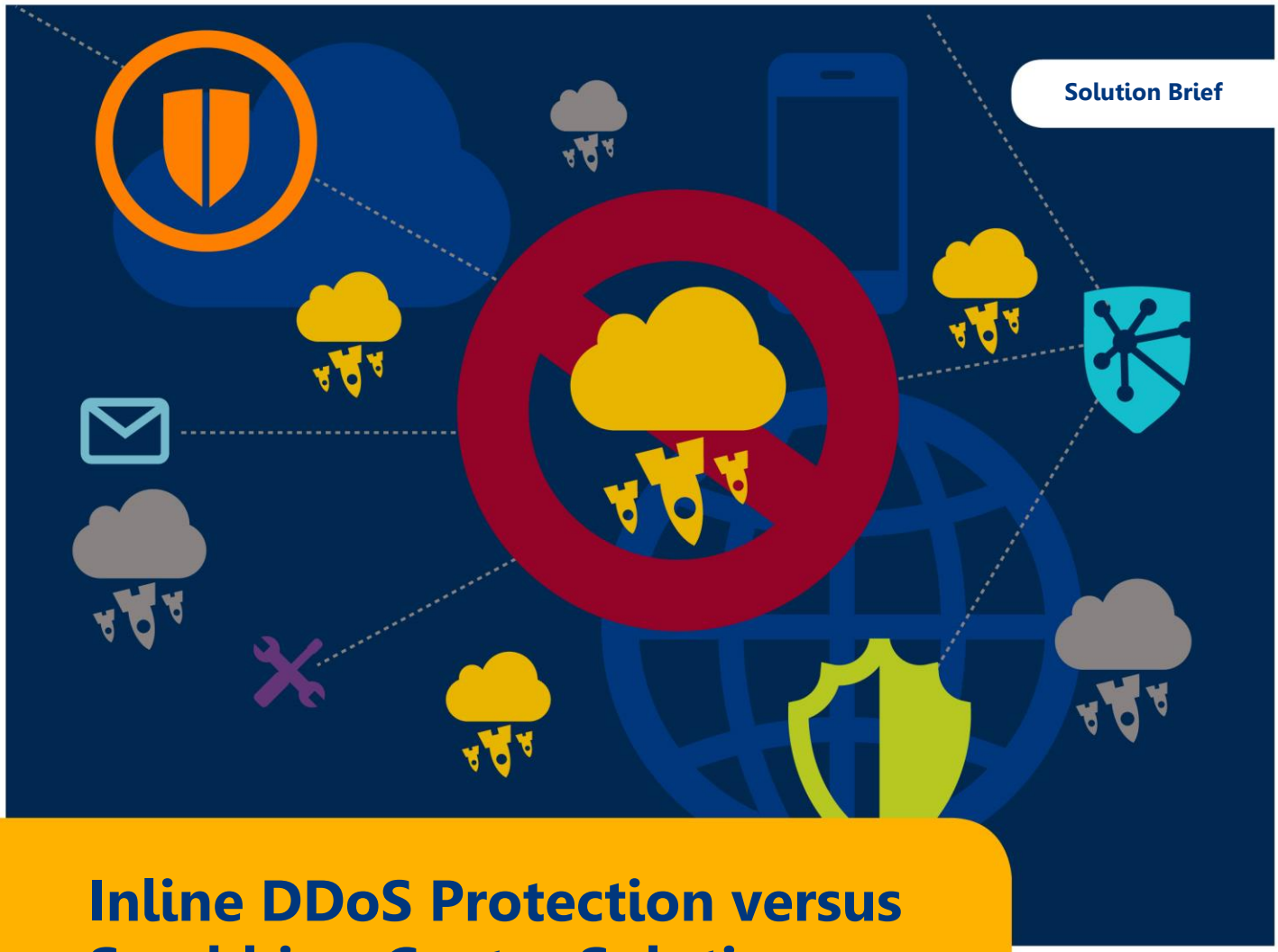
Solution Brief



Inline DDoS Protection versus Scrubbing Center Solutions

2017

Allot communications

Contents

1 Scrubbing Center vs. Inline DDoS Inspection and Mitigation

There are two main architectural approaches to protecting your network from Distributed Denial of Service (DDoS) attacks: mitigation by diverting traffic to a cloud scrubbing center or mitigation inline where the attack is occurring. This document elaborates on these architectures and their advantages and disadvantages.

