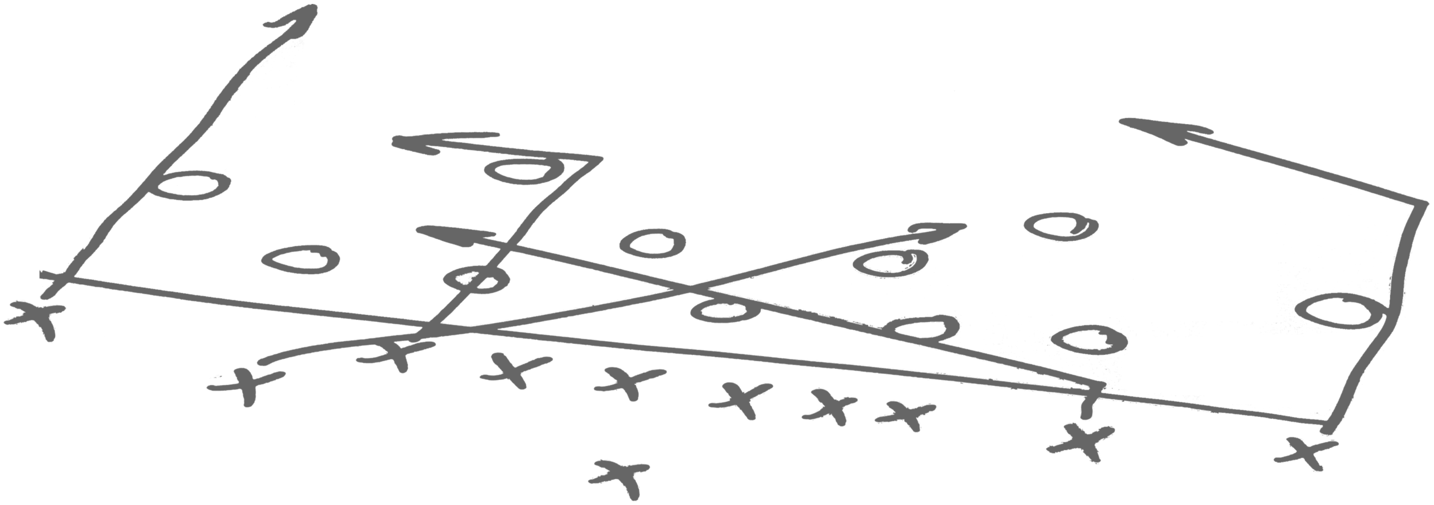
corero

FIRST LINE OF DEFENSE

Hosting Provider DDoS Protection Playbook



PLAYBOOK

INTRODUCTION

Distributed Denial of Service (DDoS) attacks are major threats to hosting providers as well as datacenter operators, and traditional game plans for protecting shared infrastructure should be revisited to better protect availability and allow hosting providers to potentially create incremental revenue streams. DDoS attacks can have a devastating impact on not only the customer under attack, but also on the hosting provider and other customers within the same shared network infrastructure.

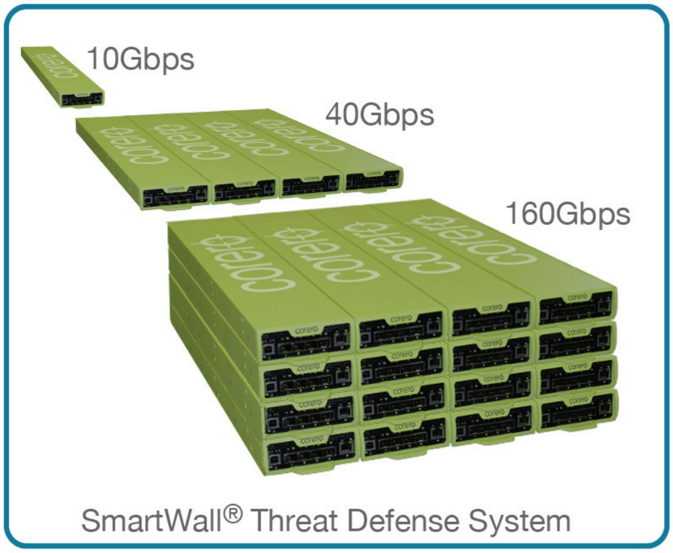
Hosting providers are often the targets for damaging DDoS attacks, since the number of customers they service and the aggregate Internet peering bandwidth they utilize greatly increases their attack surface. An attack on a single client of the provider—such as a high-traffic gaming service—can create major collateral damage to other hosted customers. These innocent bystanders are placed in the unfortunate situation of suffering from second-hand (damage) because they are hosted on the same shared facilities as the intended victim, and the results can be devastating for both the provider and their customers.

