First Line of Defense®

DDOS DEFENSE SYSTEM

corero
FIRST LINE OF DEFENSE

DATA SHEET

DDoS DEFENSE SYSTEM (DDS)

KEY BENEFITS

Comprehensive DDoS and Cyber Threat Protection

Defends against all forms of application-layer and network-layer attacks

Reliability and High Availability

ProtectionCluster™ configurations, built-in zero power port bypass, and redundant power ensure reliability

Performance and Low Latency

Transparent network performance ensures latency-sensitive applications are not impacted

ANALYST QUOTE

"The industry is in need of advanced technology like Corero's to meet changing threats and minimize the risks and losses associated with these DDoS attacks."

Richard Stiennon,
Chief Research Analyst,
IT-Harvest

NETWORK AND APPLICATION-LAYER DDoS ATTACK DEFENSE SYSTEM

DDoS Defense System (DDS), is your First Line of Defense® against today's insidious low and slow application-layer Distributed Denial of Service (DDoS) attacks, which have become the attackers' weapon of choice, as well as the more traditional high-volume network floods. The dedicated, on-premises solution, enhanced with the real-time threat protection of ReputationWatch®, delivers the most comprehensive DDoS protection available.

THE THREAT

Crippling DDoS attacks are a threat to every organization that depends on the Internet to conduct business. DDoS attacks result in loss of profits, damaged reputation, reduced productivity and costly downtime. A sustained DDoS attack on a high-transaction volume site can cost $1 million or more within a 24-hour period.

FEATURED PRODUCT

DDoS Defense System

Although DDoS attacks have been a prominent threat for more than a decade, more recently, they have become increasingly sophisticated and destructive with the evolution of application-layer techniques. Today's low-bandwidth application-layer DDoS attacks appear to be making legitimate server connections and fly under the radar of conventional DDoS detection methods. They require much smaller botnets than network flooding attacks would require, and these crippling attacks can even be launched from a single PC. An organization may be under attack without even realizing it.

With more sophisticated tools and automated programs for scanning and compromising computers on the Internet, an individual or a group with malicious intent can simply download a DDoS attack program and rent a botnet from which to launch it. Or, they can simply hire a DDoS "hit squad" by the day, week or month for very modest fees.

DDoS attacks can strike any organization, for any number of reasons. In a Vanson Bourne survey of 200 U.S. enterprises, sponsored by Corero, 38% of the respondents said they had suffered at least one DDOS attack in the past 12 months. Of those, more than half blamed unscrupulous competitors seeking to gain unfair business advantage. One in five cited politically/ideologically motivated hacktivists, followed by wanton malicious attacks ("just for laughs") and extortion under threat of DDoS, a cyber-variant of the "protection racket."

SOLUTION: THE CORERO DDoS DEFENSE SYSTEM

The Corero DDoS Defense System is a purpose-built, on-premises DDoS defense solution designed to deliver non-disruptive protection against constantly evolving threats. It provides maximum protection for critical IT infrastructure while allowing full access to legitimate users and applications.

The Corero DDS gives your IT staff an easy-to-install and reliable solution that:

- Automatically detects and mitigates both advanced application-layer attacks and traditional network-layer attacks
- Responds immediately, protecting your servers from malicious traffic
- Protects your IT infrastructure investment
- Ensures business continuity, allowing your customers to keep receiving quality service, even while under attack

The Corero DDS delivers by far the most comprehensive DDoS protection available, leveraging its patented DDoS Defense algorithms and extensive rate-based protection mechanisms as well as reputation and geo-location based filtering to protect against unwanted access and malicious content.

Based on intelligent behavioral analysis, the Corero DDS uses an adaptive, patented DDoS defense algorithm to detect and block malicious incoming requests while passing legitimate traffic to the company's protected servers. This system debits a DDS maintained credit balance associated with each source IP address and blocks further requests from an IP address when the credits are depleted.

For example, if a client makes repeated HTTP GET requests to the same web page or server object, or multiple DNS requests that result in error responses, many credits are debited even if requests are low and slow. Repeating such requests will result in the client credit balance going below zero, and all new transactions from that client will be blocked until new credits are earned.

The Corero DDS defends against:

- Application-layer DDoS such as slow repeated HTTP GET attacks, also known as connection-based attacks
- TCP SYN, UDP and ICMP flood attacks
- Attacks on your DNS infrastructure
- Attacks on your web application servers

SecureWatch™: EXPERT, AROUND THE CLOCK PROTECTION

All the Corero customers are monitored 24x7 by our Security Operations Center (SOC) ensuring around the clock protection against the latest threats. The Corero SOC ensures that your First Line of Defense installation is constantly monitored for system faults and security events, and notifies you in case of equipment failures or suspicious activities that would compromise your web services. We also summarize your First Line of Defense installation in a quarterly security report customized to your environment. Customers can always view the network health and security posture of their installation through Corero SecureWatch Analytics, a web-based portal hosted by the Corero SOC.

