Visibility for Protecting VPN Availability and Assuring Performance

With NETSCOUT nGeniusONE and Arbor Edge Defense

Unprecedented and unforeseen. The COVID-19 pandemic has driven governments worldwide to issue shelter-in-place orders, forcing a sudden, massive workforce migration from corporate offices to working from home. Now, Virtual Private Networks (VPNs) constitute vital connectivity for remote workforces that cannot function without a way to connect laptops, tablets, phones, and workstations to critical business applications.

This explosive growth has led to quick saturation of VPN bandwidth, and IT and security teams must find a way to protect availability and assure performance of the network and application services employees need to conduct business. Of course VPN availability is crucial. However, the employees' quality of experience is equally important. Poor performance using applications over the corporate VPN is both inefficient and frustrating from the user's standpoint. User experience for at-home workers needs to match the high quality they were accustomed to in their offices.

Issue

Building a robust VPN support strategy needs to go well beyond adding VPN bandwidth to alleviate performance and access degradation. Rather, IT teams must be able to quickly analyze resource consumption, prioritize essential services, troubleshoot performance, evaluate end-user quality of experience, protect VPN gateways from cyber attackers eager to target this new opportunity.

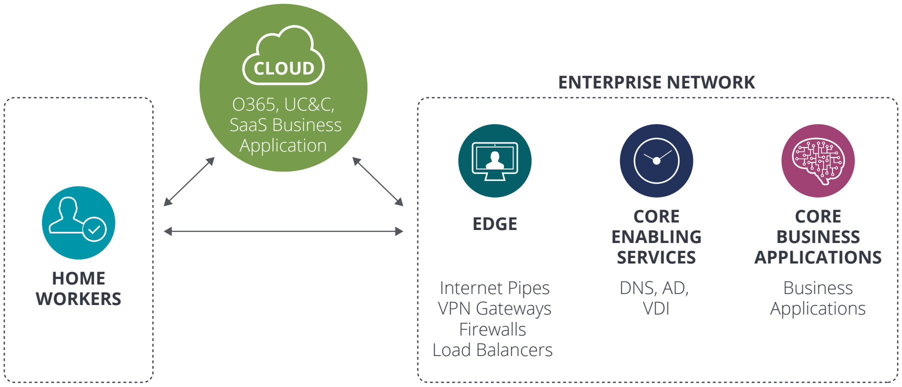


Figure 1: VPNs have become a crucial link for remote workers accessing corporate resources to do their jobs.

TWO BASIC SCENARIOS

Visibility is crucial for all of these challenges, as shown by highlighting two basic scenarios:

- Rapidly finding and fixing the source of performance problems causing traffic slowdowns and bottlenecks through VPN gateways.
- Accurately identifying whether the root cause of application access timeouts is lack of capacity or a volumetric DDoS attack.

Solving these problems rapidly requires visibility across a number of environments, as performance issues can be found both inside and outside the VPN gateway.

Having nGeniusONE® Service Assurance solution and Arbor Edge Defense (AED) available will provide answers that will help IT and security teams get to the root cause quickly. Consider the following:

- Performance issues that can impact remote employee's experience aren't always apparent internally. Having the right metrics to see packet loss outside the VPN gateway is an important indicator of upstream performance issues, such as with a cloud provider. For example, when the VPN gateway is sandwiched between points of InfiniStreamNG visibility on either side, we see packet loss happening at the front door.
- VPNs can falter when demand exceeds capacity. DDoS attacks, specifically TCP state exhaustion attacks, can have the same effect. IT needs to have visibility and the ability to identify both.
- Not all traffic is business critical, and IT needs metrics to analyze the various applications and services making up the traffic volume coming through the VPN. Metrics also help companies hone and articulate remote access policies. For example, something as simple as constant communication about which applications require VPN access and those that do not can have a positive effect.
- Traffic metrics allow organizations to make better-informed decisions. For instance, should non-business traffic like streaming music, TV, or movies be discovered, IT may choose to either add VPN capacity or implement a split tunneling strategy to offload that Internet traffic and reduce consuming corporate bandwidth resources.
- Are the capacity limits of your VPN gateway accurately reflected in performance or does performance degrade with a lower-than-expected usage rate? If so, IT needs visibility into what's driving that saturation and what can be done to reduce the volume.
- Resident DDoS alert and mitigation capabilities mean that IT does not have to wait for notification from a cloud provider.

