WHITE PAPER

Why IPS Devices and Firewalls Fail to Stop DDoS Threats

HOW TO PROTECT YOUR DATA CENTER'S AVAILABILITY

ARBOR® NETWORKS

Executive Summary

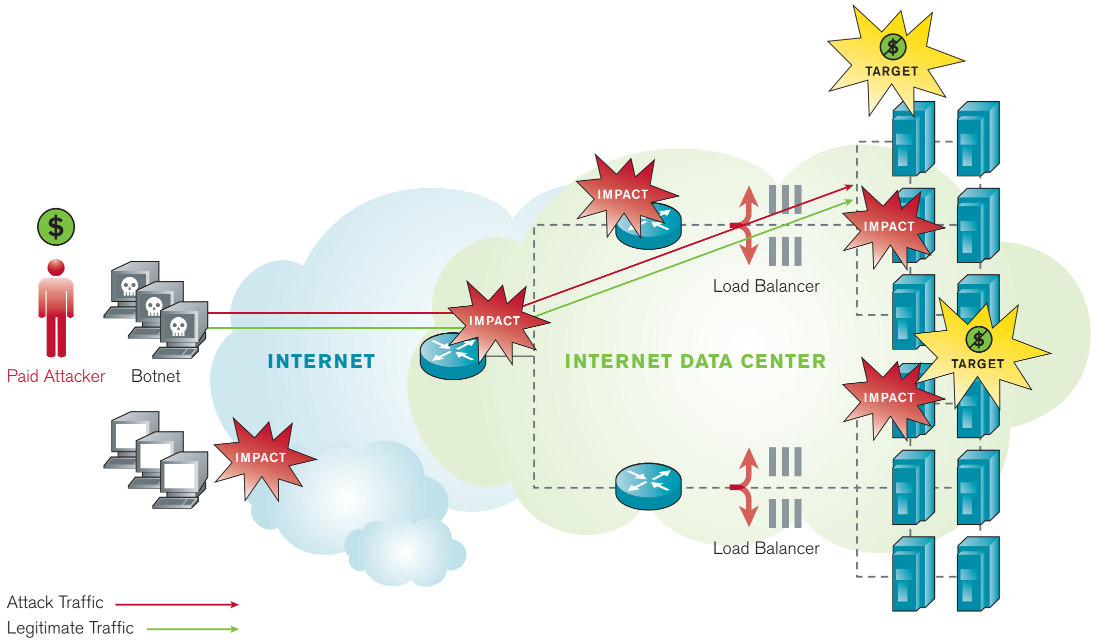
As e-commerce continues to proliferate and deliver profitable results, more business is being done online. The growing adoption of online retailing, Internet banking, cloud-based data storage and other commercial services represents a natural evolution of Internet use. For online businesses, however, any downtime can dramatically impact the bottom line. As a result, the growing scale and frequency of distributed denial of service (DDoS) attacks are taking a toll on these businesses. While DDoS attacks may have been driven by non-economic reasons in the past, they now have monetary drivers including extortion, competitive advantage and corporate revenge.

When it comes to DDoS protection, many enterprises and Internet data center (IDC) operators have a false sense of security. They think they have secured their key services against DDoS attacks simply by deploying intrusion prevention system (IPS) devices or firewalls in front of their servers. Unfortunately, such deployments can actually expose these organizations to service outages and irate customers. When business-critical services are not available, enterprises and IDC operators lose money and damage important customer relationships. What's more, when services are unavailable due to external attacks, it can be sensational and unwelcome front-page news—especially when the damages could have been easily prevented.

This white paper examines why IPS devices and firewalls fail to stop DDoS threats. It also describes how an ***intelligent DDoS mitigation system (IDMS)*** offers an ideal solution by enabling a layered defense strategy to combat both volumetric and application-layer DDoS attacks.

The Growing and Evolving DDoS Threat

During the last few years, DDoS attacks have been dominated by "volumetric" attacks usually generated by Internet bots or compromised PCs that are grouped together in large-scale botnets. Some examples include the DDoS attacks against UK-based online betting sites[1] where the hackers extorted the gambling firms, and the politically motivated DDoS attacks against the Georgian government.[2] 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, and they remain a major threat to enterprises and Internet service providers (ISPs) alike.



