corero

CORERO SMARTWALL® TDD

Empowering the Network Edge

SmartWall Threat Defense Director (TDD) delivers full edge protection for even the largest provider networks. Powering the filtering capabilities increasingly built into modern edge routers, TDD scales to tens-of-terabits per second of protection, without the need to deploy dedicated appliances at the edge, or needing to back-haul large volumes of attack traffic to scrubbing centers.

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. This has pushed maximum, and average, attack sizes up, as well as significantly increasing their frequency, due to the ease with which they can now be launched, by anyone with a motive.

The sophistication of DDoS also continues to evolve each year. These attacks now present a more challenging detection and mitigation task due to their varying amplitudes, 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 a few seconds.

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, short duration, IoT Botnet, and pulsing attacks directly on the network edge, for even the largest provider-scale networks.

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.

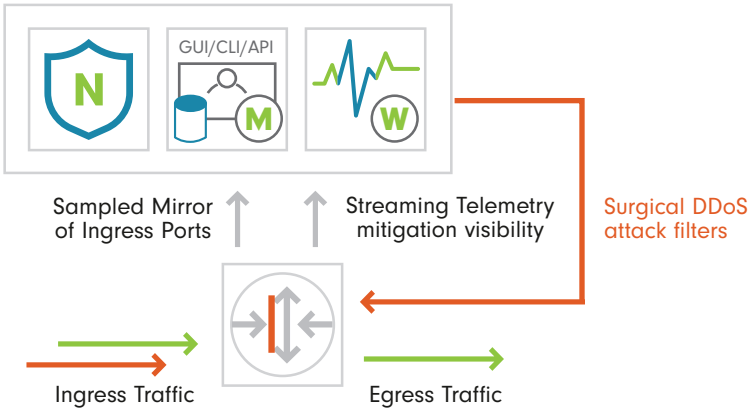
Proactive DDoS Protection with Comprehensive Attack Visibility

The SmartWall Threat Defense Director has the same accurate, real-time, automatic detection of Corero's SmartWall Threat Defense System at it's core, coupled with the high-performance packet filtering of smart infrastructure devices, for mitigation, to deliver SmartWall's award winning protection at unprecedented scale and simplicity of deployment.

The solution includes the SmartWall Central Management Server (CMS), which offers multiple options for managing, configuring, and monitoring the TDD detection appliances, including a flexible Browser-based GUI, a full SSH CLI and powerful REST API, that supports open integration with existing management frameworks. The CMS is delivered as a virtual appliance to run on customer-provided hardware.

The TDD solution also includes Corero's SmartWall SecureWatch® Analytics application; a powerful web-based security analytics tool that delivers comprehensive and easy-to-read dashboards, as well as enabling sophisticated DDoS attack forensics. The analytics capability in TDD is driven by security event and traffic flow feeds from the SmartWall detection appliances and supported infrastructure device telemetry.

The solution leverages Splunk software for big data analytics and advanced visualization capabilities, to transform sophisticated security event data into dashboards that deliver actionable intelligence, before, during and after an attack.



Infrastructure	Devices monitor ingress traffic via sampled mirrors that include both header and payload to accurately identify the threat.
Visibility	TDD inspects every packet in the sample feeds to quickly and accurately detect any DDoS attack traffic.
Mitigation	TDD dynamically generates surgical filters to mitigate attacks directly on the supported infrastructure devices.
Automation	TDD automatically configures the infrastructure devices using the NETCONF network management protocol to install filters which block DDoS packets directly at the ingress points of the network.
Simplicity	Telemetry, machine analytics, and network programmability make the detection and mitigation process more intelligent, automated, and adaptable.

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.

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.

Managed Services Enabler

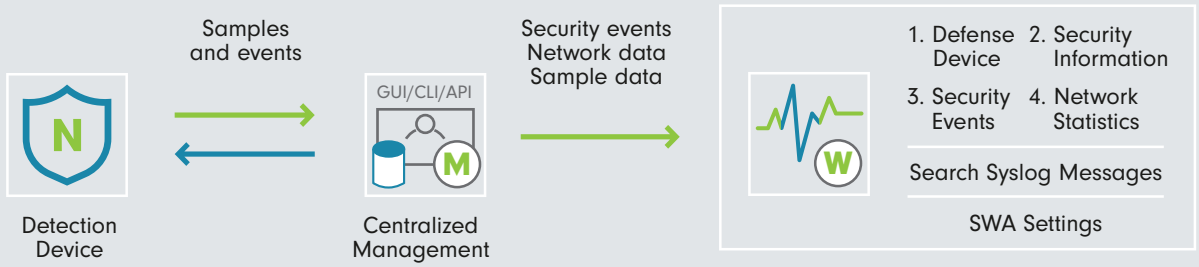
Service and hosting providers can enhance security service offerings with real-time, automatic DDoS protection to their customers without 'blackholing' or disrupting legitimate customer traffic combined with an online portal for customer visibility and reporting.

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 is a powerful security analysis application that delivers comprehensive visibility into DDoS attacks with easy-to-read dashboards delivering actionable intelligence.



TDD Security Coverage

Protection Capabilities

- Defends attacks to single/multiple IPs and Subnets
- Flex-Rules - Programmable filters using the Berkeley Packet (BPF) syntax with Corero enhancements
  - Detect a variety of volumetric attack vectors, from reflective through to those leveraging specific payloads
- Smart-Rules – Patented high-performance heuristics-based engine that automatically detects volumetric DDoS attacks, including zero-day
- Botnet protection
- Blacklisting or Whitelisting of IP Addresses
- TCP/UDP port-based attacks
- Rate Limiting Policies
- Cloud Mitigation, FlowSpec and RTBH signalling

Reflection DDoS

- NTP Monlist
- SSDP/UPnP
- SNMP
- Chargen
- DNS
- Connectionless LDAP (CLDAP)
- Memcached
- Portmapper
- Netbios
- RIP

Volumetric DDoS

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

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

Technical Specifications

Performance

Maximum Throughput

40 Terabits per Second

Maximum Throughput

60 Billion Packets per Second

Time to Mitigation

<10 Seconds (Typical)

Physical Environment

Hypervisors

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

Minimum Requirements

32GB Memory, 620GB Disk

Mitigation Devices

Juniper MX Series Routers
(Junos OS 17R4, or later)

Juniper PTX Series Routers
(Junos EVO 22.3 and later versions)

Network Interfaces

1G - Virtio
10G - XL710 NIC
100G - E810 NIC

Management	Centralized Object-Oriented Management from a Seperate Virtual (VMware/KVM) Appliance
Interfaces	1 x 10/100/1000 Virtual Ethernet
Web-Base 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
Security Dashboards	Link utilization (Gbps/PPS), Attack Targets, Attack Vectors, Alerts, Detailed Drill Downs, Top IP's/Ports/TTLs/Packet Sizes
Reporting & 3rd 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)

US HEADQUARTERS
Email: info@corero.com

EMEA HEADQUARTERS
Email: info_uk@corero.com