Impact

The impact for enterprises and government agencies with a completely remote workforce is stark: No access, no business. The reality is, companies can no longer survive in an analog world, and companies must find a way to support this new normal. Think of the day-to-day operations of a bank, for example. Bank employees and their customers depend on online services across the entirety of the financial spectrum: loan and mortgage applications and processing; investment management; moving funds between accounts; paying bills; talking to customer service representatives. All of this is online these days, and that just scratches the surface of a bank's reliance on digital applications and services.

Banks are hardly alone, and sustaining online operations is essential to both employee productivity and customer experience. Companies simply cannot afford to have traffic volume from their newly remote workforce overwhelming VPN bandwidth and creating a bottleneck for employees and customers. Nor can they afford to have DDoS attacks effectively consume bandwidth, particularly when VPN gateways are already running near capacity for many of these businesses. Even a small attack could take down the business.

When the bank is unable to process loans or payments, or a manufacturer or retailer is unable to receive orders or ship products to customers, revenue, profitability, customer satisfaction are all at risk. Visibility to quickly address these threats is essential and regardless of whether it is a performance issue or security threat, NETSCOUT® has the answer.

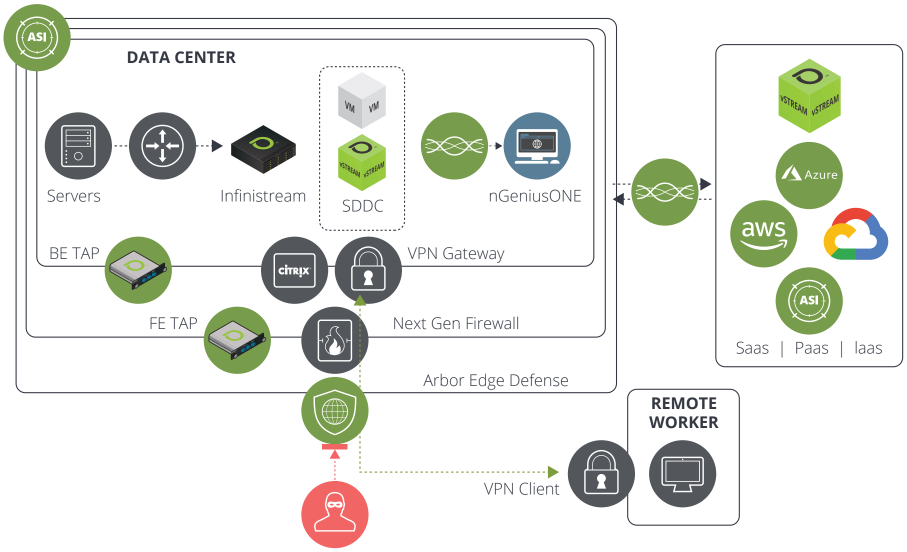


Figure 2: Network diagram showing nGeniusONE and AED visibility around the internet access circuits and the VPNs coming into the data center.

Performance Use Case – Protecting Experience of Users over VPN

To protect their quality of experience as employees working remotely communicate over Internet Service Provider (ISP) circuits into data centers and over the VPNs, organizations have implemented the nGeniusONE Service Assurance solution. With consistent, real-time monitoring and analysis, nGeniusONE and InfiniStreamNG® (ISNG) appliances provide the visibility necessary to quickly identify the source of the issue for rapid resolution of quality performance for your end-users – employees, partners, and customers alike.