Hosting providers and their customers can experience hours or even days of downtime, and the situation is becoming more challenging due to the increased accessibility of tools and limitless attacker motivations. The sophistication and sheer brute force of recent attacks suggests an escalation of tactics to new levels of severity. As the size, complexity and regularity of DDoS attacks on hosting providers and their customers continues to increase, providers have to field new plays to mitigate risks and avoid the crippling downtime that comes with being the victim of DDoS attacks.

Few hosting providers today offer sufficient protection from DDoS attacks, so those that can implement robust DDoS attack protection will be able to more efficiently protect their hosted infrastructure and gain a competitive advantage in the marketplace. They'll also be positioned to create incremental revenue streams from high-value, managed DDoS attack protection services.

THE FIRST LINE OF DEFENSE

The Corero First Line of Defense® solutions offer hosting providers the ability to offer comprehensive DDoS and cyber threat protection to their hosted customers as an extension of their current service offerings, improving the overall value proposition and providing an opportunity to offer differentiated, value-added security services.



The Corero SmartWall® Threat Defense System (TDS) for hosting providers is architected to overcome the challenges associated with a wide range of hosting requirements, such as maintaining highly available applications, supporting mission-critical systems and delivering maximum levels of reliability. Providers that work with Corero to deploy always on DDoS attack mitigation services can expect the highest levels of performance and security.

The Corero SmartWall TDS is a purpose-built family of network security appliances that is configurable to meet the needs of hosting providers. These appliances deliver comprehensive threat defense services in rapidly scalable deployments for higher performance, greater connectivity and broader functionality than previously possible.

THE FIRST LINE OF DEFENSE (cont.)

This unique, slim-line appliance family delivers 10 Gbps full-duplex performance in a ¼ wide, 1 RU form factor. Hosting providers can deploy a combination of SmartWall TDS appliances to deliver the performance, connectivity and security required. Customers benefit from progressive inspection, threat detection and policy-based protection with always on visibility at any throughput—1 RU delivers 40 Gbps, and 4 RU delivers 160 Gbps. SmartWall TDS appliances simultaneously provide continuous visibility and security policy enforcement at layers 3 - 7 for both IPv4 and IPv6 traffic. SmartWall TDS provides the First Line of Defense against DDoS attacks for hosting providers, and is available in several appliance models, including:

> The Corero SmartWall Network Threat Defense appliance provides continuous visibility and security policy enforcement so that hosting providers can establish a proactive First Line of Defense for inspecting traffic, detecting threats and blocking attacks. It is capable of mitigating a wide range of DDoS attacks while maintaining full service connectivity and availability to avoid degrading the delivery of legitimate traffic. The SmartWall Network Threat Defense appliance is designed to handle volumetric network based DDoS attacks or floods, reflective amplified spoof attacks, like DNS and NTP attacks, as well as application layer attacks that are typically too low to be detected by out of band solutions—such as slow loris, slow read etc.
>
> The Corero SmartWall Network Bypass appliance is also deployed by hosting providers for DDoS protection in high-availability deployments. It delivers transparent 10 Gbps full-duplex performance for network bypass, monitor or insertion. The SmartWall Network Bypass appliance has two passive fiber ports for 10 Gbps of zero power optical bypass and two active 10 Gbps SFP+ ports for monitoring and active inline processing. Multiple configurable protection modes are supported, including power-fail, manual bypass, programmatic bypass and automatic heartbeat detection. It delivers 100% network connectivity to hosting providers, eliminating downtime of their Internet presence due to power or equipment failures, or during maintenance windows.
>
> The Corero Network Forensics appliance can continuously record traffic and simultaneously retrieve specific historical packet captures for subsequent analysis of network packets, flows and trends over time. It provides the raw data for detailed visibility into detected threats and anomalous usage patterns, enabling robust network forensic analysis for regulatory compliance, corporate security incident response and law enforcement reporting.

Centralized operational management of multiple SmartWall TDS appliances minimizes IT overhead, speeds deployments and streamlines provisioning. Corero offers multiple integration options for configuring, controlling and monitoring the appliances including a flexible browser-based GUI, a full SSH CLI and powerful REST API that supports open integration with existing management frameworks.

Centralized management of the SmartWall TDS is performed via secure connection to the Corero Management Server (CMS). The CMS includes a dashboard for monitoring threat activity and viewing key security events. The SmartWall Network Threat Defense appliance family provides seamless integration with Security Information and Event Management (SIEM) and Operational Intelligence solutions, such as Splunk.

DEPLOYMENT SCENARIOS

Enterprises are increasingly calling on hosting providers to assist them in the detection, analysis and mitigation of DDoS attacks before they have an impact on their operations, and hosting providers can deploy the SmartWall TDS inline to ensure always on DDoS attack mitigation services while benefitting from the highest levels of performance and security.

