SmartWall®

THREAT DEFENSE SYSTEM

corero
FIRST LINE OF DEFENSE

DATA SHEET

NETWORK FORENSICS APPLIANCE

KEY BENEFITS

Total visibility into network & application traffic

Comprehensive visibility into Internet traffic to-and-from protected resources with scalable solutions for capturing and indexing 100% of the packets at 10Gbps rates.

Green, energy-efficient platform

Energy-efficient design with front-to-back cooling fully supports economic and environmental initiatives.

Powerful centralized management

Centralized Operational Management for configuring, controlling, and monitoring the appliances.

YOUR INTERNET TRAFFIC CAPTURE SOLUTION FOR DDOS ATTACKS AND CYBER THREATS

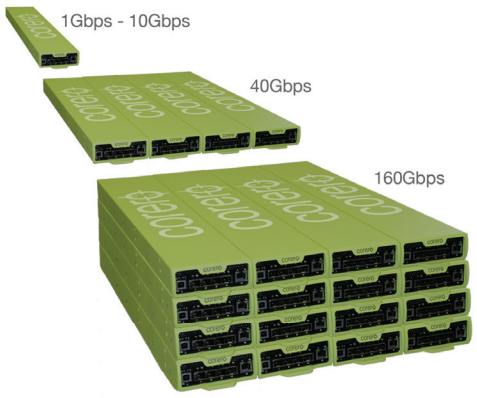
The Corero SmartWall® Network Forensics Appliance provides line-rate Internet traffic capture to support network forensics of DDoS attacks and cyber threats.

The modern cyber threat landscape is constantly evolving. As new and more sophisticated threats emerge, an organization's defense-in-depth strategy must evolve to include comprehensive visibility into Internet traffic to-and-from protected resources. The SmartWall Network Forensics Appliance provides this visibility by offering scalable solutions for capturing and indexing 100% of the packets at 10Gbps rates. Service Providers, Hosting Providers, and Managed Security Service Providers (MSSPs) can offer traffic capture as a service providing the necessary data to feed historical analysis of cyber threat activity including identification of attack vectors, fingerprinting attacker identity, breach characterization as well as intelligence gathering for preparation against emerging threats.

Storage of captured data is distributed to third-party iSCSI devices via dual 10Gbps network interfaces. This breakthrough intelligent capture appliance offers unprecedented scalability and performance. Capture rates can be scaled in 10Gbps increments, capture duration is limited only by the capacity of the network addressable iSCSI storage. The iSCSI storage does not need to be physically adjacent to the SmartWall Network Forensics Appliance or located in a single SAN implementation. The SmartWall Network Forensics Appliance can continuously record traffic and simultaneously retrieve specific historical packet captures for subsequent analysis of network packets, flows and trends over time. It provides the raw data for detailed visibility into detected threats and anomalous usage patterns, enabling robust network forensic analysis for regulatory compliance, corporate security incident response and law enforcement reporting.

FEATURED PRODUCT

10Gbps full-duplex performance in a 1/4 wide, 1 RU form factor with scalability from 10Gbps to 1Tbps in a single rack



SmartWall® Threat Defense System

The SmartWall Network Forensics Appliance provides Service Providers of all types with the ability to offer packet capture and retrieval as a value added security service to their customers.

This next-generation slimline appliance delivers 10Gbps full-duplex performance in a 1/4 wide 1RU form factor. It is a member of the new SmartWall Threat Defense System, an innovative family of space-saving, modular platforms that change the rules for performance, energy efficiency and scalability while providing a First Line of Defense against cyber threats.

GREEN, ENERGY-EFFICIENT PLATFORM

Compact packaging provides the best performance to size and power ratio in the industry. This green, energy-efficient design with front-to-back cooling fully supports economic and environmental initiatives to reduce rack space and cut back on cooling and electrical requirements.

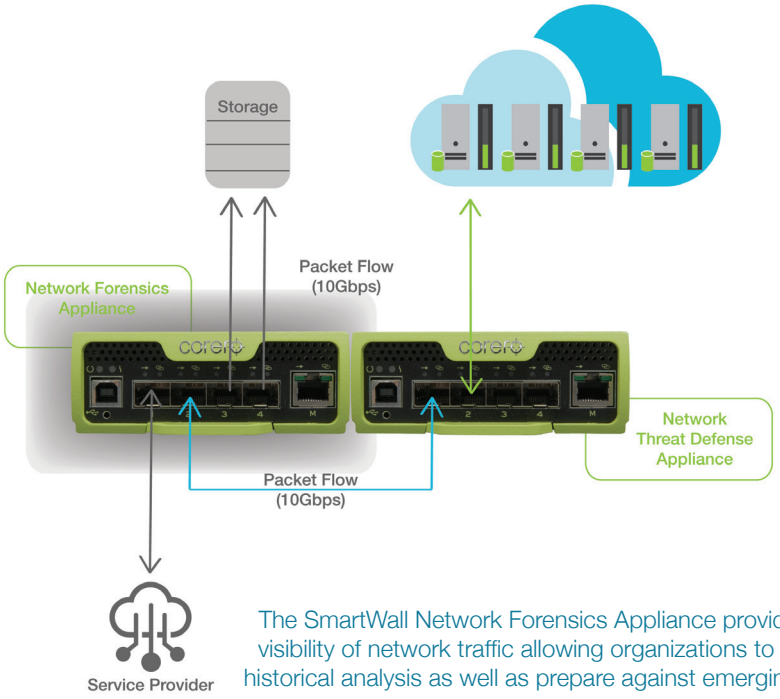
POWERFUL AND EASY-TO-USE CENTRALIZED MANAGEMENT

Each unit has a dedicated management port and is assigned a unique IP address. Centralized operational management of multiple appliances minimizes IT overhead, speeds deployments and streamlines provisioning. Corero offers multiple management options for configuring, controlling, and monitoring the appliances including a flexible Browser-based GUI, a full SSH CLI and powerful REST API that supports open integration with existing management frameworks.

Centralized management of the SmartWall Network Forensics Appliance as well as other family members of the SmartWall Threat Defense System (TDS) is performed via secure connection to the Corero Management Server (CMS). The CMS includes a dashboard for monitoring threat activity and viewing key security events. The CMS is delivered as a virtual appliance to run on customer-provided hardware.

The SmartWall Network Forensics Appliance provides seamless integration with Security Information and Event Management (SIEM) and Operational Intelligence solutions, such as Splunk.

SMARTWALL® NETWORK FORENSICS APPLIANCE



The SmartWall Network Forensics Appliance provides total visibility of network traffic allowing organizations to perform historical analysis as well as prepare against emerging threats

FLEXIBLE DEPLOYMENT CONFIGURATIONS

A single appliance can be deployed in a standalone configuration to provide 10Gbps full-duplex performance, multiple SmartWall Network Threat Defense Appliances can be distributed to key control points in the Provider network or centrally combined in 1 RU shelves in various high throughput configurations. The modular design enables rapid, flexible and expandable deployments, and lowers your risk by limiting your investments to match your current requirements while allowing you to add capacity as your needs grow.

TECHNICAL SPECIFICATIONS

Order Part Number	SmartWall Network Forensics Appliance
Regulatory Model Number	6000-10
Interfaces	
Copper 10/100/1000 Ethernet Ports	1 MGMT
Pluggable 10G Ethernet Ports (SFP+ Modules)	4
Other Ports (Serial Console, Authentication Service)	1 USB 2.0
Storage	
10G Ethernet Ports	Used for output to third-party iSCSI devices
Performance	
Maximum Capture Rate (bps)	10 Gbps
Maximum Capture Rate (pps)	15 Mpps
Device Management	
Management Interfaces	1 10/100/1000 Management Port
Management Station	Virtual Machine Deployable in VMware-capable environments
Management Options	GUI, Command Line, Programmatic API
Command Line	SSH Access Through the Management Station
Web-Based	HTTP/HTTPS Access Through the Management Station
Programmatic API	JSON-Based REST API Through the Management Station
Management Protocols for Monitoring	SNMP v2 Standard MIB GETs, SYSLOG
Software Upgrade Mechanism	Remotely Upgradeable Image and Configuration Stored on Internal SSD
Security Dashboards	
Reporting and 3rd-Party Management	Splunk, ArcSight, CA, eIQ Networks, Forensics Explorer, GuardedNet, HP OpenView, IBM Tivoli, netForensics, Open Service, RSA Envision, Q1Labs, TriGeo
Authentication Mechanisms	Role-Based Access Control (Active Directory)
Physical/Environmental	
Size	1-RU 4.0cm (H) x 10.8 cm (W) x 60.4cm (D)
Weight	3.6 Kgs (7.9 lbs.)
Operating Temperature	0 C to 40 C (32 F to 104 F)
Storage Temperature	-25 C to 70 C (-13 F to 158 F)
Humidity	5% to 95% Non Condensing
MTBF Rating	>100,000 Hours (25 deg. C Ambient)
Operating Altitude	0-10,000 Feet
Tamper Protection	Tamper-Evident Seal
Power & Cooling	
Power Supplies	Single Internal PSU
AC Input	100 to 240 VAC Auto-Ranging, 50-60Hz
Power Consumption	Typical 120W

TECHNICAL SPECIFICATIONS (cont.)

Compliance & Approvals	
Compliance to EMC Emissions	FCC Part 15-7.10.2008, EN55022: 2006+A1: 2007, CISPRR 22:2005+A1+A2:2005, VCCI-3 2009.04, AS/NZS CISPR22:2006, EN 61000-3-2:2006, EN61000-3-3:1995 +A1:2001+A2:2005, EN61000-3-11:2000, EN 61000-3-12:2005
Compliance to EMC Immunity	EN55024: 1998 Including Amendment 1:2001 & Amendment 2:2003(CISPR24:1997 +A1:2001 +A2:2002), EN 61000-4-2:1995 +A1:1998 +A2:2001, EN 61000-4-3:2006, EN 61000-4-4:2004, EN 61000-4-5:2006, EN 61000-4-6:1996 +A1:2001, EN 61000-4-8:1993 +A1:2001, EN 61000-4-11:2004
Compliance to Safety	UL 60950-1, 2nd Ed., CSA C22.2 No. 60950-1, 2nd Ed., EN 60950-1, 2nd Ed., IEC 60950-1, 2nd Ed.
International Compliance Approvals	UL Listed, CUL, AS/NZS 3260, CE, FCC Class A, VCCI Class A, ICES-003 Class A

[1]Typical latency values measured for packet sizes up to 1518 bytes

ABOUT CORERO NETWORK SECURITY

Corero Network Security, an organization's First Line of Defense® against DDoS attacks and cyber threats, is a pioneer in global network security. Corero products and services provide online enterprises, service providers, hosting providers, and Managed Security Service Providers with an additional layer of security capable of inspecting Internet traffic and enforcing real-time access and monitoring policies designed to match the needs of the protected business. Corero technology enhances any defense-in-depth security architecture with a scalable, flexible and responsive defense against DDoS attacks and cyber threats before they reach the targeted IT infrastructure allowing online services to perform as intended. For more information, visit www.corero.com.

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749 USA
Phone: +1.978.212.1500
Web: www.corero.com

EMEA Headquarters
Regus House, Highbridge, Oxford Road
Uxbridge, England
UB8 1HR, UK
Phone: +44.0.1895.876579