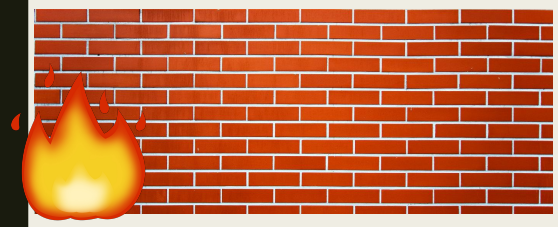
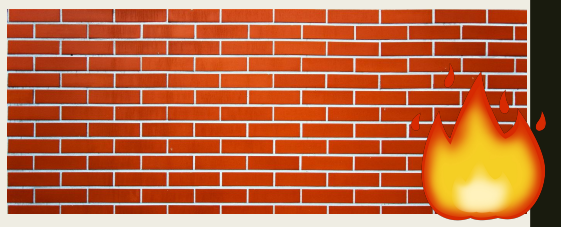


# FIRE|WALLS



Ohad Katz

# Overview

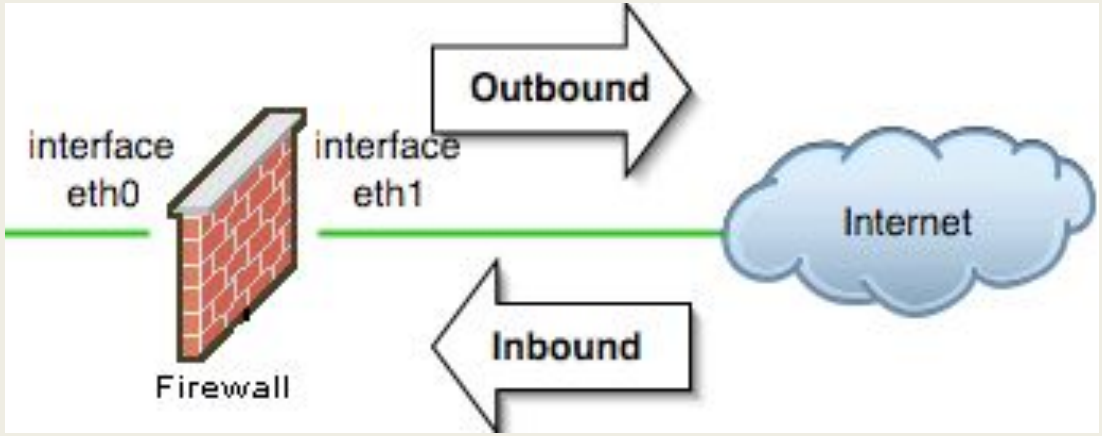
- What are Firewalls
- Why we need them
- Types of Firewalls (Categories)
- Implementation
- Best practices

# What are Firewalls?


- Network Security Device/Software
- Monitors Incoming and Outgoing traffic, decides what comes in and what goes out.

# What Do They Do?

- Essentially one GIANT filter for your network/computers

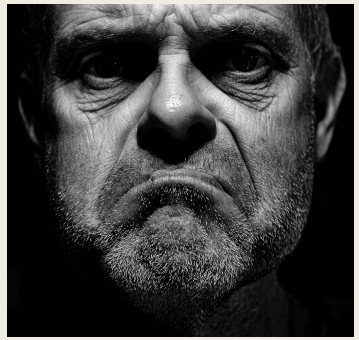



- Prevent unauthorized Internet users from accessing private networks connected to the Internet
- Protects confidential information
- First line of defense

# What Happens Without One?

- Fires Start

- People get **very** unhappy



- Things go missing

- Unauthorized people get in

# Most Companies Today

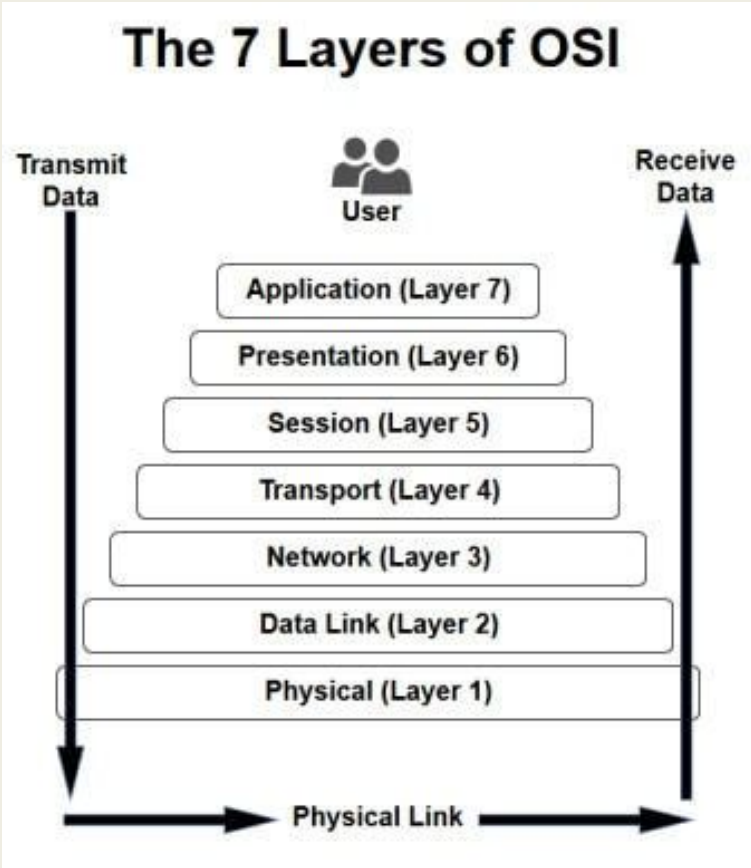
- “50% of administrators audit their firewalls once a year, and about 10% never do it”
  - *Richard Broeke (sales manager at Securicom)*

# History of Firewalls

- 1980s - Firewalls emerge
- 1990s - First Security Firewall ( IP routers with filtering )
- 1992 - First Commercial Firewall - DEC SEAL
- 2009 -Next Gen Firewall defined

# History of Firewalls

- First Generation:
  - *Packet Filters*
    - inspecting individual packets that come into the network
- Second Gen
  - *Stateful Filters*
    - More layers, wait until they get more information
    - Issues?  Overhead
- Third Gen (Next Gen)
  - *Application Layer*
    - Understand Service Context
    - Protects Applications(Go figure!)