Issue

For visibility into the activity from ISPs into the VPN gateways, the best-practices recommendation is to deploy the ISNGs with taps on both sides of the VPN gateway - the links coming into the VPN gateway, on the ISP side, and on the segments inside the VPN gateway (see Figure 2). From outside the VPN vantage point, nGeniusONE can:

- Measure user experience across the gateway to ensure that the gateway is not introducing latency for the users
- See what applications are being used and ensure that the VPN is not being consumed for non-business related purposes
- Detect and respond with precision to traffic problems such as packet loss
- Analyze usage patterns over time by concentrator
- Identify link saturations during busy times

nGeniusONE analysis of bandwidth usage over time will show increases in traffic volume, due to the recent shift of employees required to work from home to comply with government mandates. In this case, IT will monitor the activity to understand if their ISP circuits and VPNs can support the increased volume. Recently, increases in VPN traffic were double and even higher than what had been the pre-COVID-19 traffic volume, which could potentially surpass capacity at high traffic times during the day. nGeniusONE monitoring identifies early indicators and alerts of issues to be addressed, such as dropped packets which can be a sign of congestion and/or oversubscription.

The next step is to look at the traffic activity coming out of the VPN gateways. From inside the VPN vantage point, nGeniusONE can:

- Analyze the use of business services by user group
- Reassign user groups or VIP / Power users according to their usage
- Identify inappropriate use of business network over VPN (e.g., video and audio streaming services)
- Detect traffic that may become degraded due to concentrator resource starvation

For example, it is known that the VPN traffic has increased due to increased number of home users and nGeniusONE has detected a dropped packets issue, IT will look at the type of traffic coming across the VPN. With dramatic increases in traffic across the VPN and a shift in remote users, nGeniusONE can look at the breakdown of user application traffic while connected to VPN to determine if it is all appropriate business traffic. In both of these examples, the companies had configured full mesh VPNs and had not implemented split tunneling. In one case, it was discovered that 20% of the bandwidth was consumed by YouTube (see Figure 3). In another case, nGeniusONE revealed large amounts of the bandwidth consumed by streaming music, TV, and movie services, like Netflix, Comcast, and YouTube.

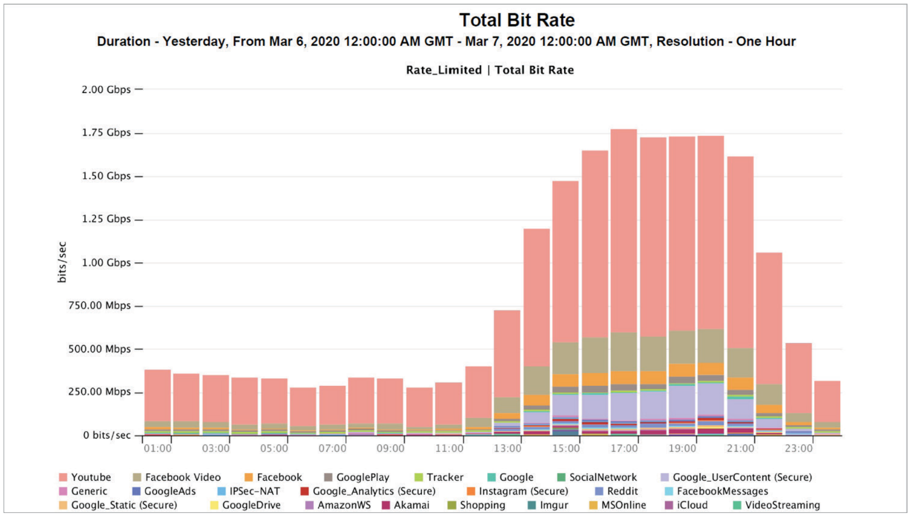


Figure 3: nGeniusONE application utilization over time, segmented by defined URLs show high YouTube utilization over the corporate VPNs.

Restoration

Using nGeniusONE traffic and application details, IT organizations can make critical decisions based on the analytical evidence provided. In both cases mentioned, employees' business use of the network was paramount, so removing the non-business traffic was the goal. In the first case, the corporate policy was NOT to use split tunneling. So, traffic destined to YouTube coming across the VPN would be routed to that URL, and the firewall was configured to block any YouTube traffic.

