DATA SHEET

Arbor Pravail

Availability Protection System (APS)

NETWORK SECURITY WITH A UNIQUE FOCUS ON STOPPING AVAILABILITY THREATS

In the last few years, distributed denial of service (DDoS) attacks have grown in size to over 100 Gbps and increased in complexity with the emergence of new application-layer attacks. Today's hackers, motivated by greater incentives to launch DDoS attacks than ever before, are using these new attack techniques to target data centers. What's more, the widespread prevalence of bots and botnets gives these cyber criminals ample ammunition to launch such attacks.

The Pravail Availability Protection System (APS) focuses on securing the Internet data center (IDC) edge from threats against availability—specifically, protection against application-layer distributed denial of service (DDoS) attacks. With the Pravail APS, Arbor Networks is bringing carrier-class DDoS detection and mitigation capabilities to the data center.

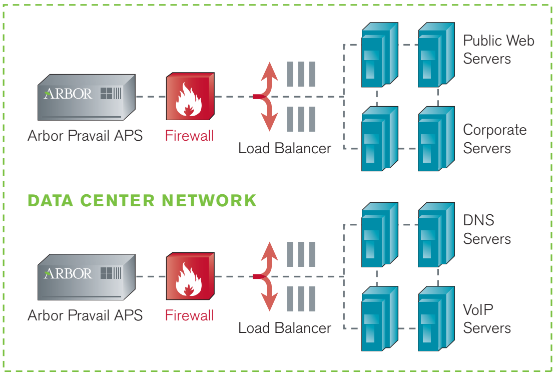
With Pravail APS, your data center can gain the power to:

- Detect and block emerging application-layer DDoS attacks.
- Deploy a turnkey solution to stop availability threats immediately.
- Prevent illegitimate botnet communications by leveraging real-time intelligence from Arbor's Active Threat Level Analysis System (ATLAS®).
- Mitigate volumetric attacks by coordinating with Cloud-Signaling enabled partners.

The Critical Need to Ensure Service Availability

As data center consolidation and cloud computing adoption accelerate, availability becomes absolutely critical. If services such as Web, domain name system (DNS), Simple Mail Transfer Protocol (SMTP), and others are not available, all other issues are irrelevant.

Pravail APS is designed to stop these availability threats. This unique, premise-based security product provides threat protection from one Gbps to beyond 10 Gbps. Through the intelligence in Arbor's exclusive ATLAS system, Pravail can also stop the most complicated DDoS attacks. Simply put, when your business depends on the availability of Internet services, Pravail APS is critical to ensuring that those services will be available for your customers and users alike.



Pravail APS Protects Internet Data Centers

Key Features and Benefits

'Out-of-the-Box' Protection
Offers immediate protection from active threats with minimal configuration.

Advanced DDoS Blocking
Introduces new packet-based detection and mitigation for emerging application-layer threats.

Botnet Threat Mitigation
Stops illegitimate communications from reaching servers and blocks DDoS attacks originating from botnets.

Diverse Deployment Models
Fits easily into most IDC on-premise deployment scenarios and requires little in-house expertise.

Cloud Signaling
Stops growing volumetric DDoS attacks by coordinating with Cloud-Signaling enabled providers.

ARBOR® NETWORKS

Can You Afford to Ignore Availability Threats Like DDoS?

When Internet-facing services are down, the impact can have severe business consequences. When determining the cost of downtime, organizations must consider the following factors:

- **Direct Loss of Revenue and Profit.** This is arguably the largest cost and easiest-to-calculate measure of downtime. For example, if an online retailer that makes 40 percent of its revenue in the last two weeks of the year suffers an outage two days before Christmas, the financial impact can be devastating.
- **Tarnished Reputation or Brand.** News travels fast in today's age of information—especially when it comes to news regarding service outages or security breaches. This negative media coverage could have a major impact on an organization's reputation or brand value.
- **Lower Productivity.** When online services go down, the productivity of employees and businesses that rely on these services can be drastically reduced. A simple calculation shows the impact: cost of lost productivity = number of employees using the application x average hourly salary x hours of downtime.
- **Penalties.** Some organizations may face financial penalties if they fail to meet certain availability requirements. For example, a company that provides a service that is part of a complex supply chain could face stiff penalties for any delays that it causes.

