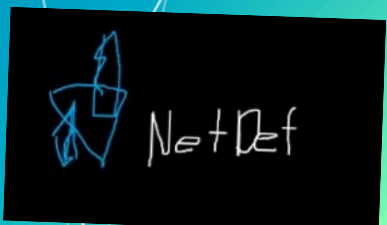
Next Generational Firewalls

UBNetDef, Spring 2023
Week 9
Lead Presenter: Ethan Viapiano



Learning Objectives - Week 9

- Understand how Next Generation firewalls direct traffic.
- Explore Zero Trust and how it can be used.
- Review the Cyber Kill Chain and how Next Generation firewalls can break the chain.
- Hands on security policy rules in Palo Alto.

Agenda - Week 9

- Review Firewalls and the OSI model
- Next Generation Firewall Features
- Zero Trust
- Cyber Kill Chain Review
- Interfaces and Zones
- Palo Alto Security Policy

Quick Review

- Firewall Rules
- OSI Model Review
- Network Traffic and Interfaces
- Service Ports and Firewalls

In Class Activity

What really are ports?

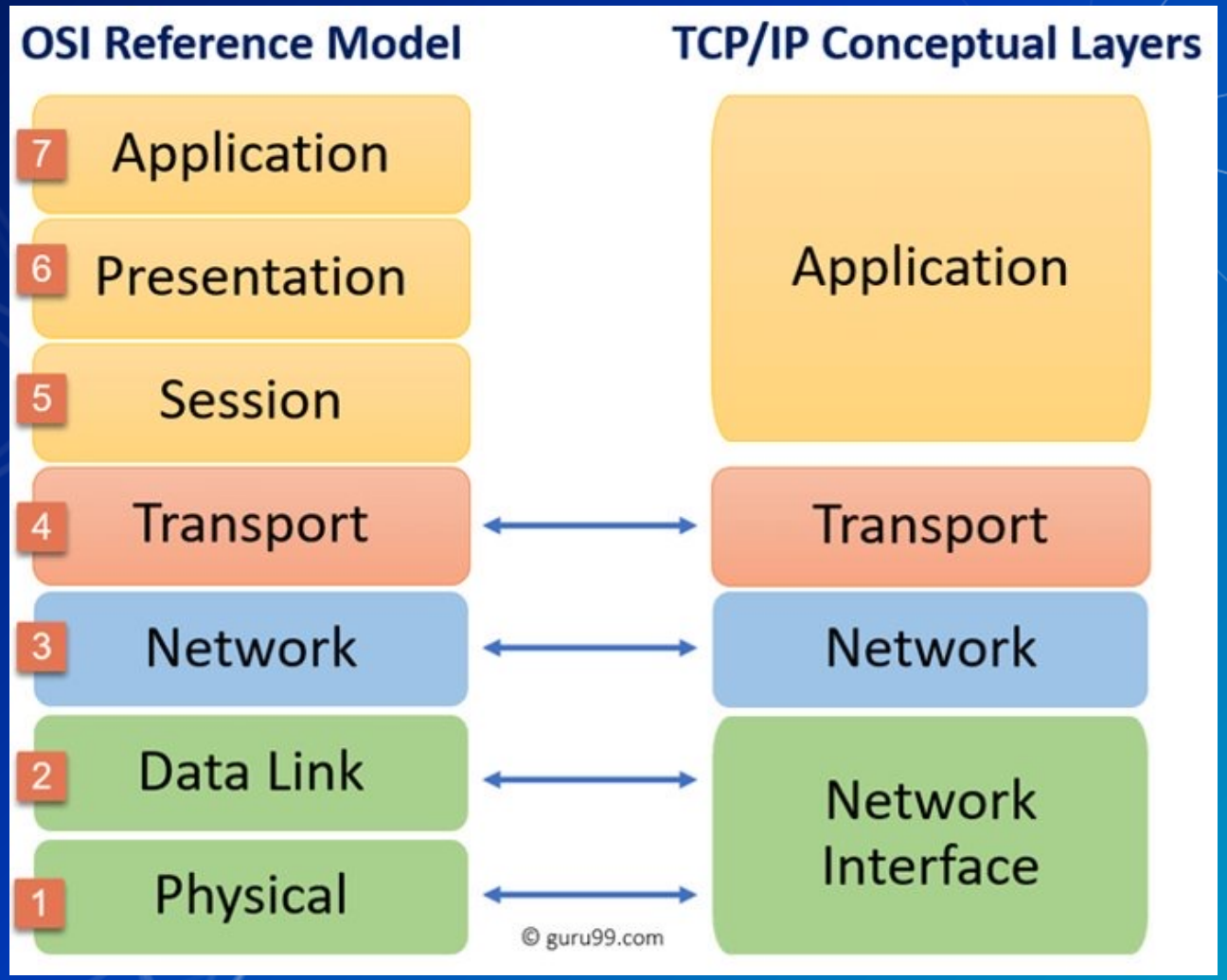
Connect to my website!

