BIGIP - L3/4 DDoS

BEST PRACTICES

Christopher Gray - cgray@f5.com
Senior Product Management Engineer

June 5, 2020

Problem

DoS / DDoS configuration is hard to do successfully.

New attacks come out daily, so the need to keep up with them is difficult.

Only people / teams that specialize in DDoS will understand the needs for certain configurations to mitigate attacks.

Extensive Testing is critical to confirm mitigations work effectively.

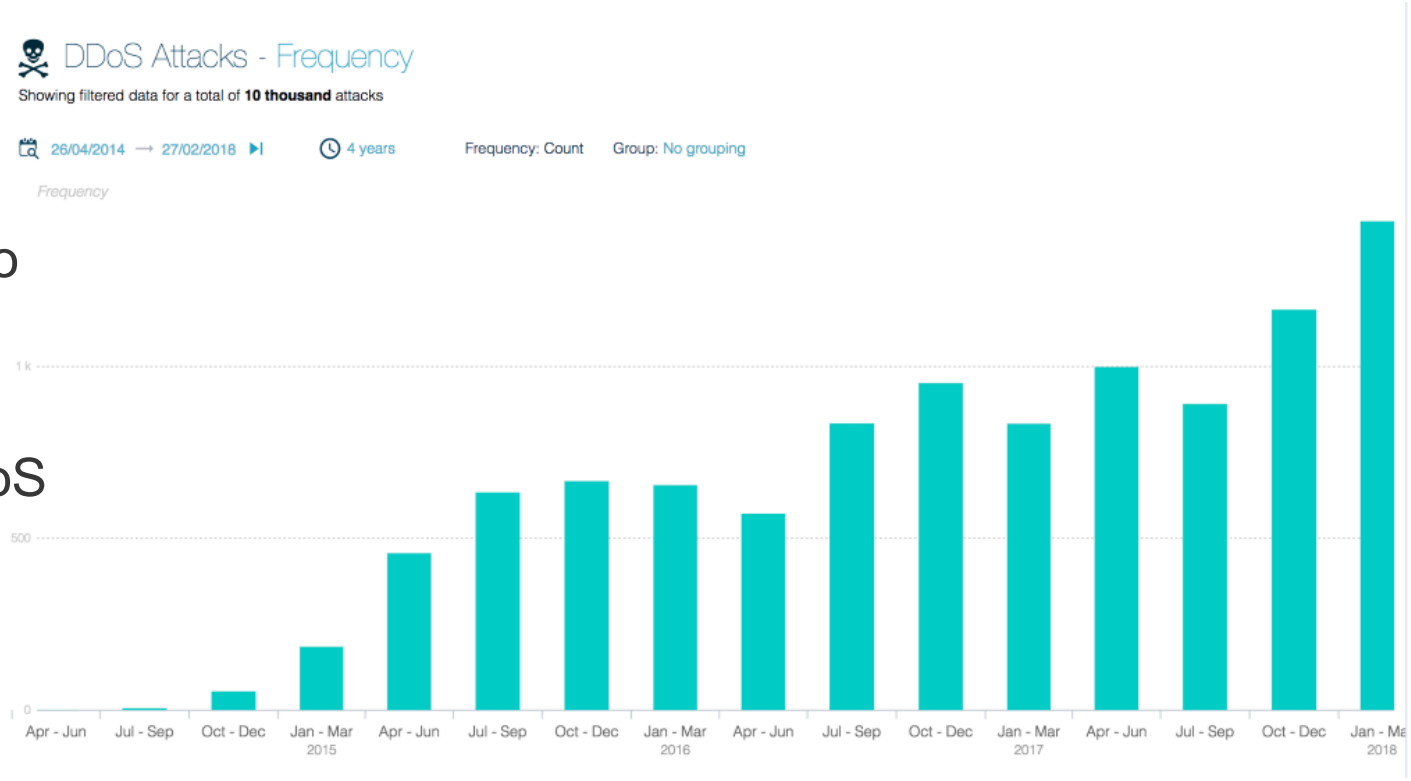


Image Source: https://www.netscout.com/blog/asert/1-terabit-ddos-attacks-become-reality-reflecting-five-years

Why is DDoS important?

