RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: LAB3-W10

How to Design and Operate a DDOS Testing Program

Murray Goldschmidt

Chief Operating Officer
Sense of Security Pty Ltd
senseofsecurity.com.au
@ITsecurityAU

Sharjil Khan

Principal Consultant
Redwolf Security Inc
redwolfsecurity.com
@redwolfsecurity

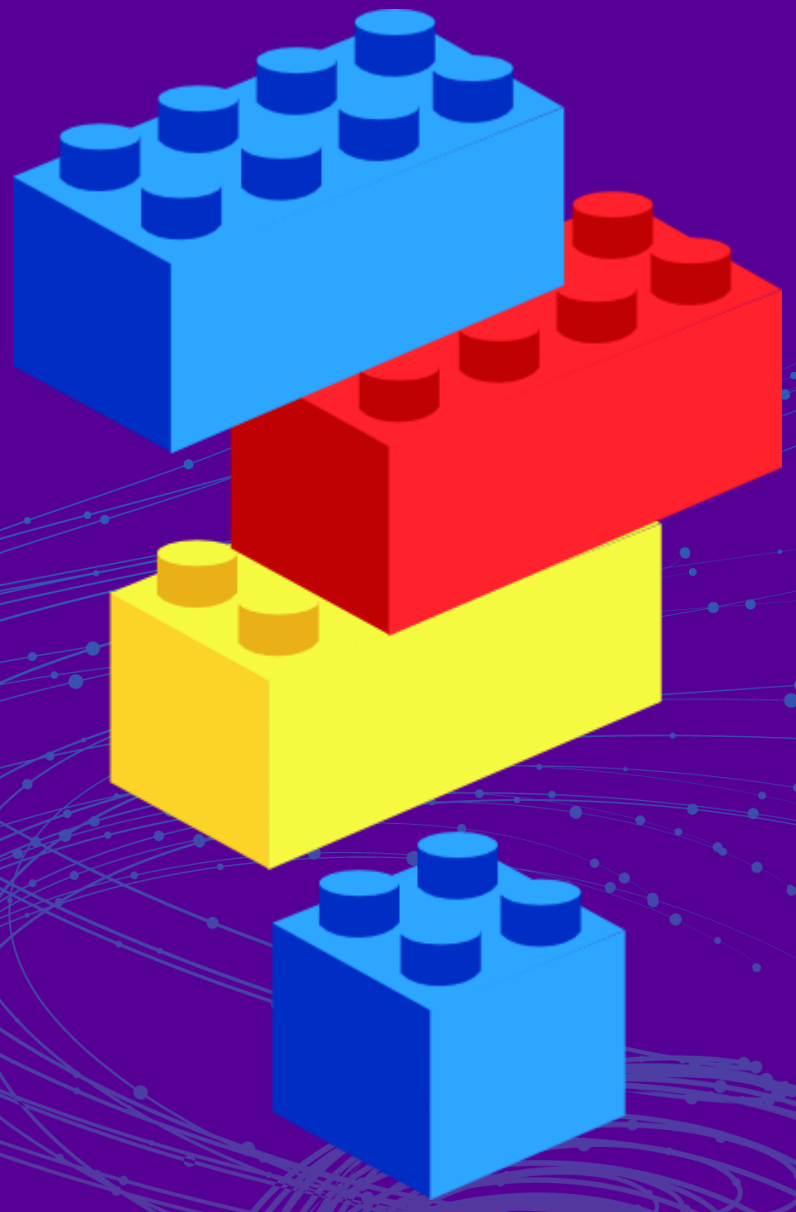
AGENDA – LAB3-W10

SESSION	COVERAGE
PART 1 – 10 MINUTES	Just What does DDoS mean in 2019?
PART 2 – 60 MINUTES COLLABORATIVE Q&A	3 Interesting DDoS Failure Scenarios Q&A & Live Attack Demos 20 min - 1) Mobile Phone Login DDoS 20 min - 2) TCP Connection DDoS 20 min - 3) Volumetric SYN FLOOD DDoS
TEA/COFFEE – 15 MINUTES	15 MIN BREAK -> HANDOUTS + GAME CARDS
COLLAB – 45 MINUTES	Let's Play A Game: "ATAK WARZ!" – TABLE-TOP ATTACK/DEFENSE CARD GAME Fun for the whole family!
PART 3 – 30 MINUTES	DDoS TESTING PROGRAM Misconceptions, Impacts, Responses, Controls, Testing Program
COLLAB – 15 MINUTES	Collaborative Game Playing – in reverse
REVIEW – 15 MINUTES	CLOSE SUM IT UP - ACTION PLAN IMMEDIATE, 3 MONTH, 6 MONTH

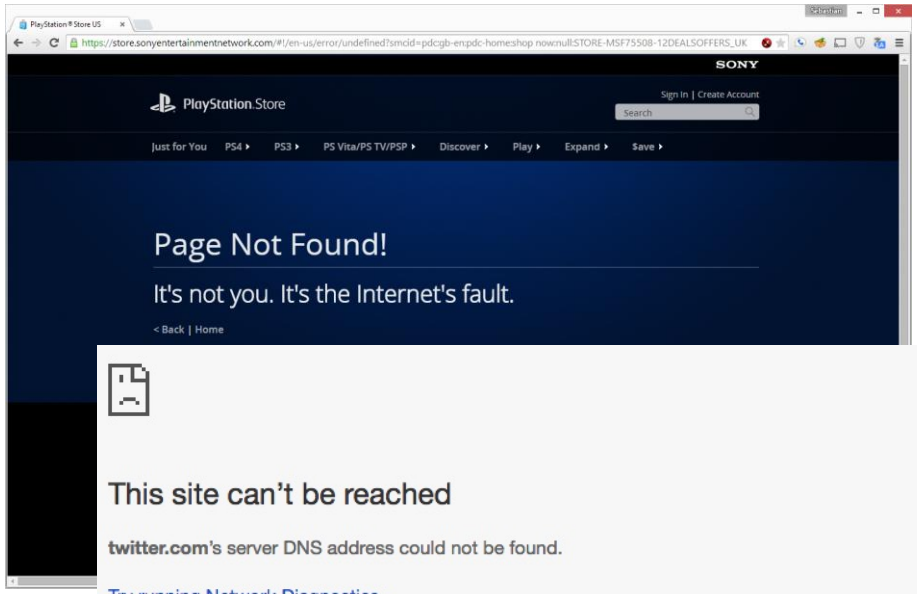
RSAConference2019

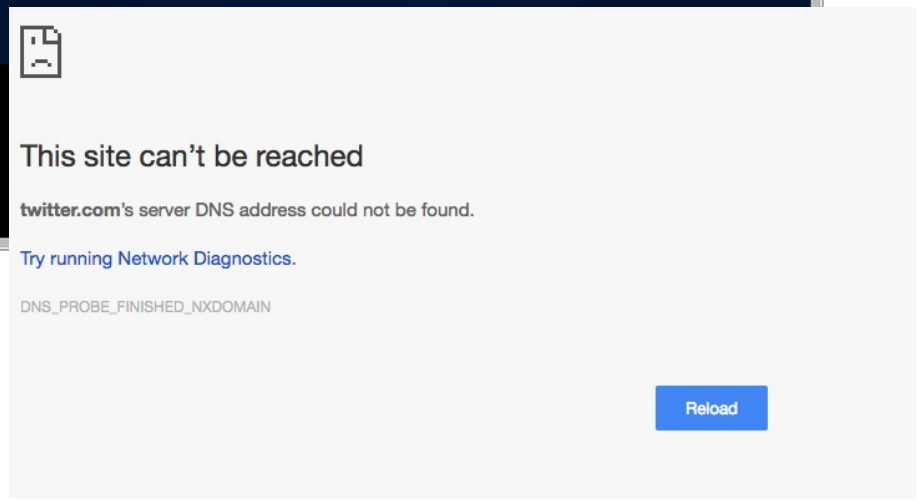
LAB3-W310
How to Design and Operate a DDOS Testing Program

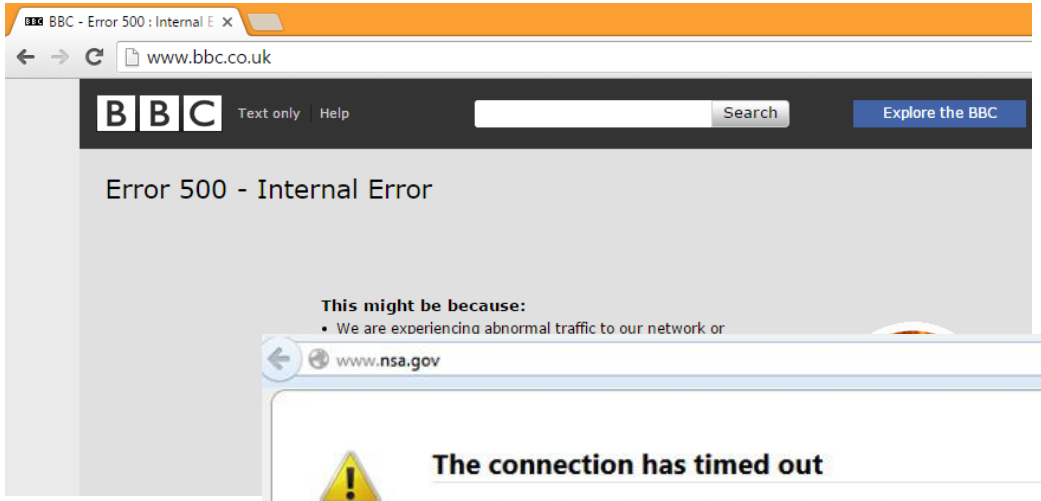
What does DDoS mean in 2019?

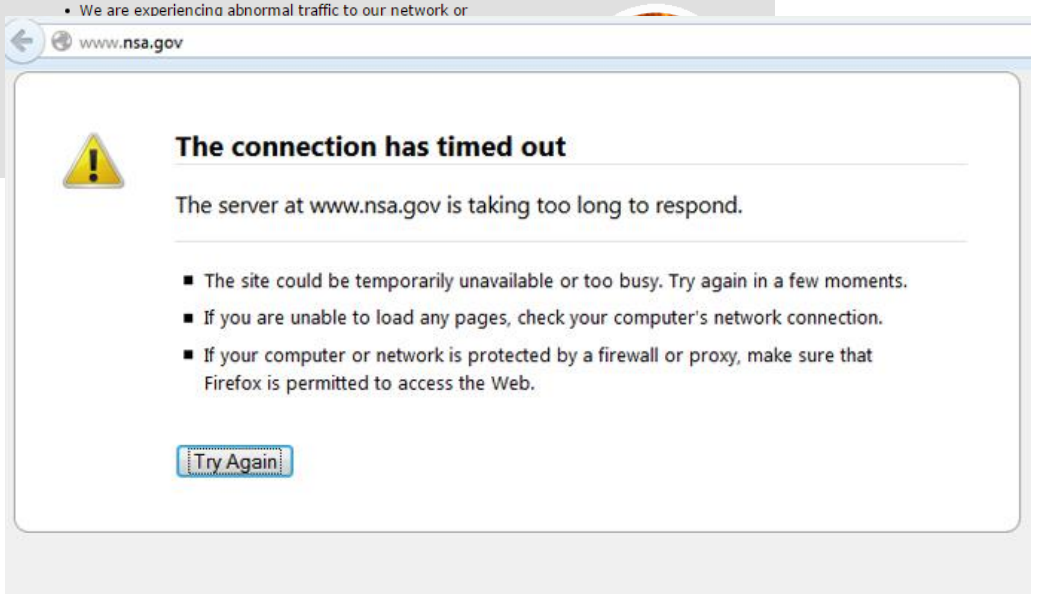


What is a DDoS?





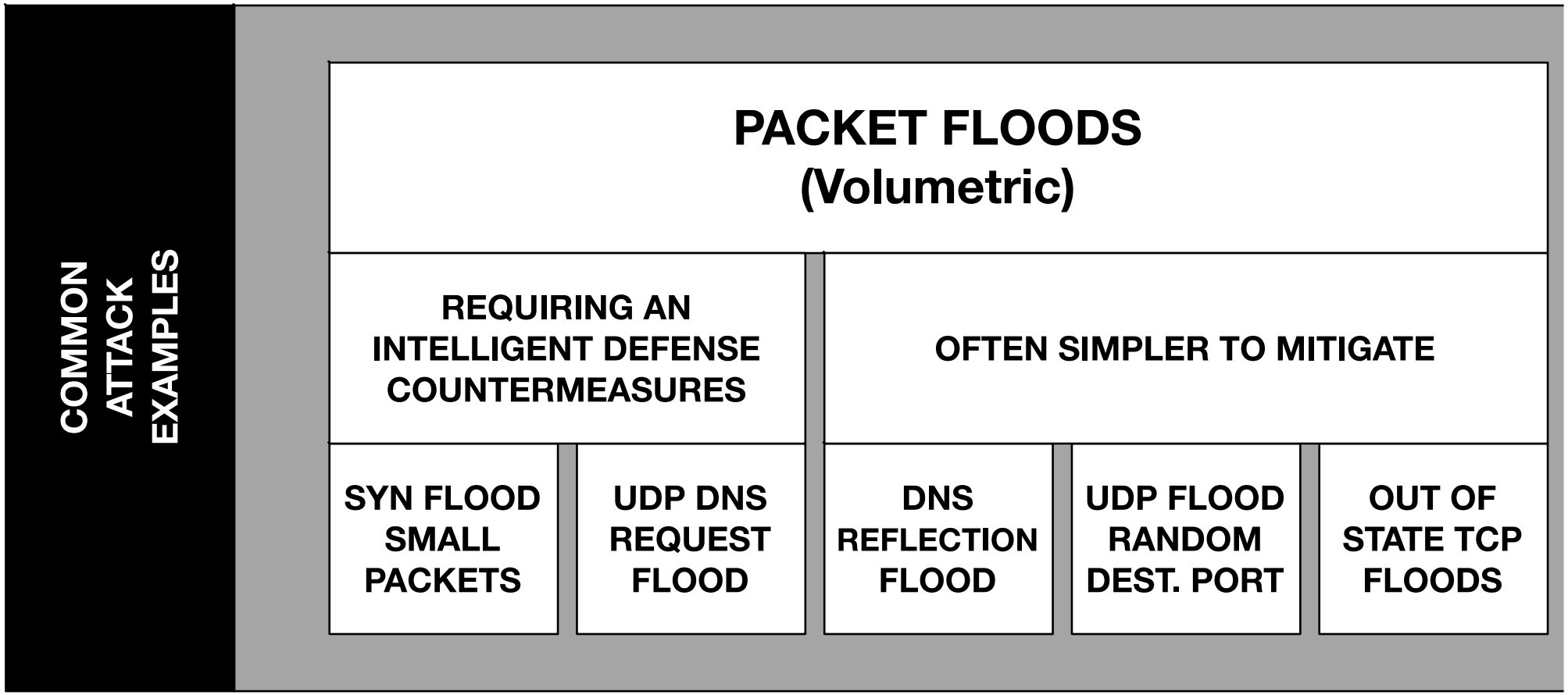




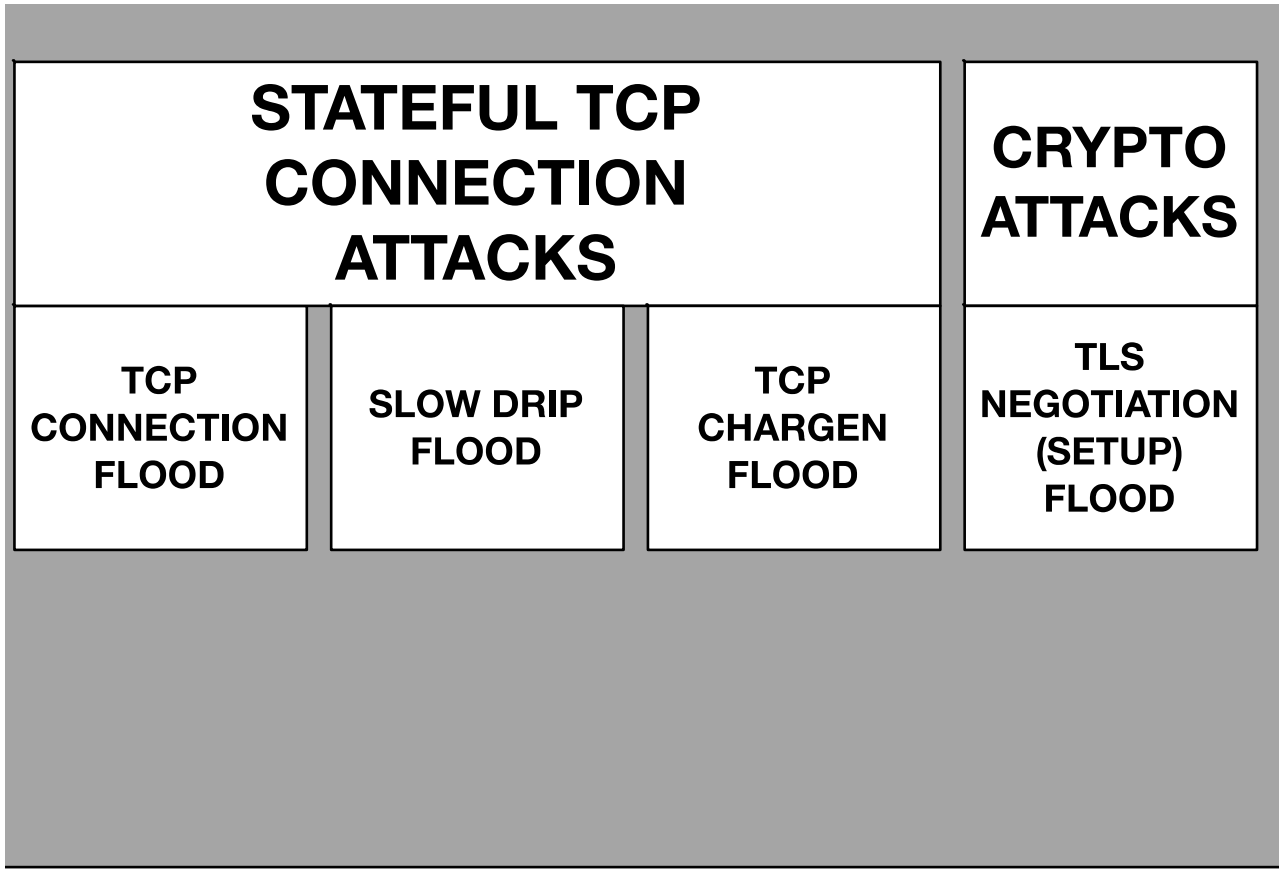
What is a DDoS in 2019 really like?

There's a whole lot of bad!

What is a DDoS in 2019 really like?



What is a DDoS in 2019 really like?

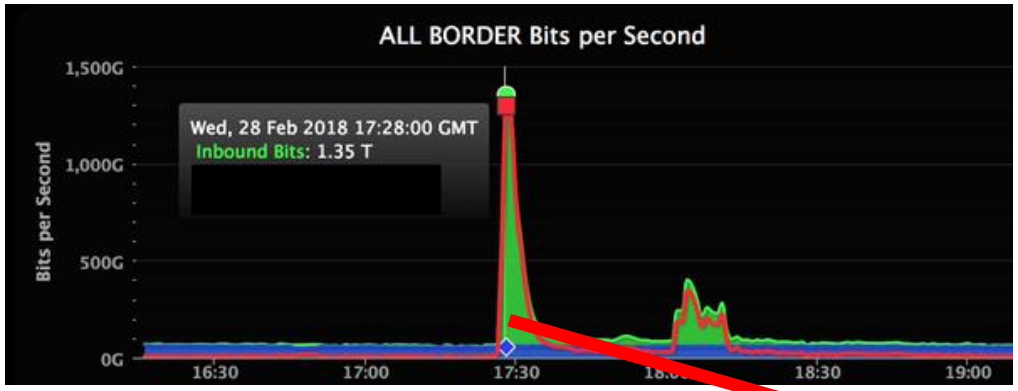


What is a DDoS in 2019 really like?

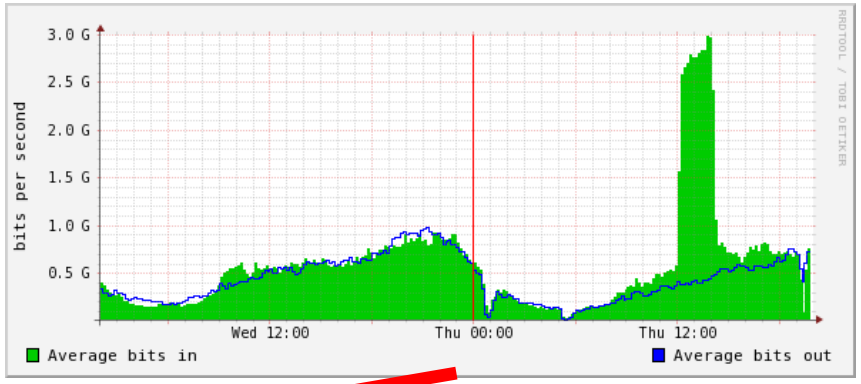
HTTP & HTTPS ATTACKS							
HIGH RATE (overloads)		SLOW (to avoid detection or make requests take a very long time)				REALISTIC (acts like people)	
SIMPLE HTTP(s) GET FLOOD	SIMPLE HTTP(s) POST FLOOD	LOW REQUEST RATE	SLOW PAGE READ	SLOW POST	SLOW LORIS	BROWSER HTTP(s) POST FLOOD	ADVANCED SPIDER / AUTOMATION

When you think "DDoS", HUGE! traffic floods come to mind

1.5 TERABIT/SEC!



3 GIGABIT/SEC – STILL BAD!



ISP Carriers Saturated
Packet Processing Devices Overloaded

Everything Down	Upstream May Null Route You	VOIP & VPN DOWN	BGP and GRE Bouncing	Firewalls Overloaded

If your defenses don't work, what happens?

IMPACTS! WHAT HAPPENS IF THINGS GO WRONG!

TYPICAL IMPACTS

ISP Carriers Saturated Packet Processing Devices Overloaded					TCP Connection State Table Exhaustion			Crypto Capacity Exhausted	HTTP REQUEST PROCESSING THROUGHPUT CAPABILITY OVERLOADED							
Everything Down	Upstream May Null Route You	VOIP & VPN DOWN	BGP and GRE Bouncing	Firewalls Overloaded	Firewall Memory Exhausted	NAT Exhaustion (65k limit)	Layer 4 Connection Pool Saturation	CDN, WAF, & Load Balancer Overloaded	Load Balancer Overloaded	WAF CPU Overloaded	Firewall Memory Exhausted	Web or App Server CPU Exhausted	Web or App Thread Pool Exhausted	Web or App Memory Exhausted	Database Overload	Authentication System Overloaded

COMMON INSTRUMENTATION & INCIDENT RESPONSE IMPACTS							REVENUE IMPACTS		SECONDARY APPLICATION IMPACTS						
SIEM OVERLOAD	LOST TELEMETRY	LOST DEVICE CONSOLE ACCESS	LOST COMM. CHANNELS (Email & Chat)	LOST HELP DESK ACCESS	LOST REMOTE VPN	CAN'T ACCESS CONTACT LISTS (Responders)	LOST REVENUE + LABOR COSTS	BRAND IMPACT	SAN / Disk I/O Overloads	Application Crashes	Auto-Scaling Out of Control ($$)	Application Garbage Collection Freezes	Message Queue Overloaded	Application Exploited	Sensitive Data Disclosure

Q:	If your network is down how do you VPN in?
A:	Ideally via a back-door VPN admin connection.
Q:	How do you know who to call? Is this info online?
A:	Network problems can break help-desk's and wiki's.

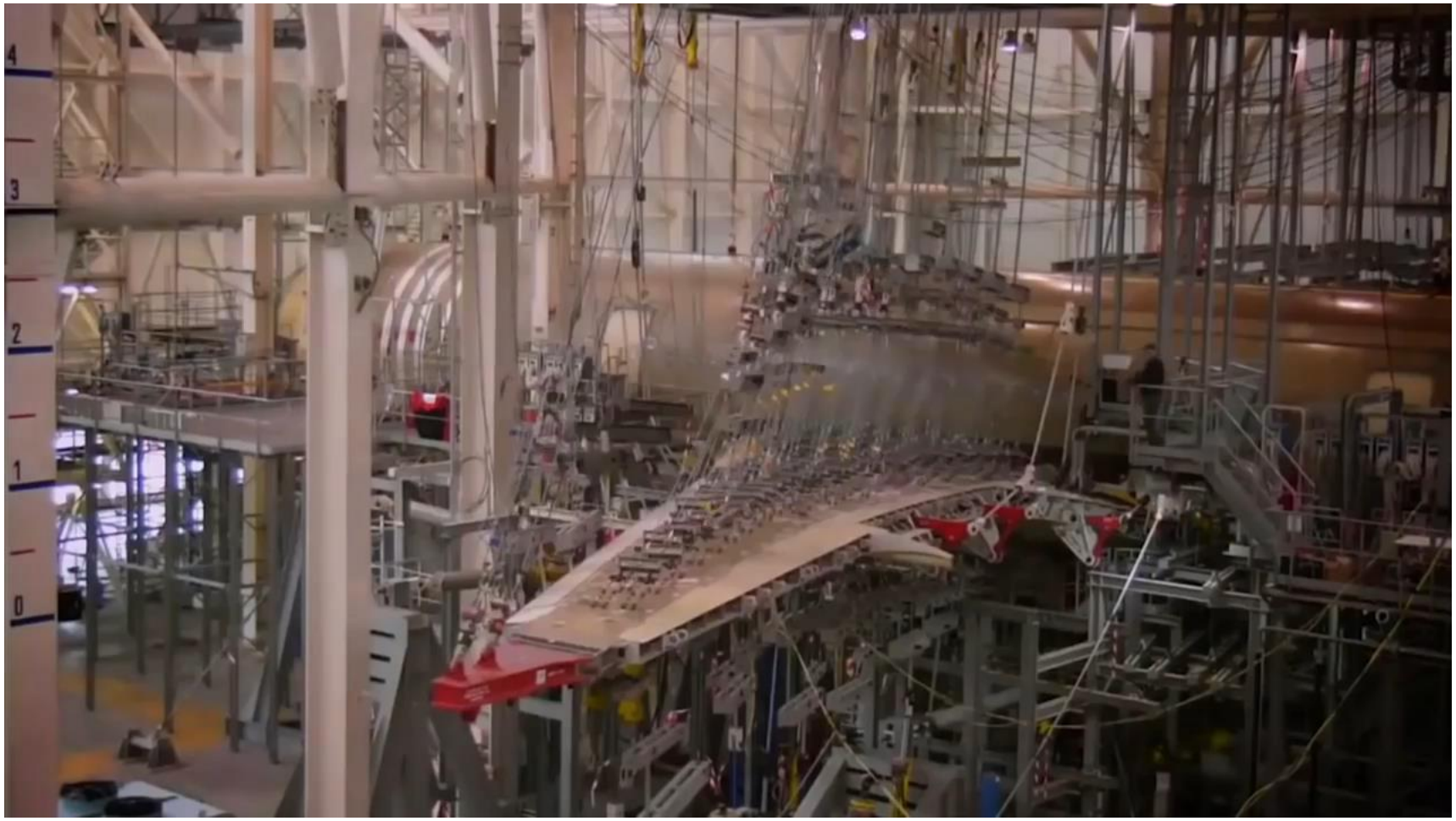
Q:	Will you get the email alert from your vendor?
A:	Probably not if networks are down.
Q:	Can problems be identified quickly?
A:	They might take hours – our teams are dispersed…

How can you know if your defenses will work? How can you avoid impacts? Testing!

How can you know if your defenses will work?
How can you avoid impacts? Testing!

How can you know if your defenses will work?
How can you avoid impacts? Testing!

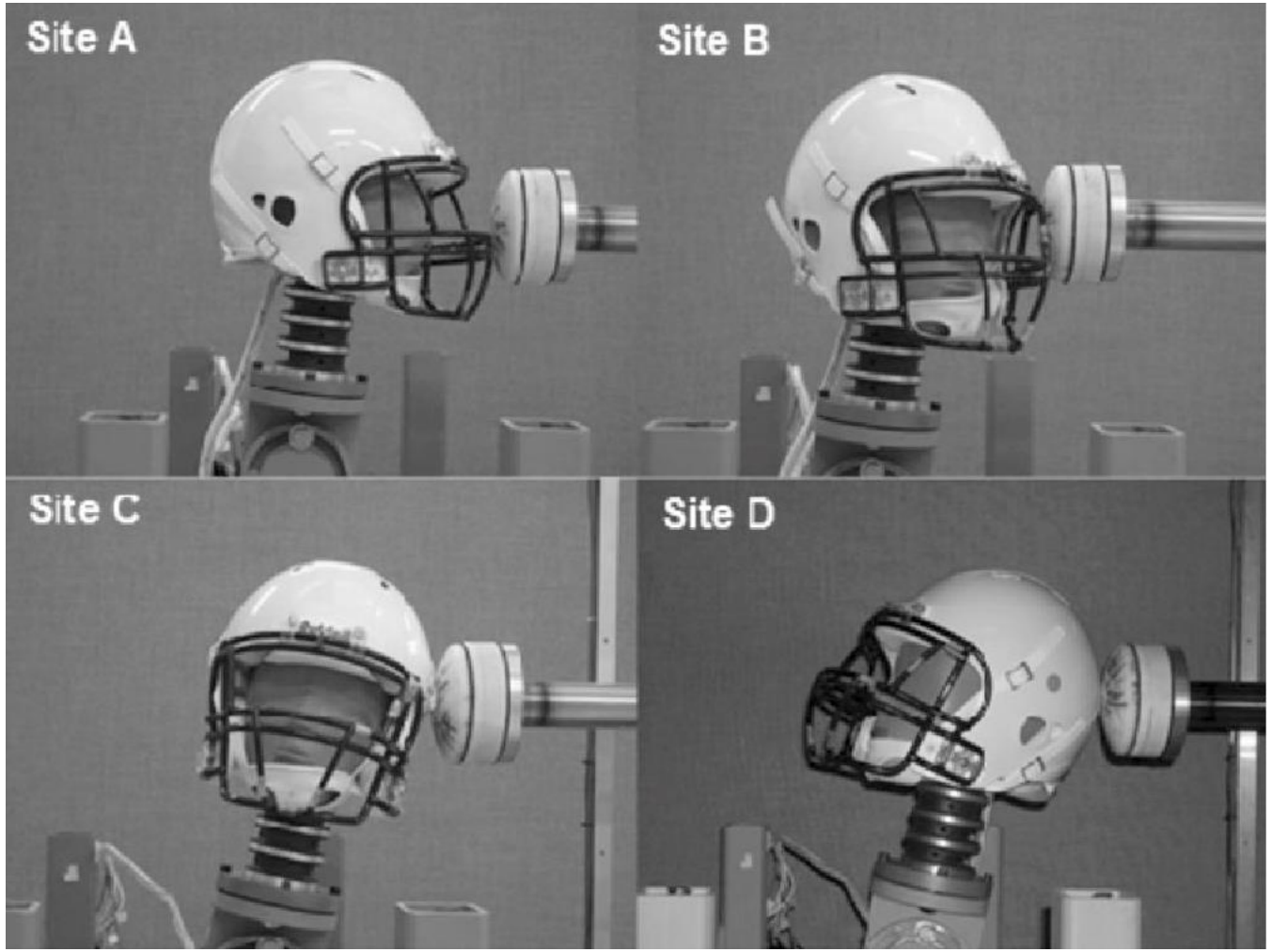
Defenses will work to a point – what happens when it stops working?



