Arbor Cloud℠ for Enterprises

Integrated DDoS Protection from the Enterprise to the Cloud

ARBOR® NETWORKS

About Arbor Networks

Arbor Networks, Inc. helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier", making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context—so customers can solve problems faster and reduce the risk to their business. To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor's research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.

Table of Contents

The New Breed of Attack: Multi-Layered DDoS

Today's DDoS threats have evolved in both complexity and sophistication. They target the availability of networks, services and applications—often at the same time—through a multi-layered attack strategy. This strategy combines high-bandwidth assaults that overwhelm the capacity of enterprise data centers with low-bandwidth, hard-to-detect attacks aimed at bringing down critical applications.

These new multi-layer attacks can negate the effectiveness of traditional perimeter security devices, such as firewalls and Intrusion Prevention Systems (IPS). High-volume flood attacks overpower the bandwidth limitations of these devices. Meanwhile, "low and slow" application-layer attacks fly under their radar—escaping detection until critical services are down or badly degraded.

Unfortunately, most organizations are unprepared for this new breed of attack—and are blindsided when their traditional security devices fail to protect their networks and core business systems. To better ensure business availability, today's enterprise should have multi-layered DDoS protection from the edge of its network to the cloud.

Protection against the new breed of DDoS attacks requires an understanding of the methodologies and tools used by attackers. Today's multi-layer DDoS assaults can combine any or all of the following approaches into a single, coordinated attack. The results can be catastrophic—including upstream saturation, state exhaustion and service outage.

Distributed DDoS Attacks

Taking advantage of the proliferation of compromised computers, attackers utilize a command-and-control network to create a botnet. They use these botnets to launch targeted DDoS attacks originating from the vast number of infected hosts.

Volumetric DDoS Attacks

These devastating attacks typically target network infrastructure components such as switches, routers or servers. By flooding bandwidth with connection requests, they cripple legitimate traffic and availability to critical resources. A myriad of volumetric attack tools are available that utilize common protocols. Some of the more widespread types include:

- UDP flood attacks that take advantage of the connectionless nature of the UDP protocol.
- Reflection flood attacks that utilize a legitimate resource such as DNS to amplify an attack. The DNS response is multiplied many times and sent to the victim's spoofed IP address, thereby exhausting resources.

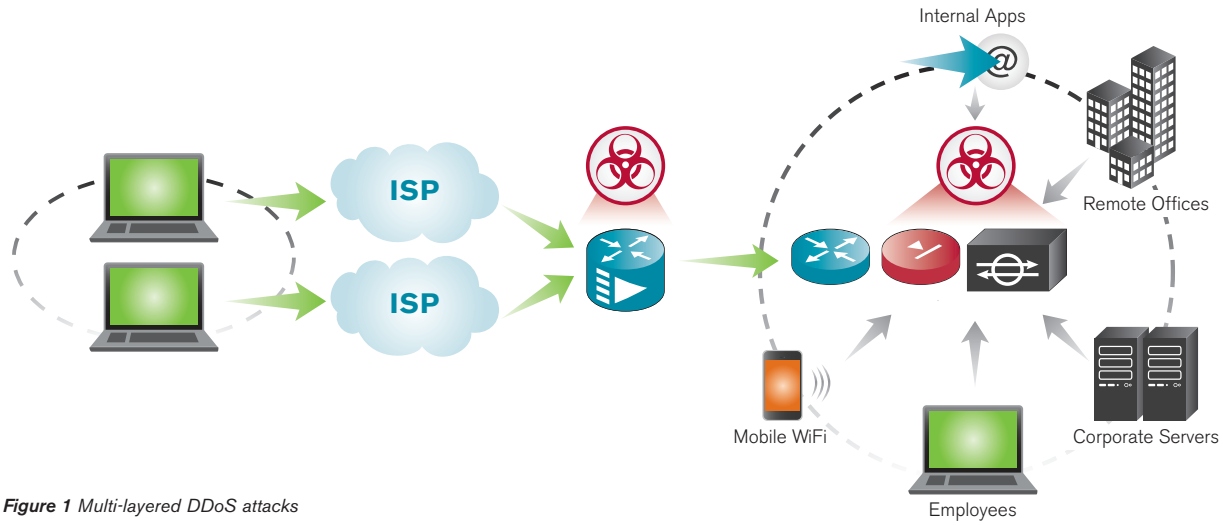

Figure 1 *Multi-layered DDoS attacks*

State Exhausting DDoS Attacks

These attacks target security infrastructure devices such as firewalls, IPS and load balancers. They take advantage of connection-state tables by flooding them with half-open connections and other TCP connection attacks.

