TECHNICAL BRIEF

Why Firewalls and Intrusion Prevention Systems (IPS) Fall Short on DDoS Protection

THE RISK OF CHOOSING THE WRONG TECHNOLOGY FOR DDOS PROTECTION

Firewall and IPS Devices: Essential Security Tools–But Not Designed to Solve the DDoS Problem

Many security teams rely on traditional security products such as firewall, intrusion prevention system (IPS) and web application firewall (WAF) devices to protect their organizations from a variety of threats including distributed denial of service (DDoS) attacks. Though these devices are essential elements of a sound security strategy, they simply are not designed to stop modern-day DDoS attacks.

IPS devices, for example, have been designed to block break-in attempts that cause data theft. Meanwhile, firewalls act as policy enforcers to prevent unauthorized access to data and services. While such products are critical security tools, they fail to address a fundamental concern regarding DDoS attacks—network availability. The table below provides other reasons why traditional, on-premise security products such as firewall and IPS devices do not offer adequate DDoS attack protection.

Why Firewall and IPS Solutions Do Not Address the DDoS Problem	
Vulnerable to DDoS attacks	- Because these devices are in-line, stateful devices, they are vulnerable and targets of DDoS attacks. - First to be affected by large flood or connection attacks.
Failure to ensure availability	- Built to protect against known (versus emerging) threats. - Designed to look for threats within single sessions, not across sessions.
Protection limited to certain attacks	- Address only specific application threats. - By default, they must allow common attack traffic such as TCP port 80 (HTTP) or UDP port 53 (DNS). Do not handle attacks containing valid requests.
Deployed in wrong location	- Very close to servers. - Too close to protect upstream router.
Incompatible with cloud DDoS protection systems	- Fail to interoperate with cloud DDoS prevention solutions. - Increase time for response to DDoS.
Lack of DDoS Expertise	- Require skilled security experts. - Demand knowledge of attack types before attacks.

Since firewall and IPS devices are “stateful” inline solutions, they are also vulnerable to DDoS attacks and often become the targets themselves. Basically, they must track every packet over every connection, which makes perfect sense given the problems that they have been optimized to solve. A firewall, especially a newer application-layer one, must track all connections to understand the context of all incoming packets, and an IPS device must track state to proactively stop intrusion attempts via signature-based detection, stateful protocol analysis and other detection methods.

Arbor’s Key Advantages

Proven and Trusted

The vast majority of the world’s leading service providers rely on Arbor Networks for DDoS defense. If your network service provider offers DDoS defense, chances are they are using Arbor products.

Leading Research

Arbor security researchers have a real-time view of over 70% of global internet traffic via our ATLAS initiative. This unmatched access to emerging threats enables the ASERT team to develop timely, automatic updates to Pravail.

Cloud Signaling Coalition

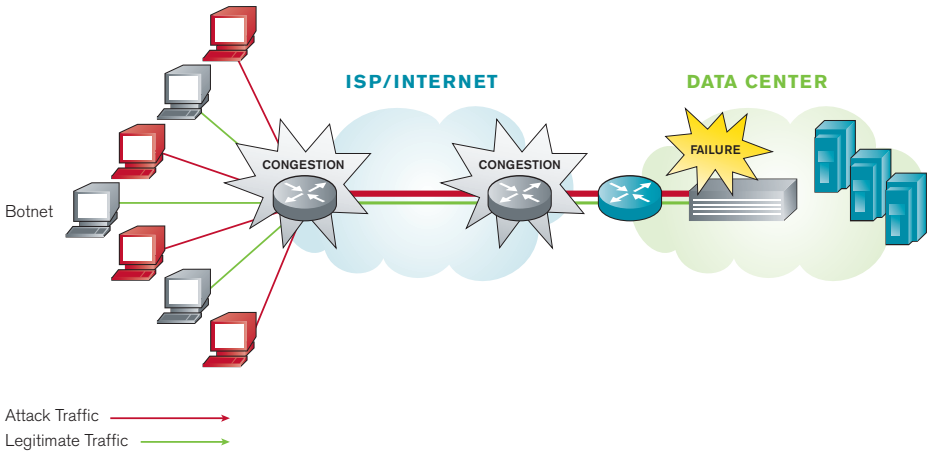
This innovative approach to DDoS defense delivers coordinated protection to the enterprise. Providers around the world are rapidly joining the coalition.

ARBOR® NETWORKS

Pravail APS is a plug-and-play device that immediately stops DDoS attacks and keeps critical services available.

Protection Level | Low Medium High

Even if state tables grow over time, the arms race will continue as hackers leverage larger botnets and more distributed attack vectors. Firewall and IPS devices will continue to choke even during moderate DDoS attacks and can be first points of failure during DDoS attacks. For instance, the ***sockstress*** attack method can quickly overwhelm the firewall's state table by opening sockets to fill the connection table. The ***slowloris*** attack, similarly, opens connections to the target web servers and keeps these connections open with partial HTTP requests, which can overwhelm the intermediate IPS device.



Traditional on-premise security devices have not been designed to solve the DDoS problem.

That being said, even though a firewall's and IPS's state tables can be a weakness with respect to DDoS, they are absolutely critical for the devices to do their jobs—such as stopping unauthorized access to critical resources, enforcing corporate security policies, preventing data loss, etc. These all remain critical security problems.

Pravail APS: Augmenting IPS and Firewall Devices with Purpose-Built DDoS Protection

The Arbor Pravail™ Availability Protection System ("Pravail APS") focuses exclusively on stopping availability threats such as DDoS attacks. By making sure the firewall and IPS state tables are filled with legitimate communications, Pravail APS can enable other CPE-based security devices to focus on their core functions. Rather than having a firewall get overwhelmed with a sockstress attack, Pravail APS can defend against the attack and allow the firewall to enforce network policy or prevent unauthorized access.

Data center operators and enterprises can also deploy Pravail APS in front of firewall and IPS devices to stop other application-layer attacks and disrupt botnet communications. With Pravail APS, an enterprise can:

- Deploy a turnkey solution to stop threats to availability immediately.
- Block emerging application-layer DDoS attacks before legitimate services go down.
- Stop DDoS attacks from botnets by leveraging real-time security intelligence from Arbor's Active Threat Level Analysis System (ATLAS®).
- Mitigate flood DDoS attacks by coordinating with Cloud Signaling℠-enabled providers.

ARBOR NETWORKS

Corporate Headquarters
6 Omni Way
Chelmsford, Massachusetts 01824
Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe
T +44 208 622 3108

Asia Pacific
T +65 6327 7152

www.arbornetworks.com

TB/IPS/EN/1011