In the second case, where the traffic included streaming music, TV, and movies, the IT staff decided to make a configuration change to the VPN clients to allow split tunneling. This would permit the employees to connect to the essential business applications and services when they were working from home via the secure VPN. However, for other activity like Web surfing and streaming services, the traffic would be routed directly over the internet, without ever touching the corporate VPN resources.

nGeniusONE helps identify how the traffic across the VPN is being used so IT organizations can meet their goal of offering a quality end-user experience when employees are using corporate business applications. With insight into the different types of application activity, they are able to make informed decisions based on policy and practice for their organization. In the examples above, either blocking non-business traffic or choosing to configure split tunneling, the organizations have benefited from restoring bandwidth for employee business use, which is the principal requirement of their VPNs. They also preserved costs and budgets as in both cases, did not need to invest in additional capacity.

Protection Use Case: Employees Blocked from Connecting to Corporate Resources

With unprecedented large-scale work-from-home policies being enforced, the VPN gateway has become a crucial link in the chain of communication from home/remote users to corporate resources that must be protected from attacks. A DDoS attack poses a major threat to the availability of the VPN gateway. Running at or near capacity, even a small DDoS attack can impact the performance or bring down a VPN gateway. The result? Business essentially stops for the remote/home user.

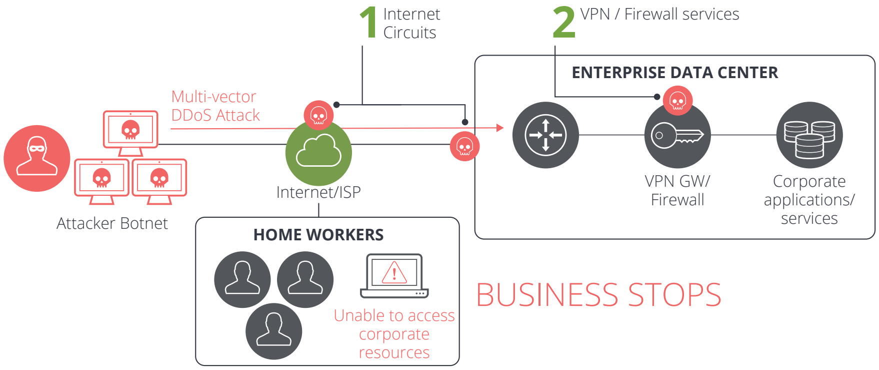


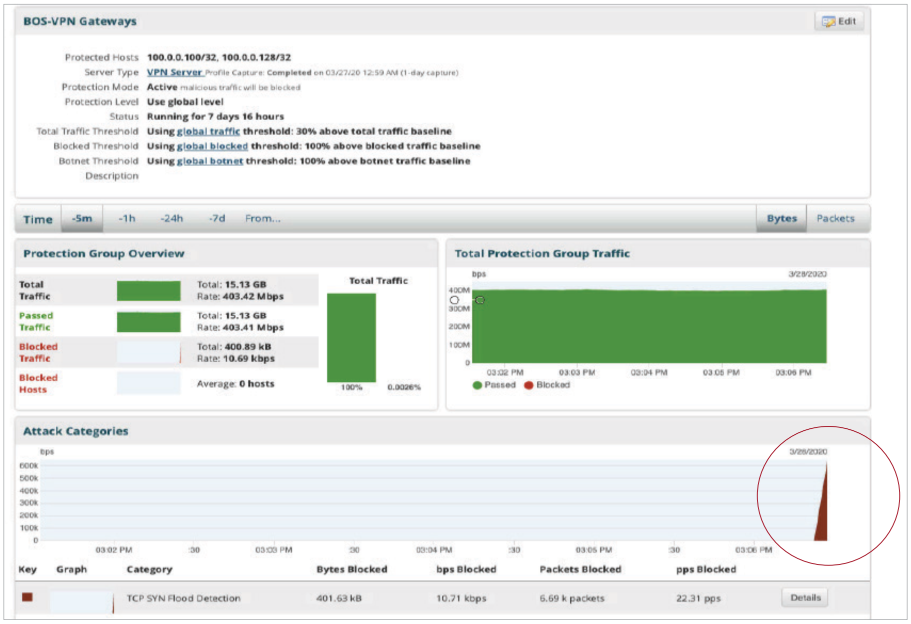
Figure 4: Multi-vector DDoS attacks deny legitimate remote workers from accessing corporate resources, effectively stopping business from being conducted.

