Extreme Networks Security Hardware Guide

9034856

Published July 2015

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

About this guide

The *Extreme Networks Security Hardware Guide* provides Extreme Security appliance descriptions, diagrams, and specifications.

Intended audience

This guide is intended for all Extreme Security users responsible for investigating and managing network security. This guide assumes that you have Extreme Security access and a knowledge of your corporate network and networking technologies.

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. Extreme Networks® systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME NETWORKS DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Note
Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. Extreme Networks Security Analytics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of Extreme Networks Security Analytics.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
📝	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.
New	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]+[Alt]+[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the "switch."

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at InternalInfoDev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Related Publications

The Extreme Security product documentation listed below can be downloaded from http://documentation.extremenetworks.com.

Extreme Security Analytics Threat Protection

- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*
- *Extreme Networks Security Log Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*

- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*

Extreme Security Threat Protection

- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Release Notes*

1 Safety Instructions

Review safety guidelines to help ensure your own personal safety and protect your system and working environment from potential damage.

This section includes safety guidelines to help ensure your own personal safety and protect your system and working environment from potential damage.

Systems are considered to be components in a rack. Thus, the term component refers to any system, various peripherals, or supporting hardware.

Observe the following precautions for rack stability and safety:

- System rack kits are intended to be installed in a rack by trained service technicians. Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing system/components in a rack, never pull more than one component out of the rack on the slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.
- Your system is safety-certified as a free-standing unit and as a component for use in a rack cabinet using the customer rack kit. The installation of your system and rack kit in any other rack cabinet has not been approved by any safety agency. It is your responsibility to ensure that the final combination of system and rack complies with all applicable safety standards and local electric code requirements. Extreme disclaims all liability and warranties in connection with such combinations.

Do not move racks by yourself. Due to the height and weight of the rack, a minimum of two people should accomplish this task.

- Always load the rack from the bottom up and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the rails can pinch your fingers.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.

2 What's new in hardware in Extreme Security V7.2.5

Extreme Networks Security Analytics V7.2.5 adds new XX28-C appliances. XX28-C appliances are manufactured by Dell®. You can use XX28-C appliances for federal government security compliance.

XX28-C appliances

The following Extreme Security Core Appliance XX28-C appliances are added to Extreme Security V7.2.5:

- Extreme Security 1400-C Data Node on page 15
- Extreme Security Event Processor 1628-C on page 18
- Extreme Security Flow Processor 1728-C on page 20
- Extreme Security Flow Processor 1828-C on page 22
- Extreme Security 3128-C (All-in-One) on page 25
- Extreme Security 3128-C (Console) on page 27
- Log Manager 1628-C on page 28
- Log Manager 3128-C (All-in-One) on page 31
- Log Manager 3128-C (Console) on page 33

3 Extreme Security appliance overview

Risk Manager
Extreme Security Incident Forensics
Extreme Security Packet Capture

Review information about Extreme Networks Security Analytics to understand hardware and license requirements.

Review this overview of Extreme Security appliances, including capabilities, and license limitations.

Extreme Security QFlow Collector 1201

The Extreme Security QFlow Collector 1201 appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar® QFlow Collector 1201 also supports external flow-based data sources.

View hardware information and requirements for the Extreme Networks Security Analytics QFlow Collector 1201 in the following table:

Table 3: Extreme Security QFlow Collector 1201

Description	Value
Network traffic	1 Gbps
Interfaces	Five 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Extreme Security QFlow Collector

For diagrams and information about the front and back panel of this appliance, see Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances on page 36.

Extreme Security QFlow Collector 1202

The Extreme Security QFlow Collector 1202 appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The Extreme Security QFlow Collector 1202 also supports external flow-based data sources.

View hardware information and requirements for the Extreme Security QFlow Collector 1202 in the following table:

Table 4: Extreme Security QFlow Collector 1202

Description	Value
Network traffic	3 Gbps
Interfaces	Napatech Network Adapter, providing four 1 Gbps 10/100/1000 Base-T network interfaces Two 10 Gbps SFP + ports One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Extreme Security QFlow Collector Napatech Network Adaptor

For diagrams and information about the front and back panel of this appliance, see Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances on page 36.

Extreme Security QFlow Collector 1301

The Extreme Security QFlow Collector 1301 appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The Extreme Security QFlow Collector 1301 also supports external flow-based data sources.

View hardware information and requirements for the Extreme Networks Security Analytics QFlow Collector 1301 in the following table:

Table 5: Extreme Security QFlow Collector 1301

Description	Value
Network traffic	3 Gbps
Interfaces	Napatech Network Adapter, providing four 1 Gbps 1000 Base SX Multi-Mode Fiber network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Extreme Security QFlow Collector Napatech Network Adaptor

For diagrams and information about the front and back panel of this appliance, see Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances on page 36.

Extreme Security QFlow Collector 1310

The Extreme Security QFlow Collector 1310 appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The Extreme Security QFlow Collector 1310 also supports external flow-based data sources.

