

Palo Alto Firewall

What are next generation firewalls and how do they operate?



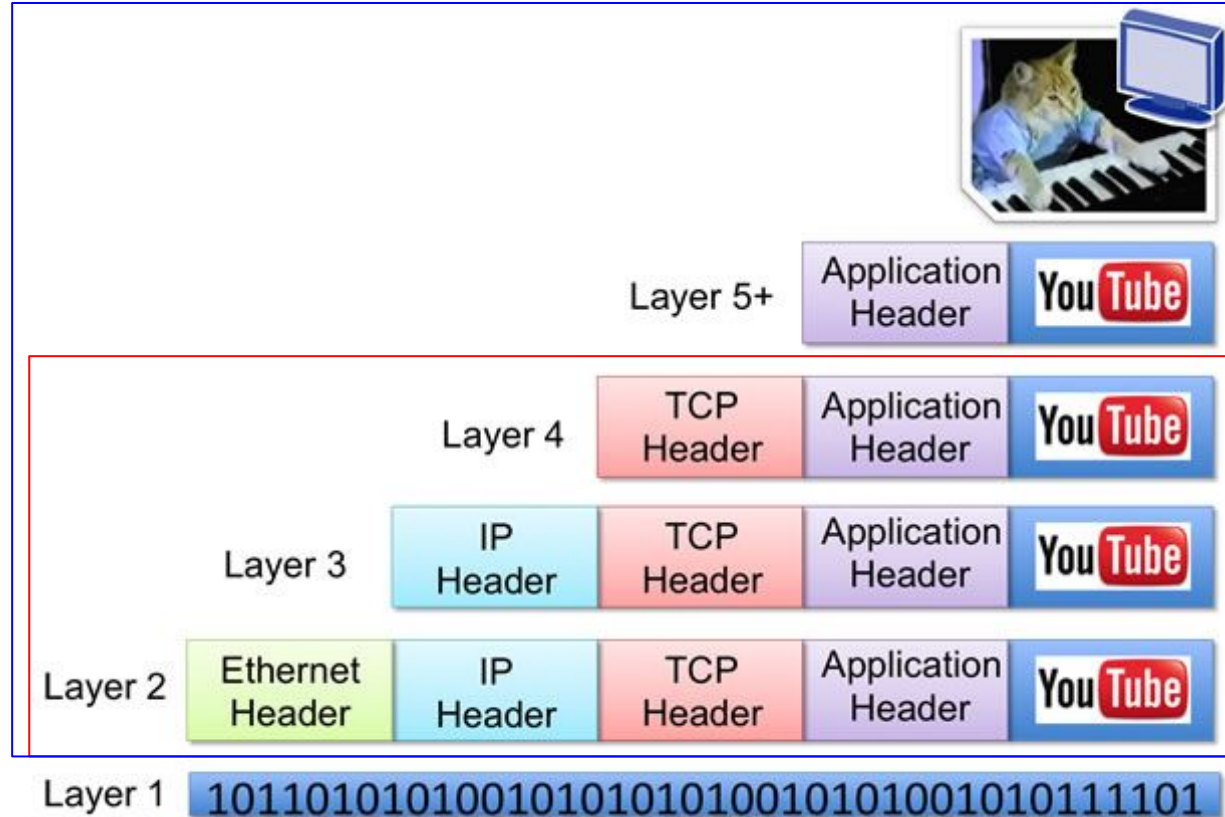
Difference between NGFW and classic firewalls:

	Classic Firewall	Next Generation Firewall
Traffic filtering using Port, IP, and protocol	Supported	Supported
VPN	Supported	Supported
NAT	Supported	Supported
Deep Packet Inspection (DPI)	Not supported	Supported
Intrusion prevention system (IPS) Intrusion detection system (IDS)	Not Supported	Supported
OSI model Layers supported	2-4	2-7
LDAP and Active Directory Integration	Not Supported	Supported
SSL and SSH Decryption	Not Supported	Supported
And Much Much more	Lv. 1 Crook	Lv. 100 Mafia Boss

