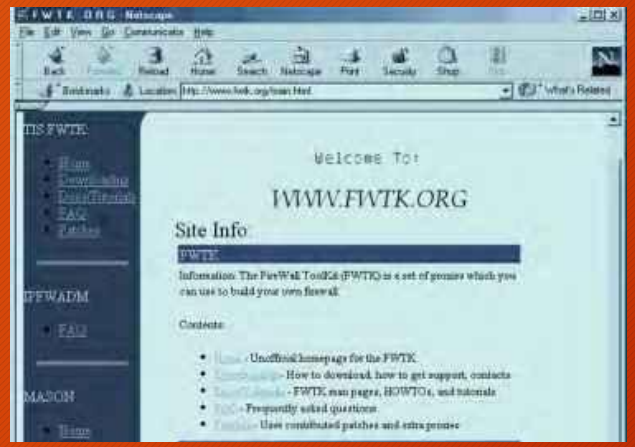
Firewalls

Summary

- Brief History of Firewalls
- What is a Firewall?
- Why Firewalls?
- Network Address Translation
- Types of Firewalls
- Linux/Windows Firewalls
- pfSense
- Blue Team Activity

Brief History

- “Firewall” inspired by physical barriers intended to contain fires
- Network routers were predecessors to modern firewalls
- Packet Filters developed in 1987 by AT&T Bell Labs
- Stateful Filters developed 1989-1990 by AT&T Bell Labs
- Firewall Toolkit (FWTK) developed in 1993