DDoS driven by financial motivations

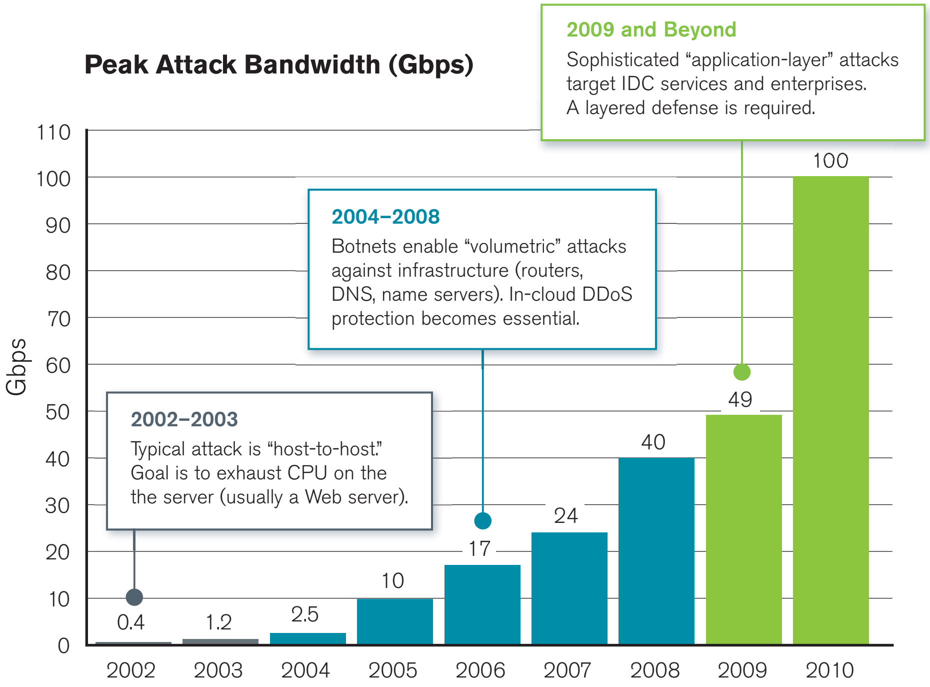
[1] news.bbc.co.uk/2/hi/technology/4169223.stm

[2] www.cnn.com/2009/TECH/08/07/russia.georgia.twitter.attack

In addition, a new type of DDoS attack has emerged that threatens the business viability of service provider customers. Two days before Christmas in 2009, last-minute shoppers could not access some of the world's most popular Internet shopping sites including Amazon, Expedia and Walmart. A targeted DDoS attack against UltraDNS,[3] a leading provider of domain name system (DNS) services, took these major retail sites offline. The attack could have dramatically affected the Christmas shopping season and the profitability of these retailers if UltraDNS had not been able to detect and stop the attack very quickly.

This attack revealed the potential impact of DDoS on e-commerce. More importantly, it revealed 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.



2002–2003
Typical attack is "host-to-host." Goal is to exhaust CPU on the the server (usually a Web server).

2004–2008
Botnets enable "volumetric" attacks against infrastructure (routers, DNS, name servers). In-cloud DDoS protection becomes essential.

2009 and Beyond
Sophisticated "application-layer" attacks target IDC services and enterprises. A layered defense is required.

Evolution of network and DDoS attacks

Attackers find Internet data centers attractive for the following reasons:

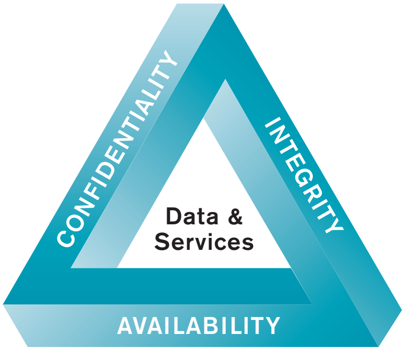
- The shared resources and multitenant nature of IDCs allow attackers to cause much collateral damage. In other words, they get "more bang for the buck!"
- Many times IDCs are running high-profile, mission-critical applications. This makes them ripe targets for extortion. By targeting such data centers, attackers are simply following the old saying "go where the money is."
- Virtualization is a big part of data centers. This not only brings benefits but also opens up a whole new set of security challenges. For example, how do you get visibility into the virtual environment to protect it from inter-VM (virtual machine) attacks?

The convergence of volumetric and application-layer DDoS attacks poses a significant threat to online services, and data center operators must be prepared to combat them both.

[3] www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html

Why IPS Devices and Firewalls Can't Stop DDoS Attacks

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, inline solutions, which means they are vulnerable to DDoS attacks and often become the targets themselves.



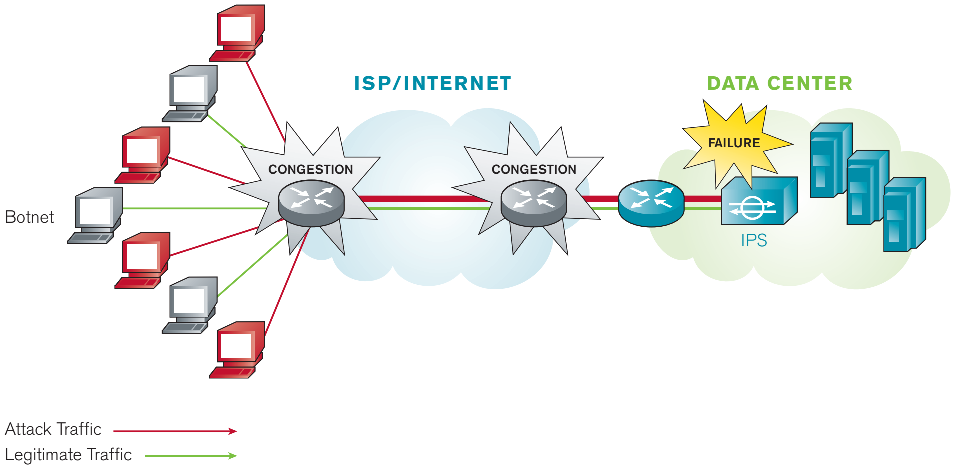
Key elements of an information security strategy

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.

IPS Devices: Part of the DDoS Problem, Not the Solution

IPS devices are normally deployed inline behind firewalls and must inspect every packet for signature matches. As stateful devices, they must also track all connections. These two requirements make IPS devices vulnerable to DDoS attacks and increased network latency.

Let's examine the full impact of this vulnerability in more detail. IPS devices are deployed inline because they are designed to prevent malware from spreading through a network. But this inline deployment adds to the "attack surface" since the connection tables can be overwhelmed—thus negatively impacting performance.



IPS devices are not designed to stop DDoS attacks

IPS devices are especially susceptible to well-known vulnerabilities including:

- **Flooding:** IPS devices depend on resources such as memory and processor power to effectively capture packets, analyze traffic and report malicious attacks. By flooding a network with noise traffic, an attacker can cause the IPS device to exhaust its resources.

- **Fragmentation:** Hackers can divide attack packets into smaller and smaller portions that evade the IPS device.

Because IPS devices depend on signature-based detection of known threats, they usually miss a new threat because the signature has yet to be developed. They are always playing catch-up to emerging threats.

