Infoblox
CONTROL YOUR NETWORK

WHITEPAPER

Defeating DoS/DDoS Attacks in Real Time

Abstract

The vulnerability of DNS servers to DoS/DDoS attacks at communications service providers is real and growing at an astounding rate, placing their customers' experience and ultimately their brand at risk. Current approaches seek to stop the attacks by adding hardware at the provider site or seeking to unmask the culprit hiding in the malware at the customer site, both of which are costly and only partially successful solutions. The new approach is to build protection against DoS/DDoS attacks directly into a high integrity DNS caching server and thwart the attack in real time as it enters the infrastructure, disabling it before it can cause any disruption to performance or service.

DNS — A Key Vulnerability for Service Providers

The DNS server is one of the primary and most vulnerable infrastructure components through which communications service providers suffer Denial of Service and Distributed Denial of Service (DoS/DDoS) attacks. ISPs, Telcos, and mobile providers are at constant risk of service interruptions due to failure of DNS servers that become overwhelmed by malicious queries and their assorted malware-generated cousins. The current threat landscape is continuing to grow rapidly as these attacks impact budgets, reputations, consumers and clients.

The cost of an attack can be counted in millions of dollars — with nefarious tactics ranging from criminal threats that force extortion payments to attacks that cause outright loss of Internet connectivity, services and web-based revenue. Effective attacks can also result in additional non-monetary losses in customer loyalty and satisfaction that, in the case of extended, high profile outages, may lead to significant brand damage.

Most ISPs focus on customer retention and growth by upgrading their infrastructure to meet the growing demand for bandwidth, driven in large part by smartphones, social media applications, and the proliferation of personal mobile devices. However, they take their eyes off a far greater threat to customer satisfaction: connectivity. Bandwidth-centric upgrades are necessary, but they are only part of the service provider's edge over competitors. Today's sophisticated consumers and businesses simply will not tolerate service disruptions. ISPs must secure their Internet infrastructure against increasingly aggressive and frequent DoS/DDoS attacks in order to maintain uninterrupted connectivity and preserve their customers' Internet experience, thereby guarding their own reputation.

DoS/DDoS Attacks — A Short History with a Long Impact

DoS/DDoS attacks have not been around with any significance for very long over the history of IT. But in little more than a decade, they have become a worldwide threat that shows no sign of abating, or even diminishing, any time soon. In fact, the problem of DoS/DDoS attacks is increasing rather than declining, both in incidence and in virility. A historic report by Arbor Networks in 2008 presciently anticipated today's explosion of DoS/DDoS attacks, finding in that year that DDoS size (in gigabits) nearly doubled over 2007. It was a trend that Arbor Networks reported had been on an alarming rise since the start of the century, as shown in Figure 1.

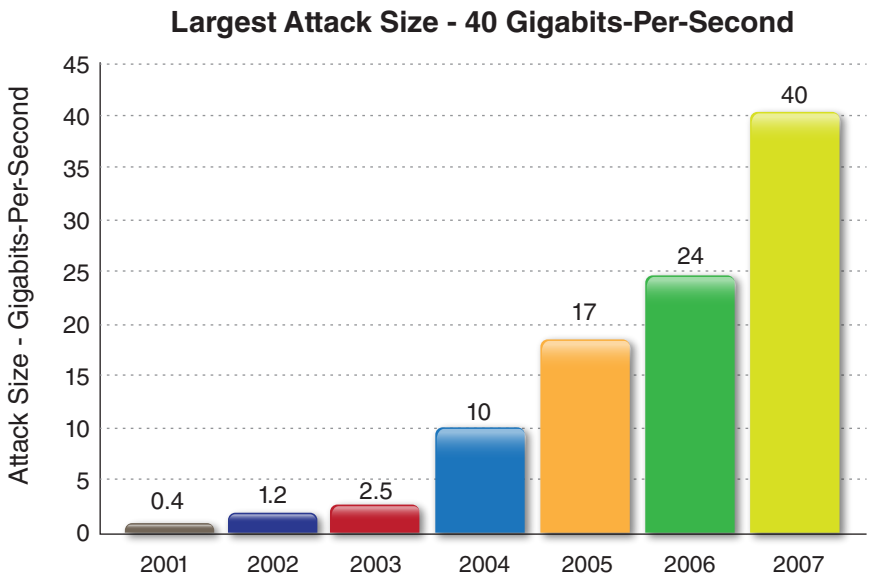

Figure 1. DDoS attacks have steadily increased at an amazing pace since 2001, and showed no signs of abating by 2008. *(Credit: Arbor Networks)*

