radware

On-Premise, Cloud or Hybrid? Approaches to Mitigate DDoS Attacks

Whitepaper

SHARE THIS WHITEPAPER

Table of Contents

Overview

This paper is written for organizations that need to guarantee availability of online services and prioritize a dedicated solution for DDoS mitigation. It reviews the current DDoS attack landscape and explains why traditional network security solutions such as firewalls, Intrusion Prevention Systems (IPS) and Web Application Firewalls (WAF) cannot stop DDoS attacks. It then reviews and compares the three main approaches for deploying dedicated DDoS solutions.

Current Threat Landscape

In the past everything enterprises protected – data centers, applications, and databases resided in the perimeter. Organizations had to secure the perimeter to keep assets protected. Yet today, as organizations adopt cloud technologies to improve overall efficiency and expand business opportunities, they face a more distributed network infrastructure and are required to protect assets beyond the perimeter.

Organizations of all sizes are struggling to finance costs associated with cyber-attack prevention and mitigation. Attacks that cause network, server and application downtime and/or service degradation can lead to reduced revenues, higher expenses, and damaged reputations.

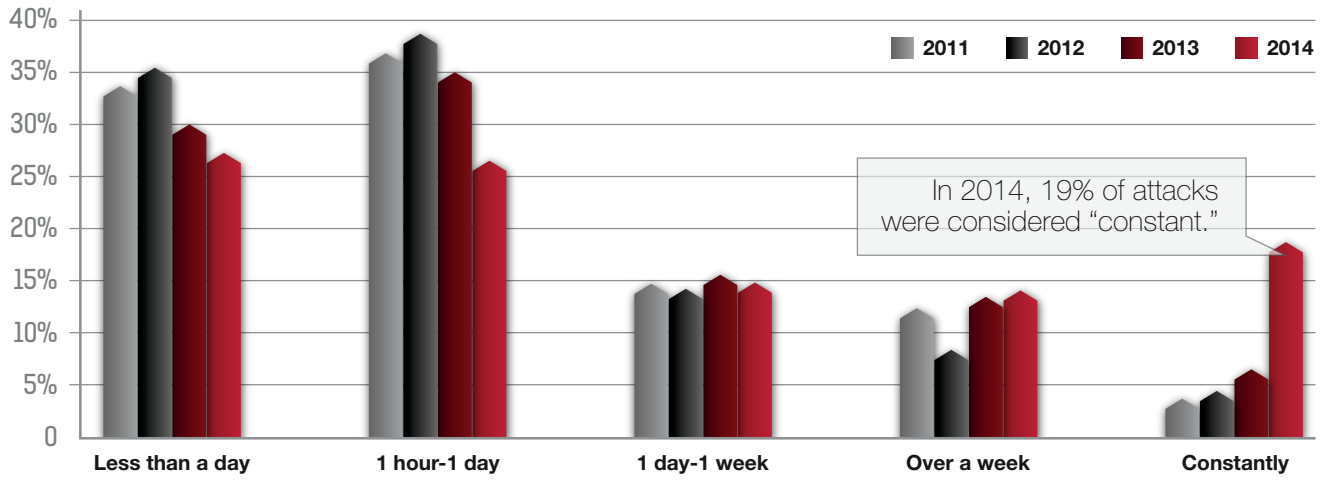
Cyber-attacks reached a tipping point in terms of quantity, length, complexity and targets. As they continue to expand to new targets, even organizations with by-the-book security programs can be caught off guard.

Attacks Are Longer, More Complex and Continuous

Attackers are deploying multi-vector (e.g., different types) attack campaigns that target all layers of the victim's IT infrastructure including the network, server and application layers. Attackers are more patient and persistent - leveraging "low & slow" attack techniques that misuse the application resource rather than resources in the network stacks. They also use more evasive techniques to avoid detection and mitigation including SSL-based attacks, changing the page request in a HTTP page flood attack and more.