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

- **TCP State Exhaustion attack** - A VPN gateway is a stateful device, meaning it must keep track of all TCP connections traversing through it. This is accomplished via the constant update of a finite-sized TCP state table. A TCP State Exhaustion attack (e.g., a TCP SYN Flood) is specifically designed to fill the TCP state table with bogus TCP connections. When this occurs in the VPN gateway, legitimate users cannot traverse through the gateway to the cooperate resources behind it. In other words, from the perspective of the remote/home users, those corporate resources are down.
- **Network Layer Flooding Attack** - Usually, this type of DDoS attack is in the form of a UDP flood, and it is designed to saturate the network interface of the VPN gateway. Normally, a VPN gateway interface will be smaller in size than its upstream internet circuit size. This means that a DDoS doesn't have to be as large as the internet circuit, but only large enough to saturate the VPN gateway's network interface(s). When this occurs, legitimate remote/home users cannot traverse the gateway to gain access to corporate resources and here again, from their perspective, it appears that the corporate resources are down.

Making matters worse is the fact that attackers can easily execute these two different attack vectors independently or simultaneously.

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 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 that are indicative of a DDoS attack – especially the TCP State Exhaustion and Network flooding types of attacks. NETSCOUT's Arbor Edge Defense (AED) provides the solution required. AED is an inline security appliance (or virtual device) deployed at the network perimeter, in between the internet router and VPN Gateway/ firewall. Because AED uses highly scalable, stateless packet processing technology, it is not susceptible to TCP state exhaustion attacks and others that can impact a VPN gateway.



BOS-VPN Gateways

Protected Hosts	100.0.0.100/32, 100.0.0.128/32
Server Type	VPN Server Profile Capture: Completed on 03/27/20 12:59 AM (1-day capture)
Protection Mode	Active malicious traffic will be blocked
Protection Level	Use global level
Status	Running for 7 days 16 hours
Total Traffic Threshold	Using global traffic threshold: 30% above total traffic baseline
Blocked Threshold	Using global blocked threshold: 100% above blocked traffic baseline
Botnet Threshold	Using global botnet threshold: 100% above botnet traffic baseline
Description	

Protection Group Overview

Total Traffic	Total: 15.13 GB Rate: 403.42 Mbps
Passed Traffic	Total: 15.13 GB Rate: 403.41 Mbps
Blocked Traffic	Total: 400.89 kB Rate: 10.69 kbps
Blocked Hosts	Average: 0 hosts

Attack Categories

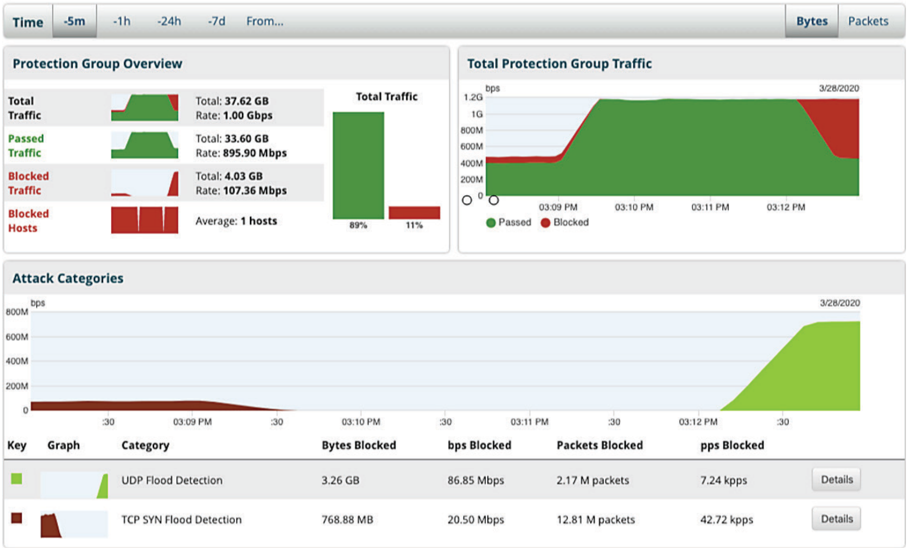
Key	Graph	Category	Bytes Blocked	bps Blocked	Packets Blocked	pps Blocked	
■		TCP SYN Flood Detection	401.63 kB	10.71 kbps	6.69 k packets	22.31 pps	Details

Figure 5: In this example, AED has detected a TCP SYN Flood attack.

