TECHNOLOGY AUDIT

Pravail Availability Protection System, Version 2

Arbor Networks

Reference Code: OI00070-085

Publication Date: July 2011

Author: Graham Titterington

SUMMARY

Catalyst

The Pravail Availability Protection System (APS) protects the Internet data center edge from application layer distributed denial of service (DDoS) attacks. This is an issue that has not been adequately addressed in the past because stateful firewalls often become overwhelmed by DDoS attacks. With the increase in online extortion and politically motivated attacks against enterprises, this issue has risen up the business agenda.

Key findings

- Pravail APS is targeted at larger enterprises and complements Arbor Networks' existing Peakflow appliance, which is designed for service providers and some enterprises with very large data flows into their data center.
- Arbor Networks has a strong position in the high-end network security market.
- Pravail APS is sold as an appliance that requires minimal configuration and management. A single box will be adequate for almost all data centers.
- Pravail APS uses a comprehensive range of techniques to detect malicious traffic.

- Pravail APS can work together with the Arbor Network Peakflow anomaly-detection product, deployed in the service provider network, to block attacks before they reach the corporate data center.
- Pravail needs to be deployed alongside other security products, as it is designed specifically to protect users against a DDoS attack and does not protect against other threats, such as data theft through the Internet gateway.

Ovum recommends

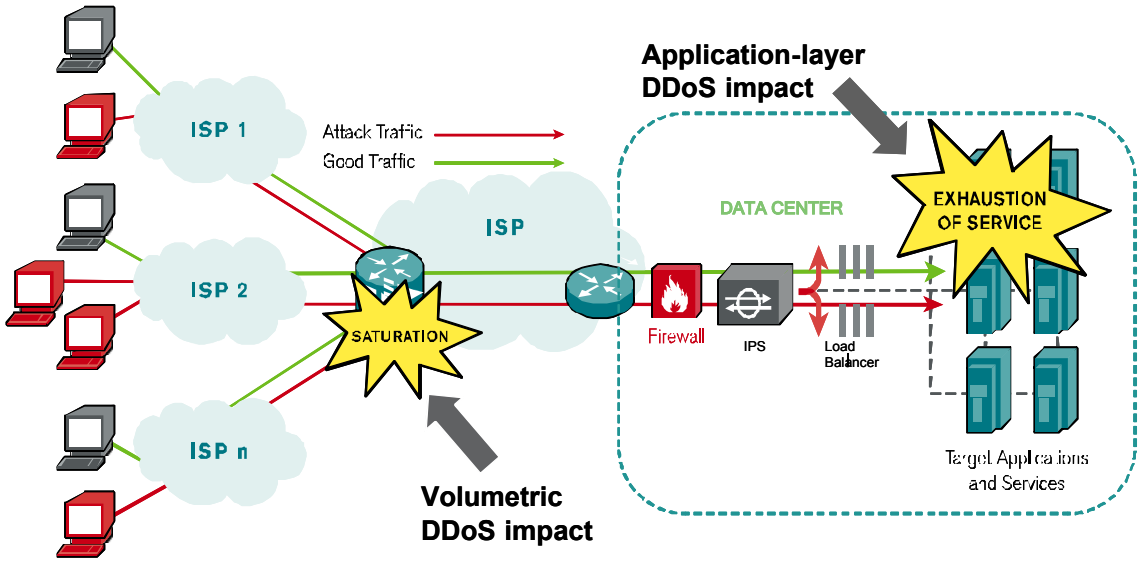
Pravail APS is a new kind of security product that is designed to perform a specific purpose, defending against DDoS attacks, effectively and with a minimum of administration. This complements, rather than replaces, existing information security provision. The decision about whether to deploy Pravail is therefore one of balancing the cost of the investment against the business benefit. With growing frequency of DDoS attacks against prominent businesses, either to threaten the business and extort money from it or to make a political point, the balance of the argument will shift towards providing more protection.

Arbor Networks has a strong record in the secure network field, and is used by most telcos and many large enterprises. Existing state-based firewalls are simply not up to the job of blocking a concerted DDoS attack because a stateful firewall or intrusion prevention appliance becomes overwhelmed and can therefore be the means by which a denial of service attack achieves its objective!

Value proposition

Protecting the availability of Internet-facing services is a crucial requirement in maintaining the brand and reputation of an enterprise, building customer confidence, and securing the revenue flow that comes from uninterrupted business. The evolving threat of both volumetric and application layer DDoS attacks against data centers is illustrated in Figure 1.

Figure 1: The evolving DDoS threat against data centers



Source: Ovum

Intrusion prevention devices and gateway firewalls enforce policy for Internet connections and prevent unauthorized access. They protect network integrity and confidentiality, but not network availability. This is why organizations also need Pravail APS.

Arbor Networks has developed Cloud Signaling (a protocol to facilitate defending against both large volume attacks and attacks against specific applications and services, as they occur). Cloud Signaling enables Arbor Networks products deployed in enterprise data centers and in service provider networks to work together to block attacks. When a data center discovers that it is suffering a DDoS attack, Cloud Signaling enables it to ask its ISP to block the malicious traffic within the operator network. This drastically reduces the traffic volume on the data center link. The ISP and the enterprise can continue to cooperate to investigate and eliminate the threat. It enables the service provider to build a closer relationship with its major customers. The Cloud Signaling Coalition is a new initiative, launched in May 2011 with 5 initial ISP members, and more are expected to join soon.

