matches the configuration of the system.

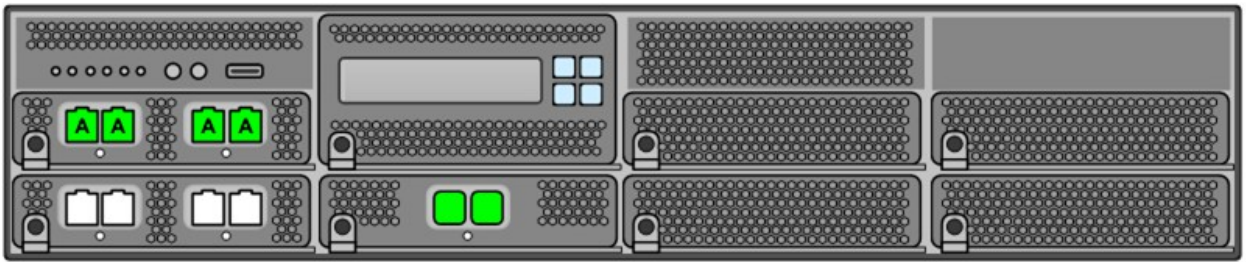


Figure 5.9 SSL8200 System Panel

Figure 5.9 shows the graphic for an SSL8200 system that has two 4 x 10/100/1000 copper Netmods installed. It shows that there is one active segment (A), and that one 10GigE port is active. All the ports that show green are up.

Figure 5.10 shows the segment status panel which displays the status of currently active segments.

- The **Segment ID** is a unique identifier that enables this segment to be distinguished from other segments that may be present in the system.
- The **Interface** numbers identify the physical ports that are being used by this segment. If any of the interfaces being used by the segment are currently down, the interface numbers will show in the **Interfaces Down** column.
- **Main Mode** indicates the operating mode of the segment.
- The **Failures** column will record any failure details.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The tools available other than the Refresh ( ) button, are the Manually Unfail icon which is normally grayed out, and the Manual Fail icon which is active if a segment is selected. The Unfail icon will only be active if the segment is in a failure mode that requires manual intervention to clear the failure. The Manual Fail tool forces a segment into a failed state.

The background color for a segment row indicates if there are any problems with the segment. In Figure 5.10 segment **A** is colored red as it has a failure.

Segments Status

Segment ID	Main Interfaces	Copy Interfaces	Interfaces Down	Main Mode	Failures
A	3, 4			Passive-Inline	Forced Failure Triggered

Figure 5.10 Dashboard Segment Status Panel

Figure 5.11 shows the **Network Interfaces** panel. This will have a row for every interface that is installed in the system so the maximum number of rows for an SSL2000 is 12 if it is fitted with three 4 x 1Gig Netmods. The maximum number of interfaces on an SSL8200 is 16. The **Link State** column will show the speed that the link is operating at when a 1G Netmod interface is in use as these can operate at 10 Mbps, 100 Mbps or GigE rates.

Network Interfaces

Port	Type	Link State	RX Packets/Bytes	TX Packets/Bytes	RX Drops
1	1G	1G	18864475/15662763383	19085341/14955569986	0
2	1G	1G	18967611/14946890174	18755544/15616215820	0
3	1G	Down	0/0	0/0	0
4	1G	Down	0/0	0/0	0
5	1G	1G	19955564/14931573650	15165425/15282183930	0
6	1G	1G	15165425/15282183930	19955571/14931583506	0
7	1G	Down	0/0	0/0	0
8	1G	Down	0/0	0/0	0

Figure 5.11 Dashboard Network Interface Panel

Each row shows the interface type and the speed it is operating at along with transmit and receive statistics. Refresh ( ) is available.

CPU Load %

cpu	cpu0	cpu1	cpu2	cpu3	cpu4	cpu5	cpu6	cpu7	cpu8	cpu9	cpu10	cpu11	cpu12	cpu13	cpu14	cpu15
0.2	1.2	0	2.9	0	0	0	0	0	0	0	0	0	0	0	1	0

Figure 5.12 Dashboard CPU Load %

Figure 5.12 shows the current **CPU Load** utilization as a percentage of the total capacity of the CPU.Refresh ( ) is available.

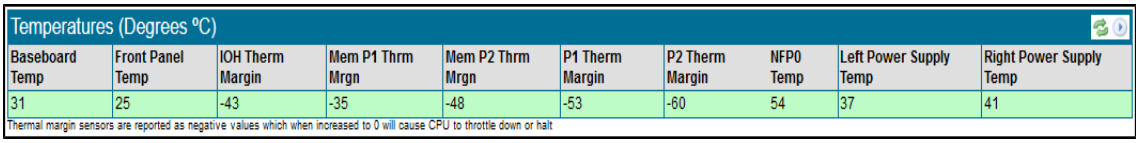
Fan Speed (RPM)

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
13276	11860	13876	11592	7237	13157	13157

Figure 5.13 Dashboard Fan Speed (RPM)

Figure 5.13 shows the **Fan Speed** panel which has the current speed values for the various fans in the system. Refresh ( ) is available.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.



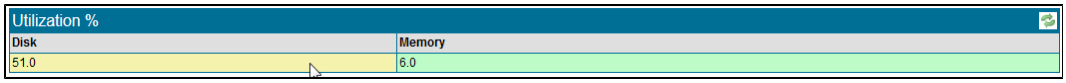
Temperatures (Degrees °C)

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
31	25	-43	-35	-48	-53	-60	54	37	41

Thermal margin sensors are reported as negative values which when increased to 0 will cause CPU to throttle down or halt

Figure 5.14 Dashboard Temperatures (Degrees °C)

Figure 5.14 shows the **Temperatures** panel which includes details of temperatures and thermal margins for components within the system. Refresh ( ) is available.

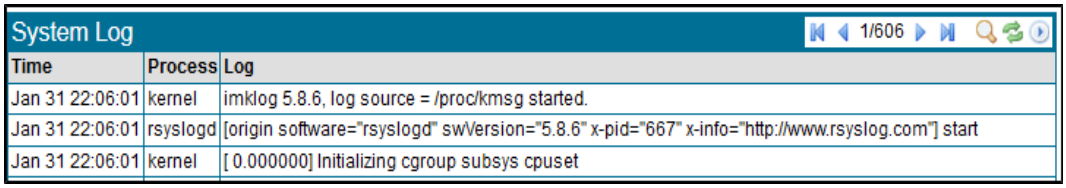


Utilization %

Disk	Memory
51.0	6.0

Figure 5.15 Dashboard Utilization %

Figure 5.15 shows the **Utilization** panel which shows the percentage utilization of system memory and disk space. Refresh ( ) is available.



System Log 1/606

Time	Process	Log
Jan 31 22:06:01	kernel	imklog 5.8.6, log source = /proc/kmsg started.
Jan 31 22:06:01	rsyslogd	[origin software="rsyslogd" swVersion="5.8.6" x-pid="667" x-info="http://www.rsyslog.com"] start
Jan 31 22:06:01	kernel	[0.000000] Initializing cgroup subsys cpuset

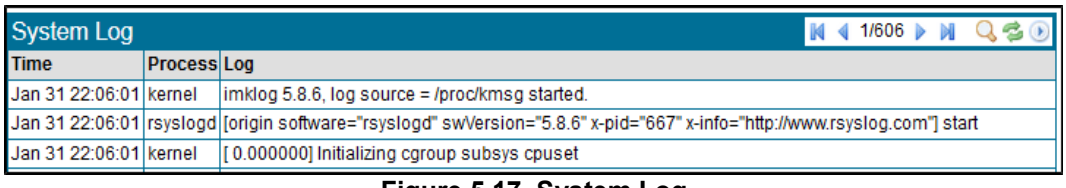
Figure 5.16 Dashboard System Log

Figure 5.16 shows the **System Log** panel that contains the most recently generated system log entries, this panel automatically refreshes.

5.2.2 System Log

The **System Log** screen (Figure 5.17) contains a single multipage panel enabling all entries in the system log to be viewed. The panel has the multipage navigation tools, as well as Refresh and Search.

Data displayed includes license information (Section4.3.4 and Section 5.5.8) as well as system processes.



System Log 1/606

Time	Process	Log
Jan 31 22:06:01	kernel	imklog 5.8.6, log source = /proc/kmsg started.
Jan 31 22:06:01	rsyslogd	[origin software="rsyslogd" swVersion="5.8.6" x-pid="667" x-info="http://www.rsyslog.com"] start
Jan 31 22:06:01	kernel	[0.000000] Initializing cgroup subsys cpuset

Figure 5.17 System Log

Clicking on the Search tool brings up the **Filter on Process** pop-up, where you can filter log entries to display only entries created by a particular process. See Figure 5.18. Valid inputs are the names of processes which appear in the process column in the panel.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

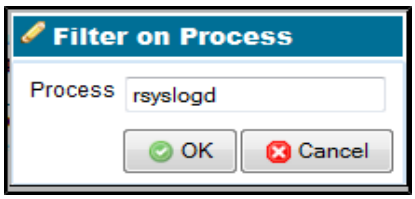


Figure 5.18 Filter on Process

To cancel a filter simply open up the **Filter on Process** window and delete the text in the input field and then click **OK**.

5.2.3 SSL Session Log

The **SSL Session Log** screen (Figure 5.19) contains a single multipage panel enabling all entries in the last 64 pages of the SSL Session log to be viewed. The panel has the usual multipage navigation buttons in addition to the Refresh button, a View Details, , button, an Export button and two filter buttons .

SSL Session Log 1/3414

Start Time	Segment ID	SrcIP:Port	DstIP:Port	Domain Name	Certificate Status	Cipher Suite	Action	Status
Mar 28 10:03:55.142	A	10.253.10.63:49760	10.2.2.154:443	Multiple domains	Invalid Issuer	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:03:24.696	A	10.253.10.62:50293	74.125.239.96:443	SNI: plus.google.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.618	A	10.253.10.62:50292	74.125.239.96:443	SNI: plus.google.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.617	A	10.253.10.62:50291	74.125.239.105:443	SNI: apis.google.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.567	A	10.253.10.62:50290	74.125.239.111:443	SNI: www.gstatic.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.013	A	10.253.10.62:50289	74.125.239.106:443	lh6.googleusercontent.com	Invalid Issuer	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Decrypt (Resign Certificate)	Success
Mar 28 10:03:23.389	A	10.253.10.103:49877	74.125.239.111:443	ssl.gstatic.com	Invalid Issuer	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:20.764	A	10.253.10.63:49759	10.2.2.154:443	Multiple domains	Invalid Issuer	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:03:19.476	A	10.253.10.62:50288	74.125.225.146:443	SNI: www.google.com		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:02:58.095	A	10.253.10.103:49876	10.253.11.104:443	piranha.pa.bluecoat.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.093	A	10.253.10.103:49875	10.253.11.104:443	piranha.pa.example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.092	A	10.253.10.103:49874	10.253.11.104:443	piranha.pa.example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.091	A	10.253.10.103:49873	10.253.11.104:443	piranha.pa.example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.088	A	10.253.10.103:49872	10.253.11.104:443	piranha.pa.example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.085	A	10.253.10.103:49871	10.253.11.104:443	piranha.pa.example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:54.230	A	10.253.10.103:49870	10.2.2.154:443	Multiple domains	Invalid Issuer	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success

Figure 5.19 Session Log

The filter on errors tool causes the session log to only display entries for flows that were not inspected successfully. The no filter tool causes the session log to revert to showing all entries.

The Export tool brings up a window where you can specify the range of SSL session log entries to export.

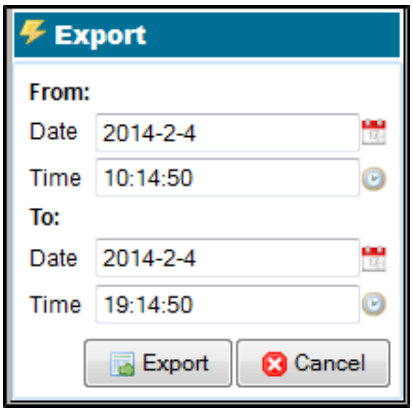


Figure 5.20 Export Session Log

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.20 shows the **Export** window, where you set the start and end date and time that the exported session logs should cover. Press the Export button and the standard save file process on the browser will be invoked, which may automatically save the export file to a default location or may prompt the user to specify a location.

The saved file contains a set of .bin files and a file that contains the public certificates used in the SSL sessions captured in the session log. In order to view the session log data the .bin files must be processed with a tool to extract the data in a user-readable form. The tool and documentation for the tool are provided separately; contact Customer Service and request the sslsessions.py tool.

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
- Domain name of the SSL server accessed during the session
- Status of the server certificate
- Cipher Suite that was used for the session
- Action taken by the Sourcefire 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 1/64 is the most recent entry and the last row on page 64/64 is the oldest entry.

The View Details button is only active when a row in the **SSL Session Log** panel has been selected. Clicking it will open a window showing more details about the selected session. Figure 5.21 shows an example of the detail available for a successful session. Clicking on the + or : symbol at the start of a line will expand or contract the level of detail displayed.

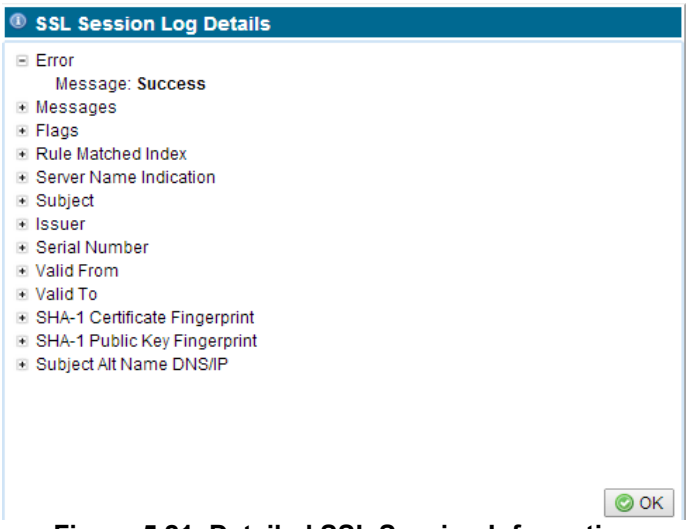


Figure 5.21 Detailed SSL Session Information

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.2.4 SSL Statistics

The **SSL Statistics** screen contains a single multipage panel enabling all entries in the last 64 pages of the **SSL Statistics** log to be viewed. The panel has the normal multipage navigation and Refresh tools.

SSL Statistics 1/64

Timestamp	#Detected	#Done	#Ignored	#Decrypt	#Decrypt Done	#Error	Detected	Decrypt
Feb 12 14:19:05	13361	13301	809	11474	11418	18	60	56
Feb 12 14:19:04	13361	13300	809	11473	11417	18	61	56
Feb 12 14:19:03	13359	13299	809	11472	11416	18	60	56
Feb 12 14:19:02	13357	13297	809	11470	11414	18	60	56
Feb 12 14:19:01	13357	13297	809	11470	11414	18	60	56
Feb 12 14:19:00	13356	13296	808	11470	11414	18	60	56
Feb 12 14:18:59	13352	13294	808	11466	11412	18	58	54
Feb 12 14:18:58	13351	13293	808	11465	11411	18	58	54
Feb 12 14:18:57	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:56	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:55	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:54	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:53	13350	13276	808	11464	11394	18	74	70
Feb 12 14:18:52	13349	13275	808	11463	11393	18	74	70
Feb 12 14:18:51	13349	13275	808	11463	11393	18	74	70
Feb 12 14:18:50	13349	13275	808	11463	11393	18	74	70

Figure 5.22 SSL Statistics

Figure 5.22 shows an example where page 1 out of the 64 pages of available statistics information is being displayed. Statistics are collected every second and each row in the table holds the data for a collection interval. Apart from the **Detected** and **Decrypted** columns all the counts are cumulative.

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. So, the first row on page 1/64 is the most recent entry and the last row on page 64/64 is the oldest entry.

5.2.5 Certificates

The **Certificates** window contains tabs for accessing the details of invalid certificates that have been received by the SSL2000/SSL8200. The panel has an acknowledge tool in addition to the Refresh () and Export () tools. Use the Export tool to export details of all invalid certificates to a .csv file.

The tabs show details for different types of invalid certificate states. You can Enable () or Disable () the dumping of invalid certificates to the system log.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

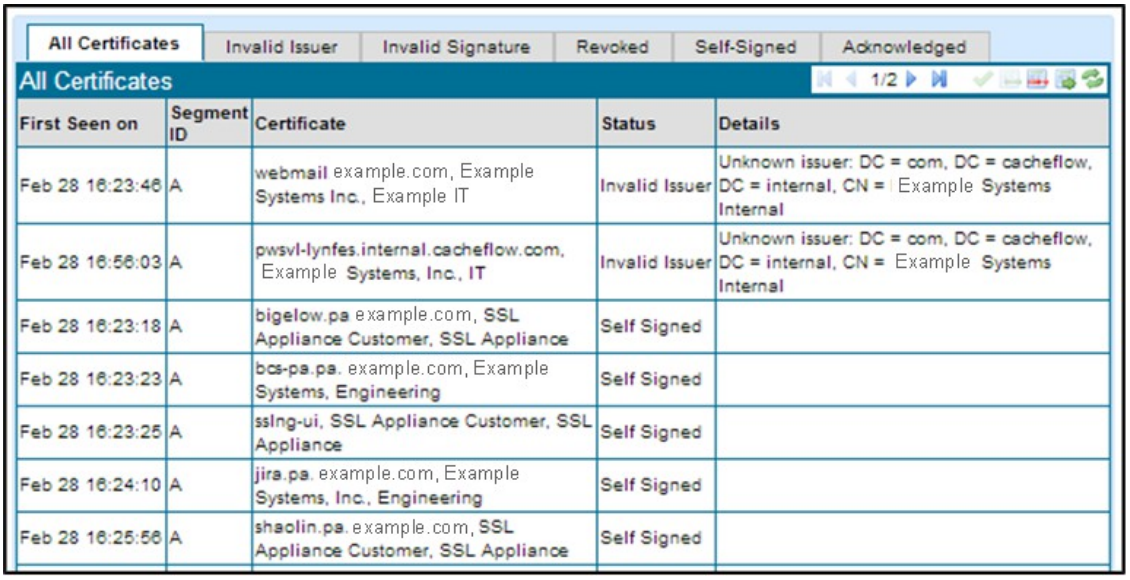


Figure 5.23 Invalid Certificates Panel

Figure 5.23 shows the panel displaying details of all certificates that the system has seen which had problems of some description. By clicking on the relevant tab details for specific types of invalid certificates can be viewed, for example Figure 5.24 shows details of self-signed certificates that have been seen by the system.

