CCDC Quick Start Guide for PA 3050 Deployment and Configuration

Also can be used for virtual firewall appliances

Jim Boardman

paloalto NETWORKS®

the enterprise security company™

Quick Start Critical Steps to Secure and Deploy Your Firewall Appliance to Protect Your Network

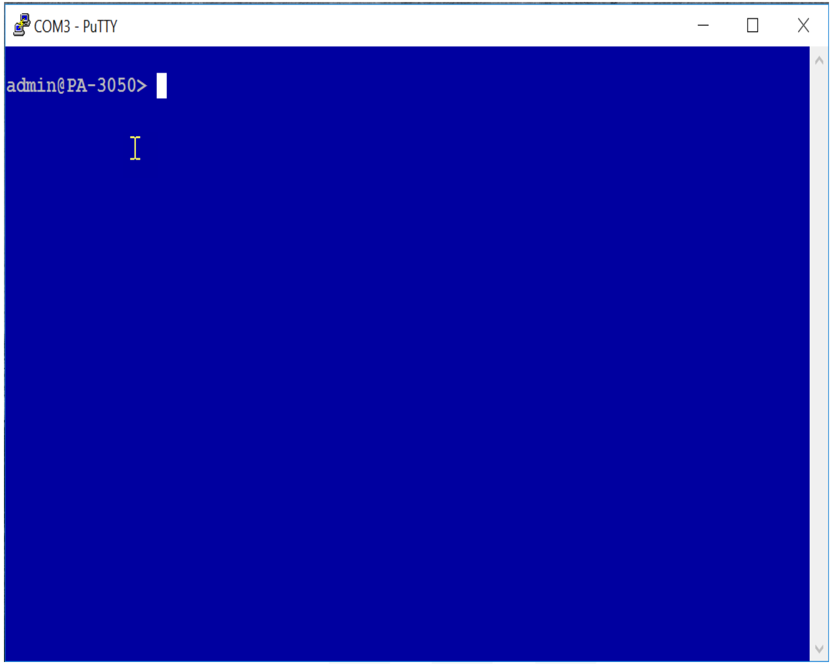
1. Secure your firewall appliance and your firewall appliance's management interface
   - By default your firewall management's interface requires Internet access to license the Firewall and retrieve the latest malware signatures
2. License your firewall appliance
3. Download the latest malware signatures for your firewall appliance
4. Determine and configure your network deployment for firewall appliance (Vwire, Layer2, Layer3)
5. Configure security policies and assign security profiles to your security policies
6. Turn on the full power of the firewall with WebUI and Best Practices
7. Dig into the CCDC2020 Moodle course to learn about configuring: decryption, zone protection, DoS policies, VPNs and User-ID to protect your network(s)

Step 1:
Secure your firewall appliance and your firewall appliance’s management interface

© 2015, Palo Alto Networks. Confidential and Proprietary.

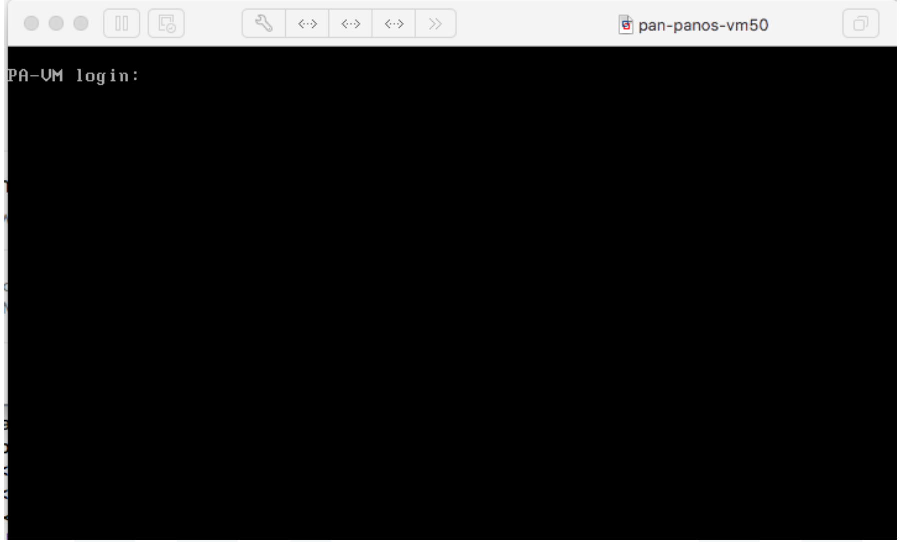
Securing Your FW Appliance: Access VM-100 Console via hypervisor and or PA 3050 Serial Port

- PA 3050 Console Port



```
admin@PA-3050>
```

- Hypervisor Console Port



```
PA-VM login:
```

© 2015, Palo Alto Networks. Confidential and Proprietary.

Securing Your Firewall Interface: Connecting to Your PA 3050 Console Serial Settings

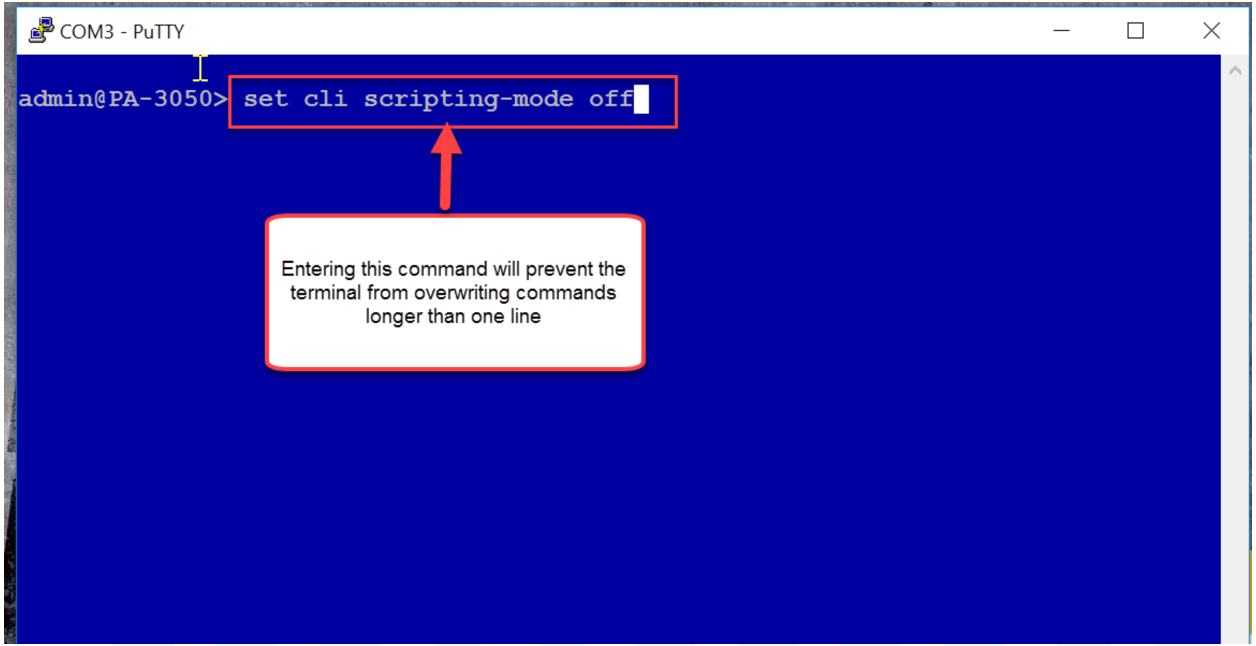
- Very important that your serial settings are correct to access console port
- The settings in the Hyper Terminal need to be set correctly; otherwise, no access or garbage characters may show up on the screen. When setting up the connection, use these settings:
  - Bits per sec : 9600
  - Data bits : 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/

- If connecting to PA 3050 console from Linux client use "screen" , sudo apt-get install screen
- Enter following command in Linux terminal to connect to FW console: **sudo screen /dev/ttyUSB0 9600,cs8,-ixon,ixoff**
- **Ctl + L to clear screen on console**

© 2015, Palo Alto Networks. Confidential and Proprietary.

Securing Your Firewall Appliance: Connect to Your PA 3050 – Turn off Scripting Mode

- Turning off scripting mode in console operations mode: > set cli scripting-mode off



```
admin@PA-3050> set cli scripting-mode off
```

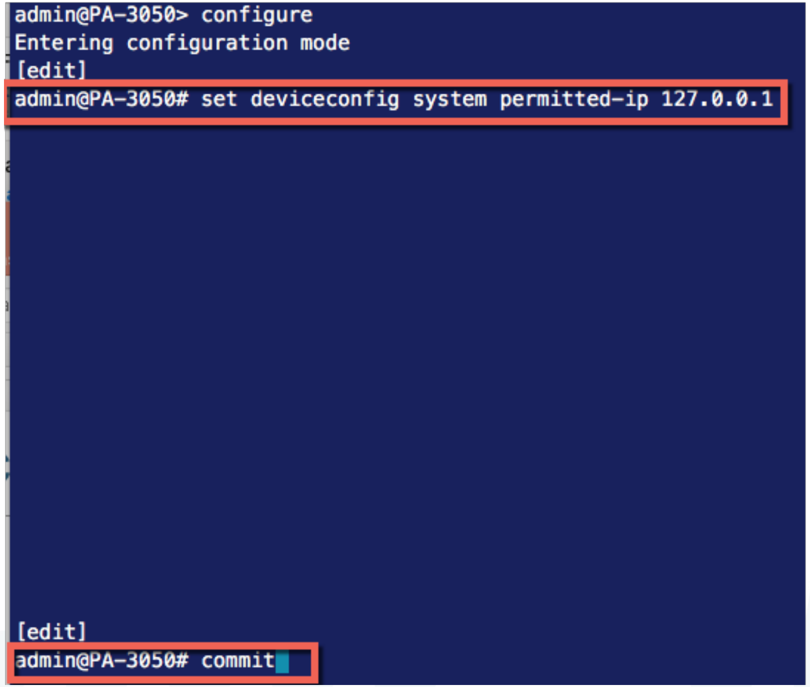
Entering this command will prevent the terminal from overwriting commands longer than one line

© 2015, Palo Alto Networks. Confidential and Proprietary.