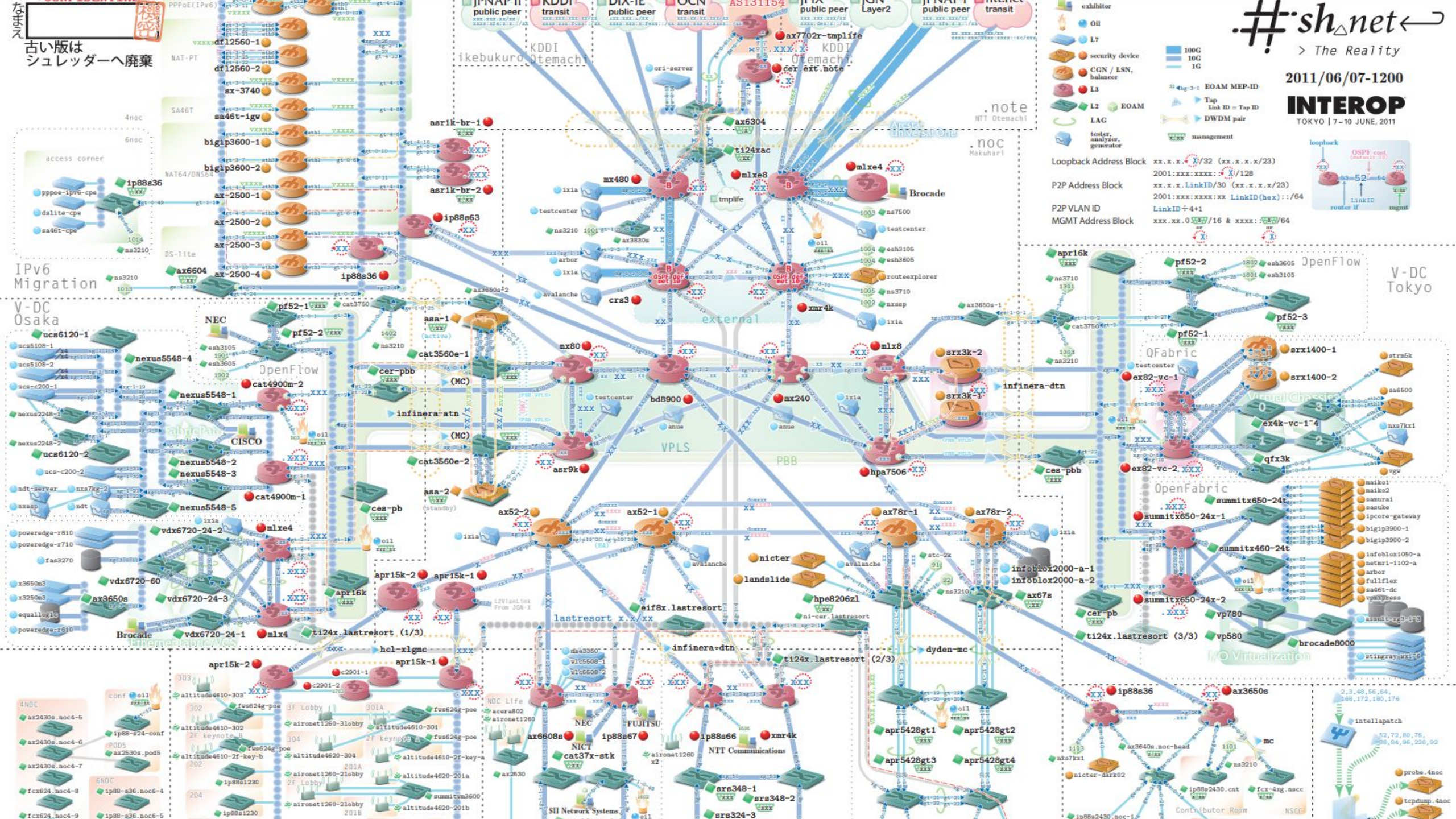
AT&T Bell Laboratories

What is a Firewall?

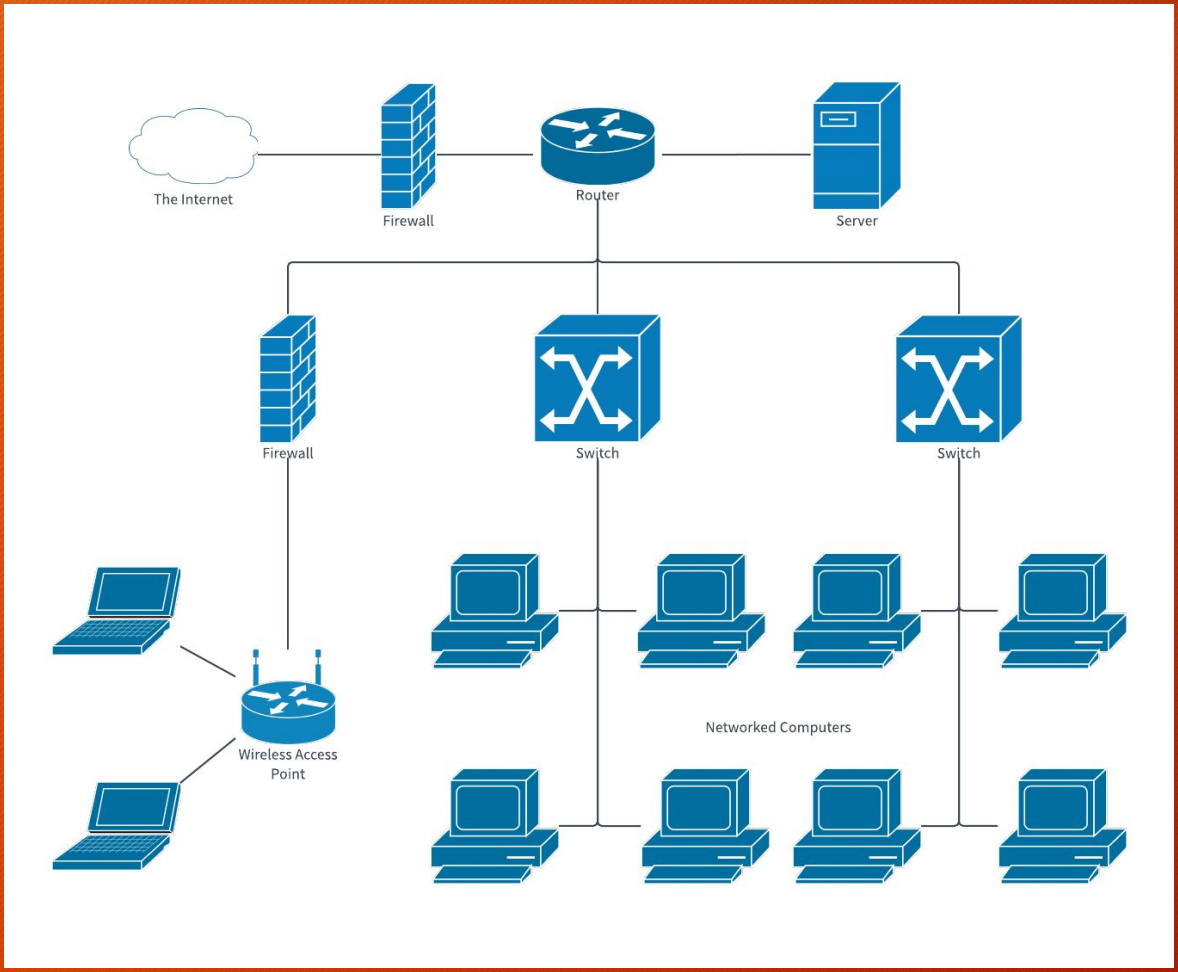
What is a Firewall?

- Types of Firewalls
  - First Generation (Packet Filters)
  - Second Generation (Stateful)
  - Third Generation (Application Layer)
    - Next Generation Firewalls

Why Firewalls?