Defenses will work to a point – what happens when it stops working?


2016 NISSAN VERSA

You need to test multiple attack scenarios



For some reason, the IT Security industry feels it is, unlike with every other industry, it doesn't need to test and verify.

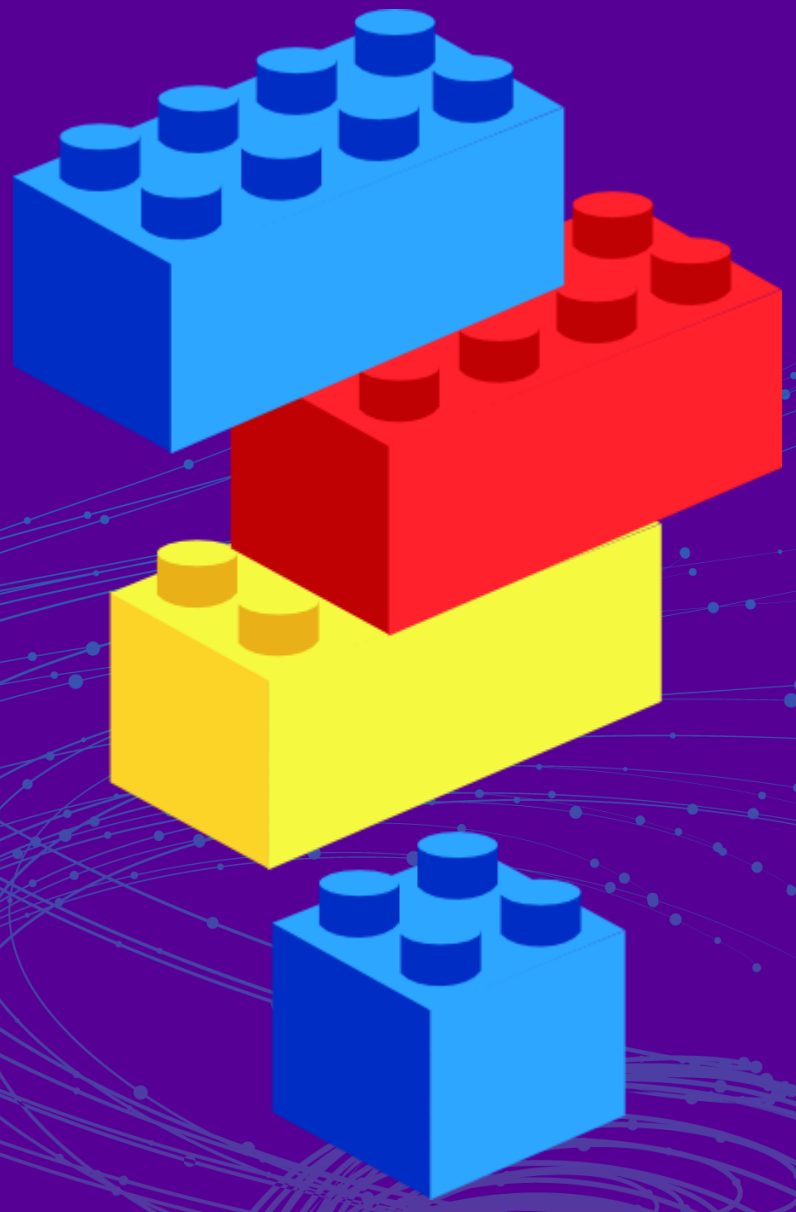
"We get attacked all the time, I see the alerts – too many alerts in fact. We don't need to test because I see attackers hammering on the defenses all the time."

What about the attacks you don't see?
Do you know what attacks you can handle, which you can't?
There are thousands of different kinds of attacks.
There are many types of attackers – robots, script-kids and really trained adversaries.
Can you be sure you can handle all of them?

MELTDOWN

RSAConference2019

LAB3-W310
How to Design and Operate a DDOS Testing Program



Collaborative – Interesting DDoS Attacks

Example 1 –Mobile Attack to Login Page (20 minutes)

But DDoS DOES NOT HIGH BANDWIDTH to DDoS effectively

Q: How likely is it that a single 3G Mobile Phone could DoS the main web site of a Fortune 500 company?

What about a 4G?

Certainly a 5G enabled device poses a considerable threat.

What about IoT devices?

Mobile Phone Attack Example 4 megabit/sec

A DoS was performed from a single mobile phone, in a basement, against the main login page of a Fortune 500 (unnamed) company.

Single Attacker

10k Connections

10k Concurrent Login Requests

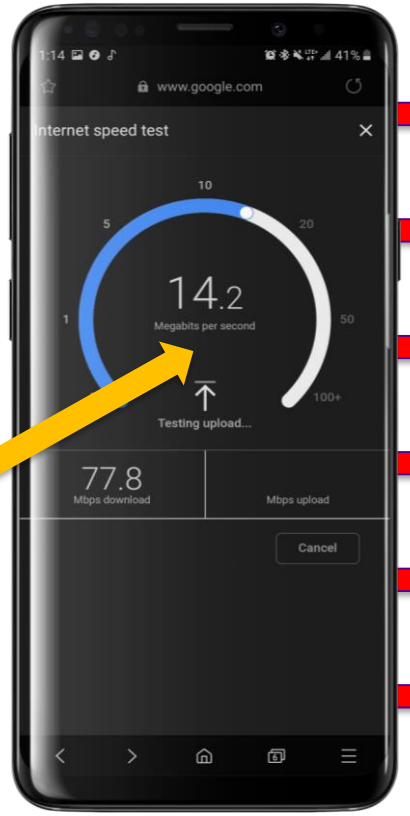
LOGIN PAGE OF FORTUNE 500

Q: What do you think happened, and why?

Mobile Phone Attack Example 4-5 megabit/sec

A DoS was performed from a single mobile phone, in a basement, against the main login page of a Fortune 500 (unnamed) company.

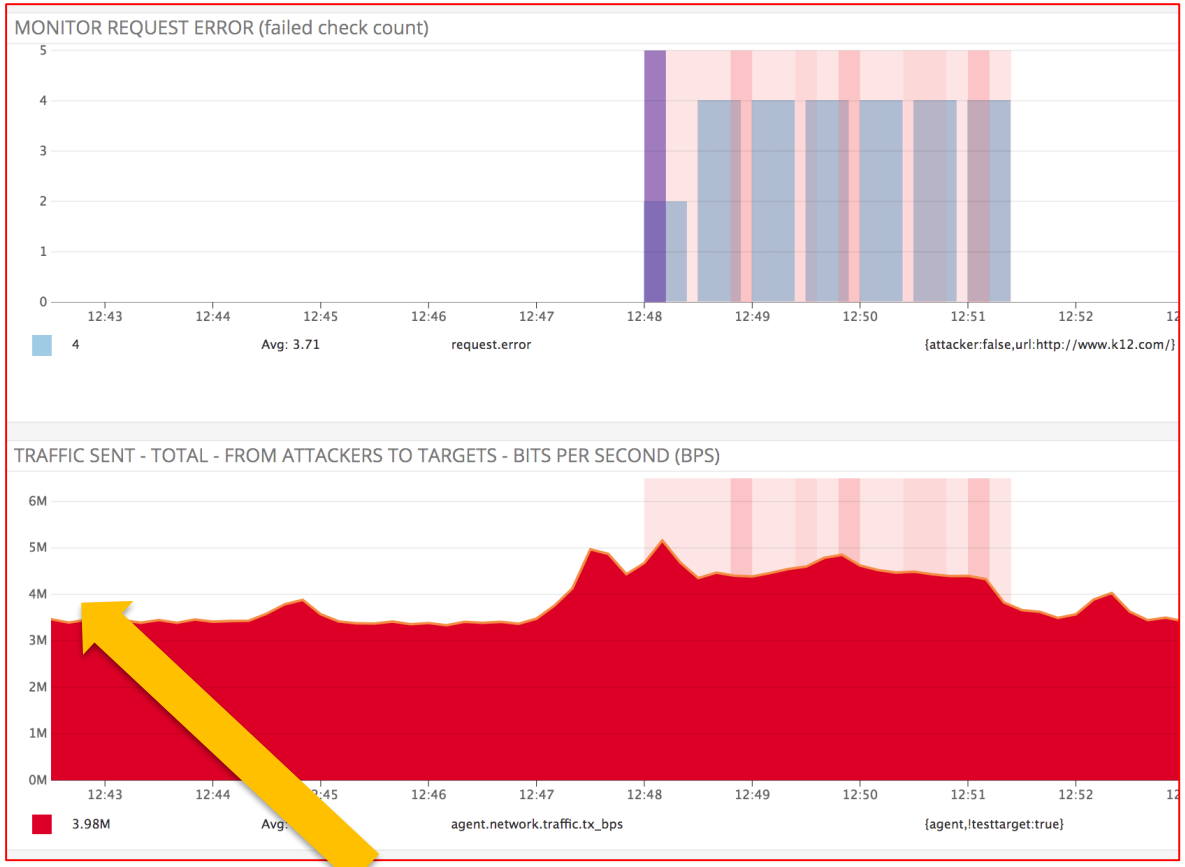
Speed test:
This phone can transmit up to 14.2 Megabit/sec Upload (4G)
(site died at <5)



Single Attacker

10k TCP Connections

10k Simultaneous Login Requests



BUT – Even though phone could send 14.2 megabit/sec, All that was needed to disable site was **4 to 5 Megabit/sec**

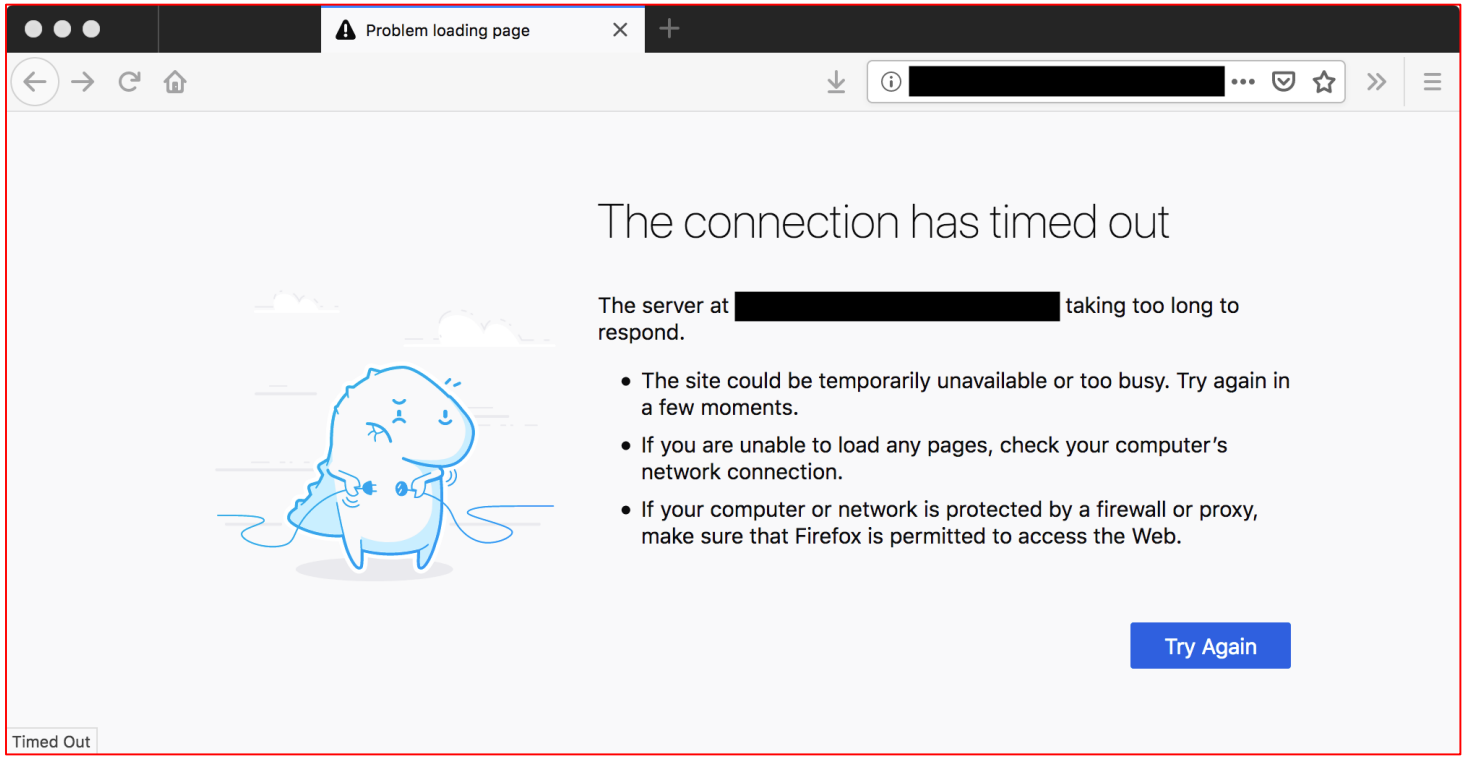
Mobile Phone Attack Example 4-5 megabit/sec

A DoS was performed from a single mobile phone, in a basement, against the main login page of a Fortune 500 (unnamed) company.

Single Attacker

10k Connections

10k Simultaneous Login Requests



Q: Why??

Why? Ideas?

How can a single device, with 4 megabit/sec, disable the login page of a major corporation? How is this possible? What resources were exhausted?

Q:	**Could it be the scalability of the back-end authentication system?**
A:	**That's a possibility! Could be database connection limit, AD limit.**

Q:	**Could it be the number of concurrent requests the authentication system could perform?**
A:	**That's likely too! Most enterprise web servers are set up with 'connection pools' and 'thread pools'**

How could this abuse have been detected / blocked?

Is it reasonable for a single device, or IP to, rather rapidly, open up 10,000 TCP Connections and start making 10,000 login requests?

Q:	**Could a WAF have protected the system?**
A:	**Sure! If it was configured to. Do you think it was in this case?**

Q:	**Could there be protections to limit the # of TCP connections a client can open?**
A:	**Yes – this can be done at many layers – DDoS, Firewalls, Load Balancers, WAF's and even at the web server and application levels. Do you think it was done at all in this case?**

What testing uncovered

- Fortune 500 Company had never previously tested the capacity of their LOGIN page, or any Internet-Facing service – despite high $ investment in tech.
- After testing, they knew:
  - How many logins/sec can system could sustain.
  - At what point should the WAF be engaged to protect the site.
- Implemented transactional monitoring to verify that the Login system worked – not just checking the page, but actually automating a login.
- Alerts are now only raised if the login system fails, not every time it is attacked (which are numerous).

Operations teams should only be alerted with a HIGH SEVERITY alert if the defense controls fail or site is down.

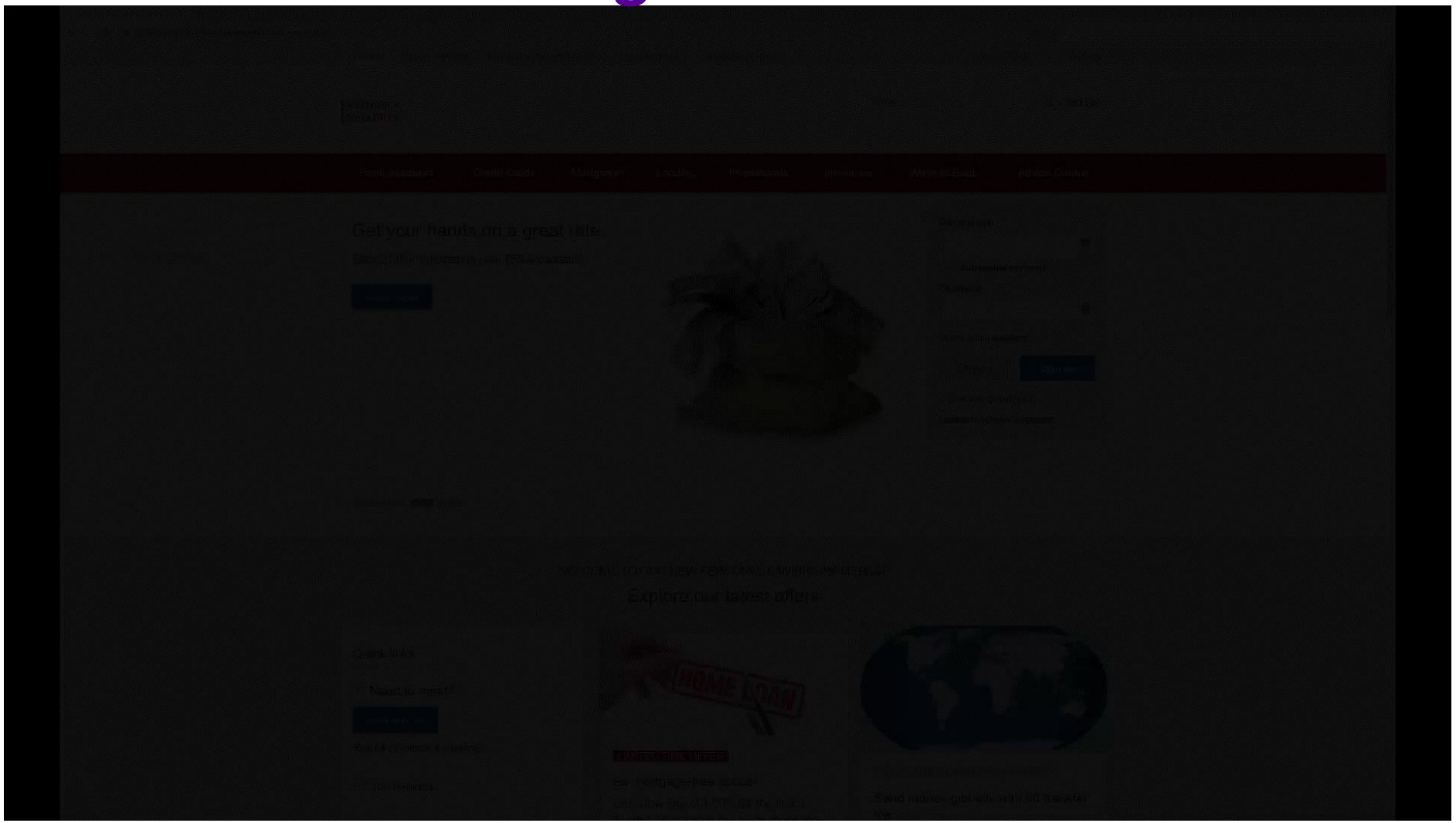
Not every time it is attacked.

Sense of Security RED WOLF

Login Flood Attack – Showing CPU and Connection Overload

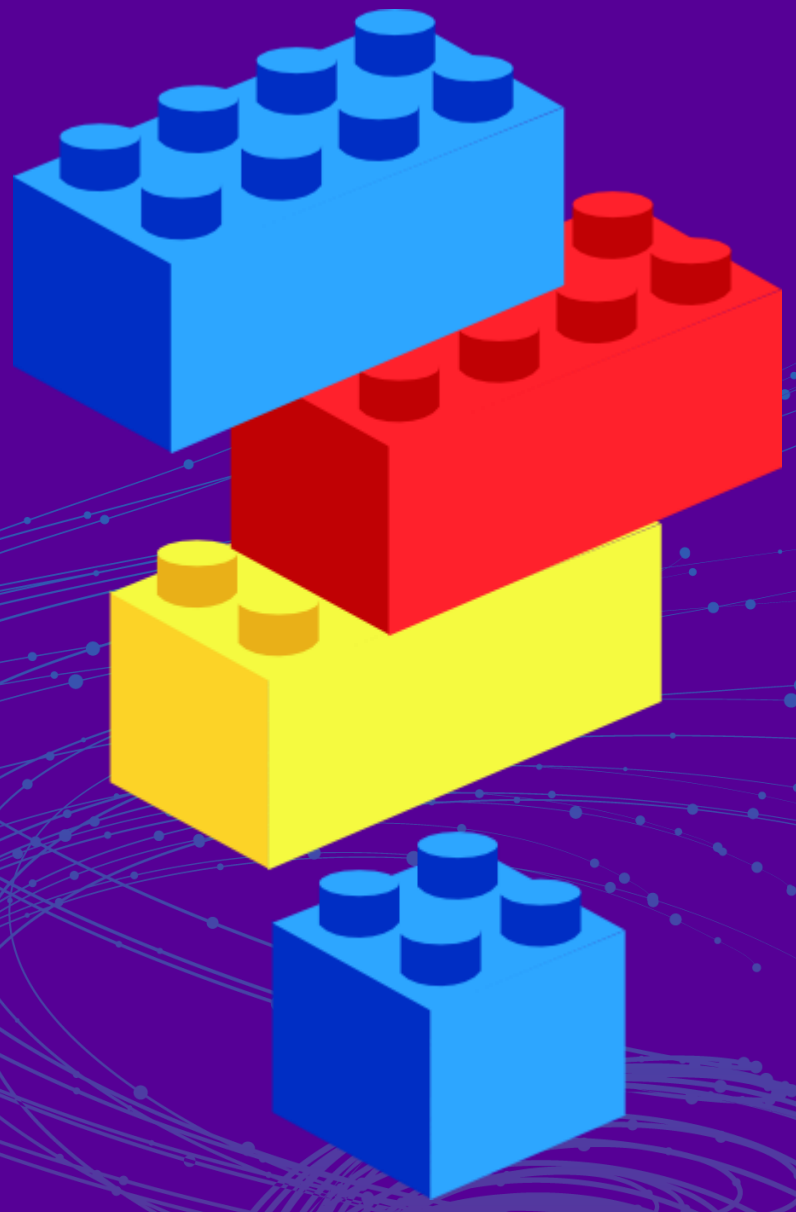
Live Demo Time

Login Flood Attack – Showing CPU and Connection Overload



RSAConference2019

LAB3-W310
How to Design and Operate a DDOS Testing Program



Collaborative – Interesting DDoS Attacks

Example 2 – TCP Connection Flood DDoS (20 minutes)

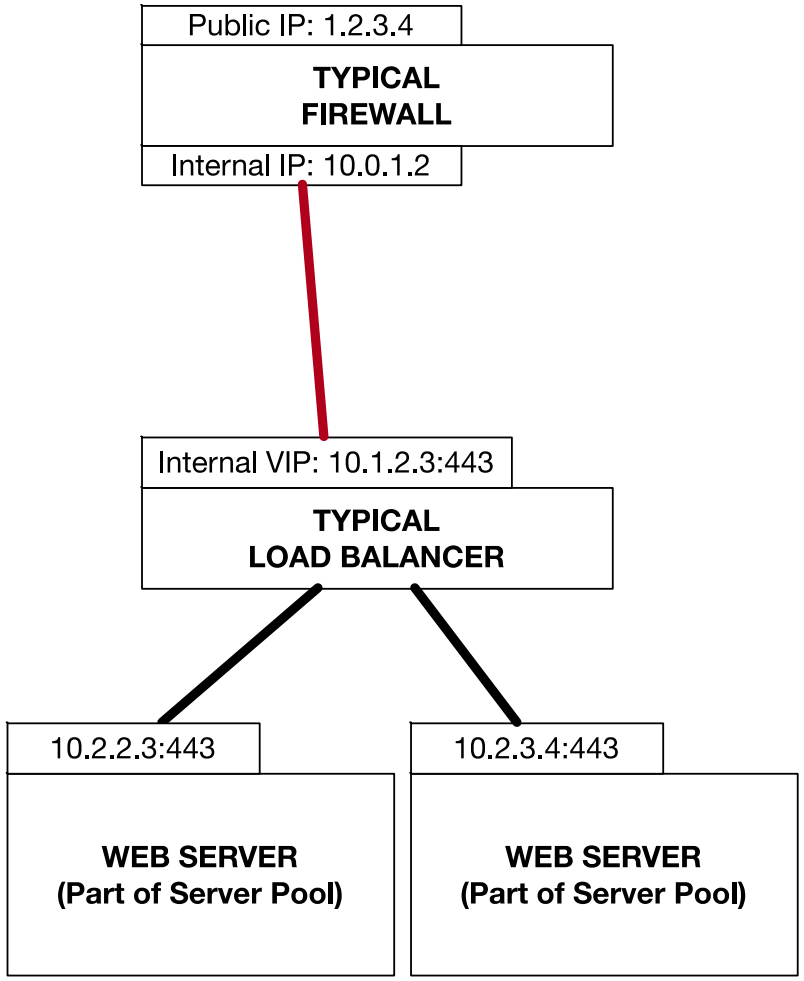
Example 2: An attack that almost everyone is vulnerable to

Q:	**How bad would it be if there was a DDoS attack:** - That 99% of Internet facing services were vulnerable to - Used very little network traffic, about 2 to 10 megabit/sec - Could take out web sites almost instantly - From a tiny attacker botnet of 200 IP's - Could take out almost any TCP service in about 1 second…
A:	**Sit back and watch…**

Do you have something like this on your network?

Q: How many of you have something that looks like this on your network?

- **A Firewall with Internet-Facing IP's**
- **NAT (Network Address Translation) to Internal Network**
- **A Load Balancer "VIP" to a web site**



Can you spot the problems? Or a problem?

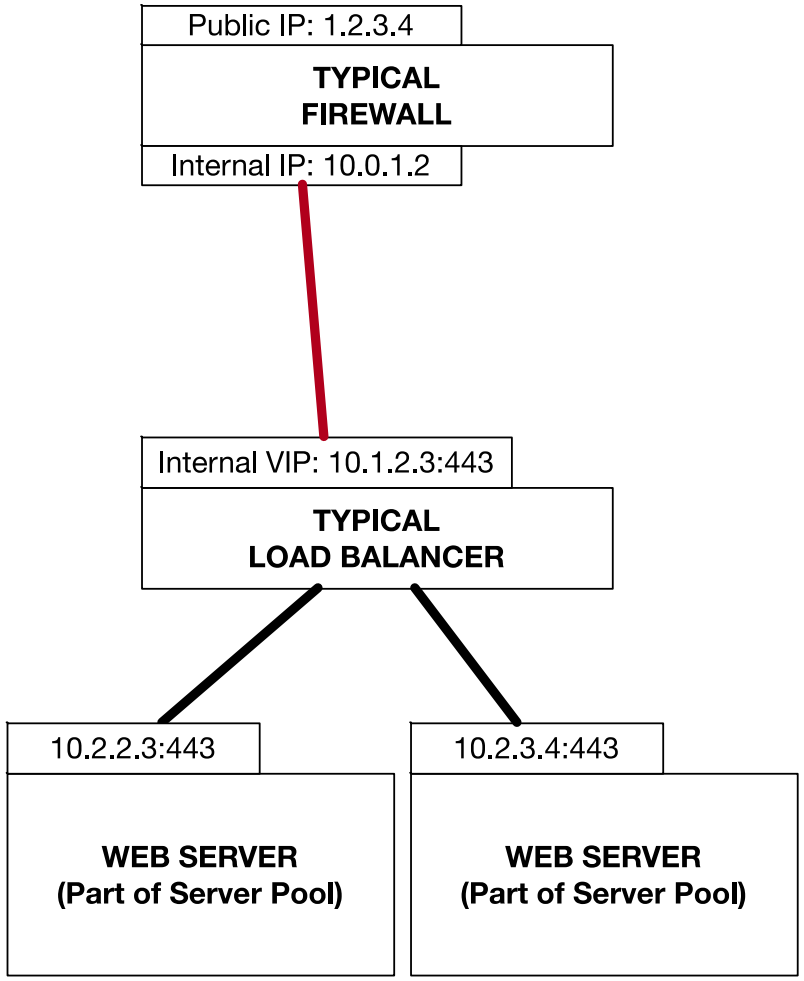
Q:

Q: Can anyone spot what the greatest vulnerability of this architecture?

Hint – it is colored RED.

There are many problems here, but there is a very significant and extremely common vulnerability here.

