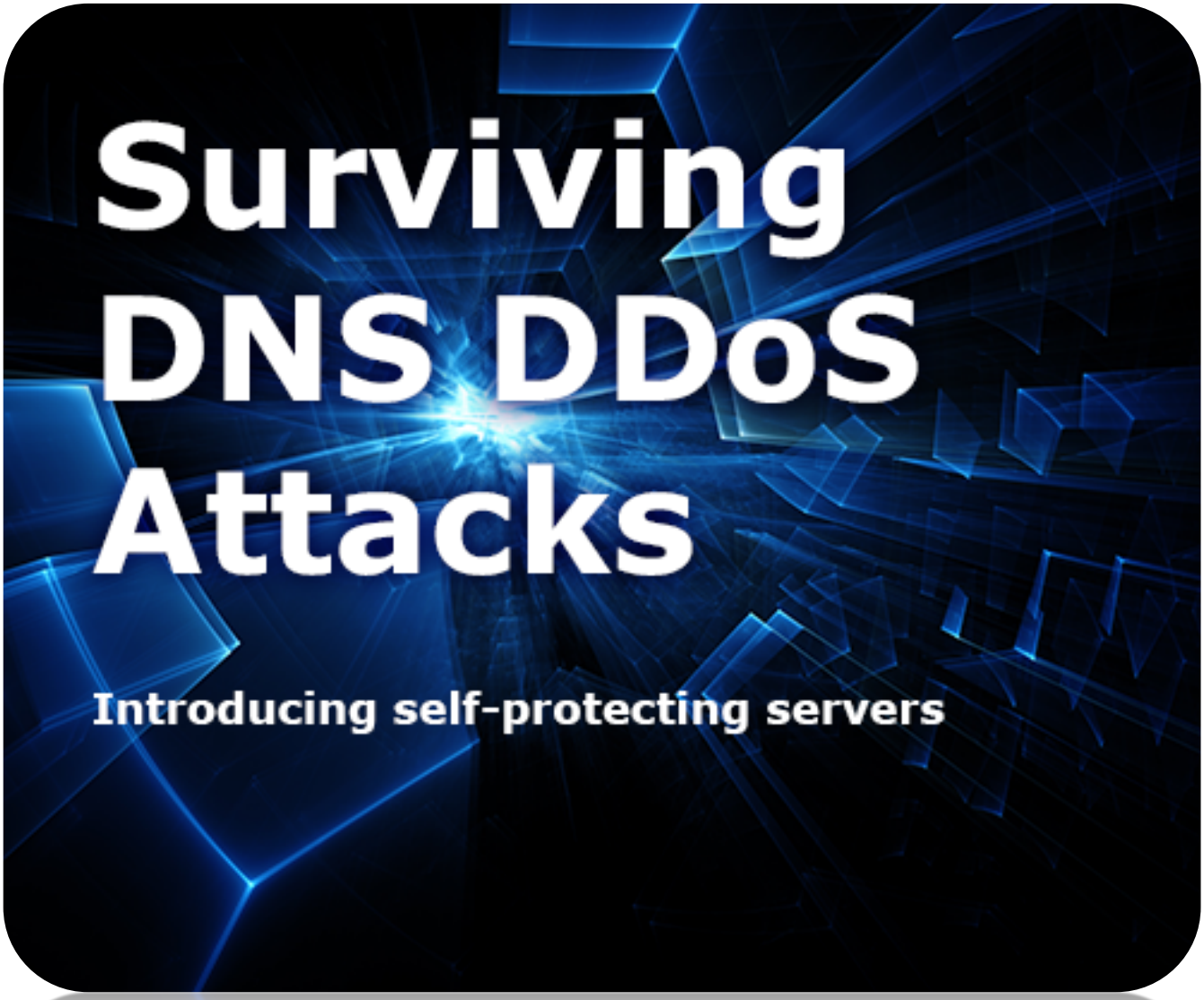
SECURE64™



Surviving Attacks

Background

2016 was the year when the Internet of Things (IoT) reached critical mass, and began being used as a force to drive massive denial of service attacks. Security researcher Bryan Krebs was the first victim of a full-scale DNS DDoS attack using IoT bots – the attack generated a record setting 620 Gbps. That record was broken a month later with the 1.2 Tbps attack on managed DNS provider Dyn. The DNS is the most frequently targeted application for DDoS attacks.

DNS-based DDoS attacks are increasingly popular with cybercriminals for two primary reasons. First, the DNS is mission-critical for virtually all IP-based communications. If an attacker can take an organization's DNS servers offline, he has effectively taken that organization completely off of the internet. Second, the DNS has proven to be an ideal weapon to attack others, as source IP addresses are easily spoofed over UDP and large responses can be easily utilized to attack the network bandwidth of intended victims.

The impact of today's DNS DDoS attacks are significant, including lost revenues, lost customers and damaged brand reputation. For organizations that need to ensure the availability of their online presence, deploying and operating a highly available, attack-resistant DNS infrastructure is mission-critical.

This white paper describes the most common types of DNS-based DDoS attacks, discusses conventional approaches to DDoS attack detection and mitigation, and introduces a new concept—a self-protecting DNS server - that incorporates DDoS countermeasures directly into the operating system, allowing it to remain responsive to legitimate DNS traffic while defending against high-volume DDoS attacks.

If you are currently experiencing a DDoS attack, please contact us immediately for assistance at **+1 (303) 242-5890.**

Types of DNS DDoS Attacks

Although there are many different types of DNS DDoS attacks, we will discuss the most common types of attacks in this white paper, which include:

- Direct floods
- Reflected floods
- DNS application attacks

Although these are the most common attacks against a DNS server, there are additional generic denial-of-service attacks such as ICMP and TCP SYN flood attacks that are also used. These attacks can be used against a DNS server, but due to their generic nature we are not describing the details in this whitepaper.

Direct Floods

This type of attack occurs when a large number of bots make more requests of the DNS server than it can handle. This causes the DNS server to drop inbound DNS requests (in the case of UDP), or refuse to establish new connections (in the case of TCP), thus achieving a denial-of-service condition for legitimate users. Although this type of attack has been rarer than other types of attacks on the DNS in the past, the availability of the IoT has enabled this type of attack to grow in usage and volume. Large botnets can also be created by using spoofed IP addresses; both non-spoofed and spoofed are shown in the illustration below.

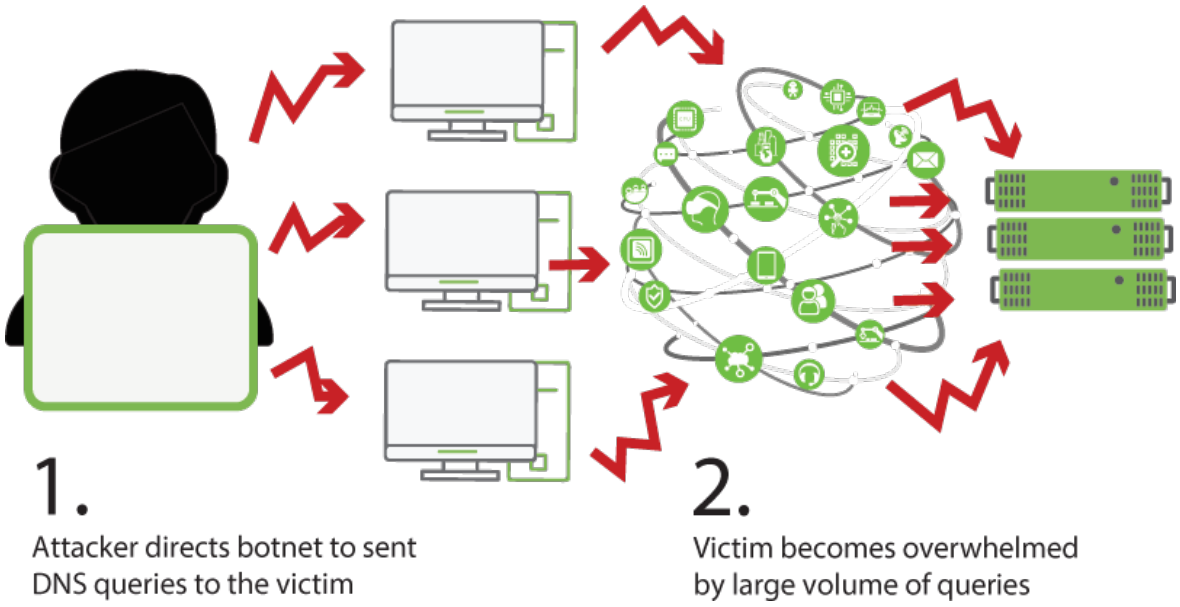


Figure 1 UDP Data Flood

Reflected Floods

Imagine an attacker with only one thousand bots under his control. It might be difficult to generate enough traffic in a direct flood attack to compromise the availability of the target victim. Reflected flood attacks provide the attacker with another option, however. Instead of sending queries directly to the victim server, specially crafted queries are sent to other DNS servers on the internet with a spoofed source IP address of the victim. The queries are crafted in such way that the response is much larger than the query. This results in a torrent of large DNS responses being sent to a victim, causing it to become unavailable, or its network connection to the Internet to fill. A reflected, amplified attack is illustrated in the figure below. It is amplified because the query from the attacker is small, whereas the response sent to the victim is much larger.

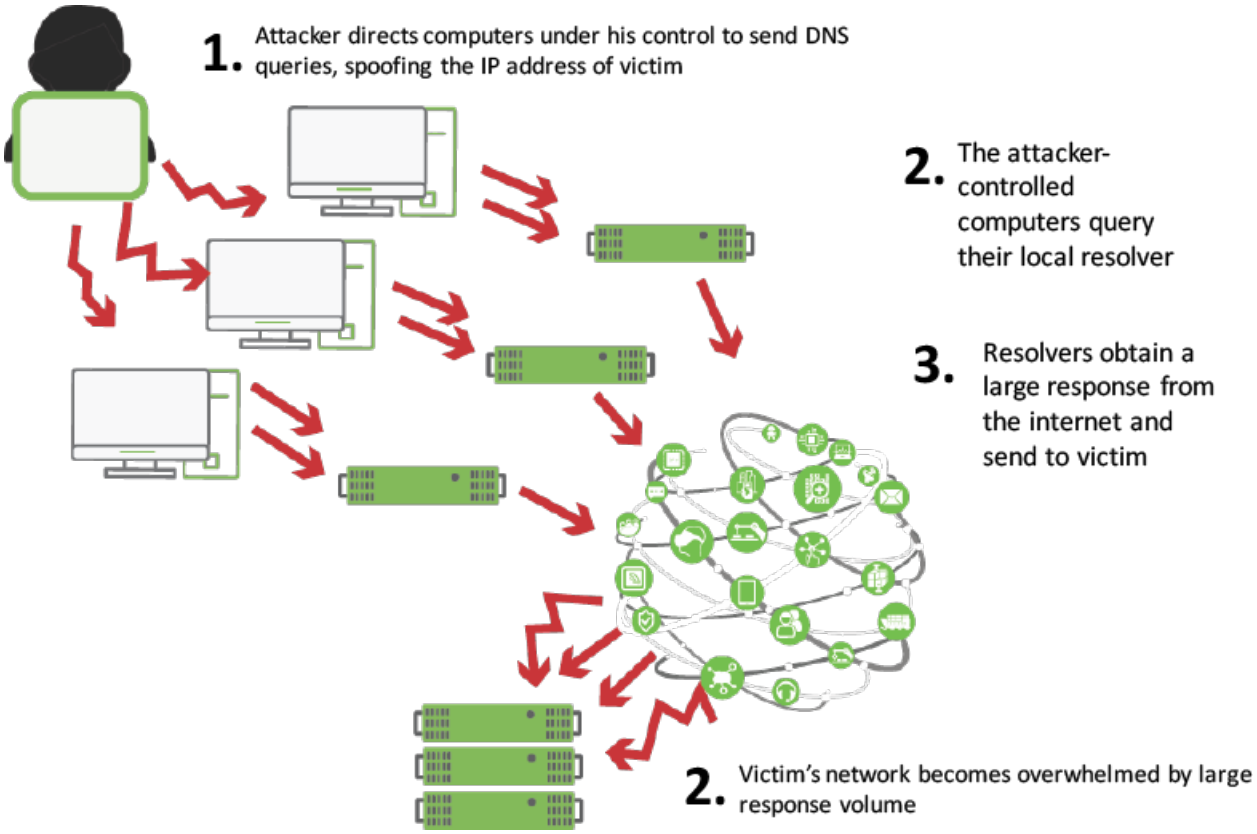


Figure 2 Reflected Flood

Early amplified attacks relied on specific queries that were known to generate large responses (e.g., queries to the root servers, ANY queries or certain TXT queries). These queries were easily blocked by either the operator of the DNS server or by the victim by simply denying every query for those query types. Although there are legitimate uses for ANY and TXT queries, many DNS operators around the world blocked such queries to minimize potential damage.

More recently, attackers have become more sophisticated and have realized that large responses can be easily generated with normal A or AAAA records, making these attacks more difficult to detect and mitigate.

Reflected flood attacks can also have a negative impact on the reflector, as this attack consumes CPU cycles on the server and significant outbound network bandwidth, which can potentially impact service availability. It is good practice to ensure that your resolvers cannot be easily used as reflectors by disallowing queries from outside your network and by setting router egress filters so that IP addresses cannot be spoofed.

DNS Application Attacks

This is the final category of attack targeting the DNS server itself. Unlike UDP and TCP data floods, which attempt to overwhelm the DNS server by sending a large number of queries, DNS application attacks attempt to exhaust some critical internal resource by sending carefully constructed queries to the victim. DNS resolvers are particularly vulnerable to this type of attack, because certain types of queries can cause a resolver to tie up significant CPU or network resources while attempting to obtain an answer.

A Pseudo Random Subdomain (PRSD) Attack (also known as a Water Torture Attack or Death by 1,000 Paper Cuts Attack) is one example of a DNS application attack - this type of attack has been successful in disrupting DNS resolvers around the world . The attacker sent queries for a fictitious subdomain of a valid domain on the internet to service providers' DNS resolvers. Because the authoritative servers became unavailable under this load, the resolvers had to spend considerable CPU and network resources to query and retry each of the authoritative servers for the valid domain. Some resolvers ran out of CPU or network resources and were forced to drop incoming queries, causing a denial-of-service condition for legitimate users.

This is not the only way an attacker might try to exhaust the resources of a target resolver. Any queries that require extra processing power can potentially be used as an attack vector. For example, an attacker might send many queries for obscure DNSSEC signed domains, causing the resolver to perform expensive recursion to obtain the answer, and even more expensive validation of the DNSSEC signed response.

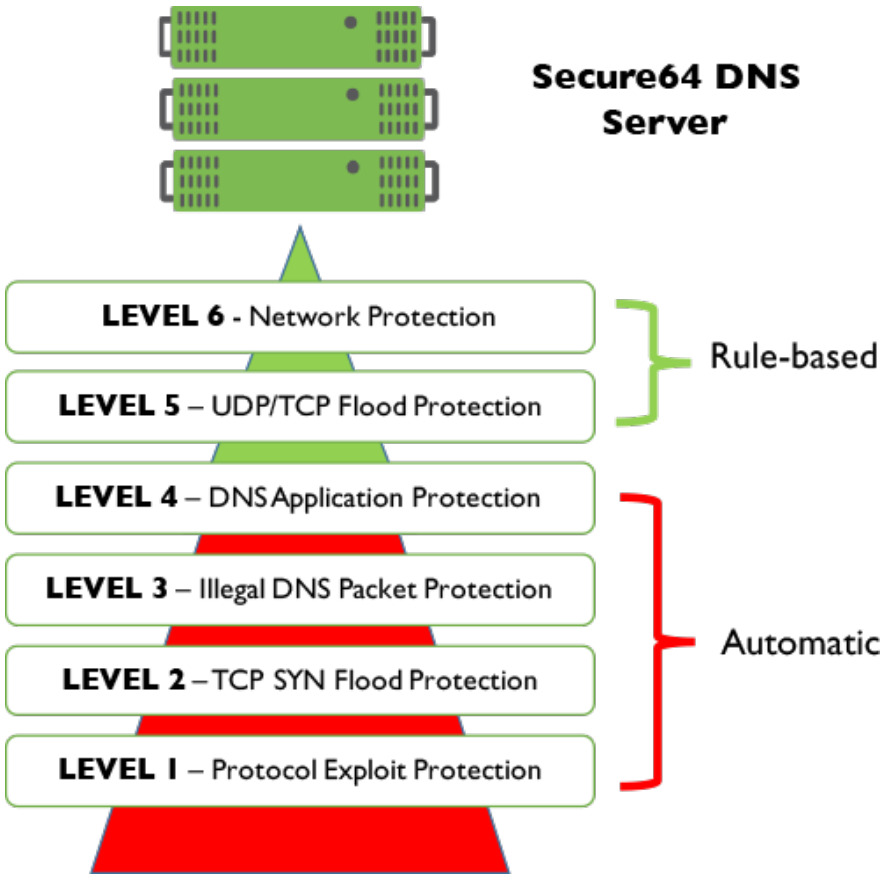
Current Defenses against DDoS Attacks

To defend against DDoS attacks, organizations have historically enlisted routers and firewalls, deployed security devices such as IPS systems, invested in dedicated DDoS equipment, and over-provisioned both network infrastructure and DNS servers for sufficient capacity to fend off attacks. These solutions are far from ideal, as they add cost, complexity and latency to the network, and are often only partially successful in defending against these types of attacks. What is needed is a self protecting DNS server that can find and mitigate the attacks themselves inside of the DNS system.

Designing a Self-Protecting DNS Server

Secure64® DNS Cache™ and Secure64®DNS Authority™ are dedicated recursive and authoritative DNS servers, respectively that run on the Secure64 SourceT® micro operating system. The SourceT network I/O stack is designed to be self-protecting, allowing it to identify and block attack traffic while continuing to respond to DNS queries from legitimate sources.

As shown in the figure below, Secure64 DNS products includes six levels of protection to defeat the types of DDoS attacks previously described.



The table below summarizes the countermeasures utilized by each of the six levels of protection.

Filter	Attack Type	Mitigation Methods
Level 1	Protocol exploits	Automatic detection of malformed packets and invalid combinations of header bits, which are dropped automatically

Filter	Attack Type	Mitigation Methods
Level 2	TCP SYN flood attacks	Automatic detection and mitigation via pre-connect/aging method
Level 3	Malformed DNS requests	Automatic detection and mitigation via DNS packet inspection
Level 4	DNS application attacks (e.g., PRSD)	Drop excessive recursive queries while answering all cache hits when under attack

Table 1 Secure64 DNS DDoS Protections

In addition, the SourceT micro operating system protects the DNS server from buffer overflow attacks and compromise by rootkits, viruses, ransomware, Trojans, and other malware. These protections are described in another white paper, "Eliminating Malware and Rootkits: Six essential characteristics of a genuinely secure OS," available from the Secure64 web site.

Level 1: Protection from protocol exploits

Inbound packets are first processed by the NIC hardware and then by the I/O driver. Common exploits involving malformed packets or invalid combination of header bits are dropped immediately. This level of protection guards against malformed ARP, MAC, TCP or IP packets.

The effectiveness of this filter was tested by ExtremeLabs, an independent test laboratory, who subjected Secure64 DNS Authority to a variety of exploit attacks . They concluded:

"The Secure64 software appeared to ignore the attacks, and delivered until the wire was full of attack queries. Illegitimate requests appeared to be totally ignored."

Level 2: Protection from TCP SYN floods

Unlike conventional operating systems that allocate connection resources upon receipt of the initial SYN request, SourceT does not establish a connection until the three-way handshake is complete, using a patented pre-connect/aging algorithm.

To validate the operation of this filter, the test laboratory placed the DNS Authority server under a legitimate traffic load while TCP SYNs were generated from a number of different source IP/MAC pairs at an increasing rate until the saturation point of a Gigabit Ethernet connection. Extreme Labs summarized the result of this test:

"Secure64 DNS Authority remained 100% responsive to legitimate queries while mitigating the SYN flood attack until the total data rate saturated the Gigabit connection at 830 Mbps of total traffic."

Level 3: Protection from illegal DNS packets

To efficiently withstand attacks while processing valid DNS queries, the I/O stack performs DNS validation on all UDP packets sent to the server's configured DNS IP address(es) and port.

The system examines the DNS packets and rejects malformed queries, such as queries that are shorter than the minimum query length. It also rejects any DNS responses sent to the configured DNS port. This is essential in the protection against reflected flood attacks and has a 0% false positive rate compared to other defense mechanisms. Inspecting and dropping illegal DNS packets in the I/O stack also helps preserve system resources for processing of legitimate traffic.

Level 4: DNS application attack protection

In conventional DNS caching applications, server availability can be compromised by an attacker that utilizes a large botnet to send a small number of queries from each bot that must be resolved over the internet rather than being answered through the cache. Because the query rate from each bot is small, conventional rate limiting techniques do not work against such an attack. When too many of these recursive queries are received, CPU and memory resources become bottlenecks, and even queries from legitimate clients for records in the cache may be dropped.

These types of attacks are extremely difficult to defend against because they utilize legitimate DNS queries for unpredictable domains that cannot be blocked by firewalls, external security devices or by URL filtering devices. This type of attack requires protections built into the DNS application itself, like Secure64's DNS application attack layer.