Unlike strictly out-of-band scrubbing solutions that detect DDoS threats and subsequently generate alerts that require an operator to take action, which can take considerable time, possibly leaving the environment under attack in some cases for multiple hours, the SmartWall TDS solution is designed to be deployed inline and respond in real-time. Alternatively, SmartWall can be deployed as an out-of-band scrubbing solution for customers that prefer this method of mitigation.

While inline deployment is the preferred way to achieve instantaneous detection and mitigation of DDoS attacks, the Corero NTD is a superior component for high-performance scrubbing centers where false positives cannot be tolerated. Legacy scrubbing center solutions have not been designed for inline deployment and therefore exhibit significant packet loss when under attack – significantly impacting legitimate traffic contained within the flows directed for scrubbing. Additionally, for large bandwidth scrubbing centers, operators can add bandwidth in 10 Gbps increments with the Corero Network Threat Defense solution as their scrubbing needs evolve.

DEPLOYMENT SCENARIOS (cont.)

The SmartWall Network Threat Defense appliance inspects network traffic, analyzes the packets and responds to the DDoS threat with absolute granularity and can mitigate the attack automatically. It employs a do-no-harm architectural philosophy that allows all good traffic to flow as intended, and surgically removes the attack traffic before it moves downstream, while never dropping any good traffic. SmartWall TDS appliances can be deployed in flexible, scalable configurations to help hosting providers combat the increasing menace of DDoS attacks. The following are a few typical deployment scenarios.

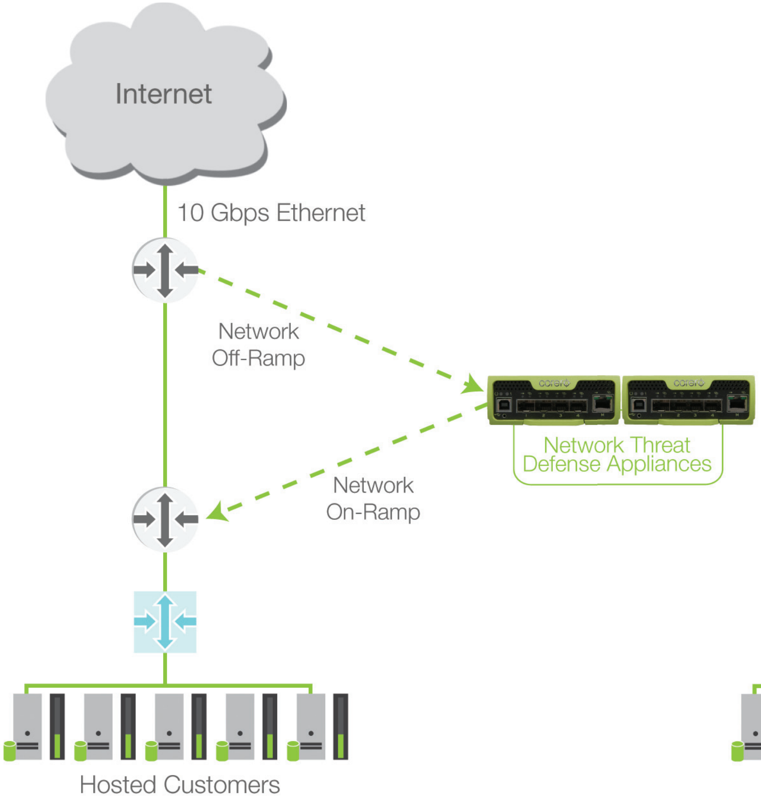
SCRUBBING CENTER

The traditional method of using an out-of-band scrubbing center is still a viable option, but it lacks the real-time visibility and rapid mitigation of inline DDoS protection deployments. Legacy scrubbing solutions are slow to detect attacks and even slower to mitigate because they require human intervention, which typically takes an hour or more.

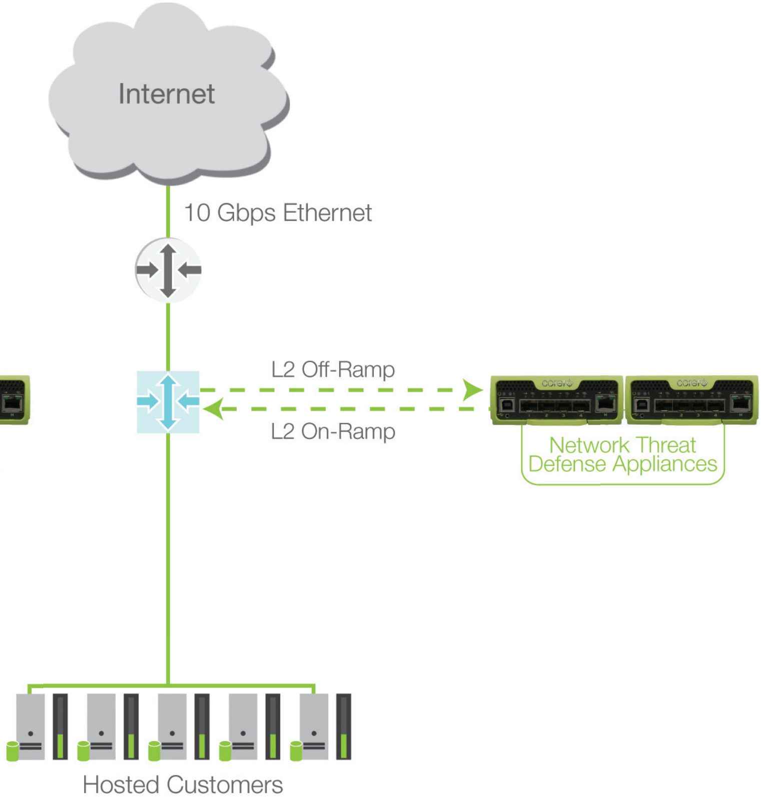
For companies that have already committed to the scrubbing center approach, the SmartWall TDS can be deployed into this scenario while offering hosting providers the ability to redeploy the SmartWall appliances inline in later implementations, thereby future-proofing DDoS mitigation investment.

