appgate

WHITEPAPER

SDP AND DOS ATTACKS APPROACH AND MITIGATION

Last revised September 2020

WHAT ARE DENIAL OF SERVICE ATTACKS?

Denial of Service [DoS] attacks are internet-based attacks that attempt to disrupt the legitimate operations of a machine or network service, typically by flooding the service with many concurrent requests.

While large-scale and sustained (distributed) DoS attacks have proven successful, especially against unprepared targets, there are concrete steps that organizations can take to prepare themselves and be able to better withstand this type of attack.

Appgate SDP is not a DoS mitigation solution but is an access solution so is in the front line for DoS attacks. Organizations should have a DoS mitigation plan in place which limits the number of concurrent requests hitting any ingress points including Appgate SDP. However, Appgate SDP, by design can be very effective at withstanding many potential DoS attack, while still maintaining user productivity and access availability.

WHO IS A TARGET OF DOS?

While any internet-facing service can potentially be a target of a DoS attack, historically these types of attacks have been mounted with differing objectives.

The most obvious objective is against the web site of a company or individual. Krebs on Security is a great example; he exposes bad actors in the online world and has suffered massive DoS attacks against his web site in retaliation.

Another objective is to cause commercial damage to a business that relies on its web services to deliver content and/or perform on-line transactions. The BBC suffered in this way in 2015 when a successful attack took all its content and streaming services off line.

Occasionally, companies are targeted by a competitor, although such attacks are typically restricted to the Dark Web.

Finally, there have been infrastructure attacks which do not target any one company directly (although a company may still be the intended target). Dyn, which controls much of the USA's DNS infrastructure, was attacked in late 2016. The effects were very widespread with numerous companies such as Facebook effectively knocked off-line.

In reality, anyone can be the target or the unintended victim of a DoS attack, so it is worth designing your infrastructure to provide the best resilience possible.

DOS ATTACKS AND APPGATE SDP

Appgate SDP appliances are engineered with some basic DoS attack mitigations which make it survive far better than a standard Ubuntu based server. These specifically relate to running the system with Single Packet Authorization [SPA] enabled in UDP-TCP mode.

DOS ATTACK WHEN IN UDP-TCP SPA MODE

Appgate SDP offers the option of a UDP based SPA mode to protect the Client port. UDP-TCP SPA requires a special UDP packet to be presented before iptables is updated to allow a TCP connection to be established from that specific source IP address. Only after this can a TLS session can be established. UDP packets are stateless so have the advantage of not establishing a new connection (as is the case with TCP) so impose very little loading on the target system when a new packet is received.

Appgate SDP uses UDP filtering rules in the kernel that detect any IP addresses sending too many packets per second to our UDP-SPA SPA ports (53 and 443). It is irrelevant if the packet is a valid SPA packet or not - they will be blocked regardless since they exceed the maximum allowed packet rate for a given IP.

With slower packet streams (below the kernel filtering rate) the UDP packets are handled by the Proxyd process in the Appliance, which decides if they are valid or not. We have tested the proxyd process up to the test system limit of 1M packets/second (2Gb/s). At this level it was still working as intended, with valid users able to establish new connections. Because Proxyd only has to handle the slower packet streams in this case, it then has the capacity to handle many of these (DoS) streams from different IP addresses at one time with only very limited performance degradation for users as shown in the table below.

DOS ATTACK USING TCP

In all other SPA modes (and for any open TCP ports) the operating system is the limiting factor as it can only accept so many new TCP connections per second (which can to some extent be changed with some system settings).

Appgate SDP hardware appliances (see Test Hardware for the specifications) can handle new TCP connections at a rate of about 2000/second which is at least 10 times greater than the rate at which the Appgate SDP software can accept valid new connections. After this time packets get dropped so valid users will start to see degraded performance such as increased log-in times.

A malformed TCP packet is not seen as a new TCP connection by the appliance. These are simply dropped which is not rate limited. The actual limitation in this case is the size of the pipe feeding Appgate SDP. The appliances are designed to support 10Gbit NICs; valid users would start to see degraded performance once the pipe is full.

Appgate SDP offers the option of a TCP based SPA mode to protect the Client port. SPA requires a special packet to be presented before a TLS session can be established. These TCP packets are handled by the Proxyd process in the Appliance who decides if they are valid or not.

Proxyd is a very light process which can handle far in excess of 2000 SPA packets per second. This means the operating system limit of 2000 new TCP connections per second applies in exactly the same way as if SPA was not in use.

RESILIENCY

Instead of thinking of a DoS attack from the perspective of an individual appliance it is better to consider how to deploy the Appgate SDP system as a whole.

Appgate SDP has a stateless token-based architecture. This architecture choice complements the distributed nature of

Software Defined Perimeter type solutions when it comes to DoS resiliency. There are a number of reasons for this:

- Once a user has received their tokens from a Controller, it can be taken off line until the tokens need renewal without the user noticing. An attack on a Controller may prevent new users receiving tokens but existing users will be unaffected. (Remember—Appgate SDP users are normally logged in automatically, so most users will be of the latter type).
- There is no real-time communication between appliances, so short term interference in the form of DoS attacks can go unnoticed by the appliances and their users.
- Normally, multiple Gateways are configured per Site and the Client chooses an available one automatically. An attack on a Gateway will go unnoticed by new users who will simply connect to alternative one on that Site.
- For established Gateway sessions Appgate SDP supports (stateful) failover. This is Client-based, so a sudden attack on a Gateway effectively removes it from the available Gateways on a Site. Established users will simply be switched to another available one on that site—even preserving the state of their connection if that feature is enabled.

MITIGATION

Proper mitigation of large-scale (D)DoS attacks can only be handled at ISP level or in extreme cases the internet backbone providers. These should block the worst of any attack, but for what remains there are some other steps which you can take to further mitigate the likelihood of a successful attack.

1. Use SPA in UDP-TCP mode.
   - Kernel level filtering removes fast DoS attacks and no TCP connections are established for slow ones.
2. IP Address based deployment of the Appgate SDP system Configure the system to use IP addresses instead of DNS names. This has two benefits:
   - Any DoS attack against DNS providers will be ineffective since the system does not rely on DNS.
   - Unlike Controllers, Gateways are only known inside the Appgate SDP system. Not even (normal) users are aware of the hostnames or IP addresses of the Gateways. By using IP addresses, the attackers will have no knowledge of what to attack in the first place.
3. Auto-scaling of Gateways.
   - The Appgate SDP system uses live entitlements so users are not required to log-out/in when things change. This means that the load on the Gateways can be monitored and when a certain limit is reached (such as during a DoS attack) then new Gateways can be auto-provisioned. Any established users will automatically be switched to the new instances. And the attackers, being unaware of these instances will not be able to divert their attack.
4. Appliance monitoring
   - Undertake some basic monitoring of the appliances and instigate some form of traffic re-direction before the problem becomes too severe. The recommended way of doing this is to monitor the appliance with SNMP for incoming drops for a given NICs (number 1...N) and for CPU use. ie the following object identifiers (OIDs):
   - RFC1213-MIB::ifInDiscards.X
   - UCD-SNMP-MIB::ssCpuUser.0
   - UCD-SNMP-MIB::ssCpuSystem.0
   - UCD-SNMP-MIB::ssCpuIdle.0

If the discards are rapidly increasing it is very likely that the machine is being hit by a DDoS attack—or (a lot less likely) the machine is trying to handle more valid user traffic than it can handle. If it's a DDoS attack the CpuUser + CpuSystem time will be very low (<5%) while CpuIdle < 90%. The exact limits are hard to say as it depends on actual hardware/cloud instance being used. Monitoring these four values and adjusting alarms based on what is normal use will be the easiest way to infer that a DDoS attack is underway.

DOS ATTACK METRICS

See Test Hardware for details of the machine used to obtain these metrics.

PORT 443 & 53 (UDP) UDP-TCP SPA

All SPA UDP-TCP (D)DoS tests were performed with valid SPA packets (which is the worst case regarding CPU usage). Test were performed on both the Controller (sign-in times) and the Gateway (throughput).

TEST A: CONTROLLER TEST – USER LOGINS

Signing in 10,000 users, 20 in parallel processes (500 user each) over a period lasting approximately two minutes, while the attacks where ongoing:

DOS TRAFFIC (PACKETS/SEC)	DOS SCENARIO (NO. OF IP ADDRESSES SENDING TRAFFIC)	AVG. SIGN IN TIME (MSEC)	CPU LOAD (% TOTAL)
0	N/A	343	40
500K	1	364	38
1M	1	380	36
500K Fast rate	128	361	42
1M Fast rate	128	371	44
500K Slow rate	64.000	366	44
1M Slow rate	64.000	404	48

TEST B: GATEWAY TEST: THROUGHPUT

It should also be remembered that tokens also require renewing 24 users perform uploads and then downloads at 300Mb/s per user, while the attacks were ongoing against the Gateway:

The same DoS scenarios were used, and the results showed no measurable difference in up/download speed. This is the expected result as the up/download traffic uses ~7.2Gb/s, and the DOS traffic @ 1Mp/s uses <2Gb/s; which is supported on a 10GbE network.

PORT 443 (TCP) NO SPA

DOS TRAFFIC	GOOD TRAFIC	LIMIT	EFFECT/CAUSE
Invalid TCP packets	Establish a valid new connection	Network Bandwidth	TCP packet drops because of bandwidth issues
Valid TCP Packets	Establish a valid new connection	2,000 connections/ second*	Valid clients take longer to connect

*The tester clients signed in to local accounts in the Controller's

PORT 443 (TCP) TCP SPA

DOS TRAFFIC	GOOD TRAFIC	LIMIT	EFFECT/CAUSE
Invalid TCP packets	Establish a valid new connection	Network Bandwidth	TCP packet drops because of bandwidth issues
Invalid SPA Packets	Establish a valid new connection	2,000 connections/ second*	Valid clients take longer to connect
Valid SPA Packets	Establish a valid new connection	2,000 connections/ second*	Valid clients take longer to connect

PORT 444 (TCP) WITH NO IPTABLES WHITELIST (FOR APPLIANCES)

DOS TRAFFIC	GOOD TRAFIC	LIMIT	EFFECT/CAUSE
Invalid TCP packets	Establish a valid new connection	Network Bandwidth	TCP packet drops because of bandwidth issues
Valid TCP Packets	Establish a valid new connection	2,000 connections/ second*	Valid clients take longer to connect

PORT 444 (TCP) WITH IPTABLES LIMITING TO ONLY KNOWN IPS

DOS TRAFFIC	GOOD TRAFIC	LIMIT	EFFECT/CAUSE
Invalid TCP packets	Establish a valid new connection	Network Bandwidth	TCP packet drops because of bandwidth issues
Valid TCP Packets	Establish a valid new connection	Network Bandwidth	TCP packet drops because of bandwidth issues

TEST HARDWARE

For testing the following machine specification was used:

MORE INFORMATION

There is a Secure Deployment Technical Whitepaper which provides more information about reducing the exposure of the Appgate SDP to the Internet. There are a number of recommendations, several of which should be implemented as part of any DoS hardening exercise.

There are additional resources on the Appgate website here: www.appgate.com/software-defined-perimeter

And the Appgate SDP product documentation is available here:

Admin Guide: https://sdphelp.appgate.com/adminguide

Client User Guide: https://sdphelp.appgate.com/userguide