Layers

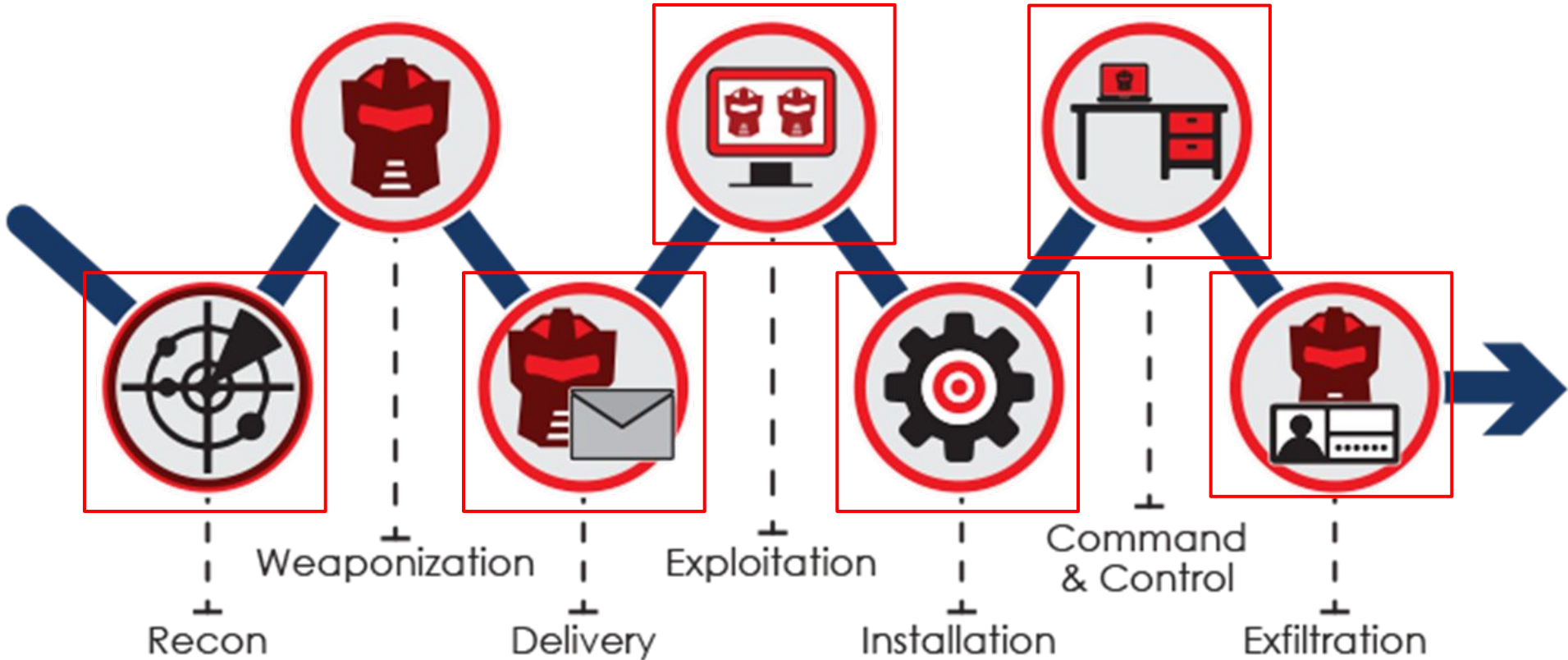
What layers do classic firewalls operate on?

What layers do NGFW operate on?



Cyber Kill Chain

At what stages could firewall be useful?



Some popular Next Generation Firewalls:

FORTINET[®]



paloalto
NETWORKS[®]

FORCEPOINT
POWERED BY Raytheon

JUNIPER
NETWORKS[®]

SONICWALL[®]

Things to consider when getting NGFW

Very Expensive /Subscription fees (Rolling updates for NGFW)

Model	Description	MSRP	Customer Cost
PA-200	Palo Alto Networks PA-200	\$2,000	\$1,600.00
PA-220	Palo Alto Networks PA-220	\$1,000	\$800.00
PA-820	Palo Alto Networks PA-820	\$4,500	\$3,600.00
...			
PAN-PA-5260-DC	Palo Alto Networks PA-5260 with redundant DC power supplies	\$180,000	\$144,000.00
PA-7000	PA-7000 Network Processing Card	\$160,000	\$128,000.00
PA-7050	PA-7050 Base AC Hardware Bundle	\$125,000	\$100,000.00

Requires knowledge to manage

Some Certifications:

- Palo Alto Networks Certified Cybersecurity Associate (PCCSA)
- Palo Alto Networks Certified Network Security Administrator (PCNSA)
- Palo Alto Networks Certified Network Security Engineer (PCNSE)
- Accredited Configuration Engineer (ACE)

Some Requirements:

- Countless hours of studying
- Having a decent background knowledge on a subject of security and networking
- Practice Practice Practice



Requires a lot of processing power

Underlying Operating System does not change much from one hardware firewall to another

