



TOP COMMONLY DEPLOYED SCENARIOS
PALO ALTO NETWORKS
FIREWALLS & PANORAMA



paloalto[®]
NETWORKS

Paula Wong, CEO and Founder/ CCIE #13062, PCNSE10,
C-7# 1086962, Senior Security Architect/Engineer

+++++

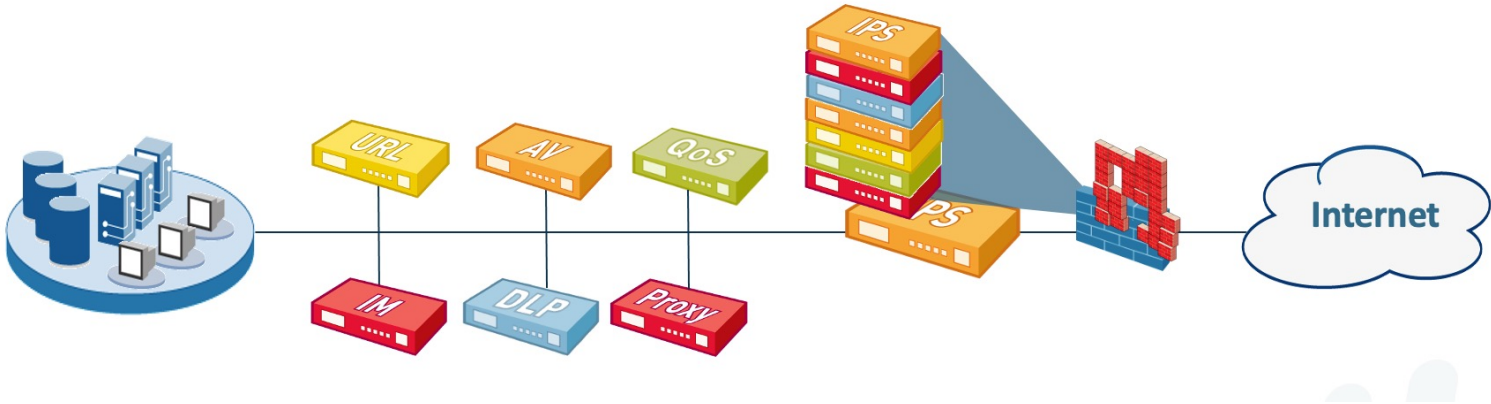
www.accendnetworks.com

Table of Contents

Day 0 Stage	03
Day 1 Stage	05
License Registration	05
Software Update, Dynamic Content Updates, and Interface Options	06
Security Policies and NAT Policy for Outbound Internet Access	07
VPN (GlobalProtect Client and Site-to-Site)	13
Other Advanced Features	20
High Availability (HA)	20
Vsys	22
HIP Profile	22
Day 2 Stage	23
Best Practice Assessment (BPA)	23
Policy Optimizer	24
Panorama	25
Managing Firewalls	28
Template and Template Stacks	31, 39
Device Group and Device Group Hierarchy	33

Day 0 Stage

CHAPTER ONE




Day 0 Stage is all about planning and choosing the correct Palo Alto Networks Firewalls for your network. When choosing the correct firewall size, make sure you plan for five to seven/ten years ahead for scaling and ensure there are enough interfaces to support your environment, along with budget.

Day 0 Stage


Planning Phase

Prior to deploying the Palo Alto Networks firewalls, one must decide on which model to select. Palo Alto Networks firewalls have different versions of the physical and virtual models, depending on the requirement.

