Arbor White Paper

Keeping the Lights On

The Importance of DDoS Defense in Business Continuity Planning

ARBOR® NETWORKS

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for enterprise and service provider networks, including the vast majority of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the ATLAS® Active Threat Level Analysis System. Representing a unique collaborative effort with 250+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.

Table of Contents

Business Continuity Planning Priorities and Operational Security 2

Actionable Security Practices are Critical to Business Continuity Planning 3

DDoS Attacks: Background and Context 4

DDoS Attacks as an Element of Operational Risk 5

Traditional Security Solutions Do Not Mitigate the Operational Risk of DDoS Attacks 5

Arbor Solutions Help Mitigate the Operational Risk of DDoS Attacks 6

Conclusion 7

Business Continuity Planning Priorities and Operational Security

Today's enterprises are increasingly motivated to formalize IT security and place it firmly within the context of enterprise risk management and business continuity planning. Current financial realities require that companies incorporate IT security into their operational and financial planning to control escalating costs. At the same time, they must provide adequate resources to address their financially, regulatory and reputation-driven security priorities and incorporate all pertinent risk factors into their organizational security model.

The abstract nature of risk management and business continuity planning can often make these processes daunting to planners and IT security professionals alike. In most cases, business continuity plans include detailed policies and procedures for keeping operations running in the wake of natural disasters such as fire, floods and earthquakes. But rarely do they incorporate contingencies for IT security incidents. This is a major oversight. Security incidents often have a negative impact on business operations—resulting in significant operational expenditure (opex) costs, lost revenues, customer satisfaction challenges and an erosion in brand reputation. As a result, IT security issues constitute significant business risks, which place them squarely within the realm of business continuity planning and disaster recovery.

The most important aspect of enterprise security—availability—is the most easily understood and quantifiable aspect of security today. This means that organizations can readily establish the economic and reputational necessity of maintaining availability in the face of attack—and the costs of failing to do so.

When measuring the risk to the availability or resiliency of services, where does the risk of availability attacks fall on the list?

Availability Scorecard

- ✓ Site Selection
- ✓ Physical Security
- ✓ Fire Protection and Detection
- ✓ Electrical and Power
- ✓ Environment and Weather
- ✓ **DDoS Attacks?**

Figure 1: Availability Scorecard

Actionable Security Practices are Critical to Business Continuity Planning

Enterprise risk management is a critical component of business continuity planning. Several ISO standards (such as ISO 27005 and ISO 31000) are related to IT risk assessment—as are other, less formalized standards such as COSO[1] and OCTAVE.[2] While these various processes generate lots of paperwork, they unfortunately produce very little in the way of actionable security practices.

Although a top-down model is the usual methodology for risk assessment, you can begin with a bottom-up threat assessment to generate actionable security practices. By using those practices as inputs into the various IT risk assessment standards, you can derive useful enterprise risk management inputs for business continuity planning.

Availability protections are the most important IT security practices to implement—and also the most quantifiable. It is relatively easy to calculate the cost of downtime for e-commerce sites, customer support applications, content delivery systems, brick-and-mortar online reference sites, etc.

Much of this information may already be available from often siloed high-availability studies/efforts related to existing business continuity planning efforts.

The Impact of Loss of Service Availability Goes Beyond Financials

Operations	How many IT personnel will be tied up addressing the attack?
Help Desk	How many more help desk calls will be received, and at what cost per call?
Recovery	How much manual work will need to be done to re-enter transactions?
Lost Worker Output	How much employee output will be lost?
Penalties	How much will have to be paid in service level agreement (SLA) credits or other penalties?
Lost Business	How much will the ability to attract new customers be affected? What is the full value of those lost customers?
Brand and Reputation Damage	What is the cost to the company brand and reputation?

Figure 2: The Impact of Loss of Service Availability Goes Beyond Financials

[1] Model for assessing internal control systems developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission

[2] Operationally Critical Threat, Assess and Vulnerability Evaluation (OCTAVE) methodology

DDoS Attacks: Background and Context

Distributed denial-of-service (DDoS) attacks are attempts to consume finite resources, exploit weaknesses in software design or implementation, or exploit lack of infrastructure capacity.

DDoS attacks target the availability and utility of computing and network resources; if a DDoS attack against a Web server, DNS server, email server, application server or other online property is successful, the availability of the target of the attack is negatively impacted.

DDoS attacks are typically launched by botnets, which are collections of compromised computers utilized by attackers without the knowledge of their legitimate owners. Hundreds of millions of botted computers are on the Internet and enterprise networks today. They represent a major threat to organizations with an online presence due to the near-infinite computing power and bandwidth available to attackers who leverage botnets to launch DDoS attacks.