With a scrubbing center deployment, suspect traffic flows are redirected to SmartWall Network Threat Defense appliances for traffic validation and scrubbing. When the SmartWall Network Threat Defense appliance is deployed offline between routers in a traditional implementation, questionable traffic is then redirected at 10 Gbps to the SmartWall Network Threat Defense appliances via a network off-ramp, where it is then scrubbed. Attacks are mitigated, and the cleaned traffic is sent back onto a network on-ramp at 10 Gbps.

Scrubbing Traffic in a Routing Scenario



Scrubbing Traffic at Layer 2



SCRUBBING CENTER (cont.)

Another, more efficient alternative scrubbing center deployment is to integrate the SmartWall Network Threat Defence appliances with Layer 2 switch technology to gain increased reliability and visibility. This will allow the hosting provider to mitigate DDoS threats more quickly because hosting providers will be able to detect threats more swiftly and reroute the traffic using VLAN technology.

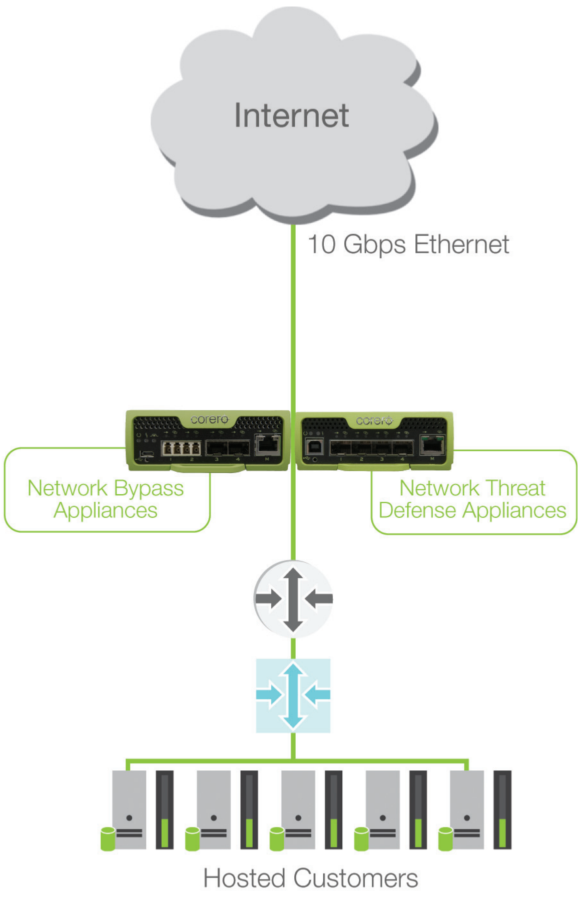
Corero recommends that hosting providers deploy one of the following inline DDoS protection solutions if possible. However, if a scrubbing center solution has been decided as the best option for the company, it is recommended to select one that provides the flexibility to support inline implementations in the future and implement scrubbing at Layer 2 if the architecture supports it.

FULL, HIGH-AVAILABILITY PROTECTED LINKS

Every hosting provider is measured on its ability to meet SLAs, and network connectivity is a key consideration for maintaining an always on Internet availability. This implementation allows hosting providers to provide inline DDoS protection with full, high-availability for a single 10 Gbps Ethernet link. SmartWall appliances are deployed between the Internet and the hosting provider networks to protect all infrastructure on the link south of the appliances from DDoS attacks.

All inbound traffic from the Internet flows into the SmartWall Network Bypass appliance at 10 Gbps and flows to the SmartWall Network Threat Defense appliance for DDoS attack mitigation. Then, clean traffic flows back to the SmartWall Bypass appliance and passes through the router and switch to hosted servers. The Internet link is fully protected from DDoS attacks all the way down to the servers. The routers, switches, firewalls, hypervisors and any other security layers located below the Corero equipment are protected from DDoS attacks and cyber threats.