With "Scrubbing Center" mitigation, once a flooding attack is detected, *all* traffic is redirected to a cloud scrubbing center, where further inspection and mitigation takes place. Attack packets are blocked (i.e., "scrubbed") and legitimate traffic is allowed to proceed to its original destination.

With inline mitigation, flooding attacks are both detected and surgically mitigated on the spot – right in the data path where the attack is coming into the network. This is the method used by Allot's DDoS Protection solution – Allot ServiceProtector – which enables service provider and enterprise networks to establish a very effective first line of defense against *inbound* DDoS attacks. From its inline vantage point, Allot ServiceProtector also detects *outbound* attacks that originate from within networks, including outbound port-scanning, flooding and IoT botnets.

2 Scrubbing Center

Scrubbing center solutions are also referred to as *Redirection*, *Diversion*, and *Netflow-based mitigation*.

2.1 Scrubbing Center Architecture

In scrubbing center mode, the traffic is redirected by the DDoS identification system.

When the system suspects an attack, all the traffic is re-routed to a 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.

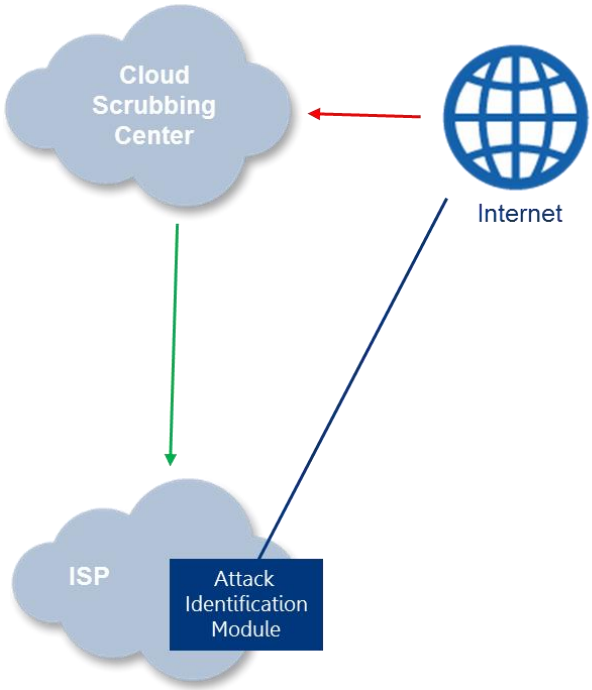


Figure 1: Scrubbing Center Architecture Schematic

2.2 Scrubbing Center Advantages

2.2.1 Minimal hardware footprint; Lower capex

Scrubbing center solutions are based on NetFlow and they rely on traffic sampling. They do not inspect all the traffic. Hence, the hardware footprint of the probes can be smaller and less expensive than a solution that inspects all traffic. Traffic is only diverted to the scrubbing center when there is suspected DDoS attack.

2.2.2 Cloud service option

In scrubbing center solutions, you have the option to use third-party services for cleaning the traffic, usually provided by a cloud-based service provider. Cloud-based services are highly scalable, and flexible. However, you need to factor in the ongoing

operating expenses (opex) for the cloud-based service provider, which will vary according to the number and volume of DDoS attacks your organization experiences.

2.3 Scrubbing Center Disadvantages

2.3.1 User experience degradation during DDoS attacks

A major disadvantage of redirection to a cloud scrubbing center is the throughput degradation it causes to existing legitimate connections, because the solution diverts **all** traffic during an attack.

When the traffic on an existing TCP connection is rerouted/diverted, there is a much greater chance of generating packet loss and jitter. This adversely affects the user experience, especially in applications like VoIP and streaming video.

Moreover, scrubbing devices are often unable to differentiate between an existing connection and bad traffic, and will block them both. Legitimate clients are then forced to reconnect, further degrading the user experience.

2.3.2 Incomplete detection

Because they only sample the traffic and do not inspect all traffic, diversion-based mitigation solutions cannot provide 100% effective attack detection. In addition Netflow is not able to detect low-rate application-based attacks.

2.3.3 Relatively slow mitigation due to diversion requirements

Diversion-based protection requires network routers to publish and propagate new routes (BGP/OSPF etc.) in order to redirect all traffic to the scrubbing center. Netflow-based detection is slow. Netflow propagation takes 2-3 minutes. When we consider the damage a flooding attack can do, that's a long time. For many new-wave "hit and run" attacks, this level of delay is unacceptable.

2.3.4 No visibility to outbound DDoS

Enterprises and service providers are under pressure to detect and block DDoS attacks emanating from within their networks. This can be done only with inline solutions.

