



# A Hackers View of DoS Attacks

---

David Robinson

ChCon  
November 2021

# #whoami

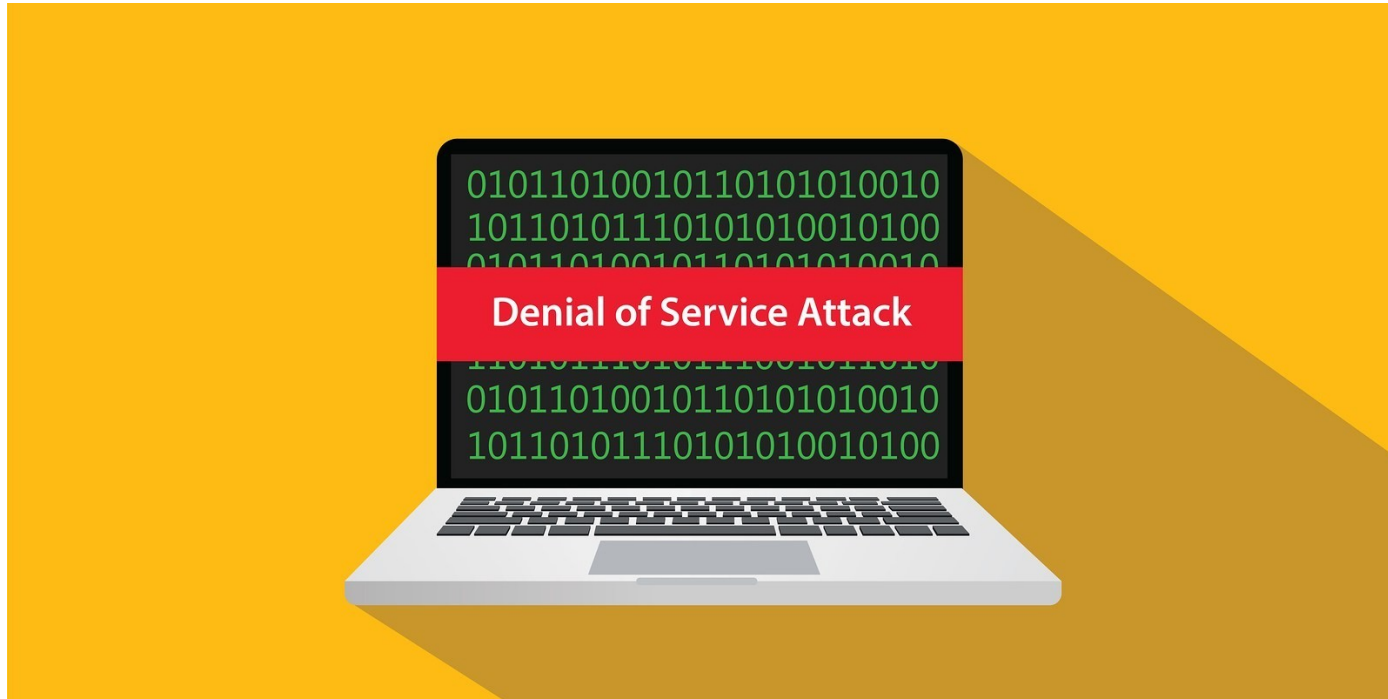


- David Robinson/Karit
- @nzkarit
- ZX Security – Hacker
- Run Kākācon
  - 13 November 2021

# Outline

- What is a DoS attack?
- Why do people perform DoS attacks?
- What do they target?
- How to identify targets
- How to protect your systems
  - Prioritising and ordering the tasks in a plan

# What is a DoS attack?



# Denial of Service

- When an attacker performs actions to make a system unusable to users
- Two main types
  - Volumetric
  - Layer 7/Protocol

# Volumetric

- Send more traffic than infrastructure can handle



[https://en.wikipedia.org/wiki/File:Miami\\_traffic\\_jam,\\_I-95\\_North\\_rush\\_hour.jpg](https://en.wikipedia.org/wiki/File:Miami_traffic_jam,_I-95_North_rush_hour.jpg)

# Layer 7/Protocol

- Exploit a weakness in the infrastructure or application
- Low input, High impact
- One request ties up resource which stops other requests
- Usually legit HTTP traffic, difficult to filter as it looks like a normal request

# Performance Test Reports

“Yes the page is slow and has an expensive DB query, but the page is rarely used”

Most Performance Test Reports



# Crash, Infinite Loops, etc

- Also examples where user input may crash application or cause infinite loops
- Zip Bombs – small zip expanding to a large file
- Billion Laughs – recursively expanding XML

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ELEMENT lolz (#PCDATA)>
  <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
  <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
  <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
  <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
  <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
  <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
  <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

# Which one do attackers use?

- Volumetric or Layer 7
- The large attacks use a mixture of both.
- They see which is having the most impact and try to get the best value for money

# DoS vs DDoS

- DoS – Denial of Service
  - May include vulnerabilities that cause applications to crash
- DDoS – Distributed Denial of Service
  - Many nodes are used to send data
  - Botnet

# Why do people perform DoS attacks?



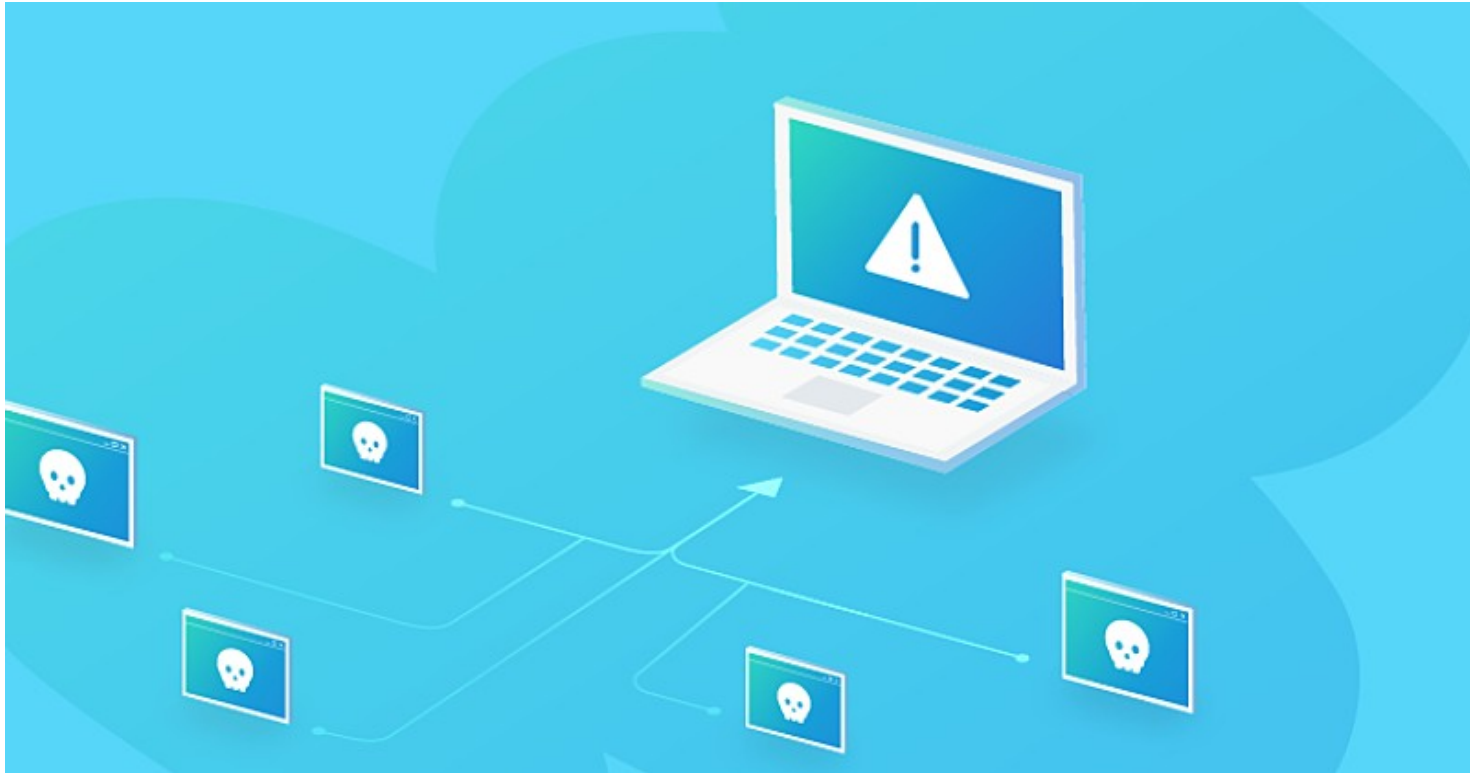
# Motives

- Ransom/blackmail
  - Often indicates a business behind the attack
  - They have monthly KPIs to achieve
  - Requirement to deliver dividends to their share holders
- May dislike your organisation
  - Issue motivated groups
- Distraction
  - Security team looking one way, while they launch an attack, exfill data, etc somewhere else