High-Availability



Unlike scrubbing-only solutions, this scenario also provides symmetric protection capabilities for both directions of the network traffic which enables significantly more precise detection and mitigation. Additionally, all outbound traffic can be inspected by the SmartWall Network Threat Defense appliance for DDoS attack mitigation purposes.

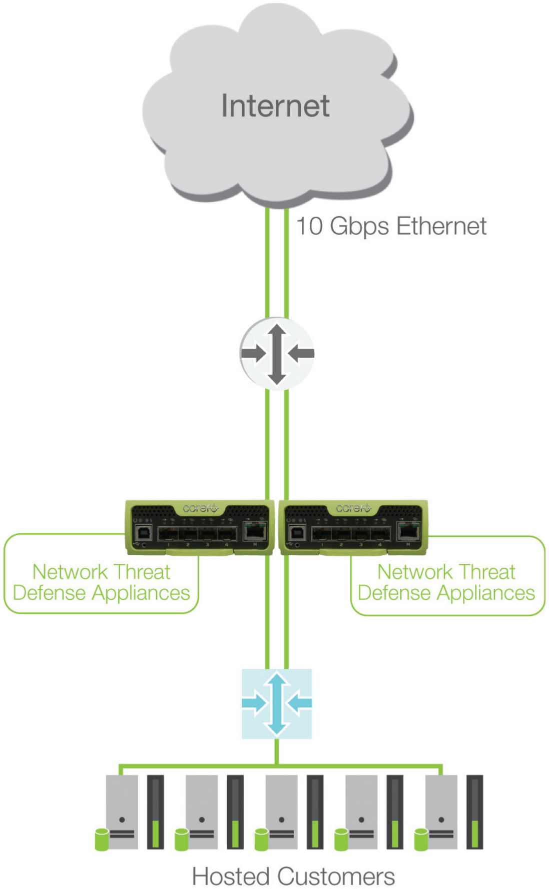
In the remote event that the SmartWall Network Threat Defense appliance fails, the SmartWall Bypass appliance would detect the lack of a heartbeat and subsequently close the bypass, maintaining the connection from the Internet to the router and triggering an alert to the Corero Management Server (CMS) to notify operations staff to immediately address the issue. This allows hosting providers to ensure availability while avoiding the risk of the DDoS threat prevention equipment ever potentially becoming a blocking element in providing Internet connectivity. Even in the event of a power failure, the SmartWall Bypass appliance will maintain the network connection; another safeguard for ensuring high availability.

This solution has no blocking elements and no single point of failure; it allows hosting providers the ability to deliver full, high availability protected links that insulate hosting providers and their customers from the ravages that DDoS can deliver.

ACTIVE/ACTIVE HIGH-AVAILABILITY LINK PROTECTION

This deployment scenario allows hosting providers to benefit from active/active redundant link protection, and is an added level of resiliency to protect against a single link failure. The SmartWall Network Threat Defense appliances are deployed below the router. One active link is connected to each of the appliances from the router, and traffic can be distributed across the SmartWall appliances using the standard Link Aggregation Control Protocol (LACP) or any other standard load sharing mechanism. SmartWall appliances are transparent, so they can be deployed in a manner that does not affect any of the protocols utilized in the link sharing function.

Active/Active High-Availability Link Protection

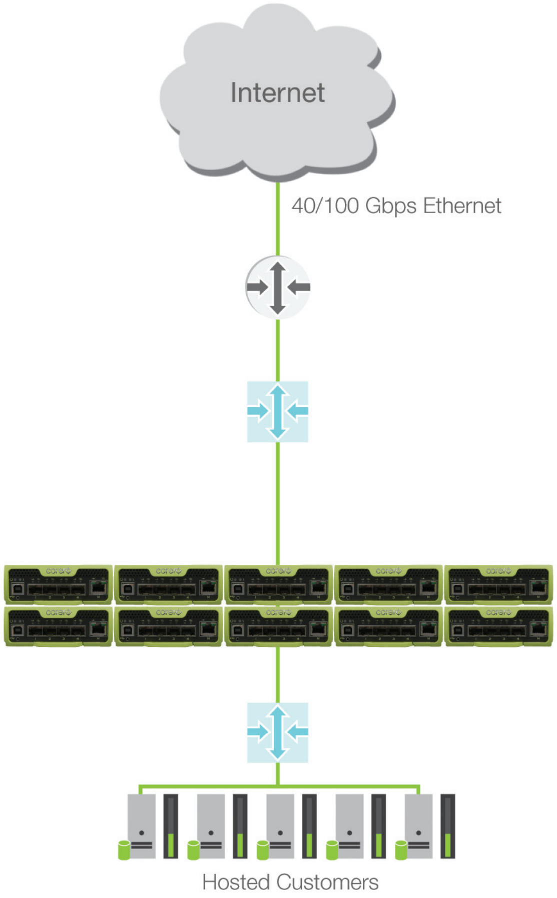

Internet
10 Gbps Ethernet
Network Threat Defense Appliances
Network Threat Defense Appliances
Hosted Customers

