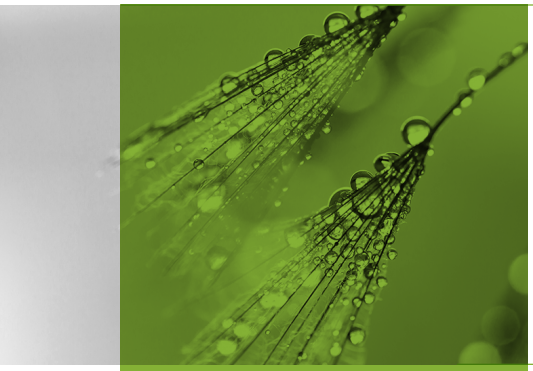

corero

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 blackholing, out-of-band scrubbing centers and manual intervention approaches.

Solution

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

Benefits

- *Reduces DDoS mitigation costs by leveraging routers at the network edge*
- *Automates responses to stop DDoS attacks in seconds*
- *Improves visibility with always-on packet-level monitoring*
- *Scales protection capacity anywhere from 50 Gbps to 40 Tbps*
- *Enables managed DDoS protection service offering*

Solution Brief

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.

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. At the same time, the ongoing rollout of 5G technologies has accelerated the proliferation of connected devices such as IoT, making it even easier to recruit a botnet army to launch DDoS attacks. Last year, we saw the largest DDoS attack took place—recorded at 2.3Tbps. We've also seen ransom-related DDoS attacks are on the rise, extorting organizations to pay millions of dollars.

As DDoS attacks grow in terms of frequency, magnitude, and sophistication, traditional defenses such as blackholing, 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 much more affordable price. 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 Integrated 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).

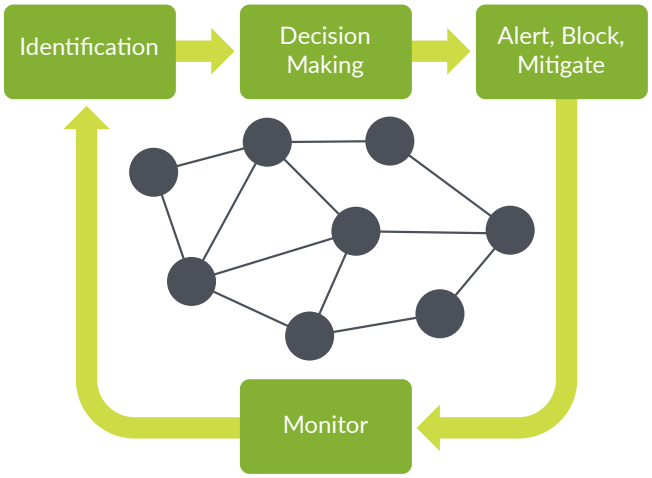

Figure 1: Self-healing network

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 anywhere from 100 Gbps to 40 Tbps capacity. It works at the network's edge, employing the following techniques to detect and mitigate DDoS attacks (see Figure 2):

- Juniper Networks® MX/PTX Series 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/PTX 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/PTX Series routers.
- TDD automatically configures the MX/PTX 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/PTX 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/PTX Series routers and resume normal operations. Mirrored samples and streaming telemetry continue to flow from the MX/PTX 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.

