FAQ

Stopping DDoS attacks and Outgoing Spam with Allot ServiceProtector

2014

Allot communications

Contents

Frequently Asked Question about Detection

1. What kind of attacks does Allot ServiceProtector detect and identify?

Allot ServiceProtector is part of Allot's portfolio of security services for the Digital Lifestyle and Workstyle. It provides a highly effective first-line system of defense against DoS/DDoS, worm and Zero Day attacks. It also detects and prevents outbound spam (that can lead to operator blacklisting) and cleanup of infected hosts (spammers).

2. How does Allot ServiceProtector detect and identify attacks?

Two detection technologies are used.

Network level attacks (DoS/DDoS/worm/Zero Day) are identified using **Network Behavior Anomaly Detection (NBAD) technology**. First, the network is modeled at a very granular level where the various types of IP traffic are tracked and compared in ratios (such as incoming TCP SYN packet rate to the outgoing TCP FIN packet rate). Ratios are important for eliminating variance due to natural traffic surges and spikes. Ratio comparison also enables the system to detect attacks that are not identified by less sophisticated threshold/baseline approaches. For example, during a large SYN flood attack (small SYN floods are worthless as attacks), the modeled incoming SYN packet rate is significantly out of balance with the corresponding FIN packet rate. This behavior is treated as anomalous. Large NBAD behavioral anomalies have been found to be more often than not large DoS/DDoS attacks.

Subscriber attacks (i.e., outgoing spam from infected hosts) are identified using **Host Behavior Anomaly Detection (HBAD) technology**. At its most basic level, HBAD identifies subscriber attacks by the anomalously high connection rates sustained by an individual host. For example, a subscriber sending spam is identified by the fact that it is highly unlikely that a single host is capable of sending 20 emails every second sustained for the last 5 minutes. Behaviorally this is highly indicative of a spambot. Experience has proven that to be the case.

In addition to these two detection approaches, Allot ServiceProtector also supports a rich set of user-definable notification parameters that permit the operator to customize the elements which pre-determine whether an alarm is sent, which further enhances the quality and relevance of the alarms.

3. How does Allot ServiceProtector handle *false positives*?

When used properly (for detecting network level attacks and subscriber based attacks) and deployed on target networks – namely high-performance, high-throughput GE and 10GE networks, Allot ServiceProtector has proven to be extremely reliable and immune to false positives. The reason for this is the nature of the threats that it aims to identify and the superior detection methods it uses.

4. What about IPS systems? Can they detect DoS/DDoS attacks?

Intrusion Detection System (IPS) vendors use a variety of methods for identifying security threats on the network, including DDoS attacks. IPS methods of detection are less sophisticated than Allot ServiceProtector for detecting network level attacks and typically rely on known signatures and rate-based thresholds with traffic baselining which suffer from false alarms or false negatives (not detecting at all).

IPS devices were originally intended for preventing "intrusion" into a host rather than network level attacks. Their signature and RFC violation-based detection are vulnerable to

not detecting network level attacks and their stateful nature makes them vulnerable to high volume network attacks.

IPS solutions are not suitable for network level attacks predominantly due to their tendency to fail or to increase network latency under heavy loads (as is the case with network level attacks) and because they may not have appropriate behavior-based detection algorithms that are more suited to reliable network-level attack detection.

5. Can Allot ServiceProtector detect slow scanning worms?

Yes. Allot ServiceProtector can detect slow scanning worms. However, Allot ServiceProtector tends to be used for higher volume connection attempts (spam, worm, DoS) because this kind of subscriber behavior that causes greater concern for management of a service provider's public network.

6. Can Allot ServiceProtector detect single packet attacks or application level attacks?

No. Single-packet and Application-level attacks are designed to target a host or to "intrude" and compromise a host. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are more suitable for these kinds of attacks since they utilize detection by signatures of known malicious packets, detection by violation of RFC specifications for applications and stateful inspection of connection behavior.