This deployment demonstrates that if a hosting provider loses a single link that the remaining active link will continue running live until the failed link is recovered. Optical bypass can optionally be deployed in this scenario to increase the availability of this solution. The scenario pictured does not offer protection for the router—but the SmartWall appliances could just as easily be deployed in an active/active scenario above the router and utilize Equal Cost Multi-Path (ECMP) routing to achieve similar result with the added benefit of protecting the router.

SCALED DDOS SECURITY ARRAY

This is an example of a large implementation that requires a scaled DDoS security array to protect a 100 Gbps Ethernet connection. The hosting provider delivers 100 Gbps DDoS protection by deploying 10 SmartWall Network Threat Defense appliances and using the link aggregation capabilities in the switches to distribute the 100 Gbps Ethernet connection to multiple 10 Gbps links.

Scaled DDoS Security Array



100 Gbps Line Rate DDoS 10X SmartWall® Threat Defense System

A DDoS security array offers hosting providers the ability to implement highly scalable, inline DDoS attack mitigation with N+1 redundancy and is ideal for large providers and providers with fast-growing Internet bandwidth.

GAINING VISIBILITY INTO DDOS ATTACKS

Corero offers hosting providers and data center operators comprehensive visibility into DDoS attacks and cyber threats that that can be integrated into existing operational support system (OSS) infrastructure utilizing a flexible GUI, a powerful CLI and a full REST API that allows integration with multiple management options. Hosting providers can rely on a single pane of glass for automated provisioning and reporting of events and alarms, and develop web portals to share monitoring and DDoS mitigation information with hosting customers.

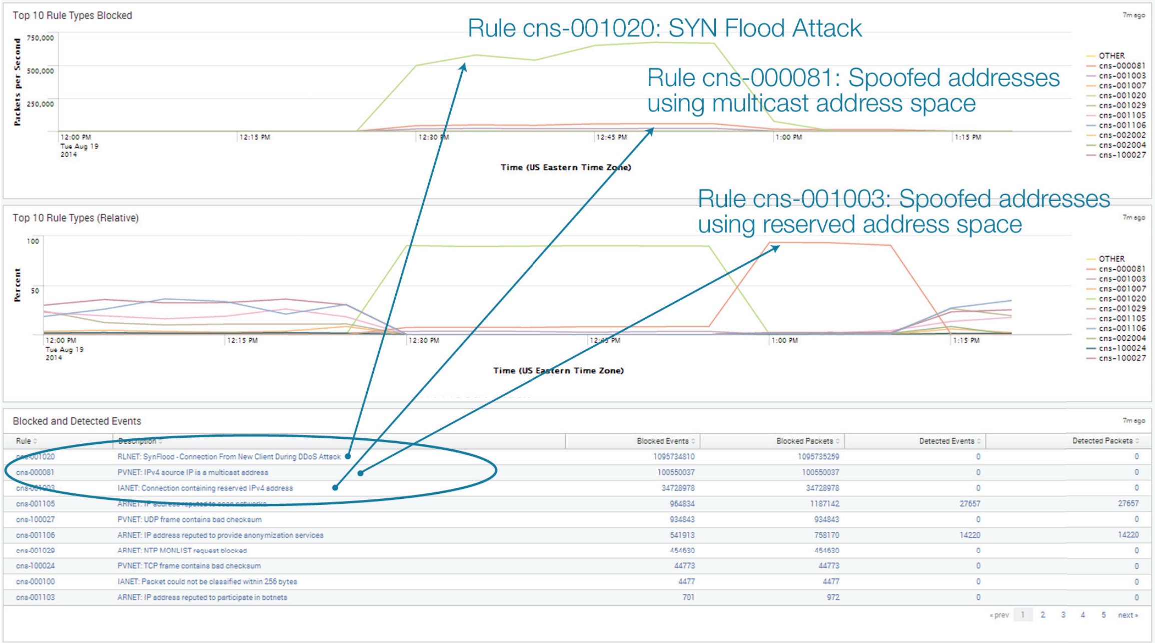
GAINING VISIBILITY INTO DDOS ATTACKS (cont.)

A significant challenge facing many organizations is how to extract meaningful real-time information on DDoS attacks and cyber threats from volumes of security events. To date, only minimal visibility into these classes of security events has been available, and only to organizations with significant investments in analytics tools and expert security staff; and in any case hosting providers and their customers are left to react to the threats after the damage has been done.

SecureWatch® Analytics is a powerful web-based security analytics portal that delivers comprehensive and easy-to-read security dashboards based on DDoS tailored security feeds from Corero First Line of Defense products. Large hosting providers and their enterprise customers can benefit from the targeted granular DDoS event data they have been lacking that complements their security event monitoring practice. All users benefit from the turn-key SecureWatch Analytics portal that delivers unprecedented DDoS and cyber threat visibility without requiring dedicated security analysts to sift through reams of unintelligible log data. SecureWatch Analytics is powered by Splunk, and it provides a portal that transforms the sophisticated Corero security feeds into dashboards of actionable security intelligence, exposing:

- Reflective amplified DDoS attacks
- Targeted application layer attacks
- Under the radar low and slow attacks
- Victim servers, ports, and services
- Malicious IP addresses and botnets

Security Visibility



Rule cns-001020: SYN Flood Attack

Rule cns-000081: Spoofed addresses using multicast address space

Rule cns-001003: Spoofed addresses using reserved address space

Blocked and Detected Events

Rule	Description	Blocked Events	Blocked Packets	Detected Events	Detected Packets
cns-001020	RLNET: SynFlood - Connection From New Client During DDoS Attack	1095734810	1095735259	0	0
cns-000081	PVNET: IPv4 source IP is a multicast address	100550037	100550037	0	0
cns-001003	IANET: Connection containing reserved IPv4 address	34728978	34728978	0	0
cns-001105	ARNET: IP address reputed to scan networks	964834	1187142	27657	27657
cns-100027	PVNET: UDP frame contains bad checksum	934843	934843	0	0
cns-001106	ARNET: IP address reputed to provide anonymization services	541913	758170	14220	14220
cns-001029	ARNET: NTP MONLIST request blocked	454630	454630	0	0
cns-100024	PVNET: TCP frame contains bad checksum	44773	44773	0	0
cns-000100	IANET: Packet could not be classified within 256 bytes	4477	4477	0	0
cns-001103	ARNET: IP address reputed to participate in botnets	701	972	0	0

Empowered by this enhanced visibility, hosting providers can utilize SecureWatch Analytics to visualize and mitigate DDoS attacks and cyber threats. Additionally, Splunk customers that have the SmartWall Threat Defense System can access the DDoS Analytics for SmartWall® App from Splunk Base, allowing for seamless integration within their existing Splunk reporting and analytics environment.

Hosting providers can also utilize the SmartWall Network Forensics appliance to capture packet flow data to disk at 10 Gbps line rates to gain forensic visibility into network traffic, with storage of captured data distributed to iSCSI arrays via dual 10 Gbps network interfaces. It provides line-rate Internet traffic capture to support visibility into DDoS attacks and cyber threats. Hosting providers can capture the necessary data to feed historical analysis of cyber threat activity, including identification of attack vectors, fingerprinting attacker identity, breach characterization as well as intelligence gathering for preparation against emerging threats.

CREATING ADDITIONAL REVENUE STREAMS

Hosting providers have an obligation to their customers to adequately protect them against DDoS attacks. Enterprise customers don't want to move their unprotected services to an unprotected cloud, so hosting providers have the opportunity to differentiate their services through their DDoS security infrastructure. Before customers consider migrating to hosted services, they need to be sure that their provider has adequate First Line of Defense DDoS protection measures in place.

As more organizations migrate critical applications and services to hosted environments, the premium placed on security is becoming increasingly important. Hosting providers that can document and demonstrate the value of their DDoS mitigation capabilities can position themselves to offer tiered services with premium pricing based on the level of advanced DDoS mitigation capabilities a customer requires.

With First Line of Defense protection from Corero, providers can offer cleaner transport streams that are better protected from volumetric DDoS attacks. Providers are now enabled to offer creative new offerings, such as DDoS and cyber threat protection, enhanced security SLAs as well as visibility and reporting through an analytics portal that can be leveraged as a comprehensive virtual Security Operations Center (SOC). This allows hosting providers the opportunity to to provide managed DDoS security services, such as 24x7 monitoring, alerting and reporting. The SmartWall Network Forensics appliance also offers hosting providers the ability to offer packet capture and retrieval as a value added security service to their customers.

Without advanced DDoS mitigation capabilities, providers risk losing customers and potential damage to their brand that may not be recoverable. By turning to a next-generation architecture with advanced DDoS and cyber threat protection—coupled with comprehensive visibility through analytics and reporting—hosting providers are now calling the plays for thwarting DDoS attacks. Hosting providers deploying this purpose-built First Line of Defense against cyber threats will be able to not only minimize churn but also create incremental revenue streams and longer-lasting customer relationships.

IMPLEMENTING 5 STEPS FOR DDOS PROTECTION

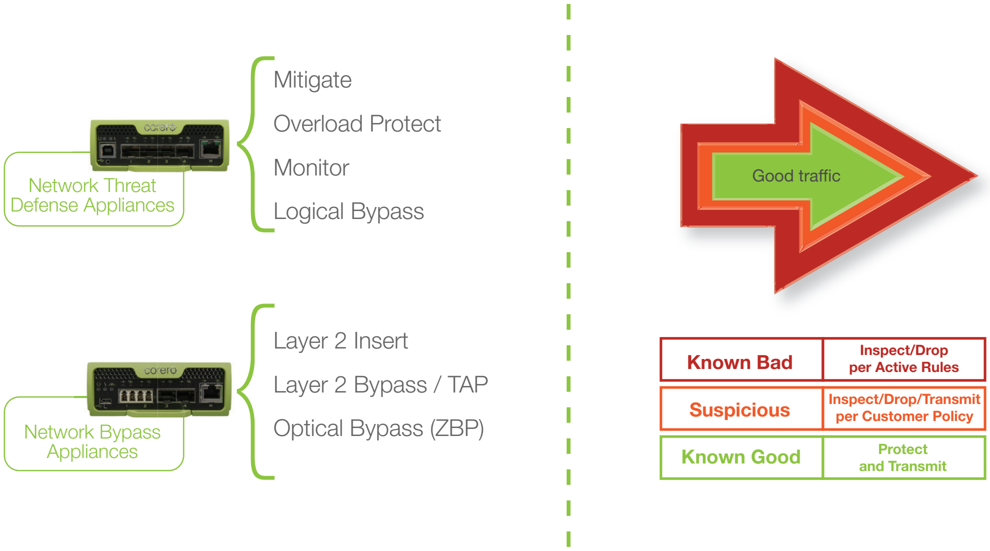
Hosting providers can re-write the defense against DDoS attacks, while enhancing their business models and building more profitable and longer-lasting relationships with their hosted customers. The following are a few clear actions that can change the playing field for improving DDoS protection:

1. **Deliver Comprehensive DDoS Protection:** Enterprises rely on their providers to ensure availability and ultimately protection against DDoS attacks and cyber threats. With a First Line of Defense against DDoS attacks deployed, providers are protecting their customers from damaging volumetric threats directed at or originating from or within the networks.
2. **Improve Visibility into DDoS Threats:** Hosting providers need clear visibility into the threats facing their infrastructure. Real-time reporting and alarm and event integration with back-end OSS infrastructure enables fast reaction times, scalable implementations and the analytics needed to understand the threat condition and proactively improve DDoS security.
3. **Implement Real-time Defense:** Providers need to change the play from deploying devices to monitor threats and generate alerts requiring manual/human intervention to deploying appliances that both monitor and mitigate DDoS threats automatically. Hosting providers can eliminate the delays incurred between the time a monitoring device detects a threat, generates an alert and an operator is able to respond.
4. **Enable Premium Services:** Hosting providers can offer baseline DDoS mitigation services to all customers, but for those customers who place a premium on high availability the provider can create value-added options and build incremental revenue streams while strengthening their brand.
5. **Move Inline Quickly:** If providers employ out-of-band devices in place to scrub traffic, deploy inline threat detection equipment that can inspect, analyze and respond to DDoS threats in real-time as soon as possible. Doing so allows you to protect higher-value assets and continue to leverage the legacy out-of-band devices as long as the provider can find a productive use for them. Inline threat detection is the only option for real-time mitigation. If scrubbing remains the preferred scenario for the organization, evaluate DDoS prevention solutions that support both scrubbing and inline DDoS prevention to future-proof the deployment.

DO-NO-HARM

As providers implement each of these 5 steps for DDoS protection, always remember to do-no-harm. One of the failings of traditional scrubbing center deployments is that they have not been architected with sufficient performance capabilities to execute their duties at line rate. They have been relegated to scrubbing center deployments where the solution can do the least amount of damage in the event of false positives. Providers should invest in a DDoS defense solution that is designed to never drop good traffic. Corero has architected the SmartWall TDS to allow the highest possible performance for DDoS attack and cyber threat protection without incurring any false positives. Providers need to have these capabilities in place to differentiate between good and bad traffic, and respond accordingly—always allowing the good traffic to pass un-interrupted.

Do-No-Harm Architecture



Known Bad	Inspect/Drop per Active Rules
Suspicious	Inspect/Drop/Transmit per Customer Policy
Known Good	Protect and Transmit

Do-no-harm protection ensures good traffic will always get though

The Corero SmartWall Threat Defense System can be deployed inline or as an out-of-band scrubbing solution to offer hosting providers and data center operators DDoS attack mitigation and protection against a continuously evolving spectrum of DDoS attacks. Hosting providers and data center operators can enhance defense-in-depth security architectures with an additional layer of security capable of inspecting traffic arriving from the Internet at line rate, in real time. Corero is an industry leader with over 500 active customers and over 8,000 units shipped.

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