- http://192.168.15.135
- Why didn't it work?
- http://192.168.15.135:8080
- Why didn't it work?
- How do we fix it without dropping the firewall rules?

What makes the Firewall "Next-Gen"?

- The actual features and functionality that the firewall is capable of (or just the buzzword)

	Classic Firewall	Next Generation Firewall
Filter network traffic using port, IP, and protocol	Supported	Supported
NAT	Support	Supported
Deep Packet Inspection	:(	Supported
Intrusion Detection System (IDS) Intrusion Prevention System (IPS)	:(	Supported
LDAP and Active Directory Intergration	:(	Supported
OSI model layers covered	2-4	2-7
And much much more	Lv. 1 Crook	Lv. 100 Mafia Boss


OSI Reference Model
TCP/IP Conceptual Layers
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Application
Transport
Network
Network Interface
© guru99.com

Some popular Next Generation Firewalls:

What's it take to manage a next gen firewall?

- Technical?
- Skillset?
- Governance?

So, what can a next gen firewall do?

- IPS/IDS
- Url Web filtering
- Live threat feeds
- DNS resolution interception
- Detonation of potentially malicious files (Wildfire)
- Web application deep inspection
  - SSL decryption/re-encryption (offloading)
- Live threat maps specific to organization
- Analytics/Dashboarding

DNS Resolution Interception

- Allow or intercept DNS queries.
- If a DNS request is for a domain that is on the Allow list the request goes through like normal.
- If a DNS request is for a domain that is on the Intercept list (blocked) the firewall can prevent that request from completing.

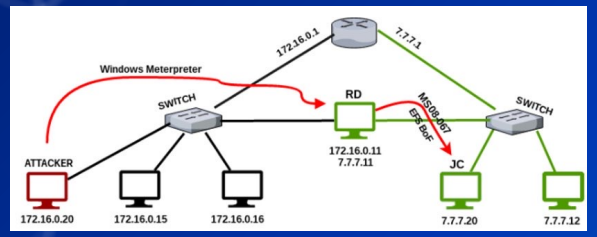
Deep Packet Inspection

- Deep packet inspection –important aspects such as it being port agnostic
  - Recall the activity earlier
- SSL and SSH decryption to allow this
  - Anyone remember what uses SSL?

Live threat maps specific to organization (Can anyone guess what organization?)

What Zero Trust Architecture Accomplishes?

- Reduces the likelihood of accidental breaches (Worker picks up a hard drive in the parking lot)
- Reduces the likelihood of insider attack
- Reduces the likelihood of successful pivoting
- Ensures that east-west traffic is monitored
- Where have we implemented Zero Trust in this class?
- Where is trust necessary in our current architecture

