Cisco Security Packet Analyzer 2400 Appliance

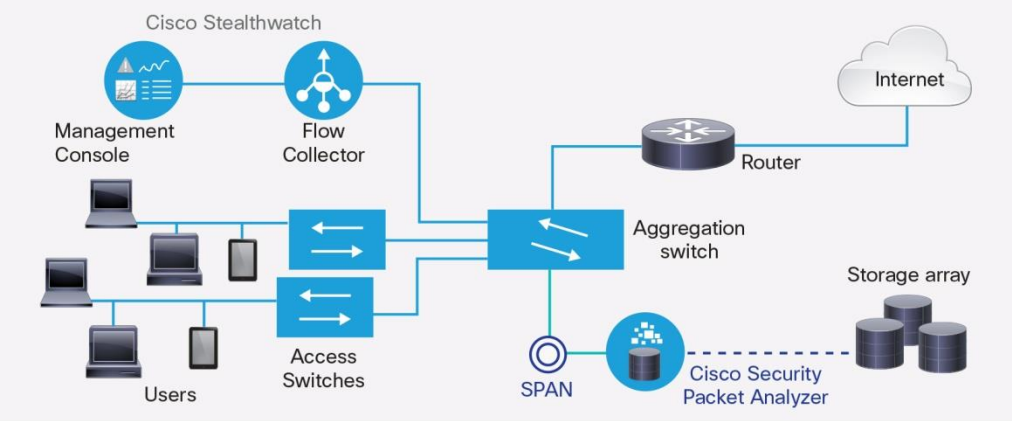
The Cisco® Security Packet Analyzer enhances “detect and respond” capabilities to help defend your network. Dive deep into anomalous network activity and security events to get the complete status of your network.

Network threats and cybercriminals are getting smarter. The question is not whether your network will be breached. The question is when. The need to have network visibility and the ability to respond to advanced threats quickly has never been greater. Many organizations possess some level of security monitoring and incident response capability. Security professionals can speed incident response in several ways. A common method is using packet capture solutions, which can collect and store all of the information that traverses the network.

Using Packet Capture for Improved Incident Response

Network forensics is the process of monitoring and analyzing data that moves over a network and using it to investigate anomalous activity. Security Packet Analyzer supports this forensics process. The Cisco Security Packet Analyzer works in conjunction with Cisco Stealthwatch. It applies the Stealthwatch NetFlow and context security analytics capabilities to captured data packets so you can dive into the context and content of network sessions in near real time. (See Figure 1.)

Figure 1. A Sample Packet Analyzer and Stealthwatch Deployment



Product Overview

Security Packet Analyzer attaches to your network by means of a Switched Port Analyzer (SPAN), a feature also called port mirroring, or a network Test Access Point (TAP). A copy of packet traffic is created from that point in the network. Security Packet Analyzer stores a complete copy of these network packets. They can be retrieved later for more detailed analysis using either the packet analysis software included in the solution or third-party analysis tools.

Figure 2. Cisco Security Packet Analyzer 2400

Features and Benefits

Feature	Benefit
High-performance packet capture	• Adds real-time 4 x 1 GE and 2 x 10 GE network performance, capturing all frames including those normally discarded by standard network interface cards (NICs)
On-premises appliance	• Provides safe and highly secure on-premises capture and storage to maintain the confidentiality of data
Integration with Stealthwatch	• Uses Stealthwatch flow data analysis to locate specific points in the data stream and to generate a detailed search query that Packet Analyzer uses to locate those packets
API	• Simplifies fast operationalization of threat intelligence with existing security and network infrastructure
Industry-standard storage	• Security Packet Analyzer stores data in industry-standard packet capture format; this enables the use of high-performance through packet capture or WinPcap

The Cisco Security Packet Analyzer is based on technology developed for the Cisco Network Analysis Module (NAM). It builds on the features and improvements delivered in NAM version 6.2. These include support for Remote Integrated Services Engine (RISE) technology, which allows the switch (Cisco Nexus® 7000 Series and others) to “see” the Packet Analyzer appliance as a blade. Other highlights include the termination of Encapsulated Remote SPAN (ERSPAN) on the data port to extend traffic capture capabilities. By terminating the high-speed ERSPAN on the data port, Packet Analyzer can access Type III ERSPAN headers and process ERSPAN at higher speeds.

The Security Packet Analyzer appliance takes full advantage of the Cisco Unified Computing System™ (Cisco UCS®) C240 rack-mounted server platform to deliver high performance, reliability, and manageability. The appliance can be configured with either four Gigabit Ethernet or two 10 Gigabit Ethernet monitoring copper (RJ-45) or optical (Small Form-Factor Pluggable, or SFP) interfaces and a 100/1000 RJ-45 Ethernet management port. This appliance solution includes 128 GB of DRAM and 48 TB of hot-swappable enterprise-class SAS storage. Storage can be extended through the external SAS port.

Product Specifications

Table 1. Product Specifications

Packet Analyzer Feature	Description
Chassis	2 rack units (2RU)
Processor	2 Intel® Xeon® E5-2660 processors
Memory	128 GB industry-standard double data rate (DDR4) main memory
Storage	48 TB (24 x 2 TB) SAS drives
Storage expansion	SAS port and modular LAN on motherboard (mLOM)

Packet Analyzer Feature	Description
Monitoring ports (choose one)	• 4 x 1 GE RJ-45 • 4 x 1 GE SFP • 2 x 10 GE SFP+
Management port	10/100/1000 RJ-45
Physical dimensions	2RU: 3.43 x 17.65 x 29.0 in. (8.71 x 44.83 x 73.66 cm.) excluding handles 3.43 x 18.96 x 30.18 in. (8.71 x 48.16 x 76.66 cm.) including handles
Temperature: operating	41 to 95°F (5 to 35°C) operating at sea level, no fan fail, no CPU throttling, turbo mode

Regulatory Standards

Table 2 lists regulatory standards compliance information.

Table 2. Regulatory Standards Compliance: Safety and EMC

Specification	Description
Safety	• UL 60950-1 No. 21CFR1040 Second Edition • CAN/CSA-C22.2 No. 60950-1 Second Edition • IEC 60950-1 Second Edition • EN 60950-1 Second Edition • IEC 60950-1 Second Edition • AS/NZS 60950-1 • GB4943 2001
EMC: Emissions	• 47CFR Part 15 (CFR 47) Class A • AS/NZS CISPR22 Class A • CISPR2 2 Class A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A
EMC: Immunity	• EN55024 • CISPR24 • EN300386 • KN24

Warranty Information

You can find warranty information on Cisco.com at the Product Warranties page.

Ordering Information

To place an order, visit the Cisco Ordering homepage. To download software, visit the Cisco Software Center. See Table 3 for ordering information.

Table 3. Cisco Security Packet Analyzer Ordering Information

Product Name	Part Number
Cisco Security Packet Analyzer 2400	SEC-PA-2400-K9

For ordering convenience, the SFP part numbers (Table 4) are available on the Cisco Ordering homepage when you order the Cisco Security Packet Analyzer.

Table 4. SFP Ordering Information

Product Name	Part Number	Ordering Information
10GBASE-SR SFP+ Module for MMF	SFP-10G-SR=	Refer to the Cisco 10GBASE SFP+ Modules data sheet for ordering information related to these Cisco SFP+ modules and related cables.
10GBASE-LR SFP+ Module for SMF	SFP-10G-LR=	
10GBASE-ER SFP+ Module for SMF	SFP-10G-ER=	
1000BASE-T Standard	GLC-T=	Refer to the Cisco SFP Modules data sheet for ordering information related to these Cisco SFP modules.
1000BASE-SX Short Wavelength; With DOM	GLC-SX-MMD=	
1000BASE-LX/LH Long-Wavelength; With DOM	GLC-LH-SMD=	

Cisco Services

Services from Cisco and Our Partners

Realize the full business value of your technology investments with smart, personalized services from Cisco and our partners. Backed by deep networking expertise and a broad ecosystem of partners, Cisco Services help you to successfully plan, build, and run your network as a powerful business platform. Whether you are looking to quickly seize new opportunities to meet rising customer expectations, improve operational efficiency to lower costs, mitigate risk, or accelerate growth, we have a service that can help you. For information about Cisco Services, go to http://www.cisco.com/go/services. Table 5 shows the technical support service recommended for Cisco Security Packet Analyzer.

Table 5. Cisco Technical Services

Technical Services
Cisco Smart Net Total Care™ Service provides: • Global 24-hour access to the Cisco Technical Assistance Center (TAC) • Access to online knowledge base, communities, and tools • Hardware replacement options, including 2-hour, 4-hour, and next-business-day* service • Ongoing operating system software updates** • Smart, proactive diagnostics and real-time alerts on devices enabled with Smart Call Home

* Advance hardware replacement is available in various service-level combinations. For example, “8x5xNBD” indicates that shipment will be initiated during the standard 8-hour business day, 5 days a week (the generally accepted business days within the relevant region), with next business day (NBD) delivery. Where NBD is not available, same-day shipping is provided. Restrictions apply; please review the appropriate service descriptions for details.

** Cisco operating system updates include maintenance releases, minor updates, and major updates within the licensed feature set.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

For more information about Cisco Security Packet Analyzer Appliance, visit your local account representative, or email the Cisco Security Product Analyzer product marketing group at secpa-info@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-737589-01 08/16