

# Network Attacks

Denial-of-Service & Man-in-the-Middle

# Agenda

---

- Two categories of attacks on networks
    - Denial-of-Service
    - Man-in-the-Middle
  - Defence
- 

Security 360

## (D) DoS & MitM

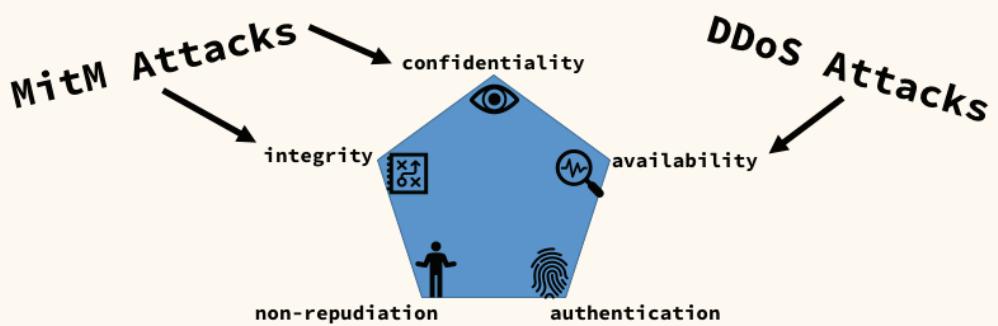
---

- Denial-of-Service Attacks
  - An attacker sends packets until your server fails
- Distributed Denial-of-Service Attacks
  - Many attackers (and/or bots) send the packets
- Man-in-the-Middle Attacks
  - An attacker places themselves between two parties

---

Security 360

## Where's the threat?



Security 360

# Denial-of-Service

---

- Single attacker
  - Quite literal
    - Deny access to a service
    - Impair function of a service
  - Probably the strongest attack against availability
- 

Security 360



"No Entry" by Joshua Rappenecker is licensed under CC BY-SA 2.0

# Distributed Denial-of-Service

- Multiple attackers coordinate
  - Geographically separate
  - Usually involves a botnet
- BOTNET
  - Infected hosts (zombies/slaves) unwillingly and unknowingly participate in the attack



---

Security 360

*"A little 'bot of kindness is sometimes all that is needed."* by [Swijak](#) is licensed under [CC PDM 1.0](#)

## Mirai

---

- Largest botnet at the time (2016)
  - > 1Tbps & 600,000 affected devices
- nmap scans for open ports 23/22 (Telnet/SSH)
  - Try a simple list (~10) of common username/passwords
  - Targets IoT devices with default credentials
- Drop bot code on the device
  - Bot connects to command & control
  - C&C orders the attack when many bots are connected

---

Security 360

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M. and Kumar, D., 2017. Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 1093-1110).

