

On-Premises Defense Against Network and Application Layer DDoS Attacks

Product Highlights

- **Easy to Deploy and Manage**
Flexible interface options speed installation, protecting networks within 30 minutes.
- **Business Continuity**
Allows customers and employees to access services, even during an attack.
- **SecureWatch® PLUS**
Specialized configuration, monitoring and incident response DDoS defense services tailored to each customer's specific needs.
- **Threat Update Services**
Automated protection pack updates optimized for DDoS Defense.
- **DDoS-Optimized Three Dimensional Protection**
Protection against rate-based attacks, malicious content and undesired access.
- **Lowest Network Latency**
At under 60 uSec, there's no interruption to critical applications such as VoIP.
- **Reliability and High Availability**
ProtectionCluster configurations, built-in zero power port bypass, and redundant power ensure reliability.
- **Green Design**
1RU rack space for most models and low power consumption.

When a business depends on the availability of its network, a Distributed Denial of Service (DDoS) attack is crippling. The cyber attack can cause loss of profits, damaged reputation, reduced productivity, downtime costs, and in some cases, the attackers may even demand extortion fees to cease the attack. Although DDoS attacks have been a prominent threat to networks for nearly a decade, more recently, they have become increasingly sophisticated and destructive with the evolution of new application layer variants. Today's application layer DDoS attacks fly under the radar of conventional DDoS detection methods and can exhaust local server resources without showing up on the bandwidth consumption screen.

Attackers routinely recruit tens of thousands or even greater numbers of compromised computers, called bots or zombies, to form botnets, which are remotely controlled to initiate network attacks against a single victim. With the newer application layer variants, the attacker can cause the same damage with a much smaller number of bots. Attackers no longer require strong skills: With more sophisticated tools and automated programs for scanning and compromising computers on the Internet, an individual with malicious intent can simply download a DDoS program and then rent a botnet from which to launch it.

The resulting rise in DDoS attacks has raised organizations' concerns that they will be victimized and fuels interest in adopting proactive protection.

According to a 2011 report from VeriSign, 63% of midsize to large organizations say they suffered at least one DDoS attack in the past year, and 11% reported six or more attacks. Approximately 70% of respondents said they plan to deploy a DDoS defense solution in the next 12 months.



The DDoS Defense System (DDS) is Corero's newest product family leveraging its award-winning DDoS defense technology, designed to deliver nondisruptive protection against constantly evolving threats. It provides maximum protection for critical IT assets while allowing full access to legitimate users and applications. The purpose-built Tilera multicore processor architecture provides real-world protection at real-world performance levels.

Corero's DDS gives your staff an easy-to-install and reliable solution that:

- Automatically detects and mitigates both traditional network layer DDoS attacks and more advanced application layer attacks.
- Responds immediately, protecting your servers from malicious traffic.
- Protects your network, allowing legitimate communications to pass without delay.
- Enables business continuity, allowing your customers to keep receiving quality service.

In a business era in which changing threats and dynamic business requirements demand protection of information and the stability of computing infrastructure, Corero's solutions are the clear and safe choice.

Corero DDoS Defense System

Emerging Threats

The primary objectives for attacks used to be bragging rights and recognition of hacking skills. Today, the attacks are being launched for financial gain, criminal intent and cyber-terror. Organized crime is now enlisting the aid of and incorporating the techniques of hackers for criminal intent such as identity theft, online fraud and extortion. Real time cyber-crime attacks are now listed as the FBI's third highest priority, behind terrorism and espionage.

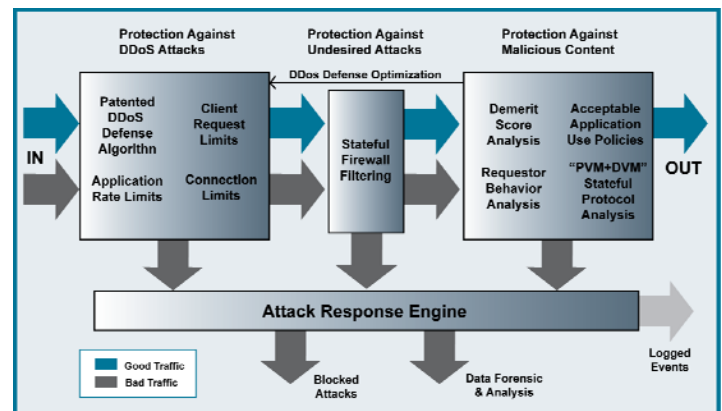
Recently, a national government suffered a politically motivated 15Gbps DDoS attack. In another incident, a bank's website was attacked for two days. During this time, its individual customers couldn't access their accounts, and a large merchant was not able to process financial transactions. The Internet's infrastructure has even been targeted when an attack was directed at the DNS root name servers. The DNS function, which translates web and other Internet addresses into their numeric equivalents, is essential to all Internet users, and the loss of availability massively degrades Internet usage. The hacker group Anonymous launched DDoS attacks on MasterCard, VISA and PayPal; the CIA and the Serious Organized Crime Agency, the United Kingdom's equivalent of the FBI, came under DDoS attack by LulzSec; SONY, WordPress and the Hong King Stock Exchange were also all recent victims of DDoS .