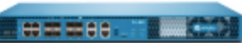
Below are some different Palo Alto Networks Next-Generation firewalls to choose from (both physical appliances and virtualized firewalls):

• **PA-5410:** 


App-ID firewall throughput	43.5 Gps
Threat prevention throughput	26.7 Ggps
Connections per second.	270,000
Max sessions (IPv4 or IPv6).	3,600,000

• **PA-3410:** 


App-ID firewall throughput	11 Gps
Threat prevention throughput	5.6 Ggps
Connections per second	145,000
Max sessions (IPv4 or IPv6)	1,400,000

• **PA-850:** 


App-ID firewall throughput	1.9 Gps
Threat prevention throughput	1 Ggps
Connections per second	13,100
Max sessions (IPv4 or IPv6)	192,000

• **PA-220:** 

App-ID firewall throughput	535 Mbps
Threat prevention throughput	320 Mbps
Connections per second.	4,200
Max sessions (IPv4 or IPv6).	64,000

• **VM-Series (2 vCPU, 4.5 GB):** 

App-ID firewall throughput	3 Gps
Threat prevention throughput	1.5 Gbps
Connections per second	3,000
Max sessions (IPv4 or IPv6)	50,000

• **VM-Series (4 vCPU, 9GB):** 

App-ID firewall throughput	6 Gps
Threat prevention throughput	3 Ggps
Connections per second	30,000
Max sessions (IPv4 or IPv6)	819,200

Besides the App-ID, Threat, Connections per second and Max sessions, other critical factors are below:

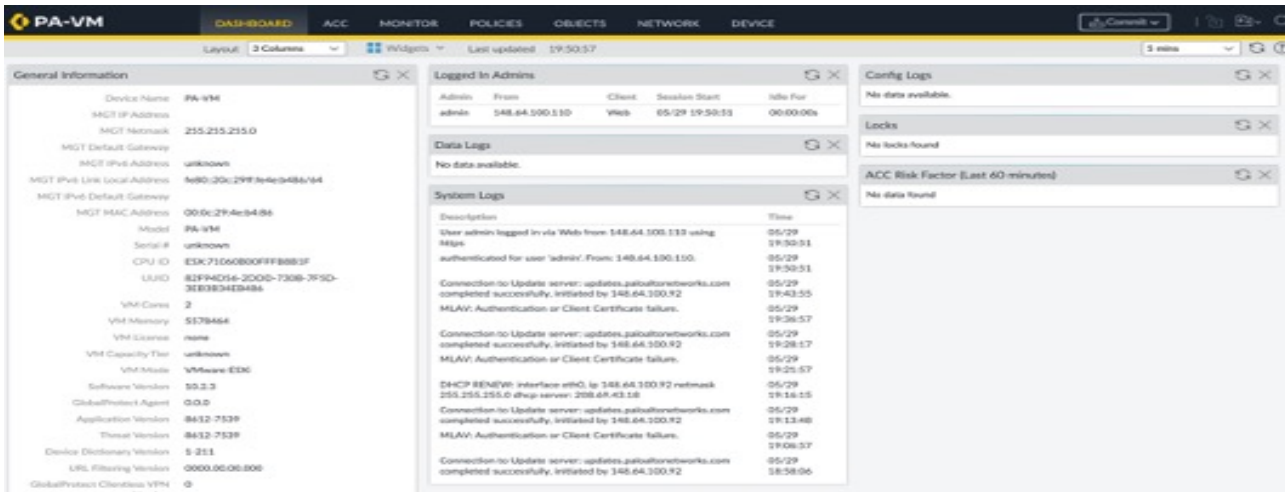
- Interfaces Type (SFP/SFP+, Copper)
- Interfaces Throughput (1000/10Gbps/40Gbps, 100Gbps)
- Number of Interfaces
- Number of IPSec VPN Peers Supported
- Number of GlobalProtect Client/Clientless VPN Supported

See the following URL for more details and other platforms available:

<https://www.paloaltonetworks.com/products/product-selection.html>

Day 1 Stage

Initial Configuration



Initial Configuration, License Registration, Software Update, Base Firewalls and NAT Rules

After procuring your Palo Alto Networks firewalls, some initial configuration needs to be done prior to deploying it into production.

The steps required for Day 1 phase are below:

- License Registration
- Software Update and Dynamic Content Updates
- Interfaces (Type, Speed, and Quantity)
- Security and NAT Policies
- Wildfire, URL Filtering, and App-ID
- VPN (Global Protect and Site-to-Site VPN)
- Other Advanced Features:
 - High Availability (HA)
 - VSYS
 - HIPS Profile

License Registration:

License activation can be achieved through several methods and the two methods commonly used are:

- Activate feature using authorization code
- Manually upload license key

You should have device serial number ready when activating the license and have access to the Customer Support Portal.

