SmartWall®

THREAT DEFENSE SYSTEM

corero
FIRST LINE OF DEFENSE

DATA SHEET

NETWORK THREAT DEFENSE APPLIANCE

KEY BENEFITS

Robust security coverage

Comprehensive network security protection against layers 3 -7 for both IPv4 and IPv6 traffic.

Industry-leading density, scalability & performance

Protection is provided through configurable access policies with scalability from 10/20Gbps up to 2Tbps in a single rack.

Comprehensive Visibility

Leveraging Splunk software for big data analytics and advanced DDoS visualization capabilities.

Powerful centralized management

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

Flexible deployment configurations

Multiple appliances can be distributed to key control points in the Provider network or centrally combined in 1 RU shelves in various configurations.

Your First Line of Defense® AGAINST DDOS ATTACKS

The Corero SmartWall® Network Threat Defense Appliance provides First Line of Defense® protection against DDoS attacks and cyber threats. It delivers the industry's highest performance in a compact, energy efficient form factor for scalability in 10/20Gbps up to 2Tbps in a single rack.

Disruptions to Internet-facing online services can cripple operations, impact customers and result in major economic losses. The SmartWall Network Threat Defense Appliance is an intelligent, always on platform that inspects traffic, detects threats and blocks attacks against protected network resources. It allows Enterprises, Service Providers, Hosting Providers, and Managed Security Service Providers (MSSPs) to deploy centralized or distributed threat defense solutions via purpose-built network security appliances that provide advanced Layer 3-7 cyber threat protection.

The SmartWall Network Threat Defense Appliance provides continuous visibility and security policy enforcement so that organizations can establish a proactive First Line of Defense for inspecting traffic, detecting threats and blocking attacks. It is capable of mitigating a wide range of DDoS attacks (including volumetric, multi-vector, layers 3-7, etc.) and cyber threats while maintaining full service connectivity and availability to avoid degrading the delivery of legitimate traffic. In addition, Service Providers and Hosting Providers can leverage scale-as-you-grow deployments of SmartWall Network Threat Defense Appliances to create incremental service revenue streams by offering high-value DDoS and cyber threat protection services to their enterprise or hosted customers.

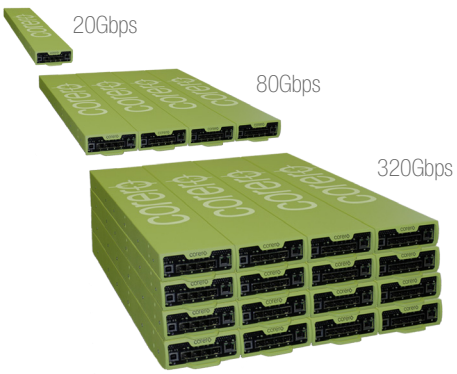
This next-generation slimline appliance delivers 10Gbps full-duplex or 20Gbps unidirectional performance in a ¼ wide, 1 RU form factor. It is a member of the Corero SmartWall Threat Defense System (TDS), an innovative family of space-saving, modular security platforms that will change the rules for inspection performance, security intelligence and network forensics, while providing an unprecedented level of scalability for First Line of Defense protection against cyber threats.

ROBUST SECURITY COVERAGE

The SmartWall Network Threat Defense Appliance provides comprehensive network security protection against layers 3-7 DDoS attacks and cyber-threats for both IPv4 and IPv6 traffic. It leverages the Corero award-winning DDoS defense technology to deliver non-disruptive, always on protection against the

FEATURED PRODUCT

10Gbps full-duplex or 20Gbps unidirectional performance in a 1/4 wide, 1 RU form factor with scalability from 10/20Gbps up to 2Tbps in a single rack



SmartWall® Threat Defense System

ROBUST SECURITY COVERAGE (cont.)