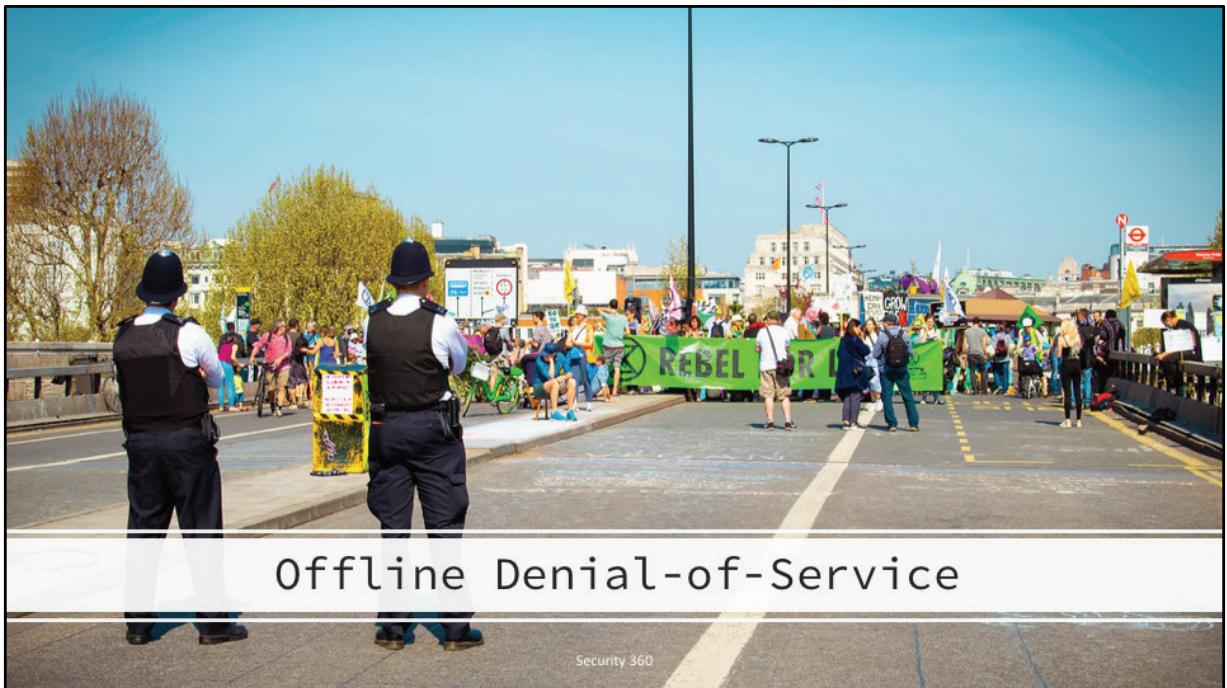
## Mirai & Variants: Targets

- Krebs on Security
- OVH (Cloud Computing)
- Liberia Telecom
- Deutsche Telkom
- DYN (DNS Service)
  - Amazon
  - Github
  - Twitter
  - Netflix
  - Reddit

Security 360

LUPUS

*"Smart Home Product Family"* by Lina Kuroi, Ning Zhou is licensed under [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nd/4.0/)



["Extinction Rebellion London"](#) by [Alexander Savin](#) is licensed under [CC BY 2.0](#)

# Motivations

for launching a denial-of-service

- Public & popular websites
  - To make a point
  - Political, environmental, socio-economic
- Company websites & servers
  - To make a point / €€€
  - To draw attention away from another simultaneous attack

## The rise of hacktivism

Security 360

*"Anonymous Mask Art 1" by [anongraphics](#) is licensed under [CC BY-NC-SA 2.0](#)*

## The Electrum DDoS Attack

- Electrum
  - Enhanced Bitcoin Wallet
  - Adds some enhanced functionality
  - Checks when transactions are verified
- Users should connect to Electrum servers
- Attackers create malicious servers
- DDoS the real servers
- Users get forced onto malicious servers



Security 360

*"Coinkite Coldcard Hardware Wallet" by [ghalfacree](#) is licensed under [CC BY-SA 2.0](#)*

# Measuring Attacks

---

**91%** UK businesses affected by Denial-of-Service

**£140 000** cost of the average attack

**£1 000 000 000** total cost to UK businesses

*NETSCOUT report 2018*



---

Security 360

"Error 404" by Alessandro Ceporina is licensed under [CC BY-NC 4.0](#)

# Measuring Uptime

---



- Service Level Agreement (SLA)
  - A uptime promise from a service provider

99.99% (~4m downtime per month)

99.9% (~43m downtime per month) Google Cloud credits 10%

99% (~7hrs downtime per month) Google Cloud credits 25%

95% (~36hrs downtime per month) Google Cloud credits 50%

---

Security 360

"Wecker" by [anka.albrecht](#) is licensed under [CC BY 2.0](#)

## Common (D)DoS Attacks

- SYN Flood
- UDP Flood
- HTTP Flood
- ICMP Flood
- Ping of Death
- Smurf Attack
- Fraggle Attack
- Slowloris



Security 360

["Viking Attack"](#) by [The Brickstons Group](#) is licensed under [CC BY-NC-SA 2.0](#)

## Floods (resource exhaustion)



- SYN Flood (remember the 3-way handshake?)
  - Attacker sends SYN packets to all victim ports
  - Never responds with ACK, victim waits patiently
  - Holding all the open connections == DoS
- UDP Flood
  - Attacker sends lots of UDP packets to victim
  - When UDP hits a port without a service, it responds to tell the attacker it failed
  - Responding to all the attacker packets == DoS

Security 360

["Floods125"](#) by [NRCS Montana](#) is licensed under [CC PDM 1.0](#)

## HTTP Floods

- Attacker sends HTTP requests
  - GET requests
    - Requests generate info
    - Return to user
  - POST requests
    - Requests take info
    - Send to database/backend
- Server unable to handle them
- Insufficient resources == DoS



Security 360

["Waterfall"](#) by [Jordan Cole](#) is licensed under [CC BY-NC-SA 2.0](#)

# ICMP Flood, Ping of Death

- PING! An echo request
  - Alice says hi, Bob says hi
  - Protocol: ICMP (in an IP packet)
- ICMP Flood – A flood of pings
- Ping of Death (patched)
  - Send an IPv4 packet which is too big
  - Attacker receives it, system crashes
  - Returned in 2012 with IPv6! (patched)