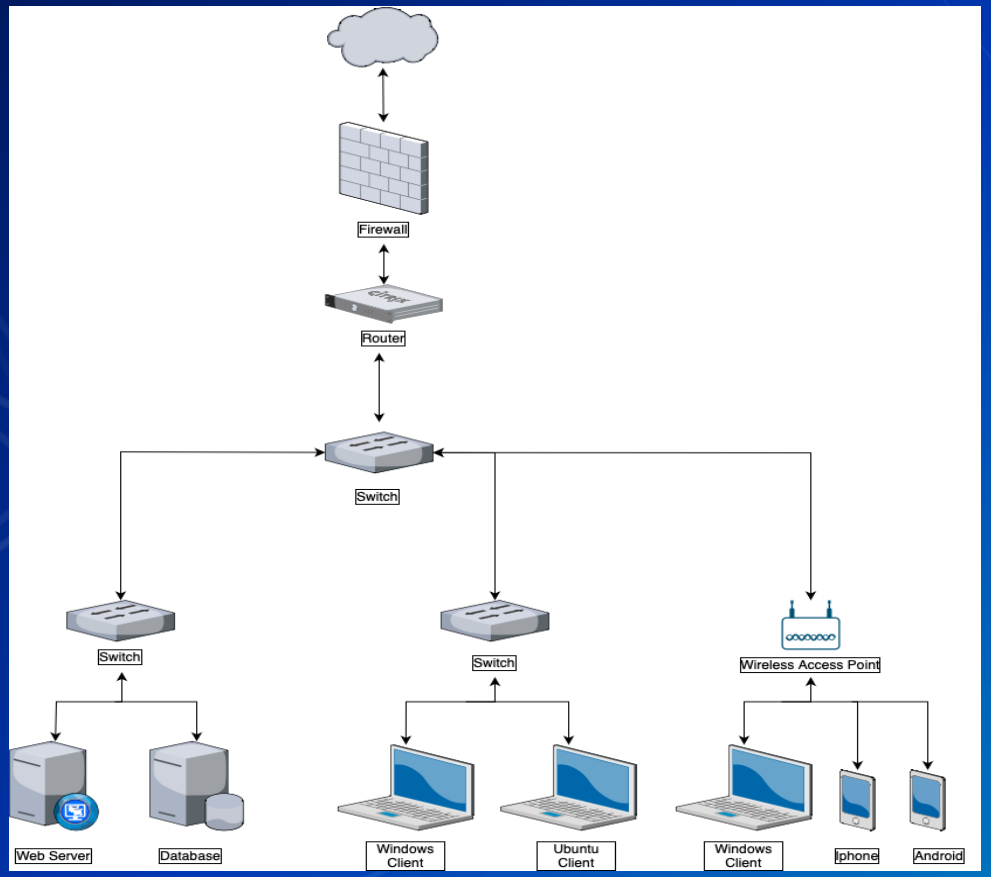


Intra and inter network traffic

- Intra network traffic is traffic within a zone (Win10Client connecting to IISServer)
- Inter network traffic is traffic moving between zones (OutsideDevice connecting to IISServer)

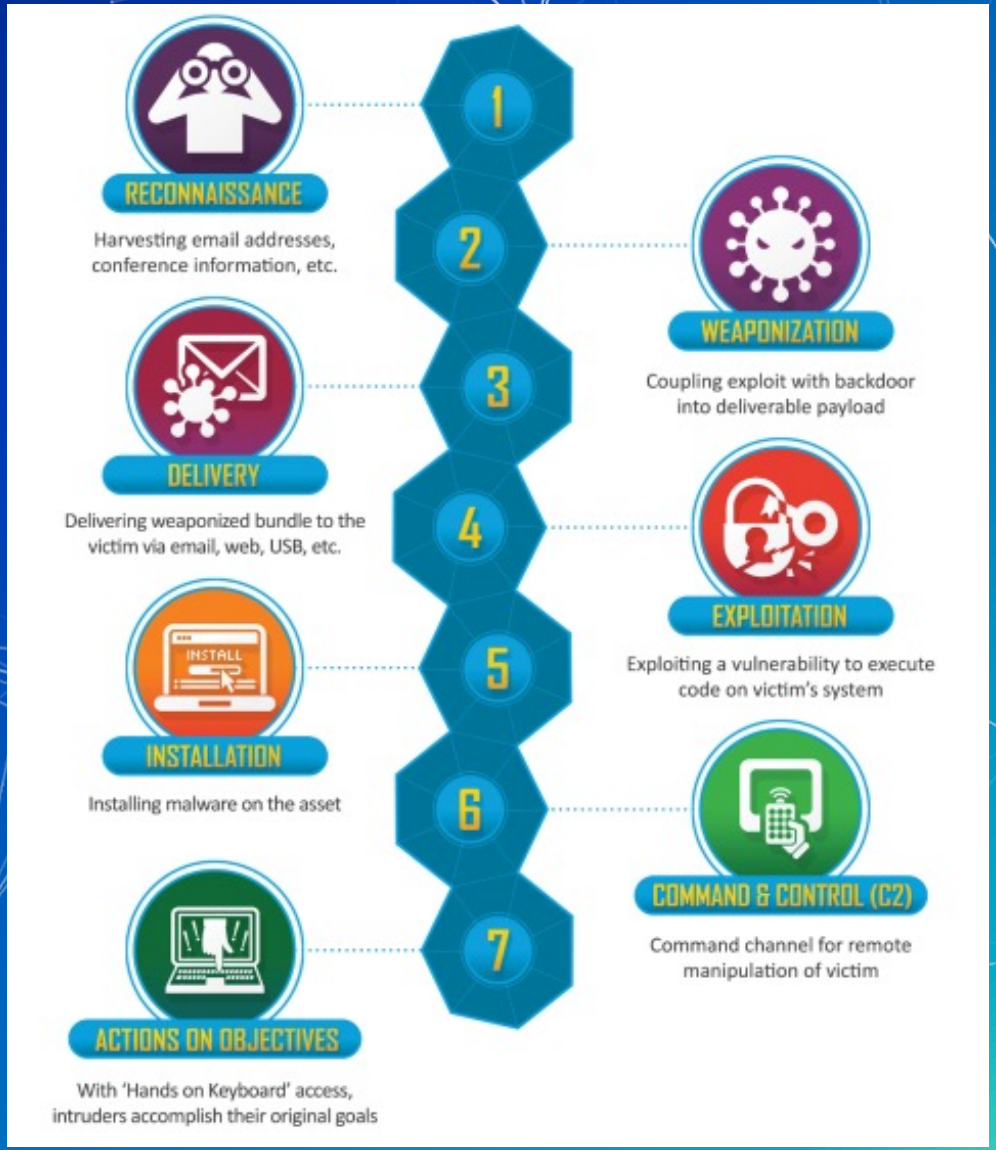
What is wrong on this image?

