Corero SmartWall® TDS

DDoS Defense Appliances

SmartWall Threat Defense System (TDS) appliances deliver full line-rate performance for the fastest, always-on, or scrubbing DDoS protection. Available in efficient physical and virtual form-factors, they can be deployed directly in the datapath without the risk of dropping or delaying legitimate traffic.

The DDoS threat landscape continues to have businesses and government agencies around the world concerned about outages of their online services which could impact customers, cripple operations and result in major economic losses. Well publicized volumetric attacks that harness vulnerable IoT devices have recently raised awareness of the scale of the DDoS problem but the majority of modern DDoS attacks actually last less than 10 minutes in duration, are less than 5Gbps in size and can hit networks with multiple vectors. These more sophisticated attacks can be just as damaging and slip under the radar of legacy DDoS protection that can only detect traditional attacks and has limited visibility into the latest DDoS vectors.

The sophistication of DDoS also continues to evolve each year. These attacks present a more challenging detection and mitigation task due to their varying amplitude, ports and protocols. The average attack is short, meaning real-time detection and mitigation are an essential requirement for comprehensive protection.

Avoid the Protection Gap of Legacy DDoS Solutions

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

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

Granular Visibility
Industry-leading analytics drill down on attacks so you can better understand the types of attacks and deliver increased threat intelligence.

Comprehensive Defense
Protection from volumetric, state exhaustion, short duration, IoT Botnet, Carpet Bomb, and pulsing attacks with available cloud hybrid protection, to guard against the largest saturating attacks.

Advanced Protection
Many attacks that Corero mitigates are now multi-vector, where attackers combine one or more volumetric, or state exhaustion techniques sequentially, in an attempt to evade detection or mitigation.

corero

Proactive DDoS Protection with Comprehensive Attack Visibility

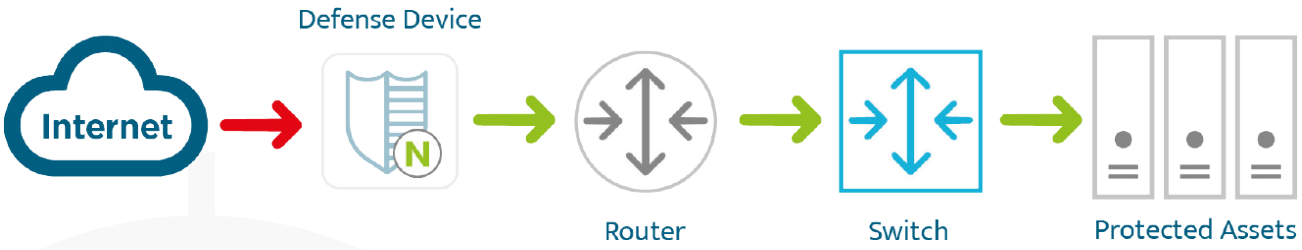
SmartWall® Threat Defense System provides the best DDoS protection for digital enterprises, service providers and hosting providers with real-time, automated traffic inspection and mitigation. Corero's solution does this in seconds, compared to the minutes, or tens of minutes experienced with legacy solutions. Our purpose-built DDoS network defense devices can be deployed in a centralized or distributed mode.

Proactive DDoS protection is a critical cybersecurity practice to defend against loss of service availability. The continuously evolving everyday DDoS attacks cannot be effectively defeated with traditional Internet gateway security solutions, such as firewalls, Intrusion Prevention Systems and the like. Similarly, cloud-based DDoS protection services alone cannot achieve successful mitigation of the frequent, short duration attacks that are impacting organizations every day.

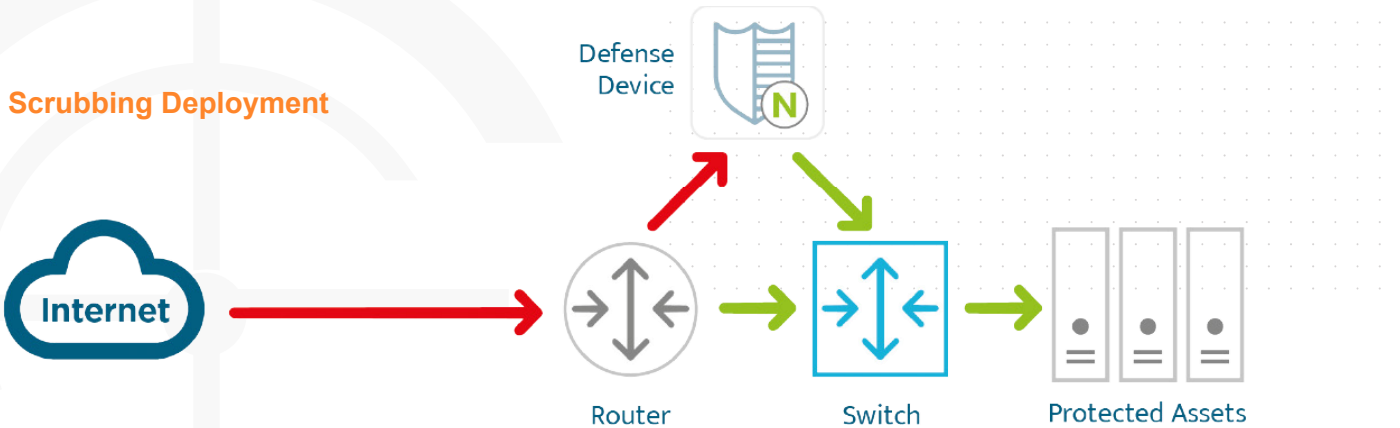
SmartWall's protection includes patented mechanisms which accurately detect and automatically stop volumetric and state exhaustion DDoS attacks, to prevent downtime. SmartWall protections are continually enhanced based on the experience of Corero's SOC team analyzing real-world attacks across our diverse customer base. The team leverages SmartWall's own comprehensive visibility and analytics capabilities, enriched using behavioral and machine analysis, to deliver SmartWall's industry-leading DDoS protection.

