SmartWall®

THREAT DEFENSE SYSTEM

corero
FIRST LINE OF DEFENSE

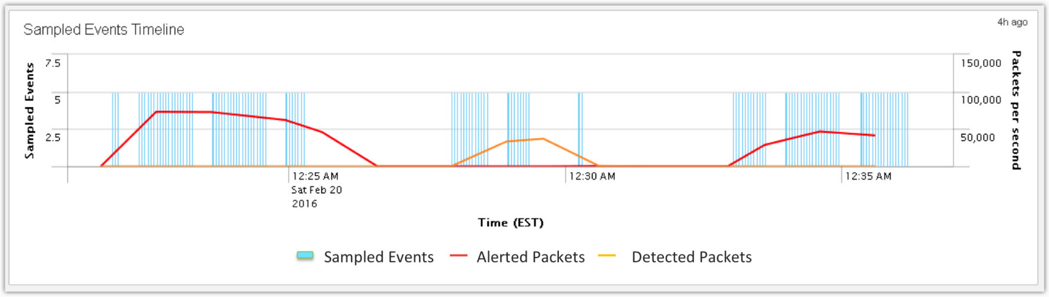
DATA SHEET

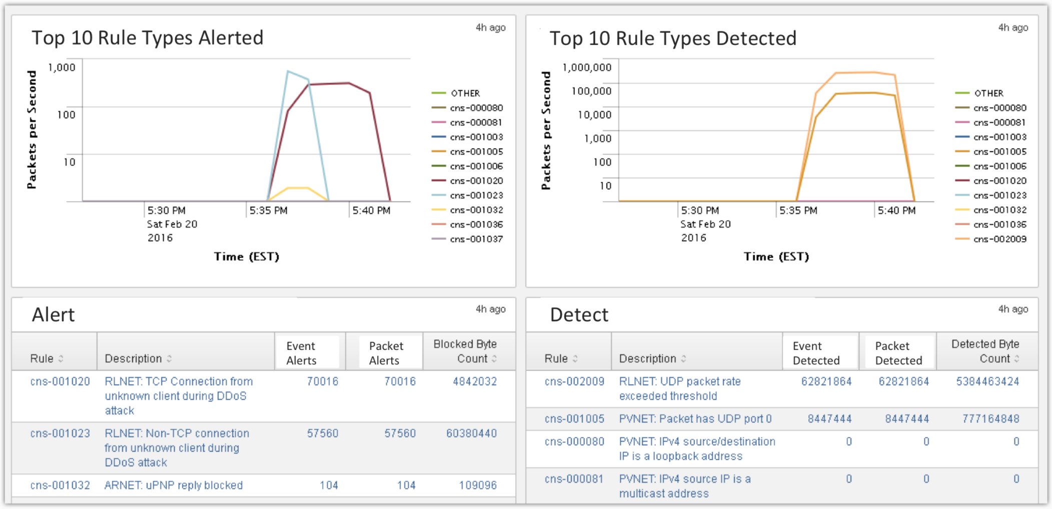
CORERO SMARTWALL® NETWORK THREAT DEFENSE - VIRTUAL EDITION (vNTD MONITOR)

This industry first technology brings real-time DDoS event detection and visibility to Virtual Machine (VM) instances for more diverse deployment possibilities, with the same powerful and rich DDoS security event analytics and reporting found in the award-winning Corero SmartWall Threat Defense System. This leading-edge technology brings real-time DDoS event visibility to the VM environment giving customers more clarity into DDoS threats such as localized quick strike multi-vector attacks that are proliferating worldwide.

COMPREHENSIVE VISIBILITY

Disruptions to Internet-facing online services can cripple operations, impact customers and result in major economic losses. The SmartWall vNTD is an intelligent, always on virtualized monitoring solution, specifically designed to inspect traffic, detect DDoS threats and provide unique visibility, reporting and analytics against those security events. It allows Service Providers, Hosting Providers, and the Online Enterprise to deploy centralized or distributed DDoS monitoring capabilities that provide advanced Layer 3-7 DDoS attack visibility.