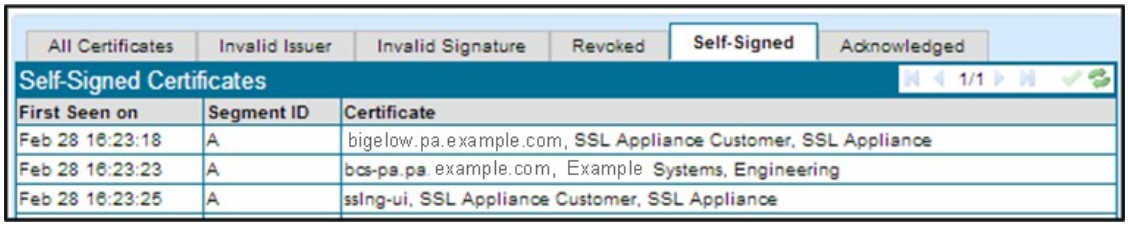


Figure 5.24 Invalid Certificates Panel with Self-Signed Certificate Details

If a certificate is invalid for more than one reason then it will appear on more than one tab. The acknowledge tool can be used to notify the system that the certificate status has been noted. Once a certificate has been acknowledged it will appear on the acknowledged tab only. To acknowledge a certificate, select the certificate and then click on the ✔ tool. Acknowledged certificates will not be included in details on invalid certificates that are collected in the system log files.

Note: Invalid certificate details are automatically cleared from any tab when the segment that they occurred on is deactivated.

5.2.6 Errors

The **Errors** screen contains a single panel that shows SSL Error counts for each active segment. Error counts are cleared when changes are made to the current ruleset, and policy is reset. The panel has the standard multipage controls in addition to the Refresh (🔄) and Export (📤) buttons. Use the Export button to export the details of all errors to a .csv file.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Note: An appliance functioning perfectly may have a non-zero **SSL Error Count**. An error count doesn't necessarily mean something is wrong.

SSL Error Counts 1/1

Segment ID	Code	Message	Count
A	0x34000017	Invalid MAC	1
A	0xc800014e	TCP queue processing timeout	1
A	0xc800034e	TCP queue processing timeout	4
A	0xc800044e	TCP queue processing timeout	19

Figure 5.25 SSL Error Counts

Figure 5.25 shows a panel with a single invalid MAC address error, and multiple flows which ended without a FIN/RST sequence. There may be multiple rows for a single segment if there have been more than one type of error seen on that segment. Whenever a segment is activated or deactivated the error counts associated with that segment is reset to zero.

5.2.7 Diagnostics

The **Diagnostics** screen contains a single dialog box that allows the user to specify what types of information should be included in the diagnostic file and the to cause the file to be generated.

Figure 5.26 shows the dialog box with SSL Statistics currently selected for inclusion in the diagnostic file. Checking the box against an item will cause it to be included in the diagnostic file. Click **OK** to create the file. The date fields can be used to limit the statistics/history data included in the diagnostic file.

! Including the SSL Statistics and/or the Host Statistics, and/or the NFP statistics, may result in a large diagnostic file. Use these only if really required.

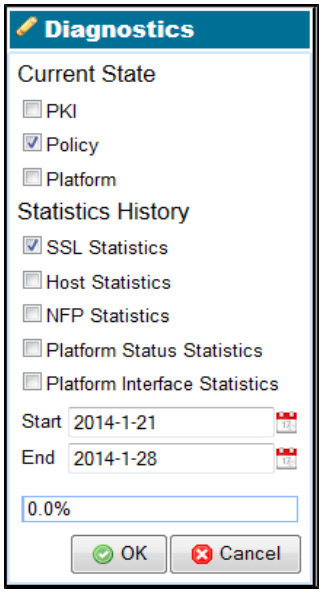


Figure 5.26 Diagnostics

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.2.8 Debug

The **Debug** display contains a single multipage panel containing **NFE Network Statistics**. The information on this screen is, as the name implies, primarily intended to assist with debugging issues with the SSL2000 and SSL8200. Support personnel may ask for information from the debug screens when providing support. The **NFE Network Statistics** panels contain information that may be useful to a user in diagnosing configuration issues; some of the pages on the panel are described below.

The panel has multipage navigation and Refresh tools.

The **NFE Network Statistics** panel shows details of traffic to and from the NFE acceleration card(s) used in the SSL2000 and SSL8200. The NFE card has two 10 Gbps links that connect to an Ethernet switch which in turn connects to the set of Netmods that provide the external interfaces on the SSL2000 and SSL8200.

Figure 5.27, Figure 5.28 and Figure 5.29 show details for two NFE links. For the SSL2000 there are two NFE links in the system; an SSL8200 has four NFE links, and will display two extra columns of data.

NFE Network Statistics 1/3

	i/f 0	i/f 1
BadCRC	0	0
BadOctetsReceived	0	0
BroadcastFramesReceived	23775	23775
BroadcastFramesSent	23775	23775
CRCErrorsSent	0	0
Collisions	0	0
ControlFrameReceived	0	0
ExcessiveCollisions	0	0
FCReceived	0	0
FCSent	71437997	71437997
Fragments	0	0
Frames1024toMaxOctets	3136667	5244443
Frames128to255Octets	699907	701201
Frames256to511Octets	220317	226869
Frames512to1023Octets	227059	244350
Frames64Octets	0	0

Figure 5.27 Debug NFE Network Statistics 1

NFE Network Statistics 2/3

	i/f 0	i/f 1
Frames65to127Octets	4335636	3455977
GoodOctetsReceived	1894206543	4869814510
GoodOctetsSent	3400165410	3368384592
GoodUnicastFramesReceived	3598608	5361243
InRangeLengthErrorsReceived	0	0
Jabber	0	0
LateCollisions	0	0
MulticastFramesReceived	129060	129060
MulticastFramesSent	129060	129060
OutOfRangeLengthErrorsReceived	0	0
Oversize	0	0
ReceiveFIFOOverrun	0	0
RxErrorFrameReceived	0	0
SentDeferred	0	0
SentMultiple	0	0
SymbolErrorReceived	0	0

Figure 5.28 Debug NFE Network Statistics 2

NFE Network Statistics 3/3

	i/f 0	i/f 1
TxBackoff	0	0
TxCarrierSenseErrors	0	0
TxExcessiveDefer	0	0
Undersize	0	0
UnicastFramesSent	4725363	4216526

Figure 5.29 Debug NFE Network Statistics 3

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.3 Configuring Segments and Policies

The **Policies** menu contains options for configuring segments and defining policies and rules that determine how SSL traffic is handled, and which SSL traffic is inspected.

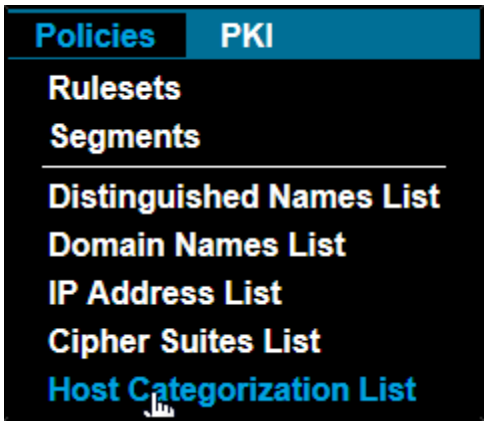


Figure 5.30 Policies Menu

Figure 5.30 shows the **Policies** menu options. The top two options let you configure **Rulesets** and **Segments**, while the remaining options let you configure lists that can be used within Rulesets. These options are described in detail below in the order in which they appear on the menu.

In order to configure policy referencing a Host Categorization List database, a valid Host Categorization license is required. See Section 5.3.7 for information on Host Categorization.

See Section 5.5.8 for details on managing licenses.

5.3.1 Rulesets

Rulesets contain the rules and policies that control how SSL traffic is handled. They are associated with one or more segments. Rulesets can also exist unassociated with any segment.

The **Rulesets** display contains three panels. The lower two panels display information which depends on the row selected in the first panel.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

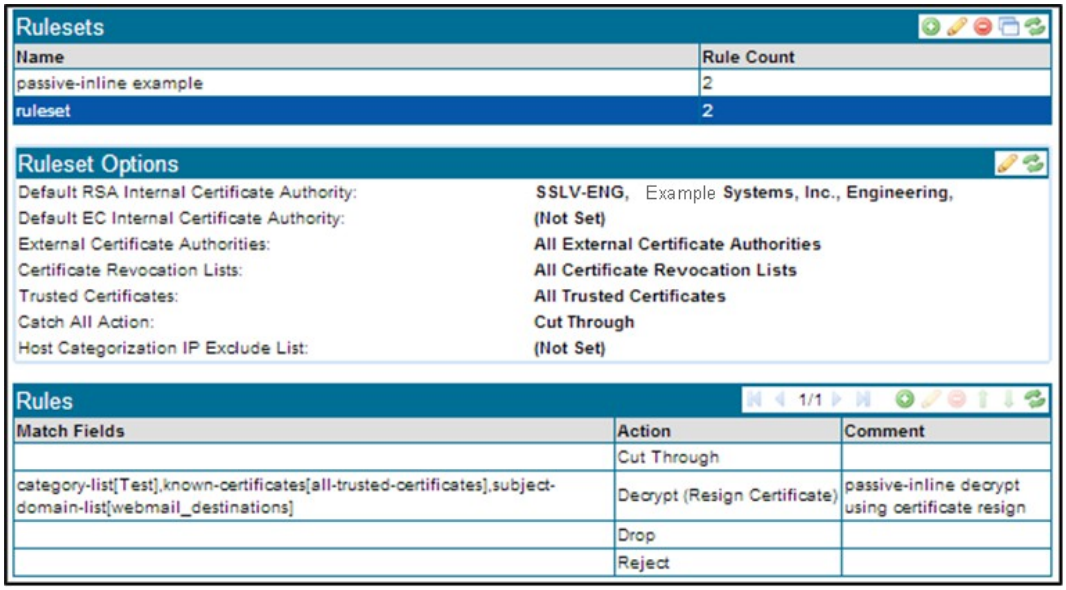


Figure 5.31 Rulesets

Figure 5.31 shows the **Rulesets** panel with two existing rulesets. Each existing ruleset occupies one row in the table and the right hand column shows the number of rules that are currently within that ruleset. Tools on this panel let you Add, Remove or Clone a ruleset. The remove and cloning tools will be grayed out unless an entry in the table is selected. If the clone tool is used a window appears for configuring the ruleset's clone.

Figure 5.32 shows the dialog box. A similar dialog box will appear if the add ruleset option is selected.

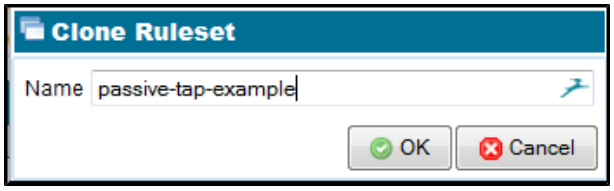


Figure 5.32 Rulesets Clone

To cause the second and third panels to display information, select a ruleset entry in the **Rulesets** panel. To do so, click on an entry; this will highlight the entry in the **Rulesets** panel, and cause the **Rulesets Options** panel to expand and become active. The **Rules** panel displays the rules that exist within the selected ruleset.

Figure 5.33 shows the Rule set **Option** panel, where you configure the ruleset settings. The panel provides Edit and Refresh tools.

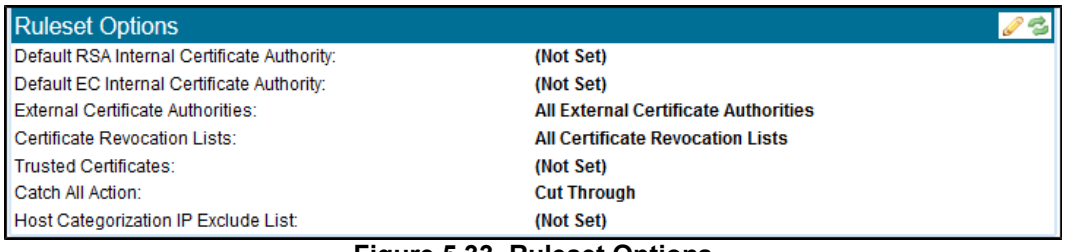


Figure 5.33 Ruleset Options

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

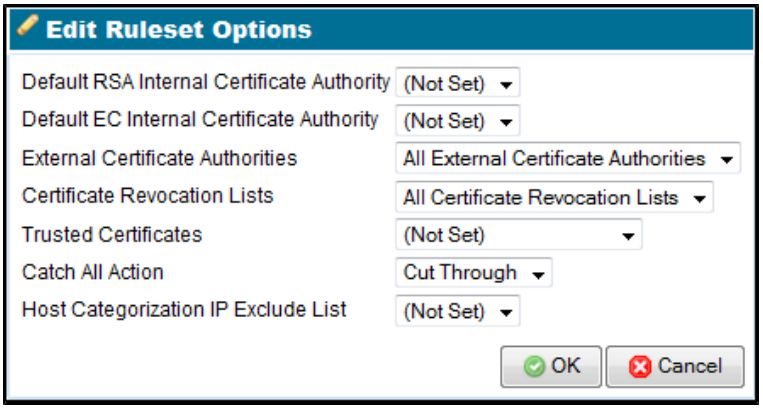


Figure 5.34 Edit Ruleset Options

Figure 5.34 shows the edit box with drop-down menus to allow selection of the desired settings for this ruleset. The options that can be configured are:

- **Default RSA Internal Certificate Authority**: Used for "Decrypt (Resign Certificate)" rules where no RSA internal CA is specified
- **Default EC Internal Certificate Authority**: Used for "Decrypt (Resign Certificate)" rules where EC internal CA is specified
- **External Certificate Authorities**: Selects the list of trusted external CAs that will be checked against when SSL sessions are processed by rules within this ruleset
- **Certificate Revocation Lists**: Selects the set of CRLs that will be checked against when SSL sessions are processed by rules within this ruleset
- **Trusted Certificates**: Selects the set of trusted certificates that will be checked against when SSL sessions are processed by rules within this ruleset
- **Catch All Action**: Defines what happens to an SSL session that does not trigger any rules within this ruleset
- **Host Categorization IP Exclude List**: Selects the Host Categorization IP Exclude list as the list to check against when SSL sessions are processed by rules within this ruleset. See Section 5.3.7.

The **Rules** panel, the bottom panel in Figure 5.31, displays the rules currently defined in the ruleset being edited.

Rule Set Tools

The multipage selection tool is used to move between pages of rules when there are many rules in the ruleset.

	Multipage tools
	Add
	Delete
,	Move up, move down
	Refresh

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Clicking the Add tool opens up the **Insert Rule** window, as shown in Figure 5.35. Use the **Action** drop-down menu to select of the type of rule to create. Choosing an option from the drop-down will cause the window to update to contain fields relevant for the type of rule selected.

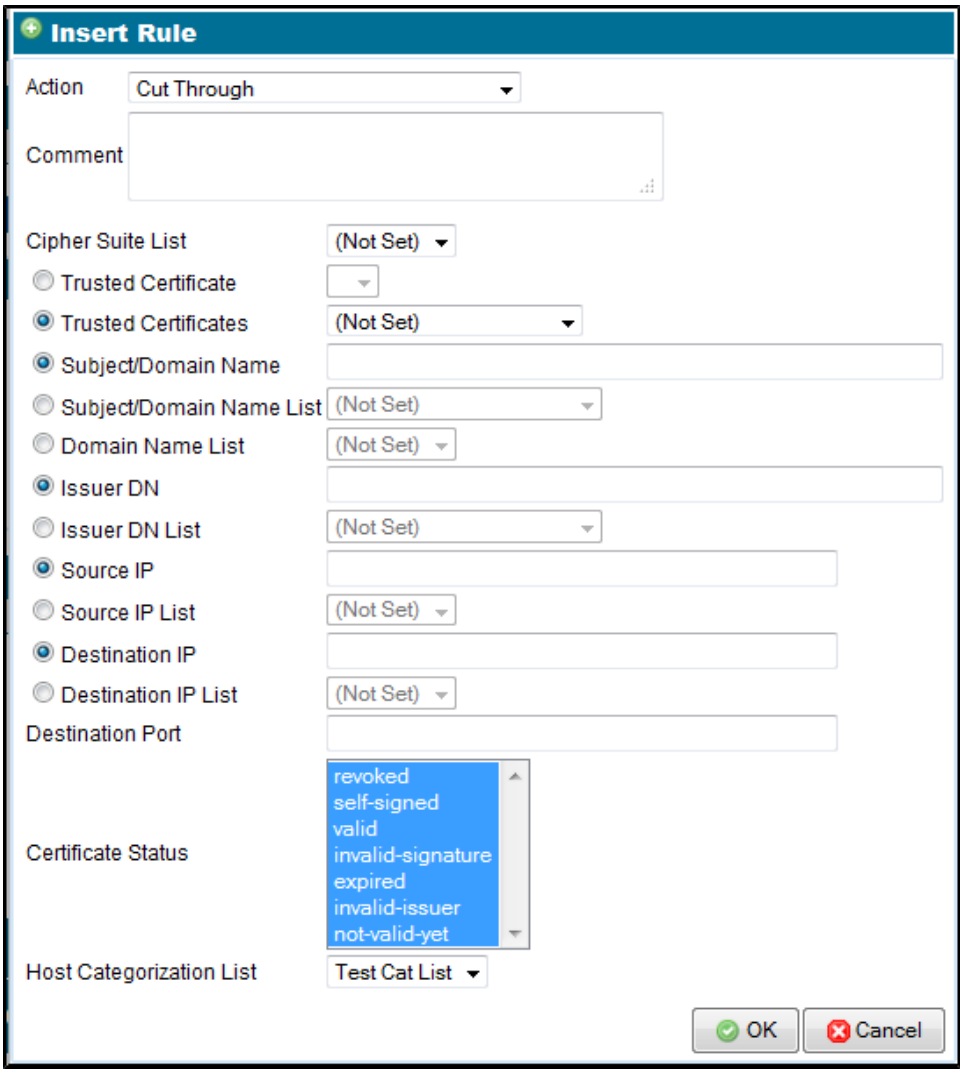


Figure 5.35 Insert Rule

See Section 2.4.2 for an explanation of the parameters that can be configured for the different types of rules. For example, if **Decrypt (Certificate and Key known)** is selected, the **Insert Rule** window will appear as in Figure 5.36.