# Ransomware vs DDoS Blackmail

- Different in that it is money for a threat vs money for a resolution
  - This makes it harder to extract the money
- With ransomware you can just restore from backup (maybe)
- NZX DoS continued while it was being covered by the media.
  - The group was using it to advertise that they were competent.

# How are DoS attacks performed?

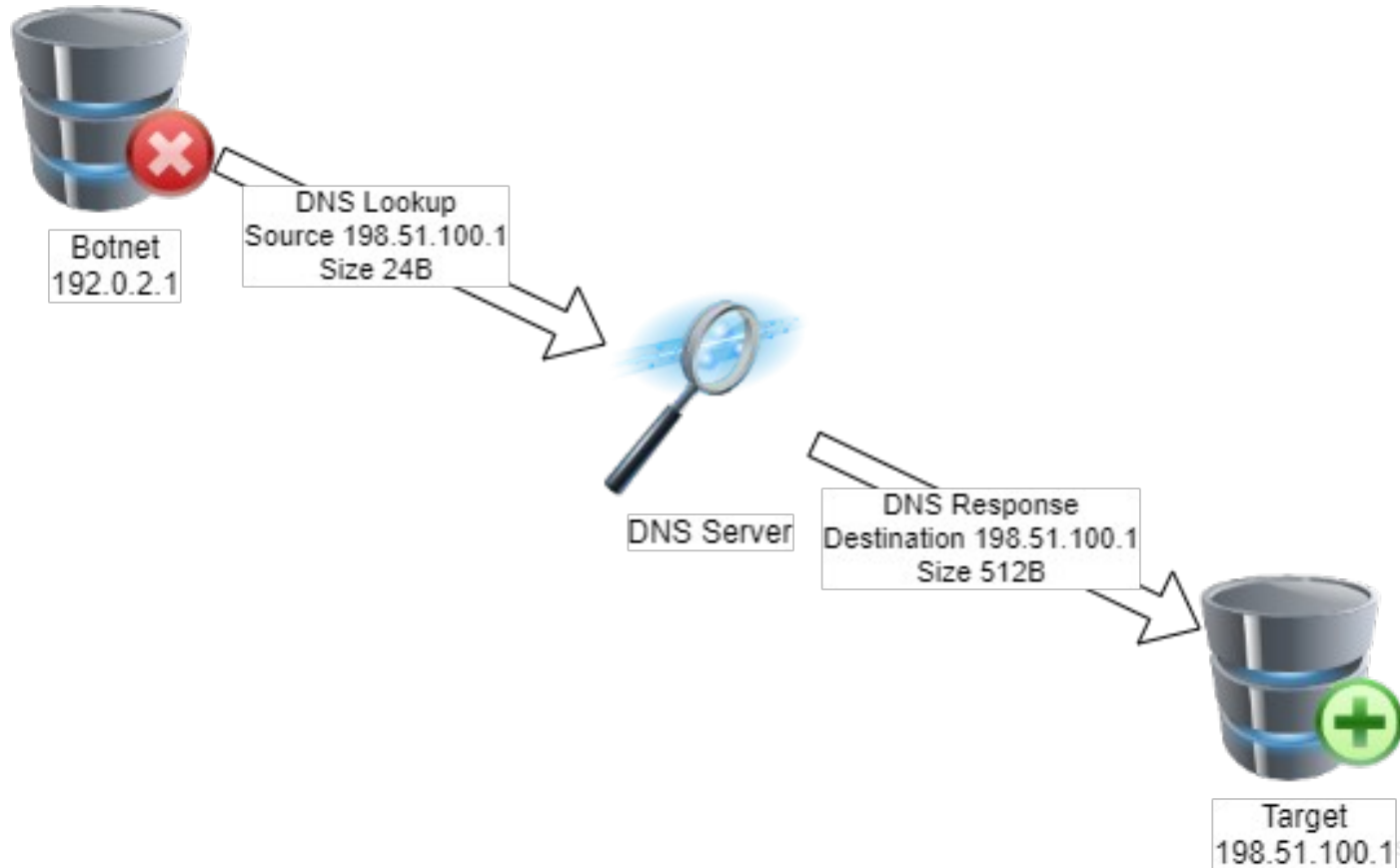


# Methodology - Volumetric

- Botnet
  - Compromise a range of devices (e.g cheap ISP modem/router with default creds), get them to send a lot of traffic
- ICMP
- UDP Reflective
  - E.g. DNS, NTP, SNMP
  - Spoofing of source IP address
  - Small request, large response



# DNS Reflection and Amplification



# Dangers of open UDP ports

- Customer who had MSSQL (UDP) open to internet
- Used in a reflective attack
- Customer received a multi-thousand dollar Azure bill
  - They were just a relay, they were not the target of the attack

# How are Botnets made?



## RouterOS v6.1 *2013-06-12*

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

Login:

Password:

 Winbox  Telnet  Graphs  License  Help

© mikrotik

# DrayTek

## Vigor2760 Series

### Login

**Username**

**Password**

**Login**

*Delight*

Copyright © 2013 DrayTek Corp. All Rights Reserved.



**Hewlett Packard**  
Enterprise

# Integrated Lights-Out 3

HP ProLiant

*2016-10-24*

Firmware Version 1.88

HP, the HP logo, and the HP ProLiant logo are trademarks of Hewlett-Packard Development Company, L.P. © 2016 Hewlett-Packard Development Company, L.P. All rights reserved.



Local user name:

Password:

Log In



## ZEG Virtual Appliance

This ZEG virtual machine (Zero Effort Groupware) is intended to provide a complete testing environment of SOGo, the Open Source messaging and calendaring software.

The appliance is based on packaged with the following preconfigured components:

- [SOG](#)
- [OpenChange/Samba4](#) (Outlook compatibility)
- [PostgreSQL](#) (database server)
- [OpenLDAP](#) (LDAP directory)
- [Cyrus](#) (IMAP server)
- [Postfix](#) (SMTP server)

## How To Login To Web Interface

The SOGo login page is accessible from this URL:

[https://\[redacted\]nz:8443/SOG](https://[redacted]nz:8443/SOG)

There are some predefined accounts which you can use to login:

username	password	email
sogo1	sogo	sogo1@example.com
sogo2	sogo	sogo2@example.com
sogo3	sogo	sogo3@example.com

Please configure the password >>

- General
- Address Book
- Fax
- Copy
- Print
- Scan
- Administrator
- Network

- ▶ Status
  - Auto Refresh Interval
  - Maintenance Information
  - Lists/Reports
  - Find Device
  - Contact & Location
  - Sleep Time
  - Mode Timer
  - Sound Volume
  - Date&Time
  - Panel
  - Replace Toner

## Status

### Device Status

Sleep

Automatic Refresh

Off  On

### Toner Level



BK

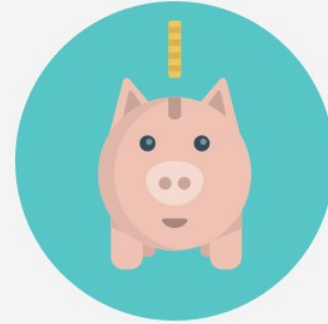
### Web Language

Auto

## How do I purchase a vDos plan?

Purchasing a booter plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

₿ Bitcoin, we believe in the huge potential of this new digital currency.