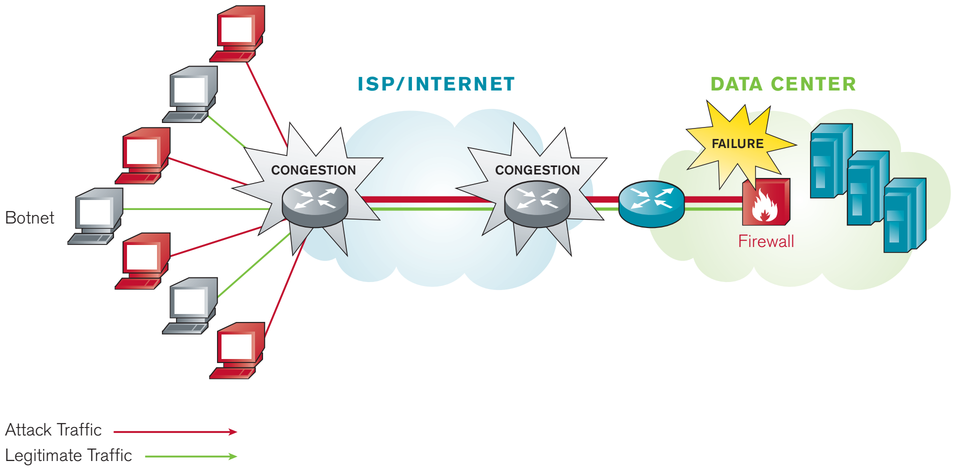
Network-based IPS devices also use protocol anomaly-based detection, which is not effective in detecting and stopping DDoS attacks. That is because this method of detection does not allow IPS devices to analyze traffic simultaneously across multiple links. As a result, it prevents them from detecting and stopping a true "distributed" DoS attack.

Lastly, because IPS devices are usually deployed inline, they can introduce unacceptable latency in high-capacity networks. The complex algorithms in IPS devices can significantly add to this latency; in addition, the devices can be overwhelmed during packet floods while performing this complicated analysis. Such latency is unacceptable in the high-bandwidth networks of hosting providers and large online enterprises. As a result, IPS devices are simply not effective on very high traffic links.

Firewalls: Ripe Targets for DDoS Attacks

Like IPS devices, firewalls are designed to solve an important security problem—in this case, policy enforcement to prevent unauthorized data access. To do this job effectively, modern firewalls perform stateful packet inspection—maintaining records of all connections passing through the firewall. They determine whether a packet is the start of a new connection, part of an existing connection or invalid.

But as stateful and inline devices, firewalls add to the attack surface and can be DDoS targets. They have no inherent capability to detect or stop DDoS attacks because attack vectors use open ports and protocols. As a result, firewalls are prone to become the first victims of DDoS as their capacity to track connections is exhausted. Because they are inline, they can also add network latency. And because they are stateful, they are susceptible to resource-exhausting attacks such as Transmission Control Protocol synchronous (TCP SYN) floods and spoofed Internet Control Message Protocol (ICMP) ping floods. Major data center operators do not deploy firewalls in front of services because of this, and there is just no reason to deploy them in front of servers.



Firewalls can actually be the targets of DDoS attacks

The Obvious Need for Intelligent DDoS Mitigation Systems (IDMS)

The ideal solution is an IDMS that can stop both volumetric and application-layer DDoS attacks. It must also be deployable in the ISP network (in cloud) and at the enterprise or data-center edge.

