Pravail® Availability Protection System

Always-On, In-Line, DDoS Protection

As your dependency for web-based applications and services increase, the risk of distributed denial of service (DDoS) attacks grows. In Arbor Networks' latest *Worldwide Infrastructure Security Report,* respondents reported seeing more complex attacks—such as botnets or malware in conjunction with DDoS. And in more traditional volumetric-based attacks, the size of the attack continues to grow. The Pravail portfolio of solutions from Arbor Networks tackles these advanced threats head-on by providing you a complete view of network activities for fast remediation and expert-level blocking.

The Pravail® Availability Protection System helps protect business continuity and availability from the growing constellation of application-layer threats. It provides the world's most advanced and sophisticated attack detection and mitigation technology in an easy-to-deploy platform designed to automatically neutralize IPv4 and IPv6 attacks before they impact critical applications and services.

With the ATLAS® Intelligence Feed capability, real-time updates containing actionable intelligence on DDoS and advanced threats attacks can help prevent an attack from entering your network. Such capabilities are:

- DDoS protection from active botnets
- DDoS protection from active DDoS campaigns based on IP reputation
- Advanced web crawler service
- GeoIP tracking
- Domain and IP reputation to block threats

The Pravail Availability Protection System enhances your overall protection by using Cloud Signaling™ to connect local protection with cloud-based DDoS services. With Cloud Signaling, the Pravail Availability Protection System automatically alerts upstream service providers, such as your ISP or Arbor Cloud℠, when larger attacks threaten availability. This allows for a faster time to mitigate attacks. In conjunction with Arbor Cloud, this time can be reflected in just seconds.

Combining the comprehensive intelligence of the ATLAS Intelligence Feed, and the expanded mitigation capability of Arbor Cloud with the Pravail Availability Protection System, you have a multi-layered integrated solution that provides the most advanced DDoS protection.

Key Pravail Availability Protection System Technologies

Key Capabilities	
• Stateless analysis filtering engine • Centralized management of multiple devices via Pravail Threat Console or Pravail Network Security Intelligence • "Out-of-the-box" blocking with custom protection recommendations • Secure Socket Layer (SSL) Inspection	• Automated and advanced DDoS protection • Outbound threat filter for non-DDoS threats • Visibility, control and alerting • Real-time and historical attack forensics and reporting • Protection for both IPV4 and IPv6 networks environments.

Can You Afford to Ignore Availability Threats Like DDoS?

When your Internet-facing services are down, the impact to business has severe consequences. Consider the following:

Loss of Revenue
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.

ARBOR® NETWORKS

Arbor Leadership

Availability Protection

The Pravail Availability Protection System uses stateless attack detection and filtering. This allows the Pravail Availability Protection System to remain functional during attacks designed to overwhelm and cripple stateful devices, such as firewalls and IPS devices.

Groundbreaking Research

With over 120 Tbps of global Internet traffic analyzed in real-time, Arbor security researchers have unmatched access to emerging threats. This capability combined with Arbor's expertise enables the Arbor Security Engineering & Response Team (ASERT) to develop timely, automatic updates to the Pravail Availability Protection System.

Cloud Signaling™ Coalition

With providers from around the world actively participating, this innovative approach to DDoS defense establishes a coordinated, automated cloud and perimeter-based protection architecture.

Proven and Trusted

It's no accident that the majority of the world's largest service providers rely on Arbor Networks for DDoS defense. It is likely that your network service provider is using Arbor products today, especially if they offer DDoS protection services.

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

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 68096226

www.arbornetworks.com

DS/PRAVAILAPS/EN/0415-LETTER

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 • Common Criteria Certified EAL-2 (2100-series appliances, version 5.4)
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 Availability Protection System does not track connections
Protected Endpoints	Unlimited
User-Configured Protection Groups	50
Reporting and Forensics	Real-time and historical IPV4 and IPV6 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.
Maximum DDoS Flood Prevention Rate	**2000-series:** Up to 3 Mpps **2100-series:** Up to 11.4 Mpps
Modes	Inline active; inline inactive (reporting, no blocking); SPAN port monitor
Notifications	SNMP trap, syslog, email
Cloud Signaling	Yes (collaborative DDoS attack mitigation with service providers)

Hardware Options

2000 Series Features	2002	2003
Memory	24 GB	24 GB
Inspected Throughput	500 Mbps	1 Gbps
Latency	Less than 80 microseconds	
HTTP(s) Connections per Second	111K at recommended protection level; 186K filter list only protection	
Processor	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	
Traffic Bypass Options	• Integrated hardware bypass • Internal "software" bypass to pass traffic without inspection	
SSL Decryption Options	• Inspected Throughput: Up to 500 Mbps • HTTPS Connections: Up to 7,500	• Inspected Throughput: Up to 750 Mbps • HTTPS Connections: Up to 7,500

2100 Series Features	2104	2105	2107	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
Latency	Less than 80 microseconds			
HTTP(s) Connections per Second	368K at recommended protection level; 613K filter list only protection			
Processor	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	
Bypass Options	• Integrated hardware bypass • Internal "software" bypass to pass traffic without inspection			
SSL Decryption Options	Inspected Throughput: Up to 2 Gbps	Inspected Throughput: Up to 4 Gbps	Inspected Throughput: Up to 5 Gbps	Inspected Throughput: Up to 5 Gbps
	HTTPS Connections: Up to 45,000			
	Concurrent Sessions: Up to 150,000			