allot
See. Control. Secure.

DDoS Protection

Technical Use-Case and Deployment Scenarios for Enterprise

Solution Brief

February 2022

Contents

1 Allot DDoS Protection

Distributed Denial of Service (DDoS) attacks are here to stay. They are getting bigger, more frequent, and more sophisticated in their aim to flood your network and disrupt availability.

Allot DDoS Secure protects against fast moving, high volume, encrypted or very short duration threats and provides the first line of defense against both inbound and outbound attacks to assure business continuity. Allot's outbound protection identifies compromised hosts or IoT devices within the organization which participate in a DDoS attack and automatically mitigates the threat by isolating the infected host before it can impact the business

1.1 Introduction

Allot DDoS Secure is a DDoS Protection and Threat Containment solution designed to mitigate large scale network DoS/DDoS attacks as well as "Low and Slow" attacks which can be hard to detect, as they require very little bandwidth and generate traffic that is difficult to distinguish from normal traffic. Inbound DDoS attacks are automatically mitigated by discarding the DDoS traffic and allowing legitimate traffic to pass through. For outbound attacks, it identifies and then isolates possible threats originating from individual hosts that disrupt the performance and integrity of network infrastructure and services.

1.2 Multi-Layer Defense Strategy

Integrated with Allot's Secure Service Gateway platforms, DDoS Secure delivers a powerful multi-layer DDoS defense solution to protect your enterprise network. It combines proactive defense measures of policy-based traffic shaping using machine learning based anomaly detection. It prevents firewalls and routers from being overwhelmed and failing by providing the required protection under the load of massive DDoS attacks. This is done by controlling the traffic to these network elements making sure they don`t receive more than they can handle. At the same time, it monitors the network to look for anomalies corresponding to DDoS attacks and automatically mitigates them in real time.

1.3 Real-Time DDoS Protection

Allot DDoS Secure detects and surgically blocks Denial of Service, or Distributed Denial of Service (DoS/DDoS) attacks within seconds before they can threaten or disrupt the network service and applications. Allot inspects every packet on the network to ensure that no threat goes undetected. Allot's advanced Network Behavior Anomaly Detection (NBAD) machine learning based technology accurately identifies zero-day DDoS attacks, detecting the anomalies they cause in the normally time-invariant behavior of Layer 3 and Layer 4 packets. Finally, the solution dynamically creates mitigation rules for surgical filtering of attack packets to enable legitimate traffic to flow through and avoids over-blocking, keeping your business online and protected, always.

1.4 Outbound Threat Containment

Allot DDoS Secure automatically detects and blocks abusive or compromised users/ hosts participating in outbound worm propagation, port scanning as well as IoT traffic generated by bot-infected end points, so enterprises can prevent network blacklisting and eliminate additional traffic load on their network. Allot advanced Host Behavior Anomaly Detection (HBAD) technology identifies host infection and abusive behavior according to abnormal outbound connection activity and malicious connection patterns, enabling enterprises to keep anomalous traffic off the network and treat the root cause of the threat as well as the symptoms.

2 DDoS Secure Network Elements

DDoS Secure deployments consist of a DDoS Secure Controller and one or more DDoS Secure Sensors, an element embedded in the Allot Secure Service Gateway. All appliances (or virtual appliances) are connected to the same administration network, which they use to communicate and through which users access the system.

2.1 DDoS Secure Controller

The Controller functionality is to analyze all information arriving from the distributed sensors and make decisions regarding attack detection and mitigation. The controller also contains the management configuration, policies and database.

2.2 DDoS Secure Sensor

Each DDoS Secure deployment must include one or more Sensor installed on an Allot Secure Service Gateway. These sensors are typically deployed at key points in the network.

The sensor's role is to inspect network traffic and pass information to the controller for further analysis and actions. Two types of events are reported by the Sensor to the Controller:

- **NBAD** (Network Behavior Anomaly Detection) events refer to incoming or outgoing DoS/DDoS attacks
- **HBAD** (Host Behavior Anomaly Detection) events refer to outgoing Zombie/Botnet activity.

A minimum of one sensor is required and additional sensors can be deployed depending on the network topology

3 DDoS Secure In-Line Architecture

All traffic flows through the Allot DDoS sensors as shown in Figure 1 below. The sensors inspect inbound and outbound traffic. The central controller receives data from all the sensors. It analyzes the data to detect attacks and form a pattern for filtering the malicious traffic. The central controller also keeps packet captures to deliver comprehensive attack reporting and enable attack forensics.