North-South Traffic



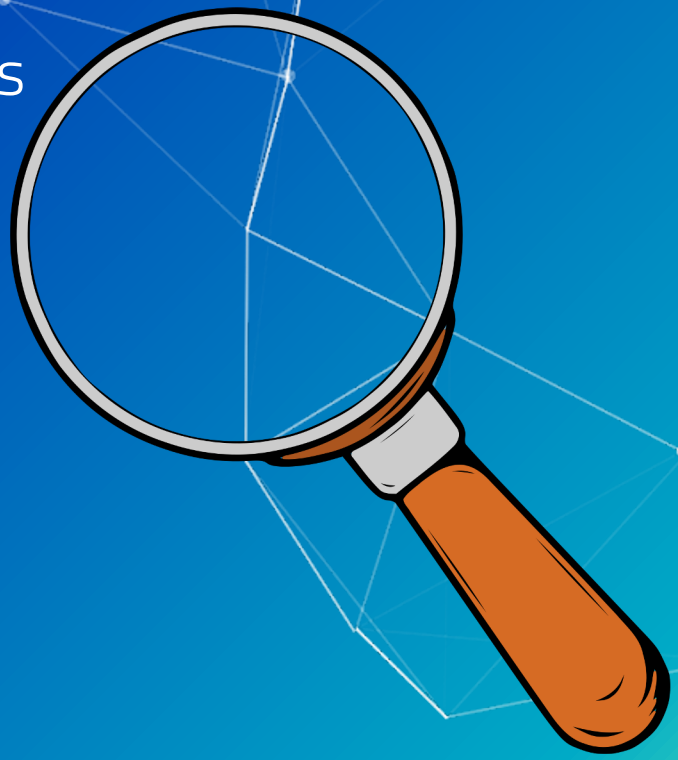
East-West Traffic

What is the Cyber Kill Chain



Reconnaissance

Gathering information, email lists, hardware information, and software versions. Reconnaissance can also be network scans to detect open ports and services.



Weaponization

Creating a payload to deliver to a system. Making a script that runs when a PDF is open or a website that downloads a malicious file.

Delivery

You have (3) New Emails!

Delivery can be done through USB Hotplugs, Emails or Downloads on websites.

Exploitation

Use the vulnerability discovered in Reconnaissance, packaged in Weaponization and delivered in Delivery. Are we noticing a pattern?

