Corero SmartWall® TDS

Real-time, Automatic and Highly-Scalable DDoS Defense Solutions

The Corero SmartWall® Threat Defense System leads the industry with real-time protection that stops volumetric DDoS attacks faster and more effectively. SmartWall delivers the highest performance available in a compact, energy-efficient form factor, for scalability up to 4Tbps in a single rack.

DDoS attacks have businesses and government agencies around the world concerned about outages to their web-based services which could impact customers, cripple operations and result in major economic losses. Well publicized volumetric attacks that harness vulnerable IoT devices have raised awareness of the scale of the DDoS problem. But the majority of modern DDoS attacks last less than 10 minutes in duration, are less than 5Gbps in size and can hit networks across multiple vectors.

These more calculated DDoS attacks can be just as damaging and slip under the radar of legacy DDoS attack protection that can only detect larger saturation attacks and has no visibility into advanced attacks.

Digital Enterprises, Internet Service Providers and Hosting Providers can spend thousands of operational hours annually on the manual intervention required by legacy DDoS mitigation solutions to defeat advanced attacks. SmartWall Threat Defense System automatically determines what traffic is legitimate during DDoS attacks and delivers it uninterrupted, while simultaneously eliminating unwanted DDoS traffic and preventing outages.

Avoid the Protection Gap of Legacy DDoS Solutions

SmartWall® TDS delivers intelligent DDoS mitigation that inspects traffic and automatically defends against DDoS attacks, typically in under a second.

Protect uptime. DDoS attacks are a security and availability issue. SmartWall ensures continuity for organizations that have rigid SLA's for service uptime and availability and cannot afford latency or outages related to DDoS.

Granular Attack Visibility. Our industry-leading analytics drill down on attacks so our customers can better understand the types of attacks they are experiencing for cross-network threat intelligence.

Be Ready for ALL Attack Types. Bursty, volumetric, short duration, Botnets including IoT, and pulsing attacks. Legacy solutions can no longer keep up with the evolving and sophisticated DDoS threat landscape.

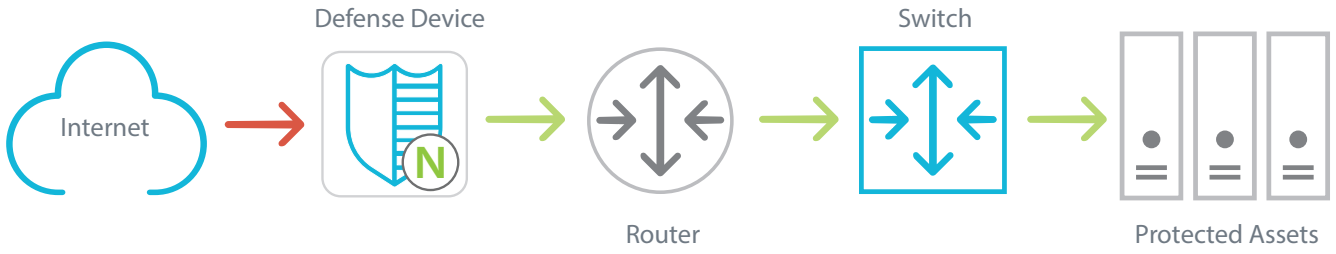
Defeat Multi-vector attacks. Many attacks Corero helps prevent are multi-vector, where attackers use DDoS as a distraction technique for more nefarious data exfiltration or breach activity.

