SmartWall® THREAT DEFENSE SYSTEM

corero
FIRST LINE OF DEFENSE

DATA SHEET

NETWORK BYPASS APPLIANCE

KEY BENEFITS

100% around-the-clock connectivity
100% network connectivity protection to eliminate Internet downtime in case of power or equipment failures and during planned maintenance or equipment upgrade windows.

Multiple protection modes
Transparent 10Gbps full-duplex performance for network bypass, monitor or insertion.

Active TAP capability
10Gbps full-duplex test access point (TAP) monitoring of both of the protected fiber ports.

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

ENSURING NETWORK CONNECTIVITY

Network connectivity is a key consideration for maintaining an always on Internet presence. The Corero SmartWall® Network Bypass Appliance provides you with 100% network connectivity protection to eliminate Internet downtime in case of power or equipment failures and during planned maintenance or equipment upgrade windows.

100% AROUND-THE-CLOCK CONNECTIVITY

As a member of the Corero SmartWall Threat Defense System (TDS), the Network Bypass Appliance allows service providers and enterprises to ensure business continuity of their Internet facing services and applications. The bypass appliance can be deployed seamlessly with other members of the SmartWall family to deliver around-the-clock connectivity.

MULTIPLE PROTECTION MODES

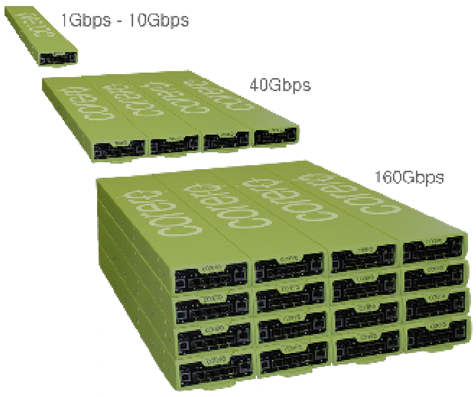
The SmartWall Network Bypass Appliance delivers transparent 10Gbps full-duplex performance for network bypass, monitor or insertion. It has two passive fiber ports for 10Gbps of zero power optical bypass and two active 10Gbps SFP+ ports for monitoring and active inline processing. Multiple configurable protection modes are supported including power-fail, manual bypass, programmatic bypass and automatic heartbeat detection.

ACTIVE TAP CAPABILITY

The SmartWall Network Bypass Appliance provides 10Gbps full-duplex test access point (TAP) monitoring of both of the protected fiber ports delivering the replicated traffic to the two SFP+ ports for connection to other SmartWall monitoring, threat detection or capture appliances.

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

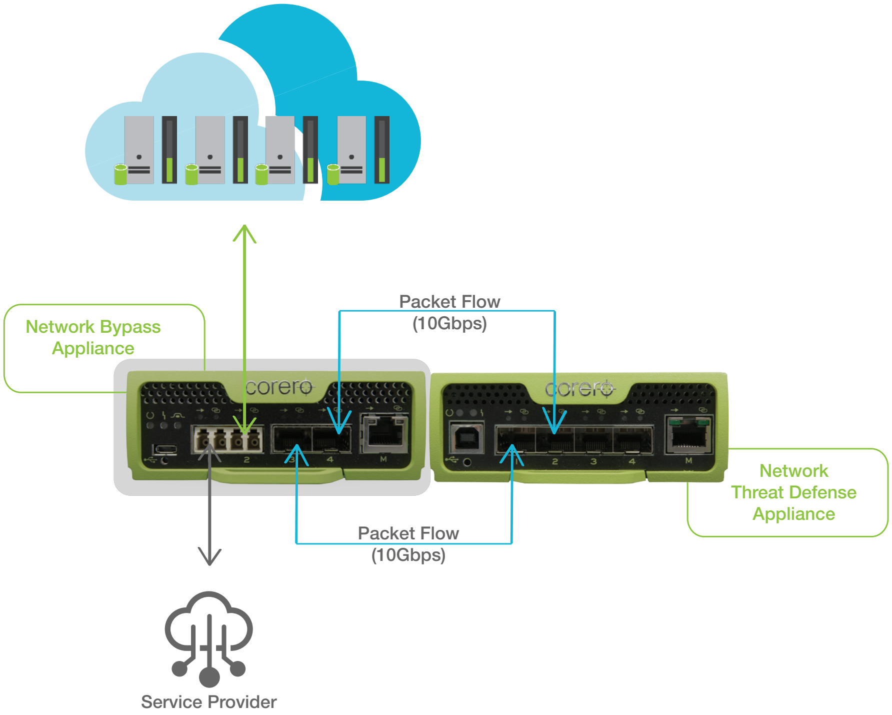
GREEN, ENERGY-EFFICIENT PLATFORM

This slimline appliance delivers 10Gbps full-duplex performance in a ¼ 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. A single Network Bypass appliance consumes less than 50 watts of power. This green, energy-efficient, compact design supports economic and environmental initiatives to reduce rack space and cut back on cooling and electrical requirements.

POWERFUL AND EASY-TO-USE CENTRALIZED MANAGEMENT

Corero offers multiple management options, including a flexible GUI, a powerful CLI and a full REST API that allows integration with existing management frameworks. You can centrally manage multiple SmartWall Network Bypass Appliance as well as other members of the SmartWall Threat Defense System using the Corero Management Server (CMS). It includes a configuration wizard and offers an easy-to-use, web-based interface as well as a browser-based CMS dashboard. The CMS is delivered as a virtual appliance to run on customer-provided hardware. The CMS is integrated with directory services, and provides seamless integration with state-of-the-art Security Information and Event Management (SIEM) and Operations Intelligence solutions.

SmartWall® NETWORK BYPASS APPLIANCE



The SmartWall® Network Bypass Appliance has a Mission-In and Mission-Out pair of passive fiber ports for zero power optical bypass, as well as two active SFP+ ports for transparent connectivity to security or forensics devices.

TECHNICAL SPECIFICATIONS

Order Part Number	**SmartWall Network Bypass Appliance**
Copper 10/100/1000 Ethernet Ports	1 MGMT
Pluggable 10G Ethernet Ports (SFP+ Modules)	2
Optical Bypass Ports	2
Other Ports (Serial Console, Authentication Service)	1 USB 2.0
Performance	
Maximum Throughput (Gbps)	10 Gbps
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 Server
Programmatic API	JSON-Based REST API through the Management Server
Management Protocols for Monitoring	SNMP v2 Standard MIB GETs, SYSLOG
Software Upgrade Mechanism	Remotely Upgradeable Image and Configuration Stored on Internal SSD
Reporting and 3rd-Party Management	Examples: Splunk, ArcSight, RSA Envision, Q1Labs.
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 Feeds	Dual AC and DC* Support
AC Input	100 to 240 VAC Auto-Ranging, 50-60Hz
DC* Input	-75 to -40V DC
Power Consumption	Typical 50W
Cooling	Internal N+1 Fans
Compliance & Approvals	
Compliance to EMC Emissions	FCC Part 15-7.10.2008, EN55022: 2006+A1: 2007, CIS-PRR 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

TECHNICAL SPECIFICATIONS (cont.)

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

*Available Q4 2015

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 re-al-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

Update: 10.1.2015