ARBOR INSIGHT

At-a-Glance: Enterprise Guide to DDoS Protection

1. Always-on security integrated with cloud scrubbing
2. Stateless inspection
3. Intelligent botnet detection and mitigation
4. Automatic protection for application-layer attacks
5. Intelligent identification of Web crawlers
6. Asymmetric traffic
7. Packet capture and custom policy creation
8. CDN and proxy aware

Distributed Denial of Service attacks are a common thread in today's advanced threat landscape. When it comes to addressing these attacks, organizations have several options.

Firewalls and IPS/IDS devices often highlight their DDoS features. Load balancers can offer some relief from traffic floods. A good partnership with your Internet Service Provider (ISP) can help by blocking high volume traffic. However, none of these options provides a complete solution that really solves the problem.

With more than a dozen years of experience addressing DDoS attacks in service provider environments, Arbor Networks has developed a solution with the specific needs of the enterprise in mind. The following table outlines specific needs and considerations enterprise organizations must remember when evaluating DDoS solutions and how Arbor Networks meets these needs.

How do other vendors stack up against these considerations?

Key Considerations	The Arbor Difference
Always-on Security Integrated with Cloud Scrubbing *Does the product or service provide both on premise and cloud-based DDoS options?* ISP-based DDoS protection is important for blocking high volume flood attacks (>10G) to the enterprise. However, it can take 45-60 minutes for an ISP to identify the attack and be able to set up mitigation for each enterprise. A complete DDoS protection solution includes always-on protection for targeted application-layer attacks that integrate with upstream providers to block larger attacks.	Pravail® APS helps provide organizations with on-premise, always-on protection against availability attacks. Customers can strengthen this protection with targeted cloud scrubbing via Cloud Signaling™ functionality. This Cloud Signaling feature includes the ability to create detailed attack alerts that are sent to upstream providers for greater protection before threats reach the perimeter.
Stateless Inspection *Can the product or service detect DDoS attacks without relying on session state?* Traditional perimeter security devices (firewalls and IPS) rely on tracking session state to enforce security policies. However, this makes them vulnerable to attacks that are designed to exhaust session state and take that inline device out of commission. Organizations then have to make the choice to fail open and leave the network exposed, or to fail closed, cutting off access to network resources.	Pravail APS utilizes the Stateless Analysis Filtering Engine (SAFE), which does not rely on tracking session state to detect or mitigate DDoS attacks. As a result, Pravail APS can better withstand the low-volumetric attacks that hinder other products and threaten availability.

ARBOR® NETWORKS

ARBOR INSIGHT

Arbor Networks is a leading provider of network security and management solutions for enterprise and service provider networks. The Pravail APS product line offers comprehensive DDoS protection in a package uniquely suited to the enterprise. For more information about how Arbor Networks can help protect your data center from availability attacks, please visit **www.arbornetworks.com/products/pravail.**

Key Considerations	The Arbor Difference
Intelligent Botnet Detection and Mitigation *Does the product or service receive updated intelligence to identify and block today's active botnets?* While many security devices ship with a few botnet signatures, the ever changing nature of botnets requires a solution that includes daily updates for today's threats. Many security vendors either fail to effectively identify a bot or they go to the other extreme and provide "blanket" protection which can inadvertently impede certain business functions.	Pravail APS uses up-to-date protection from ASERT to accurately identify and block DDoS botnet attacks. Each day, ASERT receives hundreds of thousands of malware and other malicious IPs from ATLAS.® This research is then developed into protections that are delivered to the Pravail APS device via the ATLAS Intelligence Feed.
Automatic Protection for Application-Layer Attacks *Can the product or service identify and block DDoS attacks targeting the application-layer?* The application-layer often includes the organization's web servers and applications that run on them. Attacks on Web servers are often very small and fly below the radar of ISP-based DDoS protection.	Pravail APS sits inline within the company network to better identify and block attacks targeted at the application-layer, such as HTTP or SMPT.
Intelligent Identification of Web Crawlers *Can the product or service automatically determine the difference between malicious bot activity and legitimate search engine web crawlers?* Search engine vendors use custom Web crawlers to mine enterprise websites for information or terms used to rank the sites during user searches. However, many Web crawlers behave like bots causing some security vendors to block them.	Pravail APS relies on ATLAS Intelligence Feed for accurate identification of attacks targeting the network. The AIF subscription includes updates to recognize legitimate Web crawlers so that marketing efforts are not hindered.
Asymmetric Traffic *Does the product or service deliver complete protection for asymmetric traffic?* Many enterprises rely on redundant links and ISPs, which can cause inbound and outbound traffic from a single connection to cross different interfaces. Like other security offerings, DDoS solutions must deliver complete protection for asymmetric traffic.	Pravail APS supports asymmetric traffic deployments and can effectively block attacks in these environments.
Packet Capture and Custom Policy Creation *Does the product or service make it easy to capture packets and use those for custom policy generation?* Attacks can be highly customized to your specific network. In these instances, organizations don't have the time to figure out how to create new attack policies.	Pravail APS provides detailed attack information about the threats hitting your network. This attack information can include packet capture which can easily (and immediately) be turned into a protection policy.
CDN and Proxy Aware *Does the product or service deliver full protection for traffic that flows through proxies and CDNs?* If an attack targets your network through a CDN or proxy, the attackers' real addresses can be hidden. If the DDoS solution blacklists the CDN's IP address, the attack "protection" actually amplifies the attack, taking legitimate traffic offline.	Pravail APS recognizes proxies and CDNs, providing necessary protection (and visibility) without impacting legitimate traffic.

ARBOR® NETWORKS

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

Europe
T +44 207 127 8147

Asia Pacific
T +65 6809 6226

www.arbornetworks.com

AI/ATAGLANCE/EN/0513