Note: If a scrubbing center solution is already in use, this and other disadvantages can be alleviated by using it in conjunction with an inline solution.

3 Inline DDoS Protection

Allot ServiceProtector provides anti-DDoS, anti-botnet and outbound spam protection that is deployed inline, enabling attack detection and surgical mitigation on the spot, without diverting huge volumes of legitimate traffic and introducing delays.

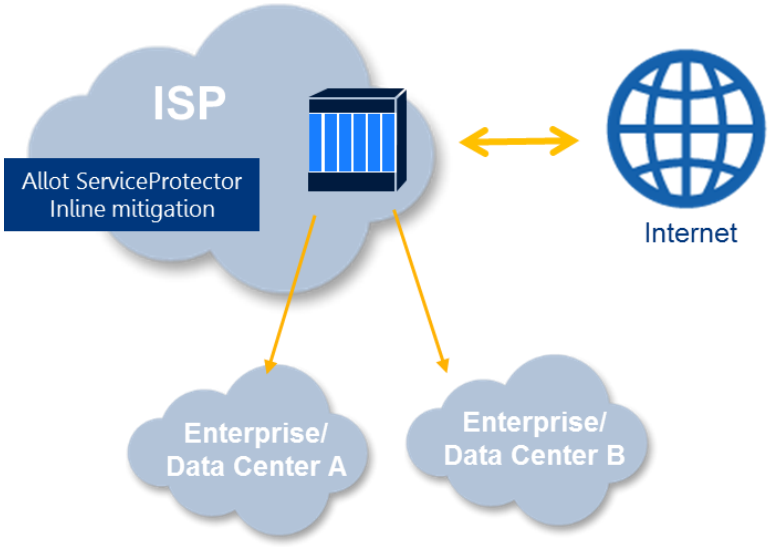


Figure 2: Inline DDoS Protection is provided by Allot ServiceProtector which is just one of the fully integrated services in Allot's multiservice platform – Allot Service Gateway

3.1 Advantages of Inline DDoS Mitigation

3.1.1 Rapid response time

Allot's inline DDoS protection inspects all the traffic in real-time and is able to identify, analyze and mitigate within seconds (instead of minutes which is the case with Netflow).

3.1.2 Accuracy

Allot's inline DDoS protection inspects outbound traffic as well as inbound traffic, enabling correlation of traffic flows to improve accuracy and to reduce the incidence of false positive or false negative identifications.

3.1.3 Ability to stop Reflection Attacks

In a reflection attack, infected devices send a considerable number of requests to open DNS/NTP/SSDP servers while spoofing the source IP of the requests to be the IP of the victim, causing all the responses to be sent to the attacked IP. Typically, the responses far outnumber the requests, creating an amplification effect that magnifies the size of the attack by a factor of 100.

Filtering reflection attacks is an enormous challenge for scrubbing centers because they see only inbound traffic and are blind to outbound traffic. As a result, they are unable to determine that the replies are actually responses to outbound requests that were sent by the victim.

In comparison, Allot inline DDoS protection inspects both inbound and outbound traffic and can easily filter reflection attacks, without false positives. From its vantage point in the network, the inline system sees all outbound traffic in general, and can identify DNS/NTP/SSDP requests in particular.

3.1.4 Better TCP anti spoofing

SYN cookies are the method used by firewalls and other inline devices to filter spoofed TCP traffic, and SYN floods in particular. With SYN cookie technology, the server sends a SYN+ACK response to the client, but discards the SYN queue entry. If the server then receives a subsequent ACK response from the client, it is a "real" request and the server is able to reconstruct the SYN queue entry. This method is supported when using an inline solution.

In contrast, unidirectional scrubbing devices are not able to implement SYN cookies because they cannot "proxy" the TCP connection nor update the TCP sequence numbers for the entire life of the connection. As a result, other anti-spoofing techniques such as RST, HTTP redirect and out-of-sequence ACK were developed specifically for unidirectional scrubbing solutions. However, all of these are highly susceptible to false-positives:

- RST requires the client to reconnect automatically after the connection has been reset by the scrubber, which is not the case for many applications
- HTTP redirect works only for HTTP traffic-and not even HTTPS
- Out-of-sequence ACKs are often blocked by stateful inspection firewalls

3.1.5 Accurate calibration of “normal” traffic

Detecting DDoS attacks and attackers is based on comparing inbound traffic patterns to what is considered to be "normal” behavior. Normal behavior is site/IP/application specific, and requires precise calibration to avoid false negative/positive identifications.