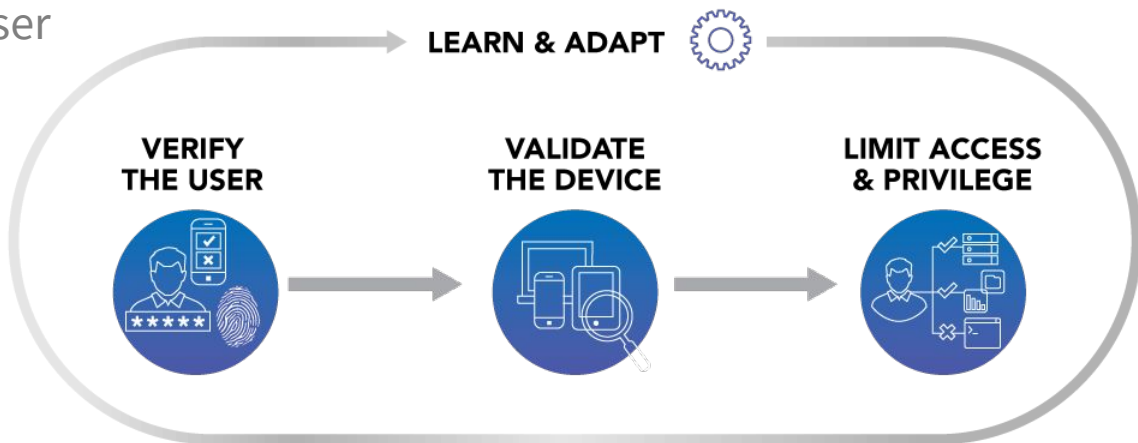
Performance and Capacities ¹	PA-7080 System ²	PA-7050 System ²	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID)	200 Gbps	120 Gbps	68 Gbps	68 Gbps	39 Gbps	18 Gbps
Threat Prevention throughput	100 Gbps	60 Gbps	30 Gbps	30 Gbps	20 Gbps	9 Gbps
IPsec VPN throughput	80 Gbps	48 Gbps	24 Gbps	24 Gbps	16 Gbps	8 Gbps
New sessions per second	1,200,000	720,000	462,000	462,000	348,000	171,000
Max sessions	40,000,000/80,000,000 ³	24,000,000/48,000,000 ³	64,000,000	32,000,000	8,000,000	4,000,000
Virtual systems (base/max ²)	25/225	25/225	25/225	25/225	25/125	10/20

What could be done:

- Have more than one firewall (load balancing)
- Putting NGFW behind traditional firewall
- Create and prioritize rules that wouldn't require too much computational power

Zero Trust Concept

- Never trust anyone, not even people at your own company
- Always verify
- Least privilege
- There is no way to differentiate between good guys and bad guys (essentially assume everyone is bad)
- Validate every device, and user