Application-Layer DDoS Attacks

These attacks represent the most popular attack vector as their stealthy nature makes them harder to detect. They target systems on the application layer—from Web services to custom applications. By making critical applications inaccessible to those who rely on them, these attacks deliver a significant blow to business availability.

Traditional Perimeter Security Solutions Are Not Designed to Defend Against DDoS

Traditional perimeter security devices such as firewalls and IPS are essential elements of a layered-defense strategy. However, they are not designed to protect against the multi-layered nature of today's complex DDoS attacks.

DDoS attacks typically utilize legitimate traffic payload distributed from large networks of hosts, and exhaust capacity in critical assets and systems. Examples include link capacity, session capacity, application service capacity (e.g., HTTP/S, DNS) and back-end databases.

Traditional security devices fail to protect from DDoS attacks because the traffic appears to be legitimate and is allowed to pass by these systems. Additionally, firewalls and IPS are stateful inspection devices, which means they are vulnerable to today's multi-layer attacks and often become the targets themselves.

Why Firewall and IPS Devices Do Not Solve the DDoS Problem

Vulnerable to DDoS Attacks

- Because these devices are inline, stateful devices, they are vulnerable and targets of DDoS attacks.
- Firewalls and IPS are the first to be affected by large flood or connection attacks.

Failure to Ensure Availability

- Built to protect against known (vs. emerging) threats.
- Designed to look for threats within single sessions, not across sessions.

Deployed in Wrong Location for DDoS Protection

- Very close to servers.
- Too close to upstream router.

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). They do not handle attacks containing valid requests.

Incompatible with Cloud-Based DDoS Protection Systems

- Fail to interoperate with cloud-based DDoS prevention solutions.
- Increase response time to DDoS attacks.

Lack of DDoS Expertise

- DDoS protection requires prior knowledge of attack types.

Arbor Cloud: On-Premise + In-Cloud DDoS Protection for Global Networks

Arbor Cloud is an integrated, multi-layer solution for protecting against today's complex DDoS attacks. This comprehensive protection is achieved by augmenting Arbor's on-premise, always-on DDoS defense product with its cloud-based, on-demand traffic scrubbing service. Using Cloud Signaling™ technology, Arbor Cloud integrates on-premise and cloud-based protection, accelerating attack identification and mitigation. This service is backed by a 24X7 Security Operations Center staffed by Arbor's DDoS and security experts.

Arbor Cloud provides on-premise protection that helps prevent stealthy, low-and-slow attacks that bypass firewalls and IPS and target critical business applications. This on-premise protection also guards against state-exhausting DDoS attacks that overwhelm existing security devices. Augmenting the on-site protection is the on-demand traffic scrubbing service staffed by Arbor's DDoS security experts. This cloud-based service defends against volumetric DDoS attacks that are too large to be mitigated on-premise.

With each layer of protection, Arbor delivers its industry-leading expertise and technology—whether through its on-premise detection and mitigation product or its globally deployed architecture for DDoS traffic scrubbing in the cloud. As a result, Arbor Cloud provides a single, carrier-agnostic security solution that helps protect globally distributed networks from multi-layer attacks that evade evade traditional perimeter defenses.

Arbor Cloud delivers a powerful first line of defense through Arbor's industry-leading on-premise DDoS attack detection and mitigation product. This easy-to-deploy and manage appliance is designed to automatically neutralize attacks before they impact critical servers or systems. It helps deliver protection from:

- Application-layer attacks
- State exhausting attacks
- Volumetric attacks (up to the limitation of the device)

Because the cost of downtime is extremely high for most global organizations, Arbor's on-premise solution is designed to automatically detect and mitigate DDoS attacks with little or no user interaction—before services are degraded. It also offers simple fallback plans and resolution techniques when attacks cannot be readily identified. Moreover, the on-premise solution can recognize legitimate CDN traffic and will not accidentally block it. With Arbor Cloud DDoS Protection Service, the enterprise manages the on-premise device, maintaining control over their first line of defense.

Arbor Multi-Layer Cloud Protection

On-Premise Protection

Provide a first line of defense against high-volume attacks; defend against "low-and-slow" attacks that fly under the radar of traditional perimeter defenses and bring down critical business applications; and guard against state-exhausting attacks that overwhelm firewalls and IPS devices.

