SmartWall®

Threat Defense System - vNTD

Key Benefits

Robust, real-time security coverage

Real-time Layer 3-7 mitigation against volumetric DDoS attacks for both IPv4 and IPv6 traffic.

Industry-leading density, scalability & performance

Protection is provided through configurable access policies with scalability from Gbps up to multi-Tbps in a single deployment.

Comprehensive visibility

Big data analytics and advanced DDoS visualization capabilities, leveraging Splunk software.

Powerful centralized management

Centralized operational management for configuring, controlling, and monitoring.

Flexible deployment configurations

SmartWall vNTD enables dynamic elastically scaled deployments distributed to key control points in the Provider network or centrally combined in various configurations.

Real-Time DDoS Mitigation

The Corero SmartWall® Network Threat Defense Virtual Edition (vNTD) delivers the industry's highest performing virtualized DDoS protection in up to 10Gbps increments.

This purpose built high-performance DDoS mitigation appliance delivers up to 10Gbps throughput performance in a virtual form factor. It is a member of the Corero SmartWall Threat Defense System (TDS) family of security platforms that change the rules for inspection performance, security intelligence and comprehensive reporting and analytics, while providing an unprecedented level of scalability for protection against DDoS attacks.

The SmartWall vNTD is an intelligent, always-on platform that inspects traffic, detects threats and blocks attacks targeting protected network resources in seconds, versus the minutes or tens of minutes experienced in legacy mitigation solutions. It allows providers and digital enterprises to deploy centralized or distributed real-time DDoS protection.

The SmartWall vNTD provides continuous visibility and security policy enforcement so that organizations can establish a proactive approach for inspecting traffic, detecting threats and blocking attacks. It is capable of protecting against layer 3-7 volumetric DDoS attacks, while maintaining full service connectivity and availability to avoid degrading the delivery of legitimate traffic. In addition, providers can leverage scale-as-you-grow deployments of SmartWall vNTD, enabling them to deliver high-value, premium DDoS Protection as-a-Service (DDPaaS) to their customers.

SmartWall vNTD enables protection to be delivered in a more agile manner, with protection capacity deployed and scaled as required.

The virtualized solution enables DDoS protection as part of existing SDN/NFV plans, fitting standard NFV models.

Robust & Real-Time Security Coverage

The SmartWall vNTD provides Layer 3-7 protection against volumetric DDoS attacks for both IPv4 and IPv6 traffic in seconds vs minutes. It leverages the Corero award-winning DDoS defense software to deliver non-disruptive, real-time protection against the constantly evolving threat landscape. This technology 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 vNTD includes Flex-Rule and Smart-Rule technology to supplement default protections with ease. These rules leverage Corero's leading analytics and forensics tools, with heuristics and a closed-loop environment, allowing for rapid creation and deployment, and the ability to respond rapidly to the evolving nature of sophisticated DDoS attacks.

The SmartWall vNTD offers new levels of scalability and performance in a virtualized platform. Protection is provided through configurable acceptable access policies supporting packet and connection rate limiting, server and service connection limits, protocol checks, as well as blacklist and whitelist capabilities. This high-performance platform is designed to maintain up to 10Gbps throughput (per virtual instance), even while under attack.

The modular architecture of SmartWall enables cost-effective scaling in increments, as bandwidth requirements increase. SmartWall vNTD can be deployed to deliver a combined protection of multiple terabits throughput, enabling the ability to dynamically and rapidly add DDoS protection with selective traffic steering.

Turn-key Visibility into DDoS Attacks

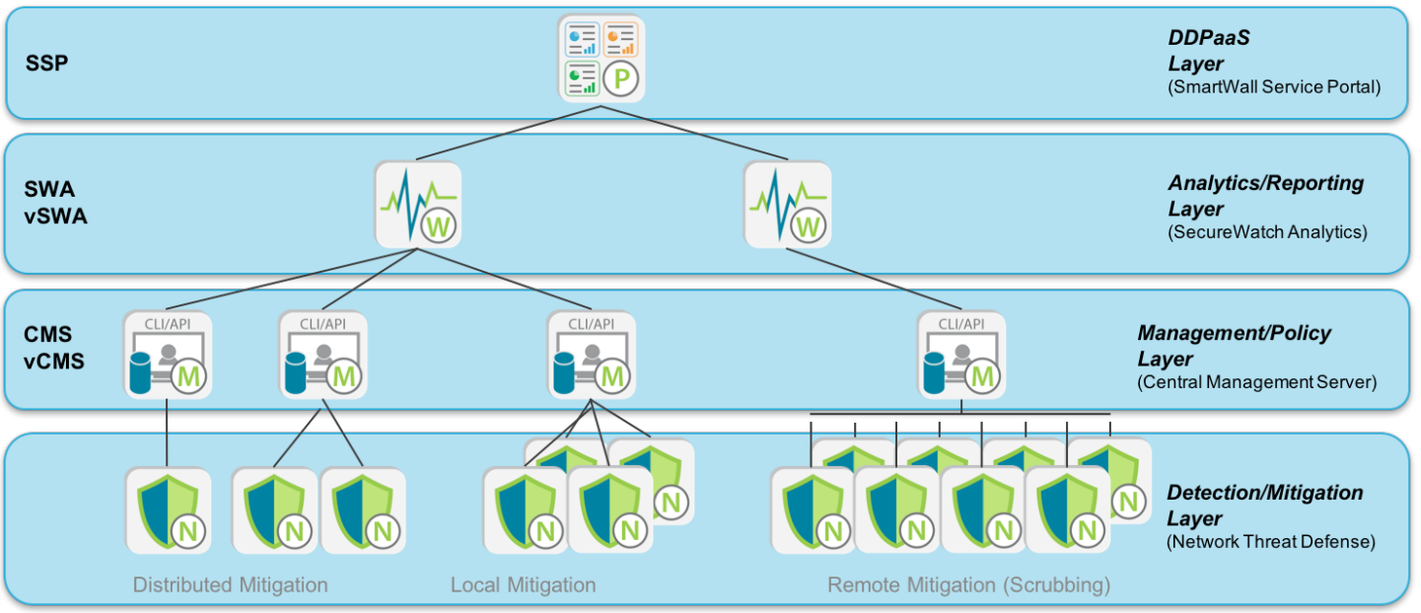
Leveraging Splunk software for big data analytics and advanced visualization capabilities, Corero has transformed its sophisticated security event data into dashboards of actionable security intelligence.