This centralized architecture allows organizations to conveniently manage security of their entire network from a single SOC where everything can be seen and managed.

It also allows attack patterns to be shared between the multiple network sensors, so if an attack is detected in one part of the network it can be proactively prevented in other parts of the same network.

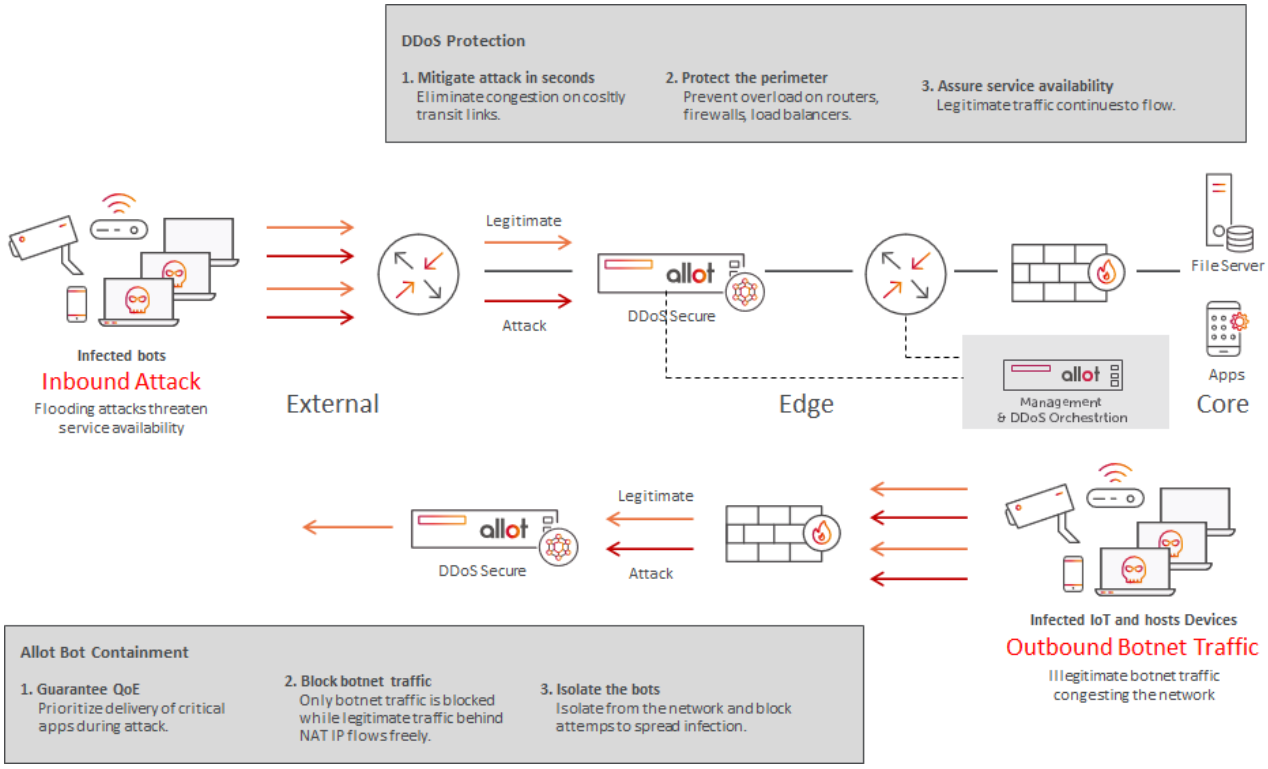

Figure 1: In-Line Architecture

4 Mitigating DDoS attacks using BGP

Where the DDoS Secure solution is not deployed in-line and in cases where the attack is larger than the link capacity, there are several possible remote-trigger options:

- **BGP Black-Hole**. In the classic black-hole scenario, all traffic in the neighboring Autonomous System and meant to be received, is instead sent to a black-hole
- **Scrubbing Center**. Another possible option is to send the traffic to a scrubbing center (e.g. Service Gateway) to remove all attack traffic, and then send the legitimate traffic on to the enterprise network
- **FlowSpec**. A third option is to use Flow Specification (Flowspec) which is a Network Layer Reachability Information (NLRI) for the BGP routing protocol. It is used to apply actions defined by specific filters on network traffic flowing through routers. By employing FlowSpec, the system can send a message to block all traffic except certain types such as an abusive IP range, TCP or UDP traffic, allowing legitimate traffic to continue flowing without interruption.