Arbor Networks has an existing product, called Peakflow, that also complements Pravail. Peakflow performs network-wide anomaly detection and traffic engineering. Service providers are the

primary users, although a few very large enterprises have also deployed it. Approximately 80% of tier-1 and -2 service providers use Peakflow. Several of these also offer managed services to their customers based on Peakflow. Pravail provides a more business-service focused view of Internet activity, protecting specific data centers and online services.

SOLUTION ANALYSIS

Functionality

The key functions of Pravail APS are:

- "Out-of-the-box" protection from active threats on the Internet
- Advanced DDoS blocking for emerging application layer threats, based on packet inspection
- Botnet threat mitigation by preventing illegitimate communications from reaching servers, and by blocking DDoS attacks originating from botnets in the enterprise environment
- Cloud Signaling to coordinate with Cloud Signaling-enabled service providers.

The blocking strategy implemented in Pravail APS is well tuned to business needs. The aim is to allow legitimate users into the system. Its filter examines each host that is trying to connect to the data center, checking its location, status, and behavior. It checks if the communications coming from it are similar to normal business interactions. Altogether Pravail uses 30 behavioral traits to check the legitimacy of hosts.

Arbor Networks uses the Active Threat Level Analysis System (ATLAS) Intelligence Feed, which monitors Layer-7 traffic in the Internet and identifies known botnets. ATLAS is a collaborative effort of over 100 ISPs who share anonymous traffic data every hour using the Arbor Networks' technology that sits on their networks, along with information from Arbor's own Internet probes and third-party sources. Currently, about 150 types of botnet are known to be responsible for DDoS attacks, with 2 or 3 new ones appearing each week. DDoS botnets are more specialized than general spam-generating botnets.

Each Pravail appliance provides comprehensive reporting facilities. There is no enterprise-wide management or reporting console for Pravail. Reporting is normally done locally on each appliance, as one box is adequate for a data center, and there is little benefit in consolidating reports about DDoS threats across the global network of data centers as each one provides different services. The DDoS reporting requirements are more local than the reporting requirements relating to data theft attacks, for example.

Go-to-market strategy

The target market is the data center of large enterprises and mid-sized businesses. Likely target verticals include financial services, online retailers, governments, and healthcare. In addition, hosting providers and ISPs may offer Pravail as a value-added service to their enterprise customers.

Arbor Networks plans to sell Pravail through OEM partners, distributors, and resellers to enterprise customers. Its direct sales organization targets ISPs and hosting providers.

The perceived competitors are the firewall and IPS device vendors but, as we have said already, Pravail has a more complementary than competitive relationship with these products.

Arbor Networks plans to release major upgrades to the product every 6–9 months, with minor updates as needed.

Deployment

The Pravail APS appliance should normally be deployed in-line and on-premise in the corporate data center. It should be deployed in front of the firewall, outside the DMZ, in order to protect the firewall from state-exhausting attacks. However, it can be deployed out-of-band if the organization only wants to monitor for threats, and there is also a "monitor only" mode of operation for in-line deployment. One physical appliance can analyze between 2GB/sec and 10GB/sec of data, depending on the license that has been purchased. The license refers to the bandwidth of filtered traffic allowed through to the data center. An organization can upgrade its license when it needs to increase this bandwidth, without making any other changes. This helps to protect investment in the product through its expected life. This range of bandwidth should be adequate for almost any corporate Internet data center.

Pravail APS has been designed to facilitate remote management by a managed service provider, and it can also be deployed by a service provider within its hosting center on behalf of an enterprise.

The configuration and setup of a Pravail appliance is simple, requiring just one person with a basic understanding of networking and security threats. The basic secure default configuration is supplied out-of-the-box but there may be some local policies or preferences that need to be configured.

Arbor Networks' technical support provides remote diagnosis of faults in the appliance, and if necessary replacement of the device within three days. It is charged at 19% of product list price and also provides 24x7 phone and email support, along with software maintenance upgrades.

A 2G Pravail appliance will be priced around $65,000.

Pravail APS is a new product that is currently undergoing beta testing and will be generally available in 3Q11. Ovum therefore cannot describe any live deployment examples at this stage.

DATA SHEET

Key facts about the solution

Table 1: Data sheet

Product name:	Pravail Availability Protection System	**Product classification:**	Network security appliance
Version number:	2	**Release date:**	September 2011
Industries covered:	Financial services, online retailers, government, healthcare, ISPs, and hosting providers	**Geographies covered:**	All
Relevant company sizes:	Mid to large businesses and enterprises	**Platforms supported:**	N/A
Languages supported:	English	**Licensing options:**	The license can be varied to match the required throughput of inspected traffic
Deployment options:	Appliance on-premise, or remotely managed, or hosted	**Route(s) to market:**	Direct, OEM, and distributor/reseller
URL:	www.arbornetworks.com	**Company headquarters:**	6 Omni Way Chelmsford, MA 01824 US T: +1.978.703.6600
European headquarters:	Lakeside House 1 Furzeground Way Stockley Park Uxbridge, Middlesex UB11 1BD United Kingdom T: +44 208 622 3108	**North America headquarters:**	Same as company headquarters
Asia/Pacific headquarters:	152 Beach Road Unit 10-07 Singapore 189721 T: +65 6299 0695		

Source: Ovum

APPENDIX

Author

Graham Titterington, IT Infrastructure team, Principal Analyst, Information Security

Graham.Titterington@ovum.com

Ovum Consulting

We hope that the analysis in this brief will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.