Real-time security engineered dashboards, accessible via the Corero SecureWatch® Portal, provide comprehensive visibility into an organization's network and security activity for rapid response in combating these threats. Additionally, this robust reporting and analytics feature supports archived security event data to enable forensic analysis of past threats and compliance reporting of security activity.

Powerful Centralized Management

Each virtual solution has a dedicated management connection IP address. Centralized operational management of hardware and software virtual appliances minimizes operational overhead, speeds deployments and streamlines provisioning. Flexible licensing models, based on capacity, allow additional virtual

appliances to be added easily. Corero offers multiple management options for configuring, controlling, and monitoring the solution including a flexible Browser-based GUI, a full SSH CLI, SNMP monitoring, and powerful REST API that supports open integration with existing management frameworks.



The Central Management Server is delivered as a physical appliance, or virtual appliance to run on customer-provided hardware.

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

Flexible Deployment Configurations

A vNTD can be deployed in a standalone configuration to provide 10Gbps bidirectional performance. Multiple SmartWall NTD appliances of any type can be distributed to key control points in the network or centrally combined in various high throughput configurations. The modular design enables rapid, flexible and expandable deployments, and lowers risk by limiting your investments to match your current requirements while allowing you to add capacity as your needs grow. vNTD can leverage hypervisor high-availability configurations to provide backup protection. Multiple appliances can also be deployed in dynamic load-balanced configurations to accommodate peak period demands.

The vNTD solution supports both symmetric and asymmetric traffic inspection enabling flexible network deployment options.

SECURITY COVERAGE

Category of Attack Type	Attack Coverage
Volumetric DDoS	TCP Flood Attacks 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
Other	NTP Monlist Requests Customized Protection with 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 Filter (BPF) syntax address a variety of attacks leveraging specific payloads (Teamspeak, RIPv1, netbios) Smart-Rule – Heuristics based engine leverages behavioral analysis to track and rate limit L2-L4 and zero-day network DDoS attacks

TECHNICAL SPECIFICATIONS

Features	SmartWall Network Threat Defense Virtual Edition
Network Interfaces	
	2 Virtual interfaces, offering a single inspection segment
Performance	
Maximum Throughput (Gigabits per second)	10 Gbps bidirectional (deployed on a pinned 8 x Intel E5-2695 or equivalent CPU cores running in KVM)
Maximum Throughput (Packets Per Second)	15 Mpps (deployed on KVM)
Jumbo Frames	Yes (9,216 Bytes)
Maximum SYN Flood DoS Protection Rate	Line-rate
Attack Reaction Time	Typically sub-second
Device Management	
Management Interfaces	1 Virtual Management Port
Management Station	Physical or Virtual (VMware/KVM)
Management Options	GUI, Command Line, Programmatic API (Rest)
Command Line	SSH Access Through the Management Station
Web-Based	HTTP/HTTPS Access Through the Management Station
Programmatic API	JSON-Based REST Through the Management Station
Management Protocols for Monitoring	SNMP v2/v3* Standard MIB GETs, SYSLOG
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 and RADIUS)
Environment	
Hypervisors	KVM running on Redhat Enterprise 7, CentOS 7 or Ubuntu 16.04, VMware ESXi 5.5+
Minimum Requirements	16GB Memory, 20GB Disk

About Corero Network Security

Corero Network Security is the leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and digital enterprises rely on Corero's award winning technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics and reporting. This industry leading technology provides cost effective, scalable protection capabilities against DDoS attacks in the most complex environments while enabling a more cost effective economic model than previously available. For more information, visit www.corero.com.

Corero Headquarters
225 Cedar Hill Street, Suite 337
Marlboro, MA 01752
Tel: +1 978 212 1500
Web: www.corero.com

EMEA Headquarters
Regus House, Highbridge, Oxford Road
Uxbridge, England
UB8 1HR, UK
Tel: +44 (0) 1895 876579