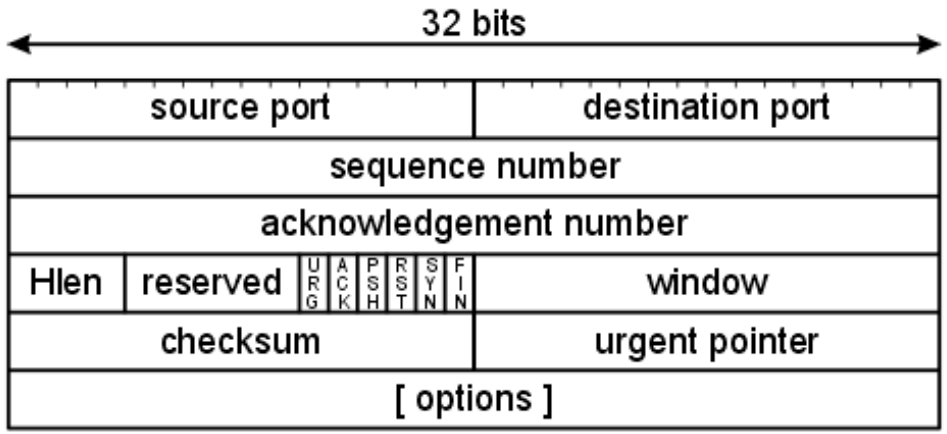
Can you spot it?

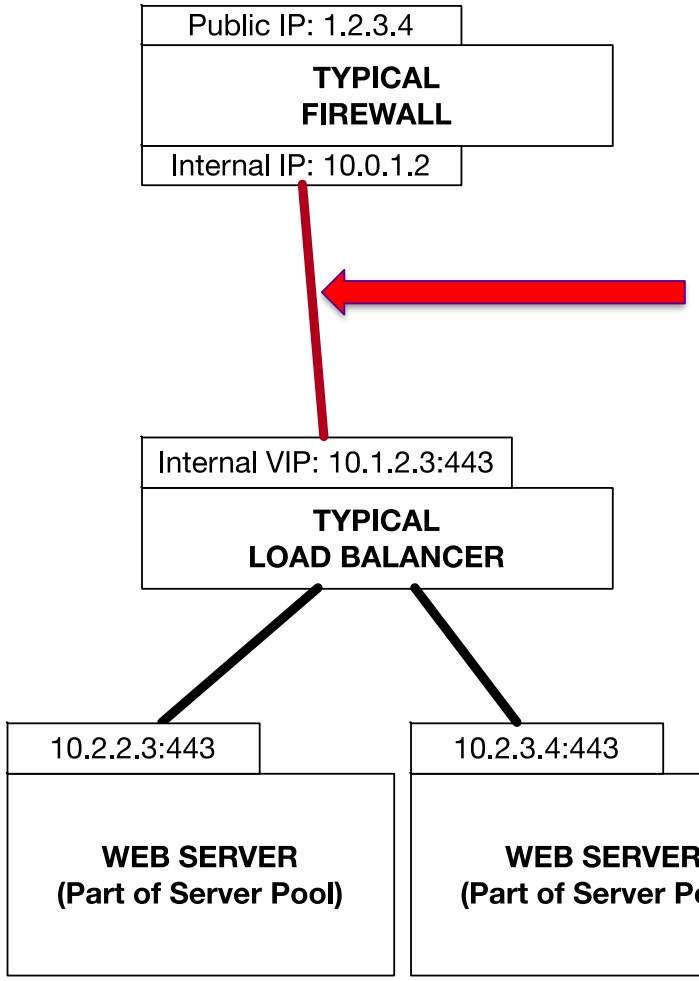


A hint

Let's go back to basic TCP/IP and look at the source port and destination port:

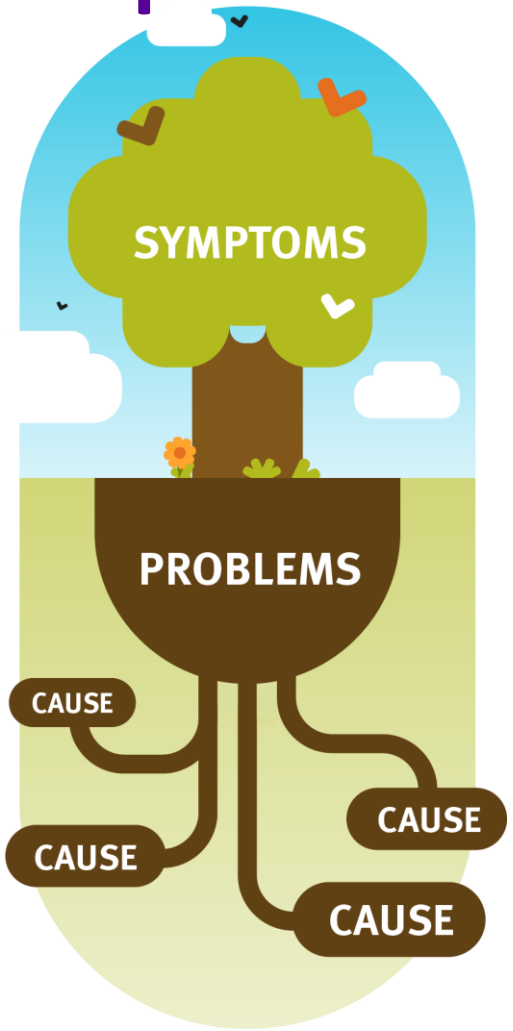
TCP header format





Q: How many TCP connections CAN one IP Address open to another IP address on port 443?

Beyond defense, how would your organization begin to root-cause this problem? Identify what was happening & recover?



Q:	What happens if an attacker opens up more than 65535 TCP connections?
A:	No more connections can be opened that's what!
Q:	Does your organization detect TCP Connection abuse?
A:	?
Q:	How long would it take to root-cause this problem?
A:	?
Q:	Do you know what countermeasures are available?
A:	CDN, Elastic Cloud Scaling, DDoS, Firewalls, Load Balancers +

Example 2: How can you know the REAL limit?
A: Test it!

Q:	**The theoretical limit is 65535 ports.** **Source port 1 to 65535.** **BUT – the true number is often less.** **Sometimes by 1024 ports and sometimes by thousands more.** **How would you find out that limit?**
A:	**On UNIX systems ports <1024 are typically reserved.**

If you know how to strike and where to strike

Consider…

200 clients or attackers on the Internet

… Each opens up **400** TCP Connections

200 attackers X **400** TCP Connections Each

= **80,000** TCP Connections

Is 80,000 > 65,535?

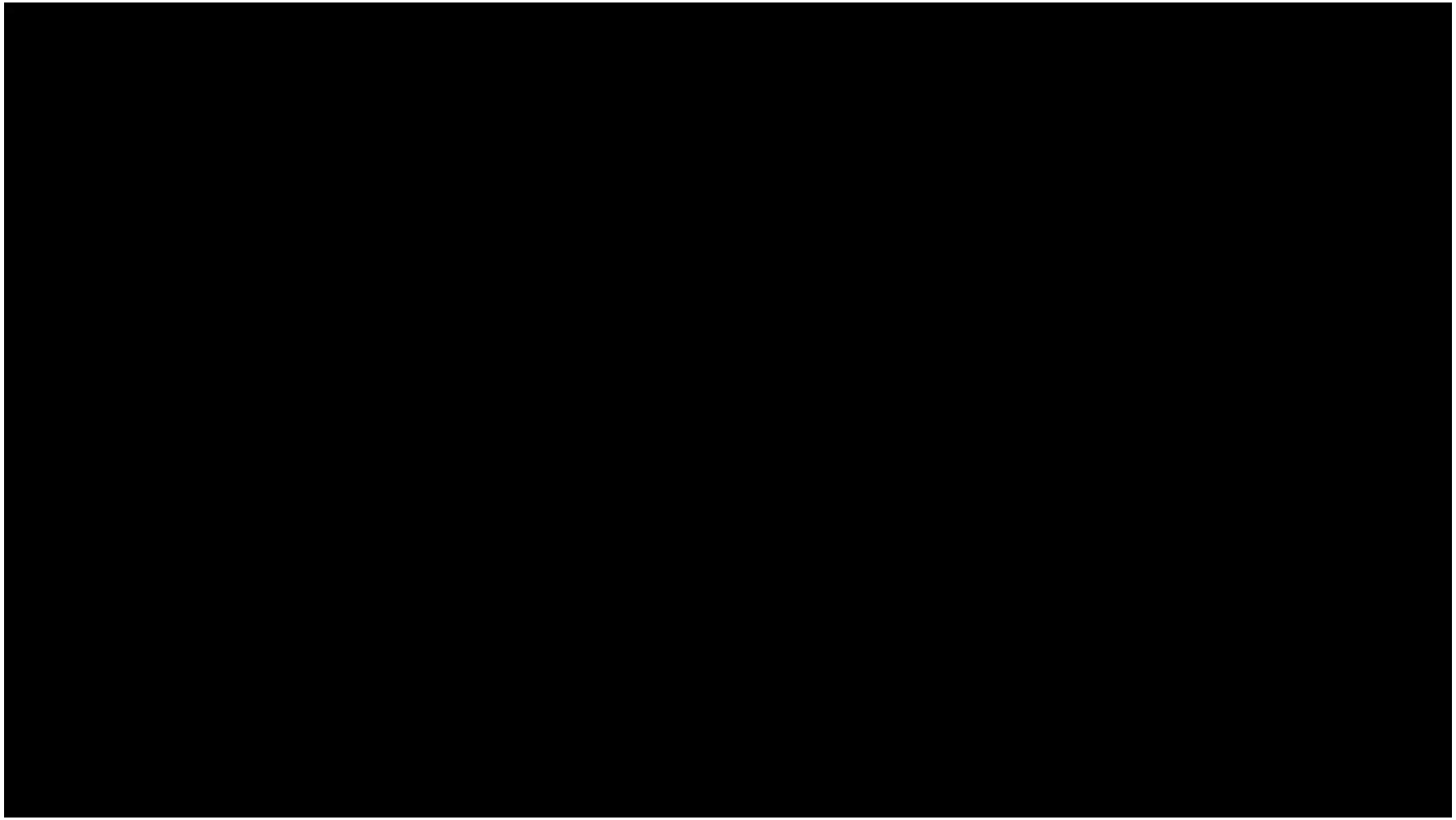
Who Wins?

Let's See!

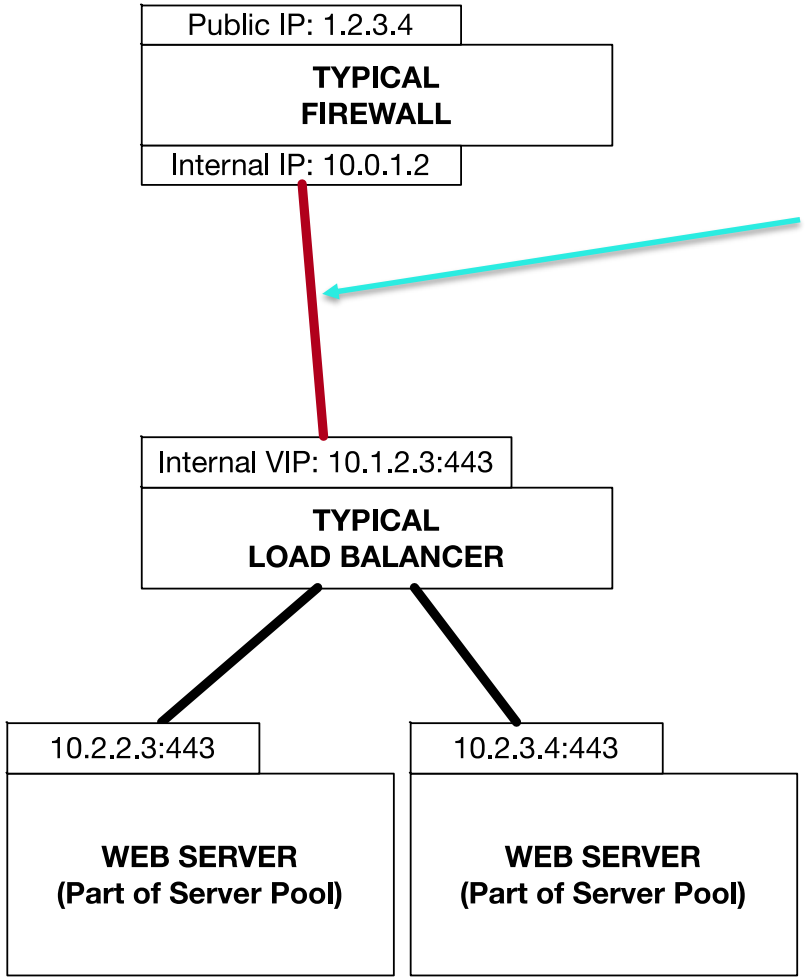
Connection Flood

Live Demo Time

Video of Connection Flood



What are the 2 limits seen?



NAT EXHAUSTION!
65k TCP Connections

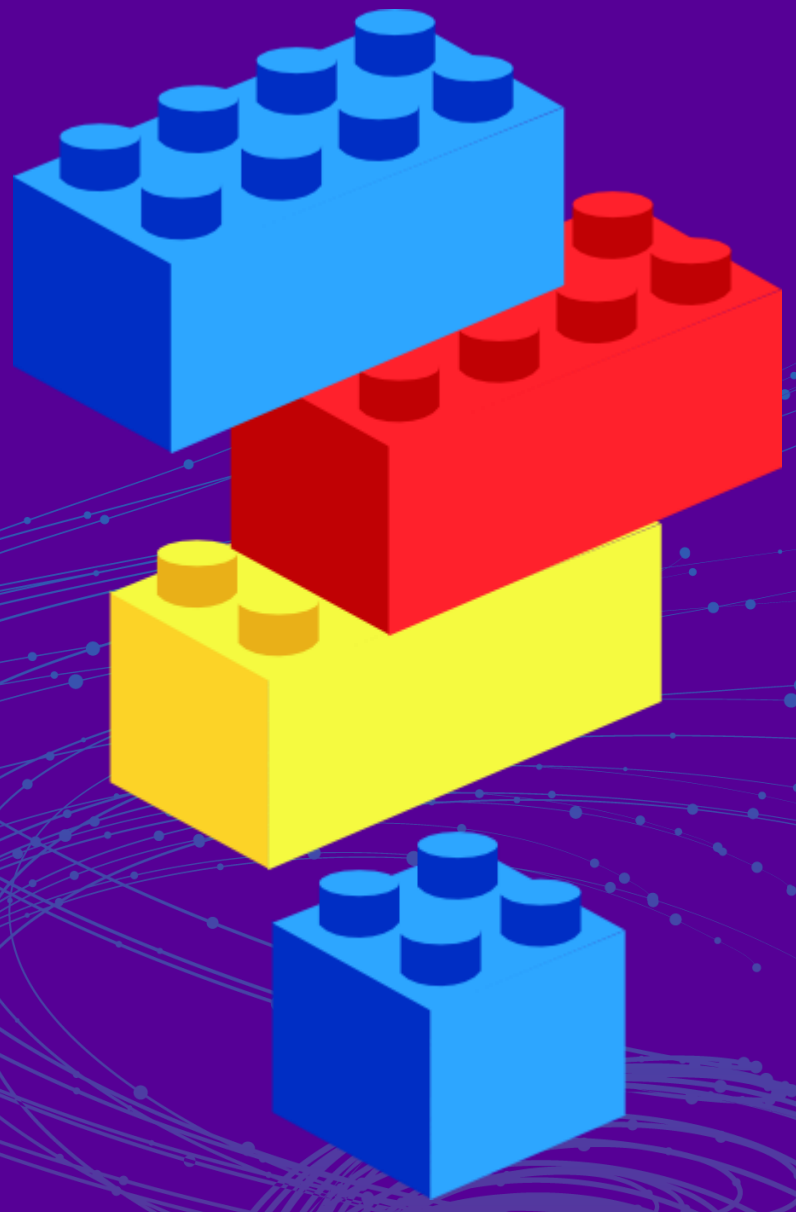
CONNECTION POOL EXHAUSTION!
<300 connections to server pool from load balancer

RSAConference2019

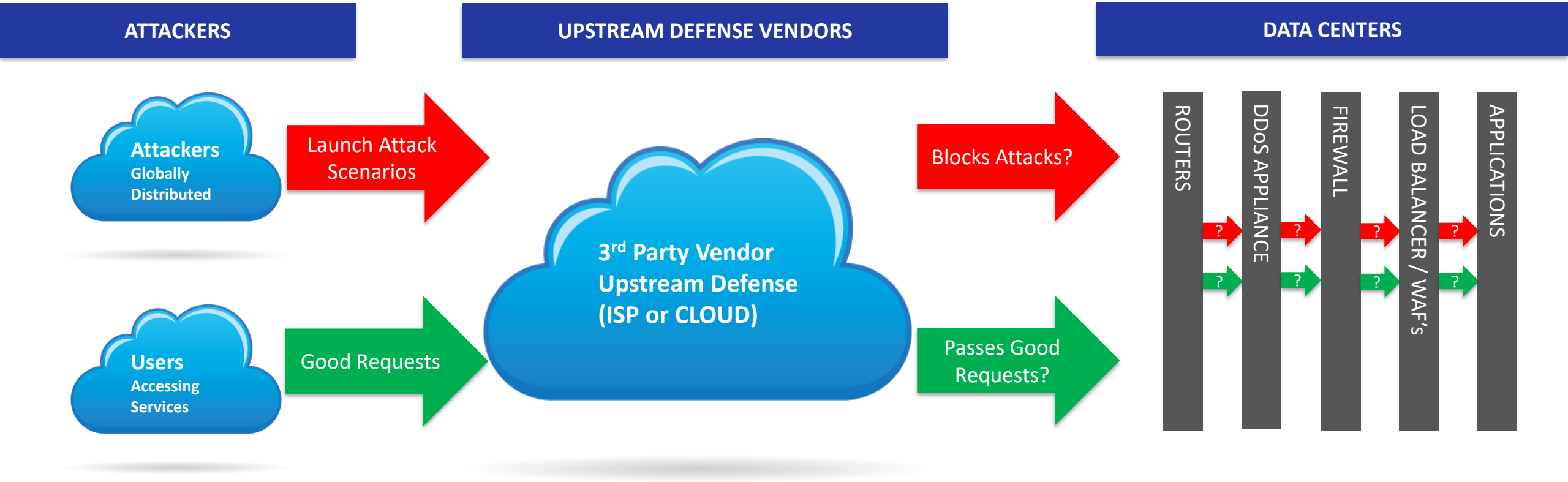
LAB3-W310
How to Design and Operate a DDOS Testing Program

Collaborative – Interesting DDoS Attacks

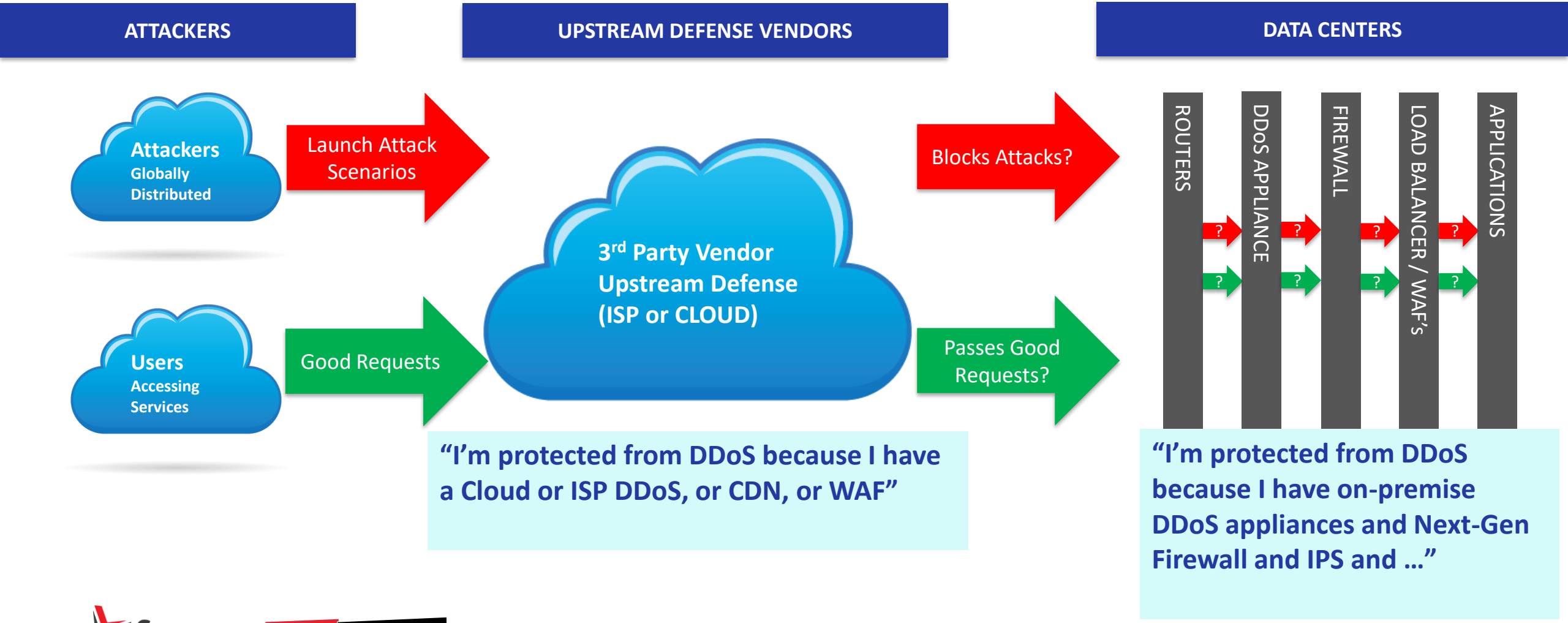
Example 2 – Volumetric SYN FLOOD (20 minutes)



Let's look at a simple 2 layered DDoS defense system: "Cloud or ISP DDoS Defense" + "Local DDoS Appliance"



Does having the device or paying a 3rd party to manage DDoS defenses mean it will work?

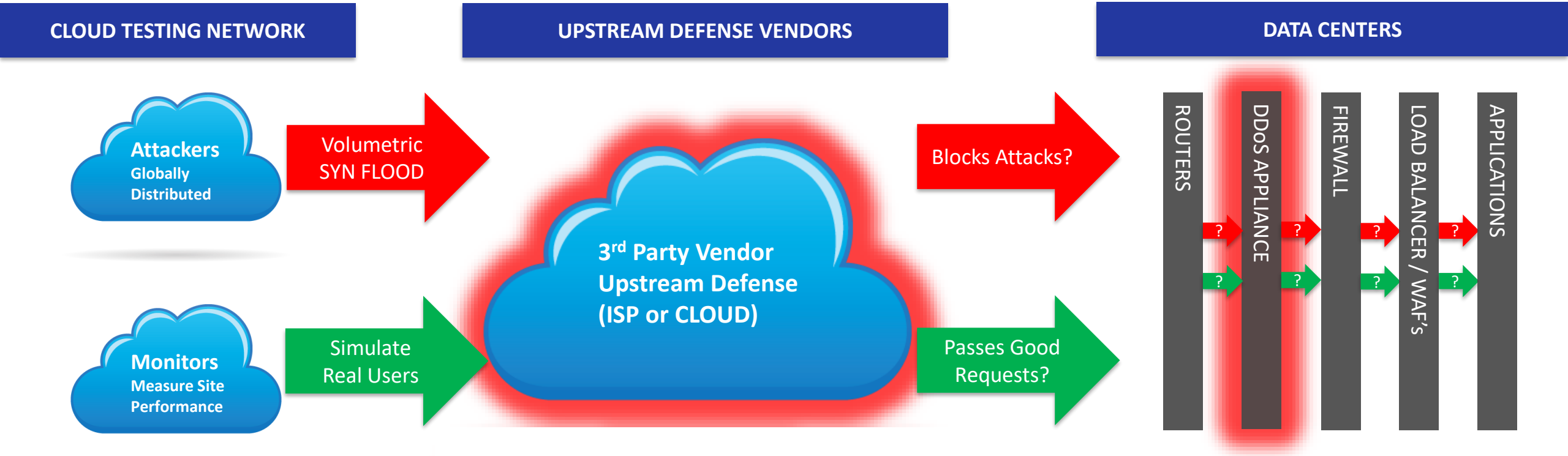


"I'm protected from DDoS because I have a Cloud or ISP DDoS, or CDN, or WAF"

"I'm protected from DDoS because I have on-premise DDoS appliances and Next-Gen Firewall and IPS and …"

Let's find out how well it works! Let's TEST!

Upstream DDoS (ISP or Cloud) & On Premise DDoS Appliance



Q:	Will the attack be detected quickly?
Q:	Will the attack be blocked quickly and completely?
Q:	Will the correct alerts, metrics, and logs be generated?

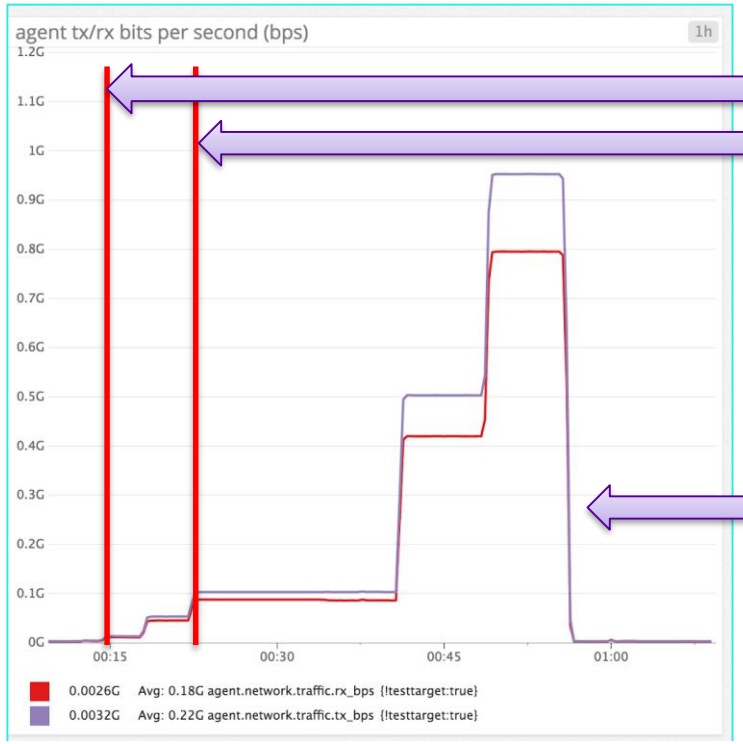
Q:	What happens if the attack is not detected?
Q:	What happens if the attack is not blocked 100%?
Q:	What if the correct alerts, metrics and logs are not available?

TEST SCENARIO 1: SYN FLOOD VOLUMETRIC DDoS

A SYN FLOOD DDoS Test was performed to test ISP and On-Premise Defenses

Tested at specific traffic levels:

1 Megabit/sec
10 Megabit/sec
100 Megabit/sec
500 Megabit/sec
950 Megabit/sec



On-Premise DDoS Activated at 10 Meg/sec

ISP DDoS Defense activated at 100 megabit/sec

Controlled DDoS SYN FLOOD Network Test 1 megabit to 950 megabit

Q:	**Was the attack be detected quickly?**	**YES**
Q:	**Was the attack be blocked quickly and completely?**	**NO**
Q:	**Were the correct alerts, metrics, and logs be generated?**	**NO**

In this case it was the Firewall CPU that was overloaded
It logged so many deny packets it even took out the SIEM

Q:	**What can happen if a Firewall is overloaded?**
A:	**If a Firewall is overloaded, many things may happen:** ▪ Packet Loss (increased latency) ▪ Too much DENY logging (can overload SIEM) ▪ Drops established connections ▪ Drops VPN's ▪ Impacts VOIP (voice communications impossible)

How can you know if your firewall is vulnerable?
How can you know if your Defenses leak attack traffic?

Q: What could cause periodic bursts of attack traffic to leak through?

A:

- Defense Configuration: Type of countermeasure being used – is it using correct countermeasure? For SYN FLOOD's there are a few, and they work differently.
- IP Blacklist Timeouts: A blacklist may drop packets for a few minutes – after that you might see a short burst of attacker traffic for a short moment!
- Low and Slow attacks that "come in under the radar" – don't trigger defenses

Q:

- Do you know what countermeasures your DDoS protection has activated?
- Do you know if it will leak traffic?
- Do you know if this could overload your firewall or other devices?
- Do you monitor firewalls, load balancers, WAF's and services for various overloads?

But after 10 minutes bursts of attack traffic started leaking past the DDoS defense and the Firewall CPU shot to 100%

WHAT TESTING UNCOVERED

① DDoS defenses did activate and begin blocking attackers as expected (good!)