Proactive DDoS Protection- with Attack Visibility Across the IT Ecosystem

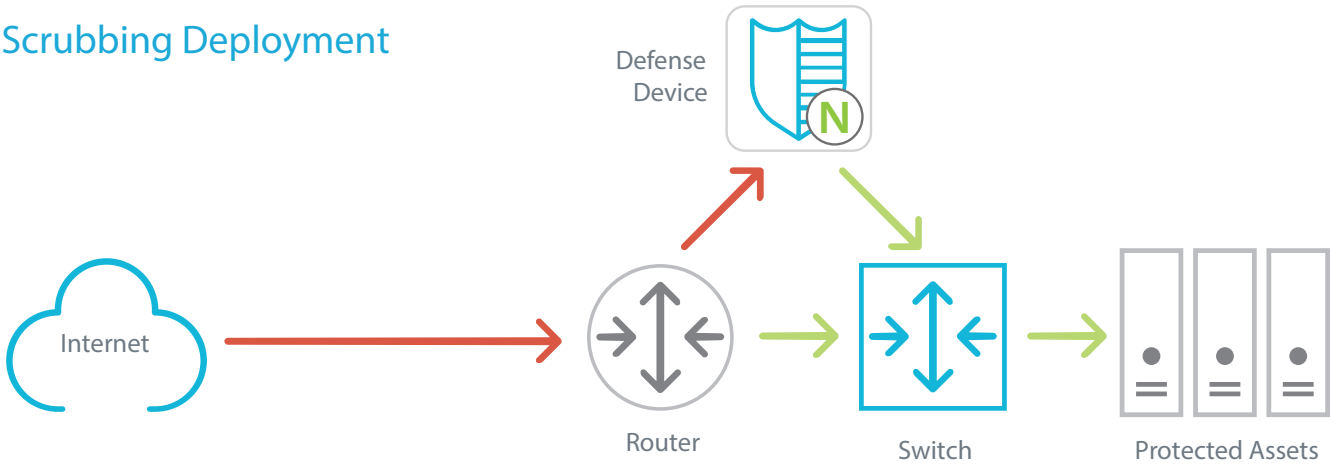
SmartWall® Threat Defense devices provide the best price/performance for digital enterprises, service providers and hosting providers with real-time, automated traffic inspection and mitigation compared to the minutes, or tens of minutes, experienced with legacy mitigation solutions. Our purpose-built DDoS network defense devices can be deployed in a centralized or distributed mode.

Multi-vector, reflection and other DDoS attack types pose security and service availability problems, yet they are still having an impact - even against security-conscious organizations. Traditional mitigation solutions cannot keep pace with the everyday DDoS attack which can't be defeated with Firewalls, IPS, IDS, WAFs or cloud scrubbing models. A dedicated approach to DDoS detection and mitigation is required.

Inline Deployment



Scrubbing Deployment



Key Benefits

Comprehensive Visibility

SmartWall leverages big data analytics to deliver sophisticated and comprehensive visibility, reporting and alerting capabilities for clear, actionable intelligence on the DDoS attack activity happening across the network.

Automatic Protection

Automatically mitigates a wide range of DDoS attacks, without operator intervention, maintaining full connectivity to avoid disrupting the delivery of legitimate traffic - stopping attacks faster.

Rapidly detect DDoS attacks of all sizes

SmartWall fills the perception gap, by not only blocking the very large volumetric attacks commonly associated with DDoS, but also detecting and surgically blocking the more common and much smaller attacks which use the same vectors - many of which are too small or short in duration to be detected by legacy solutions.

Cloud/On-Premise Hybrid Scalability

Can complement or replace legacy or cloud based mitigation solutions.

In-Line or Scrubbing Deployments

Physical or virtual flexibility with always-on or scrubbing center deployment options to best fit the attack mitigation needs of your network.

Accurately and automatically allows the good and stops the bad

Good traffic is able to flow uninterrupted, enabling services and applications to stay online, while DDoS traffic is surgically blocked before it has the chance to cause any damaging effects.

Managed Services Enabler

Service and hosting providers can enhance security service offerings with real-time, automatic DDoS protection to their customers without 'blackholing' or disrupting legitimate customer traffic.

Reduced Operating Costs

Automated DDoS response from Corero ties together attack events, significantly reducing human intervention and false positives for reduced operational costs and lowest TCO.

