Modern DDoS Protection for Large Networks

Challenge

Over recent years, DDoS attacks have become especially worrisome to large high-speed network operators. Although this type of threat is nothing new and has been around for more than a decade, organizations are having increasingly hard time mitigating it. Why? Resources for initiating a DDoS attack are becoming more easily available, which means that the scale and frequency of the attacks are rapidly growing. The nature of a DDoS attack is such that if it is not detected before it reaches its target, the harm is done – and new inventive techniques to conceal the attacks emerge constantly, too.
All mentioned considerations mean that volumetric attacks today are more likely to succeed, and that their effects are more destructive than ever. Protecting the network from DDoS attacks is therefore a key challenge for Internet service providers and backbone operators.

Solution

Effective protection depends on stopping a DDoS attack as close to its source and as far from its intended target as possible. This requires several perfectly functioning and seamlessly integrated network devices that cover the following: network visibility, traffic analysis, attack detection, and attack mitigation.

Network visibility in an ISP/telco environment is ensured by flow monitoring, which provides insight and statistics covering all communication in the network. Flow data is continuously analyzed, ideally in combination with network traffic statistics from routers or dedicated network probes for improved precision. The analysis reveals upcoming attacks and their characteristics, essential for successful mitigation.

A detected incoming attack needs to be diverted to a dedicated out-of-band DDoS mitigation appliance. The device should be able to create a dynamic attack signature (for instructing other devices in the network and for later reference) and mitigate the attack so that legitimate traffic continues unaffected.

The whole procedure is rather complex and, as mentioned, requires a perfectly coordinated network ecosystem, able to detect and stop volumetric attacks while ensuring no impact on legitimate network operations.

Benefits

What is the benefit of an out-of-band mitigation appliance? Compared to in-line deployment, it provides higher scalability; a single device can protect multiple uplinks. Particularly in case of large high-speed networks with multiple peering partners, the cost efficiency of the out-of-band solution is remarkable.

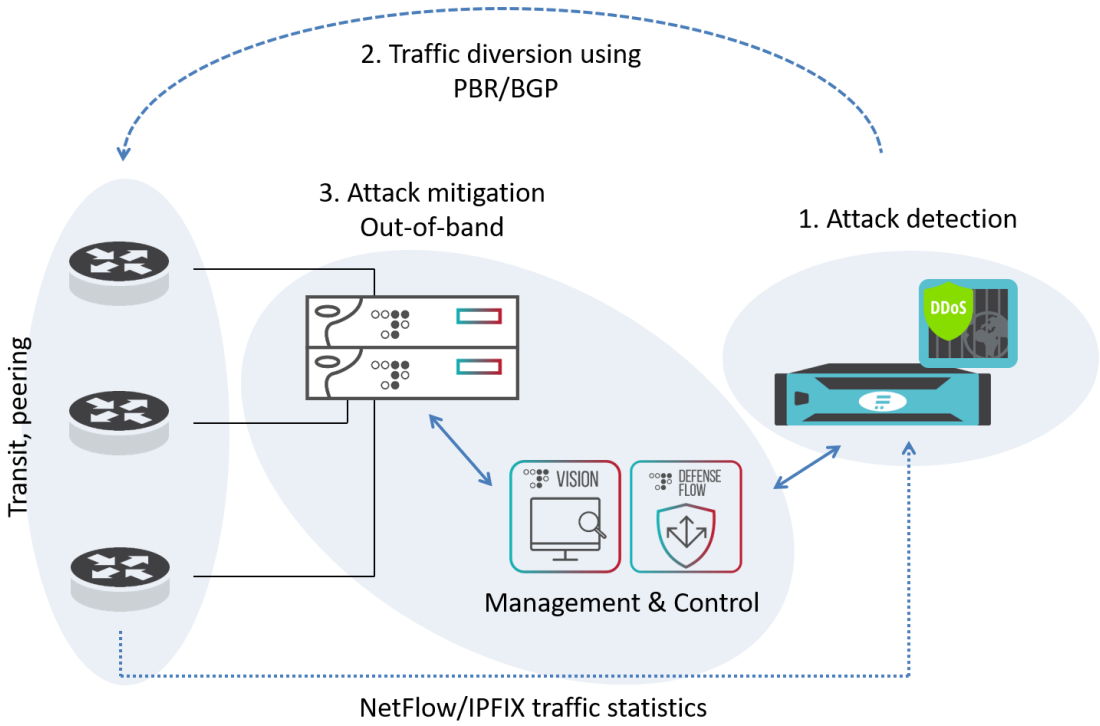
In-line appliances such as firewalls are still vital for the protection of so called “last mile”, to detect sophisticated attacks focused on application layer that do not expose themselves in high volume of network traffic. Overall, a multi-layered DDoS protection that combines out-of-band mitigation with in-line deployments is the most versatile and efficient solution for large network infrastructures.

Flowmon & Radware deployment

Flowmon Collector with the **DDoS Defender** module, **Radware DefenseFlow** and the **DefensePro** appliance together form a DDoS protection ecosystem suited to protect even the largest infrastructures and internet backbones.