Years ago, DoS attacks targeted the network through SYN, TCP, UDP and ICMP floods. From 2010-2012 there was an increase in more sophisticated application level attacks and SSL encryption-based attacks. Recently, a specific type of DoS attack—the amplification reflective flood—has not only revived network attacks but also given it an edge over counterparts that target applications. Reflective attacks, including those using DNS, NTP, and CHARGEN, started heating up in 2013 and remained a persistent threat throughout 2014. The rise in reflective attacks has contributed to crowning the Internet pipe as the major failure point in enterprise security.

The length of an attack indicates another new trend in DDoS attacks -constant attacks. In 2014, 19% of the major attacks were considered "constant" by the targeted organization. That's a stark contrast from the previous three years.



The simplicity of launching such cyber-attacks and variety of attack tools available are reasons why more organizations suffer from increased attacks such as DDoS. It is no longer a question of preventing attacks, but rather how to detect and mitigate attacks.

Traditional Network Security Solutions Cannot Mitigate DDoS Attacks

Recent DDoS attacks taught us that traditional network security solutions such as firewall, IPS and WAF cannot stop DDoS attacks. The organizations that became a target for DDoS attacks had firewalls and IPS devices in the infrastructure and yet availability of services was affected, ultimately causing the organization to go offline. Although firewall, IPS and WAF solutions have an essential role in providing security to organizations, they are simply not designed to handle today's emerging DDoS threats and can become bottlenecks themselves.

Traditional IPS devices are designed to prevent intrusions that result in a data breach through a full inspection of the session. Firewalls act as a policy enforcer and determine whether traffic should be allowed into the organization based on predetermined rules. While these are critical security tools, they cannot protect the availability of the online services for several reasons.

- **Reason #1: Firewall, WAF & IPS are stateful devices** - These devices track all connections inspected. All connections are stored in a connection table, and every packet is matched against that connection table to verify that it is being transmitted over an established legitimate connection. The connection table of a standard enterprise-class firewall, IPS or WAF can store thousands of active connections, and is sufficient for normal network activity.

  However, during a DDoS attack, an attacker will send thousands of packets per second to the target's network. In the absence of a dedicated anti-DoS device to shield the traditional network security devices from such a high volume of traffic, these devices are usually the first device in an organization's network to handle the force of the DDoS attack. Because of the way a firewall and IPS are designed, it opens a new connection in the connection table for each malicious packet, resulting in the exhaustion of the connection tables in a very short period of time. Once the connection tables have reached maximum capacity, it does not allow additional connections to be opened, ultimately blocking legitimate users from establishing connections, and subsequently preventing such users from accessing online services.

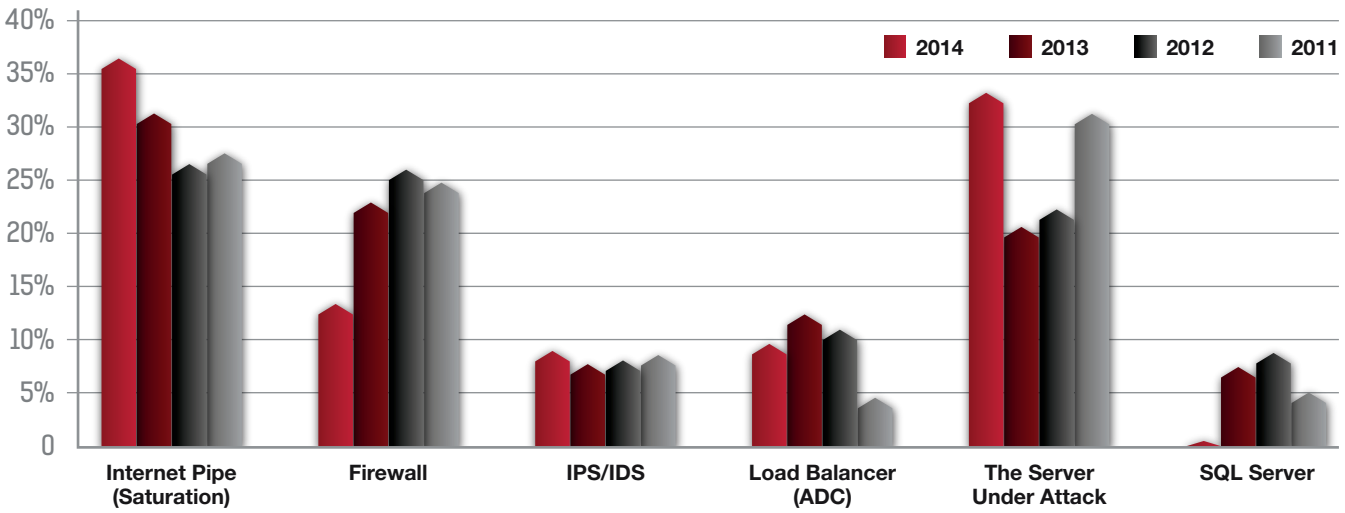
  Proper DDoS mitigation devices include a stateless DDoS protection mechanism that cannot be exploited by connection-based attacks. Such devices can handle millions of attempts to establish connections without consuming connection table entries or exhausting other system's resources.

