Protecting Your Stateful Devices

DDoS attacks are rising so much that for the first time in history, the annual number of observed DDoS attacks crossed the 10 million attack threshold, with NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) seeing 10,089,687 attacks over the course of the last year. Furthermore, as the pandemic lockdown took effect last spring, cybercriminals launched 929,000 DDoS attacks in May, the single largest number of monthly attacks we've ever seen. These attacks targeted critical work/learn-from-home stateful infrastructure such as firewalls and Virtual Private Network (VPN) concentrators.

Challenge

The attackers are not only increasing their frequency, but they are also increasing the complexity. 58% of Worldwide Infrastructure Security Survey (WISR) enterprise respondents are now reporting multi-vector attacks, which is up from 38% a year earlier. There was an attack recorded in the 2nd half of 2020 that employed 26 attack vectors in a single attack, which is a new record. These complex attacks are a dynamic mixture of state-exhaustion, volumetric and application-layer attacks. An attacker will run multiple attack types at the same time or alternately, which makes it hard to defend.

Increases in how networks are accessed by users and other devices during the rise in work-from-home populations due to the pandemic, are also a contributing factor to the breakdown of business continuity. The cybercriminals know corporations are more exposed while employees are working remotely and that's all the motivation they need to launch targeted attacks, which can crash servers and burden systems of any size. Some of the typical targets for the bad guys are stateful devices like firewalls and VPN devices. In fact, 83% of WISR enterprise respondents reported DDoS attacks in which overloaded firewalls and/or VPN devices contributed to an outage, which is up 21% from 2019.

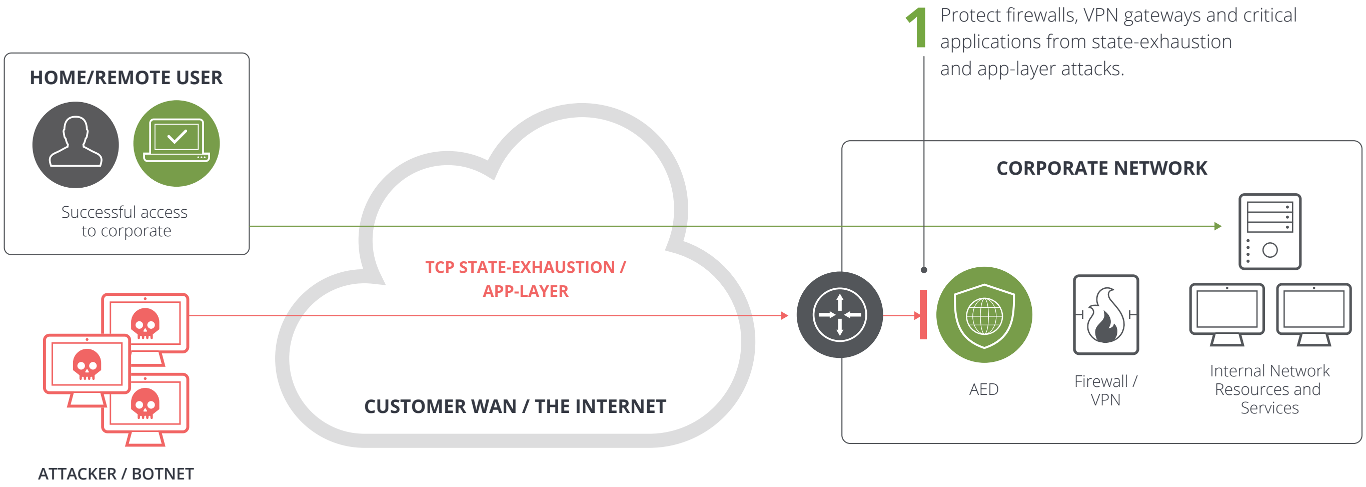
Threat

Firewalls, VPNs and other security products are essential elements of a layered-defense strategy, but they are designed to solve security problems that are fundamentally different from dedicated DDoS detection and mitigation products. The problem is that Firewalls and VPNs are typically stateful devices. Being stateful means they are using tables to collect connection details like IP addresses, ports and timestamps. The memory for these tables is limited, and even high-performance devices capable of handling millions of connections are vulnerable to flood type attacks that are designed to overwhelm these systems, which means they are vulnerable to DDoS attacks and often become the targets themselves. Since many stateful devices are also targets or partial targets of multi-layered attacks, they also require protection. Even a low-volume attack can exhaust resources on VPN concentrators and firewalls. Crafted attack volumes as low as a couple of Mbps can bring network firewalls to a point where they can't handle any newer connections.

To have adequate protection against DDoS, you need a solution that can protect against all types of attacks and guard your stateful devices.

Risk

The availability of business-critical services is essential — and not just to avoid loss of revenue. Availability of services also strengthens the company's reputation in a market and contributes to sustainable business success. Cyber resilience refers to an entity's ability to continuously deliver an intended outcome, despite adverse cyber events. Adverse cyber events are those that negatively impact the availability of networked IT systems plus associated information and services.


1 Protect firewalls, VPN gateways and critical applications from state-exhaustion and app-layer attacks.
HOME/REMOTE USER
Successful access to corporate
TCP STATE-EXHAUSTION / APP-LAYER
CUSTOMER WAN / THE INTERNET
CORPORATE NETWORK
AED
Firewall / VPN
Internal Network Resources and Services
ATTACKER / BOTNET

VPNs

Historically, VPNs weren't in constant use, but they've become the backbone of business during the COVID-19 pandemic. This means companies are far exceeding standard capacities and straining access to critical applications and resources. Now more than ever, a relatively minor DDoS attack could bring down a VPN gateway, causing the business to shut down for remote, home-based users. As pandemic lockdowns get lifted and society comes back to normal, many organizations will still offer at least a hyrbid, work-from-home environment thus maintaining the importance of protecting the VPN gateway.

Firewalls

Firewalls act as policy enforcers to prevent unauthorized access to data. While such security products effectively address "network integrity and confidentiality," they fail to address a fundamental concern regarding DDoS attacks—"network availability." A Next-Generation Firewall (NGFW) is a cybersecurity solution to protect network fronts with capabilities that extend beyond traditional firewalls. While traditional firewalls detect suspicious traffic and block network access based on a predefined blacklist, NGFWs include additional features such as intrusion prevention and deep-packet inspection. That said, even NGFWs do not provide adequate protection at this point, and they are often themselves the target.

Mitigation

Arbor Edge Defense® (AED) is an on-premise, always-on, stateless, DDoS-specific, mitigation solution. AED can identify and mitigate attacks up to 40 Gbps, and because of its stateless design, it is not susceptible to state-exhaustion attacks that target stateful devices such as VPN gateways, firewalls or load balancers. AED is designed to sit on the edge of the network between the Internet and your network's stateful devices and protect them from the very attacks designed to take them down. In the event of a large volumetric attack that's designed to saturate the Internet circuit, AED's cloud signaling feature will automatically route traffic to a cloud-based, DDoS-protection like NETSCOUT Arbor Cloud or one from your ISP.

In general, AED can eliminate the DDoS threat and the danger to your stateful devices all while assisting your organization in continued efforts to maintain availability to business-critical applications and services.

Summary

DDoS attacks are obviously increasing in frequency and complexity when measured by the amount and variety of vectors involved in each attack. And now that more employees are working from home due to the pandemic, attackers are taking advantage of the increased threat surface provided by VPN devices and firewalls. In fact, even though these devices are an integral part of the security stack and the network protection strategy, outages have increased around targeting of these stateful devices. If it has not already, this increase in attacks will degrade the availability of your services for your end users or customers, which will affect your bottom line. The best practice for DDoS protection is a hybrid approach, which includes a cloud-based and on-premise, in-line, stateless, DDoS-protection solution like AED to protect your stateful devices from further attacks.

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.