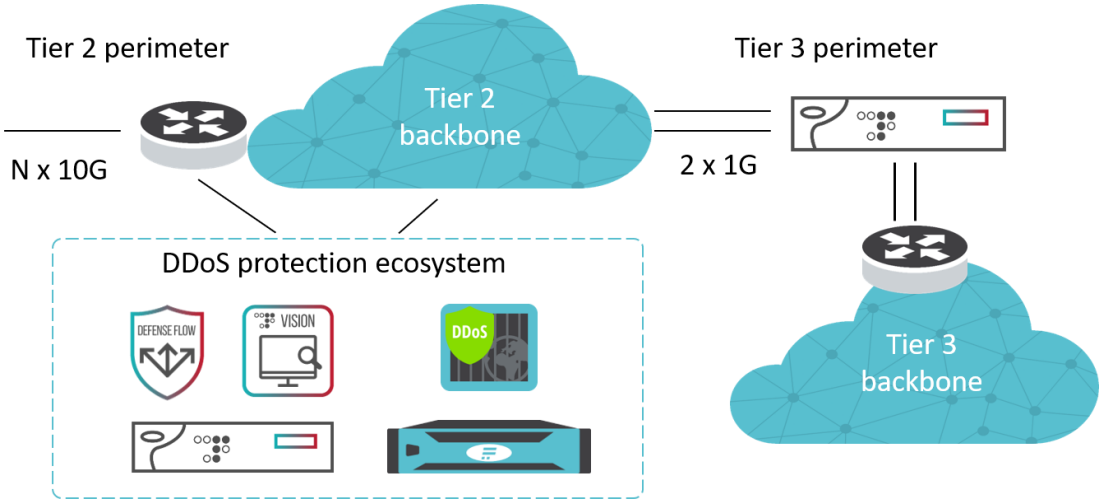
- **Flowmon Collector** aggregates and stores flow data in all major industrial formats from an unlimited number of sources. Collector provides advanced tools for reporting and analysis of network and application traffic.
- **Flowmon DDoS Defender** is a scalable multi-tenant DDoS detection module for Flowmon Collector. It uses dynamic baselines to detect various types of volumetric attacks and bandwidth consumption.
- **Radware DefenseFlow** is a network attack detection and cyber control application. It can detect extensive multi-vector attacks by applying its own patented behavior-based algorithms to traditional NetFlow statistics.
- **Radware DefensePro** is a network attack mitigation device that can be used both in-line and out-of-band to protect IT infrastructure against network and application downtime. The device uses patented signature technology to mitigate all kinds of network attacks in real time, automatically, and without blocking legitimate traffic.

The integration of **Flowmon Collector** and **DDoS Defender** with **Radware DefenseFlow** makes it possible to manage multiple **DefensePro** appliances via standard management interface. DDoS Defender also provides DefenseFlow with detailed attack parameters and standard network traffic baselines, which allows for dynamic configuration of the network protection profiles, making them very effective. Actions of the ecosystem in case of an attack are configurable, and include alerting (e-mail, syslog, SNMP trap), traffic diversion (policy-based routing for local ISPs, BGP support for Tier 1 networks, telcos and other large operators), and mitigation through the out-of-band DefensePro appliance.



Model scenario

To illustrate the functioning of a DDoS protection ecosystem and the roles of out-of-band and in-line deployment, let us assume a model Tier 3 Internet provider with multiple C-class subnets and a total network connectivity of 2 Gbps. The provider is one of tens of local Tier 3 ISPs who get Internet connectivity from a large national Tier 2 ISP. The task is to secure the model provider's service against various types of network attacks, on all levels, including layer 7.
Provision on the model provider's side: Deploying an in-line device with a capacity of 2 Gbps. This protects the network from layer 7 attacks and minor volumetric attacks of up to 2 Gbps.
However, the infrastructure is still vulnerable to attacks that consume over 2 Gbps of bandwidth. These fill the Internet pipes and overload the network, so cleaning the attack with own resources is not possible. This is a typical scenario that requires attack mitigation on a different level, in cooperation with the Tier 2 ISP.
The integrated Flowmon & Radware solution applied to this model scenario would work as follows:



Flowmon Collector continually monitors network traffics, collecting flow statistics from all edge routers of the Tier 2 ISP. The **DDoS Defender** module creates individual profiles for network subnets that correspond to specific Tier 3 ISPs. The profiles are based on dynamically calculated traffic baselines, and if a baseline for a specific profile is exceeded, it means that the corresponding Tier 3 ISP is under attack. In such a case, the protection system automatically triggers the following actions:

1. **Radware DefenseFlow** collects all relevant traffic statistics and previous baselines for the attacked network and provides it to the **DefensePro** appliance.
2. DefensePro uses the data to create a tailored protection profile.
3. DDoS Defender diverts all network traffic for affected subnets to DefensePro using either policy-based routing (PBR) or Border Gateway Protocol (BGP).
4. The attack in progress is continuously monitored. Its status and detailed characteristics (including top source 10 IP addresses, subnets, autonomy systems and countries, L4 protocols and interfaces) can be also reviewed in DDoS Defender directly.
5. When DefensePro confirms that the attack is over, the traffic is diverted back to its usual route. The ISP's users have not noticed any service disruption.

About Flowmon Networks

Flowmon Networks is an international vendor of network and security solutions specialized in Network Performance and Diagnostics (NPMD), Network Behavior Analysis (NBA), Application Performance Monitoring (APM), and DDoS protection. Companies over the globe rely on **Flowmon** solutions that provide them with deep network visibility, report on traffic volumes and top talkers, detect security issues and network anomalies, as well as troubleshoot operation issues on daily basis.

About Radware

Radware is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity, and achieve maximum productivity while keeping costs down.

Contact

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

Radware Ltd.
22 Raoul Wallenberg Street
Tel Aviv 69710
Israel
www.radware.com

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