IDC VENDOR SPOTLIGHT

Sponsored by: NETSCOUT

Stateful firewalls have unwittingly introduced the attack vector of distributed denial-of-service (DDoS) attacks. State exhaustion attacks can knock down defenses or disrupt communications. Cybersecurity vendors must rethink the role of stateful systems and how to secure them.

Security Risks of Stateful Network Architectures in the Digital Transformation Age

June 2021

Written by: Christopher Rodriguez, Research Manager, Network Security Products and Strategies

Introduction

State is a seemingly inescapable principle of networking. Communications must be divided into packets for transportation at massive scale. The process naturally entails the requirement for a means to ensure reliable, verifiable, and untainted delivery. The concept is expressed at all layers of the OSI model. For example, applications must keep track of established sessions and users who have already authenticated.

This concept of state tracking similarly applies to network security infrastructure and practices. While firewalls could rely solely on static factors such as port and protocol, this approach can be vulnerable to spoofing that allows hackers to gain illicit access. To compensate, stateful firewalls add context about the security status of connections over time. As a result, stateful firewalls have proven to be a popular component of enterprise security architecture.

However, stateful firewalls and other infrastructure have unwittingly introduced another attack vector: distributed denial-of-service (DDoS) attacks. Specifically, these devices enable state exhaustion attacks that can knock down defenses or disrupt communications. In 2020, attackers continued to scale up their efforts, launching over 10 million DDoS attacks, including state exhaustion attacks, and have shown no signs of slowing. Digital transformation is expanding this threat vector in new ways as well. As threat actors devise new tactics to abuse stateful systems, security must be rethought carefully to design IT environments that are resilient to state exhaustion attacks, from packet creation to delivery.

AT A GLANCE

KEY STATS

- Over 10 million DDoS attacks occurred in 2020.
- IDC expects nearly 2 billion container instances to be deployed by 2023.

KEY TAKEAWAY

State is a well-known threat vector for DDoS attacks. Digital transformation may introduce new opportunities for the threat vector to be abused

Stateless (or Minimal State) DDoS Mitigation Offers Business Value and Strategic Advantage

DDoS attacks can come in many forms but are always, at their core, attacks against the business itself. DDoS mitigation translates directly into business enablement. Consider the quantifiable benefits of DDoS mitigation and their correlation to business objectives:

- **Online experiences drive business growth.** Digital transformation has reshaped society, with modern applications powering an always-on connected world. The 24 x 7 model of ecommerce operations is an example of a situation that requires constant, reliable, and fast connectivity to thrive. Online shoppers have steep expectations for site performance — any annoyance, disruption, or distraction could translate to abandoned shopping carts and lost sales. The requirement for uninterrupted connectivity reached levels of life-and-death urgency in 2020 as doctors pivoted to telehealth to care for patients during the lockdown. Similarly, the global pandemic forced many organizations to become digital innovators. For example, online ordering applications extended a lifeline to restaurants, which otherwise would have had to shut down.
- **Service providers can avoid costly downtime.** Communications service providers and cloud service providers face high customer expectations for fast, reliable service. Even a few minutes of disruption can disrupt customers' business operations. Service providers offer service-level agreements (SLAs) to ensure a minimum level of performance and availability with only a few minutes of downtime per year. Ultimately, service providers endeavor to avoid any disruption at all to meet demanding customer expectations.
- **Enterprises can ensure productivity as workers require access to work from home.** The pandemic forced businesses to find a way to support remote work, to the extent that the nature of their work allows. For many organizations, this required a significant investment or expansion in remote work infrastructure, including virtual desktops, virtual private networks (VPNs), and conferencing systems. For many organizations, cloud scalability and accessibility provided further stimulus to move workloads and access to the cloud. In this case, service disruption presents the potential for quantifiable, costly work stoppages for large segments of a workforce.

Several factors can contribute to service disruption or degradation. However, DDoS attacks are one cause that businesses can mitigate. Intelligent DDoS mitigation solutions ensure that businesses maintain reliable and always-on service availability as the foundation for a thriving connected business.

The term "DDoS" conjures the vision of massive volumetric attacks. In reality, the DDoS threat landscape includes attack types such as application layer and state exhaustion attacks that are equally devastating but easily overlooked. Network devices including routers, firewalls, load balancers, and intrusion prevention systems are vulnerable to state exhaustion attacks. These devices require a separate, stateless device to provide protection against state-based attacks.

The ability to block state-based attacks, and all forms of DDoS, is a unique capability provided by intelligent DDoS mitigation systems. Notably, because the aforementioned network infrastructure and security systems are stateful devices, they are incapable of defending themselves against state exhaustion attacks. For example, consider that firewalls must reference state tables for each connection before deciding to forward or drop a packet. By comparison, intelligent DDoS mitigation solutions operate in a stateless manner, which requires less processing power for faster decisions.

