corero [NETWORK SECURITY]

SMARTWALL ONE ™

DATASHEET _

Step Beyond the Ordinary with SmartWall ONE

Designed with scalability at its core, our fully automated system delivers unrivaled ease of use, empowering you to defend your business against the most relentless DDoS attacks with confidence. SmartWall ONE isn't merely a shield; it's your fortress, meticulously crafted to ensure your network's security and resilience.

Multi-Site Resiliency

DDoS protection should be as resilient as your network. SmartWall ONE delivers adaptive, multi-site resilient protection—enforcing policies in real time across locations. Even during a fiber cut, power loss, or full site failure, mitigation continues without delays or manual reconfiguration.

Future-Proof Scalability & Flexibility

Imagine your security solution as building blocks. With our modular appliances, you have the freedom to add more blocks (up to two 400G modules) or mix and match (one 100G with one 400G, or two 100G modules) as your business grows. This way, scaling up doesn't mean starting over.

Granular Visibility

Tap into the mind of your attackers. Our top-notch analytics offer you a deep dive into the attack patterns. This isn't just data; it's actionable intelligence, empowering you to beef up your defenses with precision.

All-Around Protection

We'll keep your network safe from threats including volumetric attacks, state exhaustion, rapid-fire short-duration strikes, IoT botnets, carpet bombings, pulsing tactics, and DNS floods. Plus, our sophisticated hybrid cloud defense acts as an impenetrable barrier against the most severe attacks, keeping your network not just safe, but consistently operational without a hitch.

DDoS PROTECTION APPLIANCES

Stay Ahead with SmartWall ONE

It seems like every year DDoS attacks get a bit more cunning and complex. They're not just bigger; they're sneakier, targeting all sorts of ports and protocols with ever-changing tactics. And even though they tend to hit fast and vanish quicker, that only cranks up the pressure for real-time detection and instant action. So, what's your move? You need a DDoS protection that's not just capable but always on its toes, ready to defend at a moment's notice.

That's why you should equip your network with SmartWall ONE.

SmartWall ONE is a fast, ultra-responsive, and fully automated DDoS protection solution available as both physical appliances and virtual machines. Thanks to its flexible, software-based design, SmartWall ONE integrates seamlessly into your network and existing architecture. This adaptability ensures that regardless of your network infrastructure, you can enjoy peace of mind and the freedom to focus on your core business activities, with the assurance of uninterrupted service availability.

The Power to Scale

Our speed agnostic SmartWall ONE solution was built to scale, to grow as your company grows. Excitingly, we've expanded our capabilities with the launch of our cutting-edge 400G Network Threat Defense (NTD) appliances. These additions ensure that SmartWall ONE can be deployed on-premises, either as a physical or virtual software appliance, aligning with the latest in networking throughput advancements. This means not only meeting, but exceeding, bandwidth demands with unparalleled agility.

Software/Virtual Implementation

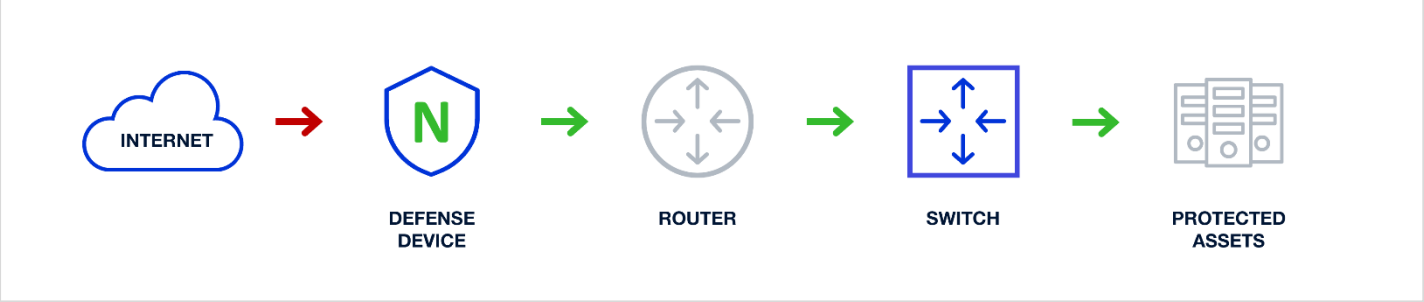
Ideal for cloud or data center environments, DDoS protection is implemented as a software instance on a virtual machine or cloud instance, offering a scalable and flexible solution. This deployment option not only allows for rapid deployment and easy scalability but also helps reduce operational costs by eliminating the need for dedicated hardware, additional rack space, and reducing energy consumption. It adapts quickly to changing protection needs without requiring physical infrastructure changes, making it an efficient choice for organizations looking to optimize their resource usage while maintaining high levels of protection.