## Pricing Lists

Select the best package based on your usage needs and size of business.

Bronze	Silver	Gold	VIP
\$19.99 /monthly	\$29.99 /monthly	\$39.99 /monthly	\$199.99 /monthly



# Methodology - Layer 7 Denial of Service

- Firstly need to find a vulnerability in the application or network
- Can be achieved using a botnet, but the number of hosts can be much smaller
- During an engagement we took down a server for US\$0.12/h on AWS
  - They were paying for DoS prevention

# What would an attacker target?



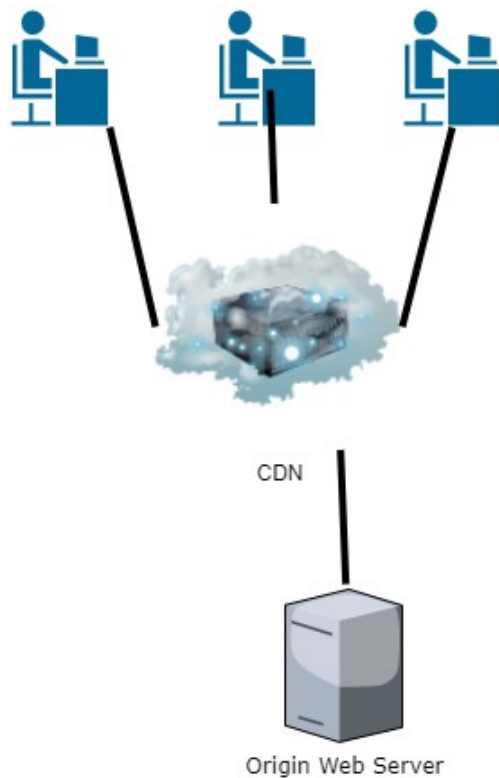
# Attacker's Goal

- The attacker's goal depends on what they want to target
- With **blackmail**, they most probably want to disrupt business operations
- If they want to impact **public relations**, something publicly facing is good
- If the motive is **distraction**, most probably a little bit everywhere.

# Target Selection – Attacker’s Mindset

- Brochureware website?
  - Why bother? Business will just continue
- They want to find targets which affect business operations

# CDN Servers



# Finding the Origin Server

- If there is a CDN in front of need to find the origin server
- To save money test.www.example.com isn't behind a CDN
- What are the chances that prod origin server and test server are behind the same firewall?
  - Or the same host???
  - And using same DB???

# Scan the internet

- At ZX Security we use Flaming Penguin, which is similar to Shodan (and metl's low hanging kiwi fruit)
  - Scanning the NZ IP space
  - Identify what is there
  - Take screenshots of web sites, etc
- Would be fair to assume that an attacker would be doing something similar

# Identify Branch Offices/Retail Sites





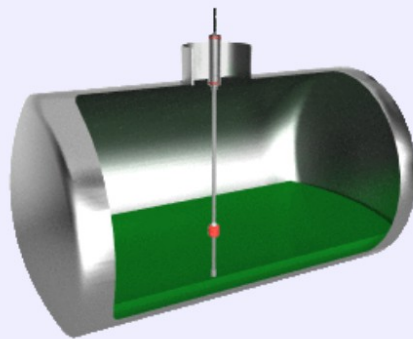
# MAGLINK LX - Web Console Configuration



English



Select



## Tank Status

System [FMS](#) [Setup](#)

[Download History](#) [Auto Refresh](#)

[Status](#) [Alarms](#) [Control](#) [Compliance](#) [Reports](#) [Data Logging](#)

[Tanks](#) [Lines](#) [Sensors](#) [Pumps](#)

### TANKS

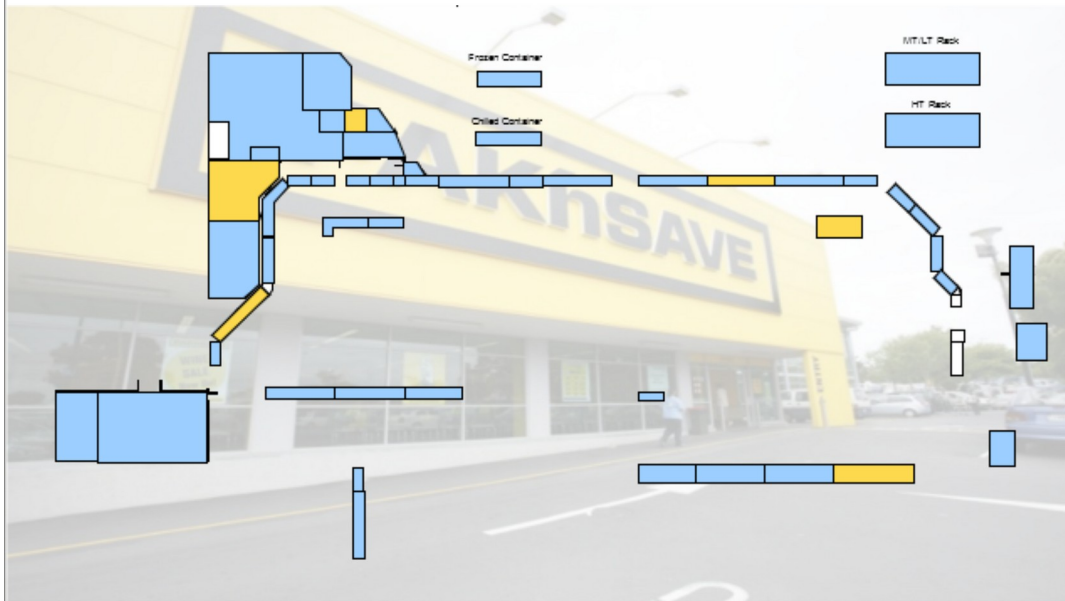
Image	Manifold ID	Tank ID	Name	Product	Alarms	Level	Gross Volume	Net Volume	Ullage	Water Level	Temperature	Max Capacity	Capacity %
		1	95	95		1785.96	15164.75	15199.24	2695.44	.66	13.75	18800.00	80.66
		2	91	91		1988.49	39193.51	39282.40	2036.49	0.00	13.76	43400.00	90.31
		3	DSL - Ago	Product 3		1728.17	37566.41	37627.75	8146.45	26.73	13.56	48200.00	77.94
		4	100 PLUS	Product 4		1251.57	7491.71	7509.83	5984.22	20.31	13.64	14200.00	52.76
		5	Go Clear	Product 5		1027.74	4086.36	4095.97	578.58	0.00	13.69	4910.46	83.22