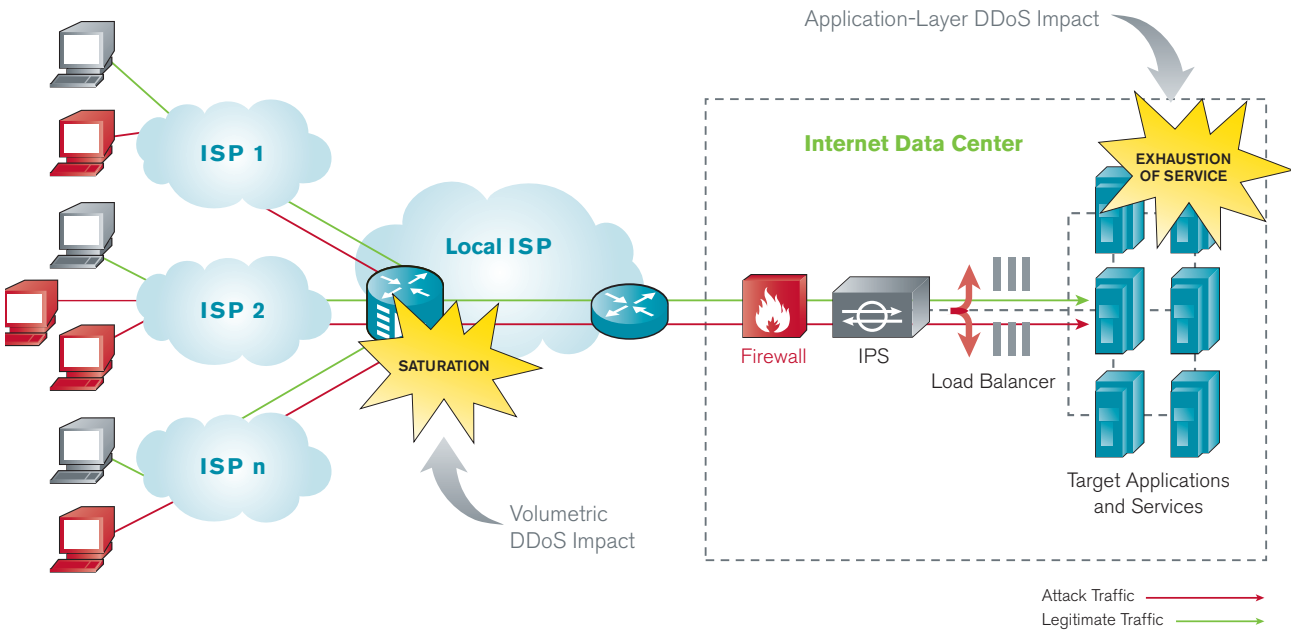

Figure 3: DDoS Attacks are a Multi-Vector, Diverse Threat

DDoS Attacks as an Element of Operational Risk

An operational risk is one that arises from the execution of an organization's normal functions. Internet presence—whether for e-commerce, customer support, content delivery, marketing, et al—is a normal function for all types of organizations. The Basel II Accords issued by the Basel Committee on Banking Supervision have become widely accepted throughout the financial industry and beyond as canonical references for defining operational risk.

The Basel II financial industry guidance for enterprise risk management defines operational risk to organizations as "The risk of loss from inadequate or failed internal processes, people, and systems, or from external events (page 94, www.bis.org/publ/bcbsca03.pdf)." Security threats, especially threats to availability, are external events that can have a negative impact in terms of financial, legal/regulatory, and/or brand reputation. As a result, organizations should incorporate security threats into enterprise risk management considerations, which form the basis for business continuity planning.

In essence, DDoS attacks are "external events" as defined in Basel II; they can be thought of as man-made disasters. The threat to availability represented by DDoS attacks cannot be overstated. No business continuity plan is complete without taking into account the need to maintain the availability of critical online properties, even in the face of a concerted attack.

Companies can successfully detect, classify, trace back and mitigate DDoS attacks with appropriate operational best practices and dedicated anti-DDoS solutions. Any enterprise risk management model and business continuity plan must account for DDoS attacks.

Traditional Security Solutions Do Not Mitigate the Operational Risk of DDoS Attacks

Contrary to popular belief, traditional security solutions such as firewalls and intrusion prevention systems (IPS) do not provide a DDoS mitigation capability. These devices are focused on maintaining confidentiality and integrity of organizational systems and, by their very nature, do not provide availability protection.

In fact, the stateful nature of these devices means that they often contribute to the impact of DDoS attacks because even relatively small attacks can readily overflow their state tables. Load-balancers and web application firewalls (WAFs) are also stateful devices, and suffer from the same vulnerability to state-table overflow as stateful firewalls and IPS.

If these devices are present on public-facing networks, they must be protected against DDoS attacks, along with the hosts, applications and data that they are intended to protect and scale.

Arbor Solutions Help Mitigate the Operational Risk of DDoS Attacks

Basel II defines four strategies for mitigating operational risk: *Avoid, Retain, Reduce* and *Transfer.* Avoidance simply isn't possible in today's globally-interconnected, online world. Most organizations must maintain an online presence solely for marketing and customer support purposes. Now that e-commerce systems and online supply-chains are critical assets for organizations of all sizes, the risk represented by DDoS attacks cannot be simply avoided.