Note: If there is more than one rule specified in a ruleset then the position of a rule in the Rules table becomes important. Rules are processed from the first rule in the table (top row on page 1) to the last rule in the table (bottom row on last page) so if a more generic rule occurs in front of a more specific rule then the generic rule will be encountered first and will always be used. An example will make this clear:

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Rules 1/1

Match Fields	Action	Comment
subject-domain-list[sslng-unsupported-sites]	Cut Through	cut through sites cannot inspect to
subject-domain[webmail systems]	Decrypt (Resign Certificate)	webmail systems
known-certificates-with-keys[all-known-certificates-with-keys]	Decrypt (Certificate and Key known)	inspect local server traffic
known-certificates[all-trusted-certificates]	Reject	reject sessions to servers with expired certificates
	Decrypt (Resign Certificate)	inspect using certificate resign

Figure 5.36 Rules Table Positioning

Figure 5.36 shows a table containing five rules. The fourth rule is highlighted and is a rule that prevents any SSL sessions to destinations that have an expired SSL server certificate. The third rule causes traffic to destinations that are in the webmail list to be inspected. As the third rule will always be processed before the fourth rule traffic to any system in the webmail list will be inspected even if that system has an expired SSL server certificate.

In order to ensure that traffic is not allowed to a system in the webmail list if it has an expired server certificate the position of the highlighted rule needs to be changed so that it comes before the rule inspecting traffic to systems in the webmail list. To correct this, select the highlighted rule, then use the ⇧ tool to move it up in the table so that it is positioned above the rule inspecting traffic to systems in the webmail list.

> **!** If a rule does not appear to be working, always check that it is not below a more generic rule that will apply to the traffic it is intended to match.

5.3.2 Segments

The Segments display contains a graphical display of the system and six panels. The information displayed on the lower four panels depends on the row selected in the second panel.

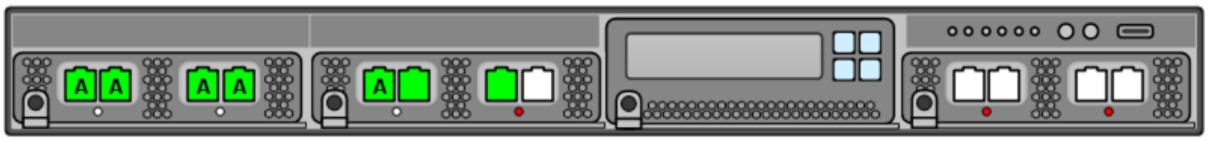


Figure 5.37 System Graphic on Segment Screen

Figure 5.37 shows an example of the graphic for an SSL2000 device. The graphic is dynamically created so it will reflect the set of interfaces that are installed in the box, in this case the unit has three 4 x 10/100/1000 Netmods installed.

- Any interface that does not have a letter is currently not being used by an active segment.
- Any interface that shows as green indicates that the relevant link is up.
- Deactivating an active segment releases the external interfaces used by that segment and they become available for use by other segments.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

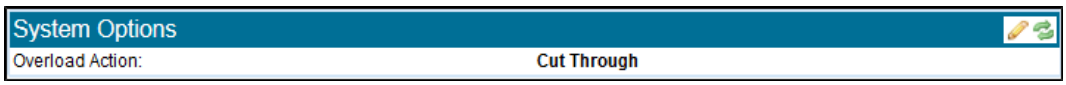


Figure 5.38 Segment System Options

Figure 5.38 shows the first panel on the **Segments** screen where you can configure the default action that the system should take if it is overloaded. In the example shown the action is to cut through traffic, other options are drop or reject. This panel has Edit and Refresh tools.

The **Segments** panel (second from top) contains a row for each segment that is configured in the system. In addition to the Add, Edit, Delete and Refresh tools, it includes Activate and Deactivate tools ad an Edit Copy Mode tool.

See Section 2.3 for details of the modes of operation that can be selected for a segment when it is created. Section 2.4.1 and Sections 4.6, 4.7 and 4.8 provide examples of how to configure segments using the **Segments** panel.

Once a segment definition exists in the **Segments** panel it can be selected by clicking on it. Once selected, the lower four panels on the screen display information relevant to the selected segment.

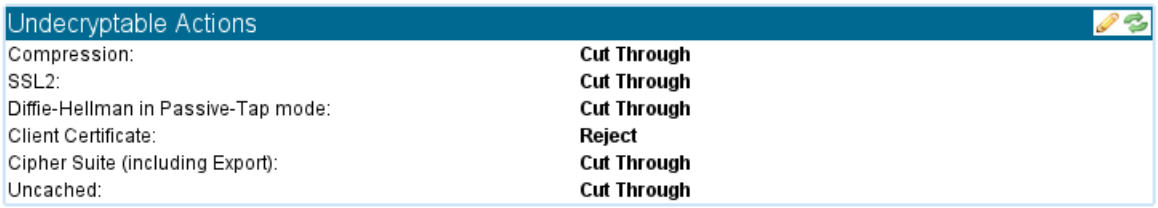


Figure 5.39 Segment Undecryptable Actions

Figure 5.39 shows the **Undecryptable Actions** panel which lets you control how SSL sessions on this segment that cannot be decrypted are handled. The panel has Edit and Refresh tools. Click the Edit tool to open a window where you can select the action to be take when a session is not decryptable for the specific reason. An SSL session cannot be decrypted for the following reasons:

- **Compression**: The system does not support inspection of SSL sessions that use compression
- **SSL2**: The system only provides partial support for inspecting SSL sessions using SSLv2 (SSL v2 is an old and insecure version of SSL and its use is not recommended).
- **Diffie-Hellman in Passive-Tap mode:** In Passive-Tap mode it is impossible to inspect sessions that use Diffie-Hellman (DHE) for key exchange (inspection of sessions using DHE is only possible if the inspecting device is installed in-line).
- **Client Certificate**: The use of client certificates in some situations can prevent an SSL Session being inspected. This action is applied when such a session is present.
- **Cipher Suite**: The system does not support all possible SSL cipher suites: this action is applied when a cipher suite that is not supported is used by an SSL session.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- **Uncached**: An SSL session established using session re-use can only be inspected if the system has the session state for the session being re-used in its cache; this action is applied when the session state is not cached.

Figure 5.40 Certificate Status Actions

Figure 5.40 shows the **Certificate Status Actions** panel which lets you control of how the system deals with SSL sessions on this segment that have particular states in the server certificate used for the session. The possible actions are, **Not Set**, **Cut Through**, **Drop**, and **Reject**. **Not Set** means that the particular status will be ignored.

Figure 5.41 Edit Certificate Status Actions

Figure 5.41 shows the **Edit Certificate Status Actions** dialog. You can configure the **Status Override Order.** This option determines whether or not the segment settings in this box take precedence over any settings in rules within the ruleset used by this segment. The options are either "Rule over Segment" and "Segment over Rule".

The remaining two panels on this screen are the **Plaintext Marker** panel and the **Failure Mode Options** panel, each of which has Edit and Refresh tools, and lets you configure the failure mode and High Availability (HA) options.

Clicking on the edit tool for the **Plaintext Marker** panel produces a dialog box that lets you control of how generated TCP flows containing inspected traffic are marked; see Figure 5.42. There are two reasons for marking these flows:

1. An attached passive security appliance may wish to be able to determine which traffic that it receives has been decrypted by the Sourcefire SSL appliance and which has not. Configuring marking means the Sourcefire SSL appliance will mark all generated flows and the attached appliance can use the marker to distinguish between inspected and non-inspected traffic.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

2. If the Sourcefire SSL appliance is configured to operate in Active-Inline mode then marking MUST be enabled as the Sourcefire SSL appliance needs to be able to distinguish between inspected and non inspected traffic when it returns to the Sourcefire SSL appliance from the active security appliance.

The options available for marking generated flows are:

- **Source MAC**: Modifies the SRC MAC address in generated flows
- **VLAN**: Tags generated flows with a specific VLAN ID

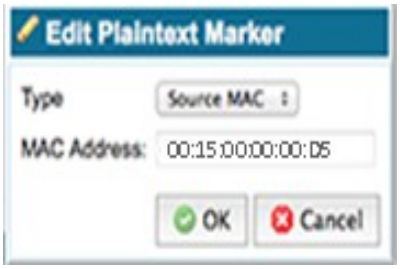


Figure 5.42 Edit Plaintext Marker

Clicking on the edit tool for the **Failure Mode Options** panel produces a dialog box (Figure 5.43) allowing configuration of how the system deals with software failures. The options, listed below, determine how this segment will behave in the event of software failure:

- Disable Interfaces
- Drop Packets (Auto Recovery)
- Fail-to-wire (Auto Recovery)
- Fail-to-wire (Manual Reset)
- Ignore Failure

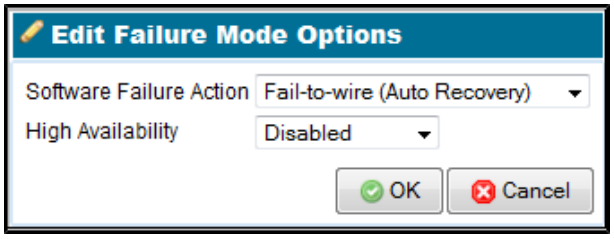


Figure 5.43 Segment Failure Mode Options

The options for High Availability mode are:

- **Disabled**: HA mode is not active
- **Auto Recovery**: Automatic recovery from failure mode when the cause of the failure is removed
- **Manual Reset**: Manual action via the WebUI is needed to exit failure mode.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.3.3 Subject/Domain Names List

Entries in a **Subject/Domain Names List** are matched against the domain names and certificate subject of the SSL server for a session. The server Common Name (CN) and Subject Alternate Names (SAN) fields in the SSL server certificate are used in addition to the Server Name Indication (SNI) field from the Client Hello message.

The set of server domain names derived from the SSL handshake is used to match against the Subject/Domain name values specified in a rule, and if one of them matches, the rule will be triggered, and the appropriate policy applied. The server domain name appears in the SSL session log (Section 5.2.3).

The **Subject/Domain Names List** display contains two panels. A **Subject/Domain Names List** called **sslng-unsupported-sites** is configured by default. It contains the domain names of SSL sites, the traffic to which cannot be inspected. Selecting the list in the upper panel causes the set of names in the list to display in the lower **Subject/Domain Names** panel. Figure 5.44 shows the first page of names in the default **sslng-unsupported-sites** list.

List Tools

The Remove and Clone tools will be grayed out unless an entry in the table is selected.

Multipage tools

Add

Delete

Clone

Refresh

> **!** A cut-through rule using the **sslng-unsupported-sites** list should be included in the ruleset used on any in-line segment in order to enable applications using these sites to function normally.

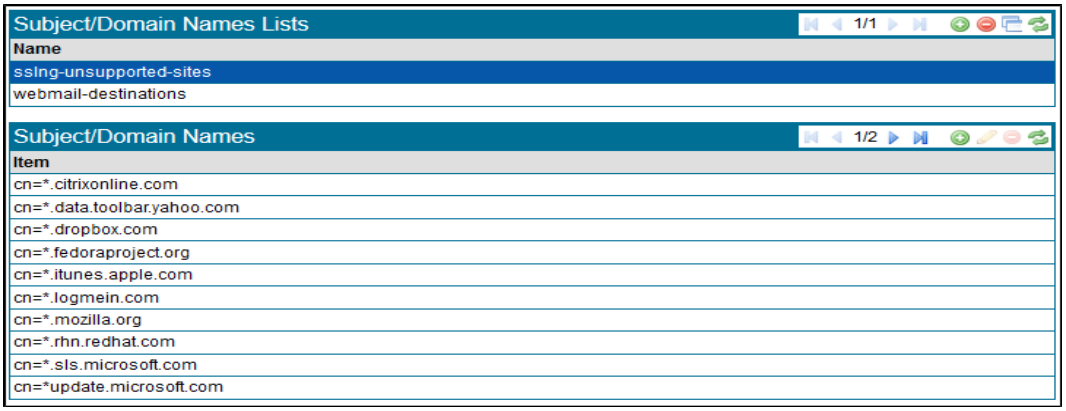


Figure 5.44 Subject/Domain Names list for Unsupported Sites

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Click in the **Subject/Domains Names List** panel to bring up the **Add Subject/Domain Names List.**

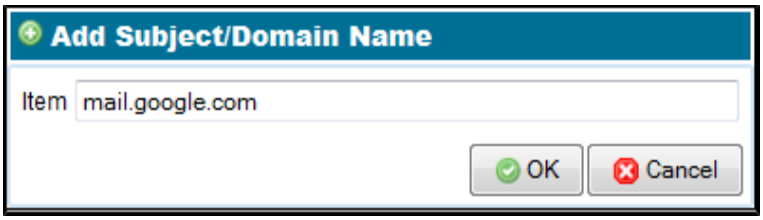


Figure 5.45 Add a Subject/Domain Name to a List

Enter the name of the new list, then press OK.

Domain Names entered here can begin with the "*" character. For example, "*.example.com" will match flows to all example.com subdomains. Subject distinguished name attributes can be entered using CN=, O=, OU=, and C= DN attribute prefixes. The following example shows how a subject DN may be entered using this syntax:

- *cn= www.example.com
- CN=*.example.com, OU=Research, O=Example Company, C=US

The entries are case insensitive. Figure 5.46 shows examples of name entries.

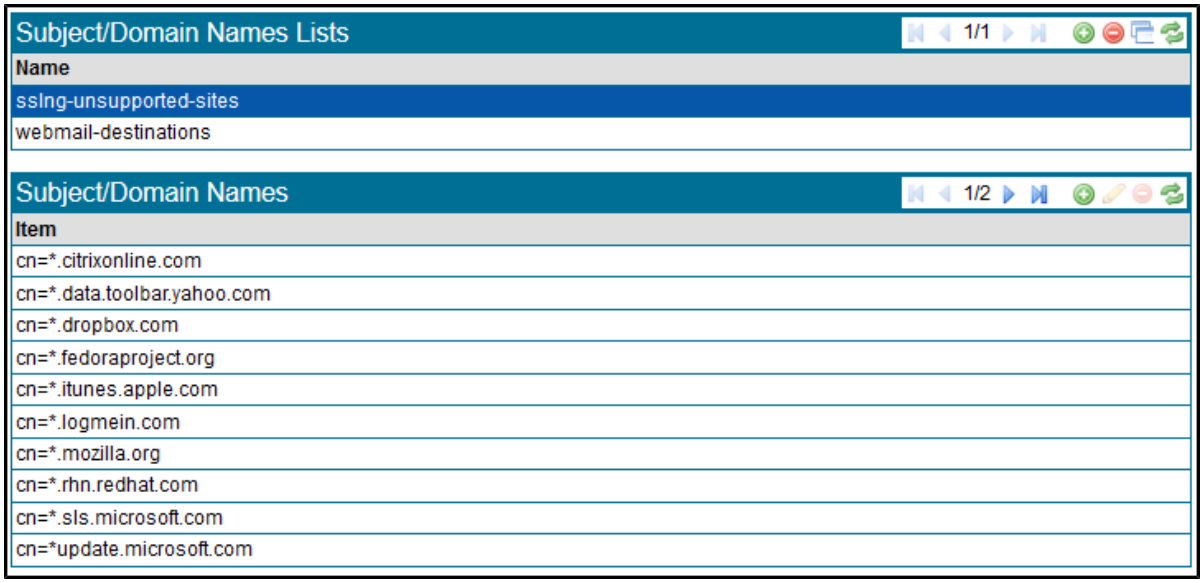


Figure 5.46 Examples of Subject/Domain Names Formats

5.3.4 Domain Names List

Use **Domain Names Lists** to use a list of domain names as a rule match field. **Domain Names Lists** can only contain domain names, and not subject distinguished name attributes. When a domain names list rule match field is used, the Sourcefire SSL appliances deduces the SSL flow domain name and compares it against the domain names in the list."

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Searching of **Domains Names Lists** is optimized so that these lists can contain many thousands of entries. A typical user for **Domains Names List** might be to prevent inspection of traffic to many different sites of a particular type; for example, banking sites. Selecting the list in the upper panel causes the set of names in the list to be displayed in the lower panel.

Maintaining large **Domains Names Lists** using the WebUI is a very manual task. **External tools** that simplify and automate the management of such lists may be available to simplify this task.

Tool icons include the multipage, Add List, Remove List and Clone List tools. The Remove and Clone tools are inaccessible unless an entry in the table is selected.

Figure 5.47 Add a New Domain Name presents the **Domains Names** panels, including how to add a new **Domain Name**.

