Citrix NetScaler: A Powerful Defense Against Denial of Service Attacks

CITRIX®

The past couple of years have seen a marked resurgence of denial of service (DoS) attacks. Not only is this availability-threatening class of attack firmly back on the radar screens of today's network and security operations teams, but the nature of the threat has changed as well. The largest Internet companies are no longer the primary targets. Now every business, regardless of size or industry segment, is at risk. Detecting these attacks is also much harder than in the past, as stealthy, lowbandwidth application layer variants focused on exhausting backend resources join the ever-familiar, high-volume attacks intended to flood network pipes or knock over critical network devices/services.

This white paper examines the current DoS landscape and discusses common approaches for dealing with the modern DoS threat. It explains how the Citrix® NetScaler® application delivery controller (ADC) provides a robust yet highly affordable foundation for an organization's DoS defenses. Benefits of the NetScaler solution include:

- A rich set of protection mechanisms capable of effectively thwarting DoS attacks across all layers of the computing stack.
- The inclusion of innovative, sensible techniques for dealing with the most insidious forms of DoS attacks without having to needlessly impact legitimate transactions.
- The ability to leverage the same NetScaler footprint to also enable the transformation from the rigid, legacy datacenters of the past to the scalable and adaptable cloud networks of today.

Understanding the DoS landscape

Once a staple of hackers intent on disrupting the largest properties on the Internet, DoS attacks later faded into the background in favor of financially motivated attacks. In general, these profit-oriented attacks required stealthier, non-disruptive techniques to accomplish their goal of stealing valuable data. During this period, DoS attacks were used primarily for extortion. In this scenario, the bad guy threatens to execute a DoS attack unless a nominal payment is received by a certain deadline. Pay, and you get a nice "thank you" email; don't, and your business suffers the consequences.

The return of DoS attacks

Over the past few years, however, DoS attacks have returned with a vengeance. This development can be attributed foremost to their becoming a favored technique for socially and politically motivated attacks. Objectively speaking, they're a good fit in these cases. It's not valuable data that matters to the attackers, but getting the attention of the target and, even more important, the public at large.

A notable by-product of this "hacktivism" was the release of free or inexpensive toolkits for creating DoS attacks. Combined with easy access to botnets, these toolkits cemented the return of DoS attacks to the mainstream. They also contributed to a handful of characteristics of the current DoS landscape that are particularly important to acknowledge.

To begin with, low technical and financial barriers to entry mean that practically anyone can execute a DoS attack these days. Secondly, and for the same basic reasons, it is now easy to leverage DoS techniques for financially motivated attacks as well. Such attacks can be accomplished either by directly disrupting a competitor or by using DoS techniques as a smoke screen for a multi-vector attack ultimately designed to steal valuable data. The key take-away here is that every organization is now a potential DoS target, regardless of size, vertical industry or agenda.

The evolution of DoS attacks

While ease of execution has facilitated the return of DoS attacks, another major change is having an equally profound effect when it comes to defending against them. Consistent with what's happened across the threat landscape in general, DoS attacks are migrating up the computing stack. Because "migrating" suggests a departure from the area of origin, however, it's more accurate to say that they're adding new tricks to their arsenal.

Noisy, high-volume, network-focused DoS attacks aren't necessarily going away. But they are being joined by a new breed of DoS attacks that operate at higher layers of the computing stack. A major challenge with these new attacks is that they often mirror legitimate sessions/transactions, a characteristic that allows them to pass unthwarted through a wide array of defenses, including firewalls and intrusion prevention systems.

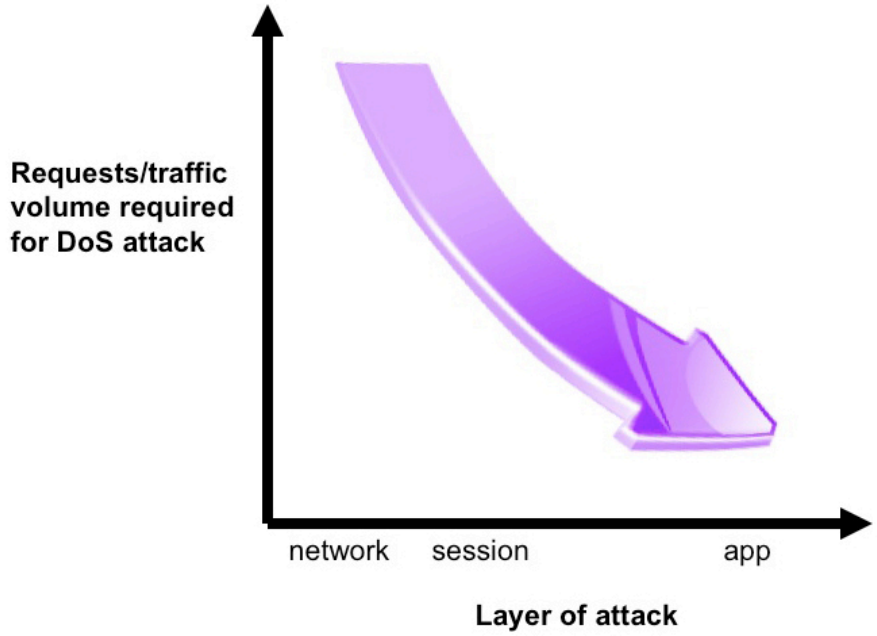


Figure 1: DoS Attack Asymmetry

A second issue is their increasingly asymmetric nature [shown in Figure 1]. From a technical perspective, this refers to requiring only a relatively small number of application requests and/or small amount of bandwidth to trigger disproportionate consumption of backend resources. From a practical perspective, it again means that they are harder to detect, as unexpected spikes in transaction counts or network traffic are no longer indicators of their presence.

For all that's changed, however, DoS attacks remain focused on causing resource exhaustion at some point in the end-to-end computing chain—be it the network "pipes," the state tables of network devices and servers or the processing capacity of application hosts. Staying focused on this fact is the key to formulating a successful DoS mitigation strategy.

High-level strategies for DoS mitigation

DoS mitigation solutions break down into two general classes: customer premise- based devices and cloud-based service offerings. Within each of these classes there are multiple options, each with its own pros and cons.

Customer premise-based devices

The first DoS mitigation option in this class, and one that quickly needs to be dismissed as a poor choice, is the firewall or intrusion prevention system. To be fair, these devices often do incorporate a number of DoS protection mechanisms (some more than others). However, these mechanisms are generally limited to counteracting network DoS attacks, and provide no protection against higher-layer variants. Moreover, these devices are inherently stateful. The need to closely track the state of packets and flows passing through them makes the devices themselves susceptible to DoS attacks.

Dedicated DoS mitigation devices are a second option. Although they generally offer a robust set of multi-layer DoS protection mechanisms, they too have some shortcomings. To begin with, they suffer from the same limitation as every other customer premise-based solution: they're irrelevant if the attack floods your Internet connection(s) and prevents traffic from getting to them in the first place. They're also likely to be susceptible to SSL-based attacks, which carry a heavy processing penalty, especially in the absence of dedicated hardware for SSL termination and inspection. One other tradeoff to consider is the degree to which any unique DoS prevention capability outweighs the need to purchase, deploy and maintain "yet another device" at each Internet connection of significance.

Already a strategic point of control in most networks, the modern ADC represents a third, often ideal option to pursue. Market-leading ADCs—such as NetScaler— combine a wealth of DoS mitigation capabilities that account for all layers of the computing stack. They even include support for compute-intensive SSL-based DoS attacks. The result is a solution that provides substantial coverage for DoS threats without the need to implement another set of dedicated devices.

Cloud-based service offerings

The primary advantage of cloud-based DoS mitigation options is that, unlike customer premise-based solutions, they can account for DoS attacks focused on swamping your Internet bandwidth. Generally speaking, the two offerings in this class—content delivery network service providers and anti-DoS service providers—involve datacenters provisioned with massive amounts of bandwidth. This approach inherently enables these options to better cope with volumetric- style attacks. In addition, both types of solution providers have typically made substantial investments in a wide variety of DoS mitigation technologies, since their businesses fundamentally depend on it. However, there are some significant differences to be aware of, not to mention potential shortcomings. These include:

- Significant variability in coverage provided for higher-layer DoS attacks. To some extent this is unavoidable, because no external provider will ever understand the "features" of your applications better than you do yourself.
- Although CDNs are an always-on solution, they're generally used only for a subset of an organization's most important, customer-facing sites and applications. Even then, there are ways attackers might get "around" or "through" the CDN—for example, by blasting away at the controlling IPs or submitting a flood of requests that result in cache misses and have to be served by your source infrastructure.
- In comparison, while anti-DoS scrubbing centers provide coverage for all of an organization's traffic, they're not always on (because that would be cost prohibitive). Instead, they're selectively engaged by the customer whenever an attack is detected. This inherently makes them a poor option for higher-layer DoS attacks, which do not always involve brute force and, therefore, not as easy to identify when they occur.

The answer: Defense-in-depth strategy

Not surprisingly, the ideal approach is to pursue a defense-in-depth strategy that combines a cloud-based service and a customer premise device operating in a complementary manner. Given the rising prevalence of application-layer attacks, a customer premise solution—in particular an ADC—stands to provide the biggest impact for your investment. It is, therefore, a great place for most organizations to start. That said, making an investment in a DoS scrubbing service capable of thwarting volumetric network attacks probably shouldn't be too far behind, especially if you're a high-profile target.

The NetScaler approach to DoS protection

A modern ADC in every respect, NetScaler delivers robust protection not only against classic, network-layer DoS attacks, but also against the more advanced and increasingly common session- and application-layer attacks, including low-bandwidth, asymmetric variants. For DoS mitigation, NetScaler takes the same approach it applies for all other aspects of security: a layered security model. This enables NetScaler to excel even as DoS attacks evolve up the computing stack.

Increasing difficulty of detection

	Sample Attacks	NetScaler Mitigation Features
Application	GET and malicious POST floods; slowloris, slow POST, and other low-bandwidth variants	Application protocol validation, surge protection, priority queuing, HTTP flood protection, HTTP low-bandwidth attack protection
Connection and Session	Connection floods, SSL floods, DNS floods (udp, query, nxdomain)	Full-proxy architecture, high- performance design, intelligent memory handling, extensive DNS protection
Network	Syn, UDP, ICMP, PUSH and ACK floods; LAND, smurf, and teardrop attacks	Embedded defenses, default deny security model, protocol validation, rate limiting

Figure 2: NetScaler DoS attack mitigation features

Note: many of the mitigation technologies listed in Figure 2 actually help mitigate DoS attacks across multiple layers. The NetScaler ADC's high-performance design, default-deny posture and proxy-based architecture are good examples, as they are applicable across all layers of the computing stack. They are shown in only one place to help streamline the discussion.

Network-layer DoS protection

Network-layer DoS attacks primarily involve overwhelming an organization's public-facing network infrastructure with a flood of traffic or specially crafted packets that can cause network devices to behave erratically. NetScaler features that thwart attacks at this layer include:

- **Embedded defenses** – NetScaler incorporates a high-performance, standards-compliant TCP/IP stack that includes enhancements specifically intended to counteract many forms of low-level DoS attacks. One example is an implementation of SYN cookies—a well-recognized mechanism for handling SYN flood attacks—which is both performance optimized (to maximize throughput for negotiated connections) and security enhanced (to render forged connection techniques obsolete). Other DoS threats accounted for similarly, or by default configuration settings, are teardrop, LAND, ping of death, smurf and fraggle attacks.

- **Default-deny security posture** – Default-deny might be a relatively simple security mechanism, at least conceptually, but it's also a very powerful one. By automatically dropping packets that are not explicitly allowed by policy, or not associated with a valid flow, NetScaler inherently stops a variety of attacks, including generic UDP, ACK, and PUSH floods.
- **Protocol validation** – One particularly troublesome variety of DoS attack relies on sending malformed data, such as packets with invalid combinations of flags, incomplete fragments or otherwise mangled headers. A good example at the network layer is known as the "Christmas tree" attack, which gets its name from the fact that bad packets are "lit up" with all possible TCP flags enabled. NetScaler defeats this sub-class of attacks by ensuring that communication protocols are used in a manner that strictly conforms to their governing specifications and otherwise prevents combinations that, while technically allowed, could still be dangerous. With NetScaler, this mitigation mechanism spans the stack, as it applies for all supported protocols, including TCP, UDP, DNS, RADIUS, Diameter, HTTP, SSL, TFTP and SIP.
- **Rate limiting** – Another general technique for mitigating DoS attacks is to keep network connections and servers from overloading by throttling or redirecting traffic that exceeds a specified limit. NetScaler provides a granular capability for doing this in the form of AppExpert rate controls. With this feature, administrators can define a wide variety of NetScaler response policies to be triggered whenever configurable thresholds for bandwidth, connection or request rates either to or from a given resource, including virtual servers, domains, and URLs, are exceeded. Care must be taken when employing this mechanism, however, because you do not want to unintentionally impact legitimate communications.

Connection and session-layer DoS protection

Connection-oriented DoS attacks focus on exhausting device state tables, while DoS attacks against the intermediate layers of the stack typically involve perversion of DNS or SSL functionality. NetScaler features that counteract both these types of attacks include the following:

- **Full-proxy architecture** – As a full-proxy solution, NetScaler is an active part of the traffic flow, not a passive component that only sees but can't affect what's happening. By terminating all inbound sessions, NetScaler not only creates an "air gap" between external and internal resources, but also provides an invaluable opportunity for inspecting and, if appropriate, manipulating traffic before forwarding it to its destination. This approach inherently screens out a variety of malicious elements while simultaneously providing a foundation for advanced inspections designed to remove the ones that remain. It also enables NetScaler to serve as a buffer for backend resources against a variety of threats, including many types of DoS attacks.
- **High-performance design** – Serving as an effective buffer for backend resources also requires a high-performance design; otherwise, NetScaler would simply supplant individual servers as the point of failure during a DoS attack. NetScaler employs a purpose-built platform on which both the hardware and the system-level software are designed and optimized explicitly for the NetScaler workload. Specific features include a customized operating system (for deterministic, low-latency processing), optimized networking stack, intelligent HTTP parsing engine and selective use of function-specific hardware accelerators. Indeed, dedicated SSL accelerators—operating in conjunction with a full proxy capable of identifying and dumping empty or malicious SSL connections—are instrumental when it comes to fending off SSL flood attacks.

NetScaler performance ratings (MPX 22000 series)	
TCP connections per second:	**8.5 million**
HTTP requests per second:	**4.7 million**
HTTP throughput:	**120 Gbps**
SSL transactions per second	**560,000**
SYN attacks per second	**38 million**
DNS requests per second	**35 million**
Concurrent SSL sessions	**7.5 million**
Concurrent TCP sessions	**75 million**

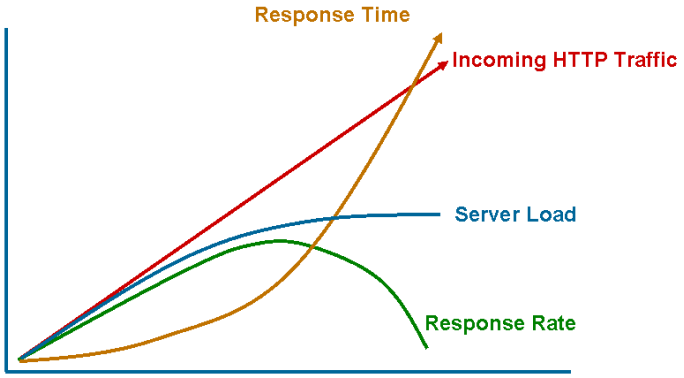
- **Intelligent memory handling** – Another way that NetScaler mitigates connection flood attacks is by incorporating "memory-less" techniques for connection negotiation. These techniques are used at multiple layers of the stack, including for TCP and HTTP setup, and keep NetScaler from having to allocate resources until a new connection has been completely validated, or until an actual application request has been submitted. This approach reduces dependency on an excessively large connection table and eliminates the need for numerous reaping routines. Reaping is still used in other scenarios to intelligently manage memory—for example, by prioritizing elimination of fragments under low-memory conditions—and to help counteract some of the "slow" application layer attacks discussed in later sections. The net result is further hardening of NetScaler itself against DoS attacks and better buffering of backend systems.
- **Extensive DNS protection**s – DoS attacks against DNS—an essential infrastructure service for the modern datacenter—are neither new nor uncommon. They include ordinary UDP floods, as well as query-based floods that use numerous tricks, such as requesting records for nonexistent hosts, to overload DNS servers. NetScaler addresses these threats by supporting two modes of operation: 1. DNS proxy mode, where it load balances an organization's internal DNS servers; and 2. authoritative mode, where it directly serves as the organization's solution for name and IP resolution requests. Mitigation features that apply to one or both of these modes include the NetScaler full-proxy architecture and high-performance design, a hardened DNS implementation, DNS protocol validation and DNS-specific rate limiting capabilities. NetScaler support for DNSSEC enables it to neutralize threats that use forged and corrupted host records for spreading to new targets.