However, awareness of state-based risks is expanding beyond the networking level. Digital transformation is driving IT organizations to adopt next-generation workloads and applications to unlock business agility and operational advantages. These next-generation workloads are distributed, modular, and stateless, enabling speed and scale. While developers rush to take advantage of modern application development and delivery technologies, cybermiscreants will also focus their attention on these new technologies in search of a fresh attack vector. Stateful infrastructure protection, combined with modern stateless and state minimization application delivery architecture, provides thorough protection against state as an emerging attack vector.

Digital Transformation Renews State-Based Risk

Attackers are continually seeking new ways to disrupt network or application performance. Stateful systems are one threat vector with a known history of abuse, yet they continue to challenge traditional network and security systems. For most enterprises, the idea of switching to a stateless firewall is not feasible due to the risk of spoofing and other evasion techniques. These security systems will continue to require separate, dedicated stateless defenses.

> Stateful systems are one threat vector with a known history of abuse, yet they continue to challenge traditional networks and security systems.

More importantly, excessive state presents the possibility of future complications in the wake of digital transformation as changing technologies and business practices introduce new attack vectors. Next-generation applications are typically designed to be stateless — processes run as independent instances with no need to reference past iterations of the process. Although next-generation applications and workloads favor stateless design, in a practical sense, state must be tracked in some form or another. For example, web applications must track the status of users who have logged in to their accounts already, even if they open new browser tabs or change windows or navigate away temporarily. Typically, these sessions can be tracked via cookies or tokens, or state may be otherwise maintained in the client.

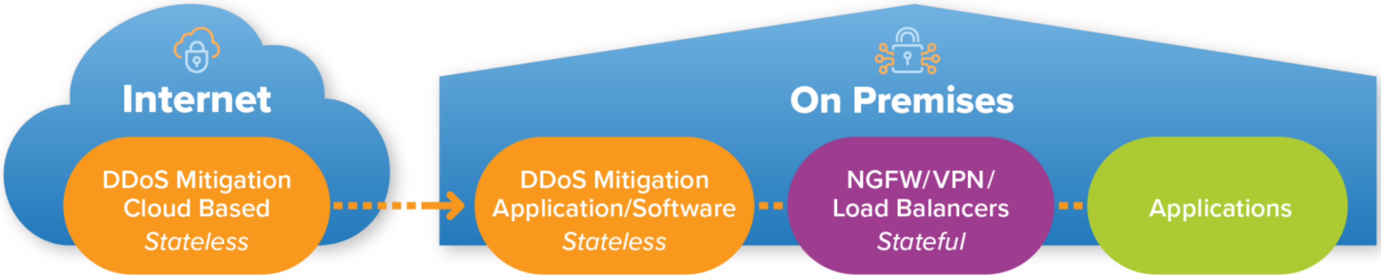
State minimization should be a key consideration in modern application development and delivery architectures such as containerization and microservices, which enable benefits such as workload agility, dynamic resource allocation, and horizontal scale out. These benefits are instrumental for web apps that may experience surges in use, as containers can be quickly spun up and then disposed as needed. For reference, IDC expects nearly 2 billion container instances to be deployed by 2023.

Containers are increasingly popular for use in enterprise workloads as well, as businesses are eager to leverage the scale and speed of Kubernetes. However, developers are designing stateful containers for enterprise workloads to store the state of the application and associated data as well as any data created by the application. The failure to track state would represent an availability and reliability issue for containerized stateful applications. Whereas stateless applications can simply restart a container in the case of failure or other problems, stateful applications require state tracking capabilities in order to reconnect to databases and other storage systems in case of failure. The potential DDoS risk is magnified if application traffic and storage data traffic share resources with a network being attacked. For now, the potential risk for these next-generation workloads is not fully known, but inevitably, cybercriminals will start to test these applications for vulnerabilities in earnest.

State-based risk is a unique threat vector because it crosses over into real-world logistics. For example, malicious bots represent a newer form of business disruption — akin to a DDoS attack that exploits gaps in business logic to disrupt real-world operations. Some bots are designed to create a race condition in inventory systems. While a retailer may limit the number of items that can be placed in a digital cart by any one shopper, bots can generate many digital carts, thereby circumventing limits and loading up on inventory. This forces the retailer to mark the inventory as temporarily unavailable to avoid promising the same item to two different buyers. Of course, the attacker has no intention of purchasing the inventory; rather, it seeks only to make the temporary inventory hold into a permanent one.

Overall, the technology industry is at an inflection point. There is no likely workaround for stateless defenses at a networking level. However, digital transformation is injecting the threat vector into the rest of the communications stack. As modern applications leverage technologies such as containerization to become more scalable, the underlying network infrastructure will continue to feature firewalls, intrusion prevention systems, web application firewalls, and load balancers that are brittle and susceptible to DDoS attacks. These stateful systems will continue to require specialized protection against state exhaustion attacks in the form of a stateless network edge security stack (Figure 1 provides a reference architecture). Additionally, it is critical to reconsider the use of state in application development, such as adoption of next-generation workload principles and moving state from the server to clients.