The ability to inspect both inbound and outbound flows enables accurate calibration of “normal” traffic patterns. Allot’s inline DDoS Protection solution constantly monitors and learns inbound and outbound traffic behaviors and continuously updates the “normal” calibration according to quantitative and qualitative changes detected.

Scrubbing centers do not inspect outbound traffic and therefore cannot achieve the same level of calibration accuracy.

3.2 Disadvantages of Inline DDoS Mitigation

3.2.1 More hardware intensive

Since the inline DDoS protection solution monitors all traffic and performs mitigation at the point of detection, it requires carrier-grade capacity, throughput, reliability, and scalability. Therefore, it requires a bigger up-front capital expense to deploy in your network infrastructure, than is required by scrubbing center solutions, especially cloud-based scrubbers.

3.2.2 No cloud service option

While the inline DDoS protection solution provides no cloud-based option, it is compatible with cloud scrubbing centers. You can seamlessly migrate from existing cloud-based scrubbing services while using both simultaneously.

4 Allot ServiceProtector

Allot ServiceProtector provides fast and accurate DDoS protection by offering:

- Fully integrated system embedded in Allot inline, multiservice platforms
- Ability to inspect both inbound and outbound traffic for anomalous behavior
- Dynamic attack detection and surgical mitigation within seconds
- No service interruption or resource downtime
- Proven technologies
  - NBAD (Network Behavior Anomaly Detection)
  - HBAD (Host Behavior Anomaly Detection)
  - Asymmetric traffic monitoring
- Zero-day attack resilient—quick response, no user action required
- Real-time alerts and threat analytics with customizable view
- Scalable to 500 Gbps in single platform and 4 Tbps in clustered platform node
- Carrier-grade high availability with no single point of failure

4.1 Advanced Detection and Mitigation Technology

Allot's patented NBAD technology (Network Behavior Anomaly Detection) identifies DDoS and other network flooding events by the anomalies they cause in the normally time-invariant behavior of "network ratios" i.e., combinations of Layer 3 and 4 packet rate statistics. Packet filtering rules are obtained dynamically by searching deep into the captured DDoS packets for unique repeating patterns in each event. Surgical filtering accuracy is often achieved using the patterns detected in the Layer 3 and 4 headers and layer 7 payload.

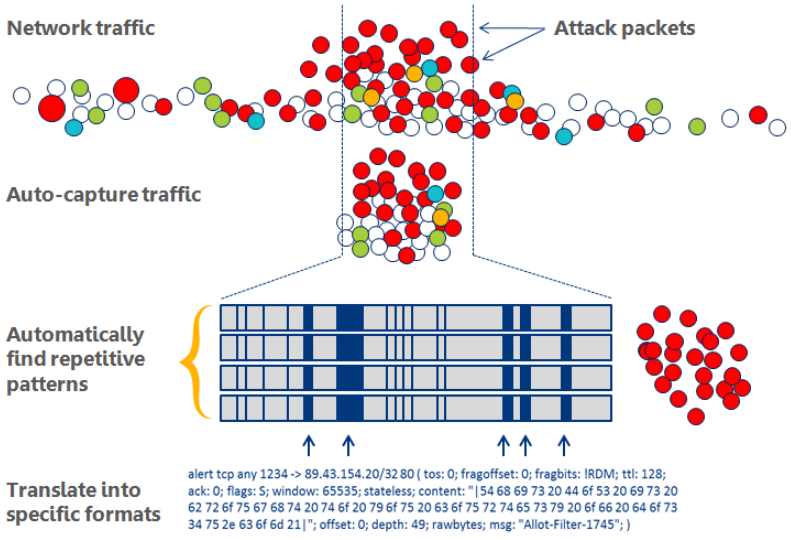


Figure 3: Network Behavior Anomaly Detection technology

4.2 Efficient DDoS Protection Architecture

Allot ServiceProtector is fully integrated service in Allot Service Gateway – the leading multiservice platform in the industry - which is deployed inline at critical network core and edge junctures. From these vantage points, Allot monitors and inspects all the traffic on the network at line-speed and without introducing any delay. When attack behavior is detected, Allot NBAD technology creates attack pattern signatures in 20-50 seconds; notifies you of the attack via email, syslog, and SNMP trap (v2c), and immediately begins surgical mitigation. The inline deployment of Allot DDoS Protection solutions means that flooding attacks are stopped on the spot at the edge of your network, without having to divert huge volumes of traffic to cloud scrubbing centers.