Application-layer DoS protection

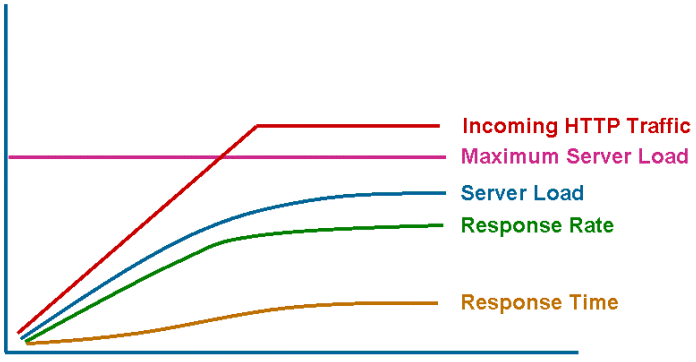
The latest domain of innovation for DoS attacks, the application layer, is problematic for several reasons. To begin with, application-layer attacks are narrower in definition, often specific not just to a given application layer protocol (e.g., HTTP), but to an individual application. Compounding matters is the fact that the attack traffic is often indistinguishable in content and volume from normal traffic. A classic example is a low-bandwidth attack that involves nothing more than a steady series of requests to an application that are known to require substantial backend processing (e.g., a complex calculation or search operation). Lower-level security devices, such as network firewalls, are largely useless against such attacks; and even higher-level devices are likely to require periodic tuning to keep up with new tactics and application-specific variables.

NetScaler features that address application-layer DoS attacks include:

- **Application protocol validation** – Enforcing RFC compliance and best practices for HTTP use is a highly effective way in which NetScaler eliminates an entire swath of attacks based on malformed requests and illegal HTTP protocol behavior. Other custom checks and protections can be added to the security policy by taking advantage of integrated content filtering, custom response actions and bidirectional HTTP rewrite capabilities.
- **Surge protection and priority queuing** – In addition to protecting backend servers from being loaded beyond their capacity, successful DoS mitigation requires ensuring that clients get a response and critical business traffic is not adversely impacted under attack conditions. NetScaler features that address these requirements include surge protection and priority queuing. NetScaler gracefully handles intermittent traffic surges by basing the rate at which new connections are presented to backend servers on their current capacity. Significantly, no connections are dropped with this mechanism. Instead, NetScaler caches and delivers them, in the order received, once the backend servers are ready to handle them. A closely related feature, priority queuing, provides a weighting scheme that can be used to control the order in which queued requests are processed. The order is based on the relative importance of the associated applications.



Server behavior without surge protection



Server behavior with surge protection

- HTTP flood protection – An innovative method is used to mitigate HTTP GET floods. When an attack condition is detected (based on a configurable threshold for queued requests), NetScaler sends a low-impact computational challenge to a tunable percentage of the associated clients. The challenge is designed such that legitimate clients can easily respond to it properly but "dumb" DoS drones cannot. This information enables NetScaler to distinguish and drop bogus requests while maintaining those sent by legitimate application users. Similar techniques, combined with application-level rate limiting, are used to thwart HTTP POST and recursive GET floods.
- HTTP low-bandwidth attack protection – NetScaler automatically defeats slowloris attacks, which deliver HTTP headers piecemeal just under the timeout limits for the target server, by never acknowledging the setup of a valid connection. In contrast, defeating slow POST attacks, which feed the HTTP data to the server very slowly, is a bit more challenging, but still possible. In these cases, NetScaler uses specialized algorithms to monitor for telltale conditions at the application request level, moderate the number of very slow connections being served at any time and proactively reap excess slow connections from memory. Health monitoring for server performance anomalies and custom rate limiting rules can also be used to help thwart other low-bandwidth DoS variants that emerge.

Conclusion

Availability-threatening DoS attacks have been growing in frequency and sophistication in recent years. For most organizations, comprehensively defending against this class of threats will involve a combination of complementary cloud-based scrubbing services and customer premise-based DoS mitigation technologies. On the customer-premise side of the equation, Citrix NetScaler represents an ideal solution. With NetScaler, organizations can leverage the same platform that enables them to transition from yesterday's rigid computing environments to highly adaptable cloud datacenters to establish a robust, multi- layer defense against potentially business crippling DoS attacks.

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.