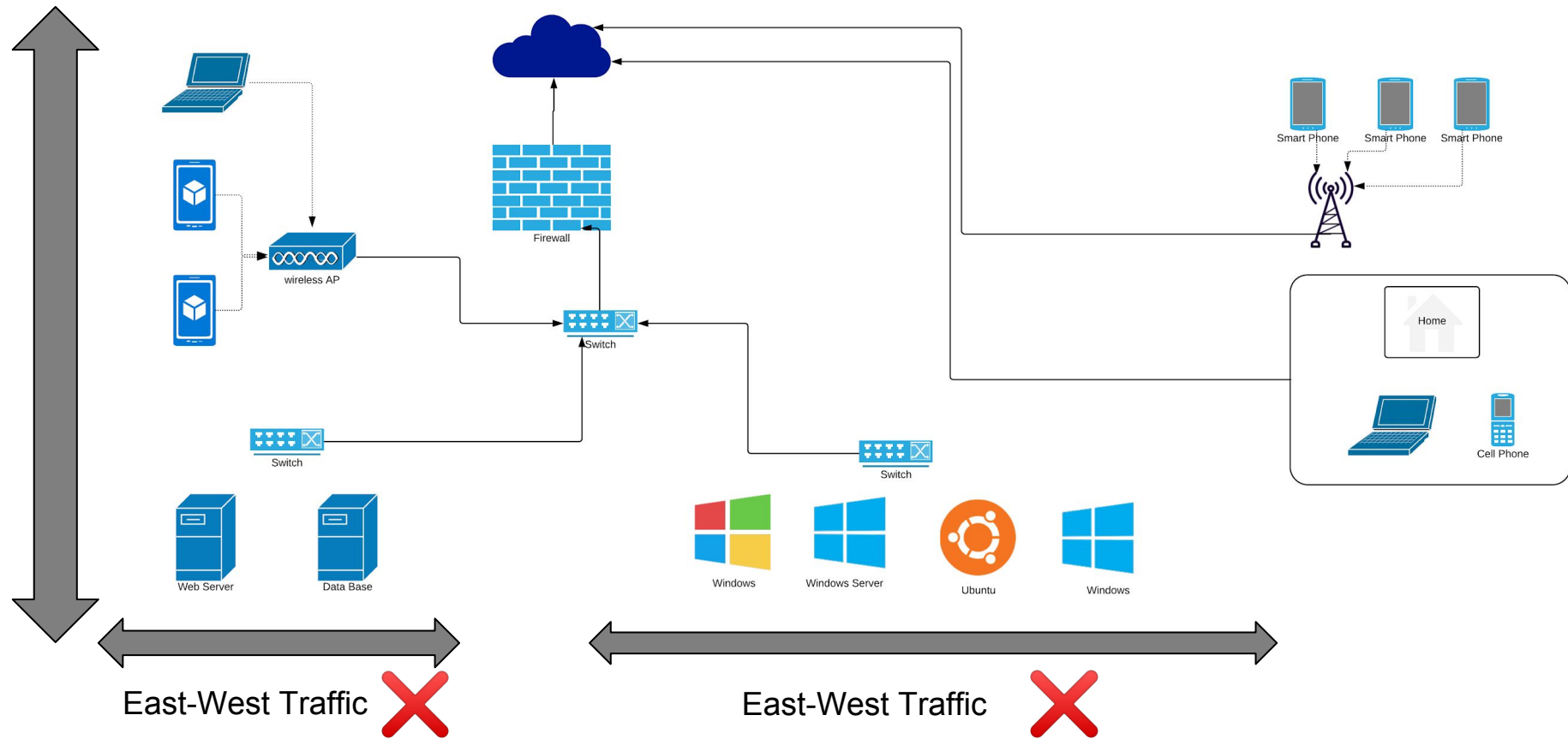
What Zero Trust Architecture accomplishes?

- Reduces the likelihood of accidental breaches (Worker picks up a hard drive on a parking lot)
- Reduces the likelihood of insider attack
- Reduces the likelihood of successful pivoting
- Ensures that east-west traffic is monitored

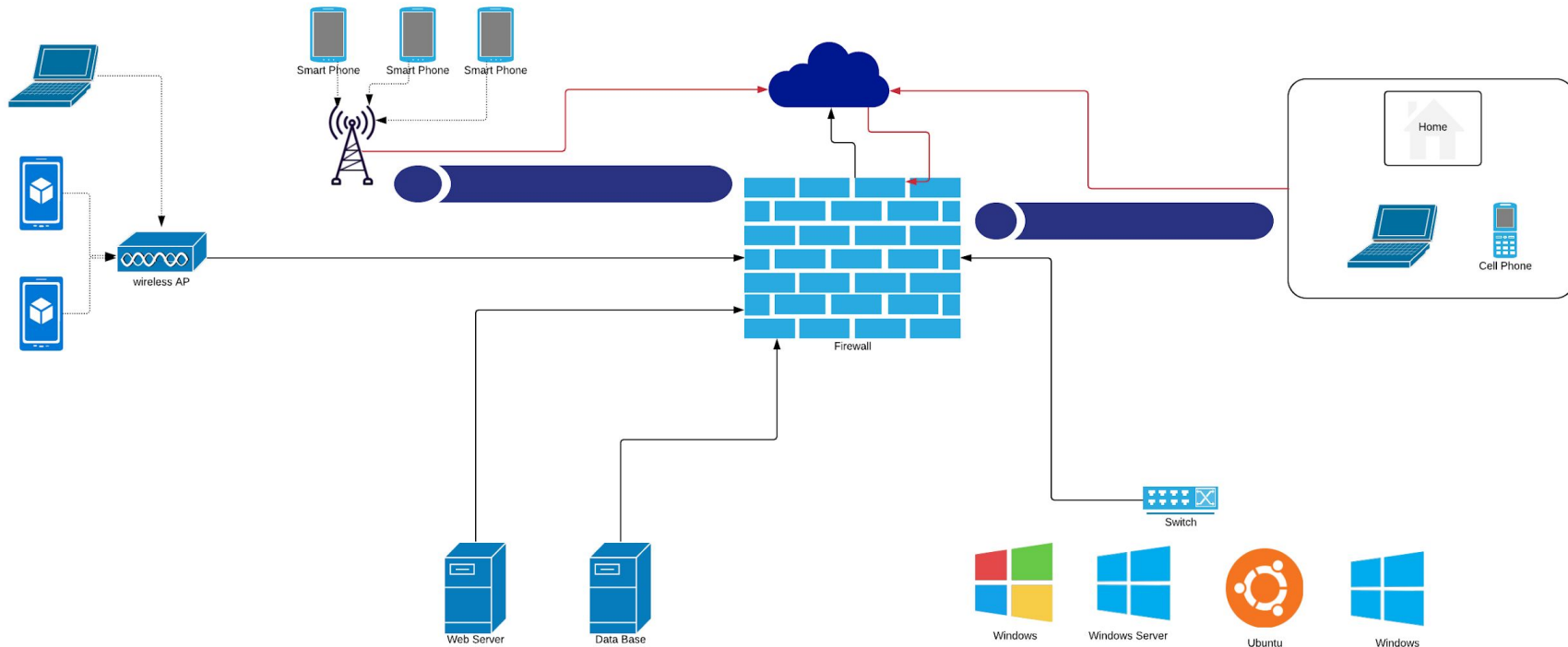
North-South
Traffic



What is wrong on this image?



North-South
Traffic



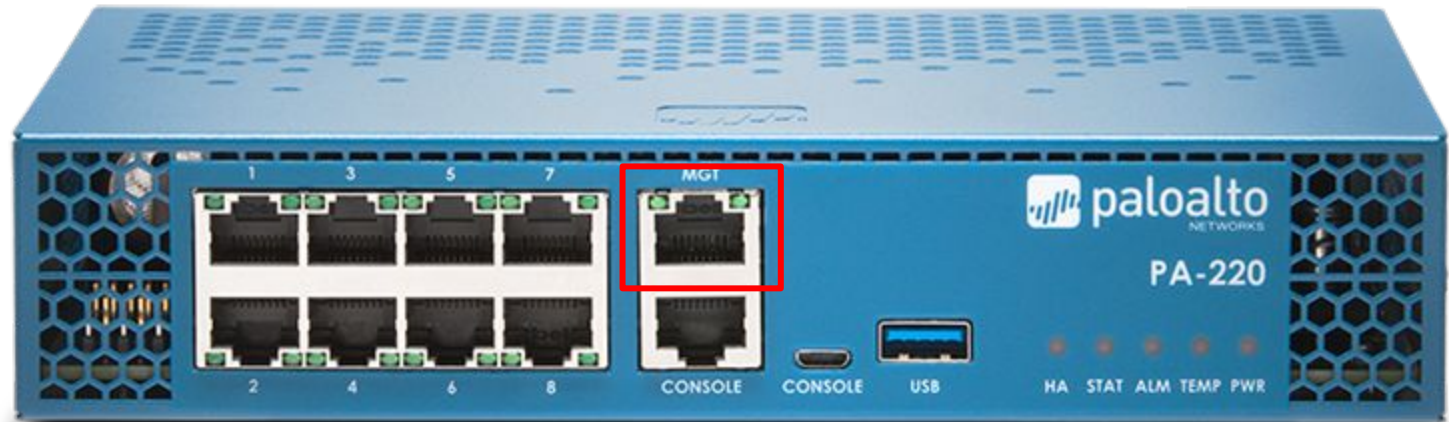
East-West Traffic



East-West Traffic

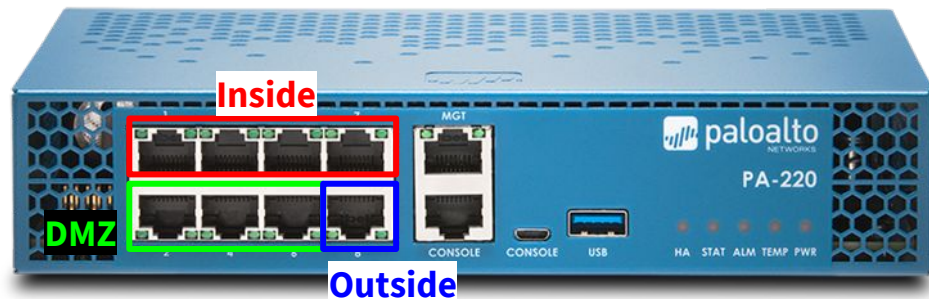


Management Interface



Zones

- A zone is a grouping of interfaces (physical or virtual) that represents a segment of your network that is connected to, and controlled by, the firewall
- Helps you organize your security policies better
- Allows for a proper segmentation of the network
- Easy to understand