In-Cloud Protection

Block high-bandwidth DDoS attacks that overpower the mitigation capacity of enterprise data centers, and provide cloud-based traffic scrubbing for stealthy, high-volume attacks that evade traditional security checkpoints.

Coordinated Protection

Accelerate detection and mitigation by seamlessly integrating on-premise via Pravail and in-cloud protection through Cloud Signaling.

A Global Protection Layer from a Single Vendor

Rely on comprehensive, carrier-agnostic protection for your global enterprise network backed by world-leading security and network research and intelligence from ATLAS/ASERT and 24x 7 service and support by our experts.

Additional benefits of Arbor's on-premise solution include:

Automatic Threat Updates

Arbor enjoys a close and privileged relationship with leading ISPs around the world. Through its extensive network of sensors and data feeds, Arbor has real-time visibility into 70Tb/sec of global Internet traffic. This gives Arbor unmatched insight into emerging threats—information used by the Arbor Security Engineering & Response Team (ASERT) to develop defenses against new and emerging threats. The ATLAS® Intelligence Feed (AIF) delivers threat updates directly to the on-premise solution in real-time, requiring no action on the part of enterprise security and IT teams.

Visibility, Control and Alerting

On-premise protection delivers real-time visibility into attacks, blocked hosts and even packets. It offers the flexibility operators need to alter attack countermeasures and thresholds, if required. It also includes active alerting that notifies security engineers of ongoing attacks that are blocked, as well as other network events that may require attention.

Real-Time and Historical Attack Forensics and Reporting

Enterprises can visually understand the actions taken by the on-premise solution through detailed, real-time attack reports. Besides documenting these actions in audit logs, the solution provides forensic reports detailing blocked hosts, origin countries of attacks and historical trends. These easy-to-understand reports can also be given to peers or management to educate them on the threats to service availability and the steps taken to address the attacks.

Full Control of Mitigation

Unlike other managed DDoS solutions, Arbor Cloud enables enterprises to maintain control over DDoS mitigation via the on-premise solution. The Arbor Cloud Portal provides information regarding the attack and mitigation, a timer for measuring attack duration, granular reporting on attack traffic and account management tools.

Manual or Automatic Mitigation Alerts

When the on-premise solution detects an attack, you can manually alert the cloud deployment about the attack. Alternatively, you can preset the on-premise solution to automatically send an alert to the cloud upstream when a threshold is reached.

Advanced Web Crawler Service

Arbor has even taken into consideration a Web site's page ranking and search engine results. ASERT maintains policies in AIF designed to allow specific Web crawlers to access your site, while blocking those that are identified as malicious or irrelevant.

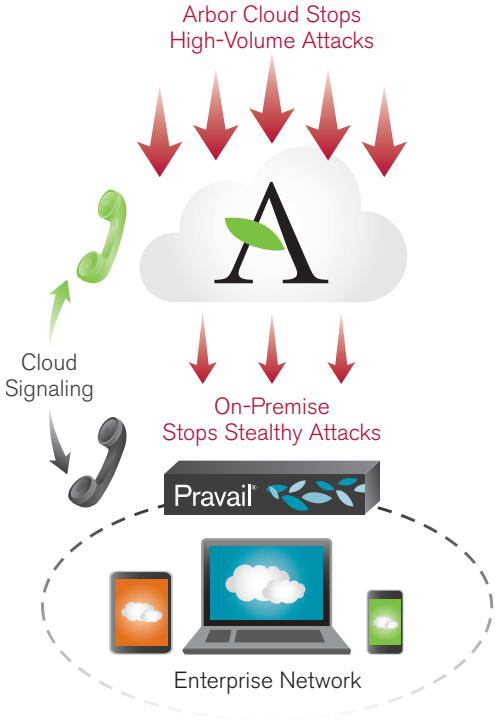

Figure 2 *On-premise + Cloud protection*

In-Cloud Protection: Powerful, Proactive, On-Demand

When an attack occurs, speed and agility are critical to business continuity. In the event of a volumetric attack, Arbor's on-premise solution serves as a first line of defense—rerouting inbound traffic to one of Arbor Cloud's four global scrubbing centers for cloud-based mitigation. These four scrubbing centers are located in: Ashburn, VA, San Jose, CA, Amsterdam and Singapore. The SOC is located in Sterling, VA. When this occurs, Arbor's experienced security experts and engineers work hand-in-hand with the enterprise IT team to quickly redirect malicious DDoS traffic away from the affected infrastructure based on predetermined methods.