That earlier predictive trend has more than reached its dire expectations according to current studies. In July, 2012, Prolexic Technologies' "Quarterly Global DDoS Attack Report" found that in just three months since the first quarter of 2012 there had been a 10% increase in the total number of DDoS attacks, that an 8% rise in Layer 3 and 4 infrastructure attacks had occurred, and that the average attack duration was now about 17 hours, with China as the main source country for DDoS attacks. Compared to the second quarter of 2011, the report found a 50% increase in the total number of DDoS attacks over just a single year, and a 63% higher packet-per-second (pps) volume over the same time period.

Also in July, 2012, the biannual "DDoS Prevention Appliances" report from market research firm Infonetics Research forecast the DDoS prevention market to grow 24% in 2012 over 2011. Combined, all segments of the DDoS prevention market — data center, carrier transport, mobile and government — are forecast by Infonetics to top $420 million by 2016, with mobile networks seeing the strongest growth of 30% in that period.

Clearly, the problem is not going away, but rather getting worse.

Slow Response to Common Attacks

Many service providers do not know they are under a DoS/DDoS attack when it begins. The invidious, cumulative nature of DoS/DDoS attacks makes their detection difficult until the assault is well underway and some level of damage has been done. Suspicion that an attack may be in progress usually arises after performance levels slip noticeably or customer complaints begin to mount. Only after asking engineers to look back at DNS server logs — sometimes days' worth of data — will the attack be confirmed. The delay in gaining that knowledge often extends as long as 4 to 6 days prior to any remedial action being initiated, by which time disruption to service is usually widespread.

Most service providers are running their DNS on Hewlett-Packard or Sun hardware, and are using mostly open-source BIND DNS software. Almost all use multiple DNS servers, and some may employ high numbers of DNS servers in their data centers. These configurations are particularly susceptible to three of the most common types of DoS/DDoS attacks:

- TCP SYN Flood Attacks
- UDP Flood Attacks
- Spoofed Source Address/LAND Attacks

There are many other ways a DNS server may be compromised, and newer, more complex methods are being devised all the time in the underworld of botnets, but these three happen with the most frequency and have characteristics common to many others.

TCP SYN Flood Attacks — Hello, No Answer

TCP SYN floods are DoS attacks that attempt to flood the DNS server with new TCP connection requests. Normally, a client initiates a TCP connection through a three-way handshake of messages:

- The client requests a connection by sending a SYN (synchronize) message to the server.
- The server acknowledges the request by sending SYN-ACK back to the client.
- The client answers with a responding ACK, establishing the connection.

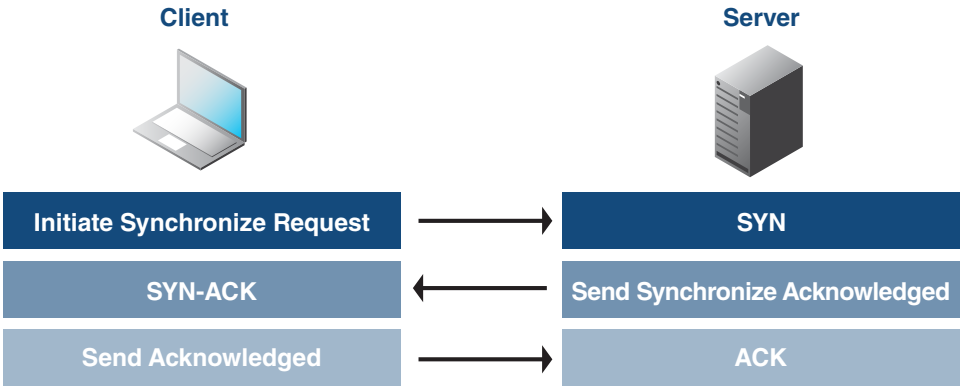

Figure 2: Normal TCP Connection

This triple exchange is the foundation for every connection established using the Transmission Control Protocol (TCP).

A TCP SYN flood attack works by sending SYN requests to the server and then deliberately not responding to the server with the expected ACK code. The malicious client can either simply not send the expected final ACK, or can spoof the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address — which, of course, will not send back an ACK because it "knows" that it never sent a SYN. The result is multiple, unopened, "hanging" connections awaiting client acknowledgements in the server. While the server correctly waits for the ACKs (to allow for network congestion or delay), increasingly large numbers of half-open connections continually consume resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic and ultimately causing the server to crash.

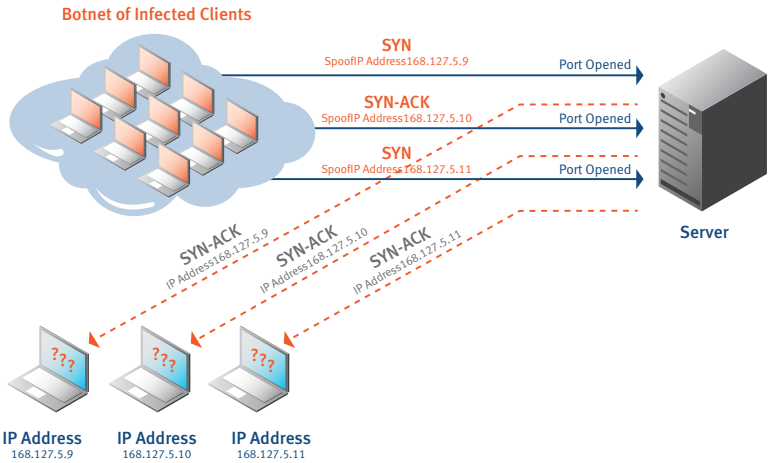

Figure 3: TCP SYN Flood Attack

UDP Flood Attack — Any Port in a Packet Storm

A UDP (User Diagram Protocol) flood attack can be initiated by sending a large number of UDP packets to random ports on the target host. The host under attack will check for traffic from the application listening at that port. Then, when it sees that no application listens at that port, it will reply with an ICMP Destination Unreachable packet.

As a result, when a large number of UDP packets are sent, the system under attack will send many ICMP packets back out, eventually causing it to become unreachable by other clients. The attacker may also spoof the IP address of the UDP packets, thereby ensuring that the excessive ICMP return packets do not reach him, and rendering his outlaw network location anonymous.