Alert

4h ago

Rule	Description	Event Alerts	Packet Alerts	Blocked Byte Count
cns-001020	RLNET: TCP Connection from unknown client during DDoS attack	70016	70016	4842032
cns-001023	RLNET: Non-TCP connection from unknown client during DDoS attack	57560	57560	60380440
cns-001032	ARNET: uPNP reply blocked	104	104	109096

Detect

4h ago

Rule	Description	Event Detected	Packet Detected	Detected Byte Count
cns-002009	RLNET: UDP packet rate exceeded threshold	62821864	62821864	5384463424
cns-001005	PVNET: Packet has UDP port 0	8447444	8447444	777164848
cns-000080	PVNET: IPv4 source/destination IP is a loopback address	0	0	0
cns-000081	PVNET: IPv4 source IP is a multicast address	0	0	0

KEY BENEFITS

✓ **Flexible Deployment Capabilities**

Delivered as virtual machine (VM) for more flexible deployments, management and scale. Leverages the power of Vmware/vSphere tools to enable a true cloud scale DDoS monitoring environment.

✓ **Powerful Centralized Management**

Carrier class Centralized Operational Management for configuration, controlling and monitoring of DDoS security events.

✓ **Scalable Performance**

Adjusting sampling rates allows system to scale to monitor links for DDoS events in a performance range from 100Mbps to 100Gbps for a single VM.

✓ **Powerful and flexible DDoS filtering algorithms**

Leverages the patented DDoS detection algorithms used by the award winning Corero SmartWall TDS which delivers manual, behavioral and automated DDoS detection.

✓ **Comprehensive Visibility**

Leveraging built in Splunk software for big data analytics and advanced DDoS visualization capabilities. The system can also send DDoS event data to 3rd party SIEM environments.

TECHNOLOGY COMPONENTS

Corero SmartWall® Network Threat Defense - Virtual Edition (vNTD Monitor)

vNTD monitors and inspects traffic, sending sFlow data, security events and syslog messages to Corero SmartWall Site Management Server - Virtual Edition (vSMS) providing granular visibility into DDoS attacks and traffic anomalies at the network and application layers. The vNTD technology can detect DDoS attack vectors ranging from volumetric, reflection, resource exhaustion, and application layer to provide a detailed analysis and summary of DDoS threats present on the network.

Corero SmartWall® Site Management Server - Virtual Edition (vSMS)

vSMS provides centralized management of a single or multiple vNTD VMs. It processes event information, sending aggregated statistics and security metadata about DDoS attacks to Corero SecureWatch® Analytics - Virtual Edition (vSWA). vSMS uses industry standard Cisco Network Service Orchestrator (NSO) enabled by Tail-f, which is used by Tier 1 Carriers for scalable configuration management.

Corero SmartWall® Analytics - Virtual Edition (vSWA)

vSWA indexes data received from all vSMS instances and presents the information in an easy to read graphical user interface (GUI) that incorporates pre-built DDoS information dashboards and enables detailed analysis and drill-down on an event-by-event basis. Additionally, vSWA can be connected to the Corero SecureWatch Analytics portal for global remote access to DDoS event information and integration of vNTD Monitor data with a commercial Corero SmartWall Threat Defense System deployment. The vSWA can also be used to signal cloud or Scrubbing DDoS solutions based on user specified attack thresholds, using the pre-standard IETF DOTs signaling format.

Additionally, vSMS and vSWA can also connect back to the Corero SecureWatch Security Operations Center (SOC). Allowing Corero security personnel to deliver 7x24x365 security analysis and monitoring included as part of the SecureWatch PLUS service.

