DDoS protection for high-speed networks

Challenge

Every minute of downtime, resulting from a DDoS attack, can cost tens of thousands of dollars and that's just the immediate financial loss. As a result of such attacks many service providers, hosting providers and the online enterprise lose millions and their reputation can be significantly harmed. Motivations for these attacks vary from political hacktivism to those looking for competitive advantage. Industry sources are reporting significant yearly increases in the number of DDoS attacks. Attacks of hundreds of Gigabits per second continue to grow in size and frequency and while typical attacks are much smaller, their surgically-crafted nature can make them equally as damaging.

Although these attacks have been around for over a decade, the scale and frequency of DDoS attacks are even outpacing the capacity of most providers to be able to absorb them. Due to their destructive nature, collateral damage, and ability to affect networks with relative ease, the approach to dealing with DDoS in a more automated matter has become a heightened priority for providers. The attack landscape is changing every day, and attackers are employing new techniques to increase the magnitude and sophistication of attacks and make them more difficult to mitigate using conventional approaches.

Solution

Internet providers are best positioned to eliminate DDoS attack traffic from transiting downstream to individual organizations. Network visibility, traffic analysis and attack detection, coupled with automatic, surgical attack mitigation capabilities are essential to eliminating the DDoS challenge closer to the source. If the deployment of in-line detection on each transit ingress point is not feasible, out-of-band detection offers an effective alternative. Leveraging network traffic statistics from edge routers, or dedicated network probes, can enable early enough detection of attacks, with a good understanding of their characteristics, to enable centralised, out-of-band, mitigation to be rapidly and accurately engaged.

The synonym for network visibility in ISP/Telco environments, is flow monitoring. Routers and switches are able to export aggregated traffic statistics based on packet flow from source IP address, source port, destination IP address, destination port and protocol. In addition, these statistics include the amount of transferred data, number of packets, TCP flags and other information from network layers 3 and 4.

There are various industrial standards corresponding to network equipment vendors:

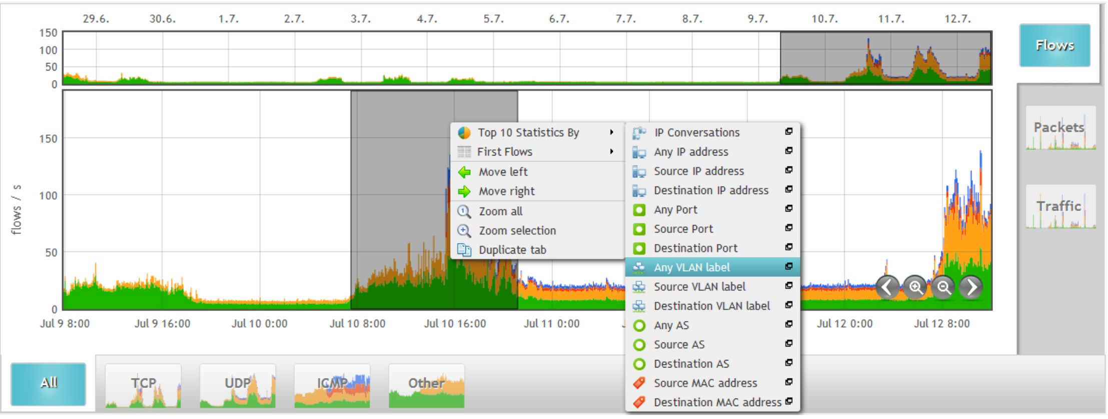
- sFlow – industry standard for packet data export and flow monitoring
- NetFlow – original flow monitoring standard introduced by Cisco
- jFlow – flow monitoring implementation available in Juniper routers
- NetStream – similar to NetFlow, available in Huawei network equipment
- IPFIX – latest international IETF standard, which is now adopted by many vendors

For out-of-band deployments, once an attack is detected in the flow data, dynamic attack signatures may be created, using BGP Flowspec, and the subsequent allowed network traffic is diverted to a dedicated DDoS mitigation solution which surgically removes the attack packets, while allowing only the legitimate traffic to continue unaffected. This attack detection and out-of-band mitigation ecosystem works seamlessly together to ensure uninterrupted network operations. And, when compared to in-line DDoS protection deployment, this approach can offer cost efficiencies, by taking the calculated risk of over-subscribing the available mitigation capacity, compared to the aggregate total for incoming transit or peering bandwidth.

Network visibility and attack detection

Flowmon provides the following components for advanced DDoS protection:

- **Flowmon Collector** – aggregation and storage of flow data, in all major industry formats, from an unlimited number of sources. The collector provides advanced tools to report and analyse network and application traffic.
- **Flowmon DDoS Defender** – scalable multi-tenant DDoS detection module for Flowmon Collector using dynamic baselines to detect various types of volumetric attacks and bandwidth consumption.
- **Flowmon Probe** – optional export of NetFlow/IPFIX data for infrastructures without flow-enabled network equipment.



Flowmon Collector equipped with the DDoS Defender module observes and profiles volumetric characteristics of network traffic to create and maintain dynamic baselines. In case of unexpected increases in network traffic, it creates dynamic attack signature and triggers configurable actions that include; alerting (email, syslog, SNMP trap), traffic diversion (policy-based routing, border gateway protocol, remotely triggered black hole or BGP Flowspec), script execution, or redirection through a dedicated out-of-band DDoS mitigation system. Flowmon DDoS Defender supports individual detection profiles that correspond to different IP ranges, subnets or network services. In the case where a DDoS attack is detected, all the attack characteristics, including; top source IP addresses, subnets, Autonomous Systems, countries, L4 protocols and interfaces, are part of the attack details.