FIGURE 1: ***A Stateless Network Edge Security Stack for Network and Application Protection***



Source: IDC, 2021

Considering NETSCOUT

NETSCOUT offers multiple options for DDoS mitigation, including protection of stateful network infrastructure and applications. NETSCOUT Arbor Edge Defense (AED) is a DDoS protection and threat intelligence enforcement device that offers inline, stateless, bidirectional protection on premises at the customer's network edge. NETSCOUT's Arbor Sightline and Arbor Threat Mitigation System (TMS) provide visibility into and protection against all types of DDoS attacks for large-scale networks. Both solutions can be augmented and coordinated with NETSCOUT's Arbor Cloud. Arbor Cloud is NETSCOUT's global DDoS mitigation service offering over 11Tbps of mitigation capacity.

Arbor Edge Defense

NETSCOUT's Arbor Edge Defense (AED) is an on-premises security gateway that deploys between the internet router and firewall. AED leverages highly scalable stateless packet processing technology and threat intelligence to automatically block state exhaustion, application layer, and volumetric DDoS attacks. AED can block inbound and outbound non-DDoS threats by leveraging indicators of compromise (IOCs) and threat intelligence such as malware hash values, malicious URLs, and IP reputation from NETSCOUT's ASERT research division. The solution offers integration with third-party threat intelligence sources via REST APIs and STIX and TAXII formats and can also integrate with security information and event management (SIEM) tools via Syslog CEF and LEEF formats, enabling security teams to fully investigate and assess threats in proper context.

Because AED uses patented, "bump in the wire," stateless packet processing technology, it is not susceptible to state exhaustion DDoS attacks that threaten stateful infrastructure such as firewalls, VPN concentrators, load balancers, and intrusion prevention systems. AED combined with modern stateless and state minimization application development practices and delivery architectures provides complete protection against state exhaustion attacks, other DDoS attacks, inbound and outbound threats, and multivector attacks. In the event of a DDoS attack that is larger than the internet circuit, AED's Cloud Signaling feature will automatically and intelligently route traffic to a cloud-based mitigation service such as NETSCOUT's Arbor Cloud or an internet service provider.

Arbor Sightline and Threat Mitigation System

Arbor Sightline analyzes various forms of network telemetry such as Netflow, BGP, and SNMP from across the network to detect, classify, and trace back DDoS attacks. Combined with the Arbor TMS, the solution can mitigate all forms of DDoS, including large, multi-terabyte volumetric attacks or much smaller application layer attacks. Furthermore, because TMS is an out-of-band, stateless packet processing solution, it can be used to mitigate state exhaustion attacks without becoming a target itself. The solution set includes detailed reporting, logging, and centralized management capabilities and has an embedded portal, a user interface, and full APIs for additional services. Additionally, the company recently introduced Arbor Sentinel, an add-on that is designed to intelligently orchestrate multiple methods of mitigation for multivector DDoS attacks. The Sightline/Sentinel/TMS solution can be further augmented with Arbor Cloud for additional mitigation capacity.

Challenges

NETSCOUT faces challenges in the form of the ongoing customer education required to relay the value of its solution to buyers. DDoS is commonly discussed in the media in terms of large, record-breaking volumetric attacks. As a result, buyers are likely to be confused about the requirements for a dedicated approach for protection of state-based infrastructure and applications. This confusion can lead to project delays and frustration as a result of panic buying at the onset of an attack that confounds legacy approaches to DDoS mitigation. NETSCOUT is challenged to continue to educate the market while making products that provide clear value and are easy to operationalize.

Conclusion

For service providers and enterprises, DDoS attacks represent a severe threat to business operations and profitability. For cybermiscreants, DDoS attacks represent a cat-and-mouse game, with stateful systems offering a prime target for wreaking havoc. While stateful infrastructure threats have been long understood, digital transformation has introduced numerous new attack vectors. At this critical juncture, the cybersecurity industry must rethink the role of stateful systems and how to best secure these systems.

About the Analyst

***Christopher Rodriguez,** Research Manager, Network Security Products and Strategies*

Chris Rodriguez is a Research Manager in IDC's Network Security Products and Strategies program covering technologies designed to secure today's complex enterprise networks. The Network Security Products and Strategies practice covers specific functions including firewall/UTM, IDS/IPS, VPN, DDoS mitigation products, cloud security gateway, messaging security, web security, and web application firewall.

MESSAGE FROM THE SPONSOR

About NETSCOUT

The facts are clear. DDoS attacks continue to increase in size, frequency, and most of all complexity. State has been and always will be a target of DDoS attacks. As organization execute their digital transformations, they must make a concerted effort to minimize state in network infrastructure, applications and stateful cybersecurity solutions to avoid downtime.

To learn more about the NETSCOUT Arbor DDoS protection solutions visit:

https://www.netscout.com/ddos-protection

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

IDC