[DATA SHEET]

Arbor Pravail

Availability Protection System (APS)

SIMPLIFIED, PROVEN PROTECTION FOR YOUR WEBSITE & ONLINE BUSINESS

Data centers are exposed to a growing variety of distributed denial of service (DDoS) attacks. These range from flood attacks that exhaust network bandwidth to attacks that target key applications such as email, web services, e-commerce and Voice over IP (VoIP). Attacks are becoming more sophisticated yet easier to perpetrate. As a result, data center operators around the world are experiencing outages due to DDoS more frequently and with more severe consequences to their businesses than ever before.

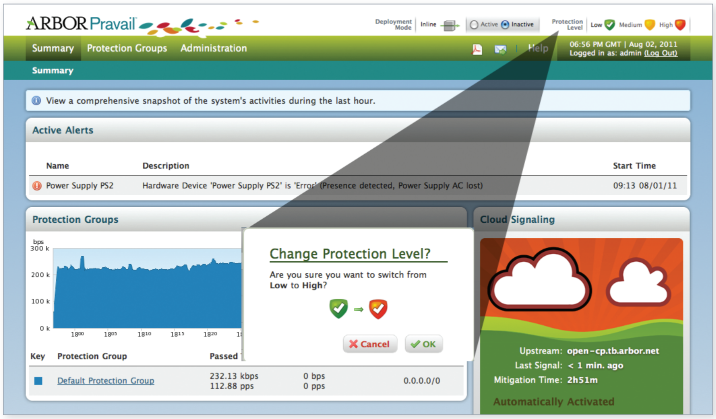
Arbor Networks® is the preferred provider of DDoS defense solutions to service providers, large hosting providers and cloud providers. As the defacto standard for DDoS defense at the vast majority of Tier-1 and Tier-2 ISPs, Arbor has the most proven and trusted technology for neutralizing DDoS attacks. With the Arbor Pravail™ Availability Protection System ("Pravail APS"), proven, carrier-grade DDoS defense technology is available to protect the enterprise data center.

Data Center Consolidation, Cloud Computing and Botnets

The accelerating trend of consolidation and cloud computing means enterprises are more dependent than ever on their data centers. Availability of services (such as web, e-commerce, financial transactions, supply chain, email, etc.) is critical. If key applications are down, business grinds to a halt.

The global spread of botnets (collections of compromised computers) has led to an epidemic of DDoS attacks. As attack tools become more sophisticated and easier to use, botnet operators are bringing down targeted applications with low bandwidth attacks that escape detection both in provider networks and by traditional perimeter security devices. Data center operators are typically unaware of such attacks until critical services are down or badly degraded. At that point, there can be extreme pressure to find and fix the problem. Yet the tools and expertise to do so are often lacking.

Pravail APS is designed specifically to 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 that automatically neutralizes attacks before they impact critical services.



06:56 PM GMT | Aug 02, 2011
Logged in as: admin (Log Out)

View a comprehensive snapshot of the system's activities during the last hour.

Active Alerts

Name	Description	Start Time
Power Supply PS2	Hardware Device 'Power Supply PS2' is 'Error' (Presence detected, Power Supply AC lost)	09:13 08/01/11

Protection Groups

Key	Protection Group	Passed		
■	Default Protection Group	232.13 kbps 112.88 pps	0 bps 0 pps	0.0.0.0/0

Change Protection Level?

Are you sure you want to switch from **Low to High?**

Cloud Signaling

Upstream: open-cp.tb.arbor.net
Last Signal: < 1 min. ago
Mitigation Time: 2h51m

Automatically Activated

Pravail APS Web GUI summary screen. By clicking on the "Protection Level" icons you can enable preset protections for your Web server or other specified servers/groups in your data center.

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, chances are it is using Arbor products.

Leading Research

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 and Response Team (ASERT) to develop timely, automatic updates to Pravail APS.

Cloud Signaling℠ Coalition

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

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.*

Traditional Perimeter Security Solutions Cannot Fully Defend Against DDoS

Traditional perimeter security 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 block malware that can infect end systems or exploit known vulnerabilities. DDoS is a different problem. DDoS attacks consist of legitimate traffic from multiple sources crafted to exhaust critical resources—whether that be link capacity, session capacity, application service capacity (e.g. http, DNS) or back-end databases. Because such traffic is authorized and does not contain signature content of known malware it is not stopped by firewalls and IPS. In fact, firewall 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 is that solution.