# - Site Layout

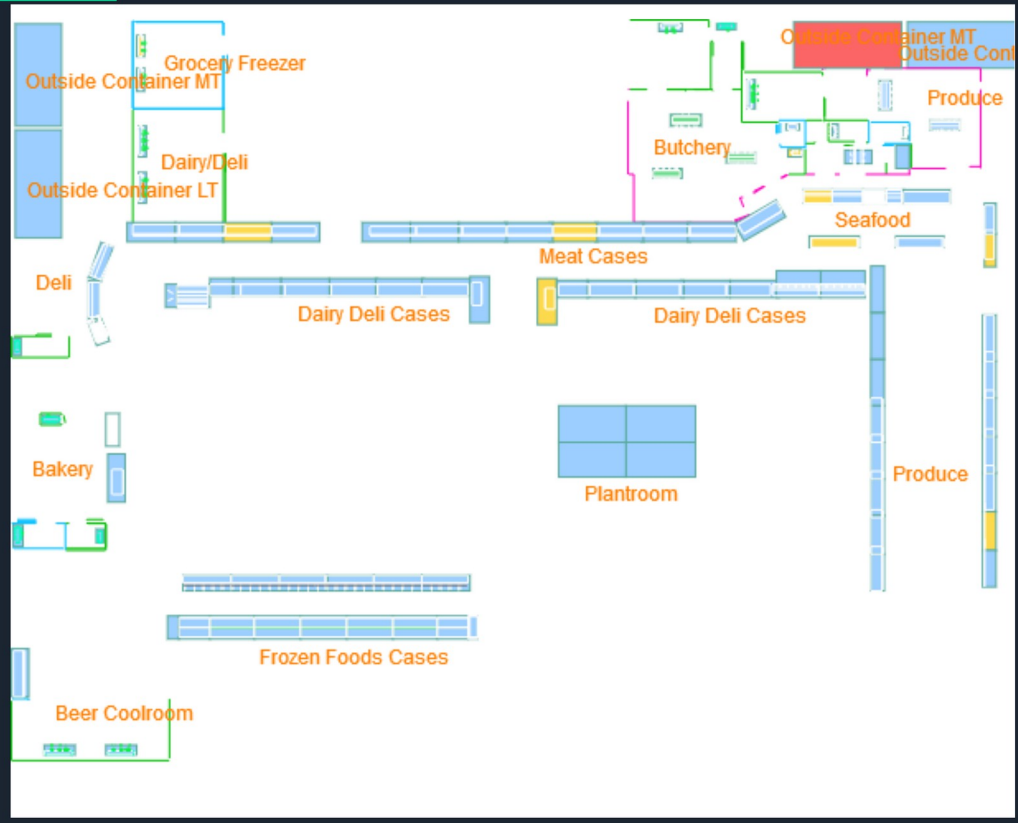


new layout





Layout



POS

- Make Line
- Cut Table
- Orders

\$0

Place Order

- Value Pizza
- Extra Value Pizza
- Traditional Pizza
- Gourmet Pizza
- Combo
- SIDES
- DELIVERY
- Shakes
- Misc
- DRINKS
- DESSERTS
- BURGER
- BURGER SIDES
- Juice
- Toppings
- Sauces

BBQ ITALIAN SAUSAGES	Beef & Onion Pizza	Cheesy Garlic Pizza	HALF & HALF	HAM & CHEESE PIZZA	Hawaiian Pizza
Margaretta Pizza	Pepperoni Pizza	Simply Cheese Pizza	Tropical Vege Pizza		

# Retail sites

- Most probably use a UFB or Cellular Connection
  - Retail level connection probably does not have DDoS scrubbing or monitoring by ISP
- Point of Sale most probably uses the same connection
- What is the financial impact if a location can not make sales?
  
- Could an attacker identify these assets easily?

# Remote Access





 Council  
SCADA VPN

Login

[Forgot Password](#)

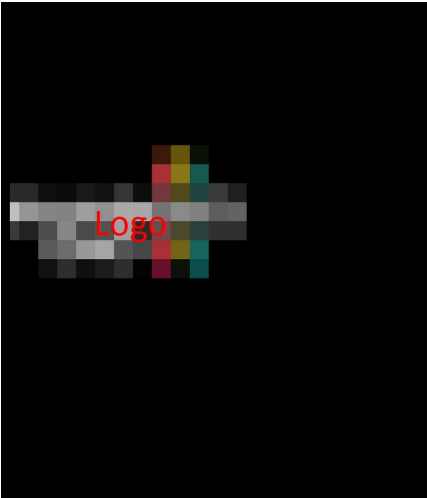


Company Name  Webmail

User name:

Password:

 sign in



# Remote Access Endpoints

- Disrupts people working from home
- Makes remote support difficult
- Consider other services which traverse the same firewall
  - They don't have to take out a server
  - They could take out the firewall in front of the target

# Certificate Transparency

- All HTTPS certificates are now added to the Certificate Transparency Log
- We can use this to find hosts and look them up in DNS
- Becomes interesting if the target is not behind a CDN
- Useful for identifying Origin Servers

**Criteria**

Type: Identity Match: ILIKE Search: 'google.com'

<a href="#">crt.sh ID</a>	<a href="#">Logged At</a> ↑	<a href="#">Not Before</a>	<a href="#">Not After</a>	<b>Common Name</b>	<b>Matching Identities</b>
<a href="#">3144337544</a>	2020-07-26	2011-07-10	2013-07-09	*.google.com	admin@google.com *.google.com
<a href="#">2381394777</a>	2020-01-27	2011-07-13	2012-07-13	*.mail.google.com	*.docs.google.com *.mail.google.com *.plus.google.com *.sites.google.com *.talkgadget.google.com
<a href="#">2380986199</a>	2020-01-26	2011-02-16	2012-02-16	*.mail.google.com	*.docs.google.com *.mail.google.com *.sites.google.com *.talkgadget.google.com
<a href="#">2380850988</a>	2020-01-26	2012-02-29	2013-02-28	onex.wifi.google.com	onex.wifi.google.com
<a href="#">2380841885</a>	2020-01-26	2011-07-13	2012-07-13	accounts.google.com	accounts.google.com
<a href="#">2380681291</a>	2020-01-26	2013-11-22	2013-11-24	hosted-id.google.com	hosted-id.google.com
<a href="#">2380579544</a>	2020-01-26	2011-05-11	2012-05-11	accounts.google.com	accounts.google.com
<a href="#">2379825238</a>	2020-01-26	2011-05-11	2012-05-11	adwords.google.com	adwords.google.com adwords.google.com.ar adwords.google.com.au

# Spider Site

- Find the slow pages
- Useful for sites that are on a CDN
  - Slow pages may indicate that the page can't be cached and is going to the origin server

# Spidering weak sites

- While penetration testing sites we have taken them down, by accident
  - From our laptop
  - With as little as 10 threads
  - Using tools, like Dirbuster, Burp
  - Using the search dialogue box on the site

# Email headers

- Email headers reveal IP addresses and domain names
  - Particularly server generated ones like signups and password resets

```
Received: from ns2.██████████.net (ns2.██████████.net. [██████████])  
  by mx.google.com with ESMTP id ██████████  
  for <██████████>;  
  Fri, 04 Jan 2019 14:03:35 -0800 (PST)  
Received-SPF: pass (google.com: best guess record for domain of apache@ns2.██████████.net designates 1██████████ as permitted  
sender) client-ip=1██████████;  
Authentication-Results: mx.google.com;  
  dkim=neutral (body hash did not verify) header.i=@██████████.com header.s=default header.b=██████████l;  
  spf=pass (google.com: best guess record for domain of apache@ns2.██████████.net designates 1██████████ as permitted  
sender) smtp.mailfrom=apache@ns2.██████████.net  
Received: by ns2.██████████.net (Postfix, from userid 48) id ██████████; Fri,  
  4 Jan 2019 22:03:24 +0000 (UTC)
```

# Historical DNS

- Search historic DNS records
- Client has changed their DNS to point to a CDN, but the historic DNS records store the origin server

IP history results for google.com.

=====

IP Address	Location	IP Address Owner	Last seen on this IP
64.233.165.139	United States	Unknown	2021-01-14
64.233.165.138	United States	Unknown	2021-01-14
64.233.165.113	United States	Unknown	2021-01-14
64.233.165.102	United States	Unknown	2021-01-14
64.233.165.101	United States	Unknown	2021-01-14
64.233.165.100	United States	Unknown	2021-01-14



# Regulatory Requirements

- Is the business subject to regulatory requirements?
- For example with the NZX:
  - Web site was attacked
  - The trading platform was fine
  - They had to halt the market as the web site attack meant that regulatorily requirements documents were not accessible to market participants