- **Reason #2: Cannot distinguish between malicious and legitimate users** – Unlike intrusion attempts that firewalls and IPS are designed to detect and block, certain DDoS attack vectors such as HTTP floods, are composed of millions of legitimate sessions. Each session during a DDoS attack is legitimate and does not comply with any predefined IPS or firewall rule. Each session by itself is not a problem and cannot be detected as a threat by IPS and firewalls. However when there are millions of concurrent sessions as a DDoS attack emerges, the solution must look on all sessions and its behavior. IPS and firewalls are not designed to look on all sessions, but rather on a session-by-session basis.

- **Reason #3: Inappropriate network location** – Firewalls, IPS and WAF solutions are deployed too close to the protected servers and not deployed as the first line of defense where DDoS attacks should be mitigated. This results in DDoS attacks that go through the protected data center without being detected by traditional network security solutions. A dedicated DDoS mitigation solution should be deployed even before the access router at the ISP hand-off.

There are additional reasons why firewalls, IPS and WAF devices fail to protect from DDoS attacks including lack of DDoS expertise, limited security coverage of DDoS threats, and lack of a 24x7 emergency response team to fight DDoS attacks.

At the end of 2014, Radware's Emergency Response Team (ERT) released its annual security report which analyzed several DoS and DDoS attacks the team handled over the last year. The ERT checked which network devices were bottlenecks during these DDoS attacks, and found that the Internet pipe has increased as a point of failure. In fact, it has become the number-one failure point—most likely because of the increase in User Datagram Protocol (UDP) reflected amplification attacks.



Which services or network elements are (or have been) the bottleneck of DoS?

Choosing DDoS Mitigation Solutions

Enterprises and organizations that want to guarantee the availability of online services from DDoS attacks should consider a dedicated DDoS attack mitigation solution that is especially designed to deal with today's emerging availability based threats. There are three approaches to DDoS attack mitigation solutions: on-premise, cloud and hybrid.

On-premise

An on-premise DDoS attack mitigation solution is a dedicated, specially designed device to detect and mitigate DDoS attacks. The device is usually deployed as the first device in the organization's network, even before the access router. Such a device provides protection to the entire data center and especially to online services. On-premise DDoS devices should provide protection from many types of DDoS attacks including:

- UDP / ICMP network flood attacks
- SYN flood attacks
- SSL based attacks
- HTTP GET / POST application layer attacks
- Low & Slow attacks
- SSL-based encrypted attacks

Mitigation systems deployed on-premise in proximity to the protected online applications can be easily fine-tuned to have greater awareness to changes in network traffic flows in and out of the application servers, and therefore have a greater chance of detecting suspicious traffic on the application layer.

When a DDoS solution is deployed on-premise, organizations benefit from an immediate and automatic attack detection and mitigation solution. Within a few seconds from the attack initiation the online services are well protected and the attack is mitigated.

However, on-premise DDoS solution cannot handle volumetric network floods that saturate the Internet pipe of the enterprise. Such attacks must be mitigated from the cloud.