② DDoS defenses leaked attack traffic AFTER 10 minutes

③ The firewall was vulnerable to this attack traffic leakage and it's CPU went to 100% and packet loss was seen

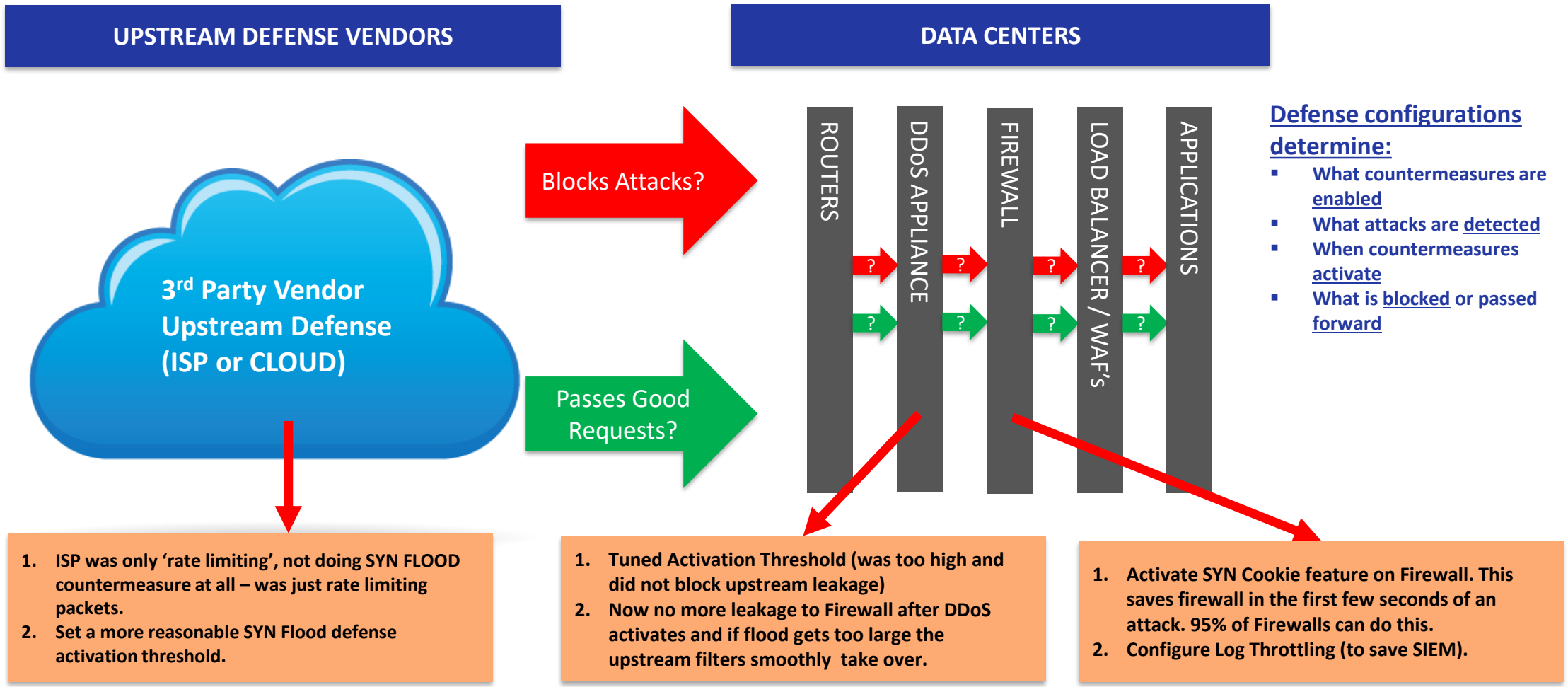
④ SIEM was overloaded and Operation's couldn't see what was going on.

⑤ Vendor unable to stop all leakage. Vendor defense SOC said attack leakage is "normal" and "expected".

!!!! Don’t Forget to Read the Small Print in Your Contracts !!!!

⑤ <u>Vendor unable to stop all leakage</u>. Vendor defense SOC said attack leakage is “normal” and “expected”.

Q: How was this corrected?
A: By tuning three configurations and re-testing

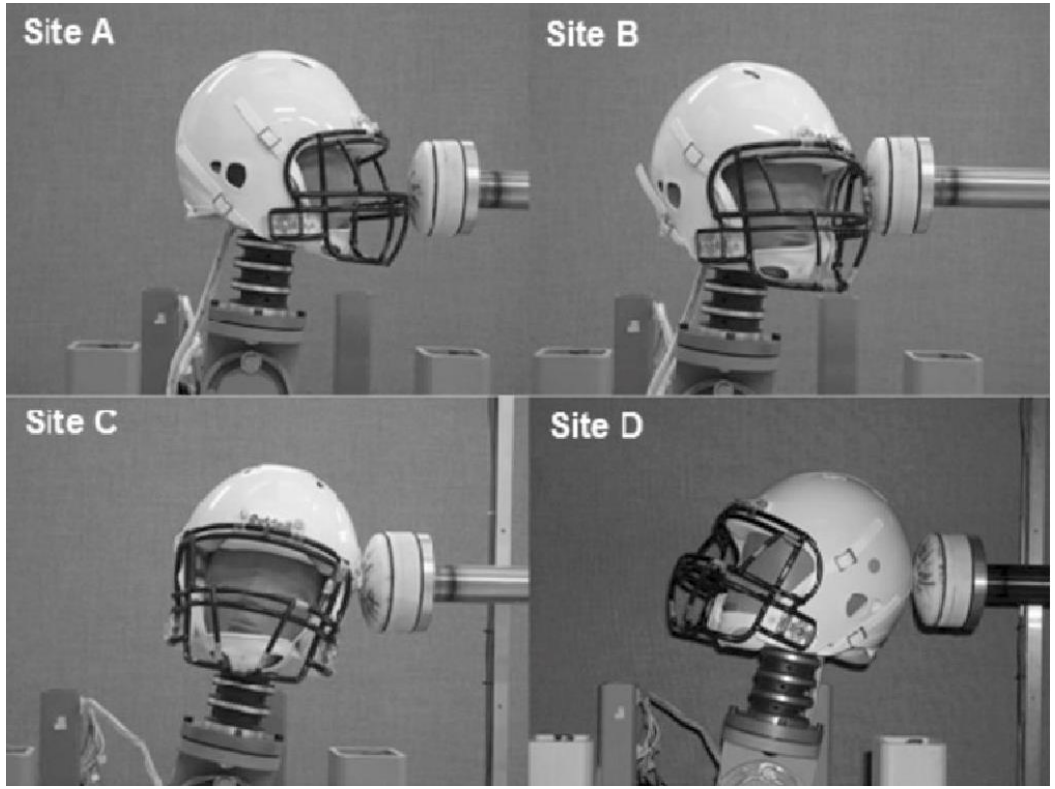


Unexpected Consequences – It's all connected? A system view is necessary

Q:	How many have a SIEM / Logging System?
Q:	How many have Firewalls?
Q:	Is it common for Firewalls to log 'denies'?
Q:	What happens if a Firewall has to log 10k to 20k+ denies every second? A DDoS attack can easily cause that with 10 megabit/sec of traffic.
Q:	Have you benchmarked your SIEM? Do you have licenses that limit the event rate? Do you know how many events your I/O Disk systems can handle? Does your SIEM perform well under heavy load? … … … … …

A: A DDoS Testing Program must take a system-wide view and not a device view – the scope must include all devices in path (Firewalls, Load Balancers, WAF's, Servers) as well as monitoring and logging systems – they are part of a connected system.

Lessons learned



- Devices don't operate in isolation, they are part of a system – you test the system.
- Without testing you'd probably never get the devices configured optimally. You'd never get the full benefit / ROI from the defenses.
- After testing you can prove you can handle the scenarios you've tested. Without testing, how confident can you be?

Is Cloud different?

While Cloud systems are more scalable, they still are just groups of regular computers processing things.

Some problems are the same.
Some are different.

We'll give an example of testing cloud scaling and cloud WAF defenses after the break.

Q:	**Does anyone here think that something like the AWS stateful security group is limitless in its capacity?**
A:	**Everything has limits – everything. The TCP NAT exhaustion we performed was on AWS. Also, later on more detail.**

Cloud scales
Cloud also fails
Nothing is perfect
☺

There are actually MANY MANY other kinds of DDoS attacks beyond high bandwidth packet floods

FOR THE NEXT FEW SLIDES – EXPECT TO BE OVERWHELMED ☺

We are going to show how complex this situation is

Then we'll talk about how to tackle it

There are actually MANY MANY other kinds of DDoS attacks beyond high bandwidth packet floods

COMMON ATTACK SCENARIOS - WHAT IF _____ HAPPENED?

COMMON ATTACK SCENARIOS

- PACKET FLOODS (Volumetric)
  - REQUIRING AN INTELLIGENT DEFENSE COUNTERMEASURES
    - SYN FLOOD SMALL PACKETS
    - UDP DNS REQUEST FLOOD
  - OFTEN SIMPLER TO MITIGATE
    - DNS REFLECTION FLOOD
    - UDP FLOOD RANDOM DEST. PORT
    - OUT OF STATE TCP FLOODS
- STATEFUL TCP CONNECTION ATTACKS
  - TCP CONNECTION FLOOD
  - SLOW DRIP FLOOD
  - TCP CHARGEN FLOOD
- CRYPTO ATTACKS
  - TLS NEGOTIATION (SETUP) FLOOD
- HTTP & HTTPS ATTACKS
  - HIGH RATE (overloads)
    - SIMPLE HTTP(s) GET FLOOD
    - SIMPLE HTTP(s) POST FLOOD
  - SLOW (to avoid detection or make requests take a very long time)
    - LOW REQUEST RATE
    - SLOW PAGE READ
    - SLOW POST
    - SLOW LORIS
  - REALISTIC (acts like people)
    - BROWSER HTTP(s) POST FLOOD
    - ADVANCED SPIDER / AUTOMATION

For every attack there are many available countermeasures

COMMON ATTACK SCENARIOS - WHAT IF _____ HAPPENED?

COMMON ATTACK SCENARIOS

PACKET FLOODS (Volumetric)					STATEFUL TCP CONNECTION ATTACKS			CRYPTO ATTACKS	HTTP & HTTPS ATTACKS							
REQUIRING AN INTELLIGENT DEFENSE COUNTERMEASURES		OFTEN SIMPLER TO MITIGATE			TCP CONNECTION FLOOD	SLOW DRIP FLOOD	TCP CHARGEN FLOOD	TLS NEGOTIATION (SETUP) FLOOD	HIGH RATE (overloads)		SLOW (to avoid detection or make requests take a very long time)				REALISTIC (acts like people)	
SYN FLOOD SMALL PACKETS	UDP DNS REQUEST FLOOD	DNS REFLECTION FLOOD	UDP FLOOD RANDOM DEST. PORT	OUT OF STATE TCP FLOODS					SIMPLE HTTP(s) GET FLOOD	SIMPLE HTTP(s) POST FLOOD	LOW REQUEST RATE	SLOW PAGE READ	SLOW POST	SLOW LORIS	BROWSER HTTP(s) POST FLOOD	ADVANCED SPIDER / AUTOMATION

COMMON DEFENSE TECHNOLOGIES (Vendors, Appliances, Automations)

DEFENSES TECHNOLOIES

COMMON CLOUD DEFENSE TECHNOLOGIES & APPROACHES						COMMON ISP DEFENSE TECHNOLOGIES			COMMON ON-PREMISE DEFENSES TECHNOLOGIES							
Cloud Routed Scrubbing DDoS	Cloud Layer 7 Proxy	Cloud Layer 7 Proxy with WAF	Cloud Layer 4 TCP Proxy	Pubic Cloud (Auto-Scale, 'Lambda')	Cloud DLP	ISP Packet Scrubbing DDoS	ISP Layer 7 Defense (Proxy)	ISP Managed ACL / FW	Router ACL's	On-Premise DDoS Appliance	On-Premise Next-Gen Firewall	On-Premise IPS	On-Premise WAF	On-Premise Load Balancer Configuration	On-Premise Data Leak Prevention	On-Premise Anti Virus
Always-On	On-Demand	Automatic Defense	"Expert" Guided Defense	Default Defense Policy Config	Customized Defense Configuration	IP Reputation Threat Blocking			Mail SPAM & Phishing Filters	Hardened Application Logic Defenses	Network Monitoring Correlation & Response	Active SIEM Correlation	Behavioral Analytics & Automated Response	IP Reputation Correlation & Response	Vendor API Integration & Automation	Automation & Orchestration Frameworks

Q: For volumetric DDoS packet flood attacks, what countermeasures are common?

COMMON ATTACK SCENARIOS - WHAT IF _____ HAPPENED?

COMMON ATTACK SCENARIOS

- PACKET FLOODS (Volumetric)
  - REQUIRING AN INTELLIGENT DEFENSE COUNTERMEASURES
    - SYN FLOOD SMALL PACKETS
    - UDP DNS REQUEST FLOOD
  - OFTEN TO MITIGATE
    - DNS REFLECTION FLOOD
    - UDP FLOOD RANDOM DEST. PORT
    - OTHER STATIC FLOODS
- STATEFUL TCP CONNECTION ATTACKS
  - TCP CONNECTION FLOOD
  - SLOW DRIP FLOOD
  - TCP CHARGEN FLOOD
- CRYPTO ATTACKS
  - TLS NEGOTIATION (SETUP) FLOOD
- HTTP & HTTPS ATTACKS
  - HIGH RATE (overloads)
    - SIMPLE HTTP(s) GET FLOOD
    - SIMPLE HTTP(s) POST FLOOD
  - SLOW (to avoid detection or make requests take a very long time)
    - LOW REQUEST RATE
    - SLOW PAGE READ
    - SLOW POST
    - SLOW LORIS
  - REALISTIC (acts like people)
    - BROWSER HTTP(s) POST FLOOD
    - ADVANCED SPIDER / AUTOMATION

COMMON DEFENSE TECHNOLOGIES (Vendors, Appliances, Automations)

DEFENSES TECHNOLOIES

- COMMON CLOUD DEFENSE TECHNOLOGIES & APPROACHES
  - Cloud Routed Scrubbing DDoS
    - Always-On
  - Cloud Layer 7 Proxy
    - On-Demand
  - Cloud Layer 7 Proxy with WAF
    - Automatic Defense
  - Cloud Layer 4 TCP Proxy
    - "Expert" Guided Defense
  - Pubic Cloud (Auto-Scale, 'Lambda')
    - Default Defense Policy Config
  - Cloud DLP
    - Customized Defense Configuration
- COMMON ISP DEFENSE TECHNOLOGIES
  - ISP Packet Scrubbing DDoS
    - IP Reputation Threat Blocking
  - ISP Layer 7 Defense (Proxy)
  - ISP Managed ACL / FW
- COMMON ON-PREMISE DEFENSES TECHNOLOGIES
  - Router ACL's
    - Mail SPAM & Phishing Filters
  - On-Premise DDoS Appliance
    - Hardened Application Logic Defenses
  - On-Premise Next-Gen Firewall
    - Network Monitoring Correlation & Response
  - On-Premise IPS
    - Active SIEM Correlation
  - On-Premise WAF
    - Behavioral Analytics & Automated Response
  - On-Premise Load Balancer Configuration
    - IP Reputation Correlation & Response
  - On-Premise Data Leak Prevention
    - Vendor API Integration & Automation
  - On-Premise Anti Virus
    - Automation & Orchestration Frameworks

Q: For stateful TCP connection attacks, what are the systems used?

COMMON ATTACK SCENARIOS - WHAT IF _____ HAPPENED?

COMMON ATTACK SCENARIOS

- PACKET FLOODS (Volumetric)
  - REQUIRING AN INTELLIGENT DEFENSE COUNTERMEASURES
    - SYN FLOOD SMALL PACKETS
    - UDP DNS REQUEST FLOOD
  - OFTEN SIMPLER TO MITIGATE
    - DNS REFLECTION FLOOD
    - UDP FLOOD RANDOM DEST. PORT
    - OUT OF STATE TCP FLOODS
- STATEFUL TCP CONNECTION ATTACKS
  - TCP CONNECTION FLOODS
  - SLOW TCP FLOOD
  - TCP MANGLE
- CRYPTO ATTACKS
  - TLS NEGOTIATION (SETUP) FLOOD
- HTTP & HTTPS ATTACKS
  - HIGH RATE (overloads)
    - SIMPLE HTTP(s) GET FLOOD
    - SIMPLE HTTP(s) POST FLOOD
  - SLOW (to avoid detection or make requests take a very long time)
    - LOW REQUEST RATE
    - SLOW PAGE READ
    - SLOW POST
    - SLOW LORIS
  - REALISTIC (acts like people)
    - BROWSER HTTP(s) POST FLOOD
    - ADVANCED SPIDER / AUTOMATION

COMMON DEFENSE TECHNOLOGIES (Vendors, Appliances, Automations)

DEFENSES TECHNOLOIES

- COMMON CLOUD DEFENSE TECHNOLOGIES & APPROACHES
  - Cloud Routed Scrubbing DDoS — Always-On
  - Cloud Layer 7 Proxy — On-Demand
  - Cloud Layer 7 Proxy with WAF — Automatic Defense
  - Cloud Layer 4 TCP Proxy — "Expert" Guided Defense
  - Pubic Cloud (Auto-Scale, 'Lambda') — Default Defense Policy Config
  - Cloud DLP — Customized Defense Configuration
- COMMON ISP DEFENSE TECHNOLOGIES
  - ISP Packet Scrubbing DDoS — IP Reputation Threat Blocking
  - ISP Layer 7 Defense (Proxy)
  - ISP Managed ACL / FW
- COMMON ON-PREMISE DEFENSES TECHNOLOGIES
  - Router ACL's — Mail SPAM & Phishing Filters
  - On-Premise DDoS Appliance — Hardened Application Logic Defenses
  - On-Premise Next Gen Firewall — Network Monitoring Correlation & Response
  - On-Premise IPS — Active SIEM Correlation
  - On-Premise WAF — Behavioral Analytics & Automated Response
  - On-Premise Load Balancer Configuration — IP Reputation Correlation & Response
  - On-Premise Data Leak Prevention — Vendor API Integration & Automation
  - On-Premise Anti Virus — Automation & Orchestration Frameworks

Q: For cryptographic attacks, which exhaust SSL/TLS handshake capacity, which are the best defenses?

COMMON ATTACK SCENARIOS - WHAT IF _____ HAPPENED?

COMMON ATTACK SCENARIOS

- **PACKET FLOODS (Volumetric)**
  - REQUIRING AN INTELLIGENT DEFENSE COUNTERMEASURES
    - SYN FLOOD SMALL PACKETS
    - UDP DNS REQUEST FLOOD
  - OFTEN SIMPLER TO MITIGATE
    - DNS REFLECTION FLOOD
    - UDP FLOOD RANDOM DEST. PORT
    - OUT OF STATE TCP FLOODS
- **STATEFUL TCP CONNECTION ATTACKS**
  - TCP CONNECTION FLOOD
  - SLOW DRIP FLOOD
  - TCP CHARG[illegible]
- **CRYPTO ATTACKS**
  - [illegible] NEGOTIA[illegible] (SETUP) FLOOD
- **HTTP & HTTPS ATTACKS**
  - HIGH RATE (overloads)
    - S[illegible] HT[illegible] G[illegible] FL[illegible]
    - SIMPLE [illegible]TP(s) POS[illegible]OD
  - SLOW (to avoid detection or make requests take a very long time)
    - LOW REQUEST RATE
    - SLOW PAGE READ
    - SLOW POST
    - SLOW LORIS
  - REALISTIC (acts like people)
    - BROWSER HTTP(s) POST FLOOD
    - ADVANCED SPIDER / AUTOMATION

COMMON DEFENSE TECHNOLOGIES (Vendors, Appliances, Automations)

DEFENSES TECHNOLOIES

- **COMMON CLOUD DEFENSE TECHNOLOGIES & APPROACHES**
  - Cloud Routed Scrubbing DDoS — Always-On
  - Cloud Layer 7 Proxy — On-Demand
  - Cloud Layer 7 Proxy with WAF — Automatic Defense
  - Cloud Layer 4 TCP Proxy — "Expert" Guided Defense
  - Pubic Cloud (Auto-Scale, 'Lambda') — Default Defense Policy Config
  - Cloud DLP — Customized Defense Configuration
- **COMMON ISP DEFENSE TECHNOLOGIES**
  - ISP Packet Scrubbing DDoS — IP Reputation Threat Blocking
  - ISP Layer 7 Defense (Proxy)
  - ISP Managed ACL / FW
- **COMMON ON-PREMISE DEFENSES TECHNOLOGIES**
  - Router ACL's — Mail SPAM & Phishing Filters
  - On-Premise DDoS Appliance — Hardened Application Logic Defenses
  - On-Premise [illegible]lext-Gen [illegible]irewall — Network Monitoring Correlation & Response
  - On-Premise IP[illegible] — Active SIEM Correlation
  - On-Premise WAF — Behavioral Analytics & Automated Response
  - On-Premise Load Balancer Configuration — IP Reputation Correlation & Response
  - On-Premise Data Leak Prevention — Vendor API Integration & Automation
  - On-Premise Anti Virus — Automation & Orchestration Frameworks

Q: For HTTP and HTTPS Attacks, what are the best defenses?

COMMON ATTACK SCENARIOS - WHAT IF _____ HAPPENED?

COMMON ATTACK SCENARIOS

PACKET FLOODS (Volumetric)					STATEFUL TCP CONNECTION ATTACKS			CRYPTO ATTACKS	HTTP & HTTPS ATTACKS						
REQUIRING AN INTELLIGENT DEFENSE COUNTERMEASURES		OFTEN SIMPLER TO MITIGATE			TCP CONNECTION FLOOD	SLOW DRIP FLOOD	TCP CHARGEN FLOOD	TLS NEGOTIATION (SETUP) FLOOD	HIGH RATE (overloads)	[illegible]	[illegible]	[illegible]	[illegible]	REALISTIC (acts like people)	
SYN FLOOD SMALL PACKETS	UDP DNS REQUEST FLOOD	DNS REFLECTION FLOOD	UDP FLOOD RANDOM DEST. PORT	OUT OF STATE TCP FLOODS					[illegible]	[illegible]	LOW REQUEST RATE	[illegible]	[illegible]	SLOW LORIS	BROWSER HTTP(s) POST FLOOD	ADVANCED SPIDER / AUTOMATION

COMMON DEFENSE TECHNOLOGIES (Vendors, Appliances, Automations)

DEFENSES TECHNOLOIES

COMMON CLOUD DEFENSE TECHNOLOGIES & APPROACHES						COMMON ISP DEFENSE TECHNOLOGIES			COMMON ON-PREMISE DEFENSES TECHNOLOGIES							
Cloud Routed Scrubbing DDoS	Cloud Layer 7 Proxy	Cloud Layer 7 Proxy with WAF	Cloud Layer 4 TCP Proxy	Pubic Cloud (Auto-Scale, 'Lambda')	Cloud DLP	ISP Packet Scrubbing DDoS	ISP Layer 7 Defense (Proxy)	ISP Managed ACL / FW	Router ACL's	On-Premise DDoS Appliance	On-Premise Next-Gen Firewall	On-Premise IPS	On-Premise WAF	On-Premise Load Balancer Configuration	On-Premise Data Leak Prevention	On-Premise Anti Virus
Always-On	On-Demand	Automatic Defense	"Expert" Guided Defense	Default Defense Policy Config	Customized Defense Configuration	IP Reputation Threat Blocking			Mail SPAM & Phishing Filters	Hardened Application Logic Defenses	Network Monitoring Correlation & Response	Active SIEM Correlation	Behavioral Analytics & Automated Response	IP Reputation Correlation & Response	Vendor API Integration & Automation	Automation & Orchestration Frameworks

Confused yet? Overwhelmed?

There are a lot of different kinds of attacks.

There are a lot of defense technologies.

No one (normal) can easily answer what kind of defense is best for a certain kind of attack.

We'll give you a few more examples & then suggest a solution – a way to make it make sense.

It's not just the kind of attack, it's the 'style' of the attack.

EVASIVE TECHNIQUES	"SCRIPT KID" or "TARGETED"		REPETITIVE or REALISTIC?	
	EASY	HARD	EASY	HARD
	Attacks with known signatures and thresholds are easiest to handle	Attacks that target your specific applications and services are not 'out of the box'	It's easier to spot repetitive robotic attacks	It's harder to spot attackers that randomize and vary their requests and timings

It's not just the kind of attack, it's the 'style' of the attack.

AGGRESSIVE or SUBTLE?	
EASY	**HARD**
It's easy to spot extremely aggressive attacks.	It's hard to pick out attackers sending regular traffic levels and requests "under the radar"

It's not just the kind of attack, it's the 'style' of the attack.

ADVERSARY EXPERIENCE	
EASY	**HARD**
Automatic 'bots' can be identified by IP Reputation and simple behavioral checks	Sophisticated attackers who change vectors, targets and understand common countermeasures

Q: Why *aren't* these great for many HTTP and HTTPS?

COMMON DEFENSE TECHNOLOGIES (Vendors, Appliances, Automations)

DEFENSES TECHNOLOIES

COMMON CLOUD DEFENSE TECHNOLOGIES & APPROACHES						COMMON ISP DEFENSE TECHNOLOGIES			COMMON ON-PREMISE DEFENSES TECHNOLOGIES							
Cloud Routed Scrubbing DDoS	Cloud Layer 7 Proxy	Cloud Layer 7 Proxy with WAF	Cloud Layer 4 TCP Proxy	Pubic Cloud (Auto-Scale, 'Lambda')	Cloud DLP	ISP Packet Scrubbing DDoS	ISP Layer 7 Defense (Proxy)	ISP Managed ACL / FW	Router ACL's	On-Premise DDoS Appliance	On-Premise Next-Gen Firewall	On-Premise IPS	On-Premise WAF	On-Premise Load Balancer Configuration	On-Premise Data Leak Prevention	On-Premise Anti Virus
Always-On	On-Demand	Automatic Defense	"Expert" Guided Defense	Default Defense Policy Config	Customized Defense Configuration	IP Reputation Threat Blocking			Mail SPAM & Phishing Filters	Hardened Application Logic Defenses	Network Monitoring Correlation & Response	Active SIEM Correlation	Behavioral Analytics & Automated Response	IP Reputation Correlation & Response	Vendor API Integration & Automation	Automation & Orchestration Frameworks

Q: Why *aren't* these great for many HTTP and HTTPS?

COMMON DEFENSE TECHNOLOGIES (Vendors, Appliances, Automations)

DEFENSES TECHNOLOIES	COMMON CLOUD DEFENSE TECHNOLOGIES & APPROACHES						COMMON ISP DEFENSE TECHNOLOGIES			COMMON ON-PREMISE DEFENSES TECHNOLOGIES							
	Cloud Routed Scrubbing DDoS	Cloud Layer 7 Proxy	Cloud Layer 7 Proxy with WAF	Cloud Layer 4 TCP Proxy	Pubic Cloud (Auto-Scale, 'Lambda')	Cloud DLP	ISP Packet Scrubbing DDoS	ISP Layer 7 Defense (Proxy)	ISP Managed ACL / FW	Router ACL's	On-Premise DDoS Appliance	On-Premise Next-Gen Firewall	On-Premise IPS	On-Premise WAF	On-Premise Load Balancer Configuration	On-Premise Data Leak Prevention	On-Premise Anti Virus
	Always-On	On-Demand	Automatic Defense	"Expert" Guided Defense	Default Defense Policy Config	Customized Defense Configuration	IP Reputation Threat Blocking			Mail SPAM & Phishing Filters	Hardened Application Logic Defenses	Network Monitoring Correlation & Response	Active SIEM Correlation	Behavioral Analytics & Automated Response	IP Reputation Correlation & Response	Vendor API Integration & Automation	Automation & Orchestration Frameworks

Cloud (and ISP) Packet Scrubbing DDoS has problems with:

- Slow HTTP and HTTPS Requests
- HTTPS (decryption) – can't see into the payload
- HTTP KEEP-ALIVE (one TCP connection shared for many requests)
- Doesn't often see replies (it's usually asymmetric)
- There are certain kinds of attacks that can be stopped, for HTTP, certain TLS abuses, but in general the attacks must be very high in rate to be detected in the cloud – usually the site will go down sooner.

Cloud Layer 4:

- Not Layer 7 Aware at all (mainly used for TCP Forwarding)

Public Cloud Scaling

- It CAN scale and Scale and SCALE – but you PAY for it! ($$$)
- Scaling is not a really defense – you always need avoid processing attack requests
- Cloud without DDoS protection also does not survive.

On-Premise:

- Appliances can do pretty well, but if they are not set up for HTTPS decryption there will be limitations and attacks will go through.
- Next-Gen Firewalls strangely do very little at Layer 7 re: DDoS protection. Even if they have the capability, it is almost never enabled.
- IPS can detect many types of attacks, but most IPS do not decrypt HTTPS. If they do they can go from 'red' to green'.

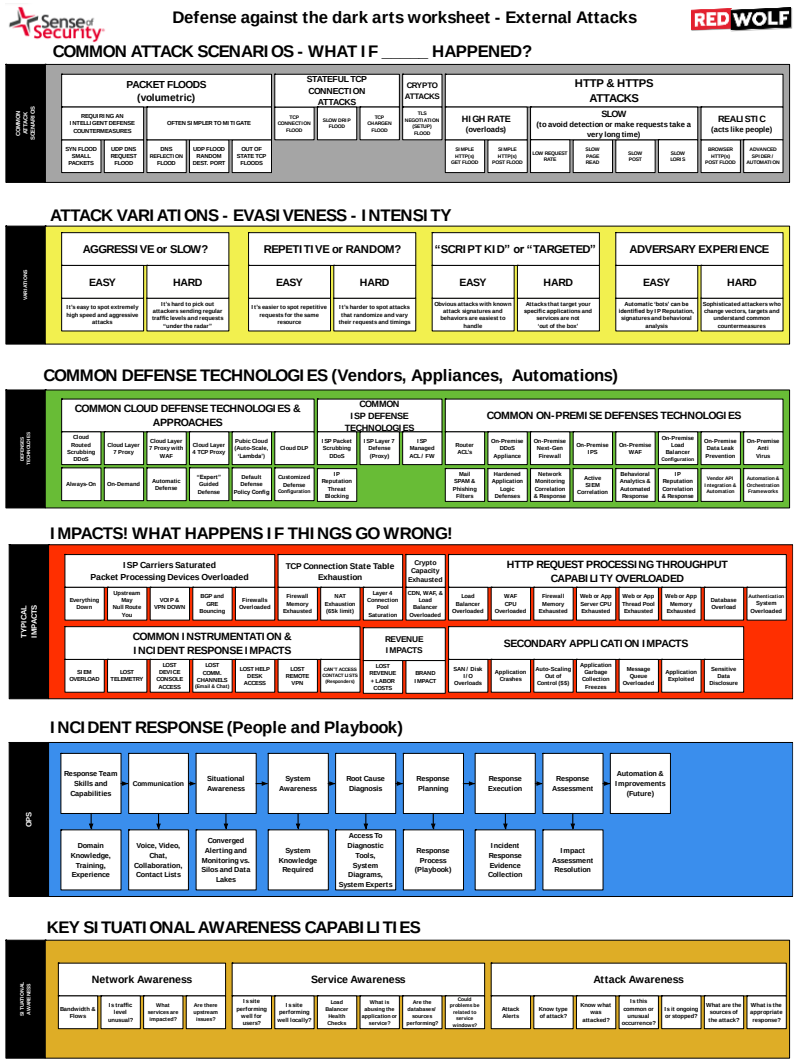
Feels hopeless? Don't Give Up!

DDoS is not one problem anymore than "Security" is a simple thing.