Hardware Implementation

No matter if you're using our hardware or sticking with your own, this robust solution is installed and operates within your physical network infrastructure, offering direct control over DDoS protection measures. The latest Corero protection appliance introduces enhanced modularity, allowing for two network modules that enable service providers to switch between configurations such as 2 x 400G, 2 x 100G and 1 x 400G, or 4 x 100G interfaces. This level of modularity provides unprecedented flexibility, and futureproofing, enabling the adaptation of the protection infrastructure to varying network demands and capacity requirements without the need for a complete system overhaul.

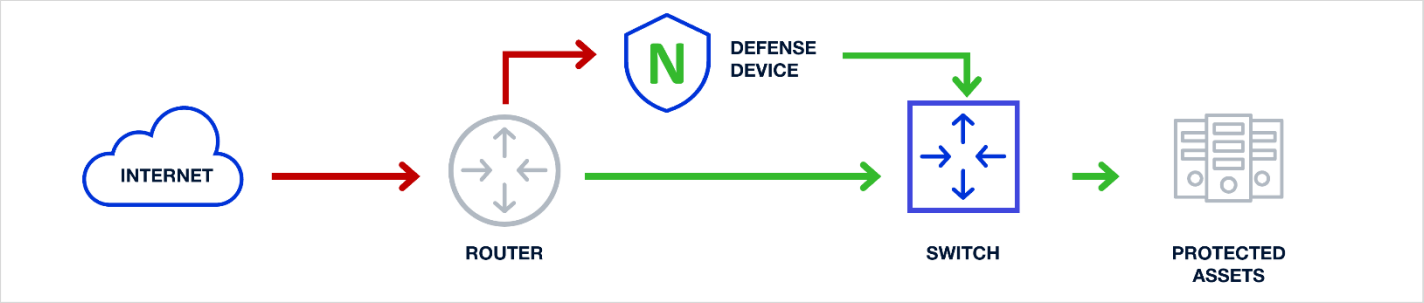
SmartWall ONE supports flexible deployment options to best suit the environment being protected. The fastest, most effective protection is delivered with appliances deployed always-on at all ingress points to the network, either inline with internet connections, or in the data path, connected to edge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

Inline Deployment



N Network Defense Device

Data Path & Scrubbing Deployments



N Network Defense Device

Difference-Making Benefits

See Everything, Miss Nothing

We use advanced data analytics to give you a crystal-clear picture of what's happening, making it super easy to spot and understand DDoS attack patterns. You get all the details you need, minus the headache.

Quick on the Draw Against DDoS

We're always on guard, blocking those massive, headline-making attacks and the sneaky, smaller ones that other systems might miss.

Sorting The Good from The Bad, Accurately and Automatically

We'll halt malicious DDoS traffic in its tracks, stopping it cold before it has a chance to disrupt your operations. And the cherry on top? We do all this seamlessly, ensuring your services run without a hiccup.

Cut Costs, Not Corners

Our automated defenses mean you spend less time and money dealing with DDoS headaches. SmartWall ONE keeps things running so smoothly, you'll wonder why you ever put up with anything less.

Set It and Forget It Protection

We'll handle DDoS attacks automatically, keeping everything connected and moving without you having to lift a finger.

On-Prem or Hybrid Protection

Enhance your cloud-only solution with our highly accurate, real-time, on-premises protection. Our hybrid protection is so seamless, you won't even know it's there.

Flexible to Fit Your Needs

No matter the deployment, SmartWall ONE molds to fit your setup. Physical, virtual, in the thick of it, or on the sidelines—we've got you covered, ensuring attacks are stopped before they can do any damage.

Amplify Your Profits and Your Services

If you're a service provider, SmartWall ONE is your golden ticket to offering top-tier, real-time DDoS protection as a service. Enhance your revenue streams while securing your customers' operations against disruptions, all without affecting their legitimate traffic.

Seamless Availability

Automatically enforces DDoS mitigation across distributed locations—no delays, no reconfigurations, no single point of failure.

Keeping an Eye on Things: Your DDoS Dashboard

SmartWall ONE SecureWatch Analytics is your all-seeing eye for DDoS attacks. It's a dashboard that not only makes sense of all the chaos but also tells you exactly what to do about it. Easy, right? You get all the insights, without having to sift through the noise.

Monitor in Real-Time

Information is presented in real-time or historical charts and dashboards.