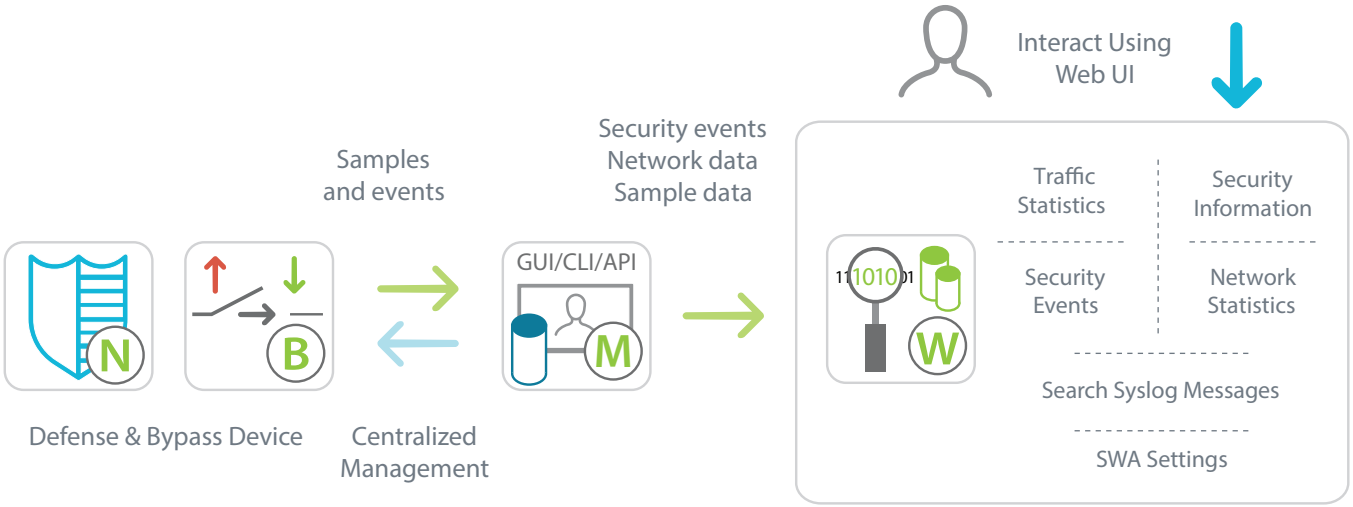
Security policy enforcement

With proactive traffic inspection, our detection and real-time mitigation solutions enforce security policies and prevent volumetric layers 3-7 DDoS attacks for both IPv4 and IPv6 traffic.

Centralized Management and Analytics

View traffic information for greater visibility into the DDoS attacks targeting your network:

1. Gather forensic information to help you tune network and security policies
2. Analyze the blocked and allowed traffic seen during attacks against your network
3. All events are stored and indexed in web-based application and available externally, via syslog
4. Information is presented in real-time or historical charts and tables



TDS Security Coverage

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

Volumetric DDoS

TCP Flood
UDP Flood
UDP Fragmentation
SYN Flood
ICMP Floods

Reflective DDoS

NTP Monlist Response Amplification
SSDP/UPnP Responses
SNMP Inbound Responses
Chargen Responses
DNS Amplification
Connectionless LDAP (CLDAP) Amplification

Custom Protection

Botnet protection

Blacklisting or Whitelisting of IP Addresses
Managed lists for Reputation/GEO blocking
TCP/UDP port-based attacks

Rate Limiting Policies

Cloud Mitigation and RTBH signalling

Flex-Rules - Programmable filters using the Berkley Packet Format (BPF) syntax

Address a variety of volumetric attack vectors, from reflective through to those leveraging specific payloads (Teamspeak, RIPv1, netbios)

Smart-Rules – Machine-learning heuristic and behavioral analysis engine

Automatically track and rate limit L2-L4 Attacks, including zero-day

Technical Specifications

SmartWall TDS	NTD120	NTD280	NTD1100
Network Interfaces	4 x 1/10G SFP+	8, 12 or 16 x 1/10G SFP+	2 x 100G QSFP28 or, 2 x 100G LR4 zero-power bypass
Management Port	1 x 10/100/1000 RJ45		
Console Port	N/A	1 x RJ45 Serial	