You can break the problem down and deal each attack "category" & "style"

Break DDoS Down Into Categories
Volumetric (Bandwidth Oriented)
Volumetric (Packet Oriented)
Connection Oriented
Cryptographic Attacks
General Layer 7 Request Oriented
Targeted Layer 7 Application Attacks

Just about to break for coffee!



ATTACK!

HTTP GET REQUEST FLOOD

A Layer 7 Request Flood
To Home Page URL
Retrieves "/" Over and over

ATTACK!

TCP SLOW DRIP

Attacker opens up TCP Connection(s) and Sends a tiny drip of information every second

ATTACK!

SYN FLOOD

Attackers send flood of SYN packets, expecting you to ACKnowledge them

DIFFICULTY

THE LONE WOLF

A single IP Address Attacks!

DIFFICULTY

A MODEST MOB

100 to 1000 Globally Distributed Attackers!

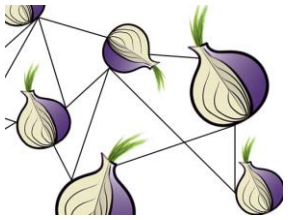
DIFFICULTY

DEEPLY DISTRIBUTED

A Large Global Botnet!
5000 to 100,000 Attackers!

DIFFICULTY

THE DARK WEB



Attackers come from "The Dark Web" and emerge from TOR EXIT NODES

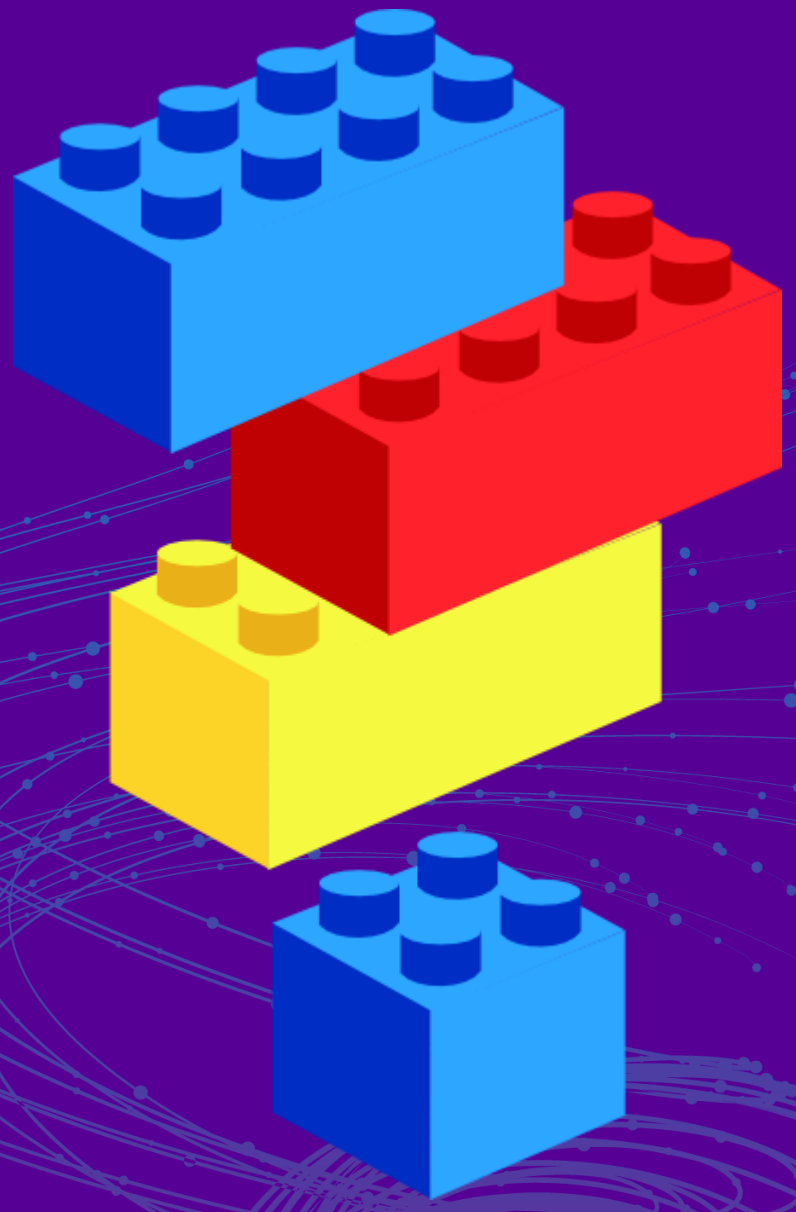
Sense of Security® RED WOLF

RSAConference2019

Tea/Coffee Break – 15 Minutes

RSAConference2019

LAB3-W310
How to Design and Operate a DDOS Testing Program



GAME TIME!

45 Minutes

Introducing: Atak Warz!

The Rulezzz – Attack Cards

ATTACK!

TCP CONNECTI ON FLOOD - SLOW DRI P

Attacker opens up TCP Connection(s) and Sends a tiny drip of information every second

ATTACK!

VOLUMETRI C SYN FLOOD

Attackers send flood of SYN packets, expecting you to ACKnowledge them

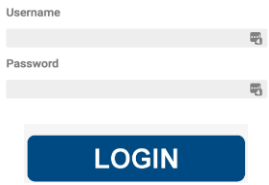
ATTACK!

HTTPS GET REQUEST FLOOD

A Layer7 HTPS Request Flood To Homepage URL Retrieves "/ " Over and over

ATTACK!

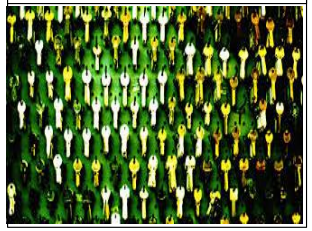
HTTPS POST FORM ATTACK



Attackers try to fill online forms repeatedly
E.g. Login Page Attack

ATTACK!

CRYPTOGRAPHI C EXHAUSTI ON



Attackers try to exhaust your SSL/ TLS Capacity

ATTACK!

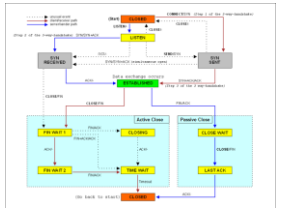
VOLUMETRI C DNS QUERY FLOOD

DNS
DOMAIN NAME SERVICES

Attackers send many legitimate DNS requests to your DNS servers

ATTACK!

VOLUMETRI C TCP OUT OF STATE



Attackers send PSH, ACK's, TCP RESET's and other out-of-state packets

ATTACK!

HTTPS GET SLOW READ

Attackers make a legitimate HTTPS request, but read response back VERY slowly

The Rulezzz – Modifiers

INTENSITY

STEALTHY

Each attacker will send a very small amount of attack traffic — much lower than a regular user

INTENSITY

LIKE A REAL USER

Each attacker generates the same amount of traffic and requests as a legitimate user

INTENSITY

A BIT AGGRESSIVE

Each attacker generates traffic that is a little bit more aggressive more than real users generate

INTENSITY

HIGH RATE FROM SOURCE

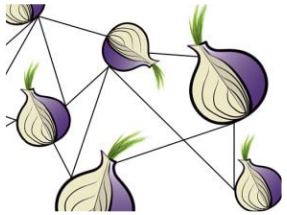
IN

OUT

Each Attacker Will Attempt High Bitrates Rates and High Packet Rates - Obvious Attackers

DISTRIBUTION

THE DARK WEB



Attackers come from "The Dark Web" and emerge from TOR EXIT NODES

DISTRIBUTION

THE LONE WOLF

A single IP Address Attacks! Bandwidth: 1-10 Megabit/sec

DISTRIBUTION

A MODEST MOB

100 to 200 Globally Distributed Attackers! Each sends between 0.5 and 10 megabit/sec

DISTRIBUTION

DEEPLY DISTRIBUTED

A Large Global Botnet! 5000 to 100,000 Attackers!

The Rulezzz – Defense Cards

DEFENSE

On-Premise Signature WAF

Blocks known signatures

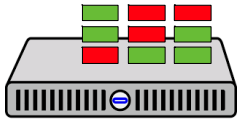
DEFENSE

On-Premise Advanced WAF

Advanced WAF with signature capability + behavioral learning and adaptive attack blocking

DEFENSE

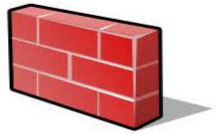
On-Premise DDoS Appliance



On Premise DDoS Defense Appliance

DEFENSE

On-Premise Next-Gen Firewall



Firewall with application defenses

DEFENSE

Generic Cloud Layer 7 HTTP Attack Defense

A Typical / Generic Cloud CDN, CDN+WAF, Proxy-Based DDoS Defense

DEFENSE

Cloud DDoS Packet Scrubbing

Traffic intercepted by cloud DDoS packet-scrubbing service

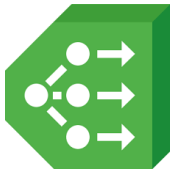
DEFENSE

Cloud CDN (Proxies Origin Server)

A Cloud CDN with no specific HTTP Protections —i.e. no WAF, no HTTP DDoS

DEFENSE

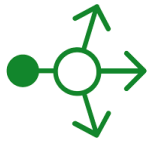
Cloud Layer 4 TCP Proxy



A Cloud service that proxies TCP connections to origin servers. A "TCP Port Forwarder"

DEFENSE

CORRELATION TCP CONNECTIONS



Correlates TCP state across multiple devices & blocks attackers by API automation

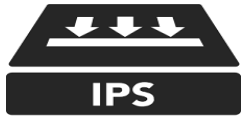
DEFENSE

CORRELATION SIEM WEB LOG

Correlates web request logs from web server's and SIEM & blocks attackers by API automation

DEFENSE

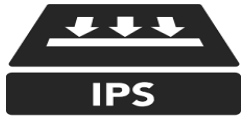
On-Premise IPS (no HTTPS)



Intrusion Prevention system with typical signatures detecting compromised hosts & attacks

DEFENSE

On-Premise IPS (HTTPS)

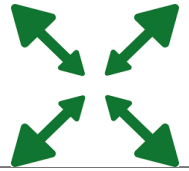


DECRYPT

Intrusion Prevention system capable of decrypting HTTPS traffic and analyzing them

DEFENSE

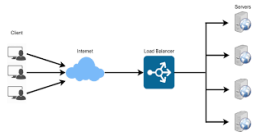
Public Cloud Auto-Scale



As request rate increases new servers will be deployed automatically to scale to load

DEFENSE

On-Premise Layer 7 Load Balancer



EXPLANATION

The Rules – Game Style 1

ATTACKER:

Choose 1 attack card
Choose 1 intensity card
choose 1 distribution card

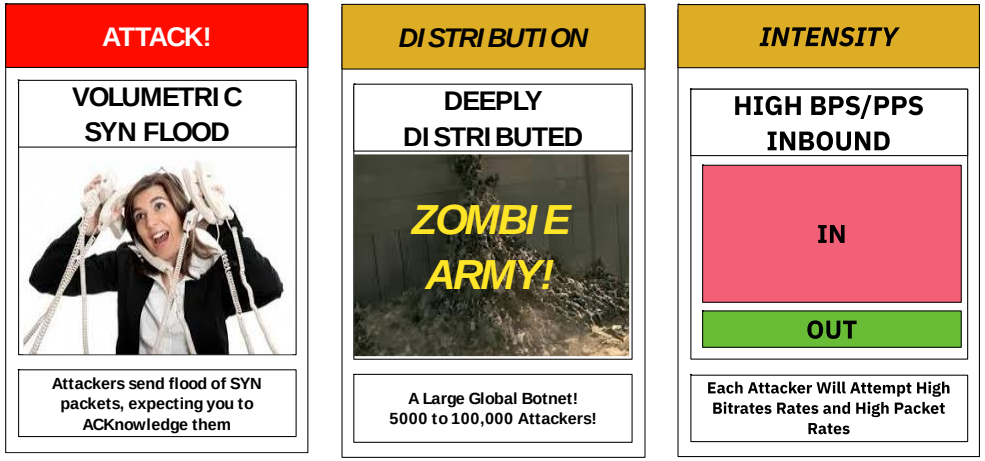
PLAY THIS

DEFENDER:

Find the best defense -> PLAY THIS
Find the ‘worst defense -> DISCUSS THIS

REPEAT for another attack

Example 1 - Attacker deploys 3 cards: Attack, Distribution, Intensity



Example 1 - Defender deploys BEST and shows WORST countermeasure

ATTACK!

VOLUMETRIC SYN FLOOD

Attackers send flood of SYN packets, expecting you to ACKnowledge them

DISTRIBUTION

DEEPLY DISTRIBUTED

A Large Global Botnet! 5000 to 100,000 Attackers!

INTENSITY

HIGH BPS/PPS INBOUND

IN

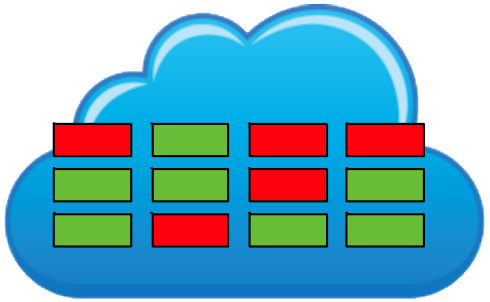
OUT

Each Attacker Will Attempt High Bitrates Rates and High Packet Rates

BEST

DEFENSE

Cloud DDoS Packet Scrubbing

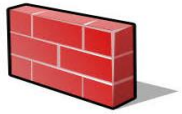


Traffic intercepted by cloud DDoS packet-scrubbing service

WORST

DEFENSE

On-Premise Next-Gen Firewall



Firewall with application defenses

Example 2

ATTACK!

TCP CONNECTION FLOOD - SLOW DRIP

Attacker opens up TCP Connection(s) and Sends a tiny drip of information every second

DISTRIBUTION

A MODEST MOB

100 to 1000 Globally Distributed Attackers!

INTENSITY

OBVIOUS ABUSE

Each attacker generates traffic that is obviously abusive —much more than real users.

Example 2

Is this the best?

ATTACK!

TCP CONNECTION FLOOD - SLOW DRIP

Attacker opens up TCP Connection(s) and Sends a tiny drip of information every second

DISTRIBUTION

A MODEST MOB

100 to 1000 Globally Distributed Attackers!

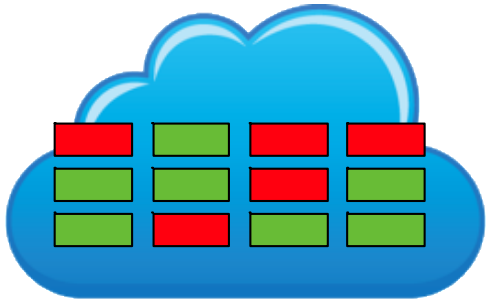
INTENSITY

OBVIOUS ABUSE

Each attacker generates traffic that is obviously abusive —much more than real users.

DEFENSE

Cloud DDoS Packet Scrubbing



Traffic intercepted by cloud DDoS packet-scrubbing service

Example 2

Or is this?

ATTACK!

TCP CONNECTION FLOOD - SLOW DRIP

Attacker opens up TCP Connection(s) and Sends a tiny drip of information every second

DISTRIBUTION

A MODEST MOB

100 to 1000 Globally Distributed Attackers!

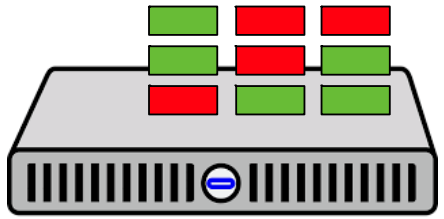
INTENSITY

OBVIOUS ABUSE

Each attacker generates traffic that is obviously abusive —much more than real users.

DEFENSE

On-Premise DDoS Appliance



On Premise DDoS Defense Appliance

There are EASY and HARD cases here

Consider three different *styles* of TCP Flood DDoS Attacks:

EASY	MEDIUM	HARD
Attackers: 1 IP Address # of TCP Connections: 1000 Rate: All At Once	Attackers: A Few (100) Attackers # of TCP Connections: 1 Million (10k TCP connections per attacker) Rate: Over 5 Minutes	Attackers: 1000's (big botnet) # of TCP Connections: As many as possible Rate: Open 1 TCP Connection Every Second

Here are the best defenses for each – note there is no silver bullet:

DDoS IPS	Load Balancers & DDoS (rare)	SIEM Correlation

Sense of Security RED WOLF

Summing it up - Is there a silver bullet? A single vendor that solves all problems? Is there ever one?

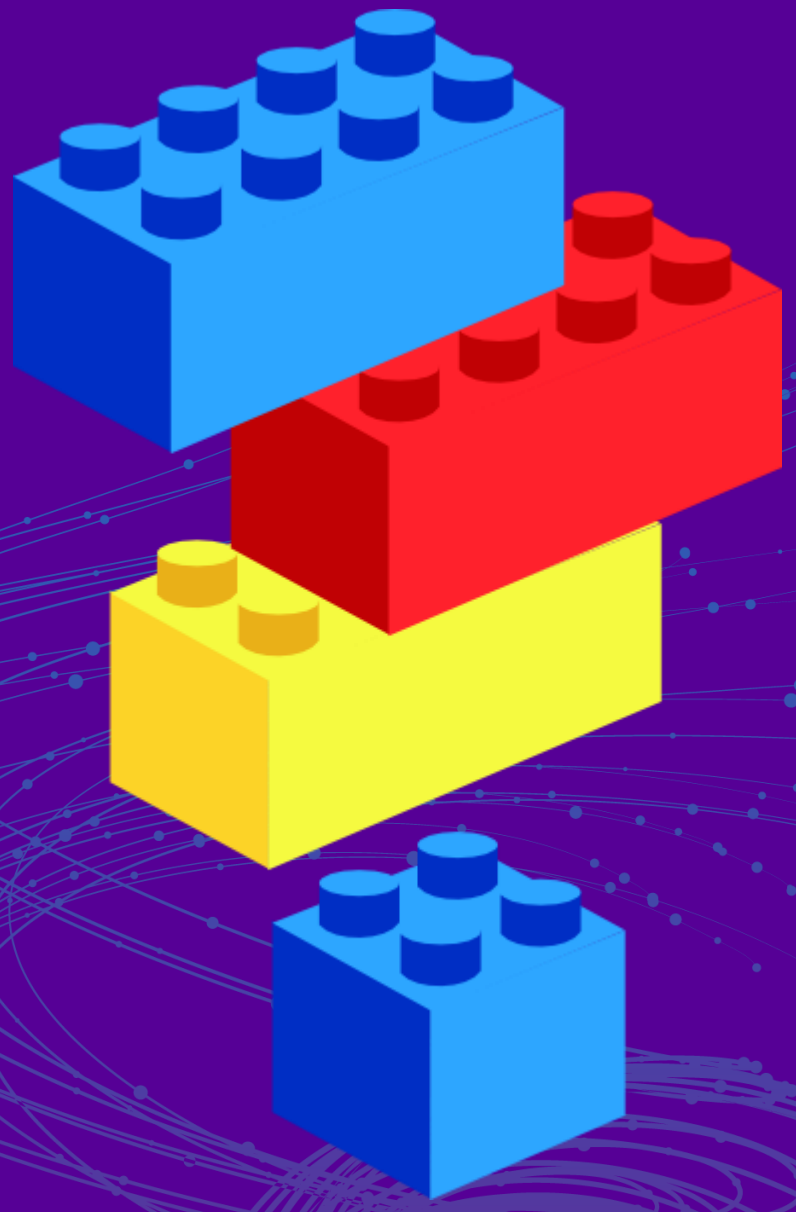
What we've covered so far:

1. DDoS IS Volumetric
   (that you knew)
2. DDoS IS more than Volumetric (Web Login Attack, TCP Attack)
   (Bandwidth doesn't matter)
3. Even within one kind of attack there are many variations – just like baseball pitches. i.e. the 'Style / Sophistication'
4. You'll need multiple defense technologies & controls

RSAConference2019

LAB3-W310
How to Design and Operate a DDOS Testing Program

Misconceptions and Why Test?



Misconceptions

"My organization has multiple layered defenses including: CDN's, Public Cloud, Lambda Functions, Cloud WAF, Cloud DDoS, On-Premise DDoS, Advanced Firewalls, The Latest WAF's and more – I have so much security and my teams are great I am confident I don't need to test it."

- CISO with a really big budget

(sounds complicated – are complicated systems easier to configure and maintain?)

Misconceptions

“ I’m Safe BECAUSE …..

my ISP does DDoS"

Misconceptions

“ I’m Safe BECAUSE …..

my ISP does DDoS"	But is it tuned?

Misconceptions

" I'm Safe BECAUSE .....

I just bought an F5 and turned on it's DDoS defenses"

Misconceptions

" I'm Safe BECAUSE .....

I just bought an F5 and turned on it's DDoS defenses"	But who is the defence protection automated?

Misconceptions

" I'm Safe BECAUSE .....

I have an on-premise DDoS appliance
- I see it blocking attacks all the time"

Misconceptions

" I'm Safe BECAUSE .....

I have an on-premise DDoS appliance - I see it blocking attacks all the time"	But what about the attacks it ISN'T blocking?

Misconceptions

“ I’m Safe BECAUSE …..

I use a leading cloud defense provider"

Misconceptions

“ I’m Safe BECAUSE …..

I use a leading cloud defense provider"	But what about app layer attacks?

Misconceptions

" I'm Safe BECAUSE …..

I have a Hybrid Solution – Both Cloud scrubbing and On Prem Technology

Misconceptions

" I'm Safe BECAUSE …..

I have a Hybrid Solution – Both Cloud scrubbing and On Prem Technology	Got Lots of $'s. Tested it yet?

Misconceptions

“ I’m Safe BECAUSE …..

I use cloud-based auto-scale servers so I will scale to the load"

Misconceptions

“ I’m Safe BECAUSE …..

I use cloud-based auto-scale servers so I will scale to the load"	But what about the backend load?

Misconceptions

" I'm Safe BECAUSE .....

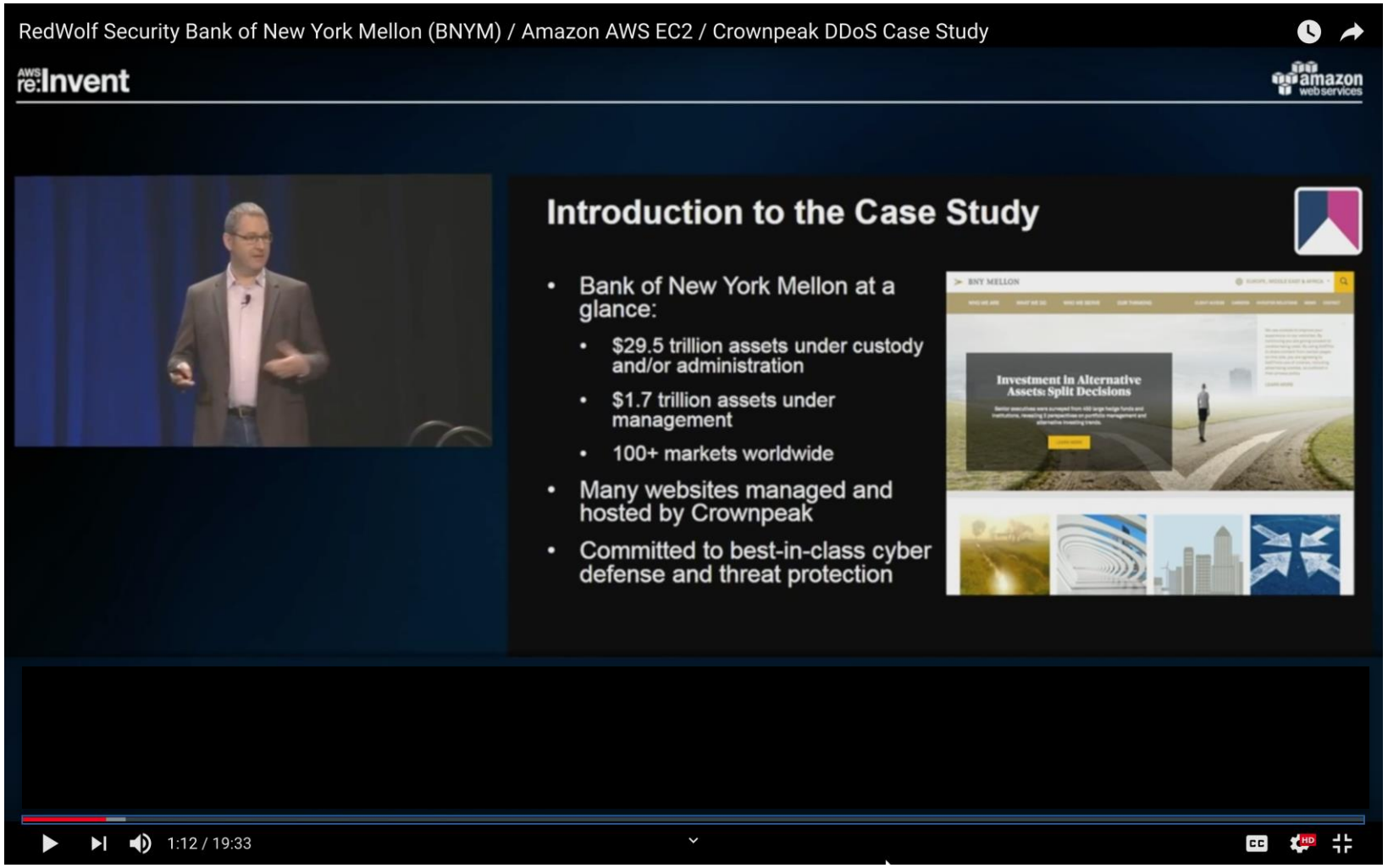
my ISP does DDoS"	But is it tuned?	YOU NEED DEFENCE IN DEPTH
I just bought an F5 and turned on it's DDoS defenses"	But who is the defence protection automated?	
I have an on-premise DDoS appliance - I see it blocking attacks all the time"	But what about the attacks it ISN'T blocking?	
I use a leading cloud defense provider"	But what about app layer attacks?	
I have a Hybrid Solution – Both Cloud scrubbing and On Prem Technology	Got Lots of $'s. Tested it yet?	
I use cloud-based auto-scale servers so I will scale to the load"	But what about the backend load?	