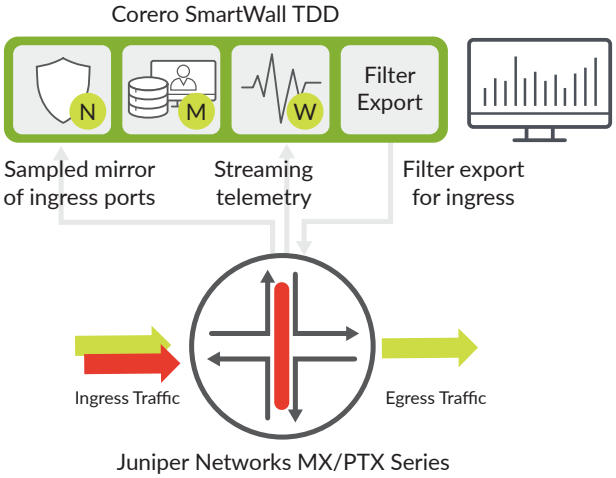

Figure 2: Juniper + Corero DDoS protection joint solution

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 the network edge, scaling from 50 Gbps to 40 Tbps—all while significantly reducing costs. The multi-tenant service portal enables providers to generate new revenue streams and stay competitive by offering managed DDoS protection services to their customers.

Reduced Cost of DDoS Mitigation

By leveraging existing filtering capabilities in the MX Series or PTX Series 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 Resource Utilization 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.

Mobile Network DDoS Visibility with GTP Payload Inspection and IP Intelligence Plug-in

The joint Juniper-Corero solution can look for attacks from the subscriber side of mobile networks. This is enabled by the new GPRS Tunneling Protocol (GTP) payload inspection feature. GTP is used in all mobile networks, including 5G. With SmartWall TDD's GTP payload inspection capability, mobile carriers can extract the tunnel endpoint identifier (TEID) inside the GTP header, then skip over the GTP header and look inside the encapsulated traffic to examine the packet payload. In addition, with the IP intelligence plug-in, carriers can track to which source country and to which ASN that the attack was coming from. With GTP payload and IP intelligence visibility, mobile carriers can identify malicious activity, inform the subscribers, and eventually stop the attacks. This way, mobile carriers can protect their brand reputation and even offer the protection as a value-add service to subscribers.

DDoS Protection Service with Service Portal and Tenant-Awareness

The DDoS protection and mitigation market was valued at $2.01 billion in 2018 and is projected to reach $5.59 billion by 2026, growing at a CAGR of 13.6% from 2019 to 2026. Offering DDoS protection services allow service providers to capitalize on high customer demand, develop a new revenue stream, and stay more competitive in the market. The SmartWall Service Portal is an optional component that enables service providers to offer DDoS protection as a managed service. Providers can define services levels and have the policy automatically matched and applied to the different tiers of defined services levels. They can view the aggregated traffic data and analyze attacks across the entire network, as well as viewing traffic data and attack activities on a per-customer basis. Additionally, their customers can log into their own view of the service portal and see the attack information that relates to their organization. This enables them to immediately see the benefit of the DDoS protection service both historically and in real time.

Flexible Traffic Control with BGP Policy and Multivendor Support

Today, when organizations encounter large-scale DDoS attacks, typically they either resort to blackholing or redirecting the traffic to a scrubbing center. With blackholing, certain tenant traffic can suffer from collateral damage and sometimes even go completely offline. Scrubbing services, which require backhauling the traffic and manual intervention, are often very costly. Now, as the joint Juniper-Corero solution supports BGP policy and multivendor network, organizations get the powerful middle ground where they can actually do more of the filtering themselves with upstream traffic control, preventing their links from being saturated. And then the payloads of remaining traffic on the links are inspected and attacks are mitigated with MX/PTX routers powered by the Trio chipset.

Solution Components

Corero SmartWall Threat Defense Director

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

- Automatic protection from "Carpet Bombing"/Subnet attacks
- Mobile Network DDoS visibility with GTP payload inspection
- Attack source country and ASN visibility with IP intelligence plug-in
- DDoS protection managed services offering with multi-tenant service portal
- Flexible traffic control with BGP policy and multivendor support
- 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/PTX Series Routing Platforms

MX /PTX 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. 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 security attacks. Telemetry, machine learning analytics, and network programmability can make the detection and mitigation process more intelligent, automated, and adaptable.

The joint DDoS solution with Corero furthers our strategy and commitment on realizing the Juniper Connected Security vision, enabling threat-aware networks for service providers and enterprises alike.

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.

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 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

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

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

3510657-005-EN Oct 2022