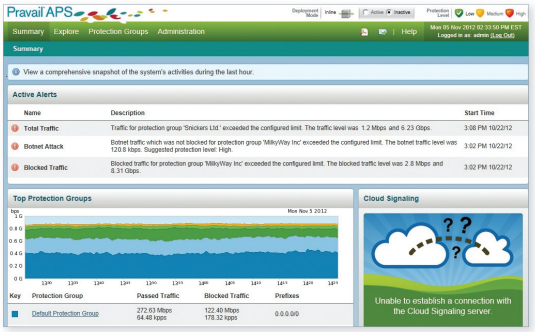
Pravail® Availability Protection System

Simplified, proven protection for enterprises and data centers

Distributed denial of service (DDoS) attacks present one of today's biggest IT threats for enterprises. With the rise of hacktivism, cyber terrorism and Internet crime, DDoS attacks are growing in size, frequency and sophistication. In fact, DDoS attacks are increasingly being used as part of the advanced threat landscape. In *Arbor Networks'® 8th Annual Worldwide Infrastructure Security Report*, respondents reported seeing more complex attacks—such as botnets or malware in conjunction with DDoS. The Pravail® portfolio of solutions from Arbor Networks® tackles these advanced threats head-on by giving organizations an enterprise-wide view of all network activities, critical attack details for fast remediation and expert-level blocking, all backed by world-class security research.

The Pravail® Availability Protection System ("Pravail APS"), Arbor provides organizations with proven, carrier-grade DDoS defense technology in a platform designed specifically for enterprise needs. Pravail APS helps protect business continuity and availability from the growing constellation of application-level threats. It provides the world's most advanced and sophisticated attack detection and mitigation technology in an easy-to-deploy appliance designed to automatically neutralize attacks before they impact critical services.



Pravail APS features an easy to navigate, easy to manage Web GUI. The opening summary page provides an overview of what types of attacks Pravail APS is seeing.

First Line of Defense for Enterprise Multi-Layer DDoS Protection

Availability attacks come in many forms, including low-bandwidth attacks aimed at the application layer and/or high volume "flood" attacks. Some low bandwidth attacks can cripple the enterprise but still 'fly under the rader of most-provider based, in cloud DDoS solutions. Flood attacks can saturate Internet links to the data center and are best mitigated within the provider network. To adequately address multiple types of attacks, enterprises need a comprehensive DDoS solution with both provider-based and on-premise protection. For enterprise's battling complex DDoS attacks, Pravail APS provides the on-premise protection that serves as an enterprise's first line of defense. Pravail APS offers proactive monitoring and blocking against:

- Application Layer DDoS Attacks
- State Exhausting Attacks
- Volumetric attacks (Up to link capacity)

Pravail APS customers can enhance their overall protection by using Cloud Signaling™. With this service, organizations can automatically alert upstream service providers when larger attacks threaten availability. With Cloud Signaling, users can enable cloud mitigation of DDoS attacks down to individual protection groups.

Arbor Leadership

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, it is likely using Arbor products.

Groundbreaking Research

Arbor security researchers have a real-time view of over 70 Tbps of global Internet traffic. This unmatched access to emerging threats enables the Arbor Security Engineering & Response Team (ASERT) to develop timely, automatic updates to Pravail APS.

Cloud Signaling™ Coalition

This innovative approach to DDoS defense delivers coordinated cloud and perimeter-based protection to the enterprise. Providers around the world are rapidly joining the coalition.

Availability Protection

Pravail APS from Arbor uses stateless attack detection and filtering. This allows Pravail APS to remain functional during low-volume attacks that are designed to overwhelm and cripple stateful devices, such as IPS or firewalls.

ARBOR® NETWORKS

Can You Afford to Ignore Availability Threats Like DDoS?

When Internet-facing services are down, the impact can have severe business consequences. Consider the following:

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. Attacks can continue for days, even weeks.

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.*

Arbor also provides another alternative for enhanced DDoS attacks with the Arbor Cloud®. Using Pravail APS as the on-premise protection, the Arbor Cloud service provides an on-demand traffic scrubbing service staffed by Arbor's DDoS security experts to quickly defend against volumetric DDoS attacks that are too large to be mitigated on-premise.

Traditional Perimeter Security Solutions Cannot Defend Against DDoS

Traditional perimeter security devices, such as firewalls and intrusion prevention systems (IPS), are essential elements of a layered-defense strategy, but are not designed to solve the DDoS problem. Firewalls enforce policies that govern access to data center resources, and IPS devices block threats that can exploit known vulnerabilities. DDoS is a different problem. DDoS attacks consist of legitimate traffic from multiple sources crafted to exhaust critical resources, such as link capacity, session capacity, application service capacity (e.g., HTTP(S), DNS) or back-end databases. Because such traffic is authorized and does not contain the signature content of known malware, it is not stopped by firewalls and IPS. In fact, firewalls and IPS are frequent victims of DDoS attacks. As inline, stateful inspection devices, they are subject to many of the vulnerabilities that DDoS attacks seek to exploit. A new class of security product is needed to specifically address DDoS threats to availability. Pravail APS is that solution.

Key Technologies

Why Firewall and IPS Devices Do Not Solve the Problem

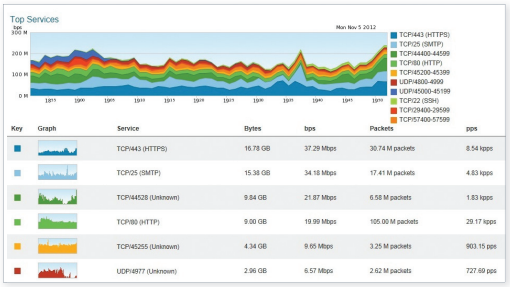
Vulnerable to DDoS Attacks	• Because these devices are inline, stateful devices, they are vulnerable and targets of DDoS attacks. • First to be affected by large flood or connection attacks.
Failure to Ensure Availability	• Built to protect against known (versus emerging) threats. • Designed to look 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-Based DDoS Protection Systems	• Fail to interoperate with cloud-based DDoS prevention solutions. • Increase time for response to DDoS attacks.
Lack of DDoS Expertise	• Require skilled security experts. • Demand knowledge of attack types before attacks.

Stateless Analysis Filtering Engine

Arbor's stateless packet filtering engine provides the foundation for both Pravail APS and Arbor service provider solutions. Unlike load balancers, IPS or firewalls, this unique packet filtering technology detects and mitigates most DDoS attacks without tracking any session state. In cases where tracking is required, it only stores minimal information for a short period of time. Tracking session state is essential for firewalls and many security appliances, but it also makes them vulnerable to DDoS attacks. Because it is not stateful, Pravail APS can withstand DDoS attacks that target session tables and knock other security appliances offline. Further, the filtering engine incorporates advanced packet-based DDoS countermeasures developed by the Arbor Security Engineering and Response Team (ASERT) to neutralize hundreds of malware families and other advanced threats.

Centralized Multi-Device Management via Pravail NSI

The Pravail Threat Console gives organizations a single dashboard to view and manage up to 25 Pravail APS devices. The Console provides full traffic visibility for each appliance and protection group, as well as a central log for all blocked threats. In addition, administrators have a single console where they can monitor security events and system status, manage black and white lists and respond to attacks with easy workflows on the console and single sign on to drill down into individual systems for more detail, such as packet captures.



Pravail APS provides detailed reports on attack traffic and allows users to easily enable different attack protections based on a variety of factors including IP Location, Web Domains or Top Services.

Customized Protection Recommendations with Immediate "Out-of-the-Box" Blocking

Pravail APS features a simple user interface that makes it easy to install, configure and use. Upon installation, the device will immediately begin blocking most attacks from causing harm to the network. However, it also features an optional calibration period where the product will record and analyze traffic patterns unique to the organization and recommend customized protection settings for that network and its specific applications. During this calibration, the network remains protected from most threats.

SSL Inspection

Many organizations rely on Secure Socket Layer (SSL) encryption for transmitting data securely. Unfortunately, attackers can also encrypt their attacks, so Pravail APS must also inspect encrypted traffic for threats. Using an off box SSL decryption device, Pravail APS can inspect data that has been previously encrypted to identify attacks that have been embedded and help block those threats from harming the network. Once the traffic has been inspected, "clean" encrypted traffic is transmitted to the intended destination.

Automated and Advanced DDoS Protection

Because the cost of downtime is extremely high for many organizations, Pravail APS is designed to automatically detect and prevent 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, Pravail APS can recognize legitimate CDN traffic and will not accidentally block it.

ATLAS® Intelligence Feed (AIF)

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 over 70% of global Internet traffic. This gives Arbor unmatched insight into emerging threats—information used by ASERT to develop defenses against new, emerging threats. ATLAS Intelligence Feed (AIF) is an update service that automatically provisions Pravail APS appliances with the latest defenses to new threats and updates IP location data—all in real time.

Advanced Web Crawler Service

Pravail APS delivers superior availability protection without impacting a Web site's page ranking and search engine results. ASERT maintains policies in AIF that allow specific Web crawlers to access your site, but blocks those that are malicious or irrelevant.

Visibility, Control and Alerting

Pravail APS is not a "black box." While it delivers automated protection from DDoS, Pravail APS also provides real-time visibility into attacks, blocked hosts and even packets. It offers the flexibility operators need to alter attack countermeasures and thresholds if required. Pravail APS includes active alerting that notifies security engineers of ongoing attacks that are blocked, as well as other network events that may require their attention.

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. 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.

Advanced DDoS Defense

Gain 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

Pravail APS also allows user-configured custom protection.

"During recent elections, our networks were under constant attack. We deployed Pravail APS in advance of the elections as a precaution and the attacks were not successful."

Rene Miranda, CIO, IFE

“Pravail APS’s ease of use, out-of-box protection readiness and automatic ATLAS intelligence feeds contribute to low management overhead without sacrificing protection on-premises.”

Michael Suby, Stratecast Vice President of Research

Pravail APS appliance: All models utilize the same 2U rack height form factor. The appliance is managed and customizable through a Web-based GUI.

System Specifications

Features	Description
HARDWARE	
Physical Dimensions	Chassis: 2U rack height Height: 3.45 inches (8.67 cm) Width: 17.4 inches (43.53 cm) Depth: 24 inches (61 cm) Weight: 41 lbs. (18.5 kg)
Power Options	2 x AC or 2 x DC redundant hot swappable power supplies; 600W max continuous output; PMB bus support
Hard Drives	2 SSD in RAID 1; 2 x 120 GB drives
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% Operating humidity: 5-85% Non-condensing at temperatures: 73° to 104°F (23° to 40°C)
Operating System	Our proprietary, embedded ArbOS® operating system
Management	SNMP gets v1, v2c; SNMP traps v1, v2c, v3; CLI; Web UI; HTTPS; SSH customizable, role-based management
Management Interfaces	2 x 10/100/1000 BaseT Copper; RJ-45 serial console port
Authentication	On device, RADIUS; TACACS
Availability	Inline bypass, dual power supplies, solid-state hard drive RAID cluster
MTBF	44K Hrs
Regulatory Compliance	Complies with RoHS Directive 2002/95/EC
Web-Based GUI	Supports multi-language translated user interfaces
Supported Browsers	Firefox ESR 24, Firefox 24, Google Chrome 29, Internet Explorer 9, Internet Explorer 10, Safari 6
MANAGEMENT AND SECURITY	
Simultaneous Connections	Not applicable: Pravail APS does not track connections
Protected Endpoints	Unlimited
Latency	Less than 80 microseconds
User-Configured Protection Groups	50
Reporting and Forensics	Real-time and historic traffic reporting, extensive drill-down by protection group and blocked host including total traffic, passed/blocked, top destination URLs/services/domains, attack types, blocked sources, top sources by IP location. Packet visibility in real-time.
DDoS Protection	TCP/UDP/HTTP(S) flood attacks, botnet protection, hacktivist protection, host behavioral protection, anti-spoofing, configurable flow expression filtering, payload expression-based filtering, permanent and dynamic blacklists/whitelists, traffic shaping, multiple protections for HTTP, DNS and SIP, TCP connection limiting, fragmentation attacks, connection attacks.
Modes	Inline active; inline inactive (reporting, no blocking); SPAN port monitor
Real-Time Updates	ATLAS Intelligence Feed (AIF): Signature database for over hundreds of families of malware—e.g. slowloris, LOIC, YoyoDDOS, BlackEnergy, etc. IP location data also updated in real time.
Notifications	SNMP trap, syslog, email
Cloud-Signaling	Yes (collaborative DDoS attack mitigation with service providers)

Hardware Options

APS 2000 Series	APS 2002	APS 2003
Memory	24 GB	24 GB
Inspected Throughput	Up to 500 Mbps	Up to 1 Gbps
HTTP(s) Connections per Second	111K at recommended protection level; 186K filter list only protection	111K at recommended protection level; 186K filter list only protection
Processor	Single Intel Xeon CPU 2.40GHz	Single Intel Xeon CPU 2.40GHz
Protection Interface Options	• 8 x 10/100/1000 BaseT Copper • 8 x GE SX; or 8 x LX Fiber	• 8 x 10/100/1000 BaseT Copper • 8 x GE SX; or 8 x LX Fiber
Traffic Bypass Options	• Integrated hardware bypass; • Internal “software” bypass to pass traffic without inspection	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection

APS 2100 Series	APS 2104	APS 2105	APS 2107	APS 2108
Memory	24 GB	24 GB	24 GB	24 GB
Inspected Throughput	Up to 2 Gbps	Up to 4 Gbps	Up to 8 Gbps	Up to 10 Gbps
Maximum Flood DDoS Prevention Rate	9M pps	9M pps	9M pps	9M pps
HTTP(s) Connections per Second	368K at recommended protection level; 613K filter list only protection	368K at recommended protection level; 613K filter list only protection	368K at recommended protection level; 613K filter list only protection	368K at recommended protection level; 613K filter list only protection
Processor	2 Intel Xeon CPU	2 Intel Xeon CPU	2 Intel Xeon CPU	2 Intel Xeon CPU
Protection Interface Options	• 12 x 10/100/1000 BaseT Copper • 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber • 12 x GE SX Fiber • 12 x GE LX Fiber • 4 x 10 GE SR Fiber • 4 x 10 GE LR Fiber	• 12 x 10/100/1000 BaseT Copper • 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber • 12 x GE SX Fiber • 12 x GE LX Fiber • 4 x 10 GE SR Fiber • 4 x 10 GE LR Fiber	• 12 x 10/100/1000 BaseT Copper • 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber • 12 x GE SX Fiber • 12 x GE LX Fiber • 4 x 10 GE SR Fiber • 4 x 10 GE LR Fiber	• 12 x 10/100/1000 BaseT Copper • 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber • 12 x GE SX Fiber • 12 x GE LX Fiber • 4 x 10 GE SR Fiber • 4 x 10 GE LR Fiber
Bypass Options	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection

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 68096226

www.arbornetworks.com

DS/PRAVAIL5.5/EN/1113-LETTER