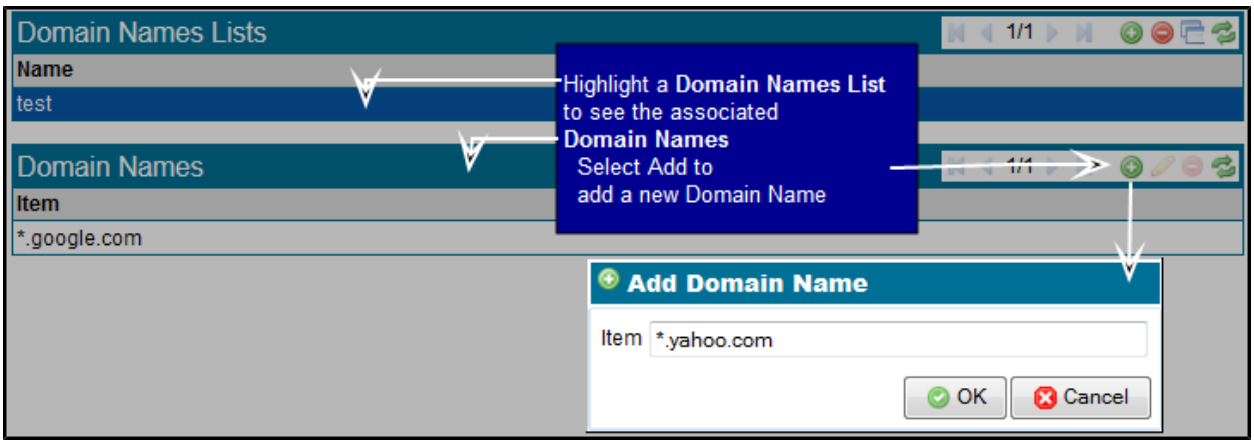


Figure 5.47 Add a New Domain Name

5.3.5 IP Address Lists

The **IP Addresses Lists** window contains two panels. The lower panel content varies depending on the row selected in the upper panel. Each IP Addresses list occupies one row. Searching is optimized so that these lists can contain many thousands of entries.

A typical use for an **IP Addresses Lists** is to prevent inspection of traffic to many different sites of a particular type based on the destination IP address of the hosts.

Tools on this panel let you Add, Remove or Clone a list.

Selecting a list in the upper panel causes the set of addresses in the list to be displayed in the lower panel. IP addresses can be specified in three different formats:

- a.b.c.d: e.g., 192.168.2.10 (netmask of 255.255.255.255 is implied)
- a.b.c.d/x: e.g., 192.168.2.1/24
- a.b.c.d:e.f.g.h: e.g., 192.168.2.1:255.255.255.224

Addresses are validated on input so the system will not allow input of an illegal IP address.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

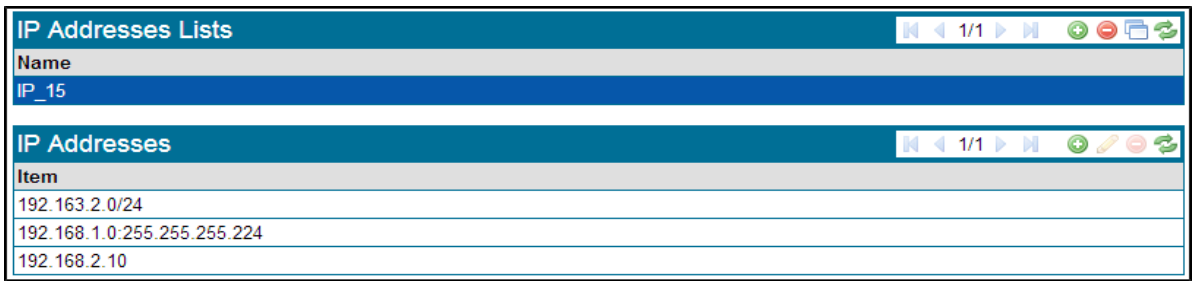


Figure 5.48 IP Address Formats

Figure 5.48 shows the **IP Addresses** panel with three addresses entered, each using one of the three different input formats. Maintaining large **IP Address Lists** using the WebUI is a very manual task. External tools that simplify and automate the management of such lists may be available to simplify this task.

5.3.6 Cipher Suites List

The **Cipher Suites Lists** window contains two panels; the content of the lower panel varies depending on the row selected in the upper panel; selecting a list in the upper panel causes the set of cipher suites in the list to be displayed in the lower panel. Each **Cipher Suites List** occupies one row. Tools allow the addition removal, and cloning of a list.

When adding a cipher suite to a list, a window appears where you can select the additional cipher suite from a drop-down list, or input it as a number in decimal or hex format.

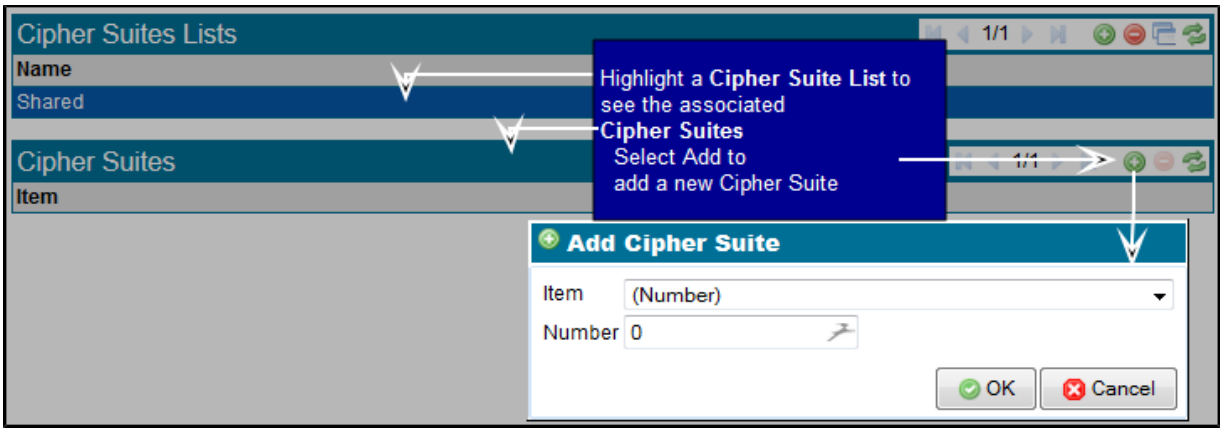


Figure 5.49: Add a Cipher Suite to a Cipher Suites List

Figure 5.49 shows the window used to add a cipher suite and Figure 5.50 shows a list with three entries each using a different input format. The drop-down menu provides a list of all cipher suites using the name format e.g., TLS_RSA_SHA_WITH_AES_CBC_SHA.

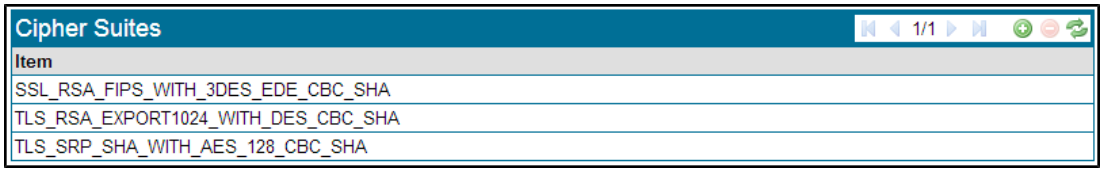


Figure 5.50 Examples of Cipher Suite Formats

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.3.7 Host Categorization Lists

Use this window to view and manage Host Categories. The Sourcefire Host Categorization service allows policy to be tailored to the destination of an SSL flow. With this feature enabled, you can write policy specific to a type of traffic. For example, you could configure a policy to cut-through all traffic to financial services sites.

The Sourcefire SSL appliance matches categories found in SSL flows and applies the policy. The updated database downloads periodically. The currently configured settings appear on initial view.

Note: The Sourcefire Host Categorization service requires a valid license. See Section 5.5.8.

The Host Categorization service uses a database that must be downloaded from Blue Coat. Proper credentials are required to download the database.

Use the **Host Categorization Status** area to get a snapshot of the current state of your Host Categorization database, with information such whether a download is in progress, and the state of the license.

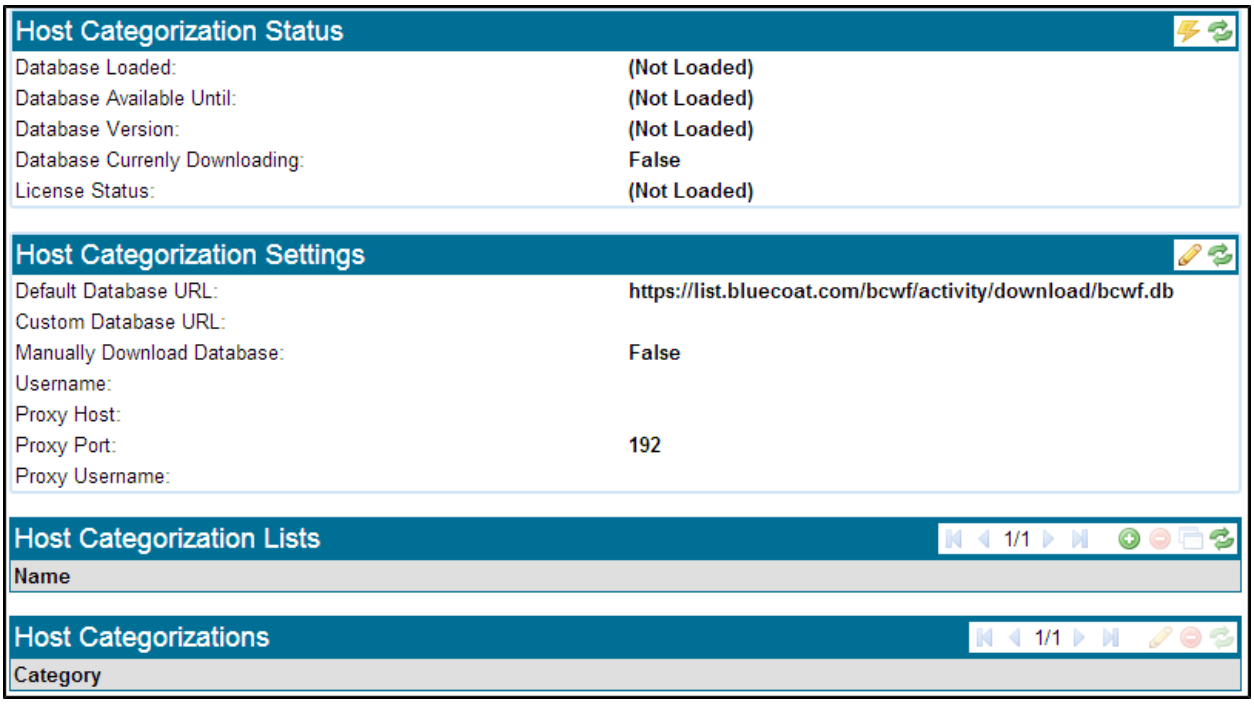


Figure 5.51 Host Categorizations

Download the Host Categorization Database

The Sourcefire **Host Categorization** service uses a database that must be downloaded from Blue Coat. The database is approximately 500 Mb in size and may take several minutes to download; it may temporarily use about 1G of space as it initializes. Use the **Host**

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Categorization Status panel to view and manage the database, and the **Host Categorization Settings** panel to view and manage the connection settings.

The first time you use the **Host Categorization List**, you must first download the Host Categorization database (license is required; Section *4.3.4*). When you update the download settings, the download begins automatically. If you have selected **Manually Download Database**, press ⚡ to start the download. You will see a confirmation message.

A **Database Currently Downloading: True** status message will appear in the **Status** window. Once installed, the database automatically updates every five minutes for the default URL (two hours if other), unless you have selected **Manually Download Database**.

Database Download Tips

- Press ⚡ only once.
- Refresh the window to see if the download has completed; the **Database Loaded** setting will indicate the download date, and the **Database Currently Downloading** status will read False.
- Press Apply to confirm your changes.
- Check the **System Log** (Section 5.2.2) for warning messages.

To change the settings, press ✎ in the far right of the **Host Categorization Settings** title bar. The **Edit Host Categorization Settings** window appears.

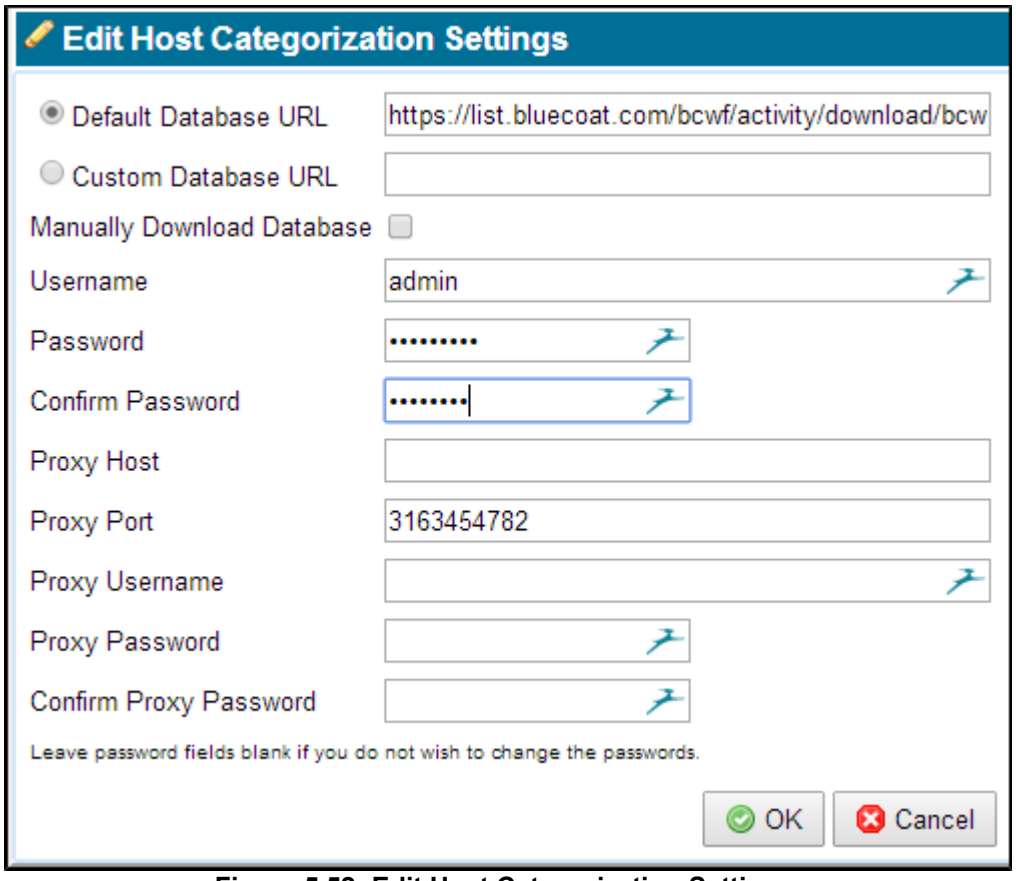


Figure 5.52: Edit Host Categorization Settings

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Tools

- Download the Host Categorization database
- Edit the Host Categorization settings
- Refresh the settings

Usually, you will select the **Default Database URL** to use the Blue Coat supplied path to the categories database, and let it update automatically. After entering the **Username** and **Password** to download the database the first time, you don't need to enter that data again, unless you are changing the values. These settings apply to the download site **not** the Sourcefire SSL appliance.

Using the Host Categorization Lists

Maintain or view your categorization lists in this panel. See Figure 5.51.

Tools

- Add a new list.
- Delete the highlighted list.
- Edit the Host Categorization Settings
- Clone the highlighted list
- Refresh the lists

The categories database (located at *https://list.bluecoat.com/bcwf/activity/download/bcwf.db*) may be downloaded securely through the Sourcefire SSL appliance, downloaded to a local web server and applied from there, or downloaded through a proxy. To use a proxy, set the proxy host and port. If required, also set the proxy username and password.

Create a New Host Categorization List

1. Click .
2. Enter the list **Name** on the **Host Categorization List** pop up.
3. Select OK.

To see what categories are included in a **Host Categorization List**, highlight the list name. The corresponding categories appear under **Host Categorizations**.