Security 360

"pls\_pong" by ~! is licensed under CC BY 2.0

# Flood Barriers

---

- **SYN** Flood Defence
    - Firewall limiting connections over time
  - **UDP** Flood Defence
    - Firewall closing/limiting UDP ports
  - **ICMP** Flood Defence
    - Firewall disabling ICMP requests
- 

Security 360

## Smurf Attack

- An ICMP Flood, in reverse
- Attacker spoofs victim IP
- Attacker pings a special network address
  - **Broadcast Address** - forwards packet to entire network
  - (patched)
- Entire network responds to the ping (@victim IP)
- Victim resources overwhelmed == DoS



Security 360

["DSC 4930"](#) by [Laurens Hop](#) is licensed under [CC BY-ND 2.0](#)

## Fraggle Attack

- Very similar to Smurf
- Sends UDP packets instead of ICMP packets
- (so, patched as well)

Security 360



*"broadcast"* by [totomaru](#) is licensed under [CC BY-NC-SA 2.0](#)

## Slowloris

- Send HTTP requests to victim
  - But slowly this time
- Connections open...
- Connections still open...
- ...just before connection timeout
  - Send another HTTP header!
- And repeat



*Affects threaded servers (Apache, Flask)*

Security 360

"01-slow" by [Draig](#) is licensed under [CC BY-NC 2.0](#)

## Defending Slow Attacks

- Web server configuration
  - Adjusting the timeout rate
  - Limiting connections per IP
  - Server firewall alerts
- OS Firewall configuration
  - Limiting concurrent connections

Security 360



*"Turtle in repose"* by [thriftyknitter](#) is licensed under [CC BY-NC-SA 2.0](#)

## Man-in-the-Middle

- An attacker places themselves between two legitimately communicating parties
- Receives the packet, and forwards it on



Security 360

## Being in the middle

---

- You sniff all the traffic between parties
  - No longer limited by switches/MAC addressing
- **tcpkill** – end the connection with an **RST** packet
- **mailSnarf/fileSnarf** – view victim emails/files
- **ssldump** – dump victim HTTPS packets
  - Later, find the key and decrypt! (< TLSv1.3\*)

---

Security 360

Suites: dsniff / cain & abel

RSA in <=TLSv1.2 has no “forward secrecy”, so if we get the key later, we can decrypt the data

DHE (Diffie-Hellman Ephemeral) in TLSv1.3 uses a new key for each communication, so is safe (provides forward secrecy)

## Getting in the middle

- ARP Cache Poisoning
- DNS Cache Poisoning
- Session/Cookie Hijacking
- SSL Hijacking
- Pineapples



Security 360

["Keys"](#) by [Wade Morgen](#) is licensed under [CC BY-NC 2.0](#)

# ARP Poisoning

- Address Resolution Protocol (L3)
  - Matches IPv4 with MAC Address
  - Sends an ARP request to network
    - *who-has 192.168.1.1 ?*
  - Stores the reply in the ARP Cache
    - Avoids performing the lookup each time
- Mallory sends fake ARP messages
  - Associates own MAC with victim/server IP
  - Cache updated with incorrect addresses
  - Traffic passes through the attacker



Security 360

["poison"](#) by [mivanov](#) is licensed under [CC BY 2.0](#)

## DNS Spoofing/Poisoning

- Altering DNS queries/entries to point to a malicious server

1. As a follow-up to ARP poisoning
  - DNS queries pass through the attacker now
  - Attacker sends back a malicious DNS response
2. By compromising the DNS server itself
  - Injecting fake DNS entries into the DNS server



Security 360

*"Malware Infection" by Visual Content is licensed under CC BY 2.0*

# Antidotes

---

- ARP
  - Static ARP entries
    - Fixed MAC – IP resolution
  - Tools: ArpON
- DNS
  - Trusted, secure DNS servers
  - DNSSEC
    - Cryptographically signed DNS responses



