

Hardware Appliance Deployment

Option 1

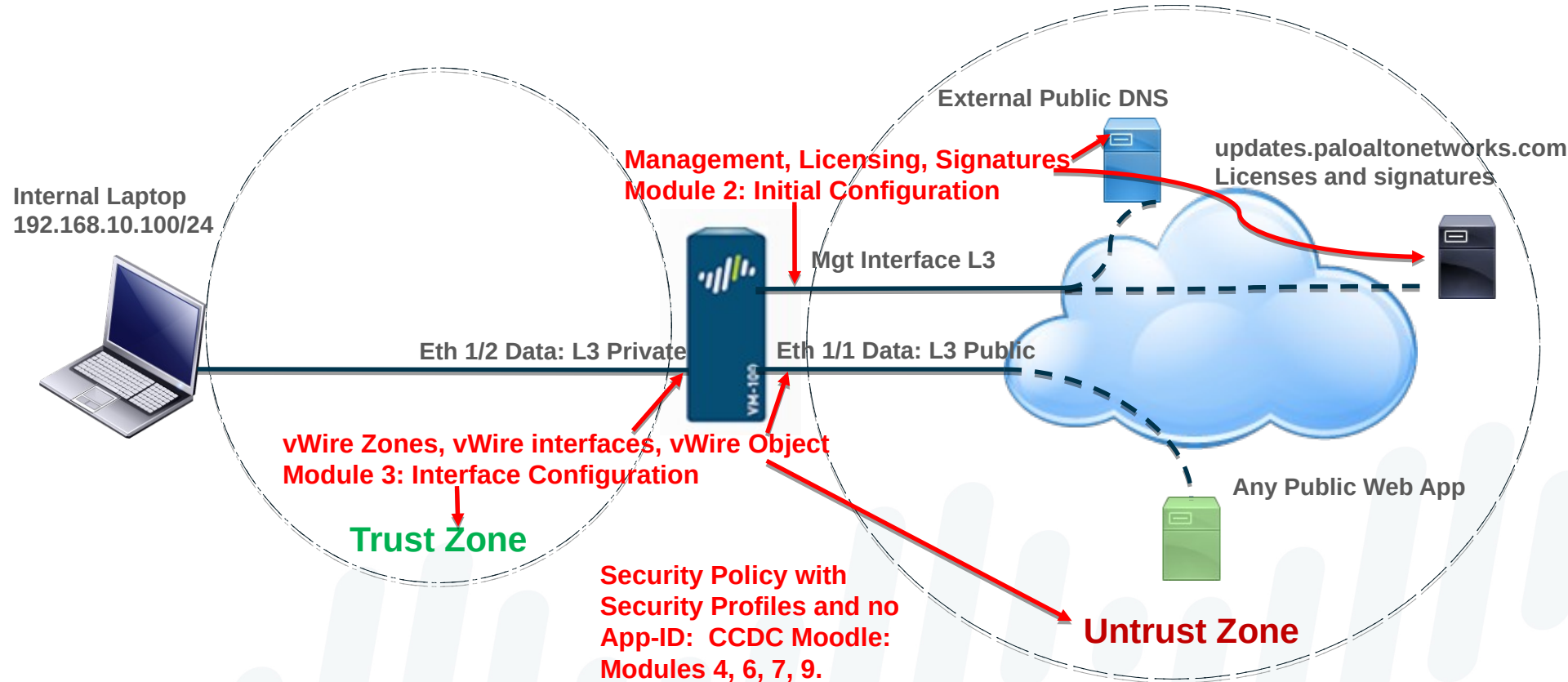
Team Hardware Firewall Appliances at CCDC

- CCDC competitions have the option to provide our hardware firewall appliances for teams to use during the competition in addition to our VM-series appliances
 - Teams may be provided hardware appliances at CCDC competitions
- Hardware appliance team distribution options
 - Option 1: Teams provided hardware appliance sometime after competition starts
 - Teams would then integrate firewall with existing network and gateway to provide protection
 - Option 2: Teams provided hardware appliance as part of their competition network at the start of competition
 - Teams would have to secure and configure deployed hardware firewall appliance
- This presentation covers Option 1

Option 1: Deployment and Configuration

- Connect and secure the management interface
 - Firewall by default receives Threat signature updates, Wildfire signatures and URL categorization from our public server via the management interface
 - You can also update firewall Threat signatures and Wildfire via computer upload if the management interface can not be connected to Internet
- Set up initial vWire security policy to provide immediate malware protection
- Transition to a Layer3 interface configuration to take full advantage for firewall features

Option 1 Initial vWire: Passing Data Using vWire and Malware Protection but no App-ID



Serial Settings

- Very important that your serial settings are correct to access console port
- The settings in the Hyper Terminal need to be set correctly; otherwise, no access or garbage characters may show up on the screen. When setting up the connection, use these settings:
- Bits per sec : 9600
- Data bits : 8
- Parity : none
- Stop bits : 1
- Flow control : none
- <https://live.paloaltonetworks.com/t5/Management-Articles/What-are-the-Serial-Settings-to-Accepts-Console-Port/ta-p/62022>
- <https://www.cyberciti.biz/faq/unix-linux-apple-osx-bsd-screen-set-baud-rate/>

