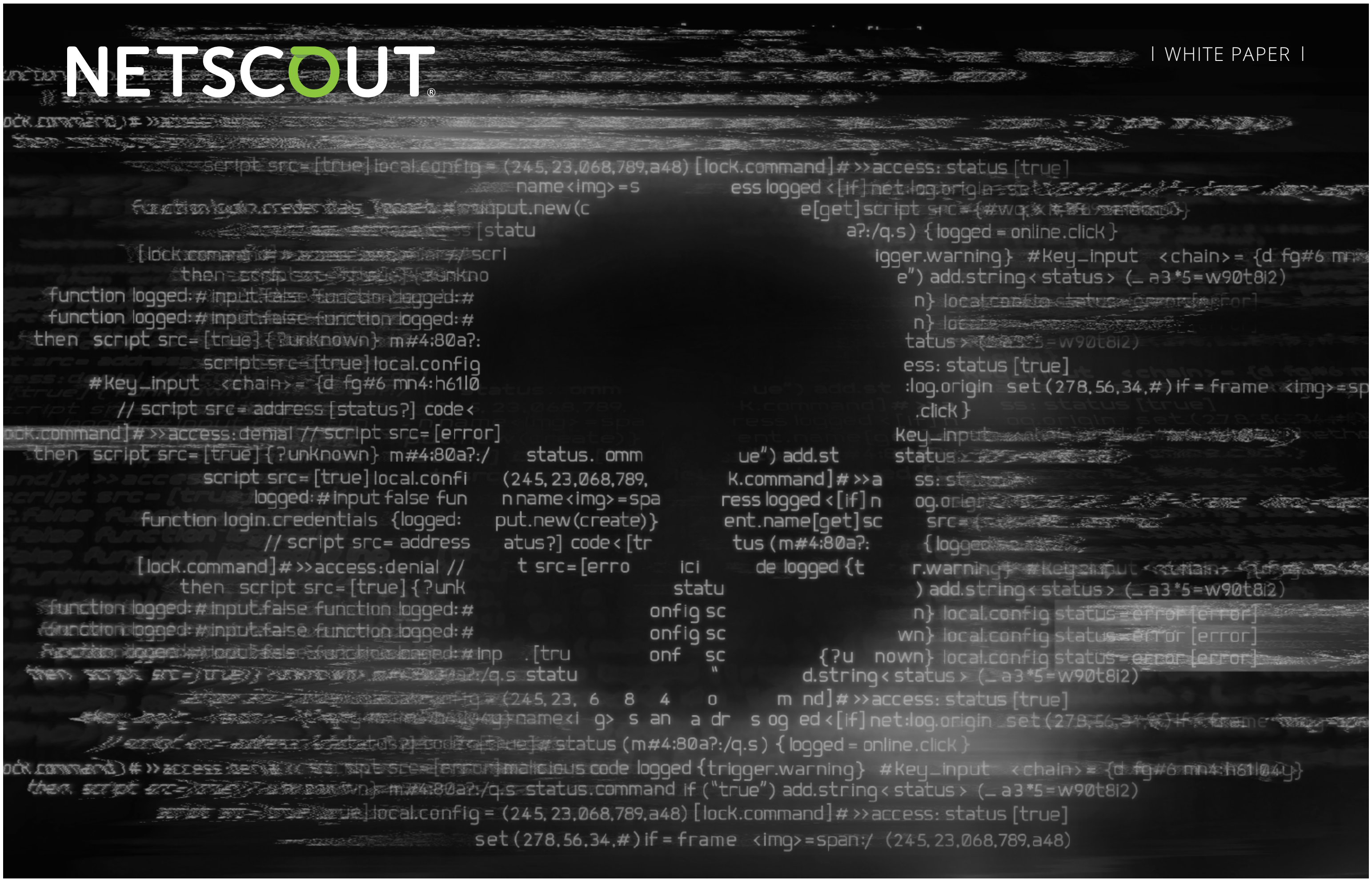

| WHITE PAPER |

Enemy of the State

Why DDoS Attacks Against Stateful Devices Have Massively Increased – And What To Do About It

SECURITY

TABLE OF CONTENTS

Enterprises Dealing With A Proliferation of Cyber Attacks

While the world grapples with the ongoing effects of the COVID-19 pandemic, enterprises continue to be bombarded with cyberattacks, especially as they support work from home (WFH) and other remote-work initiatives.

Consider the following:

- According to the 1H 2021 NETSCOUT Threat Intelligence Report, the first half of 2021 found attackers launching nearly 5.4 million distributed denial-of-service (DDoS) attacks—an 11 percent increase from the same time period in 2020.
- Attackers developed new DDoS attack techniques to evade traditional defenses. Using adaptive DDoS principles, threat actors can now customize each attack to bypass both cloud-based and on-premises static DDoS defenses.
- Successfully mitigating DDoS extortion attacks has become a high priority for enterprises and service providers alike. The 16th annual NETSCOUT® Worldwide Infrastructure Security Report (WISR) shows a 125 percent increase in DDoS extortion attacks, while survey respondents listed these attacks as a primary concern, second only to ransomware.
- The virtual private network (VPN) gained unwanted attention from attackers during the pandemic as organizations increasingly supported WFH initiatives. Attackers conducted pre-attack reconnaissance by querying Domain Name System (DNS) records for names like "VPNxxx".company.com, launching DDoS extortion attacks against VPN gateways for monetary gain.
- According to the WISR, 75 percent of enterprises reported DDoS attacks on key pandemic infrastructures, such as routers, firewalls, and VPN concentrators. Additionally, 83 percent of enterprises that suffered a DDoS attack also reported that firewalls and/or VPN devices contributed to outages.

It's no coincidence that the need for enterprises to support WFH and remote-work initiatives has coincided with increased attacks. The devices that are used to support those initiatives—VPN gateways and concentrators, firewalls, load balancers, intrusion detection systems (IDS), and intrusion prevention systems (IPS)—are stateful devices, meaning they contain state information that's used for things such as routing, security, and traffic management. It also means they are vulnerable to state-exhaustion DDoS attacks, and adversaries were quick to seize the opportunity.

Attacks against stateful devices likely contributed to a significant change in the top 10 DDoS attack vectors tracked in the 1H 2021 Threat Intelligence Report. There were 19 percent more TCP-based flood attacks than typical volumetric attacks, and TCP attacks are most often used against stateful devices.

As such, it's important to understand why stateful devices are targets, how they're vulnerable, and what should be done to stop DDoS attacks on stateful devices.

> *The unprecedented opportunities triggered by the COVID-19 pandemic have presented adversaries with an embarrassment of potential riches, so a much longer cycle of innovation seems likely.*
>
> – 1H 2021 NETSCOUT Threat Intelligence Report

Why Are Stateful Devices Targets for DDoS Attacks?

State-exhaustion DDoS attacks are the most prevalent kinds of attacks against stateful devices, used to take down services or the underlying network infrastructure that's responsible for delivering content to end users. These attacks work by filling TCP state tables with illegitimate connections, thereby blocking legitimate connections and denying service. Even high-capacity devices capable of maintaining state on millions of connections can be taken down by these attacks.

Because they are designed to be indistinguishable from legitimate traffic and operate at relatively small traffic volumes, state-exhaustion DDoS attacks are difficult to detect and block via traditional cloud-based DDoS protection services, which are generally designed to stop large volumetric DDoS attacks.

To better understand why attackers are targeting stateful devices, it's helpful to examine two of the most prevalent devices that have been targeted since the start of the pandemic: firewalls and VPNs.

Stateful Attack Target 1: Firewalls

A common misconception is that firewalls and other traditional edge defenses can stop DDoS attacks. Technically, they can. However, they are severely limited in their DDoS attack protection capabilities and can actually make matters worse. In fact, more than 50 percent of WISR respondents said their firewalls failed or contributed to outages caused by a DDoS attack. Moreover, 83 percent of respondents attributed network and services outages and/or crashes during a DDoS attack to their firewalls.

Stateful firewalls, for example, are designed to monitor specific aspects—or states—of network traffic streams and communications channels. These tools use stateful packet inspection (SPI) to make intelligent decisions about the potential risk of incoming traffic or resource requests. They can use past state evaluation experiences to inform future decision-making and improve accuracy. They may also integrate additional services, such as data encryption or traffic tunnels, to help boost overall security.

Owing to their comprehensive traffic evaluation frameworks, stateful firewalls excel at detecting unauthorized access attempts and malicious messaging efforts. They also offer substantive record-keeping and data-analysis benefits to help reduce ongoing risk.

However, traditional edge defenses such as firewalls are not the right solution for DDoS attack protection, for several reasons:

- The stateful nature of these devices makes them susceptible to state-exhaustion attacks.
- Firewalls offer rudimentary DDoS attack protection in the form of SYN, UDP, and ICMP flood protection. But even this limited DDoS protection impacts the performance of more important functionality, such as throughput of Layer-7 inspection, SSL decryption, and VPN termination.
- Because a firewall relies on inspection of bidirectional connections, it cannot work in an asymmetric-routing scenario in which only incoming DDoS attack packets are seen.
- Firewalls don't provide detailed visibility into dropped DDoS attack traffic.
- Firewalls cannot intelligently communicate with cloud-based solutions for mitigation of large DDoS attacks.

> *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.*
>
> – Security Risks of Stateful Network Architectures in the Digital Transformation Age, IDC

> *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.*
>
> – Security Risks of Stateful Network Architectures in the Digital Transformation Age, IDC

Stateful Attack Target 2: VPNs

As the population of those working and learning from home has increased, attackers quickly have realized the benefits of disrupting both the public-facing internet properties of enterprise organizations and the daily workplace routines of myriad employees who are dependent on remote-access solutions such as VPNs to perform critical job functions.