High Availability

The Concept that you will hear a lot if you go into networking is High Availability(HA)

Modes in PANOS: Active/Passive, Active/Active

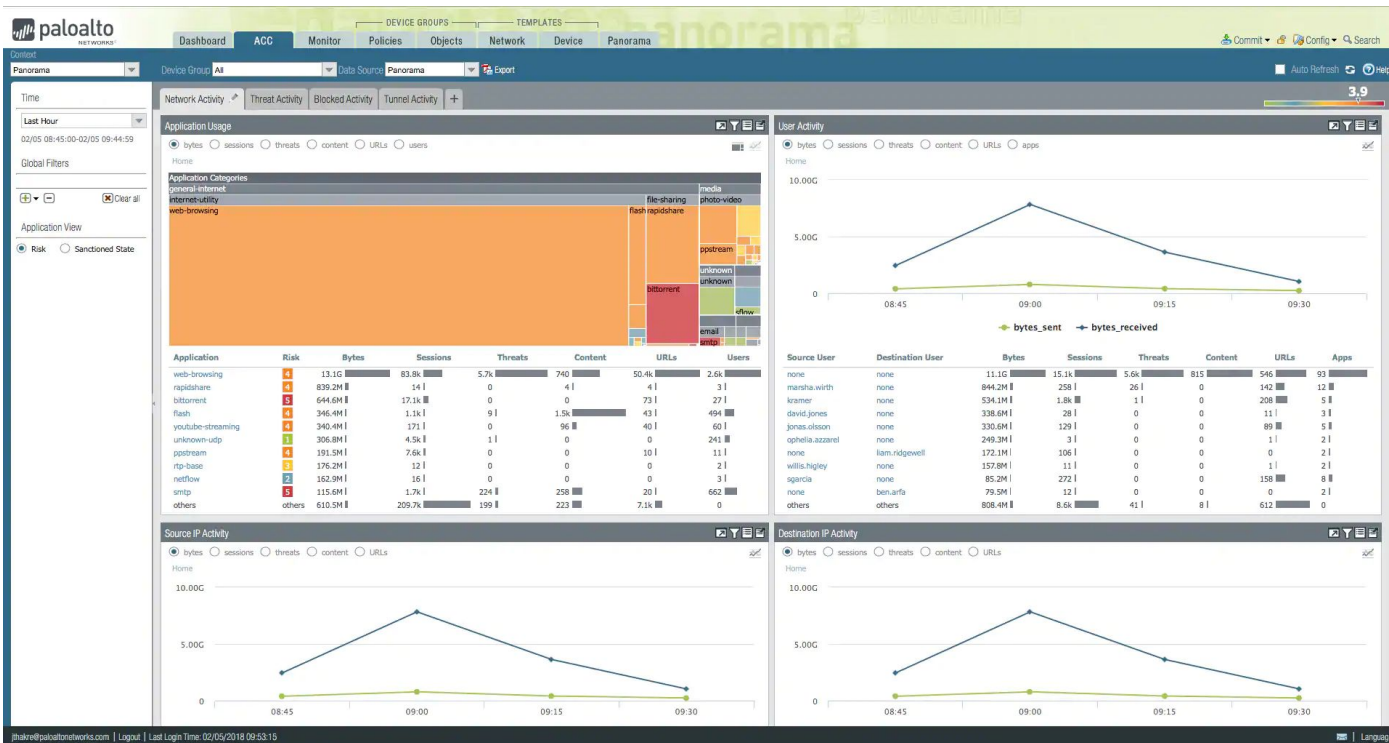
Each has its own cons and pros like ease of setup, speed of failover, and etc.