Cloud

With the rise of DDoS attacks, many Internet Service Providers (ISPs) and Managed Security Service Providers (MSSPs) have begun to offer anti-DDoS services. Such services protect organizations from network flood attacks by deploying mitigation equipment at the ISP or MSSP scrubbing centers. Often referred to as "clean pipe", this type of mitigation is guaranteed to block network flood attacks from ever reaching the organization, as attacks are mitigated before they reach the connection between the ISP or MSSP and the organization. This renders the organization's Internet pipe free of volumetric network flood attack.

However, cloud based anti-DDoS services cannot block application DDoS attacks as well as low & slow attacks since its mitigation equipment is not sensitive enough to detect the intricacies of such attacks when it's deployed in the cloud. In addition, to detect SSL based attacks the MSSP must host the SSL keys of the protected enterprise. This results in compliance and regulatory concerns for the protected enterprises, which cannot provide its SSL keys to the MSSP and therefore SSL based attacks are travelling into the enterprise data center without any mitigation.

During an attack, cloud based mitigation requires diversion of the traffic from the protected enterprise into the MSSP scrubbing center. This diversion process requires human intervention and takes at least 15 minutes in which the enterprise online services are not protected and are exposed to the attackers.

Relying solely on a 'one-size-fits-all' in-the-cloud managed security or on-premise security solution will not work against current coordinated attack campaigns.

Hybrid

Hybrid DDoS solution aspires to offer best-of-breed attack mitigation solution by combining on-premise and cloud mitigation into a single, integrated solution. The hybrid solution chooses the right mitigation location and the mitigation technique based on the attack characteristics tools and volume. In the hybrid solution, attack detection and mitigation starts immediately and automatically using the on-premise attack mitigation device that stops various attacks from diminishing the availability of the online services. All attacks are mitigated on-premise, unless they threaten to block the Internet pipe of the organization. In case of a pipe saturation threat, the hybrid solution activates the cloud mitigation and the traffic is diverted to the cloud, where it is scrubbed before sent back to the enterprise. An ideal hybrid solution also shares essential information about the attack between on-premise mitigation devices and cloud devices in order to accelerate and enhance the mitigation of the attack once it reaches the cloud.

A hybrid solution allows enterprises to benefit from:

- Widest security coverage that can only be achieved by combining on-premise and cloud coverage.
- Shortest response time by employing an on-premise solution that starts immediately and automatically to mitigate the attack.
- Single contact point during an attack both for on-premise and cloud mitigation.

The table below summarizes the aforementioned alternatives for DDoS solutions:

Capability		On-Premise	Cloud	Hybrid
Attack Coverage	UDP / ICMP network floods	V	V	V
	Floods that saturate the Internet pipe	X	V	V
	SSL based attacks	V	X	V
	HTTP application GET / POST attacks	V	X	V
	Low & slow attacks	V	X	V
Mitigation	Mitigation response time	Immediate	Slow – at least 15 minutes	Immediate
	Start automatically	Yes	No	Yes
Traffic Diversion	Divert traffic with BGP announcement or DNS	No	For every attack	Only when threaten to saturate the Internet pipe

Summary

The simplicity of launching cyber-attacks and variety of attack tools available are reasons why more organizations are suffering from increased attacks, such as DDoS. It is no longer a question of preventing attacks, but rather how to detect and mitigate attacks. A security strategy that does not address detection of network DDoS attacks, application DDoS attacks, SSL-based attacks, low & slow DoS attacks, Web stealth attacks and more, leaves the organization and its users at risk.

Traditional network security solutions such as firewalls, IPS and WAF are not sufficient to handle the emerging DDoS threats and become bottlenecks during many of the attacks. Enterprises that aspire to guarantee availability of online services are urged to prioritize specially designed DDoS attack mitigation solutions. Based on the description of the various solutions, each organization should decide whether on-premise, cloud or hybrid is the most suitable solution to its needs and move forward to deploy one.

If you're interested in learning more about how to deploy one of these methods, read about Radware's hybrid attack mitigation solution that offers integrated on-premise detection and mitigation with cloud-based volumetric attack scrubbing.