Managing DDoS Through Cooperation

Over the years DDoS attacks have come in many forms. In the early days, attacks were often just a simple flood of packets of sufficient bandwidth to overwhelm the victim's internet connectivity. As defenses for mitigating these simple techniques became widely understood, attackers responded by simply ramping up the bandwidth by employing more compromised devices in a collective botnet. Over time, they created more sophisticated techniques such as state-exhaustion and application-layer attacks. Eventually, they began to introduce more complexity by combining various attack vectors in a single campaign. Current examples of massive volume and complexity include reflection-amplification and carpet-bombing attacks. Regardless of the techniques, one constant has remained. The overall activity level has continuously increased the amount of effort required to defend against these attacks.

Challenge

Modern DDoS attacks are capable of exhausting massive amounts of network resources. In the past, almost all DDoS attack traffic originated on the internet, outside of the operator's network. With the rise of IoT based botnets, attack traffic now often originates from inside the ISP network coming from compromised hosts in data centers, in public spaces or even in Enterprise networks. This means more malicious traffic than ever traversing networks. DDoS traffic is causing network bottlenecks that potentially impact multiple services and degrading if not denying service while increasing operational complexity and cost.

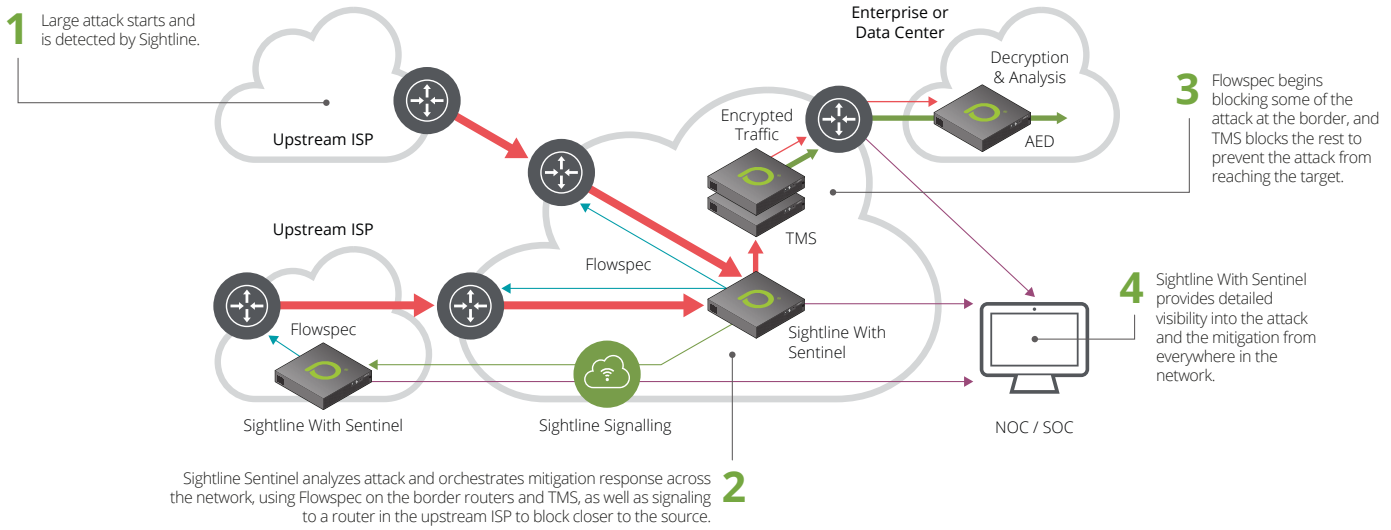
Risk

While all tier-1 ISPs currently have robust DDoS mitigation infrastructure in place, the cost and complexity of maintaining these systems is becoming ever more burdensome. Traditional defenses rely on backhauling attack traffic across the network to designated scrubbing centers. While this technique provides an effective and manageable solution, the cost burden is increased by the need for additional bandwidth in the core. Another approach is to further distribute mitigation capacity to the edges of the network in order to minimize DDoS traffic backhaul. While this reduces the need for excess capacity in the core, it increases the cost of specialized mitigation solutions thus offsetting potential savings.

Ideally, cooperation between network operators so that attack traffic can be dealt with as near to its source as possible could significantly reduce the burden for everyone. Initiatives such as 'DDoS Peering' in between tier-1 operators, have attempted to make this possible via exchanging BGP Flowspec routes between networks, using specifically provisioned infrastructure. Due to limitations in the technology and wide variance in how it is implemented across different vendors, products, and networks, successful implementations have so far been largely unattainable, unfortunately.

Solution

For years now there has been growing interest in technologies like Arbor Networks Fingerprint Sharing Alliance and Cloud Signaling, which were the genesis of DDoS Open Threat Signaling (DOTS). BGP Flowspec spawned DDoS peering initiatives, which demonstrate that the whole industry wants to fight DDoS together. NETSCOUT® has been contributing to all of these initiatives and now Sightline provides a new peer-to-peer signaling capability that allows network operators to share attack information. This functionality allows a Sightline-enabled organization under attack to select one or more Sightline DDoS alerts and forward them to preconfigured Sightline Signaling DDoS mitigation partners.



When a Sightline Signaling message is received by a mitigation partner, all the parameters of the DDoS alert from the requesting organization – attack type, packets-per-second, average packet size, protocol, port numbers, attack sources, attack targets, etc. – are included in the Sightline Signaling message. This in turn allows the receiving Sightline system to determine whether the attack traffic in question is traversing the networks it monitors. If so, a new alert on the receiving system is created, including all the relevant information about the portion of attack traffic observed in the context of the receiving network, such as ingress and egress routers/interfaces.

Once a new alert has been created on the mitigation partner's Sightline system, all the standard Sightline/TMS mitigation capabilities such as TMS countermeasures, flowspec, and/or S/RTBH are available to inform either a manually triggered mitigation, or a preconfigured auto-mitigation session. Either way, DDoS mitigation assistance can begin almost immediately, with situationally appropriate countermeasure selection, multiple mitigation technology options, and ongoing monitoring of resultant mitigations through the life of the attack.

This capability will enable:

- Multi-opco network operators to share information between their intranetwork deployments so that attacks can be dealt with as efficiently as possible.
- Groups of network operators to share information across their boundaries to deliver unified DDoS protection services to their customers.
- Large enterprises using the Sightline system to share attack information to their upstream operators or service providers so that they can get assistance in managing a DDoS attack.

Summary

Prior to the introduction of Sightline Signaling, attempting to coordinate inter-provider, cooperative mitigation of large-scale, high-impact DDoS attacks could be extremely challenging, fraught with high-response latencies, multiple levels of bureaucracy, and the inadvertent miscommunication of vital technical attack criteria during an attack – when every second counts. Sharing Sightline Signaling alerts ensures that all the relevant information can be shared by mitigation partners, swiftly, accurately, and securely.

Sightline Signaling enables DDoS defense cooperation in a number of important situations. Most obviously it can be used to enable DDoS defense between internet service providers, allowing for true end-to-end defense coordination and moving toward a world where DDoS attacks are stopped at their source rather than at their destination. But it's not limited to inter-organizational cooperation. Many network operators struggle with managing multiple independent networks. Sightline Signaling breaks down the defense barriers between networks and enables operators to coordinate defense internally across these different administrative and routing domains much more easily than before. And of course, Sightline Signaling enables faster, more seamless attack mitigation between cloud providers and their customers as part of DDoS managed services.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

© 2020 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

SECUC_010_EN-2001 05/2020