Traditional network security tools are ineffective against DDoS attacks. Commercial firewalls, which have been around since 1992, are required to defend against unauthorized access to a company's network. Intrusion prevention systems protect against attackers exploiting weaknesses in legitimate communications permitted by the firewall. Neither of these however, protects against the overuse, or flooding, of available services during a DDoS attack.

Comprehensive DDoS Defense through Three Dimensional Protection

Corero's DDS provides a "DDoS optimized" implementation of its proven Three Dimensional Protection (3DP) architecture, the core of Corero defense technology. The three dimensions of 3DP encompass patented DDoS Defense algorithms and extensive rate-based protection mechanisms, stateful firewall filtering and finally, malicious content protection, using Demerit Score and Requestor Behavioral Analysis, Acceptable Application Use and Stateful Protocol Analysis. Combined within the DDS product range, these three dimensions of protection offer a cohesive DDoS defense against:

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



SecureWatch PLUS: Expert, continuous DDoS Defense Service

The SecureWatch PLUS premium service provides the unique combination of a powerful on-premise DDoS product and specialized anti-DDoS services tailored to each customer's specific needs. The three-stage service includes:

- **Preparation:** Configuration of DDS based on business requirements, corporate policy and DDoS defense best practices; development of an incident response plan
- **Vigilance:** 24x7 monitoring to deliver real-time alerts to the customer and Corero Security Operations Center
- **Response:** Immediate response to an attack, continuous engagement until final resolution and post-incident assessment.

SecureWatch PLUS is a continuous, collaborative program engaging the customer and their trusted partner, Corero. (Corero also offers SecureWatch, a limited 8x5 DDoS Defense System maintenance service that ensures the solution is always up to date, running at peak performance, and available to protect the IT infrastructure.)

Threat Update Services Optimized for DDoS Defense

Threat Update Services is an automated protection service that provides Corero DDS customers with proactive protection against DDoS attacks and ongoing mitigation of security issues. Threat Update Services delivers frequent protection pack updates to continuously enhance and maintain currency of the security provided. 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.

Robust Protection without Sacrificing Network and Application Performance

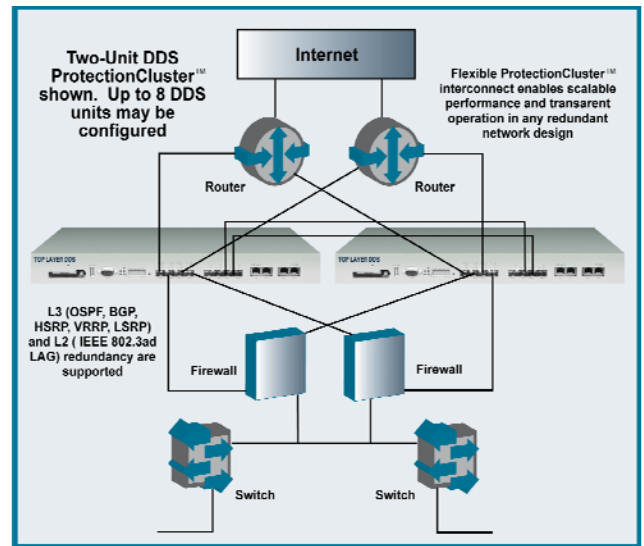
Corero's Core Platform, based on Tileria multicore processors and CoreOS software, provides real-world protection at real-world performance levels. To properly defend networks and critical online assets against today's threats, Corero delivers high levels of inline protection at industry-leading performance levels while minimizing latency, a critical factor when deploying security devices in a network. DDS includes models ranging in performance and capacity to handle throughputs from 300Mbit/sec to 10 Gbit/sec.