Performance

Maximum Throughput (Gigabits per second)	20 Gbps	80 Gbps	100 Gbps
Maximum Throughput (Packets Per Second)	30 Million	120 Million	150 Million
Jumbo Frames	Yes (9,216 bytes)		
Typical Latency[1]	< 0.5 Microsecond		
Inspected Latency[1]	< 60 Microseconds		
Maximum SYN Flood Protection (packets/second)	30 Million	120 Million	120 Million
Attack Mitigation Reaction Time (typical)	Sub-Second		

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

Management

Centralized Management	Object-oriented management from a Physical or Virtual (VMware/KVM) appliance
Interfaces	1 x RJ45/Virtual (10/100/1000) Ethernet
Web-Based GUI	HTTP/HTTPS Access Through the Management Station
Command Line Interface	SSH Access Through the Management Station
Programmatic API	JSON-Based REST Through the Management Station
Remote Monitoring	SNMP v2/v3* Standard MIB GETs, SYSLOG
Software Upgrade	Remotely Upgradeable Image and Configuration Stored on Internal SSD
Security Dashboards	Link utilization (Gbps/PPS), Attack targets, Attack vectors, Alerts, Detailed drilldowns, Top IPs/Ports/TTLs/Packet Sizes, Export to PCAP
Reporting and third-party integration	Syslog for traffic and Security events with REST API for SIEM integration. Corero Analysis application for Splunk integration.
User Authentication	Role-Based Access Control (LDAP/Active Directory and RADIUS)

Technical Specifications

Physical/Environmental	NTD120	NTD280	NTD1100
Size	1-RU / 44m (H) x 108 mm (W) x 604mm (D)	1-RU / 44mm (H) x 438 mm (W) x 630 mm (D)	
Weight	3.6 Kgs (7.9 lbs.)	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		
Tamper Protection	Tamper-Evident Seal		

Power/Cooling			
Power Feeds	Single Internal AC PSU, or Dual DC PSU	Dual Redundant, Hot-Swappable, AC or DC PSU	
AC Input	100 to 240 VAC Auto-Ranging, 50-60Hz	90 to 264 VAC Auto-Ranging, 47-63Hz	
DC Input	43 to 53 VDC		
Maximum Power Consumption	<150W	330W	340W
Cooling	Internal N+1 Fans	4 x Independent N+1, Hot-Swappable, Fan trays, with smart fan control	

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(CIS¬PR24:1997 +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

Technical Specifications - vNTD

Network Interfaces
2 x 10G Virtual Interfaces

Management Port
1 x Virtual (10/100/1000)

Performance

Maximum Throughput (Gigabits per second)
10 Gbps (deployed on 8 x Intel E5-2695, or equivalent, pinned CPU cores running KVM)

Maximum Throughput (Packets Per Second)
15 Million (deployed on KVM)

Jumbo Frames
Yes (9,216 bytes)

Typical Latency[1]
< 0.5 Microsecond

Inspected Latency[1]
< 60 Microseconds

Maximum SYN Flood Protection Rate (packets/second)
15 Million (Line-rate)

Attack Mitigation Reaction Time (typical)
Sub-Second

Management

Centralized Management
Physical or Virtual (VMware/KVM) appliance

Web-Based GUI
HTTP/HTTPS Access Through the Management Station

Command Line Interface
SSH Access Through the Management Station

User Authentication
Role-Based Access Control (LDAP/Active Directory and RADIUS)

Programmatic API
JSON-Based REST Through the Management Station

Remote Monitoring
SNMP v2/v3* Standard MIB GETs, SYSLOG

Software Upgrade
Remotely Upgradeable Image and Configuration Stored on customer VM

Security Dashboards
Link utilization (Gbps/PPS), Attack targets, Attack vectors, Alerts, Detailed drilldowns, Top IPs/Ports/TTLs/Packet Sizes, Export to PCAP

Reporting and third-party integration
Syslog for traffic and Security events with REST API for SIEM integration. Corero Analysis application for Splunk integration.

Physical/Environmental

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 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