Installation

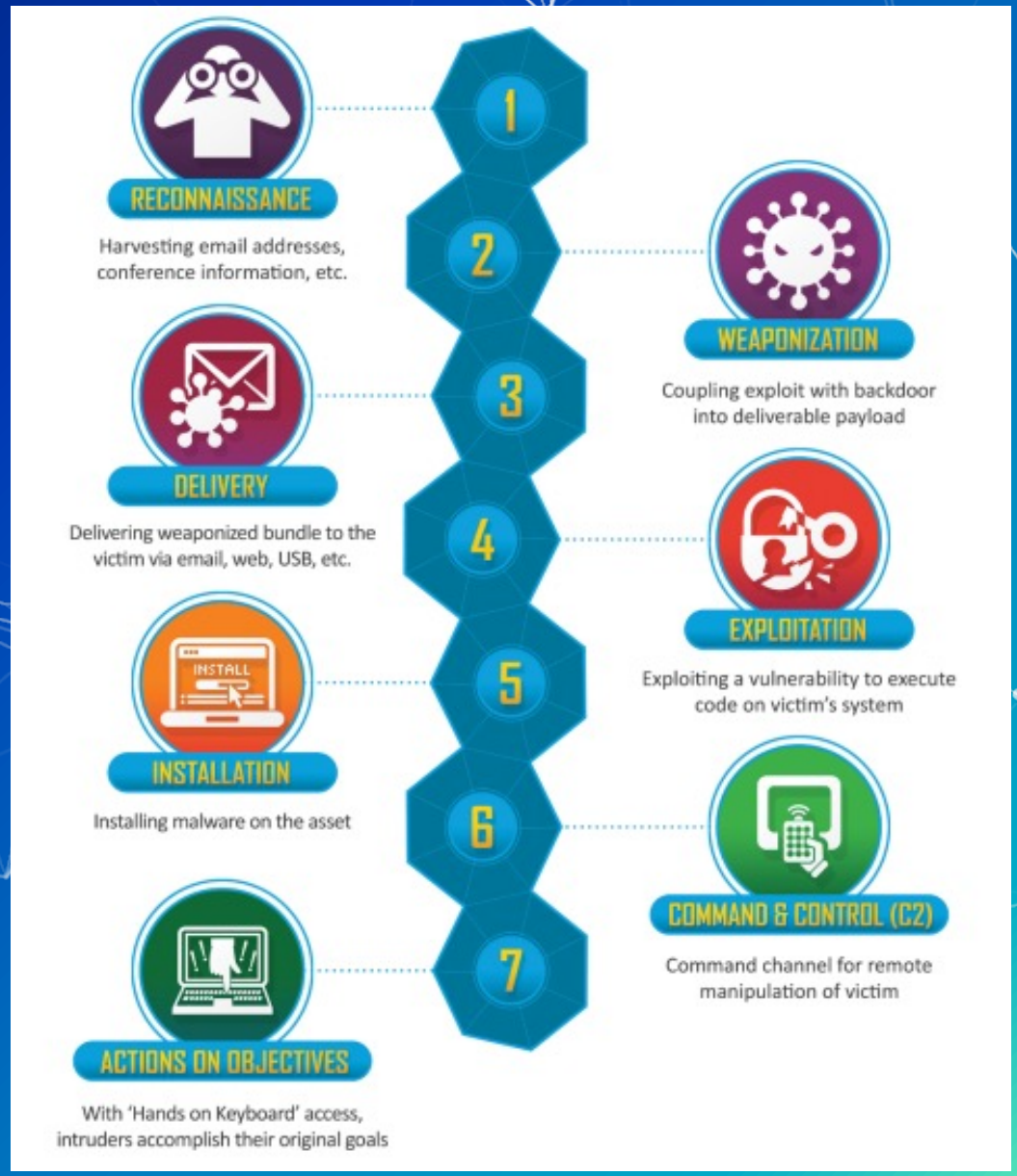
Installing malware, a backdoor, a reverse shell, or an agent.

Command and Control (C2)

The intruder now has access to the victims system, this is known as “hands on keyboard” access.

Cyber Kill Chain

At what stages could a next generation firewall be useful?



Break slide

Please return in 10 minutes

What are zones and interfaces?

- This will all be *very easy* to understand
- Zones are a logical group of traffic on a network
  - Examples of zones:
    - Adminnet, Servernet, External
  - Zones can have multiple interfaces within them