AMPLIFICATION FACTORS MATTER

With VERY little input, an Attacker could amplify their attack up to **51,000X** from the original packet.

Plus that original packet can and will be spoofed, because its UDP

New exploits to old protocols come out roughly every 2 months.

Staying up to date is paramount!

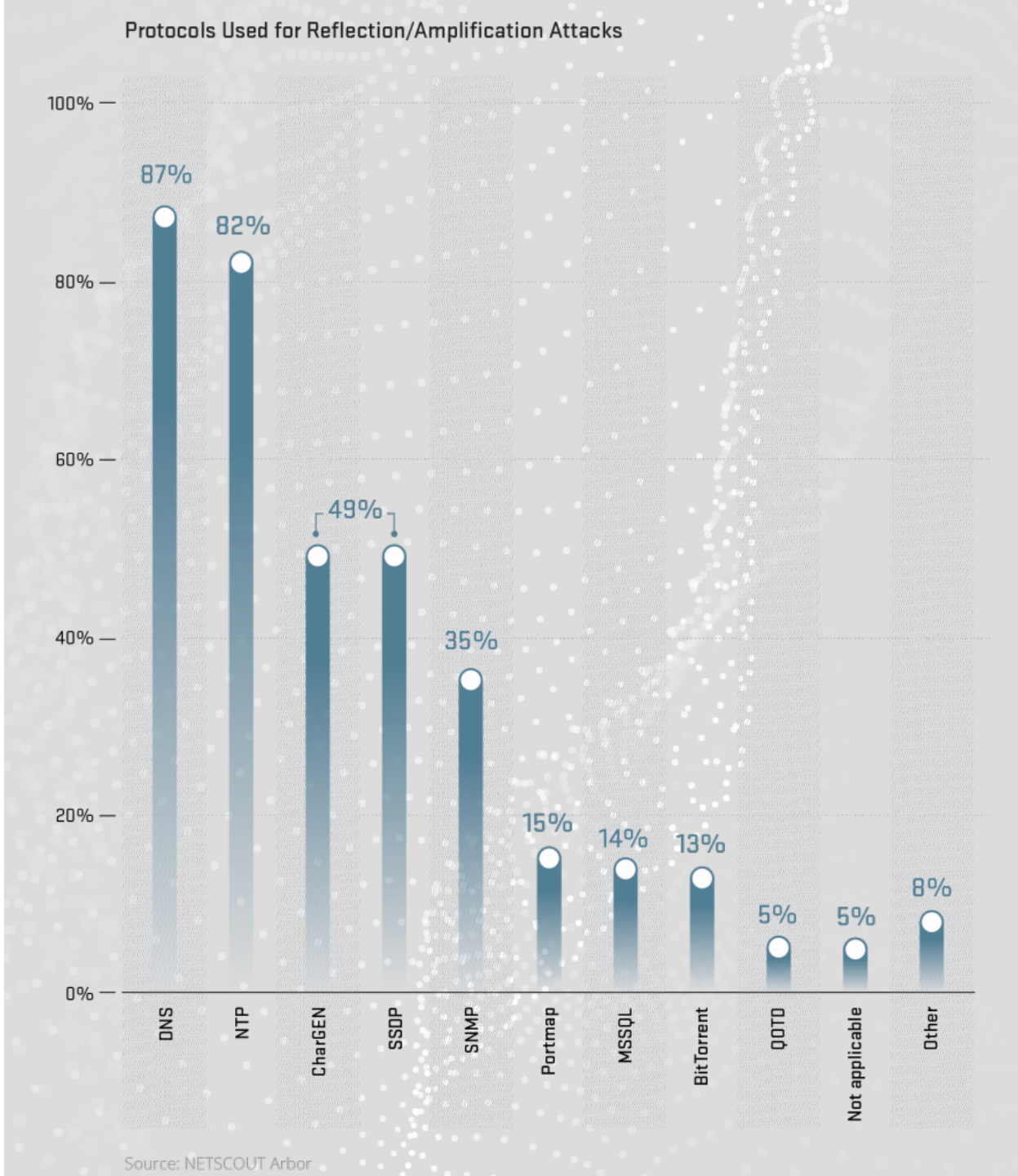
Protocol	Bandwidth Amplification Factor	Vulnerable Command	Port(s)
DNS	28 to 54	see: TA13-088A	53
NTP	556.9	see: TA14-013A	123
SNMPv2	6.3	GetBulk request	161
NetBIOS	3.8	Name resolution	137
SSDP	30.8	SEARCH request	1900
CharGEN	358.8	Character generation request	19
QOTD	140.3	Quote request	17
BitTorrent	3.8	File search	6881
Kad	16.3	Peer list exchange	751
Quake Network Protocol	63.9	Server info exchange	26000
Steam Protocol	5.5	Server info exchange	27015
Multicast DNS (mDNS)	2 to 10	Unicast query	5353
RIPv1	131.24	Malformed request	520
Portmap (RPCbind)	7 to 28	Malformed request	111
LDAP	46 to 55	Malformed request	389 T
CLDAP	56 to 70	-	389
TFTP	60	-	69
Memcached	10,000 to 51,000	-	11211
WS-Discovery	15,000	-	139,445
		-	1124, 3702
Apple Remote Desktop	35.5	-	3283
Windows Remote Desktop Gateway (RD Gateway)	?		3391