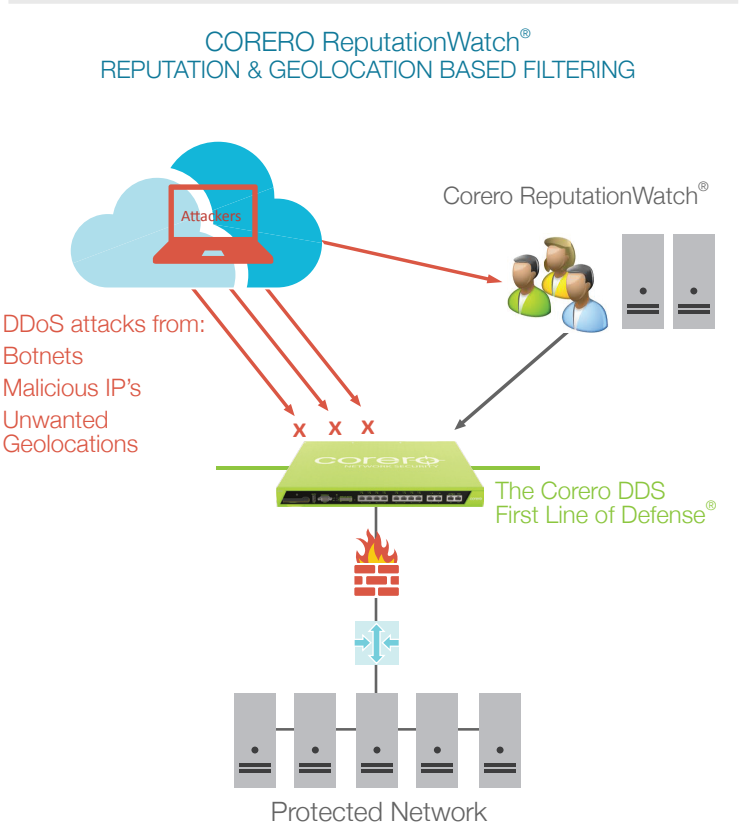
In addition, customers can upgrade to SecureWatch PLUS, a premium fully managed service which includes a comprehensive suite of First Line of Defense configuration optimization, monitoring and response services. These services are customized to meet the organization-specific security policy requirements and business goals of the customer. An assigned technical account team works closely with the customer to ensure a successful deployment and implement a swift DDoS response plan consisting of rigorous monitoring, alerting, and mitigation response. This team provides you with immediate response and expert DDoS mitigation services in the event of an attack. Each SecureWatch PLUS customer is provided with a fully customized weekly, in-depth security report for ongoing visibility, tuning, and optimization.

ReputationWatch® WITH GEOLOCATION

The ReputationWatch feed from Corero delivers up-to-date, real-time protection against “known bad” IP addresses across the Internet, ensuring that your network is secure against the latest threats. In a constantly changing Internet threat environment, IP addresses can go from bad to good and vice versa within minutes. It is impossible to maintain current security configurations manually as attack sources change. For example, PCs are hijacked into a botnet, while others are restored to a good state. Websites are compromised, and websites are remediated. ReputationWatch collects and analyzes global threat data about the current status of IP addresses and provides a continuous intelligence feed. This enables the DDS to respond by automatically blocking access to known malicious sites, including:

- Known sources of DDoS attacks
- Bots that fall within identified botnet command and control structures
- Systems delivering specially crafted denial-of-service exploits, such as KillApache
- Identified sources of malicious content attacks
- Phishing sites
- Spam sources

ReputationWatch includes geolocation based filtering, which empower organizations to enforce security policy based on national origin. Geolocation enables you to limit or block traffic from countries with which you do no business with or countries associated with high numbers of attacks.



THREAT UPDATE FEED OPTIMIZED FOR DDoS DEFENSE

Threat Update Service is an automated protection feed that provides the Corero DDS customers with proactive protection against DDoS attacks and ongoing mitigation of security issues. It delivers frequent Protection Pack updates to keep your networks protected against the latest threats. Protection Packs include data about badly behaving IP addresses collected from thousands of sensors throughout the Internet, security advisories about newly discovered threats and updated vulnerability and attack signatures.

SECURITY EVENT MANAGEMENT AND SIEM INTEGRATION

Corero provides security event management, real-time alerting, and flexible reporting. It saves time and effort in normal day-to-day security monitoring and incident response.