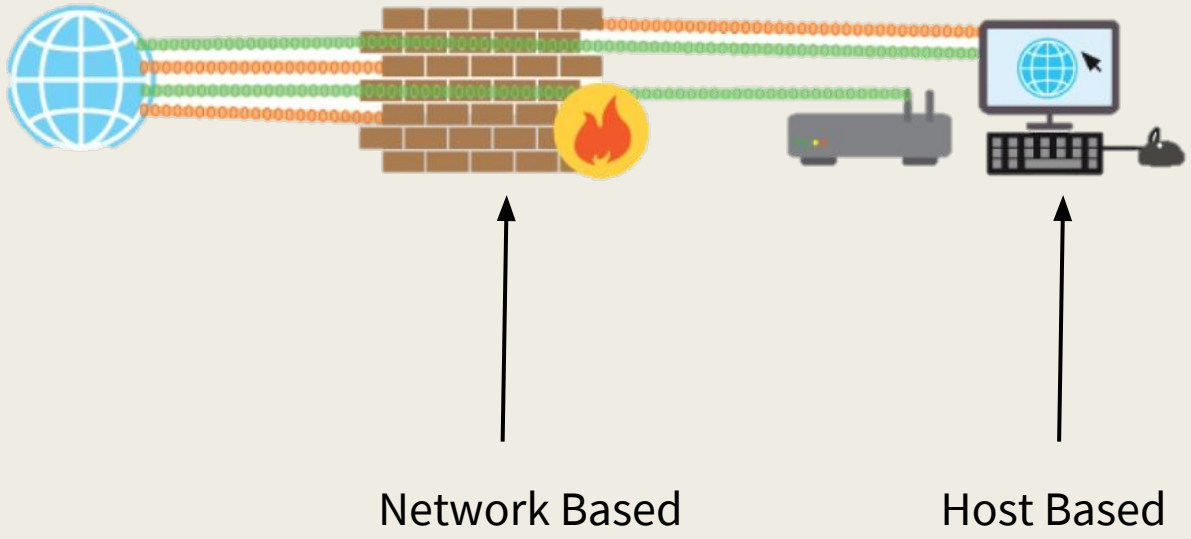


# Types of Firewalls

- Stateful vs Stateless
- Network Based  vs Host Based
- Virtual Firewall
- Packet Filters
- Application Layer
  - *Proxy Firewalls*
  - *Deep Packet Inspection*

# Network Based Firewalls
# vs
# Host Based Firewalls

- Host Based Firewall
  - *Installed on **each*** machine
    - EX: Windows Firewalls
- Network Based Firewalls
  - *Built into the infrastructure*
    - EX: pfSense



# Stateful vs Stateless Firewalls

## STATEFUL

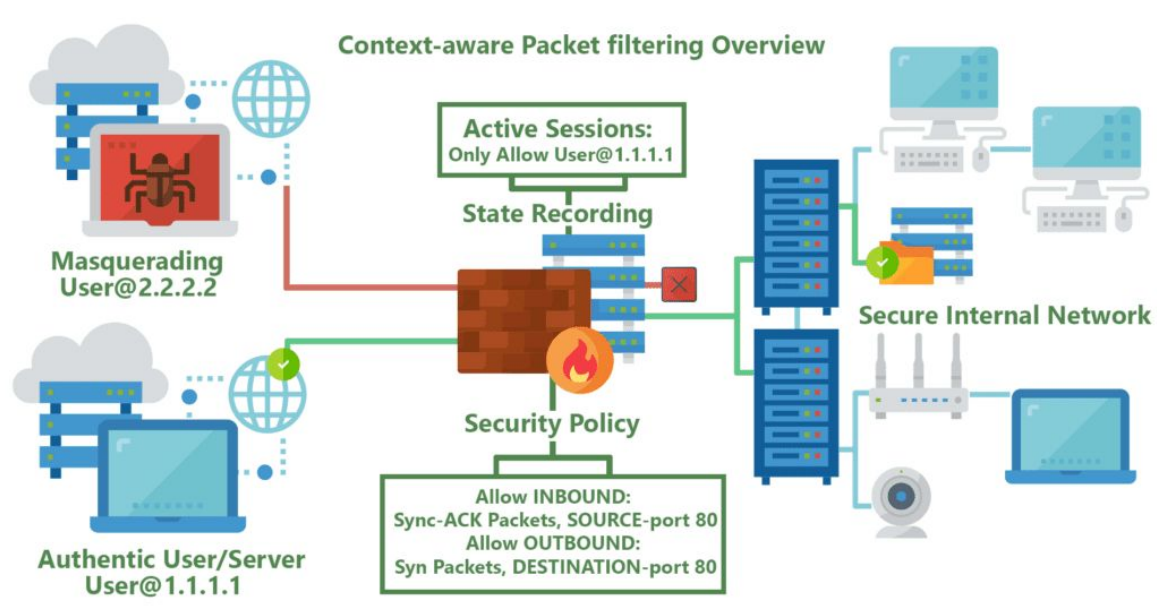
- Keeps track of data
- Watches from end to end
- Can identify forged communications