4.1 BGP Black-Hole

DDoS mitigation via BGP Black-Hole can be triggered automatically via a pre-configured policy when the amount of traffic exceeds a certain threshold or when a DDoS attack is detected based a on network behavior anomaly. Alternatively, Black Hole mitigation can be triggered manually via the DDoS Secure controller GUI.

When initiated, The DDoS Secure centralized controller initiates a BGP Black Hole command via the Allot Routing Service using a pre-configured BGP community route (either a /24 subnet or a specific target). As a result, the peering routers will drop traffic initiated from a specific subnet .

This mitigation action will cease in the following cases:

- Automatically after a configurable timeout.
- Manually by the end-user. In case the attack is still in progress, the system will immediately trigger another remote BGP Black Hole action.

This architecture requires a BGP Routing Service to be installed in addition to the DDoS Secure Controller. It is particularly suitable for large organization which have communication rights to the service provider routers.

In the flow, presented in Figure 2 below, traffic enters the network from AS1, 2 and 3.

In the example shown, an NBAD attack from AS1 blocks all access to the network.

The BGP Agent sends a message to the edge router of AS1 to notify it of the attack.

The system can then employ BGP Blackholing to drop the traffic from AS1, while traffic continues to flow via AS2 and AS3. Consequently, the attack never reaches the edge routers.

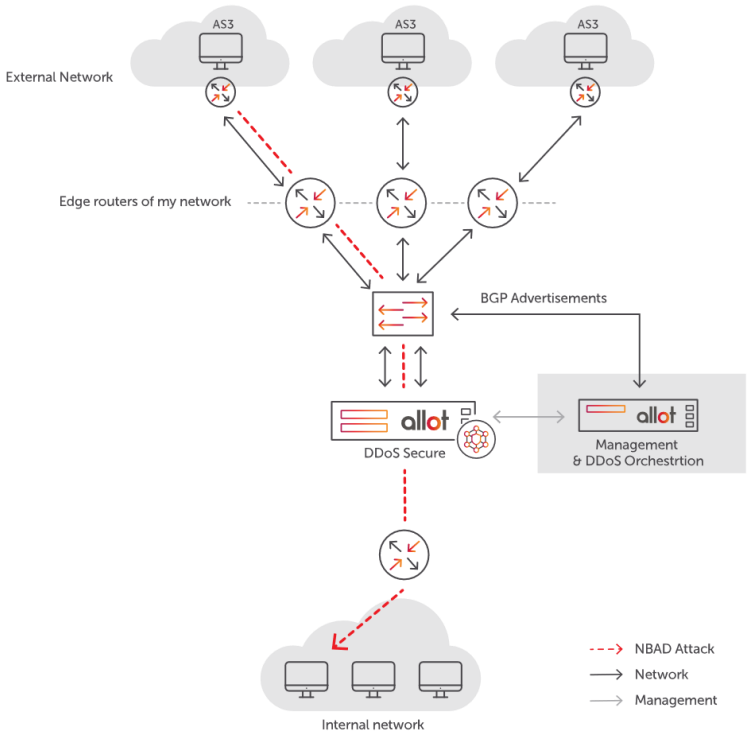

Figure 2: BGP Remote Triggering Architecture

The communication from the Controller to the BGP Agent (BGPA) is one-way: SSH from the Controller to the BGPA with expected replies from the BGPA.

Two types of communication will be observed in a live environment:

- A keep-alive from the DS-C to the BGPA, every 6 seconds.
- The request to advertise the host to blackhole to the peer\s or to withdraw such a request

4.2 BGP FlowSpec

BGP Flow Specification (Flowspec) is a Network Layer Reachability Information (NLRI) for the BGP routing protocol. It is used to apply actions on network traffic defined by specific filters to traffic flowing through routers. By employing FlowSpec, the system can send a message to block all traffic except certain types such as TCP or UDP traffic, allowing legitimate traffic to continue.

BGP FlowSpec is an alternative and a more granular method to BGP Black-Hole described in RFC5575 and in Section 4.1 above.

BGP FlowSpec defines a new Multiprotocol Network Layer Reachable Information (MP_REACH_NLRI) with AFI 1 (IPv4) and Subsequent AFI (SAFI) 133 (Flow Spec Filter). The FlowSpec NLRI collects 12 types of Layer 3 and Layer 4 filters used to define a flow specification. These are the fields that are added to NLRI within the BGP Update Message and advertised to peers.