なまえ
古い版は
シュレッダーへ廃棄
#sh△net
> The Reality
2011/06/07-1200
INTEROP
TOKYO | 7-10 JUNE, 2011
IPv6 Migration
V-DC Osaka
V-DC Tokyo
.noc
Makuhari
.note
NTT Otemachi
KDDI Otemachi
external
VPLS
PBB
OpenFlow
QFabric
OpenFabric
Virtual Chassis
I/O Virtualization
lastresort x.x/xx
Loopback Address Block
P2P Address Block
P2P VLAN ID
MGMT Address Block
Brocade
NEC
CISCO
NTT Communications
FUJITSU
NICT

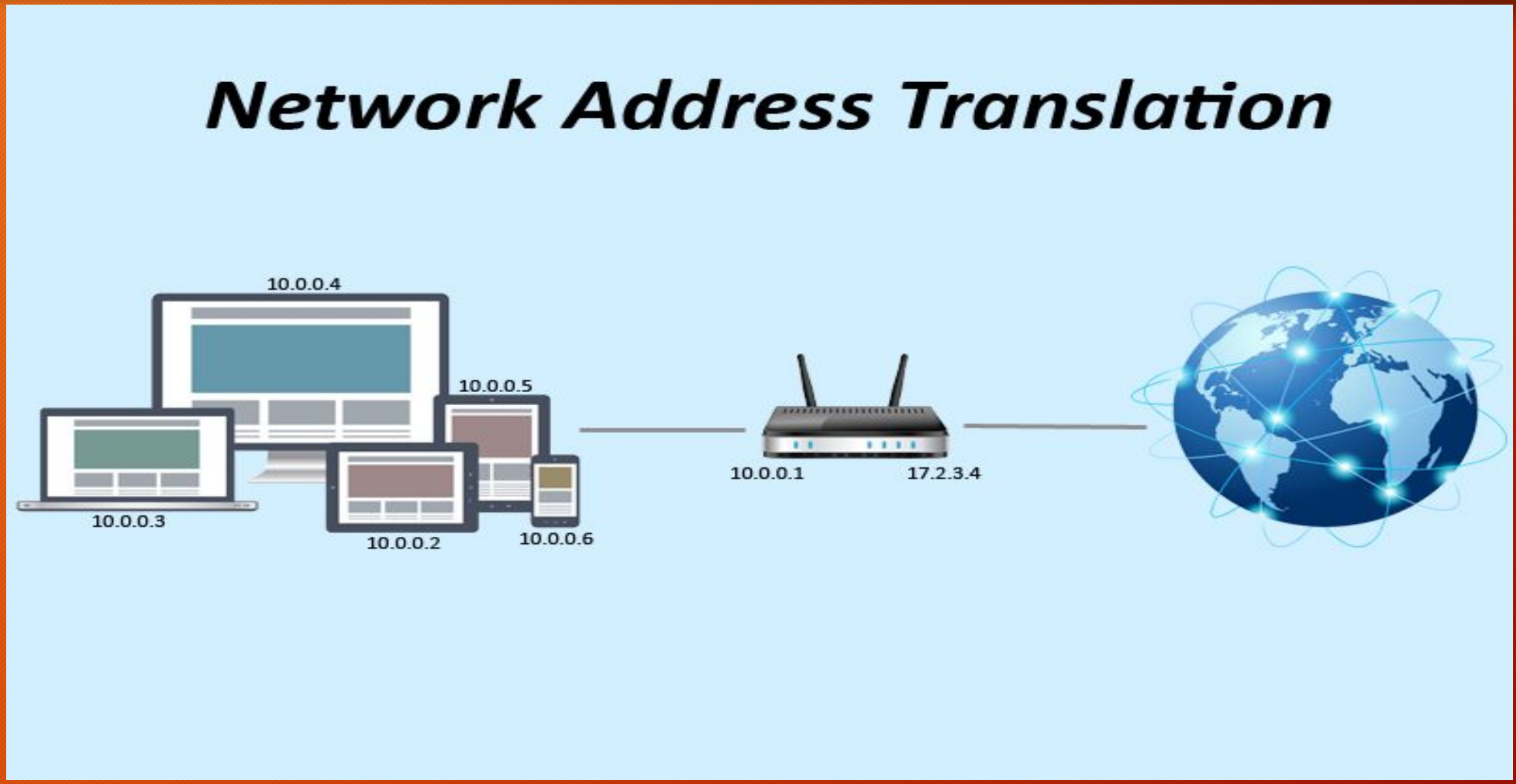
Why Firewalls?