Organizations must consider availability threats when developing risk mitigation plans. To better understand the direct and indirect costs associated with availability attacks, please refer to the Arbor white paper entitled *The Business Value of DDoS Protection.*

The Growing and Evolving Threat to Service Availability

During the last few years, DDoS events have been dominated by volumetric attacks usually generated by Internet bots or compromised PCs that are grouped together in large-scale botnets. Examples include DDoS attacks against UK-based online betting where the hackers extorted the gambling firms, and politically motivated DDoS attacks against the Georgian government. This type of DDoS attack is generally high bandwidth and originates from a large number of geographically distributed bots. The size of these volumetric DDoS attacks continues to increase year over year—reaching 100 Gbps in 2010. As a result, they remain a major threat to enterprises and Internet service providers (ISPs) alike.

In 2010, an ideological group called Anonymous launched campaigns against anti-piracy sites and firms no longer accepting donations for WikiLeaks. Both campaigns leveraged an opt-in botnet where users downloaded an application named Low Orbit Ion Cannon (LOIC), which launched TCP and HTTP flood-based DDoS attacks. These attacks targeted major online retailers such as Amazon, PayPal, MasterCard and Visa.

Such attacks on service availability reveal the potential impact of DDoS on ecommerce. More importantly, they represent a new type of "application-layer" DDoS attack that targets specific services and consumes lower bandwidth. These new application-layer DDoS attacks threaten a myriad of services ranging from Web commerce and DNS services to email and online banking. Enterprises and IDC operators are very concerned with the availability of the critical services running in their data centers. At the same time, attackers view Internet-facing data centers as new prime targets and are launching DDoS attacks to wreak havoc on these companies.

Why DDoS Requires an On-Premise Solution

Intrusion prevention system (IPS) devices, firewalls and other security products are essential elements of a layered-defense strategy, but they are designed to solve security problems that are fundamentally different from dedicated DDoS detection and mitigation products. IPS devices, for example, block break-in attempts that cause data theft. Meanwhile, a firewall acts as policy enforcer to prevent unauthorized access to data. While such security products effectively address network integrity and confidentiality, they fail to address a fundamental concern regarding DDoS attacks—network availability. What's more, IPS devices and firewalls are stateful solutions, which means they are vulnerable to DDoS attacks and often become the targets themselves. Pravail APS, on the other hand, represents a new type of on-premise security solution—one designed specifically to optimize network availability.

Why Existing On-Premise Solutions Fail to Address DDoS Security	
Vulnerable to DDoS attacks	• Targets of DDoS attacks. • First to be affected by large flood or connection attacks.
Complicated to use	• Require skilled security experts. • Demand knowledge of attack types before 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. • 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.

Key Technologies

Immediate ‘Out-of-Box’ Threat Protection

When data centers are under attack, they need security solutions that can be deployed quickly and with little effort. Pravail APS is easy to install and provides near-immediate protection from most threats. Given the many demands on security and networking personnel, they will appreciate the streamlined configuration process and simple user interface. When critical services are down, Pravail APS is built to bring them back online—fast.

The ATLAS Intelligence Feed: Stop Emerging Botnet and Application-Layer Attacks

Enterprises face an ever-changing array of DDoS attacks. The new ATLAS Intelligence Feed is integrated into Pravail APS to detect and stop emerging threats. The threat feed is constantly updated to address dynamic threats such as botnets, and it simplifies threat responses because it is updated in real time without software updates. The threat feed also utilizes application-layer analysis to stop complex application-layer attacks. The Arbor Security Engineering & Response Team (ASERT) verifies every threat feed update to ensure customers can trust the quality of the feed.

Automated and Advanced DDoS Mitigation

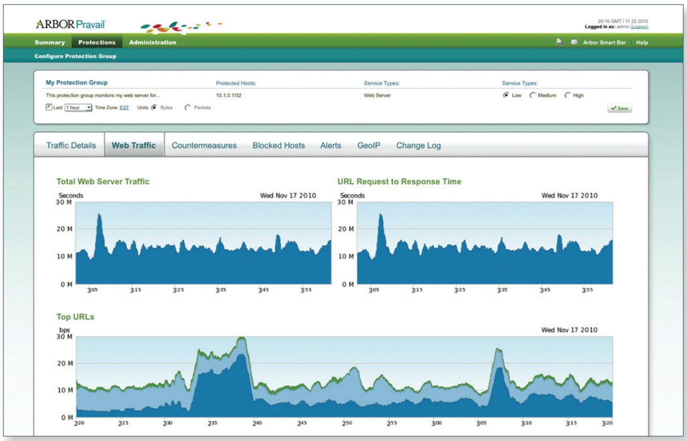
Many data center operators often do not know they are under attack until the availability of services is affected. Because the cost of downtime is extremely high for many organizations, data center operators require solutions that automatically detect and prevent DDoS attacks with little or no user interaction. The solution must also offer simple fallback plans or resolution techniques when attacks cannot be readily identified and mitigated in order to speed resolution. Data center operators can trust Pravail APS to quickly stop DDoS attacks, and Pravail’s intuitive user interface makes threat mitigation a snap.