Attack mitigation

The Corero **SmartWall® Threat Defense System** (TDS) DDoS mitigation solutions are the highest performing and most accurate in the industry, delivering automatic protection, up to multi-terabit scale, with the lowest total cost of ownership. Validated by independent testing firm, NSS Labs - earning the coveted "Recommended" rating, achieving high-performance and leading protection in all test categories - Corero's SmartWall TDS delivers real-time mitigation of DDoS attacks in seconds rather than minutes, allowing good user traffic to flow uninterrupted.

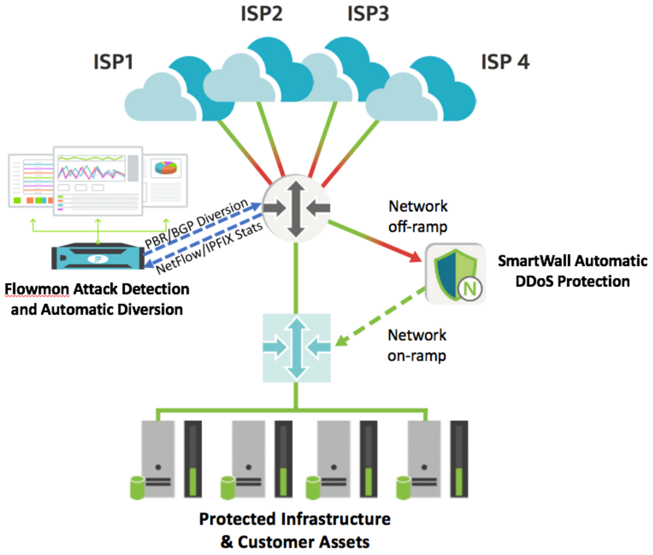
The SmartWall family of solutions are delivered as physical security appliances and in virtual form-factors, based on a purpose-built leading architecture, which delivers *surgical* DDoS mitigation, at wire-rate. The SmartWall TDS provides comprehensive real-time Layer 3-7 mitigation against volumetric attacks for both IPv4 and IPv6 traffic, including built-in protection against zero-day DDoS attacks.

DDoS protection ecosystem

Flowmon DDoS Defender, combined with Corero's SmartWall TDS, enables an ecosystem capable of delivering highly effective out-of-band DDoS mitigation. Traffic flows for attacks detected by Flowmon DDoS Defender are automatically diverted, using policy-based routing or BGP, to SmartWall TDS for rapid, automatic, surgical mitigation.

Deployment scenario

To better understand this DDoS protection ecosystem, let's assume the situation for a large national tier-2 ISP which delivers internet connectivity to tens of local tier-3 ISPs that cover various regions across the country. A typical tier-3 ISP may have multiple class-C subnets and a few gigabits of network connectivity that need to be protected against DDoS attacks. As a first step, the tier-3 provider deploys DDoS protection for their own infrastructure. However, that infrastructure is still vulnerable to attacks that consume more than their few gigabits of transit bandwidth, as their internet pipes will be full and, statistically, the volume of good traffic which can enter the pipe will be squeezed. So, even when the traffic is cleaned, there will still be an impact, due to the legitimate traffic which did not make it into the pipe.


ISP1
ISP2
ISP3
ISP 4
PBR/BGP Diversion
NetFlow/IPFIX Stats
Network off-ramp
SmartWall Automatic DDoS Protection
Flowmon Attack Detection and Automatic Diversion
Network on-ramp
Protected Infrastructure & Customer Assets

This is a classic use-case where DDoS protection benefits from being deployed at a higher level - the tier-2 ISP is better placed to provide effective DDoS mitigation for larger attacks. In this case, the tier-2 provider can utilise out-of-band DDoS mitigation. For out-of-band deployments; Flowmon Collector, with the DDoS Defender module, would monitor all edge routers of the tier-2 ISP, with individual Flowmon DDoS Defender detection profiles defined for each tier-3 ISP. In the case where the traffic baseline for particular tier-3 ISP is exceeded, a DDoS attack is detected and the following actions are performed:

- Network traffic for affected subnets is diverted to SmartWall using policy-based routing (PBR) or Border Gateway Protocol (BGP) updates.
- Operators can check attack status and characteristics directly in Flowmon DDoS Defender, as well as the SmartWall TDS Central Management Server.

About Flowmon Networks

Flowmon Networks is an international vendor of network and security solutions specializing in flow monitoring (NetFlow/IPFIX), Network Behavior Analysis (NBA), Application Performance Monitoring (APM) and on-demand packet capture. Companies across the globe rely on **Flowmon** solutions which enable them to get complete network visibility, report on traffic volumes and top-talkers, detect security issues and network anomalies as well as troubleshoot operation issues, on a daily basis.

About Corero Networks Security

Corero Network Security is the leader in automatic, high-performance, scalable DDoS defense solutions. ISPs, hosting providers and online enterprises rely on Corero's award winning technology to eliminate the DDoS threat, while providing complete visibility, analytics and reporting. This industry leading technology delivers cost-effective, real-time, scalable protection against DDoS attacks, in the most complex environments, with an economic model which enables significantly easier adoption than previously possible.

More Information

For more information, please contact your Corero or Flowmon Networks partner.

Corero Network Security
Corporate Headquarters
225 Cedar Hill Street
Marlborough, MA 01752
USA

EMEA Headquarters
Regus House,
Highbridge, Oxford Road
Uxbridge, UB8 1HR
England, UK

www.corero.com

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno
Czech Republic
www.flowmon.com