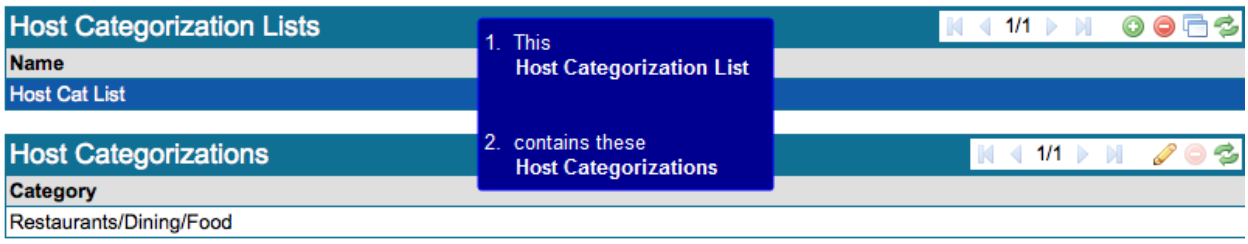


Figure 5.53 Host List with its Categorizations

Add Categories to a List

1. Highlight the row of the **Host Categorization List** you want to edit.
2. Under **Host Categorizations**, press . The **Change Selected Categories** window opens, as shown in the next figure.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

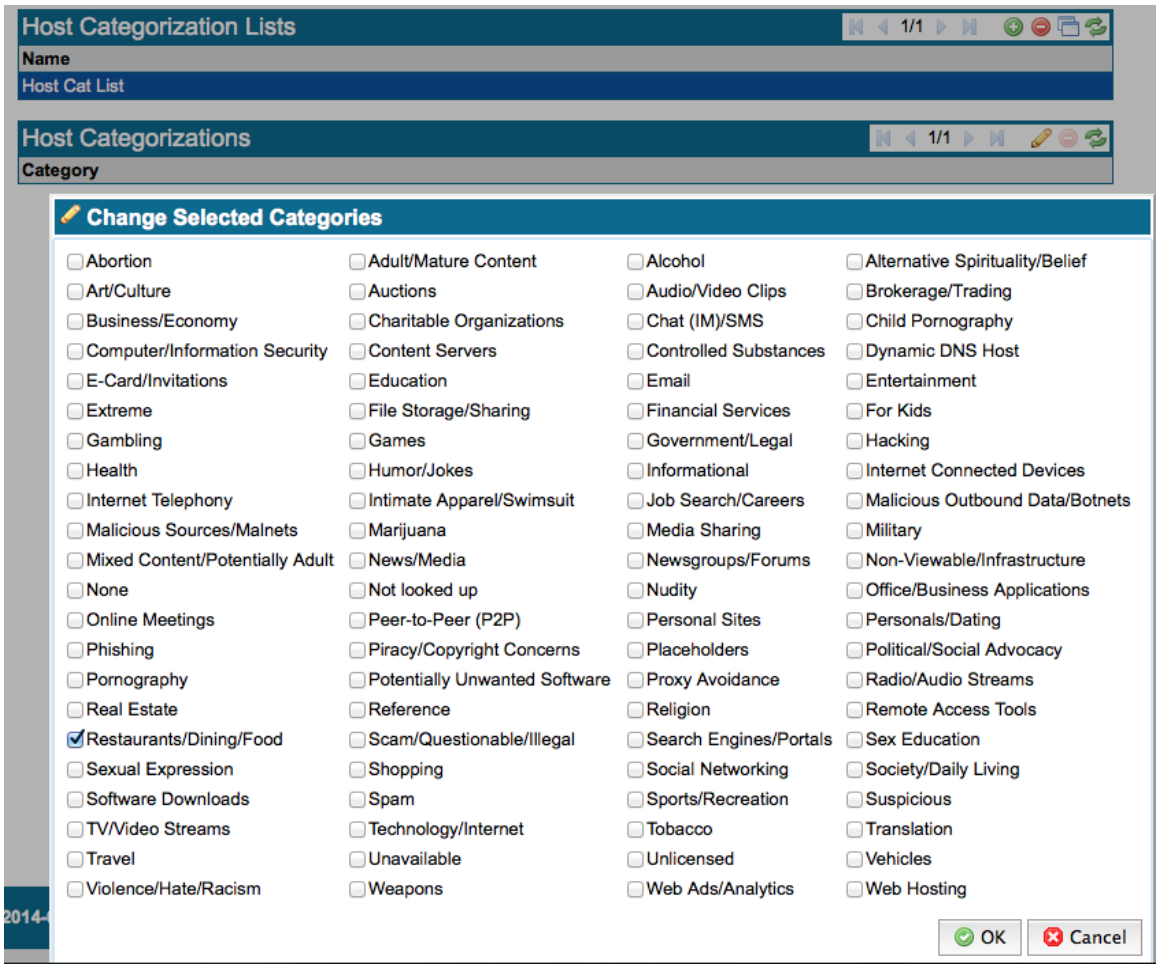


Figure 5.54: Edit Host Categories

3. Select the required categories.
4. Press OK.

Note: The categories displayed, as in Figure 5.54, may change, depending on the database.

Delete Categories from a List

Highlight the category under **Host Categorizations**, and press Delete. Alternately, deselect the category in the **Change Selected Categories** window.

Examples of Category Usage in Policy

Use rules in your policy (see Section 5.3) ruleset (see Section 5.3.1) to match SSL flows to host categories.

- Create a rule which will cut-through traffic that matches the selected category list, and decrypts everything else.
- Create a rule where only traffic matching the list will be decrypted (everything else is cut-through).

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Changing Category Names

Category names may be removed, added, or changed when the database is updated, which can affect policy. Category renames are processed automatically, and a system log is generated if the rename results in a change in policy. Removed categories will be highlighted in red in the policy. A flow cannot match a removed category name.

System Log Data

The following Host Categorization licenses warnings and errors are reported in the **System Log** (Section 5.2.2).

- An INFO message when the version of the database changes.
- WARNING message will be made 15, 5, 4, 3, 2, and 1 days before the database becomes stale.
- An ERROR message when the database becomes stale.
- A WARNING message will be made 30, 15, and 5 days before the Host Categorizations license expires.
- A WARNING level system log entry will be made every day during the last 5 days before the license expires.
- An ERROR level system log entry when the license expires.
- If the database becomes stale, the flow will be categorized as "Unavailable."
- A valid Sourcefire Host Categorization component license will be required to categorize flows. Without a license, flows will be categorized as "Unlicensed."

Session Log Data

The **Session Logs** (Section 5.2.3) include Host Categories information:

- The first specific Host Category matched by a flow (hence triggering a ruleset); only one category is included in the log, even if the flow matched multiple categories, and more than one category triggers the rule.
- The SNI for a session; this will help in troubleshooting Host Categorization issues, as you will be able to identify the site the user was trying to visit.

No Host Categorization information is included in the **Session Log** if no rule is matched. The **Session Logs** data can be exported for off-box analysis.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.4 PKI Management

The **PKI** menu contains six options that allow management of certificates and keys and the creation of lists of certificates and keys. Each of the menu options is described below.

> **!** A user must have the Manage PKI role in order to make changes to the certificates and keys on the system. Users without the Manage PKI role will find that some features of the PKI menu will not be available to them.

Figure 5.55 shows the PKI menus options.

Figure 5.55 PKI Menu

5.4.1 Internal Certificate Authorities

The **Internal Certificate Authorities** lets you create, import, export and manage Certificate Authorities

Tools

	Multipage tools		
	Generate certificate		Add certificate
	Install certificate		Delete certificate
	Export certificate ,		Edit
	View certificate details		Refresh.

Section 4.4 describes the different ways an Internal CA can be added to the system. Multiple internal Certificate Authorities can be configured and stored in the system. The choice of which internal CA is used to resign a server certificate when an SSL session is being decrypted using certificate resign is controlled by either the segment, ruleset or rule definition. Which internal CA is used can be configured to depend on details of the server certificate for the session being inspected allowing different internal CAs to be used for traffic going to different servers over the same segment.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.4.2 External Certificate Authorities

The **External Certificate Authorities Lists** display contains two panels with the lower panel displaying information that varies depending on the row selected in the upper panel. Each External Certificate Authorities list occupies one row in the **External Certificate Authorities Lists** panel. Tools on this panel let you Add , Remove or Clone a list. Selecting a list in the upper panel causes the set of **External Certificate Authorities** certificates in the list to be displayed in the lower panel.

The system has a default list installed, the **all-external-certificate-authorities** list. This contains the set of publicly-trusted CA certificates that are distributed with Internet Explorer and Firefox browsers. Selecting this list in the upper panel will cause the lower External Certificate Authorities panel to display details of the CA certificates in the list.

External Certificate Authorities Tools

Use to add CA certificates to the list, or to delete existing CA certificates.

Multipage tools

View certificate details ,

Add certificate ,

Delete certificate

Refresh

Use the Add button on the **External Certificate Authorities Lists** panel to create and add a custom list. Select the new list, then copy CA certificates from the **all-external-certificate-authorities** list to the new custom list.

The custom list is always a subset of the **all-external-certificate-authorities** list, and cannot contain entries that are not present in the **all-external-certificate-authorities** list. When a custom list is selected and the Add button in the lower panel is pressed, a dialog box appears allowing keys in the default list to be added to the custom list.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.56 shows an example where two CA certificates from the **all-external-certificate-authorities** list have been added to a custom list called "private". One of the entries that has been included in the private list is a private CA certificate that had previously been imported to the **all-external-certificate-authorities** list. The clone feature on the **External Certificate Authorities Lists** panel can be used to clone an existing list and save it with a new name. It is often quicker to clone an existing custom list and then add or remove certificates to the new version produced by the clone tool.

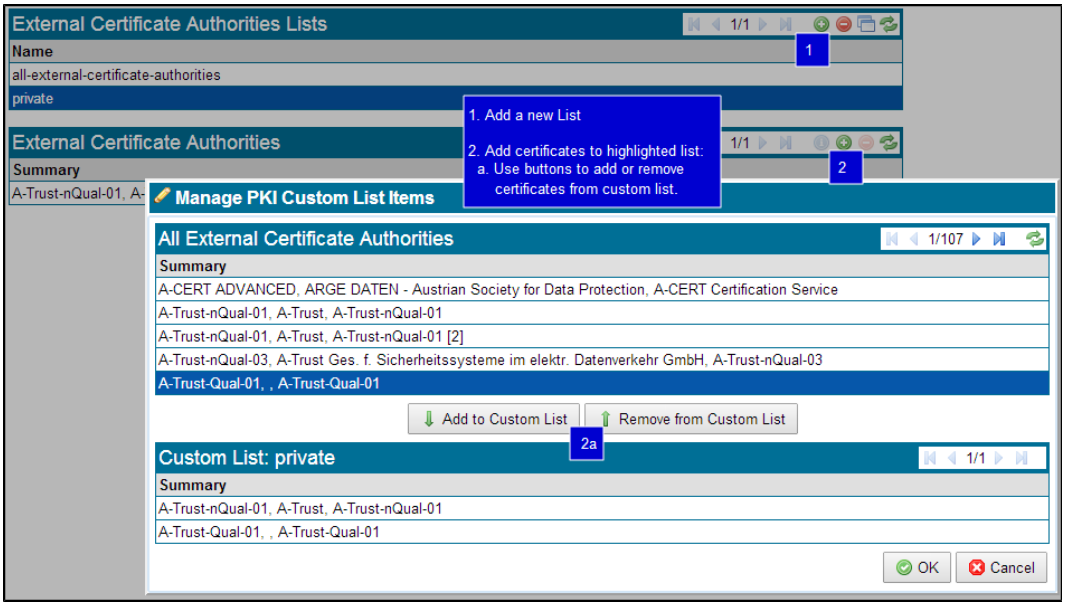


Figure 5.56 Creating a Custom External Certificate Authorities List

Figure 5.57 Clone a List

5.4.3 Certificate Revocation Lists

The **Certificate Revocation Lists** display contains two panels. The content of the lower panel pertains to the row selected in the upper panel. Selecting a list in the upper panel causes the set of CRLs in the list to be displayed in the lower panel.

Each **Certificate Revocation List** occupies one row in the **List of Certificate Revocation Lists** panel. Tools on this panel let you Add, Remove or Clone a list.

The system has a default list installed, the **all-certificate-revocation-lists** list. This list is initially empty. Selecting this list in the upper panel will cause the lower **Certificate Revocation Lists** panel to display details of the CRLs in the list. Selecting this list and then clicking on the Add button in the lower **Certificate Revocation List** panel will open up a window where you can import a CRL.

The **Certificate Revocation List** panel has these tools: multipage icon, view CRL details,

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

add CRL , delete CRL and Refresh ( ). This allows CRLs to be added to the list or existing CRLs in the system to be deleted. Figure 5.58 shows the import CRL dialog box. If the CRL file being imported is encrypted and protected with a password then the password will need to be entered in the Password field on the box.

The Add button on the **List of Certificate Revocation Lists** panel can be used to create and add a custom list. Once this list is created it can be selected and then CRLs from the "all-certificate-revocation-lists" list can be copied to the custom list. The custom list is always a subset of the "all-certificate-revocation-lists" list and cannot contain entries that are not present in the "all-certificate-revocation-lists" list. When a custom list is selected and the add button in the lower panel is pressed a dialog box appears allowing keys in the default list to be added to the custom list.

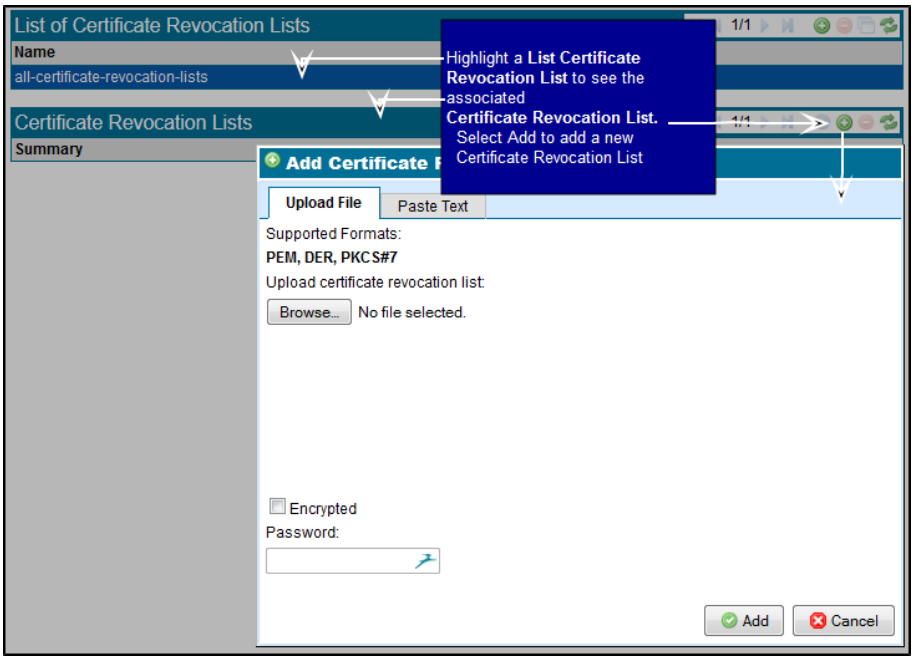


Figure 5.58 Import CRL

Use the clone feature on the **List of Certificate Revocation Lists** panel to clone an existing list and save it with a new name. It is often quicker to clone an existing custom list and then add or remove CRLs to the new version produced by the clone tool.

5.4.4 Trusted Certificates

The **Trusted Certificates** display contains two panels. The content of the lower panel pertains to the row selected in the upper panel. Selecting a list in the upper panel causes the set of certificates in the list to be displayed in the lower panel. Each **Trusted Certificates List** occupies one row in the **Trusted Certificates Lists** panel.

The system has a default list installed, the **all-trusted-certificates** list. This list is initially empty. Selecting this list in the upper panel will cause the lower **Trusted Certificates** panel to display details of the certificates in the list. Selecting this list and then clicking on the

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

add button in the lower **Trusted Certificates** panel will open up a dialog box that lets you import a certificate.

Tools

Manage your certificates.

Multipage tools

Add

Delete

Clone

Refresh

Use the Add button on the **Trusted Certificates Lists** panel to create and add a custom list. Once this list is created, select it, and then copy certificates from the **all-trusted-certificates** list to the custom list as required.

The custom list is always a subset of the **all-trusted-certificates** list, and cannot contain entries that are not present in the **all-trusted-certificates** list. When a custom list is selected and you press the Add button in the lower panel, a dialog box appears where you can add keys in the default list to the custom list.

The clone feature on the **Trusted Certificates Lists** panel can be used to clone an existing list and save it with a new name. It is often quicker to clone an existing custom list and then add or remove certificates to the new version produced by the clone tool.

5.4.5 Known Certificates and Keys

The **Known Certificates and Keys** window contains two panels. Selecting a list in the upper panel causes the set of certificates with keys in the list to be displayed in the lower panel. Each **Known Certificates and Keys List** occupies one row in the **Known Certificates and Keys Lists** panel.

Tools

Manage your certificates with keys.

Multipage tools

Add

Delete

Clone

Refresh

Tip: It is often quicker to clone an existing custom list and then add or remove certificates to the new version produced (saved and renamed) by the clone tool.

The system has a default list installed, the "all-known-certificates-with-keys" list. This list is initially empty. Selecting this list in the upper panel will cause the lower **Known Certificates and Keys** panel to display details of the certificates with keys in the list.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Add a New Certificate with Key

1. Click in the **Known Certificates and Keys** panel. The **Add Known Certificate with Key** window appears.
2. Install the certificate and key by one of these methods, after entering any required **Password** and selecting **Encrypted** if necessary:
   - On the **Upload File** tab, press **Choose File** at both the **Upload Certificate** and **Upload key** areas to browse to the license file location (.xxx) and select it, then press Add at the bottom of the window. OR
   - On the **Paste Text** tab, paste in previously-copied text of the certificate and the key into the respective fields, then press Add.

Create or Manage a Custom Certificate with Keys List

The custom list is always a subset of the "all-known-certificates-with-keys" list and cannot contain entries that are not present in the "all-known-certificates-with-keys" list.

1. Highlight a custom list in the **Known Certificates and Keys List** panel.
2. Click in the **Known Certificates with Keys** panel. The **Manage PKI Custom List Items** window appears.
3. Use the **Add to Custom List** and the **Remove from Custom List** buttons to copy a known certificate with key to, or remove it from, your custom list.

5.5 Platform Management

The **Platform Management** menu, to the right in the menu bar, and titled with the current hostname of the Sourcefire SSL appliance, contains a number of options, described in the following sections. This menu includes tools for viewing and managing the platform, and for configuring and managing access to the platform network management features. Platform management also includes managing user accounts and performing updates to the system software.

Figure 5.59 shows the items found on the platform menu.

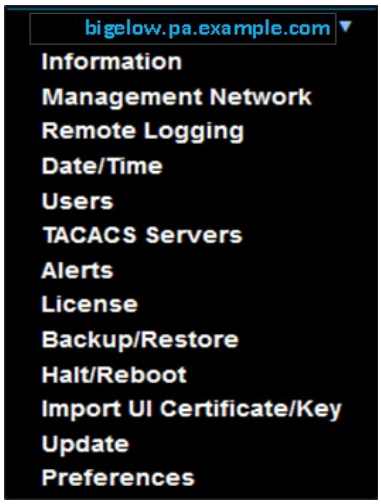


Figure 5.59 Platform Management Menu

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.5.1 Information

The **Information** window initially shows two panels, and a button to access additional information. The two panels have refresh tools for providing visibility of data, but no ability to enter or change data.

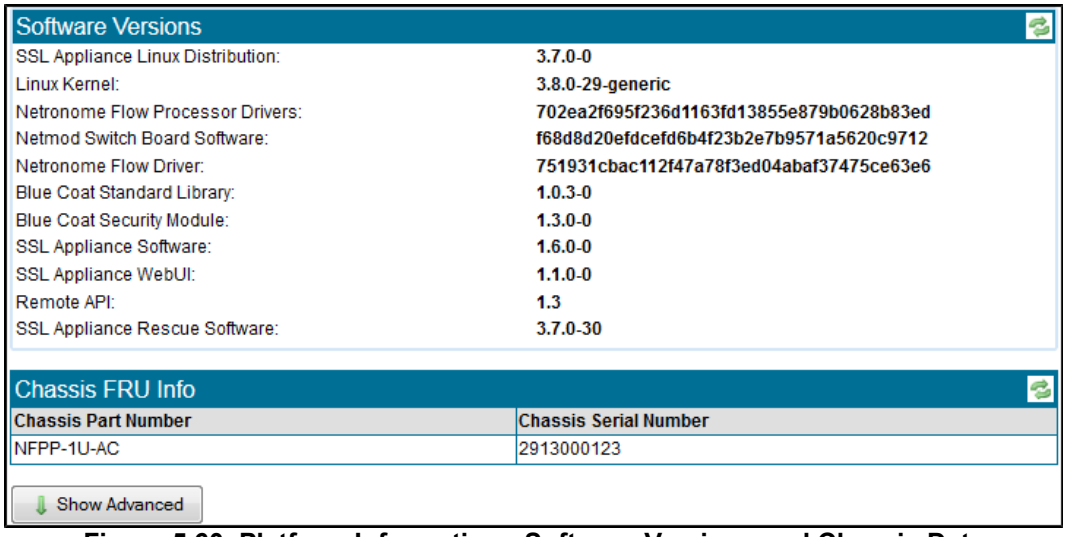


Figure 5.60 Platform Information - Software Versions and Chassis Data

In Figure 5.60, you can see the upper **Software Versions** panel which provides details of the software versions of the various software modules within the system. The **SSL Appliance Linux Distribution** value, in this example 3.7.0-0, is the most important element here as this is the version number of the software release that is running on the system. Sourcefire personnel may request the details from this panel when providing support for the device. Providing these details when filing a support ticket is useful.

Figure 5.60 also presents the **Chassis FRU Info** panel. Sourcefire personnel may request the details from this panel when providing support for the device. Providing these details when filing a support ticket is useful.

If the Show Advanced button is pressed, an additional set of panels will appear. All the additional panels are display only. These panels provide data on different hardware elements of the system. Sourcefire personnel may request the details from these panels when providing support for the device. Panels provide details for the following hardware components of the system:

- **Midplane VPD Info**: midplane that connects Netmods to switch and switch to NFE card
- **Switch Board VPD info**: switch that plugs into midplane
- **Netmod VPD Info**: details on the Netmods plugged in to the system
- **CPU Info**: details on the CPUs installed on the system motherboard
- **NFE VPD** Info: details on the NFE card(s) installed in the system
- **BIOS and BMC Version**: BIOS details

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.5.2 Management Network

The **Management Network** screen has a single panel that allows configuration of the management network settings. The panel has Edit and Refresh tools.

The system can be configured to use either a fixed IP address or to acquire an IP address using DHCP. In order for DHCP to work there must be a working DHCP server on the network that the management Ethernet is connected to.

Figure 5.61 shows the panel containing data for a system that is configured to use DHCP addressing, with the default **Hostname** of localhost, and the **Edit** window used to adjust the network settings. If the DHCP check box is ticked, the **IP Address, Netmask** and **Default Gateway** fields will be grayed out. Section 4.3.2 includes more details on configuring the management network settings.

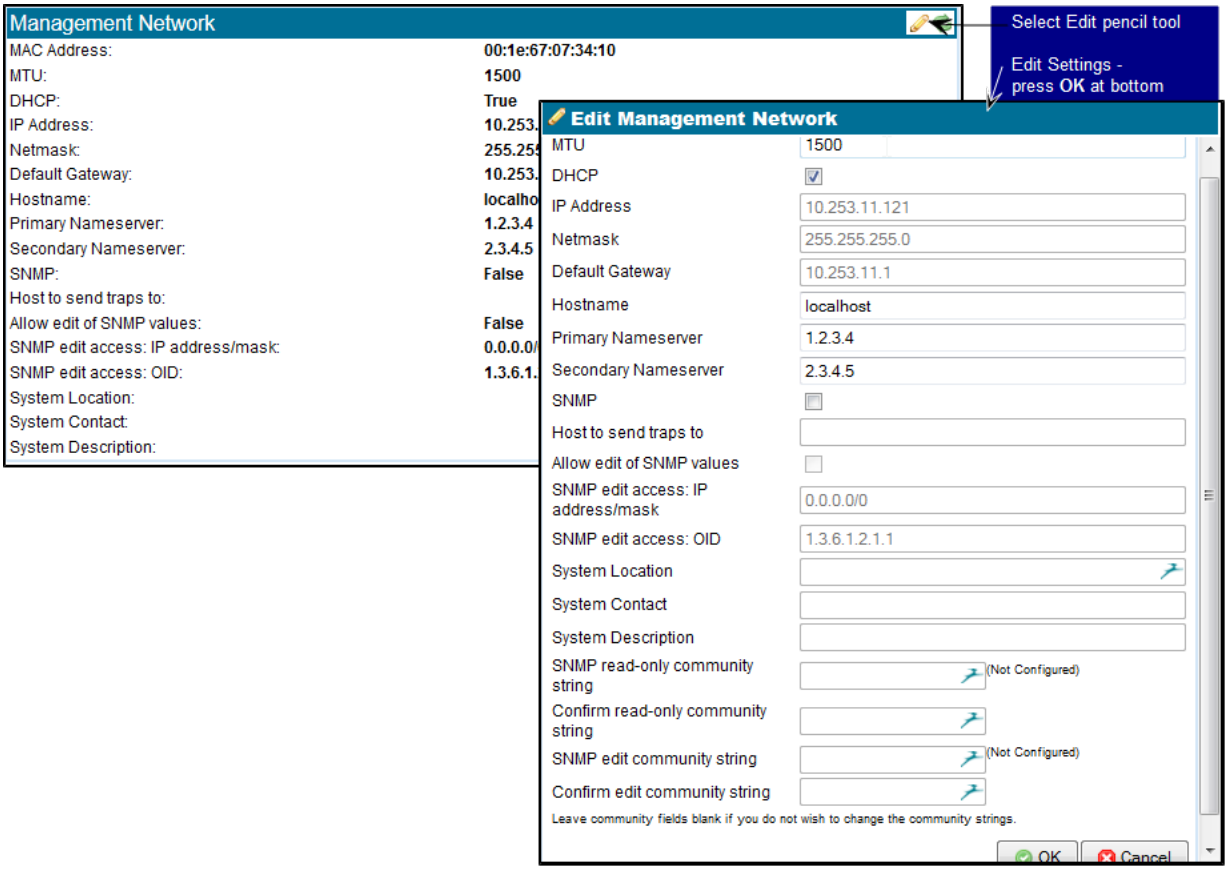


Figure 5.61 Management Network Panel with Edit Settings

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.5.3 Remote Logging

Use **Remote Logging** to send appliance system log and/or session log data to remote syslog servers. This is useful in many distributed corporate environments. Edit and enable a server in the **Remote Logging** panel, as shown in Figure 5.62. Up to eight remote syslog servers can be configured.

Note: Make sure the segment's **Session Log Mode** option is set to **All Sessions to Remote Syslog** or **Errors to Remote Syslog** if you want to send session log data for remote logging.

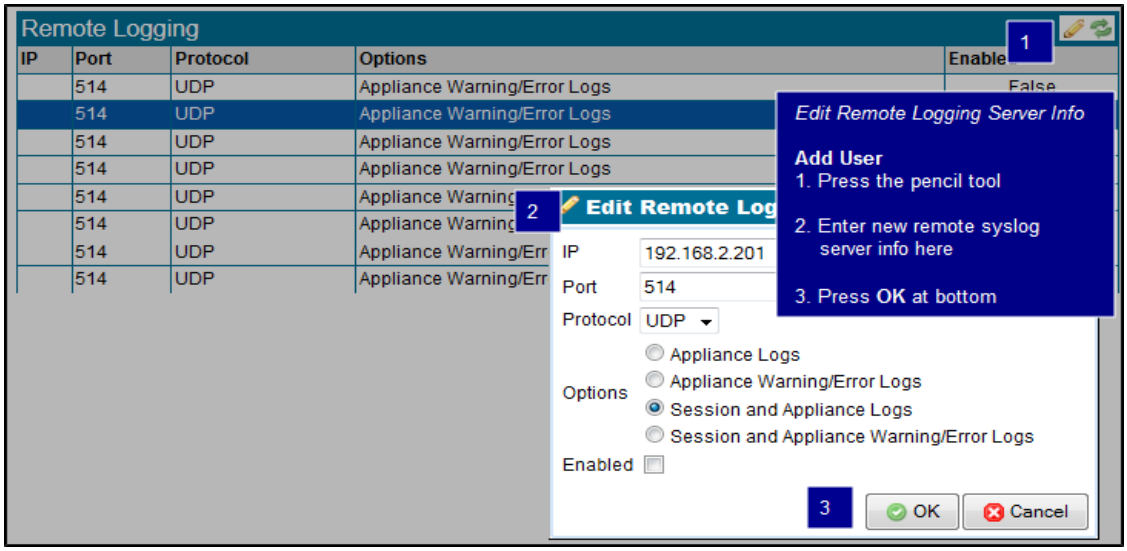


Figure 5.62 Editing Remote Logging Settings

Choosing to send **Session and Appliance Logs** may result in significant traffic to the remote syslog server.

5.5.4 Date/Time

The **Date/Time** screen has a single panel that allows configuration of the system time and date settings. The panel has Edit and Refresh tools. In addition to setting the time and date, you can configure the time zone and whether NTP is used to synchronize the system to a network time server.

Figure 5.63 shows the panel for a system that is configured to use NTP and is located in the UK timezone. Clicking on the edit tool will open up a dialog box that allows the settings to be changed. The system requires a reboot after changes are made to the date and time of day settings. More details on setting the date and time can be found in Section 4.3.1.

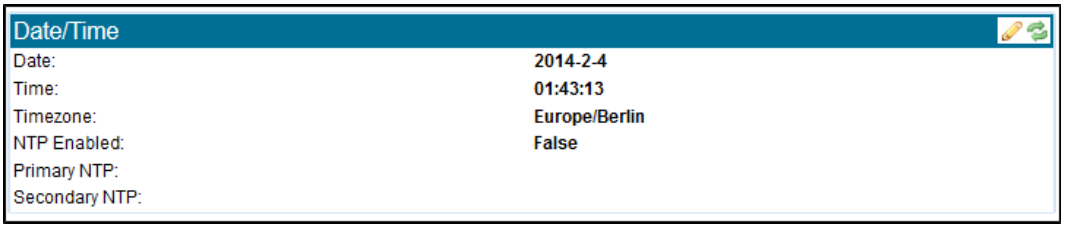


Figure 5.63 Date/Time Panel

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.5.5 Users

The **Users** menu has a single panel with tool icons for multipage, add, edit, delete and refresh. Only users with Manage Appliance or Manage PKI roles can make changes to the user accounts on the system.

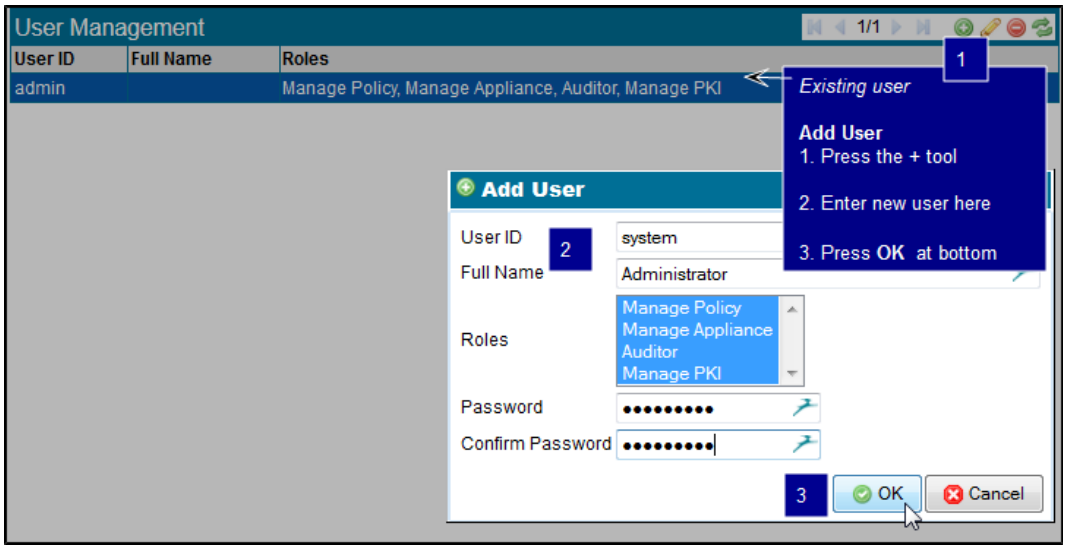


Figure 5.64 Managing User Accounts

Figure 5.64 show the **User Management** panel for a system that has three user accounts configured; each account has a different set of roles associated with it. More details on creating user accounts and on the meaning of different roles can be found in Section 4.3.3.

5.5.6 TACACS Servers

A Cisco ACS system using TACACS+ can be used to remotely authenticate access to the Sourcefire SSL appliance management WebUI. This menu option allows the system to be configured to use TACACS+ to communicate with a Cisco ACS.

Figure 5.65 shows the **TACACS Servers** panel with an entry; initially the table will be empty. Use the button to create an entry.

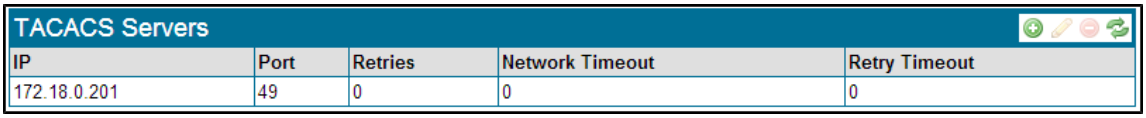


Figure 5.65 TACACS Servers Panel

Enter the required information as shown in Figure 5.67. The **Secret** value needs to match the secret value configured on the ACS server. If TACACS is in use, the login pop up on the WebUI includes a drop-down menu where you can choose if you want to be authenticated remotely or locally as shown in Figure 5.66.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.66 WebUI Login when TACACS is Used

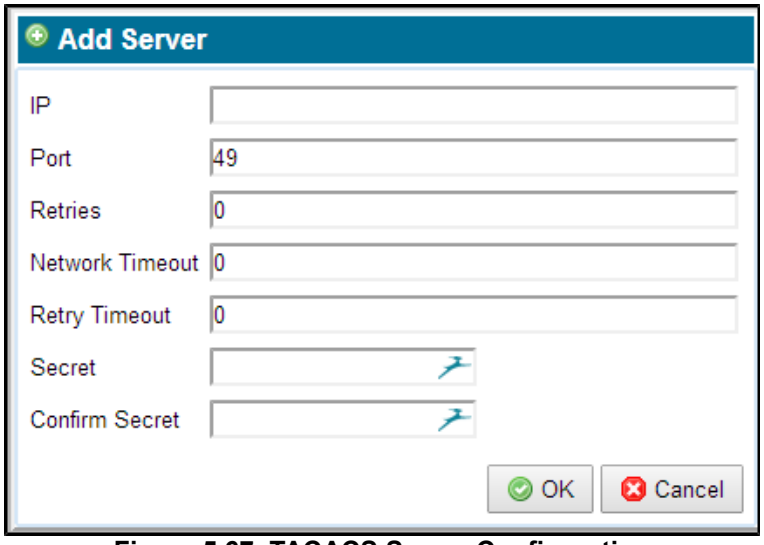


Figure 5.67 TACACS Server Configuration

TACACS Administrator Privilege Mapping

The Cisco ACS lets a privilege level be stored as part of a user's profile. When the user is authenticated, the privilege level of the profile is communicated across TACACS to the Sourcefire SSL appliance. As the appliance does not use privilege levels to control what an authenticated user can do, the privilege level is mapped to the roles supported by the Sourcefire SSL appliance, as laid out in the next table.

TACACS Level	Sourcefire SSL appliance Role
0	auditor
1	auditor + manage-appliance
2	auditor + manage-policy

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

3	auditor + manage-appliance + manage-policy
4	auditor + pki
5	auditor + manage-appliance + manage-pki
6	auditor + manage-policy + manage-pki
7	auditor + manage-appliance + manage-policy _ manage-pki
>8	invalid

Table 18 TACACS Levels to User Roles

5.5.7 Alerts

The **Alerts** menu contains two panels for configuring the e-mail details that the system will use to send out alerts, the events to be monitored, and the conditions under which an alert is generated.