Multi protocol / vectors

OPTIONAL SUBTITLE PLACEHOLDER

DDoS attacks are no longer only large UDP attacks.

Many protocols, vectors, packet payload sizes, payloads are used to bring down a victium network / service.



Solution (s)

THERE IS NO SILVER BULLET TO DDOS MITIGATION

Because BIGIP is a robust security platform, there are several different features that together make a harden attack surface optimized for L3/4 DDoS mitigation.

The following are these areas:

DDoS Protected Objects (Generic / ISP Focused)

DDoS DNS Profiles

Global (Device) DDoS Policy

Firewall – DDoS Policies

Firewall - Rules

Traffic Groups

Eviction Policies

Port Misuse Policy

IPI (IP Intelligence) – External feed lists

IPI (IP Intelligence) – Exclude & Include categories

IPS (DDoS specific) Profile

FPGA DDoS Optimized settings

Timer Policies

TCP / UDP / IP Other – Policies

Fast Layer 4 Profile

Address and Port lists

Easy button?

I have created a (growing) number of automation scripts which can be run on the BIGIP to provision it in a way that is optimized for DoS & DDoS Mitigation.

In the initial phase, the propose is ONLY for a internet facing DDoS scrubbing solution / device. This is due to the number of Firewall rules being used which are hostile to intra network communications.

These scripts provision ALL of the previous slides area's, including preconfigured Virtual Servers with different DDoS and other "Catch All" use-cases.

The scripts are on my personal GitHub and can be found here:

https://github.com/c2theg/F5_DDoS_BP

Script details and roadmap

The GitHub page is a living document which includes all the details need to deploy the configuration directly on a BIGIP. You will need to SSH into the BIGIP to provision this.

”Catch All” Virtual Servers are helpful to mitigate attacks and provide visibility for customers that might be missing specific DDoS profiles / protected objects.

A future release will allow for remote deployments of this config but will be in a different GitHub repo. This will likely use a combination of AS3 declarative provisioning, along with REST API calls

Additionally, a BIGIQ – AS3 & REST provisioning script will be added in the future.

Please send any feedback you might have with this script!