Cloud Signaling

Because many volumetric attacks (i.e., those greater than the available bandwidth) cannot be stopped on-premise, they require service providers to mitigate the attacks in the cloud. At the same time, many cloud DDoS services cannot efficiently or quickly detect and stop lower-level application DDoS attacks. As a result, enterprises need a comprehensive DDoS solution with both cloud and on-premise protection to ensure 100% availability. Cloud Signaling is the glue that binds such a solution. By facilitating the communication from the on-premise Pravail APS appliance to the cloud-based Peakflow SP solution, the data center operator can shorten the time to resolution for DDoS attacks.

Real-Time and Historical Attack Forensics and Reporting

Pravail APS offers detailed attack reports in real time so operators can visually understand the actions taken by the appliance. Besides documenting these actions in audit logs, Pravail APS provides forensic reports detailing blocked hosts, origin countries of attacks and historical trends. The easy-to-understand reports can also be given to peers or management to educate them on the threats impacting the availability of services and the steps taken to address the attacks.



20:16 GMT | 11.22.2010
Logged in as: admin (Logout)

Configure Protection Group

My Protection Group
This protection group monitors my web server for...

Protected Hosts: 10.1.0.1/32

Service Types: Web Server

Service Types: ● Low ○ Medium ○ High

Last: 1 hour Time Zone: EST Units: ● Bytes ○ Packets

Real-time Alerting and Mitigation Dashboard

How Does Pravail Stop Application-Layer DDoS Attacks?

Pravail utilizes the dynamic ATLAS Intelligence Feed to detect and stop emerging threats including the following:

- DDoS Botnet Attacks
  Examples: BlackEnergy, Darkness
- Voluntary Botnet Attacks
  Examples: LOIC, HOIC
- “Slow HTTP” Attacks
  Examples: Slowloris, Pyloris
- Emerging DDoS Attacks Detected by ATLAS

Pravail leverages the following attack counter-measures to stop DNS, SIP, HTTP, and Layer 3/4 attacks:

- Flood Detection
  Examples: TCP SYN Floods, ICMP Floods
- Application Misbehavior
  Examples: Pucodex, HTTP Header Interrupt
- HTTP Header Regular Expressions
- HTTP Rate Limiting
- DNS Authentication
- Malformed DNS Filtering
- DNS Rate Limiting
- DNS NXDomain Rate Limiting
- DNS Regular Expression
- Malformed SIP Filtering
- SIP Request Limiting
- TCP SYN Authentication
- TCP Connection Reset
- Zombie Detection
- Payload Regular Expression
- Traffic Rate-Limiting
- Filter Lists

> **“Arbor Networks knows more about the Internet’s workings than possibly anyone outside the National Security Agency.”**
>
> Wired.com, “When Google Goes Down, It Falls Hard,” May 14, 2009

Pravail Appliance

All models utilize the same 2U rack height form factor.

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 6299 0695

www.arbornetworks.com

Arbor Pravail Appliance Specifications

Power Options
600W AC or DC hot-swap, redundant power supplies with PMBus support

Physical Dimensions
Chassis: 2U rack height
Height: 3.45 in (8.76 cm)
Width: 17.4 in (43.53 cm)
Depth: 24 in (61 cm)

Hard Drives
2 SSD in RAID 1

NICs
2 x 10/100/1000BaseT management interfaces, copper only

Optional, depending on model:
2 x 10GigE, SR or LR fiber
12 x 1GigE, SR or LR fiber
12 x 1GigE, copper

Inline bypass is supported for all interface options.

Inspected Throughput
APS 2104: 2 Gbps
APS 2105: 4 Gbps
APS 2107: 8 Gbps
APS 2108: 10 Gbps

Environmental
Temperature, operating:
50° to 95°F (10° to 35°C)

Temperature, non-operating:
-40° to 158°F (-40° to 70°C)

Humidity, non-operating:
95%, non-condensing at temperatures of 73° to 104°F (23° to 40°C)

Operating System
ArbOS® our proprietary, embedded operating system.

Compatibility
Monitoring: Integrates with management consoles supporting SNMP v3

Web-Based UI: IE-8+, Firefox 3.6+, Chrome and Safari

Regulatory Compliance
Complies with RoHS Directive 2002/95/EC

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for next-generation data centers and carrier networks, including the vast majority of the world’s Internet service providers and many of the largest enterprise networks in use today. Arbor’s proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the Active Threat Level Analysis System (ATLAS®). Representing a unique collaborative effort with 100+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.