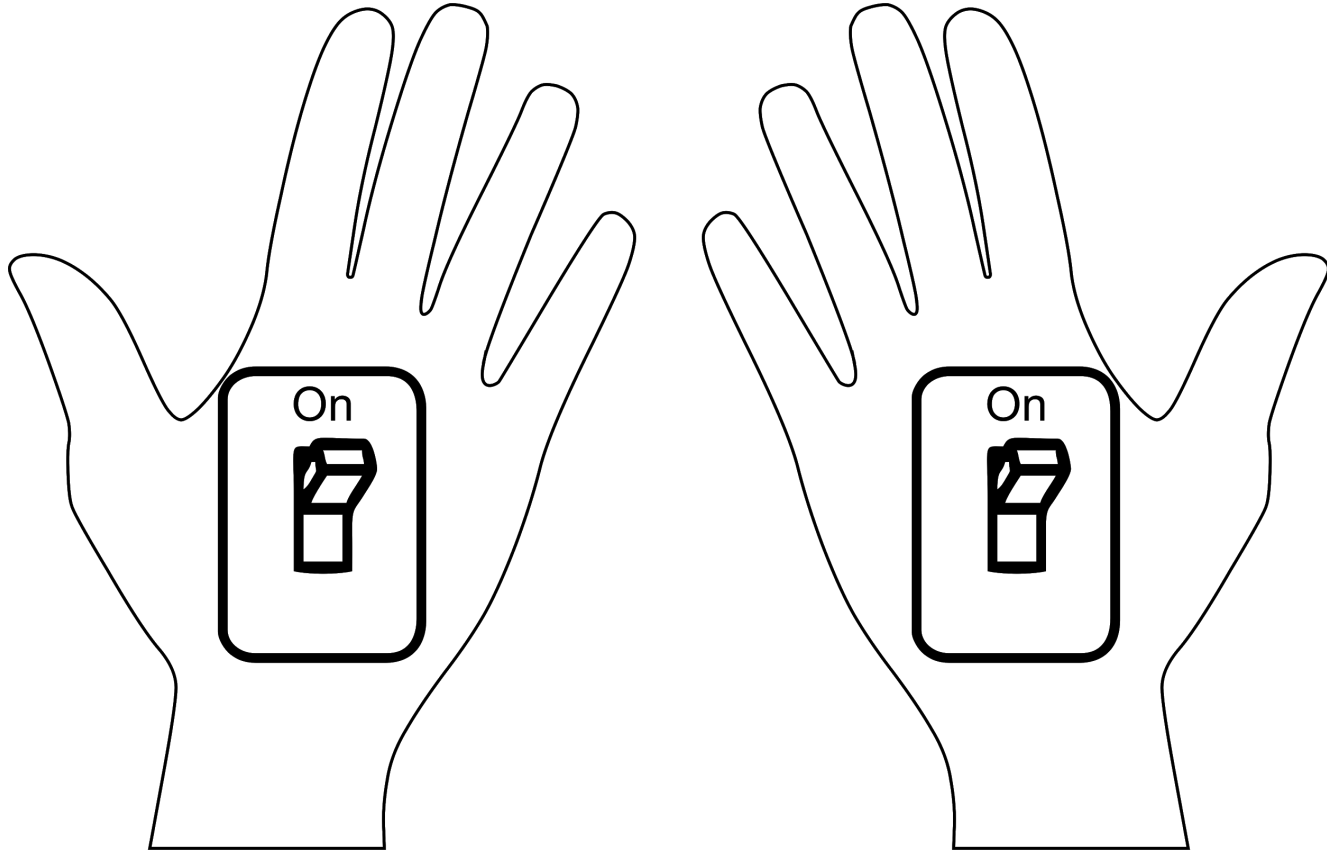
PA-5200 Series

Panorama

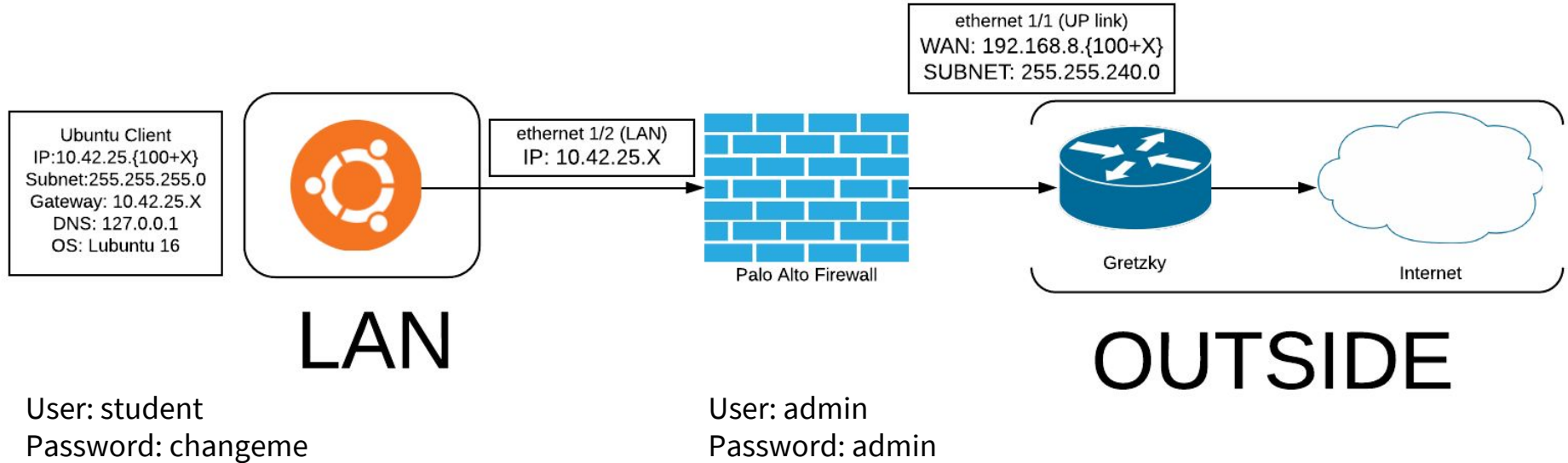
Panorama is a piece of software that helps you manage multiple Palo Alto Firewalls in centralized fashion.