System Info via Console

- General system info
 - > show system info

```
Warning: Your device is still configured with the default admin account credentials. Please change your password prior to deployment.
admin@PA-3050> show system info

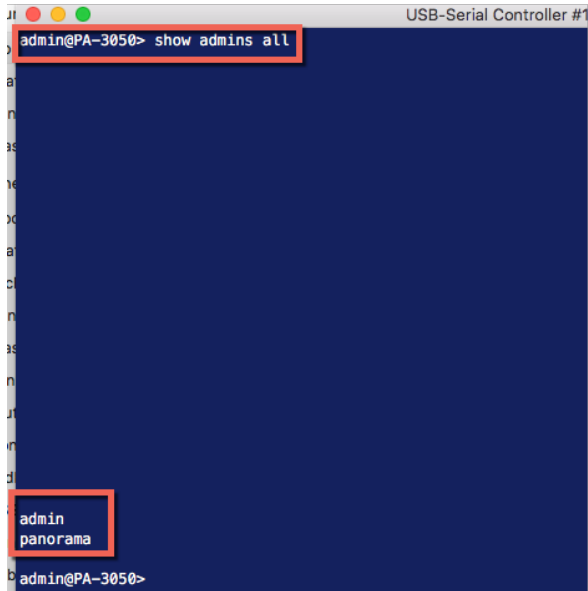
hostname: PA-3050
ip-address: 192.168.1.1
netmask: 255.255.255.0
default-gateway: 192.168.1.1
ip-assignment: static
ipv6-address: unknown
ipv6-link-local-address: unknown
ipv6-default-gateway:
mac-address: 00:1b:17:ff:f6:28
time: Tue Feb 20 13:36:42 2018
uptime: 0 days, 0:21:44
family: 3000
model: PA-3050
serial: 001701002152
sw-version: 8.0.7
global-protect-client-package-version: 4.0.3
app-version: 777-4484
app-release-date: 2018/02/06 21:20:15
```

You will need to change. Mgt interface needs Internet access

Check PANOS version and Licenses

Secure appliance: Show all admin accounts

- You want to make sure there are only two admin accounts: admin and panorama - - default configuration
 - > show admins all
 - # delete mgt-config users <any extra users> and # commit

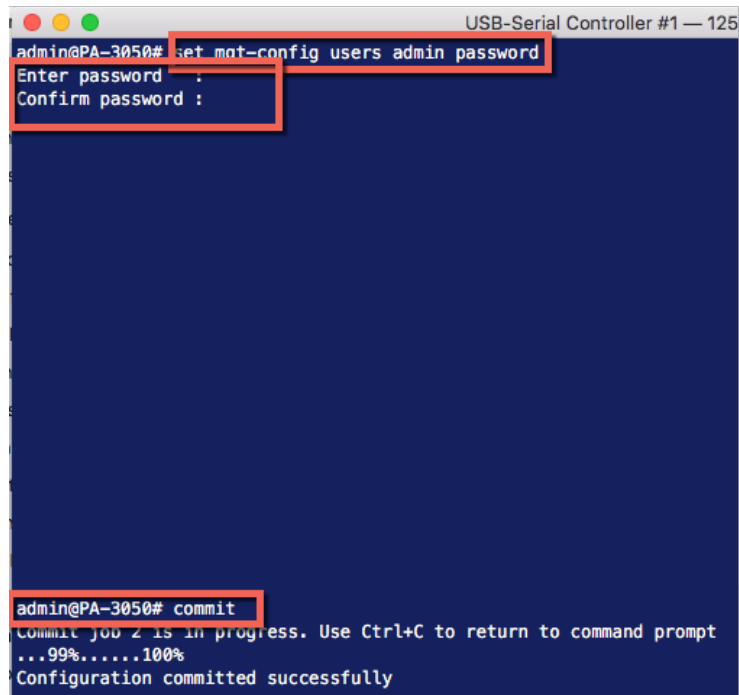


A terminal window titled "USB-Serial Controller #1" showing a command prompt. The prompt is "admin@PA-3050>". The command "show admins all" is entered and highlighted with a red box. The output of the command is displayed in a dark blue box, showing "admin" and "panorama" as the only admin accounts. The prompt "admin@PA-3050>" is visible at the bottom of the terminal window.

```
admin@PA-3050> show admins all
admin
panorama
admin@PA-3050>
```

Secure appliance: change default admin password

- Change admin password
 - # set mgt-config users admin password <your new password> and # commit



```
admin@PA-3050# set mgt-config users admin password
Enter password :
Confirm password :

admin@PA-3050# commit
Commit job 2 is in progress. Use Ctrl+C to return to command prompt
...99%.....100%
Configuration committed successfully
```


Configure mgt interface IP address and connect it

- Change mgt interface IP address, default gateway and preferred DNS server
 - # set deviceconfig system ip-address <your IP address> netmask <subnet mask> default-gateway <ip address> and # commit

