SmartWall®

Threat Defense System - NTD120

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 10/20Gbps up to 2Tbps in a single rack.

✓ **Comprehensive visibility**

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

✓ **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.

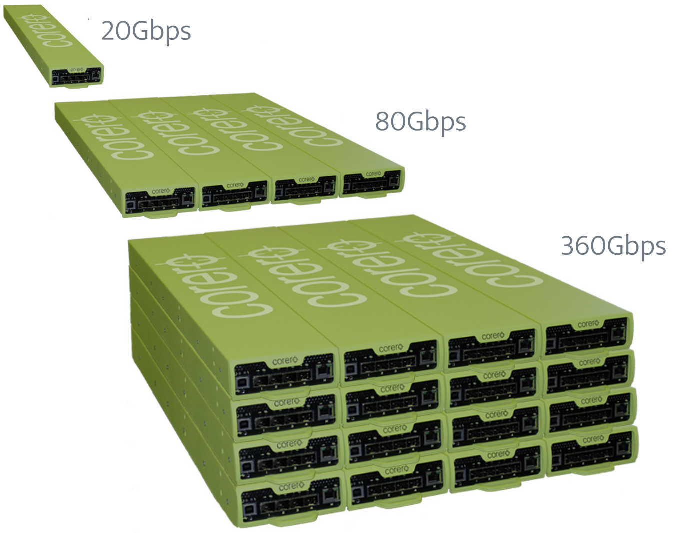
Real-Time DDoS Mitigation

The Corero SmartWall® Network Threat Defense (NTD120) Appliance provides real-time protection against damaging DDoS attacks. 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 NTD120 is an intelligent, always-on platform that inspects traffic, detects threats and blocks attacks targeting protected network resources in seconds, versus minutes or the tens of minutes experienced in legacy mitigation solutions. It allows service providers, hosting providers, and the online enterprise to deploy centralized or distributed real-time protection solutions via purpose-built network security appliances that provide advanced DDoS threat protection.

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 single rack.



SmartWall® Threat Defense System

The SmartWall NTD120 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, service providers and hosting providers can leverage scale-as-you-grow deployments of SmartWall NTD120, enabling them to deliver high-value, premium DDoS Protection as-a-Service (DDPaaS) to their customers.

This purpose built slim line DDoS mitigation 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), innovative family of security platforms that will 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.

Robust & Real-Time Security Coverage

The SmartWall NTD120 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 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 NTD120 also utilizes the concepts of Flex-Rule and Smart-Rule technology to apply granular, closed-loop detecting and blocking filters to a very specific attack 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-Leading Scalability and Performance

The SmartWall NTD120 offers new levels of scalability and performance in a compact and energy-efficient platform. Protection is provided through configurable acceptable access policies supporting packet and connection rate limiting, and geolocation checks, server and service connection limits, protocol checks, as well as blacklist and whitelist capabilities. This high-performance platform is designed to maintain 10Gbps full-duplex or 20Gbps unidirectional throughput (per appliance), even while under attack.

The modular architecture of the SmartWall Network NTD120 enables cost-effective scaling in increments, as bandwidth requirements increase. Four appliances can be deployed in a single 1 RU shelf to deliver a combined 40Gbps full-duplex or 80Gbps unidirectional throughput. 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.

Real-time security engineered dashboards accessible via the Corero SecureWatch® Portal, or via Splunk Apps https://splunkbase.splunk.com/app/1835/ 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 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 NTD120 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.

The SmartWall NTD120 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 NTD 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 NTD120 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.

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

SmartWall Network Threat Defense Deployment Examples

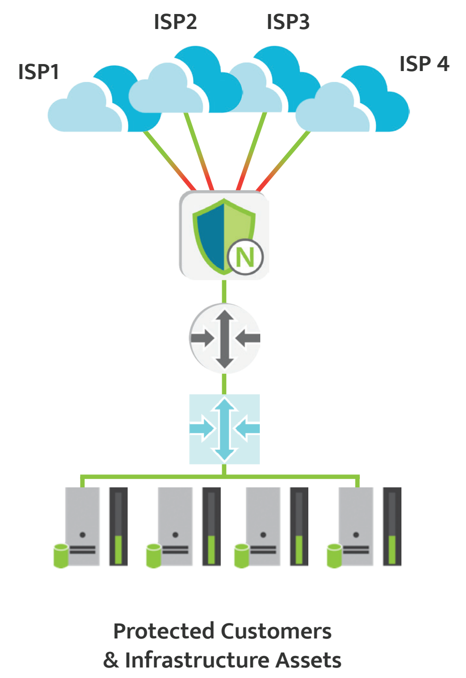


Figure 1: In-line Deployment

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.

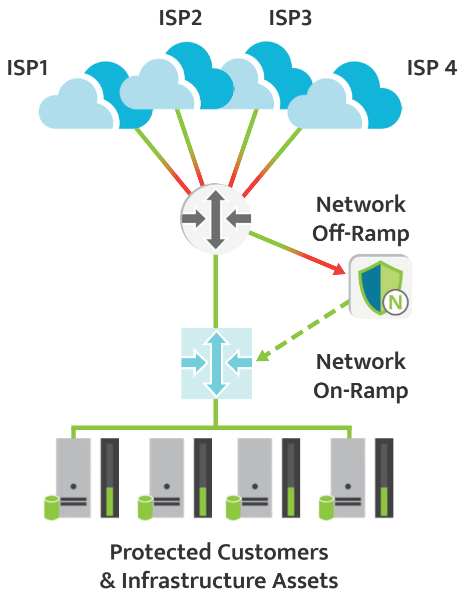


Figure 2: Scrubbing Deployment

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 Network Threat Defense Appliance NTD120**
Regulatory Model Number	6000-10
Network Interfaces	
Pluggable 1G and 10G Ethernet Ports (SFP and SFP+ Modules)	4
Performance	
Maximum Throughput (Gigabits per second)	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 9216	Line rate, 10 Gbps full-duplex or 20Gbps unidirectional
Jumbo Frames	Yes
Typical Latency[1]	<0.5uS
Typical Inspected Latency[1]	< 60 uSec
Maximum SYN Flood DoS Protection Rate	Line-rate
Attack Reaction Time	< 3 seconds
Geolocation lookups per second	1 Million/Sec
IP Addresses Blocked	15 Million/Sec blocked
Device Management	
Management Interfaces	1 10/100/1000 Management Port
Management Station	Physicalor 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
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 and RADIUS)
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)

TECHNICAL SPECIFICATIONS (cont.)

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 & Dual DC PSU
AC Input	100 to 240 VAC Auto-Ranging, 50-60Hz
Maximum Power Consumption	<200W
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
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 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