Optimize Protection

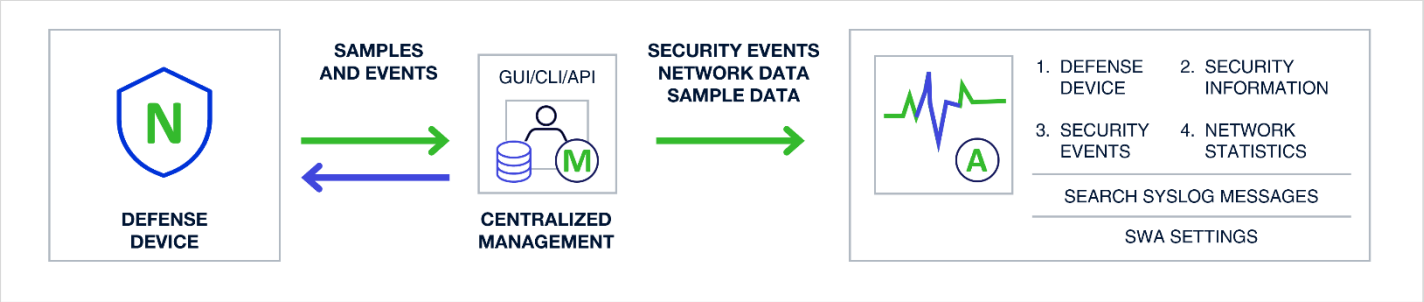
Actionable intelligence that helps you enhance your security policies.

Analyze Attacks

Drill down for detailed insight into blocked and allowed traffic seen during an attack.

Enhanced Threat Intelligence

All events are securely stored, indexed, and made accessible for analytics externally to other security tools via APIs and syslog, enhancing integration and visibility.



N Network Defense Device | **M** Provider Service Management | **W** DDoS Traffic Analysis

Appliance Security Coverage

Custom Protection

- Defends attacks to single/multiple IPs and Subnets
- Smart-Rules – Patented high-performance heuristics-based engine that automatically detects and 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 using specific payloads (TeamSpeak, RIPv1, NetBIOS)
- DDoS Intelligence predictive protection feed
- Botnet/source flood detection and blocking
- Intelligent automatic fragment blocking
- TCP/UDP port-based
- Rate limiting policies
- Cloud mitigation and BGP RTBH/FlowSpec signaling.

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
- DNS Infrastructure NXDOMAIN *water torture*

Volumetric DDoS

- TCP flood
- UDP flood
- UDP fragmentation
- SYN flood
- ICMP floods
- Carpet bombing

Reflective Amplification DDoS

- NTP monlist response amplification
- DNS query amplification
- Connectionless LDAP (CLDAP)
- SSDP/UPnP responses
- SNMP inbound responses
- CHARGEN responses

Technical Specifications

SmartWall ONE	NTD 280	NTD 1100	NTD 3400
Network Interfaces	16 x 1/10G SFP/SFP+ or 2 / 4 x 10G LR zero-power bypass	2 x 100G QSFP28 or 2 x 100G LR4 zero-power bypass	1 / 2 x 400G OSFP DR4 or 2 / 4 x 100G with QSFP28 / LR4 zero-power bypass
Management Port	1 x 10/100/100 RJ45		
Console Port	1 x RJ45 Serial		
Performance			
Maximum Throughput (Gigabits per second)	80 Gbps	100 Gbps	800 Gbps
Maximum Throughput (Packets per second)	100 Million	150 Million	400 Million
Typical Latency[1]	<0.5 Microseconds		
Inspected Latency[1]	< 60 Microseconds		
Max SYN Flood Rate (Packets per second)	100 Million	100 Million	400 Million
Attack Mitigation Reaction Time (typical)	Sub-Second		
Management			
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	HTTP(S) 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 & Confguration 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		
Physical / Environmental			
Size	1-RU / 44 mm (H) x 438 mm (W) x 630 mm (D)		1-RU / 44mm (H) x 438 mm (W) x 650 mm (D)
Operating Temperature	0°C to 40°C (32°C to 104°C)		
Storage Temperature	-20°C to 70°C (-4°C to 158°C)		
Humidity	5% to 95% Non-Condensing		
MTBF Rating	>100,000 Hours (25°CAmbient)		
Operating Altitude	0-10,000 Feet		
Tamper Protection	Tamper-Evident Seal		
Power / Cooling			
Power Feeds	Dual Redundant, Hot-Swappable, AC or DC PSUs		
AC Input	90 to 264 VAC Auto-Ranging, 47-63Hz		
DC Input	43 to 53 VDC		
Maximum Power Consumption	330W	340W	580W
Cooling	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		

NTD Virtual Edition

Network Interfaces 4 x 10/100/400G Virtual Ethernet	**Management Port** 1 x 10/100/1000 Virtual Ethernet

Performance

Maximum Protected Throughput (Gigabits per second) 400Gbps (on 32 x CPU cores running KVM)	**Maximum Throughput (Packets per second)** 80 Million (deployed on KVM)	**Maximum Detect Throughput (Packet/s-Flow samples or NetFlow records)** 0.5 Million per second
Typical Latency[1] < 0.5 Microsecond	**Inspected Latency[1]** < 60 Microseconds	**Attack Mitigation Time** < 60 Microseconds
Maximum SYN Flood Protection Rate (Packets/Second) 80 Million (Line-Rate)	**Jumbo Frames** Yes (9,216 bytes)	

Physical Environment

Hypervisors KVM running on Red Hat 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 / ConnectX-5/6 NIC 400G - ConnectX-7 NIC

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