SmartWall supports flexible deployment options to best suit the environment being protected. The fastest, most effective, protection is delivered with appliances deployed always-on at all ingress points to the network, either in-line with Internet connections, or the in-datapath, connected to edge routers with inbound traffic entering via the SmartWall appliances. SmartWall also supports traditional scrubbing deployments with built-in flow-based detection and traffic redirection capabilities.

Inline Deployment



Scrubbing Deployment



corero

Key Benefits

Comprehensive Visibility
SmartWall leverages 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.

Rapidly Detect DDoS Attacks of all Sizes
SmartWall fills the protection gap, by not only blocking the large volumetric attacks commonly associated with DDoS, but also detecting and surgically blocking the more common and smaller attacks which use the same vectors - many of which are too small or short in duration to be mitigated by legacy solutions.

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.

Reduced Operating Costs
Automated DDoS response from Corero significantly decreases human intervention and false positives for reduced operational costs and lowest TCO.

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.

Hybrid DDoS Protection
Enhances cloud-only solutions with highly accurate, real-time, on-premises protection.

Always-On or Scrubbing Deployments
Physical or virtual appliance flexibility in-line, or in-datapath, at the edge, or out-of-band scrubbing with fast and accurate sampled packet, or flow-based detection that redirects attack traffic for mitigation.

Managed Services Enabler
Hosting Providers, MSPs, MSSPs and ISPs can enhance security service offerings by delivering real-time automatic DDoS protection as-a-service to their customers with upstream signaling capabilities enabling them to protect their customers without “blackholing” or disrupting legitimate traffic.

Security Policy Enforcement
Always-on traffic inspection, and real-time mitigation enforces security policies that prevent volumetric layers 3-7 DDoS attacks for both IPv4 and IPv6 traffic.

Centralized Management and Analytics

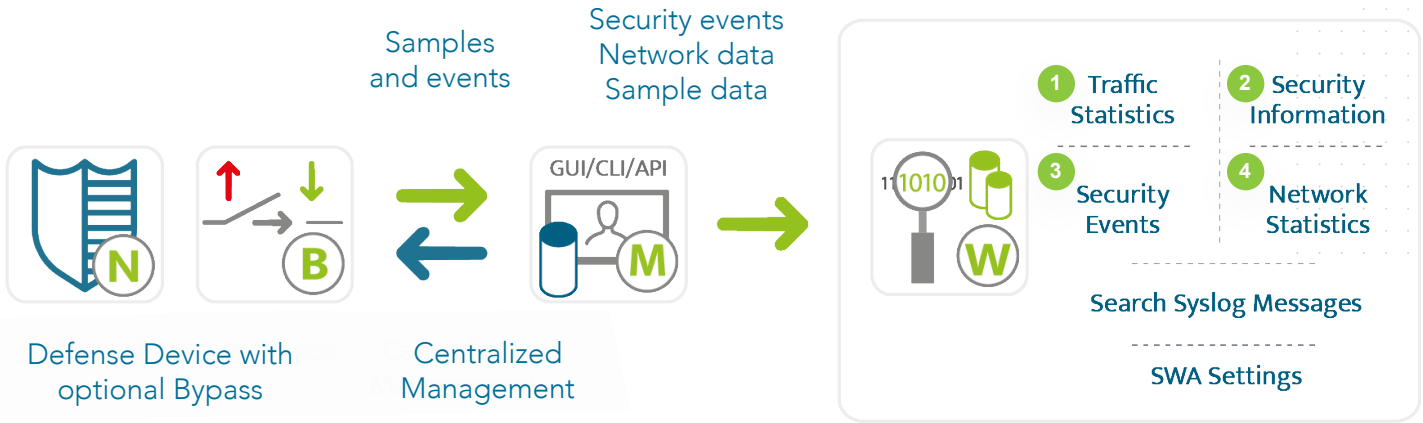
Corero SecureWatch Analytics delivers comprehensive visibility into DDoS attacks with easy-to-read dashboards delivering actionable intelligence.

1 Monitor in Real-Time
Information is presented in real-time or historical charts and tables

2 Analyze Attacks
Analyze the blocked and allowed traffic seen during attacks

3 Optimize Protection
Gather traffic information to help you fine-tune policies

4 Enhance Threat Intelligence
All events are stored and indexed in web-based application and available externally, via syslog



TDS Security Coverage

Protection Capabilities

- Defends attacks to Single/Multiple IPs and Subnets
- Smart-Rules – Patented high-performance heuristics-based engine that automatically detects & blocks volumetric DDoS attacks, including zero-day
- Flex-Rules - Programmable filters using the Berkeley Packet Filter (BPF) syntax with Corero enhancements
  - » Address a variety of volumetric attack vectors, from reflective through to those leveraging specific payloads (Teamspeak, RIPv1, netbios)
- Botnet/Source Flood detection and blocking
- Intelligent automatic Fragment blocking
- IP Address, Country and AS Number Block/Allow Lists
- TCP/UDP port-based
- Rate Limiting Policies
- Cloud Mitigation and BGP RTBH/FlowSpec signaling

Volumetric DDoS

- TCP Flood
- UDP Flood
- UDP Fragmentation
- SYN Flood
- ICMP Floods
- Carpet Bombing

Reflective Amplification DDoS

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

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

corero

Technical Specifications

SmartWall TDS	TDS 220	NTD 280	NTD 1100
Network Interfaces	4 x 1/10G SFP/SFP+	4, 8, 12 or 16 1/10G SFP/SFP+ or 2 or 4 10G LR or SR zero-power bypass	2 x 100G QSFP28 or 2 x 100G LR4 zero-power bypass
Management Port	1 x 10/100/100 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 Latency1	<0.5 Microseconds		
Inspected Latency1	< 60 Microseconds		
Max SYN Flood Rate (Packets per second)	30 Million	120 Million	120 Million
Attack Mitigation Reaction Time (typical)	Sub-Second		

Management		
Mangement	Integrated Object-Oriented Management	Centralized Object-Oriented Management from a Separate Physical or Virtual (VMware/KVM) Appliance
Interfaces	1 x 10/100/1000 RJ45/Virtual Ethernet	
Web-Based GUI	Integrated HTTP(S) Access	HTTP(S) Access Through the Management Station
Command Line Interface	Integrated SSH Access	SSH Access Through the Management Station
Programmatic API	Integrated JSON-Based REST	JSON-Based REST Through the Management Station
Remote Monitoring	SNMP v2/v3* Standard MIB GETs, SYSLOG	
Software Upgrade	Remotely Upgradeable Image & 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 & 3rd Party Integration	SYSLOG for Traffic & Security Events with REST API for SIEM Integration. Corero Analysis Application for Splunk Integration.	
User Authentication	Role-Based Access Control (LDAP/Active Directory & RADIUS)	

corero

Technical Specifications

Physical / Environmental

Size	1-RU / 44 mm (H) x 482 mm (W) x 729 mm (D)	1-RU / 44 mm (H) x 438 mm (W) x 630 mm (D)
Weight	17.64 Kgs (38.9 lbs.)	18 Kgs (39.7 lbs.)
Operating Temperature	5°C to 40°C (41°F to 104°F)	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 65°C (-40°F to 149°F)	-20°C to 70°C (-4°F to 158°F)
Humidity	5% to 95% Non-Condensing	
MTBF Rating	N/A	>100,000 Hours (25°C Ambient)
Operating Altitude	0-10,000 Feet	
Tamper Protection	N/A	Tamper-Evident Seal

Power / Cooling

Power Feeds	Dual Redundant Hot-Swappable AC PSUs	Dual Redundant, Hot-Swappable, AC or DC PSUs	
AC Input	120 to 240 VAC Auto-Ranging, 50-60Hz	90 to 264 VAC Auto-Ranging, 47-63Hz	
DC Input	N/A	43 to 53 VDC	
Maximum Power Consumption	550W	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 PRE24:1997+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 6100-4-6:1996 +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

NTD Virtual Edition

Network Interfaces
4 x 10G Virtual Ethernet

Management Port
1 x 10/100/1000 Virtual Ethernet

Performance

Maximum Protect 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)

Maximum Detect Throughput (Packet/sFlow samples or NetFlow records)
0.5 Million/sec

Typical Latency[1]
< 0.5 Microsecond

Inspected Latency[1]
< 60 Microseconds

Attack Mitigation Time
Sub-Second (typical)

Maximum SYN Flood Protection Rate (Packets/Second)
15 Million (Line-Rate)

Jumbo Frames
Yes (9,216 bytes)

Physical Environment

Hypervisors
KVM running on Redhat Enterprise 7+, CentOS 7+ or Ubuntu 16.04+
VMware ESXi 6.5+

Minimum Requirements
16GB Memory, 20GB Disk

Network Interfaces
10G - XL710 NIC
100G - E810 NIC

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

corero