# Collateral Damage

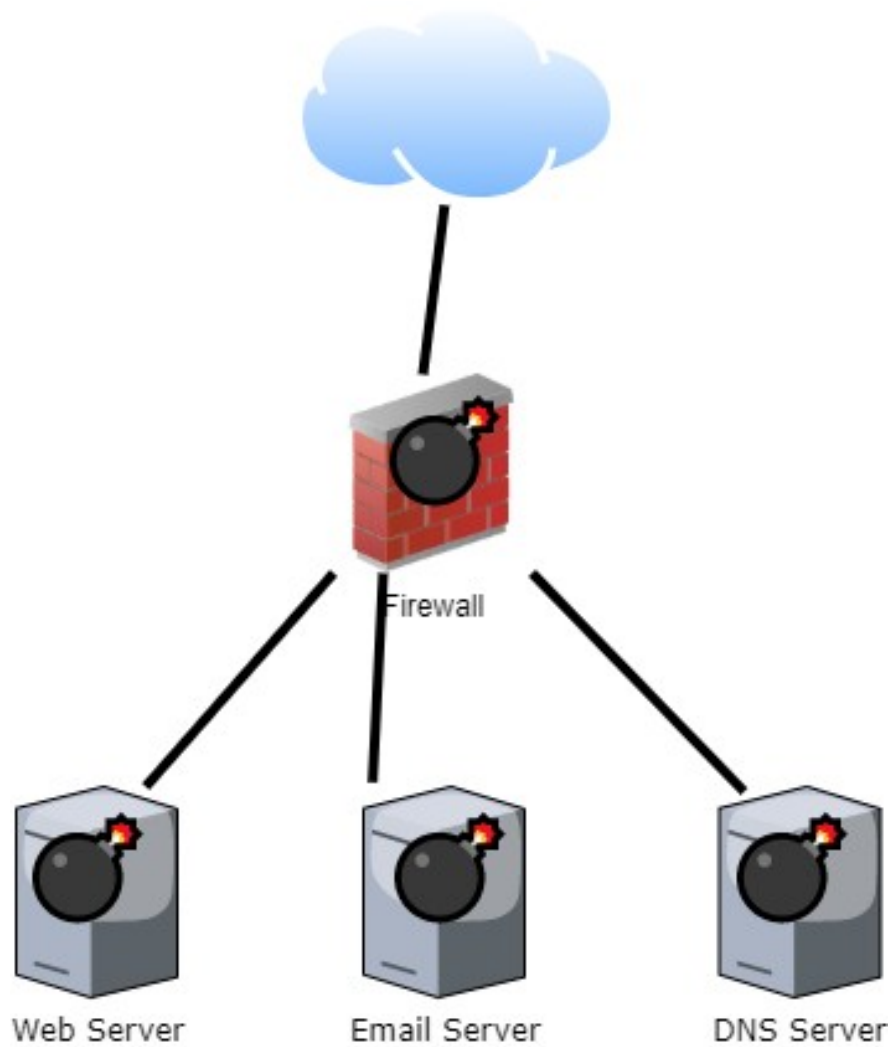
- What other organisations share the same internet connections/firewalls/web servers
  - Can an attack on them affect you?
- Attacks could affect International and Domestic Links

# How to protect your systems



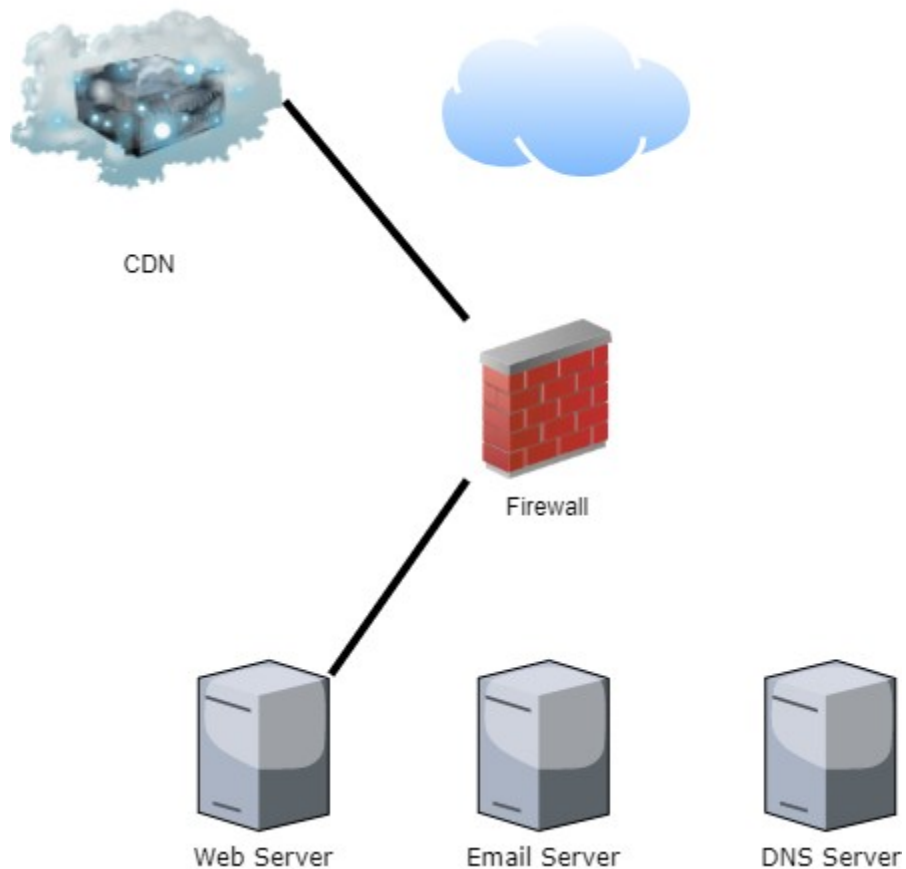
# What systems do you have?

- If you have Shadow IT the attacker most probably has a better than you
- Can't defend what you don't know about
- Even systems you don't know about can cause issues to other systems or reputational damage



# Web Content

- Use a CDN
- Problem Solved?



# CDN Considerations

- Is the content CDNable?
- How is dynamic and user sessions going to be handled?



# Does the CDN have the right tick boxes?

- Do Origin Servers only allow requests from CDN?
- Who can purge/expire documents cached in the CDN?

# CDN Purge

```
$ curl -o /dev/null -w %{time_total} -s  
https://example.com/1.html
```

0.299s

```
$ curl -X PURGE https://example.com/1.html  
{ "status": "ok", "id": "10422-1600263910-3" }
```

```
$ curl -o /dev/null -w %{time_total} -s  
https://example.com/1.html
```

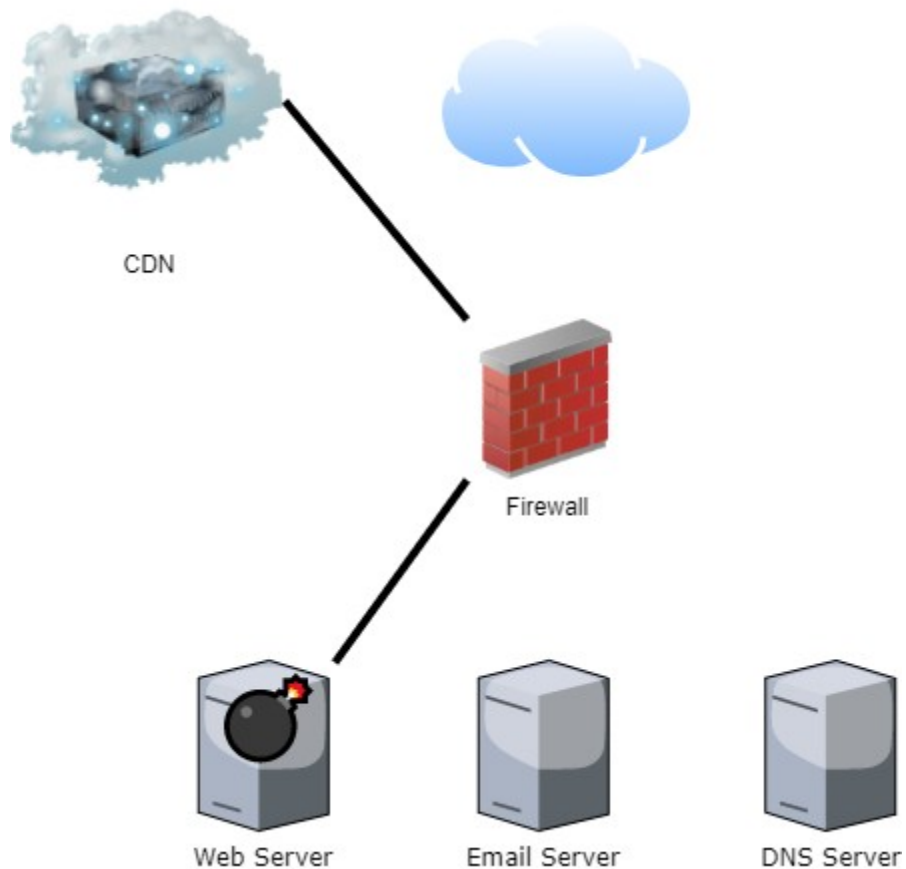
1.163

```
$ curl -o /dev/null -w %{time_total} -s  
https://example.com/1.html
```

0.268

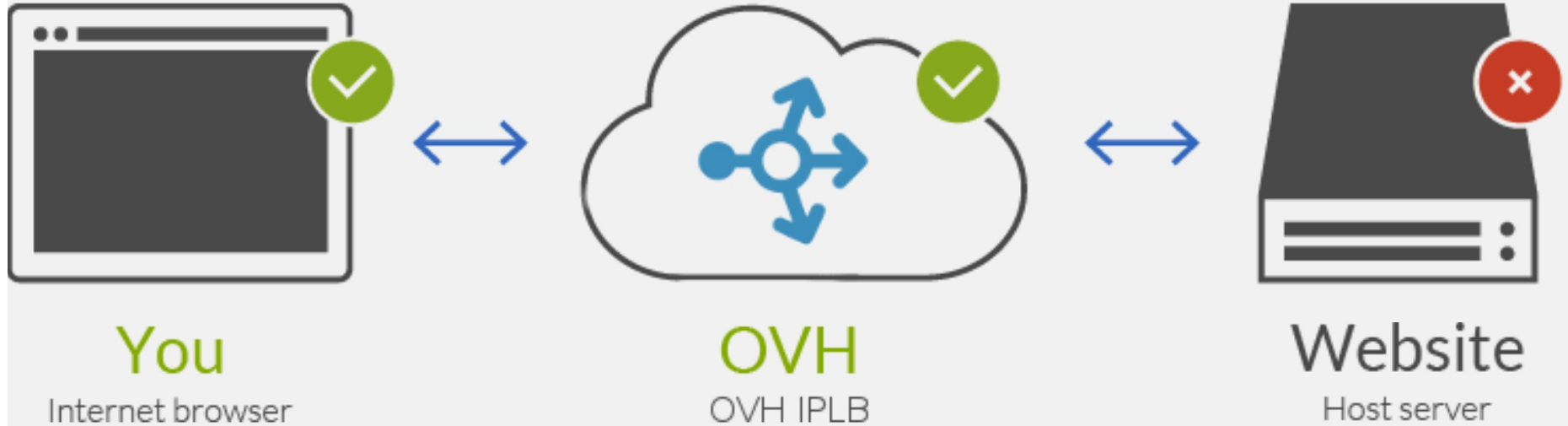
# Can people still find the Origin Servers?

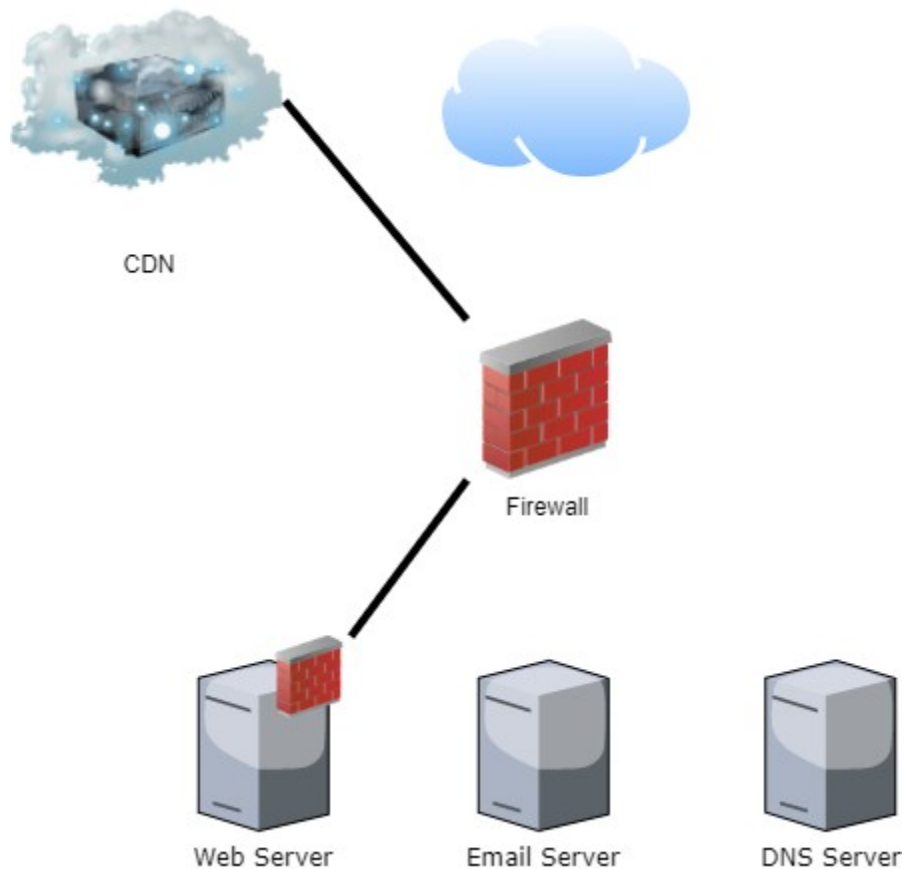
- Are your Origin Servers still on the same IP addresses?
  - Can you look up the IP address in DNS history
- Maybe you are using a domain name like `origin.www.example.com`
- Can you send traffic to those IP addresses
  - Even if the Firewall denies the packets, it still consumes some CPU resources (hopefully it can handle it)



# Error 503: Backend unavailable

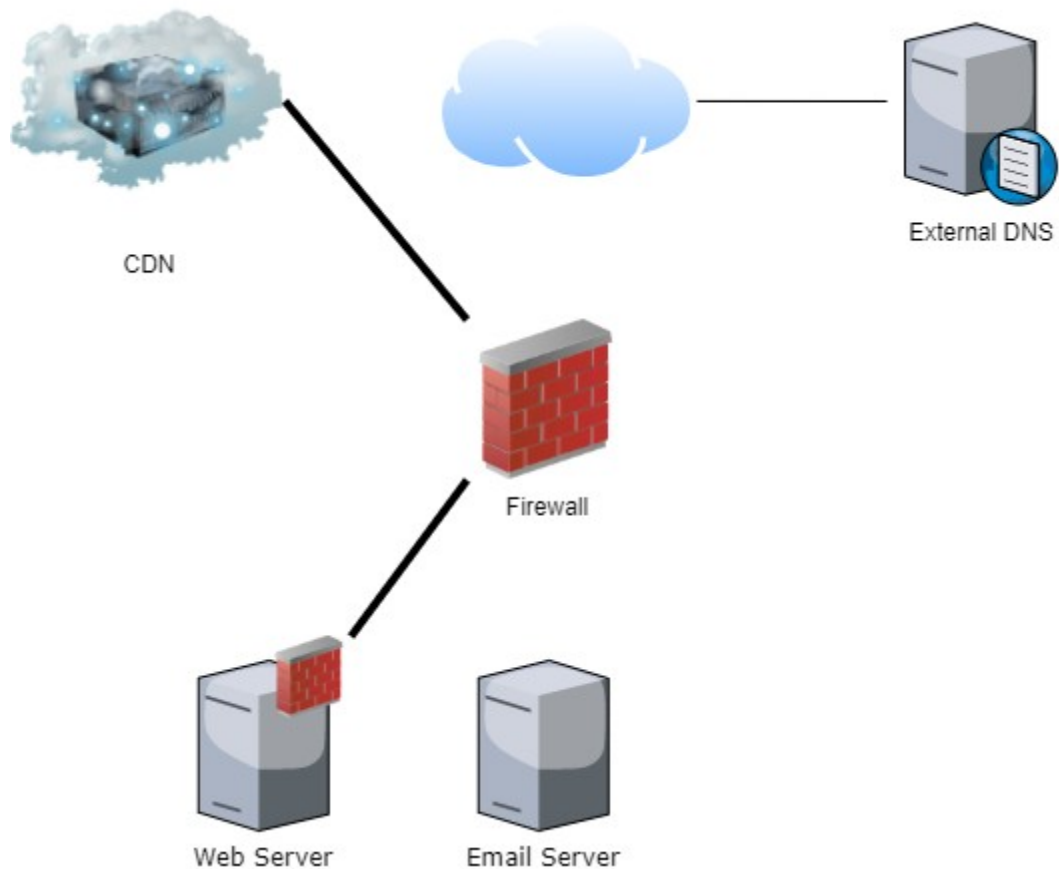
This type of error usually results of an unavailability of servers behind IP Load Balancing.





# DNS/Domain Registration

- A lot of mitigations require DNS updates to move critical systems
- Ensure public DNS is scalable to DDoS attacks
  - Use a DNS provider who has Points of Presence world wide, including NZ
  - Allows for changes quickly (subject to DNS TTL)



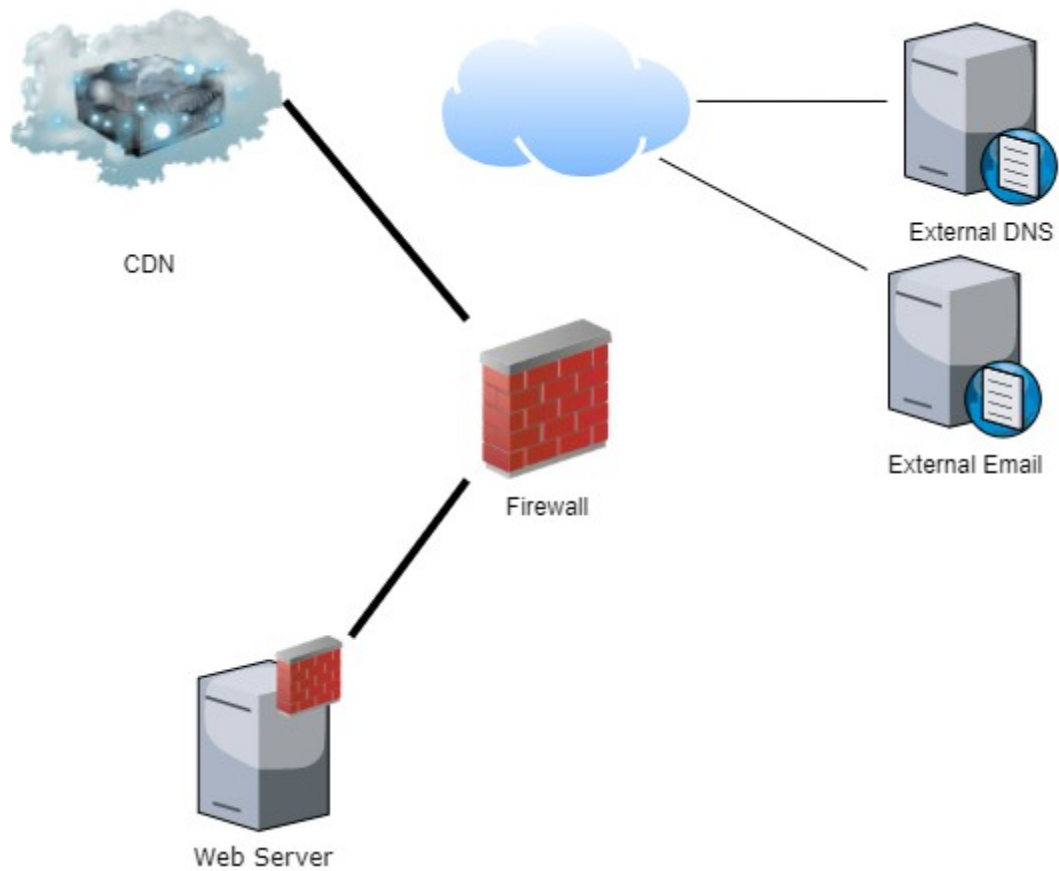


# DNS/Domain Registration

- Consolidate all the domain registration and DNS in one place
  - Know how to access it
  - Don't fail because one person is on leave

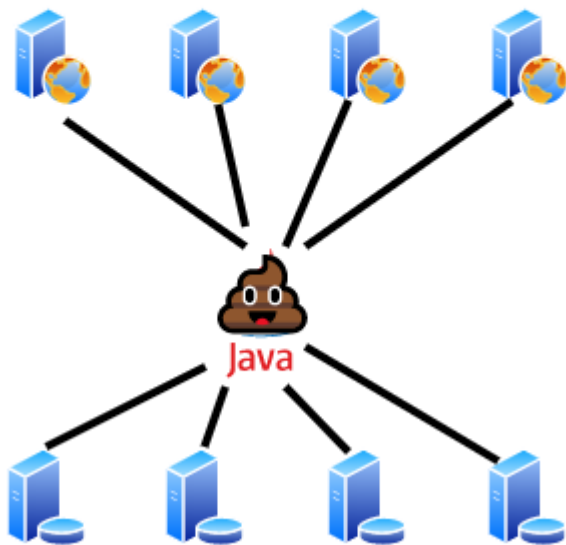
# Other Infrastructure

- BGP/Dynamic Routing
  - Appropriately restricted
- Mail
  - Consider using cloud providers
  - The days of rolling your own are dead



# Application Design/Architecture

- Design and Architect the applications/networks to best make use of caching and DDoS mitigations technologies
- Anything not cacheable should be behind a login, CAPTCHA, or other rate limiting techniques
  - Test your CAPTCHA
- Implement multi-tier architecture and make sure you don't have layer-7 bottlenecks



# Layer 7

- Conduct a detailed performance test against your web sites/infrastructure
- Understand the performance bottlenecks
- It's hard for a WAF to block traffic to endpoints affected by performance issues as the requests will look legitimate.

# 404 Pages

- 404 pages should not be a problem right???

# How to know what is a 404?

- The CDN will cache all the pages which have been requested
- Do 404s have to go to the origin server and hit the database?
- There are infinite(ish) possible 404 pages
- Make the CDN aware of the valid pages, so the CDN can return the 404 itself
  - Even if it is the first time that URL has ever been requested