Mitigation

Detecting a DDoS attack is not enough. Stopping it before it impacts the availability of the VPN gateway is what's required to maintain remote worker productivity. When AED is in an Active Blocking mode, it can automatically mitigate detected DDoS attacks. In addition to blocking the attack, AED provides real-time and post-attack details, such as attack type, size, rate, source countries/ IP hosts, protocols, and more, enabling the user to interact with and modify mitigation countermeasures as required.

AED's capabilities are highlighted below in Figures 6 through 8.



Protection Group Overview

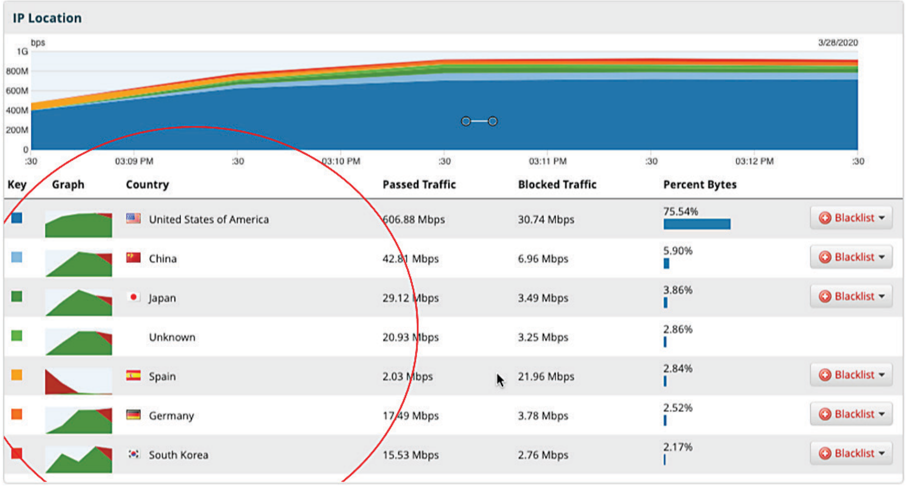
Total Traffic	Total: **37.62 GB** Rate: **1.00 Gbps**
Passed Traffic	Total: **33.60 GB** Rate: **895.90 Mbps**
Blocked Traffic	Total: **4.03 GB** Rate: **107.36 Mbps**
Blocked Hosts	Average: **1 hosts**

Total Protection Group Traffic

Attack Categories

Key	Graph	Category	Bytes Blocked	bps Blocked	Packets Blocked	pps Blocked	
🟩		UDP Flood Detection	3.26 GB	86.85 Mbps	2.17 M packets	7.24 kpps	Details
🟥		TCP SYN Flood Detection	768.88 MB	20.50 Mbps	12.81 M packets	42.72 kpps	Details

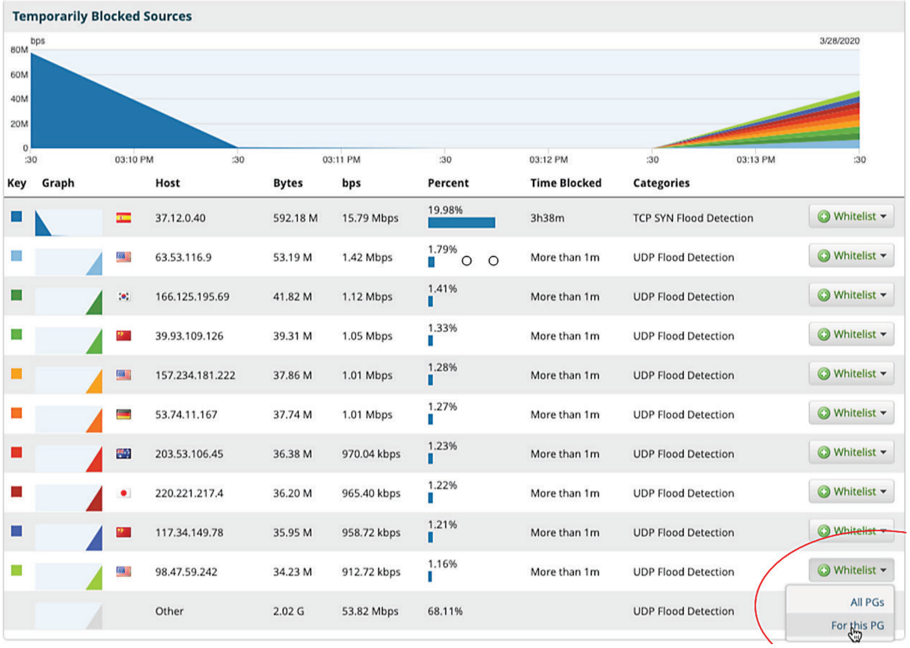
Figure 6: In this example, AED is seen blocking a 800M UDP flood attack in the upper panel, with AED providing attack details in the lower panel.