Securing Your FW Appliance: Turn Off Management Interface Temporarily - You Don’t Know Who Is Accessing It

- Configure Mode **#set deviceconfig system permitted-ip 127.0.0.1**

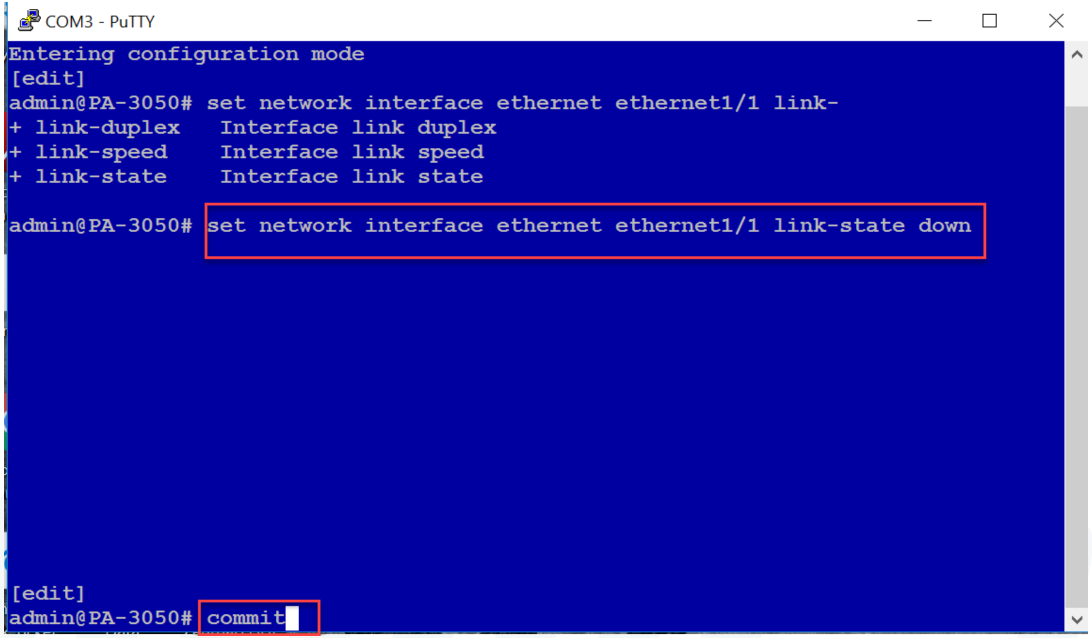
  #Commit



```
admin@PA-3050> configure
Entering configuration mode
[edit]
admin@PA-3050# set deviceconfig system permitted-ip 127.0.0.1









[edit]
admin@PA-3050# commit
```

Securing Your FW Appliance: Turn Off Data Interfaces Temporarily if connected – Red Team Could Be Managing FW Via Data Interface

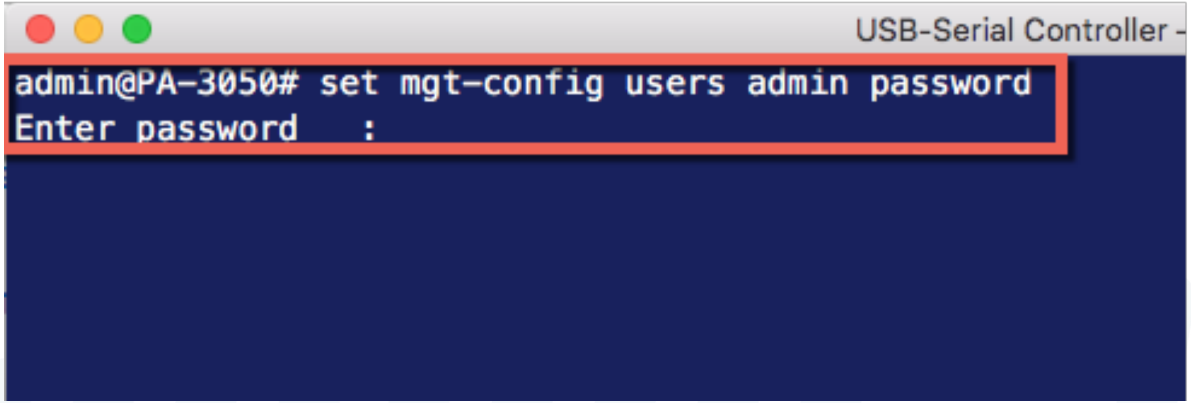
- Configure Moode #**set network interface ethernet ethernet1/x link-state down**
- **#commit**



```
Entering configuration mode
[edit]
admin@PA-3050# set network interface ethernet ethernet1/1 link-
+ link-duplex    Interface link duplex
+ link-speed     Interface link speed
+ link-state     Interface link state

admin@PA-3050# set network interface ethernet ethernet1/1 link-state down




















[edit]
admin@PA-3050# commit
```

Securing Your FW Appliance: Change Your Admin Password

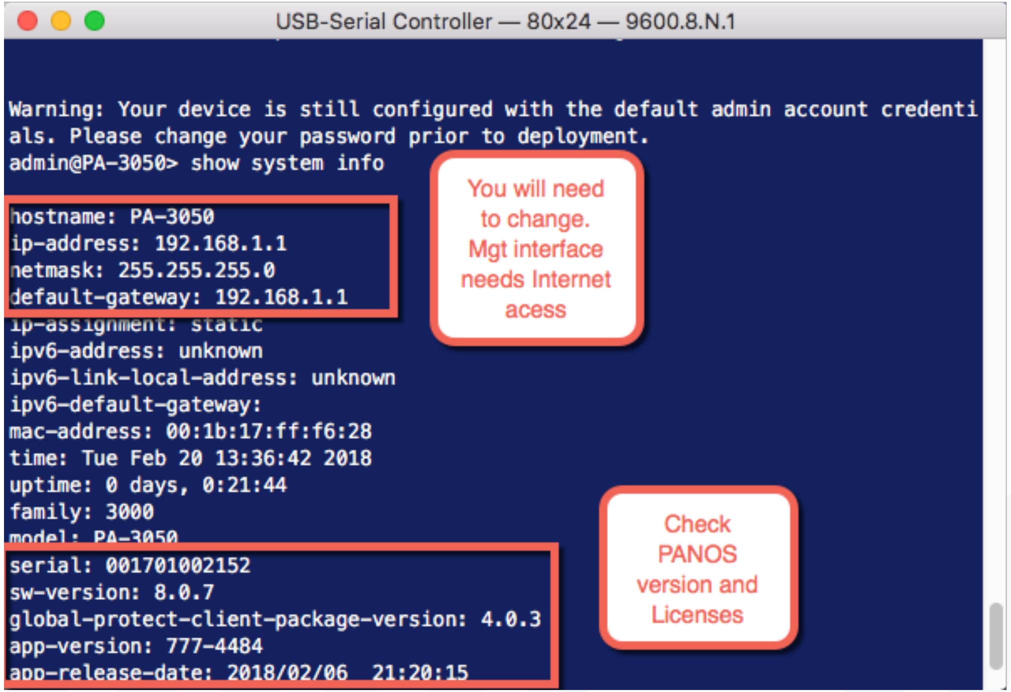
- Change default admin password
  - Operations Mode > **configure**
  - Configure Mode # **set mgt-confg users admin password <new password>**
  - Consider using ssh key for authentication
    - **https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-ssh-key-based-administrator-authentication-to-the-cli**



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

Securing Your FW Appliance: Review System Info

- General system info
  - Operations Mode> **show system info**



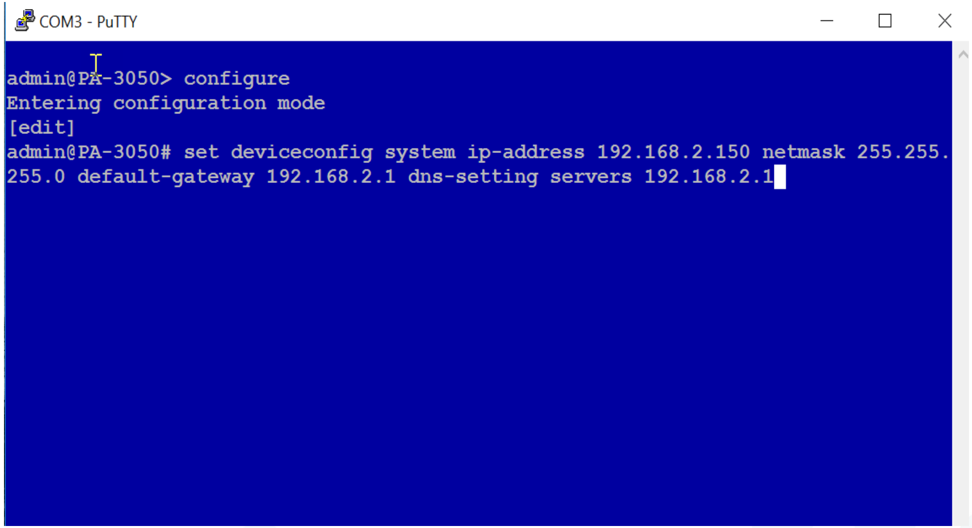
```
Warning: Your device is still configured with the default admin account credenti
als. Please change your password prior to deployment.
admin@PA-3050> show system info

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

Securing Your FW Appliance: Change Management Interface IP Address If Required

- Changing Mgt Interface IP Address
  - Configure Mode: **#set deviceconfig system ip-address x.x.x.x netmask x.x.x.x default-gateway x.x.x.x dns-setting servers primary x.x.x.x**
- Enter command “**commit**” to commit changes to running configuration
- Configure an IP address, default gateway and preferred DNS that will allow Internet access

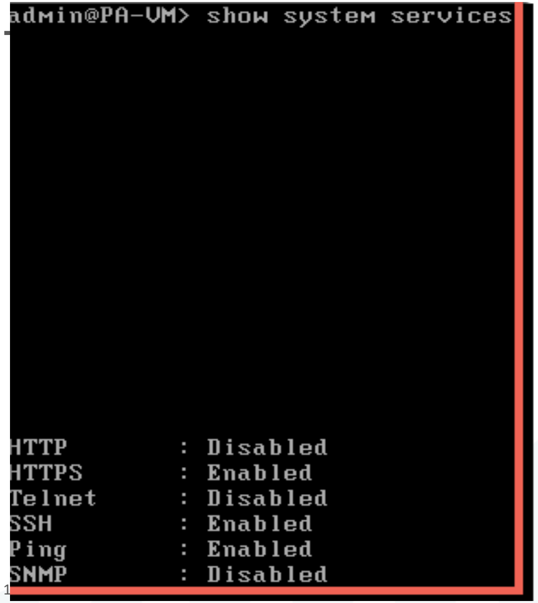


```
admin@PA-3050> configure
Entering configuration mode
[edit]
admin@PA-3050# set deviceconfig system ip-address 192.168.2.150 netmask 255.255.
255.0 default-gateway 192.168.2.1 dns-setting servers 192.168.2.1
```

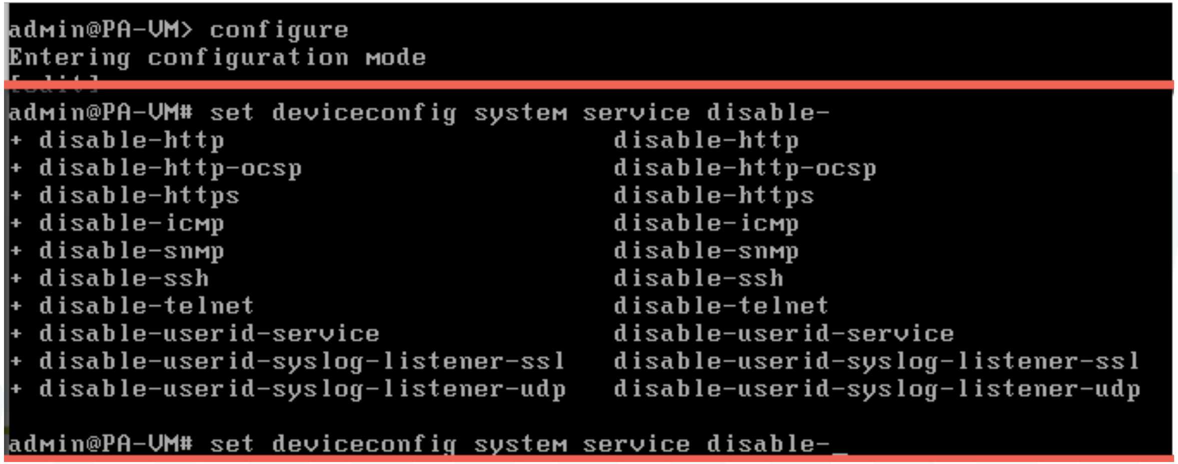
© 2015, Palo Alto Networks. Confidential and Proprietary.

Securing FW Appliance: Only Allow Secure Protocols To Connect to Mgt Interface

- Secure your management interface for allowed services
  - Only allow secure services: ssh, https, ping (for troubleshooting)
  - Configure mode: **#set deviceconfig system service disable-https no**
    #commit



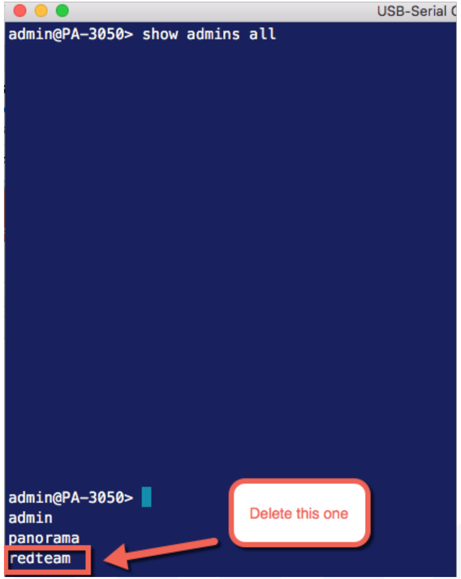
```
admin@PA-VM> show system services









HTTP         : Disabled
HTTPS        : Enabled
Telnet       : Disabled
SSH          : Enabled
Ping         : Enabled
SNMP         : Disabled
```



```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set deviceconfig system service disable-
+ disable-http                          disable-http
+ disable-http-ocsp                     disable-http-ocsp
+ disable-https                         disable-https
+ disable-icmp                          disable-icmp
+ disable-snmp                          disable-snmp
+ disable-ssh                           disable-ssh
+ disable-telnet                        disable-telnet
+ disable-userid-service                disable-userid-service
+ disable-userid-syslog-listener-ssl    disable-userid-syslog-listener-ssl
+ disable-userid-syslog-listener-udp    disable-userid-syslog-listener-udp

admin@PA-VM# set deviceconfig system service disable-_
```

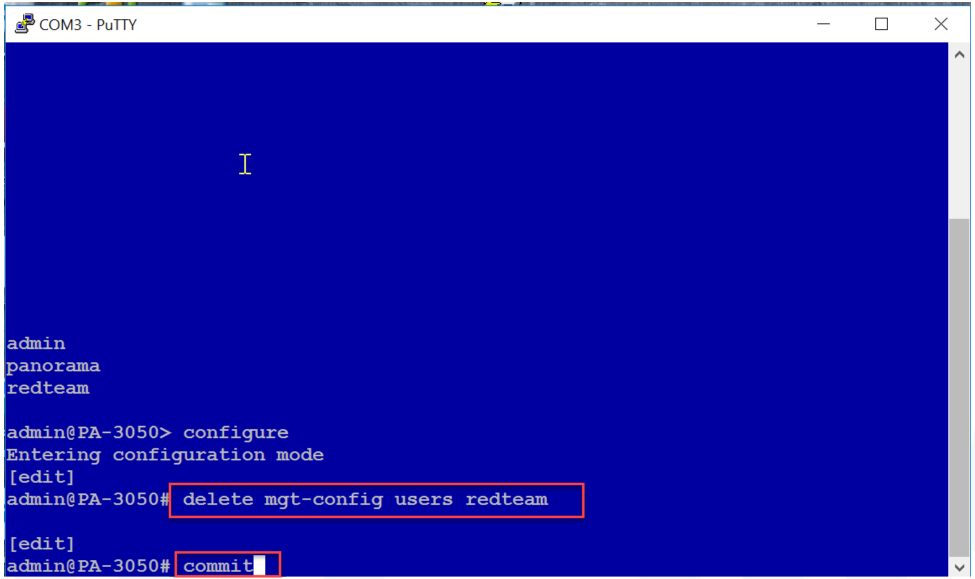
Secure FW Appliance: Show all Admin Accounts

- You want to make sure there are only two admin accounts unless directed otherwise: (admin and panorama - - default configuration)
  - **> show admins all**
  - **# delete mgt-config users redteam and # commit**



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




admin@PA-3050> 
admin
panorama
redteam
```

Delete this one

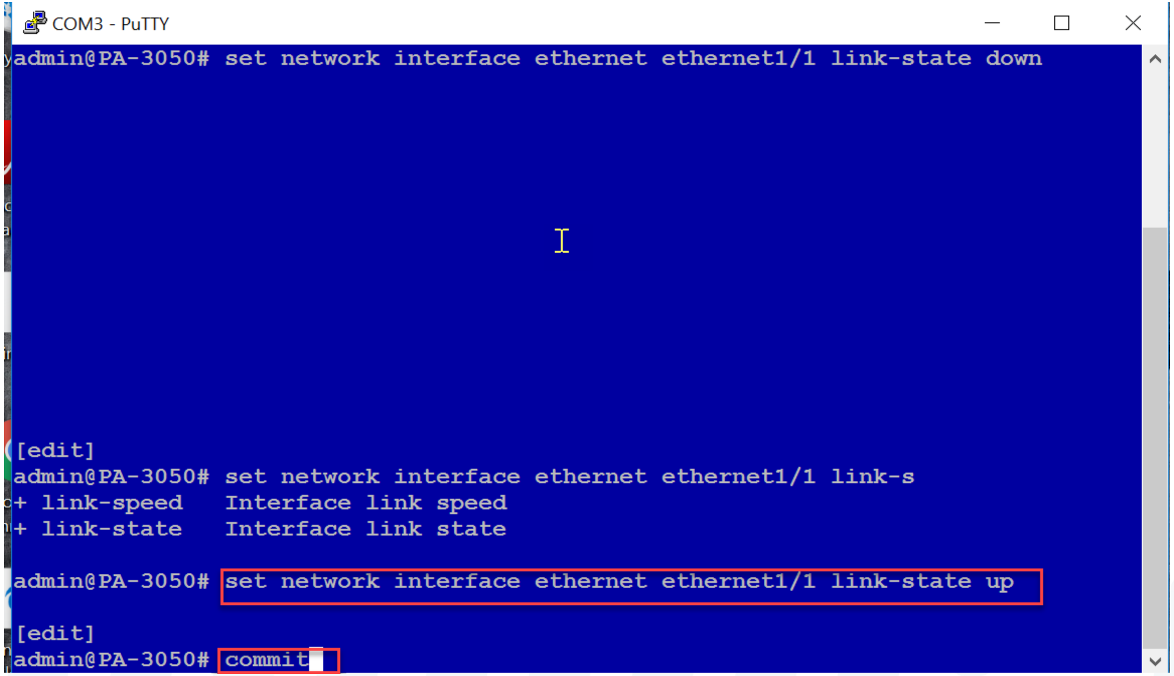


```
admin
panorama
redteam

admin@PA-3050> configure
Entering configuration mode
[edit]
admin@PA-3050# delete mgt-config users redteam

[edit]
admin@PA-3050# commit
```

© 2015, Palo Alto Networks. Confidential and Proprietary.

Secure FW Appliance: Turn Data Interfaces Back On If Turned Off

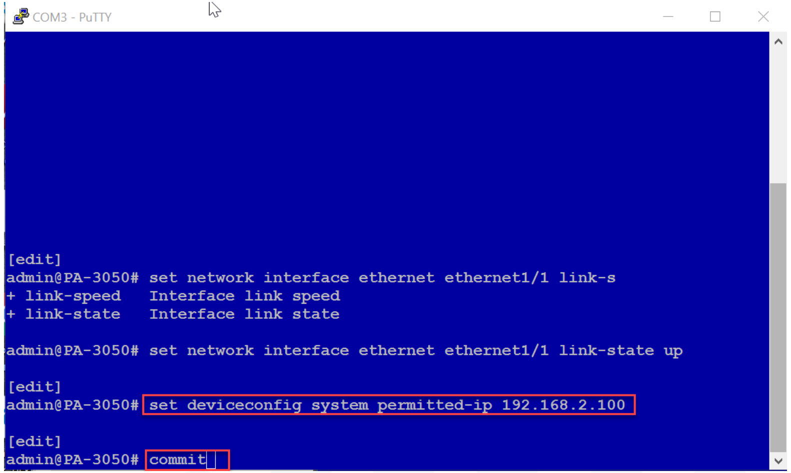
- Configuration Mode #**set network interface ethernet ethernet1/1 link-state up**



```
admin@PA-3050# set network interface ethernet ethernet1/1 link-state down










[edit]
admin@PA-3050# set network interface ethernet ethernet1/1 link-s
+ link-speed   Interface link speed
+ link-state   Interface link state

admin@PA-3050# set network interface ethernet ethernet1/1 link-state up

[edit]
admin@PA-3050# commit
```

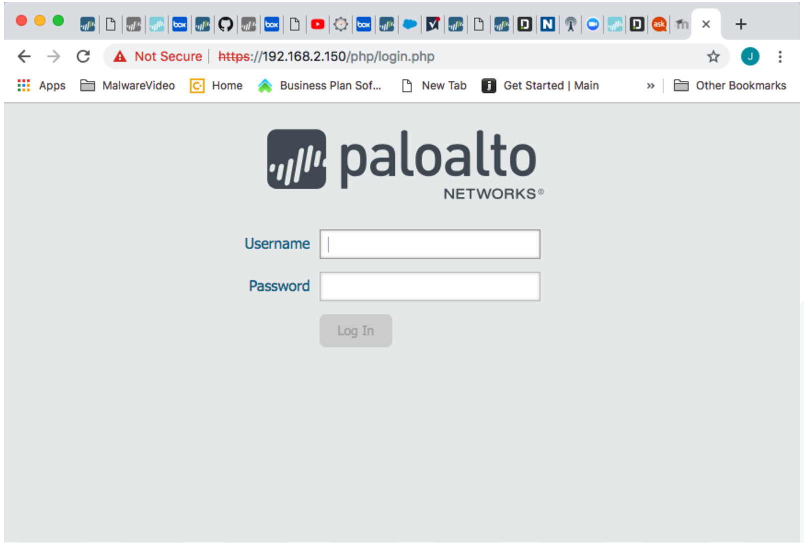
Securing Your FW Appliance: Turn Management Interface Back On

- Only allow management Interface access from your team’s computer
    - Configuration Mode# **set deviceconfig system permitted-ip x.x.x.x**



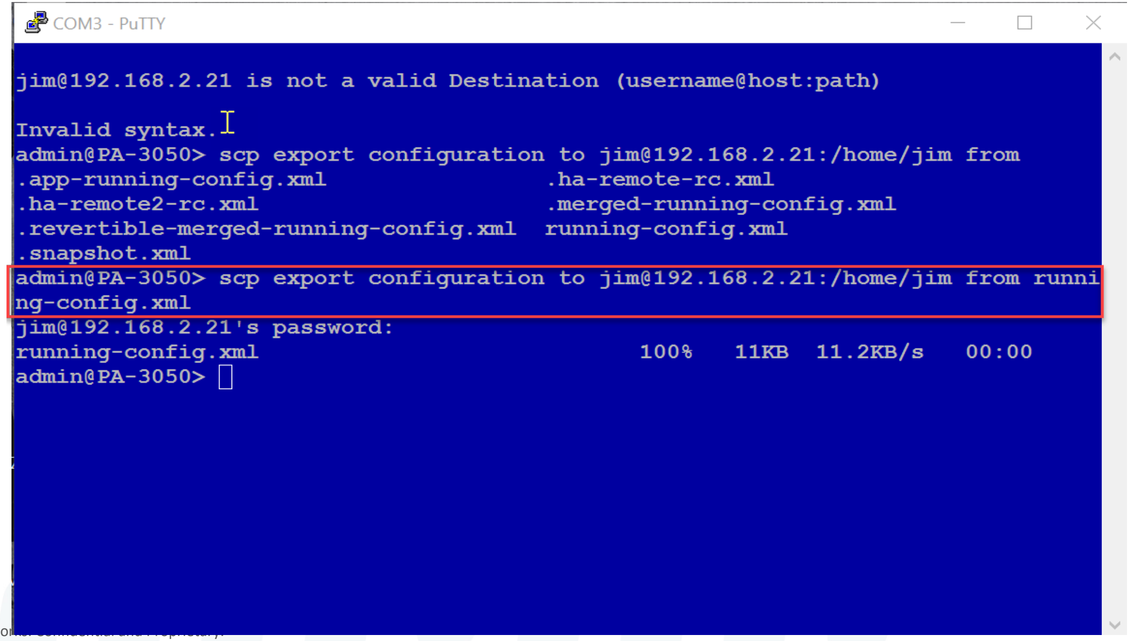
```
[edit]
admin@PA-3050# set network interface ethernet ethernet1/1 link-s
+ link-speed   Interface link speed
+ link-state   Interface link state

admin@PA-3050# set network interface ethernet ethernet1/1 link-state up

[edit]
admin@PA-3050# set deviceconfig system permitted-ip 192.168.2.100

[edit]
admin@PA-3050# commit
```

- Manage your FW appliance via mgt interface Web-UI



Securing Your FW: Back Up Your FW Config and/or Take Snapshot of Virtual Firewall Appliance

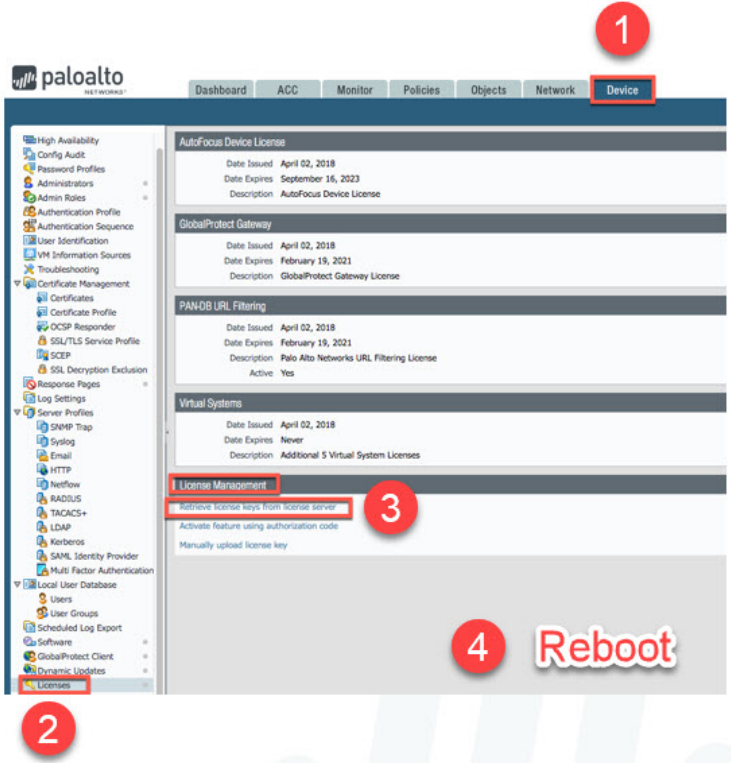
- Operations Mode >**scp export configuration to** **username@host:/home/secops from running-config.xml**



```
jim@192.168.2.21 is not a valid Destination (username@host:path)

Invalid syntax.
admin@PA-3050> scp export configuration to jim@192.168.2.21:/home/jim from
.app-running-config.xml                .ha-remote-rc.xml
.ha-remote2-rc.xml                     .merged-running-config.xml
.revertible-merged-running-config.xml  running-config.xml
.snapshot.xml
admin@PA-3050> scp export configuration to jim@192.168.2.21:/home/jim from runni
ng-config.xml
jim@192.168.2.21's password:
running-config.xml                                      100%   11KB  11.2KB/s   00:00
admin@PA-3050>
```

Step 2:
License your firewall appliance

Licensing Your FW Appliance: It's a dumb box without licenses



1

2

AutoFocus Device License

Date Issued April 02, 2018
Date Expires September 16, 2023
Description AutoFocus Device License

GlobalProtect Gateway

Date Issued April 02, 2018
Date Expires February 19, 2021
Description GlobalProtect Gateway License

PAN-DB URL Filtering

Date Issued April 02, 2018
Date Expires February 19, 2021
Description Palo Alto Networks URL Filtering License
Active Yes

Virtual Systems

Date Issued April 02, 2018
Date Expires Never
Description Additional 5 Virtual System Licenses

License Management

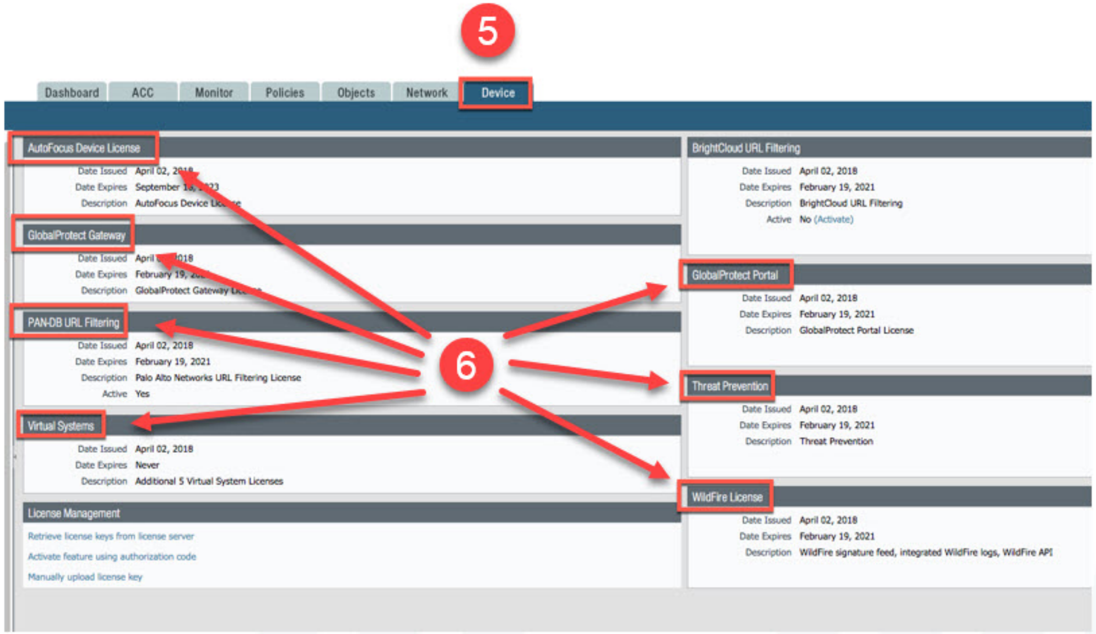
Retrieve license keys from license server

Activate feature using authorization code

Manually upload license key

3

4 Reboot



5

AutoFocus Device License

Date Issued April 02, 2018
Date Expires September 16, 2023
Description AutoFocus Device License

GlobalProtect Gateway

Date Issued April 02, 2018
Date Expires February 19, 2021
Description GlobalProtect Gateway License

PAN-DB URL Filtering

Date Issued April 02, 2018
Date Expires February 19, 2021
Description Palo Alto Networks URL Filtering License
Active Yes

Virtual Systems

Date Issued April 02, 2018
Date Expires Never
Description Additional 5 Virtual System Licenses

License Management

Retrieve license keys from license server

Activate feature using authorization code

Manually upload license key

BrightCloud URL Filtering

Date Issued April 02, 2018
Date Expires February 19, 2021
Description BrightCloud URL Filtering
Active No (Activate)

GlobalProtect Portal

Date Issued April 02, 2018
Date Expires February 19, 2021
Description GlobalProtect Portal License

Threat Prevention

Date Issued April 02, 2018
Date Expires February 19, 2021
Description Threat Prevention

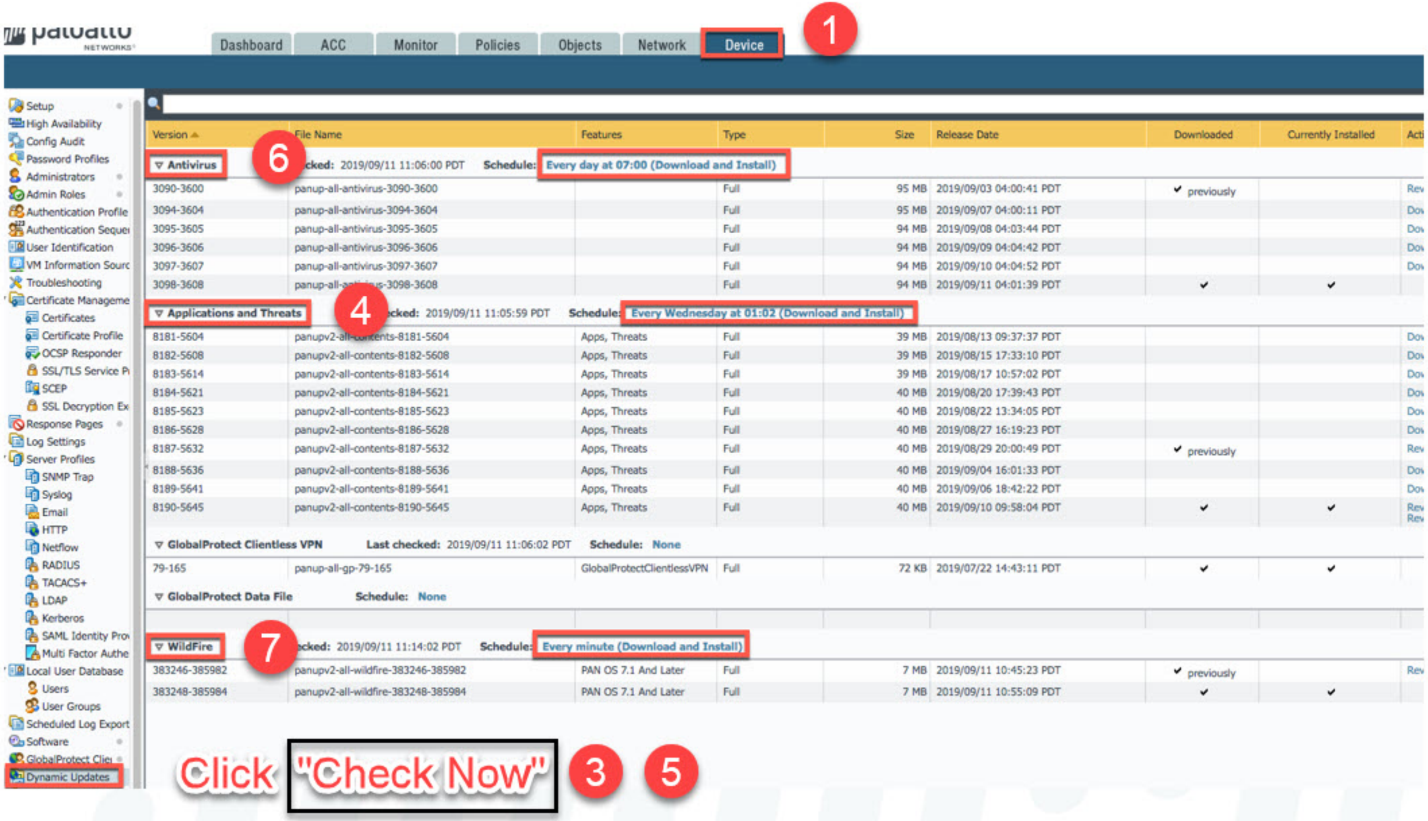
WildFire License

Date Issued April 02, 2018
Date Expires February 19, 2021
Description WildFire signature feed, integrated WildFire logs, WildFire API

6

Step 3:
Download the latest malware signatures for your firewall appliance

Signatures: Dynamic Updates, Need All The Current Malware Signatures Because It's a Dumb Box w/o Them



Version ▲	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Acti
▽ Antivirus	cked: 2019/09/11 11:06:00 PDT	Schedule: Every day at 07:00 (Download and Install)						
3090-3600	panup-all-antivirus-3090-3600		Full	95 MB	2019/09/03 04:00:41 PDT	✓ previously		Rev
3094-3604	panup-all-antivirus-3094-3604		Full	95 MB	2019/09/07 04:00:11 PDT			Dow
3095-3605	panup-all-antivirus-3095-3605		Full	94 MB	2019/09/08 04:03:44 PDT			Dow
3096-3606	panup-all-antivirus-3096-3606		Full	94 MB	2019/09/09 04:04:42 PDT			Dow
3097-3607	panup-all-antivirus-3097-3607		Full	94 MB	2019/09/10 04:04:52 PDT			Dow
3098-3608	panup-all-a[illegible]s-3098-3608		Full	94 MB	2019/09/11 04:01:39 PDT	✓	✓	
▽ Applications and Threats	cked: 2019/09/11 11:05:59 PDT	Schedule: Every Wednesday at 01:02 (Download and Install)						
8181-5604	panupv2-all-[illegible]ents-8181-5604	Apps, Threats	Full	39 MB	2019/08/13 09:37:37 PDT			Dow
8182-5608	panupv2-all-contents-8182-5608	Apps, Threats	Full	39 MB	2019/08/15 17:33:10 PDT			Dow
8183-5614	panupv2-all-contents-8183-5614	Apps, Threats	Full	39 MB	2019/08/17 10:57:02 PDT			Dow
8184-5621	panupv2-all-contents-8184-5621	Apps, Threats	Full	40 MB	2019/08/20 17:39:43 PDT			Dow
8185-5623	panupv2-all-contents-8185-5623	Apps, Threats	Full	40 MB	2019/08/22 13:34:05 PDT			Dow
8186-5628	panupv2-all-contents-8186-5628	Apps, Threats	Full	40 MB	2019/08/27 16:19:23 PDT			Dow
8187-5632	panupv2-all-contents-8187-5632	Apps, Threats	Full	40 MB	2019/08/29 20:00:49 PDT	✓ previously		Rev
8188-5636	panupv2-all-contents-8188-5636	Apps, Threats	Full	40 MB	2019/09/04 16:01:33 PDT			Dow
8189-5641	panupv2-all-contents-8189-5641	Apps, Threats	Full	40 MB	2019/09/06 18:42:22 PDT			Dow
8190-5645	panupv2-all-contents-8190-5645	Apps, Threats	Full	40 MB	2019/09/10 09:58:04 PDT	✓	✓	Rev Rev
▽ GlobalProtect Clientless VPN	Last checked: 2019/09/11 11:06:02 PDT	Schedule: None						
79-165	panup-all-gp-79-165	GlobalProtectClientlessVPN	Full	72 KB	2019/07/22 14:43:11 PDT	✓	✓	
▽ GlobalProtect Data File	Schedule: None							
▽ WildFire	cked: 2019/09/11 11:14:02 PDT	Schedule: Every minute (Download and Install)						
383246-385982	panupv2-all-wildfire-383246-385982	PAN OS 7.1 And Later	Full	7 MB	2019/09/11 10:45:23 PDT	✓ previously		Rev
383248-385984	panupv2-all-wildfire-383248-385984	PAN OS 7.1 And Later	Full	7 MB	2019/09/11 10:55:09 PDT	✓	✓	

Click "Check Now" 3 5

Step 4
Determine and configure your network deployment for firewall appliance (Vwire, Layer2, Layer3)

AND

Step 5:
Configure security policies and assign security profiles to your security policies

3 Network Deployment Options:

1. Virtual Wire

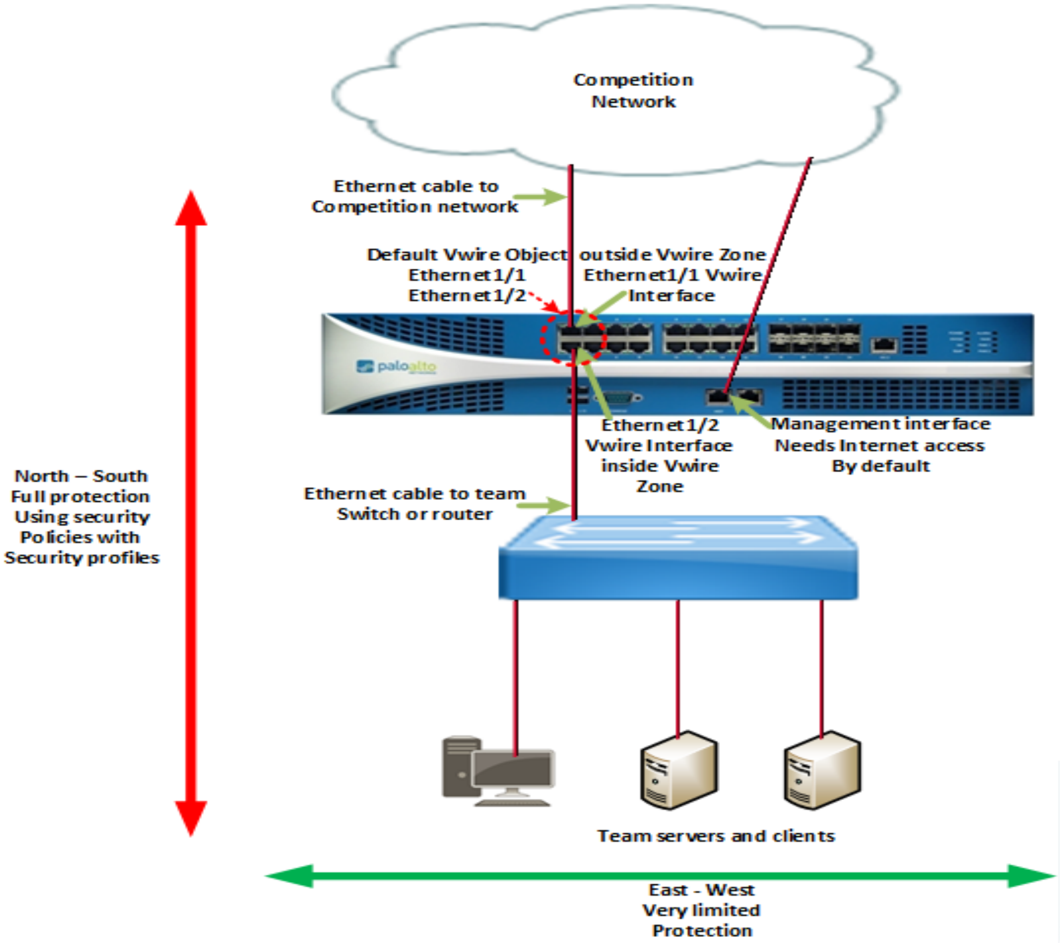
2. Layer 2

3. Layer 3

Network Deployment Option 1: Virtual Wire (Vwire)

- Recommended deployment: because it’s the easiest and quickest to set up
  - PA 3050 preconfigured for Vwire
  - Sets up a network bridge between 2 FW interfaces
  - No IP or Layer 2 addressing – therefore invisible to attackers!
- Cons: Only provides North-South full protection
  - Can’t segment internal traffic into multiple internal zones to defend against East-West pivoting
- PA 3050 setup
  - Find the Ethernet cable coming into your room and connect it to FW’s ethernet1/1 port (This is your ingress interface)
  - Connect a cable from your FW’s ethernet1/2 interface to your room’s switch/router
  - Configure outside Vwire zone for ethernet1/1 and inside Vwire zone for ethernet1/2
  - Configure your inbound and outbound security policies

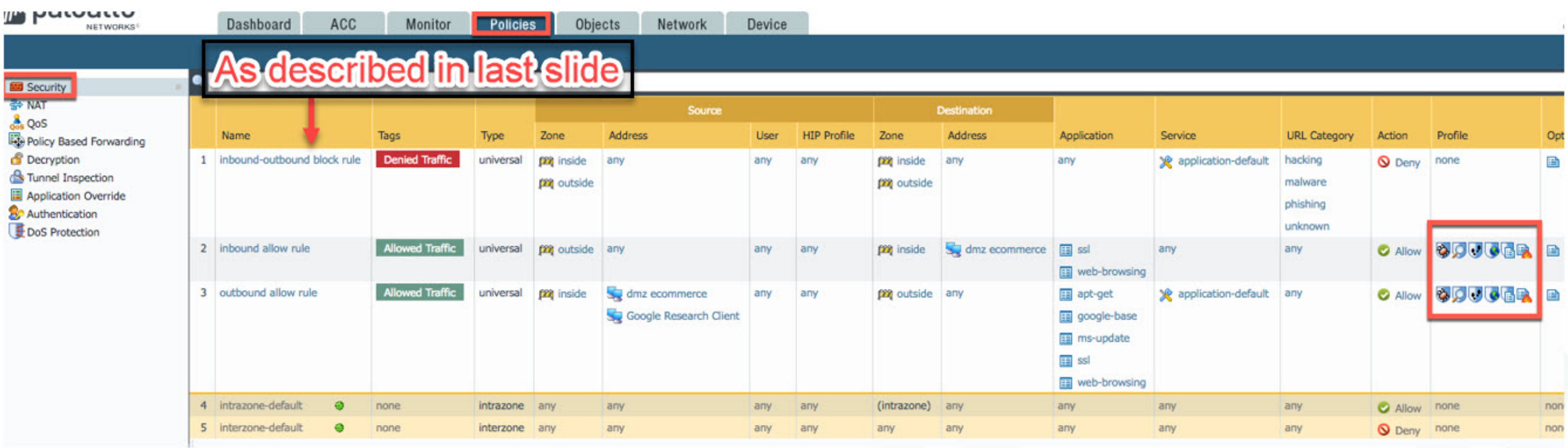
Network Deployment (Option 1): Vwire Architecture


Competition Network
Ethernet cable to Competition network
Default Vwire Object Ethernet1/1 Ethernet1/2
outside Vwire Zone Ethernet1/1 Vwire Interface
paloalto
Ethernet1/2 Vwire Interface inside Vwire Zone
Management interface Needs Internet access By default
North – South Full protection Using security Policies with Security profiles
Ethernet cable to team Switch or router
Team servers and clients
East - West Very limited Protection

Network Deployment (Option 1): Vwire Security Policies

- Configure an inbound and outbound block rule to block unknown and bad urls
- Configure inbound allow rule(s) for your scored services
  - Make rules as specific as possible by using allowed applications and destination IP addresses
- Configure outbound allow rule(s)
  - Make rules as specific as possible by using allowed applications (application default) and destination IP addresses
  - Only allow outbound traffic from specific IP addresses that is absolutely necessary for your organization and scoring
- Make sure you assign Security Profiles to all your Allow rules
  - Your FW will not block malware without Security Profiles assigned to Security Policies

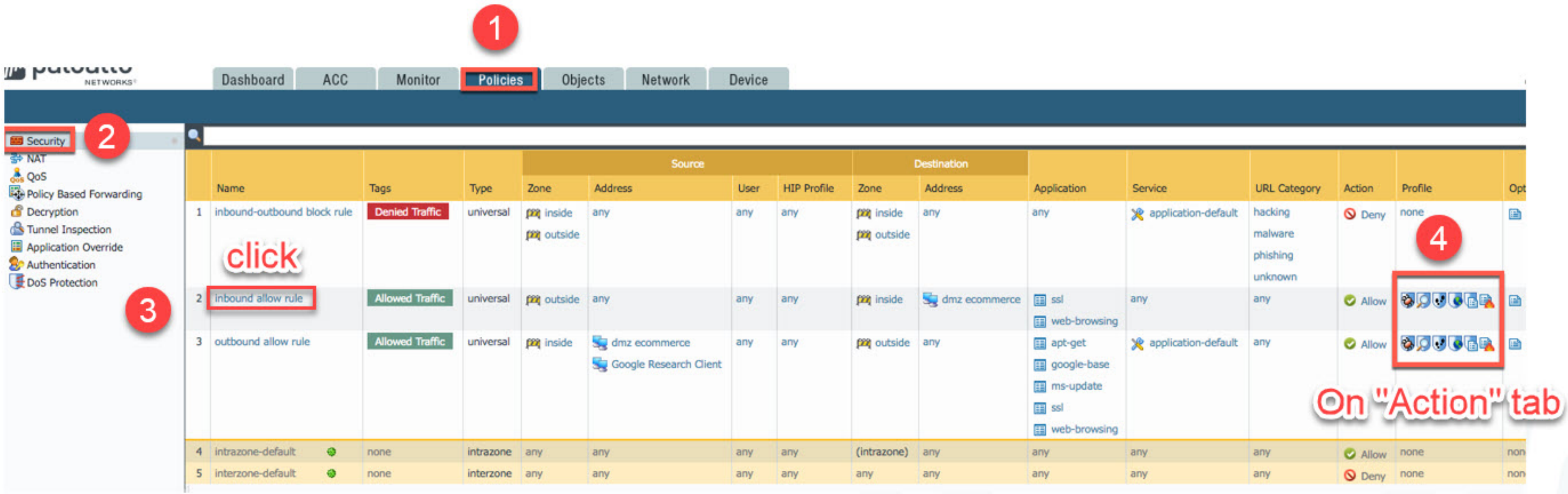
Network Deployment (Option 1): Vwire Security Policies (Cont.)



As described in last slide

				Source				Destination							
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Opt
1	inbound-outbound block rule	Denied Traffic	universal	inside outside	any	any	any	inside outside	any	any	application-default	hacking malware phishing unknown	Deny	none	
2	inbound allow rule	Allowed Traffic	universal	outside	any	any	any	inside	dmz ecommerce	ssl web-browsing	any	any	Allow		
3	outbound allow rule	Allowed Traffic	universal	inside	dmz ecommerce Google Research Client	any	any	outside	any	apt-get google-base ms-update ssl web-browsing	application-default	any	Allow		
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none	non
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	non

Network Deployment (Option 1): Vwire Security Policies (Cont.)



click

				Source				Destination							
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Opt
1	inbound-outbound block rule	Denied Traffic	universal	inside outside	any	any	any	inside outside	any	any	application-default	hacking malware phishing unknown	Deny	none	
2	inbound allow rule	Allowed Traffic	universal	outside	any	any	any	inside	dmz ecommerce	ssl web-browsing	any	any	Allow		
3	outbound allow rule	Allowed Traffic	universal	inside	dmz ecommerce Google Research Client	any	any	outside	any	apt-get google-base ms-update ssl web-browsing	application-default	any	Allow		
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none	non
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	non

On "Action" tab

© 2015, Palo Alto Networks. Confidential and Proprietary.

Network Deployment (Option 2): Layer 2 (L2)

- **Most applicable if** your team is assigned 1 subnet,1 switch, and no router
  - All team hosts are configured with a default gateway located in competition network and your team has no control over this default gateway

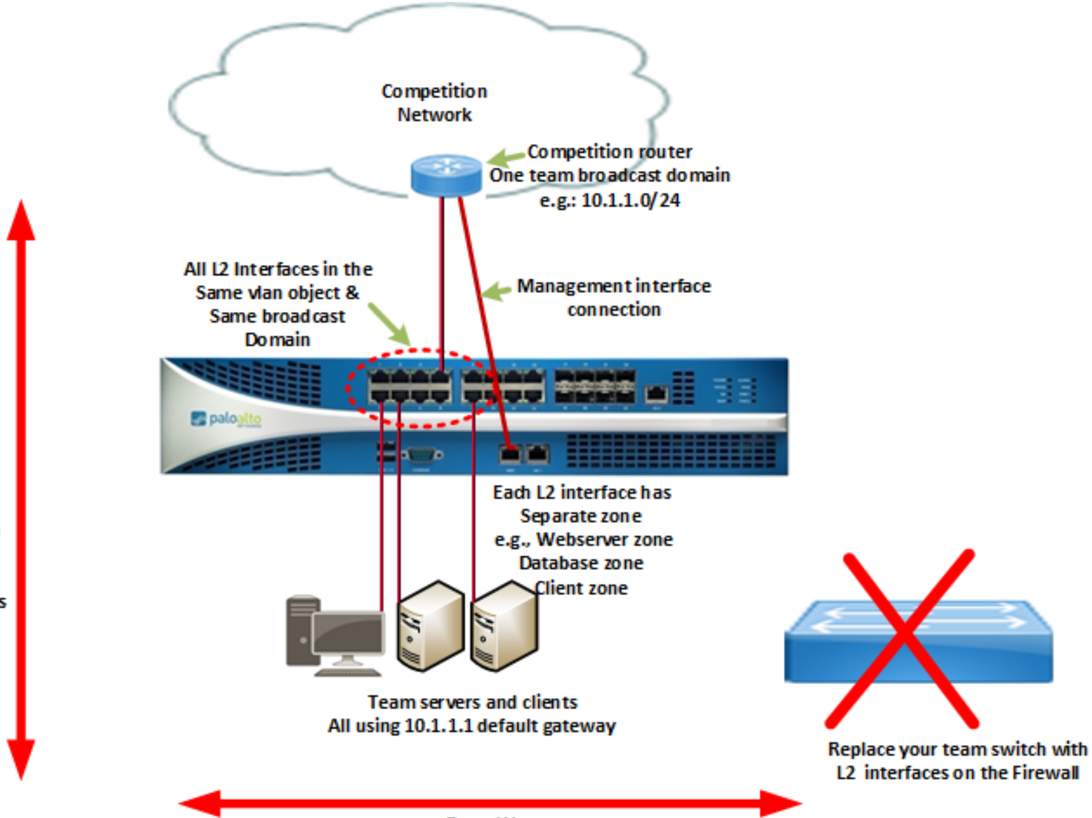
- Pro: Provides both North-South and East-West full protection

- Con: more complex to set up than Vwire, hosts have to be in same subnet and corresponding Ethernet broadcast domain and no support for vpn's

- **Replace your team switch** with your firewall configured with L2 interfaces
  - Create L2 interfaces and assign them to same firewall vlan object
  - Assign L2 zones to each L2 interface
  - Connect your team hosts to separate L2 interfaces
  - Create security policies to allow only essential North-South and East-West traffic

© 2015, Palo Alto Networks. Confidential and Proprietary.

Network Deployment (Option 2): L2 Architecture



Competition Network

Competition router
One team broadcast domain
e.g.: 10.1.1.0/24

All L2 Interfaces in the
Same vlan object &
Same broadcast
Domain

Management interface
connection

Each L2 interface has
Separate zone
e.g., Webserver zone
Database zone
Client zone

North – South
Full Protection
Using security
Policies with
Security profiles

Team servers and clients
All using 10.1.1.1 default gateway

Replace your team switch with
L2 interfaces on the Firewall

East - West
Full Protection using
Security policies with
Security profiles

Network Deployment L2 (Option 2): Security Policies

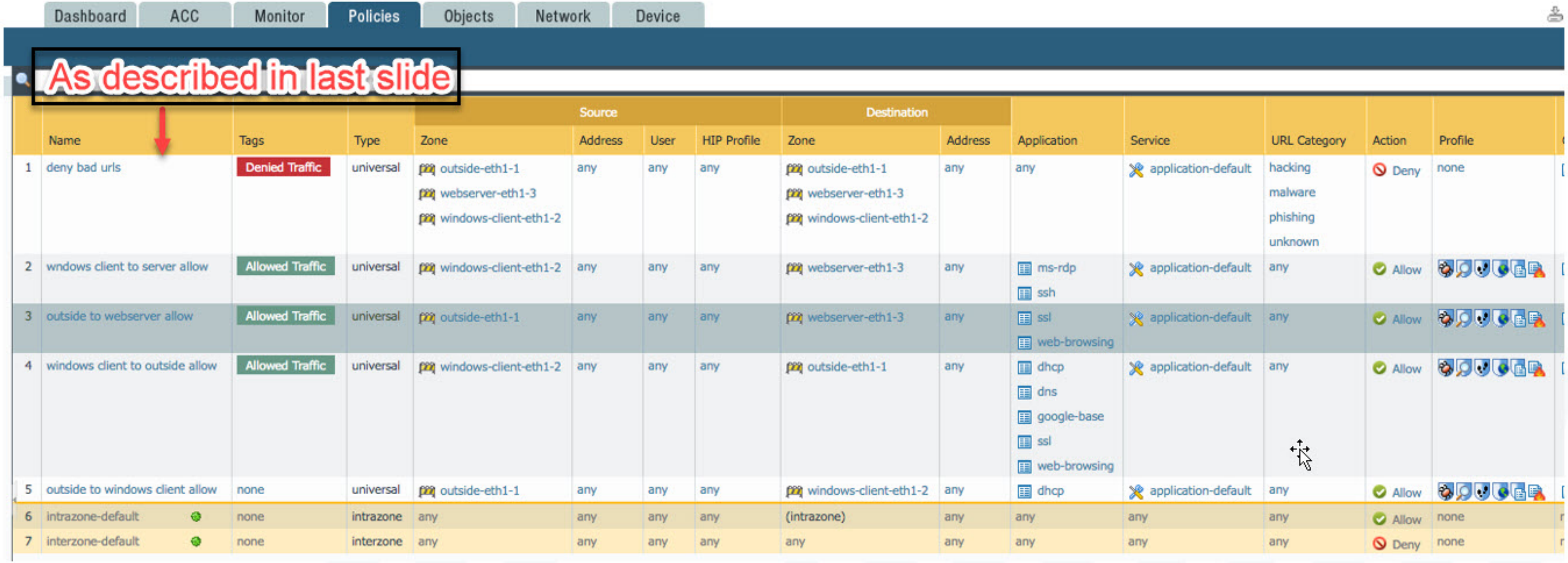
- Configure and inbound and outbound block rule to block unknown and bad urls

- Configure inbound allow rule(s) for your scored services
  - Make rules as specific as possible by using allowed applications and destination IP addresses

- Configure East-West rule(s) for internal traffic
  - Make rules as specific as possible by using allowed applications (application default) and destination IP addresses
  - Only allow internal traffic from specific IP addresses that is absolutely necessary to keep your services up
  - DHCP is a 2-way protocol requiring ingress and egress rules

- Make sure you assign Security Profiles to all your Allow rules
  - Your FW will not block malware without Security Profiles assigned to Security Policies

Network Deployment L2 (Option 2): Security Policies (cont.)



As described in last slide

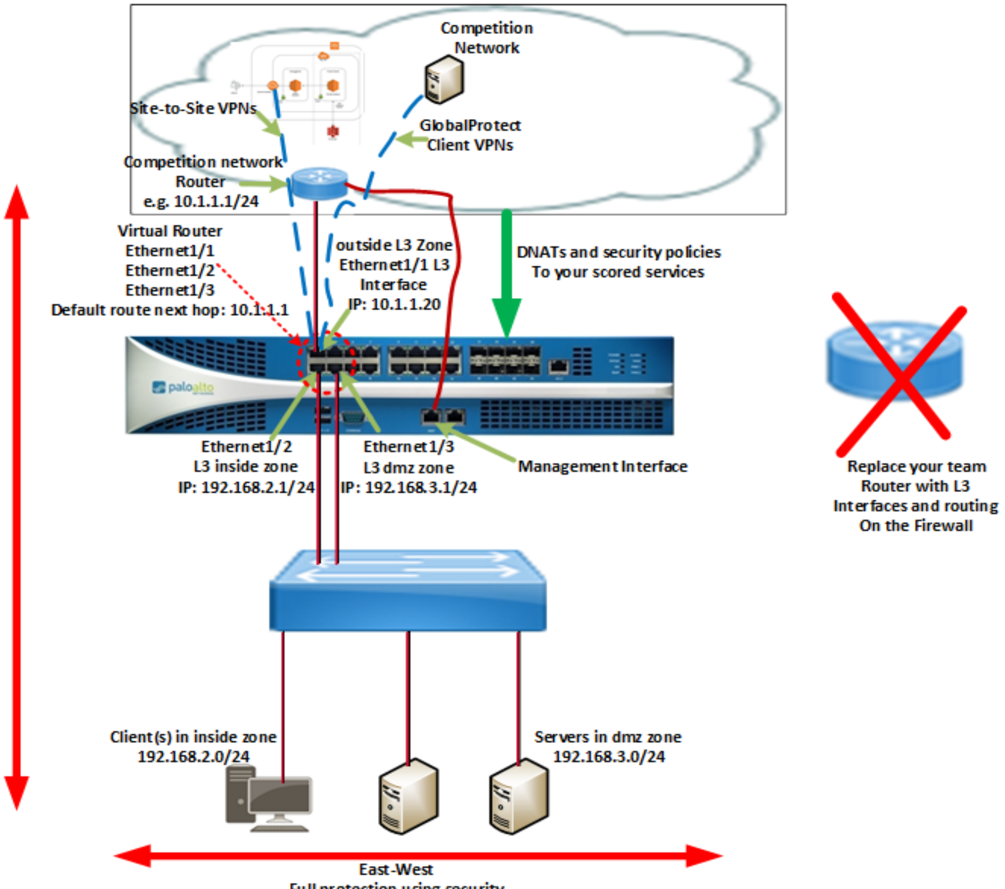
				Source				Destination						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
1	deny bad urls	Denied Traffic	universal	outside-eth1-1 webserver-eth1-3 windows-client-eth1-2	any	any	any	outside-eth1-1 webserver-eth1-3 windows-client-eth1-2	any	any	application-default	hacking malware phishing unknown	Deny	none
2	wndows client to server allow	Allowed Traffic	universal	windows-client-eth1-2	any	any	any	webserver-eth1-3	any	ms-rdp ssh	application-default	any	Allow	
3	outside to webserver allow	Allowed Traffic	universal	outside-eth1-1	any	any	any	webserver-eth1-3	any	ssl web-browsing	application-default	any	Allow	
4	windows client to outside allow	Allowed Traffic	universal	windows-client-eth1-2	any	any	any	outside-eth1-1	any	dhcp dns google-base ssl web-browsing	application-default	any	Allow	
5	outside to windows client allow	none	universal	outside-eth1-1	any	any	any	windows-client-eth1-2	any	dhcp	application-default	any	Allow	
6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
7	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none

© 2015, Palo Alto Networks. Confidential and Proprietary.

Network Deployment Option 3: Layer 3 (L3)

- **Most applicable if** your team has a router that you can replace using firewall
  - You will need to create Destination NATs (DNATs) for your scored services
  - Firewall supports dynamic routing: ripv2, ospf, ospfv3, bgp
- Pro: Provides both North-South and East-West full protection
  - Allows you to configure firewall site-to-site VPNs and GlobalProtect client VPNs
  - Allows you to use data interfaces for Web-UI access and dynamic updates instead of management interface
- Con: Most complex to set up correctly
- **Replace your team router** with your firewall configured with L3 interfaces
  - Create L3 interfaces and assign them to same firewall virtual router
  - Create a virtual router default static route if not using dynamic routing to competition gateway
  - Assign L3 zones to each L3 interface
  - Connect your team hosts to separate L3 interfaces/zones
  - Create source NAT for egress traffic and Destination NAT policies for scored services
  - Create security policies to allow only essential North-South and East-West traffic

Network Deployment L3 (Option 3): Network Architecture



Competition Network

Site-to-Site VPNs

GlobalProtect Client VPNs

Competition network Router
e.g. 10.1.1.1/24

Virtual Router
Ethernet1/1
Ethernet1/2
Ethernet1/3
Default route next hop: 10.1.1.1

outside L3 Zone
Ethernet1/1 L3 Interface
IP: 10.1.1.20

DNATs and security policies
To your scored services

Ethernet1/2
L3 inside zone
IP: 192.168.2.1/24

Ethernet1/3
L3 dmz zone
IP: 192.168.3.1/24

Management Interface

Replace your team
Router with L3
Interfaces and routing
On the Firewall

North – South
Full protection using
Security policies with
Security profiles

Client(s) in inside zone
192.168.2.0/24

Servers in dmz zone
192.168.3.0/24

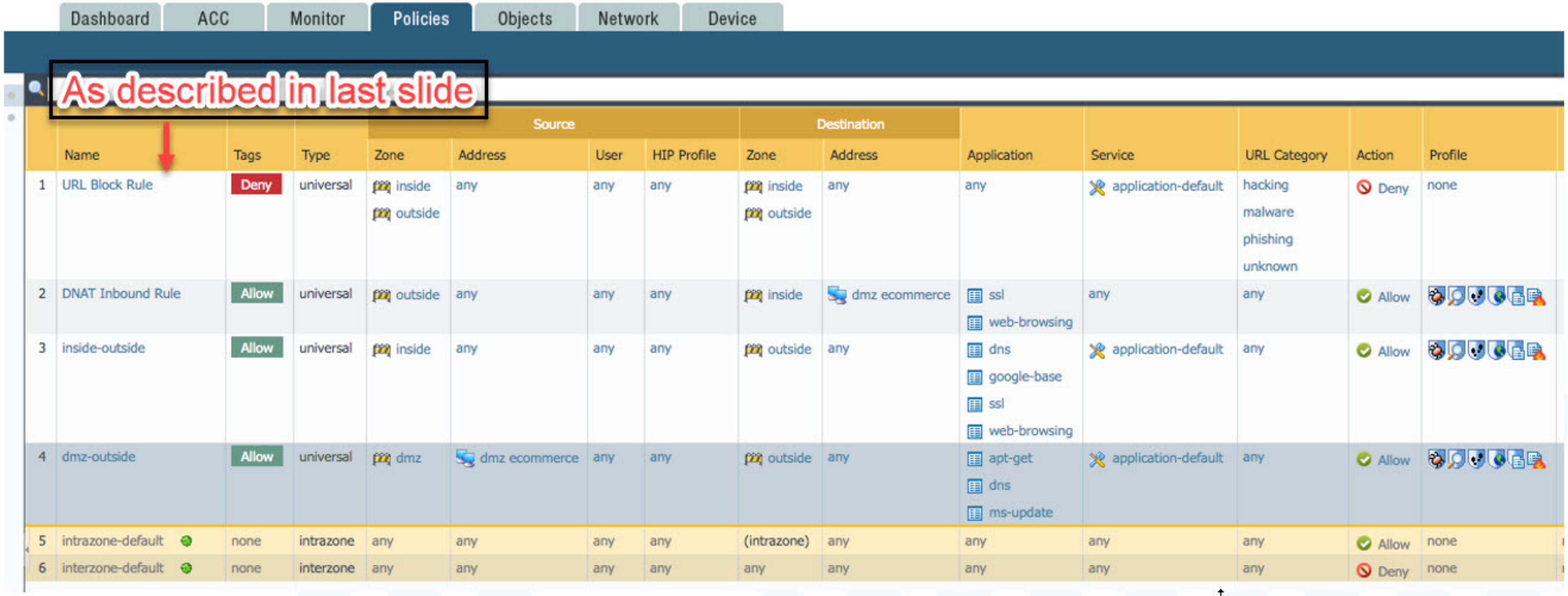
East-West
Full protection using security
Policies with security profiles

Network Deployment L3 (Option 3): Security Policies

- Configure an inbound and outbound block rule to block unknown and bad urls
- Configure inbound allow rule(s) corresponding to your DNAT policy(ies) for scored services
  - Make rules as specific as possible by using allowed applications and destination IP addresses
- Configure East-West rule(s) for internal traffic
  - Make rules as specific as possible by using allowed applications (application default) and destination IP addresses
  - Only allow internal traffic to and from specific internal IP addresses that is absolutely necessary to keep your services up
- Make sure you assign Security Profiles to all your Security Policy Allow rules
  - Your FW will not block malware without Security Profiles assigned to Security Policies

© 2015, Palo Alto Networks. Confidential and Proprietary.

Network Deployment L3 (Option 3): Security Policies (cont.)

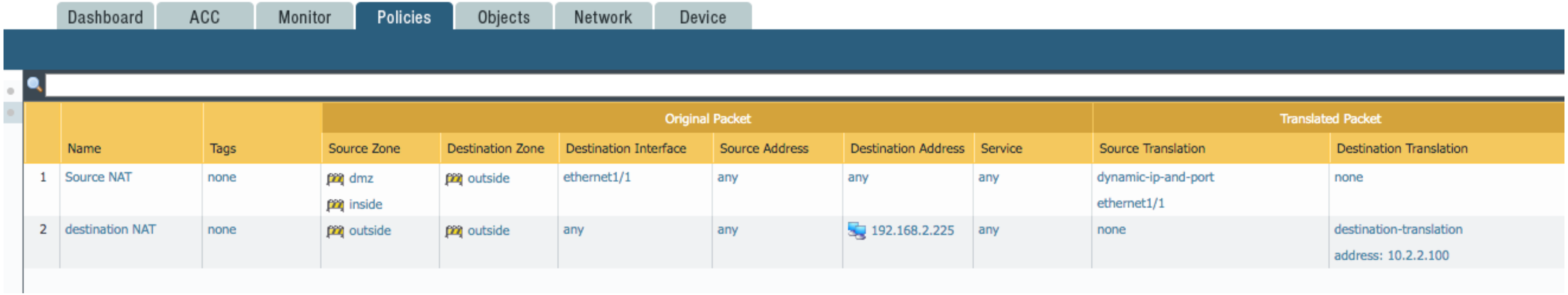


As described in last slide

				Source				Destination						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
1	URL Block Rule	Deny	universal	inside outside	any	any	any	inside outside	any	any	application-default	hacking malware phishing unknown	Deny	none
2	DNAT Inbound Rule	Allow	universal	outside	any	any	any	inside	dmz ecommerce	ssl web-browsing	any	any	Allow	
3	inside-outside	Allow	universal	inside	any	any	any	outside	any	dns google-base ssl web-browsing	application-default	any	Allow	
4	dmz-outside	Allow	universal	dmz	dmz ecommerce	any	any	outside	any	apt-get dns ms-update	application-default	any	Allow	
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none

© 2015, Palo Alto Networks. Confidential and Proprietary.

Network Deployment L3 (Option 3): NAT Policies



			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Source NAT	none	dmz inside	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	none
2	destination NAT	none	outside	outside	any	any	192.168.2.225	any	none	destination-translation address: 10.2.2.100

Step 6:
Turn on the full power of the firewall with WebUI and Best Practices

Turn On Full Power of Firewall Appliance Using Web-UI and Best Practices

1. Complete visibility of traffic

- Know applications to allow
  - Custom Apps
- SSL Decryption ← Decryption
- User-ID ← User-ID

2. Reduce attack surface area

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

Turn On Full Power of Firewall Appliance Using Web-UI and Best Practices

3. Protect against known attacks

- Assign security profiles to firewall security policies
  - Anti-virus profile
    - Enable blocking by AV signature
    - Enable blocking by Wildfire signature.
  - Vulnerability profile
  - Anti-spyware
    - DNS beacon protection
    - Block by anti-spyware signature
  - File blocking
  - URL Filtering/C2 Web sites

- Protect against DoS, Reconnaissance Malformed Packets, Bad Protocols
  - Zone protection profile
  - DoS Profile
- Use External Dynamic Lists to block bad traffic

Content-ID

URL Filtering

Turn On Full Power of Firewall Appliance Using Web-UI and Best Practices

4. Protect against unknown attacks
   - WildFire Analysis ← Unknowns file analysis & 5 min malware signature generation

Extend Firewall’s Protection

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

Step 7:

Preparing for CCDC using:

1) Automation Tools
   - Iron Skillet
   - Expedition Migration Tool VM

2) CCDC2020 Moodle Course

Automation Tolls To Use for Preparing for CCDC

- **Iron-skillet firewall configs** – available to anyone
  - https://github.com/PaloAltoNetworks/iron-skillet

- **Expedition Migration Tool** VM – free to download
  - https://live.paloaltonetworks.com/t5/Expedition-Migration-Tool/ct-p/migration_tool

- Consult **CCDC2020 Moodle course** for more deployment/configuration details
  - Free FW practice via online Netlab+ lab pod and via your team's free fully licensed VM-50 firewall appliance (Contact your regional CCDC Director for details)
  - Practice on your VM-50 firewall appliance
    - Configuration of virtual firewall appliances almost identical to PA 3050