See the following details steps on how to activate the license:

[How to Activate Authorization Codes \(Auth Codes\)](#)

Day 1 Stage (contd)

— Initial Configuration

Software Update:

After license is registered, you should check the software update for the latest software available. It is recommended to not deviate for more than six months from when the software is released and also, you should wait at least three months after a software release is available to ensure there is no software bugs and for it to stabilize.

You can check for new software update available by going to **Device – Software – Check Now** (in the lower left hand corner). Once you find the software release that you want to download, you must first download it and then install it. It is also recommended to review the PAN-OS Release Notes of the version you're downloading to for any known caveats prior to installing it.

Dynamic Content Updates:

You should also check for any dynamic content updates available for your subscriptions by going to Device -> Dynamic Updates.

See the following URL for more details:

[Dynamic Content Updates](#)

Interfaces Options:

You should plan ahead what type of interfaces you will require for your network, whether it is 1G, 10G or 40G+ SFP/SFP+ or copper connection and how many.

Palo Alto Networks will support third-party SFP modules but it is always a good idea to test the SFP module first prior to your cutover to ensure there is no connectivity issue.

Below are some links related to SFP Modules that may be useable:

[How to view SFP SFP+ or QSFP module transceiver details](#)

[Key Specifications for Palo Alto Networks Interfaces and Transceivers](#)

Other interfaces options to consider are:

Layer 2, Layer 3, Trunking, and link aggregation.

Also make sure you have the correct cable type to connect to the other end, be it the network switch downstream or upstream etc.

Day 1 Stage (contd)

Initial Configuration

Security Policies:

By default, all traffic is blocked from going inbound and outbound. And there are two default security rules and they are:

intrazone-default: Allows all traffic within the same zone

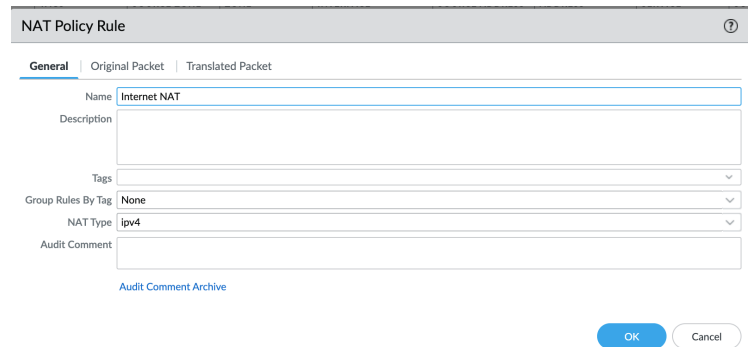
Interzone-default: Blocks all traffic between different zones

For a basic outbound interface traffic for all users on the internal network, we will need to create a NAT policy and a security policy. The NAT policy just creates the necessary translation that is needed from the internal to the external network. The security policy actually allows you to access the internet.

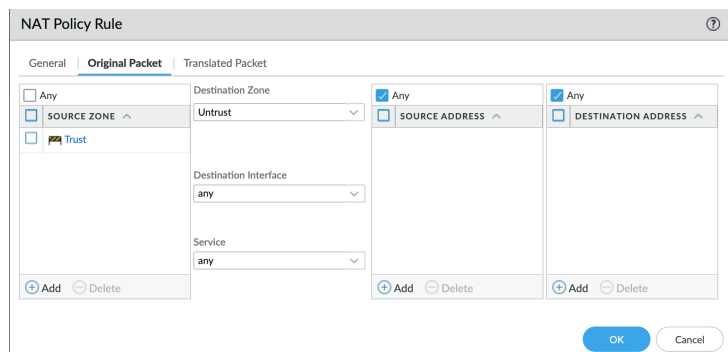
NAT Policy for Outbound Internet:

We will assume that two zones have already been created: the trust and untrust zone. We will NAT the traffic to the outside interface of ethernet1/1.