Network Address Translation (NAT)

- Assigns IP address to hosts on LAN
  - External devices cannot see the internal IP Address of device
  - All devices on same LAN have same external facing IP Address
- 1:1 NAT
  - ONE external IP Address to ONE internal IP Address

Network Address Translation (NAT)



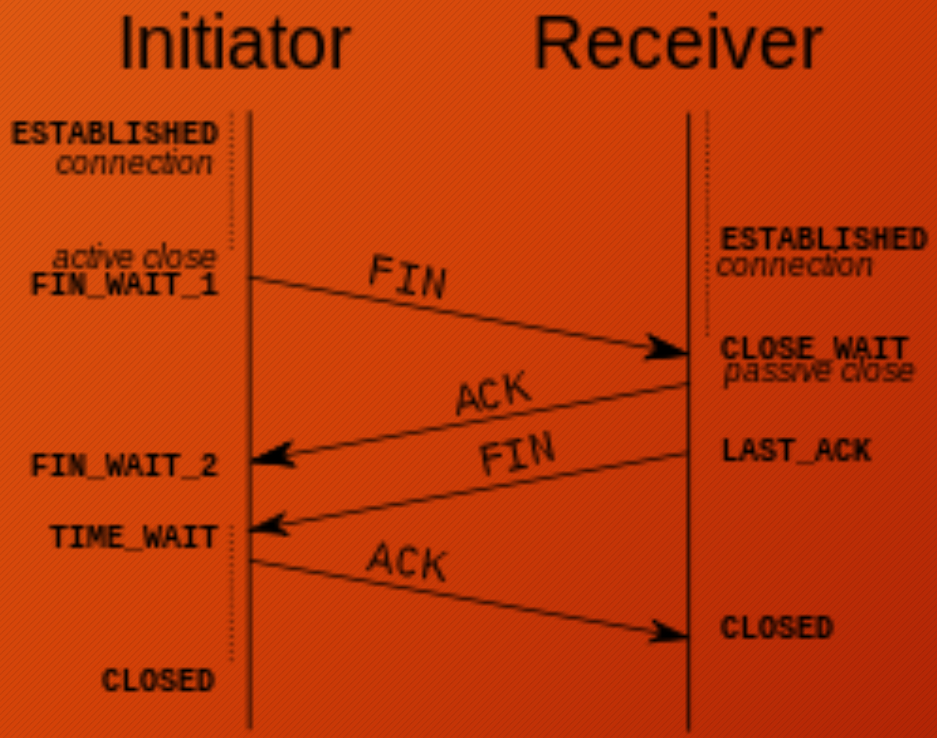
Firewall Types

Packet Filters (First Gen)

- Uses set of rules
  - Determines whether to drop or reject packet
    - Drop (Silently discard)
    - Reject (Discard and inform sender)

Stateful (Second Gen)

What is this?



Stateful (Second Gen)

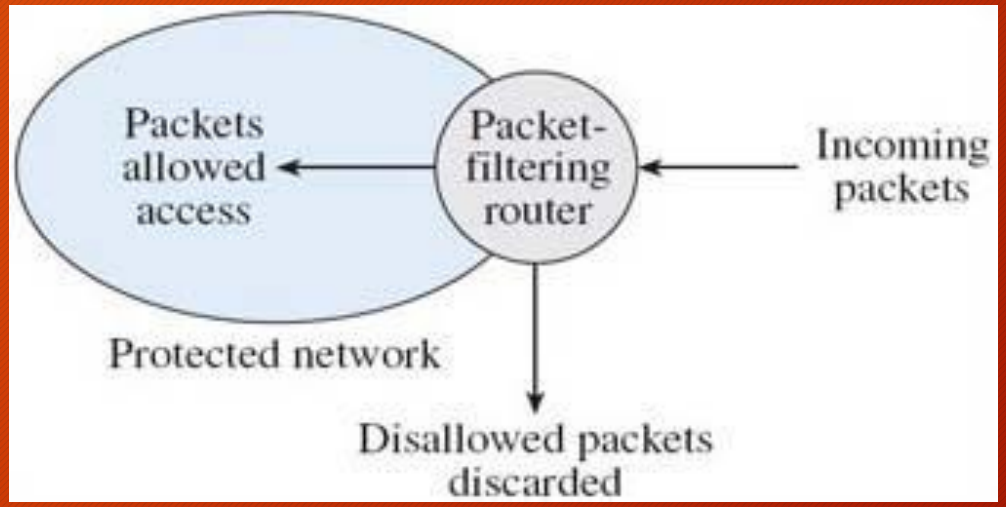
- Determines whether to drop or reject packet
  - Drop (Silently discard)
  - Reject (Discard and inform sender)
- Understands conversations happen between devices
  - Can monitor specific TCP Sessions
- Understands that data flows are bi-directional