---

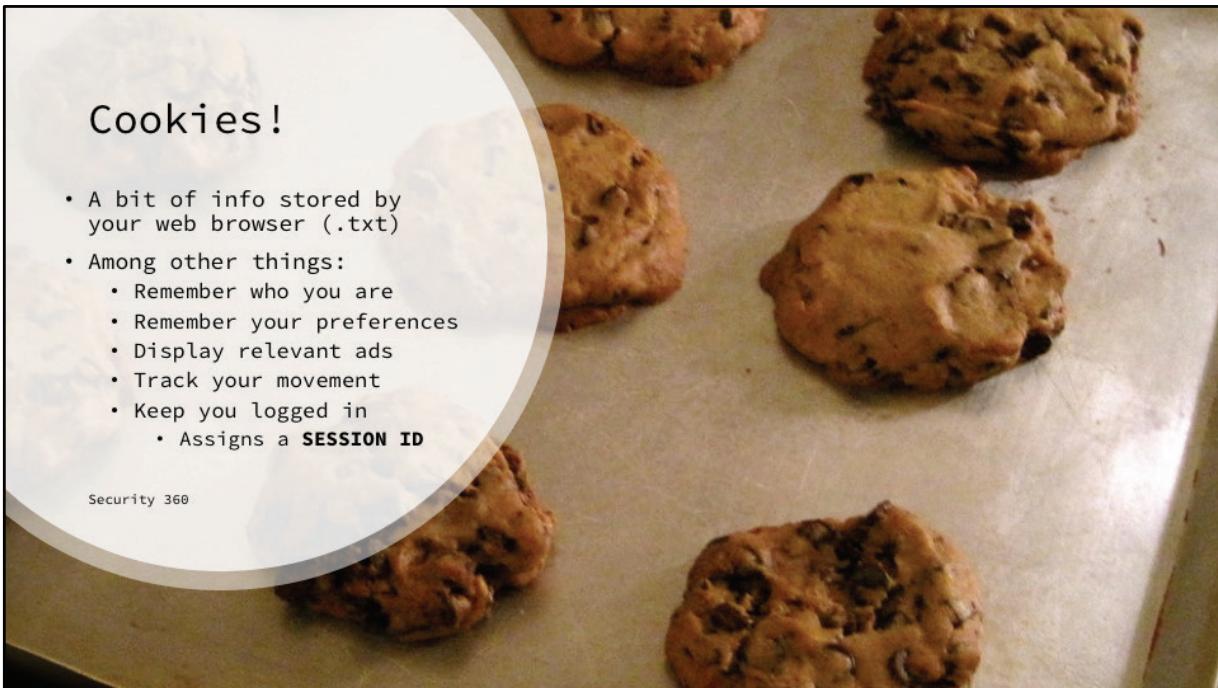
Security 360

Ipv6 is affected by neighbour discovery spoofing

## Cookies!

- A bit of info stored by your web browser (.txt)
- Among other things:
  - Remember who you are
  - Remember your preferences
  - Display relevant ads
  - Track your movement
  - Keep you logged in
  - Assigns a **SESSION ID**

Security 360



"NY Times Chocolate Chip Cookies" by lilszeto is licensed under CC BY-ND 2.0

# Session Hijacking

## Cookie Hijacking

- 
- 1.** Follow-up another MitM (side jacking)
    - Sniff & steal the cookie as it passes the attacker
  
  - 2.** Attacker sends a malicious link (fixation)
    - URL to the trusted site
    - Which defines a specific **session ID**
      - The attacker creates their own cookie with this session ID

*<https://www.myspace.com/HStwbis/login.php?sessionid=10359>*

---

Security 360

## La Cookie Défense

- Prevent other MitM attacks
  - Good ARP/DNS protection
- A secure culture and high security awareness
  - No weird links!



["La Défense, Paris \(2\)"](#) by glynneh is licensed under [CC BY-SA 2.0](#)

# SSL Hijacking

Getting in the middle of HTTPS

- Follow-up to other general MitM attacks

1. Downgrade the victim to HTTP
  - sslstrip

2. Generate our own certificates
  - ssllibsplit / mitmproxy



Security 360

["Add exception"](#) by [Kai Hendry](#) is licensed under [CC BY 2.0](#)

## SSL Hijack Defence

- Modern, updated browsers will warn the victim
  - Whether or not they choose to listen...
- All about culture, awareness
  - Be security-smart!



Security 360

*"Safety Goggles"* by [codersquid](#) is licensed under [CC BY-SA 2.0](#)

## Rogue Access Points

- Malicious Wireless Access Points
  - Managed by an attacker
- Pineapple WiFi
  - Can impersonate real APs with **Karma**
  - Since wireless NICs look for old APs, Karma just mimics them
- If a victim connects, you're MitM
- Can steal WPA credentials for other networks



Security 360

["Does this pineapple have an inferiority complex?"](#) by [adamthelibrarian](#) is licensed under [CC BY-NC-SA 2.0](#)

## A good general defence

- Virtual Private Networks
  - Encrypt all the data
- IPSec VPN
  - Asymmetric DH key exchange, symmetric encryption
  - Network layer (L3), encrypt IP Datagram
- SSL VPN
  - Asymmetric TLS key exchange, symmetric encryption
  - Transport layer (L4), encrypt UDP packet (or TCP)



Security 360

["Virtual Private Network \(VPN\)" by Infosec Images is licensed under CC BY 2.0](#)

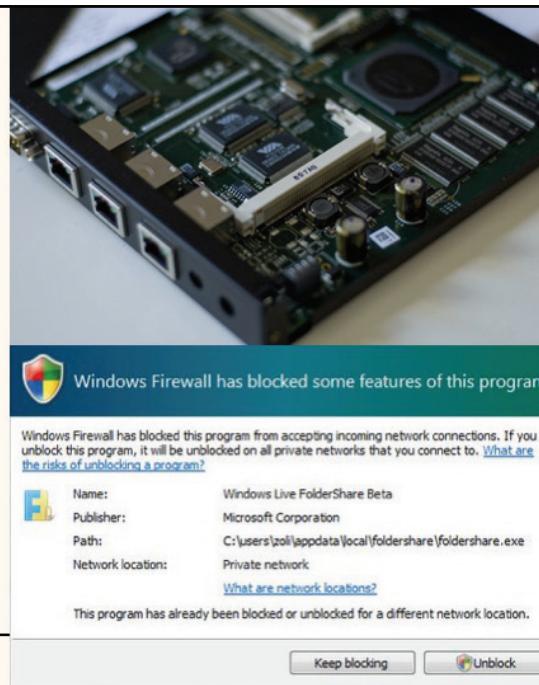
# Network Defence

Firewalls & Intrusion Detection/Prevention

# Firewalls

- A security perimeter around a network
  - Which packets can enter
- Hardware vs Software
  - A bit misleading
  - Hardware runs some software
  - Hard firewalls == Routers
  - Soft firewalls == Locally
  - Having both is ideal

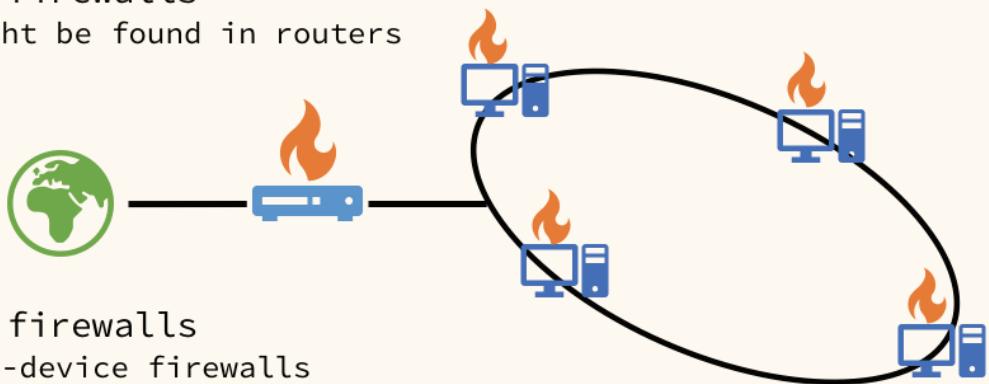
Security 360



*"The Firewall #2" by [lindstrom](#) is licensed under [CC BY-NC-ND 2.0](#).  
"firewall" by [zolierdos](#) is licensed under [CC BY-SA 2.0](#).*

## Firewalls on a Network

- Hard firewalls
  - Might be found in routers



- Soft firewalls
  - Per-device firewalls

Security 360

# Firewall Positioning

- **Perimeter** firewalls prevent unwanted traffic from entering the network
  - A first line of defence



- **Host** firewalls prevent unwanted traffic from hitting the device
  - Defence against attackers on the network



Security 360

# The State of a Firewall

- Firewalls either
  - **ACCEPT** a packet - *connection accepted*
  - **REJECT** a packet - *connection refused*
  - **DROP** a packet - *connection timeout*
- Stateless Firewalls
  - Provide basic **packet filtering**
  - Simple matches, unaware of rest of network
    - Source/destination port, source/destination IP
- Stateful Firewalls
  - Provide **dynamic** packet filtering (stateful inspection)
  - More complex matches based on other network connections