Key Features of an IDMS

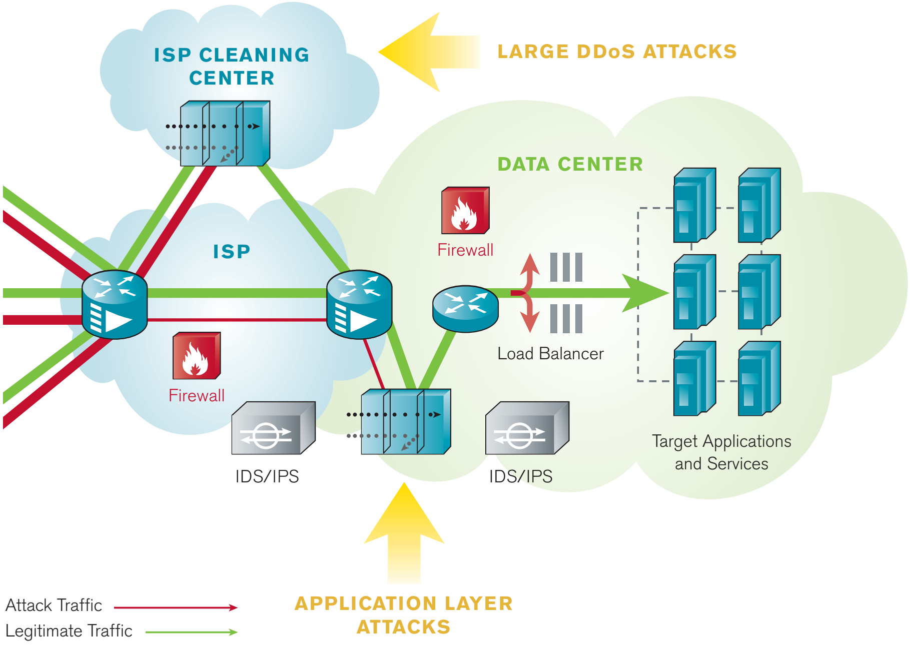
The limitations in IPS devices and firewalls reveal the key attributes required in an IDMS solution. An IDMS must be "stateless," in other words, it must not track state for all connections. As mentioned earlier, a stateful device is vulnerable to DDoS and will only add to the problem. The IDMS solution must also support various deployment configurations; most importantly, it must allow for out-of-band deployments when needed. This deployment flexibility can increase the scalability of the solution, which is a requirement as the size of DDoS attacks continues to increase.

To truly address "distributed" DoS attacks, an IDMS must be a fully integrated solution that supports a distributed detection method. IPS devices leveraging single segment-based detection will miss major attacks. Moreover, an IDMS solution must not depend on signatures created after the attack has been unleashed on the targets; rather, it must support multiple attack countermeasures. Finally, the IDMS must provide comprehensive reporting and be backed by a company that is a known industry expert in Internet-based DDoS threats. The key features of IDMS are:

- Stateless
- Inline and Out-of-Band Deployment Options
- Scalable DDoS Mitigation
- Ability to Stop "Distributed" DoS Attacks
- Multiple Attack Countermeasures
- Comprehensive Reporting
- Industry Track Record and Enterprise

IDMS Enables a Layered Defense Strategy

IDMS provides a layered network- and edge-based solution to combat both volumetric and application-layer DDoS attacks. The best place to stop volumetric DDoS attacks is in the ISP cloud (via network-based DDoS protection) because the saturation happens upstream and can only be remediated in the provider's cloud. The best place to perform application-layer DDoS detection is in the data center or the enterprise edge because the attack can only be detected and quickly stopped at the data center edge.



Multiple layers of defense required for comprehensive DDoS protection

IDC operators and enterprises should get DDoS protection from upstream providers as well as deploy DDoS protection on premises at the IDC and enterprise edge. This ideal architecture will stop both large "volumetric" and "targeted application-layer" DDoS attacks. IDMS fits perfectly in this ideal architecture.

Conclusion

IPS devices and firewalls are effective tools in addressing network integrity and confidentiality. But when it comes to DDoS protection, they provide a false sense of security. That is because they fail to address the fundamental concern regarding DDoS attacks—network availability. What is more, as stateful, inline tools, IPS devices and firewalls are vulnerable to DDoS attacks, often becoming the targets themselves. By relying on Peakflow SP and TMS, enterprises and IDC operators can deploy an IDMS that provides a layered net- work- and edge-based solution for combating both volumetric and application-layer DDoS attacks.

***For more white papers visit Arbor Networks Web site at www.arbornetworks.com.
For commentary and reports on the latest in Network Security, visit Arbor's security blog at asert.arbornetworks.com***

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

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for next-generation data centers and carrier networks. Arbor's proven solutions help grow and protect our customers' networks, businesses and brands. Arbor's unparalleled, privileged relationships with worldwide service providers and global network operators provides unequalled insight into and perspective on Internet security and traffic trends via ATLAS—a unique collaborative effort with 100+ network operators across the globe sharing real-time security, traffic and routing information that informs numerous business decisions.

For technical insight into the latest security threats and Internet traffic trends, please visit our Web site at arbornetworks.com and our blog at asert.arbornetworks.com.