The 12 FlowSpec NLRI components are listed below:

1. Destination Prefix – Defines the destination prefix to match
2. Source Prefix – Defines the source prefix
3. IP Protocol – Contains a set of pairs that are used to match the IP protocol value byte in IP packets.
4. Port – Defines whether TCP, UDP or both will be influenced
5. Destination Port – Defines the destination port that will be influenced by FlowSpec
6. Source Port – Defines the source port that will be influenced by FlowSpec
7. ICMP Type
8. ICMP Code
9. TCP flags
10. Packet Length – Match on the total IP packet length
11. DSCP – Match on the Class of Service flag
12. Fragment Encoding

In a similar fashion to the BGP Black-Hole technique, once Allot DDoS controller detects an attack it will trigger a BGP FlowSpec message to the edge Router with the required action. This action can vary depending on the configuration and allows the following:

a. Limiting traffic rate from specific source

b. Blocking a specific IP address/ protocol combination

Following the request, the remote router performs the required filtering/controlling and provides only the requested traffic to the organization. The Secure Service Gateway sensor continues to mitigate the required traffic, reducing the attack rate to zero.

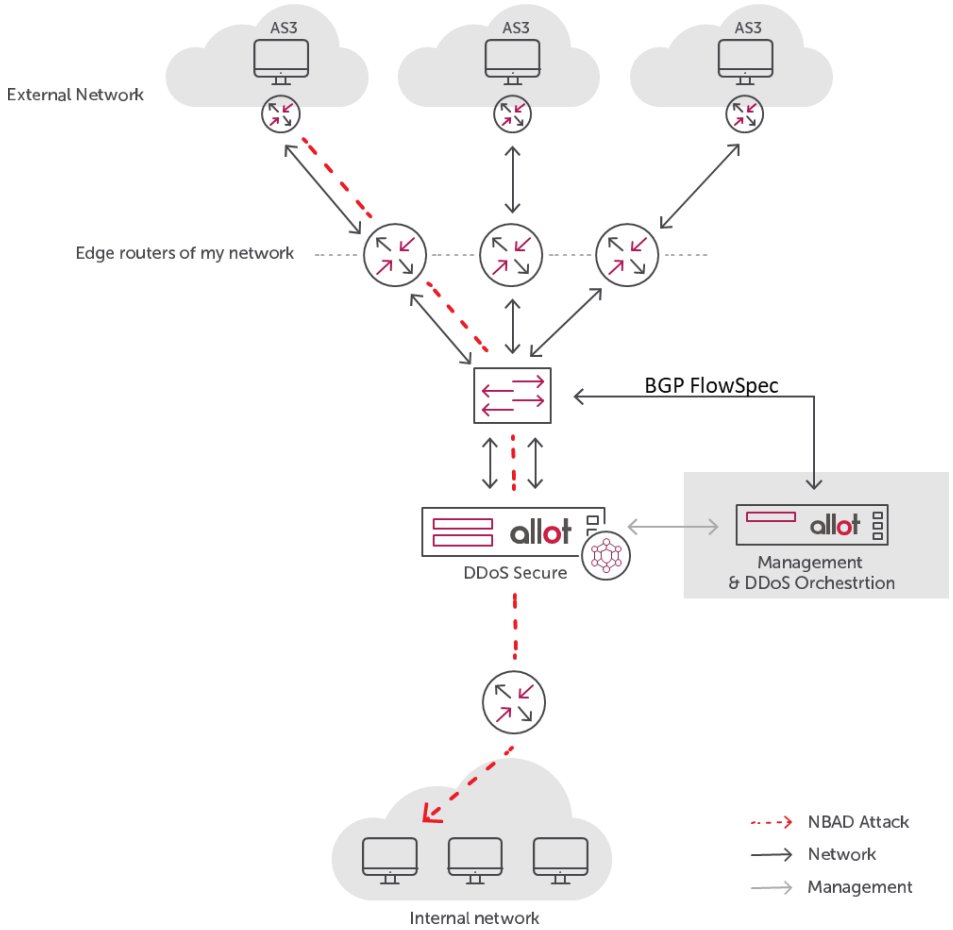

Figure 3: BGP FlowSpec Architecture

4.3 Scrubbing Center

Scrubbing centers provide cloud-based security solution for Inbound DDoS mitigation on enterprise networks. In scrubbing center mode, the traffic is redirected by a routing service to a designated cloud service, where DDoS traffic is scrubbed. When the system suspects an attack, all the traffic is re-routed to the cloud scrubbing center. In the scrubbing center the traffic is further inspected and DDoS packets are blocked while "clean" traffic is routed back to its original destination. Scrubbing center solutions can only monitor inbound traffic. Outbound traffic is not monitored. This represents a problem for enterprises and service providers, who need to ensure that they themselves are not an unwitting source of volumetric attacks.

Allot DDoS secure is open to work with any scrubbing center.

5 Hybrid DDoS Architecture

The Hybrid architecture (illustrated in figure 4) is based on the on-premises, inline detection of inbound DDoS attacks. As soon as the DDoS attack crosses a pre-defined threshold, it is re-routed to a cloud scrubbing center to fulfil the required mitigation.

The in-line sensors communicate with the DDoS controller which are also interconnected with the edge routers to transfer any signaling and BGP information when an attack is detected.

Traffic is inspected by the in-line sensor. Once a DDoS attack occurs, the in-line sensor measures the attack type and size. If the attack size if higher than a predefined threshold, for example above 80% of the link capacity, then a BGP signal is sent from the Routing Service to the edge router to divert the traffic to the scrubbing center.

The attack (which could be up to 1Tbps) is then scrubbed and customer traffic is routed from the cloud through a GRE tunnel back to the customer.

Once the attack is over, the Routing Service sends the routing information back to the organization and in-line inspection resumes.

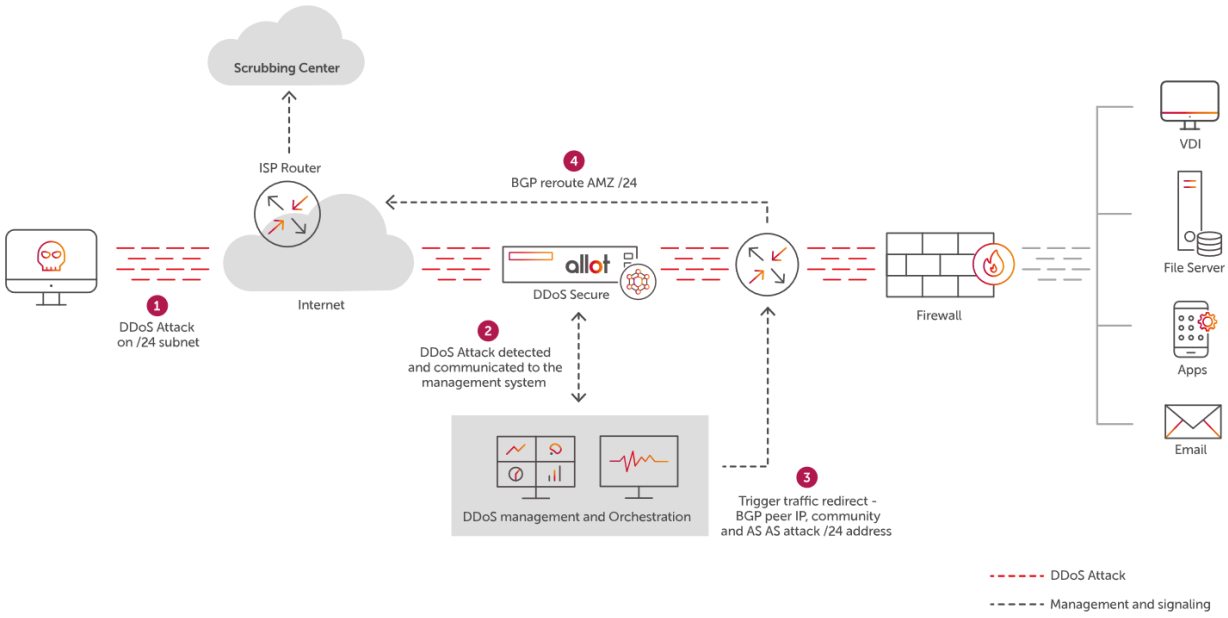

Figure 4: Hybrid Approach

6 Summary

Allot DDoS Protection is a comprehensive Inbound and outbound DDoS mitigation solution for any size of attack.

Allot's DDoS Protection solution enables you to:

- Ensure always-on, bidirectional protection that responds in seconds instead of minutes to DDOS attacks, even Zero-day attacks
- Gain full automation with no need for supervision
- Cluster multiple sensors to thwart even the largest volumetric attacks against the most distributed organizations
- Prioritize critical traffic to maintain high Quality of Experience during attacks
- Deliver comprehensive attack forensics
- Eliminate traffic overload to maintain your network efficiency while keeping your critical network elements protected
- Avoid being blacklisted and marked as an attacker or a spam source
- Choose from flexible deployment options with appliance or virtual appliance