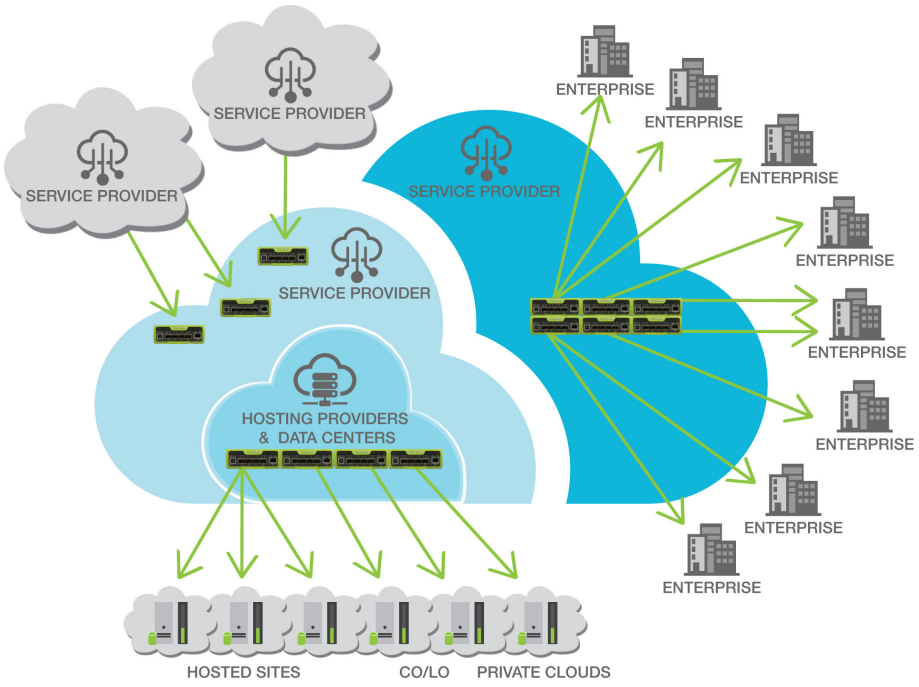
constantly evolving threat landscape. This ground breaking appliance provides configurable policies to selectively enable a broad range of specific protection mechanisms to defend critical network assets against suspicious or malicious traffic types while allowing uninterrupted service access to legitimate users and applications. The SmartWall TDS also utilizes the concepts of Flex-Rule and Smart-Rule technology to apply granular detecting and blocking filters to a very specific attack with ease. These rules, leverage heuristic and closed loop policy, allow for rapid creation and deployment, thereby providing customers with the ability to respond rapidly to the evolving nature of sophisticated DDoS attacks.

You can also configure protection against known suspicious or malicious IP addresses with the Corero ReputationWatch™ service which receives the latest intelligence data on potential sources of cyber criminal activity. ReputationWatch continuously leverages global threat feeds to determine the current IP reputation of incoming traffic. Granular policy options can be selected to automatically monitor or block access from malicious sources such as botnets or DDoS attackers.

ReputationWatch also supports country-based protection policies using SmartWall geolocation technology which allows you to control access, based on the reported national origin of an IP address. The geolocation capability lets you define policies to alert, limit or exclude traffic from countries that you do not need to connect with, or from countries associated with a high risk of potential attack.

The SmartWall Network Threat Defense Appliance supports both symmetric and asymmetric traffic inspection to support flexible network deployment options.

First Line of Defense® DEPLOYMENT OPTIONS



The SmartWall® Network Threat Defense Appliance can be deployed to protect both infrastructure and cloud resources.

INDUSTRY-LEADING SCALABILITY & PERFORMANCE

The SmartWall Network Threat Defense Appliance offers new levels of scalability and performance in a compact and energy-efficient platform. Each appliance provides dynamic threat level tracking of up to 16 million Internet based IP addresses and their associated flows. Protection is provided through configurable acceptable access policies supporting packet and connection rate limiting, reputation and geolocation checks, server and service connection limits, protocol checks, as well as blacklist, whitelist and temporary shun list enforcement. This high-performance platform is designed to maintain 10Gbps full-duplex or 20Gbps unidirectional throughput (pre appliance), even while under attack. Each appliance offers flow-based inspection of up to 10 million flows and can setup one million new flows per second. Traffic inspection can be performed in monitor or inline modes with under 0.5 microseconds of latency.

INDUSTRY-LEADING SCALABILITY & PERFORMANCE (cont.)

The modular architecture of the SmartWall Network Threat Defense Appliance enables cost-effective scaling in increments up to 20Gbps, as bandwidth, flow table and inspection requirements increase. Four appliances can be deployed in a single 1 RU shelf to deliver a combined 40Gbps full-duplex or 80Gbps unidirectional throughput or up to four times the 20Gbps inspection rate for four times the number of IP addresses. 4 RUs of appliances can deliver 160Gbps of full-duplex or 320Gbps unidirectional throughput.

TURN-KEY VISIBILITY INTO DDOS ATTACKS

Leveraging Splunk software for big data analytics and advanced visualization capabilities, Corero has transformed its sophisticated security event data into dashboards of actionable security intelligence, accessible via Corero SecureWatch® Analytics.

Real-time security engineered dashboards accessible via the Corero SecureWatch Portal, or via Splunk Apps http://apps.splunk.com/app/1835/ provide never-before-seen visibility into an organization's network and security activity for rapid response in combating these threats. Additionally, SecureWatch Analytics supports archived security event data to enable forensic analysis of past threats and compliance reporting of security activity.

SecureWatch Analytics can also be leveraged as a comprehensive virtual Security Operations Center (SOC) by Corero partners to deliver new revenue streams in the form of managed security services to the enterprise, such as 24x7 monitoring, alerting and reporting.

