Hardware Appliance Deployment

Option 1

paloalto NETWORKS®
the enterprise security company™

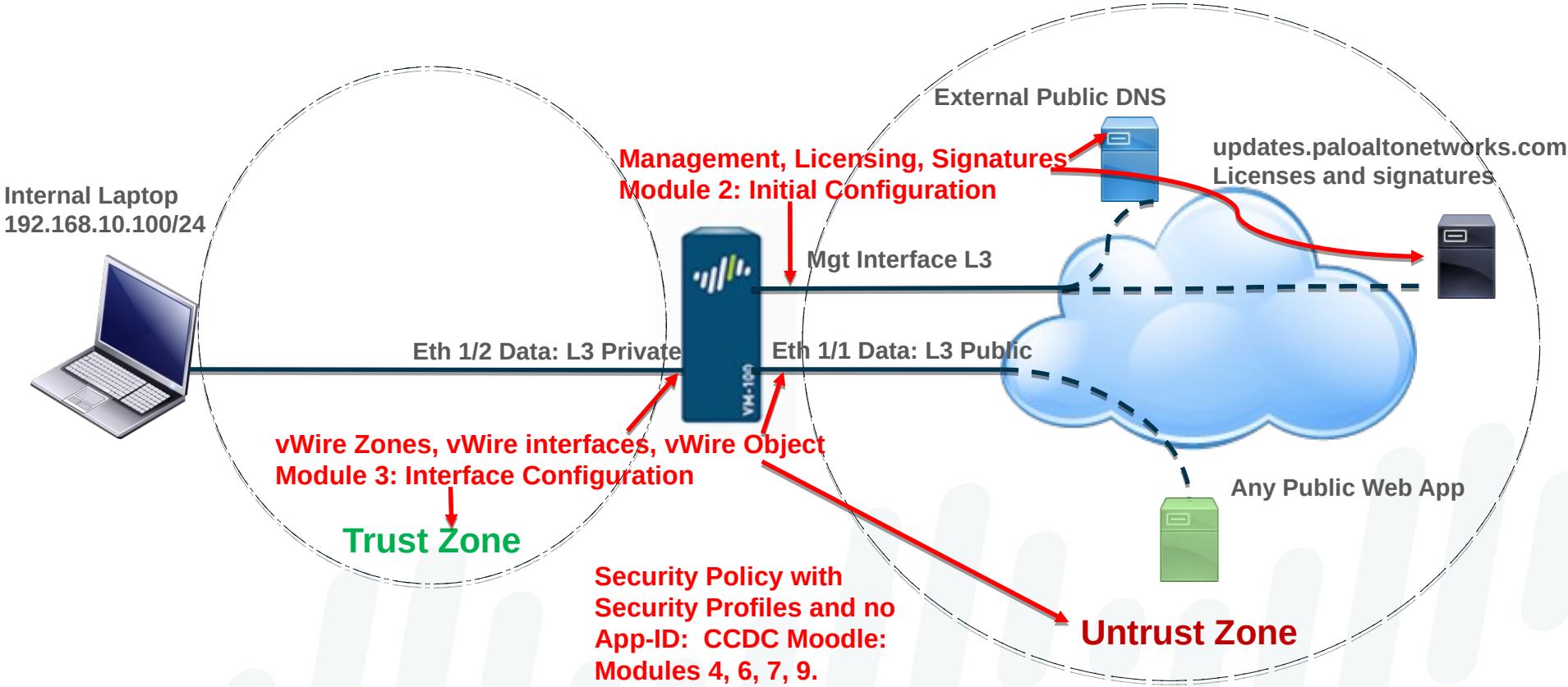
Team Hardware Firewall Appliances at CCDC

- 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-Access-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

USB-Serial Controller — 80x24 — 9600.8.N.1

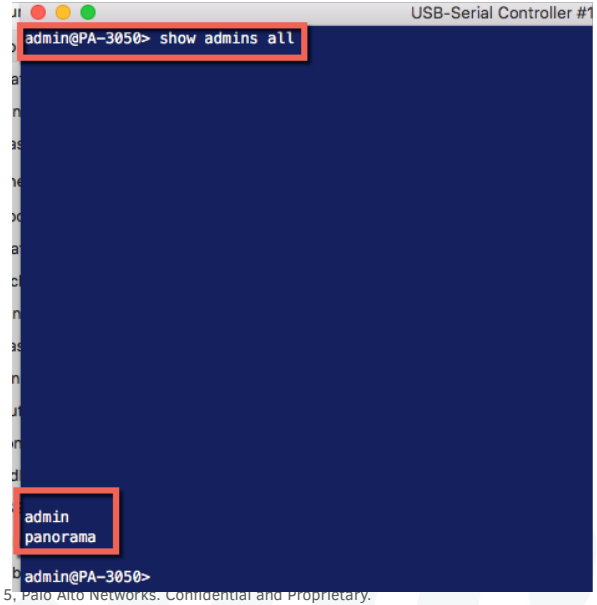
```
Warning: Your device is still configured with the default admin account credenti
als. Please change your password prior to deployment.
admin@PA-3050> show system info

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 acess

Check PANOS version and Licenses

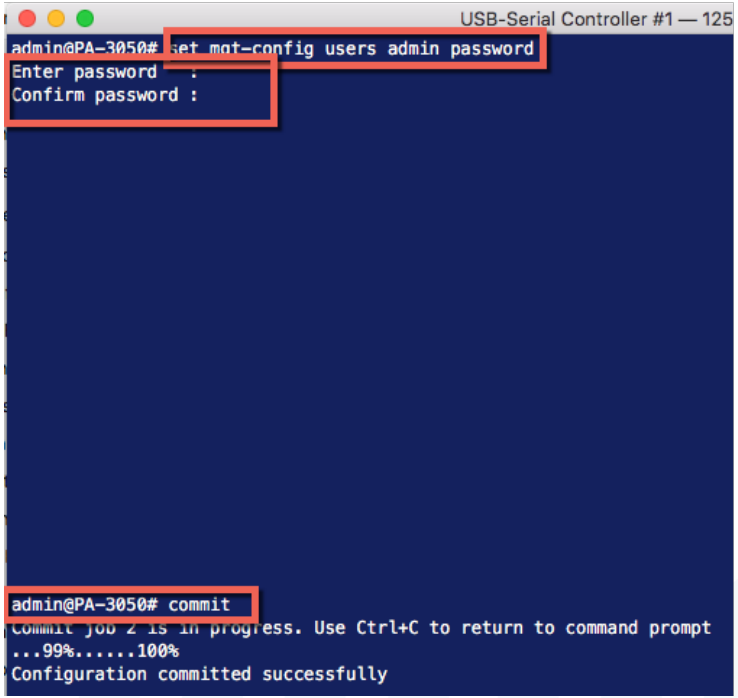
Secure appliance: Show all admin accounts

- 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



Secure appliance: change default admin password

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



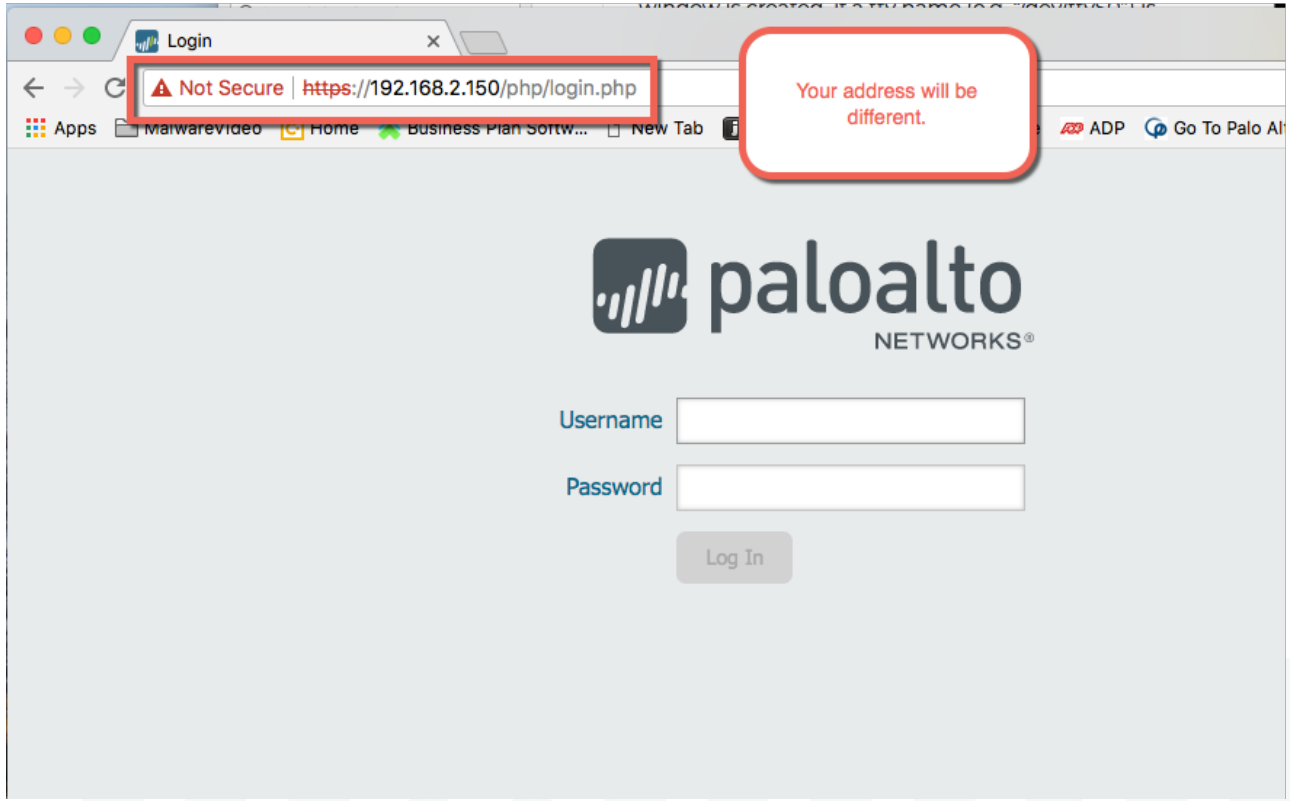
Configure mgt interface IP address and connect it

- 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

PA-3050

Not Secure | https://192.168.2.150/#device::vsys1::device/licenses

Apps | MalwareVideo | Home | Business Plan Softw... | New Tab | Get Started | Main | AdminSite | ADP | Go To Palo Alto Net... | Other Bookmarks

paloalto NETWORKS

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit | Config | Search | Help

- Certificate Profile
- OCSP Responder
- SSL/TLS Service Profile
- SCEP
- SSL Decryption Exclusion
- Response Pages
- Log Settings
- Server Profiles
  - SNMP Trap
  - Syslog
  - Email
  - HTTP
  - Netflow
  - RADIUS
  - TACACS+
  - LDAP
  - Kerberos
  - SAML Identity Provider
  - Multi Factor Authentication
- Local User Database
  - Users
  - User Groups
- Scheduled Log Export
- Software
- GlobalProtect Client
- Dynamic Updates
- Licenses
- Support
- Master Key and Diagnostics

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

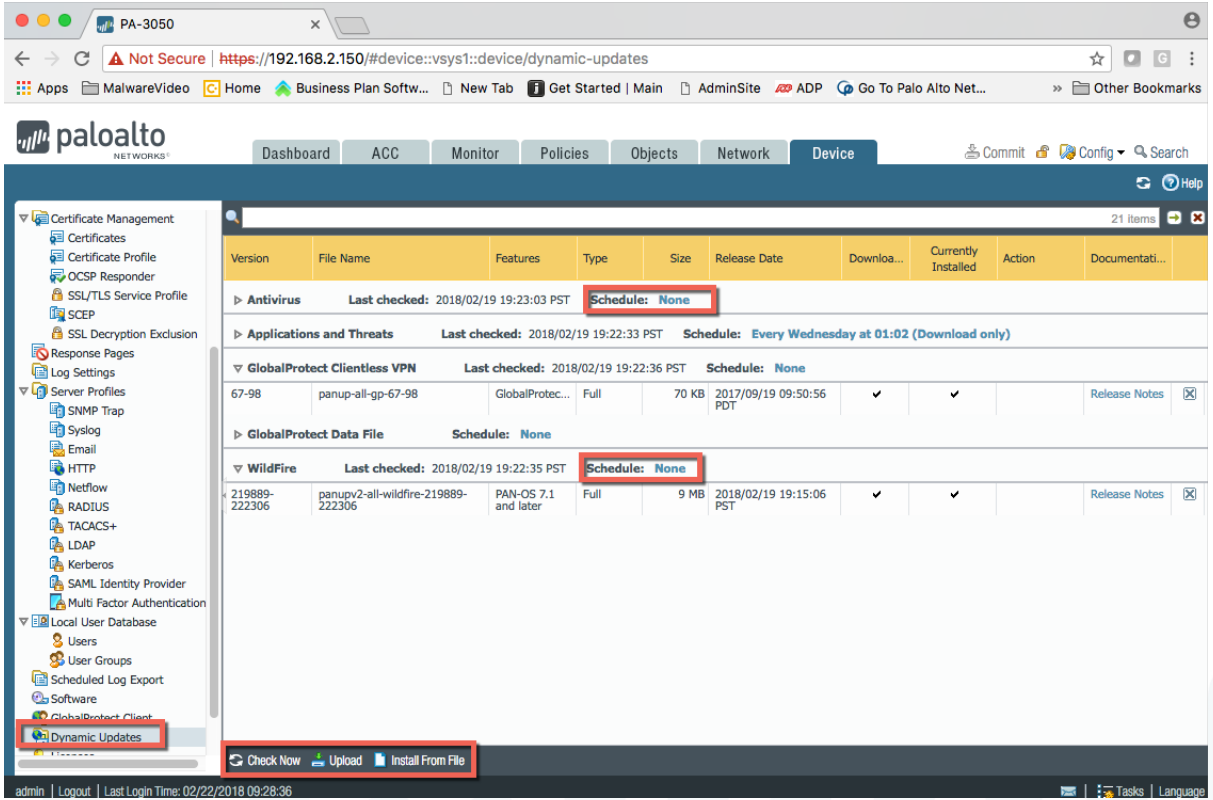
WildFire License

Date Issued	February 19, 2018
Date Expires	April 19, 2018
Description	WildFire signature feed, integrated WildFire logs, WildFire API

admin | Logout | Last Login Time: 02/22/2018 09:28:36 | Tasks | Language

paloalto NETWORKS

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



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

PA-3050

Not Secure | https://192.168.2.150/#device::vsys1::device/setup

Apps | MalwareVideo | Home | Business Plan Softw... | New Tab | Get Started | Main | AdminSite | ADP | Go To Palo Alto Net... | Other Book

paloalto NETWORKS

Dashboard | ACC | Monitor | Policies | Objects | Network | Device | Commit | Config | Se

- Setup
- High Availability
- Config Audit
- Password Profiles
- Administrators
- Admin Roles
- Authentication Profile
- Authentication Sequence
- User Identification
- VM Information Sources
- Certificate Management
  - Certificates
  - Certificate Profile
  - OCSP Responder
  - SSL/TLS Service Profile
  - SCEP
  - SSL Decryption Exclusion
- Response Pages
- Log Settings
- Server Profiles
  - SNMP Trap

Management | Operations | Services | Interfaces | Telemetry | Content-ID | WildFire | Session | HSM

General Settings

Hostname	PA-3050
Domain	
Login Banner	
Force Admins to Acknowledge Login Banner	☐
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	☐
Certificate Expiration Check	☐
Multi Virtual System Capability	☐

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	

Banners and Messages

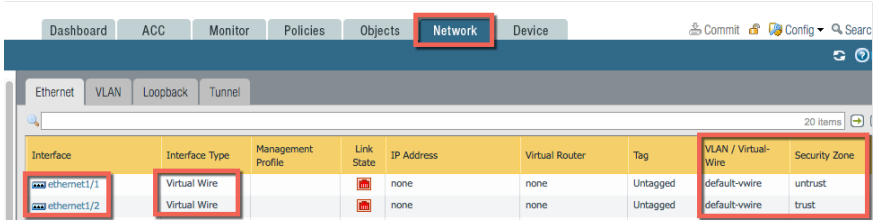
Message of the Day	
Allow Do Not Display Again	☐
Title	Message of the Day
Background Color	
Icon	
Header Banner	
Header Color	

Authentication Settings

paloalto NETWORKS

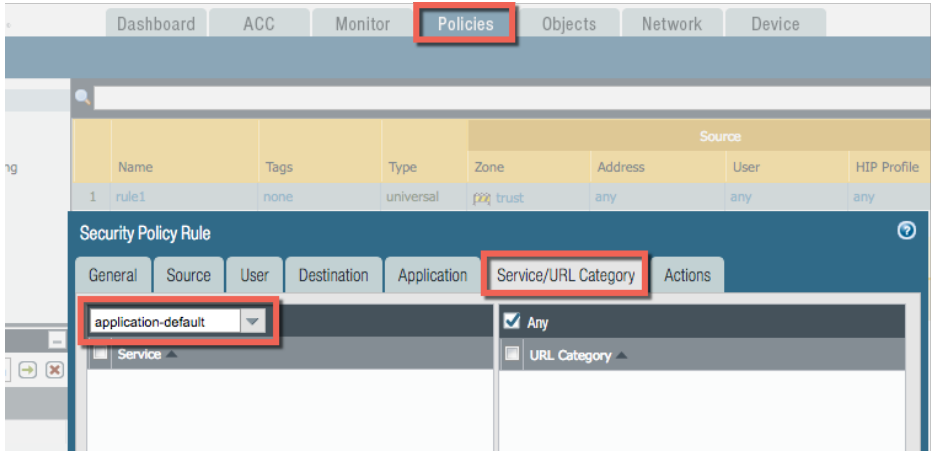
Web UI: PA 3050 Pre-Configured for Quick vWire Deployment

- 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

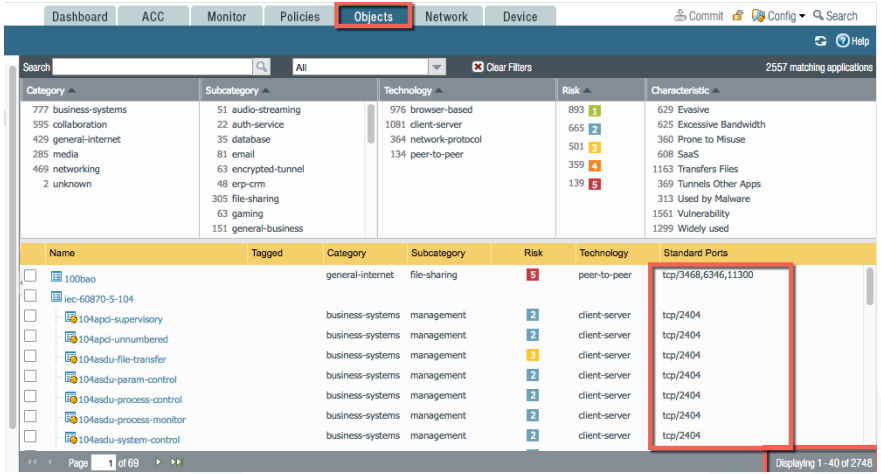


Web-UI Modify Rule1 : Change Services from any to application default

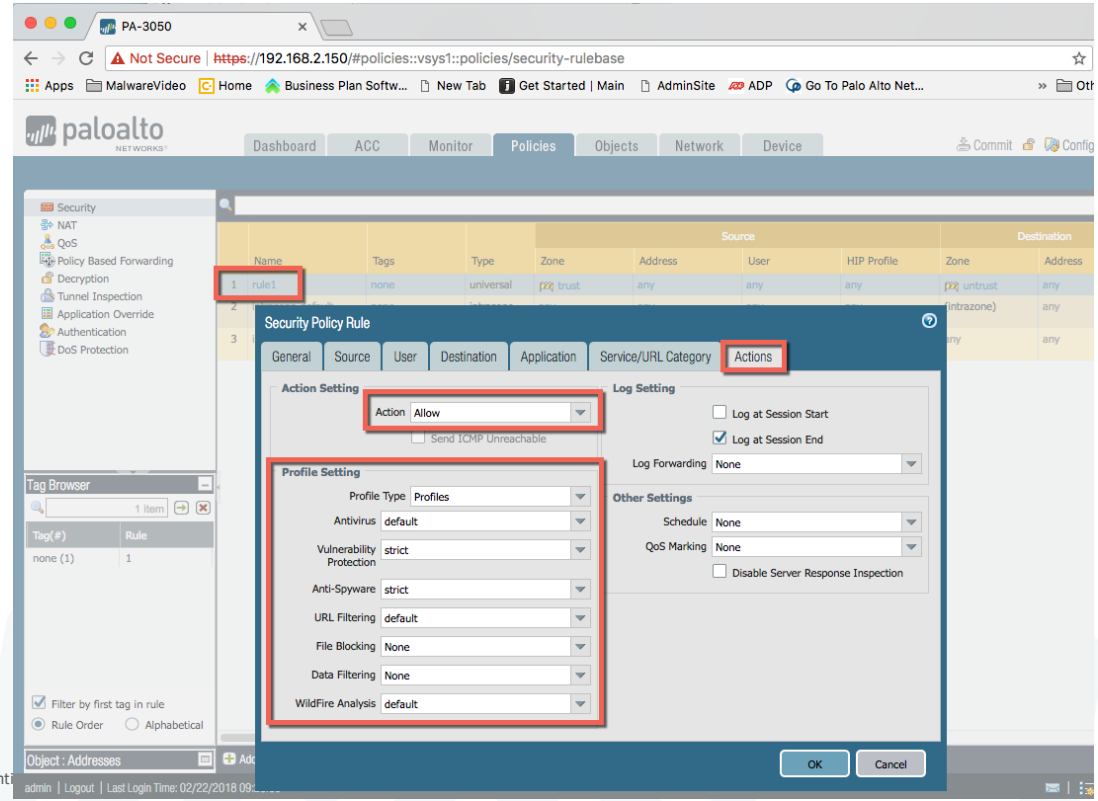
Will block sessions using ports that aren't assigned to an application ID in Objects tab>Applications



Firewall Application IDs



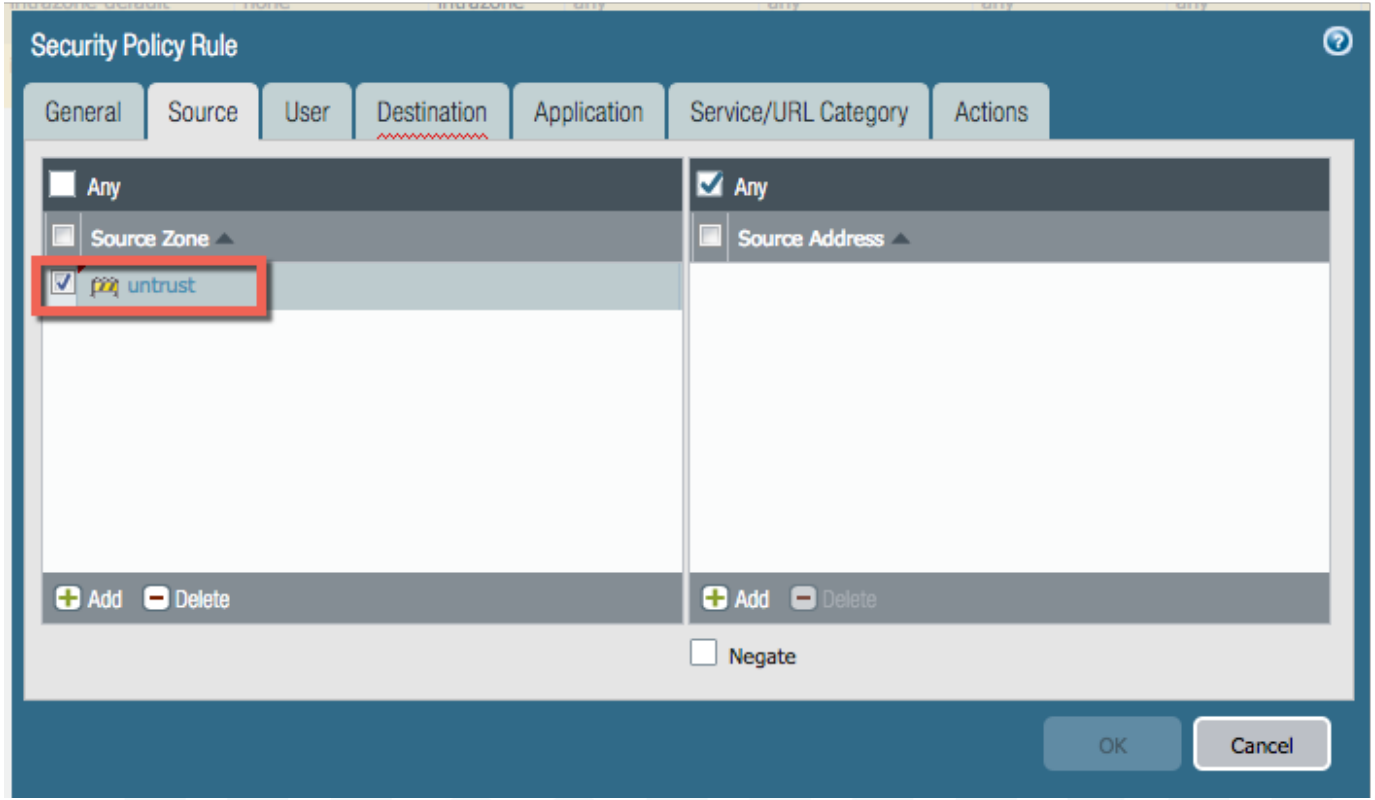
Web-UI Modify Rule1 : Add Security Profiles



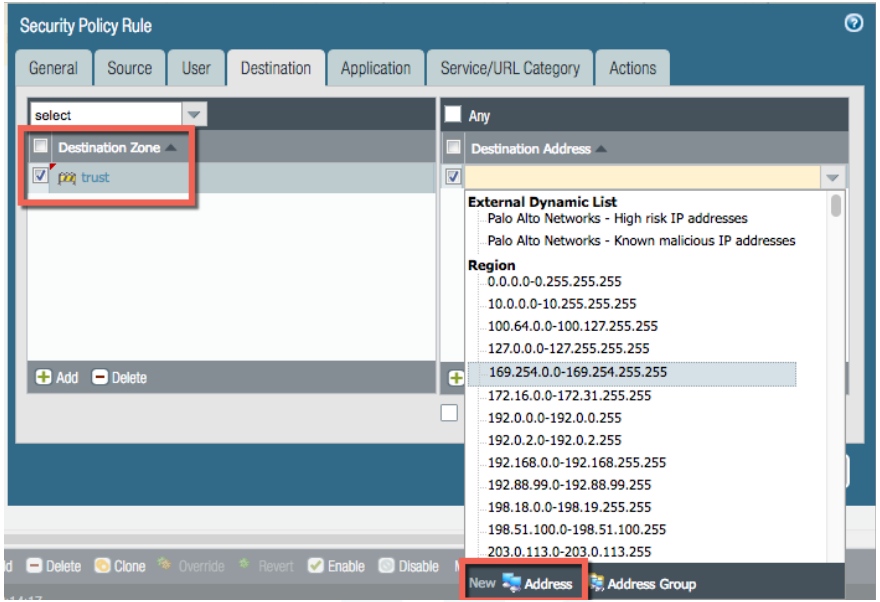
Determine Traffic to allow from Untrust Zone to Trust Zone

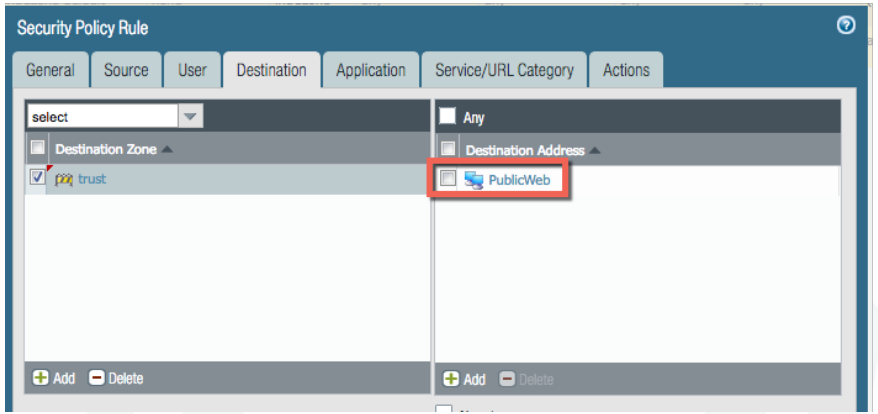
- Determine Destination IP addresses for all inbound traffic from the untrust Zone
- Create Security policy rule 2 for traffic originating from untrust zone destined for trust zone
  - Add destination IP addresses
  - Add same security profiles as in rule 1
  - Use any for app-id or specify allowed apps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

Rule2 Source Zone: Untrust

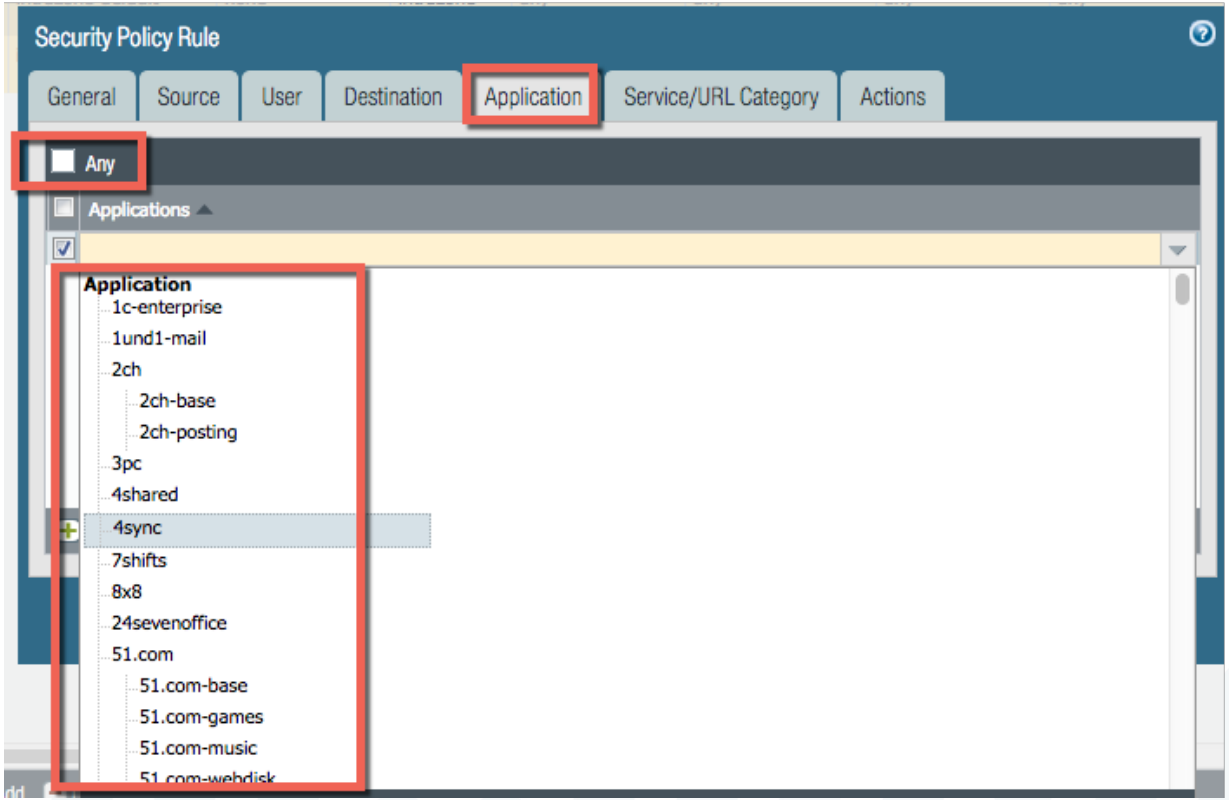


Rule Destination Zone: Trust; Destination IP: Your Public Servers

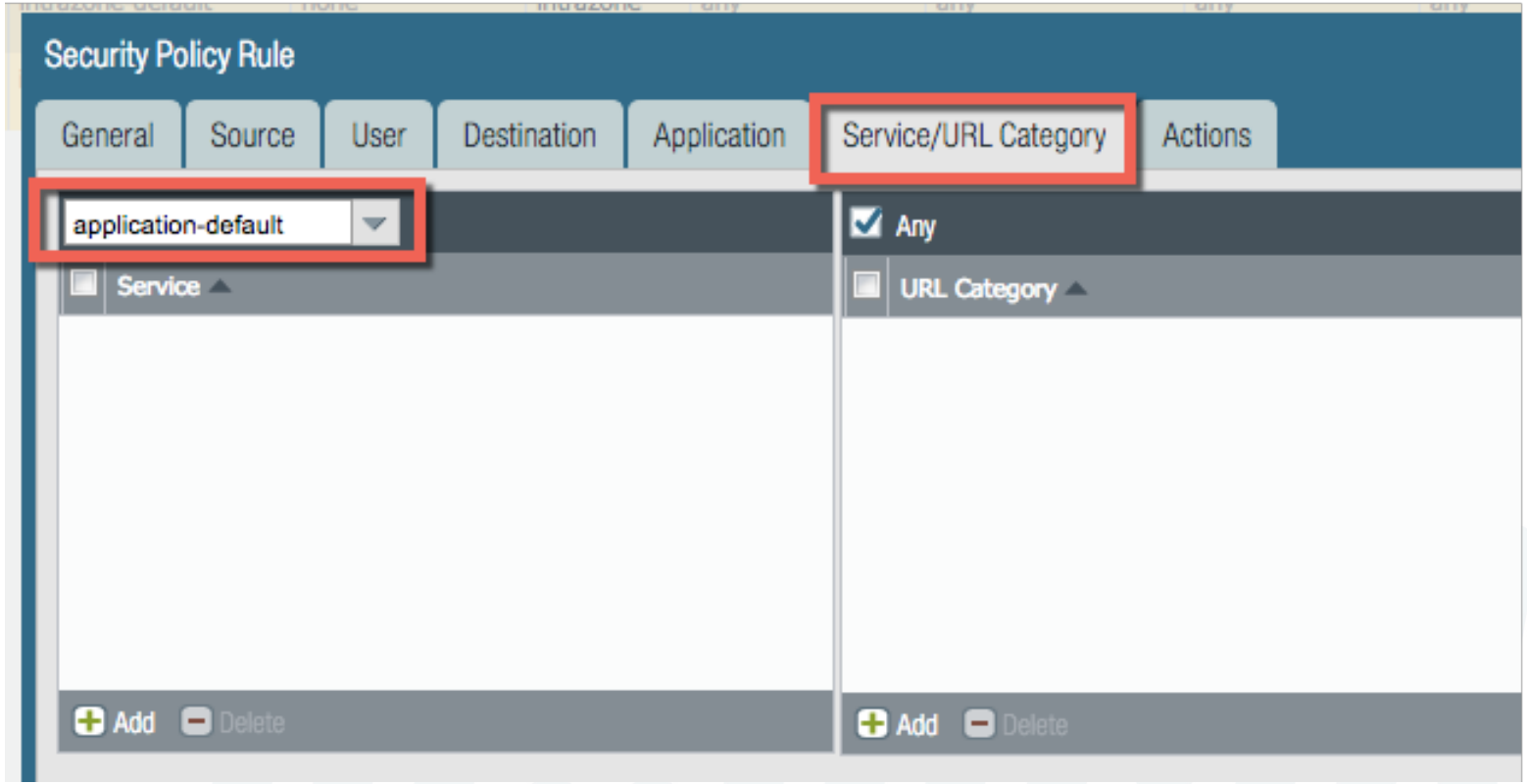




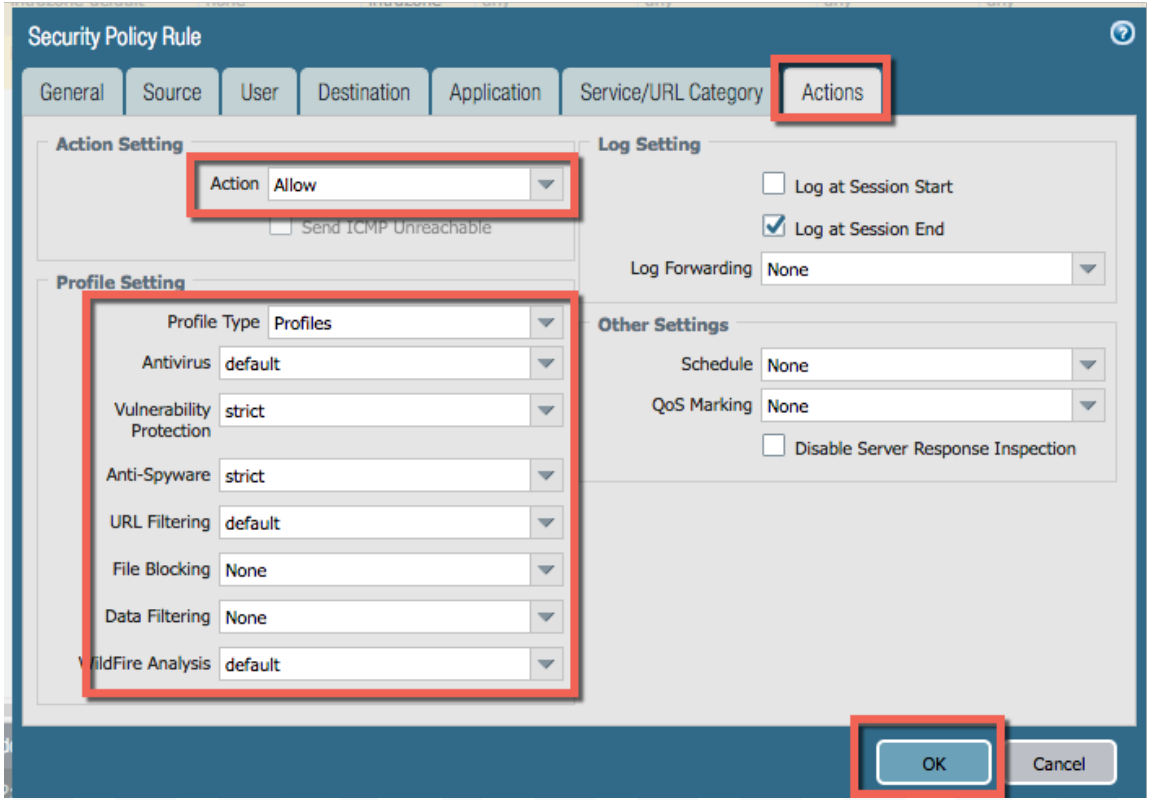
Rule2 Application: Any or Specific App-IDs



Rule2 Service: Application Default

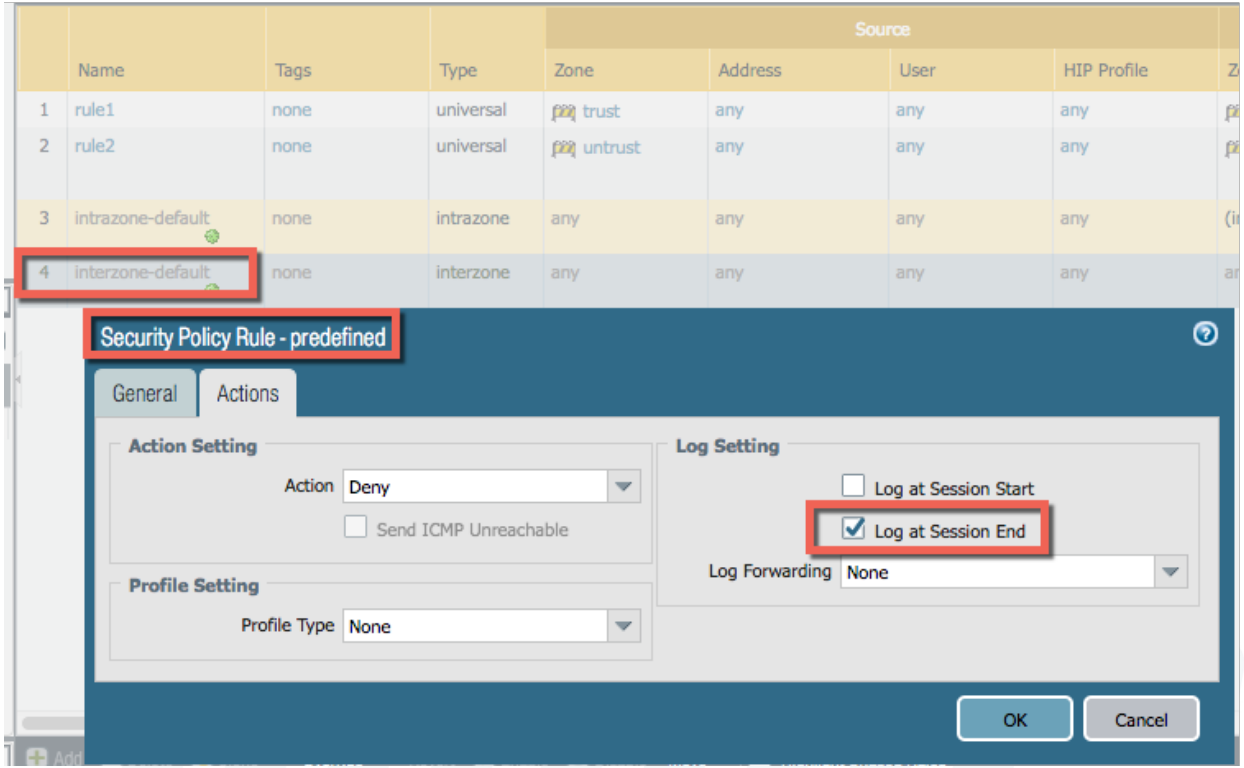


Rule2 Actions: Allow, Security profiles

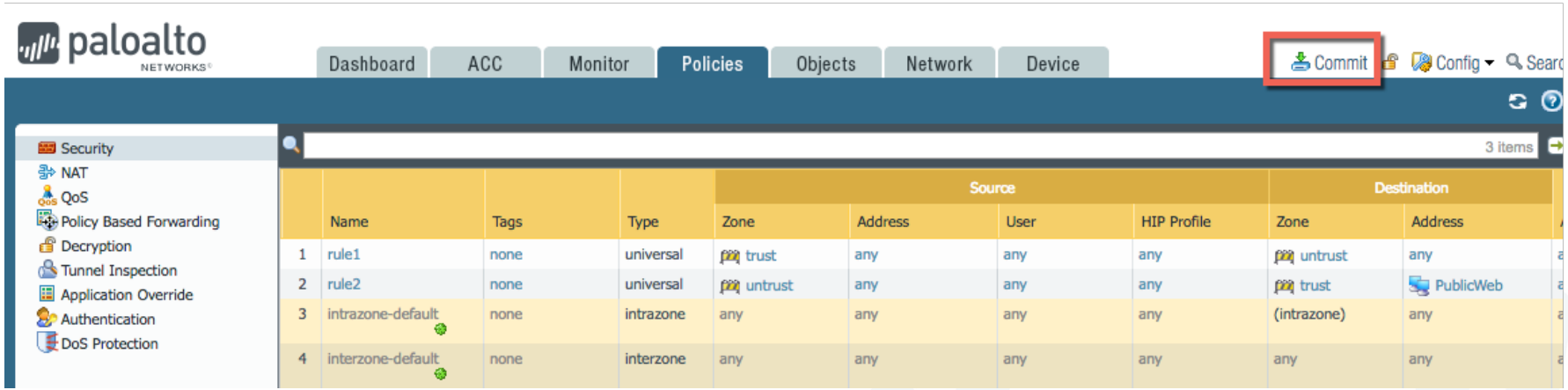


Web-UI: Change Default Policy to log traffic

- Override default policy settings to log traffic at session end



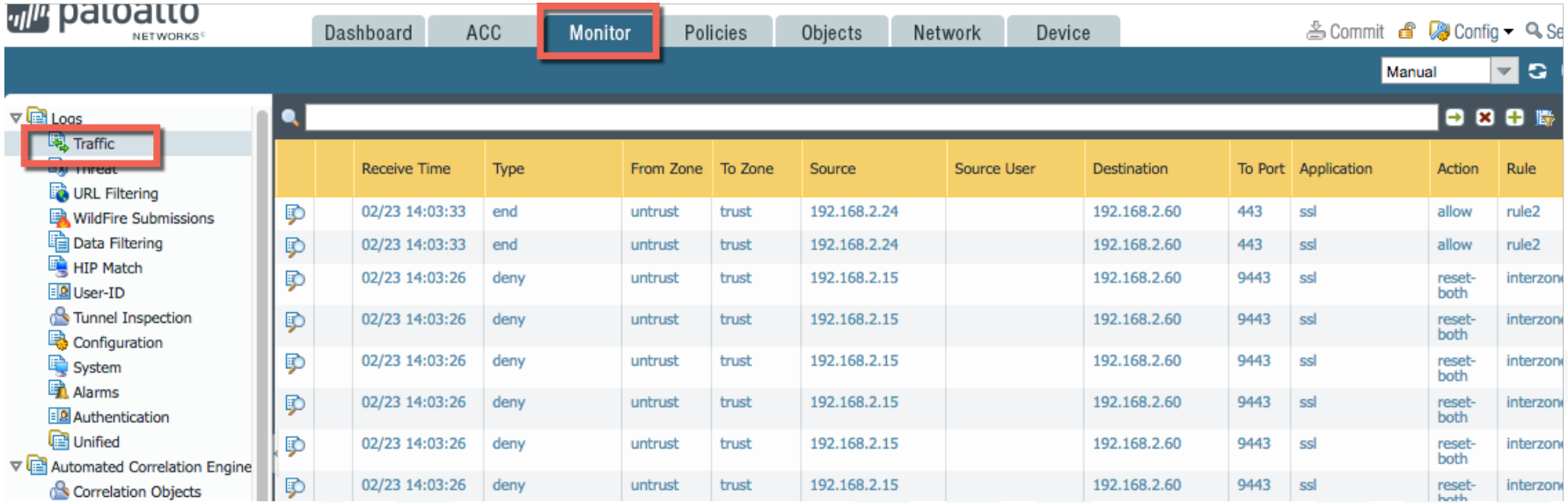
Commit Changes



PA 3050 Physical vWire Interface Connections

- Connect Etherent1/1 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



		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	interzon
		02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzon
		02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzon
		02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzon
		02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzon
		02/23 14:03:26	deny	untrust	trust	192.168.2.15		192.168.2.60	9443	ssl	reset-both	interzon

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
- User-ID

Decryption
Module 8: Decryption

User-ID
Module 10: Basic User-ID

2. Reduce attack surface area

- Whitelist Applications
- Creating Custom App-ID's
- Dynamic address lists and groups
- SSL Protocol Settings

App-ID
Module 5: App-ID

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