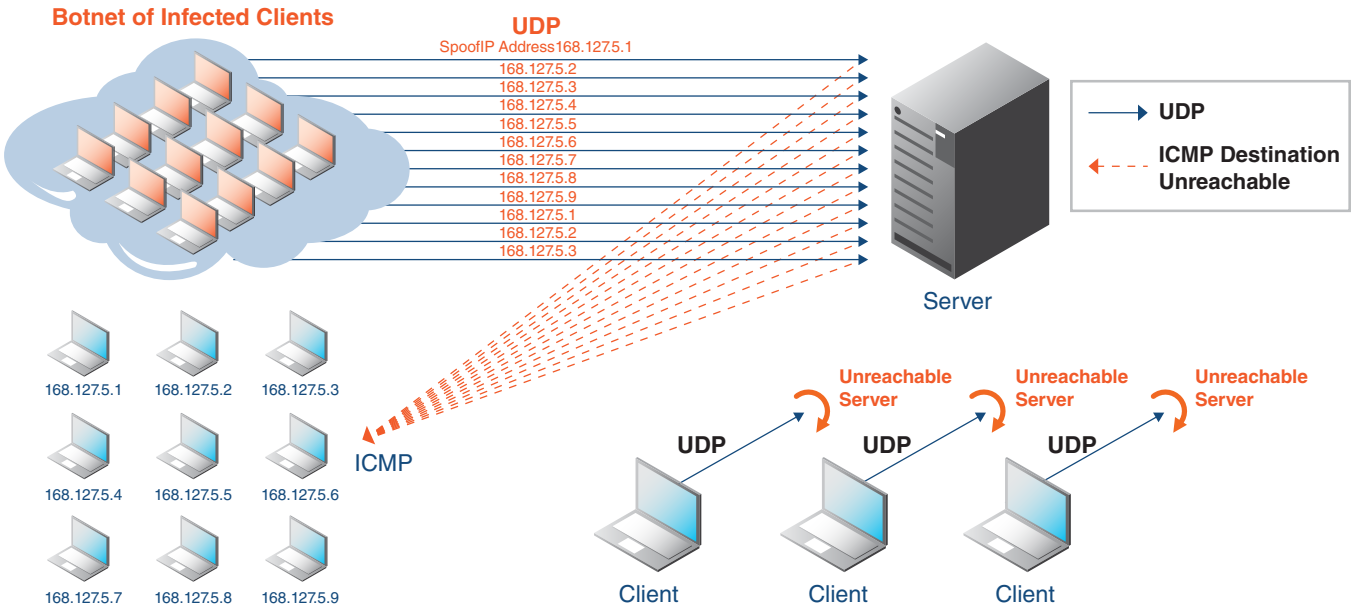

Figure 4: UDP Flood Attack

Spoofed Source Address/LAND Attacks — Self-Inflicted Wounds

A Local Area Network Denial (LAND) attack is a common form of DoS attack where a special poisoned spoofed packet is sent to a computer, causing it to lock up. The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address to an open port as both source and destination. A LAND attack works by causing the victim computer to reply to itself continuously.

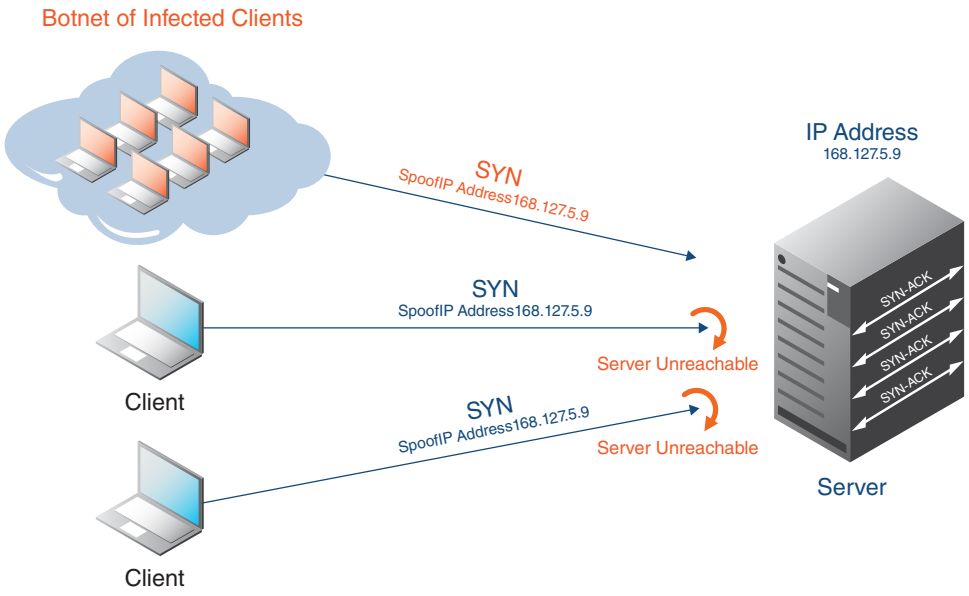

Figure 5: LAND Attack

Limitations of Current Approaches

To date, protection against all such attacks and other types of DoS/DDoS attacks has focused on two distinct approaches: thwart the attacks at the provider level or stop them at the customer level. Both approaches have failed to achieve uniform success on a consistent basis, and both are quite costly.

At the provider level, adding a load balancer to spread the load over multiple servers is an approach that's been in use for some time, but eventually the tactic reduces itself to a numbers game. Load balancers themselves can also become overwhelmed, at which time the vulnerability returns full force.

Also at the provider level, the use of clusters of smaller servers is another common practice, but one that is also not foolproof when the number of attacks exceeds the cluster capacity. Moreover, clusters of small servers crowd data center real estate, consume rack space, increase the costs of power and air conditioning, and multiply labor expenses due to service requirements for patches and upgrades on an ongoing basis. The end result from using clusters of traditional servers is merely a lessening of the provider's vulnerability rather than effective prevention — and at a bottom line cost that can be daunting.

By contrast, protection can be extended directly to customers by identifying infected users that have malware embedded in their equipment. Infected users are discovered when they show signs of communication with known malicious websites and DNS domains that house the botnet controllers that are wreaking the havoc. Once found, the provider's DNS server cuts off communication to that botnet controller. The process of discovering problem users, however, may employ offsite data parsing and reporting, which entails enormous security risks and is not legal in some countries. Customer satisfaction or privacy risks are also involved as individual customers must be closely — and some say invasively — monitored.

