SmartWall®

Threat Defense System - NTD1100

Key Benefits

Robust, real-time security coverage

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

Industry- leading density, scalability & performance

Protection is provided through configurable access policies with scalability from 100Gbps up to 4Tbps in a single rack.

Comprehensive visibility

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

Powerful centralized management

Centralized operational managemet for configuring, controlling, and monitoring defense appliances.

Flexible deployment configurations

Multiple appliances can be 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 (NTD1100) Appliance provides real-time protection against damaging DDoS attacks. It delivers the industry's highest performance protection up to 100Gbps per 1RU and 4Tbps in a single rack.

Disruptions to Internet-facing online services can cripple operations, impact customers and result in major economic losses. SmartWall NTD1100 is an intelligent, always-on platform that inspects traffic, detect threats and blocks attacks against protected network resources, in real-time. It allows service providers, hosting providers and the online enterprise to deploy centralized or distributed threat defense solutions via purpose-built network security appliances that deliver advanced DDoS threat protection.

SmartWall NTD1100 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 protecting against layer 3-7 volumetric DDoS attacks while maintaining full service connectivity and availability and without degrading the delivery of legitimate traffic. In addition, service providers and hosting providers can leverage scale-as-you-grow deployments of SmartWall NTD1100 appliances to deliver high-value, premium DDoS Protection as-a-Service (DDPaaS) to their customers.

This purpose built DDoS mitigation appliance delivers up to 100Gbps performance in a single, 1 RU form-factor. The appliances form the

Featured Product

2 x 100Gb Ethernet Interfaces, with 100Gbps performance in a 1 RU form- factor, scaling to 4Tbps of protection in a single rack

SmartWall® Network Threat Defense 1100

network layer component of the Corero SmartWall Threat Defense System (TDS), an innovative family of security platforms that deliver unparalleled inspection performance, security intelligence and visibility, while providing an unprecedented level of scalability for protection against Denial of Service threats.

Robust & Real-Time Security Coverage

SmartWall NTD1100 provides Layer 3-7 protection against volumetric DDoS attacks for both IPv4 and IPv6 traffic. It leverages the Corero award-winning DDoS defense technology 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 NTD1100 also utilizes the concepts of Flex-Rule and Smart-Rule technology to apply granular closed-loop detecting and blocking filters to very specific attacks with ease. These rules leverage heuristic and closed-loop policy, allowing for rapid creation and deployment, thereby providing customers with the ability to respond rapidly to the evolving nature of sophisticated DDoS attacks.

Industry Scalability and Performance

SmartWall NTD1100 offers new levels of scalability and performance through dynamic threat-level tracking of Internet based IP addresses and their associated flows. 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 enforcement. These high-performance platforms are designed to maintain line-rate throughput, even while under attack.

The modular architecture of SmartWall enables cost-effective scaling in increments from 10Gbps to 100Gbps, as bandwidth and inspection requirements increase. These high-performance appliances can deliver as much as 100Gbps unidirectional throughput in a single rack-unit space.

Turn-key Visibility into DDoS Attacks

Leveraging Splunk software for big data analytics and advanced visualization capabilities, Corero has transformed 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 https://splunkbase.splunk.com/app/1835/ provide comprehensive security visibility into an organization's network activity, for rapid response in combating DDoS 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 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 NTD1100 is performed via secure connection to the Corero Central Management Server (CMS). The CMS includes a dashboard for monitoring threat activity and viewing key security events. The CMS is delivered as a physical appliance, or virtual appliance to run on customer-provided hardware.

SmartWall NTD1100 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 up to 100Gbps unidirectional performance. Multiple SmartWall NTD1100 appliances can be deployed at key control points in the network or centrally combined in various high throughput configurations. 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. Redundant or hot-standby SmartWall NTD1100 appliances can be deployed in high-availability configurations to provide backup. Multiple appliances can also be deployed in dynamic load-balanced configurations to accommodate peak period demands.

SmartWall NTD1100 appliances support both symmetric and asymmetric traffic inspection, enabling flexible network deployment options.