FLEXIBLE DEPLOYMENT CAPABILITIES

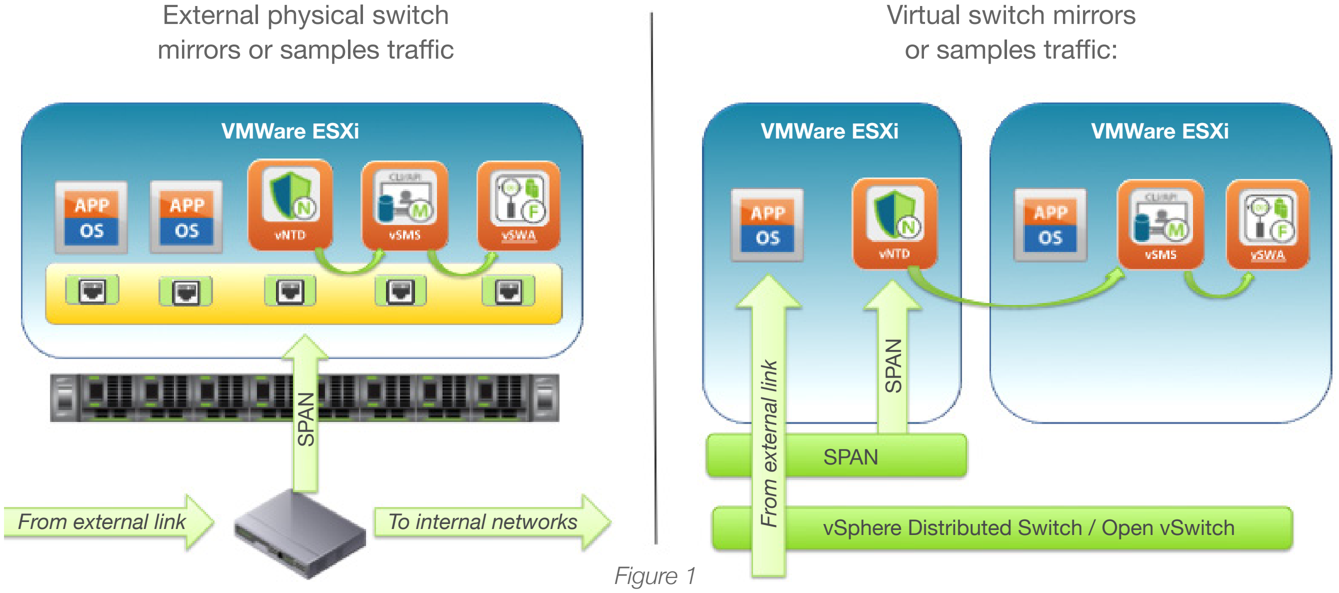


Figure 1

Fig 1. - Shows a typical deployment option for the vNTD solution. It can be placed as a tap off an edge router or layer 3 switch. In this mode all traffic will be mirrored to the vNTD. The vNTD can be configured to send sflow and DDoS event data back to the vSMS. The data is then packaged in industry standard syslog format for correlation by the vSMS and then analysis and visualization by vSWA. vSWA is built using Splunk big data analytics environment. Customers can leverage the power of Splunk and its rich analytics language to create their own customized alerts, reports and dashboards.

vNTD can also be used to monitor attack traffic in an all virtual vSwitch or vRouter environment. All three components can exist in their own VM environment thereby allowing scale and flexibility.

TECHNICAL SPECIFICATIONS

Runs on vSphere ESXi Hypervisor v5.5

Provides centralized management of multiple vNTD VMs

Powerful policy model supporting group policy with profiles

Uses vNTD network events to provide summary feeds into analytics (vSWA) and 3rd party SIEM

Streamlined deployment of vNTD virtual appliances for dynamic provisioning

Full SSH CLI and REST API for integration with management frameworks

Minimum System Requirements

vNTD	2 vCPU N.B. the vNTD will spin 1 vCPU 100% 8GB memory 3 vNICs 16GB disk
vSiteManager	4 vCPU 8GB memory 1 vNIC 80GB disk
vAnalytics	4 vCPU 5GB memory 1 vNIC 256GB disk

Supports up to 1G, 10G and 100G interfaces via configurable sample rate

Depending on ESXi host – typical processing 400K samples per second

- 1G = 1:6 sample rate, 10G = 1:64, 100G = 1:640

DDOS ATTACK DETECTION AND VISIBILITY

Category of Attack Type	Attack Coverage
Volumetric DDoS	TCP Flood Attacks UDP Flood Attacks UDP Fragmentation Attacks ICMP Floods
Reflective DDoS	NTP Monlist Response Amplification SSDP/UPnP Responses SNMP Inbound Responses Chargen Responses Smurf Attack Fraggle Attack DNS DNS Amplification
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
Other	Command and Control Operations Tunnel Inspection (GRE, MPLS etc.) GRE, MPLS etc. NTP Monlist Requests Whitelisting Blacklisting of IP Addresses Flex-Rule – Programmable filters based on the Berkley Packet Format (BPF) syntax. These can be programmed to address a variety of attack categories volumetric, reflective through to attacks leveraging specific payloads (Teamspeak, RIPv1, netbios). Smart-Rule – Heuristics based engine leverages heuristics and behavioral analysis to track and rate limit

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 next-generation technology provides a first line of defense® 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.

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749 USA
Phone: +1.978.212.1500
Web: www.corero.com

EMEA Headquarters
Regus House, Highbridge, Oxford Road
Uxbridge, England
UB8 1HR, UK
Phone: +44.0.1895.876579