Go to Policies, NAT, Add and create the NAT policy as shown below:



The screenshot shows the 'NAT Policy Rule' configuration window in the 'General' tab. The name is 'Internet NAT'. The description field is empty. The 'Tags' field is empty. The 'Group Rules By Tag' is set to 'None'. The 'NAT Type' is set to 'ipv4'. The 'Audit Comment' field is empty. There are 'OK' and 'Cancel' buttons at the bottom right.



The screenshot shows the 'NAT Policy Rule' configuration window in the 'Original Packet' tab. The 'Destination Zone' is set to 'Untrust'. The 'Destination Interface' is set to 'any'. The 'Service' is set to 'any'. There are two columns for 'SOURCE ADDRESS' and 'DESTINATION ADDRESS', both with 'Any' selected. There are 'Add' and 'Delete' buttons for each column. There are 'OK' and 'Cancel' buttons at the bottom right.

Day 1 Stage (contd)

Initial Configuration

NAT Policy for Outbound Internet:

NAT Policy Rule ?

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/1

IP Address: 192.168.2.254/24

Destination Address Translation

Translation Type: None

OK
Cancel

The result will look like below:

	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Internet NAT	none	Trust	Untrust	any	any	any	any	dynamic-ip-and-port	none
									ethernet1/1	
									192.168.2.254/24	

Security policy for outbound Internet access:

Go to **Policies -> Security-> Add**, and create the Security Policy Rule as shown below:

Security Policy Rule ?

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name: Internet Access

Rule Type: universal (default)

Description:

Tags: None

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK
Cancel

Day 1 Stage (contd)

Initial Configuration

Security policy for outbound Internet access (contd):

Security Policy Rule ?

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	any	any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	<input type="checkbox"/> SOURCE DEVICE ^
<input type="checkbox"/> Trust			
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

Negate

Security Policy Rule ?

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select	<input checked="" type="checkbox"/> Any	any
<input type="checkbox"/> DESTINATION ZONE ^	<input type="checkbox"/> DESTINATION ADDRESS ^	<input type="checkbox"/> DESTINATION DEVICE ^
<input type="checkbox"/> Untrust		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

Negate

Day 1 Stage (contd)

Initial Configuration

Security policy for outbound Internet access (contd):

Security Policy Rule ?

General | Source | Destination | **Application** | Service/URL Category | Actions | Usage

<input type="checkbox"/> Any <input checked="" type="checkbox"/> APPLICATIONS ^ <input type="checkbox"/> web-browsing	<input type="checkbox"/> DEPENDS ON 0 items → ×
---	--

+ Add - Delete Add To Current Rule Add To Existing Rule

OK Cancel

Security Policy Rule ?

General | Source | Destination | Application | **Service/URL Category** | Actions | Usage

application-default v

<input checked="" type="checkbox"/> SERVICE ^	<input checked="" type="checkbox"/> Any <input type="checkbox"/> URL CATEGORY ^
---	--

+ Add - Delete + Add - Delete

OK Cancel

About the Author

Fun Facts

A**Built First Computer at age 11****B****Voted Most Likely to Succeed in Junior High School and Fastest Typist****C****1 Future Goal: Become Certified Ethical Hacker**

Paula Wong, CEO and Founder/CCIE #13062, PCNSE, C7 #1086962, Author, Speaker, Trainer, Senior Network Architect/Security Engineer

An IT veteran with over 27+ years of experience. Worked at Cisco Security TAC, Advanced Services, Salesforce, Expedia/Hotwire/Webex, and other Fortune 500 companies.

Hobbies: Vegan, love to cook, runner/biker, and yoga enthusiast.



Contact Us Today!

For any questions , custom training, or if you need assistance with your current Palo Alto Networks Firewall and Panorama deployment, feel free to contact us below:

Paula Wong, CEO & Founder/ CCIE #13062, PNCSE, C-7 #1086962, PNCSE 10

Email: paula@accendnetworks.com

Phone: 408-784-2345 Local / 855-8ACCEND (822-2363)

We offer efficient and advanced network security consulting services.



www.accendnetworks.com