

Managed Anti-DDoS Service Protection

An Internap White Paper

February 2007



Distributed Denial of Service (or “DDoS”), in which compromised PCs controlled by remote attackers inundate a victim’s network resources with the intent of crashing the victim’s web or application servers, is among the most serious threats on the Internet today. DDoS attacks are growing larger and more destructive each day, presenting a serious threat to online organizations. The best way to deal with a DDoS attack is to utilize a comprehensive approach, which is outlined in this white paper.

250 Williams Street, Atlanta, GA 30303
Tel 404.302.9700 Toll Free 877.THE.PNAP
Fax 404.475.0520
Email: mktg_info@internap.com
www.internap.com



Table of Contents

Executive Summary3

Growing Risk4

DDoS Protection Alternatives5

 Carriers / IP Providers5

 Internap DDoS Protection5

Internap’s 5-Pronged Approach6

 Off-the-Shelf Intrusion Protection Devices6

 Custom Filtering Software6

 Bandwidth, Bandwidth, Bandwidth6

 DDoS Expertise7

Conclusion7

Appendix A8

 Internap Network Configuration8

 Customer Configuration Example9

Executive Summary

As the Internet becomes increasingly mission-critical, business executives need to be aware of a problem that can prevent customers, partners and suppliers from doing business with them online. It is called Denial of Service (or “DDoS”) in which compromised PCs controlled by remote attackers inundate a victim’s network resources with the intent of crashing the victim’s web or application servers – and is among the most serious threats on the Internet today. Twenty five percent of respondents to the 2006 CSI/FBI Computer Crime and Security Survey performed by the Computer Security Institute had experienced a DDoS attack. While no company wants to willingly publicize it, it has taken major companies offline including: *Amazon, Microsoft, Yahoo, CNN and eBay.*

The costs of these attacks are monumental. Forrester, IDS and the Yankee Group estimate that the cost of a 24-hour outage for a large e-commerce company would approach \$30 million. In addition, by violating service level agreements, these attacks trigger costly service credits. The estimated hourly down-time costs vary by industry, but are growing significantly across the board:

Retail Brokerage	\$6.45 million per hour
Credit Card Sales Authorization	\$2.6 million per hour
Infomercial/800 Number Sales	\$200,000 per hour
Catalogue Sales Center	\$90,000 per hour

Source: Cert, CSI

Further, not only do these attacks cost online organizations millions in lost revenues, they may damage reputations and customer relationships. These “soft” costs are more difficult to quantify, but could be extremely significant and include:

- Company Reputation
- Transaction / Operational Disruption
- Compliance / Regulatory Costs
- Legal Costs

Growing Risk

DDoS attacks are growing larger and more destructive each day, presenting a serious threat to online organizations. In 2006 there were 6,110 attacks per day vs. 927 in 2005. (Symantec Corp.) While the largest attacks in 2005 were 3.5 Gbps in size, they have grown by 3X during 2006 to over 10 Gbps. With these attack sizes at their disposal, assailants now have the capacity to take out entire hosting/co-location facilities with brute force. (Prolexic, Inc.)

Additionally, these easy-to-deploy attacks were originally motivated by extortion, but motivated attackers now include: disgruntled employees, industrial saboteurs, cyber-terrorists and religious zealots.

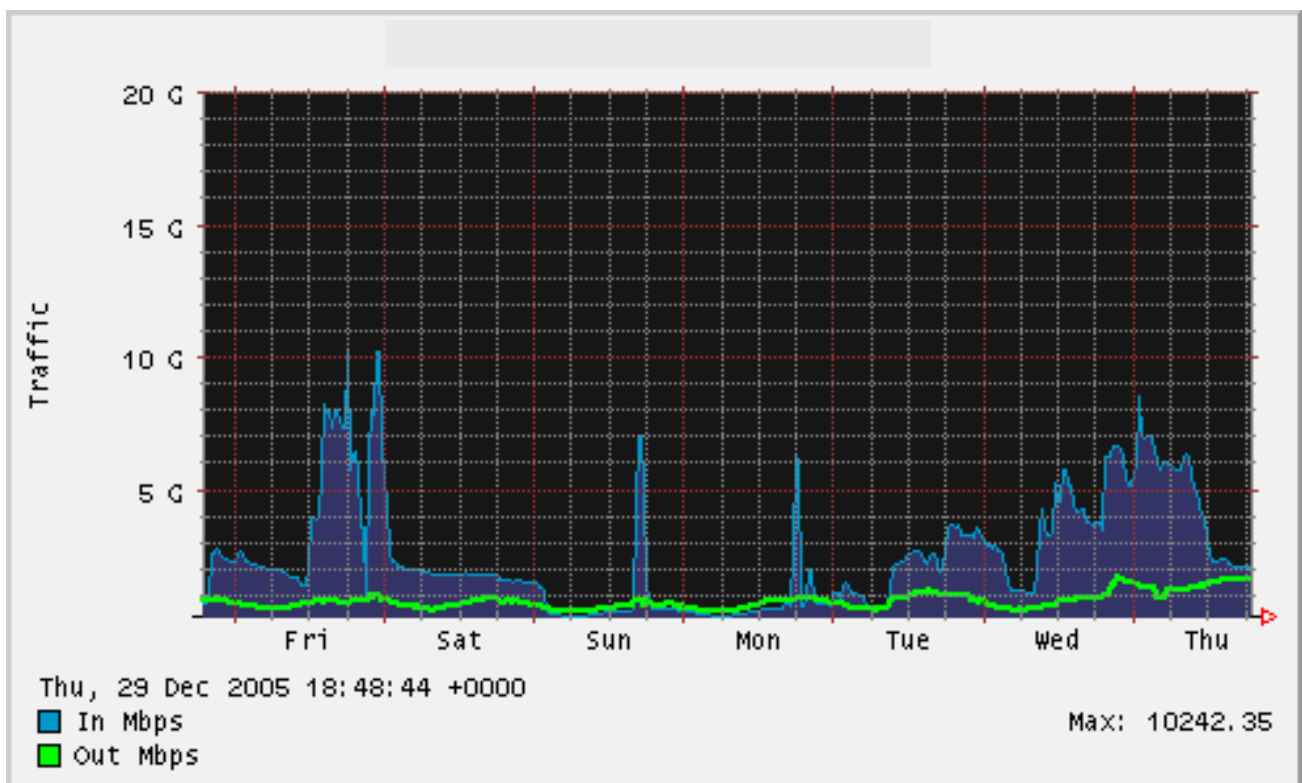


Figure 1: Recorded DDoS Attack against a sample Enterprise Client.

Protection Alternatives

Carriers / IP Providers

While large carriers have significant bandwidth to sell to their customers, no carrier dedicates bandwidth solely to stop DDoS attacks. This results in the inability to route customers under attack in favor of those not under attack, even if the attacks are only several Gbps in size. Even though carrier offers some level of DDoS mitigation for the bandwidth they provide, they do not take responsibility for another carrier's bandwidth. This lack of a multi-homed solution forces their customers to negotiate agreements with each carrier separately, receiving different levels and quality of coverage from each.

To help mitigate DDoS attacks, carriers typically acquire multiple devices from a single manufacturer, but these can only target certain attacks. As next-generation attacks pop up, they can't be stopped with these off-the-shelf manufacturer devices.

Additionally, because DDoS protection is not a carrier's main focus, understanding DDoS and protecting against it is not their main concern. Training of staff tends to be limited towards operating a specific manufacturer's mitigation device rather than on experience and training to recognize and stop the multitude of attacks themselves, as manual intervention is often required to stop certain types of attacks.

Internap DDoS Protection

Powered by Prolexic™

If Internap simply relied on a single DDoS device manufacturer for its solution, then stringing multiple boxes together would provide the least expensive and simplest approach. While this approach could be implemented as easily it does not provide adequate DDoS protection for Internap® customers. It would only be effective at stopping certain attacks, and not as effective as stopping others. Further, it wouldn't address bandwidth attacks where large botnets could overwhelm whatever mitigation gear was in place. Without the experienced DDoS experts behind the hardware and bandwidth, certain attacks could still be successful. Finally, if it provided superior protection for their customers but couldn't provide protection for all their bandwidth, even if acquired from another carrier, then it would only be providing a partial solution. Internap not only offers protection for the IP bandwidth that we provide, but we do the same for IP bandwidth from other providers as well.

Internap's 5-Pronged Approach

Because of the increasing types and size of DDoS attacks, the Internap solution has developed a 5-pronged approach designed to stop DDoS attacks that include:

- **Best-of-breed commercially available DDoS protection devices**
- **Custom filtering software** – More than 20 pending patents for filtering software designed to stop attacks types that off-the-shelf hardware can't stop as effectively
- **Bandwidth** – More than 25 Gbps dedicated exclusively to stopping DDoS attacks spread over multiple data centers, regions and carriers, and continuously increased to handle the largest attacks
- **DDoS expertise** – engineers who have seen and stopped more DDoS attacks than any other company.
- **Multi-homed protection** – protects the customer's bandwidth, not just bandwidth acquired from Internap.

Internap continuously tests the leading vendors for a best-of-breed approach, and have partnered with a combination of manufacturers including *Arbor*, *Juniper*, *Foundry*, and *TopLayer*, on top of its own custom filtering software. The Internap solution is continuously updated in hardware, software, bandwidth, and engineer training to accommodate the latest attacks and to maximize protection for all customers. So far, this solution has effectively combated the most varied and largest DDoS attacks and continues to be the market leader for this reason.

Off-the-Shelf Intrusion Protection Devices

Because each manufacturer has developed devices that are stronger at stopping certain attacks, one should not rely on any one manufacturer to stop the increasingly varied types of DDoS attacks. Stringing multiple devices from any one vendor might represent a cheaper and simpler approach, but it will not provide nearly the protection necessary to protect customers against the latest types of DDoS attacks.

Custom Filtering Software

Because even the best-of-breed, off-the-shelf hardware can't effectively stop every type of attack, we have developed custom filtering code on ASIC-based devices such as *Cloudshield* and *Bivio*.

Bandwidth, Bandwidth, Bandwidth

Beyond leveraging best-of-breed DDoS protection hardware and Internap custom filtering software, because the size of DDoS attacks have grown so significantly, we have more than 25 Gbps (and growing) of bandwidth dedicated to stopping the largest DDoS attacks. As no intrusion protection device has been developed to stop the tremendous size of the latest DDoS attacks, we have invested in over 25 Gbps of bandwidth dedicated to stopping largest brute force attacks. This is a critical component of the Internap solution, especially compared with many of the larger carriers who routinely null route those customers under attack if the attack gets beyond a few Gbps so as not to impact other customers who are not under attack.

DDoS Expertise

The Internap solution is at the forefront of the market. As a result, Internap leverages DDoS experts on staff 24x7x365 who have seen and stopped thousands of DDoS attacks. This provides a significant leverage over other service's engineers who have not had the same level of DDoS mitigation training or experience. Though a subtle point, it is important because DDoS attacks are usually operated by attackers in real-time (as opposed to canned programs), which can require manual intervention by engineers to stop certain attacks that hardware and software can't handle.

Multi-Homed Solution – offers protection for all of a company's bandwidth, not just bandwidth acquired from Internap. This means that companies can leverage the market leading solution across all of their bandwidth, ensuring consistency, economies of scale, and simplicity.

Conclusion

By taking down your websites, even for an hour, DDoS attacks will cause revenue loss, damage to your operations and customer frustration. According to the CSI/FBI study, DDoS attacks are one of the biggest problems on the Internet, and are growing significantly in both frequency and size.

While there are a variety of good commercially available devices available, each has its strengths and each manufacturer is better at mitigating certain attacks over others.

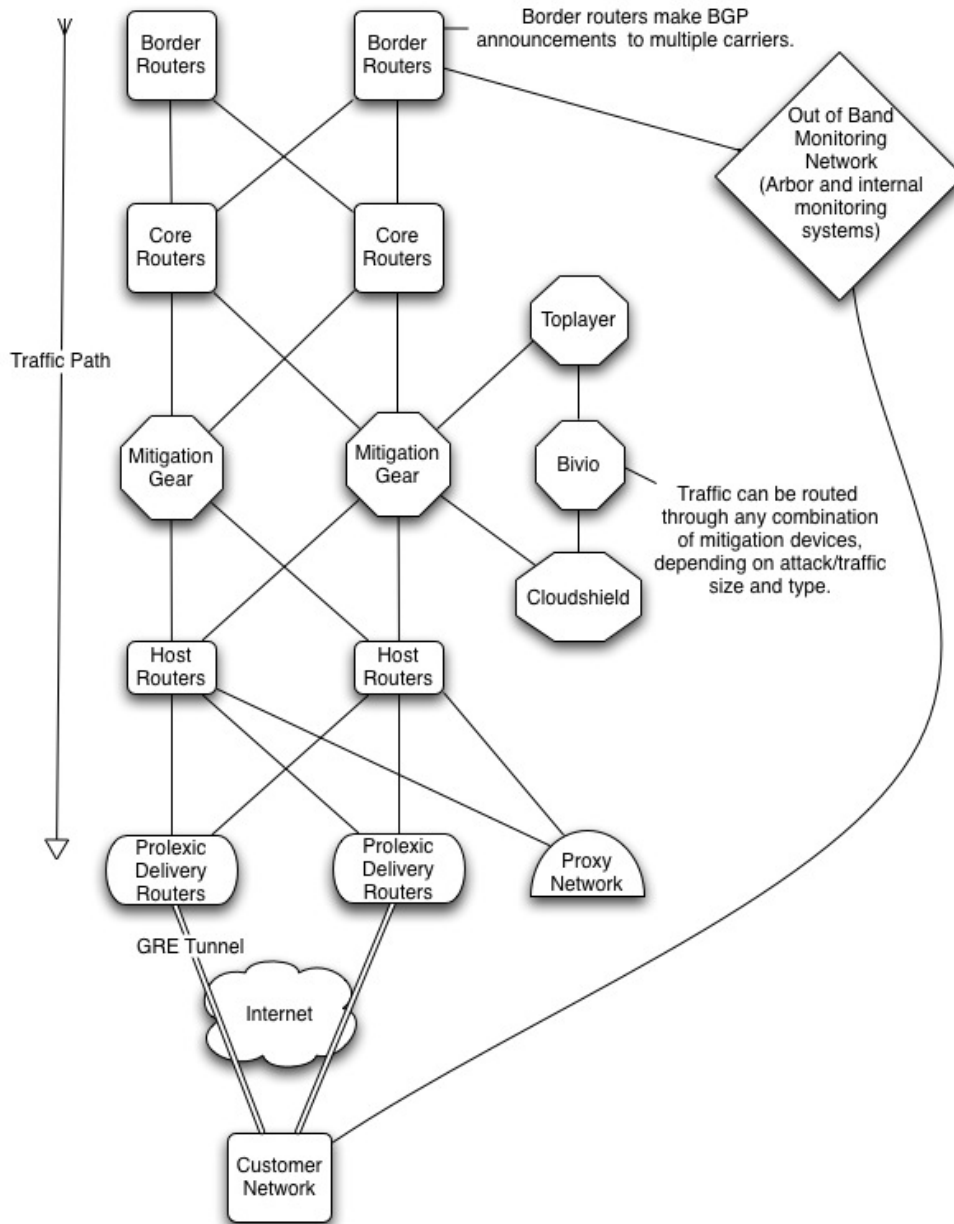
The result is that without a combination of best-of-breed manufactured devices, custom filtering software to fill the gaps, dedicated bandwidth to stop the largest attacks, and experienced DDoS experts to manually stop others, companies will only be partially protected at the exact time they need complete protection. By utilizing Internap's approach, companies can enjoy economical, yet more comprehensive protection from DDoS attacks.

Appendix A

Below are several diagrams related to the Internap solution designed for the purpose of understanding the network configuration, bandwidth allocation and an example of a typical customer configuration.

Internap Network Configuration

Powered by Prolexic™



Customer Configuration Example:

The following is a typical NAP configuration at the Miami NAP, this is mirrored from multiple locations, including Phoenix and London. In Q2 2007 the Hong Kong and New York locations will be coming on online providing additional capacity, redundancy and improved performance to support the growing needs of Internap's worldwide customers.