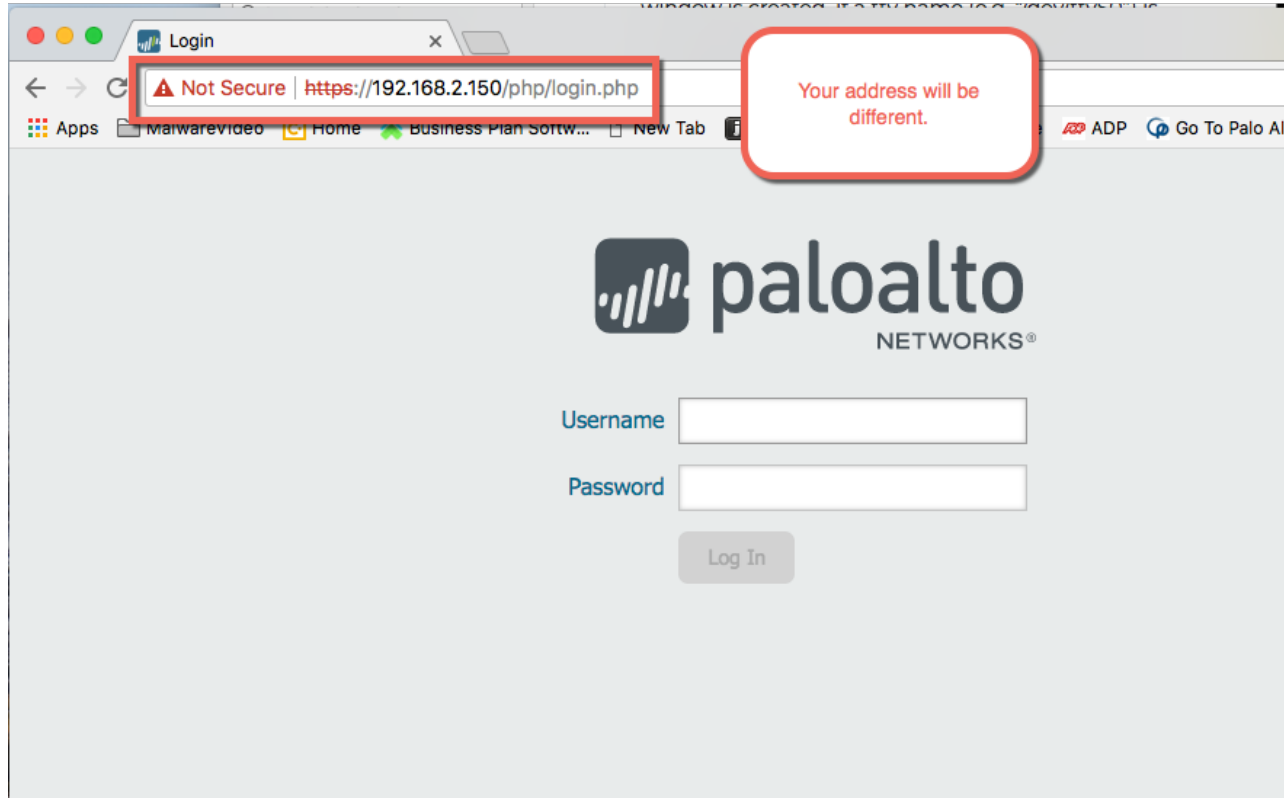
```
admin@PA-3050# set deviceconfig system ip-address 192.168.2.150 netmask 255.255.255.0 default-gateway 192.168.2.1 dns-setting servers primary 8.8.8.8
```

```
[edit]
```

```
admin@PA-3050# commit
```

Your address settings will
be different

Connect to Mgt Interface Web-UI



Web-UI: Check Licenses, DeviceTab>Licenses

The screenshot shows the Palo Alto Networks Web-UI interface. The browser address bar indicates the URL `https://192.168.2.150/#device::vsys1::device/licenses`. The page title is "PA-3050". The navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The left sidebar shows a tree view of configuration options, with "Licenses" selected under the "Device" tab. The main content area displays the "Device > Licenses" page, which is organized into several sections:

- AutoFocus Device License**
 - Date Issued: February 19, 2018
 - Date Expires: November 13, 2020
 - Description: AutoFocus Device License
- GlobalProtect Gateway**
 - Date Issued: February 19, 2018
 - Date Expires: April 19, 2018
 - Description: GlobalProtect Gateway License
- PAN-DB URL Filtering**
 - Date Issued: February 19, 2018
 - Date Expires: April 19, 2018
 - Description: Palo Alto Networks URL Filtering License
 - Active: Yes
 - Download Status: 2018-02-19 15:48:24.774 -0800 URL database download: not available. [Re-Download](#)
- Virtual Systems**
 - Date Issued: February 19, 2018
 - Date Expires: Never
 - Description: Additional 5 Virtual System Licenses
- License Management**
 - [Retrieve license keys from license server](#)
 - [Activate feature using authorization code](#)
- BrightCloud URL Filtering**
 - Date Issued: February 19, 2018
 - Date Expires: April 19, 2018
 - Description: BrightCloud URL Filtering
 - Active: No ([Activate](#))
- GlobalProtect Portal**
 - Date Issued: February 19, 2018
 - Date Expires: April 19, 2018
 - Description: GlobalProtect Portal License
- Threat Prevention**
 - Date Issued: February 19, 2018
 - Date Expires: April 19, 2018
 - Description: Threat Prevention
- WildFire License**
 - Date Issued: February 19, 2018
 - Date Expires: April 19, 2018
 - Description: WildFire signature feed, integrated WildFire logs, WildFire API

The bottom status bar shows the user is logged in as "admin" and the last login time was "02/22/2018 09:28:36".

Web-UI: Check Dynamic Updates, Device tab>Dynamic Updates

The screenshot shows the Palo Alto Networks Web-UI interface. The left sidebar contains a tree view of configuration categories, with 'Dynamic Updates' highlighted. The main content area displays a table of dynamic updates. The table has columns: Version, File Name, Features, Type, Size, Release Date, Download, Currently Installed, Action, and Documentation. The updates are grouped by category: Antivirus, Applications and Threats, GlobalProtect Clientless VPN, GlobalProtect Data File, and WildFire. The 'Schedule' column for several updates is highlighted with a red box and labeled 'None'. The 'Check Now' button at the bottom is also highlighted with a red box.

Version	File Name	Features	Type	Size	Release Date	Download	Currently Installed	Action	Documentation
Antivirus Last checked: 2018/02/19 19:23:03 PST Schedule: None									
Applications and Threats Last checked: 2018/02/19 19:22:33 PST Schedule: Every Wednesday at 01:02 (Download only)									
GlobalProtect Clientless VPN Last checked: 2018/02/19 19:22:36 PST Schedule: None									
67-98	panup-all-gp-67-98	GlobalProtect...	Full	70 KB	2017/09/19 09:50:56 PDT	✓	✓		Release Notes
GlobalProtect Data File Schedule: None									
WildFire Last checked: 2018/02/19 19:22:35 PST Schedule: None									
219889-222306	panupv2-all-wildfire-219889-222306	PAN-OS 7.1 and later	Full	9 MB	2018/02/19 19:15:06 PST	✓	✓		Release Notes

Check Now Upload Install From File

Web-UI: Check Time Settings for logs, DeviceTab>Setup>Management>General Settings

The screenshot shows the Palo Alto Networks Web-UI for a PA-3050 device. The browser address bar displays the URL <https://192.168.2.150/#device::vsys1::device/setup>. The interface includes a top navigation bar with tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. A left sidebar lists various setup options, including High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources, Certificate Management, Certificates, Certificate Profile, OSCP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusion, Response Pages, Log Settings, Server Profiles, and SNMP Trap. The main content area is divided into sections: Management, Operations, Services, Interfaces, Telemetry, Content-ID, WildFire, Session, and HSM. The General Settings section is active, showing fields for Hostname (PA-3050), Domain, Login Banner, Force Admins to Acknowledge Login Banner (unchecked), SSL/TLS Service Profile, Time Zone (US/Pacific), Locale (en), Time (Thu Feb 22 12:27:04 PST 2018), Geo Location, Automatically Acquire Commit Lock (unchecked), Certificate Expiration Check (unchecked), and Multi Virtual System Capability (unchecked). The Time field is highlighted with a red box. Other sections visible include Panorama Settings (Panorama Servers, Receive Timeout for Connection to Panorama (sec) 240, Send Timeout for Connection to Panorama (sec) 240, Retry Count for SSL Send to Panorama 25, Secure Client Communication) and Banners and Messages (Message of the Day, Allow Do Not Display Again (unchecked), Title Message of the Day, Background Color, Icon, Header Banner, Header Color).

Web UI: PA 3050 Pre-Configured for Quick vWire Deployment

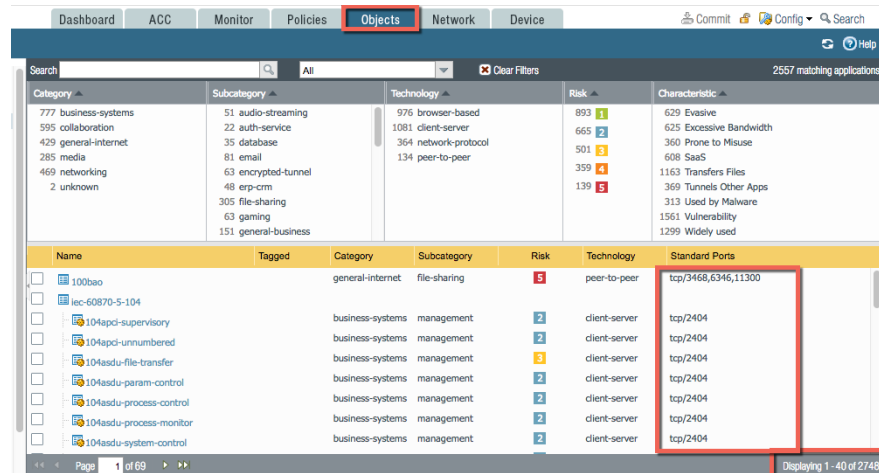
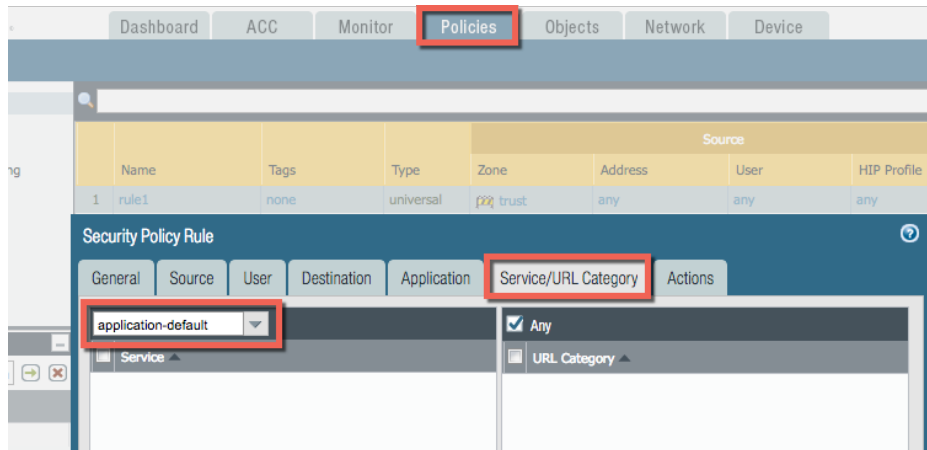
- vWire Interfaces and Zones
 - Ethernet1/1: Untrust Zone
 - Ethernet1/2: Trust Zone
- You can create vWire sub-interfaces and assign vlan tag if needed
- Rule1 Security Policy for traffic originating from trust zone

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Virtual Wire		down	none	none	Untagged	default-vwire	untrust
ethernet1/2	Virtual Wire		down	none	none	Untagged	default-vwire	trust

Web-UI Modify Rule1 : Change Services from any to application default

Will block sessions using ports that aren't assigned to an application ID in Objects tab>Applications

Firewall Application IDs



Web-UI Modify Rule1 : Add Security Profiles

The screenshot displays the Palo Alto Networks Web-UI for configuring a Security Policy Rule. The 'rule1' rule is selected in the table. The 'Actions' tab is active, showing the 'Action Setting' section with 'Action' set to 'Allow'. The 'Profile Setting' section is highlighted with a red box, showing various security profiles configured for the rule. The 'Log Setting' section has 'Log at Session End' checked. The 'Other Settings' section has 'Schedule' and 'QoS Marking' set to 'None'.

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address
rule1	none	universal	trust	any	any	any	untrust	any

Security Policy Rule

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

Action Setting

Action: **Allow**

☐ Send ICMP Unreachable

Profile Setting

Profile Type: **Profiles**

Antivirus: **default**

Vulnerability Protection: **strict**

Anti-Spyware: **strict**

URL Filtering: **default**

File Blocking: **None**

Data Filtering: **None**

WildFire Analysis: **default**

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: **None**

Other Settings

Schedule: **None**

QoS Marking: **None**

☐ Disable Server Response Inspection

Tag Browser

1 Item

Tag(#)	Rule
none (1)	1

☒ Filter by first tag in rule

☒ Rule Order ☐ Alphabetical

Object: **Addresses**

OK Cancel

Determine Traffic to allow from Untrust Zone to Trust Zone

- Determine Destination IP addresses for all inbound traffic from the untrust Zone
- Create Security policy rule 2 for traffic originating from untrust zone destined for trust zone
 - Add destination IP addresses
 - Add same security profiles as in rule 1
 - Use any for app-id or specify allowed apps (more secure)

Rule2 Source Zone: Untrust

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

☐ Any

☐ Source Zone ▲

☒ untrust

☒ Any

☐ Source Address ▲

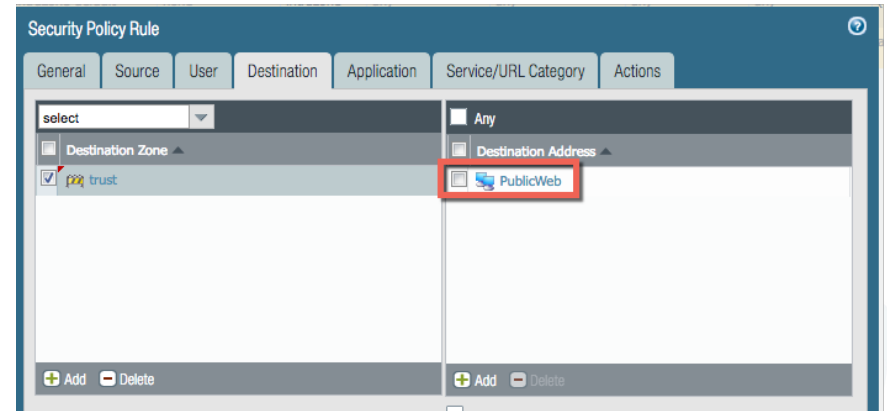
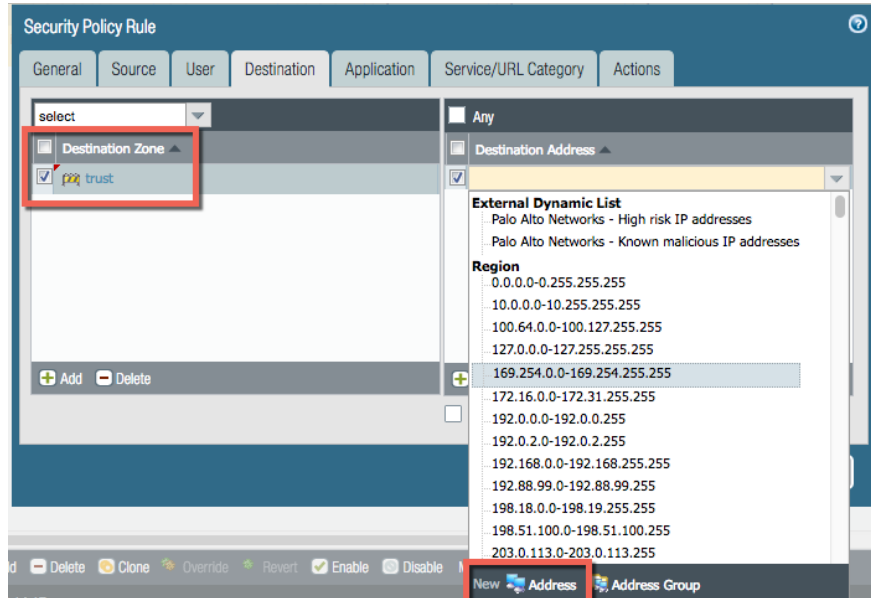
+ Add - Delete