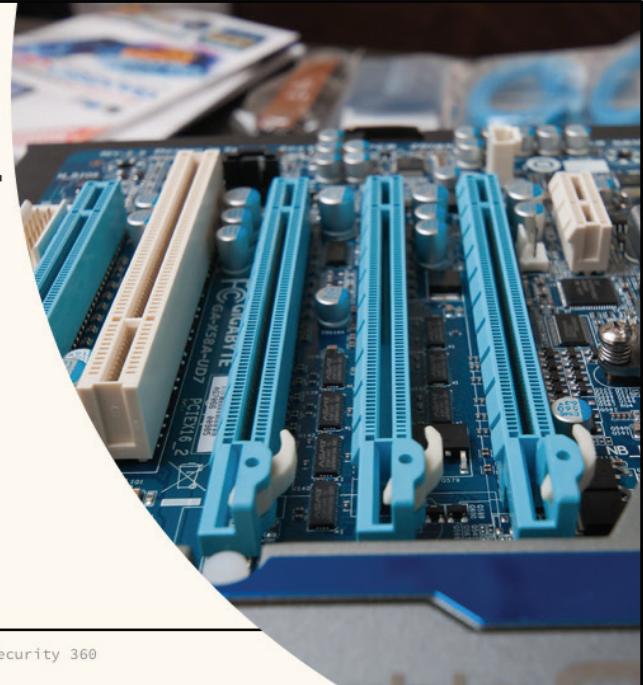
Security 360

["USA map sandshoe"](#) by [RosieConnell](#) is licensed under [CC BY-NC-ND 2.0](#)

# Hard Firewalls

perimeter firewalls

- Buy a Firewall
  - Cisco, Checkpoint
- Build-your-own with pfSense
  - A UNIX distro with firewall & router in one
- Build-your-own with Linux
  - iptables/nftables hook into the Linux kernel



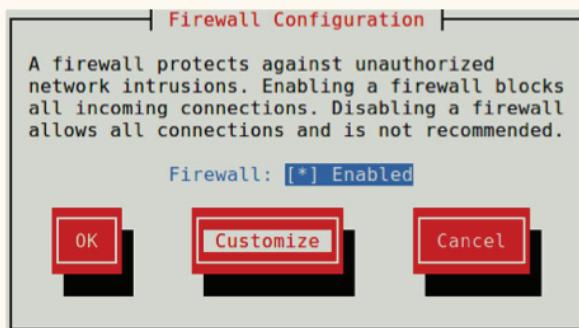
Security 360

*"Motherboard Closeups"* by [bugbbq](#) is licensed under [CC BY-NC 2.0](#)

# Soft Firewalls

soft

- If you're on Linux
  - Use iptables
- If you're on BSD
  - Use pf
- If you're on Windows
  - Use Windows



Security 360

["TUI-based Firewall Configuration"](#) by [xmodulo](#) is licensed under [CC BY 2.0](#)

# Firewall Configuration

An example with iptables

- Three default “chains”
  - INPUT – traffic incoming to host
  - OUTPUT – traffic outgoing from host
  - FORWARD – traffic passing through host
- DROP a ping (ICMP) from a specific IP
  - iptables -A INPUT -p icmp -s 192.168.1.1 -j REJECT
- REJECT outgoing SSH (TCP :22)
  - iptables -A OUTPUT -p tcp --dport 22 -j DROP

A screenshot of a terminal window titled "secker". It displays several lines of iptables command history. The commands shown include: /sbin/iptables -N ipblock, /sbin/iptables -A INPUT -i eth0 -j ipblock, /sbin/iptables -A INPUT -i lo -j ACCEPT, if [ "\$RED\_DEV" != "" ]; then /sbin/iptables -A OUTPUT -o \$RED\_DEV -j DROP; fi, and /sbin/iptables -A FORWARD -j ipblock. The background of the terminal has a dark blue gradient.