Additional major flaws in this approach are that the malicious websites and DNS domains must already be known (many are not because new ones are spawned daily), additional blacklisting feeds must be acquired on a frequent recurring basis, and every customer must be independently monitored. The technique is laborious, with the sources of attack discoverable only if offenders are known in advance, and effectiveness depends on the attack being in progress for some time before a problem is detectable.

Enter High Integrity Appliance-based DNS Caching Infrastructure

A new and dramatic shift in thinking about how to prevent DoS/DDoS attacks is the idea of building the antidote directly into a hardened, high integrity DNS appliance. Instead of trying to stop attacks when they reach the customer (which has proved very difficult), this method catches them as they enter the provider infrastructure — at the DNS server. Rather than adding more generic servers and load balancers (a mostly ineffective and costly effort), this solution installs high-integrity DNS infrastructure that is purpose-built for the task.

Such an approach requires a high-capacity DNS server that prevents most DoS/DDoS attacks outright simply by keeping up with them, employing raw horsepower to handle the increased load. An appliance approach may also use special algorithms to recognize common attack methods and harden the infrastructure against them. In order to maintain service under extreme load conditions, it is important that these DNS servers do not simply stop when they reach a saturation point. As the DNS query load increases beyond specified limits, this powerful DNS server should maintain constant, low DNS caching latency. This capability is typically dependent on a hardware implementation using advanced packet filtering and load shedding which typically cannot be implemented at high speed in software-based servers.

The Infoblox IB-4030 DNS Caching Appliance — Botnets Beware!

Infoblox has introduced just such a new DNS caching appliance that is designed specifically to meet the needs of large ISPs, Telcos and mobile providers. The IB-4030 DNS Caching Appliance serves one million DNS queries per second, more than enough to handle most DoS/DDoS attacks through processing power alone. The IB-4030 also includes built-in protection against all of the DoS/DDoS attack methods described above.

This approach enables ISPs and mobile operators to scale their DNS infrastructure to support billions of queries per second, providing high transactional scalability under extreme traffic loads, while also enabling high labor scalability by virtue of Infoblox GridTM technology. The Grid enables providers to deploy large scale, highly distributed but remotely manageable DNS infrastructure — without adding staff for administration and support.

Inherently secure, with no root access and a pre-built Infoblox software load, the Infoblox IB-4030 DNS Caching server is a purpose-built, carrier-grade appliance that includes redundant AC or DC power supplies, fans and hard disk drives. The on-board DoS/DDoS protection features are built-in and automated, so that no additional software installation or manual configuration of these functions is needed, thereby eliminating any possibility of manual configuration errors. The IB-4030 also includes automated support for DNSSEC as a standard feature to protect against Kaminsky-style attacks that poison the DNS cache to force redirection to unauthorized or malicious sites.

The IB-4030 includes role-based access controls, ensuring that only those functions for which the specific user and role has permissions can be accessed. Moreover, all changes to appliance settings by each user are time-stamped and stored in the appliance's audit logs.

Let Protection Replace Vulnerability in the DNS Infrastructure

The continued rise of DoS/DDoS attacks on service provider DNS infrastructure shows no sign of abating any time soon. Indeed, it is most likely to become an even greater scourge to the industry. As the creators of these attacks become ever more resourceful and devious, the means of combating their efforts must also evolve and add capabilities to outpace their designs. Because of the very nature of connectivity, DoS/DDoS attacks cannot simply be prevented because traffic is traffic until its malicious nature is detected. Rather, such behavior must be thwarted, overcome or defeated. High integrity DNS caching, like that offered by the Infoblox IB-4030 DNS Caching Appliance, is the latest and strongest weapon in the arsenal against botnet attacks.

Learn more about Infoblox solutions for Service Providers:

High Integrity DNS Caching Appliance with DoS/DDoS Protection
www.infoblox.com/en/solutions/service-provider/high-performance-dns-caching.html

High Integrity DNS for Service Providers Solution Note
www.infoblox.com/content/dam/infoblox/documents/solution-notes/infoblox-note-dns-for-service-providers.pdf

Infoblox-4030 DNS Caching Appliance Datasheet
www.infoblox.com/content/dam/infoblox/documents/datasheets/infoblox-datasheet-infoblox-4030.pdf

Service Provider Solutions for Wireline, Mobile and Cloud
www.infoblox.com/sp

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com