+ Add - Delete

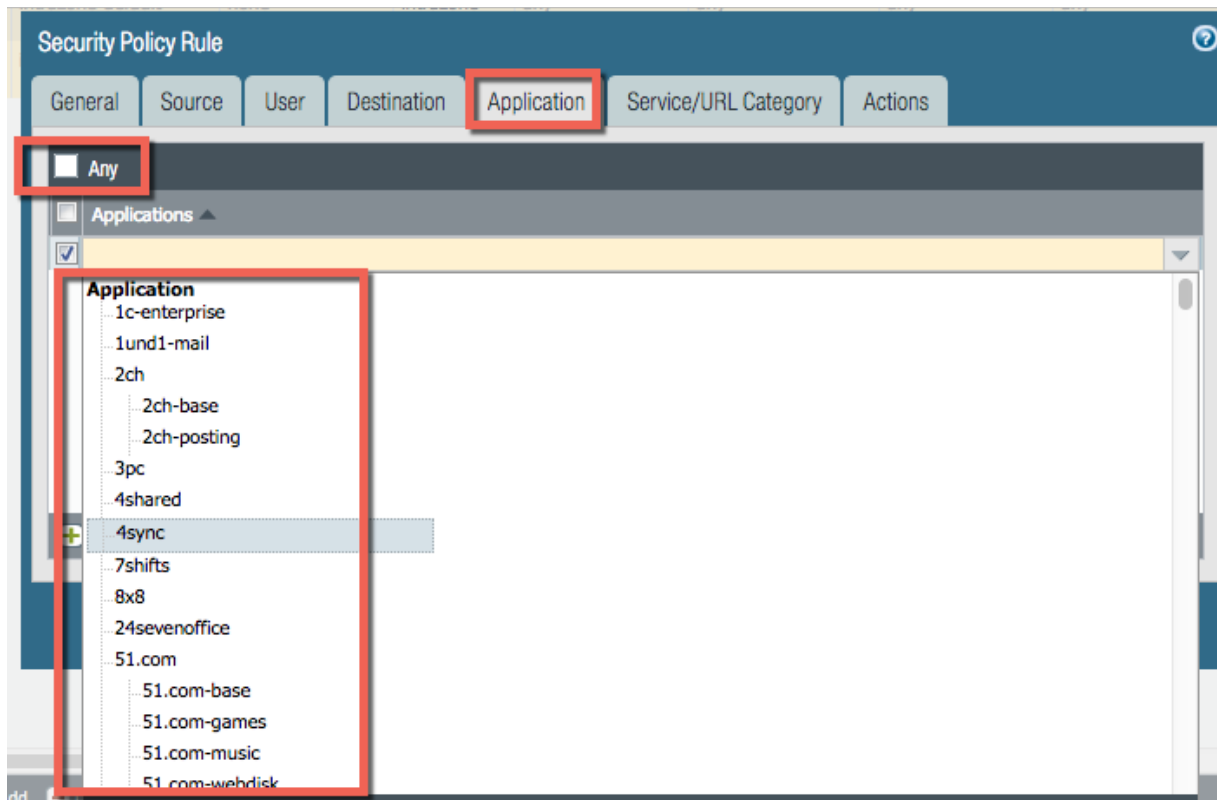
☐ Negate

OK Cancel

Rule Destination Zone: Trust; Destination IP: Your Public Servers



Rule2 Application: Any or Specific App-IDs



Rule2 Service: Application Default

The screenshot displays the 'Security Policy Rule' configuration window. The 'Service/URL Category' tab is selected and highlighted with a red box. Within this tab, the 'application-default' dropdown menu is also highlighted with a red box. Below the dropdown, the 'Service' section is visible with a collapse icon. To the right, the 'URL Category' section is expanded, showing a list with 'Any' selected (checked checkbox). At the bottom of each section are '+ Add' and '- Delete' buttons.

Rule2 Actions: Allow, Security profiles

The screenshot displays the 'Security Policy Rule' configuration window. The 'Actions' tab is selected and highlighted with a red box. Within this tab, the 'Action' dropdown is set to 'Allow' and is also highlighted with a red box. Below the 'Action' dropdown, there is a checkbox for 'Send ICMP Unreachable'. The 'Profile Setting' section is also highlighted with a red box and contains several dropdown menus: 'Profile Type' (set to 'Profiles'), 'Antivirus' (set to 'default'), 'Vulnerability Protection' (set to 'strict'), 'Anti-Spyware' (set to 'strict'), 'URL Filtering' (set to 'default'), 'File Blocking' (set to 'None'), 'Data Filtering' (set to 'None'), and 'WildFire Analysis' (set to 'default'). The 'Log Setting' section includes checkboxes for 'Log at Session Start' (unchecked) and 'Log at Session End' (checked), and a 'Log Forwarding' dropdown set to 'None'. The 'Other Settings' section includes a 'Schedule' dropdown set to 'None', a 'QoS Marking' dropdown set to 'None', and a checkbox for 'Disable Server Response Inspection' (unchecked). At the bottom right, the 'OK' button is highlighted with a red box, and the 'Cancel' button is visible next to it.

Security Policy Rule

General Source User Destination Application Service/URL Category **Actions**

Action Setting

Action **Allow**

☐ Send ICMP Unreachable

Profile Setting

Profile Type **Profiles**

Antivirus **default**

Vulnerability Protection **strict**

Anti-Spyware **strict**

URL Filtering **default**

File Blocking **None**

Data Filtering **None**

WildFire Analysis **default**

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding **None**

Other Settings

Schedule **None**

QoS Marking **None**

☐ Disable Server Response Inspection

OK Cancel

Web-UI: Change Default Policy to log traffic

- Override default policy settings to log traffic at session end

The screenshot displays the Palo Alto Networks Web-UI. At the top, a table lists predefined security policy rules. The rule 'interzone-default' is highlighted with a red box. Below the table, a modal window titled 'Security Policy Rule - predefined' is open, showing the configuration for this rule. The 'General' tab is selected. In the 'Log Setting' section, the 'Log at Session End' checkbox is checked and highlighted with a red box. The 'Action' is set to 'Deny' and the 'Profile Type' is 'None'.

	Name	Tags	Type	Source				Z
				Zone	Address	User	HIP Profile	
1	rule1	none	universal	trust	any	any	any	
2	rule2	none	universal	untrust	any	any	any	
3	intrazone-default	none	intrazone	any	any	any	any	(it
4	interzone-default	none	interzone	any	any	any	any	ar

Security Policy Rule - predefined

General | Actions

Action Setting

Action: Deny

☐ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

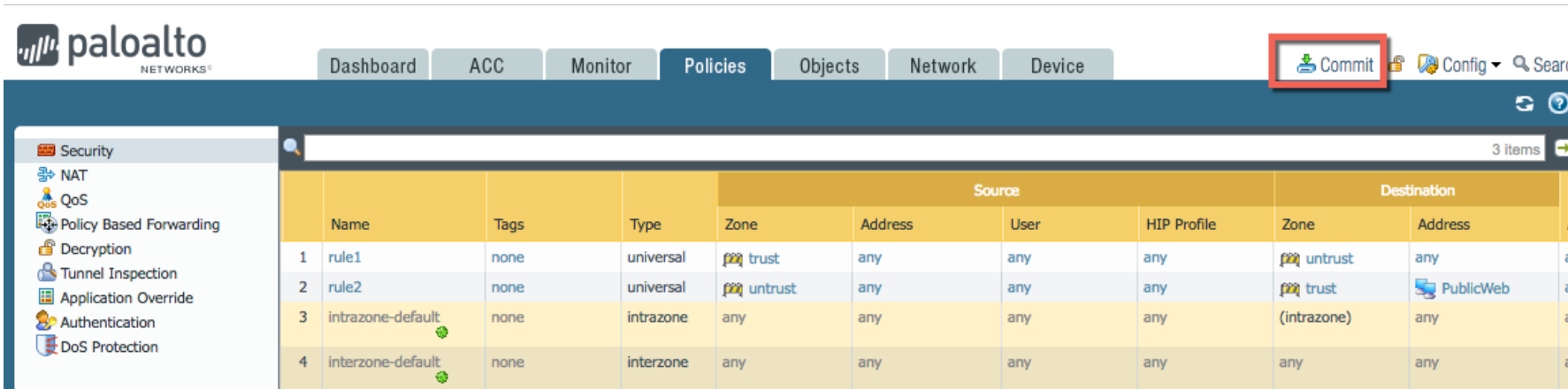
☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