The application attack protection layer ensures that queries are answered, even under such attack conditions. By decoupling the processing of cache hits and cache misses and actively managing the number of outstanding recursHiragino Kaku Gothic Pro

ive queries allowed when the system approaches overload conditions, this protection mechanism ensures that the vast majority of client queries will be answered with very low latency during application attacks.

Level 5: UDP/TCP data flood protection

By the time traffic passes through the first three filters, illegal and invalid packets have been identified and dropped. What remains are valid queries to which the DNS server should respond. However, during high-volume flood attacks, there may simply be too many queries for the DNS server to process. In this case, Secure64 DNS products supply sophisticated protection from UDP or TCP floods through user-configurable rules that can be triggered by:

- The overall inbound packet rate
- The per client inbound packet rate
- The per client query rate by RRType (A, AAAA, TXT, ANY, etc.)
- The per client inbound or outbound network bandwidth consumption

Rules can specify the action to be taken: either drop traffic from the offending clients or temporarily blacklist/greylist traffic from the offending client until it no longer exceeds the user defined threshold.

Figure 5 compares how DNS Authority and Linux running BIND protect against a direct, non-spoofed UDP flood, in which bots direct a high rate of legitimate DNS queries at the victim server in an attempt to overwhelm it. As the figure shows, the Authority server blocks traffic from the attacking bots, maintaining 100% availability to legitimate queries. The Linux/BIND server, which has no such rate limiting abilities, becomes overwhelmed by the attack, eventually becoming completely unavailable to respond to legitimate traffic.

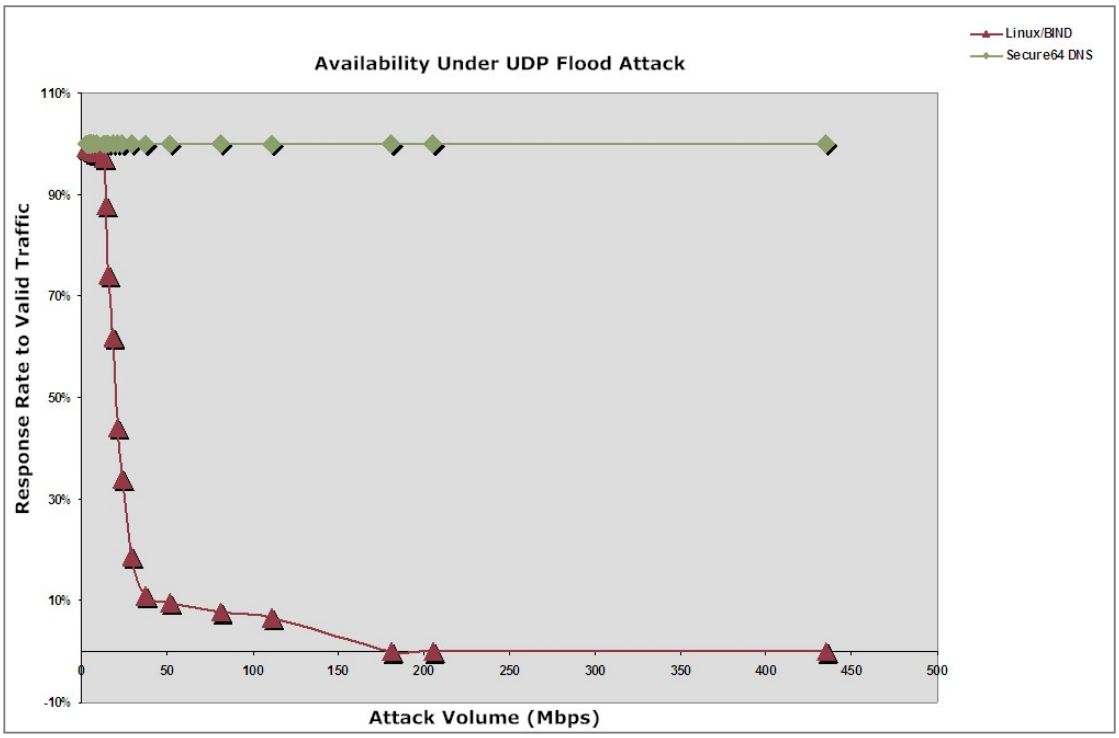
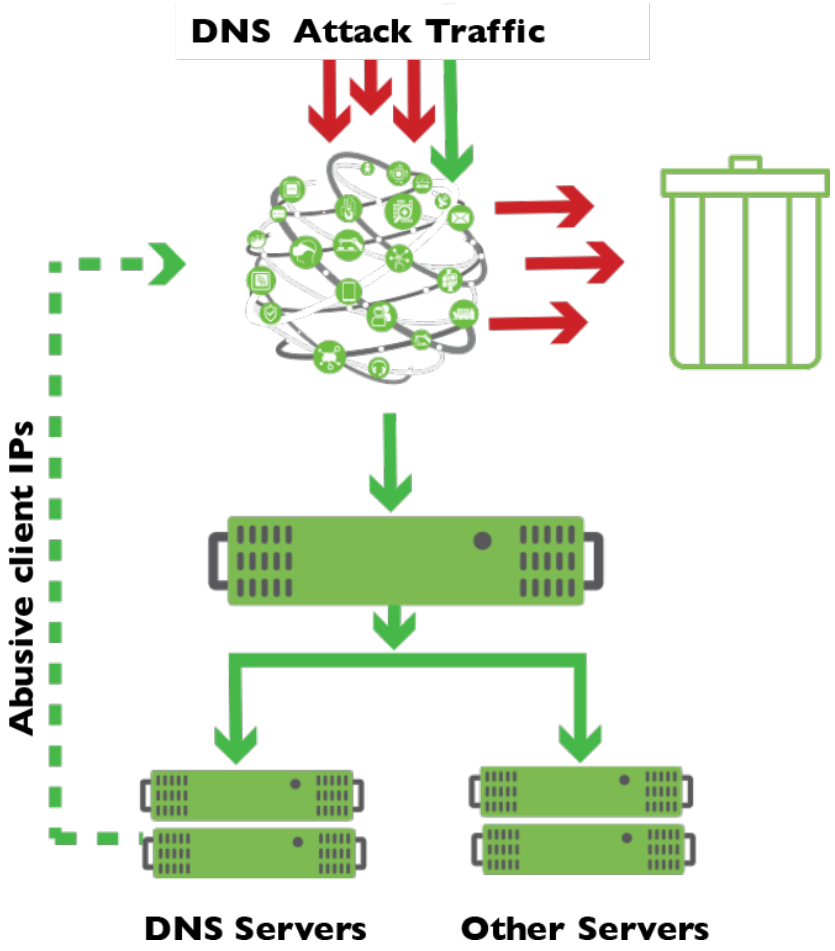


Figure 4 Availability under UDP Flood Attack

Level 6: Network protection

In a reflected, amplified flood attack, the objective is to saturate the network connection of the victim. A self-protecting server can detect that it is the victim of such an attack and drop the attack traffic to remain available, but cannot prevent the network from becoming saturated on its own.

The final level of defense provided by Secure64 DNS servers is its PipeProtector™ feature, which allows the DNS server to be configured to automatically communicate with the upstream router in order to block traffic from attacking IP addresses. User defined rules can be triggered by excessive inbound or outbound bandwidth consumption to automatically blackhole abusers at the router, thus protecting network bandwidth not only to the DNS servers, but to any other devices on the same network.



Conclusion

Self protecting servers, such as DNS Cache and DNS Authority, detect and block a wide variety of common denial-of-service attacks with little, if any, degradation in server performance. In addition, the PipeProtector feature allows the DNS server to protect network bandwidth as well as other devices on the same network from debilitating amplified flood attacks.

Deploying servers with such architecture can reduce the need to overprovision server resources and eliminates the need to protect servers with network security devices, greatly decreasing network cost and complexity while increasing performance.

About Secure64

Secure64 brings trust to the internet through its suite of purpose-built, secure, DNS-based network security products. The company was built on a foundation of security and has forged solutions that are self-protecting and immune to malware. Secure64 secures the DNS infrastructures of leading service providers, government agencies and enterprises globally.

Secure64 is a privately held company founded by HP veterans and boasts deep technical and global experience its leadership and staff. It is the only DNS solution provider that has authored a secure micro OS, automated the deployment of DNSSEC and built self-protecting DNS servers. For more information, visit www.secure64.com

For More Information:
(303) 242-5890
www.secure64.com
Secure64 Software Corporation
5600 South Quebec Street, Suite 320D
Greenwood Village, CO 80111