SmartWall Network Threat Defense Deployment Examples

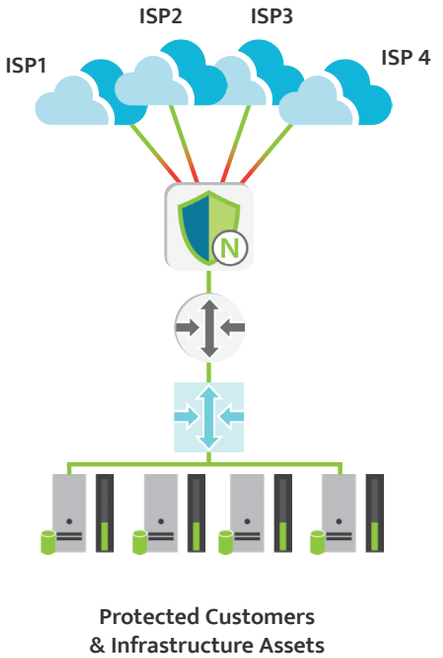

Figure 1: In-line Deployment

The In-line, always-on SmartWall NTD deployment mitigates DDoS attacks in real-time, within seconds vs minutes, while allowing good user traffic to flow uninterrupted.

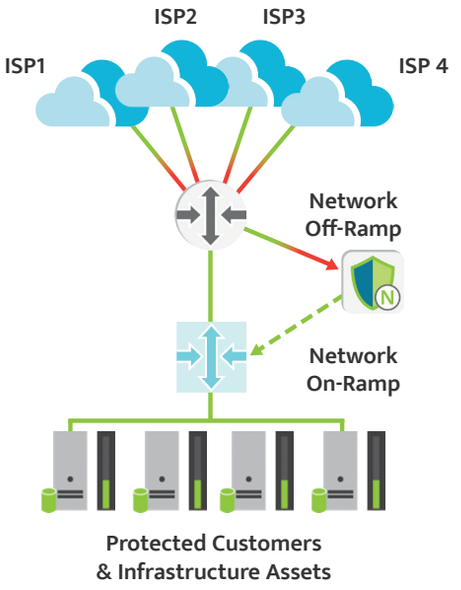

Figure 2: Scrubbing Deployment

The SmartWall NTD Scrubbing deployment can take advantage of third-party monitoring and detection or route management to steer selected traffic to centralized or distributed SmartWall systems for precise mitigation of DDoS attack traffic.

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

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	Command and Control Operations Tunnel Inspection (GRE, MPLS etc.) NTP Monlist Requests Customized Protection with 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 L2-L4 attacks and zero-day network DDoS attacks.

TECHNICAL SPECIFICATIONS

Order Part Number	SmartWall NTD1100
Network Interfaces	
Network Interfaces	2 x 100GE (QSFP28)
Console Port	1 x RJ45 (10/100/11000) and 1 x USB 2.0
Performance	
Maximum Throughput (Gigabits per second)	100 Gbps
Maximum Throughput (Packets Per Second)	90 Million
Jumbo Frames	Yes (9,216 bytes)
Typical Latency[1]	< 0.5 Microsecond
Inspected Latency[1]	< 60 Microseconds
Maximum SYN Flood Protection Rate (packets/second)	90 Million
Attack Mitigation Reaction Time (typical)	< 3 second
Management	
Options	Centralized Management from Physical or Virtual (VMware/KVM) appliance
Interfaces	Web GUI, Command Line, Programmatic API (REST)
Monitoring	SNMP v2/v3* Standard MIB GETs, SYSLOG
Reporting and third-party integration	Syslog for traffic and Security events / REST API for SIEM integration. Analysis application for Splunk integration.
User Authentication	Role-Based Access Control (Active Directory, RADIUS and LDAP)
Physical/Environmental	
Size	1-RU / 44mm (H) x 438 mm (W) x 630 mm (D)
Weight	18 Kgs (39.7 lbs.)
Operating Temperature	0 C to 40 C (32 F to 104 F)
Storage Temperature	-20 C to 70 C (-4 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
Power & Cooling	
Power Feeds	Dual Redundant, Hot-Swappable, AC or DC
AC Input	90 to 264 VAC Auto-Ranging, 47-63Hz
DC Input	43 to 53 VDC
Maximum Power Consumption	650W
Cooling	4 x Independent, Hot-Swappable, Fan trays, with smart control
Compliance & Approvals	CE Class-A, FCC Class A, RoHS

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

About Corero Network Security

Corero Network Security is the leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and online 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