OK Cancel

Commit Changes



The screenshot displays the Palo Alto Networks Security Policy configuration page. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies (selected), Objects, Network, and Device. A red box highlights the 'Commit' button in the top right corner. The left sidebar shows the Security menu with options like NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The main content area shows a table of policies with 3 items. The table has columns for Name, Tags, Type, Source (Zone, Address, User, HIP Profile), and Destination (Zone, Address).

	Name	Tags	Type	Source				Destination	
				Zone	Address	User	HIP Profile	Zone	Address
1	rule1	none	universal	trust	any	any	any	untrust	any
2	rule2	none	universal	untrust	any	any	any	trust	PublicWeb
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
4	interzone-default	none	interzone	any	any	any	any	any	any

PA 3050 Physical vWire Interface Connections

- Connect Ethernet1/1 to network default gateway or switch to default gateway, untrust zone
- Connect Ethernet1/2 to switch connecting all your internal hosts and servers, trust zone
- Use the remaining Interfaces to transition to Layer3 configuration



Web-UI: Examine Logs in Monitor tab

The screenshot displays the Palo Alto Networks Web-UI interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor (highlighted with a red box), Policies, Objects, Network, and Device. On the right of the navigation bar are buttons for Commit, Config, and Search, along with a 'Manual' dropdown menu. The left sidebar shows a 'Logs' section with 'Traffic' highlighted by a red box. Below the sidebar, a table of log entries is visible. The table has columns for Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, and Rule. The log entries show a mix of 'end' and 'deny' types, with 'deny' entries showing a 'reset-both' action.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	02/23 14:03:33	end	untrust	trust	192.168.2.24		192.168.2.60	443	ssl	allow	rule2
	02/23 14:03:33	end	untrust	trust	192.168.2.24		192.168.2.60	443	ssl	allow	rule2
	02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzone
	02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzone
	02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzone
	02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzone
	02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzone
	02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzone

Transition to Layer 3 Configuration





- Your network is protected as you use the PA-3050 other interfaces to migrate to Layer 3 configuration
- Using Layer 3 interfaces might allow you to segment your traffic and have multiple zones
 - This might be harder to do if competition rules don't allow you to change host/server addresses, iptables NAT on a host might help
- Using Layer 3 you can set up site-site VPNs and Client VPN concentrator

Firewall Best Practices

1. Complete visibility of traffic

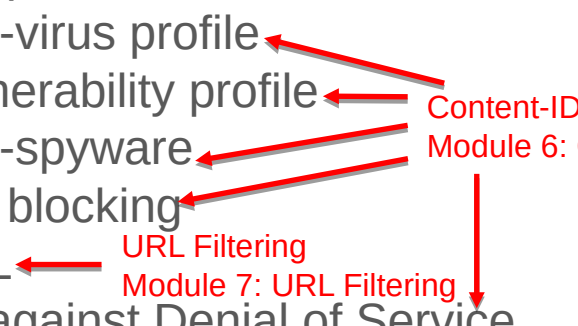
- Know applications to allow
 - Custom Apps
- SSL Decryption  Decryption
Module 8: Decryption
- User-ID  User-ID
Module 10: Basic User-ID

2. Reduce attack surface area

- Whitelist Applications  App-ID
- Creating Custom App-ID's  Module 5: App-ID
- Dynamic address lists and groups 
- SSL Protocol Settings  Reject bad certificates
Module 8: Decryption

Firewall Best Practices (continued)

3. Protect against known attacks

- Assign security profiles to firewall security policies
 - Anti-virus profile
 - Vulnerability profile
 - Anti-spyware
 - File blocking
 - URL
 - Protect against Denial of Service
 - Zone protection profile
 - DoS Profile
- 
- Content-ID
Module 6: Content-ID
- URL Filtering
Module 7: URL Filtering

4. Protect against unknown attacks

- WildFire ← WildFire
Module 9: App-ID

Extending firewall's protection, hot standby firewall, logging and reports

- Firewall Client VPNs ← Client VPNs
Module 11: GlobalProtect
- Firewall Site-to-Site VPNs ← Site-to-Site VPN
Module 12: Site-to-Site VPN
- Firewall logs and reports ← Logs and reports
Module 13: Monitoring and Reporting
- Hot standby back-up Firewall ← Backup Firewall
Module 14: Active/Passive High Availability