Security Policy (hands-on)



Lab Topology



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 committing, see the difference between Candidate Config and Running Config.



Services and App-ID

ssh 192.168.8.20

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

http://192.168.8.20

http://192.168.13.144:8000

How would we only allow google, and nothing else? (Arman's google question)

Use App-ID google-base

Security Profiles

Antivirus Profiles

Anti-Spyware Profiles

Vulnerability Protection Profiles

URL Filtering Profiles

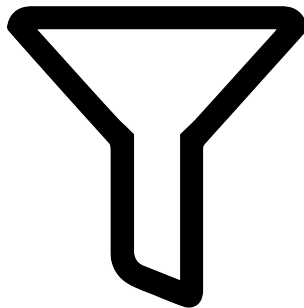
Data Filtering Profiles

File Blocking Profiles

DoS Protection Profiles

WildFire Analysis Profiles

Zone Protection Profiles



Logs

You can use logical operations like 'and', 'or' to sort your logs.

Connector	Attribute	Operator	Value
and	Action	in	Please enter value
or	Action Source	not in	
	Address		

(receive_time leq '2019/03/28 05:25:24') and (zone.src eq inside)

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
--	--------------	------	-----------	---------	--------	-------------	-------------













There are a lot of options available for you to dig more into packet 'metadata'

Detailed Log View			
General		Source	Destination
Session ID	519	User	User
Action	allow	Address	Address
Action Source	from-policy	10.42.25.123	128.205.8.12
Application	incomplete	Country	Country
Rule	Allow All	10.0.0.0-10.255.255.255	United States
Session End Reason	tcp-rst-from-server	Port	Port
Category	any	47858	443
Virtual System		Zone	Zone
Device SN		inside	outside
IP Protocol	tcp	Interface	Interface
Log Action		ethernet1/2	ethernet1/1
Generated Time	2019/03/28 05:25:24	NAT IP	NAT IP
		192.168.8.123	128.205.8.12
		NAT Port	NAT Port
		11037	443
		Details	Flags
		Type	Captive Portal
		end	Proxy Transaction

<input checked="" type="checkbox"/> Receive Time
<input type="checkbox"/> Decrypted
<input checked="" type="checkbox"/> Type
<input checked="" type="checkbox"/> From Zone
<input checked="" type="checkbox"/> To Zone
<input checked="" type="checkbox"/> Source
<input checked="" type="checkbox"/> Source User
<input checked="" type="checkbox"/> Destination
<input checked="" type="checkbox"/> To Port
<input checked="" type="checkbox"/> Application
<input checked="" type="checkbox"/> Action
<input checked="" type="checkbox"/> Rule
<input checked="" type="checkbox"/> Session End Reason
<input checked="" type="checkbox"/> Bytes
<input type="checkbox"/> Action Source
<input type="checkbox"/> Bytes Received
<input type="checkbox"/> Bytes Sent
<input type="checkbox"/> Captive Portal
<input type="checkbox"/> Client to Server
<input type="checkbox"/> Count
<input type="checkbox"/> Destination Country
<input type="checkbox"/> Destination User
<input type="checkbox"/> Destination UUID
<input type="checkbox"/> Egress I/F
<input type="checkbox"/> Elapsed Time (sec)
<input type="checkbox"/> From Port

ACC (Application Command Center)

ACC is an interface that provides you with a nice overview of the network activity.

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 

Homework

Make sure that the ip addresses are aligned according to the topology (this will make troubleshooting much easier).

Ask questions:
@lightman
@ohadkatz
@jay_c