View hardware information and requirements for the Extreme Networks Security Analytics QFlow Collector 1310 in the following table:

Table 6: Extreme Security QFlow Collector 1310 (4380-Q5C)

Description	Value
Network traffic	7.5 Gbps
Interfaces	Napatech Network Adapter for fiber, providing two 10 Gbps SFP + network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Extreme Security QFlow Collector Napatech Network Adaptor

For diagrams and information about the front and back panel of this appliance, see Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances on page 36.

Extreme Security 1400 Data Node

The Extreme Networks Security Analytics Data Node 1400 appliance provides scalable data storage solution for Extreme Security deployments. The Extreme Security Data Node enhances data retention capabilities of a deployment as well as augment overall query performance.

View hardware information and requirements for the Extreme Security Data Node in the following tables:

Table 7: Extreme Security Data Node when used with XX05 appliances

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	Storage: 9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Extreme Security Data Node appliance

Table 8: Extreme Security Data Node when used with XX28 appliances

Description	Value
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interface One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	40 TB or larger dedicated event storage: 12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Extreme Security Data Node appliance

Extreme Security 1400-C Data Node

The Extreme Networks Security Analytics Data Node 1400-C FIPS-compliant appliance provides scalable data storage solution for Extreme Security deployments. The Extreme Security Data Node enhances data retention capabilities of a deployment as well as augment overall query performance.

View hardware information and requirements for the Extreme Security Data Node in the following table:

Table 9: Extreme Security FIPS-compliant Data Node specifications

Description	Value
Basic license	2,500 EPS
Upgraded license	40,000 EPS

Table 9: Extreme Security FIPS-compliant Data Node specifications (continued)

Description	Value
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Data Node

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Extreme Security Event Collector 1501

The Extreme Networks Security Analytics Event Collector 1501 appliance is a dedicated event collector. By default, a dedicated event collector collects and parses event from various log sources and continuously forwards these events to an event processor. You can configure the QRadar® Event Collector 1501 appliance to temporarily store events and only forward the stored events on a schedule. A dedicated event collector does not process events and it does not include an on-board event processor.

View hardware information and requirements for the Extreme Security 1501 in the following table:

Table 10: Extreme Security 1501

Description	Value
Events per second	15,000 EPS
Network traffic	1 Gbps
Interfaces	Five 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 MB total (Raid 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector

For diagrams and information about the front and back panel of this appliance, see Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances on page 36.

Extreme Security Event Processor 1605

The Extreme Networks Security Analytics Event Processor 1605 appliance is a dedicated event processor that you can scale your Extreme Security deployment to manage higher EPS rates. The Extreme Security Event Processor 1605 appliance includes an on-board event collector, event processor, and internal storage for events.

The Extreme Security Event Processor 1605 is a distributed event processor appliance and requires a connection to an Extreme Security 3105 or Extreme Security 3128 console appliance.

View hardware information and requirements for the Extreme Security Event Processor 1605 in the following table:

Table 11: Extreme Security Event Processor 1605

Description	Value
Basic license	2,500 EPS
Upgraded license	20,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	Memory: 64 GB 8x 8 GB 1600 MHz RDIMM
Storage	Storage: 9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security Event Processor 1628

The Extreme Networks Security Analytics 1628 appliance is a dedicated event processor that you can use to scale your Extreme Security deployment to manage higher EPS rates. The Extreme Security Event Processor 1628 appliance includes an on-board event collector, event processor, and internal storage for events.

The Extreme Security Event Processor 1628 is a distributed event processor appliance and requires a connection to a Extreme Networks Security Analytics 3128 Console appliance.

View hardware information and requirements for the Extreme Security 1628 in the following table:

Table 12: Extreme Security 1628 Event Processor overview

Description	Value
Basic license	2,500 EPS
Upgraded license	40,000 EPS
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security Event Processor 1628-C

The Extreme Networks Security Analytics Event Processor 1628-C FIPS-compliant appliance is a dedicated event processor that you can use to scale your Extreme Security deployment to manage higher events per second (EPS) rates. The Extreme Security Event Processor 1628-C appliance includes an onboard event collector, event processor, and internal storage for events.

The Extreme Security Event Processor 1628-C is a distributed event processor appliance and requires a physical connection to a Extreme Networks Security Analytics 3128 Console appliance.

View hardware information and requirements for the Extreme Security 1628-C in the following table:

Table 13: Extreme Security 1628-C FIPS-compliant Event Processor specifications

Description	Value
Basic license	2,500 EPS
Upgraded license	40,000 EPS
Interfaces	One 2-port Emulex 8Gb FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC

Table 13: Extreme Security 1628-C FIPS-compliant Event Processor specifications (continued)

Description	Value
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Extreme Security Flow Processor 1705

The Extreme Security Flow Processor 1705 appliance is a flow processor that can scale your Extreme Security deployment to manage higher FPM rates. The Extreme Security Flow Processor 1705 includes an on-board Flow processor, and internal storage for flows.

View hardware information and requirements for the Extreme Security Flow Processor 1705 in the following table:

Table 14: Extreme Security Flow Processor 1705

Description	Value
Basic license	100,000 FPM
Upgraded license	600,000 FPM, depending on traffic types
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Flow processor

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security Flow Processor 1728

The Extreme Networks Security Analytics Flow Processor 1728 appliance is a flow processor that can scale your Extreme Security deployment to manage higher FPM rates. The Extreme Security Flow Processor 1728 includes an on-board Flow processor, and internal storage for flows.

View hardware information and requirements for the Extreme Security 1728 Flow processor in the following table:

Table 15: Extreme Security 1728 Flow Processor overview

Description	Value
Basic license	100,000 FPM
Upgraded license	1,200,000 FPM
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Flow Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security Flow Processor 1728-C

The Extreme Networks Security Analytics Flow Processor 1728-C FIPS-compliant appliance is a flow processor that can scale your Extreme Security deployment to manage higher flows per minute (FPM) rates. The Extreme Security Flow Processor 1728-C appliance includes an onboard flow processor, and internal storage for flows.

View hardware information and requirements for the Extreme Security 1728-C Flow Processor in the following table:

Table 16: Extreme Security 1728-C FIPS-compliant Flow Processor specifications

Description	Value
Basic license	100,000 FPM
Upgraded license	1,200,000 FPM
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Flow Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Extreme Security 1805

The Extreme Networks Security Analytics 1805 appliance is a combined Event Processor and Flow Processor that can scale your Extreme Security deployment to manage more events and flows. The Extreme Security 1805 includes an on-board Event Processor, an on-board Flow Processor, and internal storage for events and flows.

View hardware information and requirements for the Extreme Networks Security Analytics 1805 in the following table:

Table 17: Extreme Networks Security Analytics 1805 overview

Description	Value
Basic license	25,000 FPM 1,000 EPS
Upgraded license	200,000 FPM 5,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event processor Flow processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security Flow Processor 1828

The Extreme Networks Security Analytics 1828 appliance is a combined Event Processor and Flow Processor that you can scale your Extreme Security deployment to manage more event and flows. The Extreme Security 1828 includes an on-board Event Processor, an on-board Flow Processor, and internal storage for events and flows.

View hardware information and requirements for the Extreme Security 1828 Flow processor in the following table:

Table 18: Extreme Security 1828 Flow Processor overview

Description	Value
Basic license	25,000 FPM, 1000 EPS
Upgraded license	300,000 FPM 15,000 EPS
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Flow Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security Flow Processor 1828-C

The Extreme Networks Security Analytics 1828-C appliance is a combined Event Processor and Flow Processor that you can scale your Extreme Security deployment to manage more event and flows. The Extreme Security 1828-C includes an onboard event processor, an onboard flow processor, and internal storage for events and flows.

View hardware information and requirements for the Extreme Security 1828-C Flow Processor in the following table:

Table 19: Extreme Security 1828-C FIPS-compliant Flow Processor specifications

Description	Value
Basic license	25,000 FPM, 1000 EPS
Upgraded license	300,000 FPM 15,000 EPS
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC

Table 19: Extreme Security 1828-C FIPS-compliant Flow Processor specifications (continued)

Description	Value
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Flow Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Extreme Security 2100

The Extreme Networks Security Analytics 2100 appliance is an all-in-one system that combines Network Behavioral Anomaly Detection (NBAD) and Security Information and Event Management (SIEM) to accurately identify and appropriately prioritize threats that occur on your network.

View hardware information and requirements for the Extreme Networks Security Analytics 2100 in the following table:

Table 20: Extreme Networks Security Analytics 2100 overview

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	50,000 FPM
Interfaces	Three 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	32 GB, 4 x 8GB 1600 MHz RDIMM
Storage	6 x 2.5 inch 500 GB 7.2K rpm SATA, 3 TB total, 1.5 TB usable (Raid 10)
Power supply	Dual Redundant 750 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector Event Processor Single Extreme Security QFlow Collector

Additional Extreme Security QFlow Collectors are sold separately.

For diagrams and information about the front and back panel of this appliance, see Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances on page 36.

Extreme Security 3105 (All-in-One)

The Extreme Networks Security Analytics 3105 (All-in-One) appliance is an all-in-one Extreme Security system that can profile network behavior and identify network security threats.

View hardware information and requirements for the Extreme Security 3105 in the following table:

Table 21: Extreme Security 3105 overview

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	200,000 FPM 5,000 EPS
Network objects	1000
Log sources	750
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC Power Supply
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor for processing events and flows Internal storage for events and flows

The Extreme Security 3105 (All-in-One) appliance requires external Extreme Security QFlow Collectors for layer 7 network activity monitoring.

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security 3105 (Console)

Understand and expand the capacity of the Extreme Networks Security Analytics 3105 (All-in-One).

You can expand the capacity of the Extreme Security 3105 (All-in-One) beyond license-based upgrade options by upgrading to the Extreme Security 3105 (Console) appliance and adding one or more of the following appliances:

- Extreme Security Event Processor 1605 on page 17
- Extreme Security Flow Processor 1705 on page 19
- Extreme Security 1805 on page 21

The Extreme Security 3105 (Console) appliance you can use to manage a distributed deployment of Event Processors and Flow Processors to profile network behavior and identify network security threats.

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security 3128 (All-in-One)

The Extreme Networks Security Analytics 3128 (All-in-One) appliance is an all-in-one Extreme Security system that can profile network behavior and identify network security threats.

View hardware information and requirements for the Extreme Security 3128 (All-in-One) in the following table:

Table 22: Extreme Security 3128 (All-in-One)

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	300,000 FPM 15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interface One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor for processing events and flows Internal storage for events and flows

The Extreme Security 3128 (All-in-One) requires external QFlow Collectors for layer 7 network activity monitoring.

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security 3128-C (All-in-One)

The Extreme Networks Security Analytics 3128-C (All-in-One) FIPS-compliant appliance is an all-in-one Extreme Security system that can profile network behavior and identify network security threats.

View hardware information and requirements for the Extreme Security 3128-C (All-in-One) in the following table:

Table 23: Extreme Security 3128-C (All-in-One) FIPS-compliant specifications

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	300,000 FPM 15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interface One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor Internal storage for events and flows

The Extreme Security 3128-C (All-in-One) requires external Extreme Security QFlow Collectors for layer 7 network activity monitoring.

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Extreme Security 3128 (Console)

Understand expansion options for the Extreme Networks Security Analytics

You can expand the capacity of the Extreme Security3128 (All-in-One) appliance beyond license-based upgrade options by upgrading to the Extreme Security 3128 (Console) appliance and adding one or more of the following appliances:

- Extreme Security Event Processor 1628 on page 17
- Extreme Security Flow Processor 1728 on page 19
- Extreme Security Flow Processor 1828 on page 21

The Extreme Security 3128 (Console) appliance you can use to manage a distributed deployment of Event Processors and Flow Processors to profile network behavior and identify network security threats.

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security 3128-C (Console)

Use the Extreme Security 3128-C (Console) FIPS-compliant appliance to manage a distributed deployment of Event Processors and Flow Processors so that you can profile network behavior and identify network security threats.

You can expand the capacity of the Extreme Networks Security Analytics3128-C (All-in-One) FIPS-compliant appliance beyond license-based upgrade options by upgrading to the Extreme Security 3128-C (Console) appliance and FIPS compliant flow and event processor appliances. For example, add one or more of these appliances:

- Extreme Security Event Processor 1628-C on page 18
- Extreme Security Flow Processor 1728-C on page 20
- Extreme Security Flow Processor 1828-C on page 22

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Log Manager 1605

The Extreme Networks Security Log Manager 1605 appliance is a distributed Event Processor appliance and requires a connection to a Log Manager 3128 Console appliance.

The Log Manager 1605 is a distributed Event Processor appliance and requires a connection to a Log Manager 3105 appliance.

View hardware information and requirements for the Log Manager 1605 in the following table:

Table 24: Log Manager 1605

Description	Value
Basic license	2,500 EPS
Upgraded license	20,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Log Manager 1628

The Extreme Networks Security Log Manager 1628 appliance is a dedicated Event Processor that you can use to scale your Log Manager deployment to manage higher Event Per Second (EPS) rates. The Log Manager 1628 appliance includes an on-board Event Collector, Event Processor, and internal storage for events.

The Log Manager 1628 is a distributed Event Processor appliance and requires a connection to a Log Manager 3105 appliance.

View hardware information and requirements for the Log Manager 1628 in the following table:

Table 25: Log Manager 1628

Description	Value
Basic license	20,000 EPS
Upgraded license	40,000 EPS
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Log Manager 1628-C

The Extreme Networks Security Log Manager 1628-C FIPS-compliant appliance is a dedicated Event Processor that you can use to scale your Log Manager deployment to manage higher event per second (EPS) rates. The Log Manager 1628-C appliance includes an onboard event collector, event processor, and internal storage for events.

The Log Manager 1628-C is a distributed Event Processor appliance and requires a connection to a Log Manager 3105 appliance.

View hardware information and requirements for the Log Manager 1628-C in the following table:

Table 26: Log Manager 1628-C FIPS-compliant specifications

Description	Value
Basic license	20,000 EPS
Upgraded license	40,000 EPS
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Log Manager 2100

The Extreme Networks Security Log Manager 2100 appliance is an all-in-one system that can manage and store events from various network devices.

View hardware information and requirements for the Extreme Networks Security Log Manager 2100 in the following table:

Table 27: Extreme Networks Security Log Manager 2100 overview

Description	Value
Basic license	1000 EPS
Log sources	750
Interfaces	Three 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	32 GB, 4 x 8GB 1600 MHz RDIMM
Storage	6 x 2.5 inch 500 GB 7.2K rpm SATA, 3 TB total, 1.5 TB usable (Raid 10)
Power supply	Dual Redundant 750 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector Event Processor

Extreme Networks Security Log Manager 2100 includes external flow collection.

Additional Extreme Security QFlow Collectors are sold separately.

For diagrams and information about the front and back panel of this appliance, see Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances on page 36.

Log Manager 3105 (All-in-One)

The Extreme Networks Security Log Manager 3105 (All-in-One) appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the Log Manager 3105 in the following table:

Table 28: Log Manager 3105 overview

Description	Value
Basic license	25,000 FPM 1000 EPS
Upgraded license	200,000 FPM 5,000 EPS
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC Power Supply
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor for processing events Internal storage for events

You can upgrade your license to migrate your Log Manager 3105 (all-in-one) to Extreme Security 3105 (all-in-one). For more information, see the *Migrating Extreme Security Log Manager to Extreme SIEM Technical Note*.

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Log Manager 3105 Console

You can expand the capacity of the Log Manager (all-in-one) appliance beyond license-based upgrade options by upgrading to the Log Manager 3105 (Console) appliance. You must also add one or more Log Manager 1605 or Log Manager1628 appliances.

The Log Manager 3105 (Console) appliance manages a distributed deployment of Event Processors to collect and process events. You can upgrade your license from Log Manager 3105 to Extreme Security 3105

Log Manager 3128 (All-in-One)

The Extreme Networks Security Log Manager 3128 (All-in-One) appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the Log Manager 3128 (All-in-One) in the following table:

Table 29: Log Manager 3128 (All-in-One)

Description	Value
Basic license	1,000 EPS
Upgraded license	15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)
Interfaces	One 2-port Emulex 8Gb FC Two 10/100/1000 Base-T network monitoring interface One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual Redundant 900 W AC
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor Internal storage for events

You can upgrade your license to migrate your Log Manager 3128 (all-in-one) appliance to Extreme Security 3128 (all-in-one). For more information about migrating Log Manager to Extreme Security SIEM, see the *Migrating Extreme Security Log Manager to Extreme SIEM Technical Note*.

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Log Manager 3128-C (All-in-One)

The Extreme Networks Security Log Manager 3128-C (All-in-One) FIPS-compliant appliance is an all-in-one system that you can use to manage and store events from various network devices.

View hardware information and requirements for the Log Manager 3128-C (All-in-One) in the following table:

Table 30: Log Manager 3128-C (All-in-One) FIPS-compliant specifications

Description	Value
Basic license	1,000 EPS
Upgraded license	15,000 EPS
Network objects	Up to 1,000, depending on the license
Log sources	750 (add more devices with a licensing option)
Interfaces	One 2-port Emulex 8 Gbps FC Three 10/100/1000 Base-T network monitoring interface One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 40 TB usable (Raid 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor Internal storage for events

You can upgrade your license to migrate your Log Manager 3128-C (all-in-one) appliance to Extreme Security 3128-C (all-in-one). For more information about migrating Log Manager to Extreme Security SIEM, see the *Migrating Extreme Security Log Manager to Extreme SIEM Technical Note*.

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Log Manager 3128 (Console)

The Extreme Networks Security Log Manager 3128 (Console) appliance manages a distributed deployment of Event Processors to collect and process events. Expand and upgrade the Log Manager 3128 (Console).

You can expand the capacity of the Log Manager 3128 (all-in-one) appliance beyond license-based upgrade options by upgrading to the Log Manager 3128 (Console) appliance and adding one or more of the following appliances:

- Log Manager 1605 on page 27
- Log Manager 1628 on page 28

You can upgrade your license to migrate your Log Manager 3128 (Console) appliance to Log Manager 3128 (Console). For more information, see the *Migrating Extreme Security Log Manager to Extreme SIEM Technical Note* .

The Log Manager 3128 (Console) appliance manages a distributed deployment of Event Processors to collect and process events.

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Log Manager 3128-C (Console)

The Extreme Networks Security Log Manager 3128-C (Console) FIPS-compliant appliance manages a distributed deployment of Event Processors to collect and process events. Expand and upgrade the Log Manager 3128-C (Console).

You can expand the capacity of the Log Manager 3128-C (all-in-one) appliance beyond license-based upgrade options by upgrading to the Log Manager 3128-C (Console) appliance and adding one or more of the following appliances:

- Extreme Security Event Processor 1628 on page 17

You can upgrade your license to migrate your Log Manager 3128-C (Console) appliance to Log Manager 3128-C (Console). For more information, see the *Migrating Extreme Security Log Manager to Extreme SIEM Technical Note* .

The Log Manager 3128-C (Console) appliance manages a distributed deployment of Event Processors to collect and process events.

For diagrams and information on the front and back panel of this appliance, see Extreme Security FIPS Appliances on page 37.

Extreme Security Vulnerability Manager

The Extreme Networks Security Vulnerability Manager appliance scans and reports on network vulnerabilities. Extreme Security Vulnerability Manager provides a vulnerability management workflow that is fully integrated with Extreme Security SIEM and is available as a software option, appliance, and virtual appliance.

Extreme Security Vulnerability Manager provides the following capabilities:

- Scans inside and outside your network, network infrastructure, servers, and end points for bad configurations, weak settings, unpatched products, and other key weaknesses.
- Uses network usage, threat environment, security configuration information, virtual patch, and patch availability to bring real context to vulnerability management, which drives efficient remediation processes
- Integrates all vulnerability information from external systems to provide a single view.
- Full integration with the Extreme Security asset profile database to provide intelligent event-driven scans.
- Unlimited Extreme Security Vulnerability Manager discovery scans
- Use of hosted scanner for DMZ scanning

The Extreme Security Vulnerability Manager appliance supports:

Table 31: Extreme Security Vulnerability Manager overview

Description	Value
Basic license	255 assets
Upgraded license	32,768
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Security management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC Power Supply
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Extreme Security Vulnerability Manager

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Risk Manager

The Extreme Networks Security Analytics appliance delivers a fully integrated risk management, vulnerability prioritization, and automated configuration solution that is integrated into the Extreme Networks Security Analytics platform. Log Manager enables tightly integrated features in Extreme SIEM that enhance incident management, log and network activity searches, threat visualization, and reports.

View hardware information and requirements for the Risk Manager in the following table:

Table 32: Risk Manager in the following table

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme SIEM management interface One 10/100 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5)
Power supply	Dual Redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Risk Manager

For diagrams and information about the front and back panel of this appliance, see Extreme Security Appliances on page 37.

Extreme Security Incident Forensics

Use Extreme Networks Security Incident Forensics to retrace the step-by-step actions of a potential attacker, and conduct an in-depth forensics investigation of suspected malicious network security incidents. Extreme Security Incident Forensics reduces the time it takes security teams to investigate offense records. It can also help you remediate a network security breach and prevent it from happening again.

Extreme Security Incident Forensics shares hardware with Extreme Security XX28 appliances. For more information about XX28 appliances, see Extreme Security Appliances on page 37.

Extreme Security Packet Capture

Extreme Networks Security Incident Forensics offers an optional Extreme Networks Security Packet Capture appliance to store and manage data that is used by Extreme Security Incident Forensics when no other network packet capture (PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or sub-network to collect the raw packet data.

View hardware information and requirements for Extreme Security Packet Capture in the following table:

Table 33: Extreme Security Packet Capture overview

Description	Value
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/100 Base-T Extreme Networks Security Analytics management interface One 10/100 Base-T integrated management module interface Four 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 41 TB total, 32 TB usable (Raid 5)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Flow Processor

For diagrams and information on the front and back panel of this appliance, see Extreme Security Appliances on page 37.

4 Appliance Diagrams

View the diagrams and descriptions for the back and front panels of your appliance. These diagrams are representations of an Extreme Networks Security Analytics appliance. Your system might vary, depending on the version of appliance you purchased.

Integrated Management Module

On the back panel of each appliance type, the serial connector and Ethernet connectors can be managed using the Integrated Management Module (IMM). You can configure the IMM to share an Ethernet port with the Extreme Networks Security Analytics management interface; however, you can configure the IMM in dedicated mode to reduce the risk of losing the IMM connection when the appliance is restarted. To configure the IMM, you must access the System BIOS settings by pressing the F1 key when the splash screen is displayed. For further instructions on how to configure the IMM, see the *Integrated Management Module User's Guide* that is located on the CD that was shipped with your appliance.

Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor Appliances

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

- Extreme Security 2100 on page 23 (4380-Q1C).
- Extreme Security QFlow Collector 1202 on page 12 (4380-Q3C).
- Extreme Security QFlow Collector 1301 on page 13 (4380-Q4C).
- Extreme Security QFlow Collector 1310 on page 14 (4380-Q5C).
- Extreme Security Event Collector 1501 on page 16, Extreme Security QFlow Collector 1201 on page 12 (4380-Q2C).
- Log Manager 2100 on page 29 (4380-Q1C).

For more information about Extreme Security 2100, Extreme Security Event Collector 1501, and all Extreme Security Flow Processor appliances, including front and back panel diagrams, see IBM System X3550 M4 (http://publib-b.boulder.ibm.com/abstracts/tips0851.html?Open).

Extreme Security Appliances

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

- Extreme Security 1400 Data Node on page 14 (4380-Q1E).
- Extreme Security Event Processor 1605 on page 17 (4380-Q1E).
- Extreme Security Event Processor 1628 on page 17 (4380-Q2E).
- Extreme Security Flow Processor 1705 on page 19 (4380-Q1E).
- Extreme Security Flow Processor 1728 on page 19 (4380-Q2E).
- Extreme Security 3105 (All-in-One) on page 23 (4380-Q1E).
- Extreme Security 3105 (Console) on page 24 (4380-Q1E).
- Extreme Security 3128 (All-in-One) on page 25 (4380-Q2E).
- Extreme Security 3128 (Console) on page 26 (4380-Q2E).
- Log Manager 1605 on page 27 (4380-Q1E).
- Log Manager 1628 on page 28 (4380-Q2E).
- Log Manager 3105 (All-in-One) on page 30 (4380-Q1E).
- Log Manager 3105 Console on page 30 (4380-Q1E).
- Log Manager 3128 (All-in-One) on page 31 (4380-Q2E).
- Log Manager 3128 (Console) on page 32 (4380-Q2E).
- Extreme Security Vulnerability Manager on page 33 (4380-Q1E).
- Risk Manager on page 34 (4380-Q1E).

Extreme Security FIPS Appliances

Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality.

Important
The following graphics illustrate the features of FIPS Appliances. To be FIPS-compliant, you must attach tamper-proof labels to the appliance. For more information about physical security, see the *IBM Security QRadar Version 7.2.4 FIPS 140-2 Installation Guide*.

- Extreme Security 1400-C Data Node on page 15
- Extreme Security Event Processor 1628-C on page 18
- Extreme Security Flow Processor 1728-C on page 20
- Extreme Security Flow Processor 1828-C on page 22
- Extreme Security 3128-C (All-in-One) on page 25
- Extreme Security 3128-C (Console) on page 27
- Log Manager 1628-C on page 28
- Log Manager 3128-C (All-in-One) on page 31
- Log Manager 3128-C (Console) on page 33

Front panel indicators and features

View the front panel diagram and descriptions for the Extreme Security FIPS-compliant appliance to understand the hardware features.

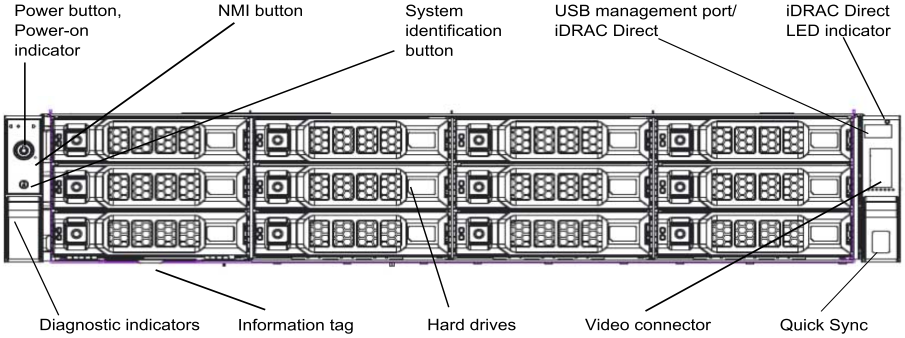

Figure 1: FIPS appliance front panel

Table 34: Front Panel Features of Extreme SecurityFIPS Appliances

Feature	Description
Diagnostic indicators	The diagnostic indicators display error status.
System identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the system status indicator on the back flashes until one of the buttons is pressed again. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. To reset the iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.
Power-on indicator, power button	The power-on indicator lights when the system power is on. The power button controls the power supply output to the system. Note On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off.
NMI button	Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel or by the operating system's documentation.
Information tag	A slide-out label panel records system information such as Service Tag, NIC, MAC address, and so on.
Hard drives	Up to twelve 3.5 inch hot-swappable hard drives.

Table 34: Front Panel Features of Extreme SecurityFIPS Appliances (continued)

Feature	Description
USB management port/iDRAC Direct	Connects USB devices to the system or provides access to the iDRAC Direct features. The USB management port is USB 2.0-compliant.
iDRAC Direct LED indicator	The indicator displays error status.
Video connector	Connects a VGA display to the system.
Quick Sync (optional)	Indicates a Quick Sync enabled system. The Quick Sync feature is optional and requires a Quick Sync bezel. This feature allows management of the system using mobile devices. This feature aggregates hardware and firmware inventory and various system level diagnostic and error information that can be used in troubleshooting the system.

Back panel indicators and features

View the back panel diagram and descriptions for the Extreme Security FIPS-compliant appliance to understand the hardware features.