## STATELESS

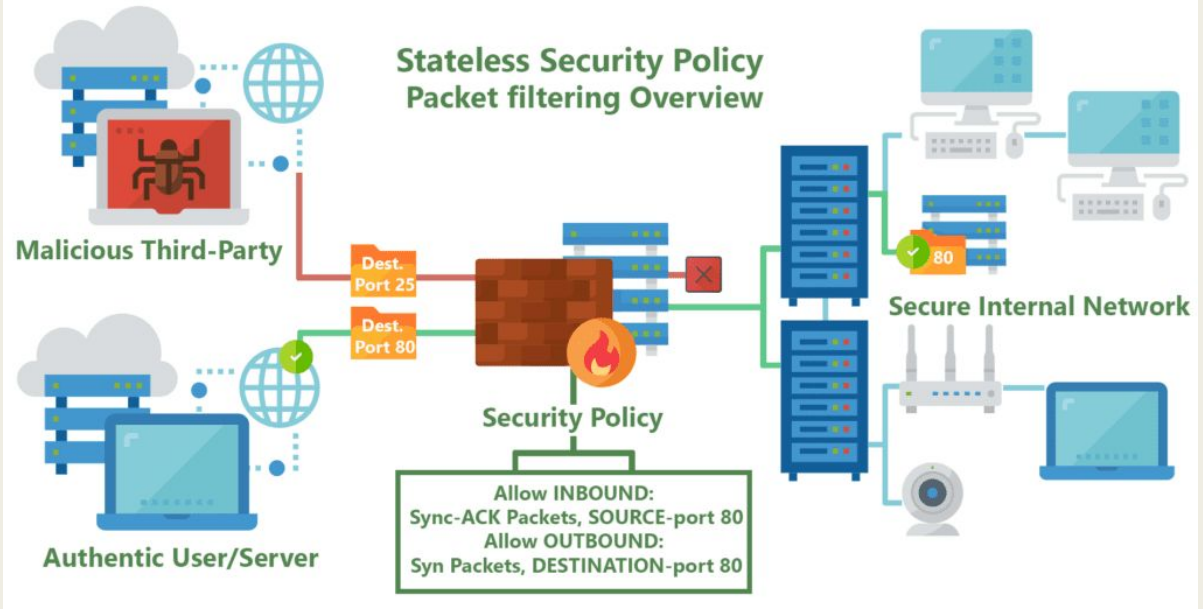
- Used for Packet Filtering
- Super Fast
- Works under heavy loads
- Monitor based on data presented to it

# Stateful vs Stateless Firewalls

## STATEFUL




## STATELESS



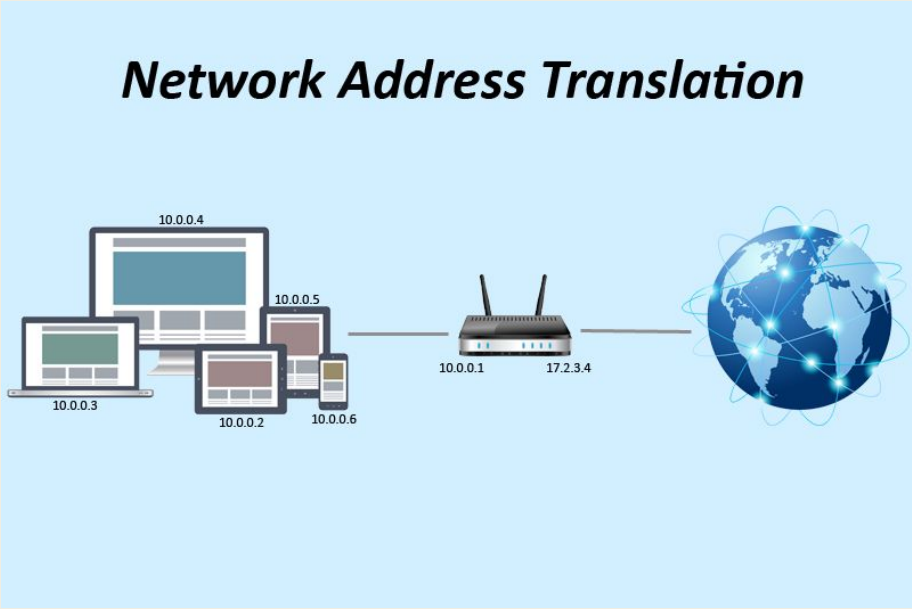
# Stateful vs Stateless Firewalls

**STATEFUL** **STATELESS**

Which is better?

# NAT + Firewall = A Match Made in Heaven?

- NAT used to limit # of public IP Addresses on a Network
- One IP = Many Computers or One Public IP = One Private
  - *Using The Internet? Same Public IP*
- Controls Public Access to Machines
  - *Only Can Get in through 1 public IP*
  - *People don't log into your internal web server IP right?*



# Scenario: Linux

# Linux 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
```

Want something a little more… Dynamic?

```
iptables -A INPUT -p tcp --state state NEW,ESTABLISHED,RELATED -j ACCEPT
```

Issue? Deleted after reboot

# But what if you want persistent iptables?

**Ubuntu(Debian)**

```
iptables-save >
```

/etc/iptables/rules.v4

/sbin/iptables-save

**Centos(Redhat)**