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.

Key Technologies

Immediate "Out-of-the-Box" Protection

Pravail APS is easy to install and provides immediate protection from most threats. Configuration is straightforward, and Pravail APS does not require a learning period. Security and networking personnel will appreciate the streamlined configuration process and simple user interface.

Automated and Advanced DDoS Protection

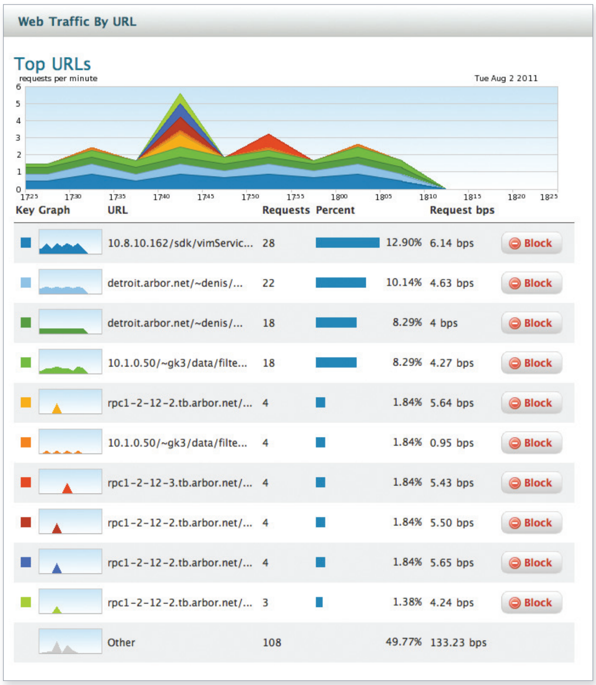
Because the cost of downtime is extremely high for many organizations, Pravail APS is designed to automatically detect and prevent DDoS attacks with little or no user interaction—before services are degraded. Pravail APS also offers simple fallback plans and resolution techniques when attacks cannot be readily identified and mitigated to speed resolution.

Visibility and Control

Pravail APS is not a "black box." While it delivers automated protection from DDoS, Pravail APS also provides real-time visibility into attacks and the flexibility operators need to alter attack countermeasures and thresholds if needed.

Full Suite of Attack Countermeasures

Pravail APS incorporates advanced DDoS countermeasures that Arbor has developed and deployed at leading ISPs, Multiple System Operators (MSO), financial institutions, and cloud and hosting providers. This technology has proven robust and effective in the most demanding environments around the world. In addition, the Arbor Security Engineering and Research Team (ASERT) has developed a new set of packet-based protections which neutralize over 150 families of malware that comprise the vast majority of the global botnet threat.



Web Traffic By URL

Top URLs

Key Graph		URL	Requests	Percent	Request bps	
■		10.8.10.162/sdk/vimServic...	28	12.90%	6.14 bps	Block
■		detroit.arbor.net/~denis/...	22	10.14%	4.63 bps	Block
■		detroit.arbor.net/~denis/...	18	8.29%	4 bps	Block
■		10.1.0.50/~gk3/data/filte...	18	8.29%	4.27 bps	Block
■		rpc1-2-12-2.tb.arbor.net/...	4	1.84%	5.64 bps	Block
■		10.1.0.50/~gk3/data/filte...	4	1.84%	0.95 bps	Block
■		rpc1-2-12-3.tb.arbor.net/...	4	1.84%	5.43 bps	Block
■		rpc1-2-12-2.tb.arbor.net/...	4	1.84%	5.50 bps	Block
■		rpc1-2-12-2.tb.arbor.net/...	4	1.84%	5.65 bps	Block
■		rpc1-2-12-2.tb.arbor.net/...	3	1.38%	4.24 bps	Block
		Other	108	49.77%	133.23 bps	

Pravail APS Web GUI top URL screen. By clicking on the "Block" icon you can surgically block traffic to your Web server or data center. Traffic summaries can also be viewed by geographic location (e.g., North America, Russia, China).