**DROP everything first, ACCEPT as needed**

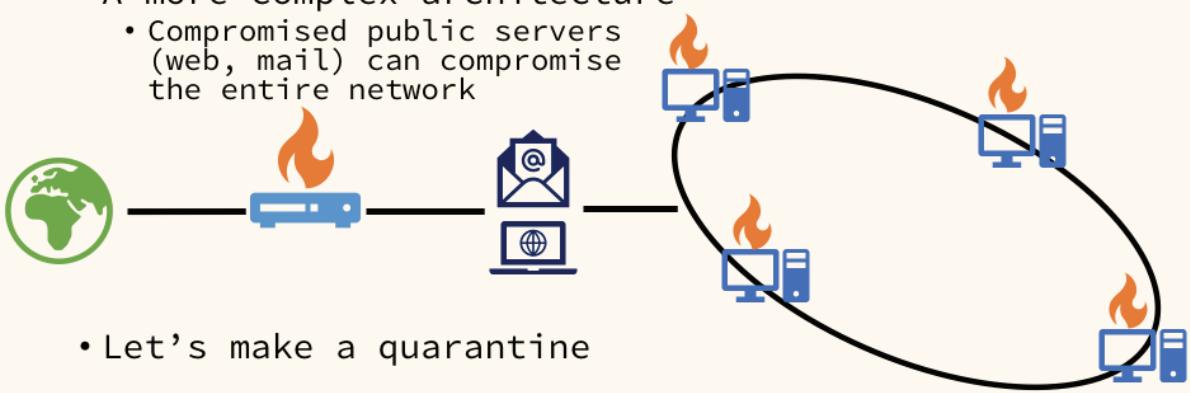
Security 360

["Iptables"](#) by [Jordan W](#) is licensed under [CC BY-NC-SA 2.0](#)

iptables has been superseded by nftables, with an outlook to move to another option  
- bpfilter - in the future

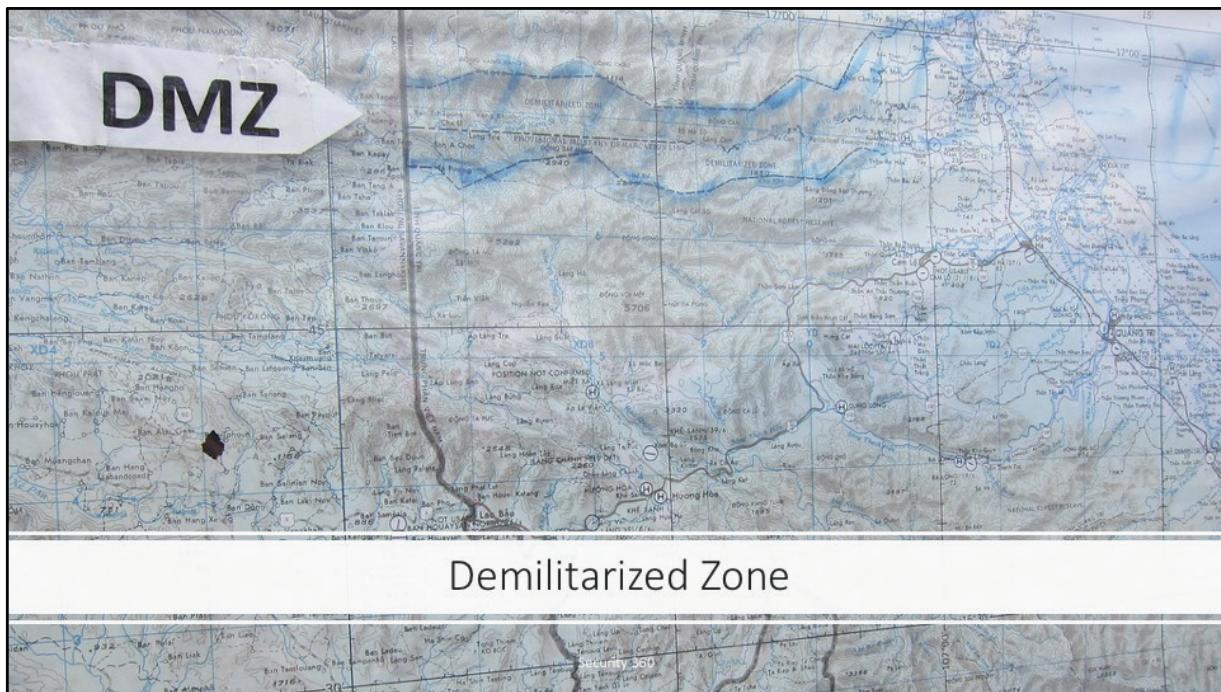
## Securing the Perimeter

- A more complex architecture
- Compromised public servers (web, mail) can compromise the entire network