Retaining the risk, or simply absorbing DDoS attacks and their negative impact on availability, is not a viable strategy due to the overwhelming resources controlled by determined attackers. In an era of 100 Gigibit/sec-plus DDoS attacks (see the recent *Worldwide Infrastructure Security Reports* from Arbor Networks), attackers can potentially overwhelm any organization. Therefore, more proactive measures are required.

Helping to reduce the operational risk of DDoS attacks is enabled by the on-premise DDoS attack detection, classification and mitigation solutions of Arbor Networks. Risk reduction is the single most important strategy for mitigating the operational risk represented by DDoS attacks. It should be a key part of business continuity planning for maintaining availability in the face of determined DDoS attacks.

Risk transfer is also a viable strategy for mitigating the operational risk of DDoS attacks. Arbor's cloud-based DDoS detection, classification and mitigation solutions help transfer risk from targeted organizations to managed security service providers (MSSPs) who specialize in DDoS attack mitigation within the MSSP network "cloud." Arbor's cloud-based solutions can also work in conjunction with its on-premise solutions.

Organizations can link together Arbor's on-premise and cloud-based DDoS defenses via Cloud Signaling™ functionality. This forms a comprehensive system that can respond quickly and precisely to sophisticated application-layer attacks, while simultaneously mitigating volumetric attacks that consume last-mile transit link bandwidth.

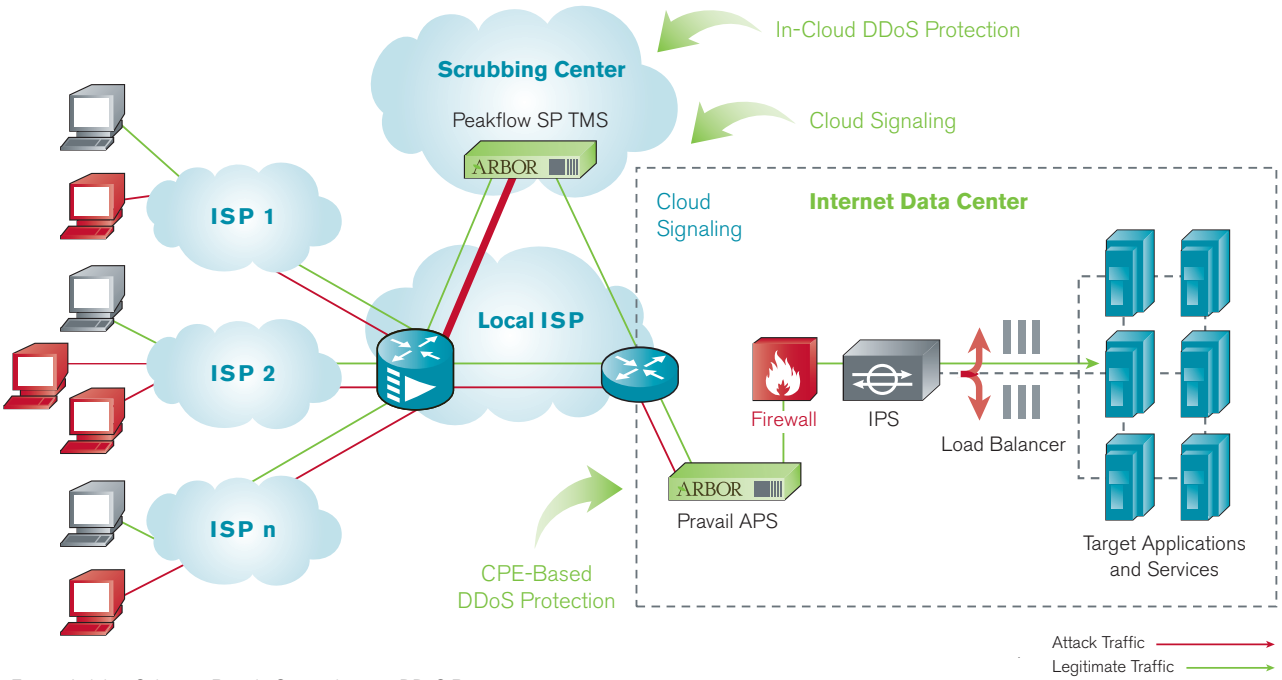

Figure 4: Arbor Solutions Provide Comprehensive DDoS Protection

Conclusion

No enterprise risk assessment and business continuity plan is complete without taking into account the operational risk represented by DDoS attacks intended to have a negative effect on the availability of key online services.

Premise- and cloud-based availability protection solutions from Arbor Networks enable organizations to successfully mitigate the operational risk represented by DDoS attacks. The design, deployment and operation of such solutions are key to ensuring that business continuity planning takes into account the "man-made disaster" of DDoS attacks, and helping to ensure that the availability of mission-critical public-facing properties is protected even in the face of determined DDoS attacks.

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

Europe
T +44 207 127 8147

Asia Pacific
T +65 6299 0695

www.arbornetworks.com

ARBOR® NETWORKS

WP/BUSCONT/EN/0213