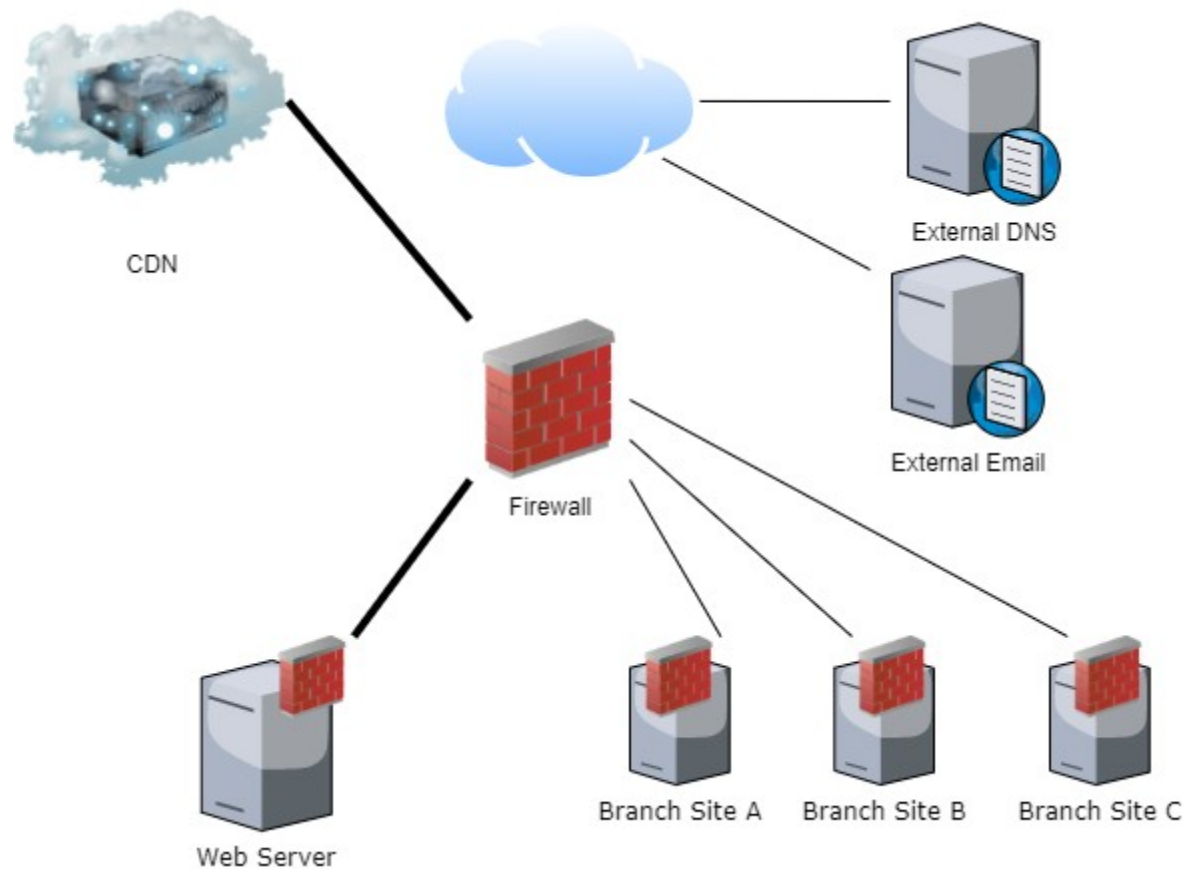


# Other Layer 7 Mitigations

- Make sure patches are installed
- This will help stop exploitation of bugs in the application or device, which will slow it down or crash it

# Branch Sites

- Restrict access to branch site firewalls
  - Geo fencing to NZ IP addresses (ok)
  - Only allow access from the head office/site-to-site VPN (better)



# Monitor all the things

- Monitor and collect statistics on your system
  - Know what **normal** looks like

**LOOKING AT TRAFFIC  
LOGS FOR THE FIRST TIME**



**IS THIS A DDOS ATTACK**

# Monitoring

- Monitor the servers / websites
  - NAGIOS, Pingdom, etc
- Do external monitoring from inside & outside of NZ

# Disk space monitoring, what's that?

- We recently caused a firewall to fail spectacularly when its disk filled up with logs during a routine port scan.
- This resulted in an outage
  - The client complained
  - We logged it as a high-risk finding

# Test/Simulation

- Does the end to end system work how you expect it to work?
- Does your service provider have the correct phone numbers?



# Wrap up

- What systems could cripple your business (or your customers) if affected, focus on those
- Hopefully you now have an idea about what:
  - Your threats are
  - A start of a plan to defend them
- This can be a little overwhelming

# Do things in a sensible order

- There is a Maturity Model for that:
- <https://zxsecurity.co.nz/maturity-models/dos-preparation-maturity-model/>

# Denial-of-Service (DoS) Attack Preparation Maturity Model



A denial-of-service attack is a cyberattack specifically designed to shut down a computer or network, making it inaccessible to its users.

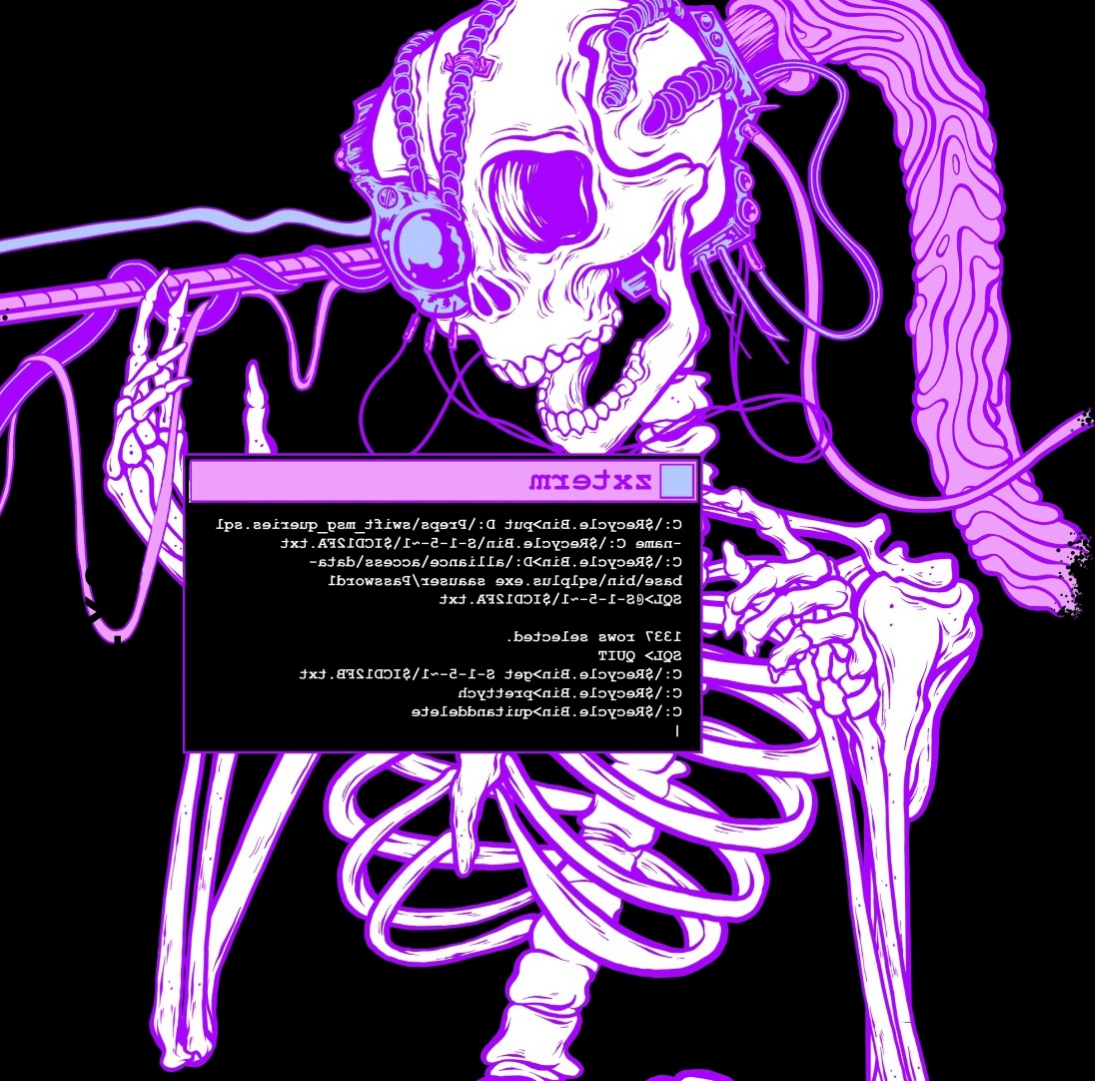


# Roughly distils down to

1. Figure out what you have to defend/what attackers are going to attack
2. Plan how you are going about defending your assets
3. Put the defences in place
4. Start monitoring and doing simulations

# Thanks

- You for coming
- Thank for ChCon Crew for accepting my talk
- ZX Team for bouncing ideas off & giving me content



zxterm

```
C:\$Recycle.Bin>dir D:\Prags\swift_mad_queries.sql
-name C:\$Recycle.Bin\2-1-2--1\%CD12FA.txt
C:\$Recycle.Bin>dir Alliance/access/data-
base\bin\edp\plus.exe sasuser\Password1
SQL>2-1-2--1\%CD12FA.txt

1337 rows selected.
SQL>QUIT
C:\$Recycle.Bin>def 2-1-2--1\%CD12FA.txt
C:\$Recycle.Bin>preftjch
C:\$Recycle.Bin>quitfanddelate
```

# Thanks

Twitter: @nzkarit

Email:

dave@zxsecurity.co.nz