Application Layer (Third Gen)

- All second and first gen features
- Can Identify certain applications and protocols
  - E.g. FTP, DNS, HTTP, etc.
- Next generation Firewalls use “deep packet inspection”
  - Intrusion detection
  - Identity management
  - Web application Firewall
- Very powerful if configured properly
  - Proper configuration will make a Red Team sad/mad

Review of Types

- Packet Filtering
- Stateful
- Application Layer
  - Next Generation



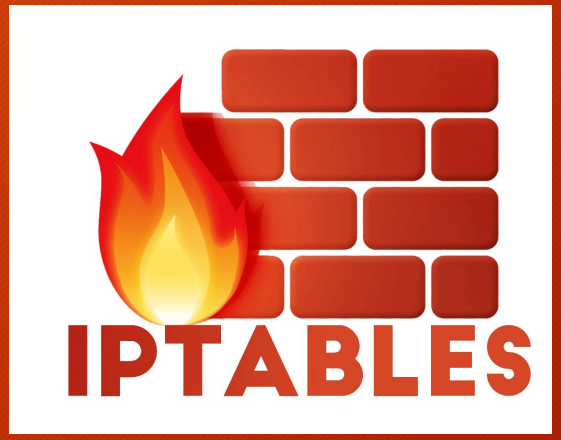
Break

Back in 10 Minutes

Host Based Firewalls

Linux Firewalls

- iptables & UFW (Uncomplicated Firewall)
  - Host based firewall
  - Tool for packet filtering



iptables

- iptables flags
  - -A Append one or more rule
  - -D Delete a Rule
  - -I Insert a Rule
  - -R Replace
  - -F FLUSH chain, delete rule one by one
  - -j Jump
  - -s Source IP
  - -d Destination IP
  - -p Protocol(TCP/IP)
  - -L List all rules
  - -N Numerically List
  - -v Verbose (More information output)
  - Need more? $ man iptables

Example rules iptables

- Block an incoming IP
  - iptables –A INPUT –s 10.42.X.XXX –j DROP
- Block outgoing IP:
  - iptables –A OUTPUT –d 10.42.X.XXX –j DROP
- Block an incoming port:
  - iptables –A INPUT –s 10.42.X.XXX –p tcp –destination-port 80 –j drop

Example rules UFW

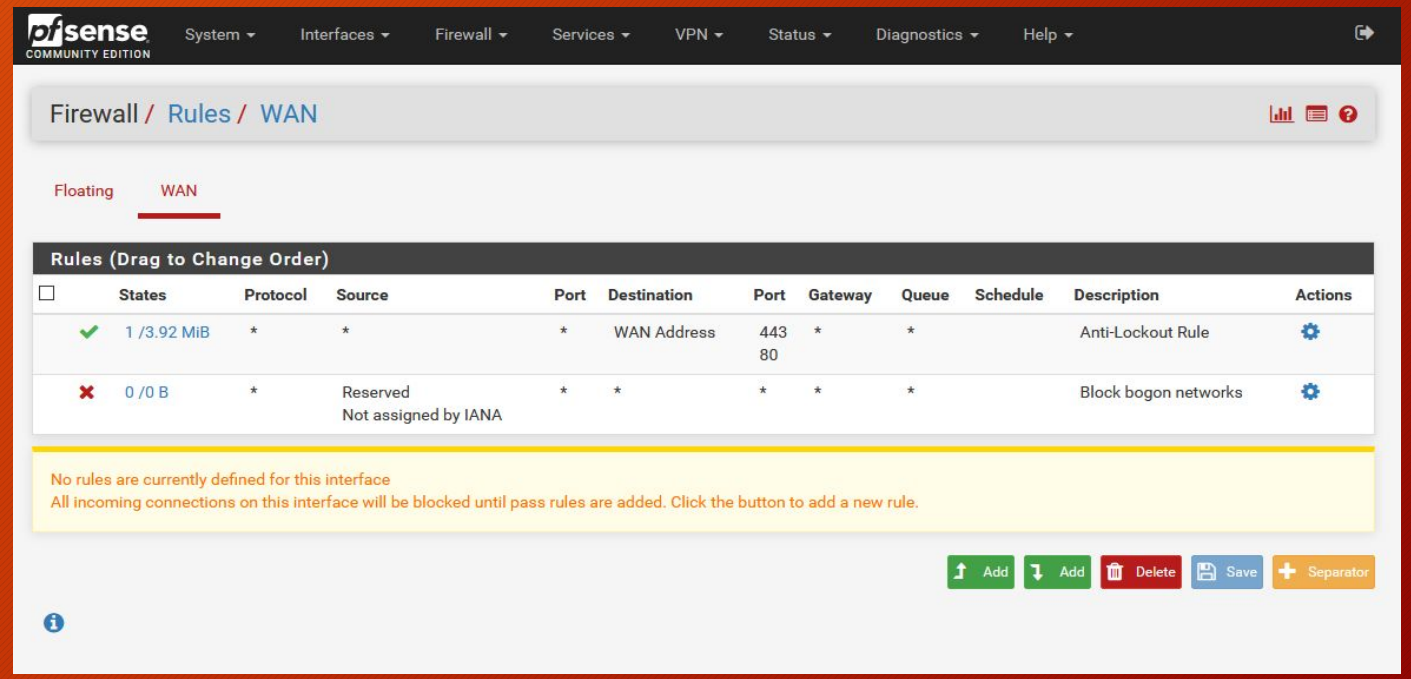
- Block an incoming IP
  - ufw deny from 10.42.X.XXX /24
- Block HTTP Protocol
  - ufw deny http(80)
- Allow an incoming port
  - ufw allow from 10.42.X.XXX to any port 22

Windows Firewall

- Windows Defender Firewall
  - GUI and CLI functionality
  - Built into Windows

pfsense

- 3rd generation firewall
  - Next Gen Capabilities
- Free



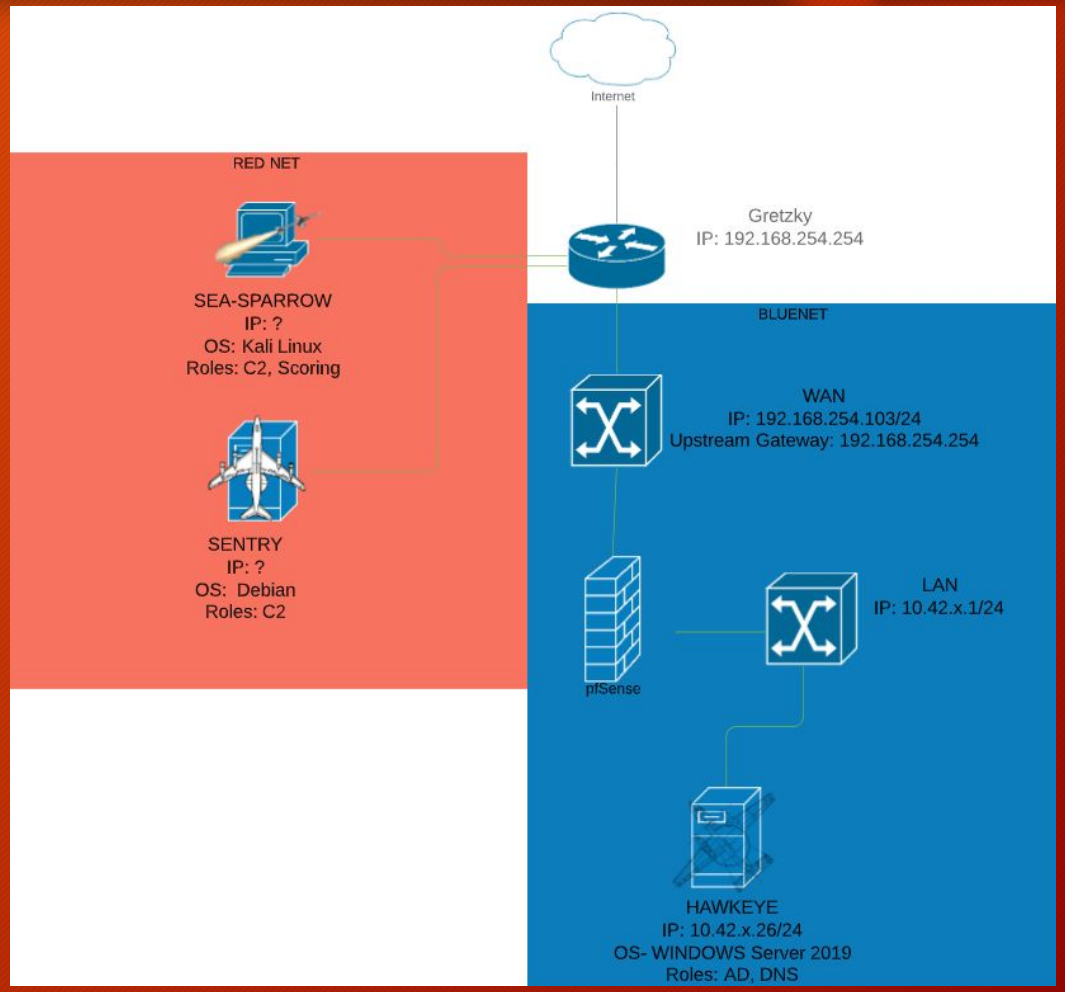
Blue Team Activity

Format

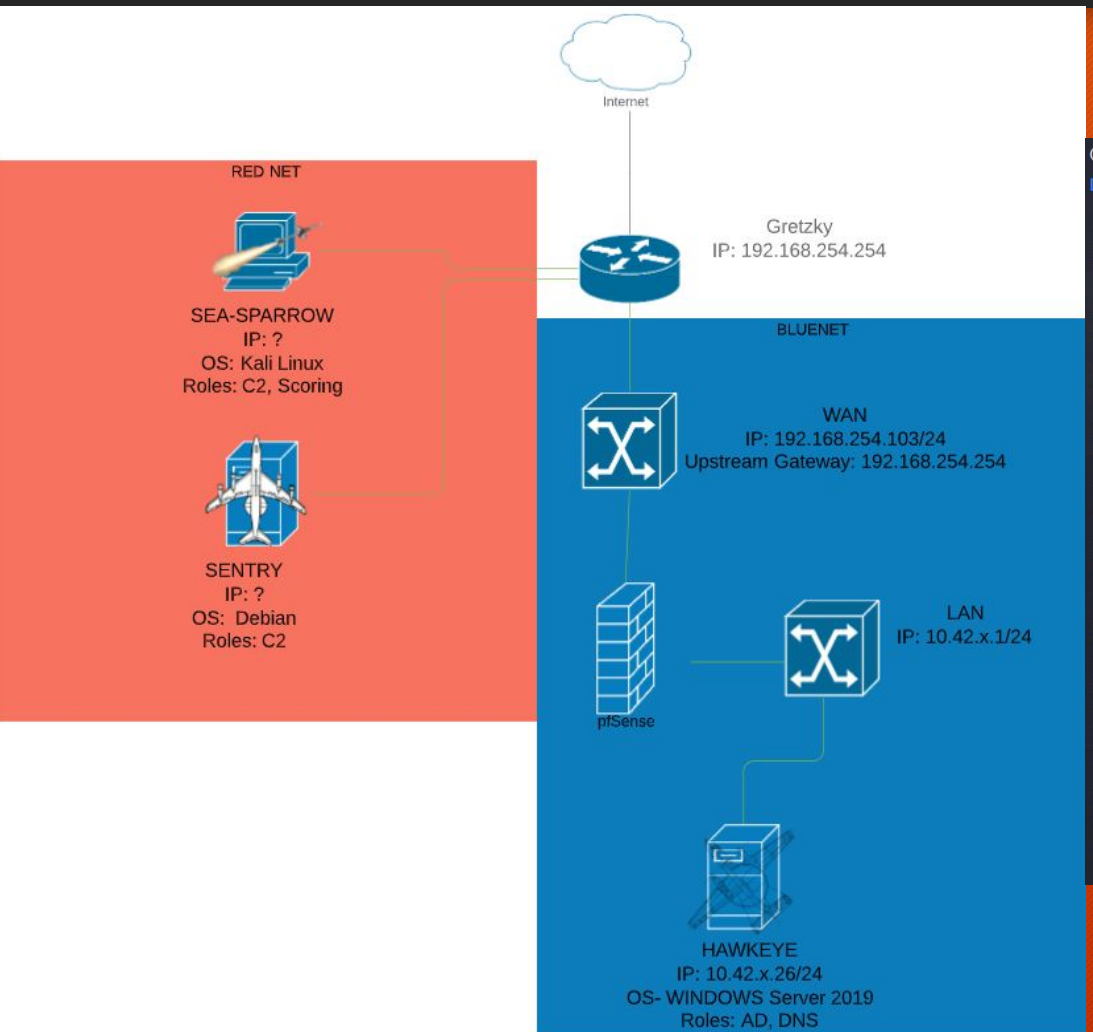
- Groups of 2
  - Will have your own Zoom break out room
- First 30 minutes are unassisted
  - Exceptions for issues that are out of scope
- If you think you have complete the task
  - Message me and I will confirm deny

Environment

- One compromised domain controller
  - Username: Administrator
  - Password: Change.me!