- Let's make a quarantine

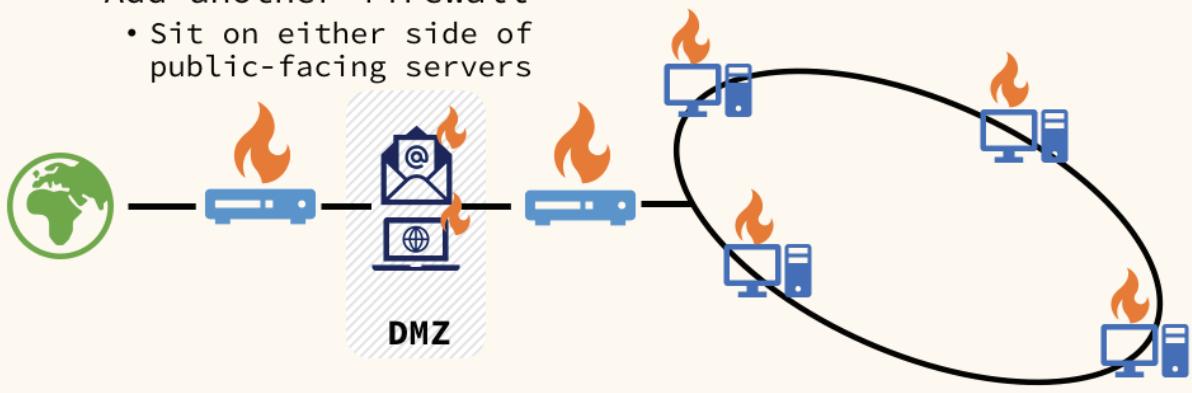
Security 360



"VHPA - DOD Evasion Chart Vietnam DMZ" by [UCFFool](#) is licensed under [CC BY 2.0](#)

## Building the DMZ

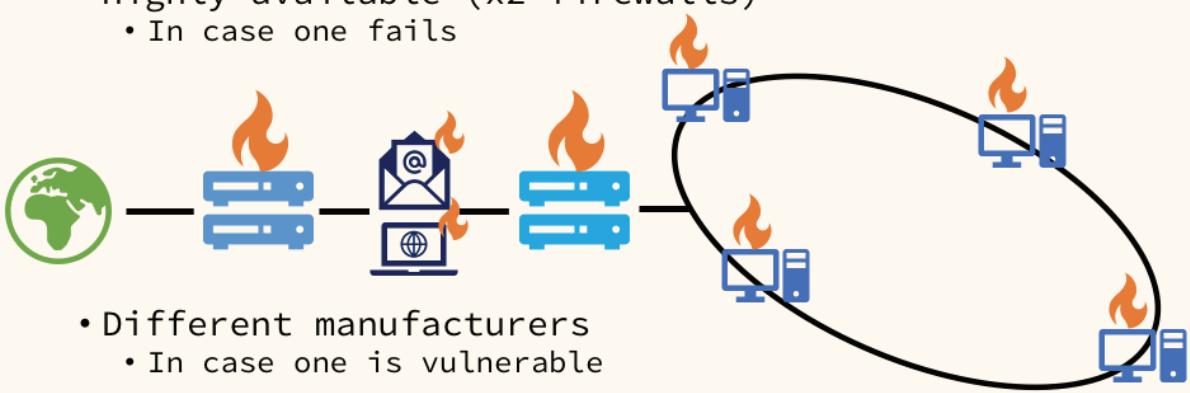
- Add another firewall
  - Sit on either side of public-facing servers



Security 360

## Firewall Best Practice

- Highly available (x2 firewalls)
  - In case one fails



- Different manufacturers
  - In case one is vulnerable

Security 360

## L3 vs L7 Firewalls

- L3/L4 Firewalls (Network Firewall)
  - What we've described so far
  - Packet-filter based on IP & Port
- L7 Firewalls (Application Firewall)
  - Group traffic into applications
    - Web browsing
    - Mail
    - Telnet
    - SSH
  - Filter based on groups



Security 360

*"elevator buttons"* by [jaded one](#) is licensed under [CC BY-NC-ND 2.0](#)

# Intrusion Detection Systems

---

- Traditional Network Firewalls
  - Shallow packet inspection – decisions made based on headers (IP & TCP)
    - Allowed - or not
- IDS
  - Packet sniffer which can raise alerts/alarms
  - Alerting on top of shallow packet inspection, and...
  - Deep packet inspection – decisions made based on the payload

---

Security 360

# Intrusion Prevention Systems

---

- IPS
    - An IDS which also works “inline”
    - Can make port filtering decisions based on the alerts generated and drop/reject packets on-the-fly
  - Open Source tools
    - Snort
    - Suricata
- 



Security 360

["Piggy Bank"](#) by [MaeDae](#) is licensed under [CC BY-NC-SA 2.0](#)

## Next-Generation Firewalls

- AKA UTM Systems
  - Unified Threat Management
- Palo Alto, Fortinet, Cisco
- Built-in
  - Intrusion Detection System
  - Intrusion Prevention System
  - L7 Application
  - Virus/Malware Scanning

Security 360



["P1060988"](#) by [NTHORPE](#) is licensed under [CC BY 2.0](#)