SDN COMMUNICATIONS.

JAN. - JUNE 2021

CYBER THREAT LANDSCAPE

Network Security Intelligence Report

EXECUTIVE SUMMARY

This report contains observations and insights from SDN's Managed DDoS Protection service and SDN Managed Firewall service. This report covers SDN services from January 1 – June 30, 2021. It represents a unique view of the cybersecurity trends SDN is seeing in the region. Sign up to receive the report twice a year at **sdncommunications.com/threat-landscape/.**

SDN MANAGED DDoS* PROTECTION: KEY TRENDS January 1 - June 30, 2021

Q1 & Q2 2021 Total Number of Attacks

6035 high alerts

The average duration of a DDoS attack during the first half of 2021 was down 39% and lasted 10 minutes on average. Conversely, the longest single attack we saw during the half was 4 hours in length.

Attack Count Year over Year

37% increase

Average Duration

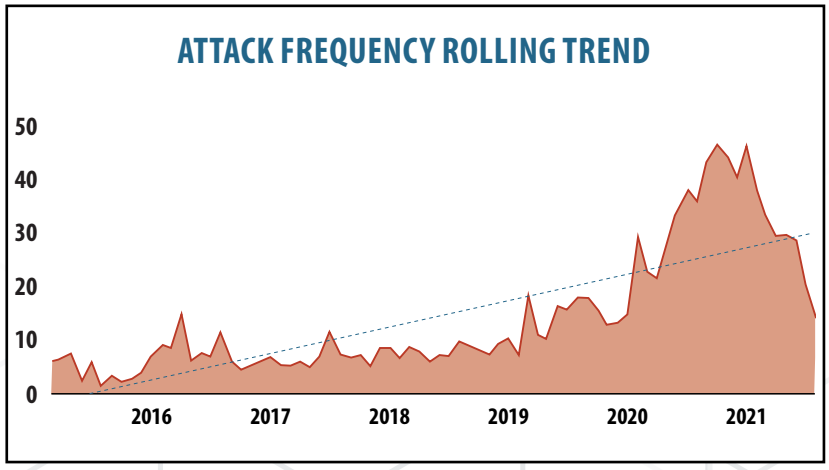
39% decrease

Average Attack Size Change**

8% decrease

Peak Attack Size**

57.6 Gbps



*As typical, we have discarded from the counts anything we believe to be a false positive such as a Global Alert, testing attacks or a high alert with only a single vector of Total Traffic – meaning the only reason it triggered is due to the high volume of traffic on the circuit.

** Attack size is the traffic crossing the network edge directed to an endpoint during the detected anomalous activity.

SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - June 30, 2021

Distributed Denial of Service attacks are nearly always multi-vector.

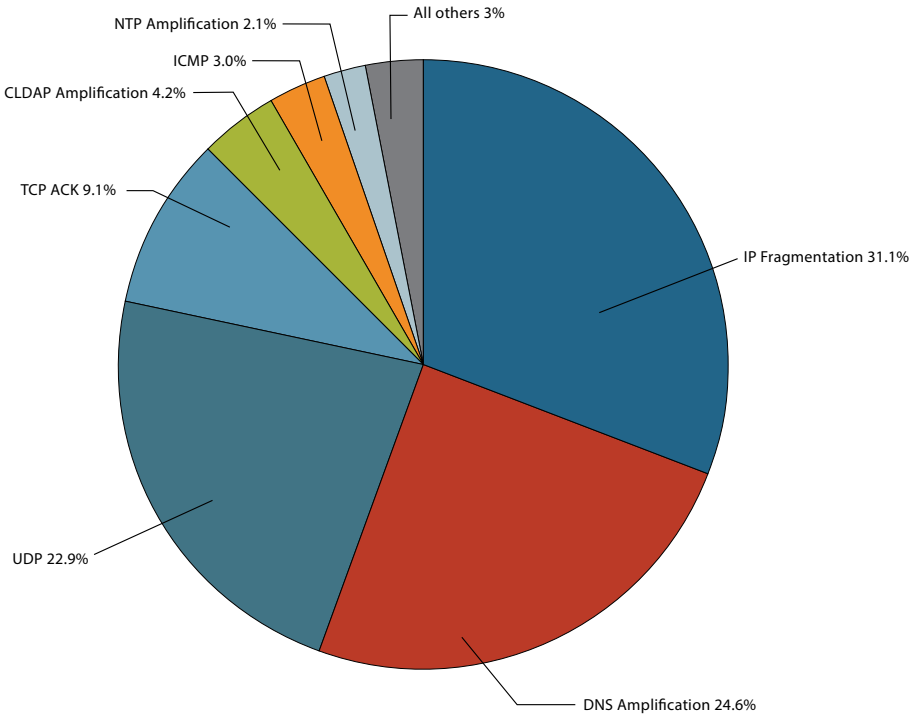
96% of all DDoS attacks in the first half of 2021 were multi-vector attacks.

In every report produced to date, DDoS attacks continue to be complex. In the first half of 2021, 96% of all attacks were multi-vector with a maximum of 11 vectors. The top five most used in the first half of 2021 are as follows:

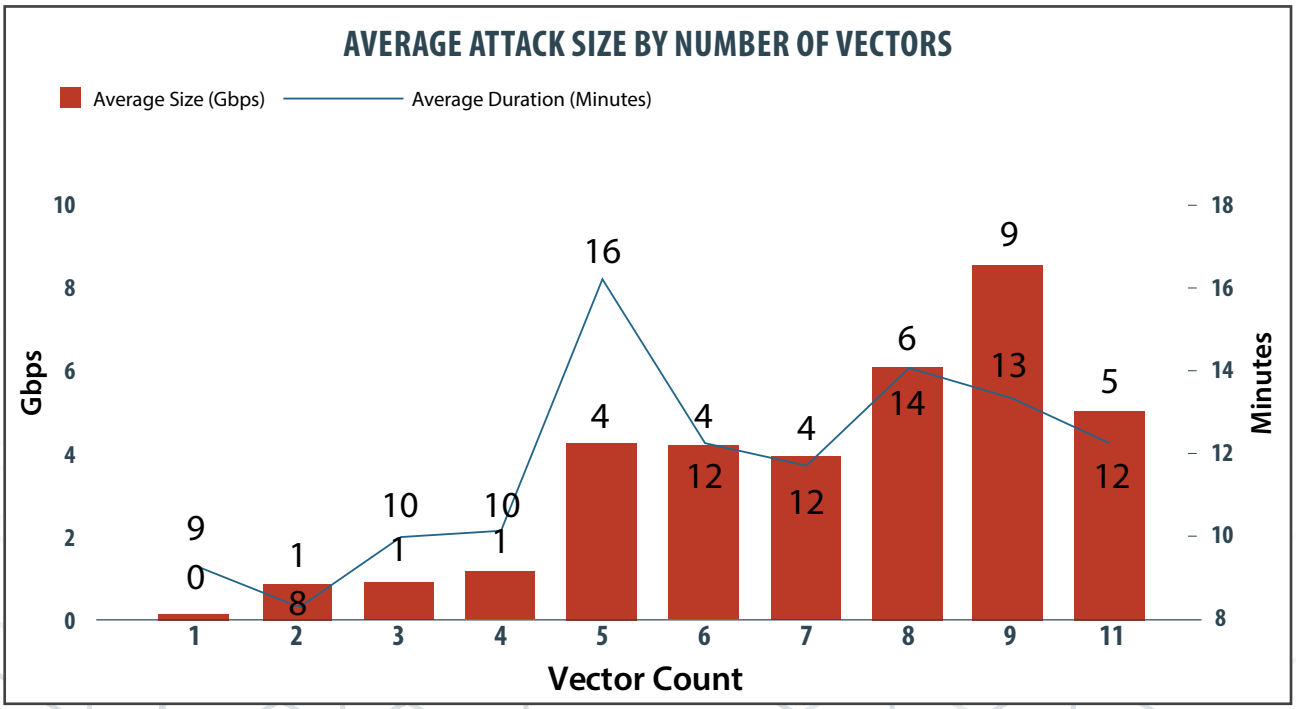
- **IP Fragmentation**
- **DNS Amplification**
- **UDP**
- **TCP ACK**
- **CLDAP Amplification**

Vector: a path or means by which a hacker can gain access to a computer or network in order to deliver a payload or malicious outcome.

2021 Q1 & Q2 ATTACKS BY VECTOR



AVERAGE ATTACK SIZE BY NUMBER OF VECTORS



The number of vectors used in DDoS attacks continues to increase. Employing five or more attacks at a time has become commonplace.

SDN MANAGED FIREWALL: KEY TRENDS January 1 - June 30, 2021

TOP ATTACKS

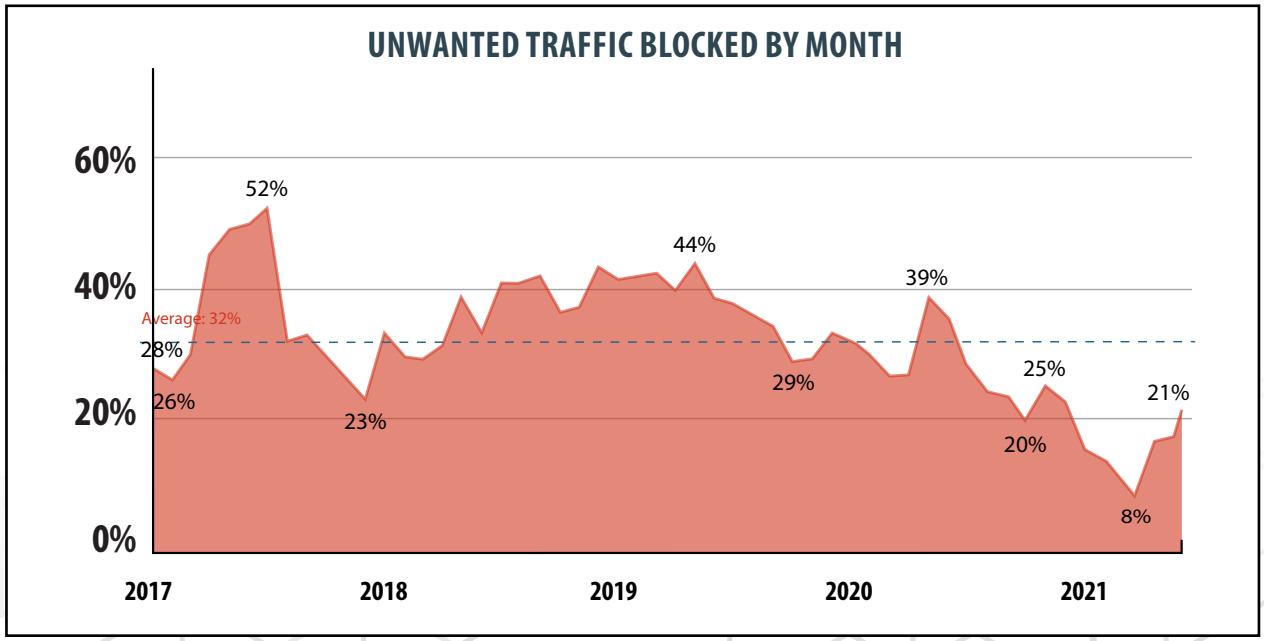
Attack Name	Impact Category
#1 SSLAnonymous.Ciphers.Negotiation	Information Disclosure
#2 udp_flood	Denial of Service
#3 Web.Server.Password.Files.Access	Information Disclosure
#4 OpenVAS.Web.Scanner	Information Disclosure
#5 Novell.NetBasic.Scripting.Server.Directory.Traversal	Information Disclosure
#6 icmp_flood	Denial of Service
#7 HTTP.URIJava.Code.Injection	System Compromise
#8 Qualys.Vulnerability.Scanner	Information Disclosure
#9 Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	System Compromise
#10 ZGrab.Scanner	Information Disclosure

Amidst increasing ransomware attacks, customer awareness of the need for additional training and managed security has also increased. In a recent survey, only 48% of respondents strongly agree with the statement "My company's telecommunications and IT systems are secure." With managed firewall, businesses can decrease the level of unwanted traffic and further insight into their network.

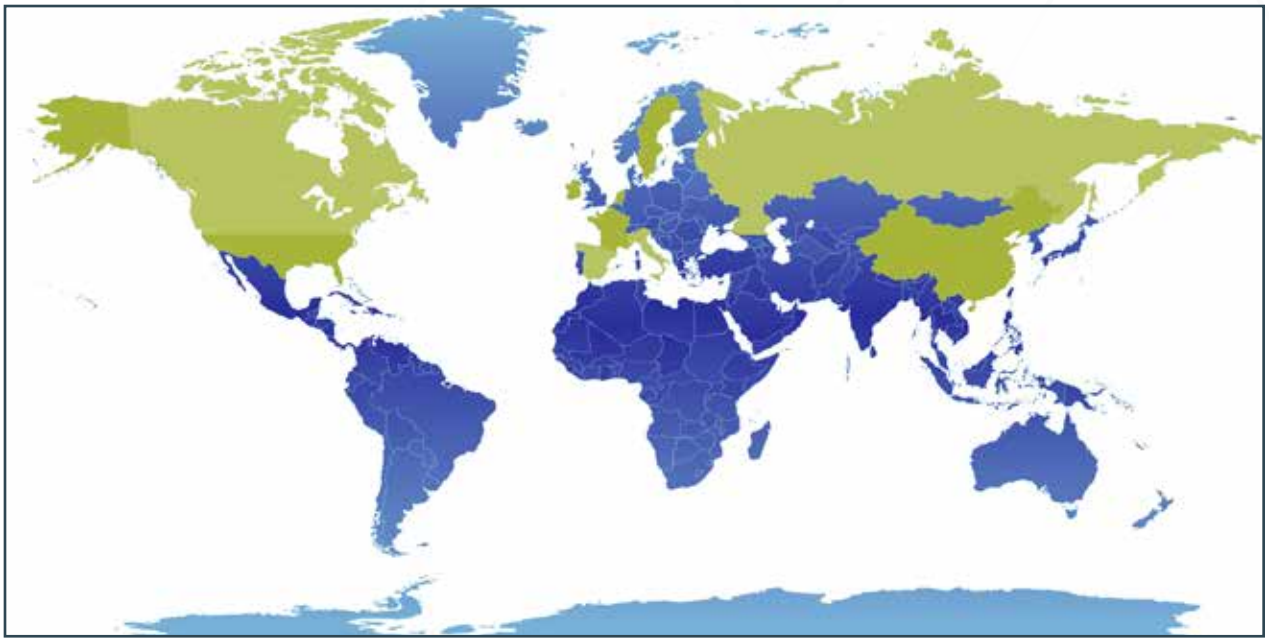
MANAGED FIREWALL PREVENTED

15.6% of all SDN Managed Firewall traffic was flagged as malicious or spam and was filtered out in Q1 & Q2.

In the first half of 2021, SDN Managed Firewalls blocked around 15.6 % of all traffic – this is down from 31.8% from the same period in 2020. However, at the same time the number of monitored endpoints increased by nearly 30% and we saw total traffic traversing all devices increase by almost 39% (38.59). This likely explains, in part, the lower percent of blocked traffic in the first half of the year. None-the-less, there was a decrease in the amount of blocked traffic in real numbers (1,442,498,441 blocked first half 2020 vs. 982,398,047 blocked first half 2021)



TOP 10 THREAT EVENTS BY COUNTRY AS SEEN BY SDN MANAGED FIREWALLS



#1 UNITED STATES
#2 RUSSIAN FEDERATION
#3 CHINA
#4 IRELAND
#5 SPAIN
#6 NETHERLANDS
#7 CANADA
#8 SWEDEN
#9 ITALY
#10 FRANCE

TAKEAWAYS

Threats originating in the United States continue to grow

In past reports our Managed Firewall data has shown that many of the threats were external to the United State. However, threats or unwanted traffic originating domestically grew to nearly 58% in the first half of 2021. That's up from just 4% when we started producing this summary back in 2017.

What does it mean? In many cases the threat actors are likely spoofing IP addresses as a means to by-pass geo location filters. But in others, they probably control compromised systems in the United States where they can originate attacks. Either way, while geo filters still have a place in layered security, they are perhaps less impactful than they were just a few short years ago.

Information Disclosure takes pole position in first half of 2021

At the end of 2020, denial of service attacks had a narrow lead over information disclosures as the top risk category reported by our managed firewalls. That changed in the first half of 2021 as information disclosures took a commanding lead as the most common threat.

This strong return in the category seems to be driven by SSL Anonymous Ciphers Negotiation which has seen almost double the number of alerts compared to all of 2020.