Through four global scrubbing centers, Arbor Cloud can help defuse the large, complex high bandwidth attacks that make headlines daily and threaten the availability of critical resources and assets.

After an attack occurs, Arbor Cloud delivers a comprehensive and granular report detailing the attack in its entirety. To ensure understanding and transparency in service delivery, this report is delivered during a one-on-one meeting with Arbor's Security Operations Center engineers and the enterprise organization.

Powered by the Arbor Security Engineering & Response Team (ASERT)

Arbor security researchers have a real-time view of over 70% of global internet traffic. This unmatched access to emerging threats enables the Arbor Security Engineering & Response Team (ASERT) to develop timely, automatic updates to on-premise solutions and the Arbor Cloud SOC.

As a part of the Arbor Cloud service, ASERT will provide customers with the same global intelligence and insight that it delivers to the Arbor SOC through weekly Threat Briefs that will be available on the ATLAS portal. Additionally, In the event of late breaking attacks or urgent threats, a Threat Brief will be released that informs customers of these threats. From the portal, customers will be able to see the following (which includes the threat briefs):

- **Global Threat Map:** Real-time visibility into globally propagating threats
- **Threat Briefs:** Summarizing the most significant security events that have taken place over the past 24 hours
- **Top Threat Sources:** Multi-dimensional visualization of originating attack activity
- **Threat Index:** Summarizing Internet malicious activity by offering detailed threat ratings
- **Top Internet Attacks:** 24-hour snapshot of the most prevalent exploits being used to launch attacks globally

Cloud Signaling™ Technology: Integration from the Data Center to the Cloud with Pravail

Arbor Cloud integrates on-premise and cloud-based protection using Arbor's unique Cloud Signaling technology. By enabling communication between the on-site and in-cloud environments, Cloud Signaling technology facilitates rapid DDoS attack detection and mitigation. When an attack begins to saturate connection bandwidth, for example, the on-premise device can trigger an alert to the Arbor Cloud scrubbing center—augmenting on-premise protection with cloud-based mitigation.

Rely on Arbor Cloud

Advanced protection against:*

- Spoofed/Non-spoofed DoS Attacks
- TCP (SYN, etc.), ICMP, UDP Floods
- Botnets
- Blackenergy, Darkness, YoYoDDoS, etc.
- Common DoS/DDoS Tools
- Slowloris/Pyloris, Pucodex, Sockstress, ApacheKiller
- Voluntary Botnets (Anonymous, etc.)
- HOIC, LOIC, etc.
- Application Attacks
- HTTP URL GET/POST Floods
- Malformed HTTP Header Attacks
- Slow-HTTP Request Attacks
- SYN Floods Against SSL Protocols
- Malformed SSL Attacks
- SSL Renegotiation Attacks
- SSL Exhaustion (Single Source/ Distributed Source)
- DNS Cache Poisoning Attacks
- DNS Request Floods
- SIP Request Floods
- Custom Attacks—Unique to Your Service
- Location-Based IP Addresses

** The Pravail® Availability Protection System ("Pravail APS") also allows user-configured custom protection.*

Conclusion

Organizations today are often ill-prepared to protect their globally dispersed networks against highly targeted, complex and multi-layered DDoS attacks. The new attack reality calls for an integrated multi-layer solution designed to fend off assaults by employing the most effective detection technique at the most efficient location, whether that means on-premise or in the cloud.

Arbor Cloud offers 24x7 DDoS protection from the premises to the cloud using Arbor's proven DDoS detection and mitigation solutions at both ends. In-cloud protection is designed to block high-bandwidth DDoS attacks that flood your network with traffic. Meanwhile, on-premise protection helps prevent low-bandwidth, hard-to-detect attacks that bypass existing security devices like firewalls and IPS devices, and target the applications that keep your business running. It's all supported by Arbor's 24x7 Security Operations Center staffed by our DDoS and security experts.

For more information about how Arbor Cloud can help protect your enterprise against today's multi-layer DDoS attacks, please contact your Arbor representative or log on to www.arbornetworks.com/products/arbor-cloud.

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 68096226

www.arbornetworks.com

ARBOR® NETWORKS

SB/ACE/EN/1113-LETTER