The Corero Attack Response Engine includes a built-in real-time Security Event Viewer that allows users to drill down and identify attackers, victims and types of attacks, then take immediate action to block or mitigate the threat. In addition, it uses a flexible event-logging format for integration with leading security information event management (SIEM) tools.

The Corero security event manager features:

- Contextually aware high-level alerting
- Compliance audit life cycle management
- Enterprise-wide security intelligence
- Real-time monitoring and correlated alerting

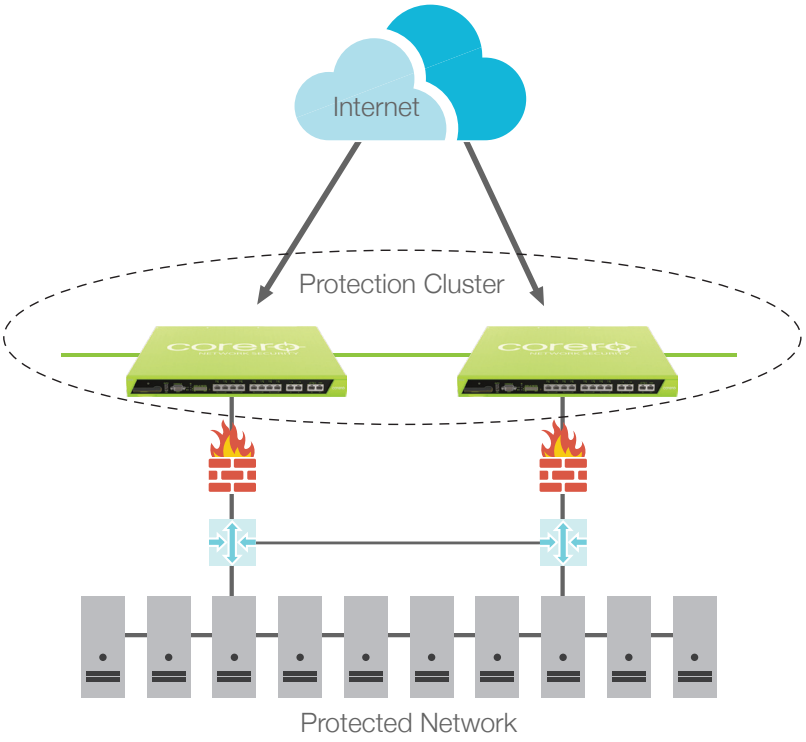
PROTECTION CLUSTER SCALABLE, TRANSPARENT HIGH AVAILABILITY

The Corero DDS ProtectionCluster can be deployed in configurations of up to four clustered units and is recommended for deployments requiring system throughput of greater than 10 Gbps. With Corero's deep networking experience, the Corero DDS offers the right solution for ensuring high reliability and nonstop availability:

- Active-Active operation
- Asymmetric traffic handling
- Scalable performance and capacity
- Seamless failover that ensures nonstop protection
- 20-30 year MTBF (mean time between failures) rating
- Hot-swappable power supply and fans
- No rotating media or chip fans

The Corero DDS has been designed to be a high-performance switch-like device to ensure that it will not interrupt latency-sensitive applications such as VoIP, and will ensure speedy response times for all applications.

DDS APPLICATION SCENARIO



GREEN DESIGN

The energy-conserving design of the Corero DDS requires only 1RU of rack space for most models, and has low power consumption. The Corero DDS fits right in with initiatives to cut back on space and reduce cooling requirements and consumption of electricity. The Corero DDS also features zero-power bypass capability for copper based interfaces to maintain connectivity in case of a total power failure.

Patented Technology

With the Corero patented algorithms, the DDoS Defense System goes beyond known DDoS attack mitigation and protects against general classes of attacks. This allows the DDS to mitigate today's threats and also tomorrow's threats as they arise.

Some of the technologies the Corero DDS implements are:

- Policy-based rules that limit traffic rates
- Sophisticated session analysis to defend against application level resource depletion attacks
- Algorithms for protecting against SYN floods, ICMP floods, UDP floods, and application level overload attacks
- Configurable rules that limit the rate at which individual clients or groups of clients can initiate transactions