The upper **Alert Mail Configuration** panel is used to configure details of the e-mail system that is used to send out alerts. Click the Edit tool bring up the **Edit Alert Mail Configuration** window, as shown in Figure 5.68. Enter the data as required:

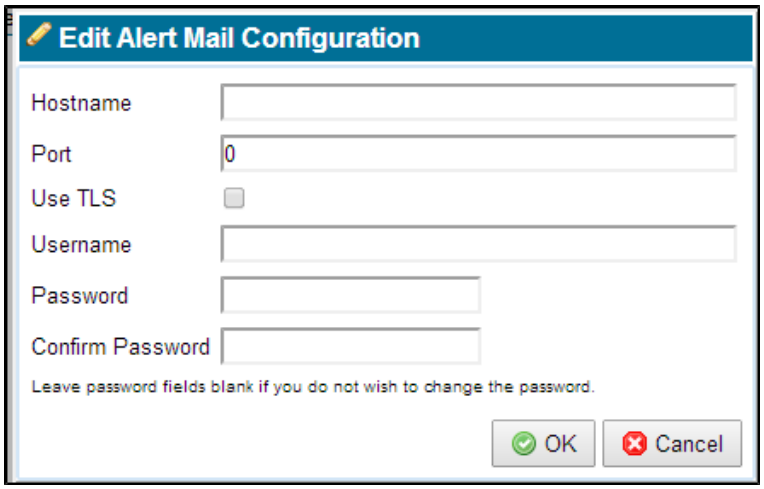


Figure 5.68 E-mail Configuration for Alert System

- **Hostname**: Name or IP address of the SMTP server used to send e-mail
- **Port**: Port number on the SMTP server that is used to send e-mail
- **Use TLS:** Enable/disable the use of encryption (TLS) when sending e-mail
- **Username:** Username of the account being used to send e-mail
- **Password**: Password for the account being used to send e-mail.

! If your enterprise is using Google Apps for e-mail then the correct SMTP Server Address is 'aspmx.l.google.com', not 'smtp.gmail.com'. Ensure that DNS resolution is properly configured. Alerts can only be sent to users on the same domain with this SMTP configuration

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Configure alerts on the lower panel. Each alert can be triggered by a specific set of conditions, and can be sent to one or more e-mail recipients. Click the Add button in the lower panel to open the **Add Rule** window and configure the rule. See Figure 5.69.

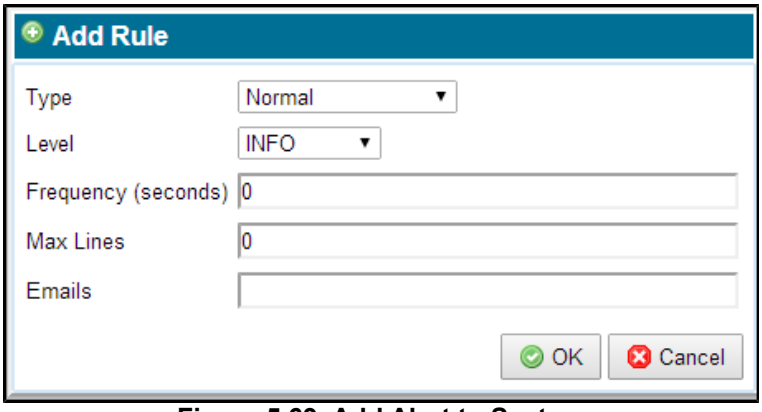


Figure 5.69 Add Alert to System

Type

- Harddrive Full: generated if out of disk space
- Normal: generated if conditions specified in alert are met
- Periodic: generated at regular time intervals
- Unclean Shutdown: generated if last system shutdown was not clean

Level: These levels correspond to levels associated with entries in the system log files. So, if the Level is set to FATAL an alert will be generated when a message with a FATAL level is added to the system log.

- ERROR
- FATAL
- INFO
- WARNING

Frequency (seconds): Control over how frequently the alert message should be sent.

Max Lines: Controls how many lines from the system log are included in the e-mail.

Emails: Specify one or more e-mail addresses; these are the users to whom the alert e-mails will be sent.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.5.8 License

View and update the Host Categorization license(es).

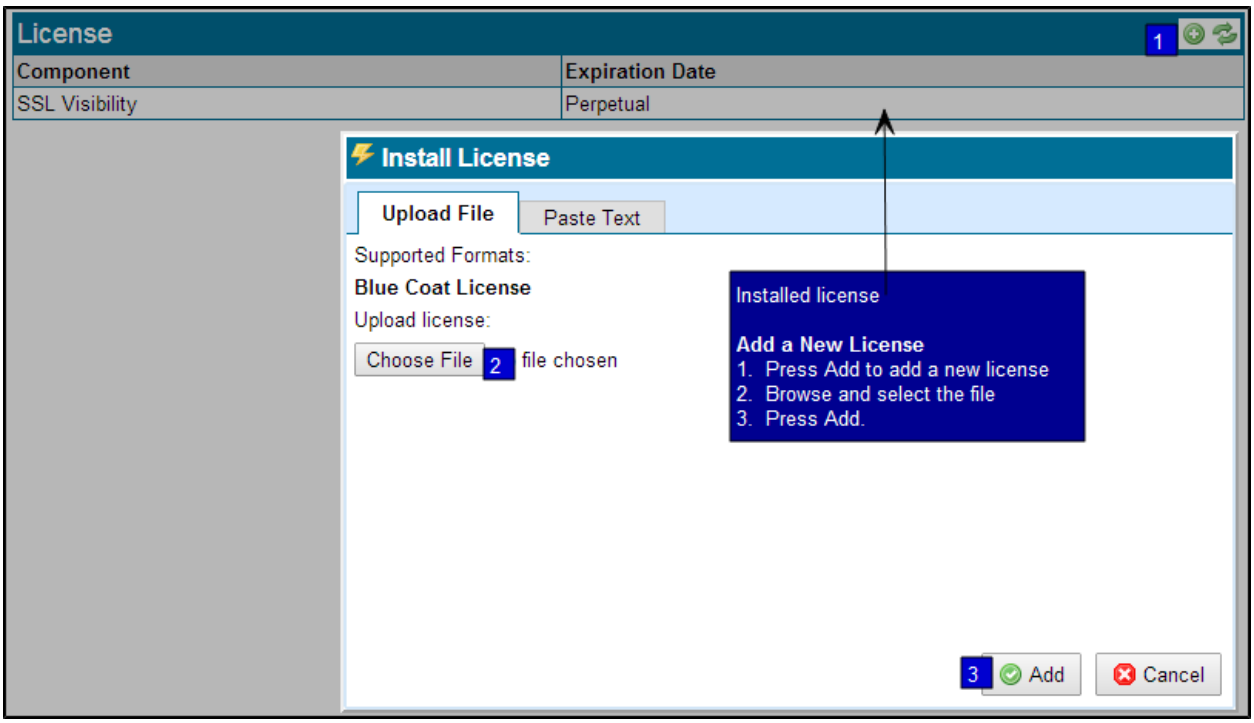


Figure 5.70 Add a New License

See Section 4.3.4 for extended information on using the **License** panel.

Any current, active licenses appear in the **License** panel.

Licensing details are available in the **System Log** (see Section 5.2.2):

- If a valid license is present and not expiring within 90 days, no system log message appears
- If a valid license is present but expiring within 30 to 90 days, an INFO message appears
- If a valid license is expiring within 30 days, a WARNING message appears
- If no valid license is present, or the existing license has expired, an ERROR message appears

License status can also be viewed on the physical LCD screen.

Tip: Configure an e-mail alert (Section 5.5.7) to remind yourself about a pending license expiration.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5.5.9 Backup/Restore

This menu option opens a dialog box which lets you the various elements of the system configuration to be saved to or restored from a remote storage system.

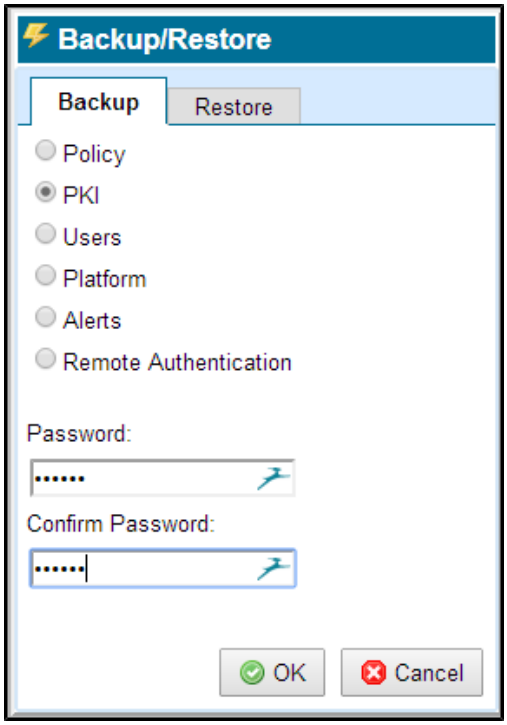


Figure 5.71 Backup

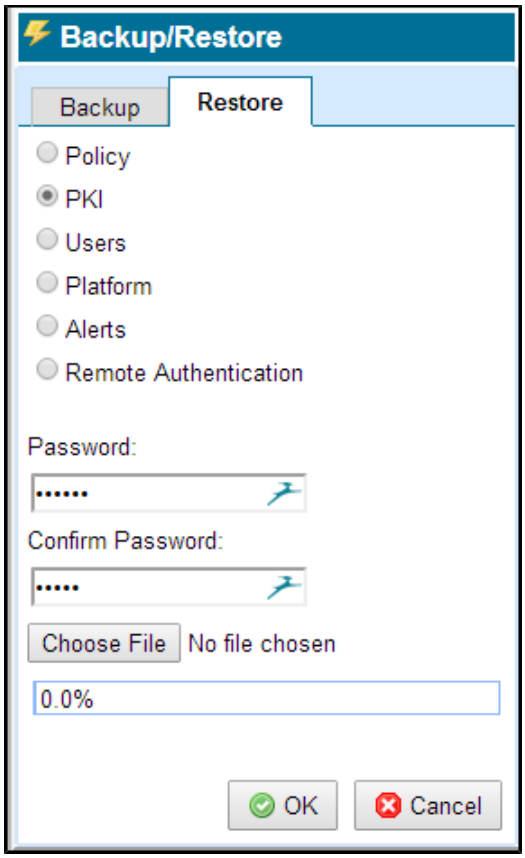


Figure 5.72 Restore

Figure 5.71 shows the **Backup** dialog box and Figure 5.72 shows the **Restore** dialog box. The item to be backed up or restored is indicated by selecting the radio button associated with that item. A password must be provided when backing up data and it is required when restoring the data.

5.5.10 Halt/Reboot

Halt or reboot the system.

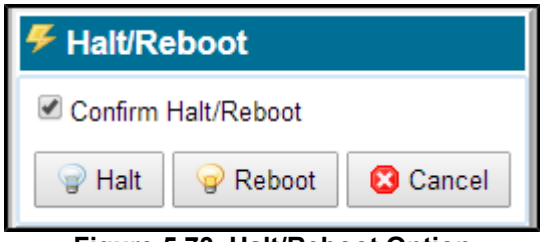


Figure 5.73 Halt/Reboot Option

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.73 shows the dialog box. The **Confirm Halt/Reboot** check box must be checked, the Halt and Reboot buttons are grayed out until this is done.

> **!** If the system is halted, it will require physical presence to power it on from the front panel power switch.

5.5.11 Import UI Certificate/Key

This menu allows a signed SSL server certificate to be imported for use by the web server that provides the WebUI management for the system. By default the system uses a self-signed server certificate which will cause warnings from browsers—see Section 5.1.1 for details.

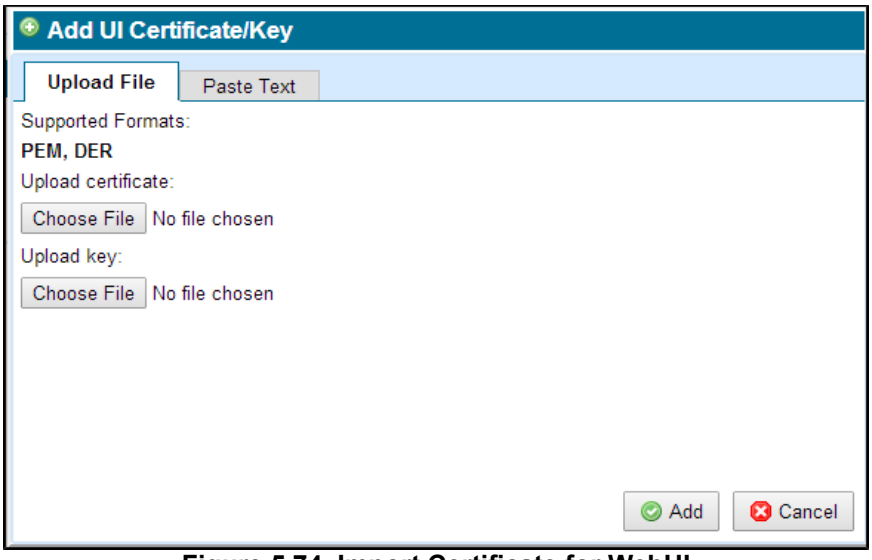


Figure 5.74 Import Certificate for WebUI

Figure 5.74 shows the dialog box used to import a certificate for use by the WebUI.

5.5.12 Update

The **Update** menu is used to load and apply an update file that will update the system software. Update files are digitally signed and are checked before they are applied to the system, an invalid update file will not be applied.

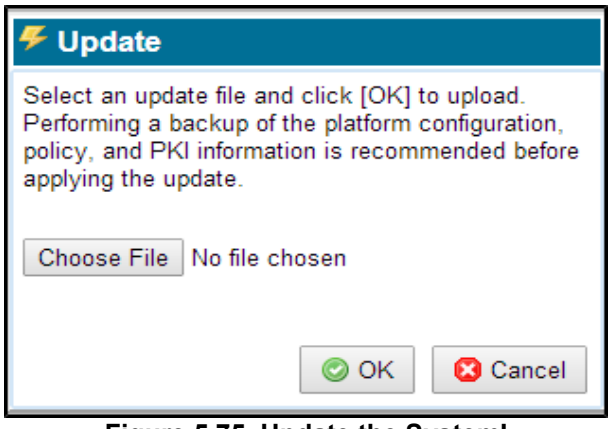


Figure 5.75 Update the Systeml

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 5.75 shows the **Update** dialog box. The Choose File button opens a window that lets the user browse their system and to select the update file that is to be used. Once the OK button is pressed the file is checked and if valid will be copied to the system and then applied.

Note: Once you have upgraded to software version 3.7, the Sourcefire SSL appliance cannot be downgraded without the assistance of customer support.

5.5.13 Preferences

The **Preferences** menu has a single panel where you can configure preferences that affect the UI screen layout.

Figure 5.76 shows the panel with the default values showing for the grid width and number of rows. Clicking on the edit button produces the **Edit UI Preferences** windows, also shown in the figure. Use it to change the values, or to force them back to the system defaults.

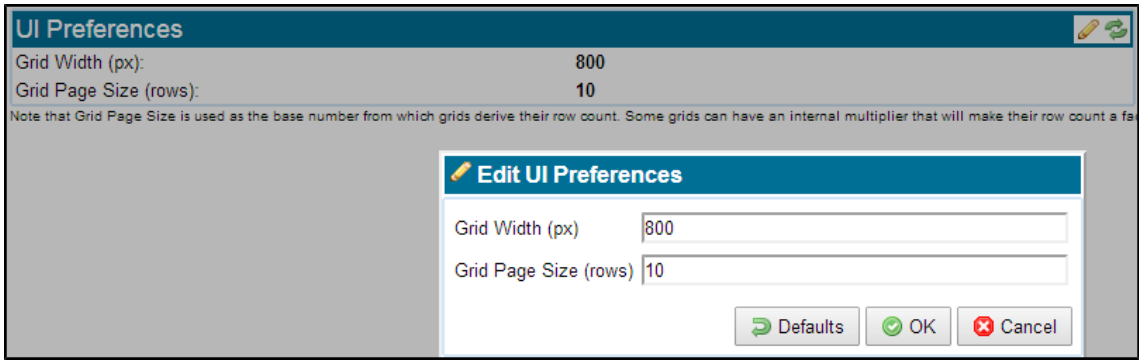


Figure 5.76 WebUI Layout Preferences with Edit Window

Note: Multistage panels have a built in multiplier that is used in conjunction with the number of rows value that is configured as the default. For example, the SSL Statistics panel has a multiplier of 1.6, so with the default row setting of 10 this will mean there are 16 rows displayed in the SSL statistics panel. If the default row count was set to 20 then the SSL Statistics panel would have 32 rows.

5.6 User Management

The User menu, Figure 5.77, lets a user change their password and log out.

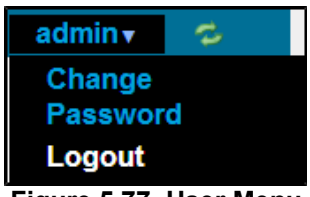


Figure 5.77 User Menu

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

5.6.1 Change Password

Figure 5.78 shows the change password window. Enter your current password, then the new password. Passwords are checked to ensure that they are at least 8 characters long, contain at least one alpha character, at least one numeric character, and at least one upper case alpha character.

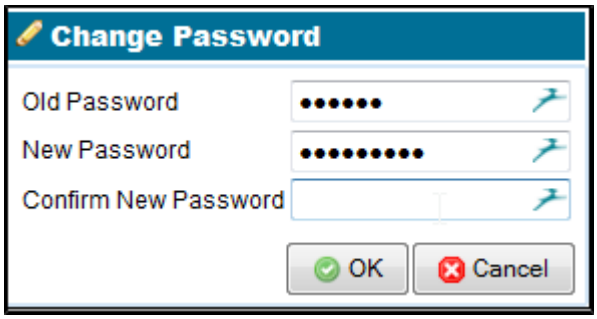


Figure 5.78 Change Password

5.6.2 Logout

Selecting the logout option will log the user off, and then display the login window.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

6. Troubleshooting the System

Note: Please read through all the information in this section of the document before contacting support.

6.1 Supported Network Protocols and Frame Encapsulations

The Sourcefire SSL appliance supports SSL processing on TCP in IPv4 and IPv6. The IP packet must be encapsulated in an Ethernet-II frame, with an optional VLAN tag (802.1Q or 802.1ad).