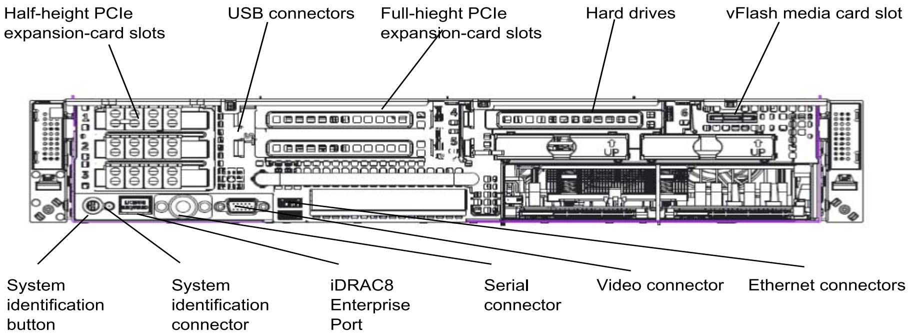
Half-height PCIe expansion-card slots
USB connectors
Full-hieght PCIe expansion-card slots
Hard drives
vFlash media card slot
System identification button
System identification connector
iDRAC8 Enterprise Port
Serial connector
Video connector
Ethernet connectors

Figure 2: FIPS appliance back panel

Table 35: Back Panel Features of Extreme Networks Security Analytics Core Appliances

Feature	Description
System identification button	The identification buttons on the front and back panels can be used to locate a particular system within a rack. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. To reset iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.
System identification connector	Connects the optional system status indicator assembly through the optional cable management arm.

Table 35: Back Panel Features of Extreme Networks Security Analytics Core Appliances (continued)

Feature	Description
iDRAC8 Enterprise port	Dedicated management port.
Half-height PCIe expansion-card slot	Connects up to three half-height PCI Express expansion cards.
Serial connector	Connects a serial device to the system.
Video connector	Connects a VGA display to the system.
USB connector	Connects USB devices to the system. The ports are USB 3.0-compliant.
Full-height PCIe expansion-card slot	Connects up to four full-height PCI Express expansion cards.
Ethernet connector	Integrated 10/100/1000 Mbps NIC connectors
Power supply unit	AC 495 W, 750 W, or 1100 W or DC 750 W or 1100 W
vFlash media card slot	Holder for a vFlash media card.

A Glossary

A
B
C
D
E
F
G
H
I
K
L
M
N
O
P
Q
R
S
T
V
W

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

accumulator
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

active system
In a high-availability (HA) cluster, the system that has all of its services running.

Address Resolution Protocol (ARP)
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

administrative share
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

anomaly
A deviation from the expected behavior of the network.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

ARP
See Address Resolution Protocol.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN
See autonomous system number.

asset
A manageable object that is either deployed or intended to be deployed in an operational environment.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior
The observable effects of an operation or event, including its results.

bonded interface
See link aggregation.

burst
A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client
A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console	A display station from which an operator can control and observe the system operation.
content capture	A process that captures a configurable amount of payload and then stores the data in a flow log.
credential	A set of information that grants a user or process certain access rights.
credibility	A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.
CVSS	See Common Vulnerability Scoring System.

D

database leaf object	A terminal object or node in a database hierarchy.
datapoint	A calculated value of a metric at a point in time.
Device Support Module (DSM)	A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.
DHCP	See Dynamic Host Configuration Protocol.
DNS	See Domain Name System.
Domain Name System (DNS)	The distributed database system that maps domain names to IP addresses.
DSM	See Device Support Module.
duplicate flow	Multiple instances of the same data transmission received from different flow sources.
Dynamic Host Configuration Protocol (DHCP)	A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption	In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.
endpoint	The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.
external scanning appliance	A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive	A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).
flow	A single transmission of data passing over a link during a conversation.
flow log	A collection of flow records.
flow sources	The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination

One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN

See fully qualified domain name.

FQNN

See fully qualified network name.

fully qualified domain name (FQDN)

In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)

In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway

A device or program used to connect networks or systems with different network architectures.

H

HA

See high availability.

HA cluster

A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)

A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)

Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC

See Hash-Based Message Authentication Code.

host context

A service that monitors components to ensure that each component is operating as expected.

I

ICMP

See Internet Control Message Protocol.

identity

A collection of attributes from a data source that represent a person, organization, place, or item.

IDS

See intrusion detection system.

Internet Control Message Protocol (ICMP)

An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)

A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)

An organization that provides access to the Internet.

intrusion detection system (IDS)

Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP
See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS
See intrusion prevention system.

ISP
See Internet service provider.

K

key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L
See Local To Local.

L2R
See Local To Remote.

LAN
See local area network.

LDAP
See Lightweight Directory Access Protocol.

leaf
In a tree, an entry or node that has no children.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

live scan
A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.

log source
Either the security equipment or the network equipment from which an event log originates.

log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT
See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

network weight
The numeric value applied to each network that signifies the importance of the network. The network weight is defined by the user.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI
See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L See Remote To Local.

R2R See Remote To Remote.

recon See reconnaissance.

reconnaissance (recon) A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L) The external traffic from a remote network to a local network.

Remote To Remote (R2R) The external traffic from a remote network to another remote network.

report In query management, the formatted data that results from running a query and applying a form to it.

report interval A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner An automated security program that searches for software vulnerabilities within web applications.

secondary HA host The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

SOAP
A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

T

TCP
See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file
A key database file that contains the public keys for a trusted entity.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

Index