corero [ THE DDoS PROTECTION SPECIALISTS ]

# SMARTWALL® ONE DATASHEET _

## Avoid the Protection Gap of Legacy DDoS Solutions

SmartWall ONE delivers intelligent DDoS protection 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 ONE ensures continuity for organizations that require SLAs for service uptime and availability without latency or service interruptions.

### Granular Visibility

Industry-leading analytics drill down on attacks so you can better under- stand them and deliver increased threat intelligence.

### Comprehensive Defense

Protection from volumetric, state exhaustion, short duration, IoT botnets, carpet bomb/spread spectrum, and pulsing attacks with available cloud hybrid protection to guard against the largest saturating attacks.

### Advanced Protection

We protect against multi-vector, attacks, which combine one or more volumetric, or state exhaustion techniques sequentially, in an attempt to evade detection or mitigation.

## DDoS PROTECTION APPLIANCES

SmartWall ONE 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 data path 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 protection 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.

### Flexible Hybrid or Provider-Based Protection

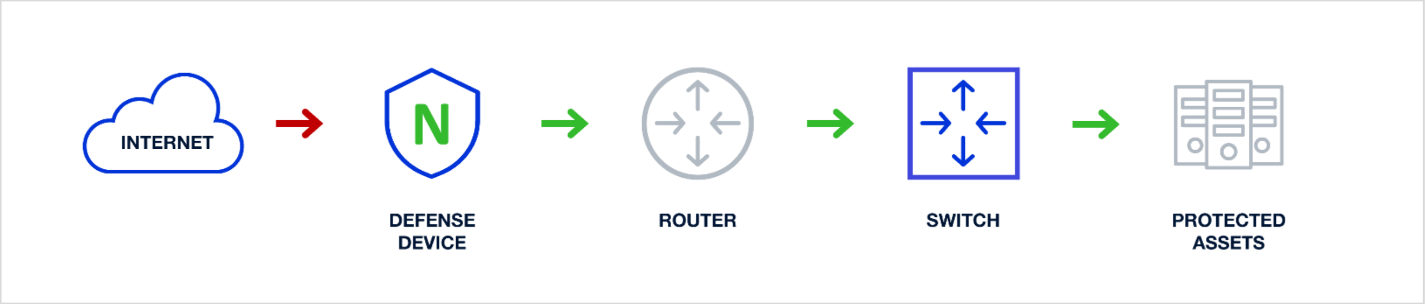
SmartWall ONE provides the best DDoS protection for digital enterprises, service providers, and hosting providers with flexible, automated traffic inspection and protection. Our solution does this in seconds, compared to the minutes, or tens of minutes experienced with legacy solutions. Our purpose-built DDoS network defense devices can be deployed in a centralized and/or distributed model.

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 protection from the frequent, short duration attacks that impact organizations every day.

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

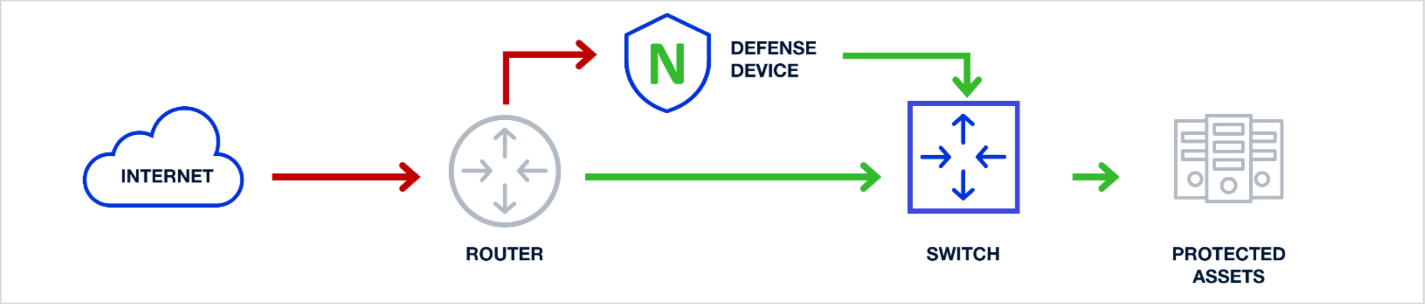
SmartWall ONE supports flexible deployment options to best suit the environment being protected. The fastest, most effective protection is delivered with appliances deployed always-on at all ingress points to the network, either inline with internet connections, or in the data path, connected to edge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

## Inline Deployment



**N** Network Defense Device

## Scrubbing Deployment



**N** Network Defense Device

## 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 Size

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 Deployment

Physical or virtual appliance flexibility inline, or in the data path, 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-ser- vice 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

SmartWall ONE secureWatch Analytics delivers comprehensive visibility into DDoS attacks with easy-to-read dashboards delivering actionable intelligence.

### Monitor in Real-Time

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

### Optimize Protection

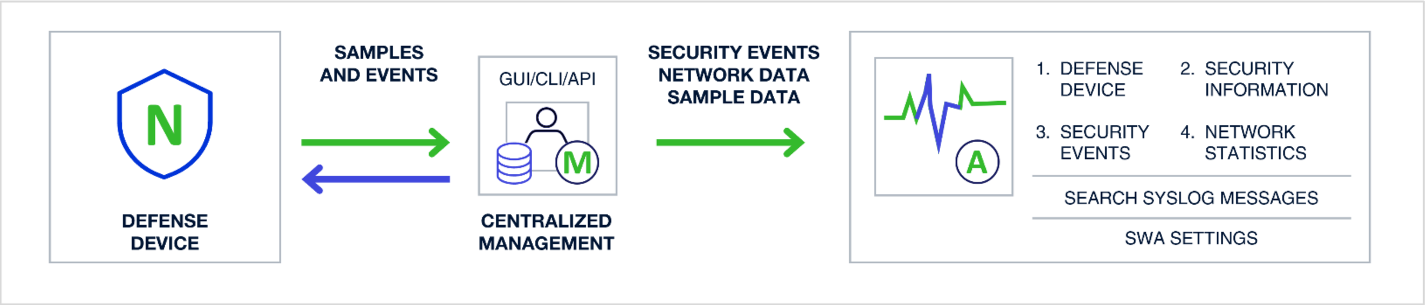
Gather traffic information to help you fine-tune policies

### Analyze Attacks

Drill down into blocked and allowed traffic seen an attack.

### Enhance Threat Intelligence

All events are stored and indexed in web-based applica- tion and available the analytics externally, to other security tools via syslog



**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 leveraging specific payloads (TeamSpeak, RIPv1, NetBIOS)
- 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

### 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

## Technical Specifications

| **SmartWall ONE** | NTD 280 | NTD 1100 |
|---|---|---|
| **Network Interfaces** | 4, 8, 12 or 16 1/10G SFP/SFP+<br>or 2 / 4 10G LR<br>zero-power bypass | 2 x 100G QSFP28<br>or 2 x 100G 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 |
| **Maximum Throughput (Packets per second)** | 120 Million | 150 Million |
| **Typical Latency[1]** | <0.5 Microseconds | |
| **Inspected Latency[1]** | < 60 Microseconds | |
| **Max SYN Flood Rate (Packets per second)** | 120 Million | 120 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 & 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 | |

| Physical / Environmental | |
|---|---|
| **Size** | 1-RU / 44 mm (H) x 438 mm (W) x 630 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 |
| **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 |

## Technical Speciications

### NTD Virtual Edition

| | |
|---|---|
| **Network Interfaces**<br>4 x 10G Virtual Ethernet | **Management Port**<br>1 x 10/100/1000 Virtual Ethernet |

### Performance

| | | |
|---|---|---|
| **Maximum Protect Throughput (Gigabits per second)**<br>100 Gbps (on 32 x CPU cores running KVM)+ | **Maximum Throughput (Packets per second)**<br>80 Million | **Maximum Detect Throughput (Packet/s-Flow samples or NetFlow records)**<br>100 Gbps (deployed on 8 x Intel CPU cores running KVM) |
| **Typical Latency**[1]<br>< 0.5 Microsecond | **Inspected Latency**[1]<br>< 60 Microseconds | **Attack Mitigation Time**<br>< 60 Microseconds |
| **Maximum SYN Flood Protection Rate (Packets/Second)**<br>80 Million (Line-Rate) | **Jumbo Frames**<br>Yes (9,216 bytes) | |

### Physical Environment

| | | |
|---|---|---|
| **Hypervisors**<br>KVM running on Red Hat Enterprise 7+,<br>CentOS 7+ or Ubuntu 16.04+<br>VMware ESXi 6.5+ | **Minimum Requirements**<br>16GB Memory, 20GB Disk | **Network Interfaces**<br>10G - XL710 NIC<br>100G - E810 NIC<br>ConnectX-5/6 |

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