```
service iptables save
```

/etc/sysconfig/iptables

# Linux Commands (ipTables)

- -A: Append one or more rules
- -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 (Show all!)
- Want More? **man iptables**

Want something a little less...complicated?

# UFW (Uncomplicated Firewall)

- Much simpler rules than iptables
  - *Still uses iptables! Just is an interface for them*

**sudo ufw allow**

**sudo ufw deny**

**sudo ufw status**

**sudo ufw delete**

https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-18-04

# Now Pair Up!

**Make sure that pfSense allows SSH or just shut off firewalls temporarily ( pfctl -d )**

## Team A

- Linux Box 1
- Block Team B with ipTables
  - *Hint (ps aux, grep)*

## Team B

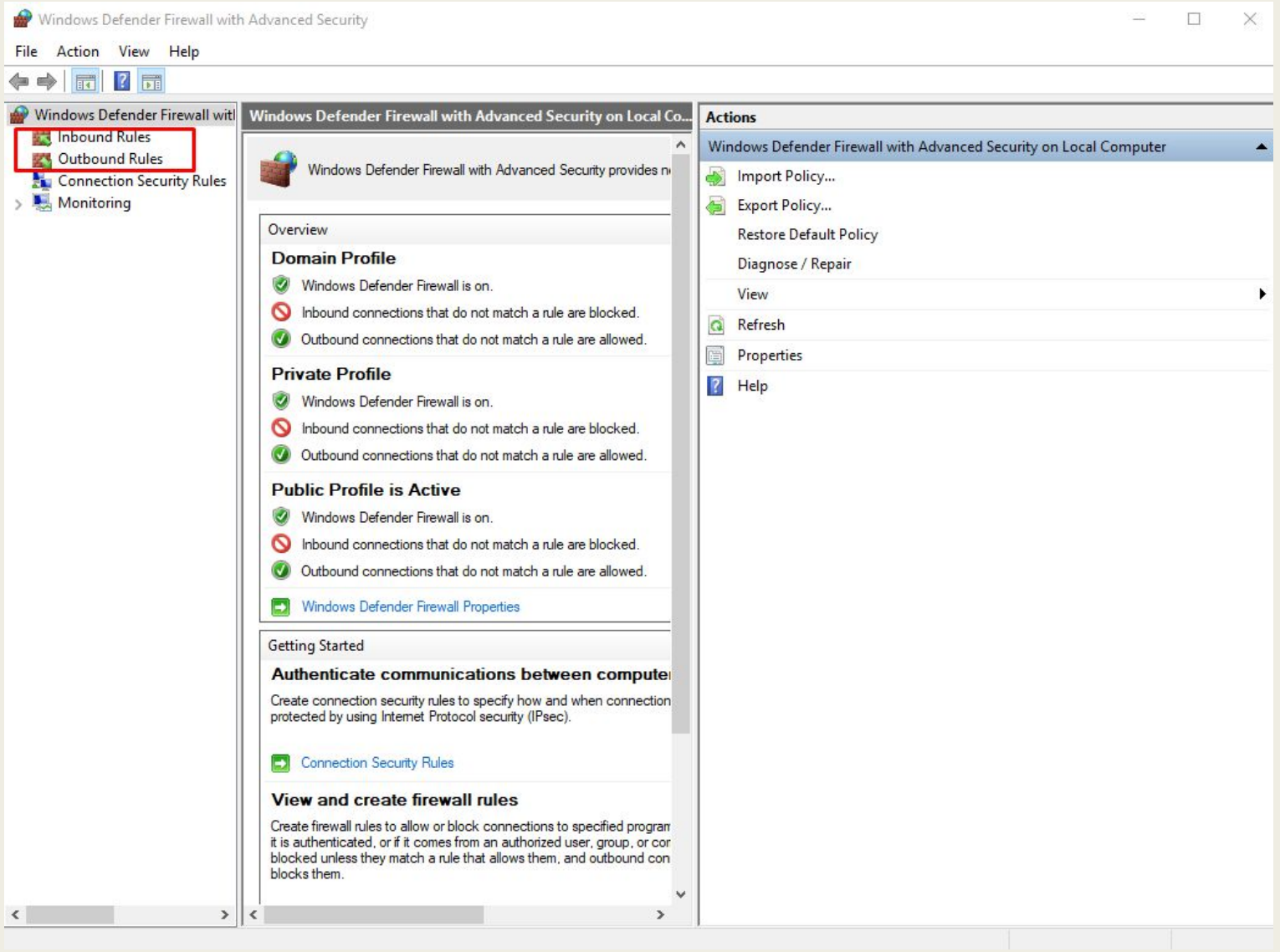
- Linux Box 2
- SSH Into Team A
- What Happens when Team A blocks you? Can you get back in? Is there a backdoor?

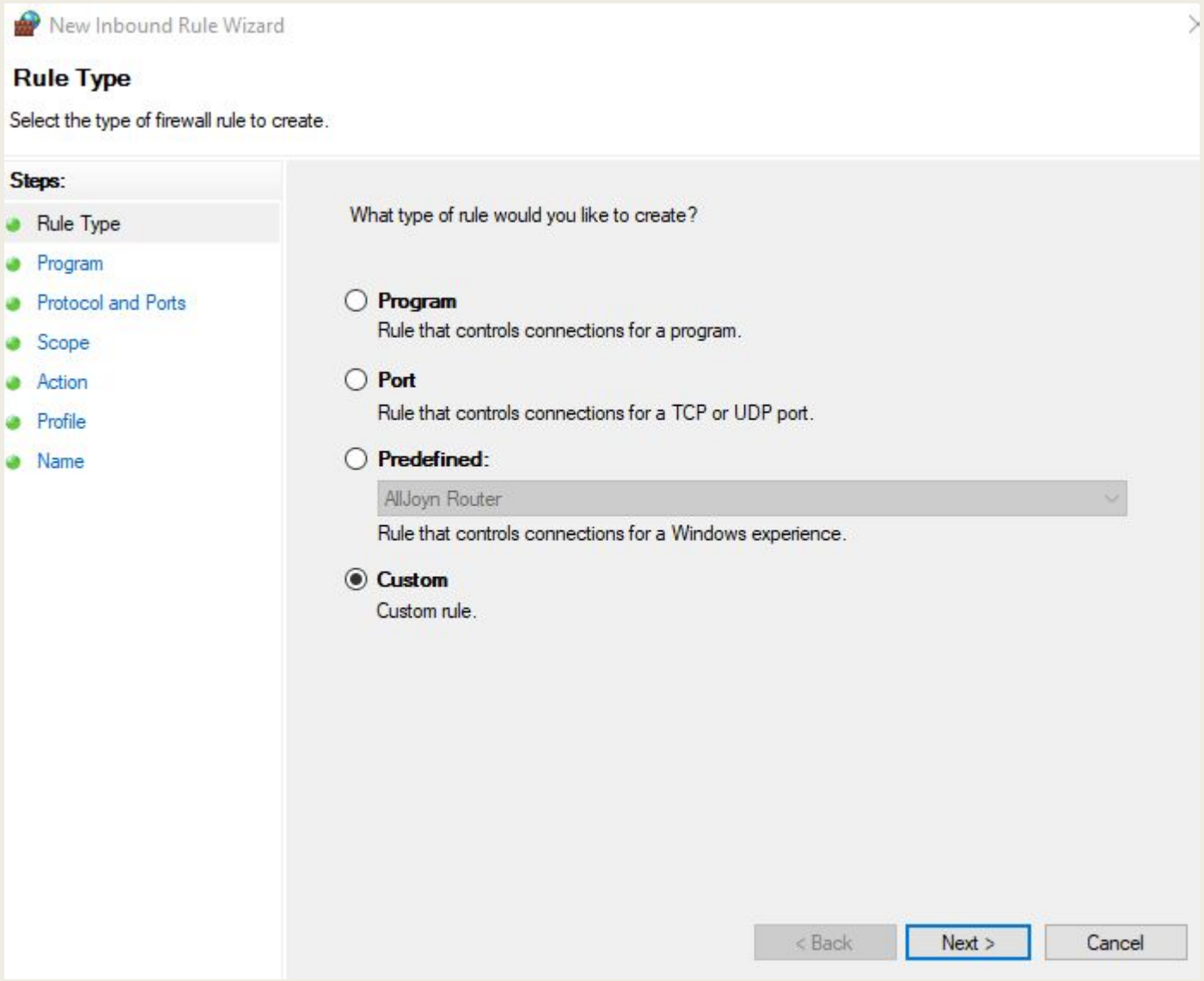
Now Switch!

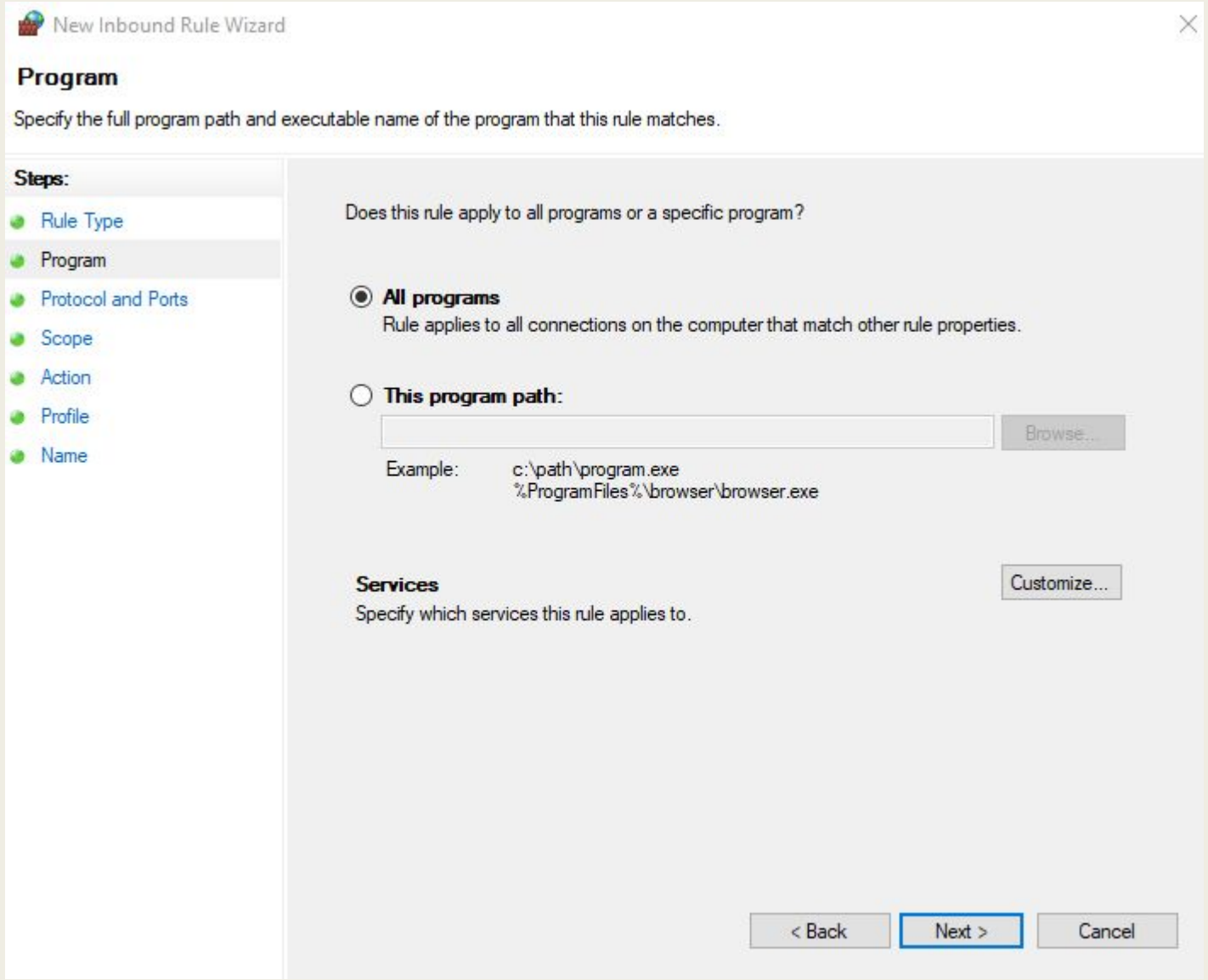
# Scenario: Windows

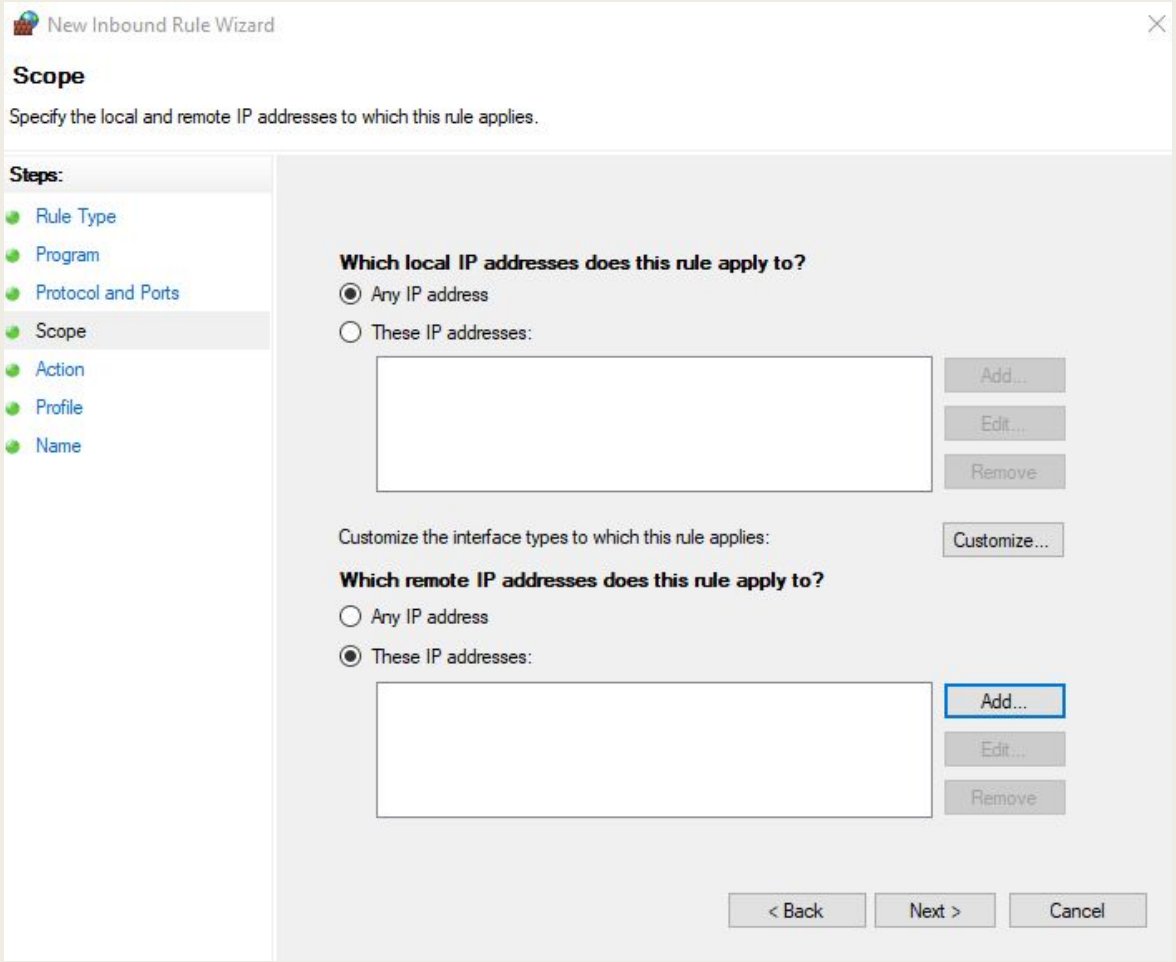
# Windows Firewalls

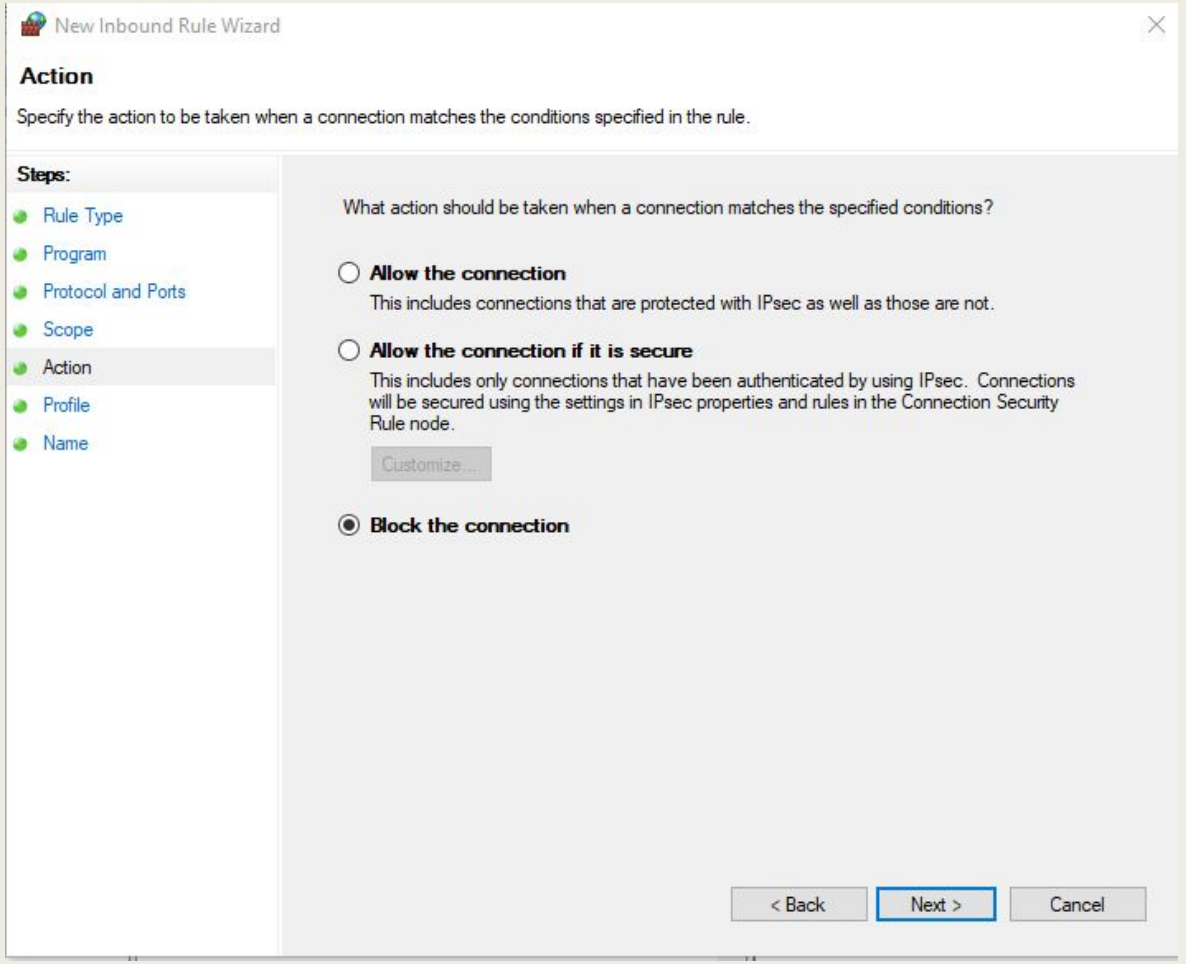

# Windows Firewall(GUI)




New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
Cancel


New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel

# Windows (CMD)

Block an incoming IP:

```
netsh advfirewall firewall add rule name="NAME" dir=in action=block remoteip=198.168.1.1/24
```

Block an outgoing ip:

```
netsh advfirewall firewall add rule name="NAME" dir=out action=block remoteip=198.168.1.1/24
```

Block an incoming port:

```
netsh advfirewall firewall add rule name="NAME" dir=in action=block protocol=TCP localport=80
```

# Windows Firewall (CMD)

```
netsh advfirewall set *
```

```
netsh advfirewall firewall add rule name="NAME" dir=in action=allow protocol=TCP localport=80
```

```
netsh advfirewall firewall add rule name="NAME" dir=out action=allow protocol=TCP localport=80
```

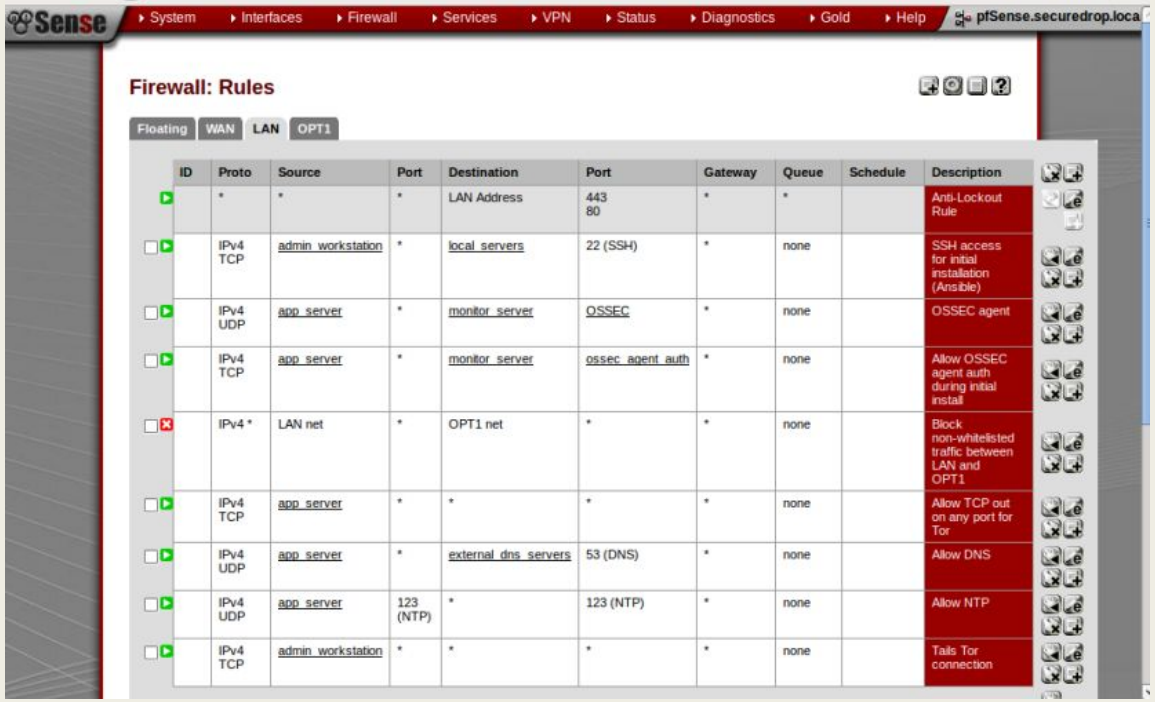
```
netsh advfirewall set currentprofile firewallpolicy
```

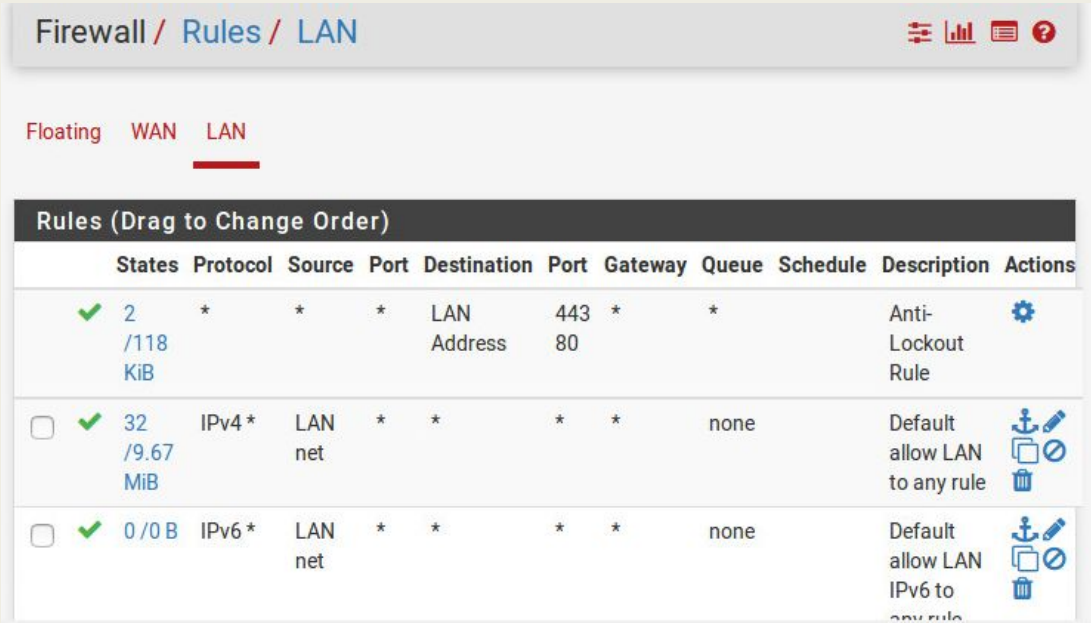
```
netsh advfirewall set publicprofile state on/off
```

```
netsh advfirewall set privateprofile state on/off
```

# Scenario: pfSense

# pfSense


Sense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
pfSense.securedrop.loca
Firewall: Rules
Floating
WAN
LAN
OPT1
ID
Proto
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
* * * LAN Address 443 80 * * Anti-Lockout Rule
IPv4 TCP admin_workstation * local_servers 22 (SSH) * none SSH access for initial installation (Ansible)
IPv4 UDP app_server * monitor_server OSSEC * none OSSEC agent
IPv4 TCP app_server * monitor_server ossec_agent_auth * none Allow OSSEC agent auth during initial install
IPv4 * LAN net * OPT1 net * * none Block non-whitelisted traffic between LAN and OPT1
IPv4 TCP app_server * * * * none Allow TCP out on any port for Tor
IPv4 UDP app_server * external_dns_servers 53 (DNS) * none Allow DNS
IPv4 UDP app_server 123 (NTP) * 123 (NTP) * none Allow NTP
IPv4 TCP admin_workstation * * * * none Tails Tor connection


Firewall / Rules / LAN
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
2 /118 KiB * * * LAN Address 443 80 * * Anti-Lockout Rule
32 /9.67 MiB IPv4 * LAN net * * * * none Default allow LAN to any rule
0 /0 B IPv6 * LAN net * * * * none Default allow LAN IPv6 to

# pfSense CLI

Blocking general IP:

```
easyrule block wan 10.42.x.xxx
```

Pass with Port:

```
easyrule pass wan tcp 10.42.x.xxx 192.168.0.4 80
```

Pass without port:

```
easyrule pass wan icmp 10.42.x.xxx 192.168.0.4
```

pfSense
when in doubt? pfctl -d :)

# Other Firewall Makers

- Check Point
- Symantec
- Cisco
- Juniper
- And...

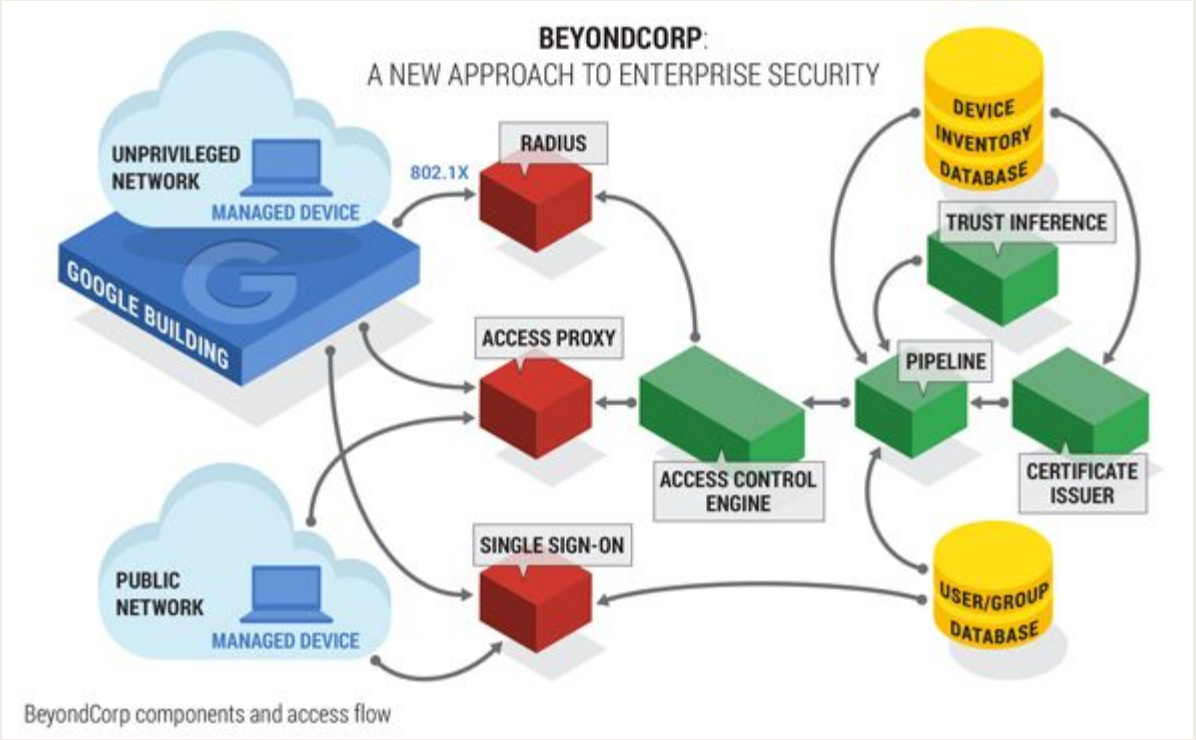
# Palo Alto

# Best Practices ( hint hint 😉 )

- Drop **ALL** connections
  - *Implicit Deny (USUALLY)*
  - *Block Services not in Use!*
- Add back only as much as you need
- Add back connections as needed
  - *Order Matters!!!!*
- watch --interval=5 ‘iptables -nvL | grep -v “0 0”
  - *MONITOR YOUR IPTABLES*
- Read ps aux from top to bottom (Processes)
- Firewalls are not your last resort!

# Where Do We Go From Here?

- Zero Trust Architecture ,
  - *“Never Trust , Always Verify”*
  - *Beyondcorp, Palo Alto, etc.*
- Defense In Depth
  - *Layer Up!*
- Next Gen Firewalls! (Palo Alto)
  - *Smarter, More Accurate*
  - *Easy, Breezy, Beautiful*



BeyondCorp components and access flow

# Now you think you know Firewalls?

- How can you improve your security?
- How can you protect yourself?
- Are Firewalls Omnipotent?
  - *What can't they do?*
  - *What Else Do You Need?*
- Do we *need* firewalls?

# Any Questions?