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 Arbor security researchers (ASERT) to develop defenses to new, emerging threats. Arbor's ATLAS Intelligence Feed (AIF) is a real-time update service that automatically provisions Pravail APS appliances with the latest defenses to new threats.

Cloud Signaling

Low bandwidth attacks that are so effective in bringing down data center applications generally "fly under the radar" of most provider-based, in-cloud DDoS solutions. However, DDoS also consists of bandwidth-consuming flood attacks that saturate Internet links to the data center. These volumetric attacks can only be mitigated within the provider network. Enterprises need a comprehensive DDoS solution with both provider-based and on-premise protection. Cloud Signaling℠ enables this comprehensive protection. With Cloud Signaling, Pravail APS automatically alerts the upstream provider to growing attacks that threaten availability.

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.

Performance

Load balancers, firewalls and IPS devices (even those with anti-DDoS features) are often the first points of failure in a DDoS attack because their capacity to track sessions becomes exhausted. The unique packet-based defenses of Pravail APS avoid this vulnerability. Pravail APS detects and mitigates most DDoS attacks without tracking any session state, and only minimal information is stored for short periods of time where some session tracking is required. Under real-world conditions, Pravail APS mitigates attacks up to the capacity of the network link to deliver traffic to it. If the link approaches saturation, Pravail APS Cloud Signaling alerts the upstream provider to initiate mitigation in the cloud. The result: the data center is fully protected.

Advanced DDoS Defense

Offering 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
- DNS Cache poisoning attacks
- DNS Request floods
- SIP Request floods
- Custom Attacks—attacks unique to your service
- IP location-based protection
- Pravail also allows for user configured custom protections

> **"If your data center is not available, all the compliance or data integrity in the world is not going to help your customers, business or your brand. Arbor is addressing the number one threat to the availability of data center resources…"**
>
> Rob Ayoub, Frost and Sullivan, Global Program Director, Network Security

> **“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 Appliance

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

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

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

Small Packet Performance
8.5M pps at recommended protection level
9.6m pps filter list only protection

HTTP Connections/Second
368K at recommended protection level
613K filter list only protection

Simultaneous Connections
N/A—Pravail does not track connections

Protected Endpoints
Unlimited

User Configured Protection Groups
50

Power Options
2 x AC or 2 x DC redundant hot swapable power supplies; 600W max continuous output; PMB bus support

Physical Dimensions
Chassis: 2U rack height
Height: 3.45 in (8.67 cm)
Width: 17.4 in (43.53 cm)
Depth: 24 in (61 cm)
Weight: 41 lbs (18.5 kg)

Hard Drives
2 SSD in RAID 1; 2 x 120GB drives

Memory
18 GB

Processor
2 Intel Xeon CPU 2.40GHz

Protection Interfaces
2 x 10 GE SR or LP fiber OR 12 x GE SX or LX Fiber OR 12 x GE copper

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.

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; 5 USB 2.0 ports

Authentication
On device, RADIUS; TACACS

Availability
Inline bypass

MTBF
44K Hrs

Regulatory Compliance
Complies with RoHS Directive 2002/95/EC

Web-based GUI
Supports multi-language translated user interfaces

Supported Browsers
Firefox 3.6, Firefox 4.0^{+} (anything past 4.0); Opera; Safari 5.0^{+} (anything past 5.0); Chrome 11.0^{+} (anything past 11.0); IE 8 and 9

Reporting and Forensics
Real time and historic traffic reporting, extensive drill down by protection group—total traffic, passed/blocked, top destination urls/services/domains, attack types, blocked sources, top sources by IP location.

DDoS Protection
TCP/UDP/HTTP 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 Stack attacks, fragmentation attacks, connection attacks.

Modes
Inline Active; Inline Inactive (reporting, no blocking); SPAN port Monitor

Real Time Updates
Active Intelligence Feed (AIF): Signature data base for over 150 families of malware—e.g. slowloris, LOIC, YoyoDDOS, BlackEnergy, etc.

Notifications
SNMP trap, syslog, email

Cloud Signaling
Yes (collaborative DDoS attack mitigation with service providers)