Network traffic for all other protocols and frame encapsulations are not sent to the SSL processing engine, including the following: Cisco ISL, MPLS, GRE, IP-in-IP, UDP, ICMP, ARP, SOCKS, DTLS, and IPsec.

6.2 Supported SSL/TLS versions

This version of the Sourcefire SSL appliance only supports SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2. There is no support for SSL 2.0. Should SSL 2.0 traffic be encountered, the Sourcefire SSL appliance will either Cut Through or Reject the flow according to the **Undecryptable SSL Handling** parameter in the SSL Inspection Policy. SSL 2.0 ClientHello messages are supported, as long as the rest of the SSL handshake is done using version 3.0 or above (more detail on this compatibility mode can be found in Section E.1 of RFC4346).

6.3 Support for Client Certificates

The Sourcefire SSL appliance supports decrypting SSL sessions with client certificates, but only if the action in the inspection policy is "Decrypt: server key is known" and RSA is used as the key exchange algorithm. The reason for this limitation is that the CertificateVerify SSL handshake message sent after the client certificate is digitally signed by a key only known to the client. The implication is that the CertificateVerify message cannot be modified, which in turn implies that no part of the SSL handshake can be modified.

SSL sessions using client certificates and the RSA key exchange in known server key mode are decrypted as usual. The Sourcefire SSL appliance rejects all other sessions with client certificates, unless they use an unsupported cipher suite (Section 9.6). SSL sessions rejected because of a client certificate appear in the SSL session log with an **Error** event value and **Reject** action.

To prevent sessions with client certificates from being rejected the Inspection Policy must have a rule that will cut through the specific session based on a combination of common name, destination IP/mask, and destination TCP port.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

6.4 Supported Cipher Suites

Table 19 lists all the cipher suites that are supported by the Sourcefire SSL appliance, and shows which can be inspected when in-line and which when in passive-tap mode. Any cipher suites that are not supported will be handled by the policies configured for undecryptable traffic.

Cipher Suite	Inline	Passive-Tap	ID
TLS_NULL_WITH_NULL_NULL	Yes	Yes	0x0000
TLS_RSA_WITH_NULL_MD5	Yes	Yes	0x0001
TLS_RSA_WITH_NULL_SHA	Yes	Yes	0x0002
TLS_RSA_WITH_RC4_128_MD5	Yes	Yes	0x0004
TLS_RSA_WITH_RC4_128_SHA	Yes	Yes	0x0005
TLS_RSA_WITH_DES_CBC_SHA	Yes	Yes	0x0009
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Yes	Yes	0x000A
TLS_DHE_RSA_WITH_DES_CBC_SHA	Yes	No	0x0015
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	Yes	No	0x0016
TLS_DH_Anon_WITH_RC4_128_MD5	Yes	No	0x0018
TLS_DH_Anon_WITH_DES_CBC_SHA	Yes	No	0x001A
TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA	Yes	No	0x001B
TLS_RSA_WITH_AES_128_CBC_SHA	Yes	Yes	0x002F
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Yes	No	0x0033
TLS_DH_Anon_WITH_AES_128_CBC_SHA	Yes	No	0x0034
TLS_RSA_WITH_AES_256_CBC_SHA	Yes	Yes	0x0035
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Yes	No	0x0039
TLS_DH_Anon_WITH_AES_256_CBC_SHA	Yes	No	0x003A
TLS_RSA_WITH_AES_128_CBC_SHA256	Yes	Yes	0x003C
TLS_RSA_WITH_AES_256_CBC_SHA256	Yes	Yes	0x003D
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Yes	Yes	0x0041
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Yes	No	0x0045
TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA	Yes	No	0x0046
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Yes	No	0x0067
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Yes	No	0x006B
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Yes	Yes	0x0084
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Yes	No	0x0088
TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA	Yes	No	0x0089

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Cipher Suite	Inline	Passive-Tap	ID
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	Yes	Yes	0x00BA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	Yes	No	0x00BE
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	Yes	No	0x00BF
TLS_RSA_WITH_AES_128_GCM_SHA256	Yes	Yes	0x009c
TLS_RSA_WITH_AES_256_GCM_SHA384	Yes	Yes	0x009d
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Yes	No	0x009e
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Yes	No	0x009f
TLS_DH_Anon_WITH_AES_128_GCM_	Yes	No	0x00a6
TLS_DH_Anon_WITH_AES_256_GCM_SHA384	Yes	No	0x00a7
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	Yes	Yes	0x00C0
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Yes	No	0x00C4
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	Yes	No	0x00C5
TLS_ECDHE_ECDSA_WITH_NULL_SHA	Yes	No	0xC006
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	Yes	No	0xC007
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Yes	No	0xC008
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Yes	No	0xC009
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Yes	No	0xC00A
TLS_ECDHE_RSA_WITH_NULL_SHA	Yes	No	0xC010
TLS_ECDHE_RSA_WITH_RC4_128_SHA	Yes	No	0xC011
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Yes	No	0xC012
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Yes	No	0xC013
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Yes	No	0xC014
TLS_ECDH_Anon_WITH_NULL_SHA	Yes	No	0xC015
TLS_ECDH_Anon_WITH_RC4_128_SHA	Yes	No	0xC016
TLS_ECDH_Anon_WITH_3DES_EDE_CBC_SHA	Yes	No	0xC017
TLS_ECDH_Anon_WITH_AES_128_CBC_SHA	Yes	No	0xC018
TLS_ECDH_Anon_WITH_AES_256_CBC_SHA	Yes	No	0xC019
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Yes	No	0xC023
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Yes	No	0xC024
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Yes	No	0xC027
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Yes	No	0xC028
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Yes	No	0xc02b
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Yes	No	0xc02c
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Yes	No	0xc02f

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Cipher Suite	Inline	Passive-Tap	ID
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Yes	No	0xc030
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Yes	No	0xcc13
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_	Yes	No	0xcc14
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Yes	No	0xcc15
SSL_RSA_FIPS_WITH_DES_CBC_SHA	Yes	Yes	0xFEFE
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	Yes	Yes	0xFEFF
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	Yes	Yes	0xFFE0
SSL_RSA_FIPS_WITH_DES_CBC_SHA	Yes	Yes	0xFFE1

Table 19 Supported Cipher Suites

There is no support for the outdated export version of the cipher suites. There is no support for static DH (Diffie-Hellman) key exchange, or DSS (Digital Signature Standard) authentication.

Note: When operating in Passive-Tap mode there are some cipher suites that cannot be inspected, e.g. Ephemeral, Elliptic Curve and Anonymous DH key exchanges. When operating in inline modes it is possible to inspect SSL sessions using Ephemeral, Elliptic Curve and Anonymous DH key exchanges.

SSL sessions using unsupported cipher suites appear in the SSL session log with an **Undecryptable** event value. The action taken depends on the **Undecryptable SSL Handling** policy option and is either **Cut through, Drop** or **Reject**.

There are no restrictions on cipher suites for policies with actions that do not involve inspecting the traffic. So, it is fine to have a policy that prevents SSL traffic using static DH from setting up connections across the network for example.

6.5 Support for SSL Record Layer Compression

The SSL specification allows for SSL record layer compression using an algorithm negotiated through the ClientHello and ServerHello handshake messages. The current version of the Sourcefire SSL appliance does not support SSL record layer compression, and all such SSL sessions will be marked as **Undecryptable** in the SSL session log. The action taken on these sessions is determined by the **Undecryptable SSL Handling** policy option.

6.6 Support for Stateless Session Resumption (RFC5077)

The Sourcefire SSL appliance supports stateless session resumption as outlined in RFC5077. Stateless sessions are typically used by content providers that balance high loads between multiple servers. An example of this is Google Mail (www.gmail.com).

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

6.7 Steps to Troubleshoot SSL Decryption

If none of the incoming SSL sessions are decrypted, follow the steps outlined below.

6.7.1 Monitor Network Port Statistics

Verify that network traffic is received on the network ports of the Sourcefire SSL appliance being used by the active segment. The Monitor/Dashboard screen on the WebUI provides the required information in the Segment Status and Network Interfaces panels.

6.7.2 Monitor the SSL Statistics

Verify that SSL sessions reach the SSL processing engine of the Sourcefire SSL appliance. The SSL Statistics option on the Monitor WebUI menu will provide the required information. If you can see the counts for detected SSL session increasing then SSL traffic is being detected by the system.

6.7.3 Monitor the SSL Session Log

Verify that SSL sessions are recorded in the SSL session log, and have the correct status. The SSL Session Log option under the Monitor menu will provide the required information.

First, ensure that the SSL Session Log is enabled for the segment being used. Next, confirm that the SSL sessions appear in the session log: ensure that you are viewing the first page of session log data and press the Refresh button and you should see new entries appear at the top of the page. Appropriate values in the "Action Taken" column confirm that the SSL sessions are being decrypted. The session log indicates which segment and entry is for so you need to know the segment ID that is associated with the segment you are troubleshooting, this can be found on the Policies/Segment screen.

6.7.4 Verify that the Inspection Policy is Set Up Correctly

Verify that the rules specified in the ruleset being used on the segment of interest are set up to inspect the traffic that you are interested in. See Section 5.3.1 for more details.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

6.8 Known Server vs Trusted Server Certificates

The server's private key and certificate must be loaded into the Known Certificates and Keys store before inspecting traffic to that server. Known Server Certificates are implicitly trusted and need not be signed by a CA trusted by the Sourcefire SSL appliance.

Figure 6.1 Certificate Status

Do not install server certificates in the Trusted Certificates store if you have the private key for that server: those certificates belong in the Known Certificates and Keys store.

The Trusted Certificates store is only used to solve specific certificate validation problems, that is, trusting self-signed certificates or trusting certificates for which you don't want to install the CA certificate chain. Refer to Section 5.4.

6.9 Caveats when Enabling/Disabling SSL Inspection

Immediately after you connect a segment to the network or activate inspection, it may not be able to decrypt some SSL flows. Such flows appear in the SSL session log, if activated, with a **Cut through** action and an **Uncached** certificate **Domain Name**, and are handled according to the **Uncached SSL Session Handling** policy option. This happens because the flows are reusing an SSL session established before the Sourcefire SSL appliance was put inline so the Sourcefire SSL appliance did not see the original full handshake and does not have the SSL session state cached.

A SSL session is established using a full SSL handshake, during which the peers negotiate the cryptographic state necessary to encrypt and decrypt traffic. SSL clients, such as web browsers and e-mail clients, cache the cryptographic state and may re-use the session multiple times in later SSL flows. Similarly, the Sourcefire SSL appliance inspects the full handshake, caches the session state, and uses it to inspect flows re-using the same session. If the full handshake occurred before the appliance was put inline, it cannot decrypt flows re-using that session. Most servers allow sessions to be re-used only for a few hours, after which they force clients to establish new sessions. Therefore, the SSL session log may show **Uncached** sessions for a few hours after installing the device on the network or activating inspection. As soon as the client and

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

server establish a new SSL session, the Sourcefire SSL appliance can decrypt that session and all subsequent sessions between the same client and server.

Another caveat is that SSL clients might report SSL session failures if you disconnect the Sourcefire SSL appliance. If an application, for example, .Microsoft Outlook, supports SSL session re-use it will report a failure when it tries to re-use the SSL session. The reason this fails is that when the full SSL handshake was used to establish the initial SSL session the SSL appliance was inline and acting as a man in the middle (MITM). So the session that the client has saved and is trying to re-use was actually a session from the client to the SSL Appliance rather than to the server. The client does not know this as the SSL Appliance is a transparent MITM. However, if the MITM is removed and the client attempts session reuse the request goes to the server and the server cannot reuse this session as it does not recognize it.

6.10 Generating the Internal CA Certificates

Inspecting SSL sessions in any of the inline modes requires at least one internal CA certificate and private key, unless only Known Key decryption is used. The Sourcefire SSL appliance can generate the internal CA private key and either a self-signed certificate or a Certificate Signing Request (CSR) that can be forwarded to another CA. If using the CSR option it is important to note that public CA companies, such as Verisign, are unlikely to issue intermediate CA certificates for use in the Sourcefire SSL appliance. See Section 4.4 and Section 5.4.1 for more details.

6.11 Access to Microsoft Windows Update Denied

When trying to access the Microsoft windows update service through the Sourcefire SSL appliance an error message may be displayed by Internet Explorer and the update service will fail.

This error occurs because the CA of the certificate presented by the update website server, is found not to be a Microsoft server, and thus the update is aborted with an error. To allow the updates to continue, add an SSL Inspection Policy for the certificate Common-Name "*update.microsoft.com" with an action of "Cut Through" without decrypting. Windows update services should now function normally.

A default list of certificate Common Names (CNs) for sites that it is not possible to inspect traffic to are included in the DN list menu. A rule using this list can be added to a ruleset to ensure that traffic to these sites is not inspected.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

6.12 Issues with Alerts

If you fail to receive e-mail alerts, check the system log file for errors. The following may also prevent e-mail from being sent or delivered:

- If your SMTP server requires authentication, check that the username and password specified in the SMTP Server Settings section are correct.
- Check that you are using the correct port for the specified SMTP server. Some servers are configured not to use the default port 25.
- Ensure that the Sourcefire SSL appliance has a fully qualified domain name (FQDN). Some SMTP servers require that the sender have a FQDN.
- Ensure that all e-mail addresses are correct.
- If your enterprise is using Google Apps for e-mail then the correct SMTP Server Address is 'aspmx.l.google.com', not 'smtp.gmail.com'. Ensure that DNS resolution is properly configured. Alerts can only be sent to users on the same domain with this SMTP configuration.

6.13 Procedure for Reporting an Issue

The first step in reporting an issue is to capture diagnostics using the WebUI. See Section 5.2.7 for details on how to generate diagnostic files.

The support engineers may request further diagnostic information such as SSL statistics, non-SSL statistics, and the SSL session log (if enabled). The engineers will not request a copy of the PKI store because it may contain sensitive key material.

6.14 Preparing for Hardware Diagnostics or Maintenance

Support engineers may request advanced hardware diagnostics, or ask that certain firmware be upgraded. Before this can commence the Sourcefire SSL appliance must be put into a state where no traffic reaches the internal network interface, and packet processing engines are disabled. If this is required then appropriate directions will be given by the support engineer.

6.15 Command Line Diagnostics Interface

You may be asked to use the Command Line Diagnostics interface via an SSH or serial console connection by Customer Service, to aid in troubleshooting. The following table lists each command, and the related action.

- Enter **?** for a list of commands.
- Enter **(command)?** For a list of related commands. For example, **platform?** returns **platform halt** and **platform reboot**.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Command	Action
capture reset	Reset the network capture state and remove all captures stored on disk
capture select	Select capture mode and interfaces
capture start	Start capturing network traffic
capture status	Show the current network capture status
capture stop	Stop capturing network traffic
challenge show	Show backend authentication challenge
clear	Clear screen
counters interface	Show external interface counters
counters npu	Show NPU counters
counters packets	Show packet counters
counters ssl	Show SSL counters
counters switch	Show switch counters
counters tcp	Show TCP counters
diags reset	Reset diagnostics state
diags select	Select options for diagnostics collection
diags start	Start diagnostics collection
diags status	Check diagnostics status
error	Translate error codes
error counts	Dump flow error codes and counts
exit	Logout
license add	Install a new license, overwriting any currently installed license
license remove	Remove the currently installed license
license status	Show license status
network set ip	Set management network static IP configuration
network set ip dhcp	Enable DHCP management network IP configuration
network set mtu	Set management network MTU
network show	Show network IP configuration
platform halt	Halt the appliance
platform reboot	Reboot the appliance
segment	Show details about an activated segment

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Command	Action
segment all	Show details about all activated segments
segment fail	Fail to wire the interfaces of an activated segment
segment fail all	Fail to wire the interfaces of all activated segments
segment interfaces	Show statistics for all external interfaces assigned to an activated segment
segment list	Show the status of all activated segments
segment unfail	Unfail the interfaces of an activated segment
segment unfail all	Unfail the interfaces of all activated segments
update reset	Reset the update state and cancel any pending updates
update status	Show the current update status
user add	Add a user
user add role	Adds a role to a user
user change password	Change a user's password
user list	List users
user remove	Remove a user
user remove role	Removes a role from a user
user set name	Set a user's full name
user show	Display user information
version	Display version information

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

7. Safety Information

In addition to the information below you should read the separate Safety Notice included in the Sourcefire SSL appliance packaging.

7.1 Safety Instructions

Please read all of the following instructions regarding the Sourcefire SSL appliance carefully.

- **Ventilation**
  The Sourcefire SSL appliance vents (on the front panel) and the fan openings on the back panel are provided for ventilation and reliable operation of the product and to protect it from overheating. These openings must not be blocked or covered. This product must not be placed in a built-in installation unless proper ventilation is provided.
- **Power Cords**
  Caution: The power-supply cords are used as the main disconnect device. Ensure that the socket outlet is located or installed near the equipment and is easily accessible. The Sourcefire SSL appliance has a dual redundant power supply that is powered by two separate power cords. Always disconnect BOTH cords to remove power from the unit.

! **WARNING**: To reduce the risk of electrical shock, do not disassemble this product. Return it to Sourcefire when service or repair work is required. Opening or removing covers may expose the user to dangerous voltage or other risks. Incorrect assembly can cause electric shock when this appliance is subsequently used.

Note: Opening the cover will void the warranty!

7.2 Rack Mounting the Equipment

If the Sourcefire SSL appliance is to be installed in an equipment rack, please follow these precautions:

- Ensure that the ambient temperature around the appliance (which may be higher than the room temperature) is within the operational limits specified in Section 1.4.
- Ensure that there is sufficient airflow around the unit.
- Ensure that the electrical circuits are not overloaded; consider the nameplate ratings of all the connected equipment and ensure that sufficient over current protection is available.
- Ensure that the equipment is properly grounded.
- Never place any objects on top of the appliance.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

8. 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.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.