Allot ServiceProtector operates at a different layer of security and is focused on protecting against network level attacks (DoS/DDoS, worm and Zero Day attacks) and subscriber originated attacks (spam, worm, DoS). These kinds of attacks undermine the stability and performance of the network upon which high value applications are being delivered. Attacks against an individual host are not in Allot ServiceProtector's solution scope.

7. Can Allot ServiceProtector detect and stop viruses?

No. Viruses are out of scope of Allot ServiceProtector. Viruses are security threats against a host and are best addressed with host, server and network based anti-virus solutions. Allot ServiceProtector is designed to protect against network level attacks (DoS/DDoS, worm and Zero Day attacks) and subscriber originated attacks (spam, worm, DoS).

8. What kind of attacks does Allot ServiceProtector detect?

Using **NBAD technology**, which identifies generic TCP/IP based behavioral anomalies, Allot ServiceProtector detects all variations of known and unknown DoS/DDoS, worms and Zero Day attacks. Against Allot ServiceProtector, attackers have been unsuccessful in evading detection by using legitimate packets or modifying packets, using extremely large packets, setting the fragment offset (and not sending the remaining packets), setting all (or other unusual combinations) of TCP flags, by using unusual IP protocol numbers such as protocol 0 or protocol 255, by using dark space source IP addresses, by reflecting the attack from intermediate devices and so on

Using **HBAD technology**, Allot ServiceProtector detects subscriber-originated attacks such as outgoing spam, worm propagation, DoS and port scanning. These are normally perpetrated by infected subscribers who unwittingly participants in a botnet.

9. If source IP addresses are spoofed, how is that info useful?

The source IP address, whether it is spoofed or not, is potentially a characteristic that can be used to filter traffic.

10. Does Allot ServiceProtector perform event correlation?

Not currently. However higher-order data correlation and representation is planned for near-future release.

11. How does Allot ServiceProtector handle asymmetric links?

Firstly this depends upon the particular behavioral detection algorithm used by Allot ServiceProtector. Allot ServiceProtector uses HBAD and NBAD detection technologies.

HBAD is immune to asymmetric traffic since it only looks at outbound connection behavior from a defined domain (for example an ISP's subscriber CIDR). HBAD is used for identifying outbound attacks or spammers inside an ISP's customer base. This requires a view of outbound traffic only.

NBAD is relatively immune to asymmetric traffic. It is only concerned with the overall balance of inbound and outbound flows of various TCP/IP statistics and does not care about sessions and state. This means, for example, that while it tracks inbound SYN packet-rate and compares that with outbound FIN packet-rate, it does not care whether the FIN packets are a direct response to the SYN packets. Experience has shown that anomalies created by asymmetric traffic flows are orders of magnitude smaller than genuine DDoS attacks. Only in the extreme case that there is only ever traffic in one direction that NBAD technology cannot be used. In this case, a traffic "threshold" based approach can be employed which does not rely on the NBAD algorithms.

12. Does Allot ServiceProtector sample traffic?

For the purpose of detection, every single packet is used, even at 1Gbps and 10Gbps throughput. As a result, there is no loss of accuracy in the process of formulating the behavioral models. However, for the process of extracting a Deep Packet Signature (DPS), packets are sampled from the anomalous traffic in order to determine the filterable packet characteristics in the attack.

13. Does Allot ServiceProtector use known signatures?

No. The reason is that pure signature based detection relies on the predetermined knowledge of malicious packets and this approach has been found to be inadequate for handling DoS/DDoS, worms and Zero Day network attacks because there are often no pre-determined signatures. In fact, attackers often use legitimately formed packets to deliberately evade the signature-based detection systems.

14. I block TCP port 25 to all my subscribers to avoid blacklisting. What benefit is Allot ServiceProtector to me?

This approach punishes the innocent as well as the guilty and probably causes annoyance. By using Allot ServiceProtector you can enhance email services and customer satisfaction by both avoiding blacklisting and keeping network services open to those who deserve it. In addition, the customers that you notify as sending spam may be unwittingly infected. Once their computers are disinfected, they will experience better Internet experience because less of their upstream connection will be consumed by spam or worm traffic.

Frequently Asked Question about Mitigation

15. How does Allot ServiceProtector mitigate the attack?

Allot ServiceProtector interoperates seamlessly with Allot NetEnforcer and Service Gateway platforms which mitigate the attack by blocking, limiting or isolating the traffic.

Allot ServiceProtector also supports mitigation with third-party devices such as routers, firewalls, IPS, and DDoS filtering devices.

16. What happens if the attack uses completely random source and destination IP addresses, random ports and random payload patterns so that there is no signature with which to block the attack?

Conceptually this is possible and clearly disastrous if the attack is in large volumes! This highlights even more the need to plan strategic implementation of an automatic network security system that can programmatically correlate multiple packets sampled out of 1Gbps and 10Gbps traffic streams and to pick-out "any" packet features that can be used to mitigate the attack. In fact, assuming that the packets are completely random, the VLAN or source MAC address will be readily identified and can be used as a mechanism to at least isolate the attack at a coarse level.

17. What happens if the signature describes a normal SYN packet? Should I block that?

Attackers may use legitimately formed packets in order to evade signature based detection techniques. However, the context and event behavior provide clues in which to determine the true intent of the packet. This includes the nature of the target (is it web site and if so, has it attracted attacks before), the impact on the network (network congestion, increased latency) and whether the event is sustained at extremely high rates beyond a brief spike lasting more than a minute or so. Empirically, these have been found to be DDoS attacks rather than transient spikes due to sudden reconnections.

18. How can you block a DDoS attack when the source addresses are spoofed?

It does not matter whether the source address is spoofed or not. The source IP address provides unique information about the attack packets that can (or not) be used to selectively filter the attack traffic.

19. How can you block a DDoS attack when there are so many source IPs?

In practice, it is impractical to use the source addresses in a DDoS attack because they are too numerous. Fortunately, the source addresses can be ignored since other characteristics of the packets can be used instead to filter the attack, including the destination IP address, protocol, port, packet size, TOS, TTL, other fields in the network and transport layer, and the payload. Allot ServiceProtector's signature extraction engine identifies the unique packet characteristics that the attack packets have in common.

It is worth noting that Allot ServiceProtector quantifies the relative amount of traffic from each source address (based upon a sample of the attack traffic). This information can be used to block using the source address if a large majority of attack packets are originating from a small set of source addresses.

Frequently Asked Questions about Deployment

20. Does *every* network link have to be tapped?

Not necessarily. This depends upon your network topology and especially the particular way in which Allot ServiceProtector is intended to be used. It is best to consult Allot on how Allot ServiceProtector can be optimally deployed within your network topology to maximize visibility and minimize the number of sensors.

In general, Allot ServiceProtector should be deployed in strategic aggregation links in the network similar to where DPI devices or IDS/IPS and network analysis devices are deployed.

This includes Internet peering points, access aggregation links to the core network, WAN links and the core network.

To identify network level attacks, deployment at the peering link or core is typical. To identify subscriber-originated attacks, the most economical deployment is usually on the access aggregation links to the core network.

Every network is different and Allot can recommend the best design to meet your requirements.

21. Can Allot ServiceProtector handle VLAN tags?

Yes. Allot ServiceProtector can be deployed inside VLAN networks. VLAN tags are not used to classify traffic and are parsed out during the behavioral modeling process*. However, during the process of Deep Packet Signature extraction, if available, the VLAN tag will be reported as a distinguishing characteristic of the network event.

(*The behavioral modeling process parses packet for the network and transport layer data from each packet).

22. Can Allot ServiceProtector handle encrypted traffic?

Yes. Allot ServiceProtector is designed to address Internet-originated network level attacks (DoS/DDoS, worm and Zero Day attacks) and subscriber originated attacks (spam, worm, DoS). There are two complementary approaches to behavioral anomaly detection used by Allot ServiceProtector. The behavioral detection algorithms for detecting subscriber originated attacks focuses on connection behavior of the subscriber and thus the payload (encrypted or not) is ignored. Hence suspicious connection behavior of a subscriber will be identified despite the payload being encrypted. On the other hand, the behavioral detection algorithms for detecting network level attacks will categorize the encrypted traffic within the anomaly type “other.”