RSAConference2019

LAB3-W310
How to Design and Operate a DDOS Testing Program

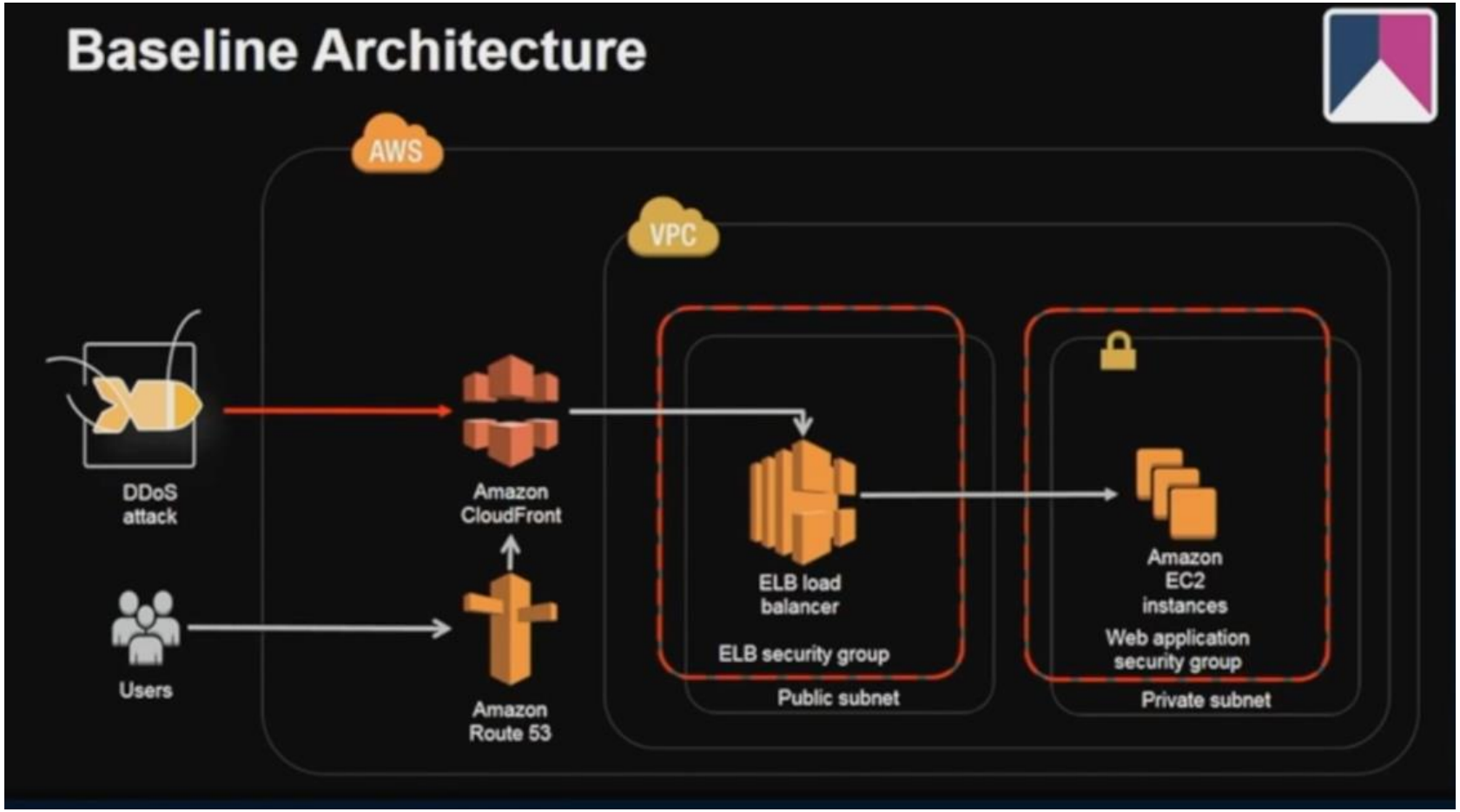
How to Develop Your DDoS Testing Program

An example of a DDoS testing program and improvements it can bring a cloud environment

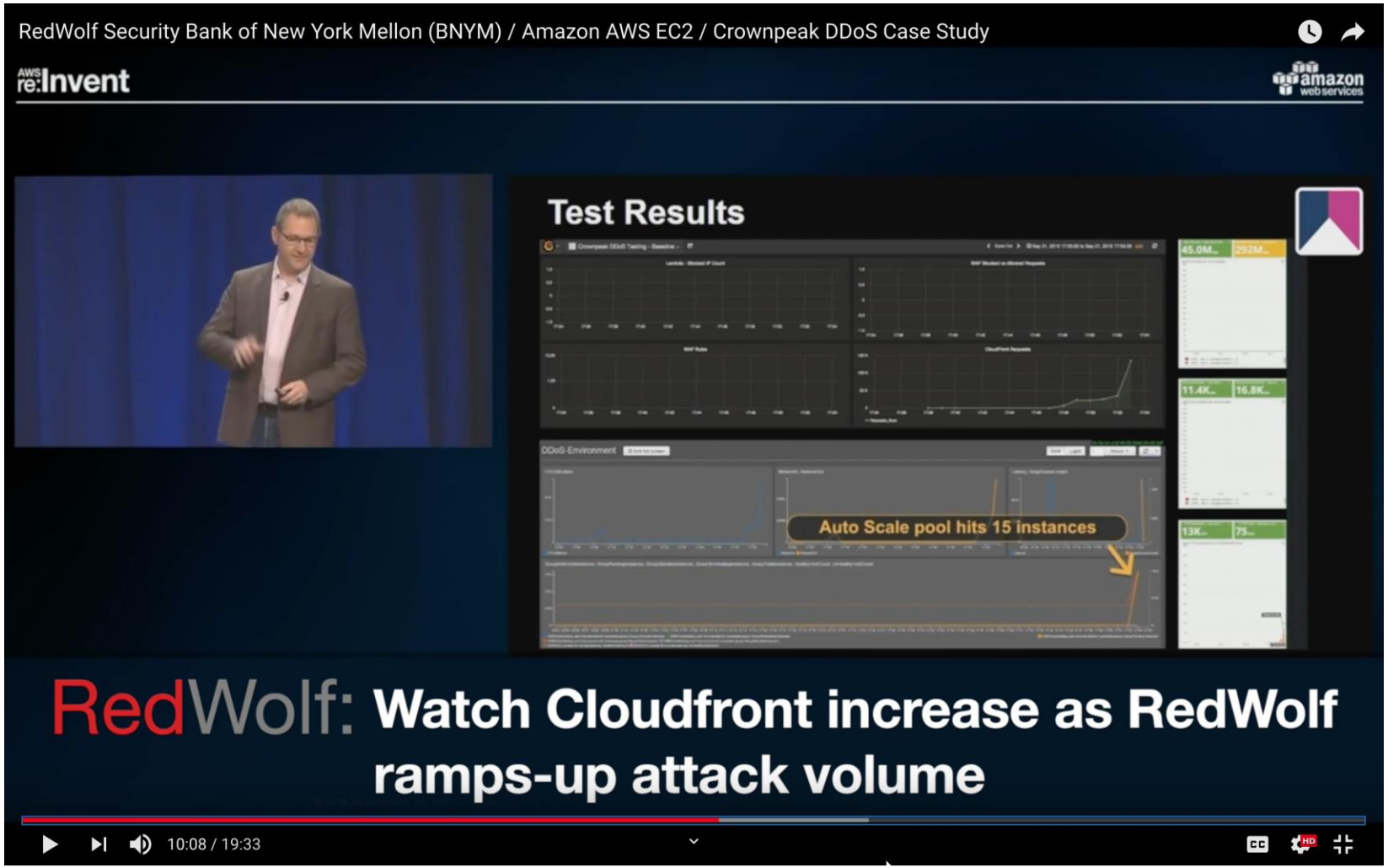


https://www.redwolfsecurity.com/resources/case-study-bank-new-york-mellon-crown-peak-amazon-aws/

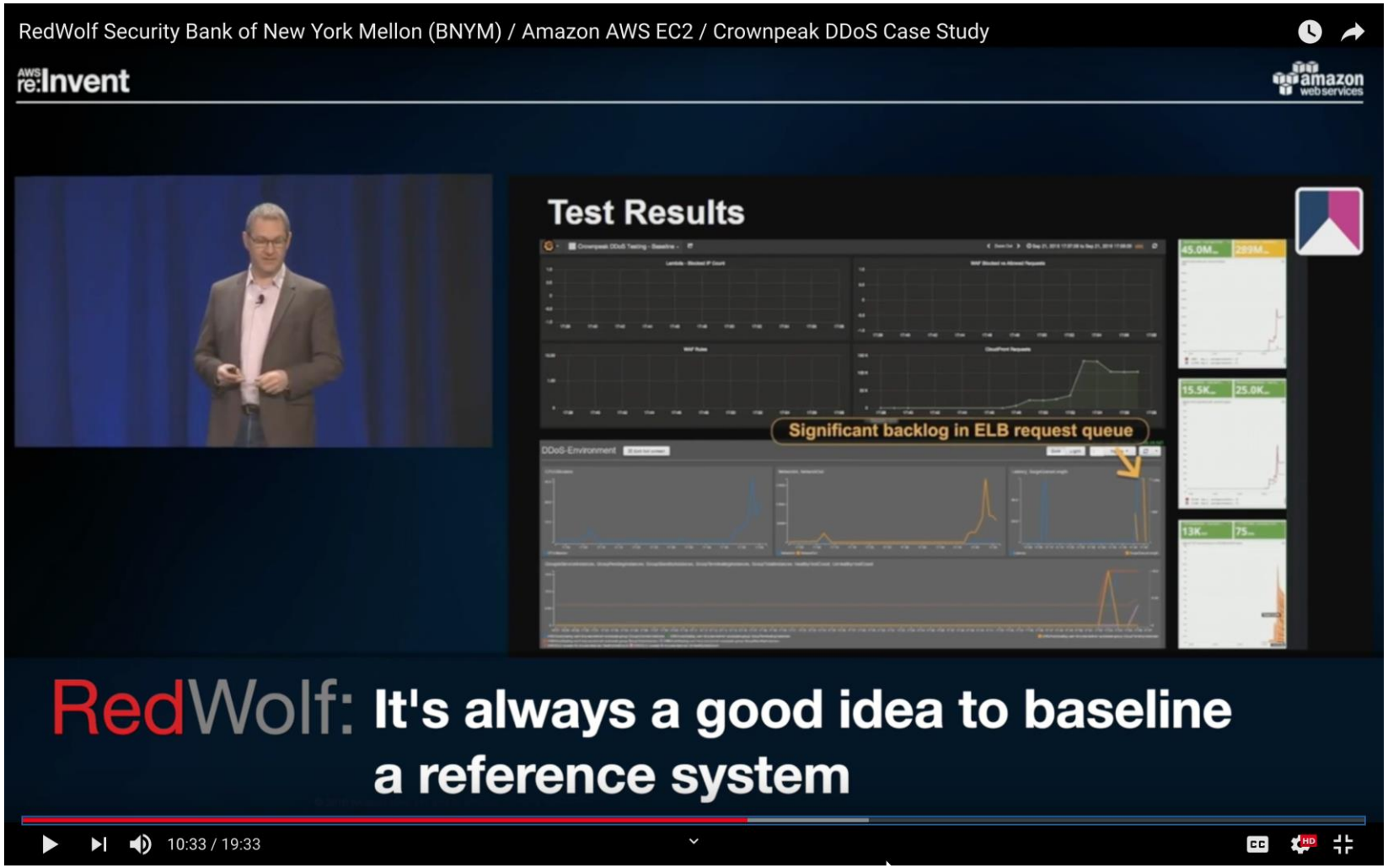
Baseline architecture – Cloud Front + ELB + Auto-Scale Group



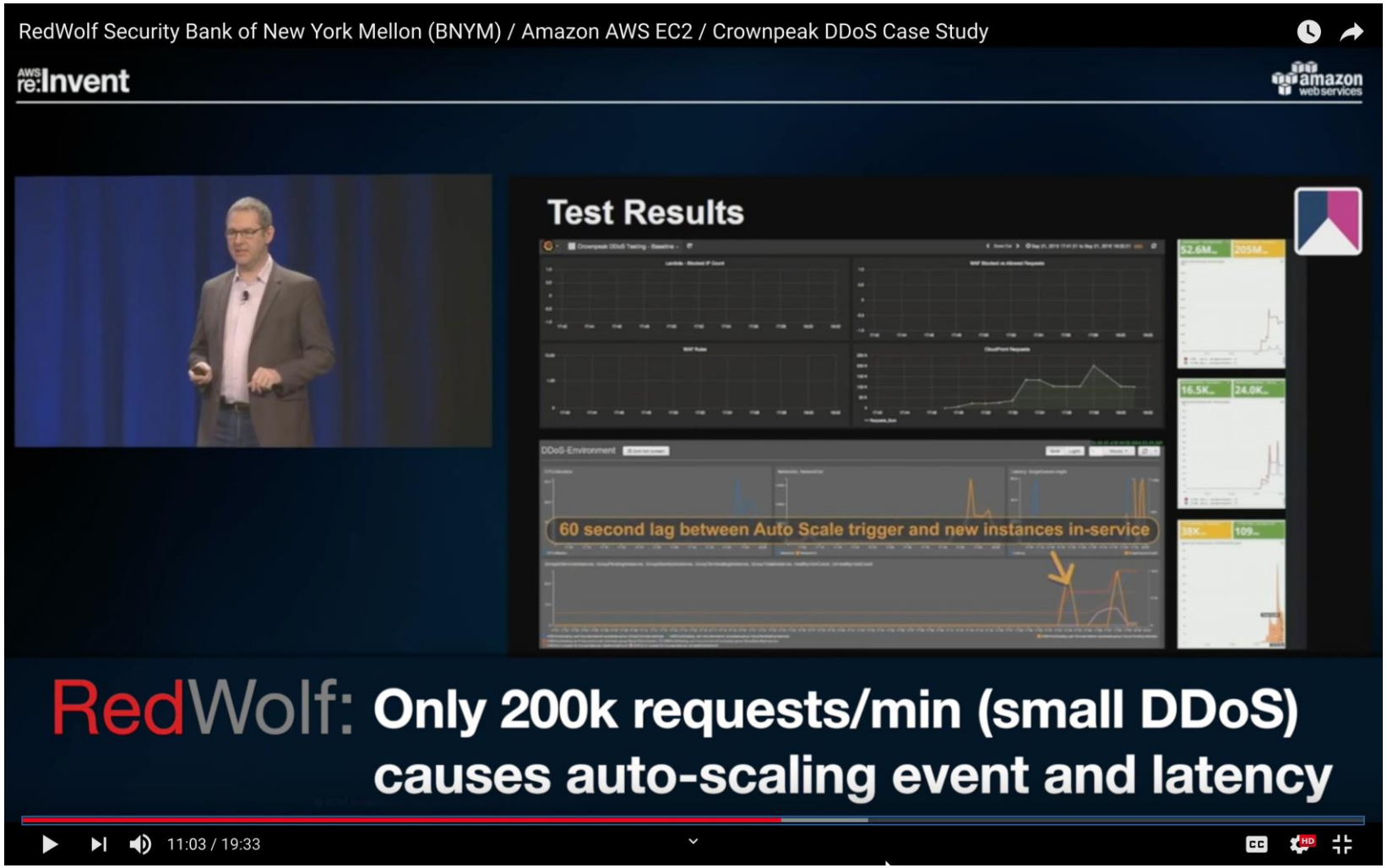
Auto-scale to 15 instances instantly



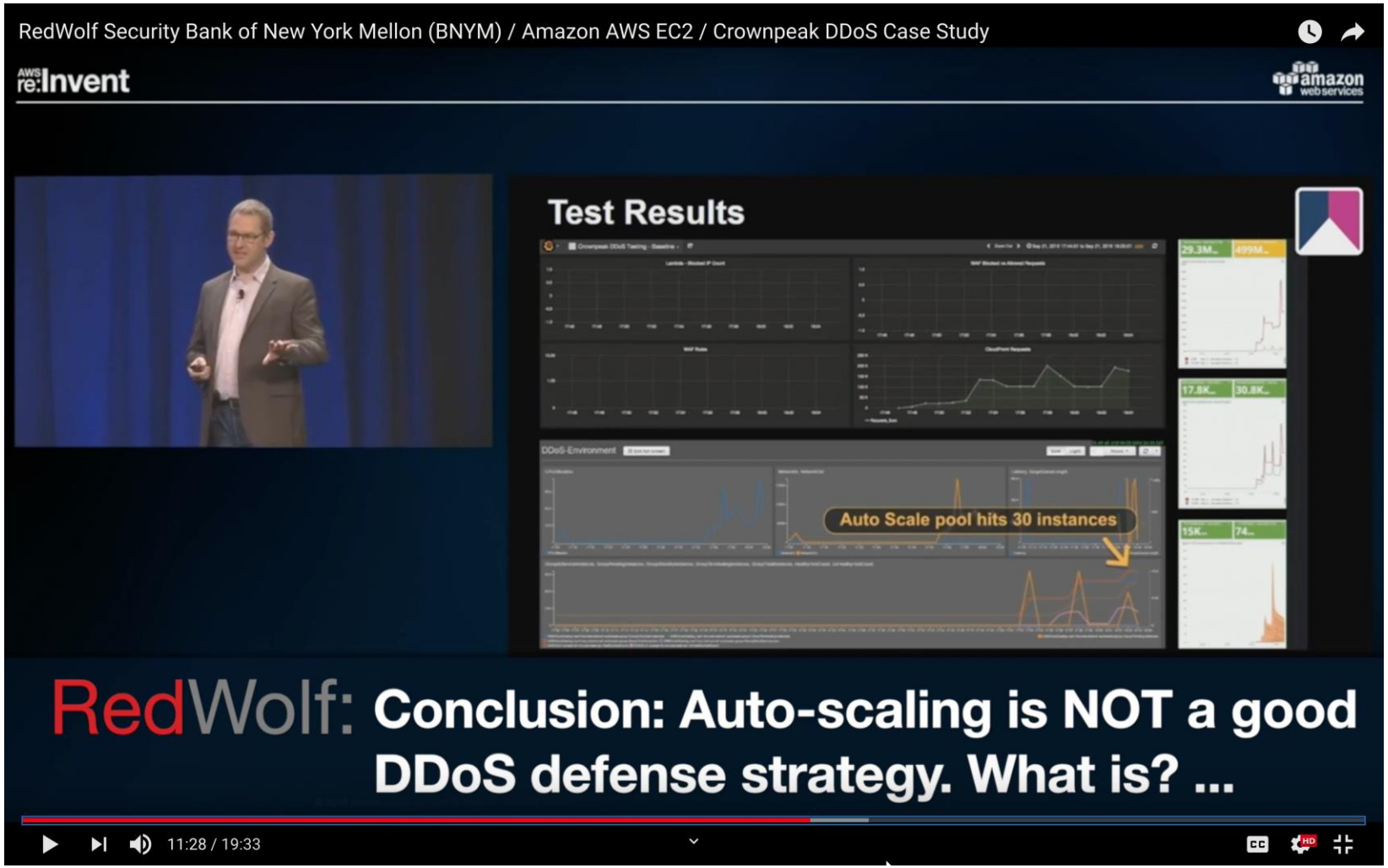
Elastic Load Balancer (ELB) backlog in request queue
Requests not being handled



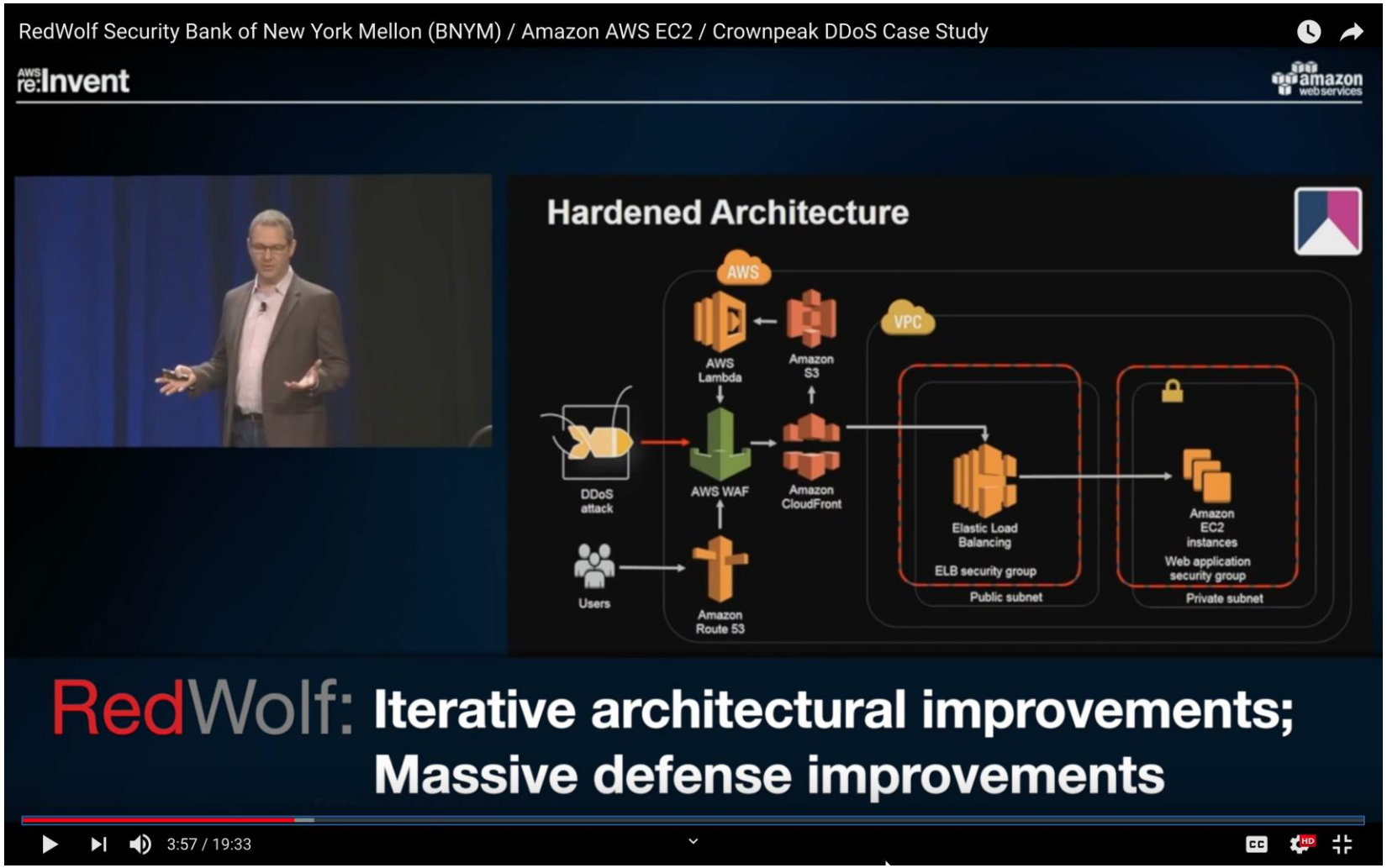
60 Second Lag between auto-scale trigger and new instances
60 second downtime too



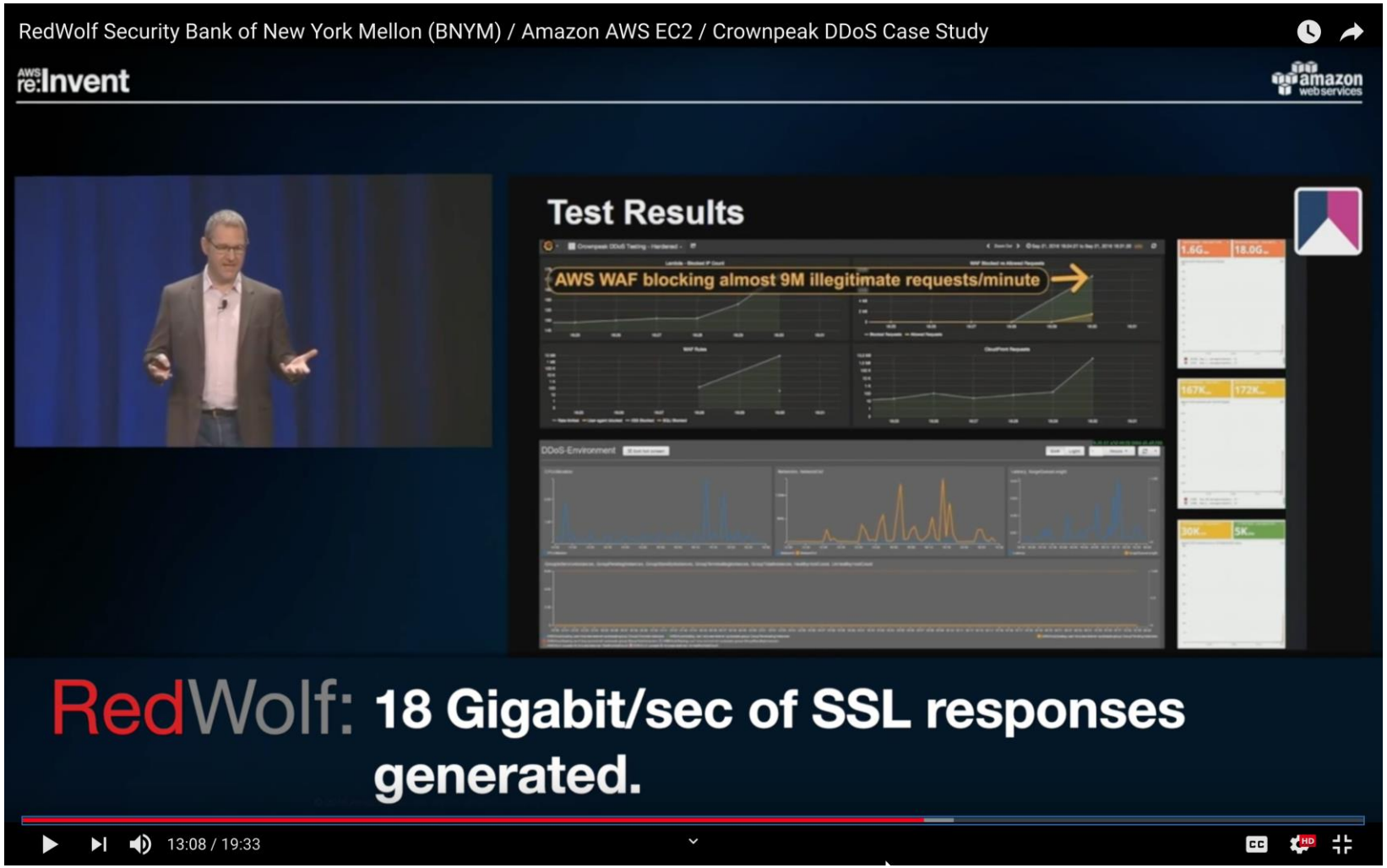
Auto-Scaling is not a DDoS defense – 30 instances
Capacity should not be used to service attack requests