COMPREHENSIVE VISIBILITY

SecureWatch® Analytics provides turn-key visibility into DDoS attacks for quick and actionable diagnosis as well as proactive reporting and analysis.

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 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 Threat Defense System 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 Threat Defense Appliance provides seamless integration with Security Information and Event Management (SIEM) and Operational Intelligence solutions, such as Splunk.

FLEXIBLE DEPLOYMENT CONFIGURATIONS

A single appliance can be deployed in a standalone configuration to provide 10Gbps full-duplex or 20Gbps unidirectional 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. Redundant or hot-standby SmartWall Network Threat Defense Appliances can be deployed in high-availability configurations to provide backup protection in up to 20Gbps increments. Multiple appliances can also be deployed in dynamic load-balanced configurations to accommodate peak period demands.

SECURITY COVERAGE

Category of Attack Type	Attack Coverage
Volumetric DDoS	TCP Flood Attacks HTTP GET/POST Floods UDP Flood Attacks UDP Fragmentation Attacks ICMP Floods
Reflective DDoS	NTP Monlist Response Amplification SSDP/UPnP Responses SNMP Inbound Responses Chargen Responses Smurf Attack Fraggle Attack DNS DNS Amplification
Resource Exhaustion	Malformed and Truncated Packets (e.g. UDP Bombs) IP Fragmentation/Segmentation AETs Invalid TCP Segment IDs Bad checksums and illegal flags in TCP/UDP frames Invalid TCP/UDP port numbers Use of reserved IP addresses Slow HTTP requests (from tools like Slowloris, RUDY, Slowread)
Other	Command and Control Operations Tunnel Inspection (GRE, MPLS etc.) GRE, MPLS etc. NTP Monlist Requests Whitelisting Known malicious IP Addresses (botnets, scanners, anonymization services, phishing sites, spammers) Customized Protection with IP Reputation and Geolocation Policies Blacklisting of IP Addresses Port address range filters (provides protection for generic TCP/UDP port based attacks) Rate Limiting Policies Flex-Rule – Programmable filters based on the Berkley Packet Format (BPF) syntax. These can be programmed to address a variety of attack categories volumetric, reflective through to attacks leveraging specific payloads (Teamspeak, RIPv1, netbios). Smart-Rule – Heuristics based engine leverages heuristics and behavioral analysis to track and rate limit L1-L4 attacks

TECHNICAL SPECIFICATIONS

Order Part Number	SmartWall Network Threat Defense Appliance
Regulatory Model Number	6000-10
Interfaces	
Copper 10/100/1000 Ethernet Ports	1 MGMT
Pluggable 1G and 10G Ethernet Ports (SFP and SFP+ Modules)	4
Other Ports (Serial Console, Authentication Service)	1 USB 2.0
Performance	
Maximum Throughput (Gbps)	10 Gbps full-duplex or 20 Gbps unidirectional (1 Gbps when deployed with 1G SFP modules)
Maximum Throughput (Packets Per Second)	30 Mpps (3 Mpps when deployed with 1G SFP modules)
MTU Performance Max PDU 9100	Line rate, 10 Gbps 30 Mpps
Jumbo Frames	Yes
Typical Latency[1]	<0.5uS
Typical Inspected Latency[1]	< 60 uSec
Maximum Concurrent Sessions	16 Million
Maximum Session Setup/Teardown	1 Million/Sec
Maximum SYN Flood DoS Protection Rate	Line-rate

TECHNICAL SPECIFICATIONS (cont.)

Attack Reaction Time	< 3 seconds
IP Reputation / Geolocation lookups per second	1 Million/Sec
IP Addresses Blocked/Shunned Per Second	15 Million/Sec blocked, 1 Million/Sec shunned
Maximum Number of TCP Connections/ UDP flows	16 Million
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 (RestAPI)
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/v3* Standard MIB GETs, SYSLOG
Software Upgrade Mechanism	Remotely Upgradeable Image and Configuration Stored on Internal SSD
Security Dashboards	Link utilization (Gbps/PPS), Attack targets, Attack vectors, Alerts, Detailed drill-downs, Top IPs/Ports/TTLs/Packet Sizes, Export to PCAP
Reporting and 3rd-Party Management	Security events and sFlow data available in a standard SYSLOG format and via a REST API for SIEM integration. Full integration supported with Splunk Enterprise and available as an app at https://apps.splunk.com/app/1835/
Authentication Mechanisms	Role-Based Access Control (Active Directory, RADIUS and LDAP)
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	Single AC and DC* support, DC supports dual A/B feeds
AC Input	100 to 240 VAC Auto-Ranging, 50-60Hz
DC* Input	-75 to -40V DC
Maximum Power Consumption	<150W
Cooling	Internal N+1 Fans
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

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

Version: 18-Nov-2015