TECHNICAL SPECIFICATIONS

Order Part Number	DDS 150 EC/ES	DDS 500 EC/ES	DDS1000 EC/ES	DDS 2000 ES	DDS 2400 ES
Interfaces					
Copper 10/100/1000 Ethernet ports	8 (EC Models only)			2 MGMT	
Pluggable 1G Ethernet ports (SFP modules)	8 (ES Models only)				
Pluggable 10G Ethernet ports (SFP+ modules)				4	
Other ports (Serial Console, Auth, Service)	1 Serial, 1 USB 2.0				2 Serial, 2 USB 2.0
Target Network Capacity	In-line Gigabit Ethernet Network Light Utilization	In-line Gigabit Ethernet Network Moderate Utilization	In-line Gigabit Ethernet Network Heavy Utilization	In-line 10 Gigabit Ethernet Network Moderate Utilization	In-line 10 Gigabit Ethernet Network Heavy Utilization
MAX Throughput	600+ Mbps	2.4 Gbps	4.4 Gbps	8 Gbps	10 Gbps
Typical Latency[1]	< 35 uSec	< 35 uSec	< 35 uSec	< 35 uSec	< 45 uSec
Typical Inspected Latency[1]	< 50 uSec	< 50 uSec	< 50 uSec	< 50 uSec	< 60 uSec
MAX Concurrent Sessions	256,000	1 Million	2 Million	2 Million	4 Million
MAX Session Setup/Teardown	40,000/Sec	40,000/Sec	40,000/Sec	50,000/Sec	100,000/Sec
MAX SYN Flood DoS Protection Rate	500,000/Sec	1,000,000/Sec	1,500,000/Sec	2,000,000/Sec	3,000,000/Sec
ProtectionCluster Capable	Yes	Yes	Yes	Yes	Yes
Device Management					
Management Interfaces	Four (4) switched 10/100/1000 Ports on isolated switch fabric with flexible assignment			Two (2) switched 10/100/1000 Ports on isolated switch fabric with flexible assignment	Four (4) switched 10/100/1000 Ports on isolated switch fabric with flexible assignment
Network Standards	IEEE 802.3-2002, 802.3-2008, 10BASE-T, 100BASE-TX, 1000BASE-T with manual or auto-negotiated speed and duplex, 802.1Q-2003 Standards for supported SFP Modules			IEEE 802.3-2002, 802.3-2008, 10BASE-T, 100BASE-TX, 1000BASE-T with manual or auto-negotiated speed and duplex, 802.1Q-2003 Standards for supported SFP+ Modules & SFF-8431 Rev4.1 10GSFP+Cu (Direct Attach)	
Out-Of-Band Access	Dedicated Management Interfaces described above, 9-pin D-Sub for Local Console				
Command Line	Yes, via local console or Telnet				
Web-Based	Yes, via Java Web Start application over HTTP, or SSL				
Management Protocols	Yes, SNMPv1 standard MIB GETs, Traps, NTPv2, SYSLOG				
Software Upgrade	Remotely upgradeable image and configuration stored on internal Compact Flash				
Secured Physical Access	Optional Compact Flash cover, console access token, tamper-evident seal				
Third Party Management Compatibility	Splunk, ArcSight, CA, eIQ Networks, Forensics Explorer, GuardedNet, HP Openview, IBM Tivoli, netForensics, Open Service, RSA Envision, Q1Labs, TriGeo				
Response Mechanisms	Packet filter, shun, session filter, session reset, forensic redirection, transparent circuit proxy				
Physical/Environmental					
Size	1-RU 4.4cm (H) x 44.0 cm (W) x 51.5cm (D)				2-RU 8.8 x 44 x 51.5
Weight	18.1 lbs. (8.2 Kgs)				36.2 lbs. (16.4 Kgs)
Operating Temperature	0 C to 40 C (32 F to 104 F)				
Storage Temperature	-25 C to 70 C (-13 F to 158 F)				
Humidity	5% to 95% non condensing				
MTBF Rating	>300,000 hours (25 deg. C ambient)			>200,000 hours (25 deg. C ambient)	>150,000 hours (25 deg. C ambient)
Operating Altitude	0-10,000 feet				
Power & Cooling					
Power Supplies	Dual Hot-swappable Power Supply Units				Four Hot-swappable Power Supply Units
AC Input	100 to 240 VAC auto-ranging, 50-60Hz				
Max Power Consumption	< 100W			< 150W	< 300W
Cooling	Hot-swappable N+1 fan tray				2 Hot-swappable N+1 fan trays
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-				
Compliance to EMC Immunity	EN55024:1998 including Amendment 1:2001 & Amendment 2:2003(CISPR24:1997 +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 61000-4-6:1996 +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				

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

ABOUT CORERO NETWORK SECURITY

Corero Network Security, an organization's First Line of Defense® against DDoS attacks and cyber threats, is a pioneer in global network security. Corero products and services provide online enterprises, service providers, hosting providers, and Managed Security Service Providers with an additional layer of security capable of inspecting Internet traffic and enforcing real-time access and monitoring policies designed to match the needs of the protected business. Corero technology enhances any defense-in-depth security architecture with a scalable, flexible and responsive defense against DDoS attacks and cyber threats before they reach the targeted IT infrastructure allowing online services to perform as intended. 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