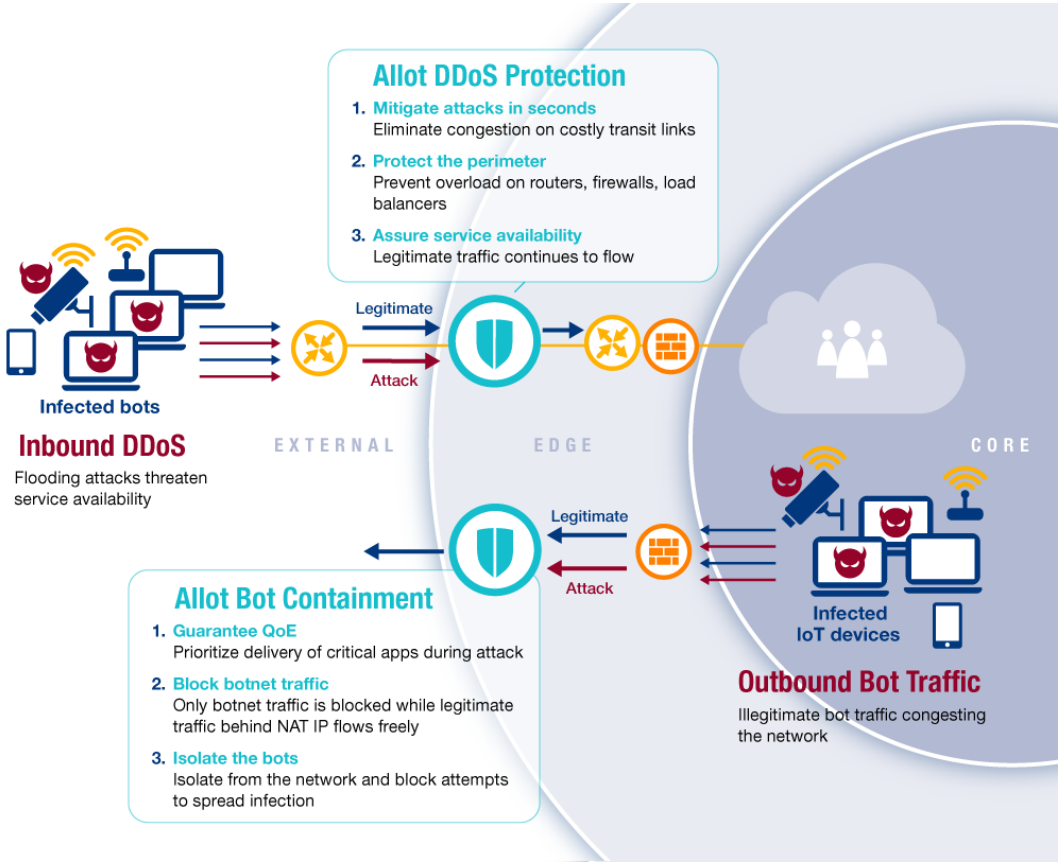


Figure 4: Allot ServiceProtector provides real-time DDoS Protection and Bot Containment for both inbound and outbound traffic

5 Summary

This paper describes the architecture, advantages, and disadvantages of both modes of DDoS identification and mitigation:

- Inline
- Scrubbing Center

5.1 Scrubbing Center

Scrubbing center solutions have gaps in DDoS detection and mitigation is relatively slow, but the solution may be more cost effective in some use cases.

5.1.1 Advantages

- Minimal hardware footprint
- Cloud service option

5.1.2 Disadvantages

- User experience degradation during DDoS attacks
- Incomplete detection
- Relatively slow mitigation due to diversion requirements
- No visibility of outbound DDoS

5.2 Inline Mode

Inline DDoS protection inspected every packet and therefore provides more accurate anomaly detection and faster mitigation, albeit with a higher capital outlay for the inline hardware.

5.2.1 Advantages

- Accurate and comprehensive detection
- Surgical mitigation in seconds
- Ability to stop Reflection Attacks
- Better TCP anti-spoofing
- Accurate calibration of “normal” traffic behavior

5.2.2 Disadvantages

- More hardware intensive
- No cloud service option

www.allot.com **sales@allot.com**

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: +1 781-939-9300; Fax: +1 781-939-9393; Toll free: +1 877-255-6826
Europe: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France - Tel: +33 (0) 4-93-001160; Fax: +33 (0) 4-93-001165
Asia Pacific: 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104, Tel: +65 6749-0213; Fax: +65 6848-1015
Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669
Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626

P/N Dxxxxxx Rev.1