Environment




```
(Empire: agents) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name  Username                Process     PID   Delay    Last Seen           Listener
 ----     -- -----------     ------------  --------                -------     ---   -----    ---------           ----------------
 CWP3V9Z7 ps 10.42.4.26      HAWKEYE       *NIMITZ\Administrator   powershell  2768  5/0.0    2020-04-01 15:08:27 http
 NF5GL4XK ps 10.42.7.26      HAWKEYE       *NIMITZ\Administrator   powershell  800   5/0.0    2020-04-01 15:08:26 http
 87PUW65A ps 10.42.7.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  1268  5/0.0    2020-04-01 15:08:26 http

 31KBFGSM ps 10.42.6.26      HAWKEYE       *NIMITZ\Administrator   powershell  3688  5/0.0    2020-04-01 15:08:25 http
 U8TBHPVX ps 10.42.8.26      HAWKEYE       *NIMITZ\Administrator   powershell  6072  5/0.0    2020-04-01 15:08:25 http
 FY48P5G3 ps 10.42.6.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  2280  5/0.0    2020-04-01 15:08:25 http

 PBN2YS8W ps 10.42.6.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  6872  5/0.0    2020-04-01 15:08:25 http
 F64BGC8L ps 10.42.8.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  5080  5/0.0    2020-04-01 15:08:26 http
 1NUR4GCL ps 10.42.8.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  4628  5/0.0    2020-04-01 15:08:25 http

 ZN68HCYL ps 10.42.6.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  4196  5/0.0    2020-04-01 15:08:28 http
 RAV8XW6T ps 10.42.8.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  2268  5/0.0    2020-04-01 15:08:27 http
 AL3NMP5D ps 10.42.7.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  2816  5/0.0    2020-04-01 15:08:28 http

 XGKNZSU7 ps 10.42.4.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  2604  5/0.0    2020-04-01 15:08:26 http
 BRXU23EF ps 10.42.15.26     HAWKEYE       *NIMITZ\Administrator   powershell  5576  5/0.0    2020-04-01 15:08:26 http
 SXWD1T3L ps 10.42.14.26     HAWKEYE       *NIMITZ\Administrator   powershell  1576  5/0.0    2020-04-01 15:08:30 http

 GUDH8EV1 ps 10.42.15.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  3524  5/0.0    2020-04-01 15:08:25 http
 78BYLV4H ps 10.42.15.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  100   5/0.0    2020-04-01 15:08:26 http
 G3K28E6D ps 10.42.14.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  5428  5/0.0    2020-04-01 15:08:26 http

 69P8SULX ps 10.42.14.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  3048  5/0.0    2020-04-01 15:08:26 http
 PBNGLC6K ps 10.42.9.26      HAWKEYE       *NIMITZ\Administrator   powershell  1848  5/0.0    2020-04-01 15:08:26 http
 LPVHN7A5 ps 10.42.9.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  4468  5/0.0    2020-04-01 15:08:25 http

 E76F9RWD ps 10.42.9.26      HAWKEYE       *NIMITZ\SYSTEM          powershell  4972  5/0.0    2020-04-01 15:08:25 http
 86STZA4C ps 10.42.25.26     HAWKEYE       *NIMITZ\Administrator   powershell  5460  5/0.0    2020-04-01 15:08:28 http
 M3WRKPG7 ps 10.42.16.26     HAWKEYE       *NIMITZ\Administrator   powershell  4892  5/0.0    2020-04-01 15:08:26 http

 53VGNUYE ps 10.42.17.26     HAWKEYE       *NIMITZ\Administrator   powershell  2936  5/0.0    2020-04-01 15:08:26 http
 564VYDN1 ps 10.42.25.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  2256  5/0.0    2020-04-01 15:08:28 http
 AF85ZD4Y ps 10.42.25.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  3416  5/0.0    2020-04-01 15:08:29 http

 FT25SMEY ps 10.42.16.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  5928  5/0.0    2020-04-01 15:08:29 http
 PZ3L2784 ps 10.42.17.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  2444  5/0.0    2020-04-01 15:08:26 http
 G942CUP3 ps 10.42.16.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  1740  5/0.0    2020-04-01 15:08:28 http

 MYCL3U2P ps 10.42.17.26     HAWKEYE       *NIMITZ\SYSTEM          powershell  5376  5/0.0    2020-04-01 15:08:29 http
 WCXS653Z ps 10.42.2.26      HAWKEYE       *NIMITZ\Administrator   powershell  5684  5/0.0    2020-04-01 15:08:25 http
```

Goals

- Goal 1: Using Firewalls (pfsense or Windows) kick me out
- Goal 2: Keep DNS online
- Bonus: After 1 & 2 remove malware

```
kali@SEA-SPARROW:/tmp$ dig HAWKEYE.nimitz.home @192.168.13.190

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> HAWKEYE.nimitz.home @192.168.13.190
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21725
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;HAWKEYE.nimitz.home.           IN      A

;; ANSWER SECTION:
HAWKEYE.nimitz.home.    3600    IN      A       192.168.13.190

;; Query time: 0 msec
;; SERVER: 192.168.13.190#53(192.168.13.190)
;; WHEN: Tue Mar 31 08:35:13 EDT 2020
;; MSG SIZE  rcvd: 64
```

Good luck and have fun!