Corero DDoS Defense System

ProtectionCluster™ Scalable, Transparent High Availability

The Corero DDS ProtectionCluster can be deployed in configurations of up to eight parallel units and is recommended for deployments requiring system throughput up to 20 Gbit/Sec or more. With Corero's deep networking experience, 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



Low Latency

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.

Easy to Deploy and Manage

With highly flexible policies, the solution can be deployed at any number of key areas in your network infrastructure, providing perimeter security, protection of critical servers, remote access and extranet entry points, and interdepartmental segmentation. Corero provides powerful DDS management through an easy-to-use firewall-like interface.

Detailed Real-Time Incident Response

Corero's 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.

Green Design

The energy-conserving design of DDS requires only 1RU of rack space for most models, and has low power consumption. DDS fits right in with initiatives to cut back on space and reduce cooling requirements and consumption of electricity.

Centralized Management System

Corero's Network Security Analyzer 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. It features:

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



“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 Stienon
Chief Research Analyst, IT-Harvest*

Patented Technology

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

Some of the technologies the DDS implements are:

- Policy-based rules that limit traffic rates
- 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
- Sophisticated session analysis to defend against application level resource depletion attacks

Corero DDoS Defense System

Technical Specifications

Order Part Number	DDS 75 EC	DDS 150 EC/ES	DDS 500 EC/ES	DDS1000 EC/ES	DDS 2000 ES	DDS 2400 ES
Interfaces						
Copper 10/100/1000 Ethernet ports	4 + 2 MGMT	8 (EC Models only) + 4 MGMT			2 MGMT	
Pluggable 1G Ethernet ports (SFP modules)	0	8 (ES Models only)				
Pluggable 10G Ethernet ports (SFP+ modules)	1 Serial, 1 USB 2.0				4	
Other ports (Serial Console, Auth, Service)	Internal, 2 port-pairs	1 Serial, 1 USB 2.0			2 Serial, 2 USB 2.0	
Performance						
Target Network Capacity	In-line 100BASE-TX Networks & Lightly Utilized Gigabit Ethernet Networks	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	300 Mbps	600+ Mbps	2.4 Gbps	4.4 Gbps	8 Gbps	10 Gbps
Typical Latency ¹	<35 uSec	< 35 uSec	< 35 uSec	< 35 uSec	< 35 uSec	< 45 uSec
Typical Inspected Latency ¹	<50 uSec	< 50 uSec	< 50 uSec	< 50 uSec	< 50 uSec	< 60 uSec
MAX Concurrent Sessions	128,000	256,000	1 Million	2 Million	4 Million ²	8 Million ²
MAX Session Setup/Teardown	15,000/Sec	40,000/Sec	40,000/Sec	40,000/Sec	50,000/Sec	100,000/Sec
MAX SYN Flood DoS Protection Rate	150,000/Sec	500,000/Sec	1,000,000/Sec	1,500,000/Sec	2,000,000/Sec	3,000,000/Sec
ProtectionCluster Capable	No	Yes	Yes	Yes	Yes	Yes
Device Management						
Management Interfaces	Two (2) 10/100/1000 Mgmt Ports	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	ArcSight, Computer Associates, eIQ Networks, Forensics Explorer, GuardedNet, HP Openview, IBM Tivoli, netForensics, Open Service, RSA					
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	Single H/S PSU (2nd Optional)	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	<90W	< 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, CISPR22:2005+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(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, 2 nd Ed., CSA C22.2 No. 60950-1, 2 nd Ed., EN 60950-1, 2 nd Ed., IEC 60950-1, 2 nd Ed.					
International Compliance Approvals	UL Listed, CUL, AS/NZS 3260, CE, FCC Class A, VCCI Class A, ICES-003 Class A					

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

²Requires SWV7.X, otherwise 2 million for Model 2000ES, 4 million for Model 2400ES

About Corero Network Security

Corero Network Security, formerly Top Layer Security, is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) attack defense solutions that enable enterprise organizations to protect their critical on-line assets against risks associated with network-borne cyber-threats. Corero is headquartered in Massachusetts, U.S. with sales and services support worldwide.

Corero Network Security, Inc. 1 Cabot Road • Hudson, MA 01749 USA
+1.978.212.1500 • Fax +1.978.212.1600 www.corero.com
169 High Street • Rickmansworth • Hertfordshire WD3 1AY • +44.0.1923.897333
Copyright 2011 Corero Network Security, Inc., All rights reserved.