But although the VPN gateway has become a crucial tool during the pandemic, it's a weak link in the chain of communication from remote users to corporate resources. As such, DDoS attacks pose a major threat to the availability of the VPN gateway. Running at or near capacity, even a small DDoS attack can impact the performance of or bring down a VPN gateway. The result is that business essentially stops for the remote user.

There are two types of DDoS attacks designed to impact a VPN gateway:

- TCP state-exhaustion attacks: These are specifically designed to fill the TCP state table with bogus TCP connections. When this occurs in the VPN gateway, legitimate users cannot traverse the gateway to access corporate resources behind it.
- Network layer flooding attacks: A VPN gateway interface will typically be smaller in size than its upstream internet circuit size. As such, a DDoS attack doesn't have to be as large—only large enough to saturate the VPN gateway's network interfaces. But from the user's perspective, the corporate resources are down.

When a VPN gateway is performing poorly or is down, it can manifest itself as a network problem. As such, it can be challenging to determine the cause of the problem by using traditional network management and troubleshooting tools. What's required is smart visibility into network traffic coming into the VPN gateway that can detect traffic anomalies indicative of a DDoS attack.

Although enterprises are gradually moving employees back to the office, the reality is that many companies still support a significant WFH population, and the expectation is that many employees will permanently shift to a hybrid WFH environment. Meanwhile, WFH initiatives have created an expanded footprint for attackers to leverage by setting up new botnets for launching bigger and more expansive DDoS attacks.

> *The firewall is a session-based device that isn't designed to scale to millions of connections-per-second (CPS) to defend against large volumetric DoS attacks.*
>
> – Palo Alto TechDocs, Firewall Placement for DoS Protection

DDoS Mitigation: It's Good for Business

The overarching goal of DDoS attacks—regardless of their form—is to attack and disrupt business. As such, businesses should view DDoS mitigation as business enablement. In fact, the benefits of DDoS mitigation correlate with several business objectives:

- **Driving business growth via online experiences:** Ecommerce sales grew by 28 percent during 2020. In the United States, ecommerce sales are projected to continue double-digit growth to surpass $1 trillion in 2022. For that growth to continue, it's vital that businesses have constant, reliable, and fast connectivity for demanding online shoppers. The dependence on digital innovation has been seen across almost all verticals during the pandemic, encompassing everything from healthcare to restaurants. Users are highly affected by any annoyance, disruption, or distraction in these digital experiences, meaning companies have to constantly protect against damaging DDoS attacks.
- **Meeting service-level agreements (SLAs):** As WFH initiatives continue, people expect fast, reliable service from the companies that provide connectivity. Communications service providers (CSPs) and cloud service providers have long known the pressure of meeting SLAs and the costly impact that just a few minutes of disruption can have on business operations. Any business that provides such services to customers is under pressure to avoid service disruption from DDoS atatcks and meet customer expectations.
- **Promoting productivity in WFH environments:** Companies have had to make significant investments to remote-work infrastructure—virtual desktops, VPNs, conferencing systems, and more. In many cases, companies also moved workloads and access to the cloud. Service disruption from DDoS attacks creates the potential for costly work delays that impact a significant part of the workforce.

> *DDoS attacks are simple: flood a resource with traffic until that resource overloads and becomes non-functional. Some attacks require vulnerabilities in the end system, while others simply require brute force. The availability of rental botnets and simple tools has made it simple for anyone to launch an attack, and the scale of the attacks is growing rapidly.*
>
> – DDoS Prevention Appliances Biannual Market Tracker: H1 2020, Omdia

What Should Be Done to Stop DDoS Attacks on Stateful Devices?

Because firewalls, VPNs, and other stateful devices are incapable of defending themselves against state exhaustion attacks, what's needed is an intelligent DDoS mitigation solution that operates in a stateless/semi-stateless manner. The solution should provide a first line of defense against DDoS attacks, while also detecting and stopping outbound indicators of compromise (IoC) that have evaded an organization's network cybersecurity stack.

Such intelligent DDoS mitigation solutions should have the following features:

- They should provide easy integration into the cybersecurity stack and processes.
- They should include stateless DDoS protection that is deployed north of the firewall to protect it and other stateful devices and the services behind them from going down.
- Stateless DDoS protection also should be deployed in front of the VPN, to stop inbound DDoS attacks, protect the availability of the VPN, and enable remote-use access.
- When stateful inspection is required—for example, intercepting a TCP connection with a challenge to verify a legitimate connection—it should be short-lived and ephemeral in nature.
- Using stateless packet processing technology at the network edge is not only good for DDoS attack protection, but it also can serve to stop inbound reconnaissance and brute-force password attacks.
- Stateless inspection technology performs better for blocking both inbound and outbound IoCs. As such, this functionality can be offloaded from the stateful firewall, preserving its resources for other tasks.

Learn more about how to protect your company and remote workers and resources from DDoS attacks, or contact us today.

> *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.*
>
> – Security Risks of Stateful Network Architectures in the Digital Transformation Age, IDC

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

© 2021 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.