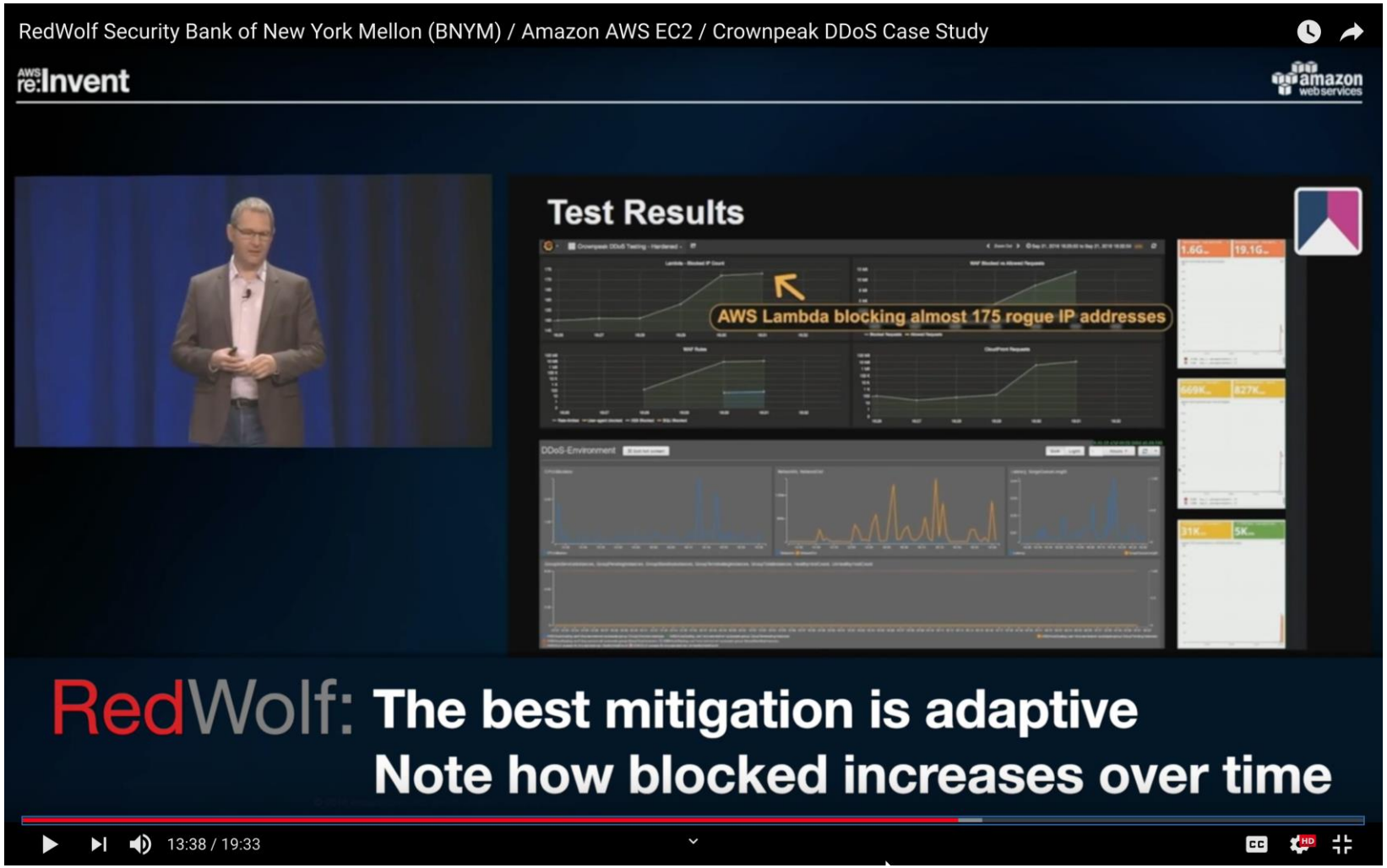
Hardened Architecture



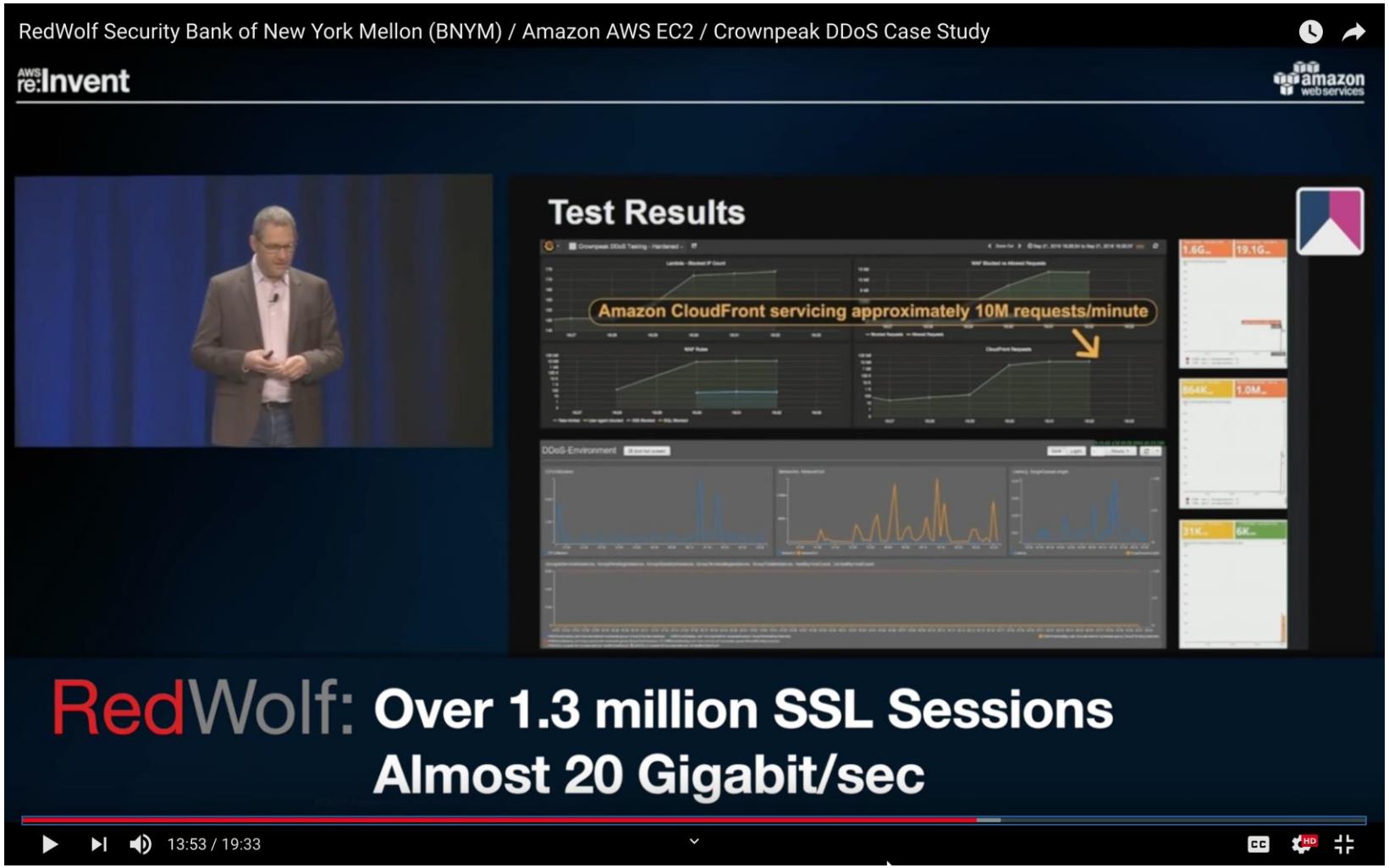
Blocking 9 million requests/minute



175 (of 200) attackers blocked

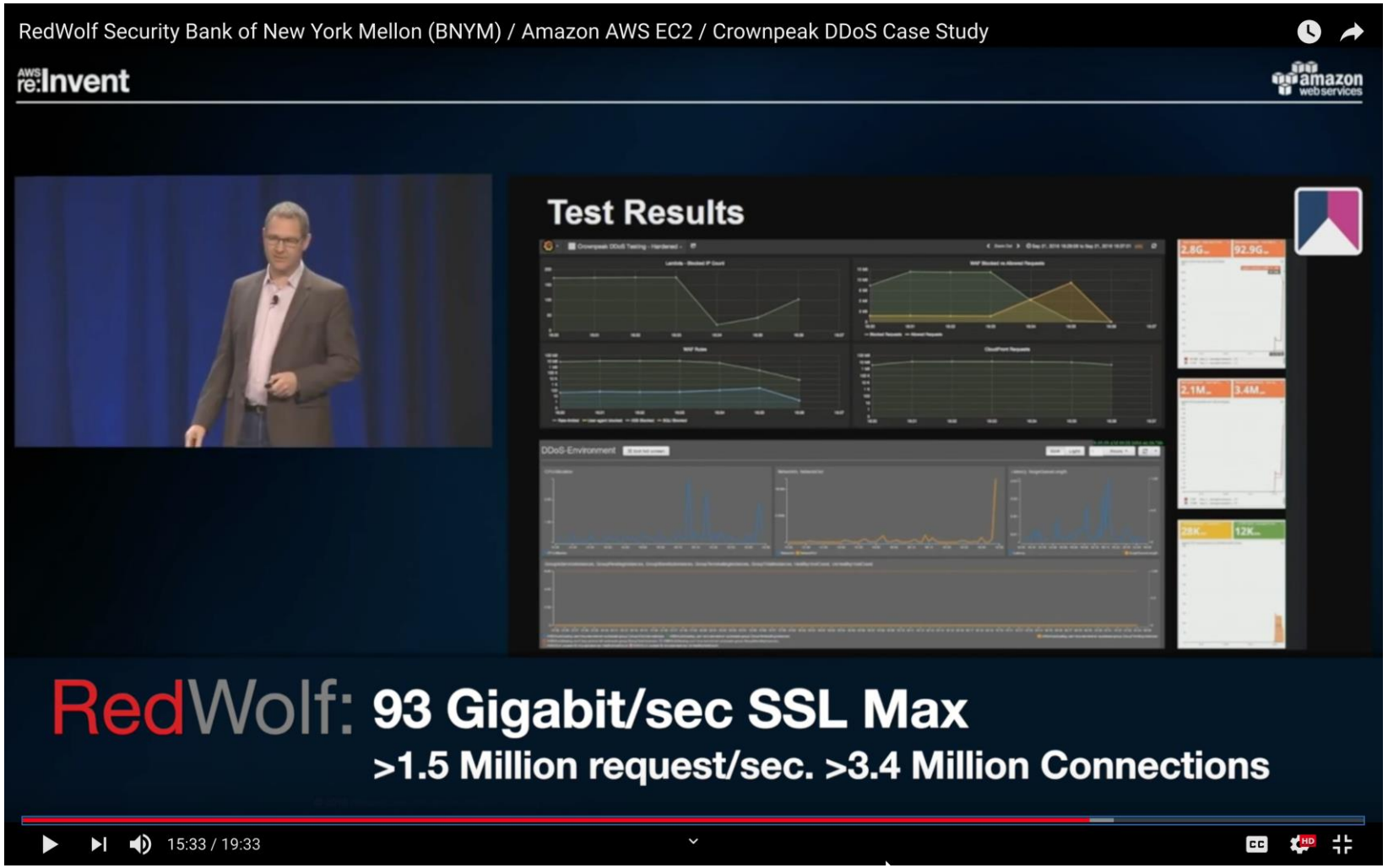


Over 1.3 million SSL sessions
Almost 20 Gigabit/sec SSL



20 Gigabit/sec SSL attack – no pressure on Auto Scale Group

Example of DDoS DDoS & Cloud (AWS) Testing Program Tuning achieved 100x improvement over baseline



Key Elements of a DDoS Testing Program

DISCOVERY	**Available Defense Systems** What defense systems do you have? On-premise, In Cloud	**Defense Capabilities** What are the defense configurations? What is enabled? What is not?	**Services to Protect** What do you need to protect? What are mission critical services?	**Application Attack Surface** What features, like forms, are likely to be attacked?
TESTING	**Baseline Service Performance** Find out how scalable the actual service Do load testing and baselining	**Test Local Defenses** Router, DDoS Appliances, Firewalls, Load Balancer, WAF, IPS, etc…	**Test 3rd Party Vendors** CDN, Cloud DDoS, Cloud WAF, Managed Monitoring & Detection	**Service Monitoring** HTTP(s), DNS, TCP, Routes BGP, SMTP, IPSEC and more
IMPROVE	**Defenses** Tighten Configurations Fill in Control-Gaps	**Operational Response Skills** Cyber-Drills, Online Run-Books, Cross-Silo Communications	**Processes** Incident Response Procedures, Triggers & Correlation Rules	**Automation** Scheduled Continuous Automated Testing Detect Regressions Automatically

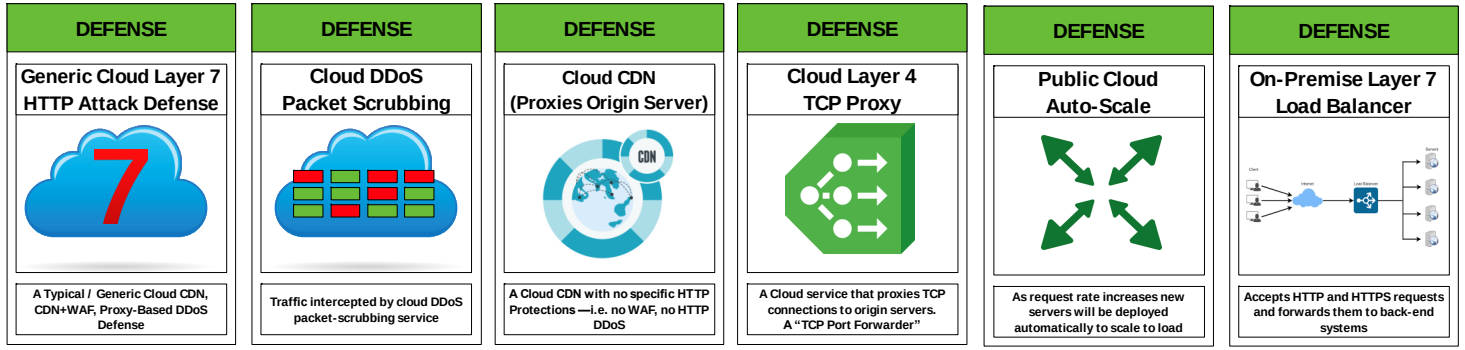
Key Elements of a DDoS Testing Program

DISCOVERY	Available Defense Systems	Defense Capabilities	Services to Protect	Application Attack Surface
	What defense systems do you have? On-premise, In Cloud	What are the defense configurations? What is enabled? What is not?	What do you need to protect? What are mission critical services?	What features, like forms, are likely to be attacked?

Identify Defense Elements

Available Defense Systems
What defense systems do you have?
On-premise, In Cloud

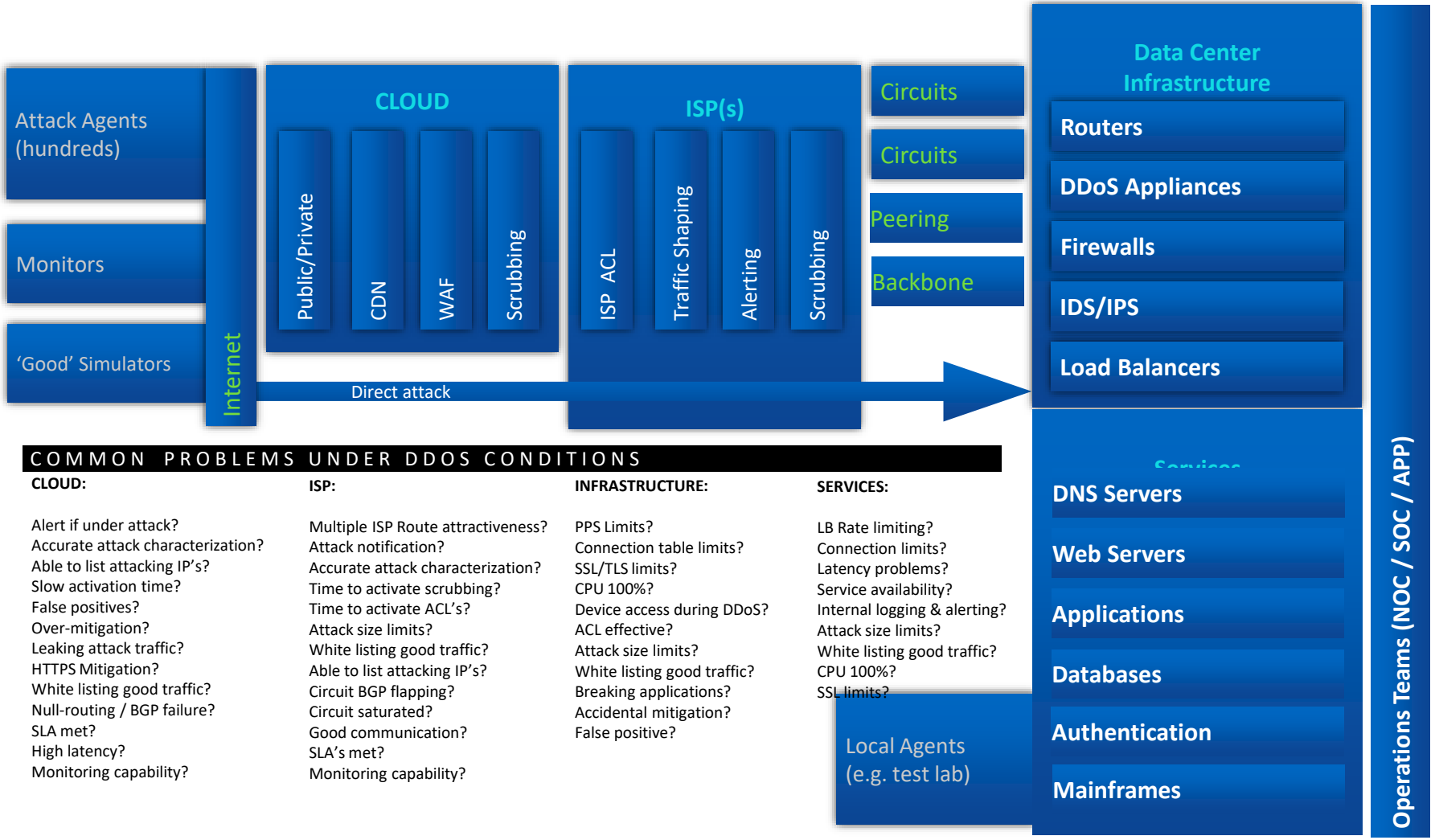
- What defense technologies do you have
  - In Cloud
  - On Premise
  - Built into the applications themselves
- Inventory should contain:
  - Is it on-premise or off-premise
  - The kind of defense it is (DDoS Scrubbing, WAF, …)
  - Vendor and key contact
  - Operational Subject-matter-expert
  - Where do logs, alerts, and metrics go



Identify Defense Elements

Available Defense Systems

What defense systems do you have?
On-premise, In Cloud



COMMON PROBLEMS UNDER DDOS CONDITIONS

CLOUD:

Alert if under attack?
Accurate attack characterization?
Able to list attacking IP's?
Slow activation time?
False positives?
Over-mitigation?
Leaking attack traffic?
HTTPS Mitigation?
White listing good traffic?
Null-routing / BGP failure?
SLA met?
High latency?
Monitoring capability?

ISP:

Multiple ISP Route attractiveness?
Attack notification?
Accurate attack characterization?
Time to activate scrubbing?
Time to activate ACL's?
Attack size limits?
White listing good traffic?
Able to list attacking IP's?
Circuit BGP flapping?
Circuit saturated?
Good communication?
SLA's met?
Monitoring capability?

INFRASTRUCTURE:

PPS Limits?
Connection table limits?
SSL/TLS limits?
CPU 100%?
Device access during DDoS?
ACL effective?
Attack size limits?
White listing good traffic?
Breaking applications?
Accidental mitigation?
False positive?

SERVICES:

LB Rate limiting?
Connection limits?
Latency problems?
Service availability?
Internal logging & alerting?
Attack size limits?
White listing good traffic?
CPU 100%?
SSL limits?

How are they configured?

Defense Capabilities
What are the defense configurations?
What is enabled? What is not?

- **The actual protection depends on the configuration**
- **For each defense system, document the features/capabilities**
- **Find out what is enabled and disabled**
- **Organizations often use only 10% to 20% of what a defense device is capable of!**

Traffic Level Controls
[ ] Block if Source IP sends high packet rate above threshold
[ ] Block if Source IP sends high bitrate above threshold

Packet Challenge
[ ] Challenge SYN packets if SYN rate to destination above threshold
[ ] Challenge UDP DNS requests if UDP rate to destination above threshold
[ ] Reset TCP idle TCP sessions

Protocol Validation Controls
[ ] Block request if source fails TLS protocol handshake
[ ] Block request fails protocol checks
[ ] Block request if buffer overflow attempt detected

Reputation and Geographic Blocking
[ ] Block if Source IP geolocation matches blocked locations
[ ] Block if Source IP has bad IP reputation (e.g. TOR, known botnet)

Signature Blocking
[ ] Block Injection Request Patterns
[ ] Block Cross-Site Scripting Patterns
[ ] Block Bad User-Agents

Behavior Blocking
[ ] Block high client request rates
[ ] Block repetitive requests for same resource
[ ] Block very slow but repetitive authentication attempts
…

Services to protect and test

Services to Protect
What do you need to protect?
What are mission critical services?

- Identify the top mission critical services – these are what you need to protect – these are what you must test.
- Inventory should show:
  - Name of service
  - Where / how it is hosted
  - Why it should be tested / importance
  - How to reach it – URL's & IP's, Ports
  - What authorization is needed to test it
  - Any testing limits

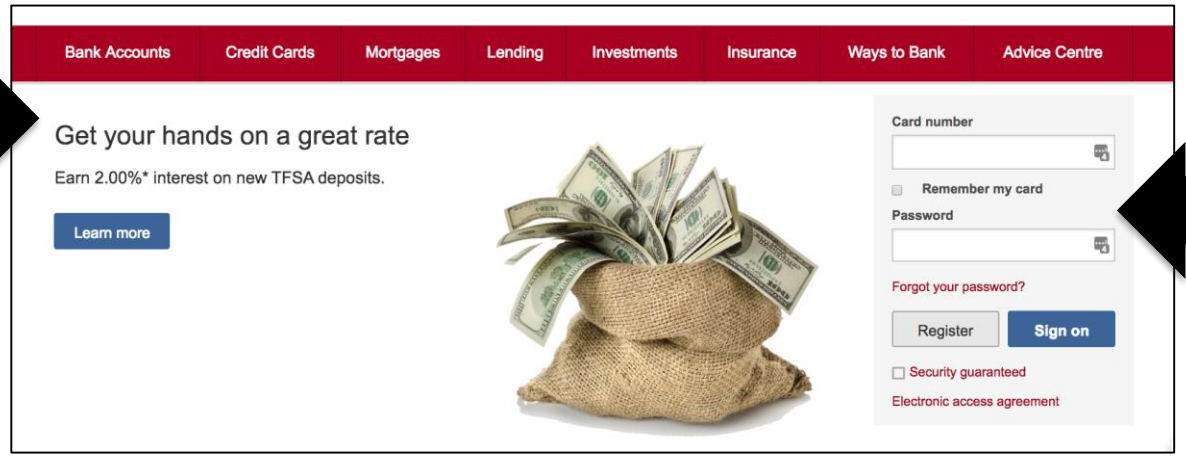
① DESCRIBE TARGET THIS IS				②DESCRIBE TARGET NETWORK DETAILS THIS TELLS WHERE THE TRAFFIC WILL BE SENT TO				③ AUTHORIZATION	④ SET LIMITS	
SERVICE OR TARGET NAME	WHAT ANSWERS FOR THE TARGET	WHY TARGET WAS SELECTED	IS PRODUCTION?	ENTER TARGET (IP / Domain Name / Full URL / Network Prefix)	IP ADDRESSES IPv4 and IPv6	RESOLVE by DOMAIN or LISTED IP's?	ACCEPTED PROTOCOLS AND PORT RANGES	IDENTIFY WHO AUTHORIZATIONS ARE REQUIRED FROM	LIMIT MAX BANDWIDTH (NO cloud defenses) (in megabit/sec)	LIMIT MAX BANDWIDTH (with cloud defenses ENGAGED) (in megabit/sec)

Application Attack Surface

Application Attack Surface
What features, like forms, are likely to be attacked?

- **If someone were to attack this application, how would they do it? What features would they attack?**
- **Browse your web-sites and look for interesting 'features':**
  - **Authentication/login pages**
  - **Dynamic web pages that call databases**
  - **Search features and other forms**
  - **API Call URL's (e.g. personalization API's)**

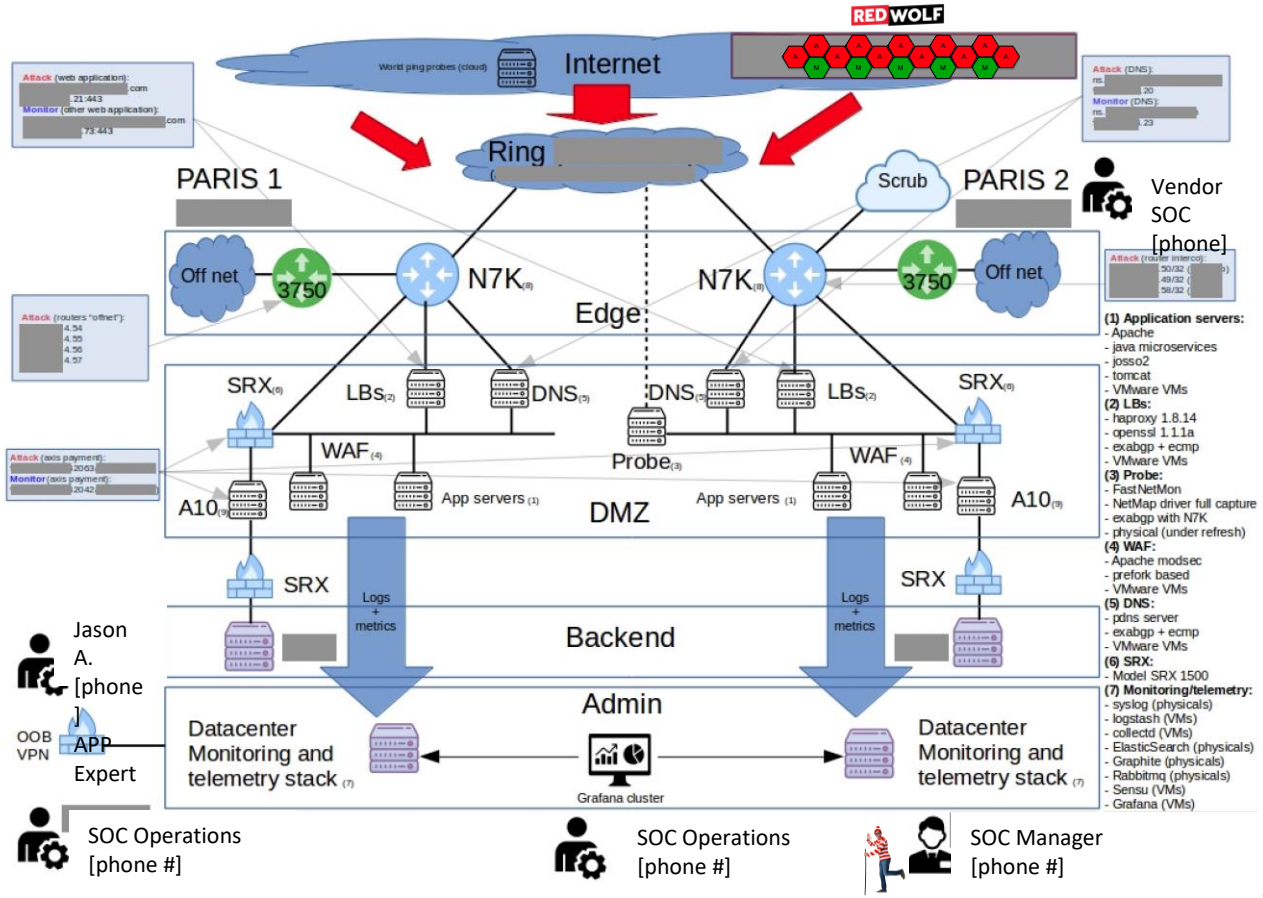
Homepages are often cached and optimized and doesn't cause a lot of server load or impact



Processing login forms can't be cached, and are resource intensive API calls and database lookups.

Often the forms post to a completely different URL.

Put it all together on a single diagram
Note – this is not a network diagram



<u>We need to identify the following and understand their relationships.</u>

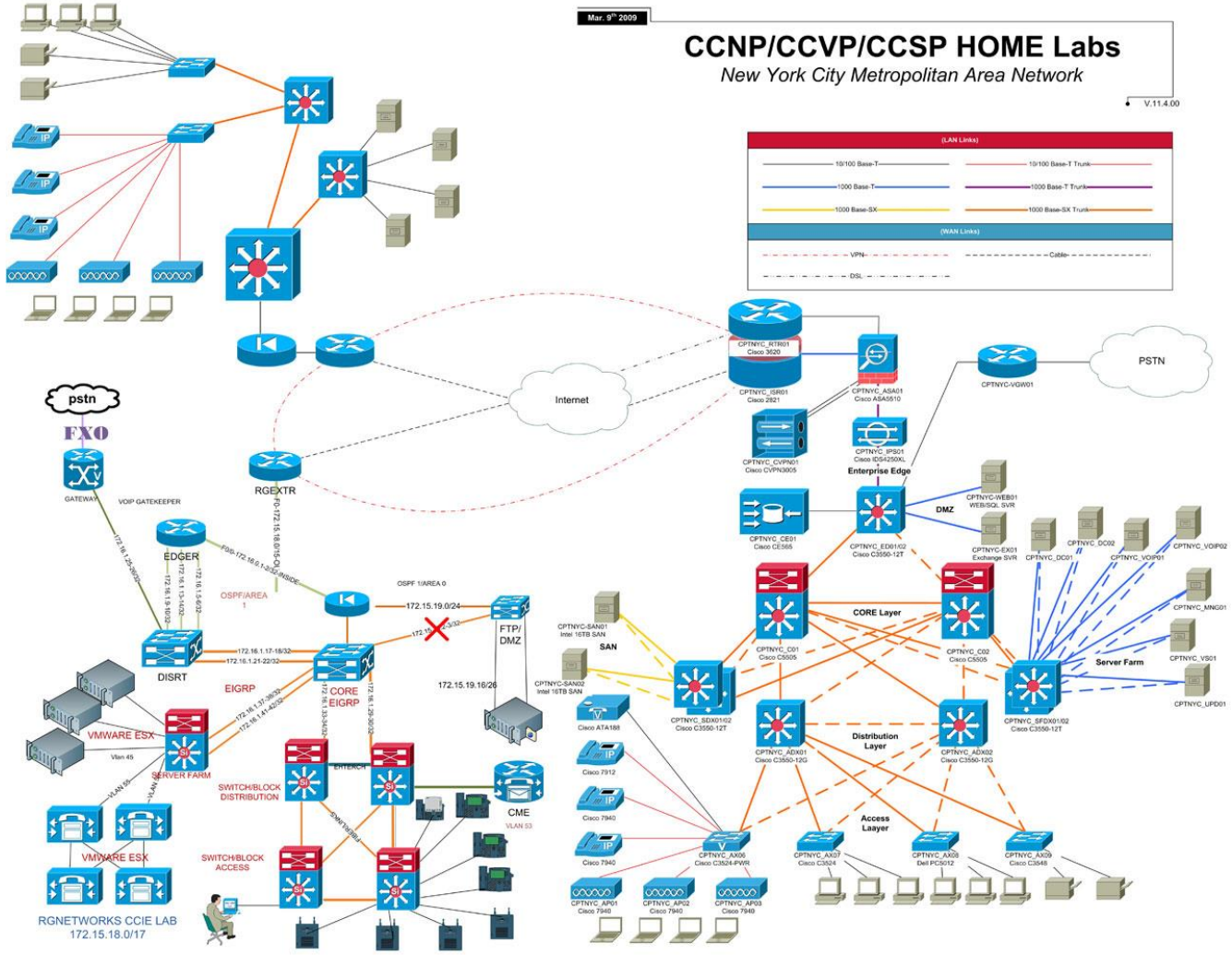
- [✓] **Cloud Monitoring**
- [✓] **Cloud Defenses**
- [✓] **Data centers & Connectivity**
- [✓] **Infrastructure devices**
- [✓] **On-Premise Defenses**
- [✓] **Controls we will test**
- [✓] **IP's and URL's we will test**
- [✓] **IP's and URL's we will monitor**
- [✓] **Internal monitoring: Logs, Alerts, Metrics**
- [✓] **<u>EXERCISE PARTICIPANTS & THEIR ROLE IN EXERCISE</u>**

E.g. Who will watch the Firewall?

E.g. Who will watch the Services?

Start with a network diagram

… Realize it won't show key information you need



Network Diagrams often lack key information required:

[✕] Cloud Monitoring

[✕] Cloud Defenses

[☑] Data centers & Connectivity

[☑] Infrastructure devices

[☑] On-Premise Defenses

[✕] Controls we will test

[✕] IP's and URL's we will test

[✕] IP's and URL's we will monitor

[✕] Internal monitoring:
Logs, Alerts, Metrics

[✕] **EXERCISE PARTICIPANTS & THEIR ROLE IN EXERCISE**

E.g. Who will watch the Firewall?

E.g. Who will watch the Services?

DDoS Testing Program – Key Testing Areas

TESTING	Baseline Service Performance	Test Local Defenses	Test 3rd Party Vendors	Service Monitoring
	Find out how scalable the actual service Do load testing and baselining	Router, DDoS Appliances, Firewalls, Load Balancer, WAF, IPS, etc…	CDN, Cloud DDoS, Cloud WAF, Managed Monitoring & Detection	HTTP(s), DNS, TCP, Routes BGP, SMTP, IPSEC and more

The importance of baselining

Baseline Service Performance

Find out how scalable the actual service
Do load testing and baselining

- Load test your services and find the 50% and 70% CPU utilization points
  - TEST WITH LEGITIMATE REQUESTS
    (this is not an attack test)
  - START LOW
    Start with low request rates per connection – i.e. 1 request/sec from a small number of clients – 100 to 500.
  - RAMP UP SLOWLY – RECORD IMPACT
    Measure Client and Server
  - CLIENTS
    Measure request latency, user-experience
  - SERVER
  - Measure CPU Cores, Overall CPU, TCP Connections, Request Rate, Memory Utilization, Application Performance Stats

The importance of baselining

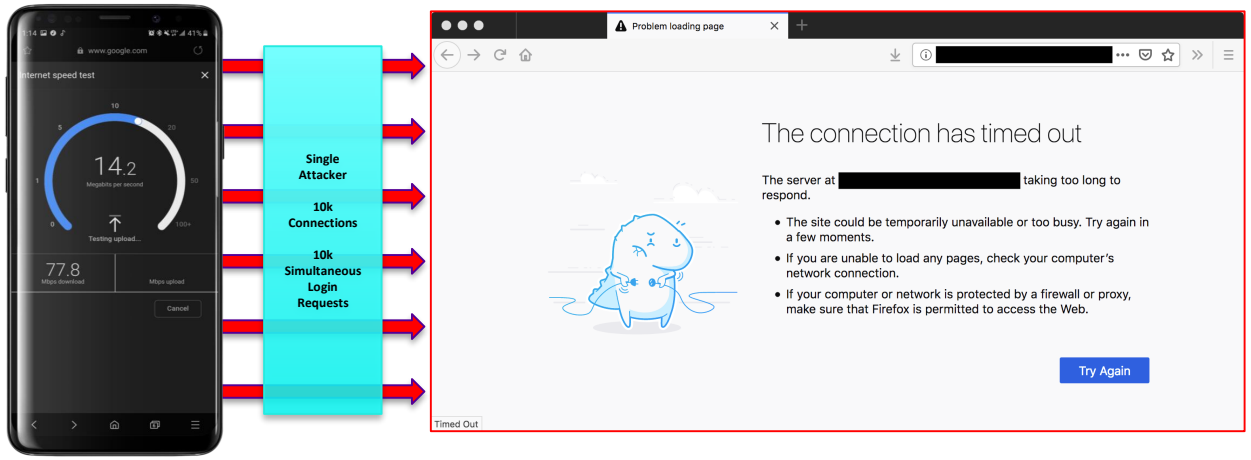
Baseline Service Performance

Find out how scalable the actual service

Do load testing and baselining

Remember the example of a single mobile phone to a login page? Baselining was done to precisely identify service capacity and tune defenses.

If you have a service that is not very scalable – you should know this and defend it accordingly!

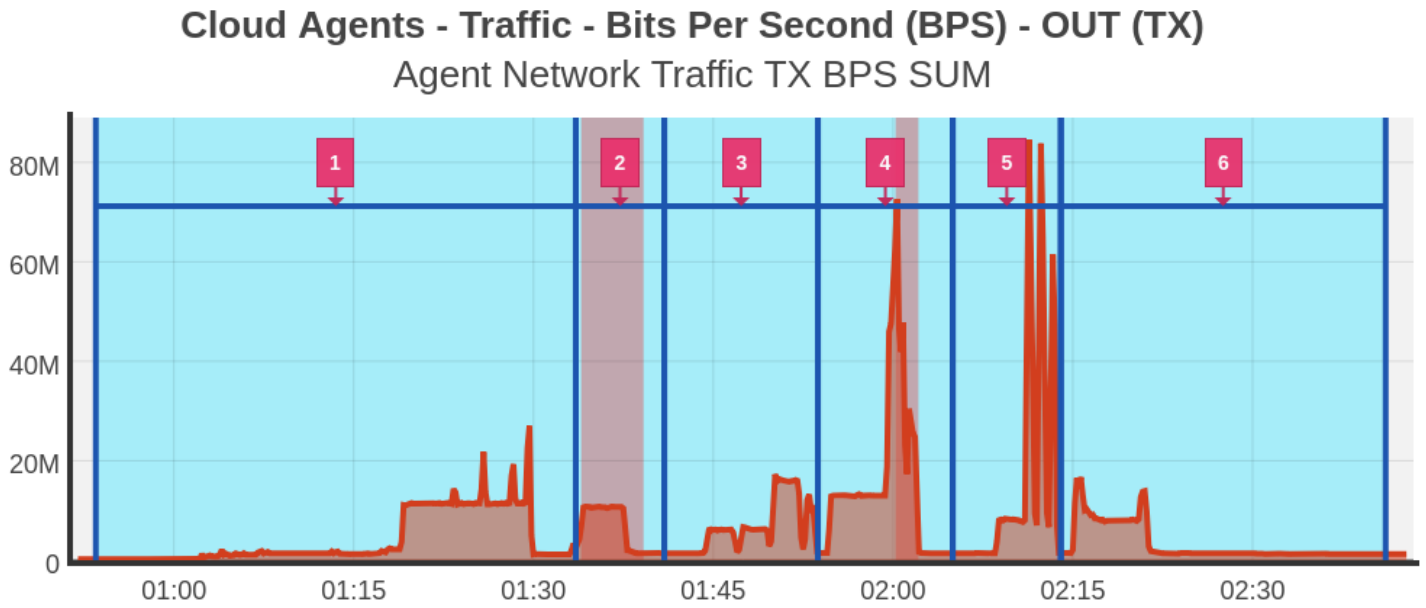


Test your local DDoS, Firewall, Load Balancers, WAF, and even your servers – they have to handle leakage and initial surge of requests

Test Local Defenses

Router, DDoS Appliances, Firewalls, Load Balancer, WAF, IPS, etc…

ID	Attack Vector & Performance
1	**Connection Flood** No impact to levels tested
2	**Slow Read** WAF did not block attack and server was impacted
3	**Slow Loris** No impact to levels tested
4	**Slow Write** WAF did not block attack and likely that WAF itself began to be overloaded.
5	**SSL Flood** No impact to levels tested but may have reached a throughput limit.
6	**WAF Overload** Attempt to overload the CPU of the WAF.

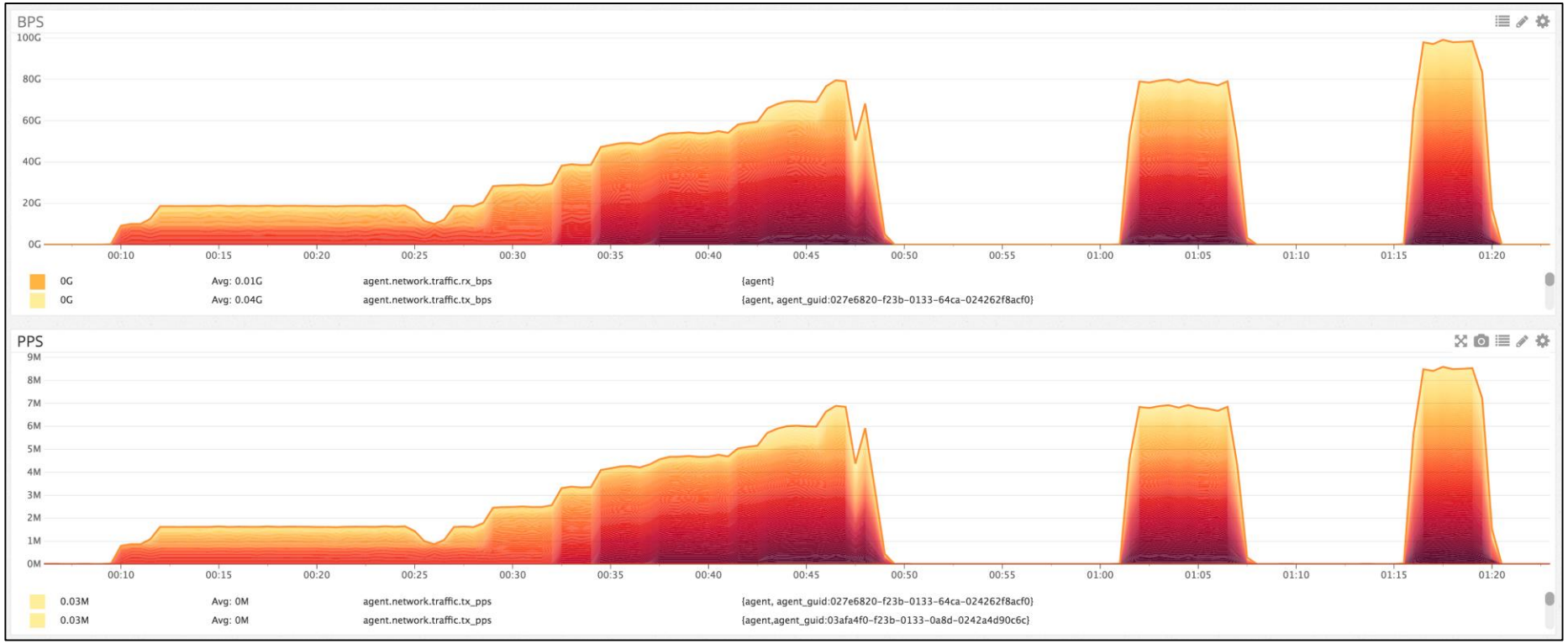


Comprehensively testing kind of attack scenario can take between 5 minutes and 45 minutes.

Test your 3rd party vendors separately

Test 3rd Party Vendors

CDN, Cloud DDoS, Cloud WAF, Managed Monitoring & Detection



- **Work WITH your vendors. They are not the enemy.**
- **Share your test plan and expectations with them – confirm they agree your expectations match the service they are offering.**

Tips for testing 3rd party vendors

Test 3rd Party Vendors
CDN, Cloud DDoS, Cloud WAF, Managed Monitoring & Detection

- Make sure to get authorizations/approval from the 3rd party vendors.

- Check the vendors acceptable use policy / testing policy.
- You legally can't launch most types of cyberattacks against most vendors without approvals!

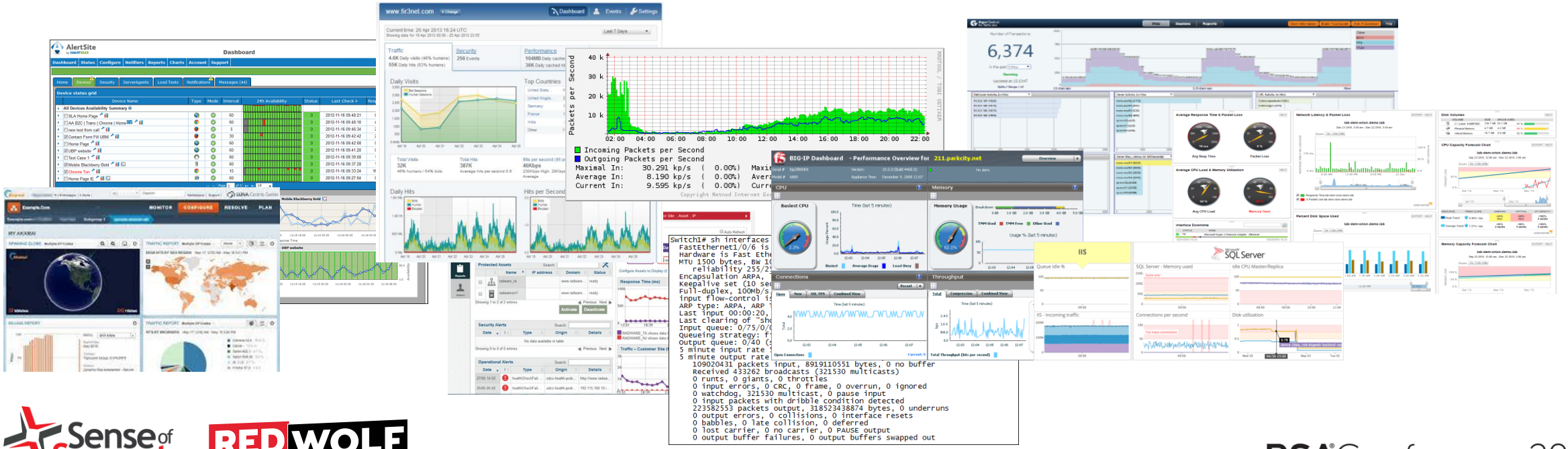
- Vendors are not the enemy! They are part of your defense system
- Work WITH your vendors – don't expect things to work perfectly the first time.
- The truth is, 70% to 80% of 3rd party vendor tests fail the first time!
- But most unsatisfactory outcomes are easily remedied.

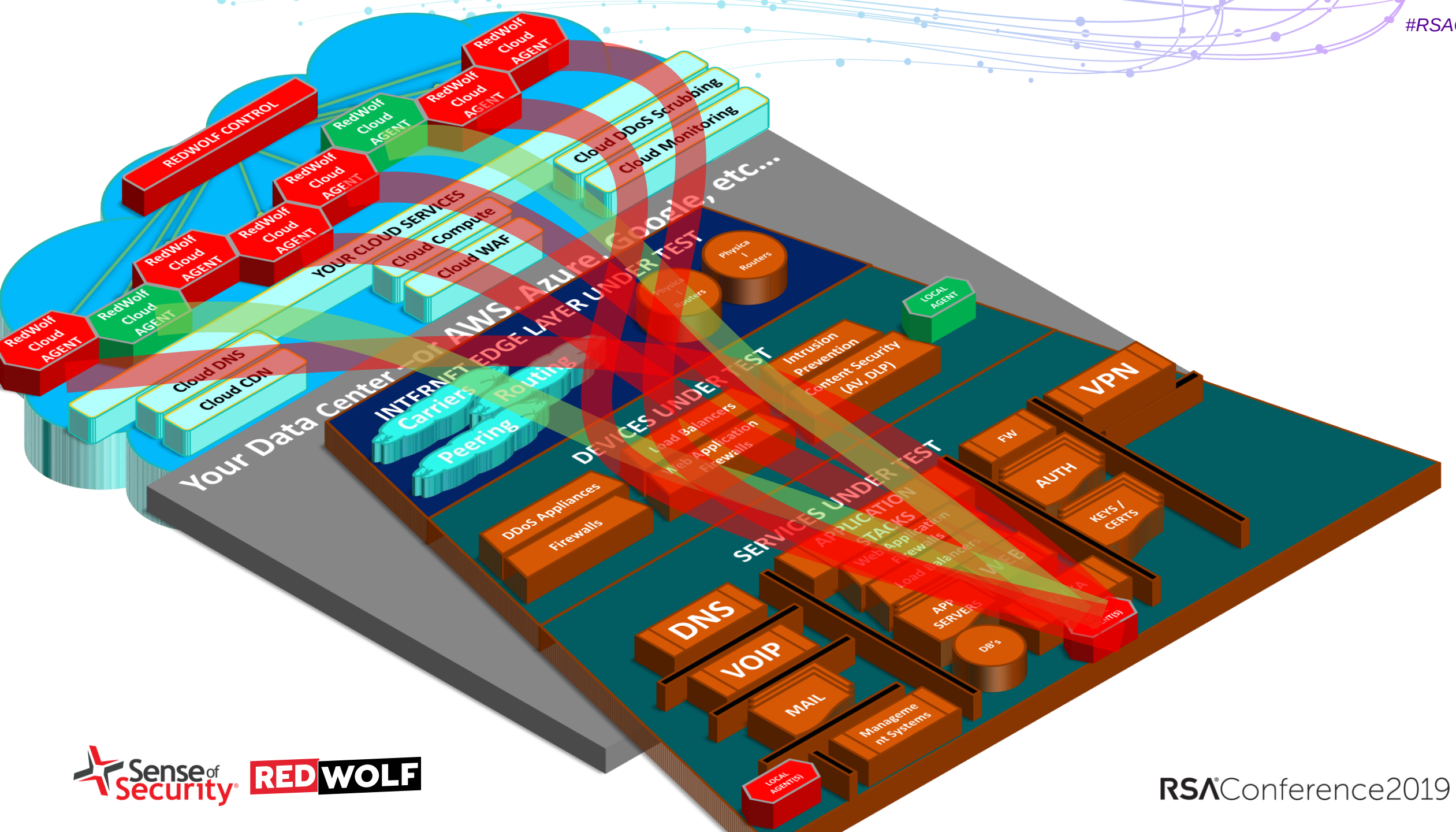
- That's one of the great values of testing!

Test your network monitoring systems

Service Monitoring
HTTP(s), DNS, TCP, Routes
BGP, SMTP, IPSEC and more

- When you do a DDoS test, your operations teams should be monitoring the systems in path
  - Network monitoring, device health, service health
  - Connection counts, request rates, latency, availability, …
- The teams ability to diagnose problems depends on their ability to see the situation clearly.




REDWOLF CONTROL
RedWolf Cloud AGENT
YOUR CLOUD SERVICES
Cloud Compute
Cloud WAF
Cloud DDoS Scrubbing
Cloud Monitoring
Cloud DNS
Cloud CDN
Your Data Center - or AWS, Azure, Google, etc...
INTERNET EDGE LAYER UNDER TEST
Carriers
Peering
Routing
Physical Routers
DEVICES UNDER TEST
Load Balancers
Web Application Firewalls
Intrusion Prevention
Content Security (AV, DLP)
DDoS Appliances
Firewalls
LOCAL AGENT
SERVICES UNDER TEST
APPLICATION STACKS
VPN
FW
AUTH
KEYS / CERTS
DNS
VOIP
MAIL
APP SERVERS
DB's
Management Systems
LOCAL AGENT(S)

You're not *just* testing a device, vendor, or process.
You're actually testing a *scenario* against some *defense controls.*

Defenses
Tighten Configurations
Fill in Control-Gaps

Q: What if ____ happened? What would happen?

A: It depends entirely on your controls:

Technical controls: detection, defense

Process controls: run-books, incident response plans

People: Teams and vendors, their knowledge, experience, communications

Don't focus on the 'device' – focus on the configuration and controls of the device

Q:	**If you turned OFF your Email SPAM filter – would you get more SPAM?**
A:	**Of course! No SPAM filter means no SPAM CONTROL, and SPAM gets through!**
Q:	**If you turned OFF your Anti Virus filter – would you get more viruses?**
A:	**Obviously no AV**
Q:	**If you turned of a specific WAF capability – say SQL Injection blocking, then…?**
A:	**Obviously SQL injection attacks would make it through to the web servers.**

It's the defense and controls that matter

Q:	**If your Cloud or ISP DDoS vendor hasn't enabled TCP FLOOD protection…?**
A:	**Then they won't be able to stop TCP FLOOD's well.**
Q:	**If your DDoS system does not have any SSL/TLS protocol protections then …**
A:	**I will be more vulnerable to SSL/TLS attacks.**
Q:	**Do you know what actual defense controls protect your services?**
A:	**… If not – that's something to do! Don't stay at the 'device' level – dive in and map different kinds of attacks to the available countermeasures.**

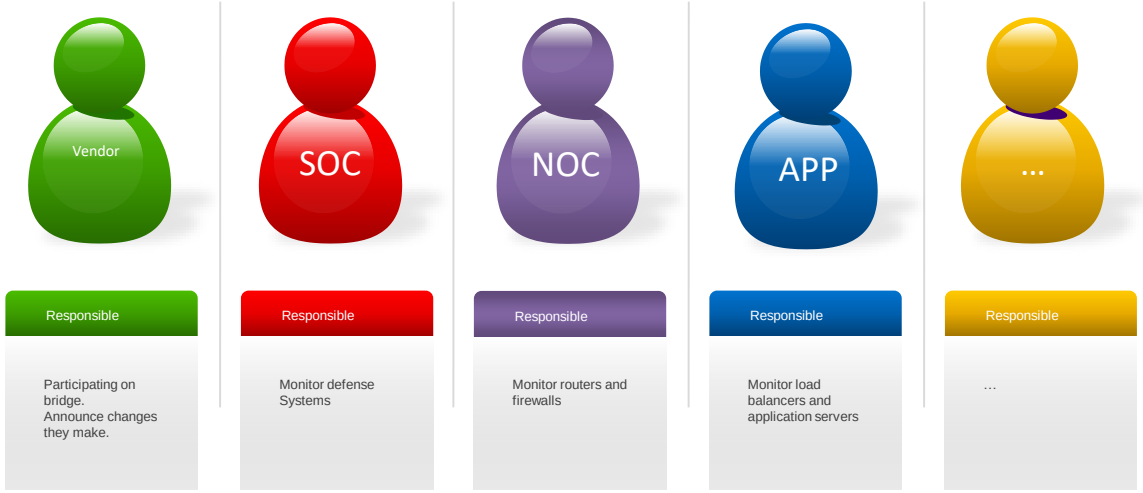
Remember your operational response team is what you rely on when something goes wrong – they need to know:

Operational Response Skills
Cyber-Drills, Online Run-Books,
Cross-Silo Communications

END TO END TOPOLOGY
Internet / Cloud
Network Diagram
(including cloud monitoring)
+
Data Center Connectivity
(ISP's / Carriers)
+
Infrastructure
(devices under test or in path)
+
Services Tested
(down to IP and URL's tested)

PEOPLE & ROLES & EXPERTISE

For each item on the left:
Who monitors it??
Who is the expert?



DDoS Testing Program – What you are improving

IMPROVE	Defenses	Operational Response Skills	Processes	Automation
	Tighten Configurations Fill in Control-Gaps	Cyber-Drills, Online Run-Books, Cross-Silo Communications	Incident Response Procedures, Triggers & Correlation Rules	Scheduled Continuous Automated Testing Detect Regressions Automatically

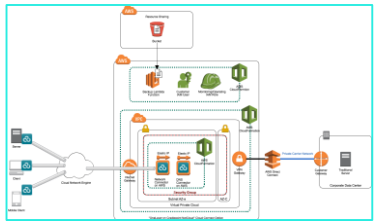
- **After every test go through the above areas and see how each can be improved.**
- **For each improvement you make – document how it can be measured.**
- **You want to be able to show capability improvements over time**

Before you run a DDoS test exercise – Remember!

PREPARE!

Who and What is being tested? When?

Document Test System



Network diagram
Defense infrastructure (devices)
Monitoring information
Vendors
Operational people / teams

Services Tested

Document the services being tested – the business services and how they are protected.

List URL's, domain names, data center names, IP's – to make sure everyone knows exactly what is being tested.

Specify any testing limits / restrictions.

Create Test Plan

There are many attack scenarios – start with simple ones, not complex ones.

Select test scenarios which. Map 1:1 to the controls being tested.

That is, the device features.

Authorizations

You **must** obtain authorization for testing as per 3rd party vendor policies.

This generally includes:
- Defense vendors
- Hosting Providers
- Asset Owners
- ISP's if loading >70% circuit size

Schedule

DDoS testing exercises can be 4-6 hours long and are usually quite realistic and are run as cyber-drills.

Usually late night.

Some exercises are run during business hours – for SOC training.

Device optimization tests can be done at any time in labs, or with small numbers of attackers and control over traffic levels to not impact production systems.

Deliver Exercise!

This is not a pen test!

Run as a cyber-drill with operations whenever possible.

Active participation is strongly recommended!

Eventual goal of automation and automatic verification.

RSAConference2019

LAB3-W310
How to Design and Operate a DDOS Testing Program

WHAT YOU SHOULD DO NEXT:

- IMMEDIATELY
- 3 MONTHS
- 6 MONTHS

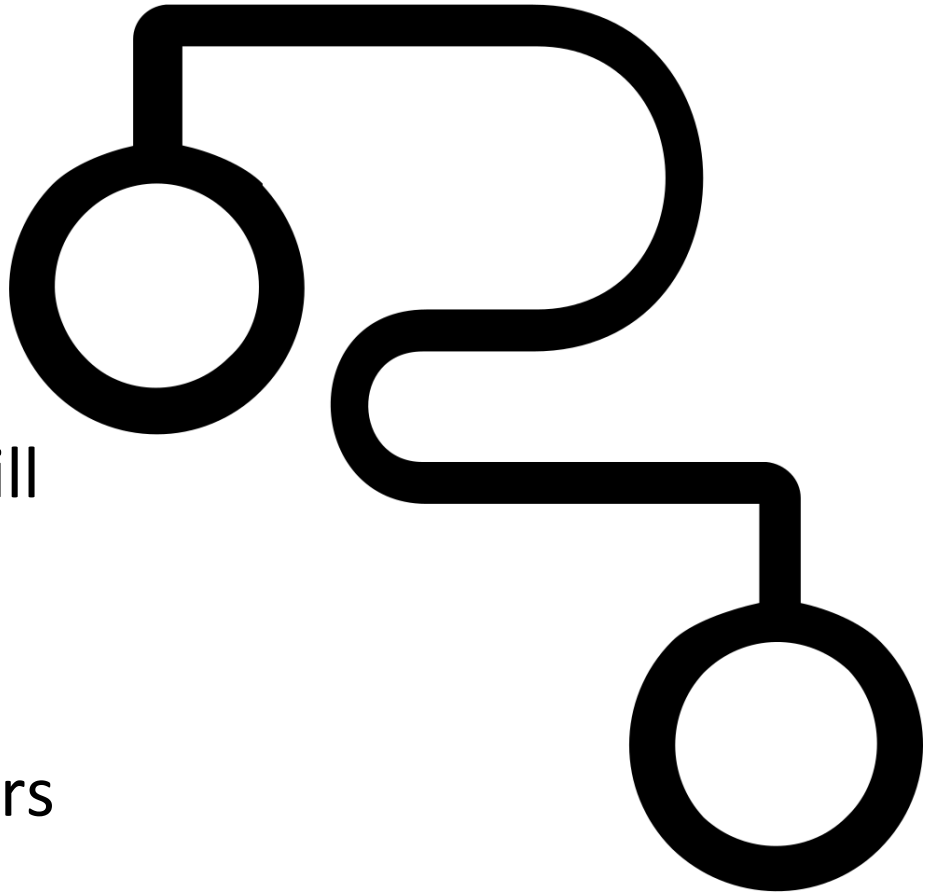
Practical Application

Apply What You Have Learned Today

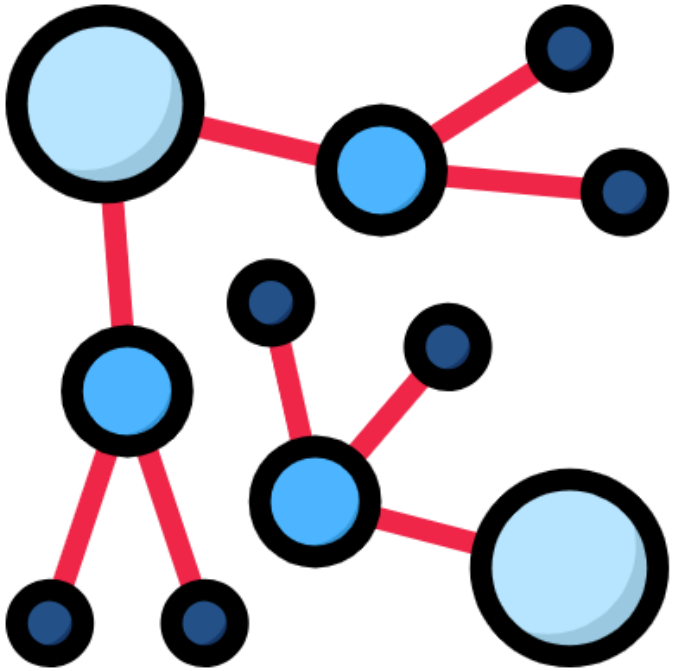
- Next week you should:
  - Characterize your environment
    - ID all the elements that affect your THREAT PROFILE
    - Devices & services that COULD be a target
    - All the infra in-front & behind the targeted systems (Routers, Firewalls, WAF's, Databases, etc)
    - Ops monitoring systems (log collection, alerting, metrics collection, both local & cloud).
    - 3rd Party Vendors & 3rd Party Techs (e.g. ISP DDoS Service, ISP DDoS Service,)

Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - **TECH, PEOPLE & SUPPLY CHAIN**
    - Identify capabilities for each element.
    - 'technically capable' ≠ activated & configured!
    - Identify alerts, evidence, & metrics that will be generated.
    - Identify how/where they are accessed.
  - **TARGETS**
    - Build a test plan, including targets & vectors



Apply What You Have Learned Today



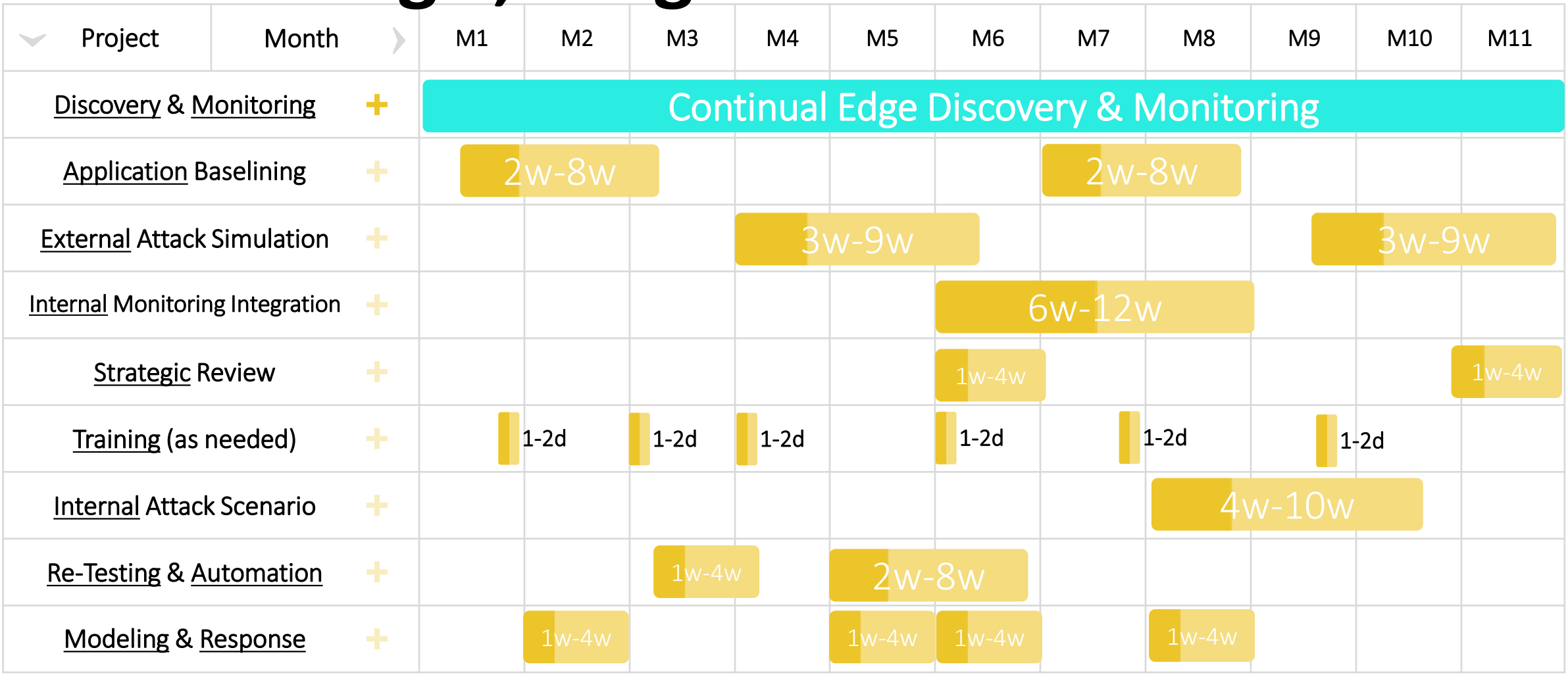
- In the first three months following this presentation you should:
  - TARGETS
    - Start building a test plan, with relevant targets & vectors

Type of Scenario	Environmental Model	Technological Capability
Scenario Sophistication	Types of Targets Selected	Operational Performance
Metrics / Telemetry	Team Observations & Notes during Exercise	Supplied evidence (Screenshots, logs, metrics)

Apply What You Have Learned Today

- Within six months you should:
  - Test & Retest:
    - Executed First Test, Identified Gaps, Resolved and Retest
  - Vuln Mgt Program
    - Should formally incl DDoS Testing
  - Expand on Frequency & Coverage.
    - Continuous Monitoring,
    - Higher Frequency in-depth tests
    - Focus on Apps!

Take a strategic, Programmatic view



Question Time

murrayg@senseofsecurity.com.au
sharjil.khan@redwolfsecurity.com