IP Location

Key	Graph	Country	Passed Traffic	Blocked Traffic	Percent Bytes	
🟦		United States of America	606.88 Mbps	30.74 Mbps	75.54%	Blacklist ▾
🟦		China	42.81 Mbps	6.96 Mbps	5.90%	Blacklist ▾
🟩		Japan	29.12 Mbps	3.49 Mbps	3.86%	Blacklist ▾
🟩		Unknown	20.93 Mbps	3.25 Mbps	2.86%	
🟧		Spain	2.03 Mbps	21.96 Mbps	2.84%	Blacklist ▾
🟧		Germany	17.49 Mbps	3.78 Mbps	2.52%	Blacklist ▾
🟥		South Korea	15.53 Mbps	2.76 Mbps	2.17%	Blacklist ▾

Figure 7: The appearance of multiple source countries indicate this is a spoofed attack coming from a botnet.



Temporarily Blocked Sources

Key	Graph	Host	Bytes	bps	Percent	Time Blocked	Categories	
🟦		37.12.0.40	592.18 M	15.79 Mbps	19.98%	3h38m	TCP SYN Flood Detection	Whitelist ▾
🟦		63.53.116.9	53.19 M	1.42 Mbps	1.79%	More than 1m	UDP Flood Detection	Whitelist ▾
🟩		166.125.195.69	41.82 M	1.12 Mbps	1.41%	More than 1m	UDP Flood Detection	Whitelist ▾
🟩		39.93.109.126	39.31 M	1.05 Mbps	1.33%	More than 1m	UDP Flood Detection	Whitelist ▾
🟧		157.234.181.222	37.86 M	1.01 Mbps	1.28%	More than 1m	UDP Flood Detection	Whitelist ▾
🟧		53.74.11.167	37.74 M	1.01 Mbps	1.27%	More than 1m	UDP Flood Detection	Whitelist ▾
🟥		203.53.106.45	36.38 M	970.04 kbps	1.23%	More than 1m	UDP Flood Detection	Whitelist ▾
🟥		220.221.217.4	36.20 M	965.40 kbps	1.22%	More than 1m	UDP Flood Detection	Whitelist ▾
🟦		117.34.149.78	35.95 M	958.72 kbps	1.21%	More than 1m	UDP Flood Detection	Whitelist ▾
🟩		98.47.59.242	34.23 M	912.72 kbps	1.16%	More than 1m	UDP Flood Detection	Whitelist ▾
		Other	2.02 G	53.82 Mbps	68.11%		UDP Flood Detection	

Figure 8: In this example, AED shows blocked hosts that are part of the attack, with the highlighted area showing how legitimate users can easily be white-listed.

AED's on premises location, stateless packet processing technology, automatic detection, and mitigation of DDoS attacks provide the best practices in defense of VPN gateways and to maintain remote/home user access to corporate resources.

Summary

Unplanned events like that of the COVID-19 pandemic demonstrate the importance of visibility for ensuring that the employees' experience using corporate application resources from home is as consistent and high quality as it was when they were working in their offices. This is about keeping enterprise businesses running and the users happy by providing IT with the information and tools they need to get this done - in a world that has changed nearly overnight. nGeniusONE and AED are the essential solutions that will help IT meet these crucial goals.

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