- Interfaces are physical (or virtual) ports that machines plug into

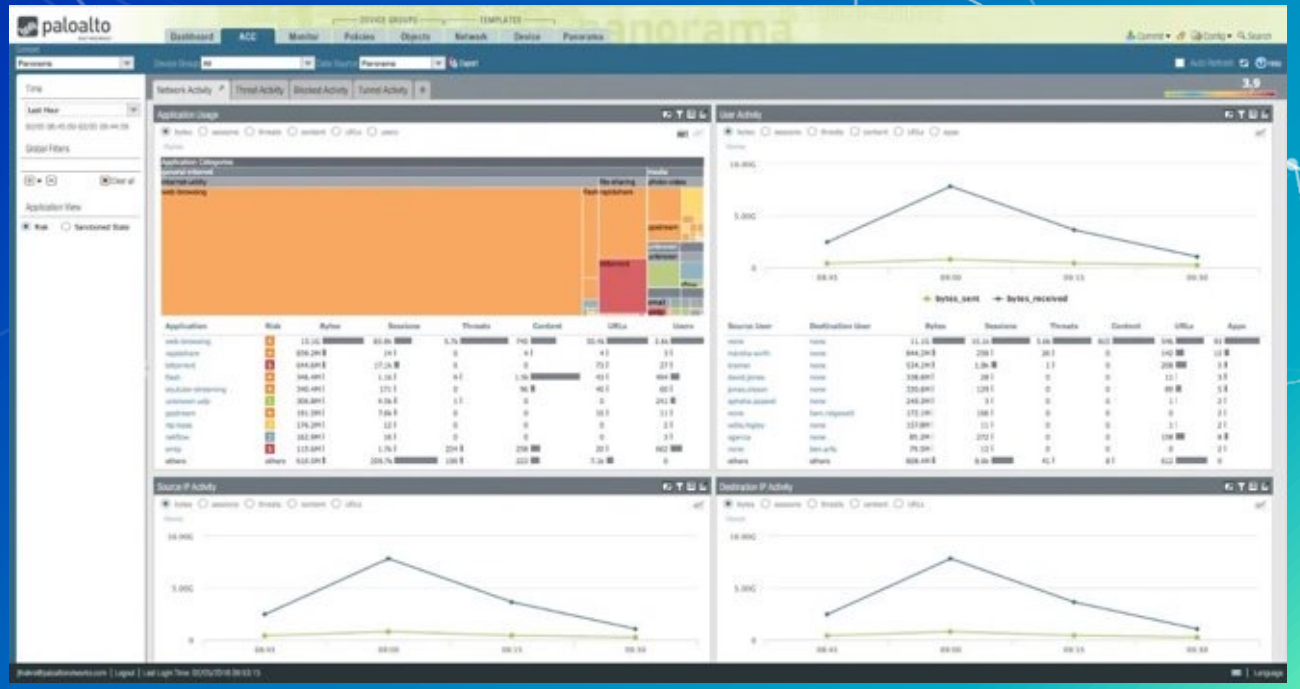
Logs

- What can be learned from logs?
- What have we logged with pfSense?
- What can Palo log?
  - What are the negatives of network logs?

Application Control Center (ACC) & Palo Panorama

- ACC is an interface that provides you with a nice overview of the network activity.
- Palo Panorama helps manage multiple PaloAlto firewalls

Application	Risk	Bytes	Sess...	Thre...	Cont...	URLs	User
google-base	4	21.2M	17	0	0	0	1
ssl	4	8.6M	62	0	0	0	1
web-browsing	4	57.0k	5	0	0	0	1
dns	4	32.5k	92	0	0	0	1
ntp	2	20.6k	229	0	0	0	1
netbios-ns	2	2.9k	3	0	0	0	2
insufficient-data	1	2.4k	10	0	0	0	2
ping	2	392	2	0	0	0	1



In Class Activity

Security Policy

Candidate Config and Running Config

All the changes you make are saved to the **Candidate Config**. The Candidate Config doesn't enforce the rules you save into it. In order to do that you will need to promote the candidate config to **running config**.

Commit Commit Commit

If unsure what exactly you are commiting, see the difference between Candidate Config and Running Config.

Services = Classical Firewall Rule
App-ID = Next Gen Firewall rule

ssh 192.168.13.174

ssh bandit0@bandit.labs.overthewire.org -p 2220

http://192.168.13.91

http://192.168.8.250:8000/

How would we only allow google, and nothing else?

Use App-ID google-base

Security Policy Rules

- By default, Palo Alto allows *intrazone* (traffic within the same zone). However, it also blocks *interzone* traffic (traffic between different zones).
- How can these be more effective than the rules we've used in pfSense? (Hint: Remember the activity at the beginning of class)

Security Profiles

- Antivirus Profiles
- Anti-Spyware Profiles
- Vulnerability Protection Profiles
- URL Filtering Profiles
- Data Filtering Profiles
- File Blocking Profiles
- DoS Protection Profiles
- WildFire Analysis Profiles
- Zone Protection Profiles

Homework

- Configure Palo Alto Zones and Interfaces.
- Configure NAT policy.
- Set Security policy to block and allow traffic.

This lecture brought to you by: