# JUNIPER NETWORKS AND CORERO: A MODERN APPROACH TO DDOS PROTECTION AT SCALE

*Detect and mitigate volumetric DDoS attacks in real time with reduced cost*

### *Challenge*

*DDoS attacks are a significant part of today's threat landscape, and they continue to grow in magnitude, frequency, and sophistication. It is no longer feasible to address this growing problem with traditional out-of-band scrubbing centers and manual intervention approaches.*

### *Solution*

*Juniper and Corero have developed a revolutionary new defense against DDoS attacks, delivering line-rate detection and mitigation in real time at very large scale by leveraging always-on packet-level monitoring, automated machine analysis, and infrastructure-based enforcement across the network edge.*

### *Benefits*

- *Reduces DDoS mitigation costs by removing malicious traffic at the network edge*
- *Automates responses to stop DDoS attacks in seconds*
- *Improves visibility with always-on packet-level monitoring, delivering detailed actionable intelligence before, during, and after an attack*
- *Expands protection capacity to tens of terabits per second*

*Since the dawn of the Internet, malicious actors have used distributed denial of service (DDoS) attacks as a form of protest, to cause mischief, to sabotage competitors, and to retaliate against perceived wrongdoers. DDoS attacks flood websites, networks, and the cloud with an overwhelming amount of traffic, resulting in outages and service downtime and denying access to legitimate users who rely on service provider and enterprise networks for every facet of their day-to-day lives. Estimates say that the average cost of a DDoS attack to businesses rose to more than $2.5 million in 2017[1].*

## The Challenge

Today, almost anyone can easily launch a crippling distributed denial of service (DDoS) attack for less than $100—no coding experience required.

For-hire services have lowered the barriers of entry for criminals to carry out these attacks, both in terms of technical ability and cost. With the rise of the Internet of Things (IoT), connected devices have become a favorite target of hackers due to the massive scale they provide and the lack of basic built-in security. In 2016, the Mirai IoT botnet compromised nearly 100,000 connected devices globally; these devices were used to launch a DDoS attack against Domain Name System (DNS) service provider Dyn with a peak capacity of 1.2 terabits per second (Tbps), causing more than four hours of service disruption and downtime. Mirai was just the beginning; since then, variants such as JenX, Hajime, Satori, and Reaper have appeared, growing increasingly sophisticated and harder to defend against.

The growing availability of DDoS-for-hire services and the proliferation of billions of unsecured IoT devices have led to a significant increase in DDoS attacks. According to the latest DDoS Trends and Analysis report from Corero, organizations experienced an average of 237 DDoS attack attempts per month during the third quarter of 2017, an increase of 35% compared to the previous quarter and equivalent to eight attack attempts every day. The move to 5G mobile networks will only compound the problem by increasing available bandwidth, providing an even more robust pipeline for generating attack traffic from compromised connected devices.

[1] https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/

As DDoS attacks grow in terms of frequency, magnitude, and sophistication, traditional defenses such as out-of-band scrubbing centers and manual interventions have become woefully inadequate and cost-prohibitive. In the case of large volumetric attacks, redirecting suspicious traffic to a scrubbing center adds latency and imposes a significant financial burden, since mitigation costs are directly tied to the volume of the data traffic. Such a traditional approach also requires manual analysis and human intervention, which adds even more latency and cost to the remediation process. Using these methods, up to 30 minutes can elapse between detection and mitigation—unacceptable in an era where DDoS attacks can take websites down in a matter of minutes.

In an always-on world, where downtime is a huge problem for any business, service providers and enterprises must seriously re-examine their existing DDoS protection strategy and consider new techniques that deliver faster, more effective protection at a far lower cost. The IP network should be an integral part of the solution as the first line of defense against volumetric attack, while telemetry, machine analysis, and network programmability make the detection and mitigation process more intelligent, automated, and adaptable.

## The Juniper Networks and Corero DDoS Protection Solution

Juniper Networks and Corero Network Security have partnered to develop a joint solution for DDoS protection that self-heals the network through rapid identification, precise decision making, automated mitigation at strategic places in the network, and continuous monitoring (Figure 1).

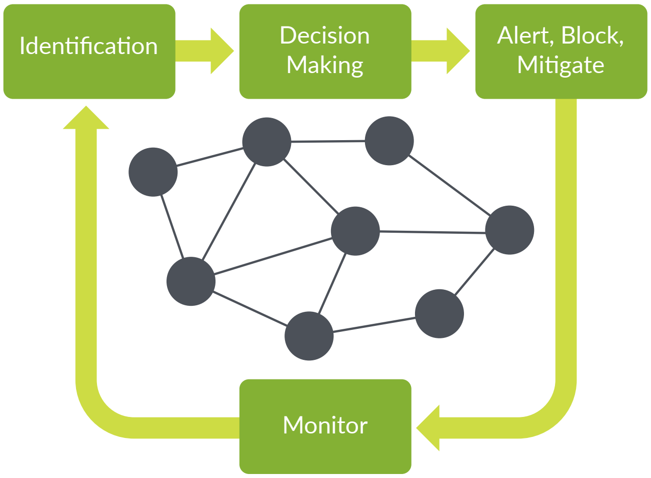

*Figure 1: Self-healing network*

Best practice for effective DDoS protection is to thwart attacks as close to the source as possible—typically at the edges of the network. Therefore, three common DDoS mitigation locations are service provider peering points, the data center edge, and the subscriber edge.

The joint Juniper Networks-Corero Network Security DDoS solution is highly effective, automated, and scales to multi-terabit capacity at a lower cost than any other available DDoS solutions. It works at the network's edge, employing the following techniques to detect and mitigate DDoS attacks (see Figure 2):

- Juniper Networks® MX Series 5G Universal Routing Platforms, deployed at the network edge, monitor ingress traffic via sampled mirrors that include both header and payload and can dynamically scale with the attack to adapt to the size of the threat.
- MX Series routers forward sampled mirrors to the Corero SmartWall Threat Defense Director (TDD), which inspects every packet in the feeds to quickly and accurately detect any DDoS attack traffic using a combination of rule-based and machine analysis.
- Within seconds, TDD will identify any attack and automatically generate flexible firewall match filters to mitigate the attack via the MX Series routers.
- TDD automatically configures the MX Series routers via Network Configuration Protocol (NETCONF) to install an ephemeral configuration that applies filters to block DDoS packets at the ingress point closest to the source of the disruptive traffic. Just as critical, good traffic is allowed to flow to its intended destination, without any forwarding performance degradation.
- Streaming telemetry on the MX Series routers forwards allowed/blocked traffic statistics to Corero SmartWall TDD.
- SmartWall TDD SecureWatch Analytics delivers comprehensive visibility into network traffic before, during, and after any attack. This Splunk-powered application provides the operations team with attack summaries and other detailed actionable intelligence on the efficacy of the mitigation process.

This process will continue throughout the life cycle of the attack until the mirrored samples indicate the ingress points are no longer under attack, at which point the SmartWall TDD will remove the filters on the MX Series routers and resume normal operations. Mirrored samples and streaming telemetry continue to flow from the MX Series routers to Corero's TDD, ensuring that traffic flows are back to normal while monitoring for the next attack.

This operational model is completely automated, ensuring that business operations are fully protected and visibility is always provided to the operations team.

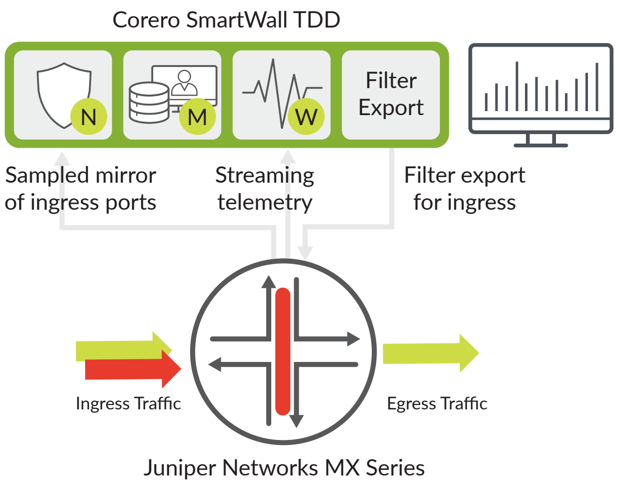

*Figure 2: Juniper + Corero DDoS protection joint solution*

## Features and Benefits

The joint Juniper-Corero DDoS defense combines the benefits of inspecting traffic at the packet level with the power of infrastructure-based enforcement, enabling real-time, automatic mitigation of DDoS attacks at unprecedented tens of terabits scale—all while significantly reducing costs.

### Reduced Cost of DDoS Mitigation

By leveraging existing filtering capabilities in the MX Series 5G Universal Routing Platforms, malicious traffic is removed at the network edge in a distributed fashion. Rather than redirecting all traffic under attack to an out-of-band centralized scrubbing center, adding latency and expense, this approach helps service providers and enterprises vastly reduce the DDoS mitigation service costs associated with such traffic volumes while avoiding expensive capacity upgrades. In addition, more than 95% of the joint protection is fully automatic, without any operator or analyst intervention. This dramatically lowers TCO compared to solutions that rely on traditional, manually intensive approaches.

### Faster Response and Improved Customer Experience

Automation means that DDoS attacks are identified and blocked in a matter of seconds—a considerable improvement over traditional approaches that rely heavily on manual intervention, which can take 30 minutes or longer. Speed matters, and by selectively blocking just attack packets while leaving legitimate traffic to continue flowing, the joint Juniper-Corero solution ensures that customer business is not impacted, even during a peak attack.

### Improved Visibility, Resource Efficiency, and Mitigation Efficacy

The joint Juniper-Corero solution enables always-on monitoring at the packet level. Compared to traditional flow-based detection approaches, packet-based inspection increases efficacy and gives operators greater visibility into not only header information but also payload data. Additionally, compared to IP Flow Information Export (IPFIX) protocol, sampled mirroring imposes a very light load on router resources since the router does not have to aggregate and process large amounts of data. Finally, the joint solution doesn't require rip-and-replace; it works seamlessly with existing solutions in a layered DDoS defense model where IP edge routers at the network perimeter are the first line of defense, offloading volumetric attack traffic and using centralized scrubbing resources to cope with more sophisticated application-layer attacks.

### Tens of Terabits of Scalability

Corero SmartWall TDD scales up to 40 Tbps of line-rate mitigation capacity, without the need to backhaul DDoS traffic across the network. Combined with MX Series 5G Series Universal Routing Platforms and their ability to scale up to 80 Tbps of packet forwarding, the joint solution delivers the highest scalability on a single DDoS mitigation system available in the market today.

## Solution Components

### Corero SmartWall Threat Defense Director

Corero SmartWall TDD represents a breakthrough in real-time volumetric DDoS defense, offering the following features:

- Scalable to tens of terabits of volumetric monitoring and mitigation
- Packet-level inspection for accurate volumetric DDoS detection
- Automatic filtering via machine analysis, for intelligent mitigation
- Real-time response, with time-to-mitigation measured in seconds
- Closed-loop feedback to eliminate false positives
- Full log resolution for seconds, minutes, days, weeks, months, and years
- Packet sample forensics of both allowed and blocked traffic
- Splunk-powered analytics, reporting, alerting, and automation
- Open integration APIs for autonomic response and SecOps
- Mitigation signaling via BGP, NETCONF, Representational State Transfer (REST), JavaScript Object Notation (JSON), and cloud

### Juniper Networks MX Series 5G Universal Routing Platforms

MX Series platforms deliver a robust portfolio of SDN-enabled routers that offer the following features:

- Unparalleled system capacity, density, security, and performance

- Industry-first inline data plane security with no compromise in throughput performance
- Progressive support for future innovations with infinite programmability
- Accelerated service delivery with automation
- Multiservice network and node slicing capabilities that provide up to 40% TCO savings
- Reduced downtime risk with Junos® Continuity and unified in-service software upgrade (unified ISSU)
- Unmatched network and service availability with a broad set of resiliency features
- Ability to treat traffic on a per-application basis with deep packet inspection (DPI)
- Streaming of component-level data to monitoring and analytics tools via Junos Telemetry Interface (JTI)
- Unrivaled space and power efficiency

## Summary—A Modern Approach to DDoS Protection in Real-Time at Scale with Reduced Cost

In the era of multicloud, IoT, and 5G, cybersecurity threats are constantly evolving. DDoS attacks in particular are continuing to increase in magnitude, frequency, and sophistication, and service providers and enterprises alike need to explore ways to augment their existing defenses with solutions that offer faster, more effective protection at a lower cost.

The IP network should be an integral part of the modern security solution as the first line of defense against volumetric attacks. Telemetry, machine learning analytics, and network programmability can make the detection and mitigation process more intelligent, automated, and adaptable.

The joint Juniper-Corero DDoS protection solution combines the benefits of inspecting traffic at the packet level with the power of infrastructure-based enforcement, enabling real-time, automatic mitigation of DDoS attacks at unprecedented tens of terabits scale while significantly reducing cost.

### Next Steps

To learn more about how Juniper Networks and Corero can help your company secure your network from malicious DDoS attacks, contact your Juniper or Corero sales representative.

## About Corero

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 DDoS threats to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics, and reporting. This industry-leading technology provides cost-effective, scalable protection capabilities 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.

## About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

**Corporate and Sales Headquarters**
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
**www.juniper.net**

**APAC and EMEA Headquarters**
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity