CCDC Palo Alto Playbook – Max Banner

Initial Configuration:

Run INIT.SH script on ubuntu box while doing initial configuration

Update – RCE present on competition version 10.0. RCE's not present past version 10.0.8.

Change Admin password via CLI

> configure

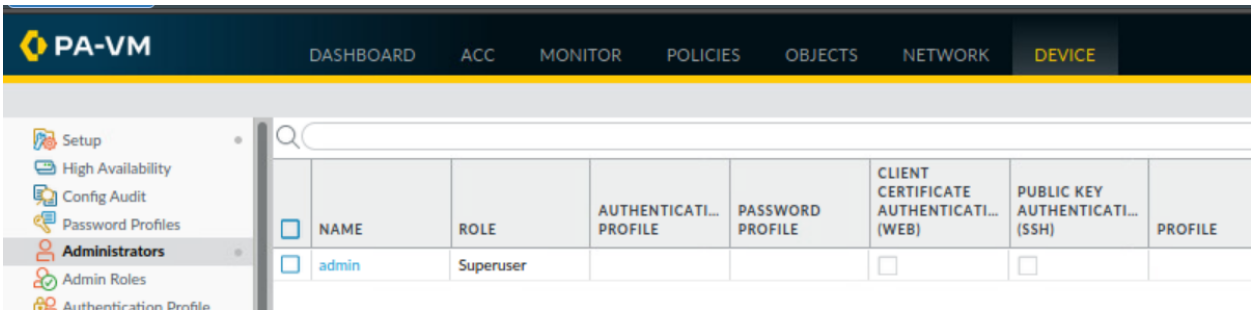
set mgt-config users admin password <new password>

Change Admin password via GUI

Admin password changes are effective before commit.

Device > Administrators

Change all admin passwords. Invitational had two administrator accounts

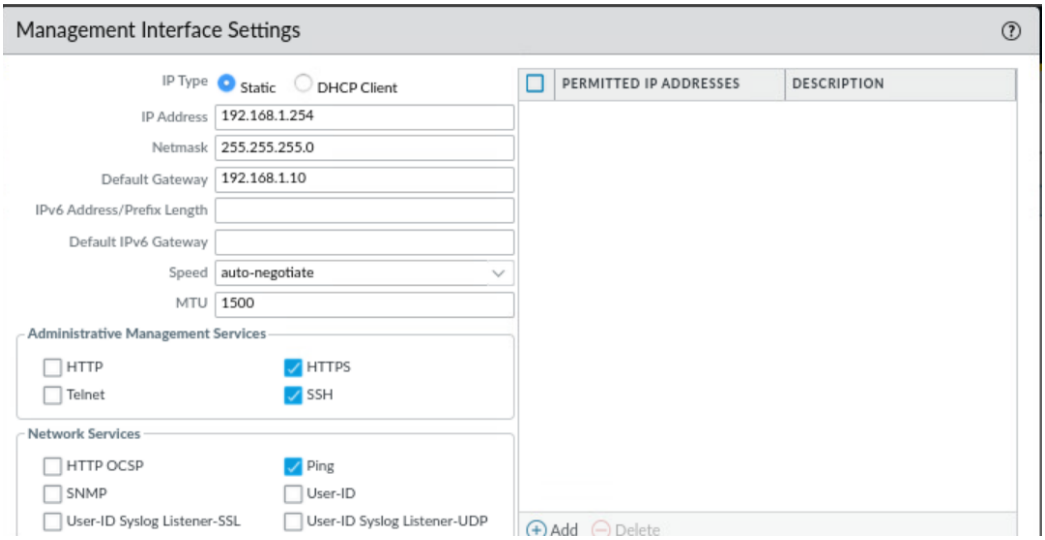


Modify Management Interface:

Device > Setup > Interfaces > Management

Add Permitted IP address X.X.X.X/24 of ubuntu wrkstn with note "MTG access from this host only"

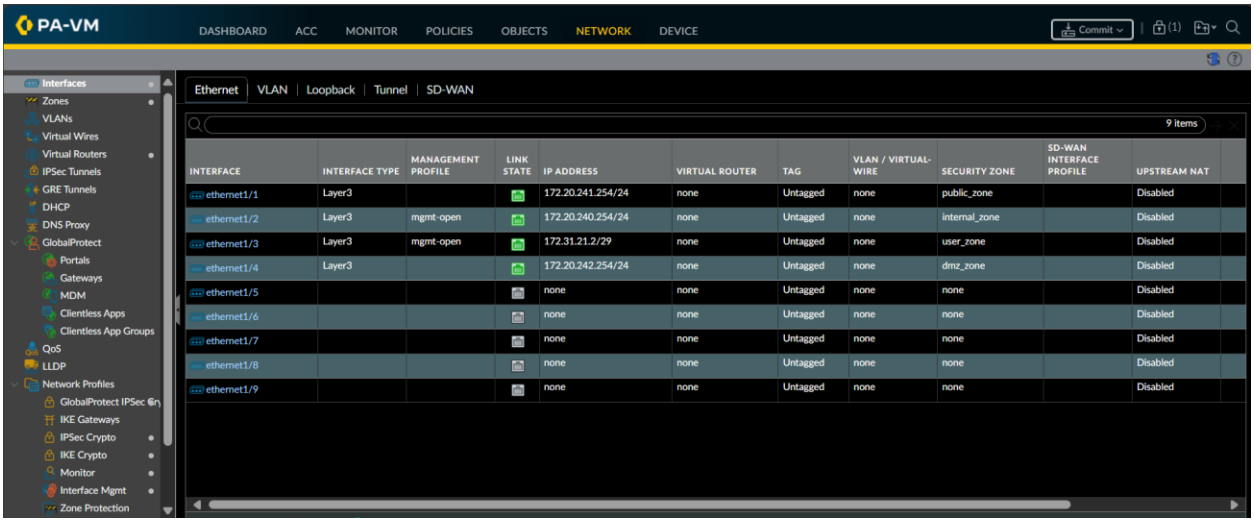
Disable Telnet & HTTP options & disallow network services



Create / Adjust Management Profile

No telnet no http no SSH

Remove management access from external interfaces:



Remove Management profile from external interfaces

** Do not remove from ubuntu workstation's zone as it may lock you out**

Create closed management profile from CLI:

set network profiles interface-management-profile closed telnet no

assign management profiles:

set network interface ethernet ethernet1/3 layer3 interface-management-profile closed

There is no way to remove a profile without use of GUI.

Creating Firewall Rules

Inbound Rules

Allow only services inbound (web browsing, dns, and box specific services) by application rather than port number/service group. If address objects are not pre-populated make sure to use public address for inbound rules. These rules do not work with private IP addresses

Using the CLI:

	Operational Mode >	Configuration Mode #
Use:	Default mode (or exit)	configure command
Sample commands	show less test debug	show seg or delete commit
Variable working context	No	Yes, via edit com
Operational Effect	Immediate	After commit
Shared Features	Role-based access control Autocomplete Suggestions Short explanations for options	

** what you can do in operational mode is also applied immediately when done through the GUI and similar for configuration mode options when configured through the GUI. **

All Security Rules in CLI format:

Create an empty secure policy group first and add it to internal rules to stream basic configuration

set profile-group SecurityGroup

Creating this empty group allows anti-malware & anti-spyware policies to be created later and added to all the rules by adding them to this one group.

Firewall rules are ineffective until commit

~~set rulebase security rules InboundDocker from external-zone to internal-zone source any destination 172.20.240.20 service application-default application any action deny profile-setting group SecurityGroup~~
~~set rulebase security rules InboundDebian from external-zone to internal-zone source any destination 172.20.242.20 service application-default application [dns websocket icmp ntp] action allow profile-setting group SecurityGroup~~

~~# set rulebase security rules InboundUbuntuWeb from external-zone to dmz-zone source any destination 172.20.242.10 service application-default application [dns websocket icmp ntp] action allow profile-setting group SecurityGroup~~

~~# set rulebase security rules InboundADDNS from external-zone to dmz-zone source any destination 172.20.242.200 service application-default application [dns websocket ldap dhcp icmp ntp] action allow profile-setting group SecurityGroup~~

~~# set rulebase security rules InboundUbuntuWKST from external-zone to dmz-zone source any destination ubuntuwkst service application-default application [dns websocket icmp ntp] action allow profile-setting group SecurityGroup~~

~~# set rulebase security rules InboundSplunk from external-zone to public-zone source any destination 172.20.241.20 service application-default application [dns websocket icmp ntp] action allow profile-setting group SecurityGroup~~

~~# set rulebase security rules InboundCentOS from external-zone to public-zone source any destination 172.20.241.30 service application-default application [dns websocket icmp ntp] action allow profile-setting group SecurityGroup~~

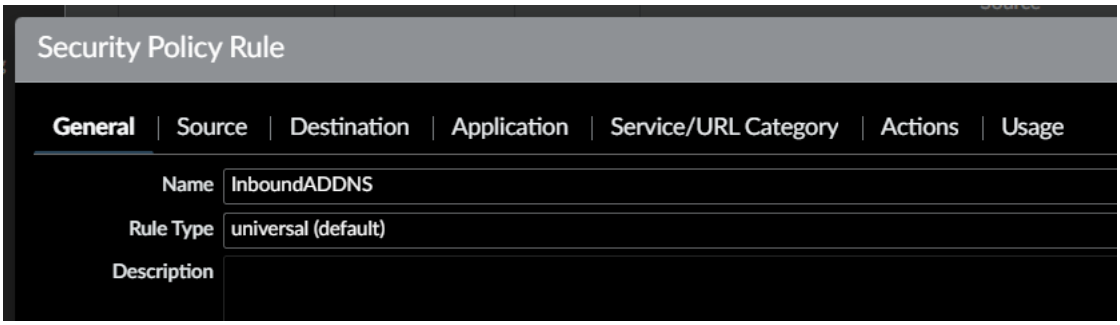
~~# set rulebase security rules InboundFedora from external-zone to public-zone source any destination 172.20.241.40 service application-default application [dns websocket imap pop3 smtp icmp ntp] action allow profile-setting group SecurityGroup~~

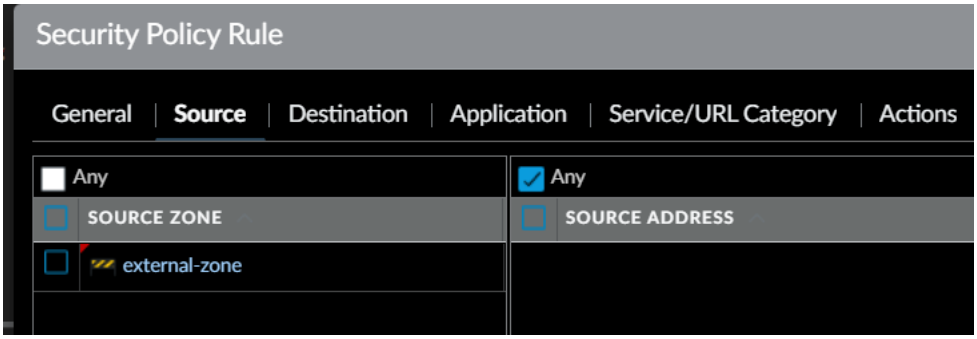
~~# set rulebase security rules Outbound from [dmz-zone public-zone internal-zone] to external-zone source any destination any service application-default application [dns websocket imap pop3 smtp ldap dhcp icmp ntp] action allow~~

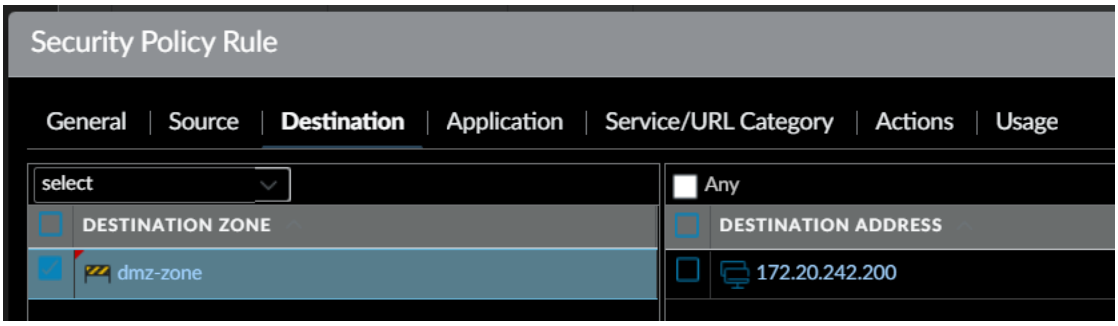
~~# set rulebase security rules DenyANYANY from external-zone to [dmz-zone public-zone internal-zone] service any application any source any destination any service any application any action deny~~

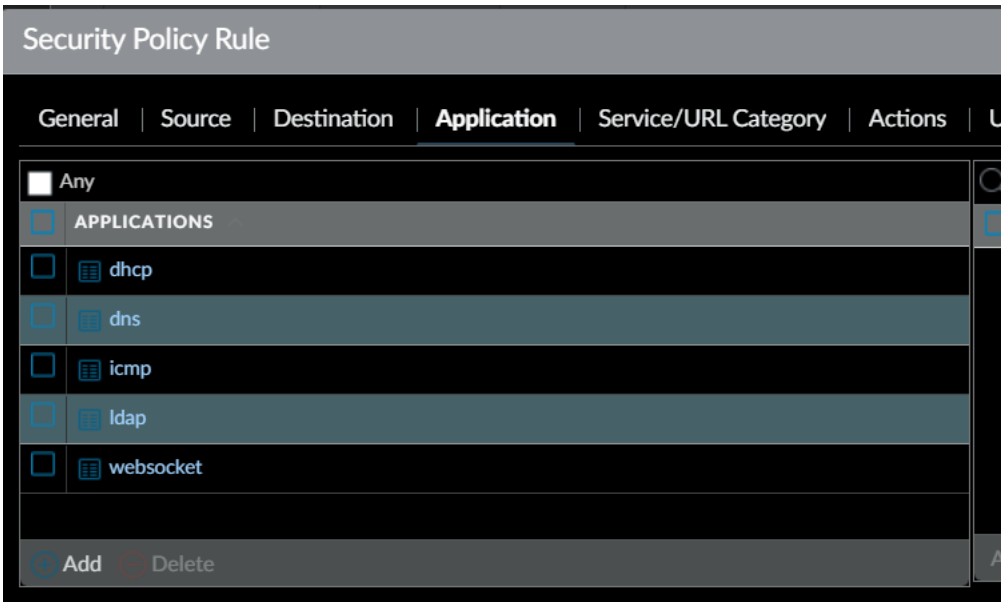
Spaces between DNS websocket etc. and [ ] are very important

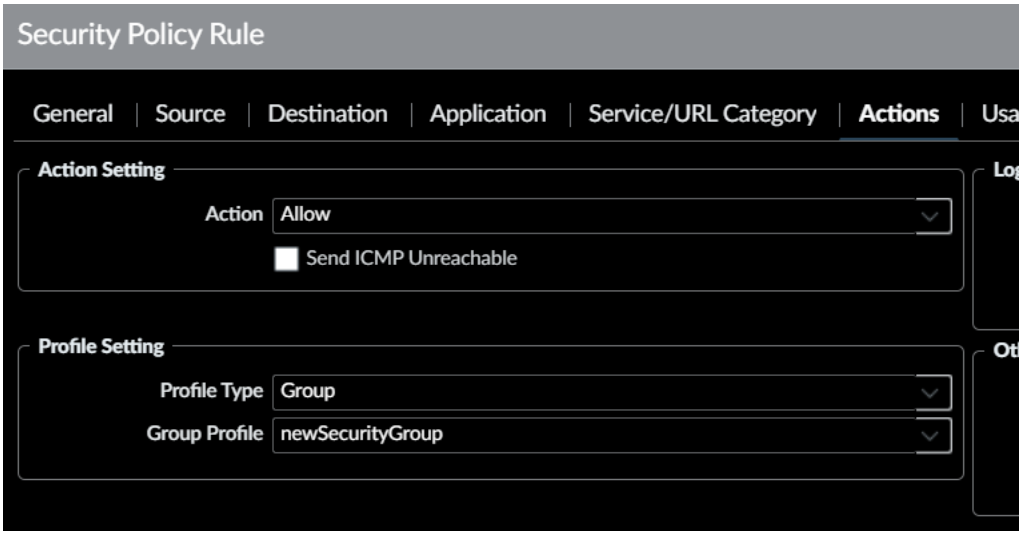
Making rules through GUI:




Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Any
SOURCE ZONE
external-zone
Any
SOURCE ADDRESS


Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Usage
select
DESTINATION ZONE
dmz-zone
Any
DESTINATION ADDRESS
172.20.242.200


Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Any
APPLICATIONS
dhcp
dns
icmp
ldap
websocket
Add
Delete



****Web-browsing only covers port 80, add SSL applications for port 443****

Deny Any-Any once all rules created. ***IT MUST BE THE BOTTOMMOST RULE***

COMMIT CHANGES

Check for version updates

Device > Dynamic Updates

DO NOT PERFORM MAJOR VERSION UPGRADE – takes too long and breaks things unless trying to rid RCE from version 10

Dynamic updates may be completed when all configuration is completed

Antivirus, Definitions, Wildfire, etc

Download & install all most recently available

24 items

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOAD...	CURRENTLY INSTALLED	ACTION	DOCUMENTATI...
Antivirus	Last checked: 2022/06/01 19:22:55 UTC	Schedule: None								
4096-4608	panup-all-antivirus-4096-4608		Full	95 MB	9df183462...	2022/05/28 11:03:56 UTC			Download	Release Notes
4097-4609	panup-all-antivirus-4097-4609		Full	95 MB	7679d3b4e...	2022/05/29 11:04:03 UTC			Download	Release Notes
4098-4610	panup-all-antivirus-4098-4610		Full	95 MB	1b47929c0...	2022/05/30 11:01:52 UTC			Download	Release Notes
4099-4611	panup-all-antivirus-4099-4611		Full	96 MB	19eb464a4...	2022/05/31 11:03:33 UTC			Download	Release Notes
4100-4612	panup-all-antivirus-4100-4612		Full	96 MB	9a40ca027...	2022/06/01 11:01:40 UTC	✓	✓		Release Notes
Applications and Threats	Last checked: 2022/06/01 19:22:53 UTC	Schedule: Every Wednesday at 01:02 (Download only)								
8564-7375	panupv2-all-contents-8564-7375	Apps, Threats	Full	54 MB	8237e8fb2...	2022/05/03 02:03:23 UTC			Download	Release Notes
8565-7379	panupv2-all-contents-8565-7379	Apps, Threats	Full	54 MB	ff46a43b82...	2022/05/04 04:59:52 UTC			Download	Release Notes
8566-7381	panupv2-all-contents-8566-7381	Apps, Threats	Full	54 MB	dcc592245...	2022/05/06 03:38:48 UTC			Download	Release Notes
8567-7386	panupv2-all-contents-8567-7386	Apps, Threats	Full	54 MB	bd9e1ac67...	2022/05/10 04:10:01 UTC			Download	Release Notes
8568-7388	panupv2-all-contents-8568-7388	Apps, Threats	Full	54 MB	2d8603658...	2022/05/10 17:12:37 UTC			Download	Release Notes
8569-7390	panupv2-all-contents-8569-7390	Apps, Threats	Full	54 MB	61f0c3f952...	2022/05/12 21:05:33 UTC			Download	Release Notes
8570-7393	panupv2-all-contents-8570-7393	Apps, Threats	Full	54 MB	7bd70d6a5...	2022/05/16 23:47:55 UTC			Download	Release Notes
8571-7398	panupv2-all-contents-8571-7398	Apps, Threats	Full	54 MB	f3a0ee0e2d...	2022/05/18 20:25:48 UTC			Download	Release Notes
8572-7403	panupv2-all-contents-8572-7403	Apps, Threats	Full	54 MB	57c63c6c4...	2022/05/24 00:43:06 UTC			Download	Release Notes
8573-7406	panupv2-all-contents-8573-7406	Apps, Threats	Full	54 MB	8e7f34b07...	2022/05/25 03:52:40 UTC			Download	Release Notes
8574-7407	panupv2-all-contents-8574-7407	Apps, Threats	Full	54 MB	15446b748...	2022/05/26 22:14:25 UTC			Download	Release Notes

Check Now Upload Install From File

FIXING RCE PRESENT IN 10.0.0

Links below to CVE for vulnerabilities:

Update to 10.0.8 for CVE-2021-2050

CVE-2021-3050 PAN-OS: OS Command Injection Vulnerability in Web Interface (paloaltonetworks.com)

Disable Telnet on management interface to mitigate CVE-2020-10188

CVE-2020-10188 PAN-OS: Impact of Telnet Remote-Code-Execution (RCE) Vulnerability (CVE-2020-10188) (paloaltonetworks.com)

Device > Setup > Management > General Settings

Set timezone and time for accurate logging

Set login banner if time allows

Reference link:

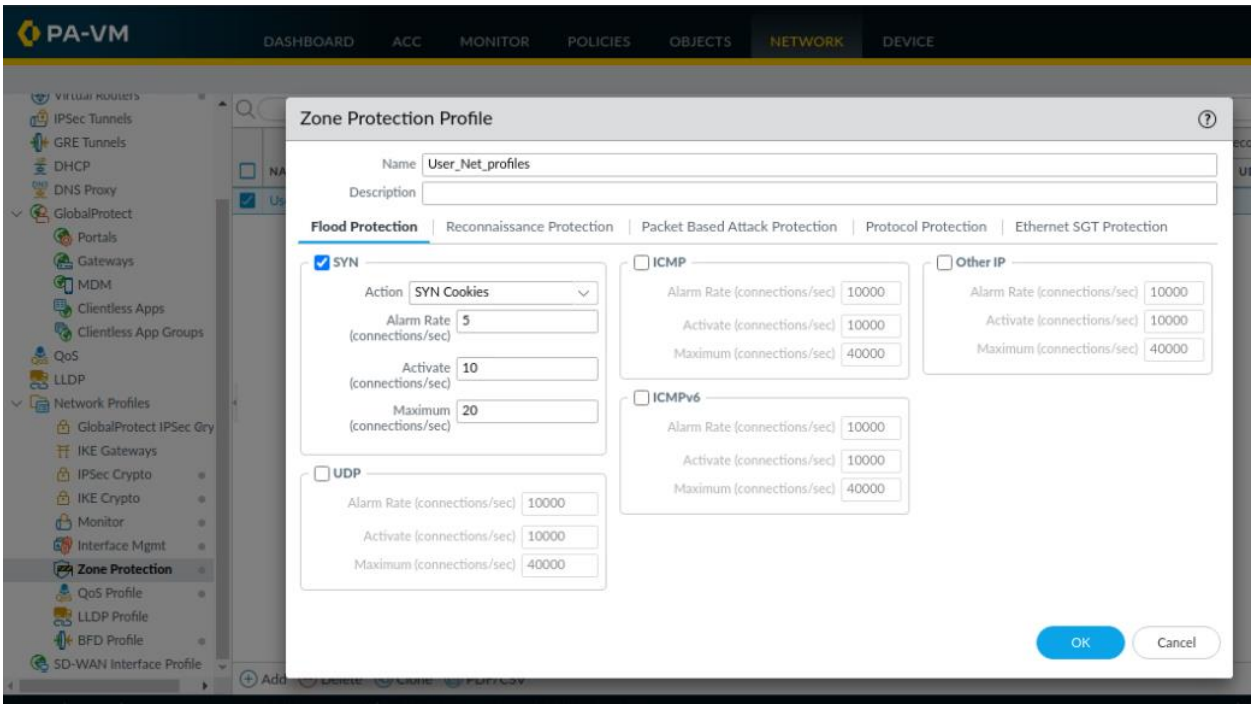
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/getting-started/integrate-the-firewall-into-your-management-network/perform-initial-configuration

Zone protection profiles

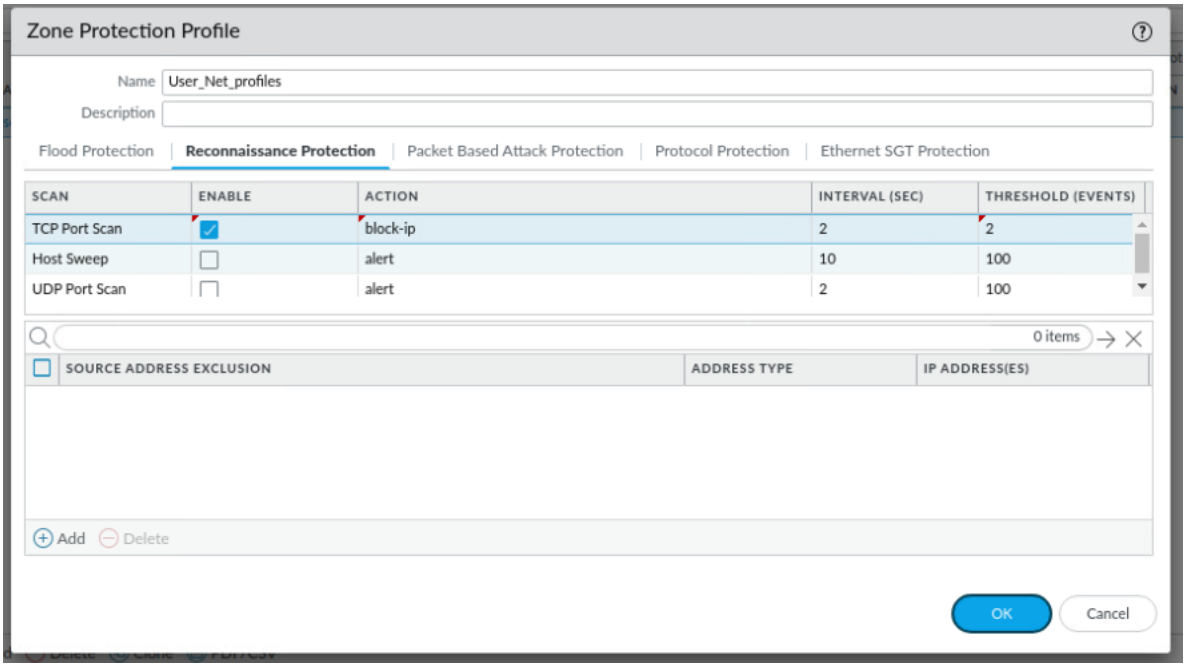
Ref Lab 6

Stop SYN Flood attacks:

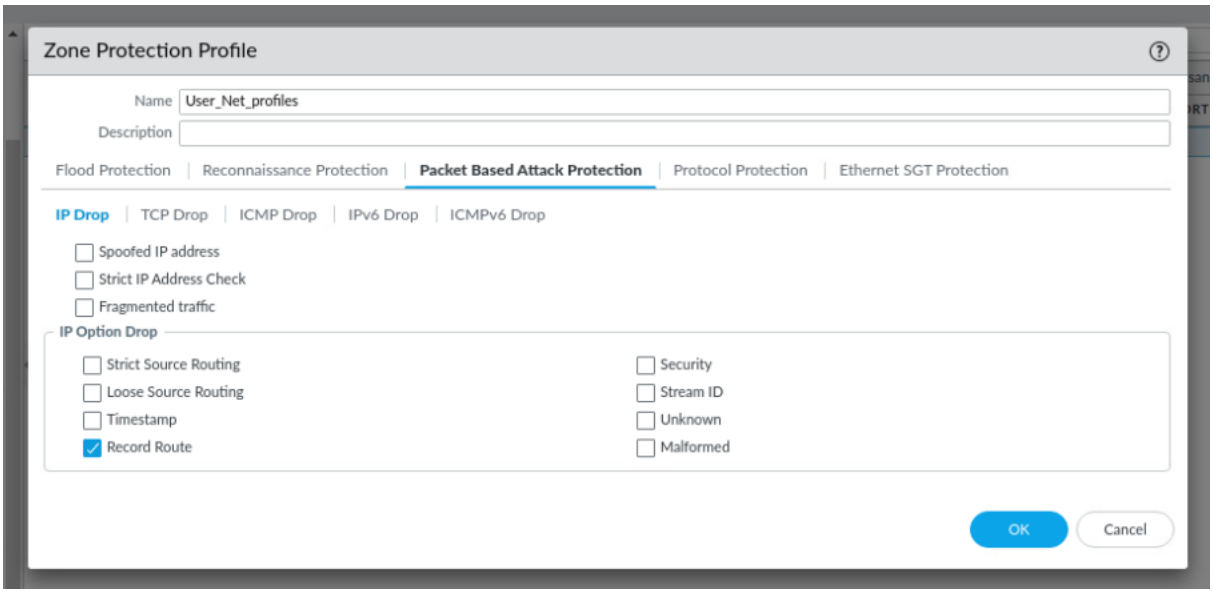
Use numbers greater than SYN Flood example if implementing DoS protection so DoS protection hits SYN Flood limits first.



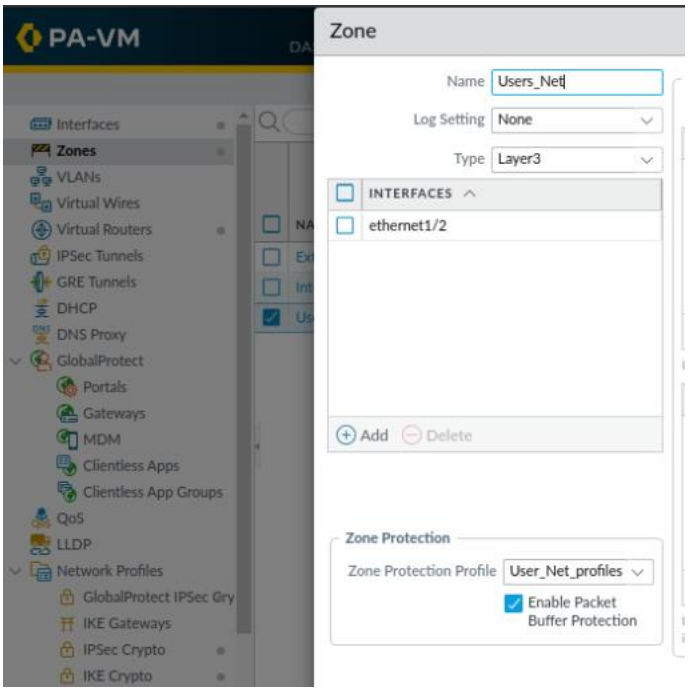
Block TCP Port Scan from entering the network:



Block Ip Route Recorders: (ex: traceroute and nmap equivalent)



Apply profile to zone:



much faster to create profiles in GUI, do not attempt through cli as there are too many default values to reasonably enter quickly.

set network profiles zone-protection-profile ZoneProtectionProfile flood icmp enable yes

set network profiles zone-protection-profile ZoneProtectionProfile flood icmpv6 enable yes

set network profiles zone-protection-profile ZoneProtectionProfile flood other-ip enable yes

set network profiles zone-protection-profile ZoneProtectionProfile flood tcp-syn enable yes

set network profiles zone-protection-profile ZoneProtectionProfile flood udp enable yes

Apply zone protection profile to zones:

set zone dmz-zone network zone-protection-profile ZoneProtectionProfile

set zone internal-zone network zone-protection-profile ZoneProtectionProfile

set zone public-zone network zone-protection-profile ZoneProtectionProfile

DoS Protection: (unlikely but not impossible)

Considering option of zone protection profile instead? Seems to have similar functionality but DoS will blacklist source IPs of DoS?

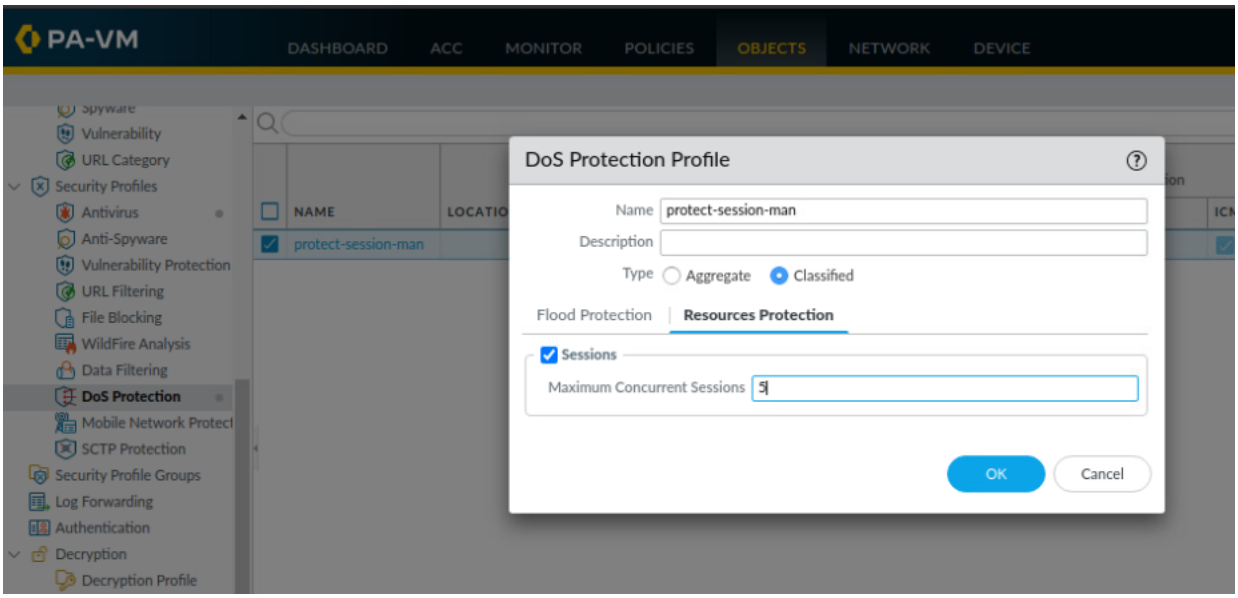
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClW6CAK#:~:text=A%20DoS%20protection%20policy%20can%20be%20used%20to,threshold%20that%20applies%20to%20a%20single%20source%20IP.

Ref Lab 6 of Palo Alto Academy

This will drop packets send from commands like: *nmap --script http-slowloris --max-parallelism 10 192.168.50.80*

Objects > DoS Protection > add

Classified Option allows for object assignment in DoS Policy.



Implement DoS Protection Policy:

Policies > DoS Protection > add

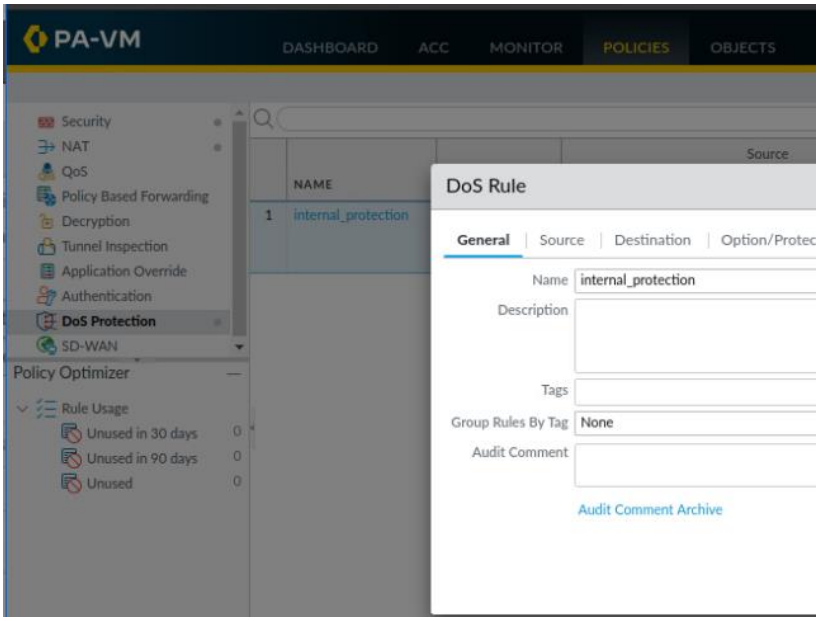
General > name

Source > external zone

Destination > internal zones

Options > Action: Deny or Protect

Classified > Profile > select name of DoS Protection Profile made in previous step.



may be faster to gui

set profiles dos-protection DosProtection type classified flood udp enable yes

set profiles dos-protection DosProtection type classified flood tcp-syn enable yes

set profiles dos-protection DosProtection type classified flood icmp enable yes

Apply to policy

set rulebase dos rules DOSPolicy service any source any destination any action deny

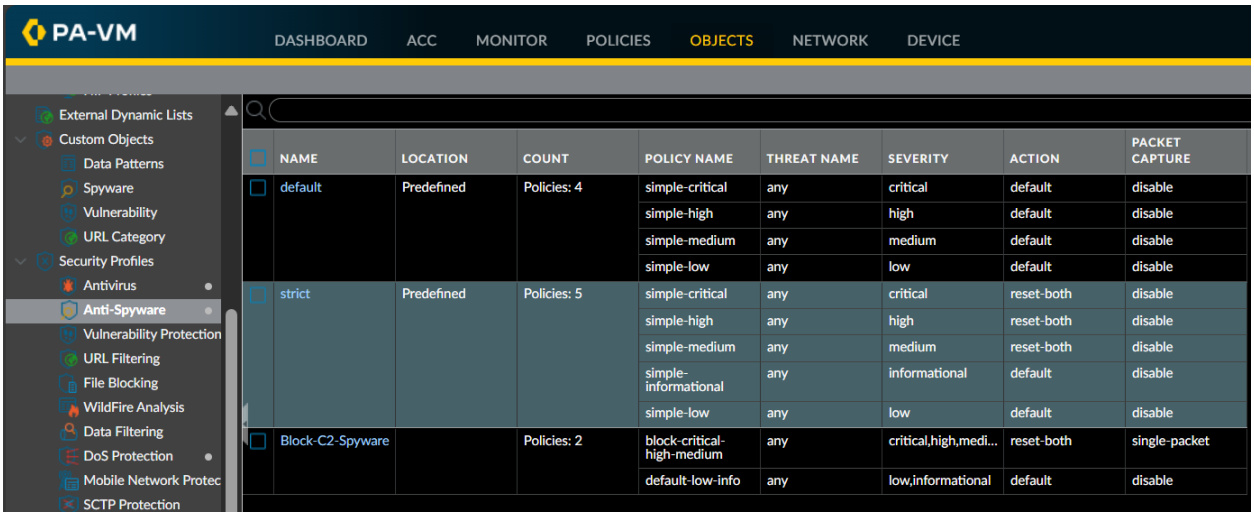
set rulebase dos rules DOSPolicy to zone [internal-zone public-zone dmz-zone]

set rulebase dos rules DOSPolicy from zone external-zone

set rulebase dos rules DOSPolicy protection classified profile dosprotection classification-criteria address source-ip-only

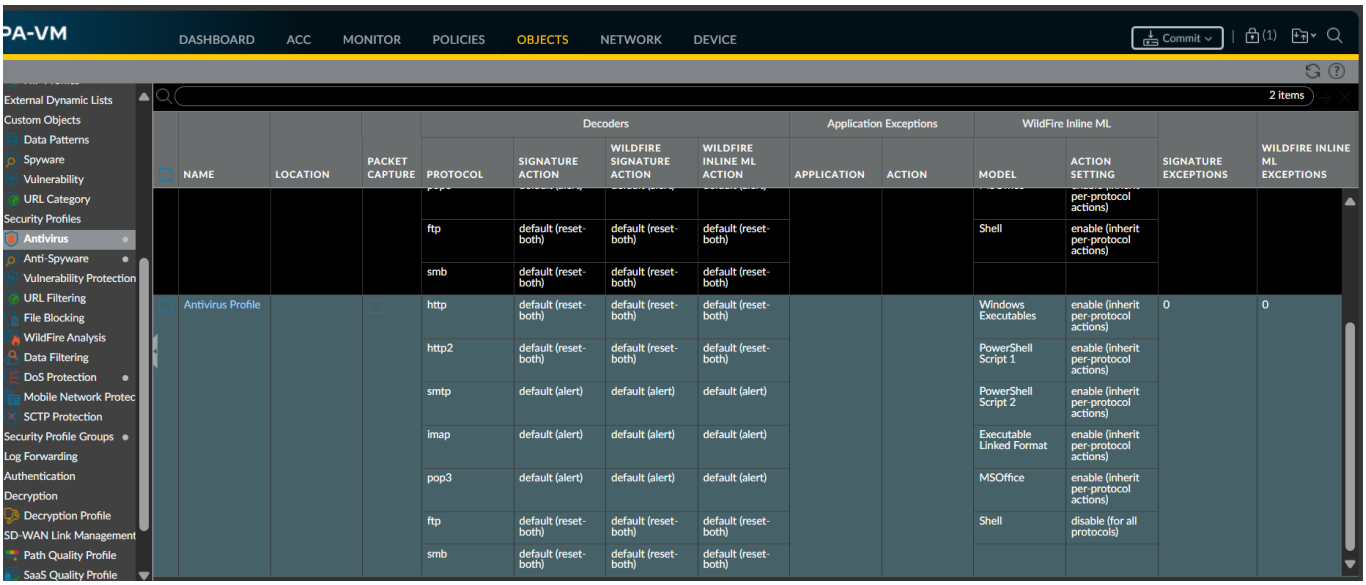
Antivirus & Anti-Spyware profiles:

Objects > Anti-Spyware > strict policy is good enough

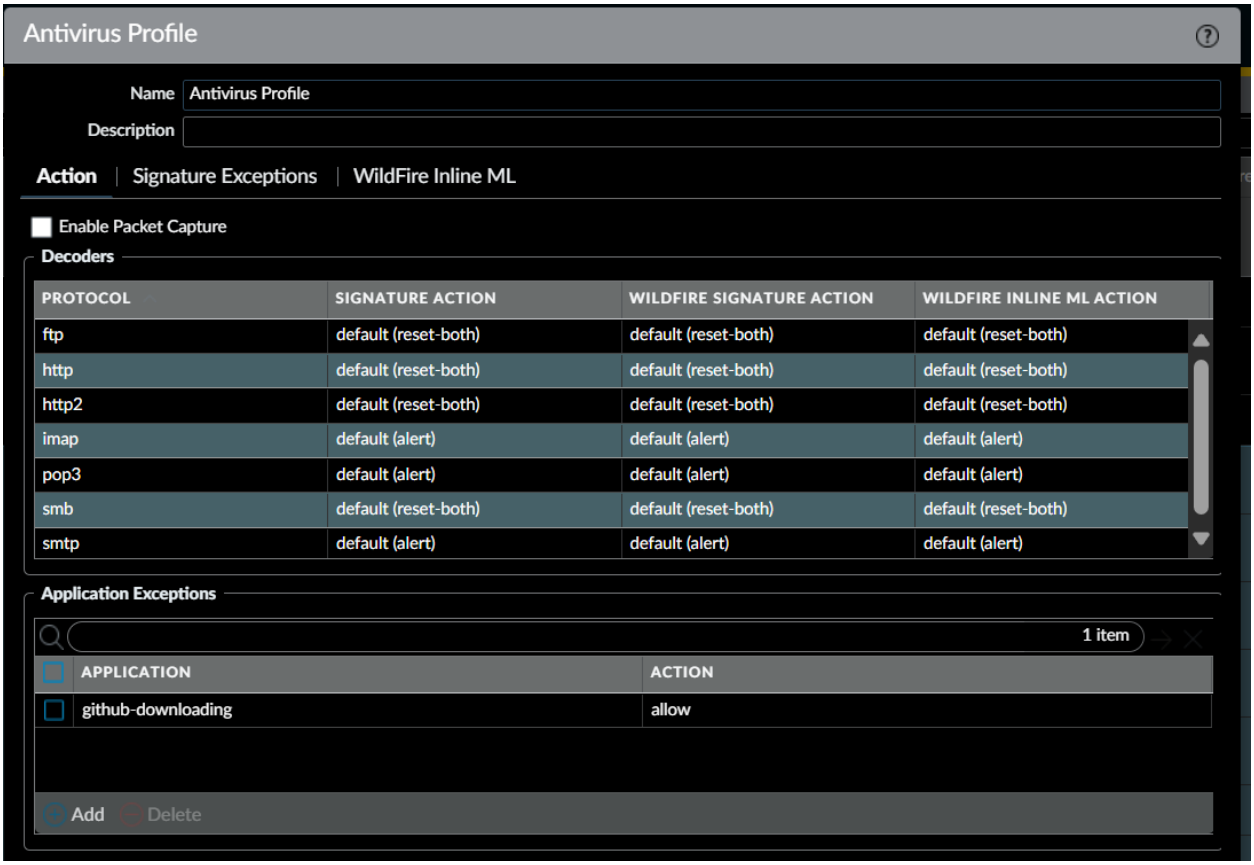


NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
			simple-high	any	high	default	disable
			simple-medium	any	medium	default	disable
			simple-low	any	low	default	disable
strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple-informational	any	informational	default	disable
			simple-low	any	low	default	disable
Block-C2-Spyware		Policies: 2	block-critical-high-medium	any	critical,high,medi...	reset-both	single-packet
			default-low-info	any	low,informational	default	disable

Objects > Antivirus > create new



NAME	LOCATION	PACKET CAPTURE	Decoders				Application Exceptions		WildFire Inline ML		SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
			PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	APPLICATION	ACTION	MODEL	ACTION SETTING		
										per-protocol actions)		
			ftp	default (reset-both)	default (reset-both)	default (reset-both)			Shell	enable (inherit per-protocol actions)		
			smb	default (reset-both)	default (reset-both)	default (reset-both)						
Antivirus Profile			http	default (reset-both)	default (reset-both)	default (reset-both)			Windows Executables	enable (inherit per-protocol actions)	0	0
			http2	default (reset-both)	default (reset-both)	default (reset-both)			PowerShell Script 1	enable (inherit per-protocol actions)		
			smtp	default (alert)	default (alert)	default (alert)			PowerShell Script 2	enable (inherit per-protocol actions)		
			imap	default (alert)	default (alert)	default (alert)			Executable Linked Format	enable (inherit per-protocol actions)		
			pop3	default (alert)	default (alert)	default (alert)			MSOffice	enable (inherit per-protocol actions)		
			ftp	default (reset-both)	default (reset-both)	default (reset-both)			Shell	disable (for all protocols)		
			smb	default (reset-both)	default (reset-both)	default (reset-both)						



Allow github-downloading

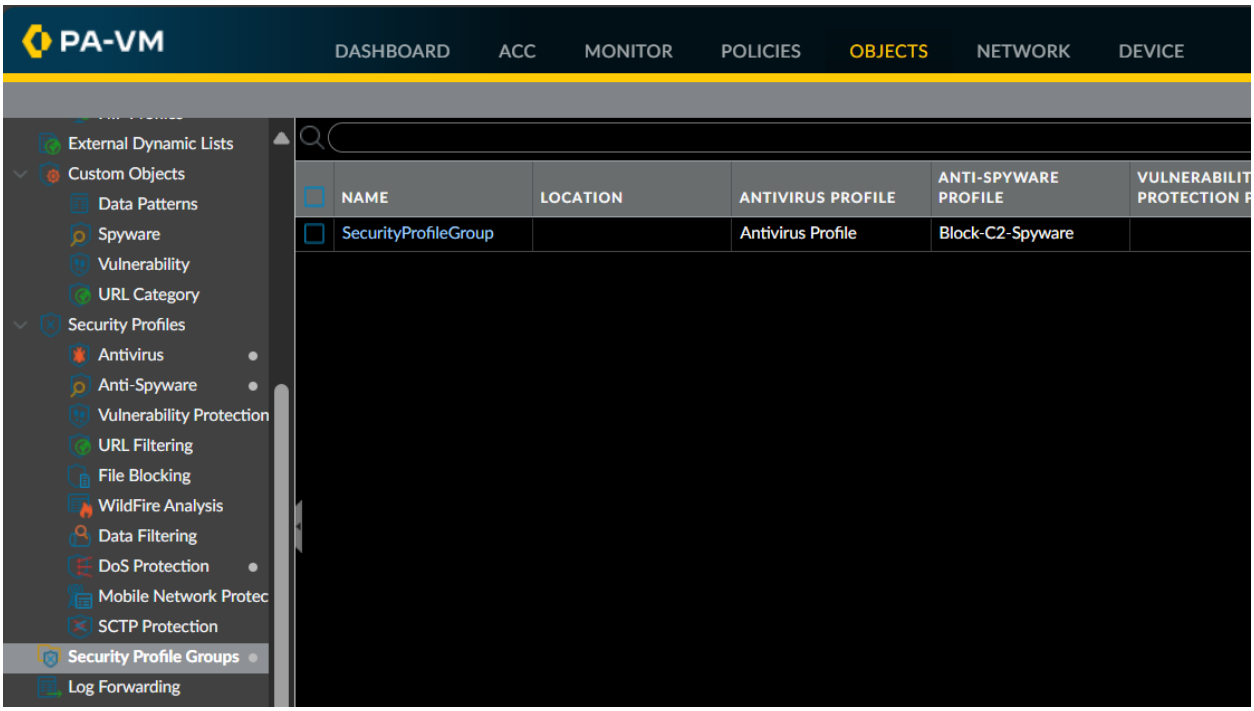
Objects > Security Profile Groups > create new > add policies

CLI: # set profile-group <name> <option>

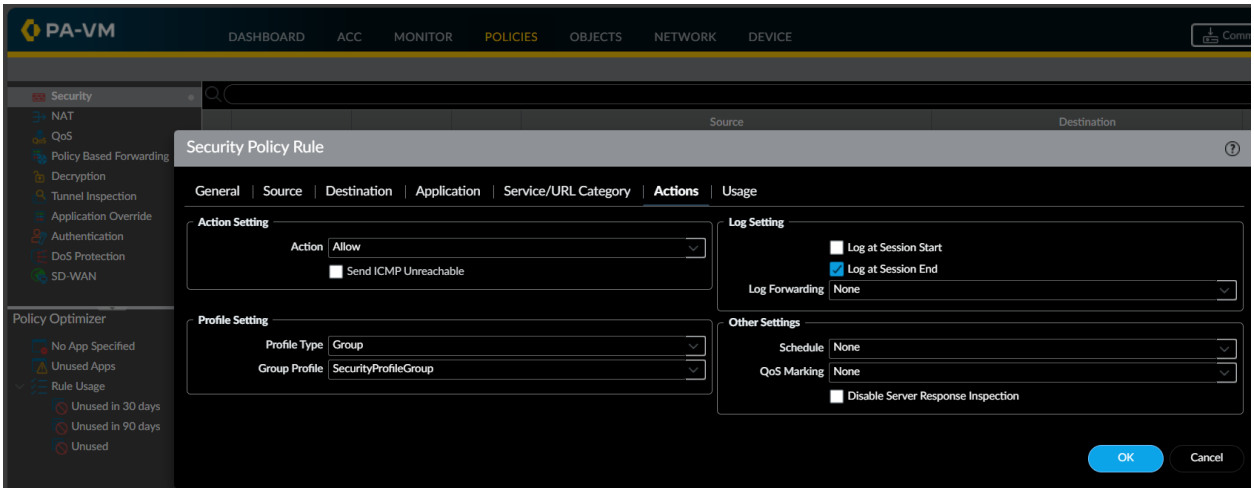
set profile-group SecurityGroup spyware strict virus AntivirusProfile

set rulebase security rules InboundADDNS profile-setting group SecurityGroup

repeat for all inbound security rules



Policies > Security > Edit > Actions > set Profile Setting to Group > select group from dropdown



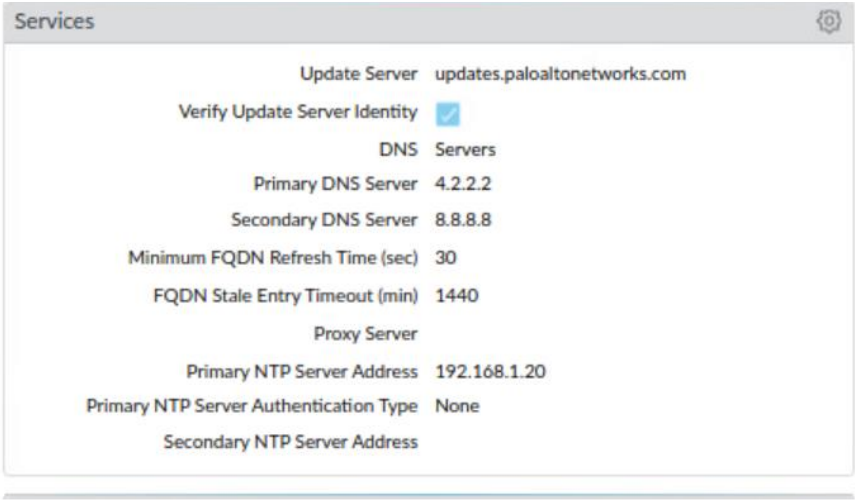
Set DNS

Device > Setup > Services

Primary = 8.8.8.8 (or any valid DNS server)

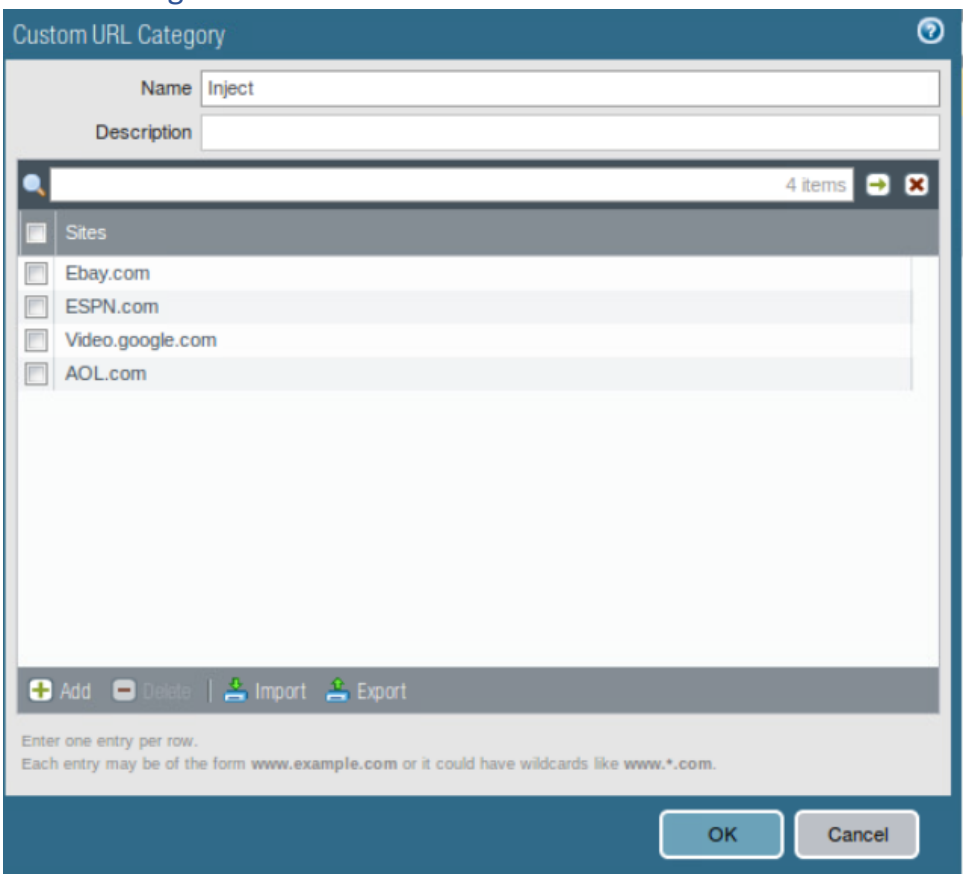
Secondary = 7.7.7.7

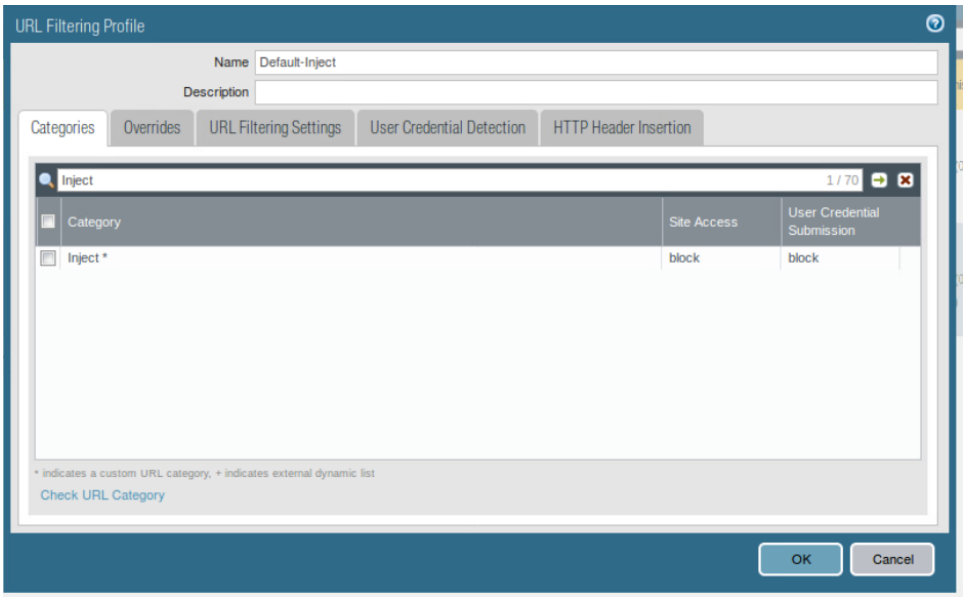
Make sure updates come from updates.paloaltonetworks.com

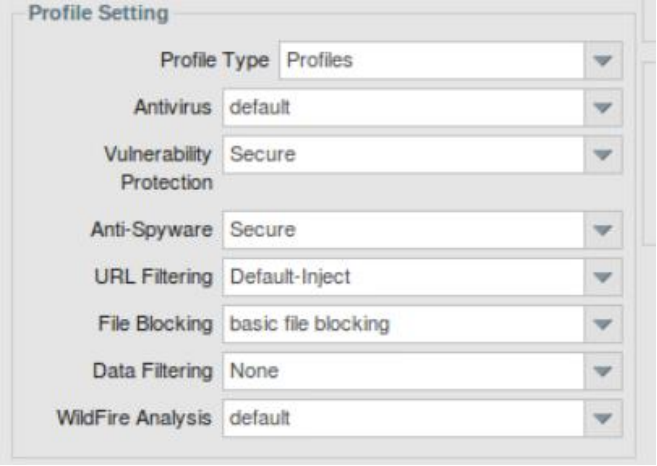


BONUS TODOs & INCIDENT REPORTS

URL Blocking





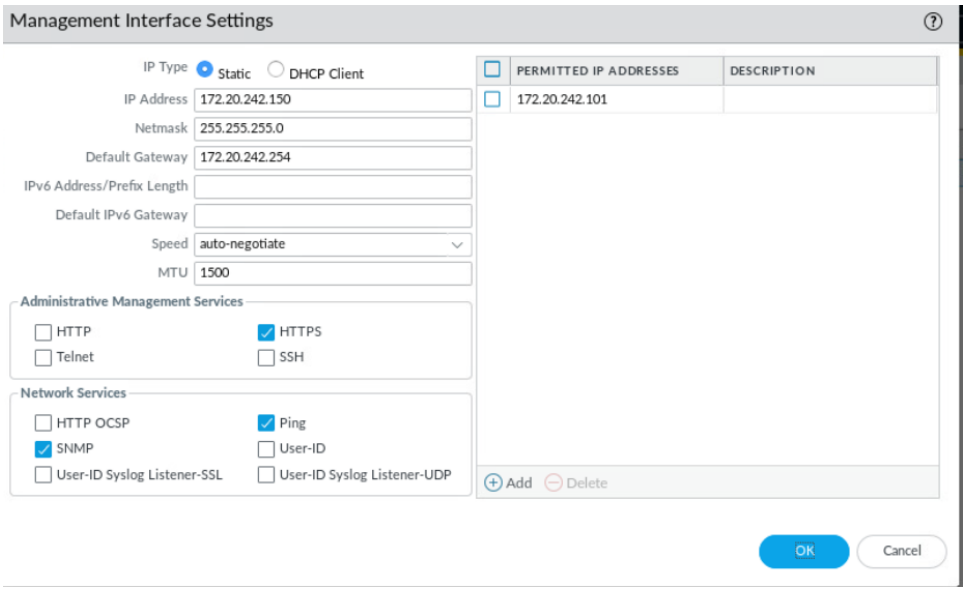


Management Interface

Palo Alto devices can have their management services accessed in two different ways: either through the management interface or through an interface with a management profile. On both Palo Alto devices, the management interface has been secured to only allow ping, HTTPS, and SNMP to communicate with it and has limited connection to their respective Ubuntu workstations. Along with that each ethernet interface on the Palo Altos has had management access disabled.

Below are the screen shots of each Palo Also's management interface and regular interface configuration:

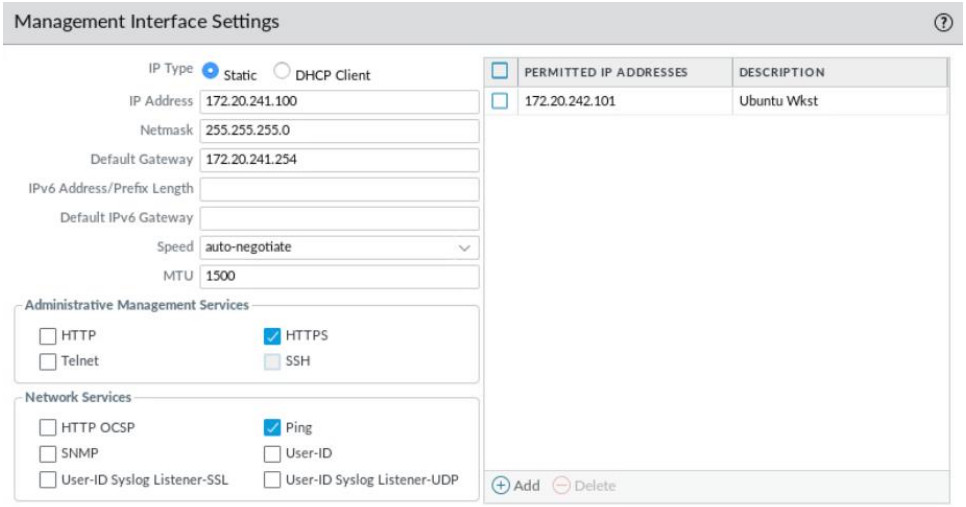
Virtual



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE
ethernet1/1	Layer3	Ping-Response
ethernet1/2	Layer3	Ping-Response
ethernet1/3	Layer3	Ping
ethernet1/4	Layer3	Ping-Response

NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGES	USER-ID	LISTENER-SSL	LISTENER-UDP	IP AD
Ping-Response	✓							✓				
Ping	✓											

Hardware

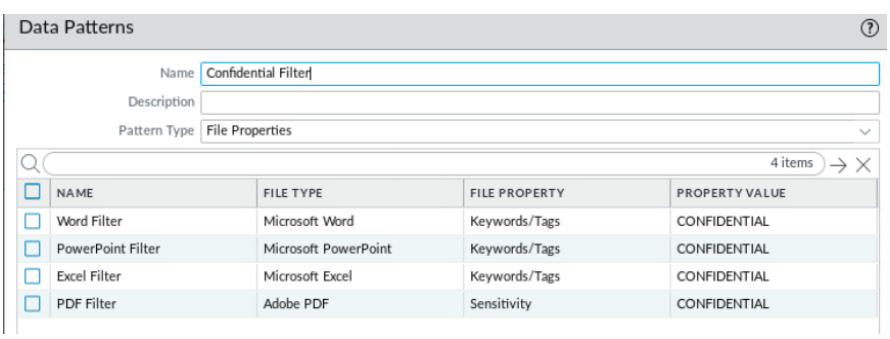


ethernet1/1	Layer3	Ping-Response
ethernet1/2	Layer3	Ping-Response
ethernet1/3	Layer3	Ping
ethernet1/4	Layer3	Manage

NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGES	USER-ID	USER-ID SYSLOG LISTENER-SSL	USER-ID SYSLOG LISTENER-UDP	PERMITTED IP ADDRESSES
Ping-Response	✓							✓				
Ping	✓											
Manage	✓					✓		✓				

DLP (Data Loss Prevention) Policy

A DLP filter has been successfully created on both Palo Altos to filter out files leaving the organization. The Palo Alto has a decryption rule in place to strip off the headers of the files. It then looks at each header and checks it against a data filter rule which states that any Office file with the tags CONFIDENTIAL or a PDF with its sensitivity set to CONFIDENTIAL. If there is a match, the file is blocked from leaving the network. Below are the screenshots of the configuration:



Data Filtering Profile

Name: Confidential Filter

Description:

Data Capture

1 item

	DATA PATTERN	APPLICATIONS	FILE TYPE	DIRECTION	ALERT THRESHOLD	BLOCK THRESHOLD	LOG SEVERITY
	Confidential Filter	any	Adobe PDF Microsoft Excel Microsoft Excel 97-2004 Microsoft PowerPoint Microsoft PowerPoint 97-2004 Microsoft Word Microsoft Word 97-2004	both	1	1	high

Security Profile Group

Name	Main
Antivirus Profile	default
Anti-Spyware Profile	Main
Vulnerability Protection Profile	strict
URL Filtering Profile	default
File Blocking Profile	strict file blocking
Data Filtering Profile	Confidential Filter
WildFire Analysis Profile	default

OK Cancel

Decryption Profile

Name: DLP Decryption

SSL Decryption | No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | SSL Protocol Settings

Server Certificate Verification

- Block sessions with expired certificates
- Block sessions with untrusted issuers
- Block sessions with unknown certificate status
- Block sessions on certificate status check timeout
- Restrict certificate extensions Details
- Append certificate's CN value to SAN extension

Unsupported Mode Checks

- Block sessions with unsupported versions
- Block sessions with unsupported cipher suites
- Block sessions with client authentication

Failure Checks

- Block sessions if resources not available
- Block sessions if HSM not available
- Block downgrade on no resource

Client Extension

- Strip ALPN

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted.

	NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CAT
1	DLP Decryption	none	External Internal User	any	any	any	External	any	any	any

This configuration is applied to all rules allowing connections outbound and inbound on both Palo Altos.

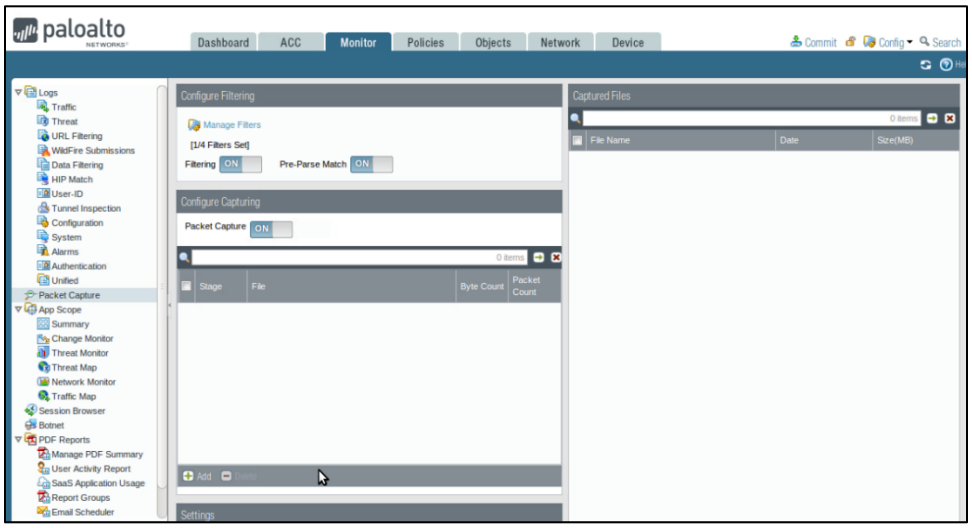
VPN Tunnel

Here is how I would attempt to do it / I ran out of time to write it here is palo docs:

https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/set-up-site-to-site-vpn

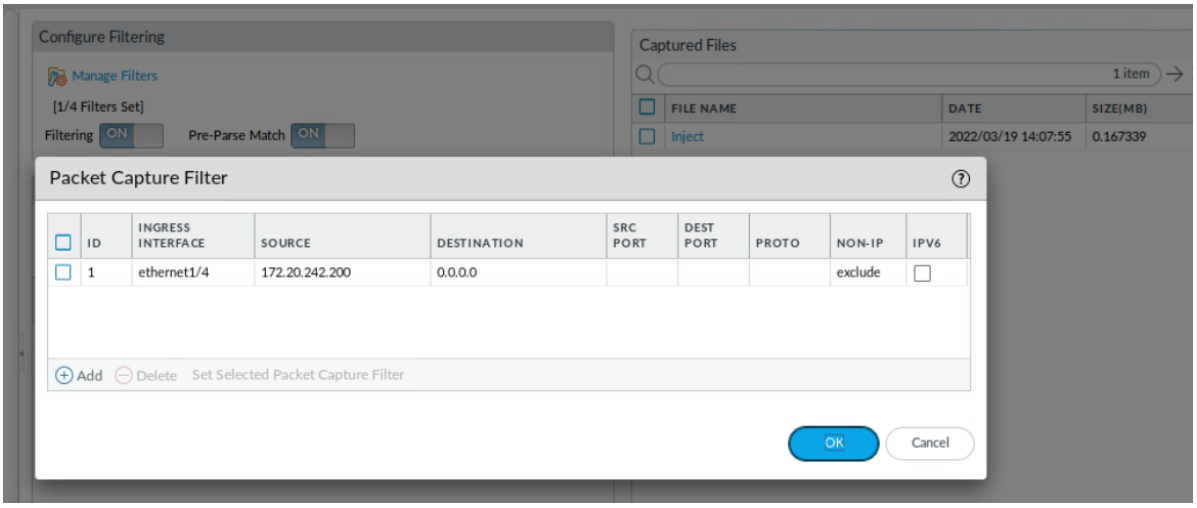
Firewall Packet Capture

Below is the screen capture of the Palo Alto.



The Palo Alto firewall's ability to capture packets is very strong for debugging purposes, as it allows you to see exactly what is being communicated between hosts. This is also good for short-term monitoring of a device that is actively under attack as you can see what is being sent against the host. Below are screenshots of packets being captured from the Windows 2012 host in the Virtual Pod and the scoring engine.

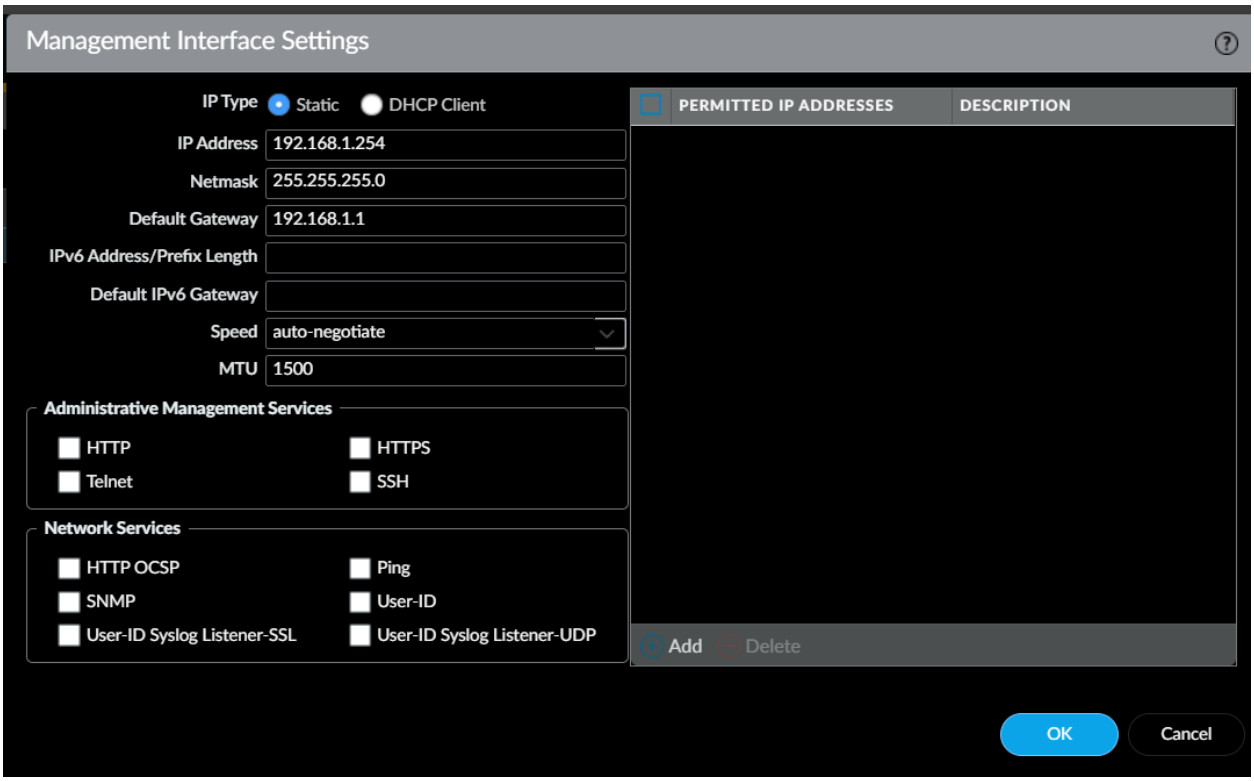
Packet capture filter



*Note: Nmap, Zenmap, Wireshark, etc. are all much better for packet analysis than this firewall but it will do in a pinch. *

Regaining GUI Access:

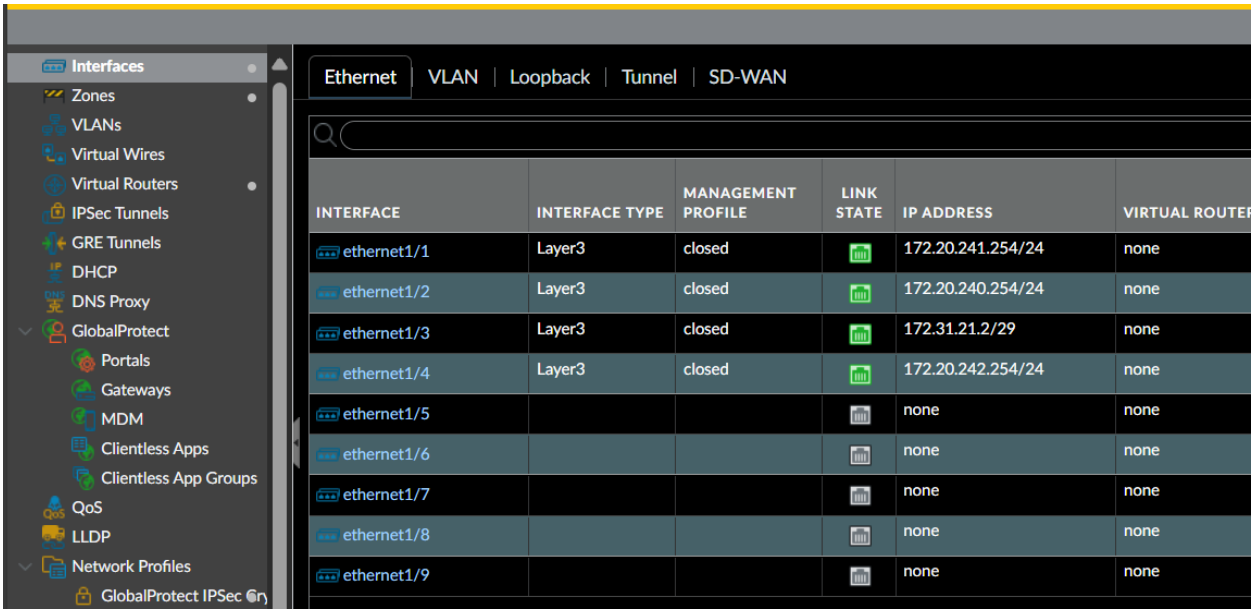
If you committed something like this by accident:



Set deviceconfig system service disable-https no

commit

If you closed all your interfaces:

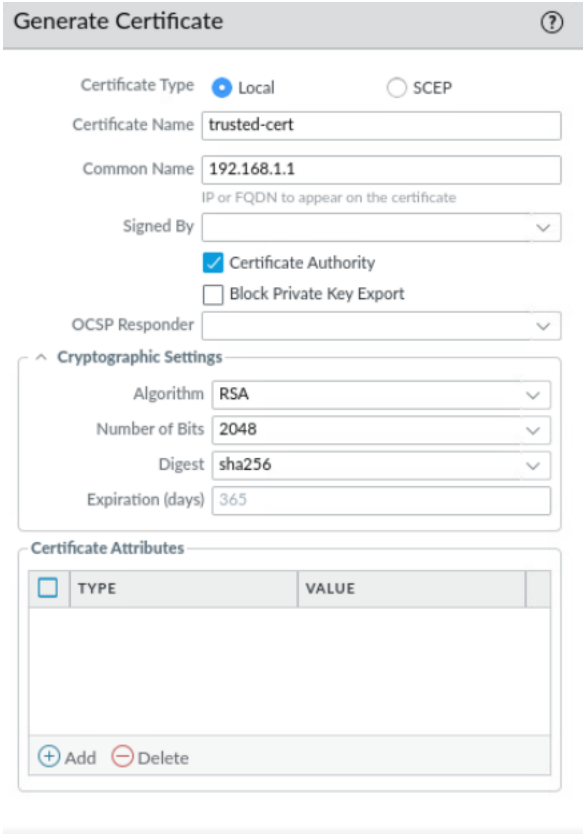


set network interface ethernet ethernet1/4 layer3 interface-management-profile open-mgmt

** ethernet1/? and profile name are subject to change **

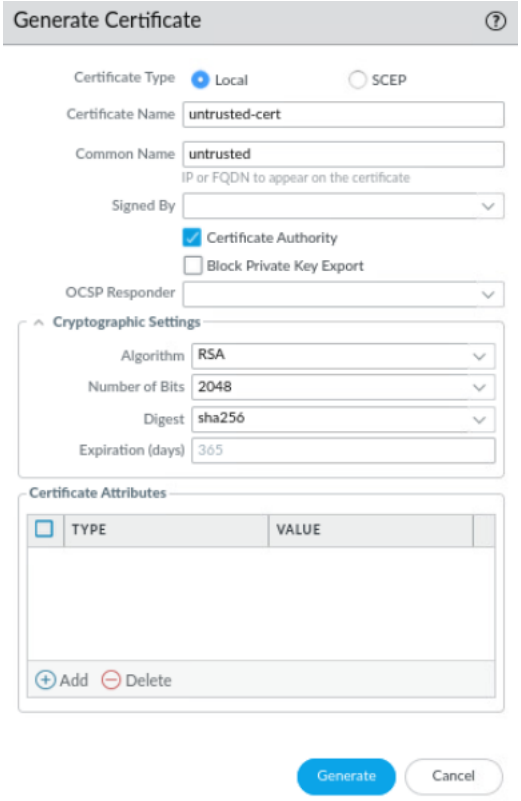
Creating a self-signed certificate for SSL Decryption

Device > Certificates > Generate



Create > Edit > check Forward Trust Certificate

Create second cert for HTTPS website without a cert of have a self-signed cert



Generate > Edit > check Forward Untrust Certificate

Policies > Decryption > Add

Source Zone > Internal / User

Destination Zone > External / DMZ & Internet

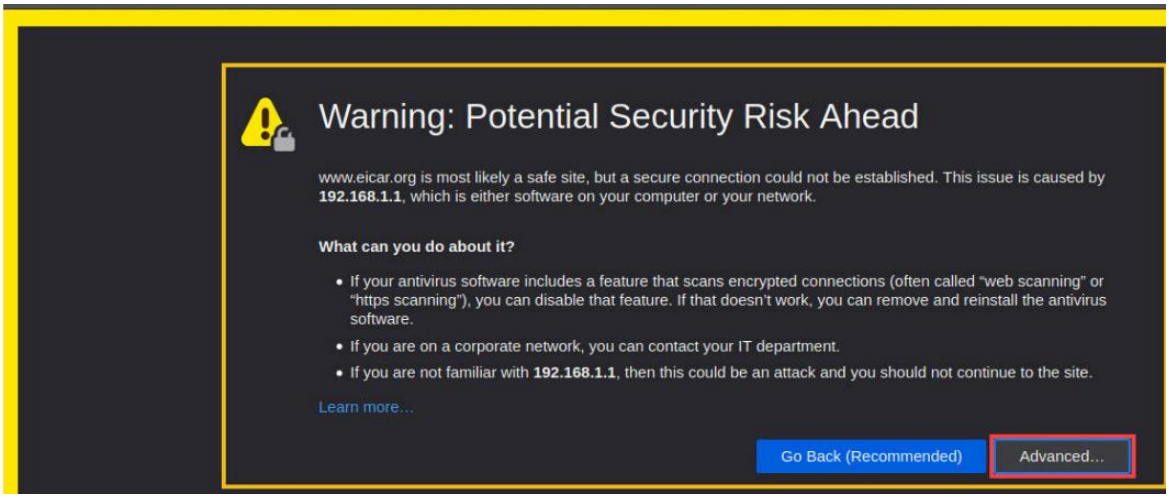
Service/URL category > Any

Options > Action = Decrypt > Type = SSL Forward Proxy > Decryption Profile = none

Commit

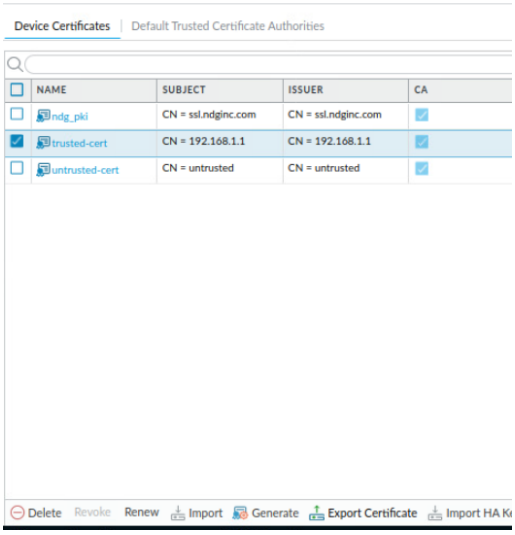
Getting clients to trust a self-signed certificate

If this stage is completed and the following steps are not this will be the result when accessing most websites:

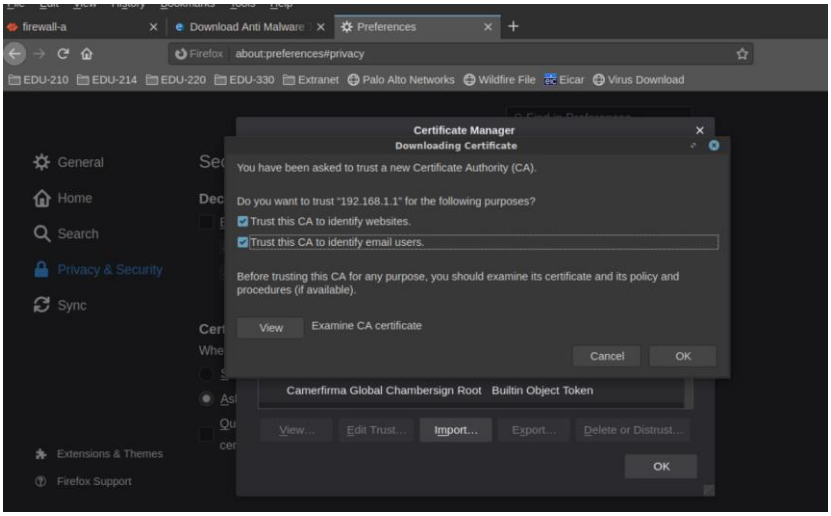


This is because the client (your computer) does not trust the certificate signed by the firewall. (Duh)

Select and export the trusted certificate:



Then just import the certificate into your browser:



This isn't the greatest or a complete solution to fix this across the network, but I guess it works for immediate/temporary fix.

Please Note

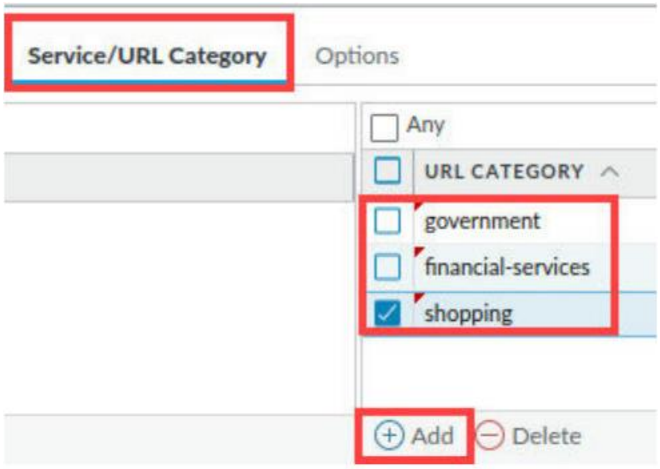
The filter syntax "flags has proxy" displays entries which have been decrypted (the value will show as **yes** in the **Decrypted** column). Entries that match the filter indicate that the firewall carried out a proxy connection for decryption.

Sample Threat log showing malware file blocking in action:

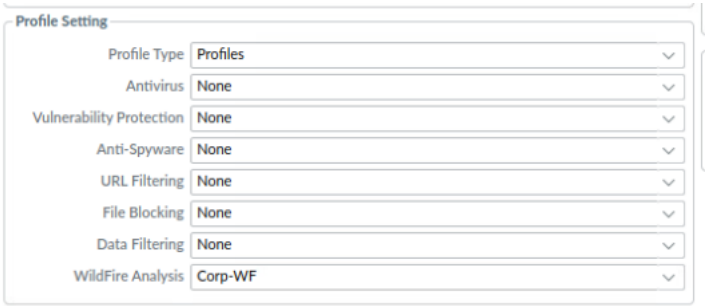
	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLI
	02/29 20:31:01	virus	Eicar Test File	Users_Net	Extranet	192.168.1.20			192.168.50.80			80	web-b

Protecting Personally Identifiable Information from being decrypted:

Add government, financial-services, and shopping to a second, no decrypt, decryption policy and make sure it is above all other policies.



Blocking Unknown Malicious Files with Wildfire
Apply a wildfire analysis policy to a security rule:



Any files that are unknown and may be malicious may take up to 15 minutes to report to:

Monitor > logs > Wildfire Submissions

IPSec VPN Tunnel:

1. Creating a New IPSec Tunnel
    a. Navigate to the "Network" menu and then click on "IPSec Tunnels."
    b. Click on "Add" to create a new IPSec tunnel.
2. Configuring IPSec Tunnel Parameters
    a. Give your VPN tunnel a name that helps you identify it easily.
    b. Select or create an IKE Gateway, which contains information about the remote device (FTD).
    c. Choose an IPSec Crypto Profile that specifies how data will be encrypted and authenticated.
    d. Specify the local and peer IP addresses, which are the IP addresses of your Palo Alto firewall and the FTD device respectively.
3. Setting Up IKE Phase 1 and Phase 2 Parameters
    a. Configure Phase 1 settings including encryption, integrity, DH group, lifetime, and authentication method.
    b. Configure Phase 2 settings including encryption, integrity, lifetime, and PFS (Perfect Forward Secrecy).
4. Defining Proxy ID Settings
    a. Configure Proxy ID settings to specify which remote subnets can communicate through the VPN tunnel.
5. Creating Security Policies
    a. Create security policies that allow traffic to flow through the VPN tunnel.
    b. Specify the source and destination zones, addresses, and services.

Helpful Configuration links:

Decryption Profile:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-profile

Site-to-Site IPSec VPN:

https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/set-up-site-to-site-vpn

Threat packet captures:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-threat-packet-capture#id7e4dc92e-d3ce-4e2b-b180-8bf1566fb221