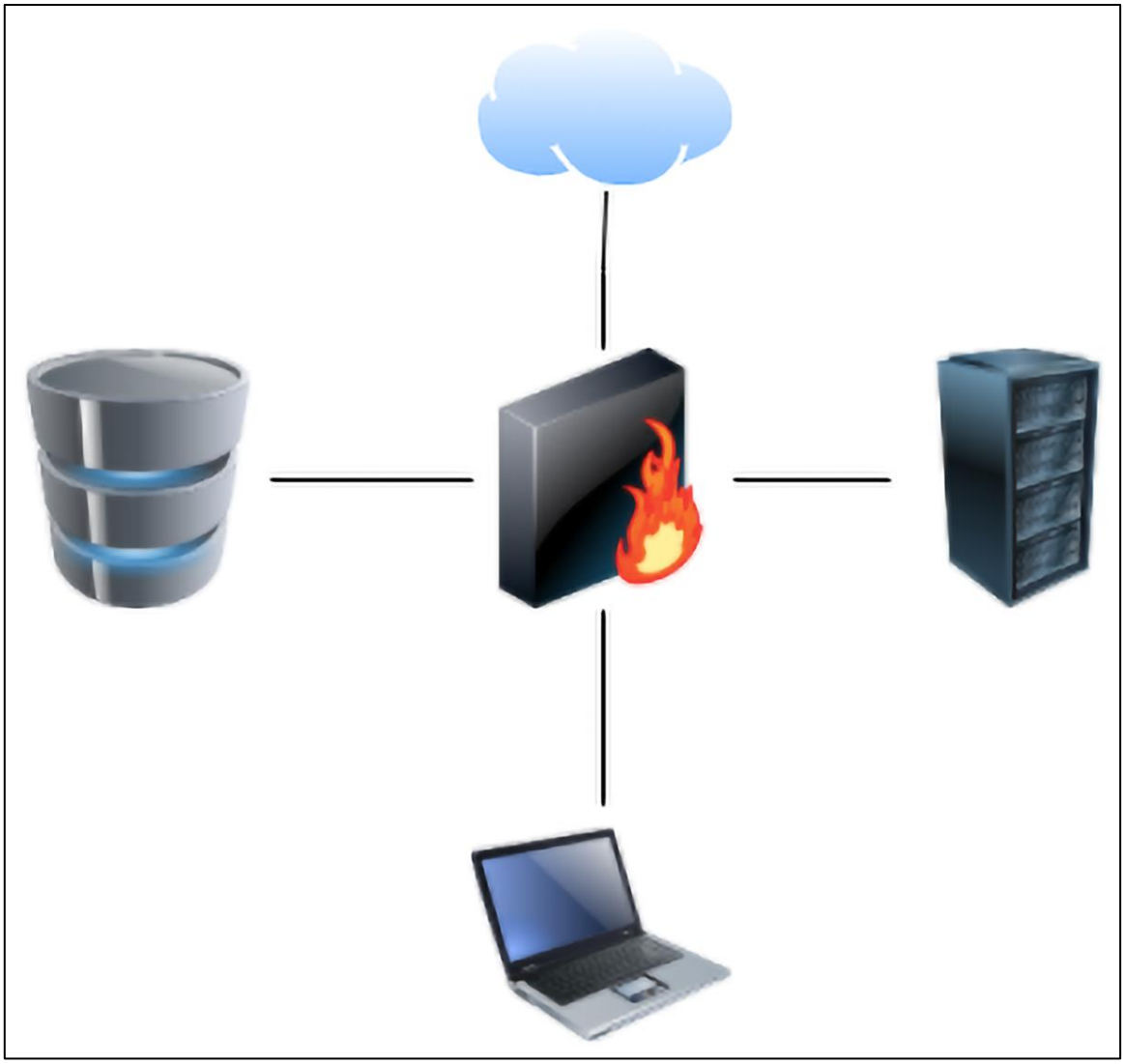
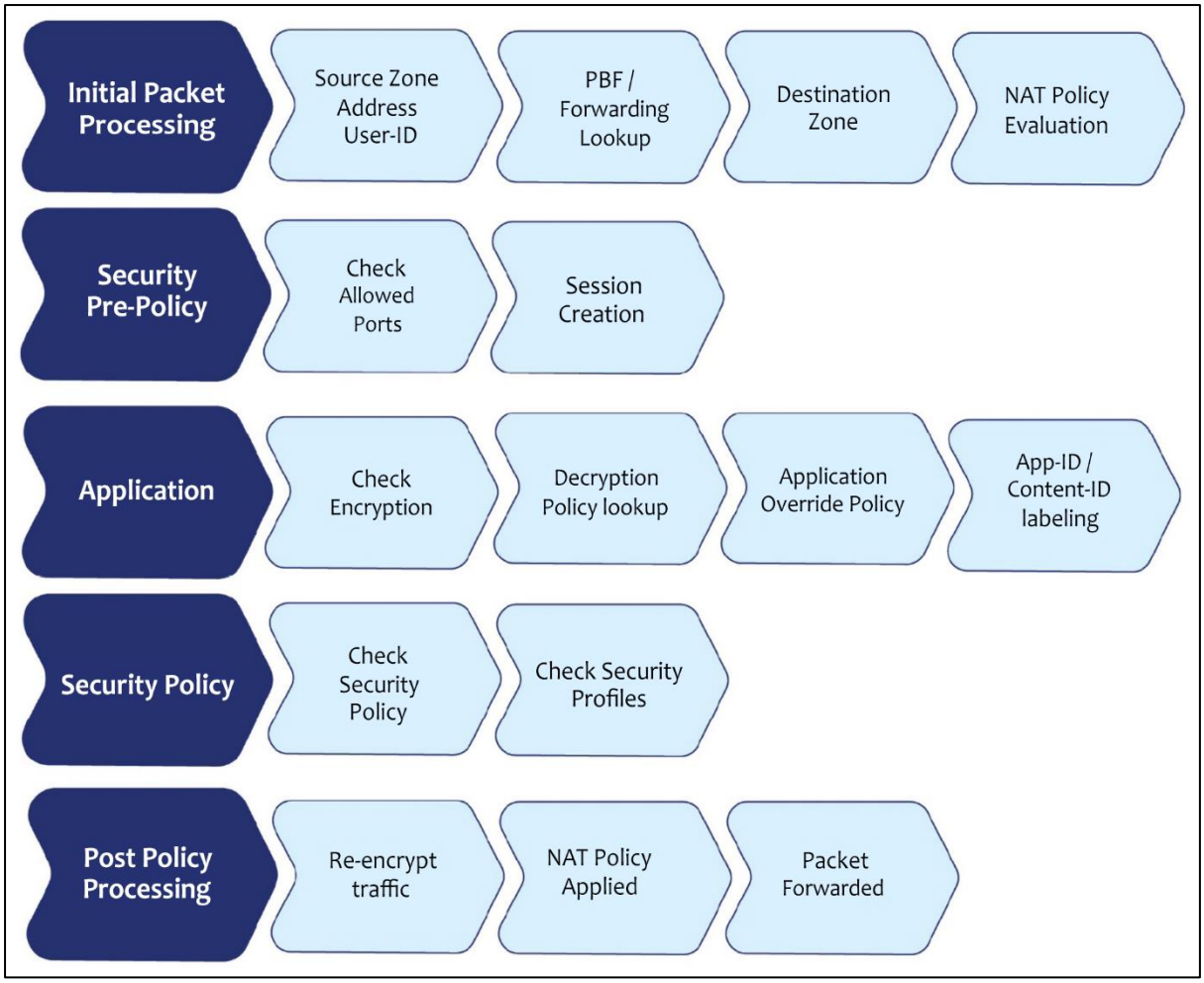
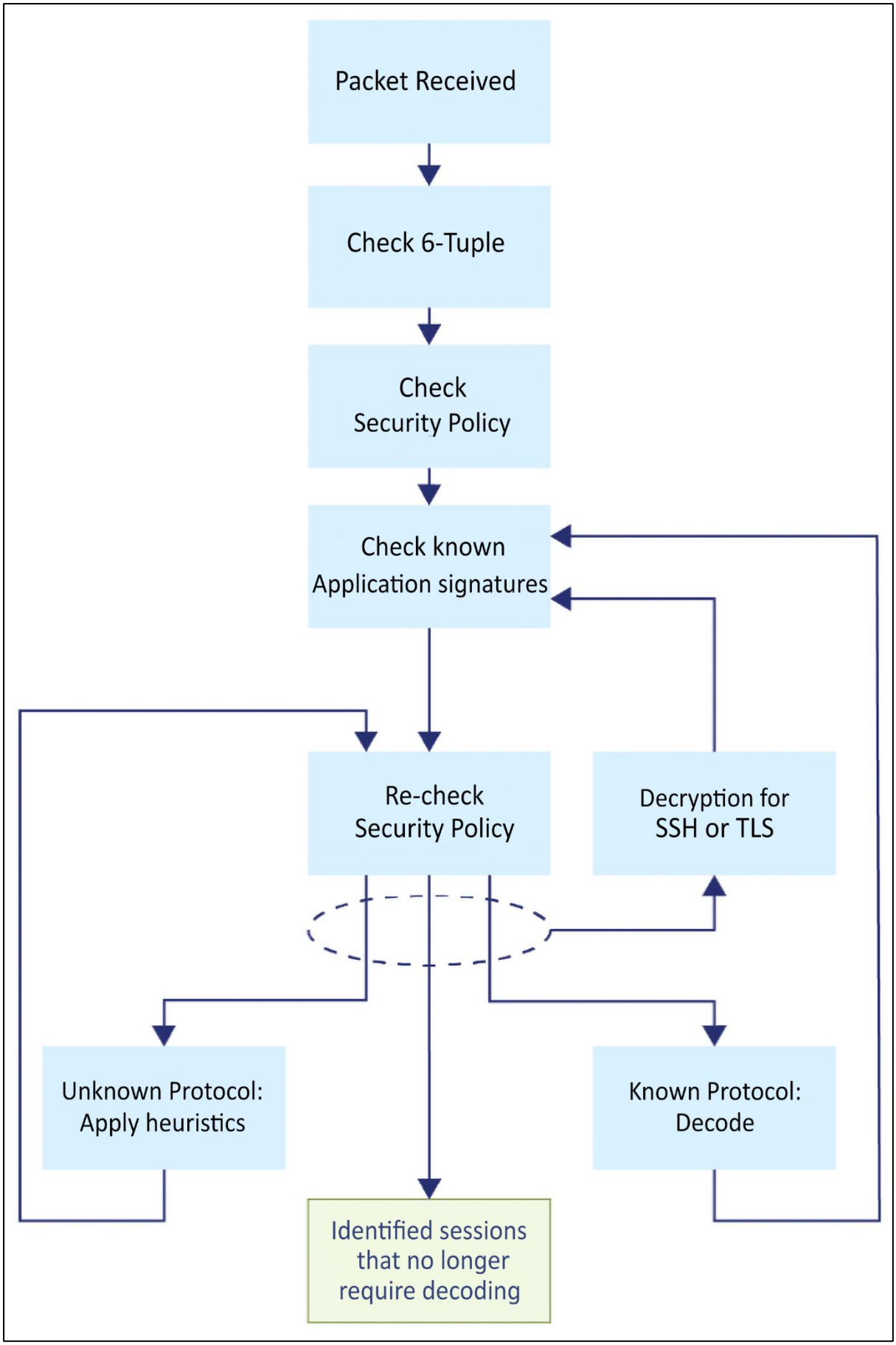
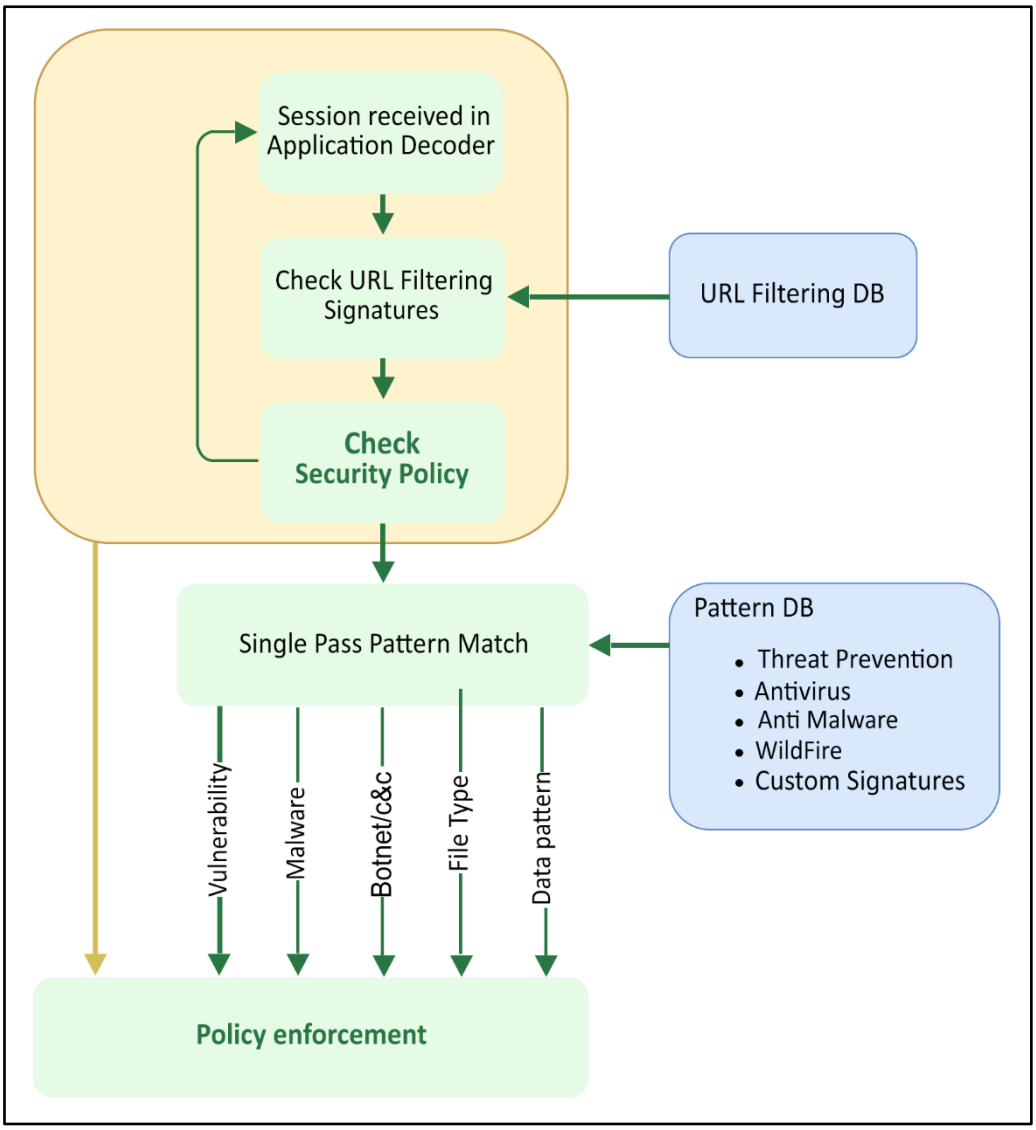
Chapter 1: Understanding the Core Technologies





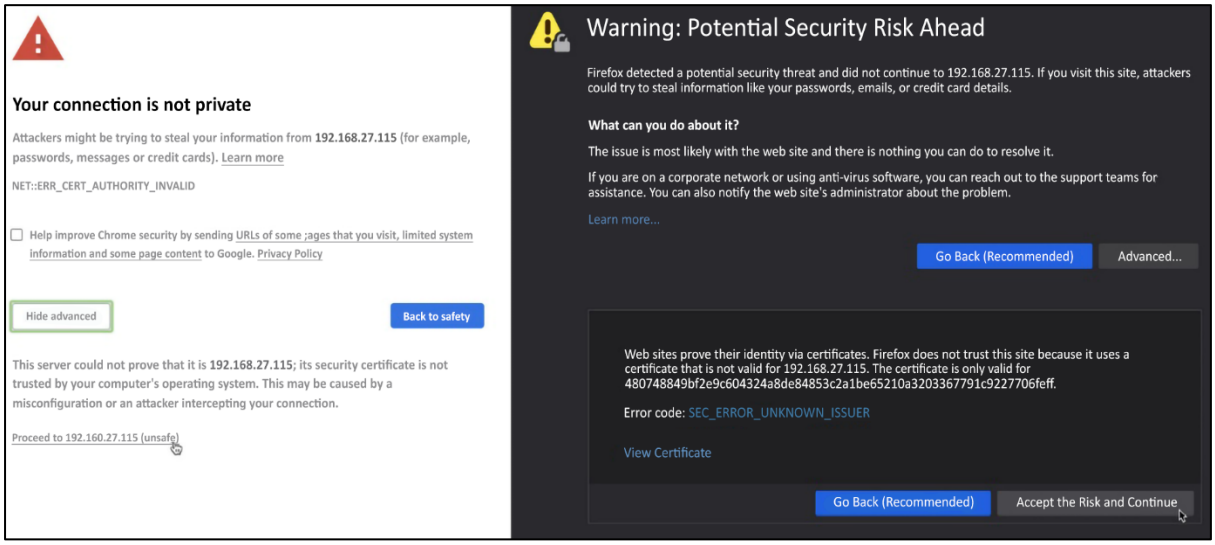
			Source		Destination						
	NAME	TYPE	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	intrazone	intrazone	DMZ LAN	any	(intrazone)	any	allowed web apps	application-default	Allow		
2	interzone	interzone	DMZ LAN	any	DMZ LAN	any	allowed web apps	application-default	Allow		
3	universal	universal	DMZ LAN	any	DMZ LAN	any	allowed web apps	application-default	Allow		
4	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-default	interzone	any	any	any	any	any	any	Deny	none	none

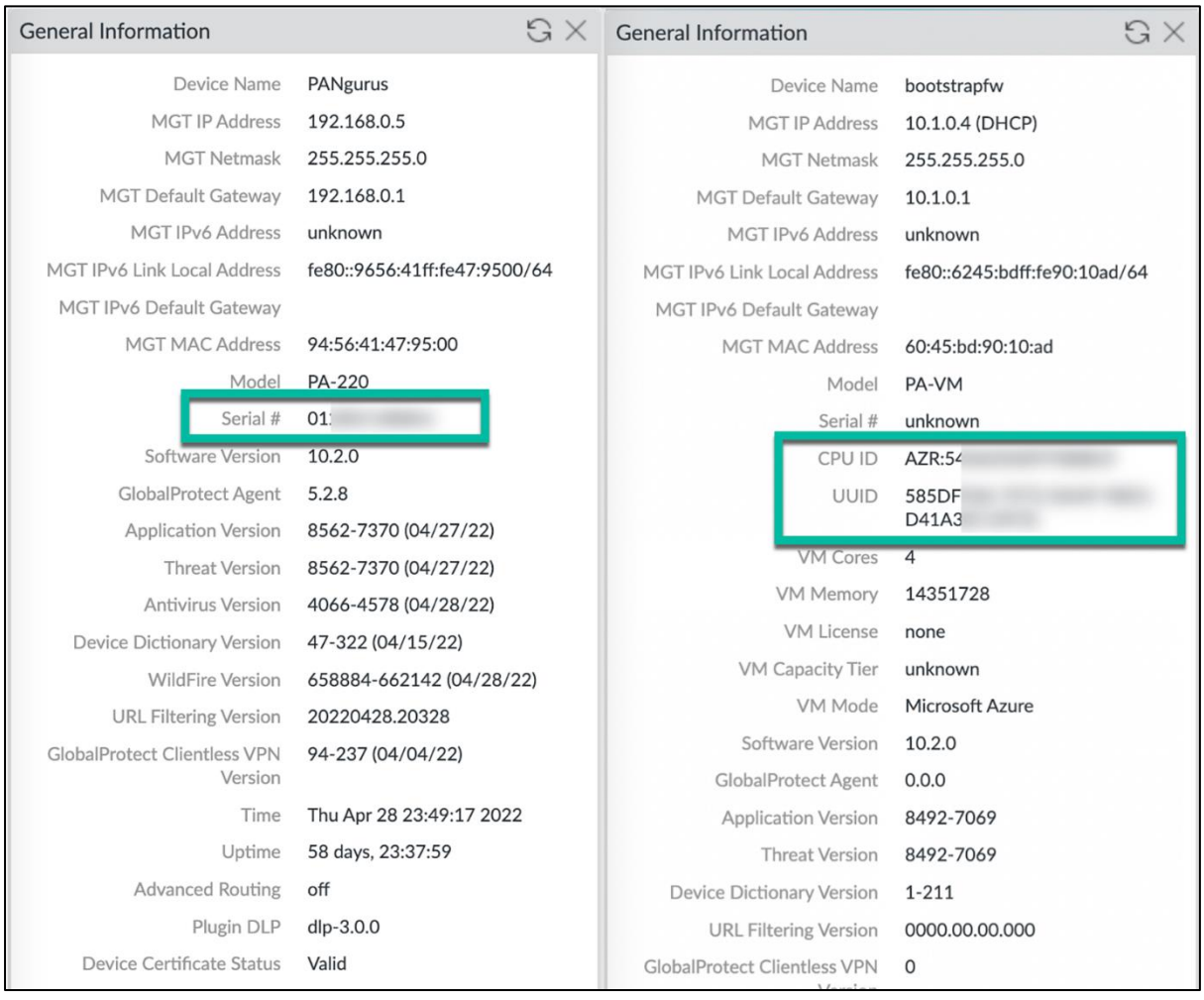

Packet Received
Check 6-Tuple
Check
Security Policy
Check known
Application signatures
Re-check
Security Policy
Decryption for
SSH or TLS
Unknown Protocol:
Apply heuristics
Known Protocol:
Decode
Identified sessions
that no longer
require decoding

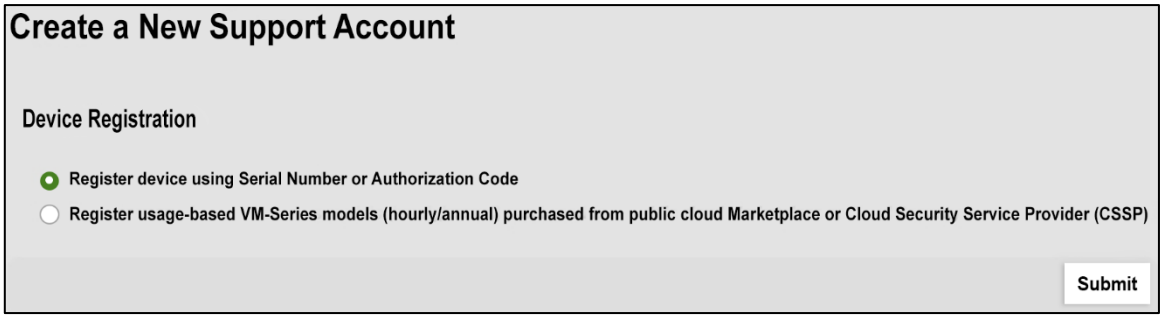

Session received in Application Decoder
Check URL Filtering Signatures
URL Filtering DB
Check Security Policy
Single Pass Pattern Match
Pattern DB
Threat Prevention
Antivirus
Anti Malware
WildFire
Custom Signatures
Vulnerability
Malware
Botnet/c&c
File Type
Data pattern
Policy enforcement

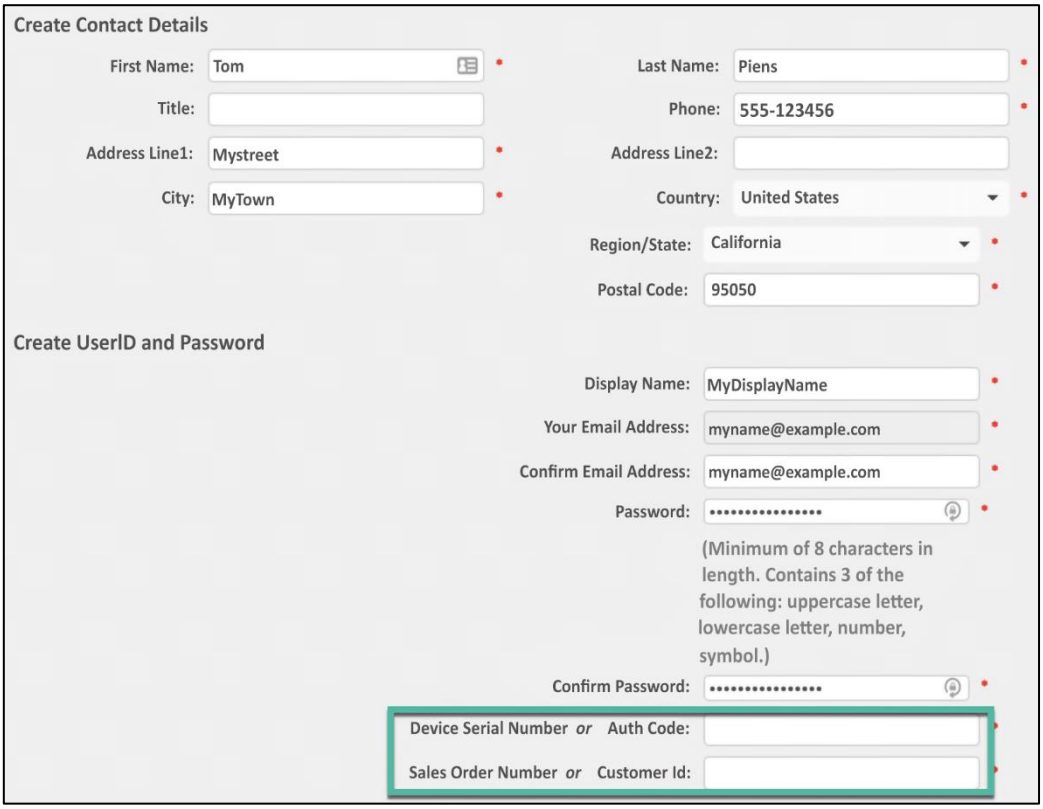
Chapter 2: Setting Up a New Device

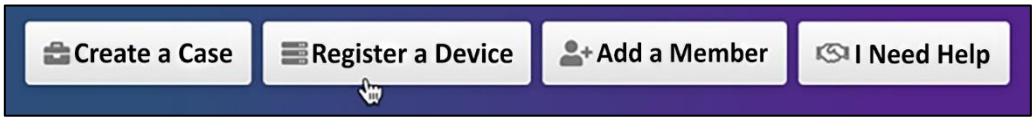

PA-VM-ESX-clean
PA-UM log in: DHCP: new ip 192.168.27.115 : mask 255.255.255.0

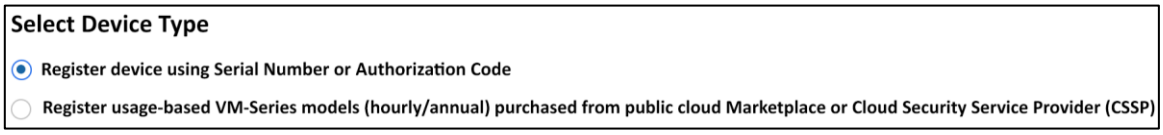

Your connection is not private
Attackers might be trying to steal your information from 192.168.27.115 (for example, passwords, messages or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Help improve Chrome security by sending URLs of some ;ages that you visit, limited system information and some page content to Google. Privacy Policy
Hide advanced
Back to safety
This server could not prove that it is 192.168.27.115; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to 192.160.27.115 (unsafe)
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 192.168.27.115. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the web site and there is nothing you can do to resolve it.
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the web site's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...
Web sites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.27.115. The certificate is only valid for 480748849bf2e9c604324a8de84853c2a1be65210a3203367791c9227706feff.
Error code: SEC_ERROR_UNKNOWN_ISSUER
View Certificate
Go Back (Recommended)
Accept the Risk and Continue


General Information
Device Name PANgurus
MGT IP Address 192.168.0.5
MGT Netmask 255.255.255.0
MGT Default Gateway 192.168.0.1
MGT IPv6 Address unknown
MGT IPv6 Link Local Address fe80::9656:41ff:fe47:9500/64
MGT IPv6 Default Gateway
MGT MAC Address 94:56:41:47:95:00
Model PA-220
Serial # 01
Software Version 10.2.0
GlobalProtect Agent 5.2.8
Application Version 8562-7370 (04/27/22)
Threat Version 8562-7370 (04/27/22)
Antivirus Version 4066-4578 (04/28/22)
Device Dictionary Version 47-322 (04/15/22)
WildFire Version 658884-662142 (04/28/22)
URL Filtering Version 20220428.20328
GlobalProtect Clientless VPN Version 94-237 (04/04/22)
Time Thu Apr 28 23:49:17 2022
Uptime 58 days, 23:37:59
Advanced Routing off
Plugin DLP dlp-3.0.0
Device Certificate Status Valid
General Information
Device Name bootstrapfw
MGT IP Address 10.1.0.4 (DHCP)
MGT Netmask 255.255.255.0
MGT Default Gateway 10.1.0.1
MGT IPv6 Address unknown
MGT IPv6 Link Local Address fe80::6245:bdff:fe90:10ad/64
MGT IPv6 Default Gateway
MGT MAC Address 60:45:bd:90:10:ad
Model PA-VM
Serial # unknown
CPU ID AZR:5
UUID 585DF
D41A3
VM Cores 4
VM Memory 14351728
VM License none
VM Capacity Tier unknown
VM Mode Microsoft Azure
Software Version 10.2.0
GlobalProtect Agent 0.0.0
Application Version 8492-7069
Threat Version 8492-7069
Device Dictionary Version 1-211
URL Filtering Version 0000.00.00.000
GlobalProtect Clientless VPN 0


Create a New Support Account
Device Registration
Register device using Serial Number or Authorization Code
Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP)
Submit


Create Contact Details
First Name: Tom
Last Name: Piens
Title:
Phone: 555-123456
Address Line1: Mystreet
Address Line2:
City: MyTown
Country: United States
Region/State: California
Postal Code: 95050
Create UserID and Password
Display Name: MyDisplayName
Your Email Address: myname@example.com
Confirm Email Address: myname@example.com
Password:
(Minimum of 8 characters in length. Contains 3 of the following: uppercase letter, lowercase letter, number, symbol.)
Confirm Password:
Device Serial Number or Auth Code:
Sales Order Number or Customer Id:


Create a Case
Register a Device
Add a Member
I Need Help


Select Device Type
Register device using Serial Number or Authorization Code
Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP)

Device Information

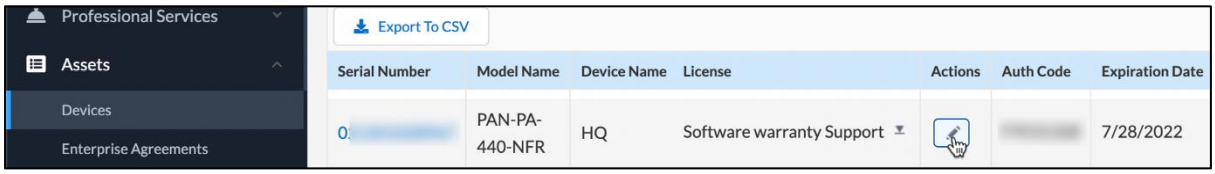
Serial Number*

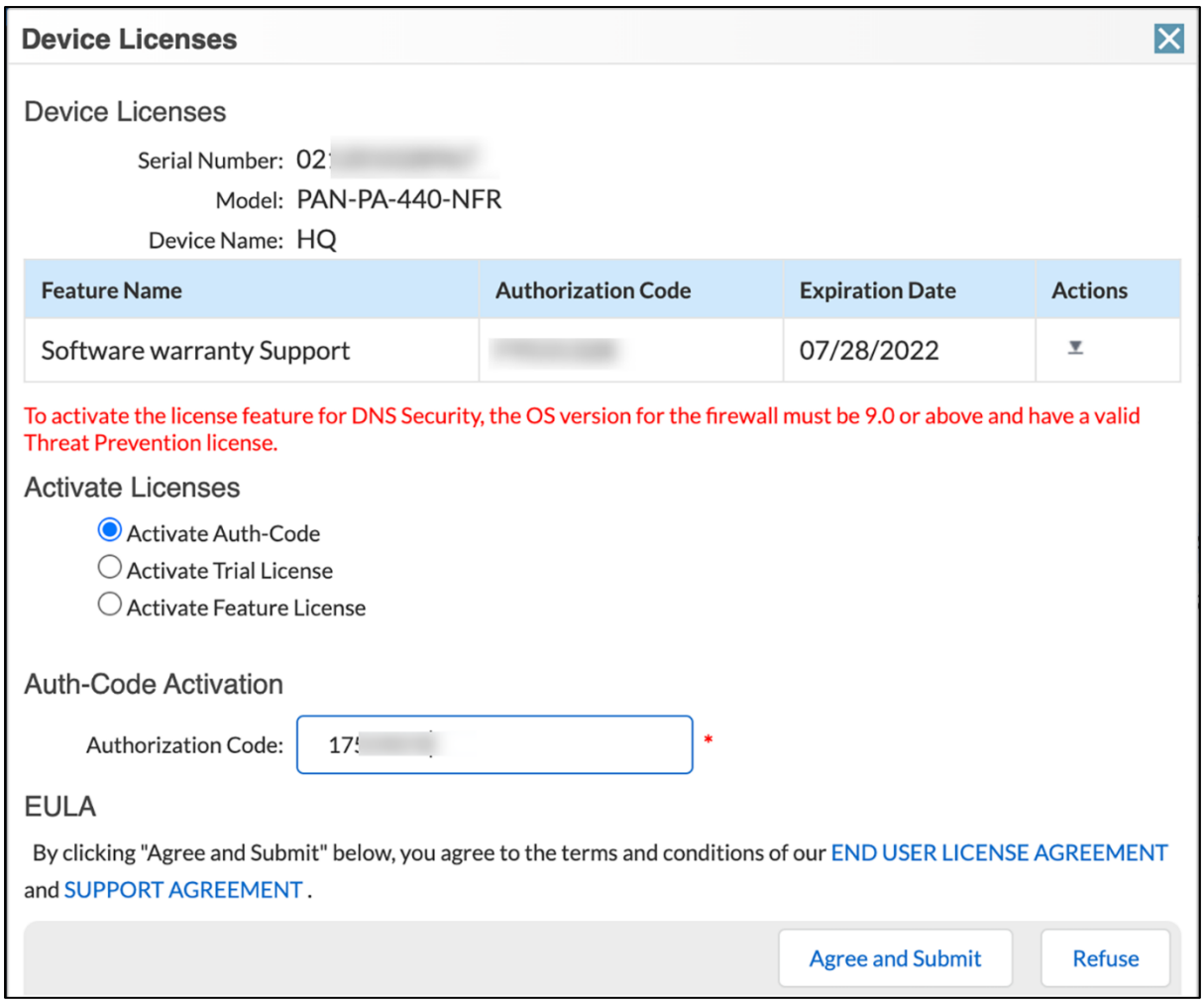
CPUID*

UUID

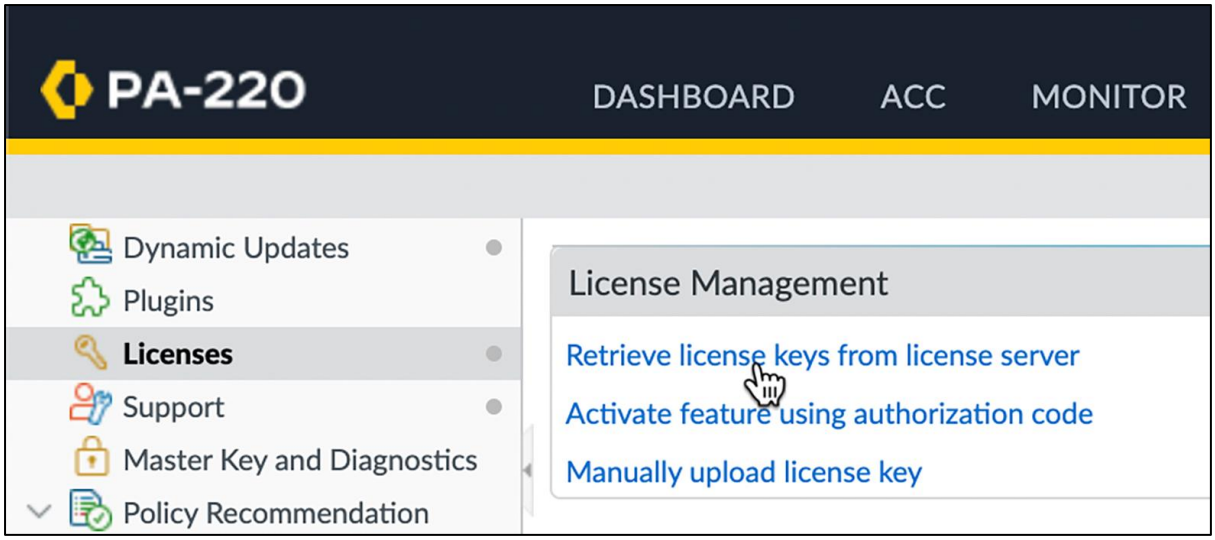
Device Name

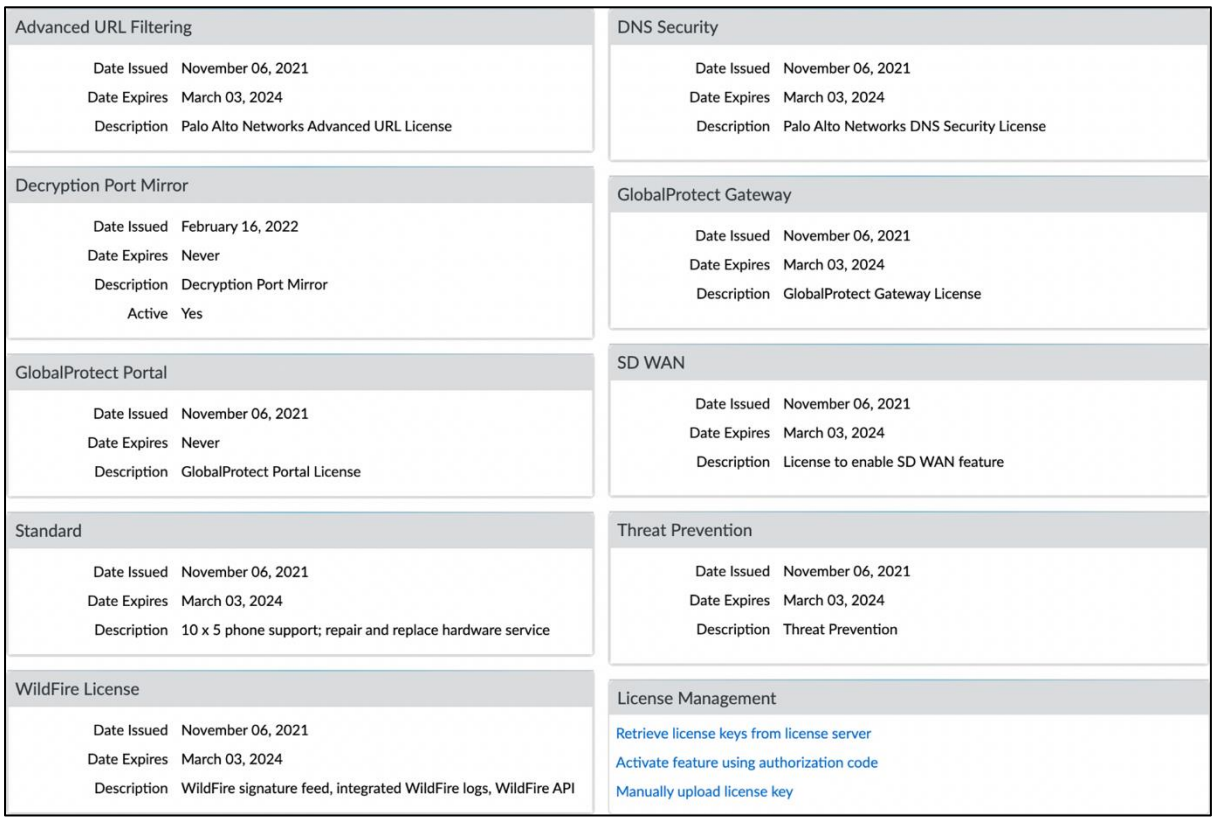
Device Tag — Choose one Device Tag...

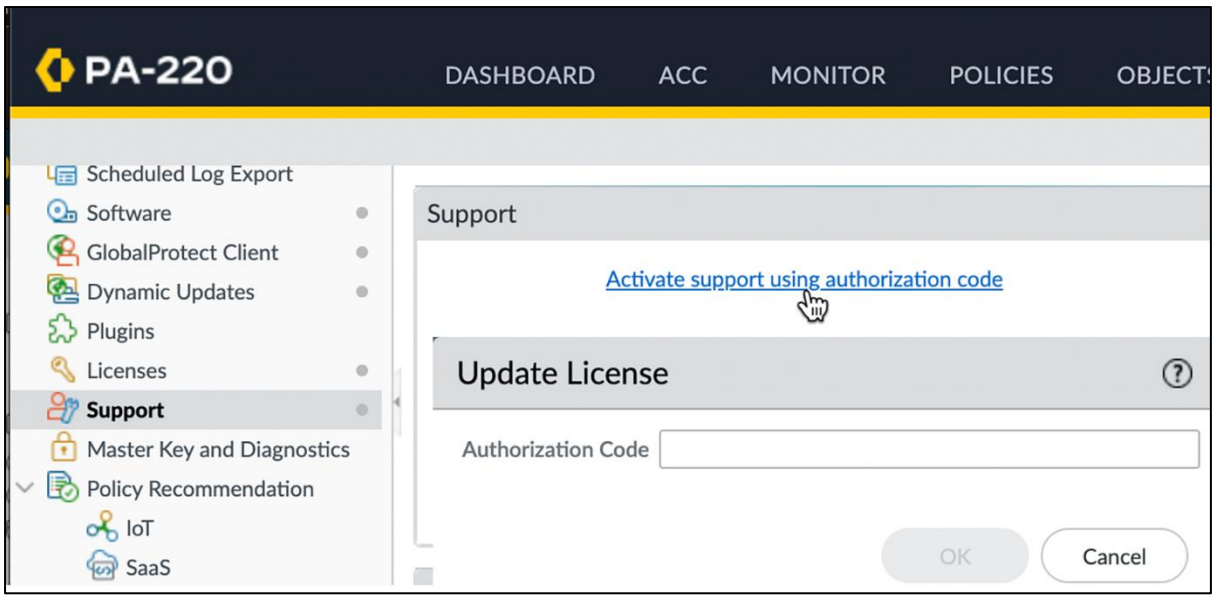


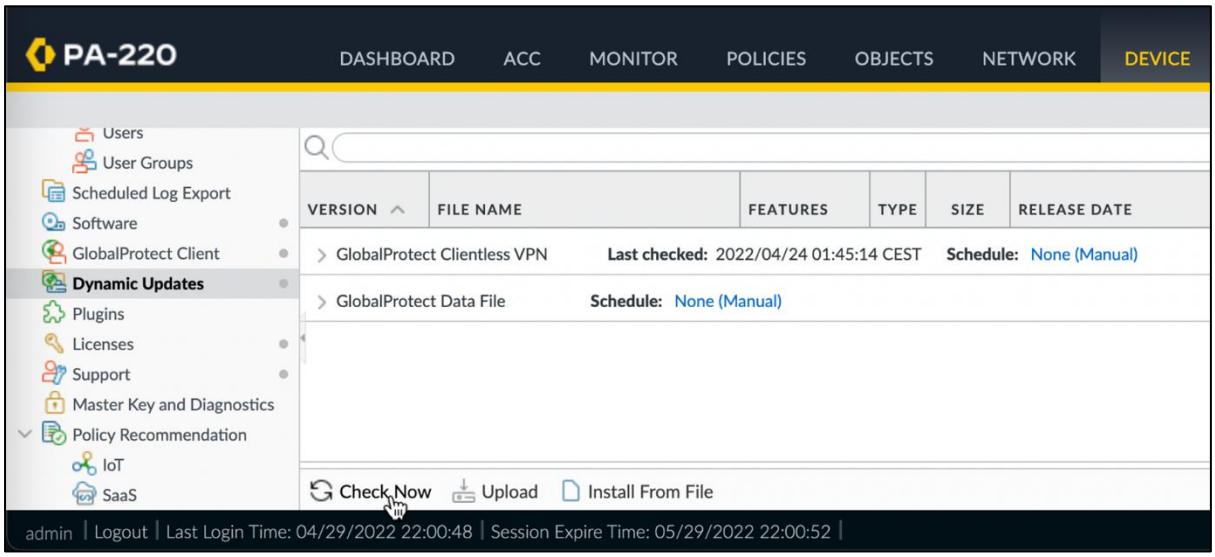


02	PAN-PA-440-NFR	HQ		NFR Bundle			4/28/2023
				Threat Prevention			4/28/2023
				Advanced URL Filtering			4/28/2023
				DNS Security			4/28/2023
				GlobalProtect Gateway			4/28/2023
				SD WAN			4/28/2023
				Standard Support			4/28/2023
				WildFire License			4/28/2023

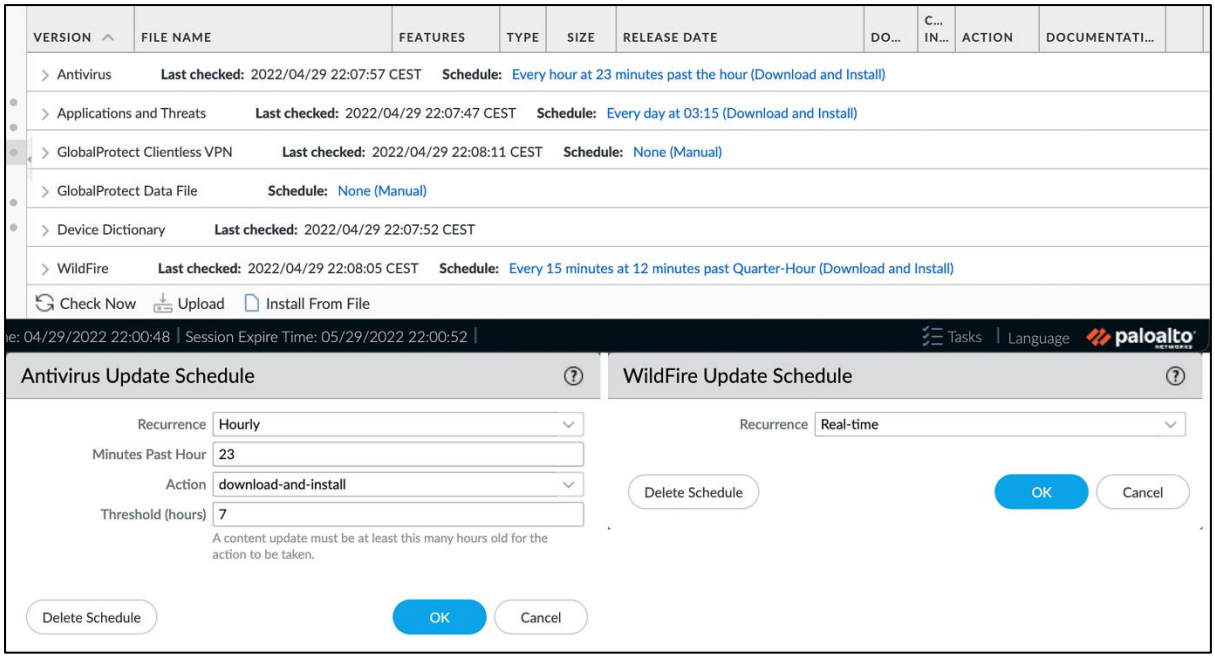

PA-220
DASHBOARD
ACC
MONITOR
Dynamic Updates
Plugins
Licenses
Support
Master Key and Diagnostics
Policy Recommendation
License Management
Retrieve license keys from license server
Activate feature using authorization code
Manually upload license key

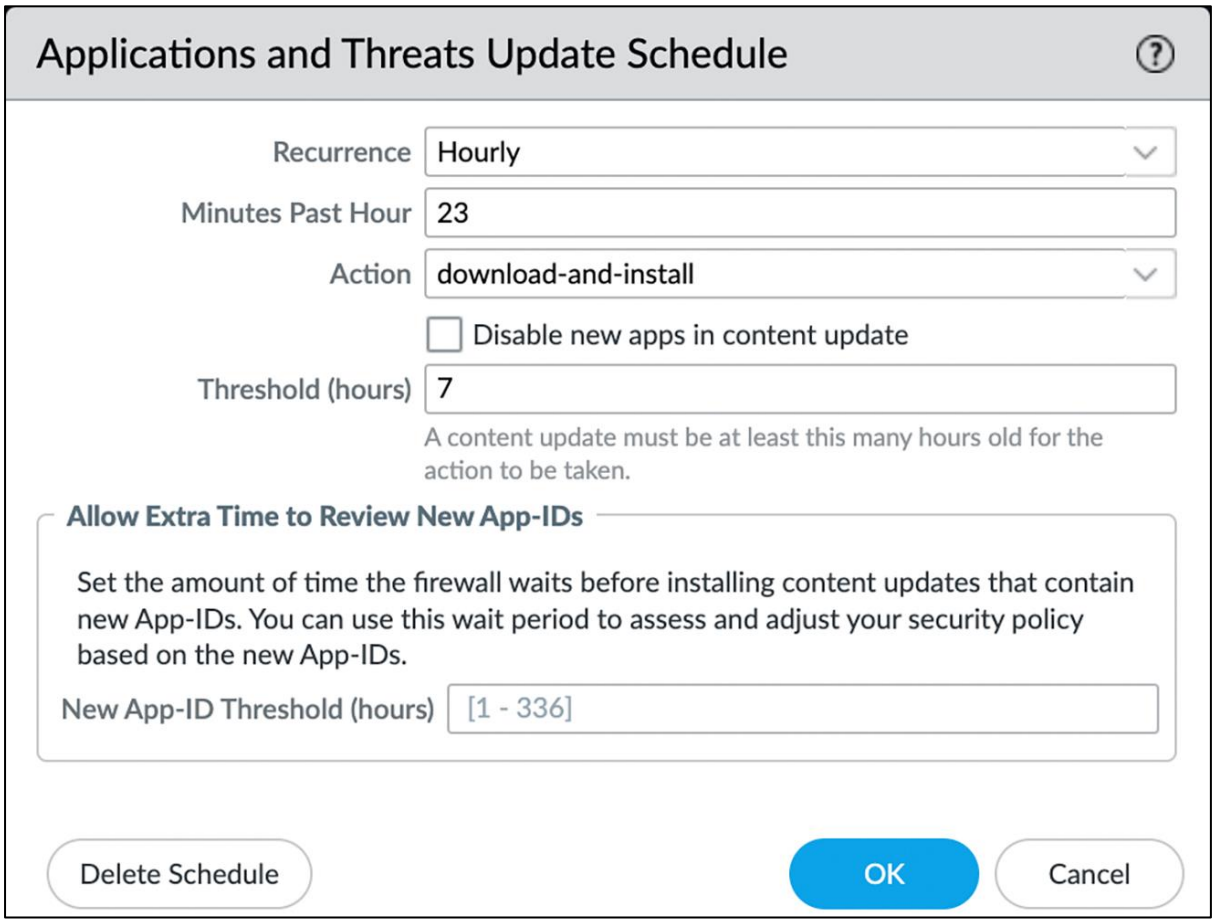

Advanced URL Filtering
Date Issued November 06, 2021
Date Expires March 03, 2024
Description Palo Alto Networks Advanced URL License
DNS Security
Date Issued November 06, 2021
Date Expires March 03, 2024
Description Palo Alto Networks DNS Security License
Decryption Port Mirror
Date Issued February 16, 2022
Date Expires Never
Description Decryption Port Mirror
Active Yes
GlobalProtect Gateway
Date Issued November 06, 2021
Date Expires March 03, 2024
Description GlobalProtect Gateway License
GlobalProtect Portal
Date Issued November 06, 2021
Date Expires Never
Description GlobalProtect Portal License
SD WAN
Date Issued November 06, 2021
Date Expires March 03, 2024
Description License to enable SD WAN feature
Standard
Date Issued November 06, 2021
Date Expires March 03, 2024
Description 10 x 5 phone support; repair and replace hardware service
Threat Prevention
Date Issued November 06, 2021
Date Expires March 03, 2024
Description Threat Prevention
WildFire License
Date Issued November 06, 2021
Date Expires March 03, 2024
Description WildFire signature feed, integrated WildFire logs, WildFire API
License Management
Retrieve license keys from license server
Activate feature using authorization code
Manually upload license key

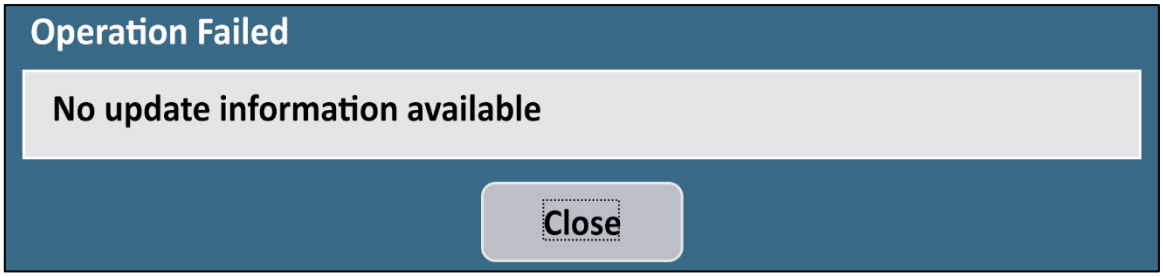




VERSION	FILE NAME	FEATURES	TYPE	SIZE	RELEASE DATE	DOW...	CURRE... INSTA...	ACTION
Applications and Threats	Last checked: 2022/04/28 03:15:14 CEST	Schedule: Every day at 03:15 (Download and Install)						
8548-7321	panupv2-all-contents-8548-7321	Apps, Threats	Full	53 MB	2022/03/31 06:20:36 CEST			Download
8549-7323	panupv2-all-contents-8549-7323	Apps, Threats	Full	53 MB	2022/04/01 03:46:34 CEST			Download
8550-7325	panupv2-all-contents-8550-7325	Apps, Threats	Full	53 MB	2022/04/05 01:37:16 CEST			Download
8551-7330	panupv2-all-contents-8551-7330	Apps, Threats	Full	53 MB	2022/04/05 23:43:41 CEST			Download

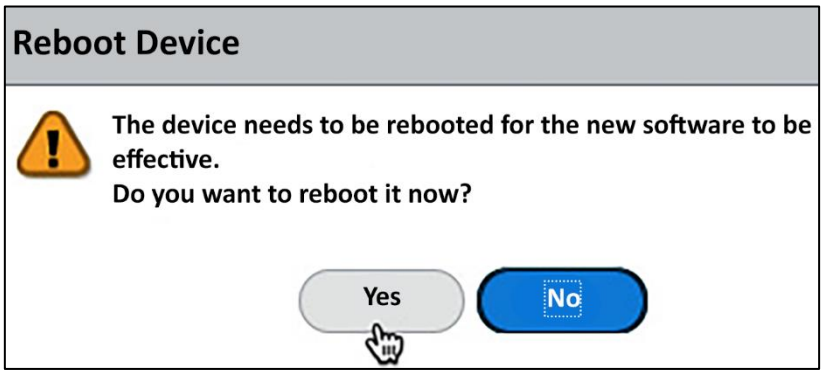

VERSION
FILE NAME
FEATURES
TYPE
SIZE
RELEASE DATE
DO...
C... IN...
ACTION
DOCUMENTATI...
Antivirus Last checked: 2022/04/29 22:07:57 CEST Schedule: Every hour at 23 minutes past the hour (Download and Install)
Applications and Threats Last checked: 2022/04/29 22:07:47 CEST Schedule: Every day at 03:15 (Download and Install)
GlobalProtect Clientless VPN Last checked: 2022/04/29 22:08:11 CEST Schedule: None (Manual)
GlobalProtect Data File Schedule: None (Manual)
Device Dictionary Last checked: 2022/04/29 22:07:52 CEST
WildFire Last checked: 2022/04/29 22:08:05 CEST Schedule: Every 15 minutes at 12 minutes past Quarter-Hour (Download and Install)
Check Now
Upload
Install From File
04/29/2022 22:00:48 | Session Expire Time: 05/29/2022 22:00:52
Tasks
Language
paloalto
Antivirus Update Schedule
Recurrence Hourly
Minutes Past Hour 23
Action download-and-install
Threshold (hours) 7
A content update must be at least this many hours old for the action to be taken.
Delete Schedule
OK
Cancel
WildFire Update Schedule
Recurrence Real-time
Delete Schedule
OK
Cancel

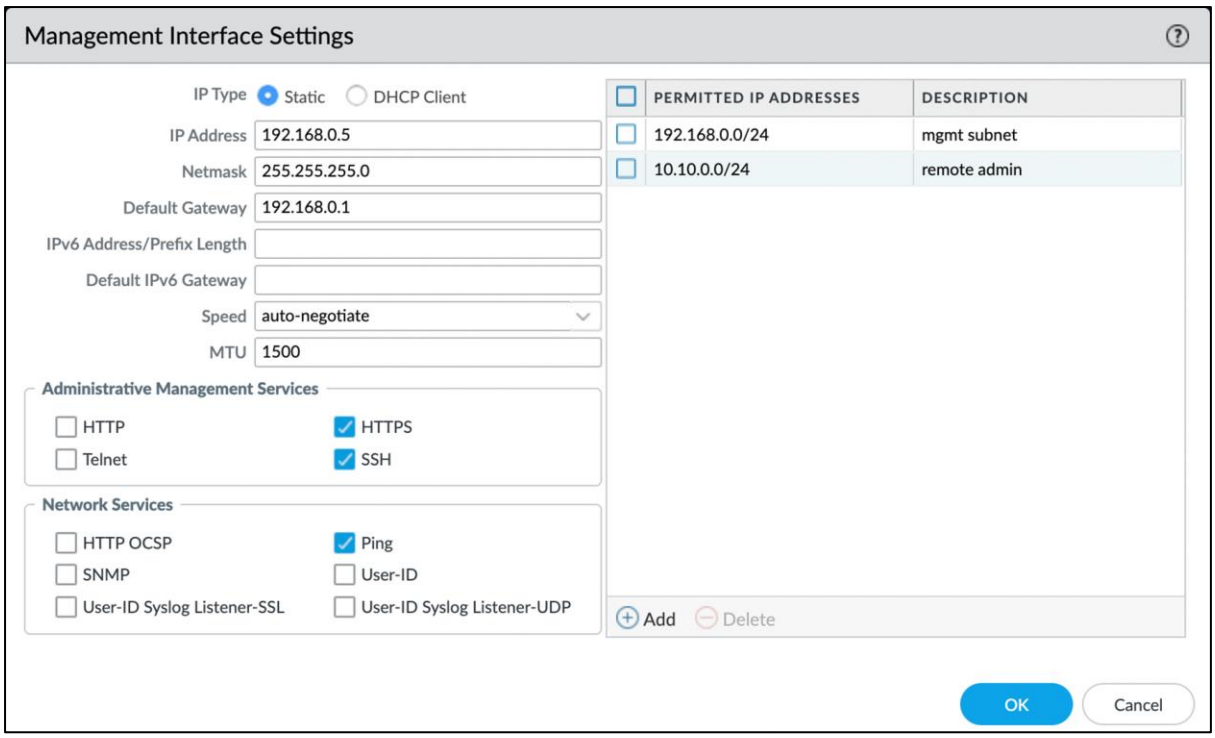

Applications and Threats Update Schedule
Recurrence Hourly
Minutes Past Hour 23
Action download-and-install
Disable new apps in content update
Threshold (hours) 7
A content update must be at least this many hours old for the action to be taken.
Allow Extra Time to Review New App-IDs
Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.
New App-ID Threshold (hours) [1 - 336]
Delete Schedule
OK
Cancel

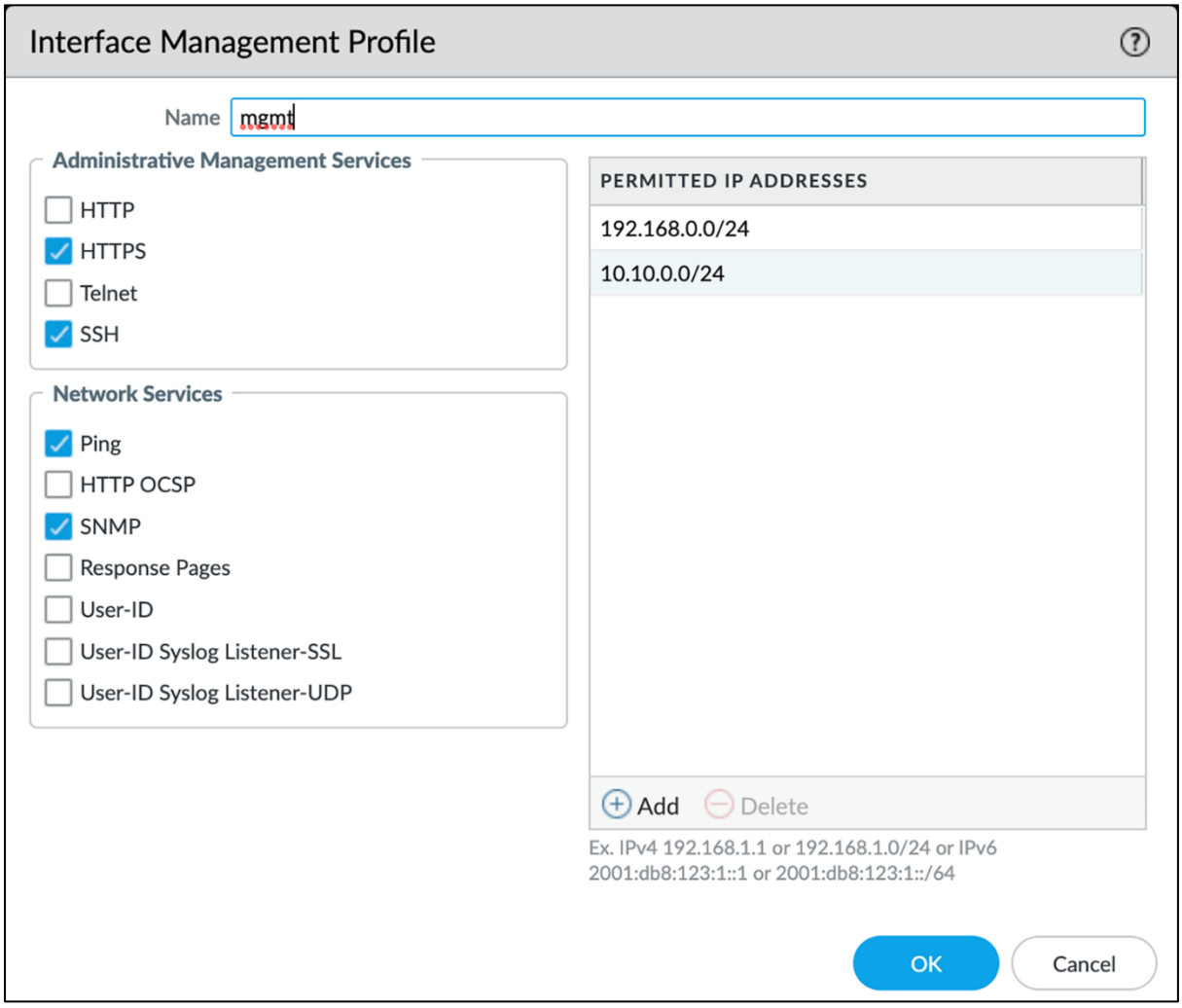


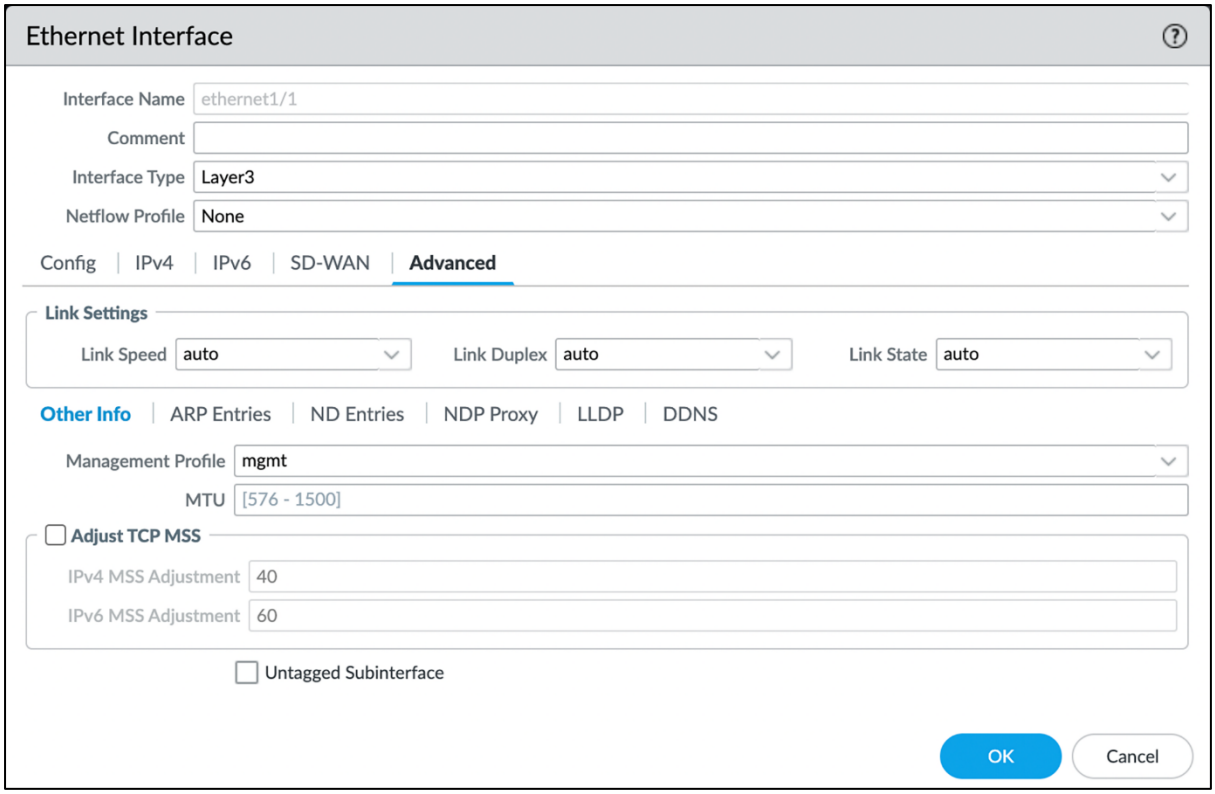
VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION		
10.1.4	353 MB	2021/12/22 11:51:17			Download	Release Notes	
10.1.3	298 MB	2021/10/26 18:51:50	Downloaded	✓	Reinstall	Release Notes	
10.1.2	297 MB	2021/08/16 14:51:59			Download	Release Notes	
10.1.1	280 MB	2021/07/21 09:33:49			Download	Release Notes	
10.1.0	540 MB	2021/06/02 08:15:33	Downloaded		Install	Release Notes	☒
10.0.8	363 MB	2021/10/21 22:42:18			Download	Release Notes	
10.0.8-h8	359 MB	2021/12/20 12:23:36			Download	Release Notes	

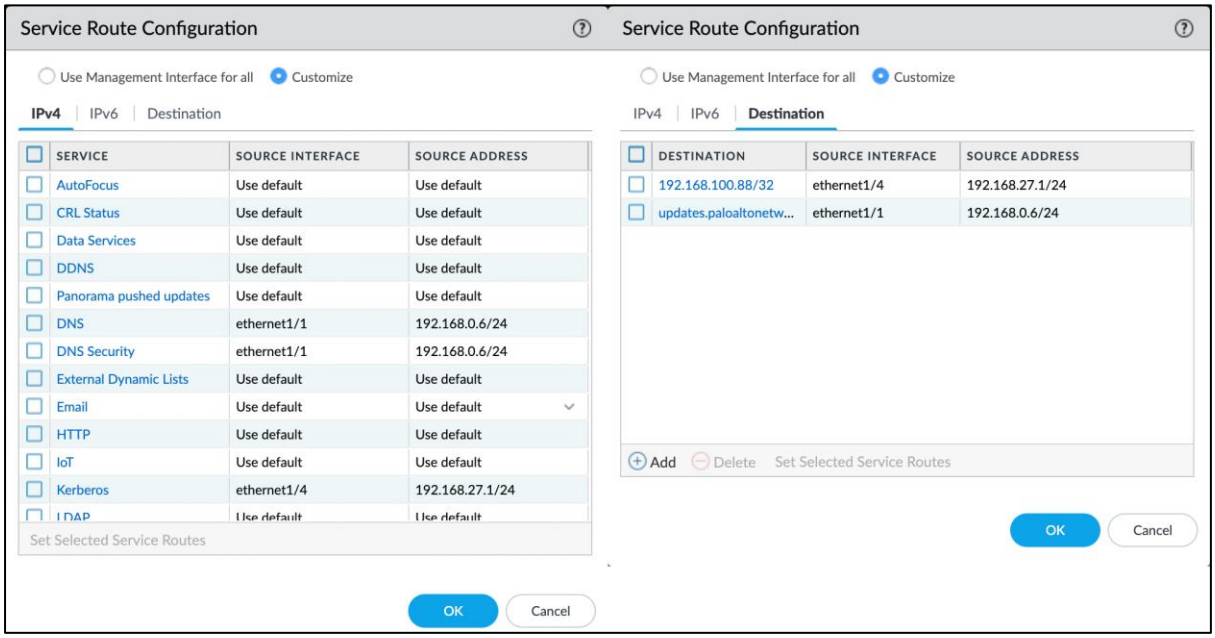
VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION		
10.1.4	353 MB	2021/12/22 11:51:17	Downloaded		Install	Release Notes	☒
10.1.3	298 MB	2021/10/26 18:51:50	Downloaded	✓	Reinstall	Release Notes	
10.1.2	297 MB	2021/08/16 14:51:59			Download	Release Notes	
10.1.1	280 MB	2021/07/21 09:33:49			Download	Release Notes	
10.1.0	540 MB	2021/06/02 08:15:33	Downloaded		Install	Release Notes	☒
10.0.8	363 MB	2021/10/21 22:42:18			Download	Release Notes	
10.0.8-h8	359 MB	2021/12/20 12:23:36			Download	Release Notes	

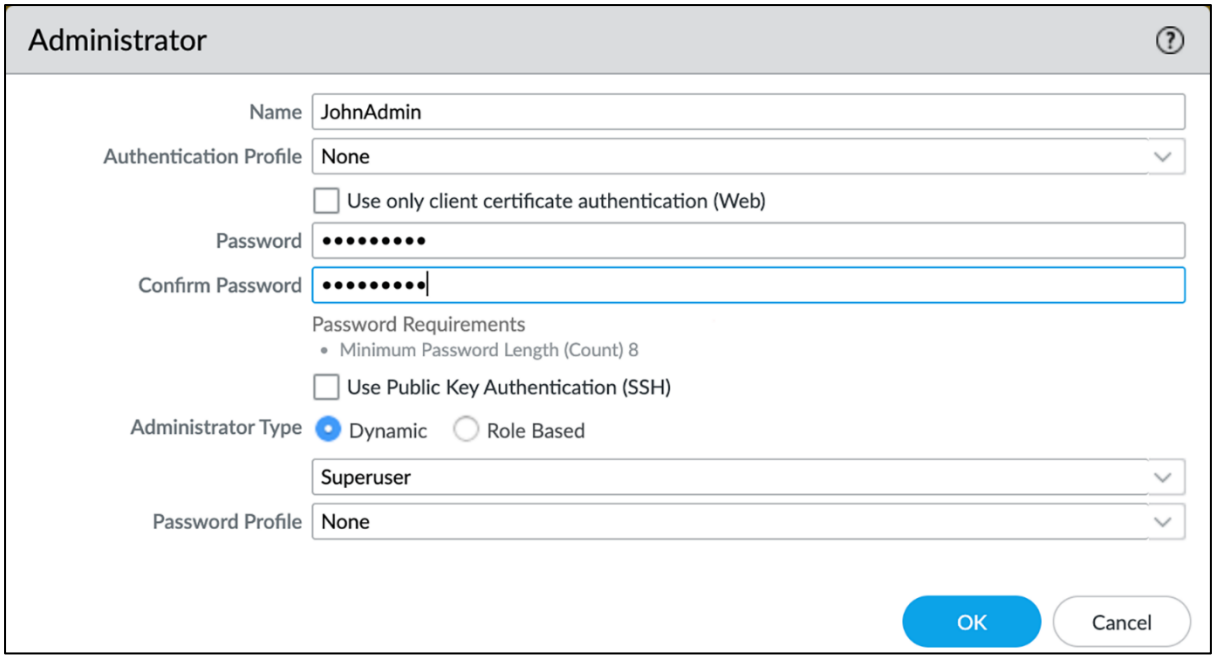


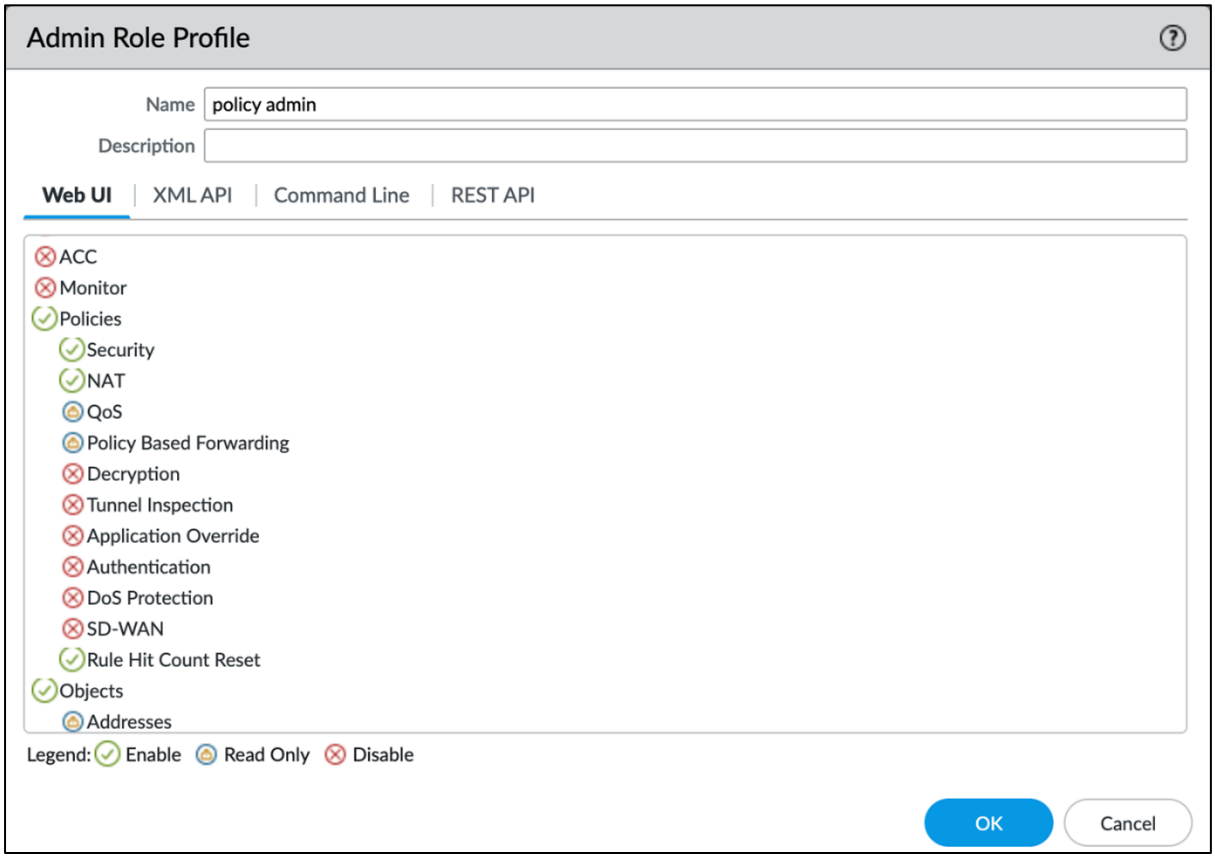

Management Interface Settings
IP Type
Static
DHCP Client
IP Address
192.168.0.5
Netmask
255.255.255.0
Default Gateway
192.168.0.1
IPv6 Address/Prefix Length
Default IPv6 Gateway
Speed
auto-negotiate
MTU
1500
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
HTTP OCSP
Ping
SNMP
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
PERMITTED IP ADDRESSES
DESCRIPTION
192.168.0.0/24
mgmt subnet
10.10.0.0/24
remote admin
Add
Delete
OK
Cancel

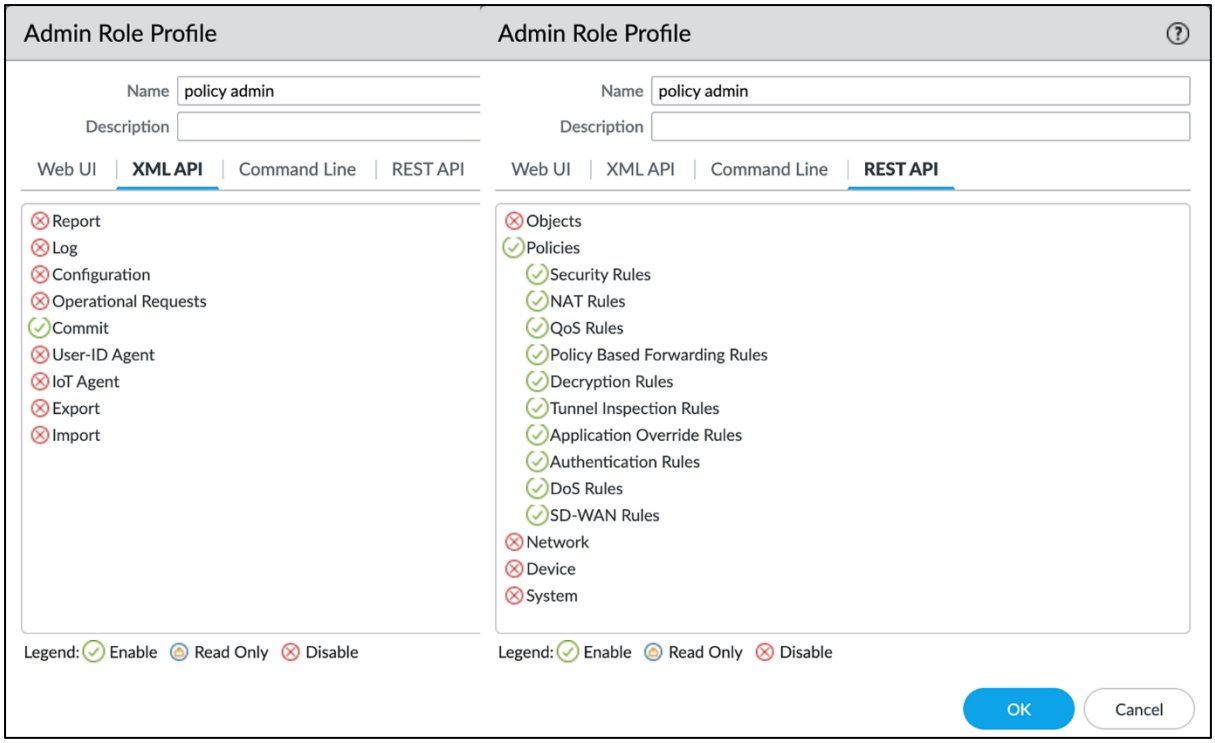

Interface Management Profile
Name
mgmt
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
PERMITTED IP ADDRESSES
192.168.0.0/24
10.10.0.0/24
Add
Delete
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64
OK
Cancel

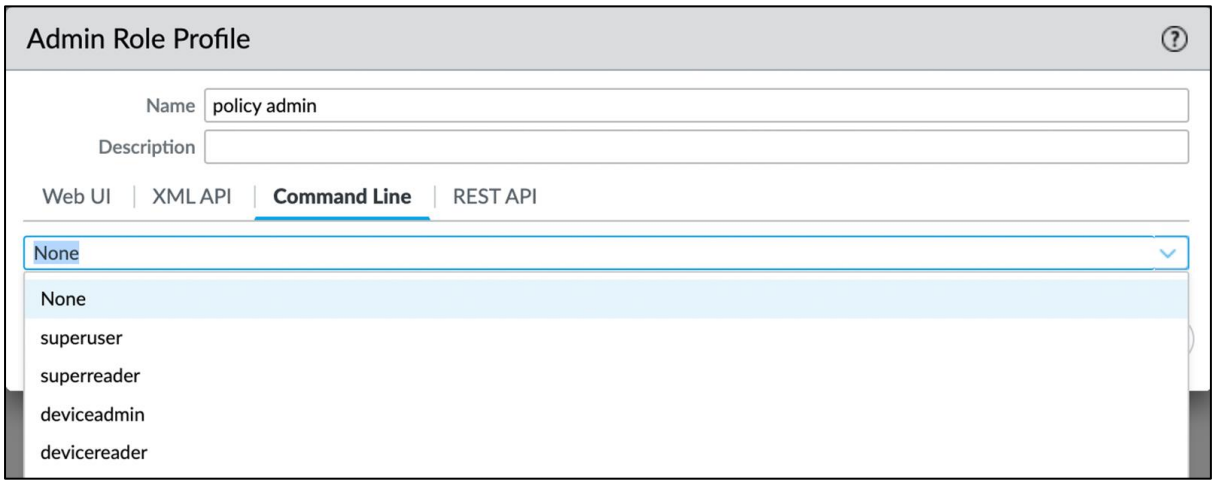

Ethernet Interface
Interface Name
ethernet1/1
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
SD-WAN
Advanced
Link Settings
Link Speed
auto
Link Duplex
auto
Link State
auto
Other Info
ARP Entries
ND Entries
NDP Proxy
LLDP
DDNS
Management Profile
mgmt
MTU
[576 - 1500]
Adjust TCP MSS
IPv4 MSS Adjustment
40
IPv6 MSS Adjustment
60
Untagged Subinterface
OK
Cancel

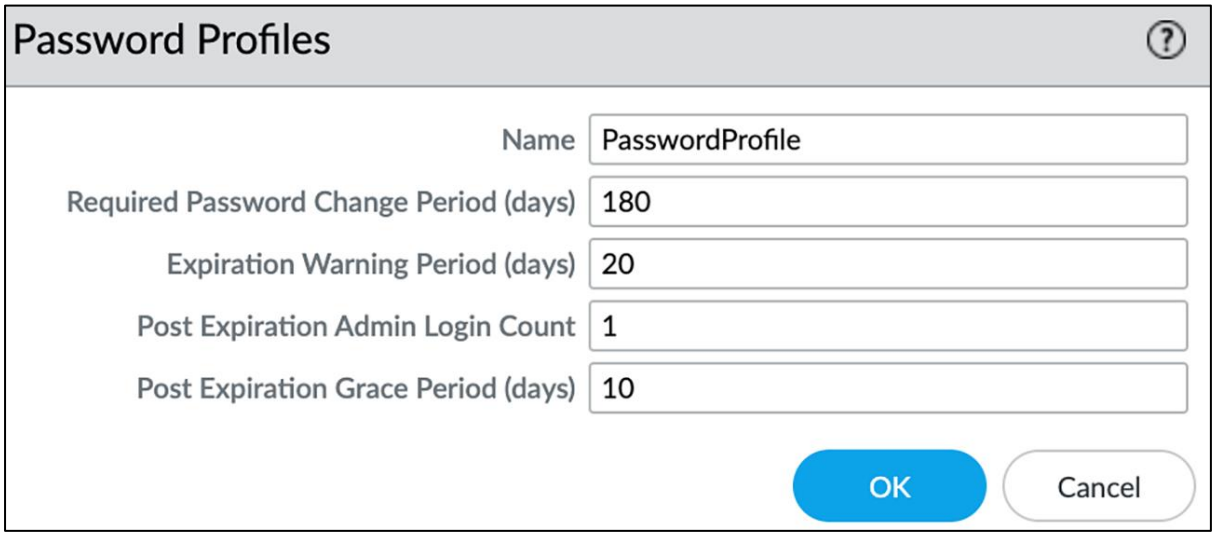

Service Route Configuration
Use Management Interface for all
Customize
IPv4
IPv6
Destination
SERVICE
SOURCE INTERFACE
SOURCE ADDRESS
AutoFocus
Use default
Use default
CRL Status
Use default
Use default
Data Services
Use default
Use default
DDNS
Use default
Use default
Panorama pushed updates
Use default
Use default
DNS
ethernet1/1
192.168.0.6/24
DNS Security
ethernet1/1
192.168.0.6/24
External Dynamic Lists
Use default
Use default
Email
Use default
Use default
HTTP
Use default
Use default
IoT
Use default
Use default
Kerberos
ethernet1/4
192.168.27.1/24
LDAP
Use default
Use default
Set Selected Service Routes
OK
Cancel
Service Route Configuration
Use Management Interface for all
Customize
IPv4
IPv6
Destination
DESTINATION
SOURCE INTERFACE
SOURCE ADDRESS
192.168.100.88/32
ethernet1/4
192.168.27.1/24
updates.paloaltonetw...
ethernet1/1
192.168.0.6/24
Add
Delete
Set Selected Service Routes
OK
Cancel

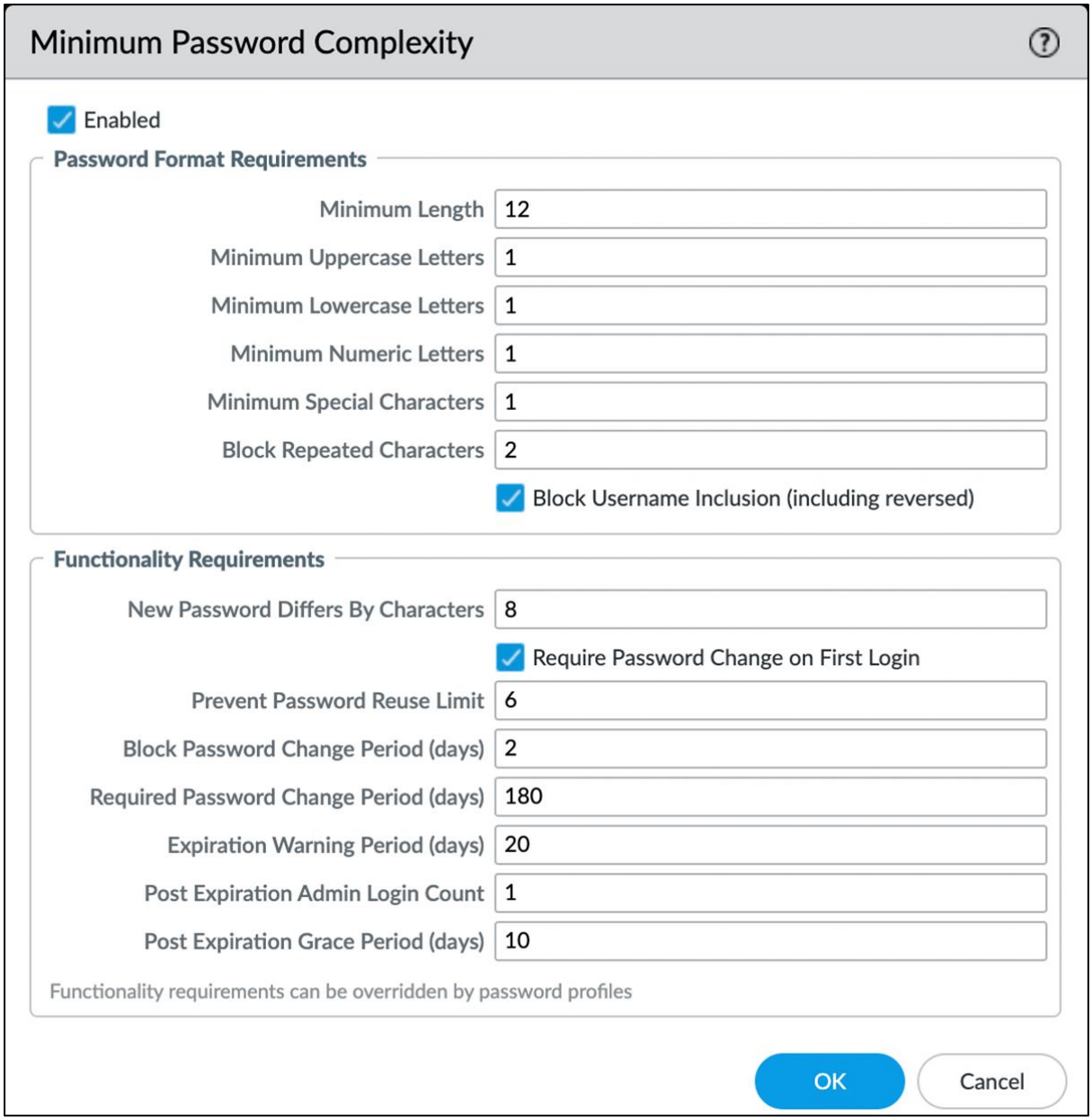

Administrator
Name
JohnAdmin
Authentication Profile
None
Use only client certificate authentication (Web)
Password
Confirm Password
Password Requirements
Minimum Password Length (Count) 8
Use Public Key Authentication (SSH)
Administrator Type
Dynamic
Role Based
Superuser
Password Profile
None
OK
Cancel

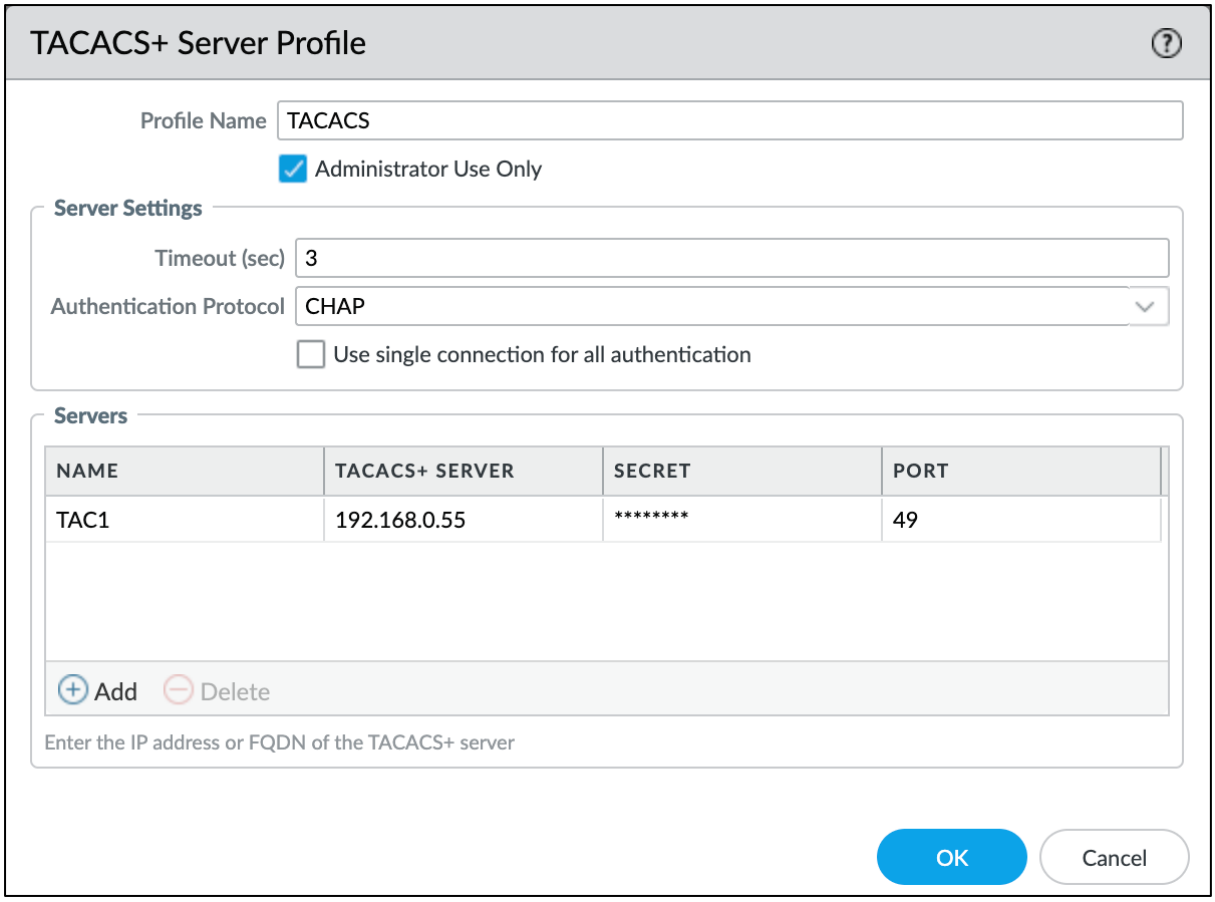

Admin Role Profile
Name
policy admin
Description
Web UI
XML API
Command Line
REST API
ACC
Monitor
Policies
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN
Rule Hit Count Reset
Objects
Addresses
Legend:
Enable
Read Only
Disable
OK
Cancel

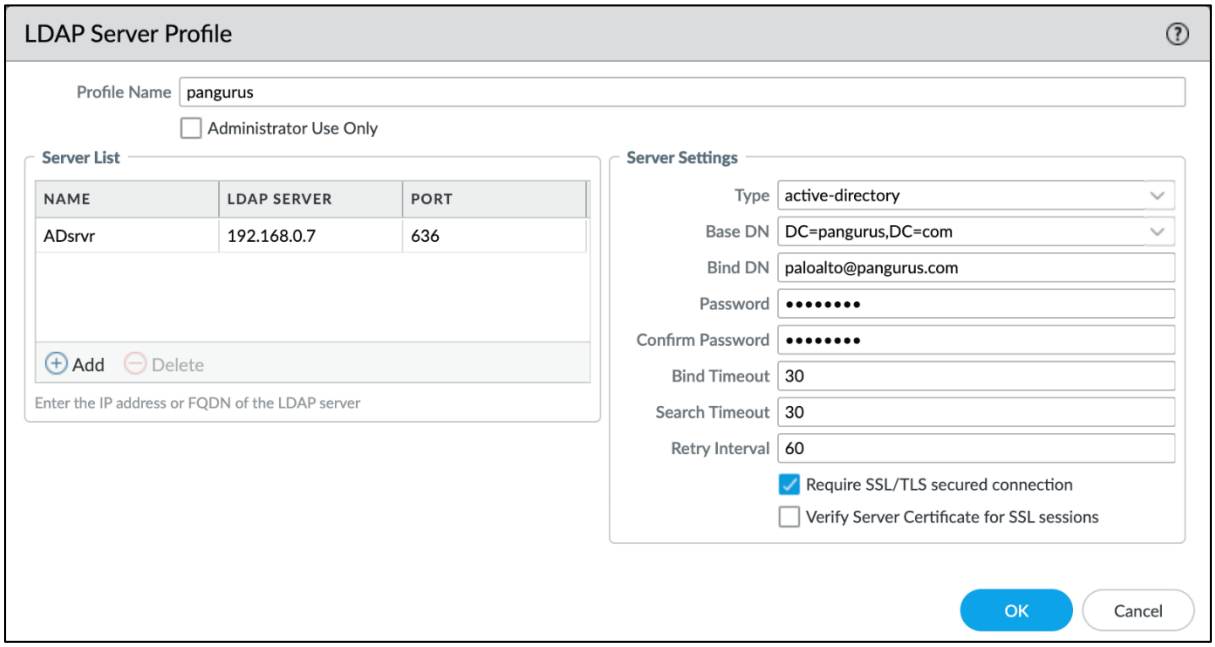

Admin Role Profile
Name policy admin
Description
Web UI | XML API | Command Line | REST API
Report
Log
Configuration
Operational Requests
Commit
User-ID Agent
IoT Agent
Export
Import
Legend: Enable Read Only Disable
Admin Role Profile
Name policy admin
Description
Web UI | XML API | Command Line | REST API
Objects
Policies
Security Rules
NAT Rules
QoS Rules
Policy Based Forwarding Rules
Decryption Rules
Tunnel Inspection Rules
Application Override Rules
Authentication Rules
DoS Rules
SD-WAN Rules
Network
Device
System
Legend: Enable Read Only Disable
OK
Cancel

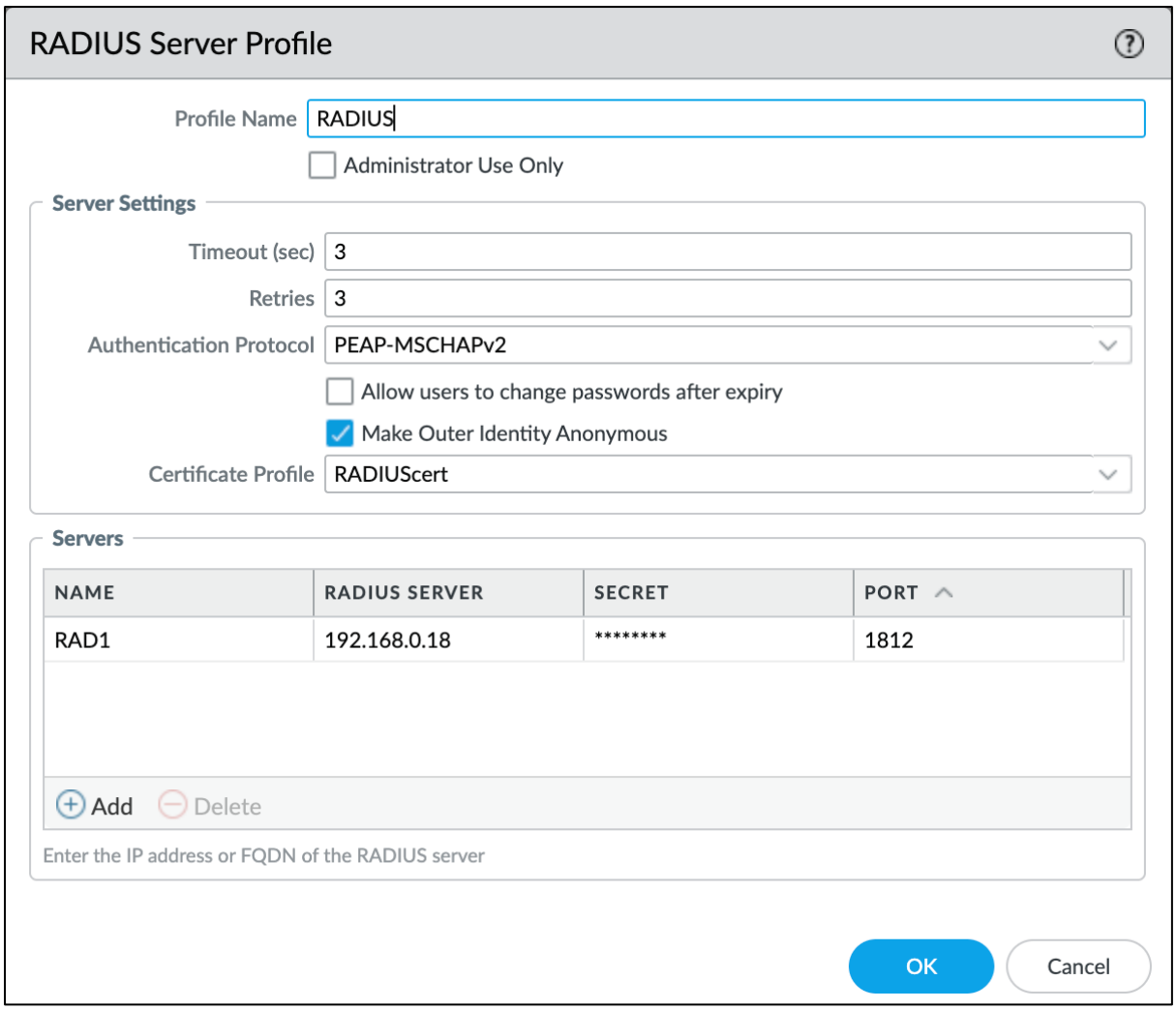

Admin Role Profile
Name policy admin
Description
Web UI | XML API | Command Line | REST API
None
None
superuser
superreader
deviceadmin
devicereader

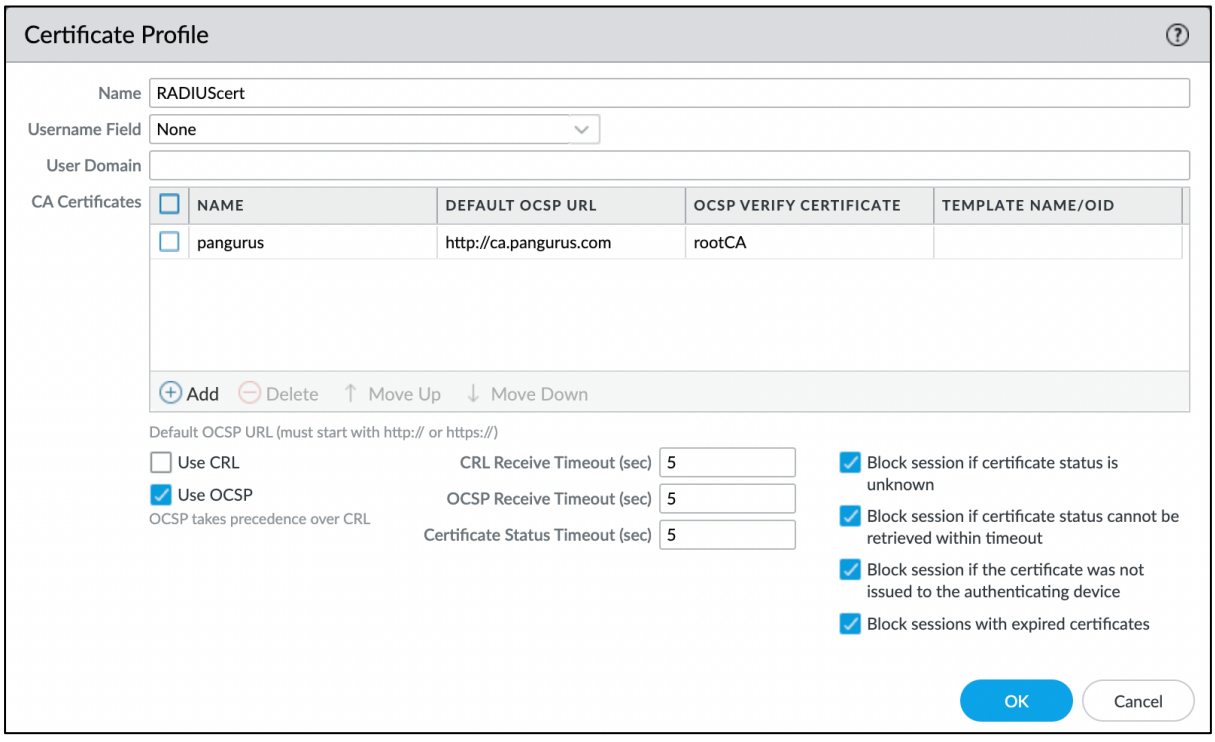

Password Profiles
Name PasswordProfile
Required Password Change Period (days) 180
Expiration Warning Period (days) 20
Post Expiration Admin Login Count 1
Post Expiration Grace Period (days) 10
OK
Cancel

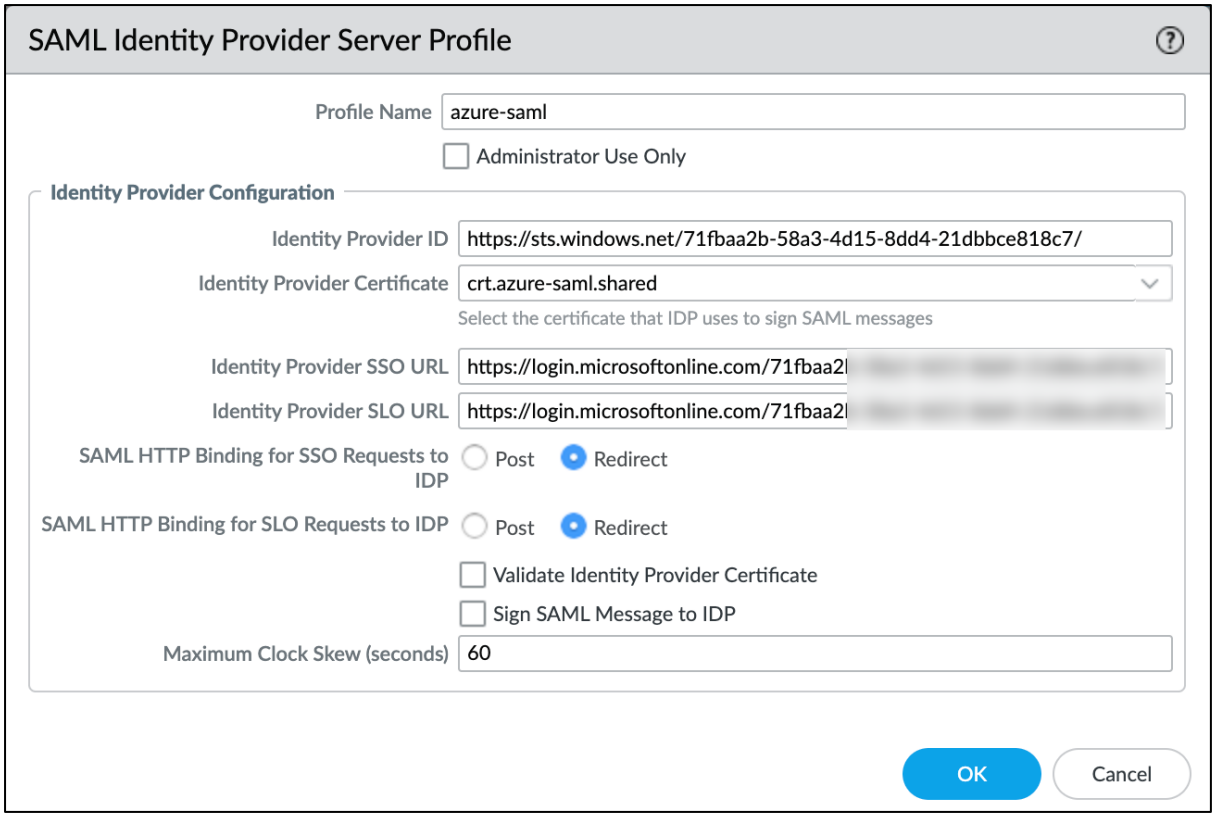

Minimum Password Complexity
Enabled
Password Format Requirements
Minimum Length
12
Minimum Uppercase Letters
1
Minimum Lowercase Letters
1
Minimum Numeric Letters
1
Minimum Special Characters
1
Block Repeated Characters
2
Block Username Inclusion (including reversed)
Functionality Requirements
New Password Differs By Characters
8
Require Password Change on First Login
Prevent Password Reuse Limit
6
Block Password Change Period (days)
2
Required Password Change Period (days)
180
Expiration Warning Period (days)
20
Post Expiration Admin Login Count
1
Post Expiration Grace Period (days)
10
Functionality requirements can be overridden by password profiles
OK
Cancel

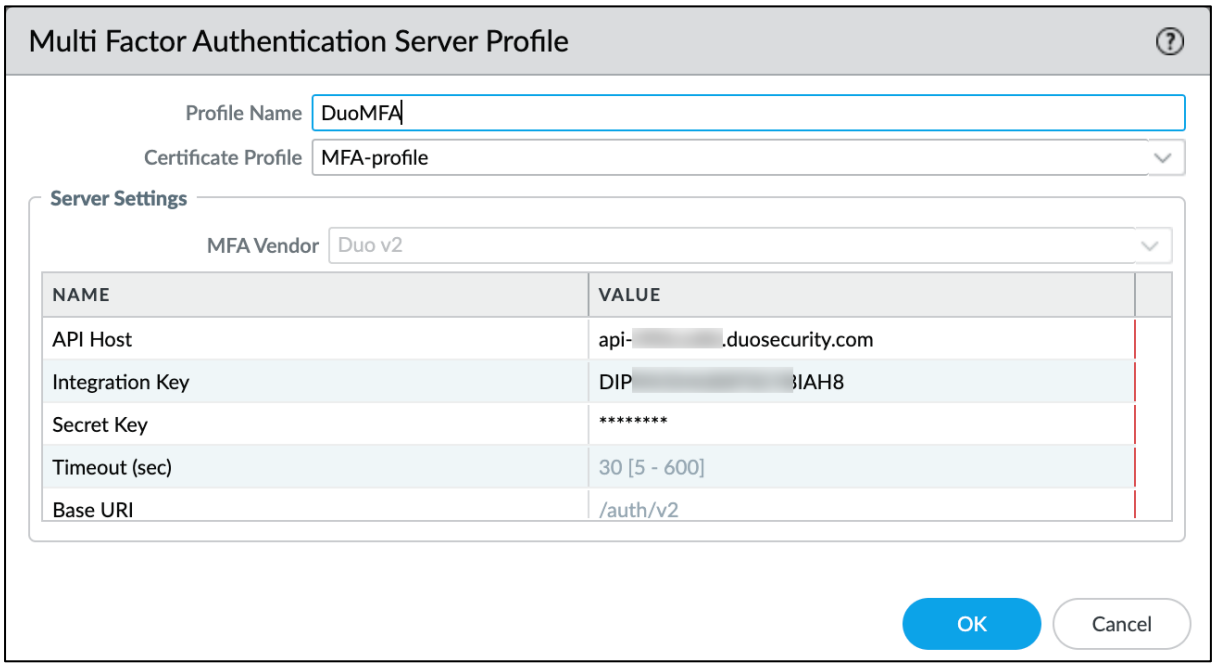

TACACS+ Server Profile
Profile Name
TACACS
Administrator Use Only
Server Settings
Timeout (sec)
3
Authentication Protocol
CHAP
Use single connection for all authentication
Servers
NAME
TACACS+ SERVER
SECRET
PORT
TAC1
192.168.0.55
****
49
Add
Delete
Enter the IP address or FQDN of the TACACS+ server
OK
Cancel

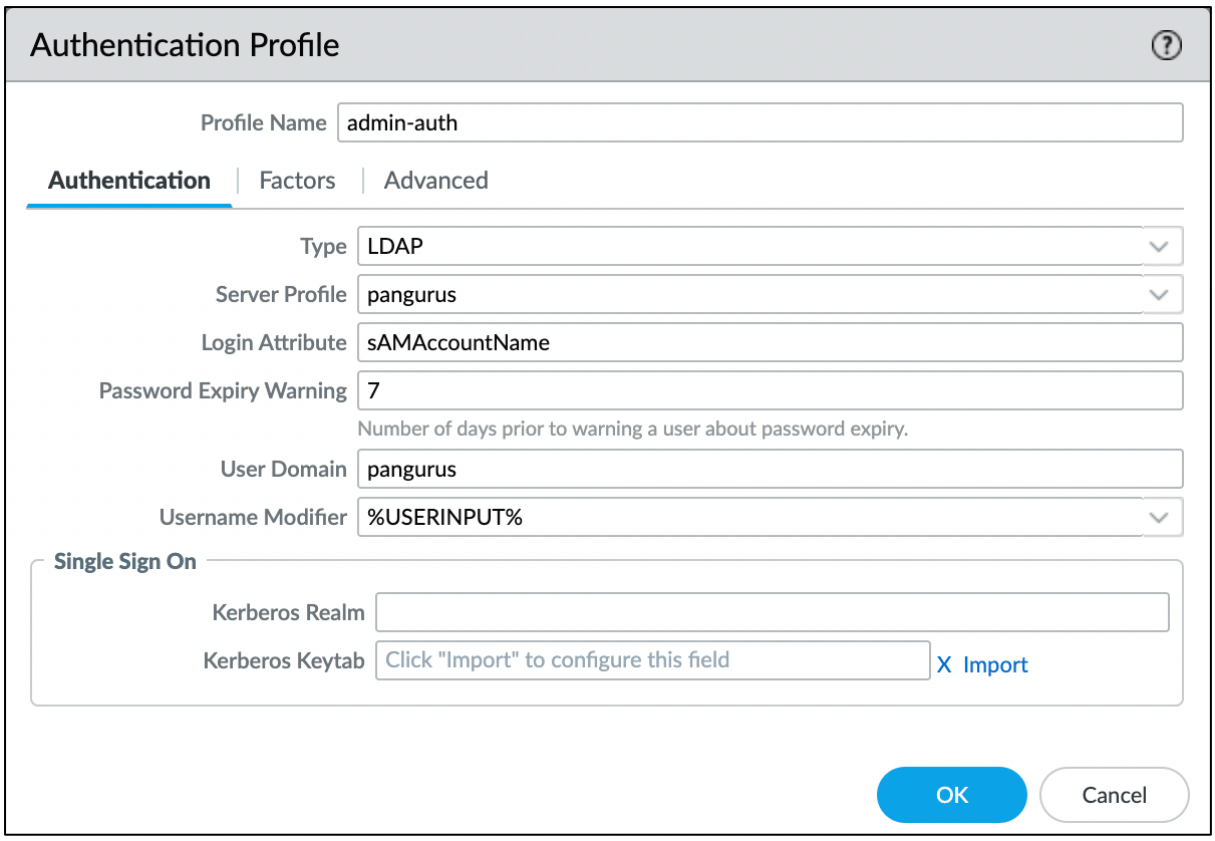

LDAP Server Profile
Profile Name
pangurus
Administrator Use Only
Server List
NAME
LDAP SERVER
PORT
ADsrvr
192.168.0.7
636
Add
Delete
Enter the IP address or FQDN of the LDAP server
Server Settings
Type
active-directory
Base DN
DC=pangurus,DC=com
Bind DN
paloalto@pangurus.com
Password
Confirm Password
Bind Timeout
30
Search Timeout
30
Retry Interval
60
Require SSL/TLS secured connection
Verify Server Certificate for SSL sessions
OK
Cancel

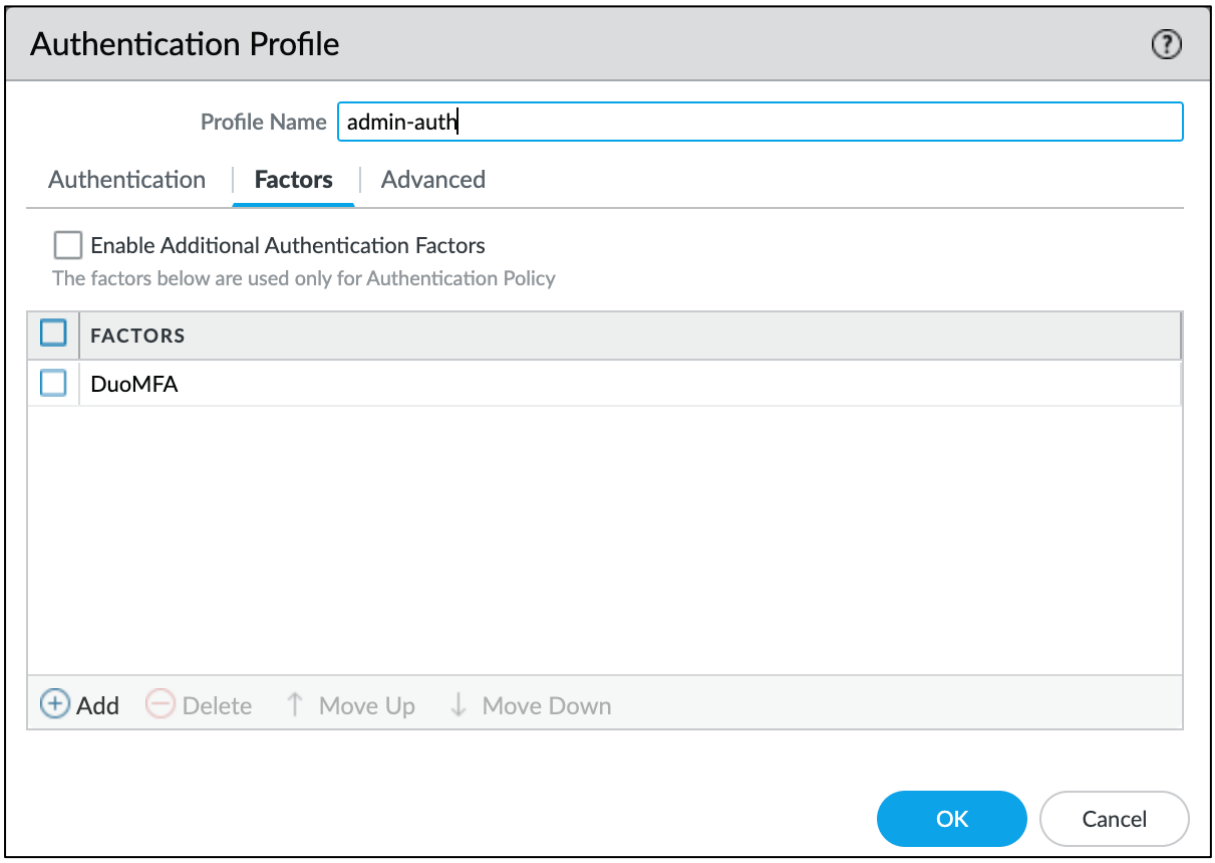

RADIUS Server Profile
Profile Name
RADIUS
Administrator Use Only
Server Settings
Timeout (sec)
3
Retries
3
Authentication Protocol
PEAP-MSCHAPv2
Allow users to change passwords after expiry
Make Outer Identity Anonymous
Certificate Profile
RADIUScert
Servers
NAME
RADIUS SERVER
SECRET
PORT
RAD1
192.168.0.18
****
1812
Add
Delete
Enter the IP address or FQDN of the RADIUS server
OK
Cancel

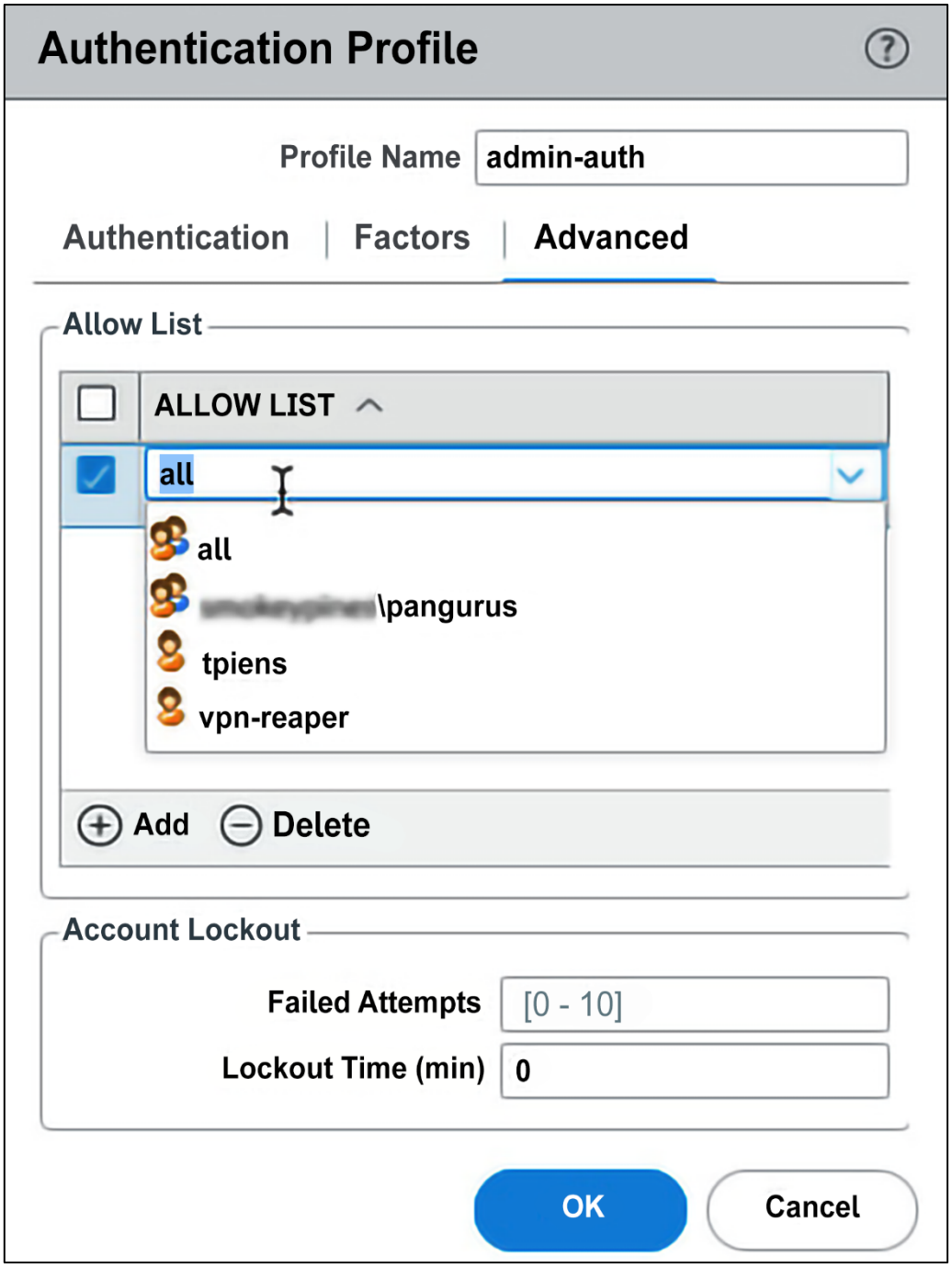

Certificate Profile
Name
RADIUScert
Username Field
None
User Domain
CA Certificates
NAME
DEFAULT OCSP URL
OCSP VERIFY CERTIFICATE
TEMPLATE NAME/OID
pangurus
http://ca.pangurus.com
rootCA
Add
Delete
Move Up
Move Down
Default OCSP URL (must start with http:// or https://)
Use CRL
Use OCSP
OCSP takes precedence over CRL
CRL Receive Timeout (sec)
5
OCSP Receive Timeout (sec)
5
Certificate Status Timeout (sec)
5
Block session if certificate status is unknown
Block session if certificate status cannot be retrieved within timeout
Block session if the certificate was not issued to the authenticating device
Block sessions with expired certificates
OK
Cancel

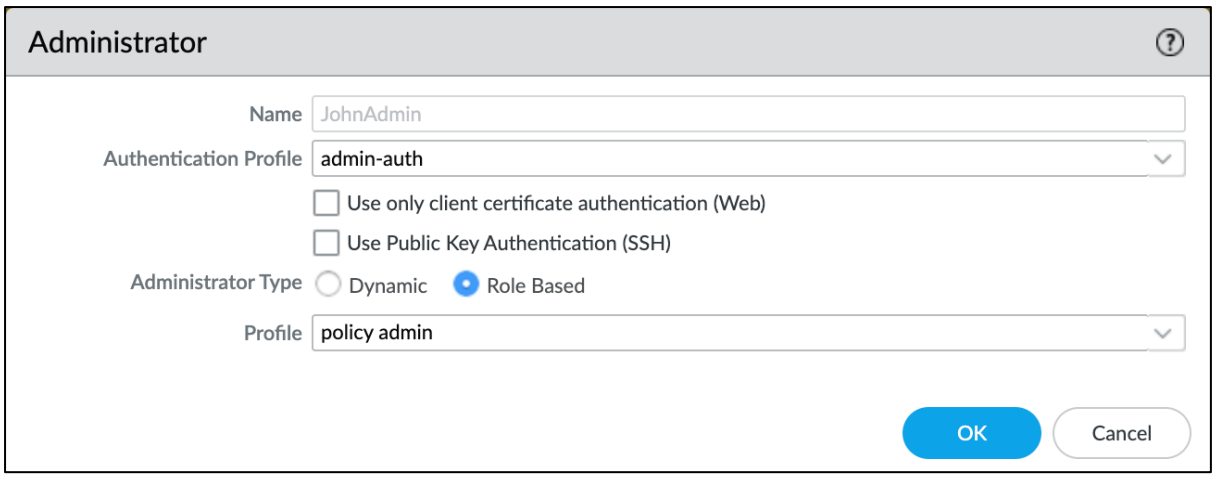

SAML Identity Provider Server Profile
Profile Name
azure-saml
Administrator Use Only
Identity Provider Configuration
Identity Provider ID
https://sts.windows.net/71fbaa2b-58a3-4d15-8dd4-21dbbce818c7/
Identity Provider Certificate
crt.azure-saml.shared
Select the certificate that IDP uses to sign SAML messages
Identity Provider SSO URL
https://login.microsoftonline.com/71fbaa2
Identity Provider SLO URL
https://login.microsoftonline.com/71fbaa2
SAML HTTP Binding for SSO Requests to IDP
Post
Redirect
SAML HTTP Binding for SLO Requests to IDP
Post
Redirect
Validate Identity Provider Certificate
Sign SAML Message to IDP
Maximum Clock Skew (seconds)
60
OK
Cancel

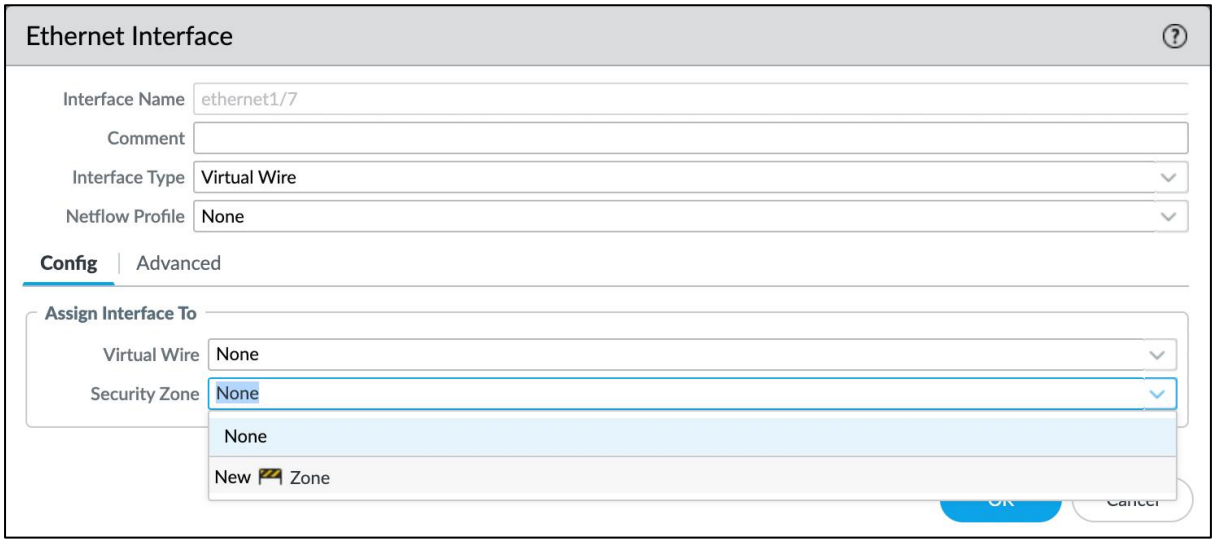

Multi Factor Authentication Server Profile
Profile Name
DuoMFA
Certificate Profile
MFA-profile
Server Settings
MFA Vendor
Duo v2
NAME
VALUE
API Host
api-.duosecurity.com
Integration Key
DIP IAH8
Secret Key
****
Timeout (sec)
30 [5 - 600]
Base URI
/auth/v2
OK
Cancel

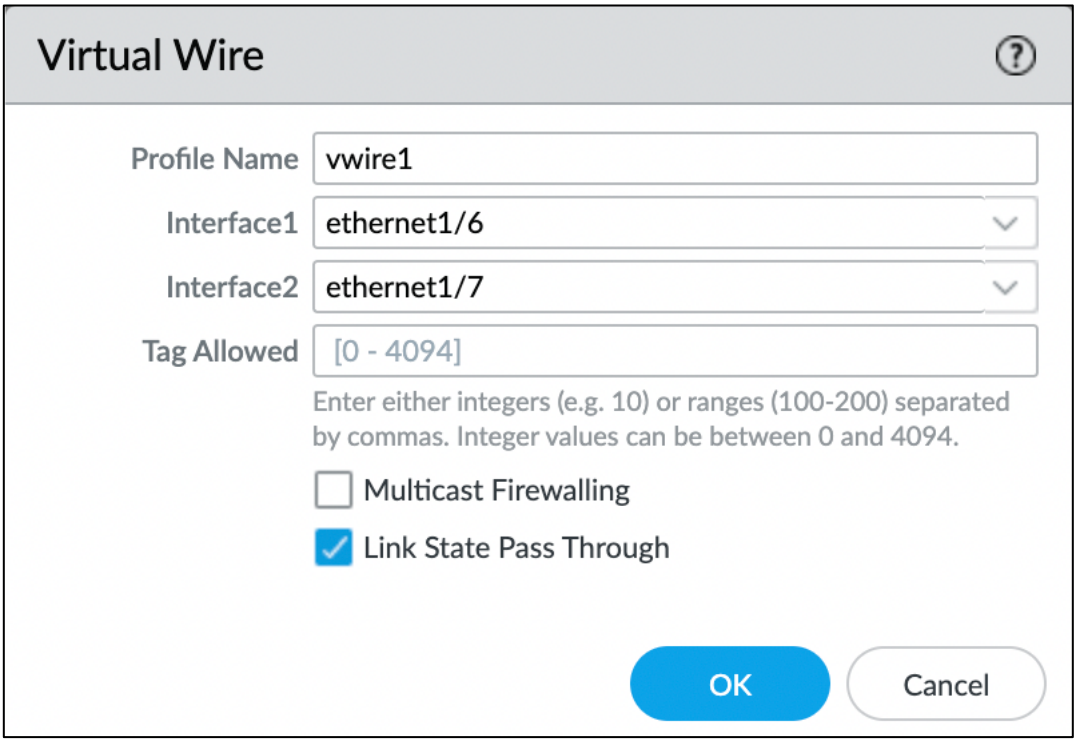

Authentication Profile
Profile Name
admin-auth
Authentication
Factors
Advanced
Type
LDAP
Server Profile
pangurus
Login Attribute
sAMAccountName
Password Expiry Warning
7
Number of days prior to warning a user about password expiry.
User Domain
pangurus
Username Modifier
%USERINPUT%
Single Sign On
Kerberos Realm
Kerberos Keytab
Click "Import" to configure this field
X Import
OK
Cancel

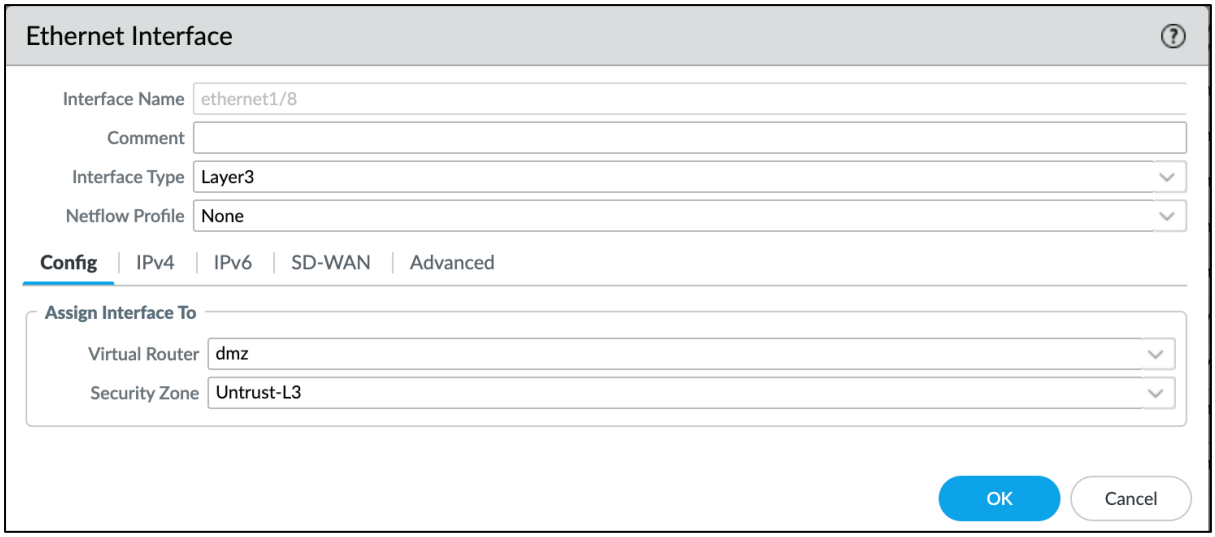

Authentication Profile
Profile Name
admin-auth
Authentication
Factors
Advanced
Enable Additional Authentication Factors
The factors below are used only for Authentication Policy
FACTORS
DuoMFA
Add
Delete
Move Up
Move Down
OK
Cancel

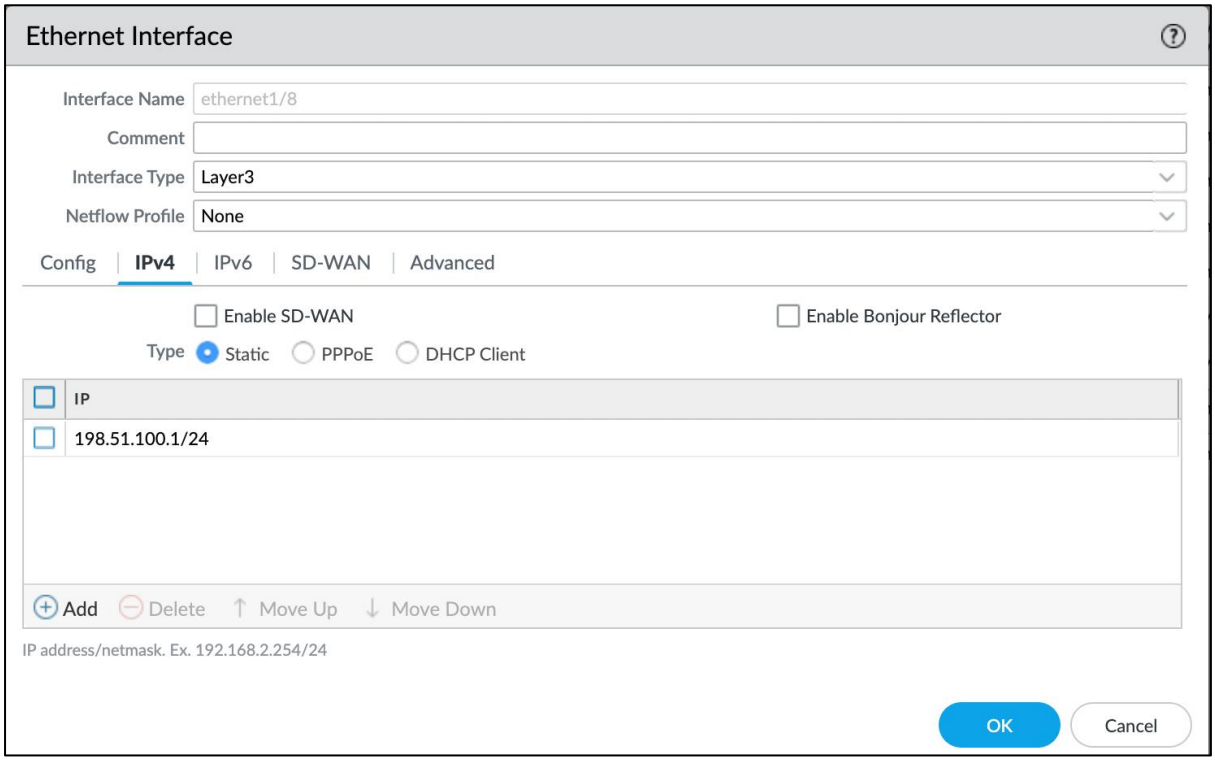

Authentication Profile
Profile Name
admin-auth
Authentication
Factors
Advanced
Allow List
ALLOW LIST
all
all
\pangurus
tpiens
vpn-reaper
Add
Delete
Account Lockout
Failed Attempts
[0 - 10]
Lockout Time (min)
0
OK
Cancel

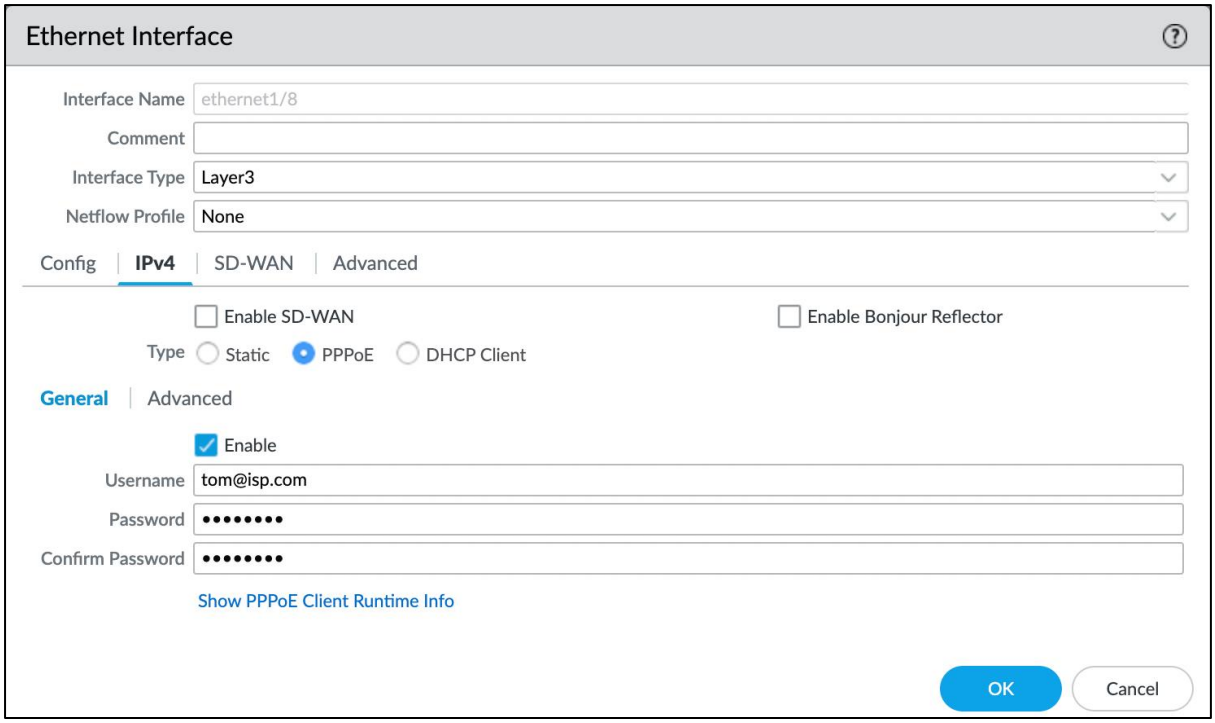

Administrator
Name
JohnAdmin
Authentication Profile
admin-auth
Use only client certificate authentication (Web)
Use Public Key Authentication (SSH)
Administrator Type
Dynamic
Role Based
Profile
policy admin
OK
Cancel

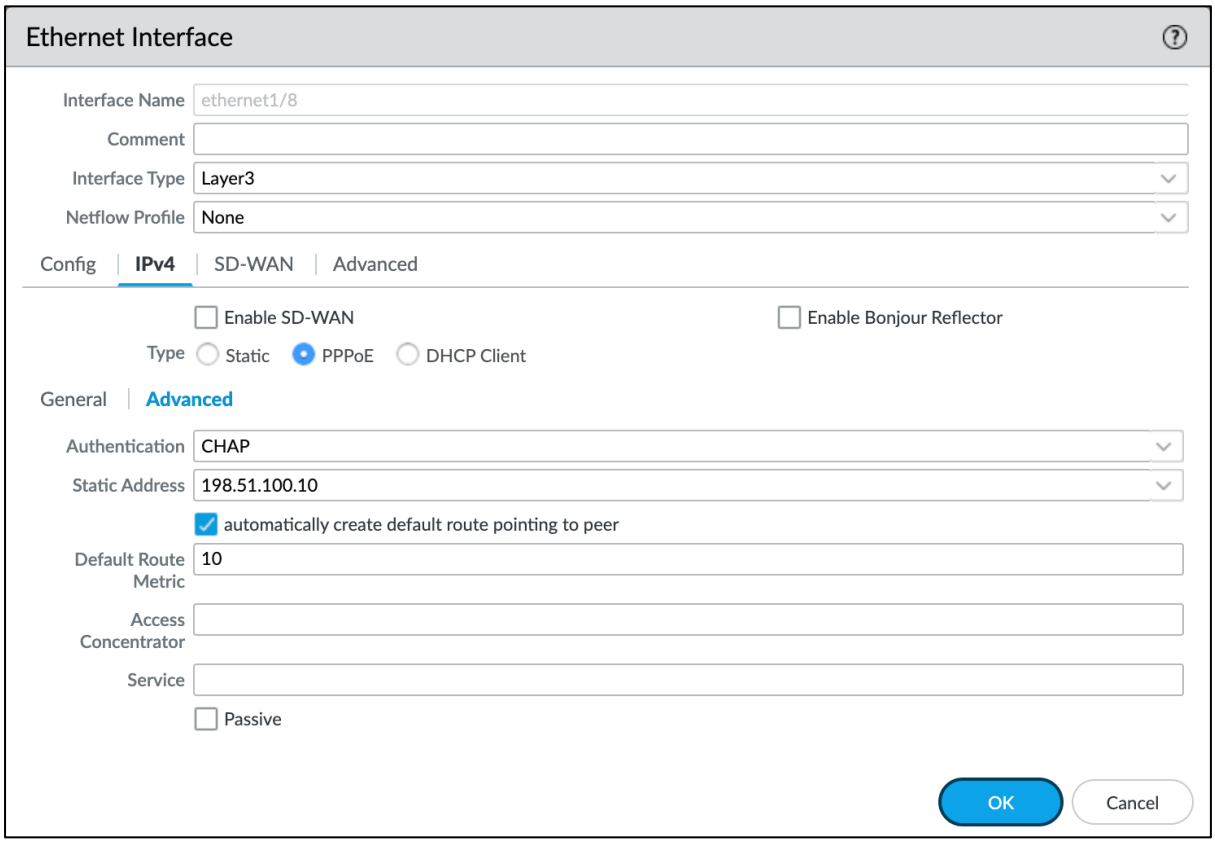

Ethernet Interface
Interface Name
ethernet1/7
Comment
Interface Type
Virtual Wire
Netflow Profile
None
Config
Advanced
Assign Interface To
Virtual Wire
None
Security Zone
None
None
New
Zone

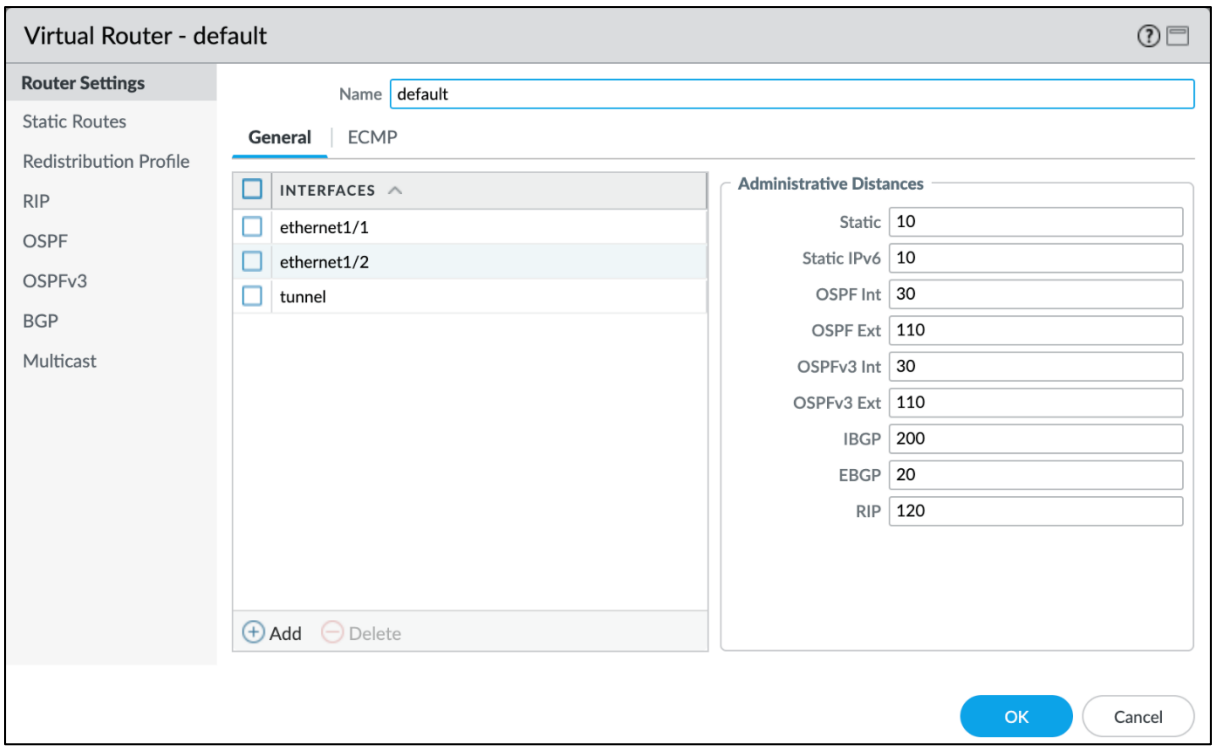

Virtual Wire
Profile Name
vwire1
Interface1
ethernet1/6
Interface2
ethernet1/7
Tag Allowed
[0 - 4094]
Enter either integers (e.g. 10) or ranges (100-200) separated by commas. Integer values can be between 0 and 4094.
Multicast Firewalling
Link State Pass Through
OK
Cancel

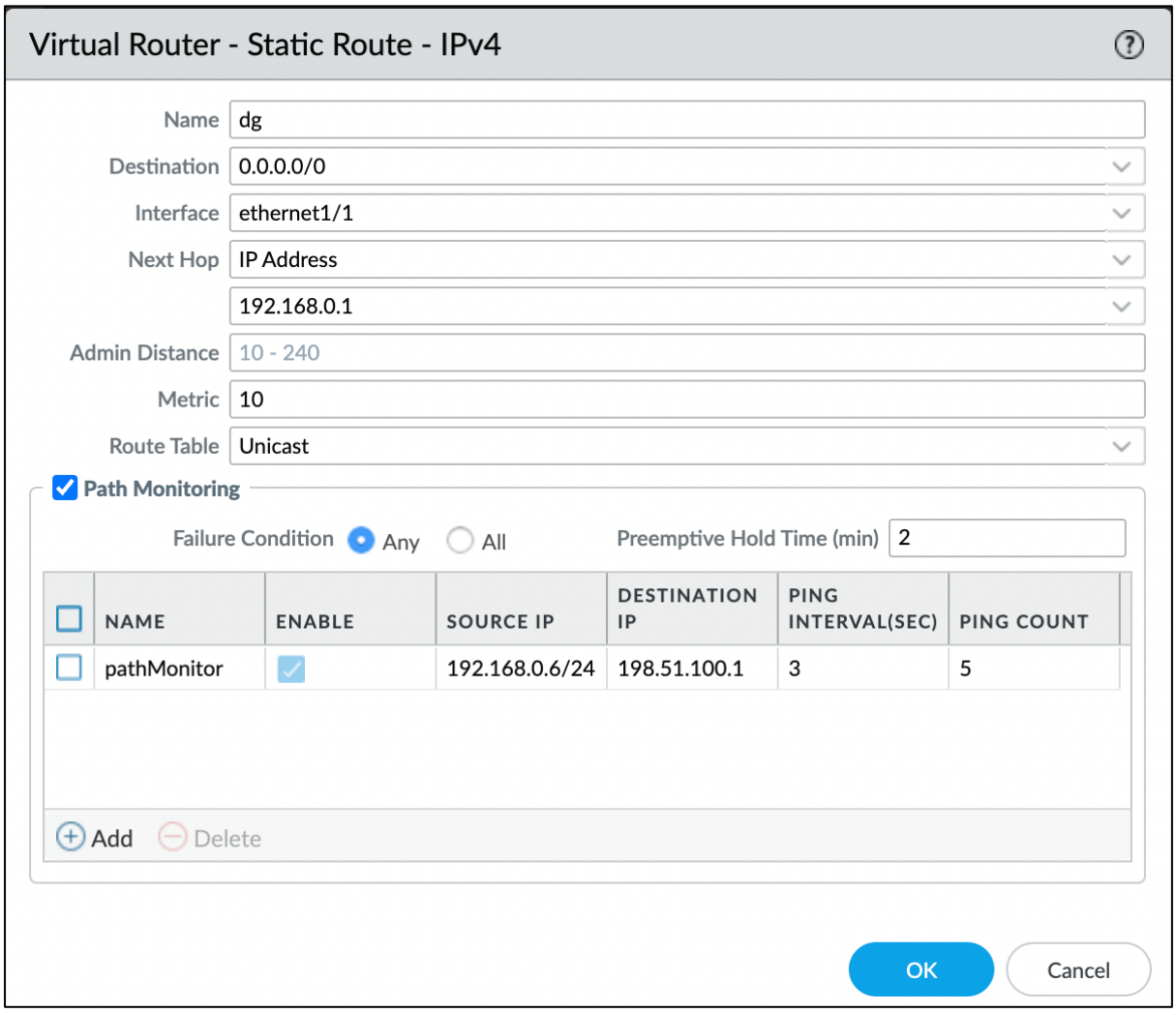

Ethernet Interface
Interface Name
ethernet1/8
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
SD-WAN
Advanced
Assign Interface To
Virtual Router
dmz
Security Zone
Untrust-L3
OK
Cancel

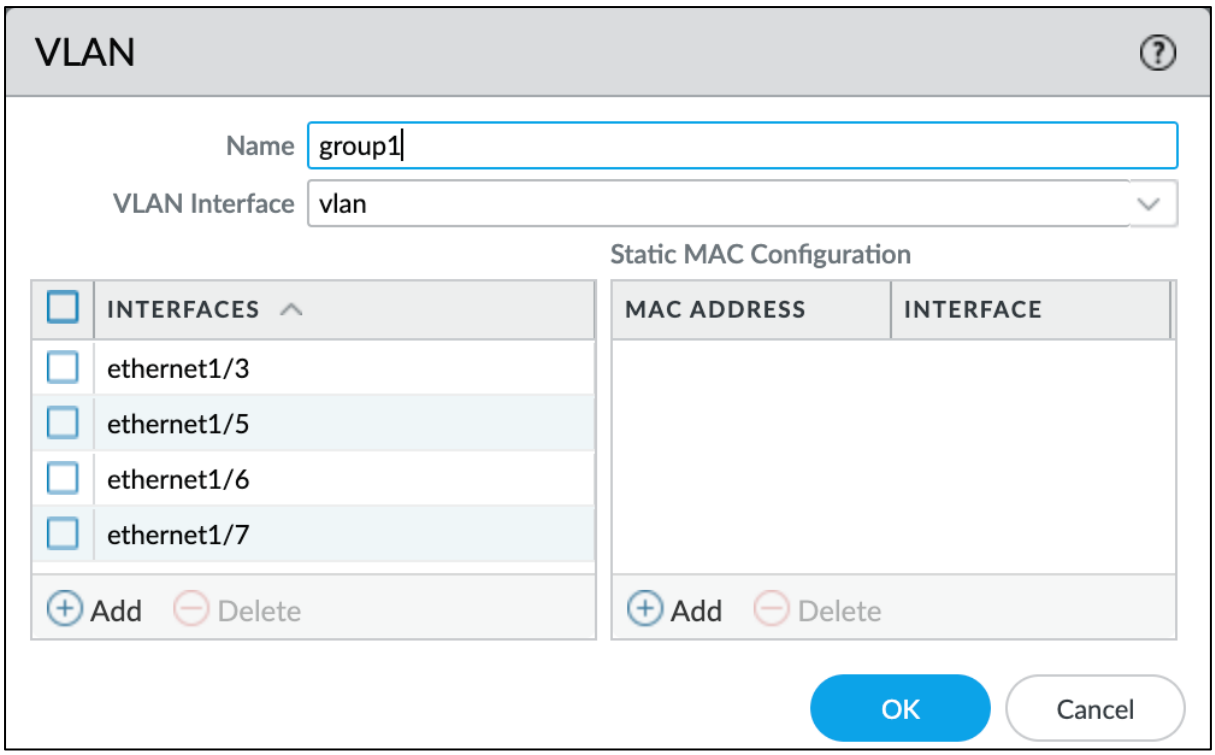

Ethernet Interface
Interface Name
ethernet1/8
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
SD-WAN
Advanced
Enable SD-WAN
Enable Bonjour Reflector
Type
Static
PPPoE
DHCP Client
IP
198.51.100.1/24
Add
Delete
Move Up
Move Down
IP address/netmask. Ex. 192.168.2.254/24
OK
Cancel

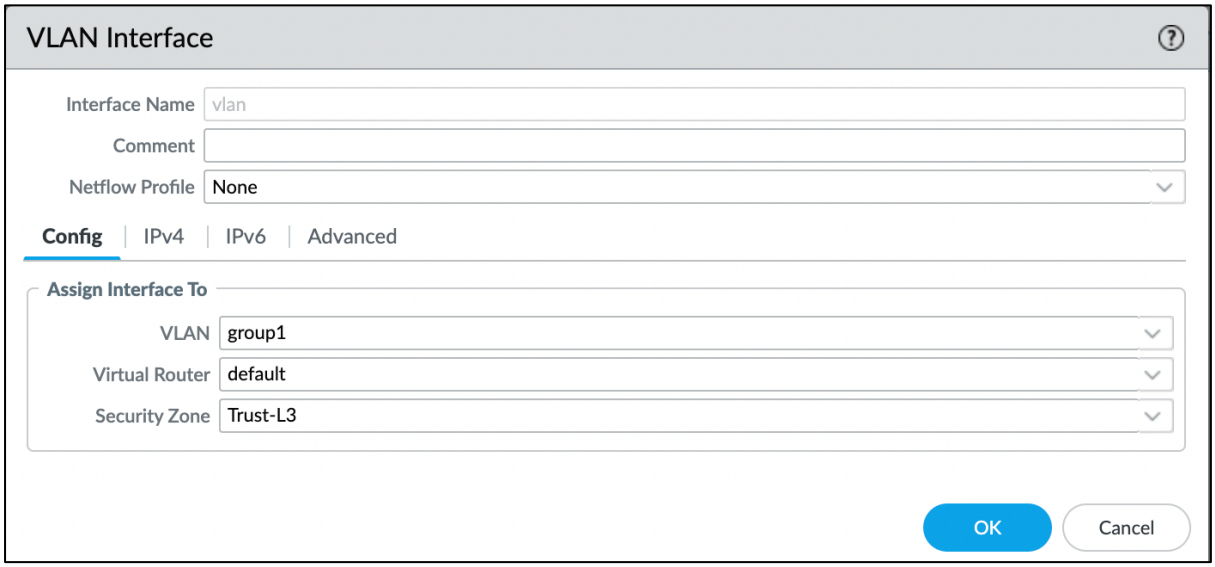

Ethernet Interface
Interface Name
ethernet1/8
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
SD-WAN
Advanced
Enable SD-WAN
Enable Bonjour Reflector
Type
Static
PPPoE
DHCP Client
General
Advanced
Enable
Username
tom@isp.com
Password
Confirm Password
Show PPPoE Client Runtime Info
OK
Cancel

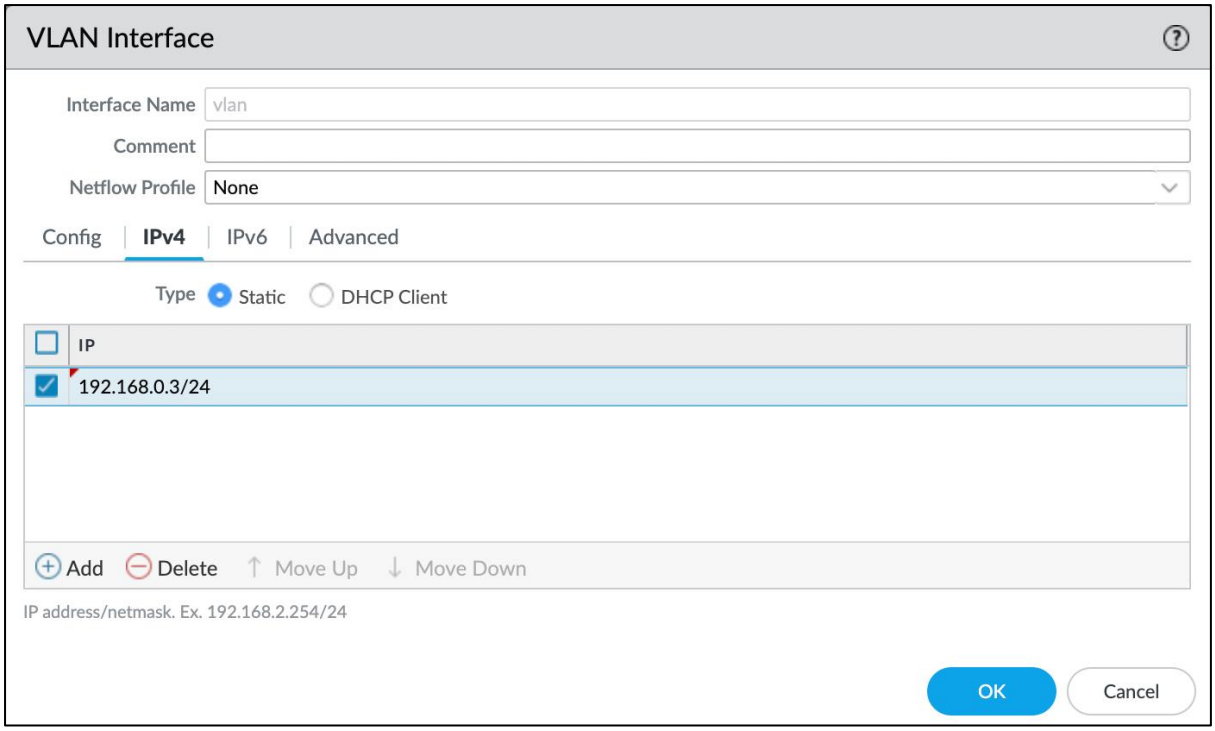

Ethernet Interface
Interface Name
ethernet1/8
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
SD-WAN
Advanced
Enable SD-WAN
Enable Bonjour Reflector
Type
Static
PPPoE
DHCP Client
General
Advanced
Authentication
CHAP
Static Address
198.51.100.10
automatically create default route pointing to peer
Default Route Metric
10
Access Concentrator
Service
Passive
OK
Cancel

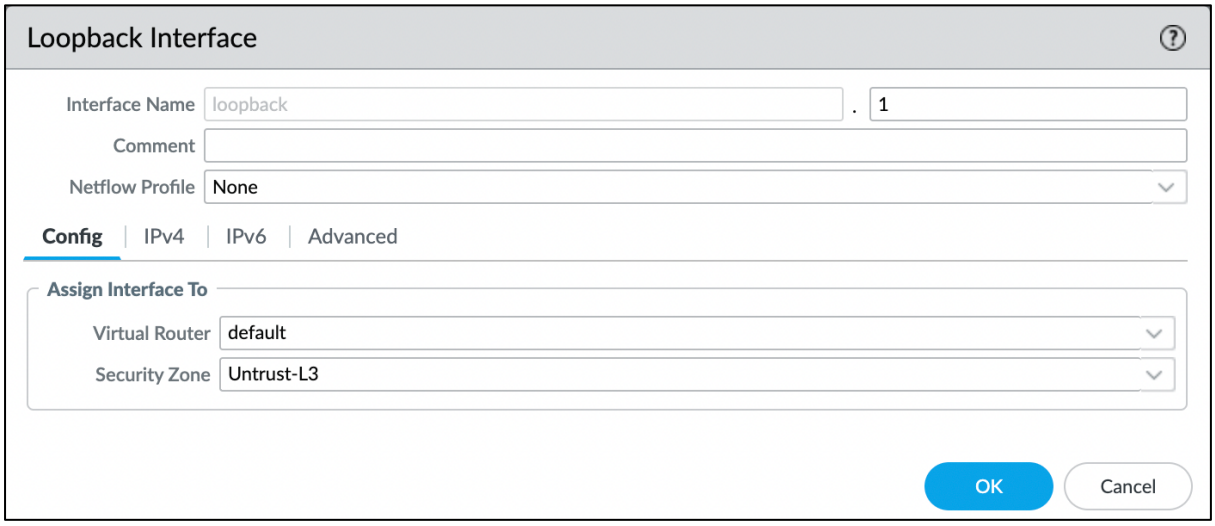

Virtual Router - default
Router Settings
Static Routes
Redistribution Profile
RIP
OSPF
OSPFv3
BGP
Multicast
Name
default
General
ECMP
INTERFACES
ethernet1/1
ethernet1/2
tunnel
Add
Delete
Administrative Distances
Static
10
Static IPv6
10
OSPF Int
30
OSPF Ext
110
OSPFv3 Int
30
OSPFv3 Ext
110
IBGP
200
EBGP
20
RIP
120
OK
Cancel

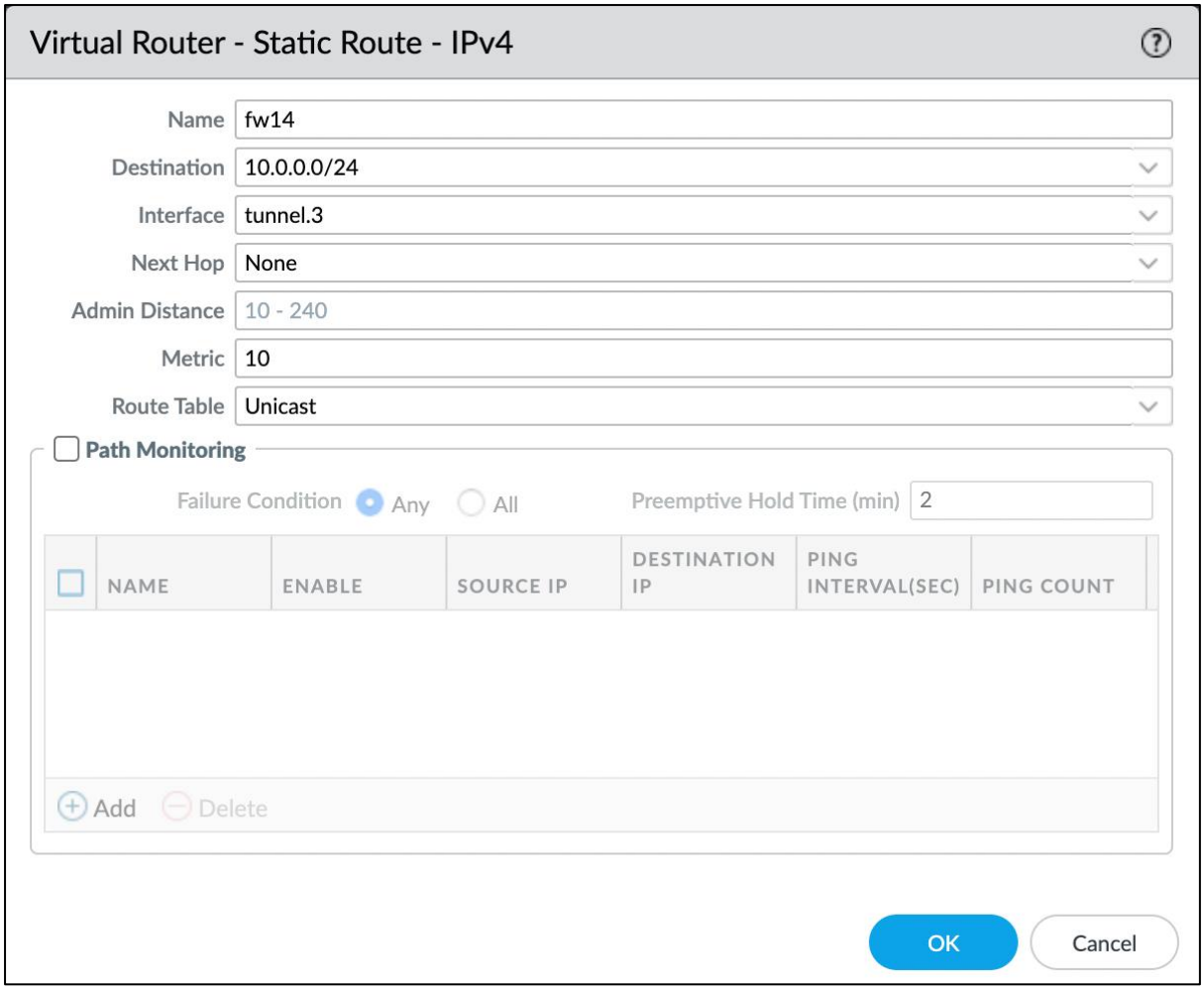

Virtual Router - Static Route - IPv4
Name
dg
Destination
0.0.0.0/0
Interface
ethernet1/1
Next Hop
IP Address
192.168.0.1
Admin Distance
10 - 240
Metric
10
Route Table
Unicast
Path Monitoring
Failure Condition
Any
All
Preemptive Hold Time (min)
2
NAME
ENABLE
SOURCE IP
DESTINATION IP
PING INTERVAL(SEC)
PING COUNT
pathMonitor
192.168.0.6/24
198.51.100.1
3
5
Add
Delete
OK
Cancel

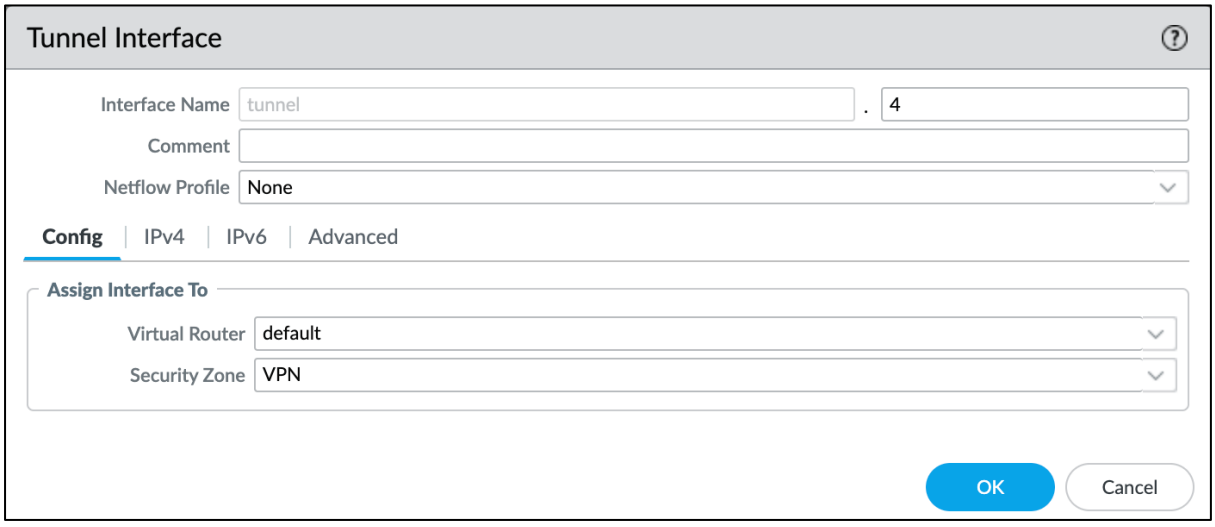

VLAN
Name
group1
VLAN Interface
vlan
Static MAC Configuration
INTERFACES
MAC ADDRESS
INTERFACE
ethernet1/3
ethernet1/5
ethernet1/6
ethernet1/7
Add
Delete
Add
Delete
OK
Cancel


VLAN Interface
Interface Name
vlan
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Assign Interface To
VLAN
group1
Virtual Router
default
Security Zone
Trust-L3
OK
Cancel

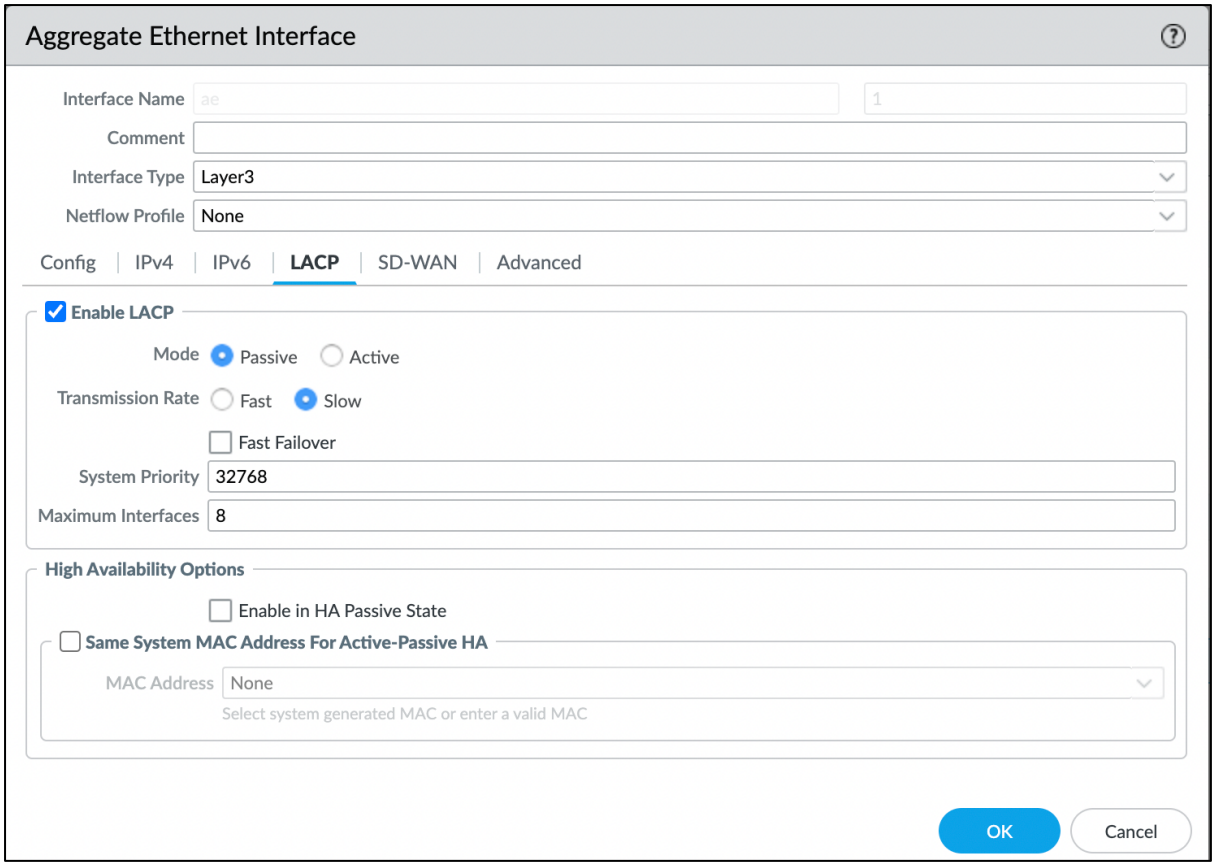

VLAN Interface
Interface Name
vlan
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Type
Static
DHCP Client
IP
192.168.0.3/24
Add
Delete
Move Up
Move Down
IP address/netmask. Ex. 192.168.2.254/24
OK
Cancel

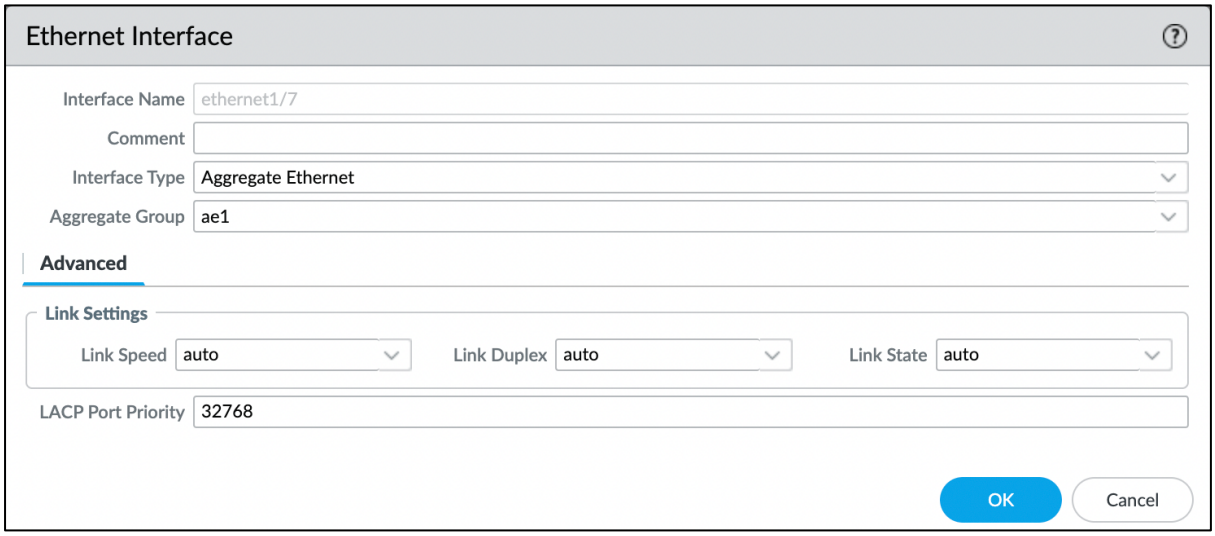

Loopback Interface
Interface Name
loopback
1
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Assign Interface To
Virtual Router
default
Security Zone
Untrust-L3
OK
Cancel

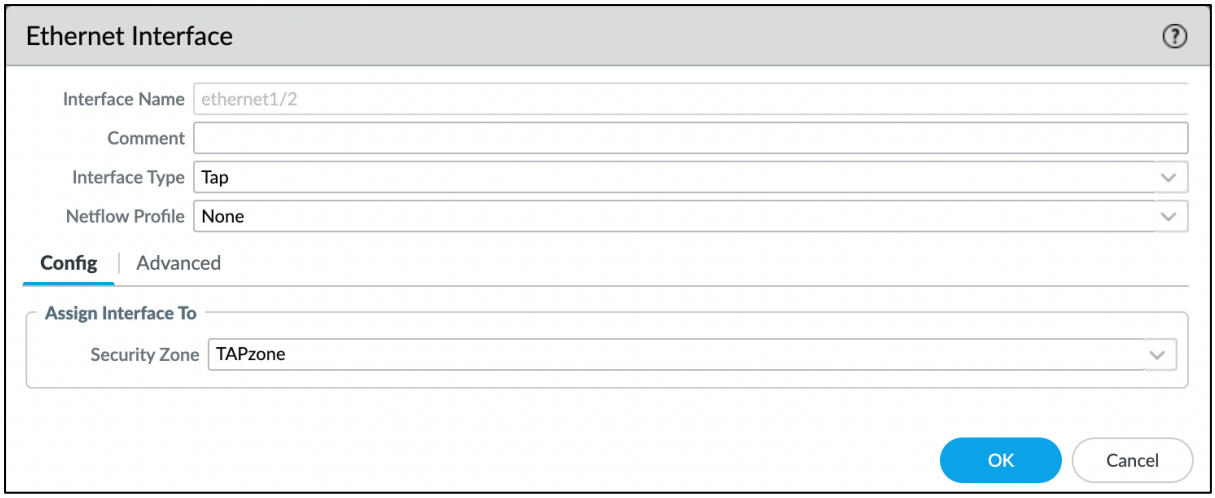




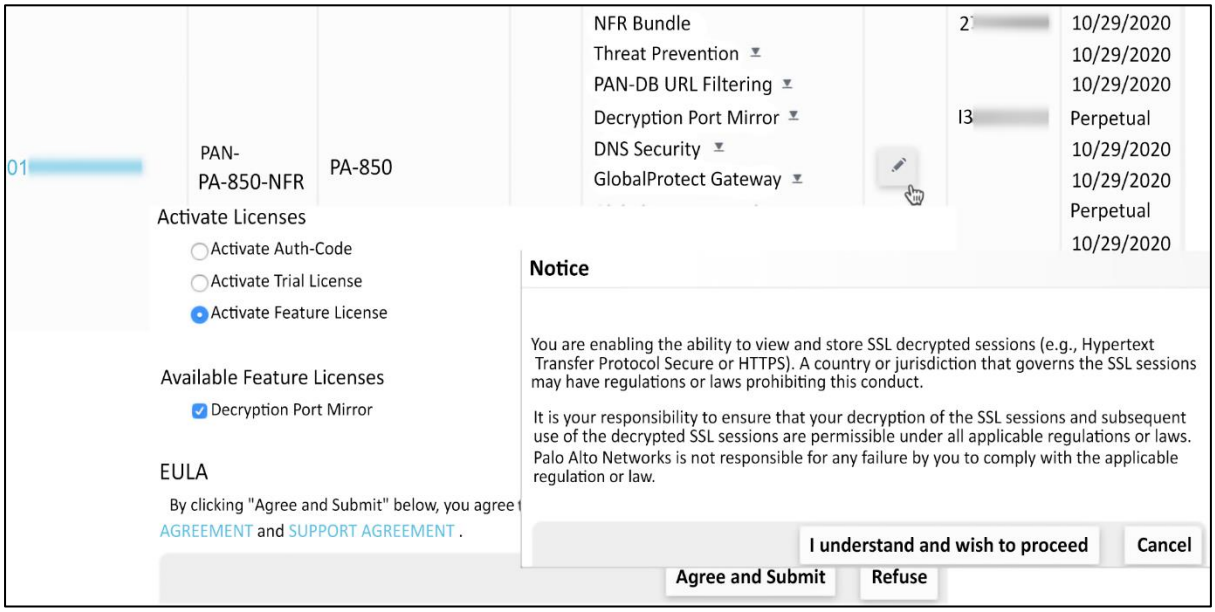
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/8	Layer3			none	none	Untagged	none	none
ethernet1/8.10	Layer3			172.16.0.1/24	default	10	none	LAN
ethernet1/8.20	Layer3			192.168.0.1/24	default	20	none	DMZ


Aggregate Ethernet Interface
Interface Name
ae
1
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
LACP
SD-WAN
Advanced
Enable LACP
Mode
Passive
Active
Transmission Rate
Fast
Slow
Fast Failover
System Priority
32768
Maximum Interfaces
8
High Availability Options
Enable in HA Passive State
Same System MAC Address For Active-Passive HA
MAC Address
None
Select system generated MAC or enter a valid MAC
OK
Cancel

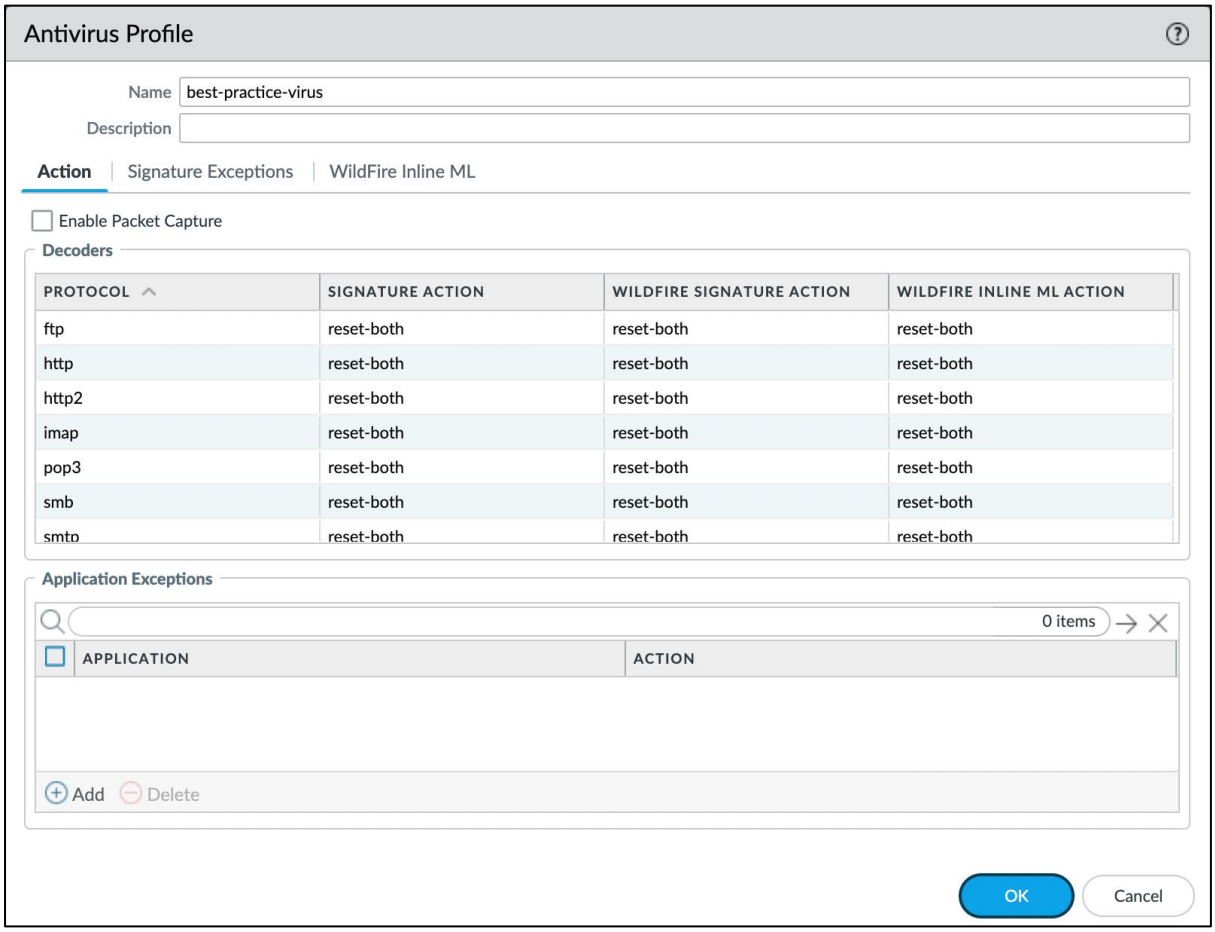

Ethernet Interface
Interface Name
ethernet1/7
Comment
Interface Type
Aggregate Ethernet
Aggregate Group
ae1
Advanced
Link Settings
Link Speed
auto
Link Duplex
auto
Link State
auto
LACP Port Priority
32768
OK
Cancel

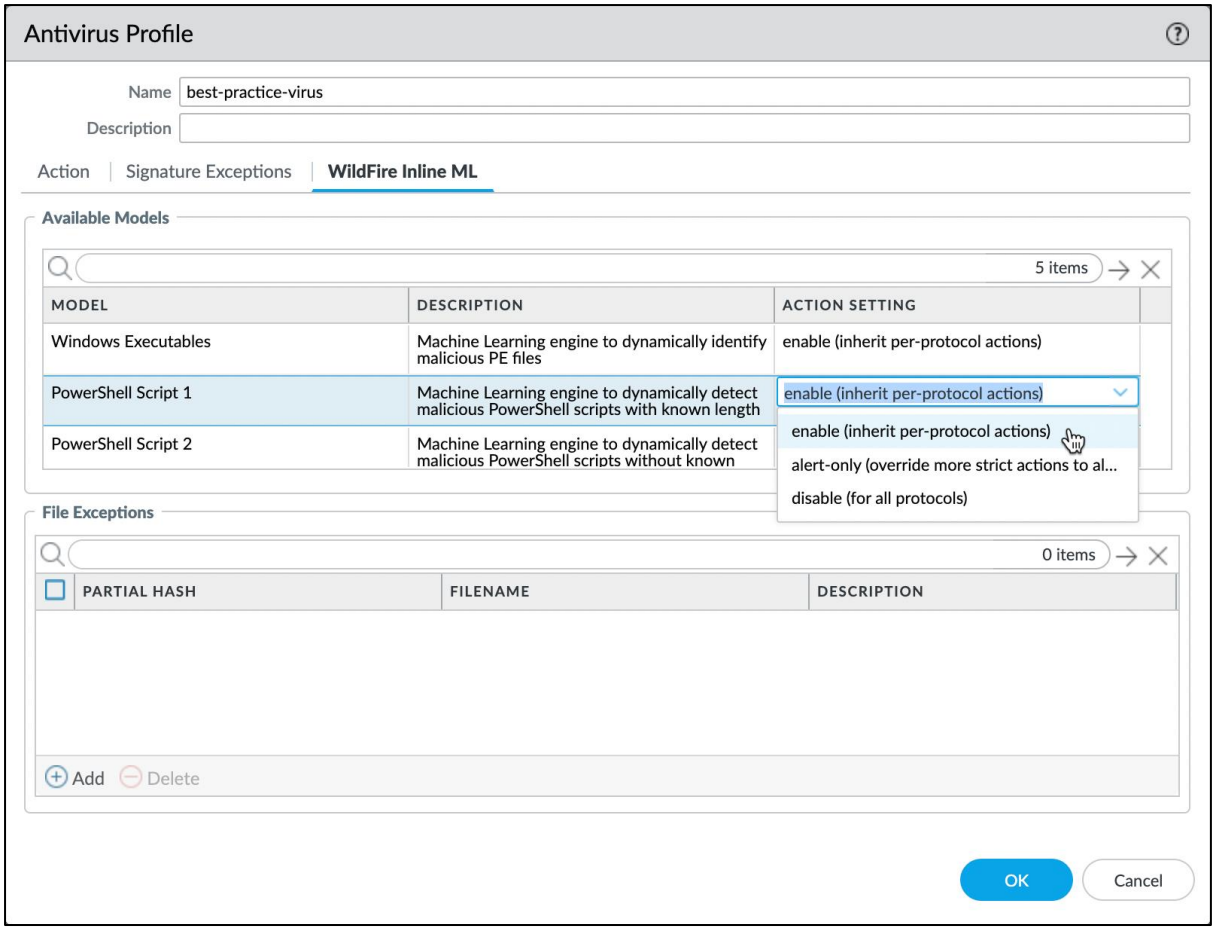

Ethernet Interface
Interface Name
ethernet1/2
Comment
Interface Type
Tap
Netflow Profile
None
Config
Advanced
Assign Interface To
Security Zone
TAPzone
OK
Cancel

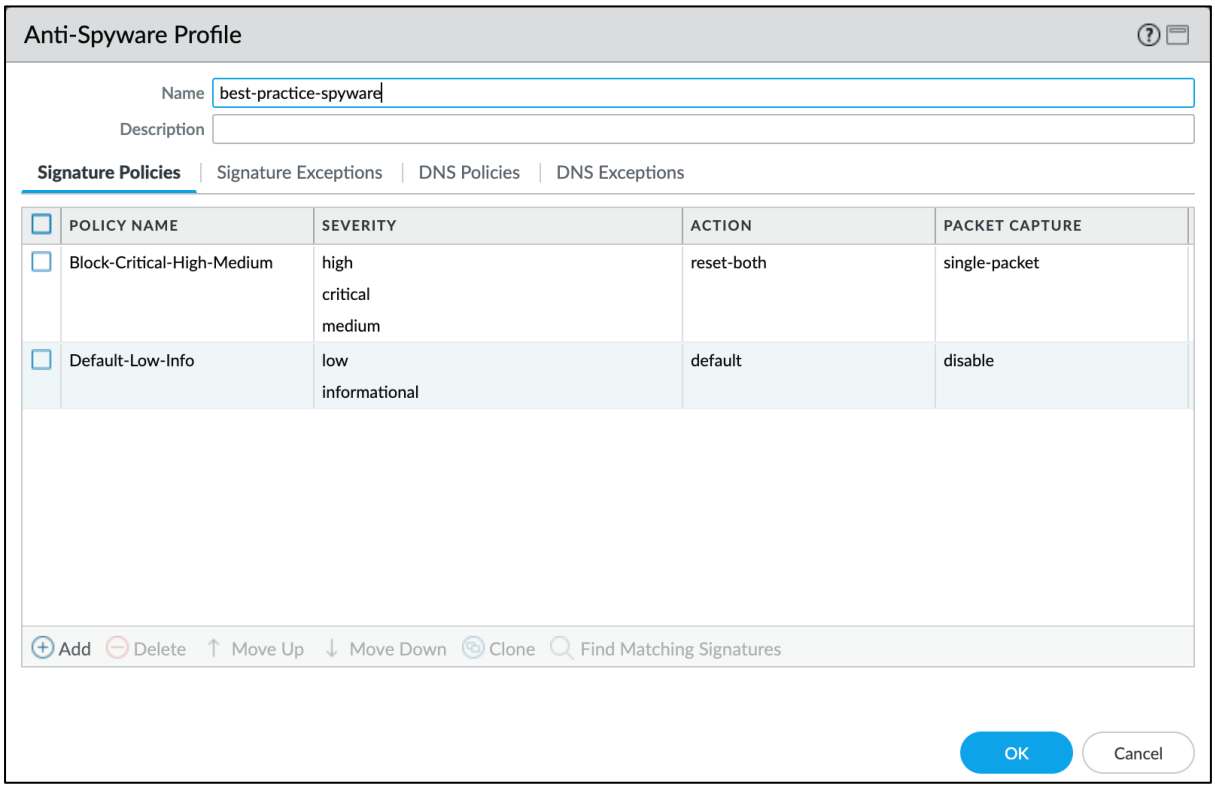

NAME
TYPE
Source
ZONE
ADDRESS
Destination
ZONE
ADDRESS
APPLICATION
SERVICE
ACTION
PROFILE
OPTIONS
1
TAP-inspect
universal
TAP...
any
TAPz...
any
any
application-default
Allow

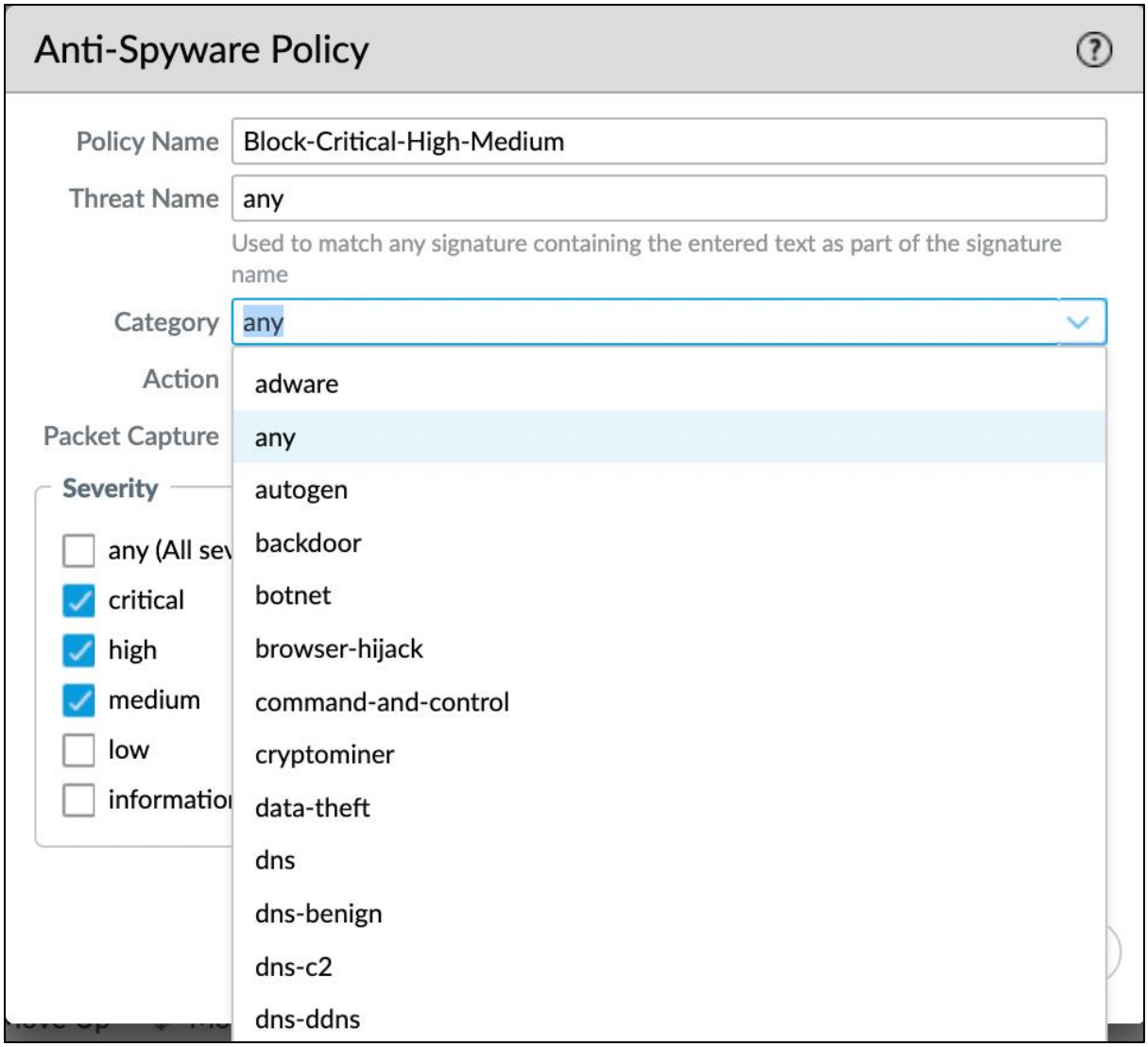

NFR Bundle
Threat Prevention
PAN-DB URL Filtering
Decryption Port Mirror
DNS Security
GlobalProtect Gateway
10/29/2020
10/29/2020
10/29/2020
Perpetual
10/29/2020
10/29/2020
Perpetual
10/29/2020
PAN-
PA-850-NFR
PA-850
Activate Licenses
Activate Auth-Code
Activate Trial License
Activate Feature License
Available Feature Licenses
Decryption Port Mirror
EULA
By clicking "Agree and Submit" below, you agree
AGREEMENT and SUPPORT AGREEMENT .
Notice
You are enabling the ability to view and store SSL decrypted sessions (e.g., Hypertext Transfer Protocol Secure or HTTPS). A country or jurisdiction that governs the SSL sessions may have regulations or laws prohibiting this conduct.
It is your responsibility to ensure that your decryption of the SSL sessions and subsequent use of the decrypted SSL sessions are permissible under all applicable regulations or laws. Palo Alto Networks is not responsible for any failure by you to comply with the applicable regulation or law.
I understand and wish to proceed
Cancel
Agree and Submit
Refuse

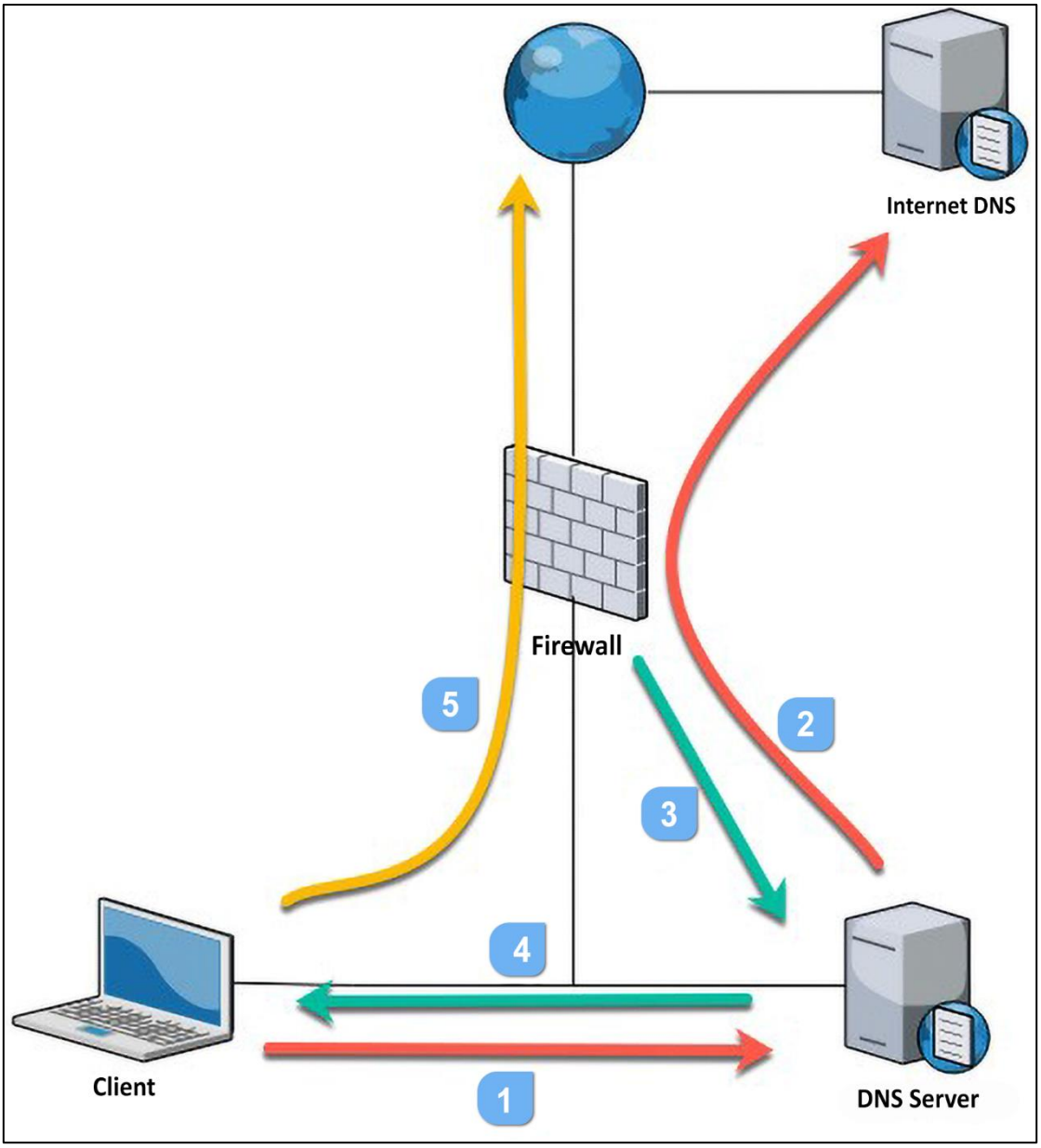
Chapter 3: Building Strong Policies

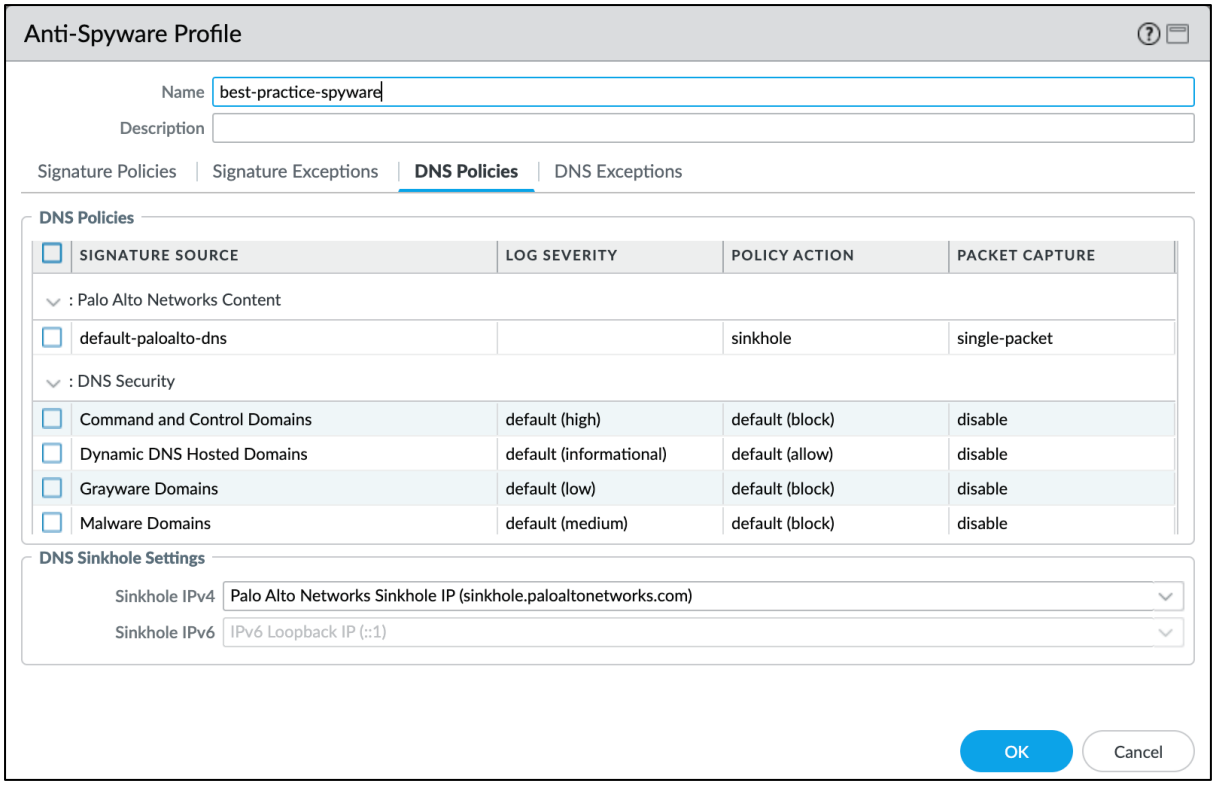


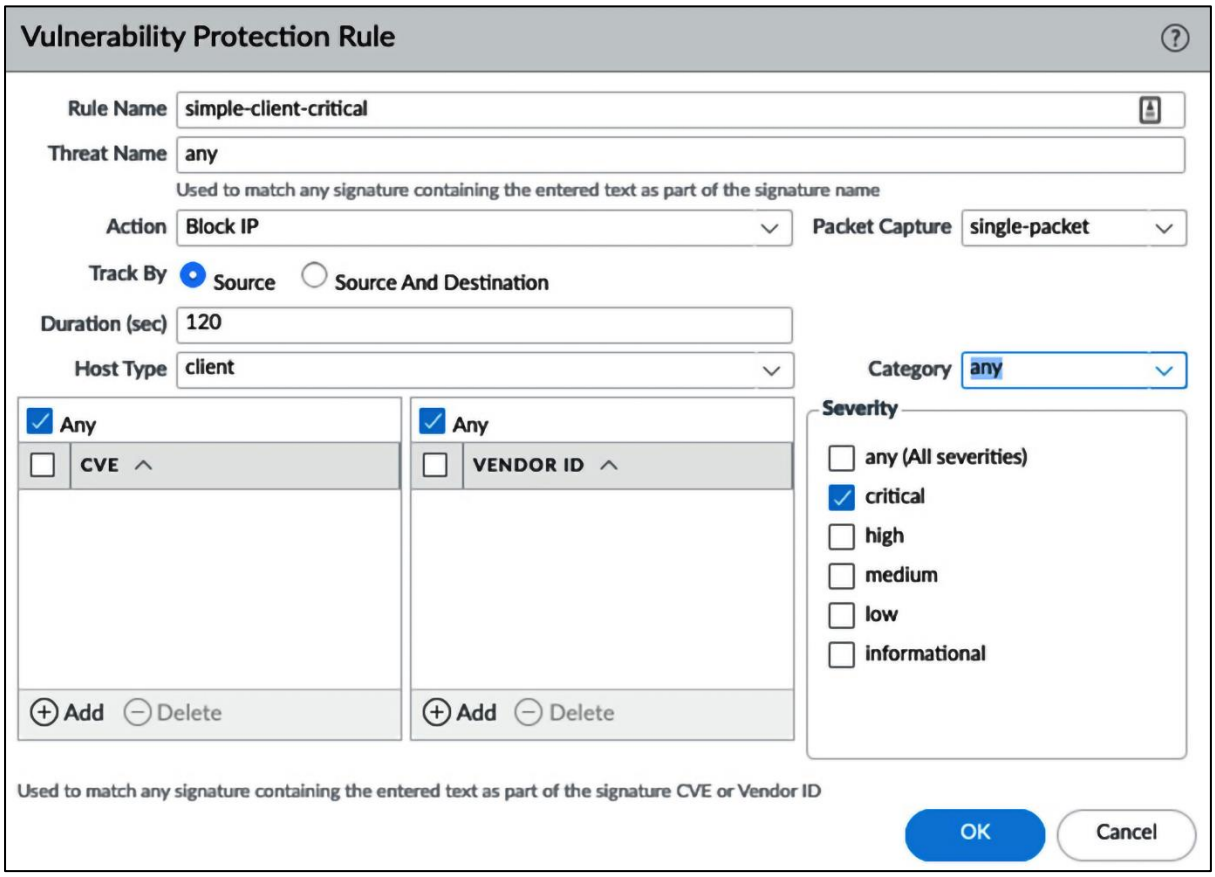

Antivirus Profile
Name best-practice-virus
Description
Action | Signature Exceptions | WildFire Inline ML
Available Models
5 items
MODEL
DESCRIPTION
ACTION SETTING
Windows Executables
Machine Learning engine to dynamically identify malicious PE files
enable (inherit per-protocol actions)
PowerShell Script 1
Machine Learning engine to dynamically detect malicious PowerShell scripts with known length
enable (inherit per-protocol actions)
PowerShell Script 2
Machine Learning engine to dynamically detect malicious PowerShell scripts without known
enable (inherit per-protocol actions)
alert-only (override more strict actions to al...
disable (for all protocols)
File Exceptions
0 items
PARTIAL HASH
FILENAME
DESCRIPTION
Add
Delete
OK
Cancel


Anti-Spyware Profile
Name best-practice-spyware
Description
Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions
POLICY NAME
SEVERITY
ACTION
PACKET CAPTURE
Block-Critical-High-Medium
high
critical
medium
reset-both
single-packet
Default-Low-Info
low
informational
default
disable
Add
Delete
Move Up
Move Down
Clone
Find Matching Signatures
OK
Cancel


Anti-Spyware Policy
Policy Name
Block-Critical-High-Medium
Threat Name
any
Used to match any signature containing the entered text as part of the signature name
Category
any
Action
Packet Capture
Severity
any (All sev
critical
high
medium
low
informatio
adware
any
autogen
backdoor
botnet
browser-hijack
command-and-control
cryptominer
data-theft
dns
dns-benign
dns-c2
dns-ddns


Internet DNS
Firewall
5
2
3
4
Client
1
DNS Server


Anti-Spyware Profile
Name
best-practice-spyware
Description
Signature Policies
Signature Exceptions
DNS Policies
DNS Exceptions
DNS Policies
SIGNATURE SOURCE
LOG SEVERITY
POLICY ACTION
PACKET CAPTURE
: Palo Alto Networks Content
default-paloalto-dns
sinkhole
single-packet
: DNS Security
Command and Control Domains
default (high)
default (block)
disable
Dynamic DNS Hosted Domains
default (informational)
default (allow)
disable
Grayware Domains
default (low)
default (block)
disable
Malware Domains
default (medium)
default (block)
disable
DNS Sinkhole Settings
Sinkhole IPv4
Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)
Sinkhole IPv6
IPv6 Loopback IP (::1)
OK
Cancel


Vulnerability Protection Rule
Rule Name
simple-client-critical
Threat Name
any
Used to match any signature containing the entered text as part of the signature name
Action
Block IP
Packet Capture
single-packet
Track By
Source
Source And Destination
Duration (sec)
120
Host Type
client
Category
any
Any
CVE
Add
Delete
Any
VENDOR ID
Add
Delete
Severity
any (All severities)
critical
high
medium
low
informational
Used to match any signature containing the entered text as part of the signature CVE or Vendor ID
OK
Cancel

Vulnerability Protection Profile

Name: best-practice-vulnerability

Description: Best practice Vulnerability Protection profile created through BPA Plus configuration commands

Rules | Exceptions

RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
Block-Critical-High-Medium	any	any	any	critical high medium	reset-both	single-packet
Default-Low-Info	any	any	any	low informational	default	disable

Add | Delete | Move Up | Move Down | Clone | Find Matching Signatures

OK | Cancel

URL Filtering Profile

Name: CorpURL

Description:

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

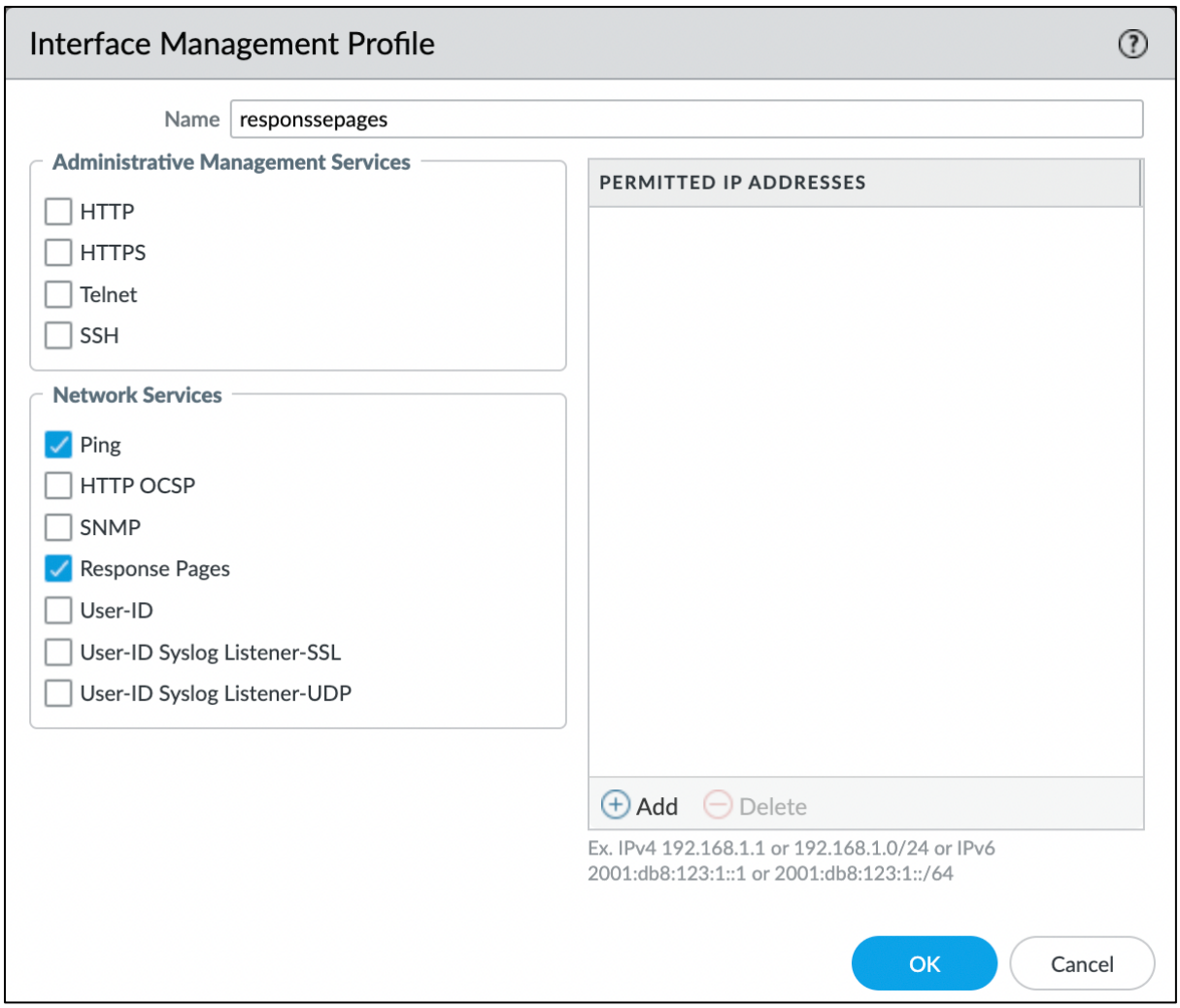
75 items

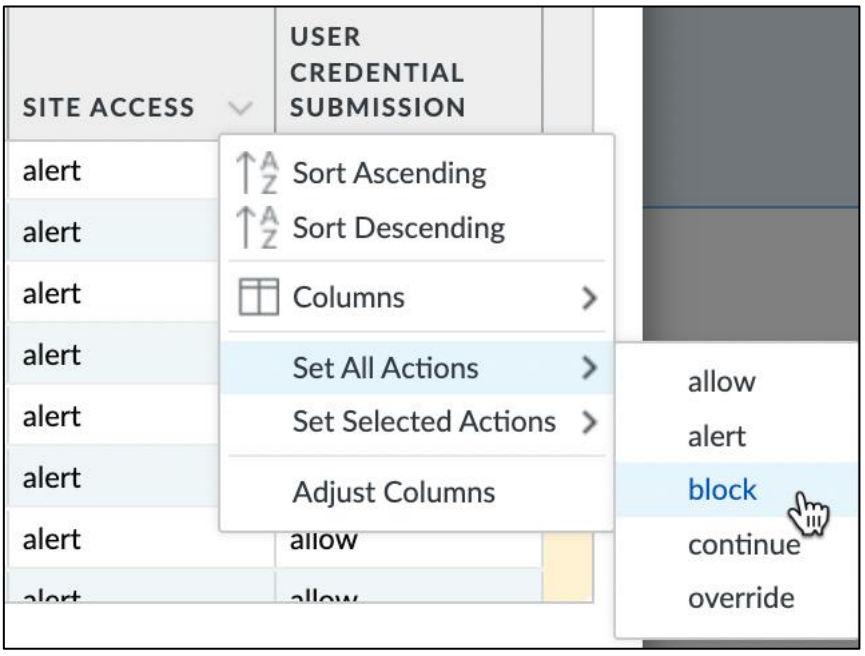
CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Custom URL Categories		
risky-sites *	continue	block
customcategory *	alert	none
External Dynamic URL Lists		
phishing +	block	block
Pre-defined Categories		
web-hosting	alert	allow

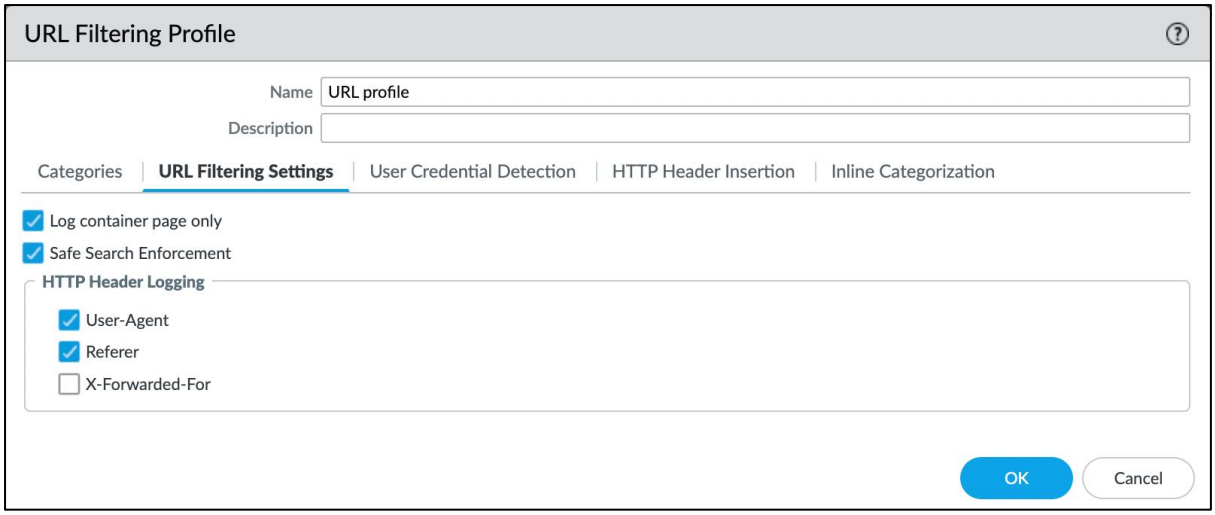
* indicates a custom URL category, + indicates external dynamic list

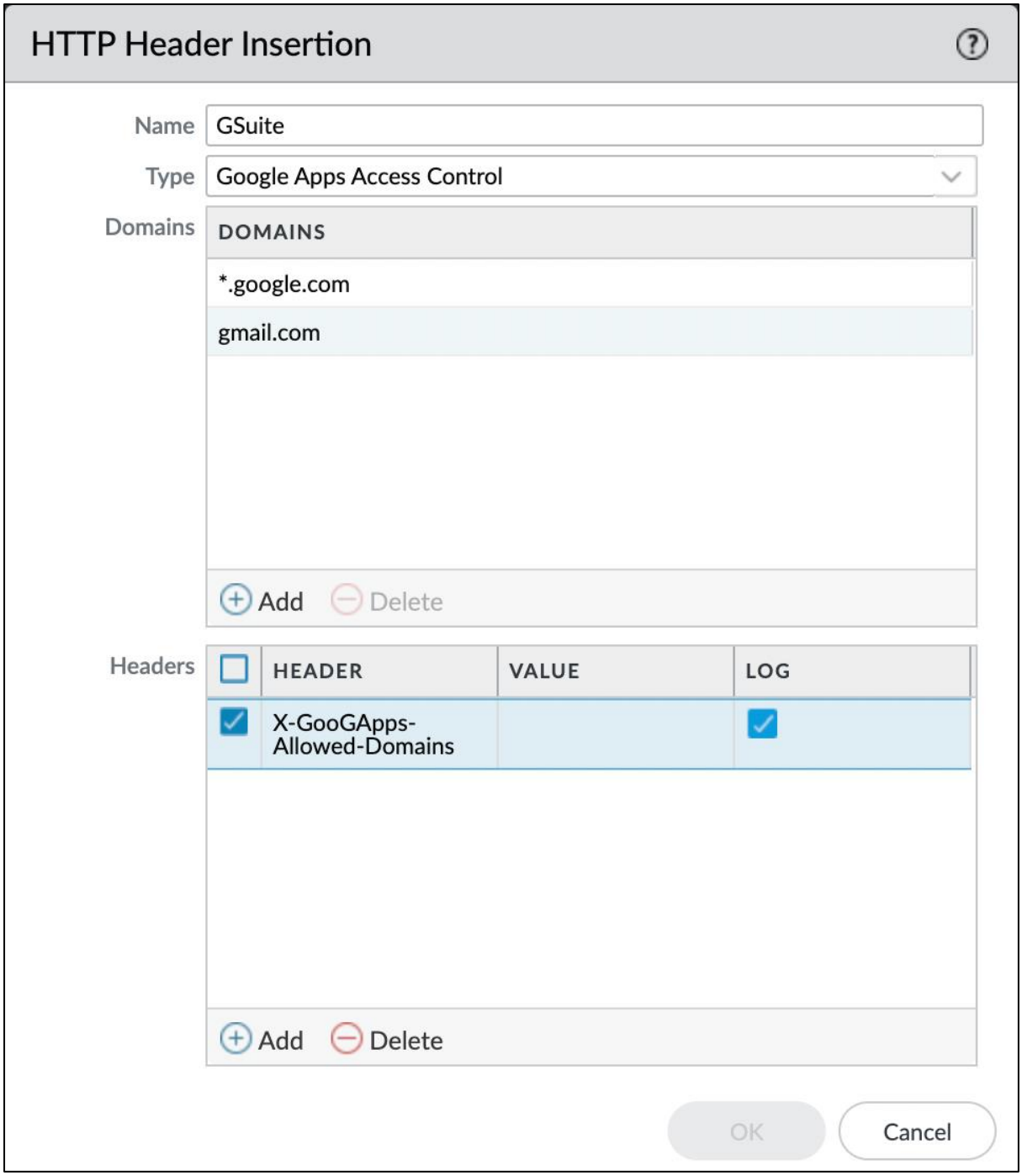
Check URL Category

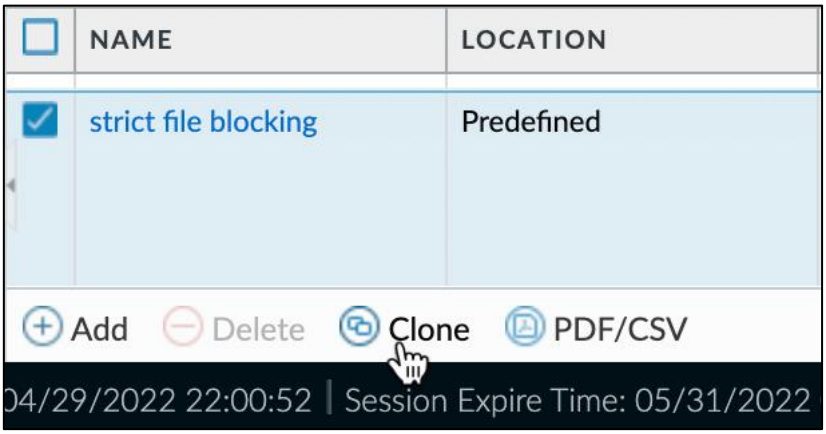
OK | Cancel

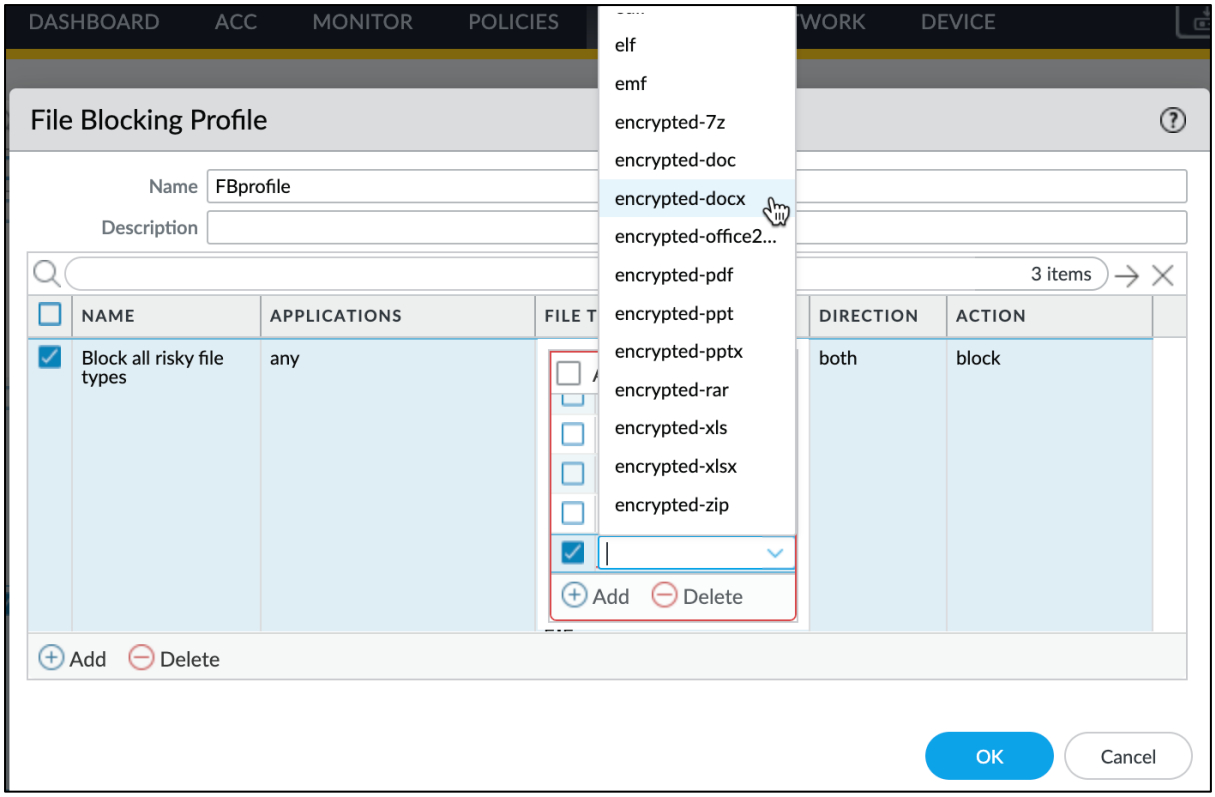

Interface Management Profile
Name
responssepages
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
PERMITTED IP ADDRESSES
Add
Delete
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64
OK
Cancel

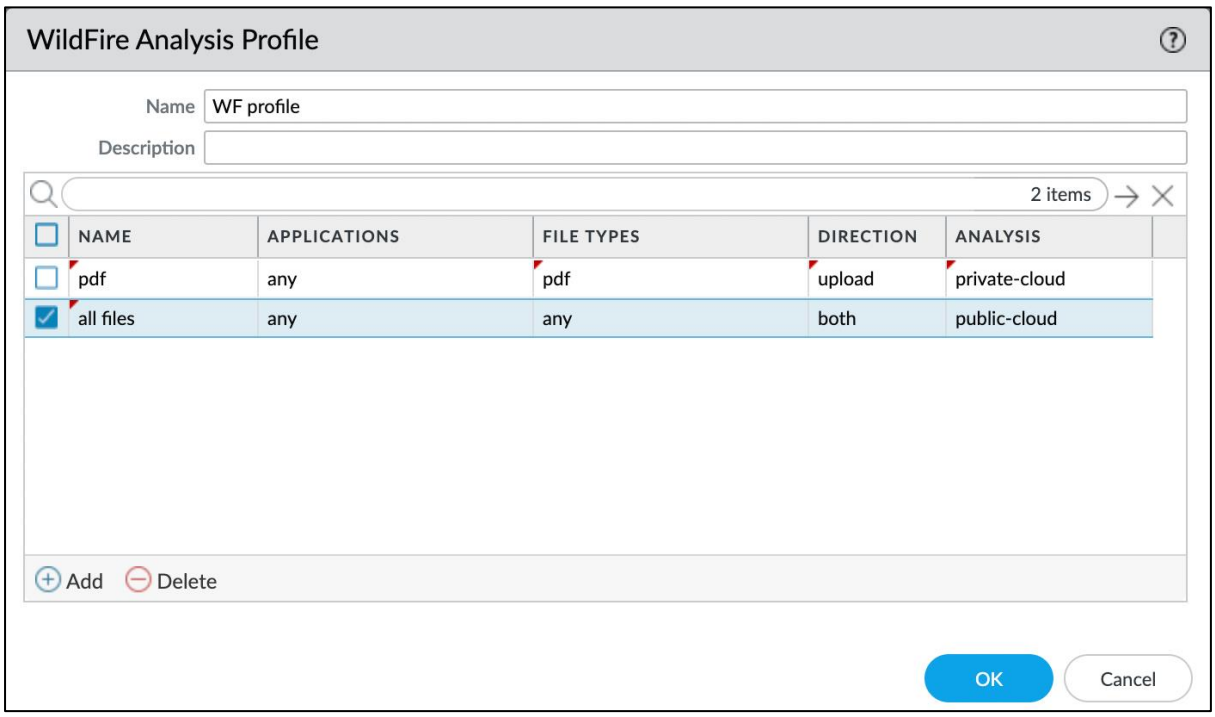

SITE ACCESS
USER CREDENTIAL SUBMISSION
alert
alert
alert
alert
alert
alert
alert
allow
Sort Ascending
Sort Descending
Columns
Set All Actions
Set Selected Actions
Adjust Columns
allow
alert
block
continue
override

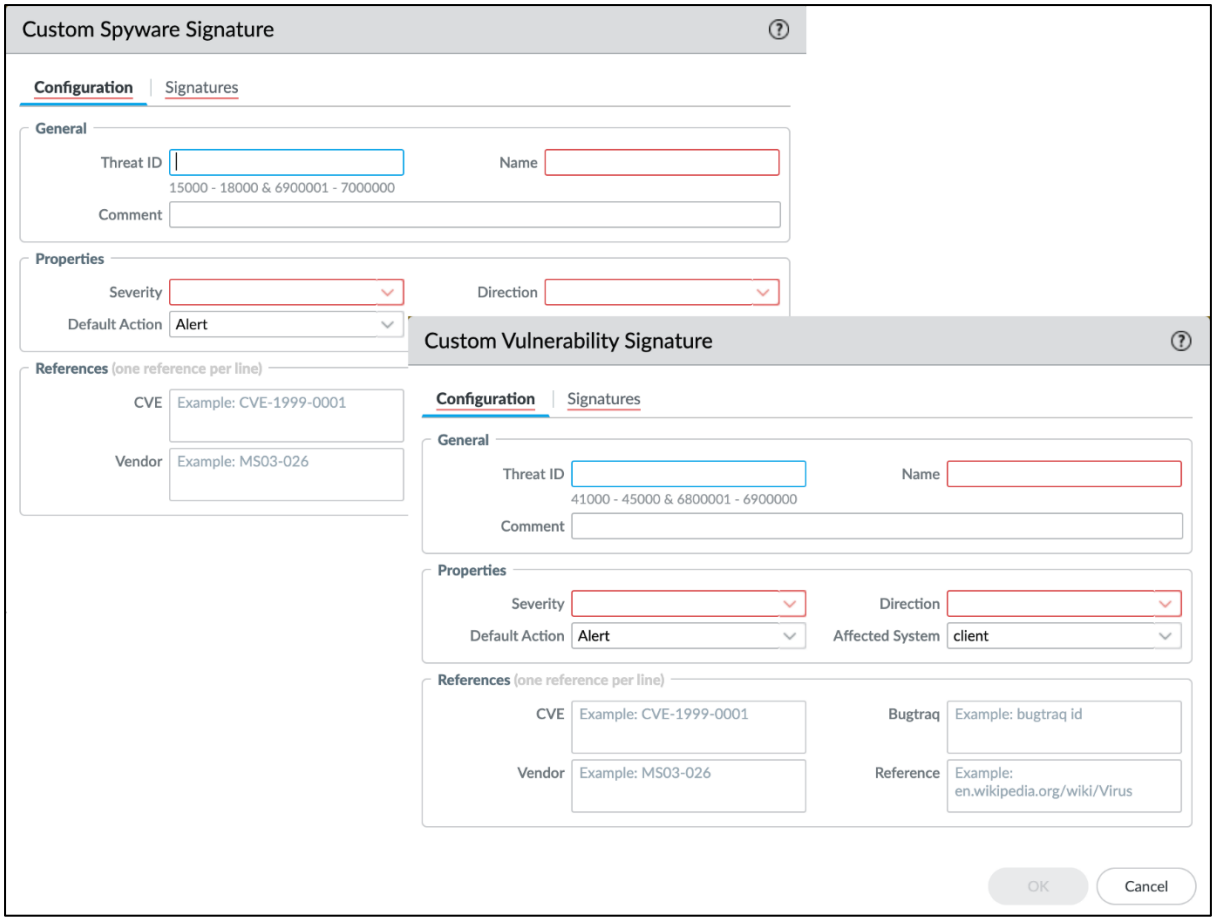

URL Filtering Profile
Name
URL profile
Description
Categories
URL Filtering Settings
User Credential Detection
HTTP Header Insertion
Inline Categorization
Log container page only
Safe Search Enforcement
HTTP Header Logging
User-Agent
Referer
X-Forwarded-For
OK
Cancel

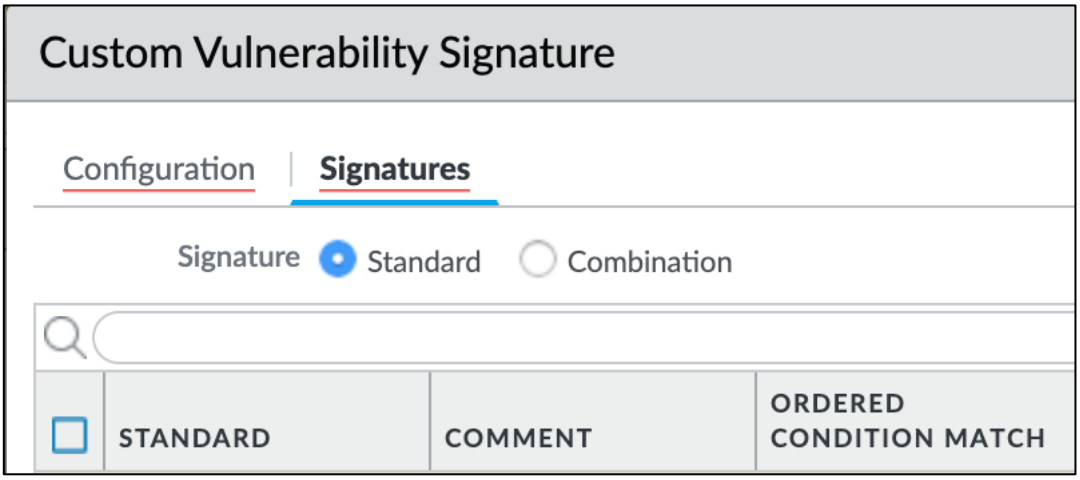

HTTP Header Insertion
Name
GSuite
Type
Google Apps Access Control
Domains
DOMAINS
*.google.com
gmail.com
Add
Delete
Headers
HEADER
VALUE
LOG
X-GooGApps-Allowed-Domains
Add
Delete
OK
Cancel

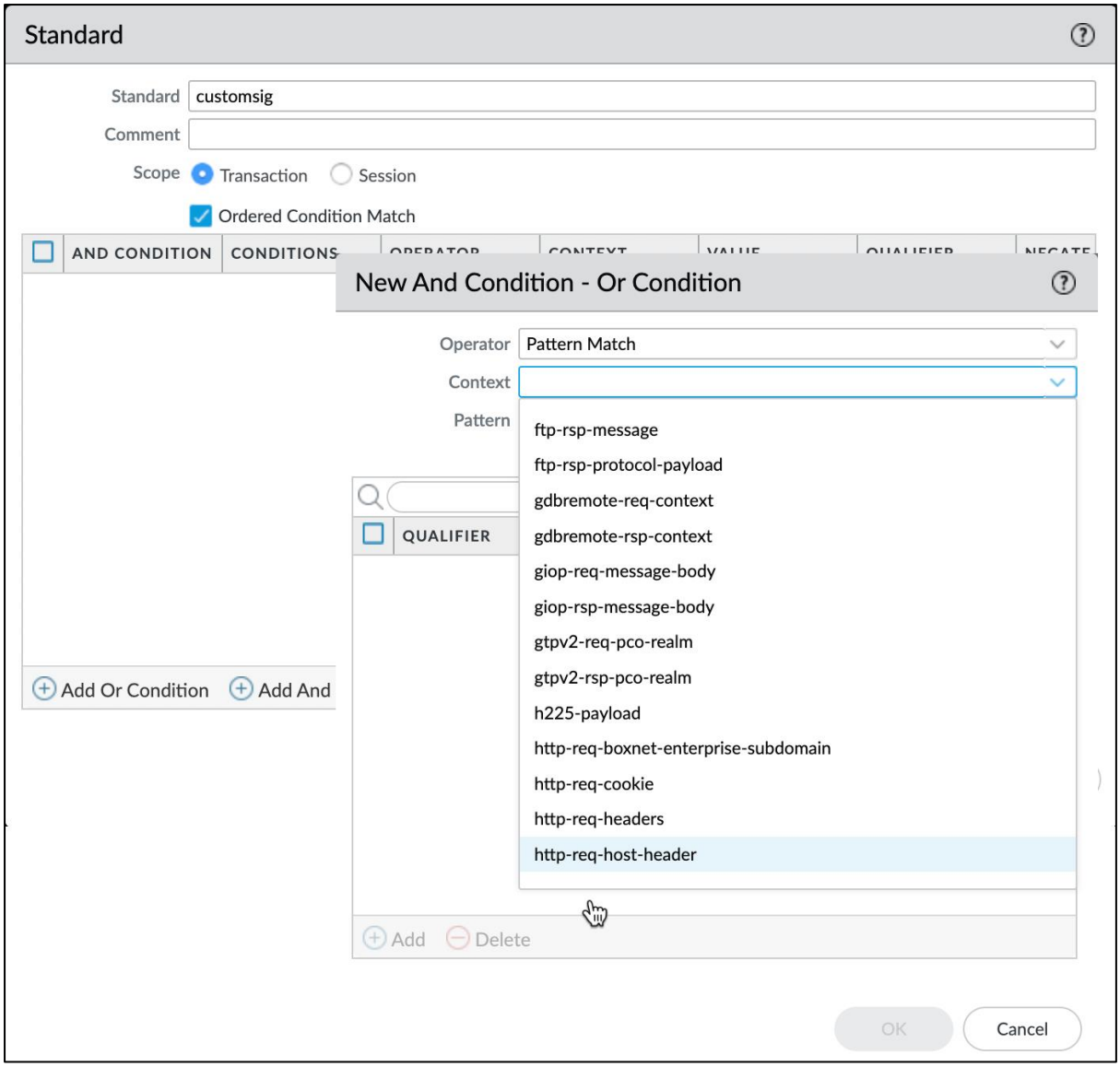

NAME
LOCATION
strict file blocking
Predefined
Add
Delete
Clone
PDF/CSV
04/29/2022 22:00:52 | Session Expire Time: 05/31/2022


DASHBOARD
ACC
MONITOR
POLICIES
WORK
DEVICE
File Blocking Profile
Name
FBprofile
Description
3 items
NAME
APPLICATIONS
FILE T
DIRECTION
ACTION
Block all risky file types
any
both
block
elf
emf
encrypted-7z
encrypted-doc
encrypted-docx
encrypted-office2...
encrypted-pdf
encrypted-ppt
encrypted-pptx
encrypted-rar
encrypted-xls
encrypted-xlsx
encrypted-zip
Add
Delete
Add
Delete
OK
Cancel

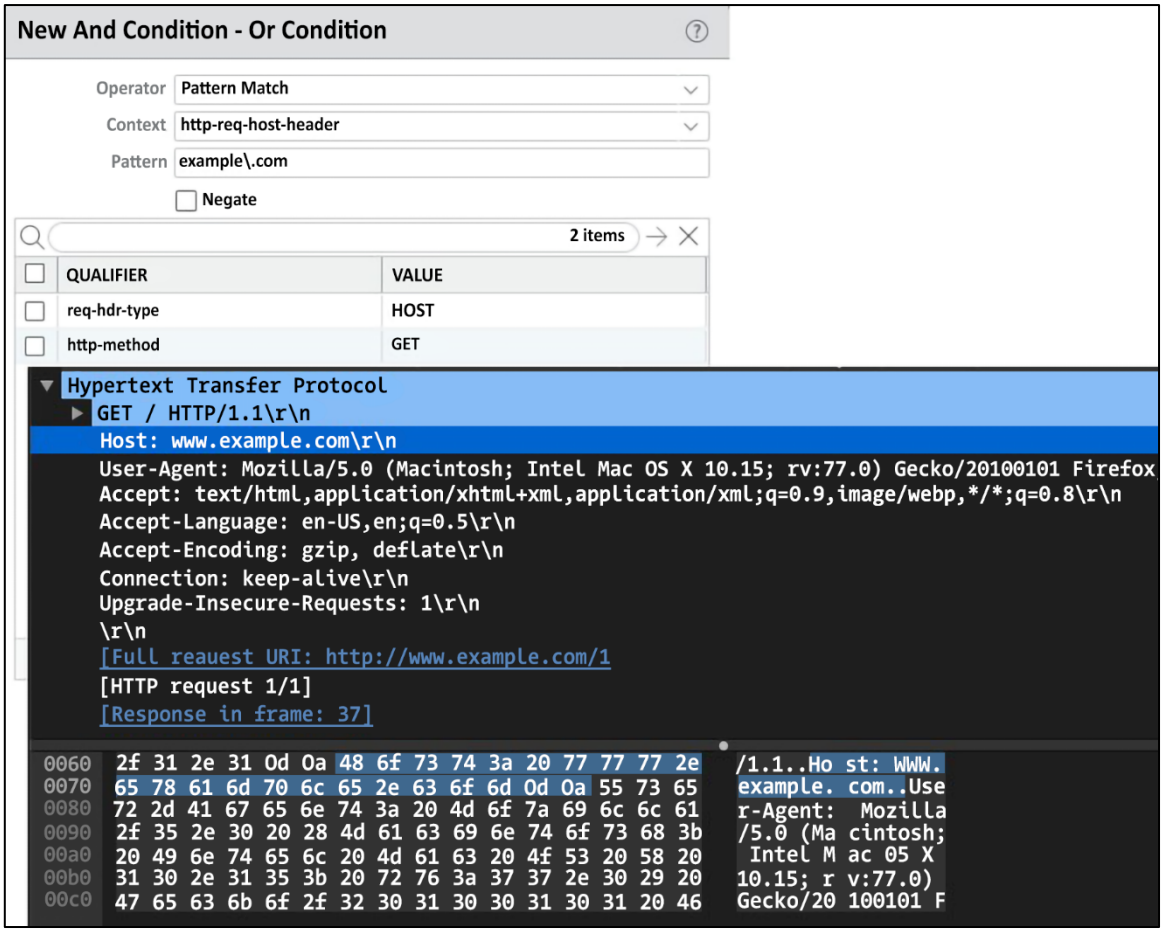

WildFire Analysis Profile
Name
WF profile
Description
2 items
NAME
APPLICATIONS
FILE TYPES
DIRECTION
ANALYSIS
pdf
any
pdf
upload
private-cloud
all files
any
any
both
public-cloud
Add
Delete
OK
Cancel

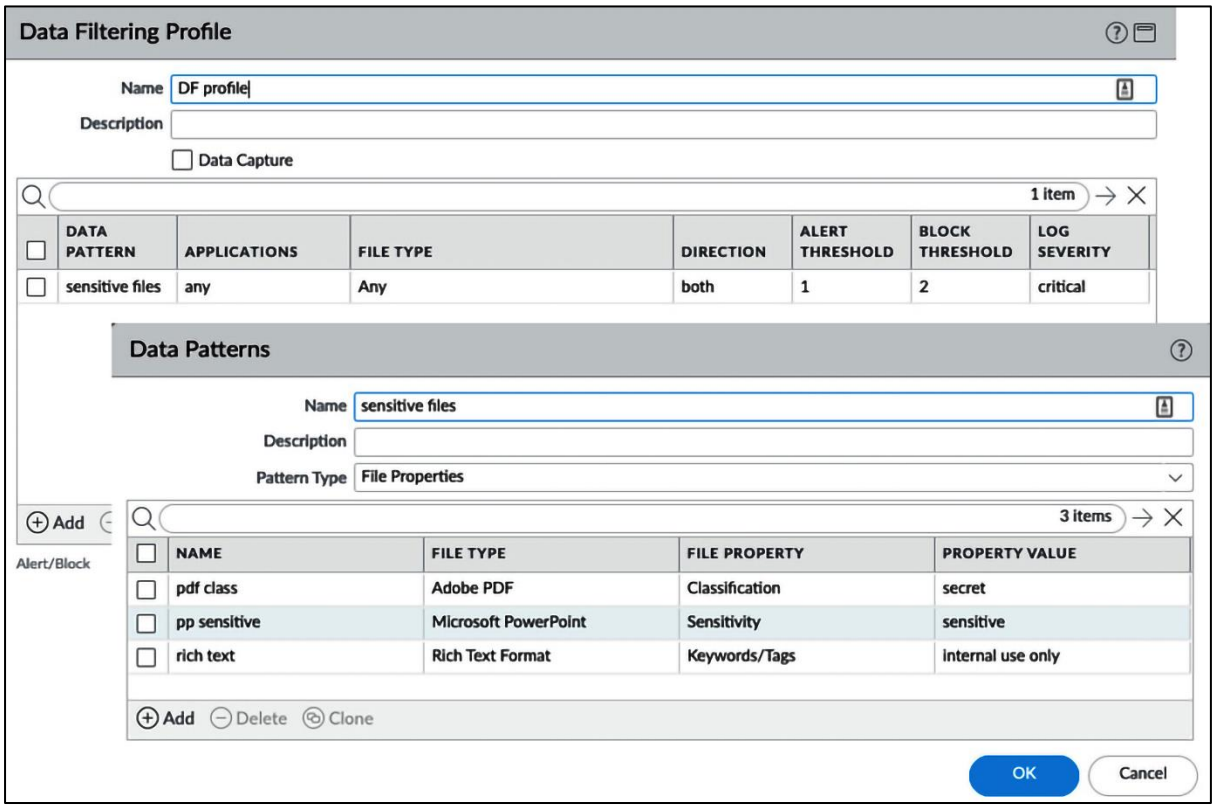

Custom Spyware Signature
Configuration
Signatures
General
Threat ID
15000 - 18000 & 6900001 - 7000000
Name
Comment
Properties
Severity
Direction
Default Action
Alert
References (one reference per line)
CVE
Example: CVE-1999-0001
Vendor
Example: MS03-026
Custom Vulnerability Signature
Configuration
Signatures
General
Threat ID
41000 - 45000 & 6800001 - 6900000
Name
Comment
Properties
Severity
Direction
Default Action
Alert
Affected System
client
References (one reference per line)
CVE
Example: CVE-1999-0001
Bugtraq
Example: bugtraq id
Vendor
Example: MS03-026
Reference
Example: en.wikipedia.org/wiki/Virus
OK
Cancel

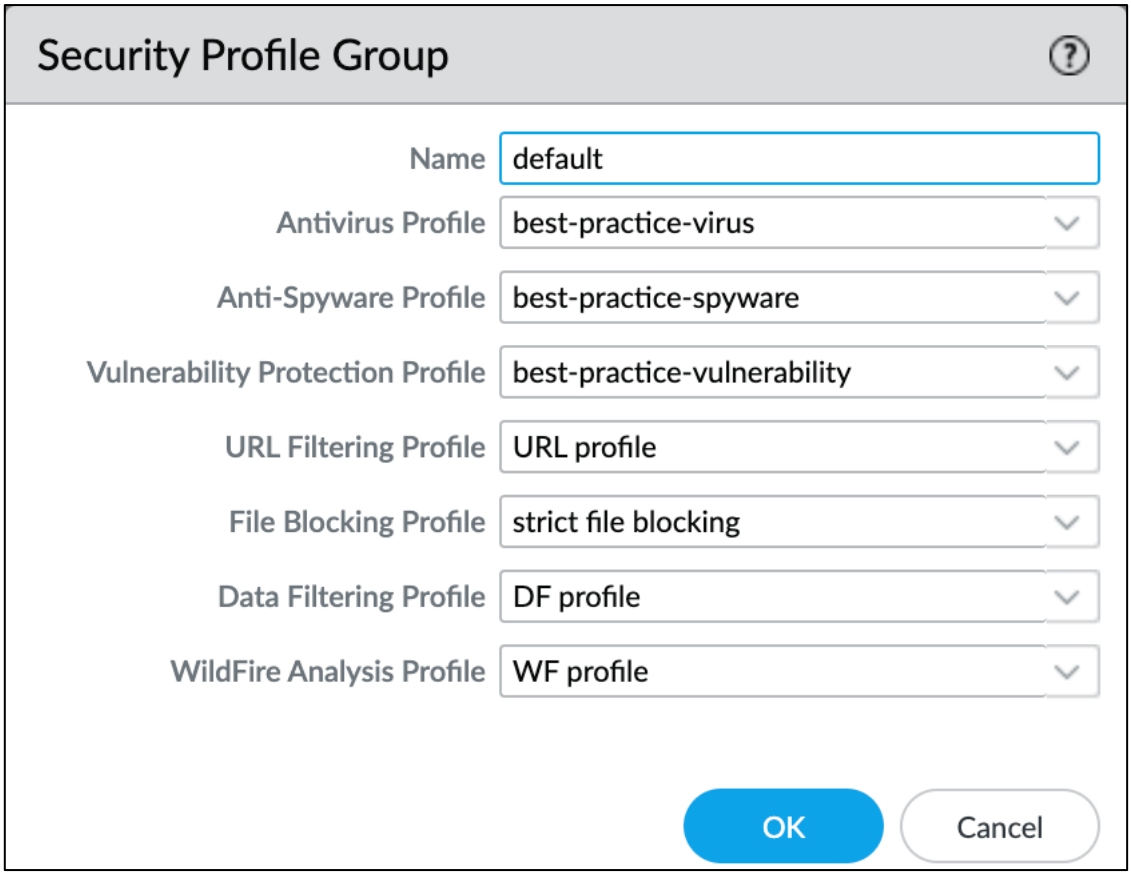

Custom Vulnerability Signature
Configuration
Signatures
Signature
Standard
Combination
STANDARD
COMMENT
ORDERED CONDITION MATCH



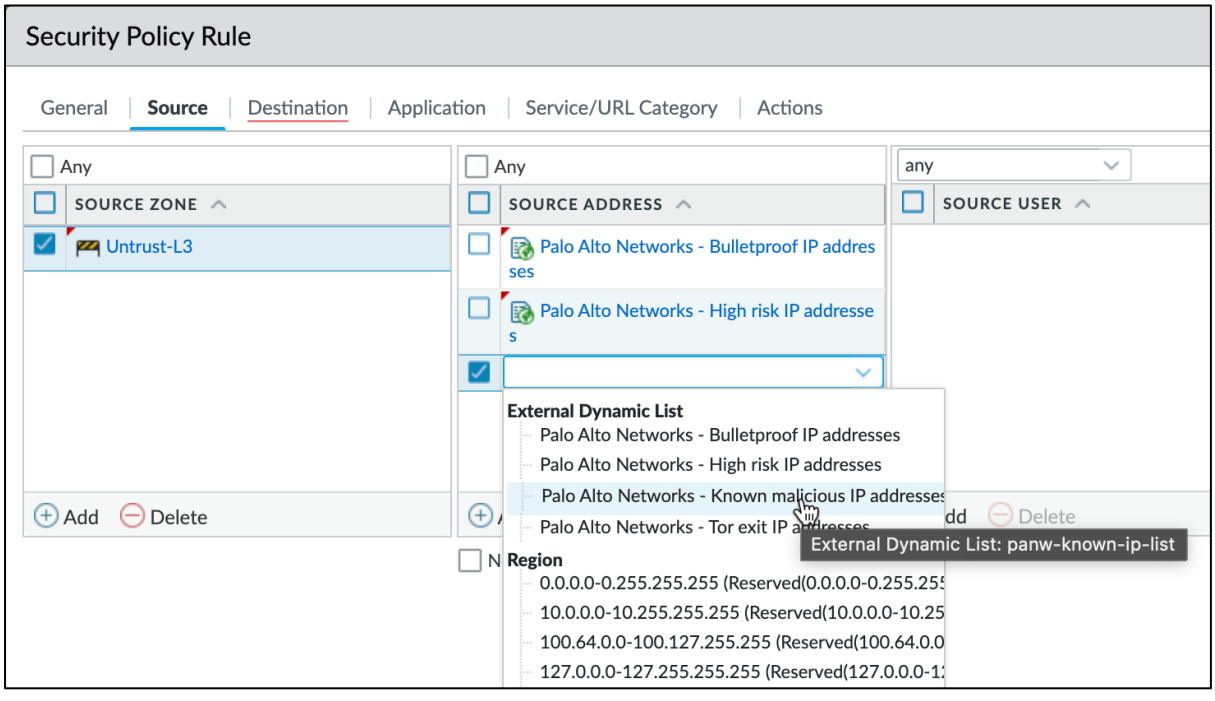
.	1.3	matches a single character (e.g. 123, 133)
?	dots?	matches string with or without last character (e.g. dot, dots)
*	dots*	matches string with or without last character, and multiple repeats of last character (e.g. dot, dots, dotssss)
+	dots+	matches single or multiple repetitions of the preceding letter (e.g. dots, dotssss)
|	((exe)|(msi))	OR function to match multiple possible strings (e.g. dot.exe, dot.msi)
[ ]	x[abc]	matches preceding string followed by any character between squared brackets (e.g. xa, xb, xc)
-	x[a-z]	matches any character in a range (e.g. xa,xm)
^	x[^AB]	matches any character except the ones listed (e.g. xC, x5)
{ }	x{1,3}	matches anything after x as long as it is 1 to 3 bytes in length (e.g. xl, x123)
\	x\.y	Escape character to exactly match a special character (e.g. www\.pangurus\.com)
&amp		used to match & in a string

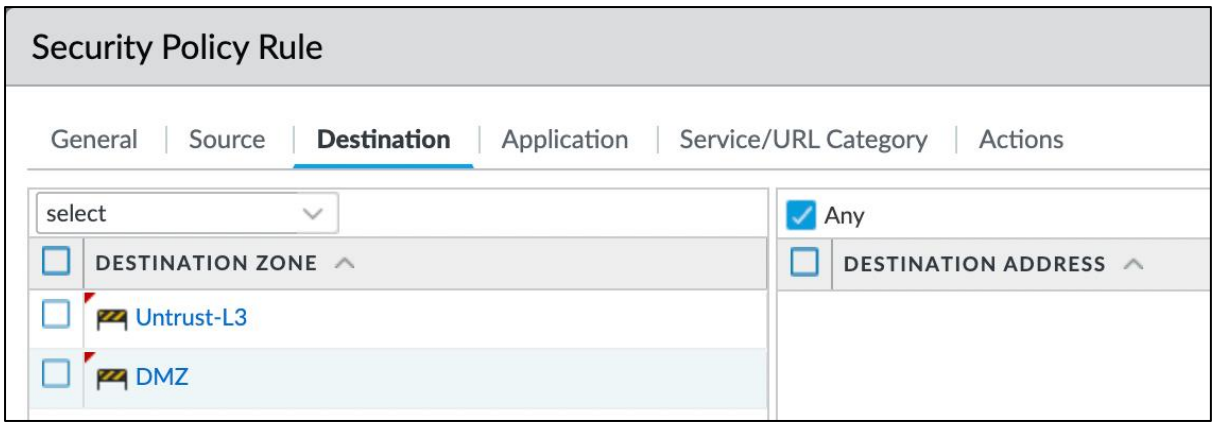

New And Condition - Or Condition
Operator
Pattern Match
Context
http-req-host-header
Pattern
example\.com
Negate
2 items
QUALIFIER
VALUE
req-hdr-type
HOST
http-method
GET
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: www.example.com\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full reauest URI: http://www.example.com/1
[HTTP request 1/1]
[Response in frame: 37]
0060 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: WWW.
0070 65 78 61 6d 70 6c 65 2e 63 6f 6d 0d 0a 55 73 65 example. com..Use
0080 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
0090 2f 35 2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 3b /5.0 (Ma cintosh;
00a0 20 49 6e 74 65 6c 20 4d 61 63 20 4f 53 20 58 20 Intel M ac 05 X
00b0 31 30 2e 31 35 3b 20 72 76 3a 37 37 2e 30 29 20 10.15; r v:77.0)
00c0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F

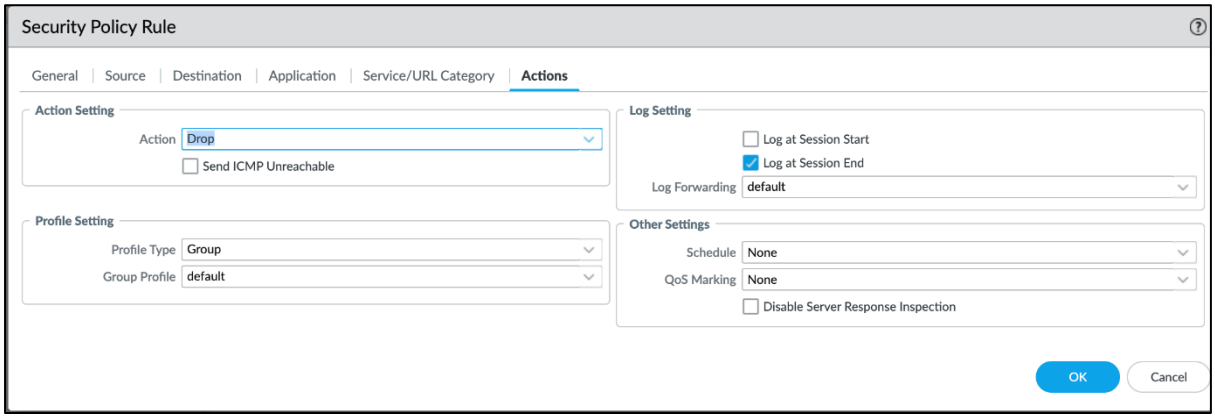

Data Filtering Profile
Name
DF profile
Description
Data Capture
1 item
DATA PATTERN
APPLICATIONS
FILE TYPE
DIRECTION
ALERT THRESHOLD
BLOCK THRESHOLD
LOG SEVERITY
sensitive files
any
Any
both
1
2
critical
Data Patterns
Name
sensitive files
Description
Pattern Type
File Properties
Add
Alert/Block
3 items
NAME
FILE TYPE
FILE PROPERTY
PROPERTY VALUE
pdf class
Adobe PDF
Classification
secret
pp sensitive
Microsoft PowerPoint
Sensitivity
sensitive
rich text
Rich Text Format
Keywords/Tags
internal use only
Add
Delete
Clone
OK
Cancel

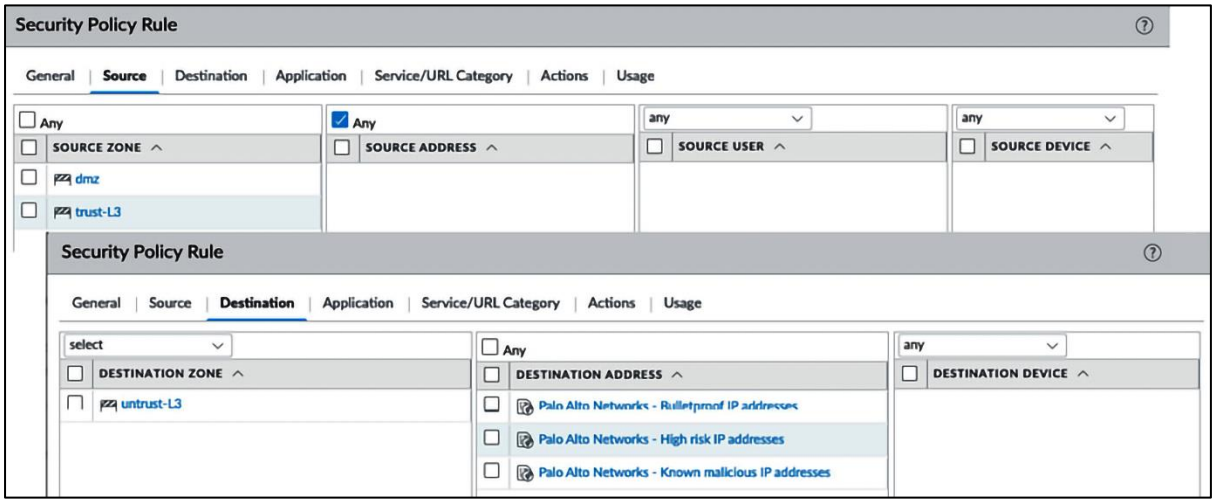


	NAME	TYPE	Source		Destination		APPLICATIO...	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	ZONE	ADDRESS					
1	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow	none	none
2	interzone-default	interzone	any	any	any	any	any	any	Deny	none	none

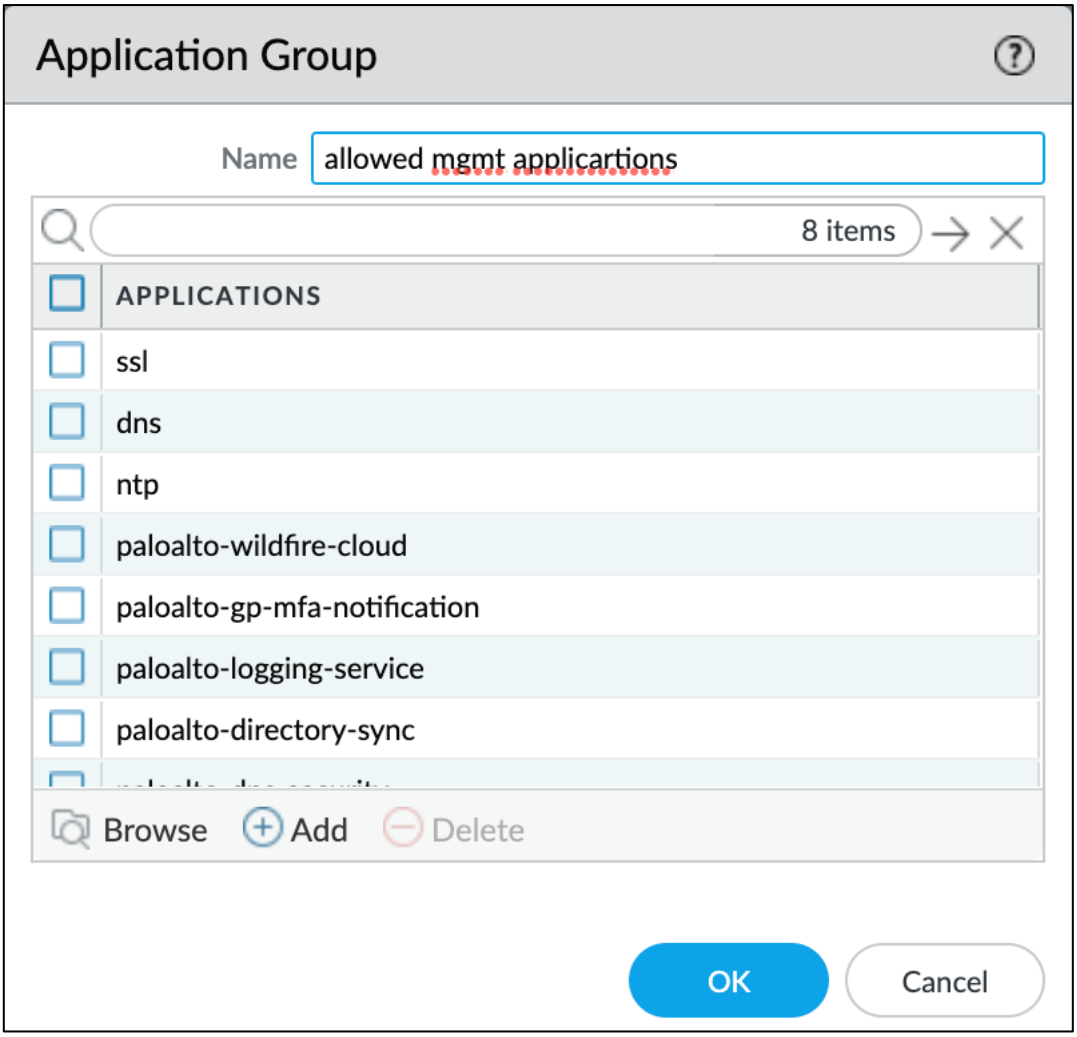


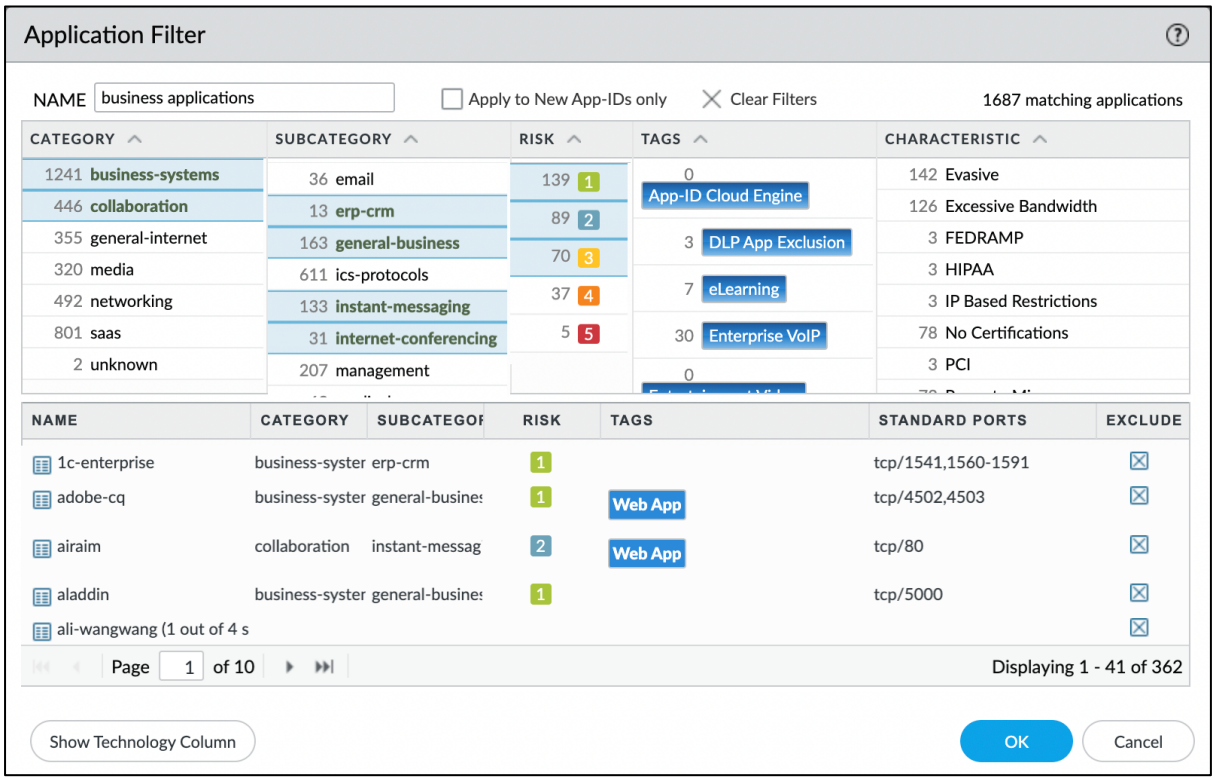


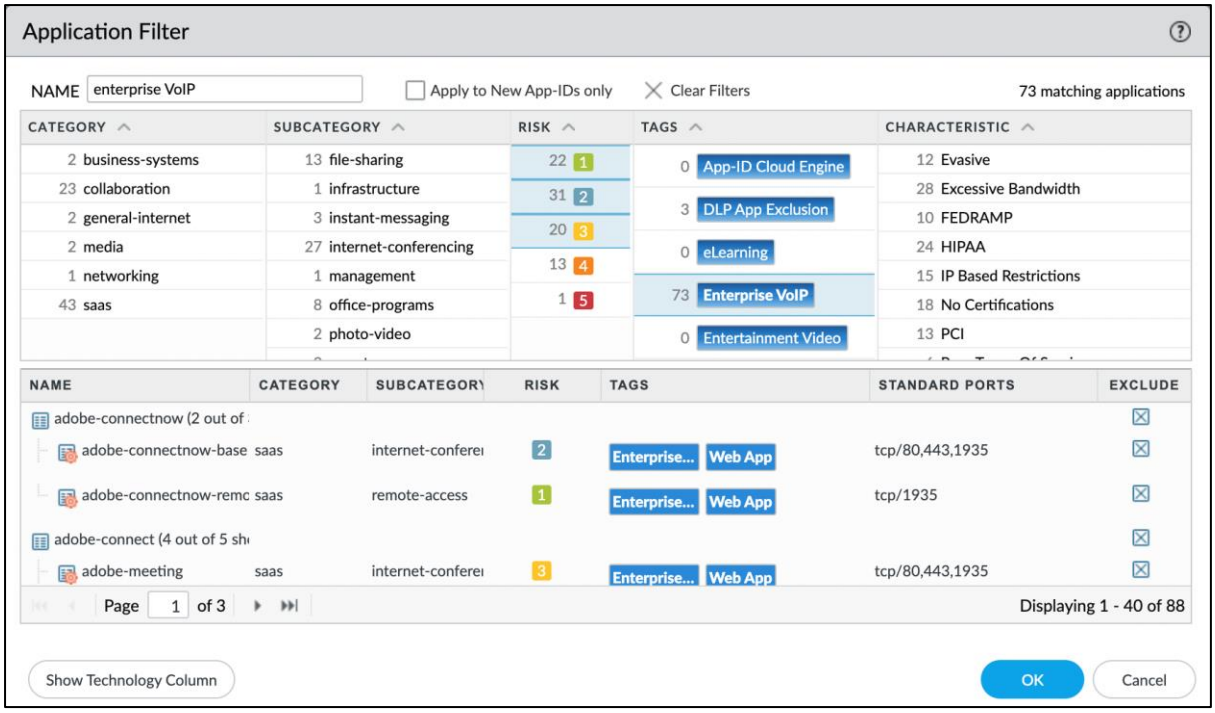


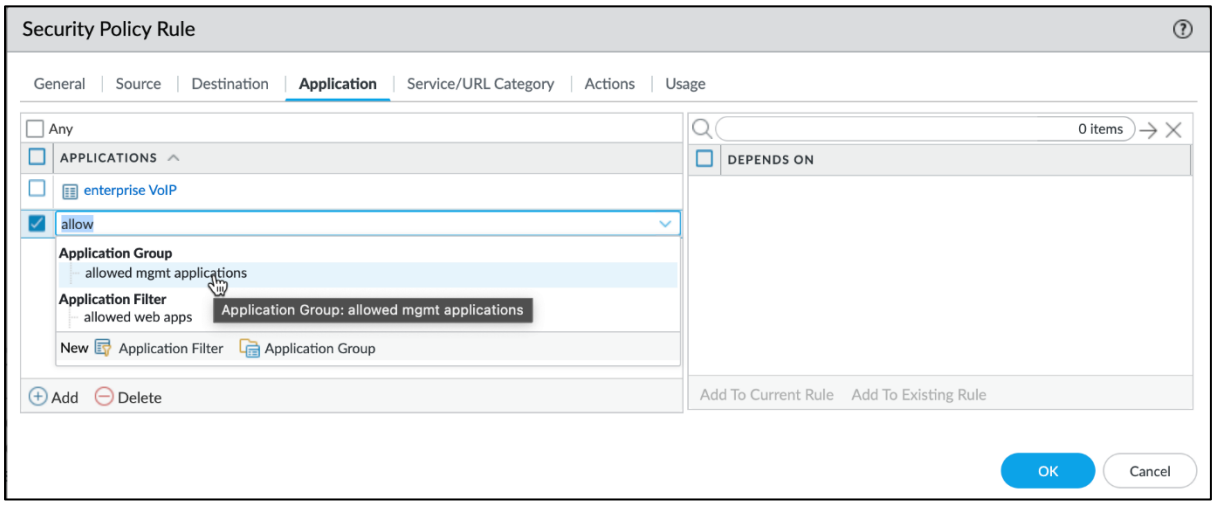


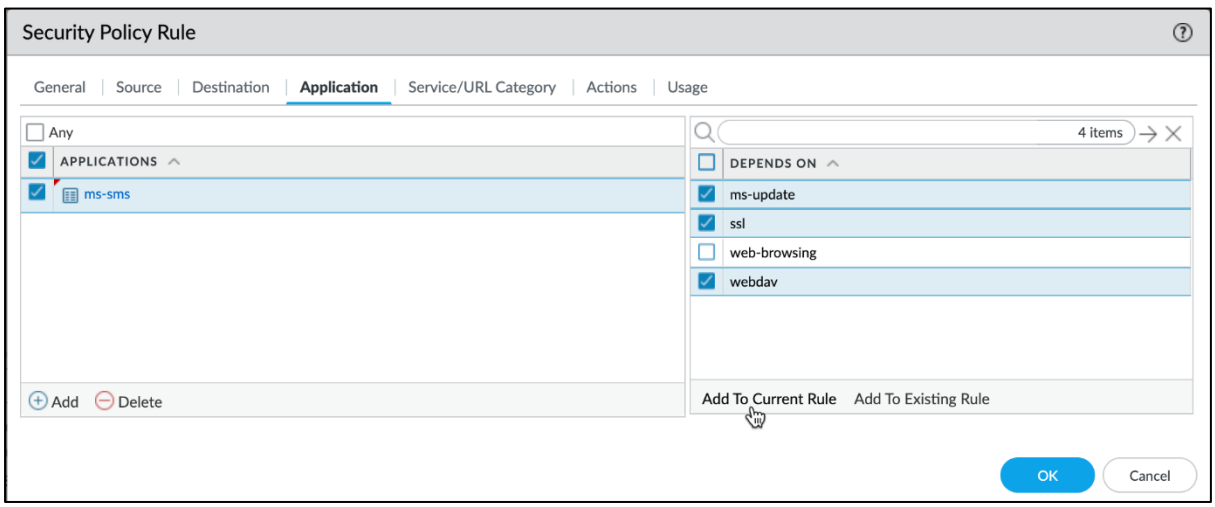
	NAME	TYPE	Source		Destination		APPLICATIO...	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	ZONE	ADDRESS					
1	catchall	universal	untrust	any	any	any	any	application-default	Allow		
2	catchall-any	universal	untrust	any	any	any	any	any	Allow		
3	catchall-DMZ	universal	DMZ	any	any	any	any	any	Allow		
4	intrazone-defa...	intrazone	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-defa...	interzone	any	any	any	any	any	any	Deny	none	none

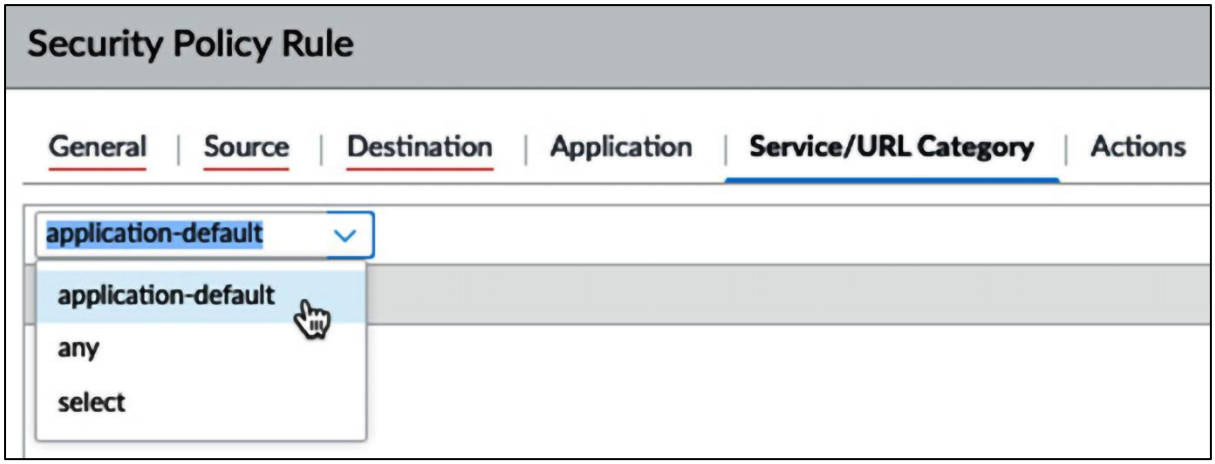

Application Group
Name
allowed mgmt applicartions
8 items
APPLICATIONS
ssl
dns
ntp
paloalto-wildfire-cloud
paloalto-gp-mfa-notification
paloalto-logging-service
paloalto-directory-sync
Browse
Add
Delete
OK
Cancel

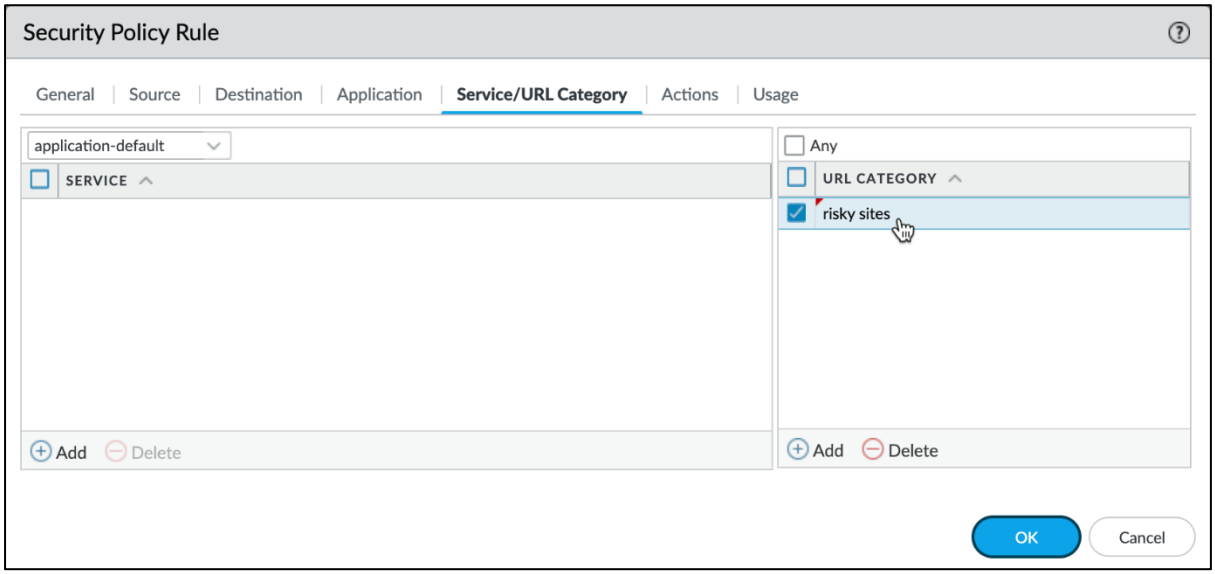

Application Filter
NAME
business applications
Apply to New App-IDs only
Clear Filters
1687 matching applications
CATEGORY
SUBCATEGORY
RISK
TAGS
CHARACTERISTIC
1241 business-systems
446 collaboration
355 general-internet
320 media
492 networking
801 saas
2 unknown
36 email
13 erp-crm
163 general-business
611 ics-protocols
133 instant-messaging
31 internet-conferencing
207 management
139 1
89 2
70 3
37 4
5 5
0
App-ID Cloud Engine
3 DLP App Exclusion
7 eLearning
30 Enterprise VoIP
0
142 Evasive
126 Excessive Bandwidth
3 FEDRAMP
3 HIPAA
3 IP Based Restrictions
78 No Certifications
3 PCI
NAME
CATEGORY
SUBCATEGOI
RISK
TAGS
STANDARD PORTS
EXCLUDE
1c-enterprise
business-syster
erp-crm
1
tcp/1541,1560-1591
adobe-cq
business-syster
general-busines
1
Web App
tcp/4502,4503
airaim
collaboration
instant-messag
2
Web App
tcp/80
aladdin
business-syster
general-busines
1
tcp/5000
ali-wangwang (1 out of 4 s
Page
1
of 10
Displaying 1 - 41 of 362
Show Technology Column
OK
Cancel

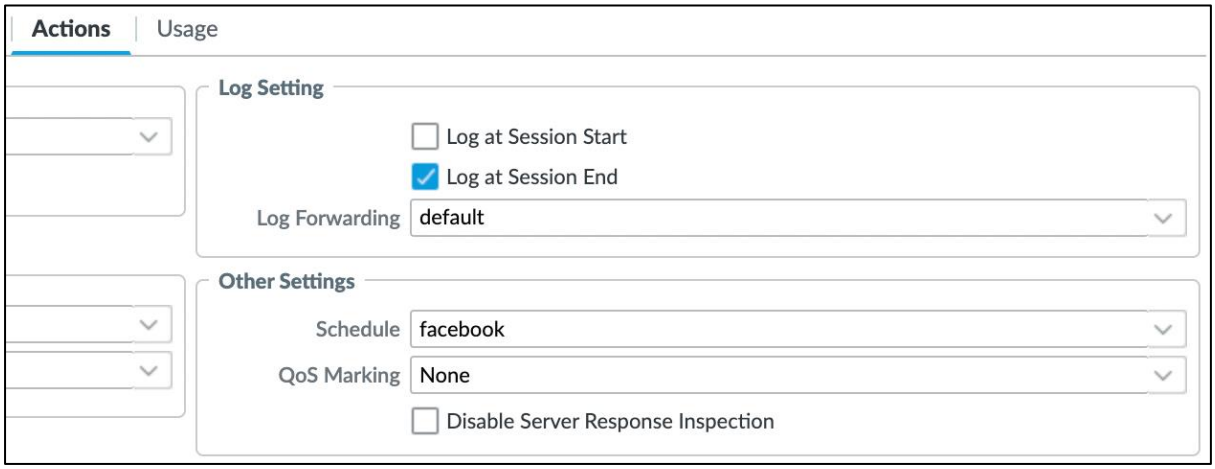

Application Filter
NAME enterprise VoIP
Apply to New App-IDs only
Clear Filters
73 matching applications
CATEGORY
SUBCATEGORY
RISK
TAGS
CHARACTERISTIC
2 business-systems
23 collaboration
2 general-internet
2 media
1 networking
43 saas
13 file-sharing
1 infrastructure
3 instant-messaging
27 internet-conferencing
1 management
8 office-programs
2 photo-video
22 1
31 2
20 3
13 4
1 5
0 App-ID Cloud Engine
3 DLP App Exclusion
0 eLearning
73 Enterprise VoIP
0 Entertainment Video
12 Evasive
28 Excessive Bandwidth
10 FEDRAMP
24 HIPAA
15 IP Based Restrictions
18 No Certifications
13 PCI
NAME
CATEGORY
SUBCATEGORY
RISK
TAGS
STANDARD PORTS
EXCLUDE
adobe-connectnow (2 out of
adobe-connectnow-base saas internet-confere 2 Enterprise... Web App tcp/80,443,1935
adobe-connectnow-remc saas remote-access 1 Enterprise... Web App tcp/1935
adobe-connect (4 out of 5 sh
adobe-meeting saas internet-confere 3 Enterprise... Web App tcp/80,443,1935
Page 1 of 3
Displaying 1 - 40 of 88
Show Technology Column
OK
Cancel

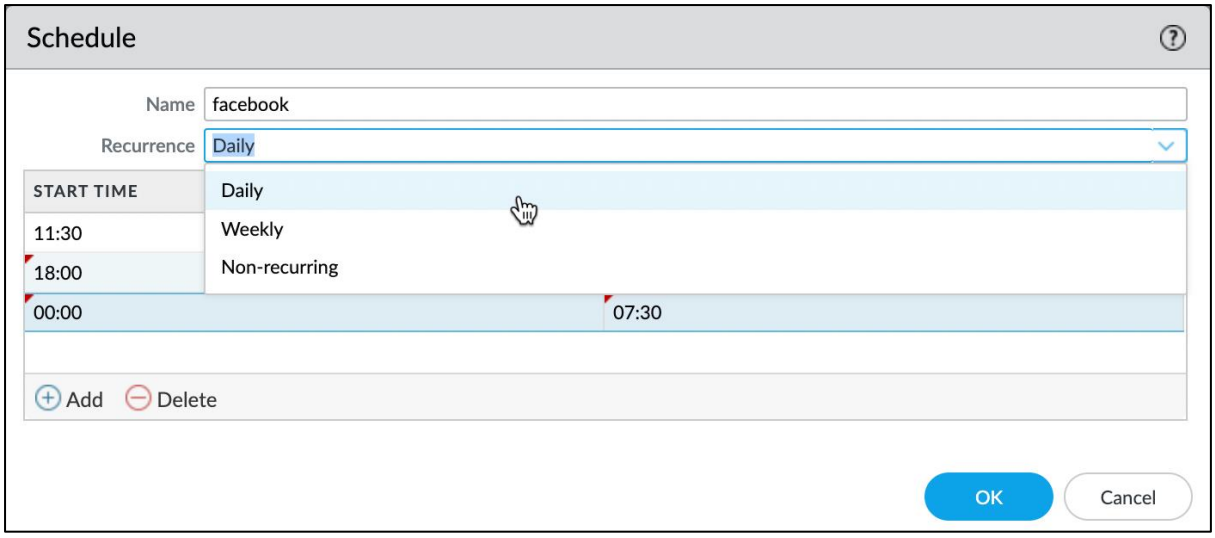

Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Usage
Any
APPLICATIONS
enterprise VoIP
allow
Application Group
allowed mgmt applications
Application Filter
allowed web apps
Application Group: allowed mgmt applications
New Application Filter
Application Group
Add
Delete
0 items
DEPENDS ON
Add To Current Rule
Add To Existing Rule
OK
Cancel

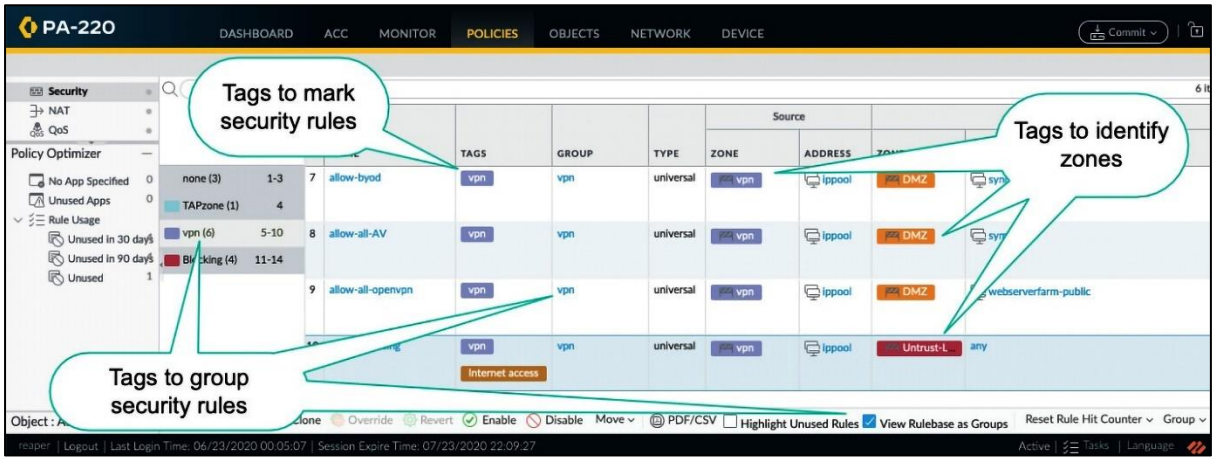

Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Usage
Any
APPLICATIONS
ms-sms
Add
Delete
4 items
DEPENDS ON
ms-update
ssl
web-browsing
webdav
Add To Current Rule
Add To Existing Rule
OK
Cancel

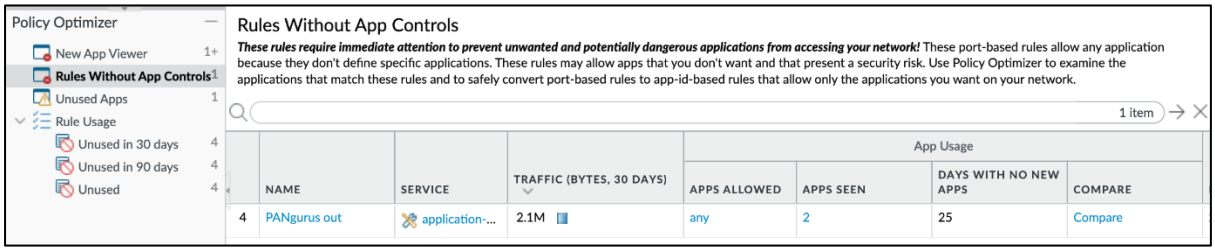

Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
application-default
application-default
any
select

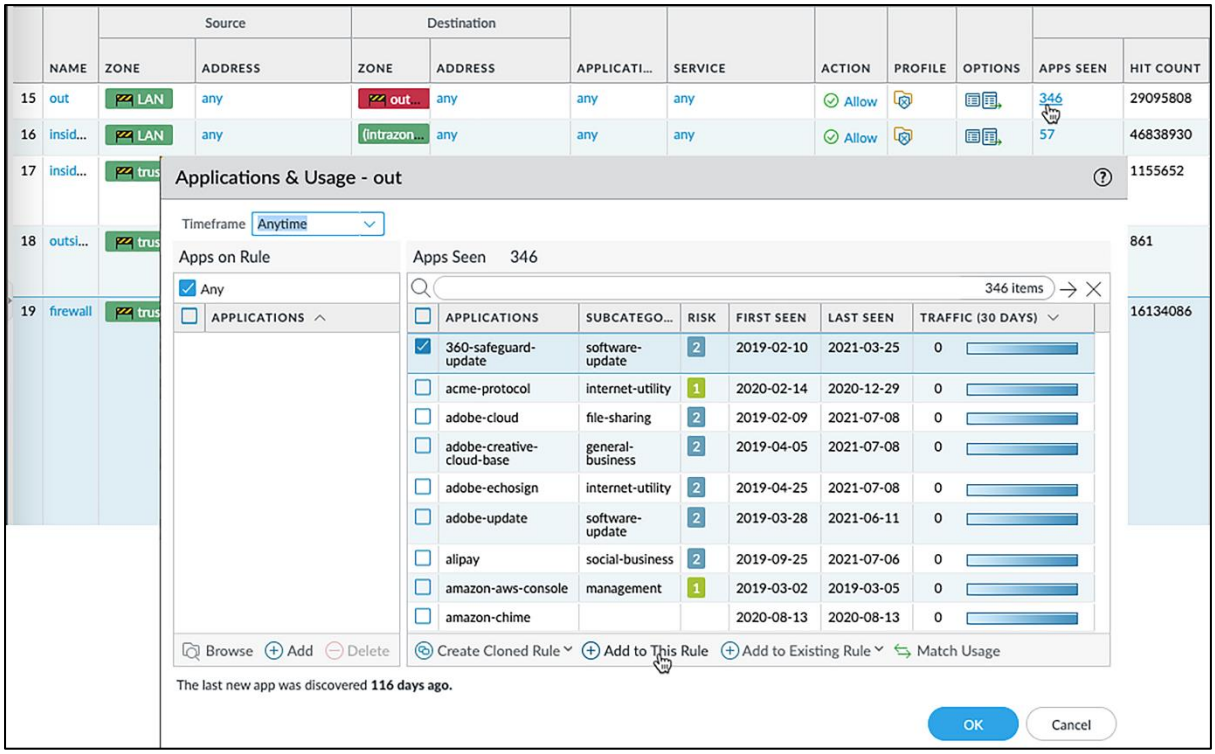

Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Usage
application-default
SERVICE
Any
URL CATEGORY
risky sites
Add
Delete
Add
Delete
OK
Cancel


Actions
Usage
Log Setting
Log at Session Start
Log at Session End
Log Forwarding
default
Other Settings
Schedule
facebook
QoS Marking
None
Disable Server Response Inspection

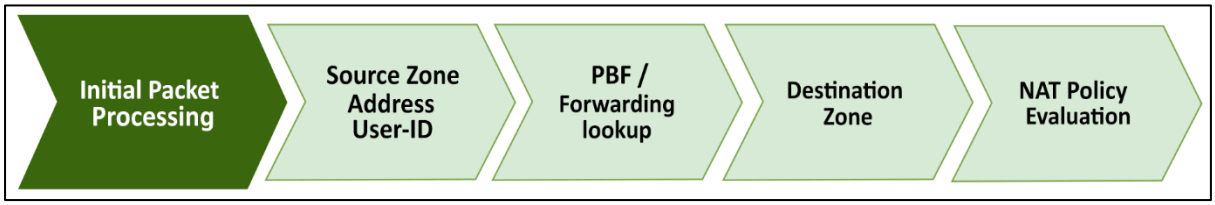

Schedule
Name
facebook
Recurrence
Daily
START TIME
Daily
Weekly
Non-recurring
11:30
18:00
00:00
07:30
Add
Delete
OK
Cancel

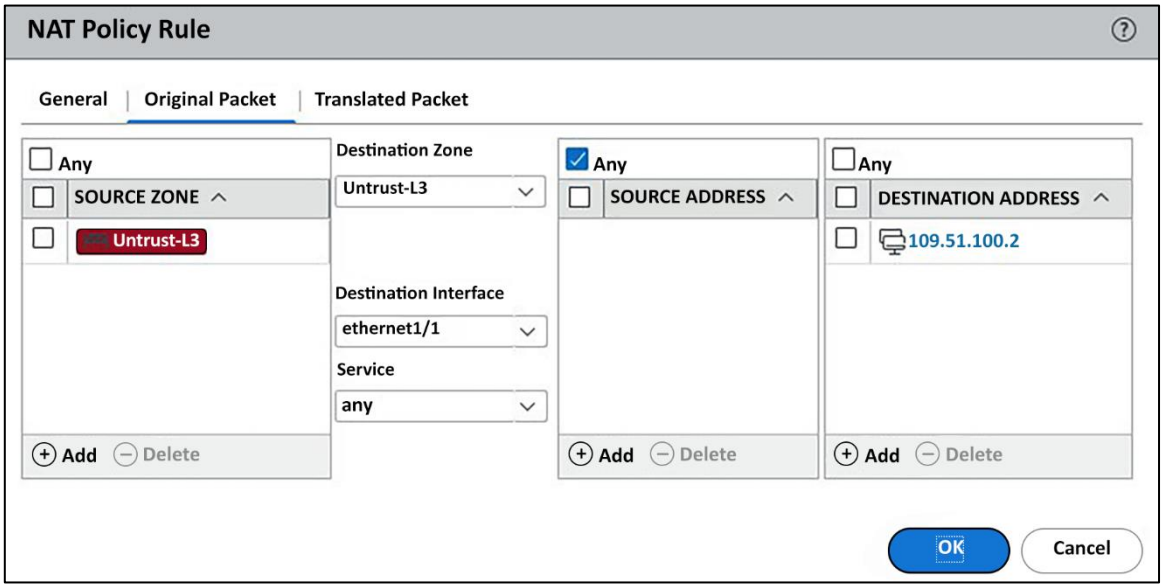

PA-220
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Optimizer
No App Specified
Unused Apps
Rule Usage
Unused in 30 days
Unused in 90 days
Unused
Tags to mark security rules
Tags to identify zones
Tags to group security rules
TAGS
GROUP
TYPE
Source
ZONE
ADDRESS
allow-byod
allow-all-AV
allow-all-openvpn
webserverfarm-public
Internet access
Untrust-L
any
Override
Revert
Enable
Disable
Move
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
Group

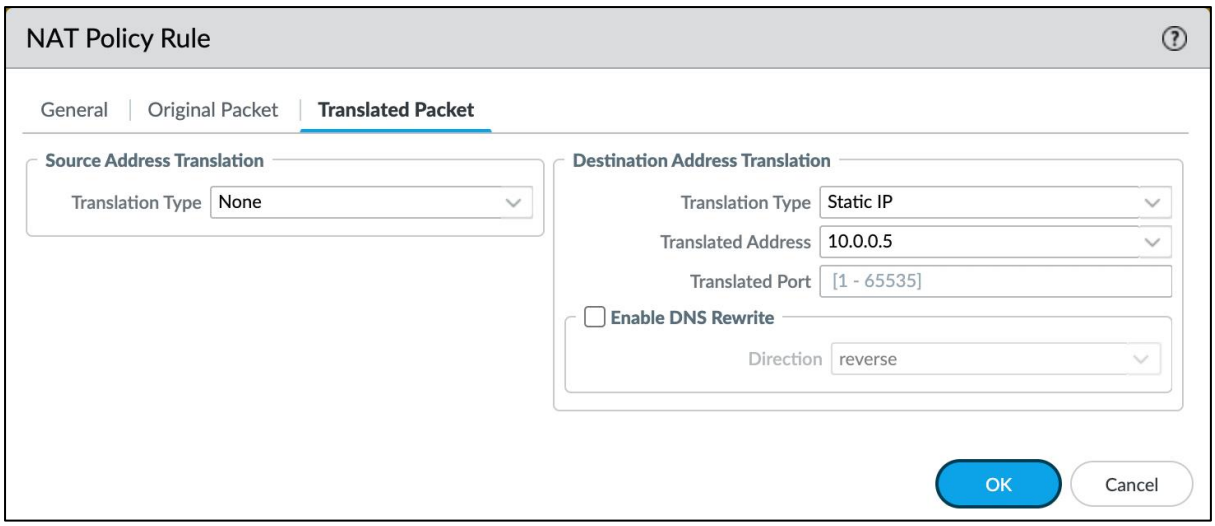

Policy Optimizer
New App Viewer
Rules Without App Controls
Unused Apps
Rule Usage
Unused in 30 days
Unused in 90 days
Unused
Rules Without App Controls
These rules require immediate attention to prevent unwanted and potentially dangerous applications from accessing your network! These port-based rules allow any application because they don't define specific applications. These rules may allow apps that you don't want and that present a security risk. Use Policy Optimizer to examine the applications that match these rules and to safely convert port-based rules to app-id-based rules that allow only the applications you want on your network.
1 item
NAME
SERVICE
TRAFFIC (BYTES, 30 DAYS)
App Usage
APPS ALLOWED
APPS SEEN
DAYS WITH NO NEW APPS
COMPARE
4
PANgurus out
application-...
2.1M
any
2
25
Compare

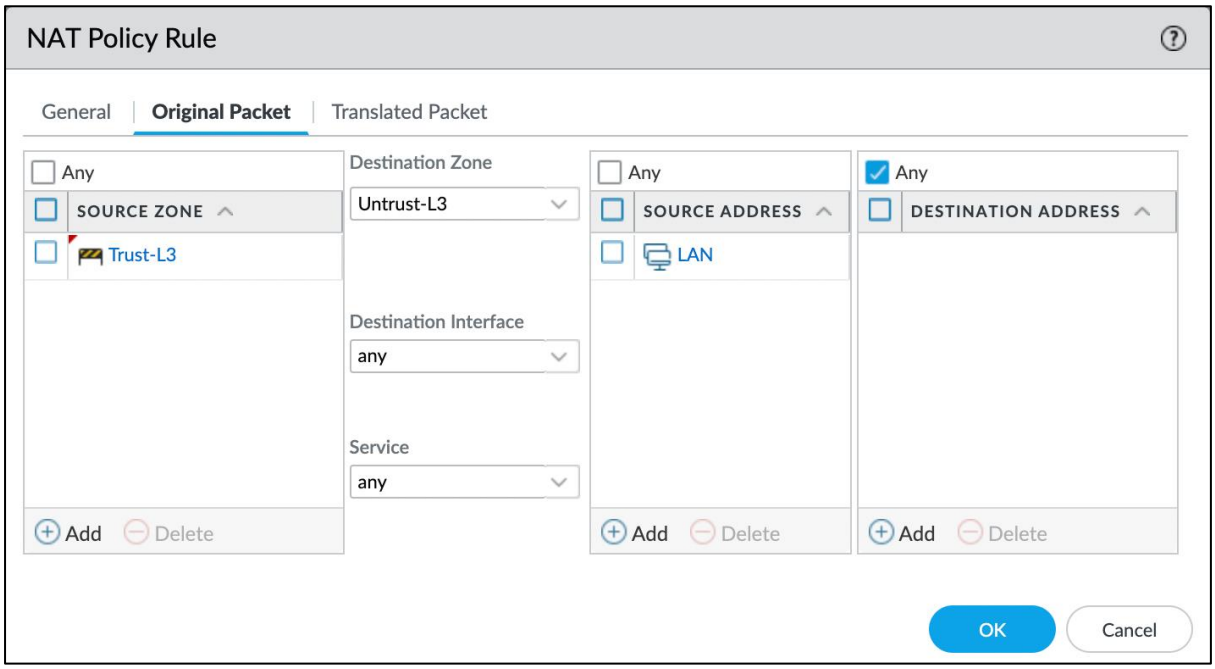


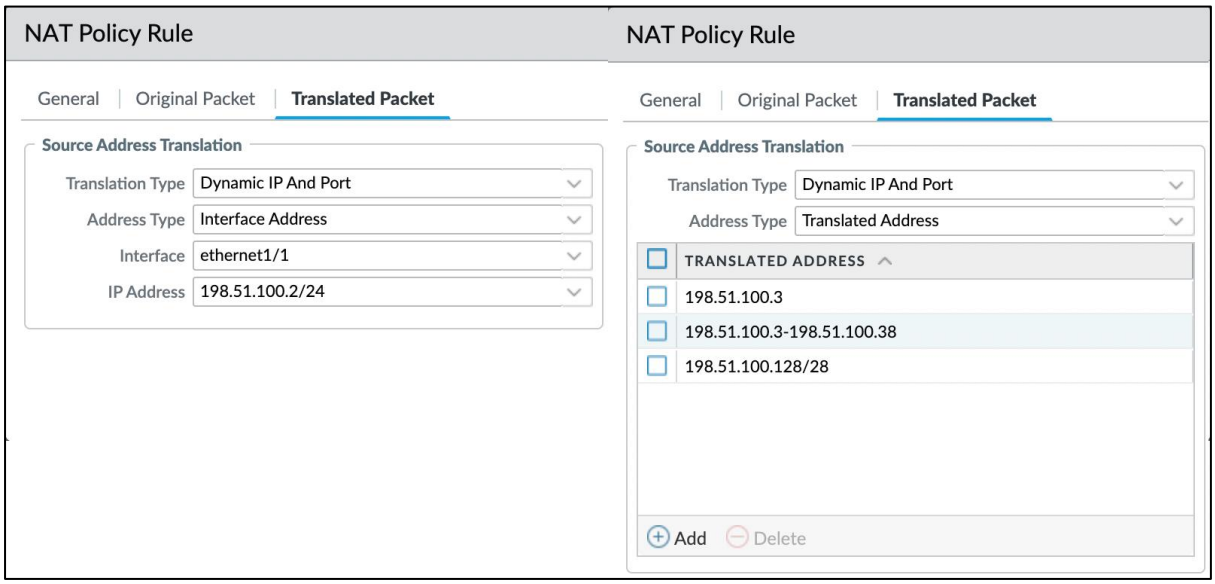
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE
ethernet1/1	Layer3			198.51.100.2/24	default	Untrust-L3
ethernet1/2	Layer3			192.168.27.1/24	default	Trust-L3
ethernet1/3	Layer3			10.0.0.1/24	default	DMZ-L3

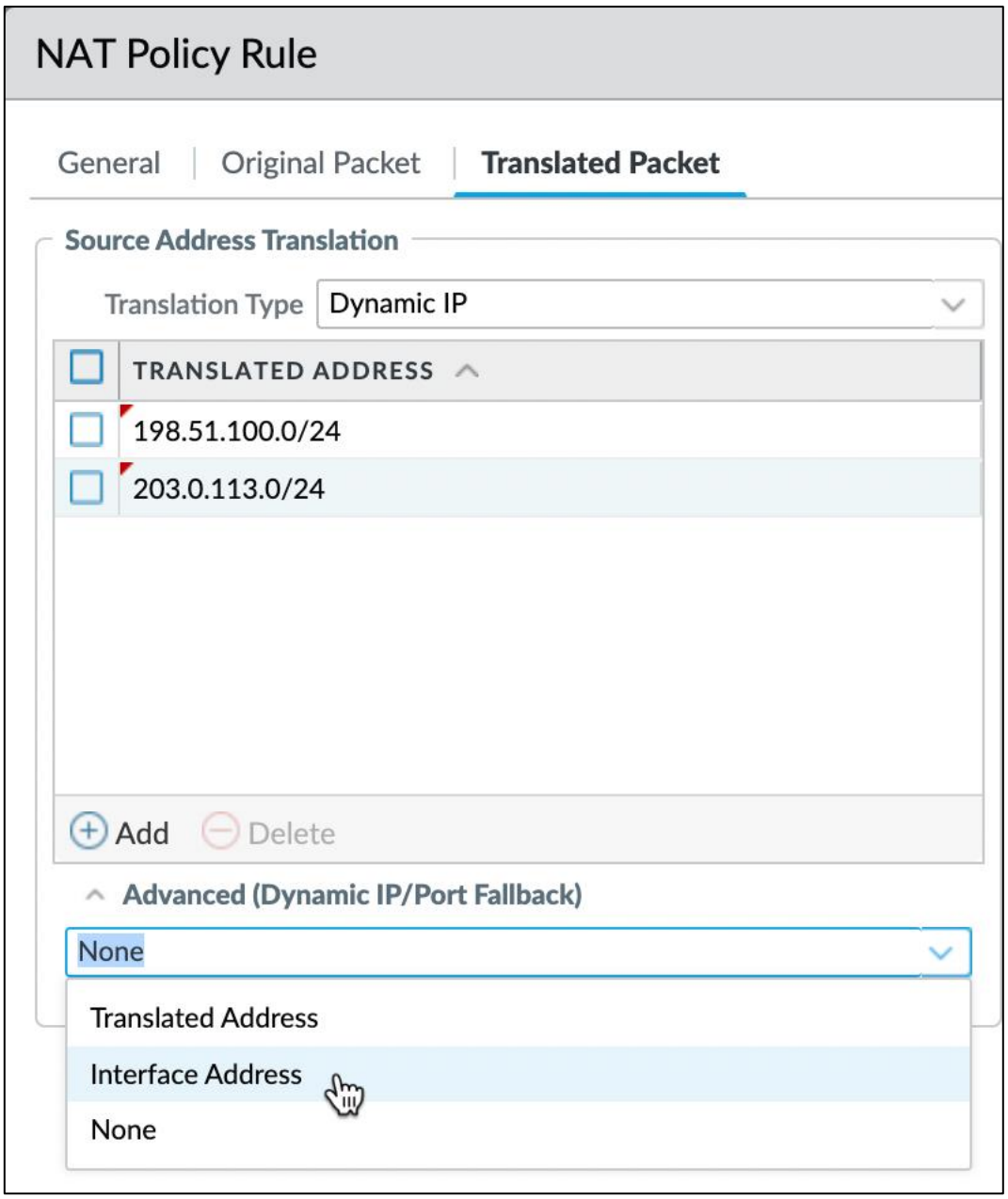


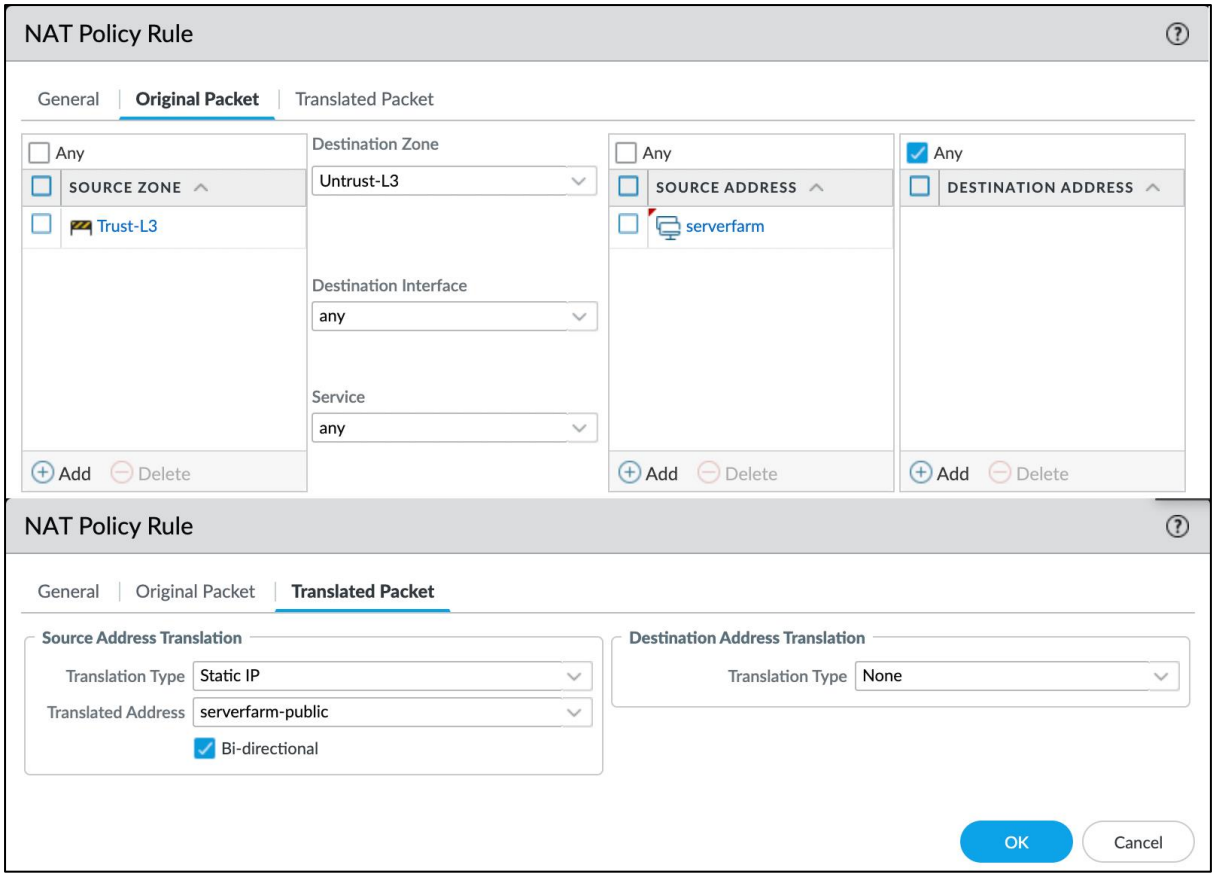


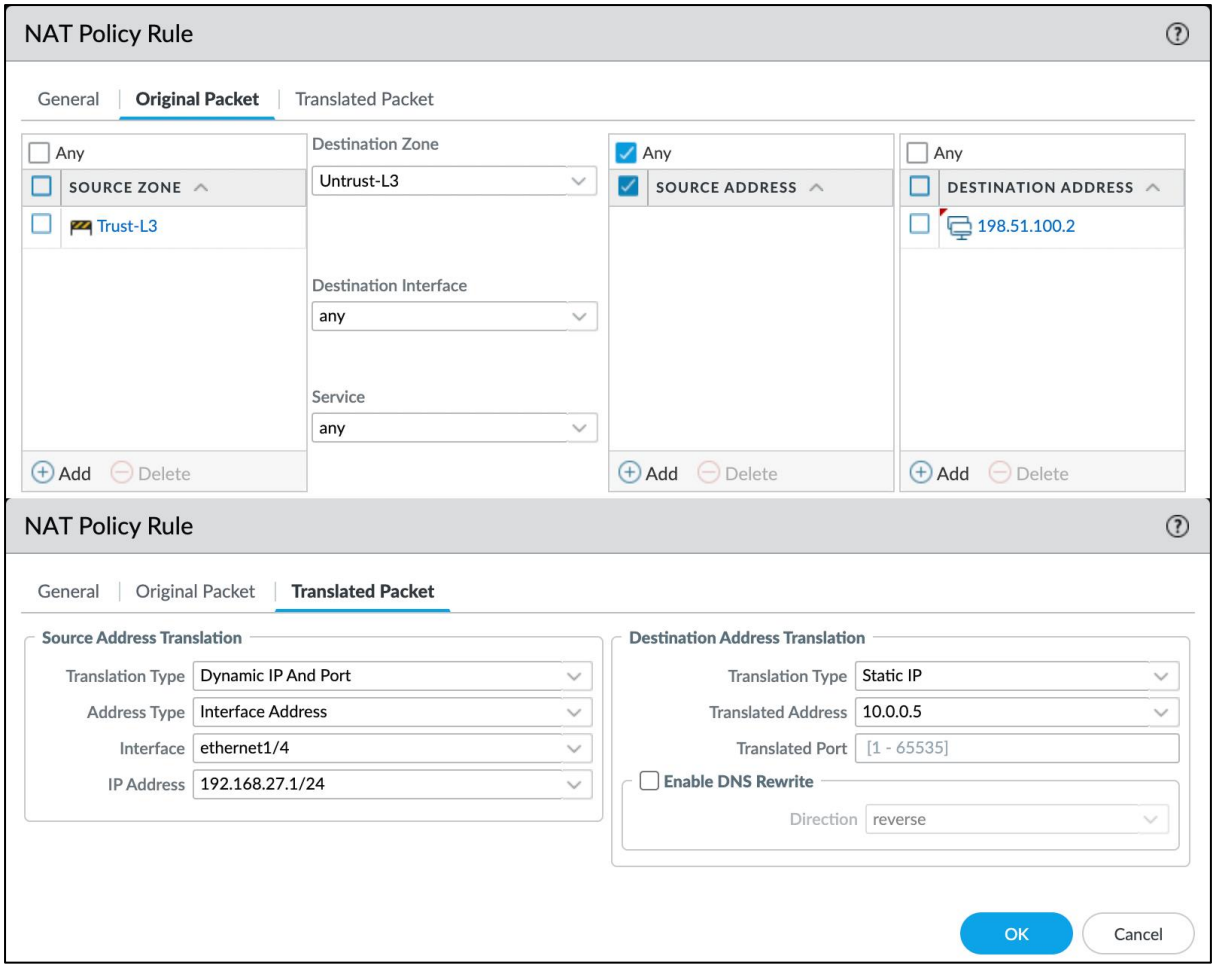

NAT Policy Rule
General
Original Packet
Translated Packet
Source Address Translation
Translation Type
None
Destination Address Translation
Translation Type
Static IP
Translated Address
10.0.0.5
Translated Port
[1 - 65535]
Enable DNS Rewrite
Direction
reverse
OK
Cancel

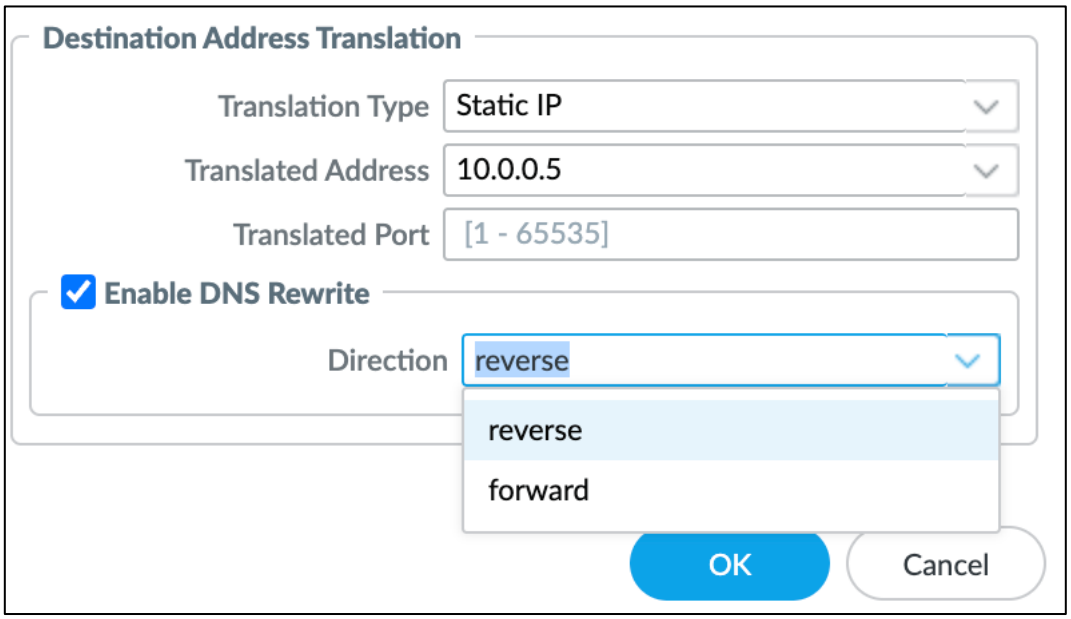

NAT Policy Rule
General
Original Packet
Translated Packet
Any
SOURCE ZONE
Trust-L3
Add
Delete
Destination Zone
Untrust-L3
Destination Interface
any
Service
any
Any
SOURCE ADDRESS
LAN
Add
Delete
Any
DESTINATION ADDRESS
Add
Delete
OK
Cancel

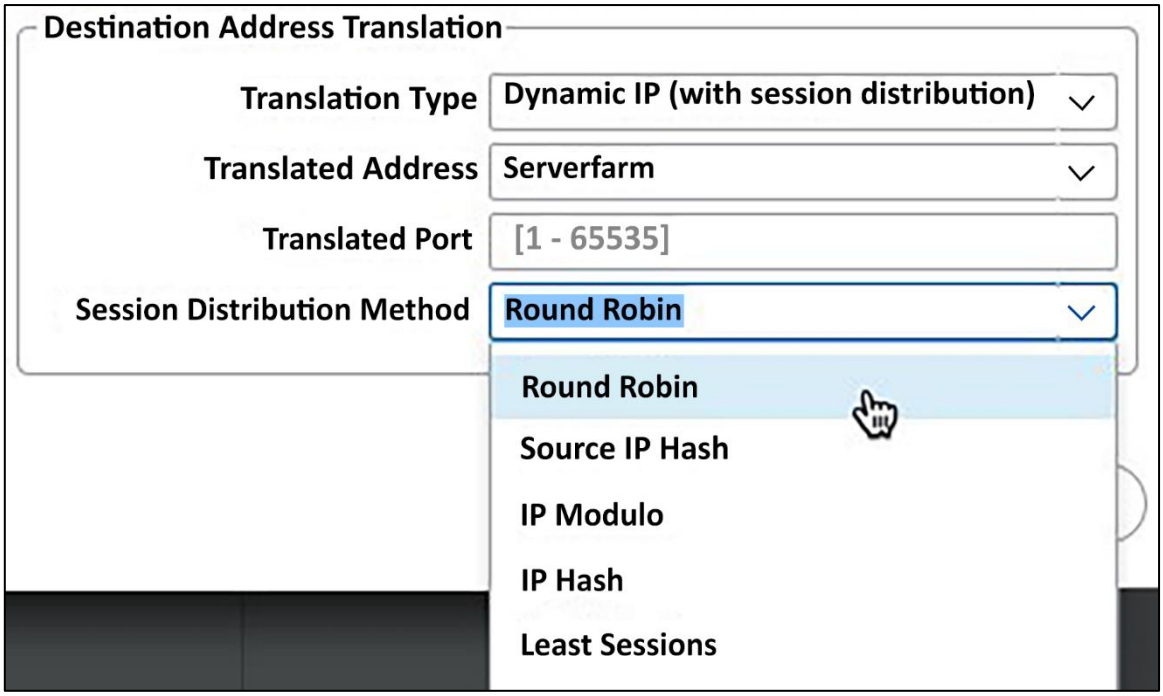

NAT Policy Rule
General
Original Packet
Translated Packet
Source Address Translation
Translation Type
Dynamic IP And Port
Address Type
Interface Address
Interface
ethernet1/1
IP Address
198.51.100.2/24
NAT Policy Rule
General
Original Packet
Translated Packet
Source Address Translation
Translation Type
Dynamic IP And Port
Address Type
Translated Address
TRANSLATED ADDRESS
198.51.100.3
198.51.100.3-198.51.100.38
198.51.100.128/28
Add
Delete


NAT Policy Rule
General
Original Packet
Translated Packet
Source Address Translation
Translation Type
Dynamic IP
TRANSLATED ADDRESS
198.51.100.0/24
203.0.113.0/24
Add
Delete
Advanced (Dynamic IP/Port Fallback)
None
Translated Address
Interface Address
None

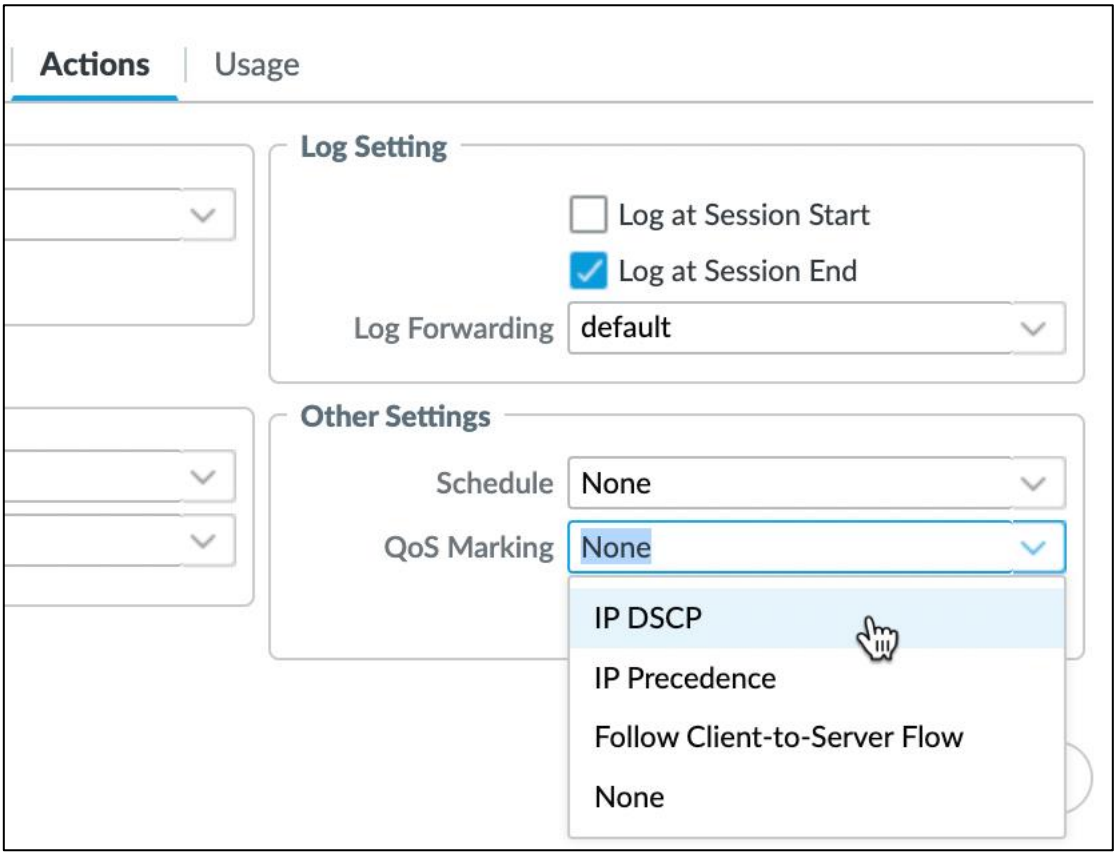

NAT Policy Rule
General
Original Packet
Translated Packet
Any
SOURCE ZONE
Trust-L3
Add
Delete
Destination Zone
Untrust-L3
Destination Interface
any
Service
any
Any
SOURCE ADDRESS
serverfarm
Add
Delete
Any
DESTINATION ADDRESS
Add
Delete
NAT Policy Rule
General
Original Packet
Translated Packet
Source Address Translation
Translation Type
Static IP
Translated Address
serverfarm-public
Bi-directional
Destination Address Translation
Translation Type
None
OK
Cancel

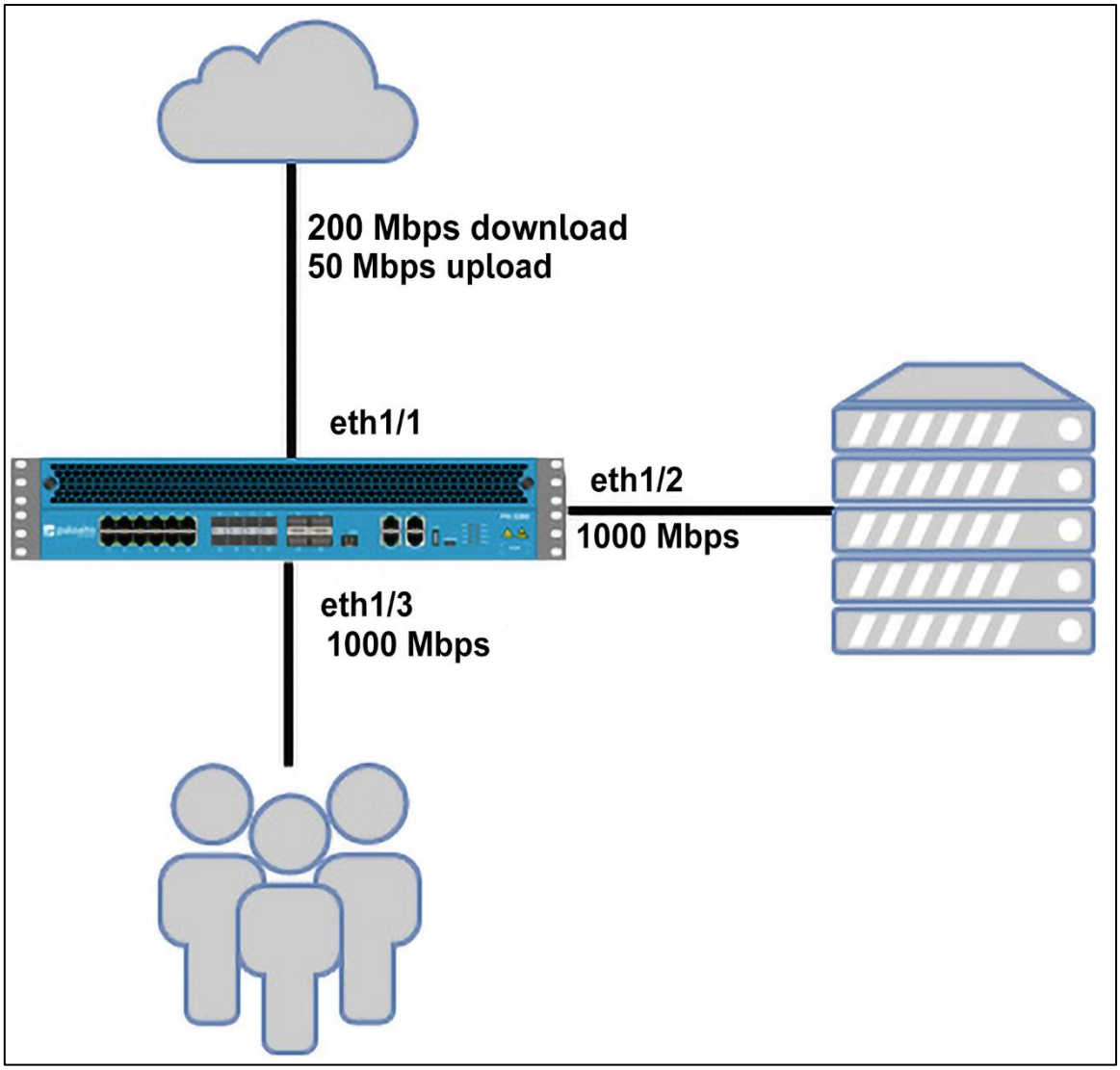

NAT Policy Rule
General
Original Packet
Translated Packet
Any
SOURCE ZONE
Trust-L3
Destination Zone
Untrust-L3
Destination Interface
any
Service
any
Any
SOURCE ADDRESS
Any
DESTINATION ADDRESS
198.51.100.2
Add
Delete
NAT Policy Rule
General
Original Packet
Translated Packet
Source Address Translation
Translation Type
Dynamic IP And Port
Address Type
Interface Address
Interface
ethernet1/4
IP Address
192.168.27.1/24
Destination Address Translation
Translation Type
Static IP
Translated Address
10.0.0.5
Translated Port
[1 - 65535]
Enable DNS Rewrite
Direction
reverse
OK
Cancel


Destination Address Translation
Translation Type
Static IP
Translated Address
10.0.0.5
Translated Port
[1 - 65535]
Enable DNS Rewrite
Direction
reverse
reverse
forward
OK
Cancel



Chapter 4: Taking Control of Sessions





QoS Profile

Profile

Profile Name: internet-download
Egress Max: 200
Egress Guaranteed: 0

Classes

Class Bandwidth Type: Mbps / Percentage

CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
class5	medium	50	0
class1	real-time	0	20

QoS Profile

Profile

Profile Name: internet-upload
Egress Max: 50
Egress Guaranteed: 0

Classes

Class Bandwidth Type: Mbps / Percentage

CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
class1	real-time	0	20

QoS Profile

Profile

Profile Name: vpn
Egress Max: 0
Egress Guaranteed: 0

Classes

Class Bandwidth Type: Mbps / Percentage

CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
class4	medium	0	20

QoS Profile

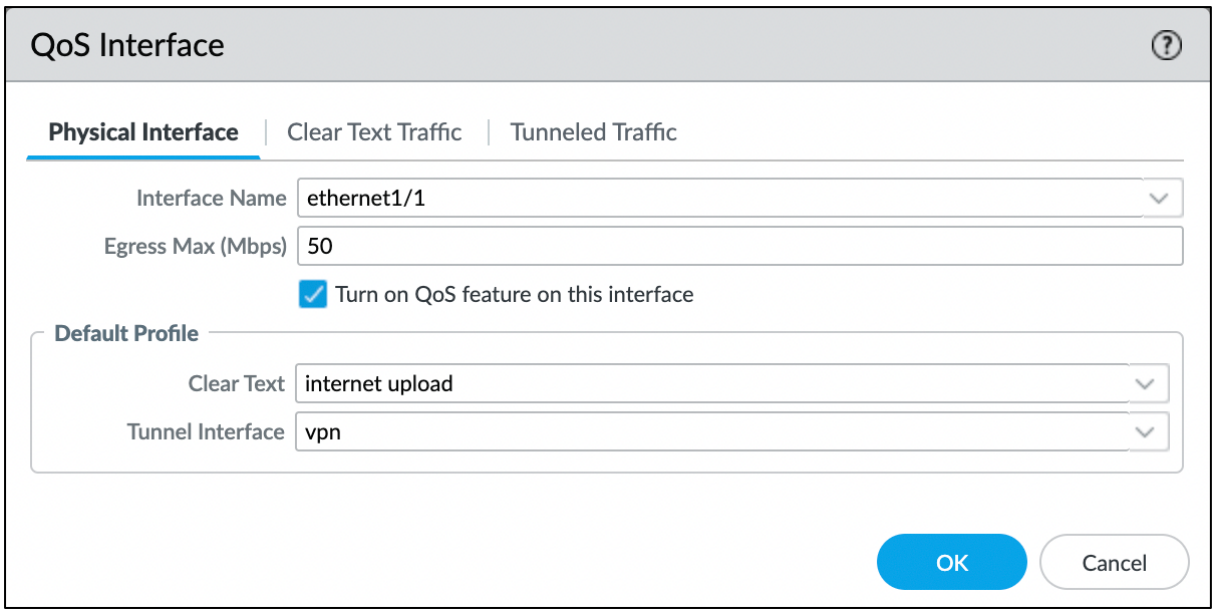
Profile

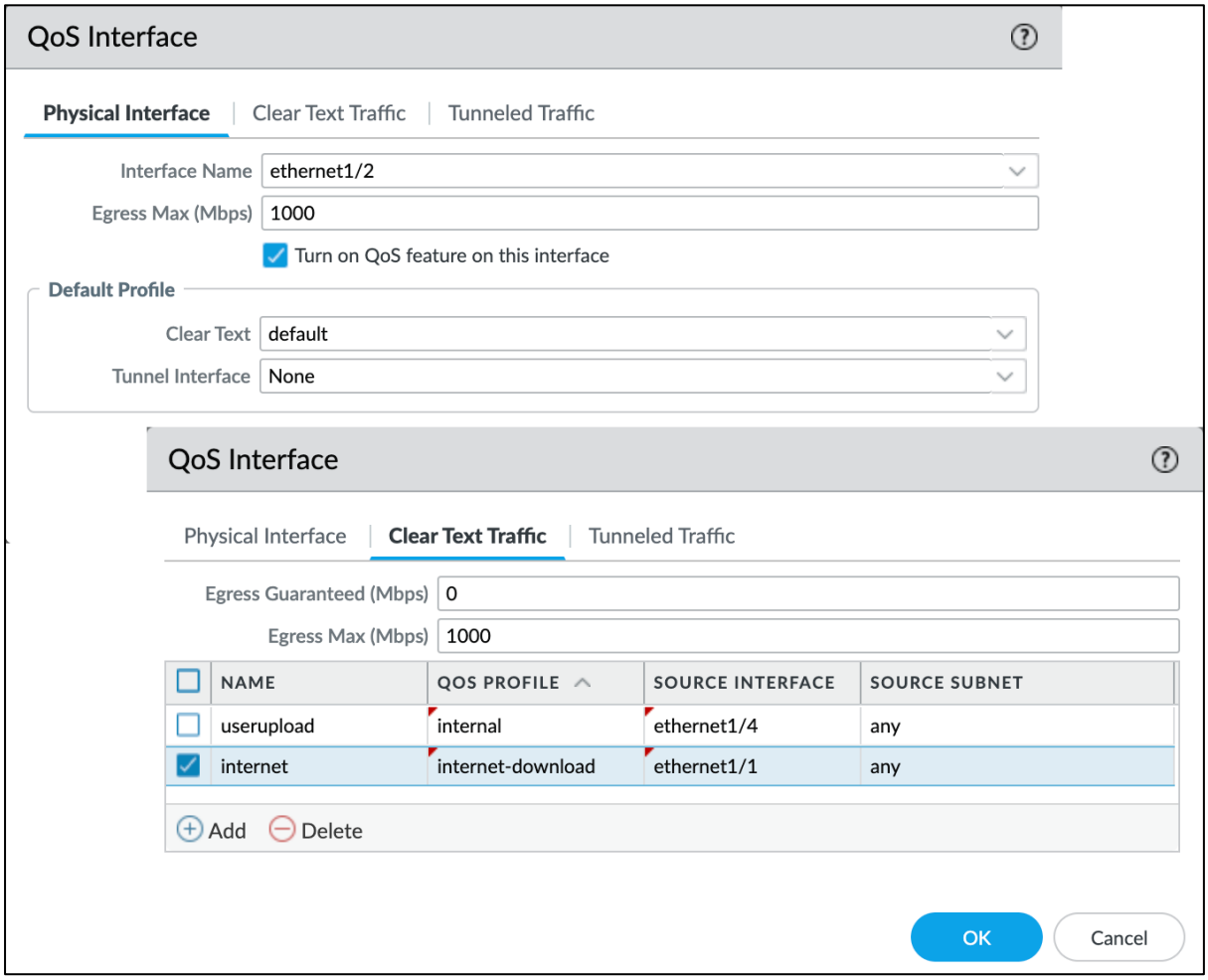
Profile Name: internal
Egress Max: 0
Egress Guaranteed: 0

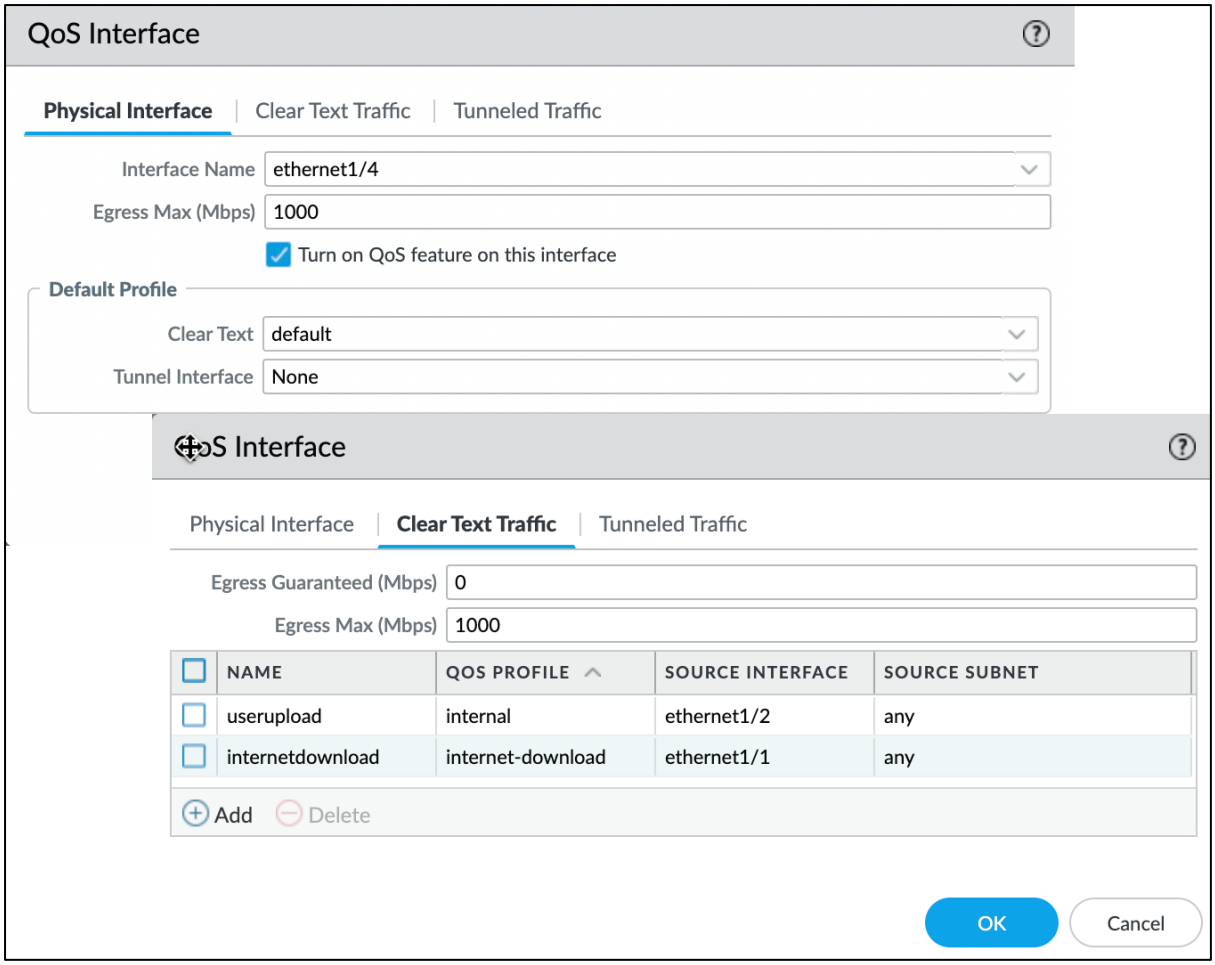
Classes

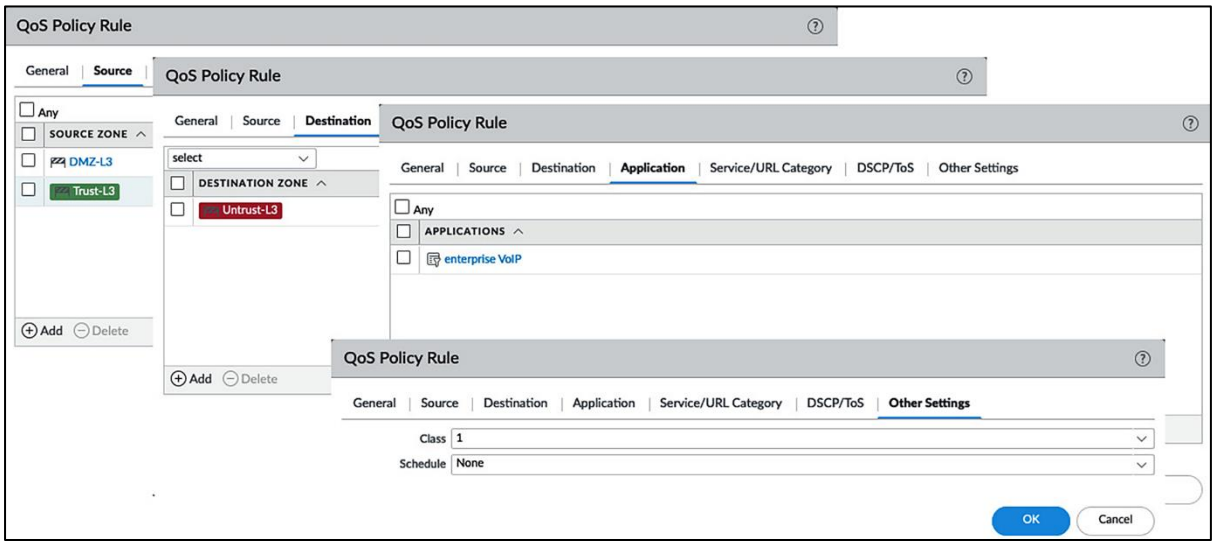
Class Bandwidth Type: Mbps / Percentage

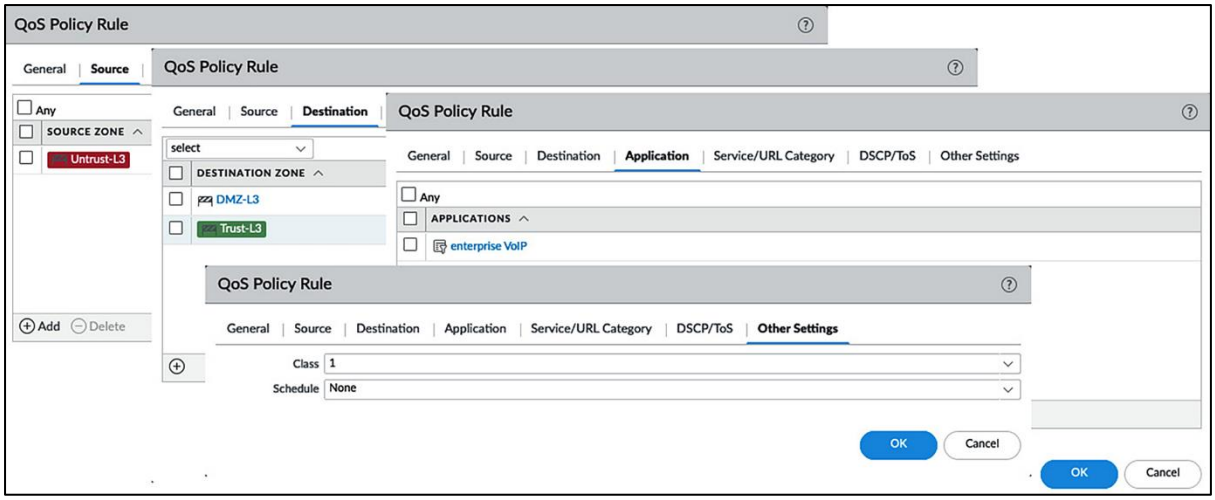
CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
class8	low	300	0

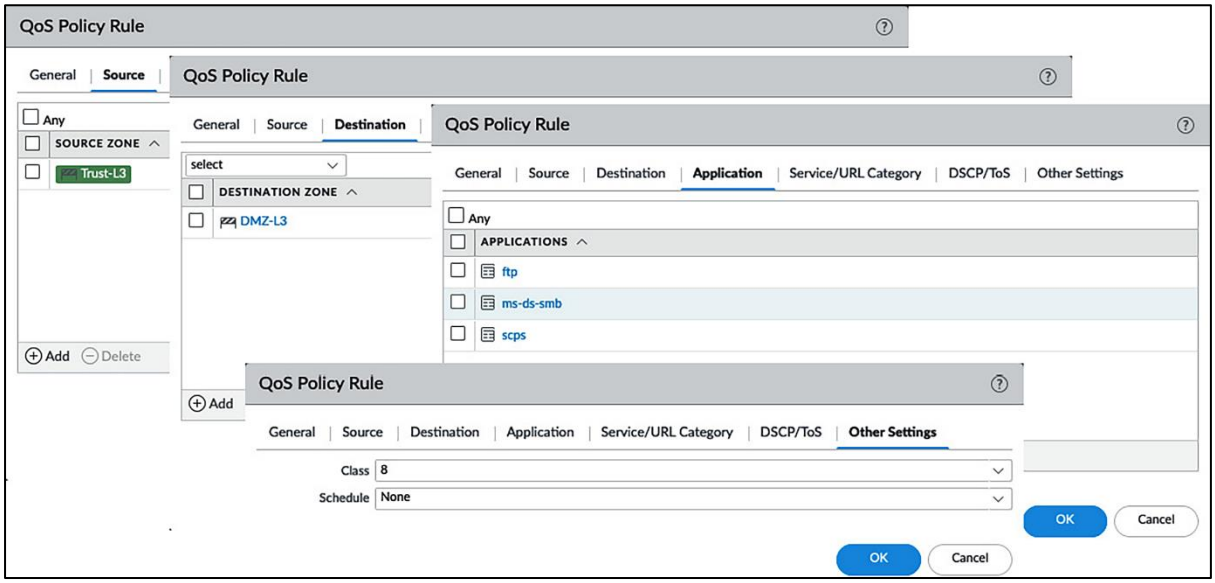

QoS Interface
Physical Interface
Clear Text Traffic
Tunneled Traffic
Interface Name
ethernet1/1
Egress Max (Mbps)
50
Turn on QoS feature on this interface
Default Profile
Clear Text
internet upload
Tunnel Interface
vpn
OK
Cancel

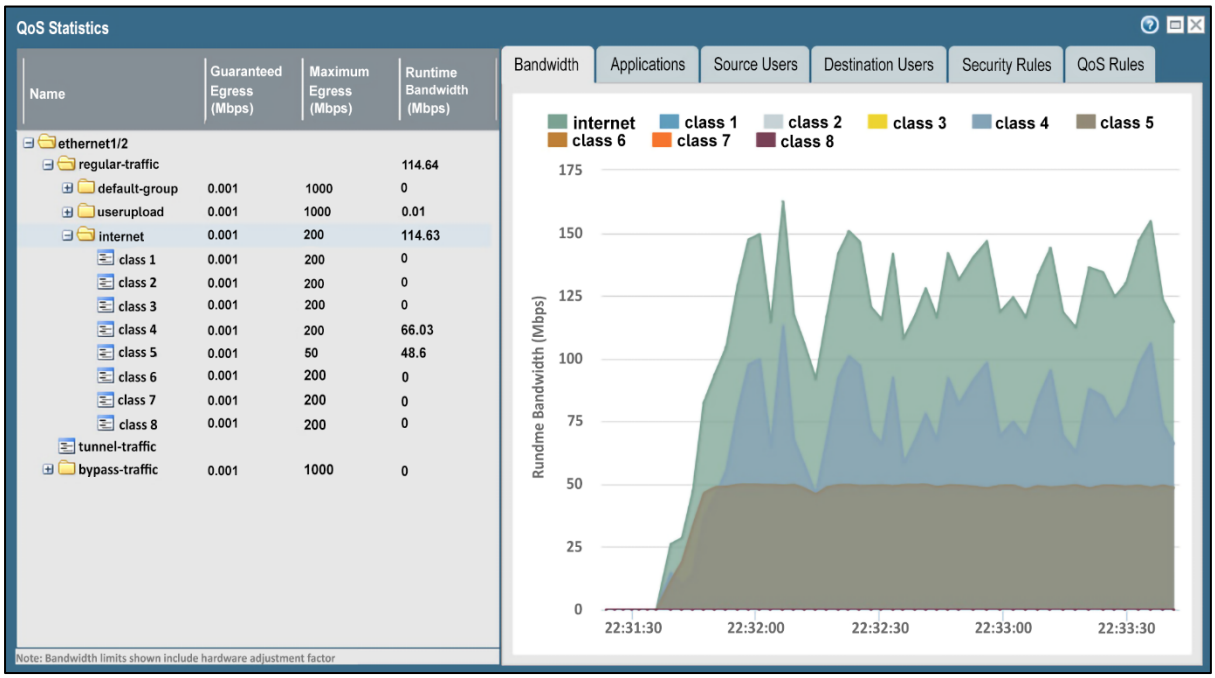

QoS Interface
Physical Interface
Clear Text Traffic
Tunneled Traffic
Interface Name
ethernet1/2
Egress Max (Mbps)
1000
Turn on QoS feature on this interface
Default Profile
Clear Text
default
Tunnel Interface
None
QoS Interface
Physical Interface
Clear Text Traffic
Tunneled Traffic
Egress Guaranteed (Mbps)
0
Egress Max (Mbps)
1000
NAME
QOS PROFILE
SOURCE INTERFACE
SOURCE SUBNET
userupload
internal
ethernet1/4
any
internet
internet-download
ethernet1/1
any
Add
Delete
OK
Cancel

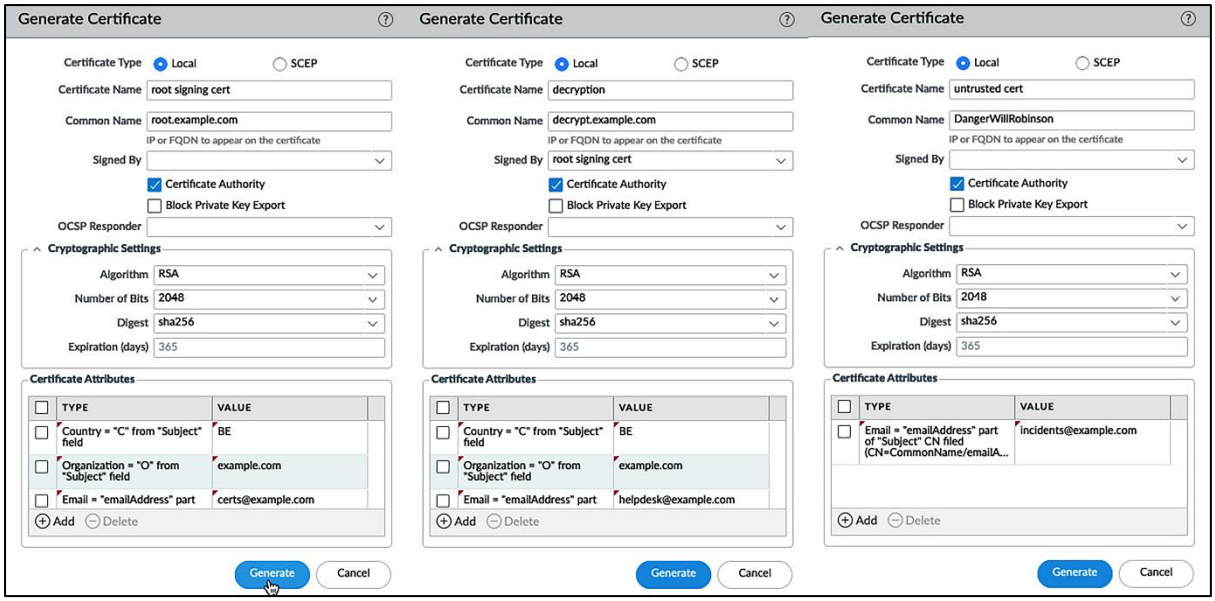

QoS Interface
Physical Interface
Clear Text Traffic
Tunneled Traffic
Interface Name
ethernet1/4
Egress Max (Mbps)
1000
Turn on QoS feature on this interface
Default Profile
Clear Text
default
Tunnel Interface
None
QoS Interface
Physical Interface
Clear Text Traffic
Tunneled Traffic
Egress Guaranteed (Mbps)
0
Egress Max (Mbps)
1000
NAME
QOS PROFILE
SOURCE INTERFACE
SOURCE SUBNET
userupload
internal
ethernet1/2
any
internetdownload
internet-download
ethernet1/1
any
Add
Delete
OK
Cancel

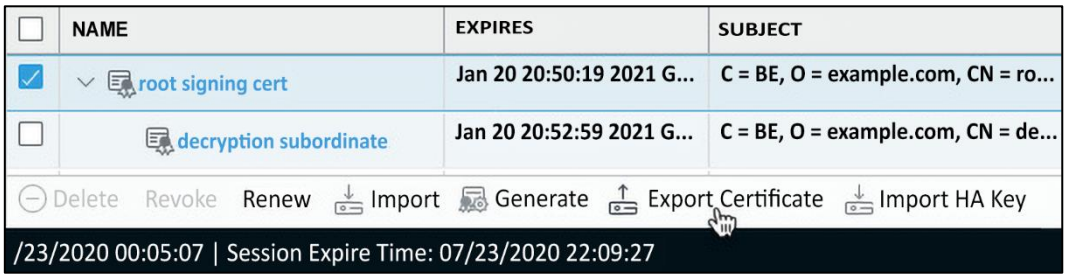

QoS Policy Rule
General
Source
Destination
Application
Service/URL Category
DSCP/ToS
Other Settings
Any
SOURCE ZONE
DMZ-L3
Trust-L3
DESTINATION ZONE
Untrust-L3
APPLICATIONS
enterprise VoIP
Add
Delete
Class
1
Schedule
None
OK
Cancel

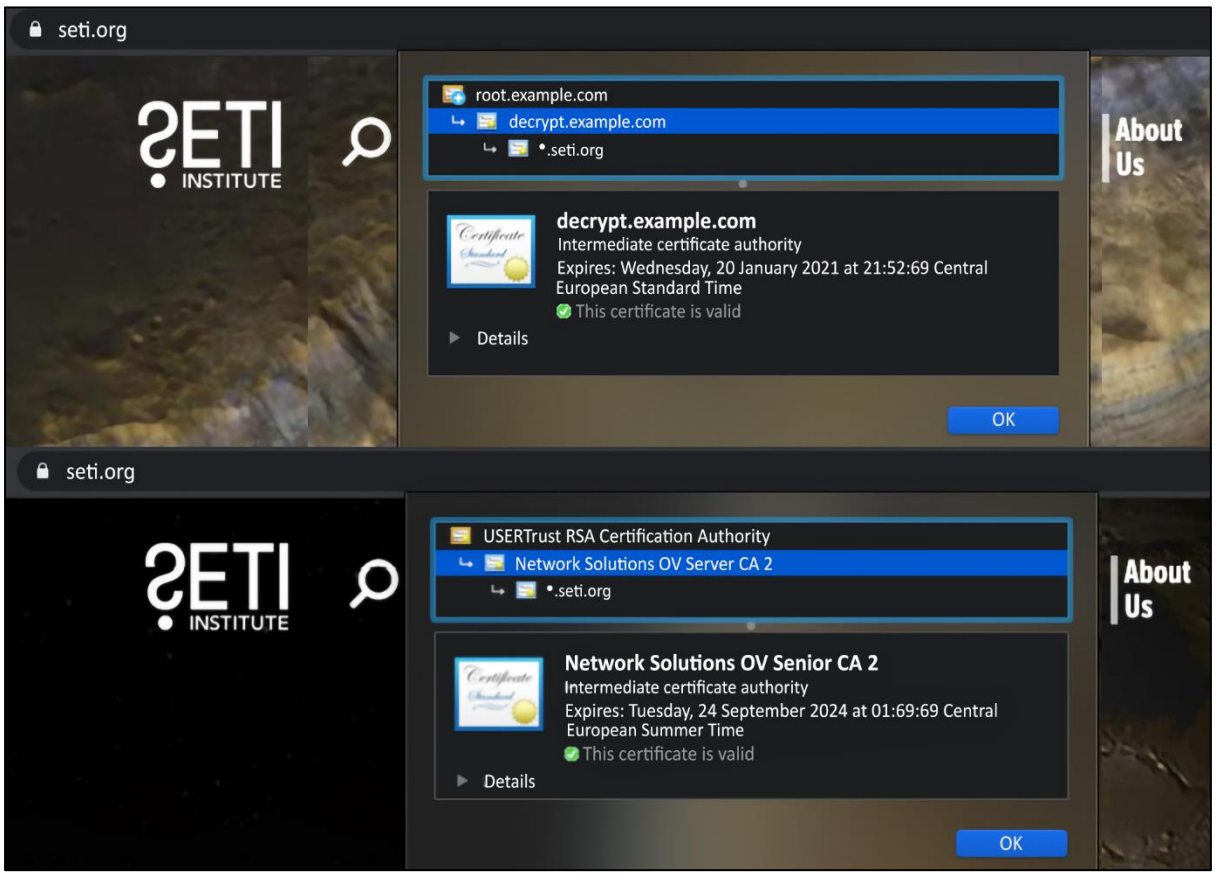

QoS Policy Rule
General | Source
QoS Policy Rule
Any
SOURCE ZONE
Untrust-L3
General | Source | Destination
QoS Policy Rule
select
DESTINATION ZONE
DMZ-L3
Trust-L3
General | Source | Destination | Application | Service/URL Category | DSCP/ToS | Other Settings
Any
APPLICATIONS
enterprise VoIP
QoS Policy Rule
General | Source | Destination | Application | Service/URL Category | DSCP/ToS | Other Settings
Class 1
Schedule None
Add
Delete
OK
Cancel
OK
Cancel


QoS Policy Rule
General | Source
QoS Policy Rule
Any
SOURCE ZONE
Trust-L3
General | Source | Destination
QoS Policy Rule
select
DESTINATION ZONE
DMZ-L3
General | Source | Destination | Application | Service/URL Category | DSCP/ToS | Other Settings
Any
APPLICATIONS
ftp
ms-ds-smb
scps
Add
Delete
Add
QoS Policy Rule
General | Source | Destination | Application | Service/URL Category | DSCP/ToS | Other Settings
Class 8
Schedule None
OK
Cancel
OK
Cancel

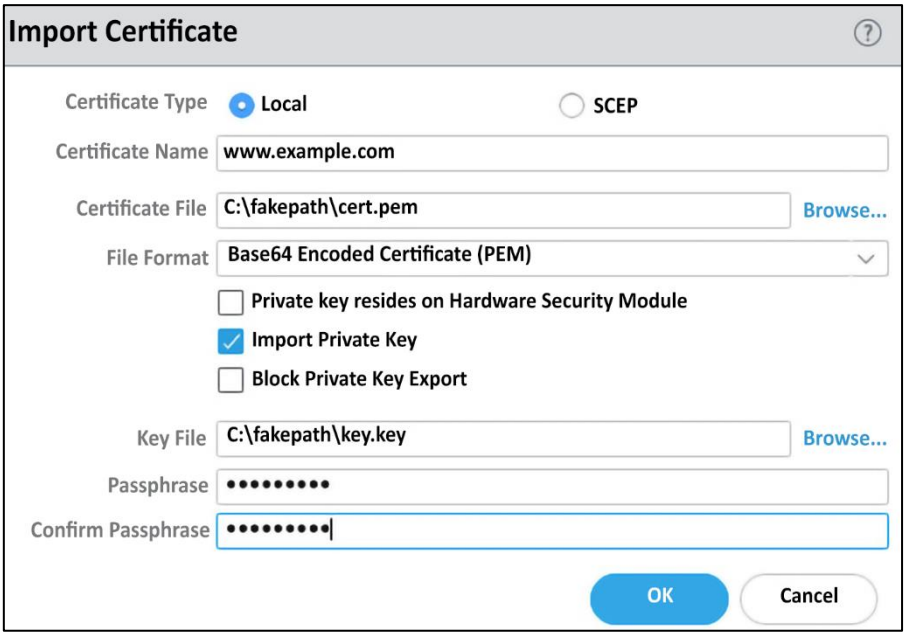

QoS Statistics
Name
Guaranteed Egress (Mbps)
Maximum Egress (Mbps)
Runtime Bandwidth (Mbps)
ethernet1/2
regular-traffic 114.64
default-group 0.001 1000 0
userupload 0.001 1000 0.01
internet 0.001 200 114.63
class 1 0.001 200 0
class 2 0.001 200 0
class 3 0.001 200 0
class 4 0.001 200 66.03
class 5 0.001 50 48.6
class 6 0.001 200 0
class 7 0.001 200 0
class 8 0.001 200 0
tunnel-traffic
bypass-traffic 0.001 1000 0
Note: Bandwidth limits shown include hardware adjustment factor
Bandwidth
Applications
Source Users
Destination Users
Security Rules
QoS Rules
internet
class 1
class 2
class 3
class 4
class 5
class 6
class 7
class 8
Rundme Bandwidth (Mbps)
175
150
125
100
75
50
25
0
22:31:30
22:32:00
22:32:30
22:33:00
22:33:30


Generate Certificate
Certificate Type Local SCEP
Certificate Name root signing cert
Common Name root.example.com
IP or FQDN to appear on the certificate
Signed By
Certificate Authority
Block Private Key Export
OCSP Responder
Cryptographic Settings
Algorithm RSA
Number of Bits 2048
Digest sha256
Expiration (days) 365
Certificate Attributes
TYPE VALUE
Country = "C" from "Subject" field BE
Organization = "O" from "Subject" field example.com
Email = "emailAddress" part certs@example.com
Add Delete
Generate Cancel
Generate Certificate
Certificate Type Local SCEP
Certificate Name decryption
Common Name decrypt.example.com
IP or FQDN to appear on the certificate
Signed By root signing cert
Certificate Authority
Block Private Key Export
OCSP Responder
Cryptographic Settings
Algorithm RSA
Number of Bits 2048
Digest sha256
Expiration (days) 365
Certificate Attributes
TYPE VALUE
Country = "C" from "Subject" field BE
Organization = "O" from "Subject" field example.com
Email = "emailAddress" part helpdesk@example.com
Add Delete
Generate Cancel
Generate Certificate
Certificate Type Local SCEP
Certificate Name untrusted cert
Common Name DangerWillRobinson
IP or FQDN to appear on the certificate
Signed By
Certificate Authority
Block Private Key Export
OCSP Responder
Cryptographic Settings
Algorithm RSA
Number of Bits 2048
Digest sha256
Expiration (days) 365
Certificate Attributes
TYPE VALUE
Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailA... incidents@example.com
Add Delete
Generate Cancel

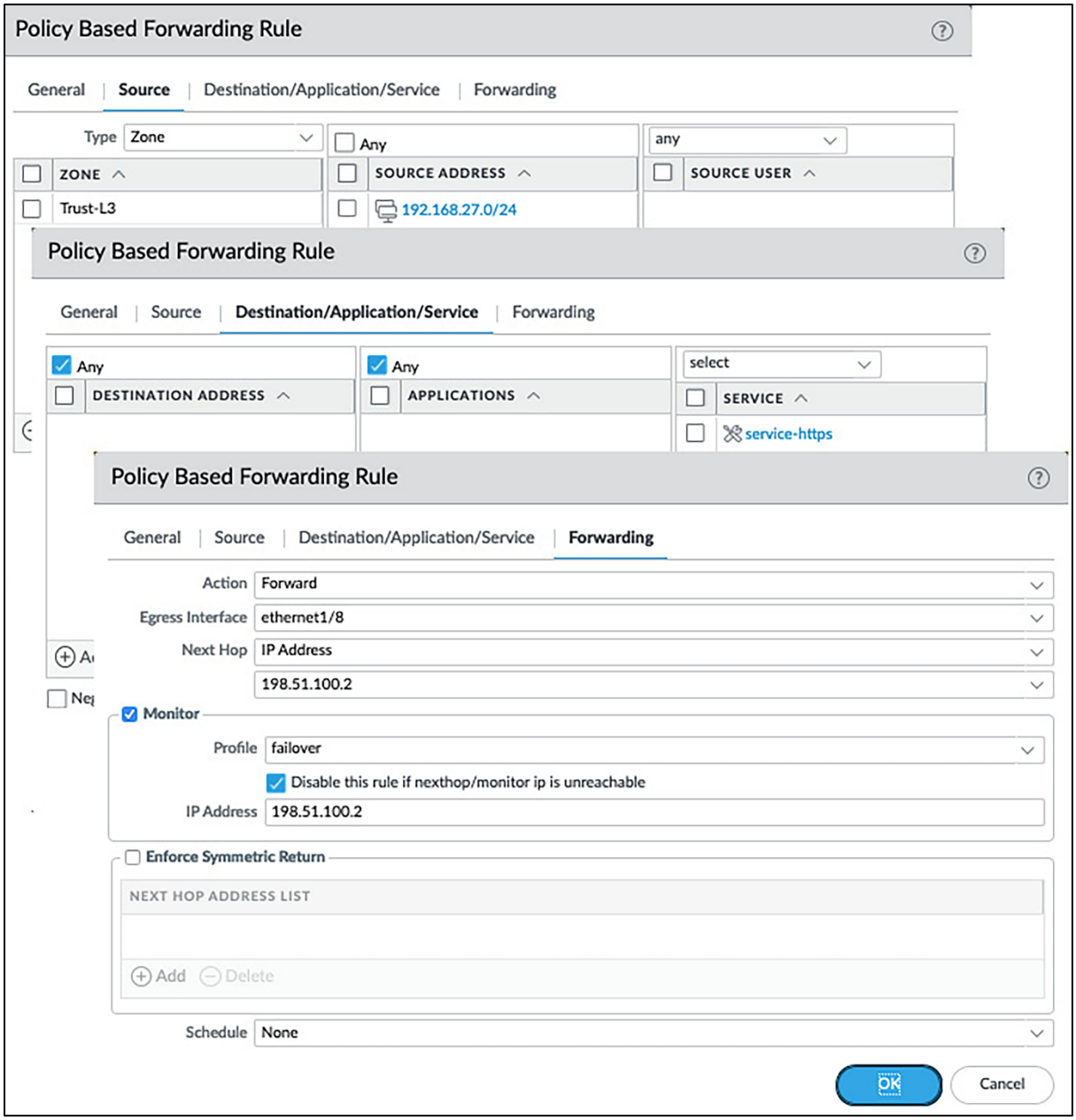

NAME
EXPIRES
SUBJECT
root signing cert
Jan 20 20:50:19 2021 G...
C = BE, O = example.com, CN = ro...
decryption subordinate
Jan 20 20:52:59 2021 G...
C = BE, O = example.com, CN = de...
Delete Revoke Renew Import Generate Export Certificate Import HA Key
/23/2020 00:05:07 | Session Expire Time: 07/23/2020 22:09:27

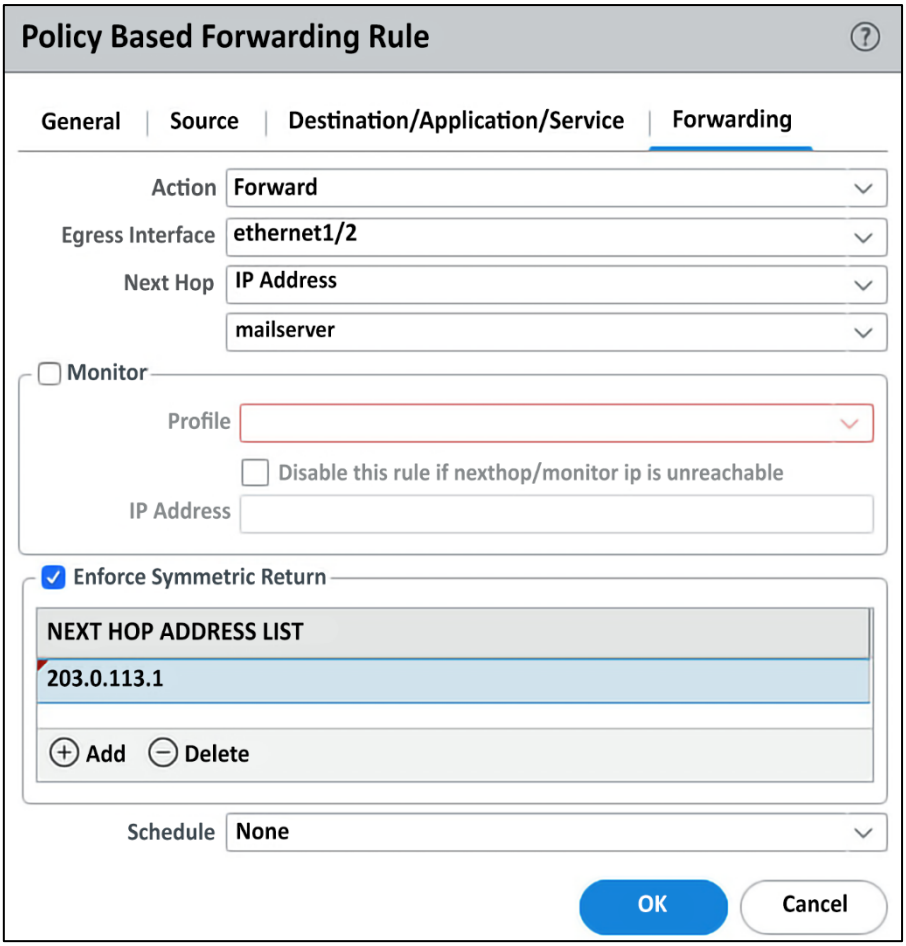

seti.org
SETI INSTITUTE
root.example.com
decrypt.example.com
*.seti.org
decrypt.example.com
Intermediate certificate authority
Expires: Wednesday, 20 January 2021 at 21:52:69 Central European Standard Time
This certificate is valid
Details
OK
About Us
seti.org
SETI INSTITUTE
USERTrust RSA Certification Authority
Network Solutions OV Server CA 2
*.seti.org
Network Solutions OV Senior CA 2
Intermediate certificate authority
Expires: Tuesday, 24 September 2024 at 01:69:69 Central European Summer Time
This certificate is valid
Details
OK
About Us

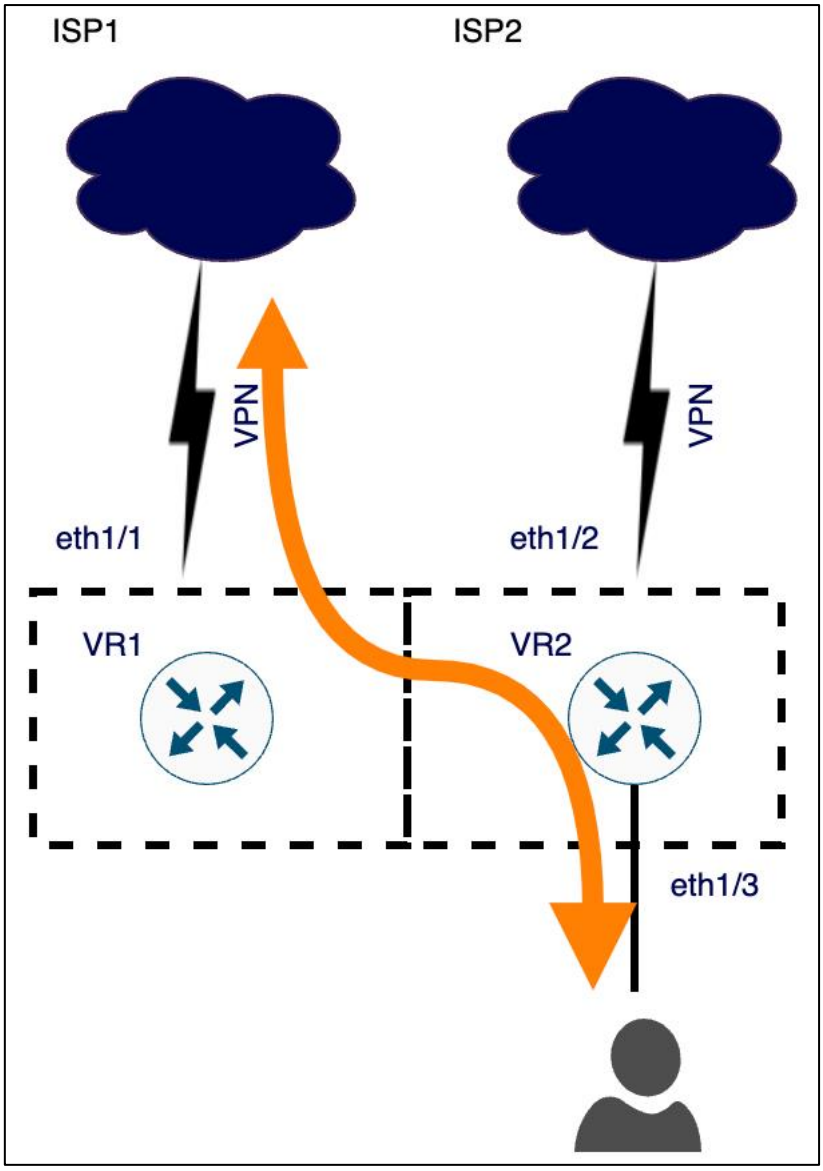
	NAME	TAGS	TYPE	Source			Destination		APPLICA...	SERVICE	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS			
4	Block Quic	none	universal	PANgurus	any	any	perimeter	any	quic	application-default	Drop

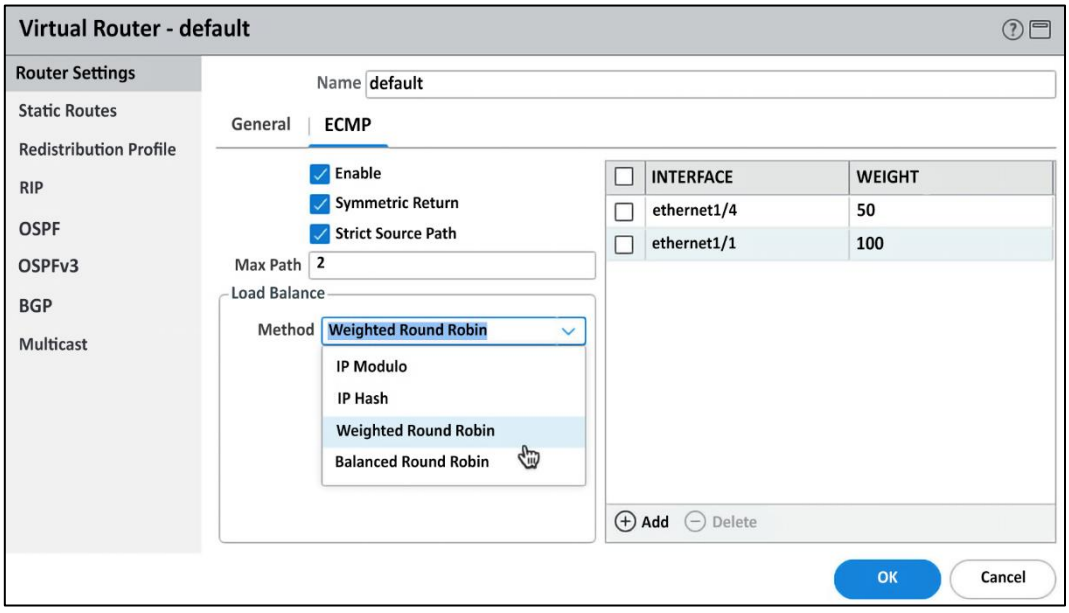


DigiCert Global Root CA	CN = DigiCert Global Root CA	CN = DigiCert Global Root CA	
DigiCert SHA2 Secure Server CA	CN = DigiCert SHA2 Secure Server CA	CN = DigiCert Global Root CA	
www example com	CN = www example com	CN = DigiCert SHA2 Secure Server CA	

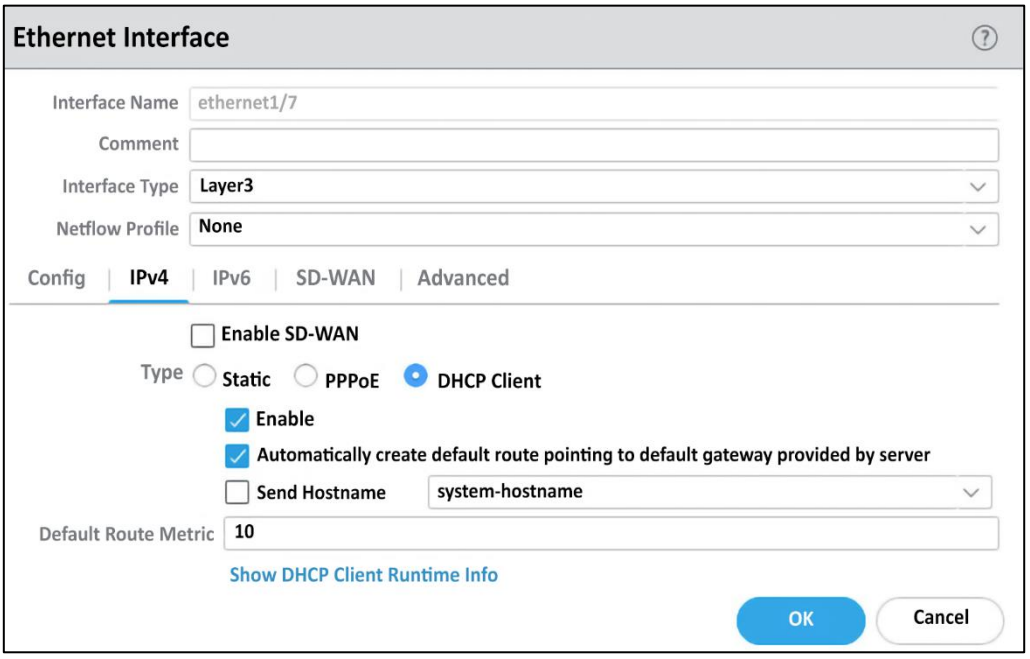

Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Type
Zone
Any
any
ZONE
SOURCE ADDRESS
SOURCE USER
Trust-L3
192.168.27.0/24
Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Any
Any
select
DESTINATION ADDRESS
APPLICATIONS
SERVICE
service-https
Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Action
Forward
Egress Interface
ethernet1/8
Next Hop
IP Address
198.51.100.2
Monitor
Profile
failover
Disable this rule if nexthop/monitor ip is unreachable
IP Address
198.51.100.2
Enforce Symmetric Return
NEXT HOP ADDRESS LIST
Add
Delete
Schedule
None
OK
Cancel

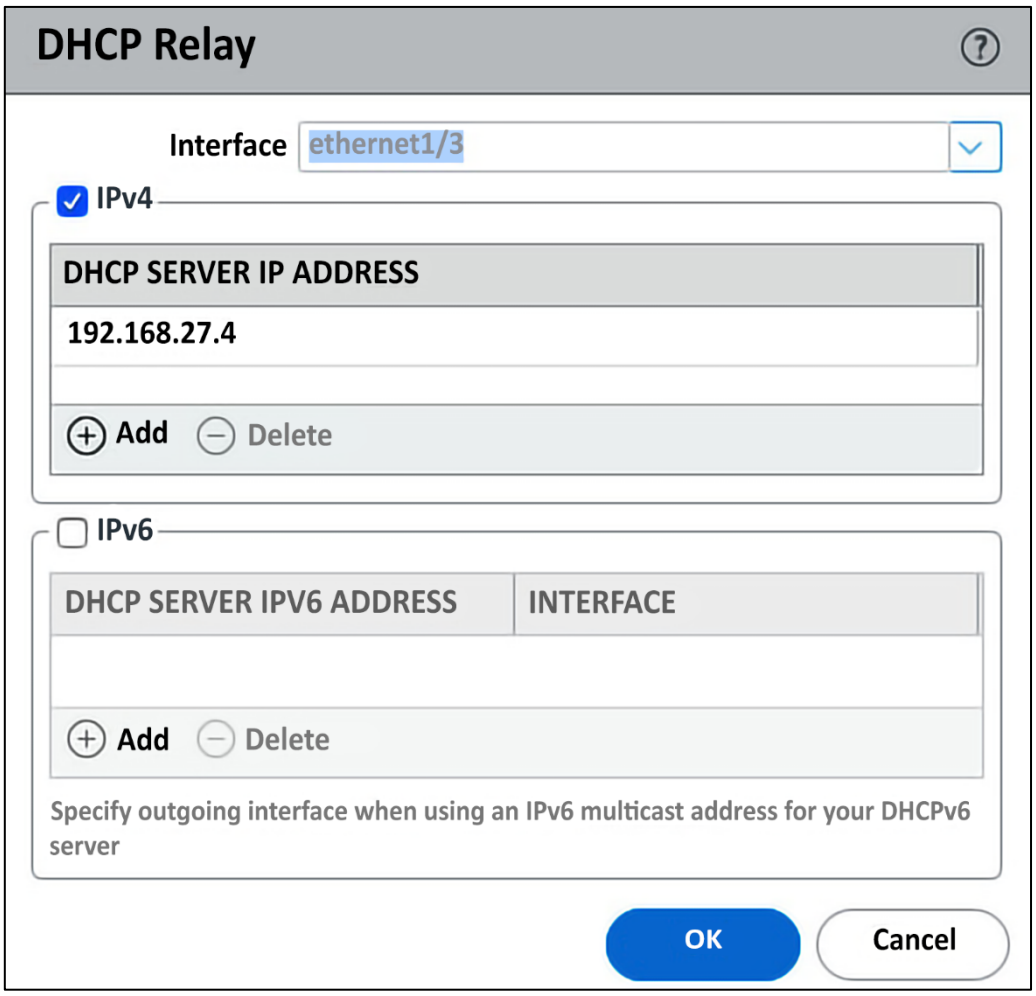

Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Action
Forward
Egress Interface
ethernet1/2
Next Hop
IP Address
mailserver
Monitor
Profile
Disable this rule if nexthop/monitor ip is unreachable
IP Address
Enforce Symmetric Return
NEXT HOP ADDRESS LIST
203.0.113.1
Add
Delete
Schedule
None
OK
Cancel

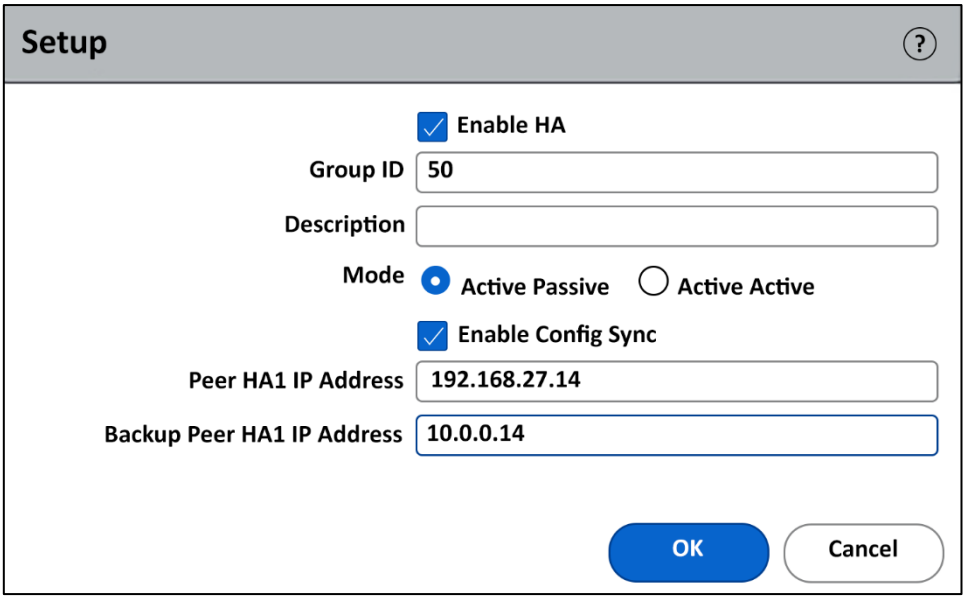

ISP1
ISP2
VPN
VPN
eth1/1
eth1/2
VR1
VR2
eth1/3

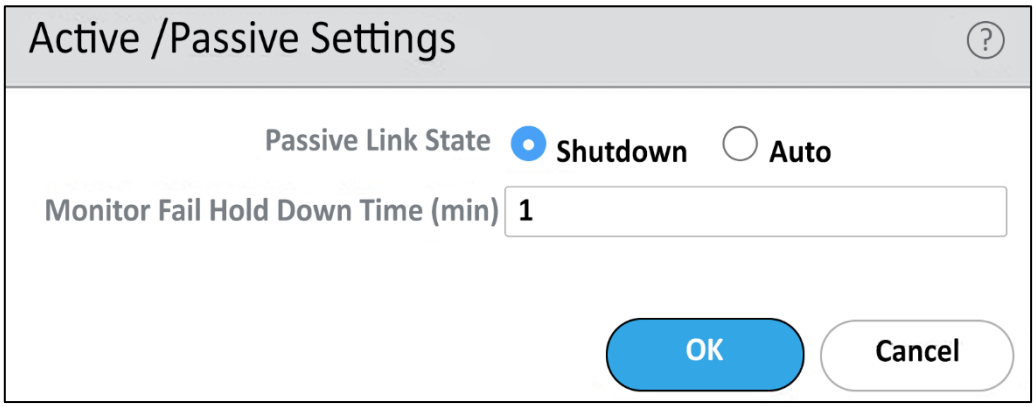

Virtual Router - default
Router Settings
Static Routes
Redistribution Profile
RIP
OSPF
OSPFv3
BGP
Multicast
Name default
General
ECMP
Enable
Symmetric Return
Strict Source Path
Max Path 2
Load Balance
Method Weighted Round Robin
IP Modulo
IP Hash
Weighted Round Robin
Balanced Round Robin
INTERFACE
WEIGHT
ethernet1/4 50
ethernet1/1 100
Add
Delete
OK
Cancel

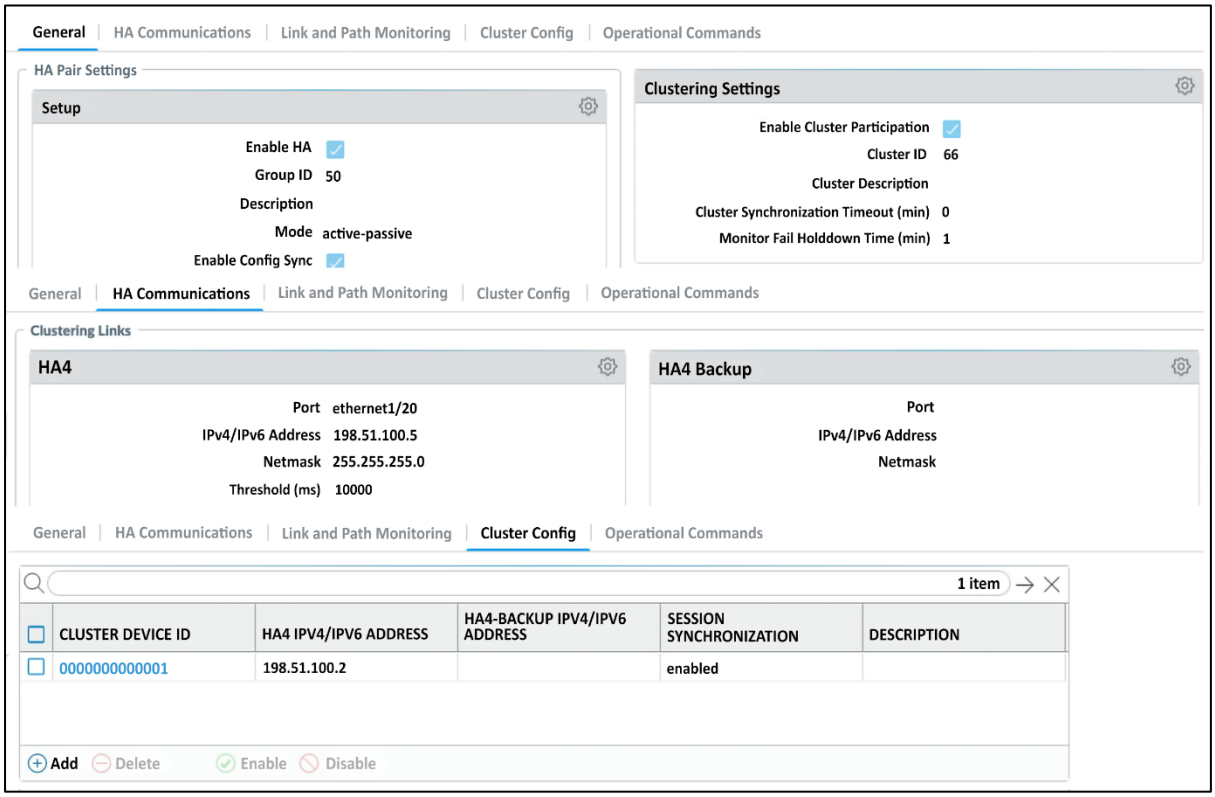
Chapter 5: Services and Operational Modes



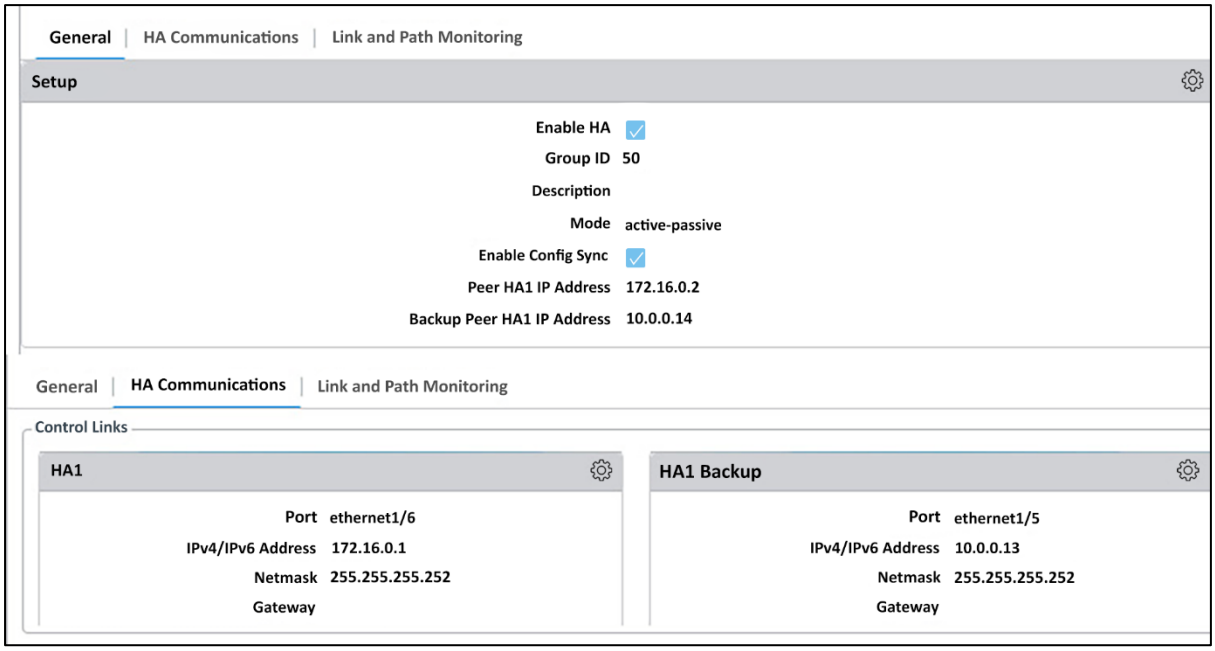


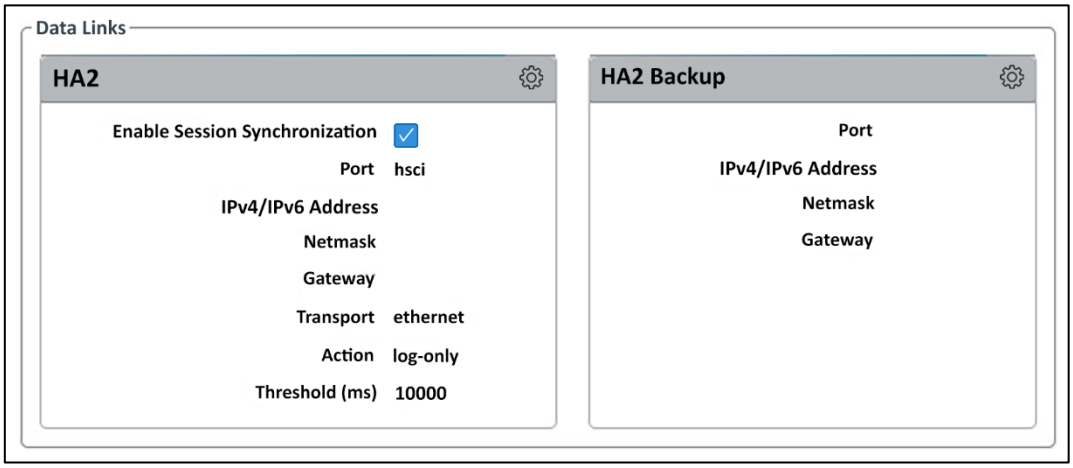

Setup
Enable HA
Group ID
50
Description
Mode
Active Passive
Active Active
Enable Config Sync
Peer HA1 IP Address
192.168.27.14
Backup Peer HA1 IP Address
10.0.0.14
OK
Cancel

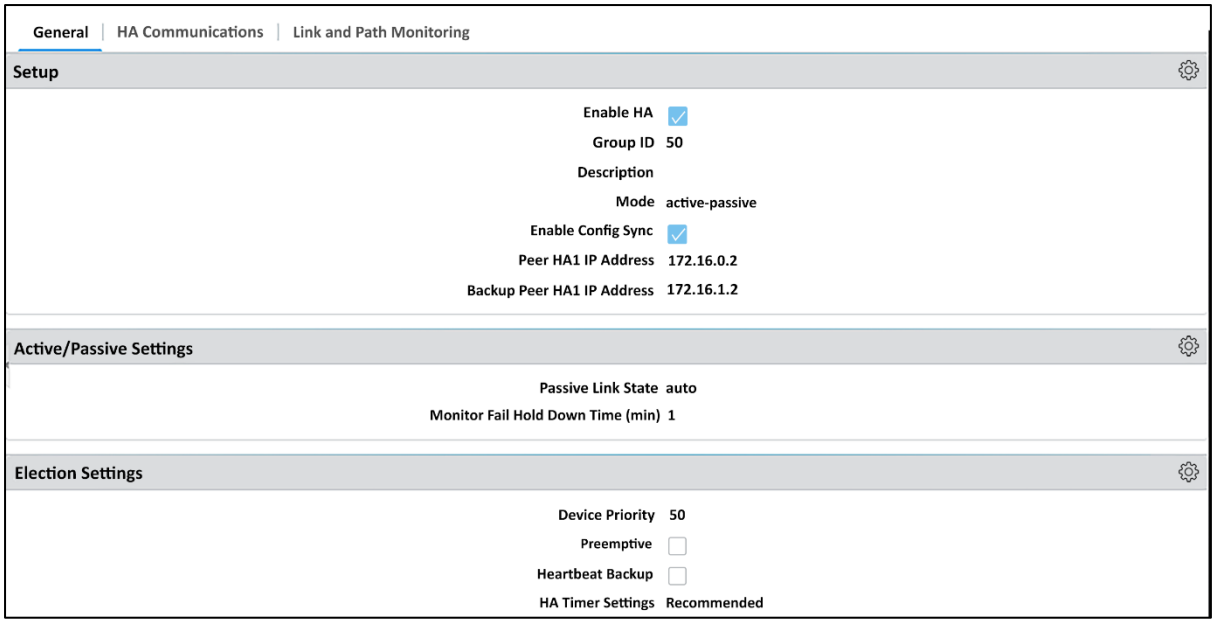

Active /Passive Settings
Passive Link State
Shutdown
Auto
Monitor Fail Hold Down Time (min)
1
OK
Cancel

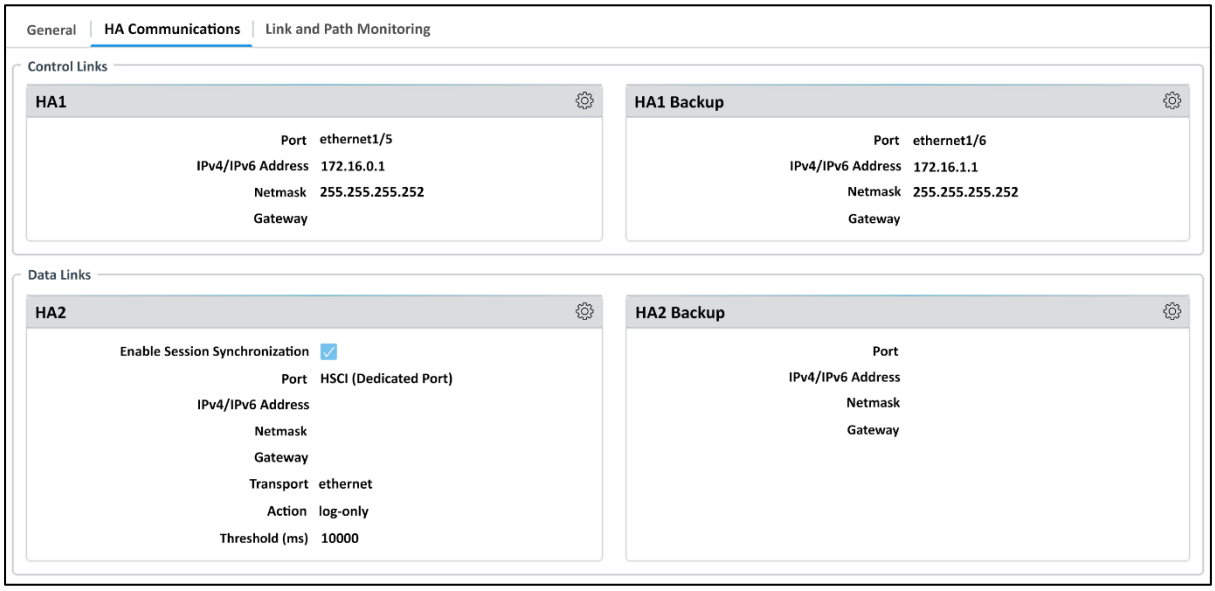

General
HA Communications
Link and Path Monitoring
Cluster Config
Operational Commands
HA Pair Settings
Setup
Enable HA
Group ID 50
Description
Mode active-passive
Enable Config Sync
Clustering Settings
Enable Cluster Participation
Cluster ID 66
Cluster Description
Cluster Synchronization Timeout (min) 0
Monitor Fail Holddown Time (min) 1
Clustering Links
HA4
Port ethernet1/20
IPv4/IPv6 Address 198.51.100.5
Netmask 255.255.255.0
Threshold (ms) 10000
HA4 Backup
Port
IPv4/IPv6 Address
Netmask
1 item
CLUSTER DEVICE ID
HA4 IPV4/IPV6 ADDRESS
HA4-BACKUP IPV4/IPV6 ADDRESS
SESSION SYNCHRONIZATION
DESCRIPTION
0000000000001
198.51.100.2
enabled
Add
Delete
Enable
Disable

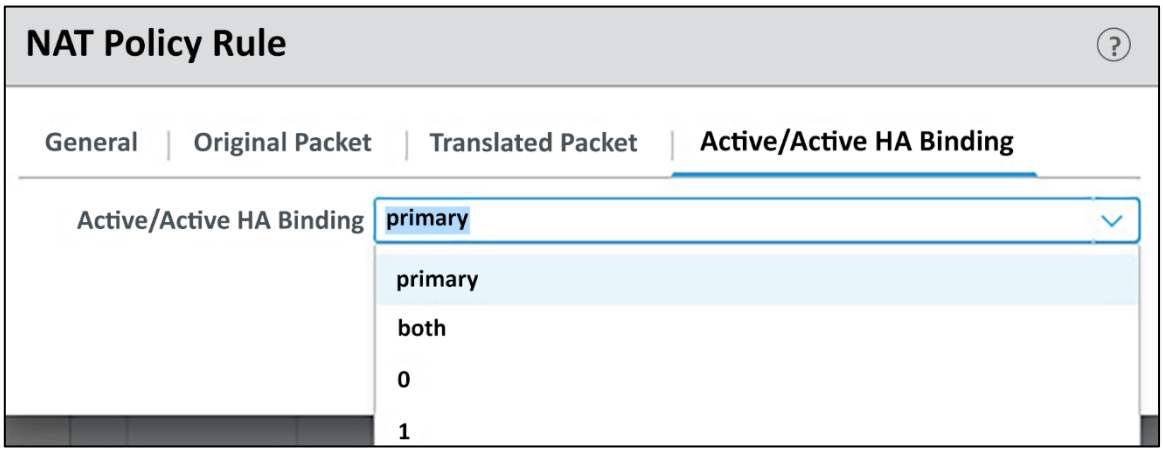

Import HA Key
Export HA Key

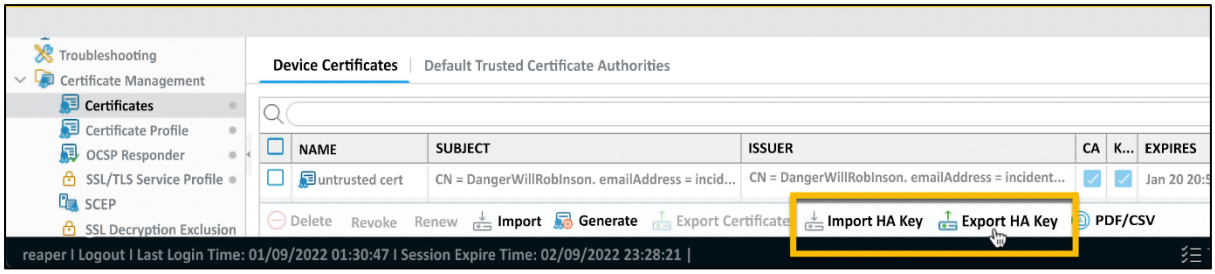

General | HA Communications | Link and Path Monitoring
Setup
Enable HA
Group ID 50
Description
Mode active-passive
Enable Config Sync
Peer HA1 IP Address 172.16.0.2
Backup Peer HA1 IP Address 10.0.0.14
General | HA Communications | Link and Path Monitoring
Control Links
HA1
Port ethernet1/6
IPv4/IPv6 Address 172.16.0.1
Netmask 255.255.255.252
Gateway
HA1 Backup
Port ethernet1/5
IPv4/IPv6 Address 10.0.0.13
Netmask 255.255.255.252
Gateway

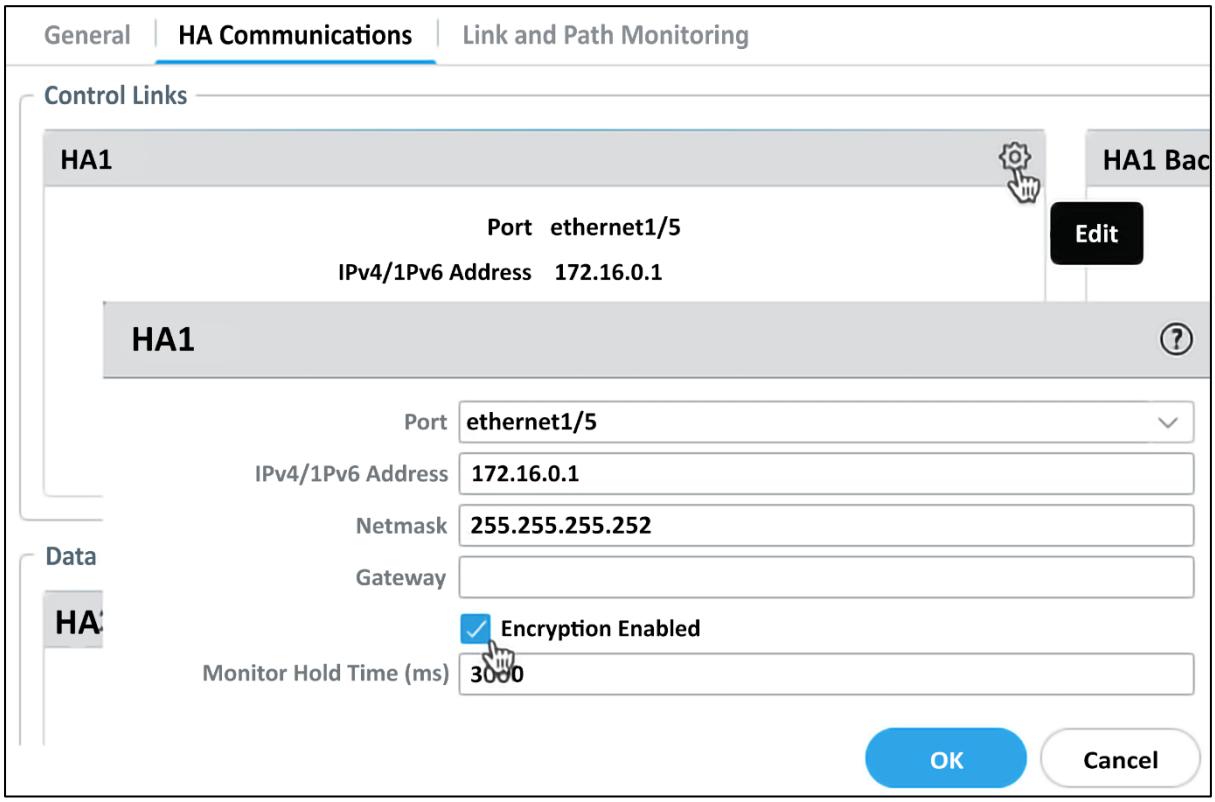

Data Links
HA2
Enable Session Synchronization
Port hsci
IPv4/IPv6 Address
Netmask
Gateway
Transport ethernet
Action log-only
Threshold (ms) 10000
HA2 Backup
Port
IPv4/IPv6 Address
Netmask
Gateway

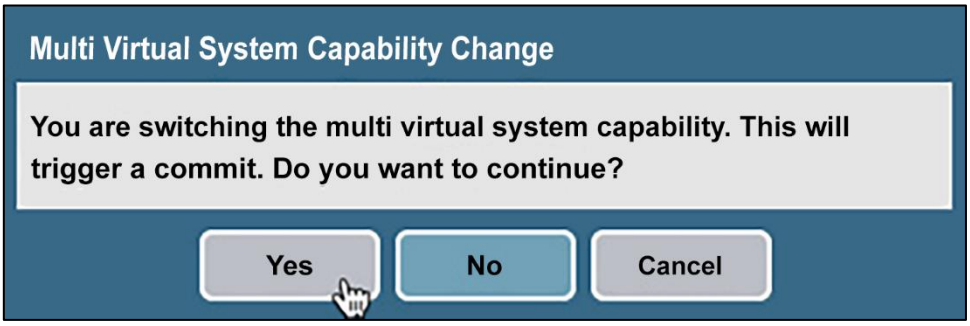

General
HA Communications
Link and Path Monitoring
Setup
Enable HA
Group ID 50
Description
Mode active-passive
Enable Config Sync
Peer HA1 IP Address 172.16.0.2
Backup Peer HA1 IP Address 172.16.1.2
Active/Passive Settings
Passive Link State auto
Monitor Fail Hold Down Time (min) 1
Election Settings
Device Priority 50
Preemptive
Heartbeat Backup
HA Timer Settings Recommended

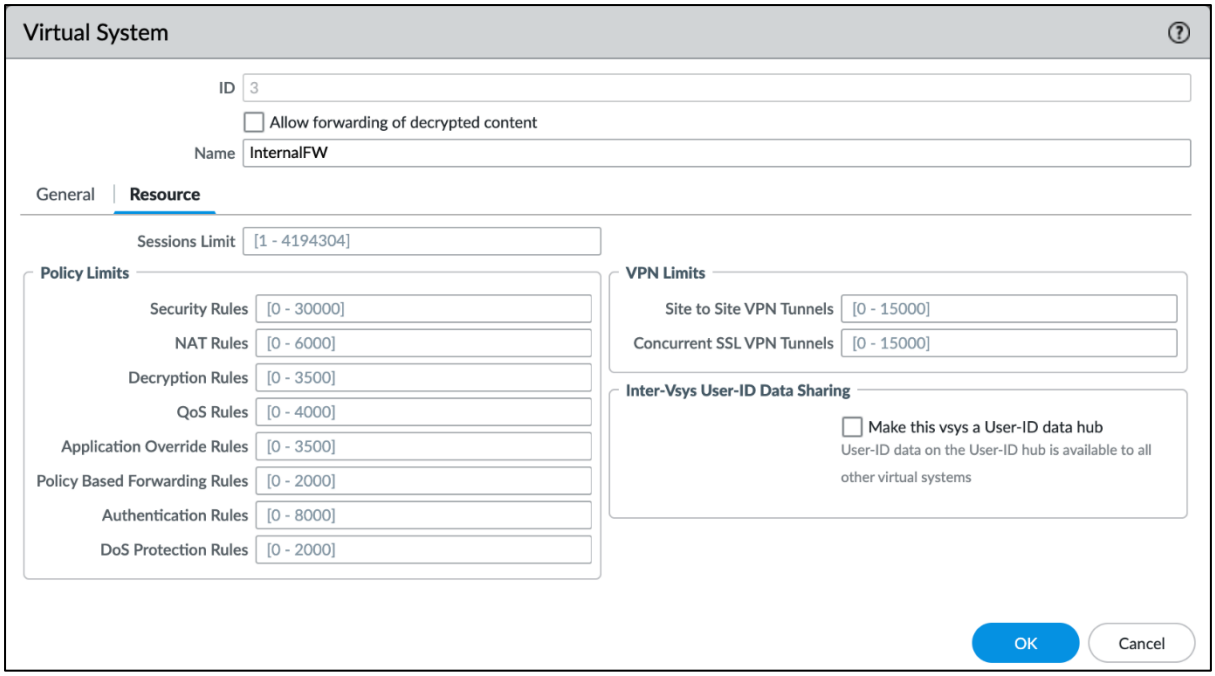

General
HA Communications
Link and Path Monitoring
Control Links
HA1
Port ethernet1/5
IPv4/IPv6 Address 172.16.0.1
Netmask 255.255.255.252
Gateway
HA1 Backup
Port ethernet1/6
IPv4/IPv6 Address 172.16.1.1
Netmask 255.255.255.252
Gateway
Data Links
HA2
Enable Session Synchronization
Port HSCI (Dedicated Port)
IPv4/IPv6 Address
Netmask
Gateway
Transport ethernet
Action log-only
Threshold (ms) 10000
HA2 Backup
Port
IPv4/IPv6 Address
Netmask
Gateway

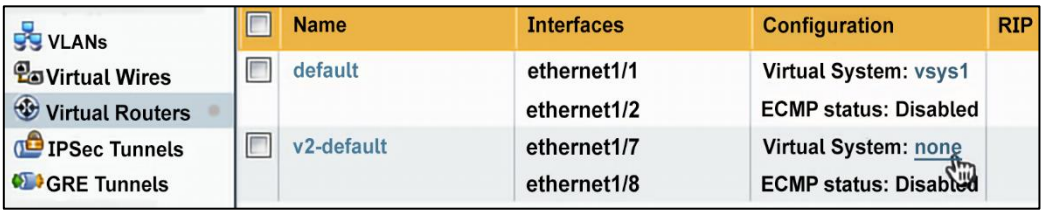

NAT Policy Rule
General
Original Packet
Translated Packet
Active/Active HA Binding
Active/Active HA Binding
primary
primary
both
0
1


Troubleshooting
Certificate Management
Certificates
Certificate Profile
OCSP Responder
SSL/TLS Service Profile
SCEP
SSL Decryption Exclusion
Device Certificates
Default Trusted Certificate Authorities
NAME
SUBJECT
ISSUER
CA
K...
EXPIRES
untrusted cert
CN = DangerWillRobInson. emailAddress = incid...
CN = DangerWillRobInson. emailAddress = incident...
Jan 20 20:5
Delete
Revoke
Renew
Import
Generate
Export Certificate
Import HA Key
Export HA Key
PDF/CSV
reaper I Logout I Last Login Time: 01/09/2022 01:30:47 I Session Expire Time: 02/09/2022 23:28:21 |

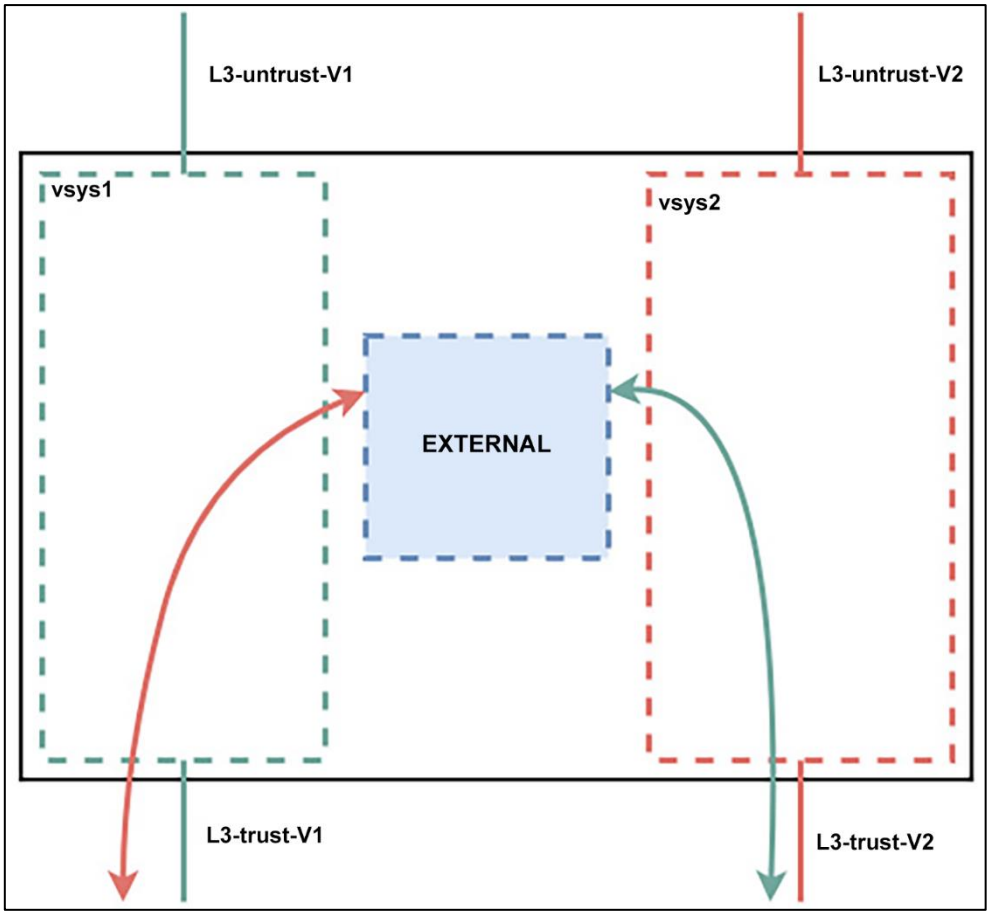

General
HA Communications
Link and Path Monitoring
Control Links
HA1
HA1 Bac
Port ethernet1/5
IPv4/1Pv6 Address 172.16.0.1
Edit
HA1
Port
ethernet1/5
IPv4/1Pv6 Address
172.16.0.1
Netmask
255.255.255.252
Gateway
Data
HA
Encryption Enabled
Monitor Hold Time (ms)
3000
OK
Cancel


Multi Virtual System Capability Change
You are switching the multi virtual system capability. This will trigger a commit. Do you want to continue?
Yes
No
Cancel





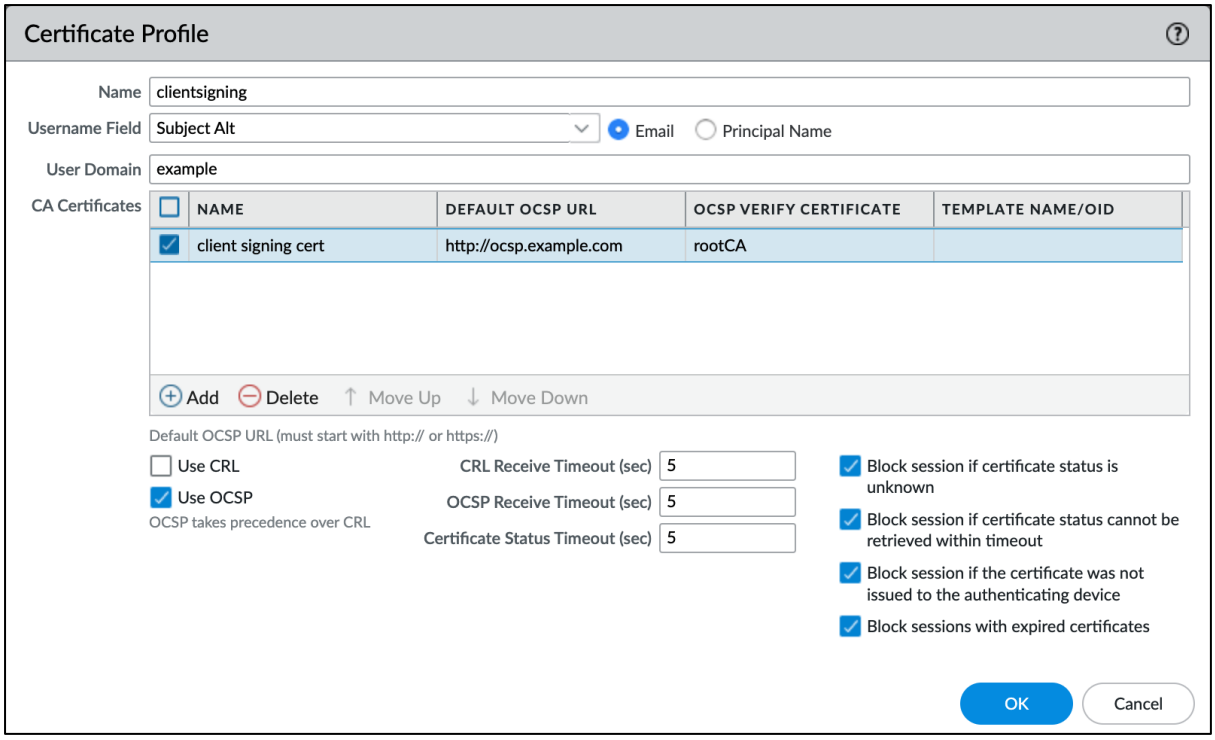
Interface	Interface Type	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Virtual System	Security Zone
ethernet1/1	Layer3		198.51.100.2/24	default	Untagged	none	vsys1	L3-untrust-V1
ethernet1/2	Layer3		10.0.0.0/24	default	Untagged	none	vsys1	L3-trust-V1
ethernet1/7	Layer3		198.51.100.6/24	v2-default	Untagged	none	Beta environment	L3-untrust-V2
ethernet1/8	Layer3		10.1.0.0/24	v2-default	Untagged	none	Beta environment	L3-trust-V2

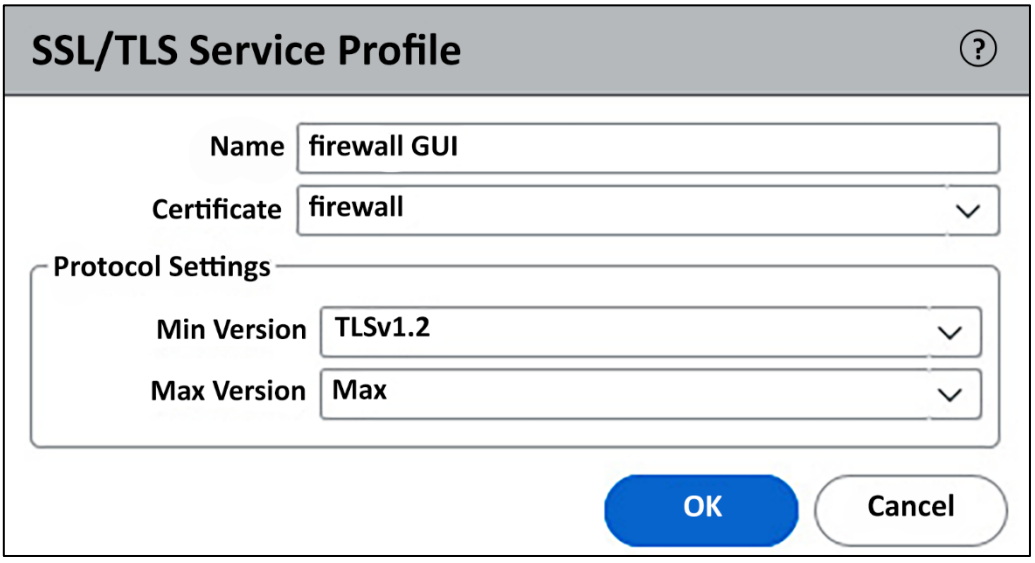


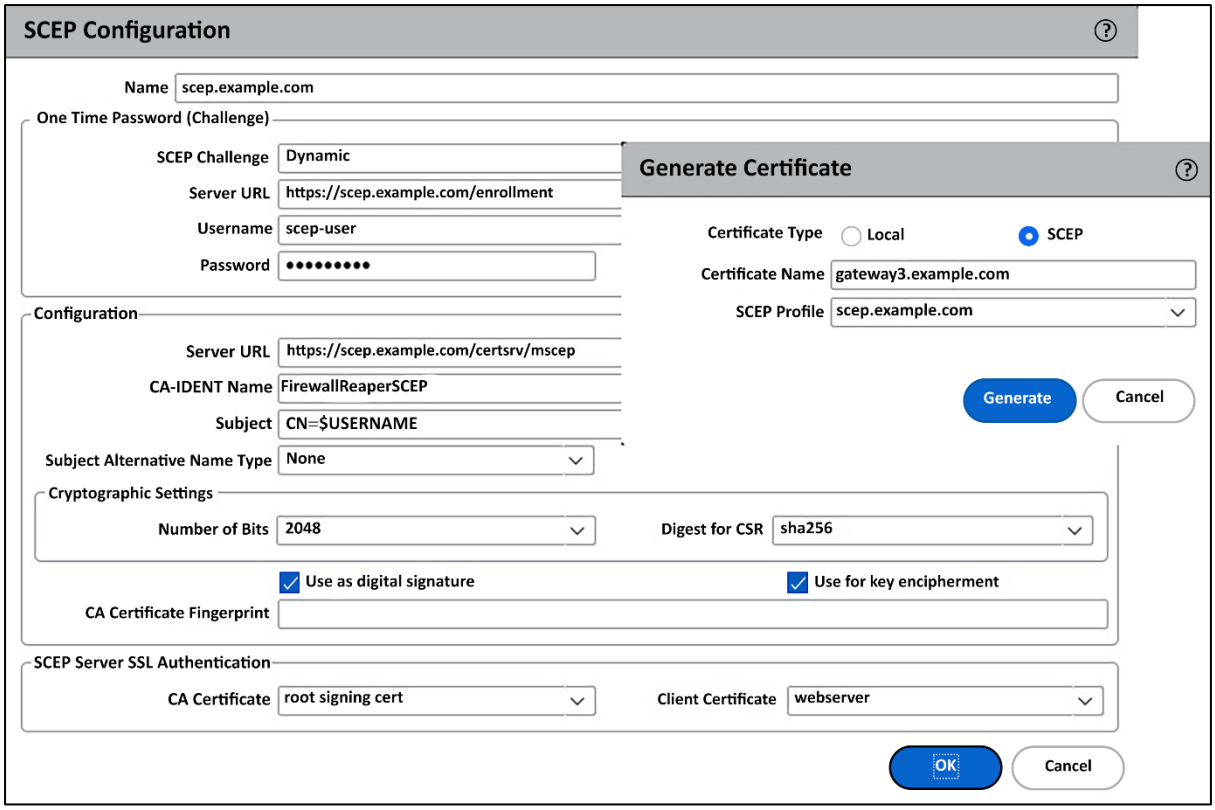
Device Certificates | Default Trusted Certificate Authorities

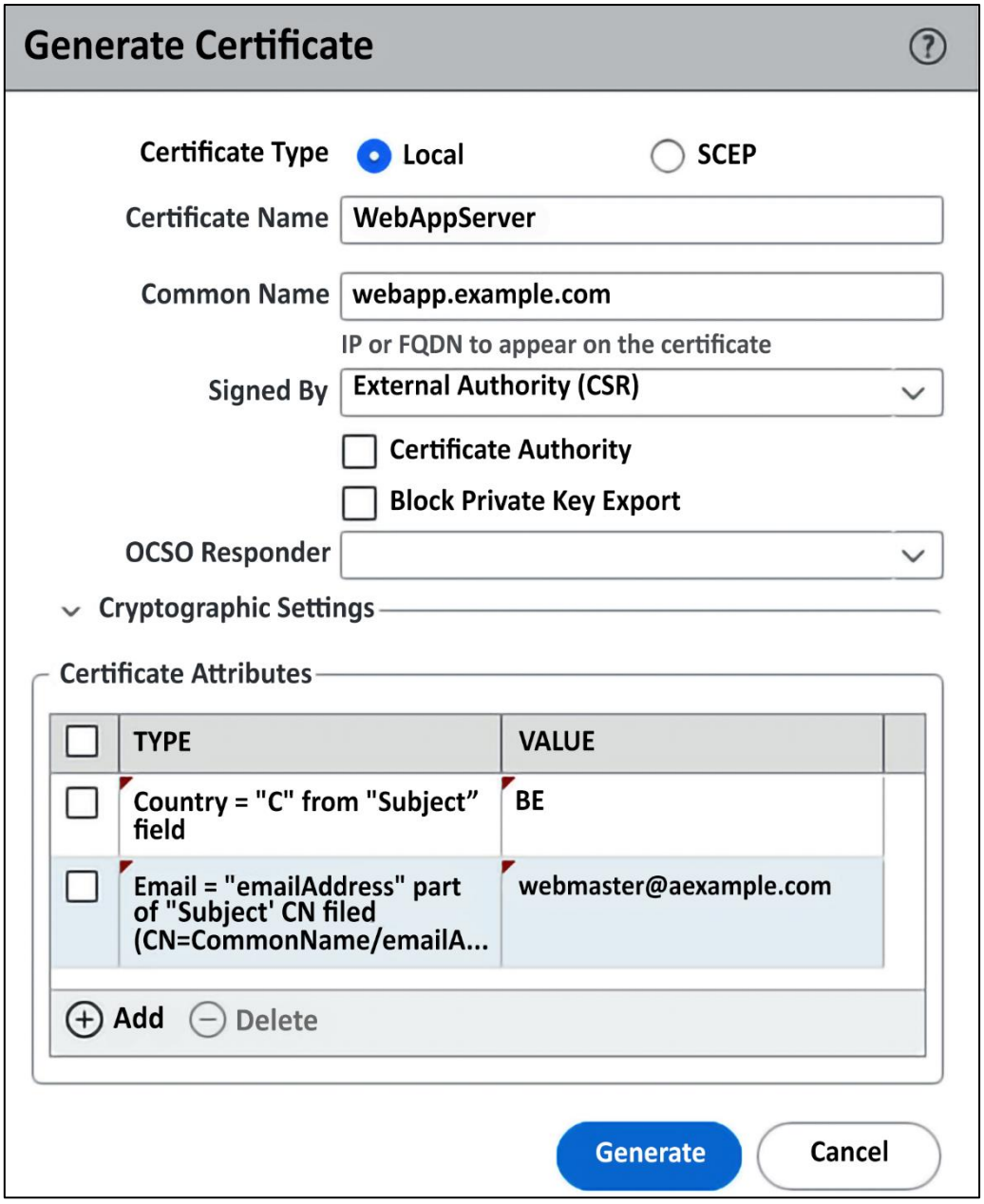
15 items

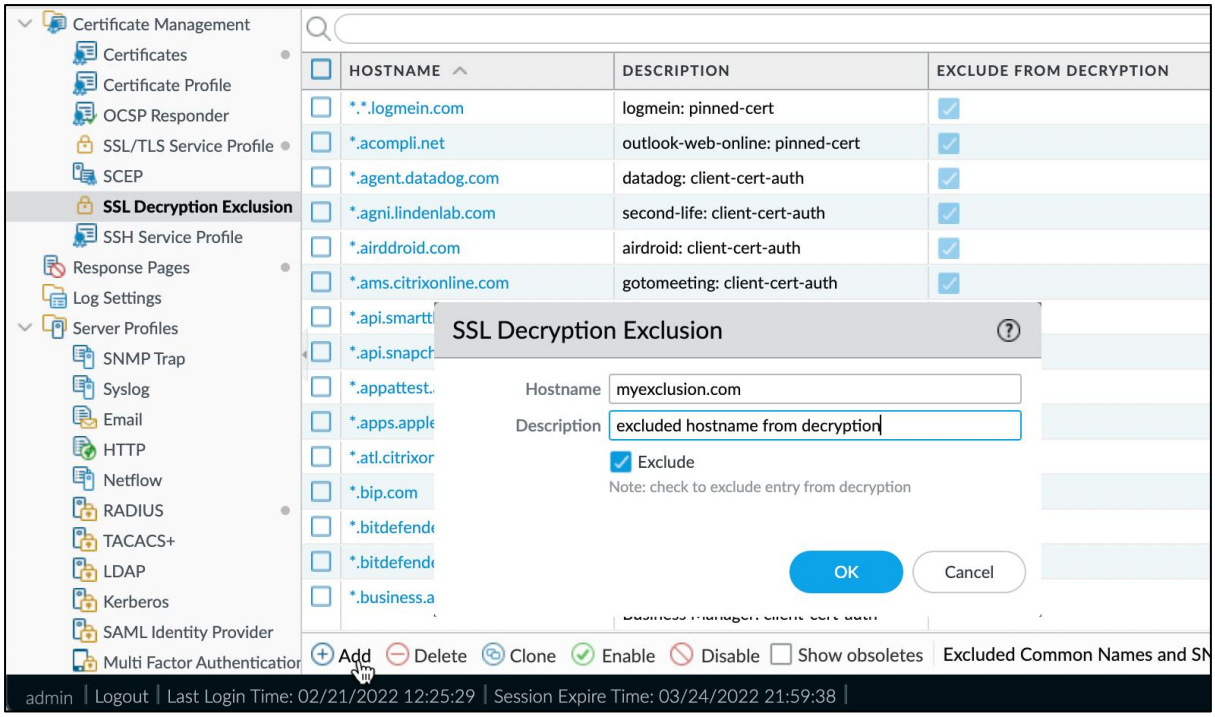
NAME	EXPIRES	SUBJECT	ISSUER	CA	K...	USAGE
root signing cert	Jan 20 20:50:19 2021 GMT	C = BE, O = example.com, CN = ro...	C = BE, O = example.co...	☑	☑	Trusted Root CA Certificate
decryption subordinate	Jan 20 20:52:59 2021 GMT	C = BE, O = example.com, CN = de...	C = BE, O = example.co...	☑	☑	Forward Trust Certificate
portal	Apr 16 21:10:19 2021 GMT	CN = portal.example.com	C = BE, O = example.co...	☐	☑	
captiveportal	May 1 23:24:32 2021 GMT	CN = captiveportal.pangurus.com	C = BE, O = example.co...	☐	☑	
gateway	Jun 24 22:35:47 2021 GMT	CN = gateway.example.com	C = BE, O = example.co...	☐	☑	
webserver	Jun 24 22:37:12 2021 GMT	C = BE, CN = www.example.com, e...	C = BE, O = example.co...	☐	☑	
firewall	Jun 24 22:37:35 2021 GMT	CN = firewall.example.com	C = BE, O = example.co...	☐	☑	
untrusted cert	Jan 20 20:57:29 2021 GMT	CN = DangerWIIIRobinson, emailA...	CN = DangerWillRobins...	☑	☑	Forward Untrust Certificate


Certificate Profile
Name
clientsigning
Username Field
Subject Alt
Email
Principal Name
User Domain
example
CA Certificates
NAME
DEFAULT OCSP URL
OCSP VERIFY CERTIFICATE
TEMPLATE NAME/OID
client signing cert
http://ocsp.example.com
rootCA
Add
Delete
Move Up
Move Down
Default OCSP URL (must start with http:// or https://)
Use CRL
Use OCSP
OCSP takes precedence over CRL
CRL Receive Timeout (sec)
5
OCSP Receive Timeout (sec)
5
Certificate Status Timeout (sec)
5
Block session if certificate status is unknown
Block session if certificate status cannot be retrieved within timeout
Block session if the certificate was not issued to the authenticating device
Block sessions with expired certificates
OK
Cancel

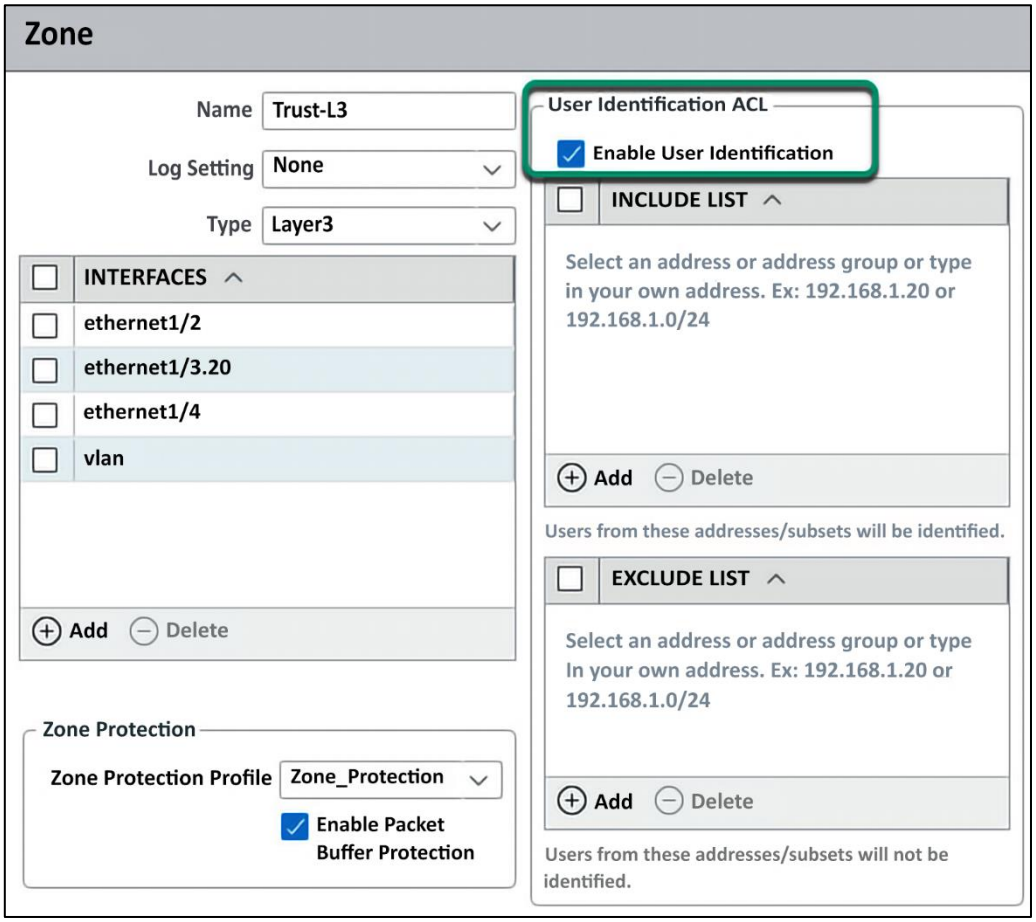

SSL/TLS Service Profile
Name
firewall GUI
Certificate
firewall
Protocol Settings
Min Version
TLSv1.2
Max Version
Max
OK
Cancel

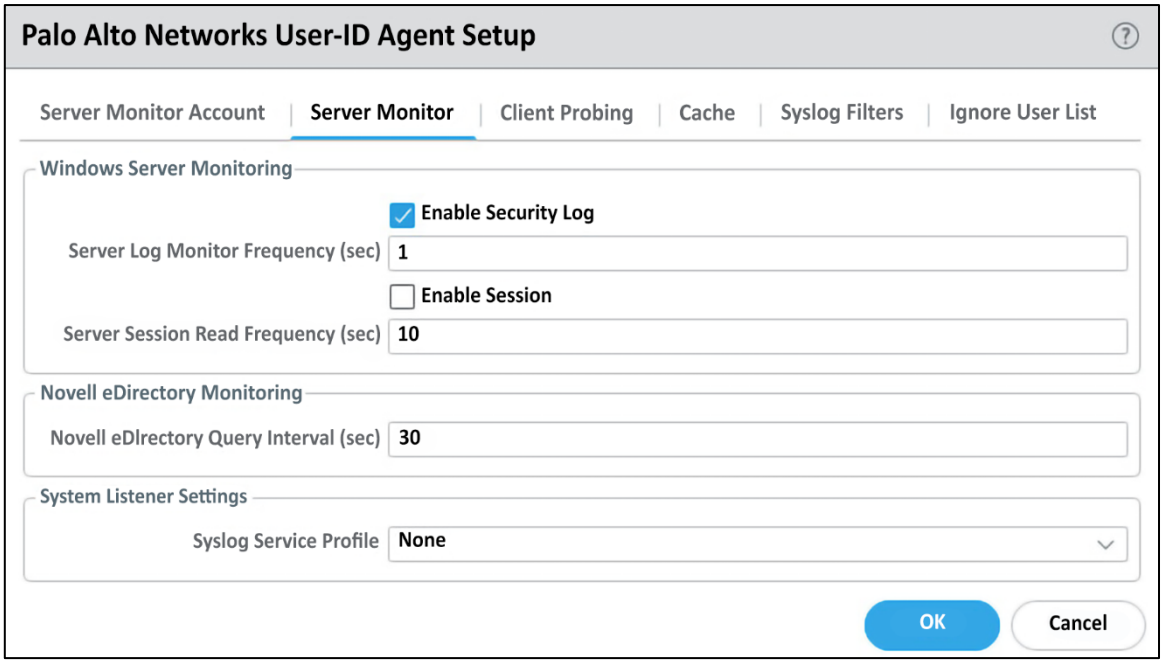

SCEP Configuration
Name
scep.example.com
One Time Password (Challenge)
SCEP Challenge
Dynamic
Server URL
https://scep.example.com/enrollment
Username
scep-user
Password
Configuration
Server URL
https://scep.example.com/certsrv/mscep
CA-IDENT Name
FirewallReaperSCEP
Subject
CN=$USERNAME
Subject Alternative Name Type
None
Cryptographic Settings
Number of Bits
2048
Digest for CSR
sha256
Use as digital signature
Use for key encipherment
CA Certificate Fingerprint
SCEP Server SSL Authentication
CA Certificate
root signing cert
Client Certificate
webserver
OK
Cancel
Generate Certificate
Certificate Type
Local
SCEP
Certificate Name
gateway3.example.com
SCEP Profile
scep.example.com
Generate
Cancel

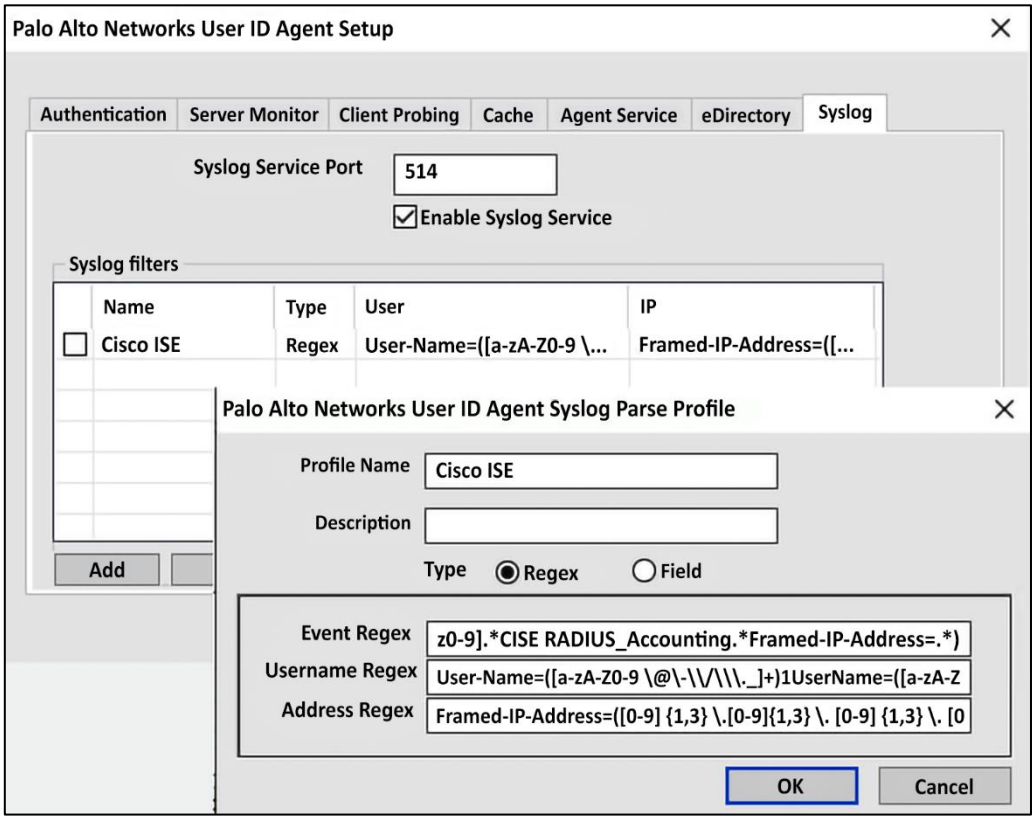

Generate Certificate
Certificate Type
Local
SCEP
Certificate Name
WebAppServer
Common Name
webapp.example.com
IP or FQDN to appear on the certificate
Signed By
External Authority (CSR)
Certificate Authority
Block Private Key Export
OCSO Responder
Cryptographic Settings
Certificate Attributes
TYPE
VALUE
Country = "C" from "Subject" field
BE
Email = "emailAddress" part of "Subject' CN filed (CN=CommonName/emailA...
webmaster@aexample.com
Add
Delete
Generate
Cancel

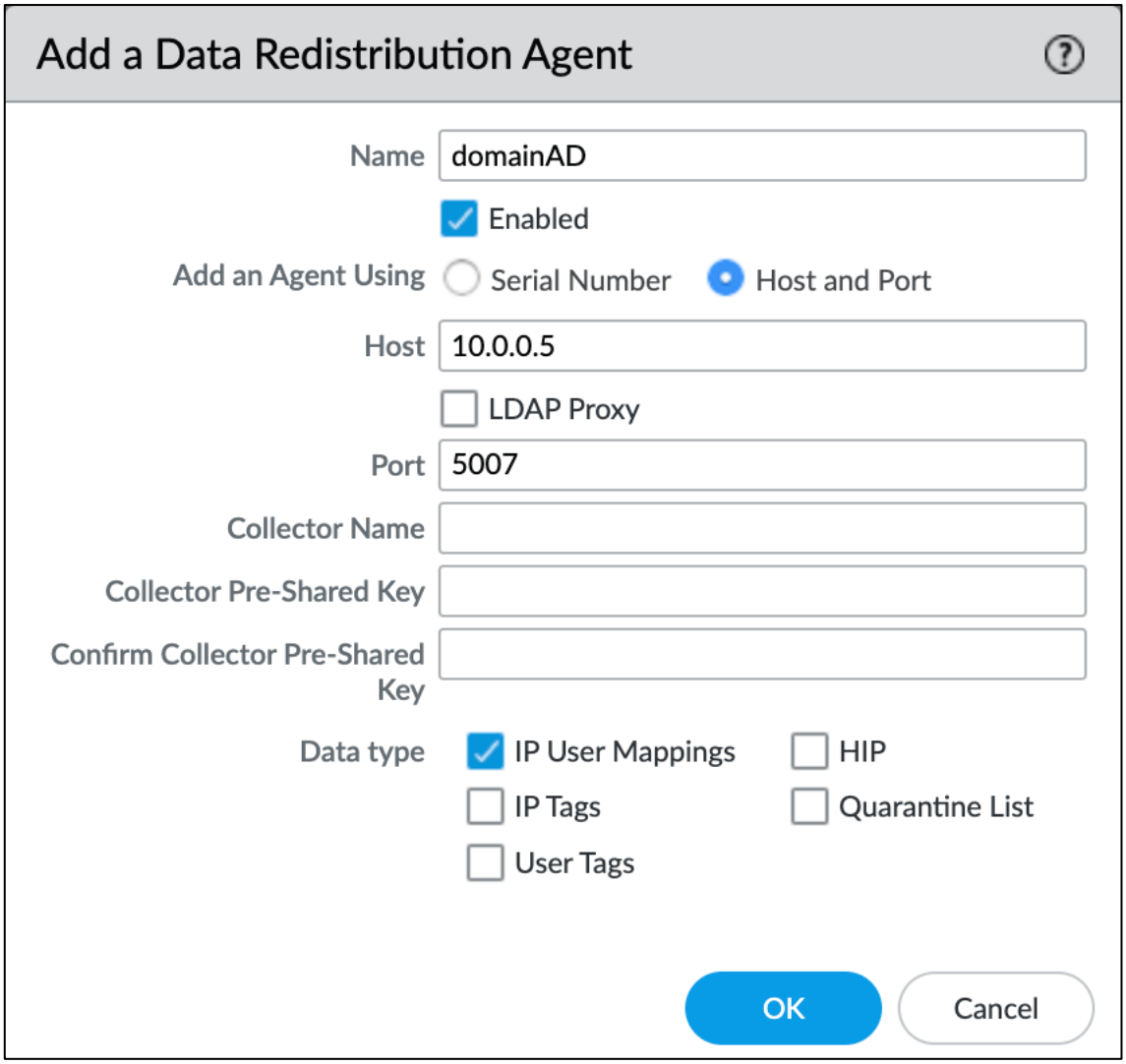


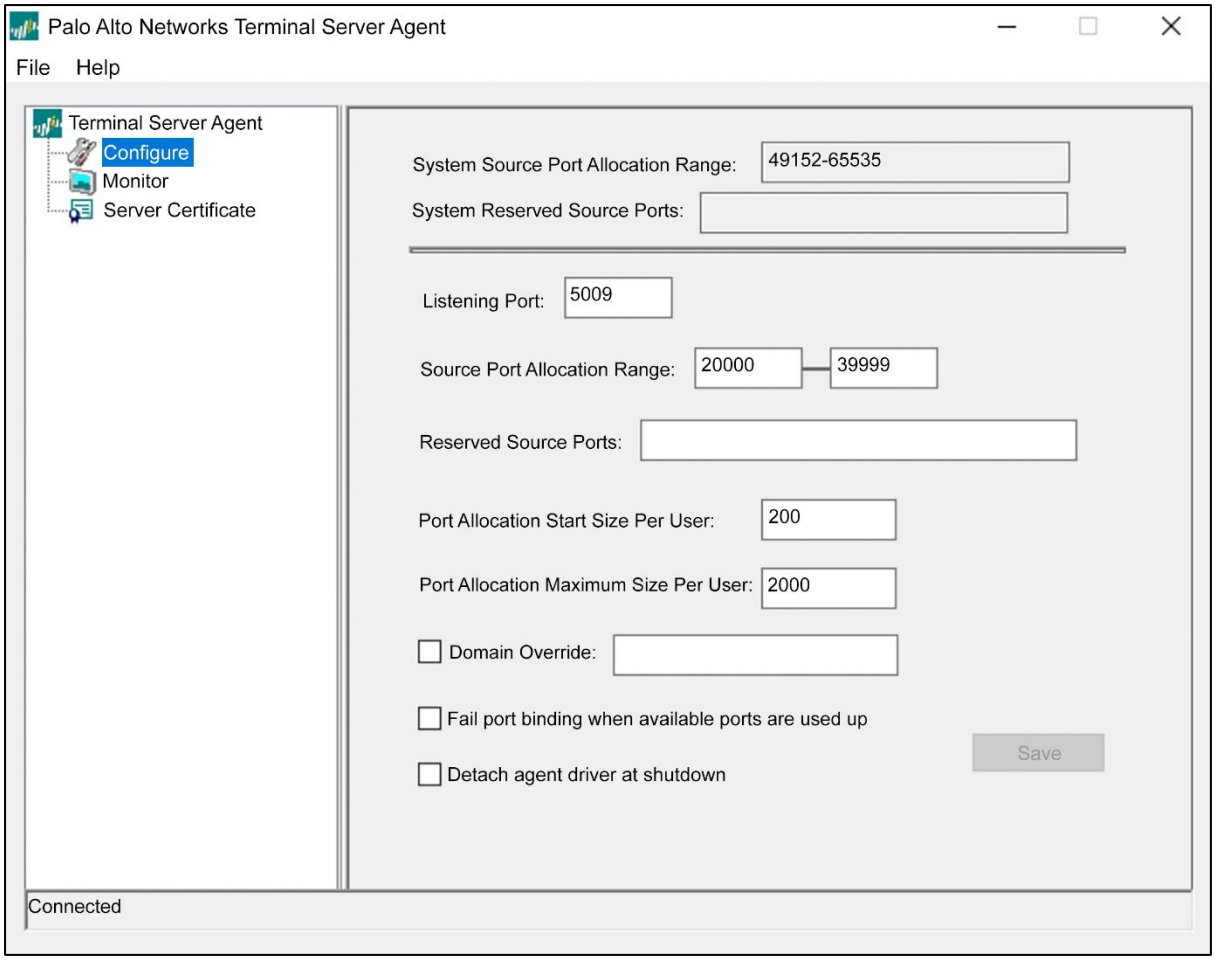
Chapter 6: Identifying Users and Controlling Access

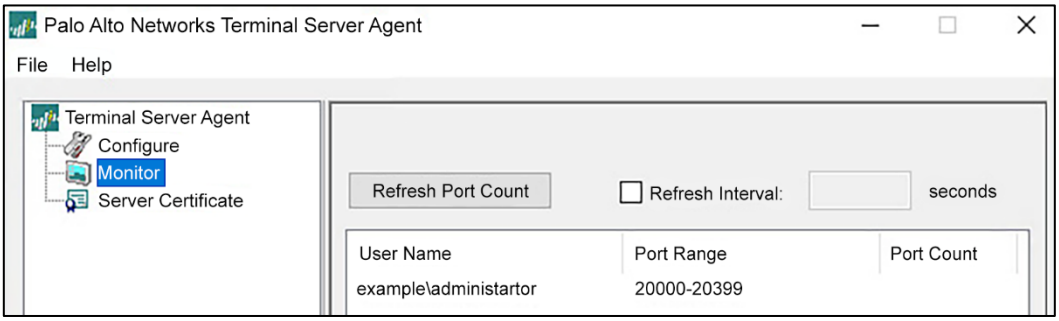


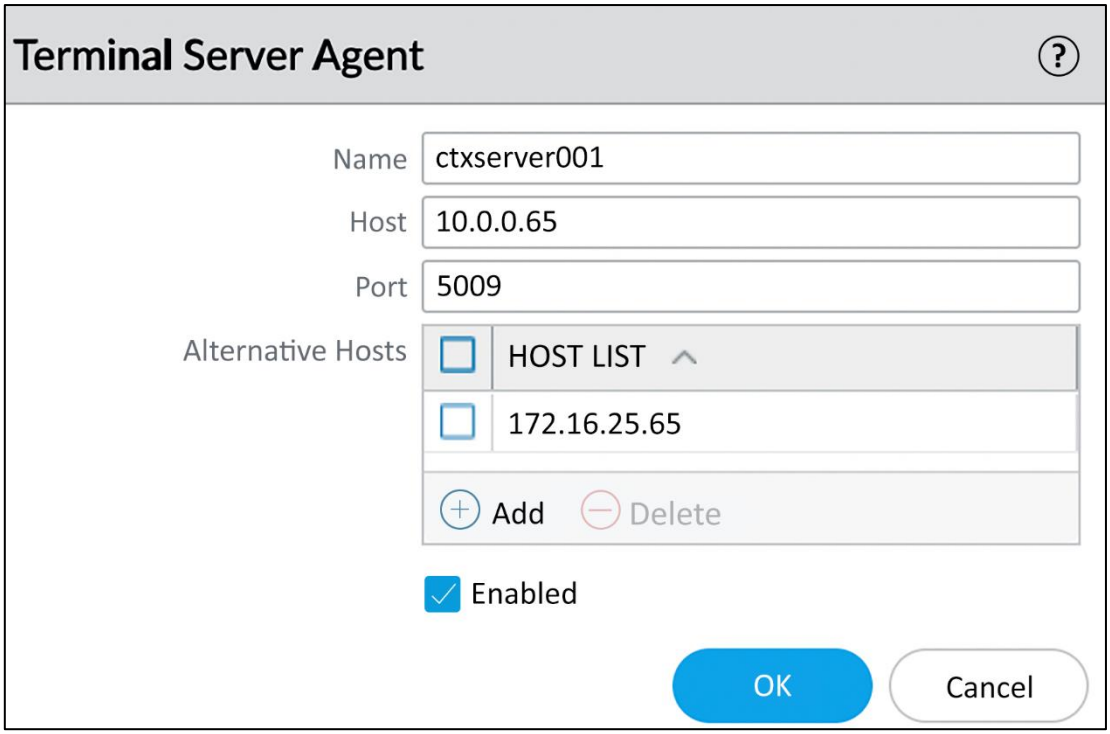

Palo Alto Networks User-ID Agent Setup
Server Monitor Account
Server Monitor
Client Probing
Cache
Syslog Filters
Ignore User List
Windows Server Monitoring
Enable Security Log
Server Log Monitor Frequency (sec)
1
Enable Session
Server Session Read Frequency (sec)
10
Novell eDirectory Monitoring
Novell eDIrectory Query Interval (sec)
30
System Listener Settings
Syslog Service Profile
None
OK
Cancel

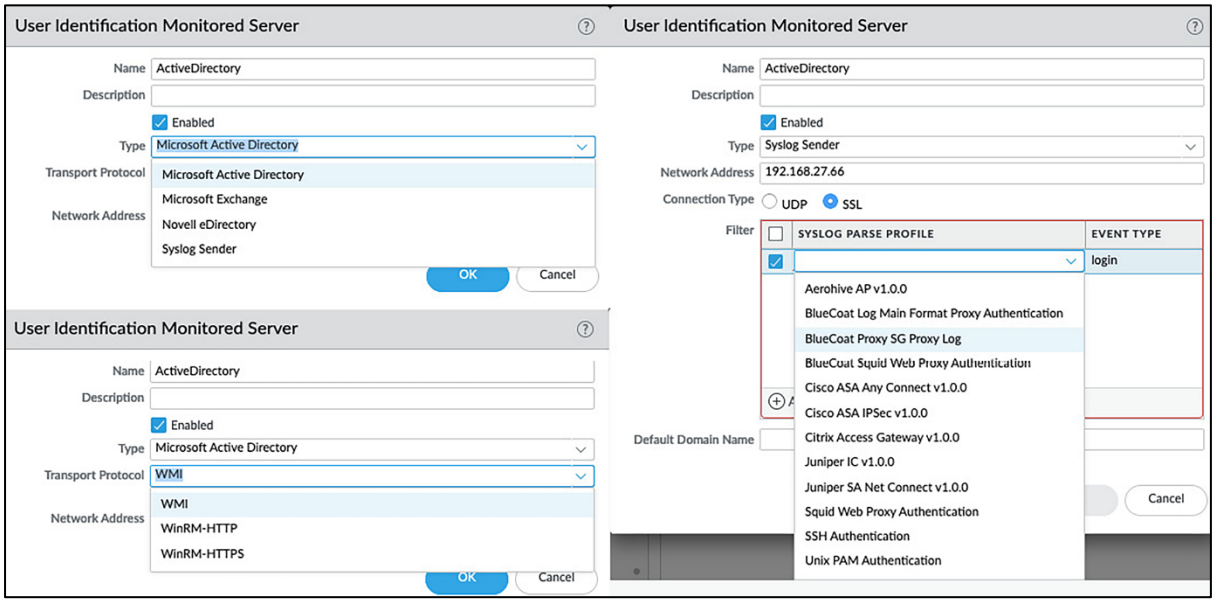

Palo Alto Networks User ID Agent Setup
Authentication
Server Monitor
Client Probing
Cache
Agent Service
eDirectory
Syslog
Syslog Service Port
514
Enable Syslog Service
Syslog filters
Name
Type
User
IP
Cisco ISE
Regex
User-Name=([a-zA-Z0-9 \...
Framed-IP-Address=([...
Add
Palo Alto Networks User ID Agent Syslog Parse Profile
Profile Name
Cisco ISE
Description
Type
Regex
Field
Event Regex
z0-9].*CISE RADIUS_Accounting.*Framed-IP-Address=.*)
Username Regex
User-Name=([a-zA-Z0-9 \@\-\\/\\\._]+)1UserName=([a-zA-Z
Address Regex
Framed-IP-Address=([0-9] {1,3} \.[0-9]{1,3} \. [0-9] {1,3} \. [0
OK
Cancel

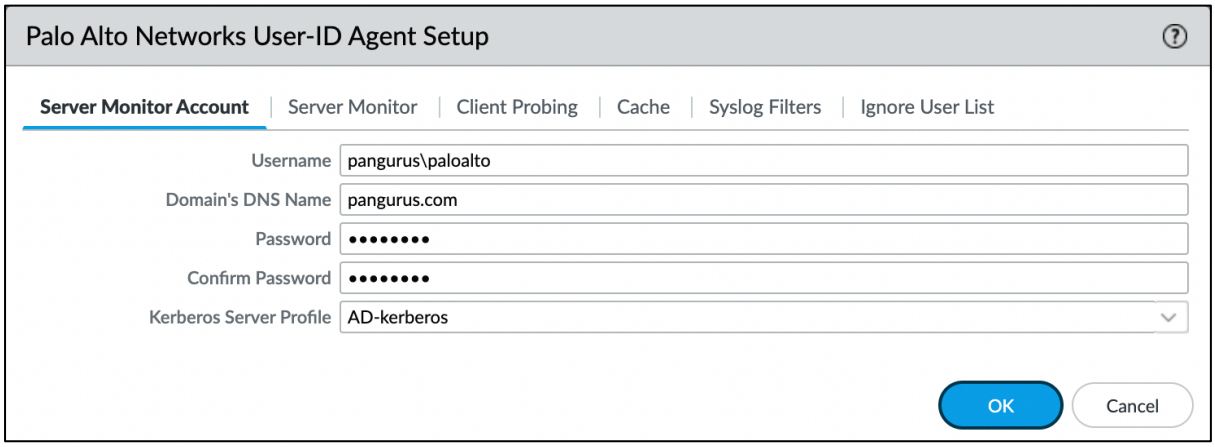

Add a Data Redistribution Agent
Name
domainAD
Enabled
Add an Agent Using
Serial Number
Host and Port
Host
10.0.0.5
LDAP Proxy
Port
5007
Collector Name
Collector Pre-Shared Key
Confirm Collector Pre-Shared Key
Data type
IP User Mappings
HIP
IP Tags
Quarantine List
User Tags
OK
Cancel

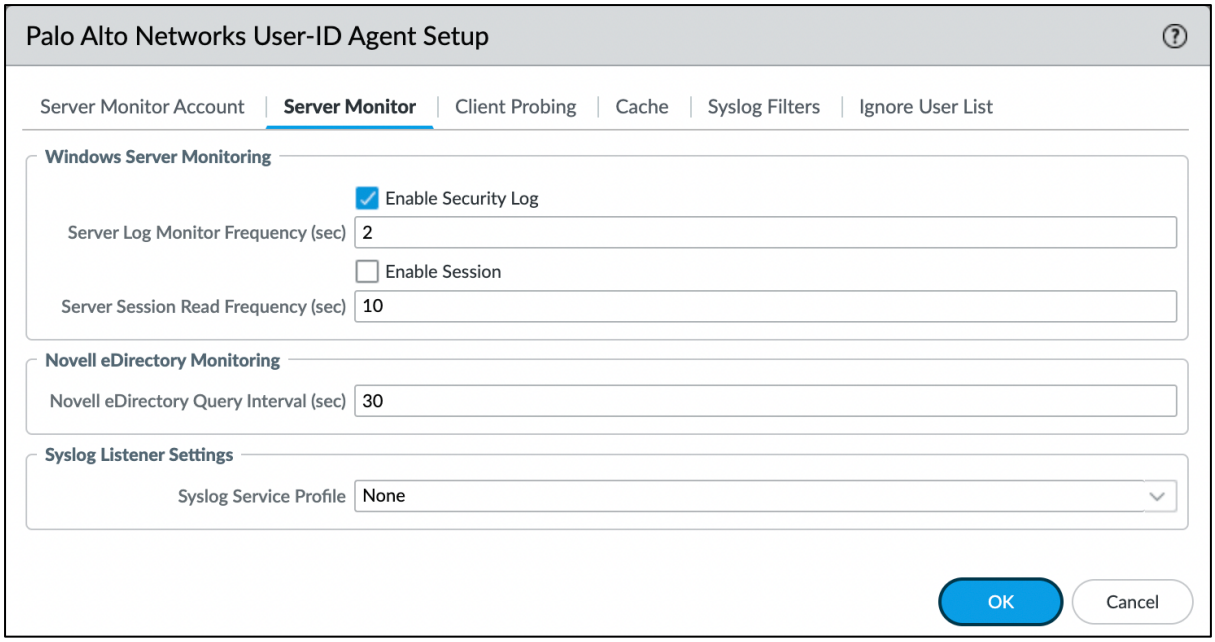

Palo Alto Networks Terminal Server Agent
File
Help
Terminal Server Agent
Configure
Monitor
Server Certificate
System Source Port Allocation Range:
49152-65535
System Reserved Source Ports:
Listening Port:
5009
Source Port Allocation Range:
20000
39999
Reserved Source Ports:
Port Allocation Start Size Per User:
200
Port Allocation Maximum Size Per User:
2000
Domain Override:
Fail port binding when available ports are used up
Detach agent driver at shutdown
Save
Connected

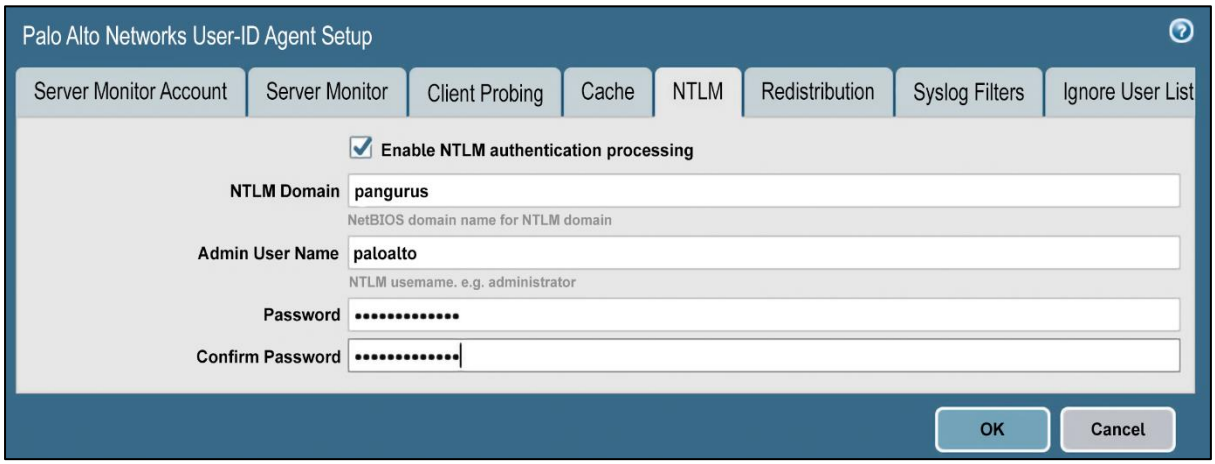

Palo Alto Networks Terminal Server Agent
File
Help
Terminal Server Agent
Configure
Monitor
Server Certificate
Refresh Port Count
Refresh Interval:
seconds
User Name
Port Range
Port Count
example\administartor
20000-20399

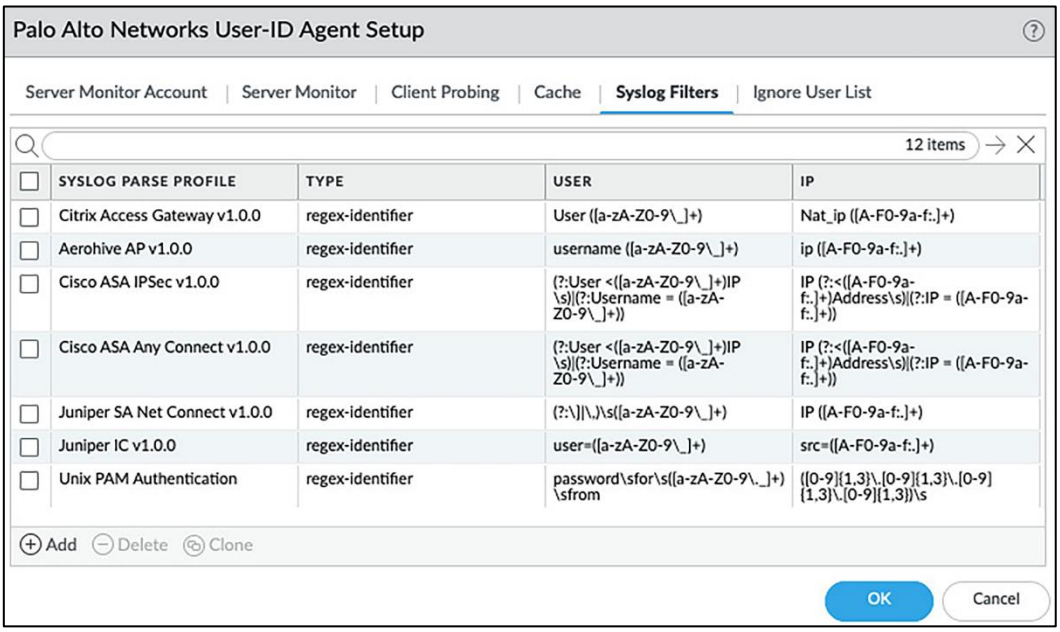

Terminal Server Agent
Name
ctxserver001
Host
10.0.0.65
Port
5009
Alternative Hosts
HOST LIST
172.16.25.65
Add
Delete
Enabled
OK
Cancel

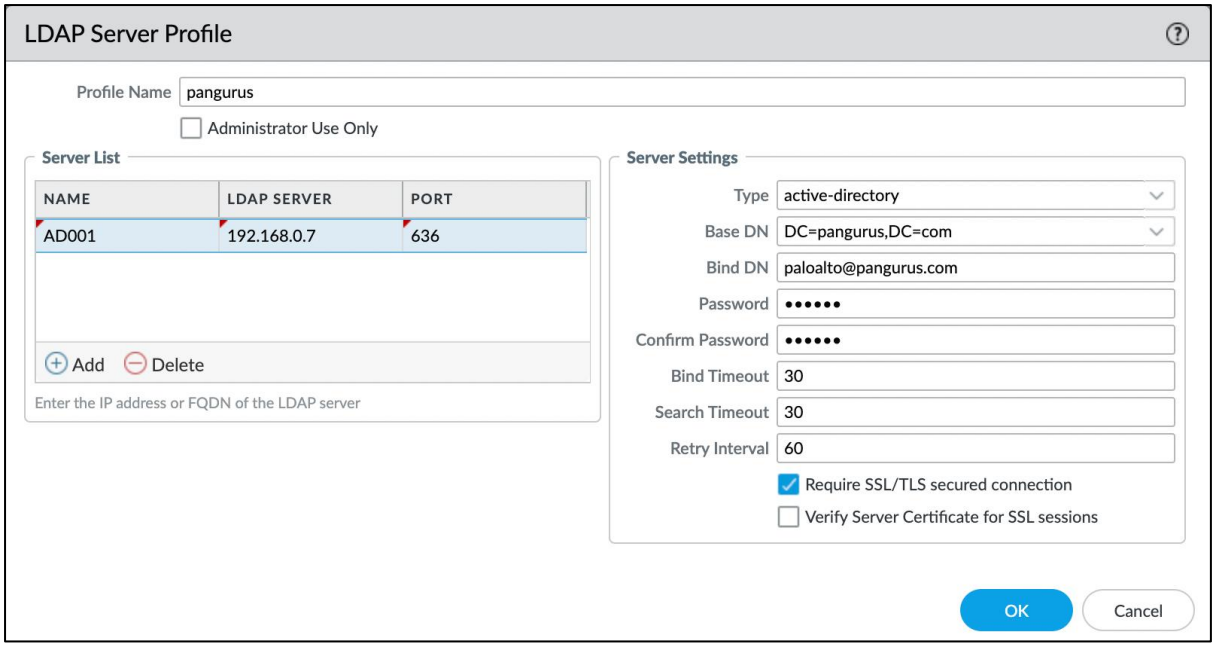

User Identification Monitored Server
Name
ActiveDirectory
Description
Enabled
Type
Microsoft Active Directory
Transport Protocol
Network Address
Microsoft Active Directory
Microsoft Exchange
Novell eDirectory
Syslog Sender
OK
Cancel
User Identification Monitored Server
Name
ActiveDirectory
Description
Enabled
Type
Microsoft Active Directory
Transport Protocol
WMI
Network Address
WMI
WinRM-HTTP
WinRM-HTTPS
OK
Cancel
User Identification Monitored Server
Name
ActiveDirectory
Description
Enabled
Type
Syslog Sender
Network Address
192.168.27.66
Connection Type
UDP
SSL
Filter
SYSLOG PARSE PROFILE
EVENT TYPE
login
Aerohive AP v1.0.0
BlueCoat Log Main Format Proxy Authentication
BlueCoat Proxy SG Proxy Log
BlueCoat Squid Web Proxy Authentication
Cisco ASA Any Connect v1.0.0
Cisco ASA IPSec v1.0.0
Citrix Access Gateway v1.0.0
Juniper IC v1.0.0
Juniper SA Net Connect v1.0.0
Squid Web Proxy Authentication
SSH Authentication
Unix PAM Authentication
Default Domain Name
Cancel

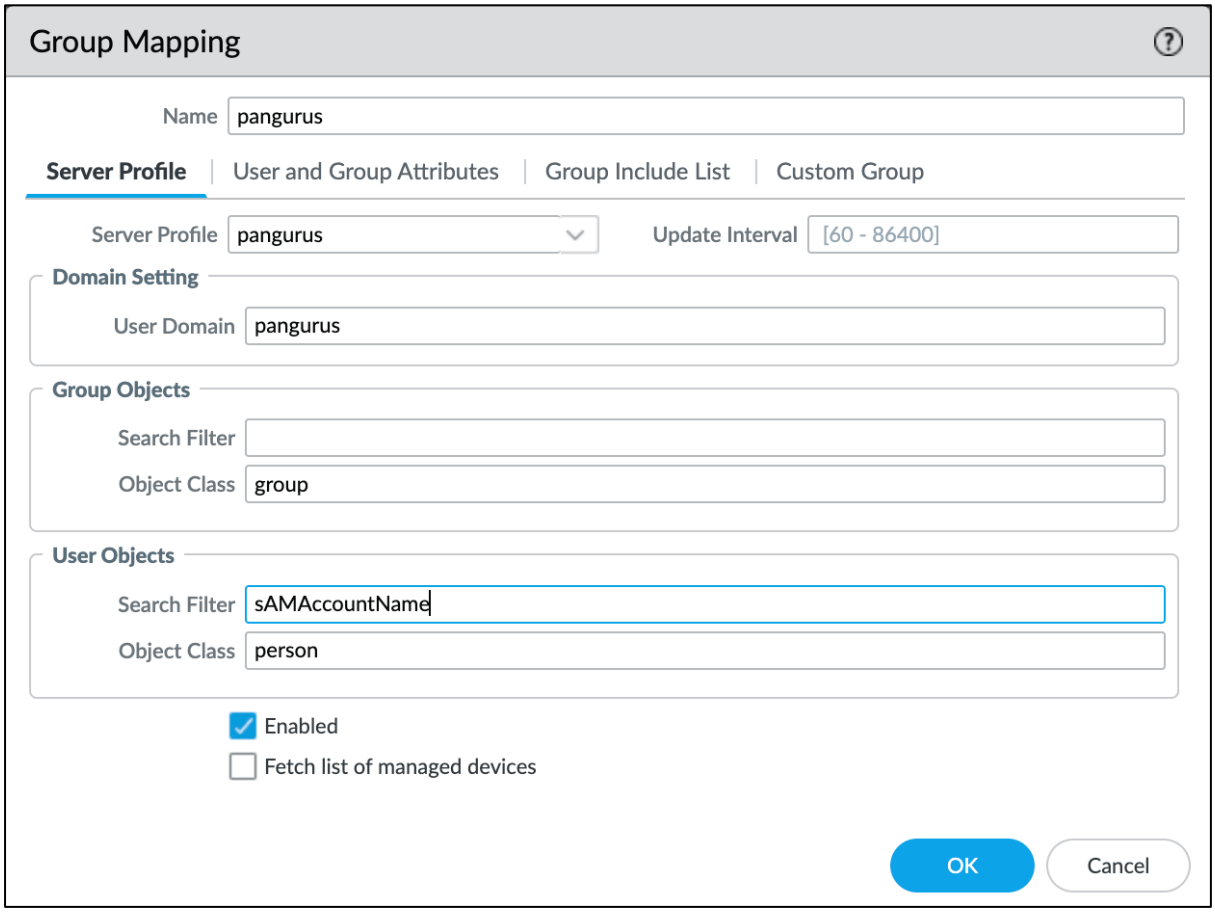

Palo Alto Networks User-ID Agent Setup
Server Monitor Account
Server Monitor
Client Probing
Cache
Syslog Filters
Ignore User List
Username
pangurus\paloalto
Domain's DNS Name
pangurus.com
Password
Confirm Password
Kerberos Server Profile
AD-kerberos
OK
Cancel

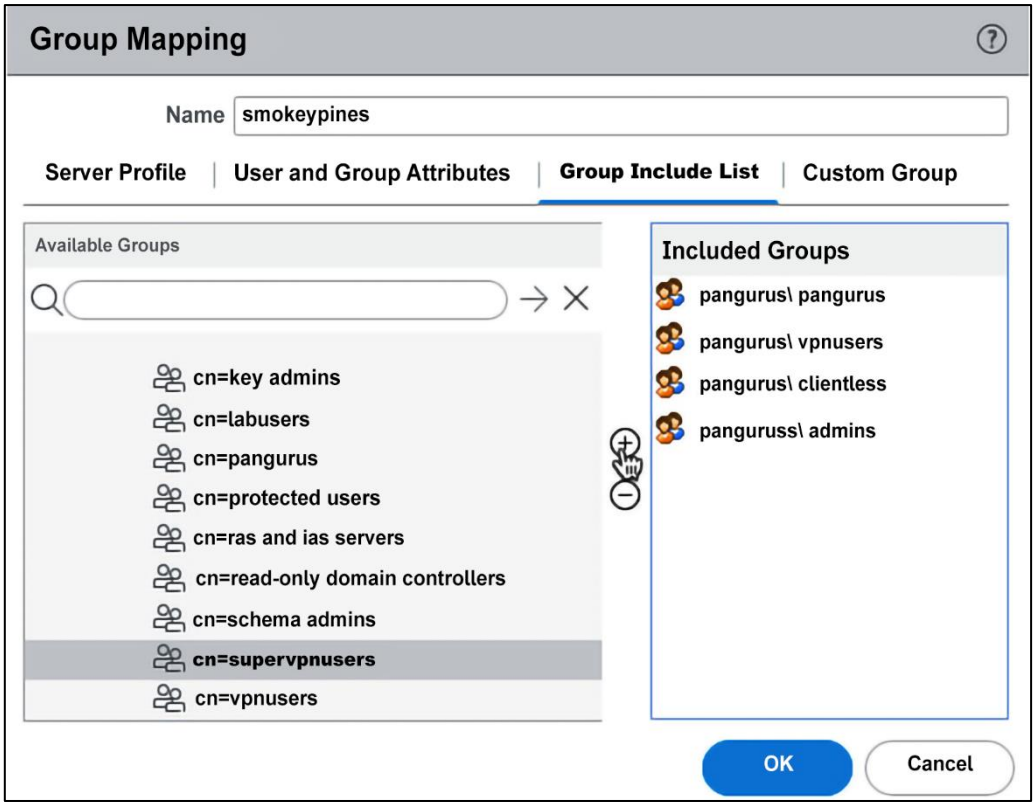

Palo Alto Networks User-ID Agent Setup
Server Monitor Account
Server Monitor
Client Probing
Cache
Syslog Filters
Ignore User List
Windows Server Monitoring
Enable Security Log
Server Log Monitor Frequency (sec)
2
Enable Session
Server Session Read Frequency (sec)
10
Novell eDirectory Monitoring
Novell eDirectory Query Interval (sec)
30
Syslog Listener Settings
Syslog Service Profile
None
OK
Cancel


Palo Alto Networks User-ID Agent Setup
Server Monitor Account
Server Monitor
Client Probing
Cache
NTLM
Redistribution
Syslog Filters
Ignore User List
Enable NTLM authentication processing
NTLM Domain
pangurus
NetBIOS domain name for NTLM domain
Admin User Name
paloalto
NTLM username. e.g. administrator
Password
Confirm Password
OK
Cancel

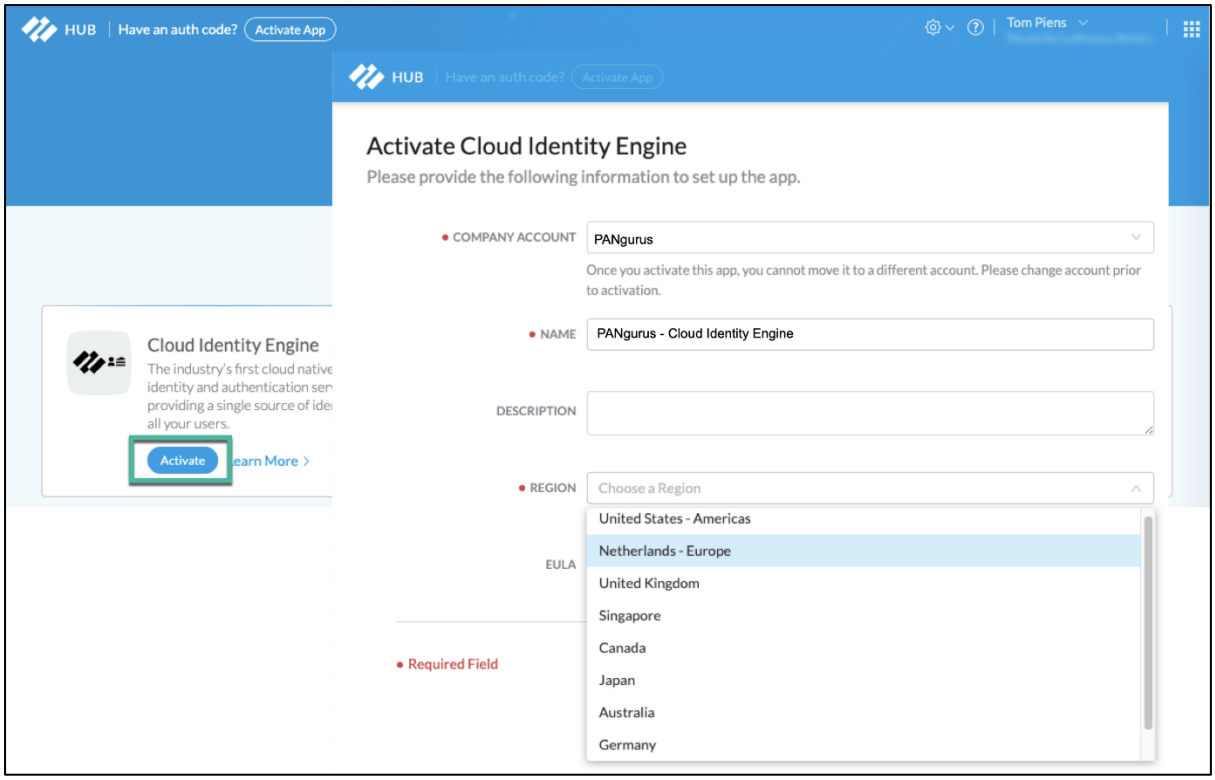

Palo Alto Networks User-ID Agent Setup
Server Monitor Account
Server Monitor
Client Probing
Cache
Syslog Filters
Ignore User List
12 items
SYSLOG PARSE PROFILE
TYPE
USER
IP
Citrix Access Gateway v1.0.0
regex-identifier
User ([a-zA-Z0-9_]+)
Nat_ip ([A-F0-9a-f:.]+)
Aerohive AP v1.0.0
regex-identifier
username ([a-zA-Z0-9_]+)
ip ([A-F0-9a-f:.]+)
Cisco ASA IPSec v1.0.0
regex-identifier
(?:User <([a-zA-Z0-9_]+)IP \s)|(?:Username = ([a-zA-Z0-9_]+))
IP (?:<([A-F0-9a-f:.]+)Address\s)|(?:IP = ([A-F0-9a-f:.]+))
Cisco ASA Any Connect v1.0.0
regex-identifier
(?:User <([a-zA-Z0-9_]+)IP \s)|(?:Username = ([a-zA-Z0-9_]+))
IP (?:<([A-F0-9a-f:.]+)Address\s)|(?:IP = ([A-F0-9a-f:.]+))
Juniper SA Net Connect v1.0.0
regex-identifier
(?:\]|\,)\s([a-zA-Z0-9_]+)
IP ([A-F0-9a-f:.]+)
Juniper IC v1.0.0
regex-identifier
user=([a-zA-Z0-9_]+)
src=([A-F0-9a-f:.]+)
Unix PAM Authentication
regex-identifier
password\sfor\s([a-zA-Z0-9\._]+)\sfrom
([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s
Add
Delete
Clone
OK
Cancel

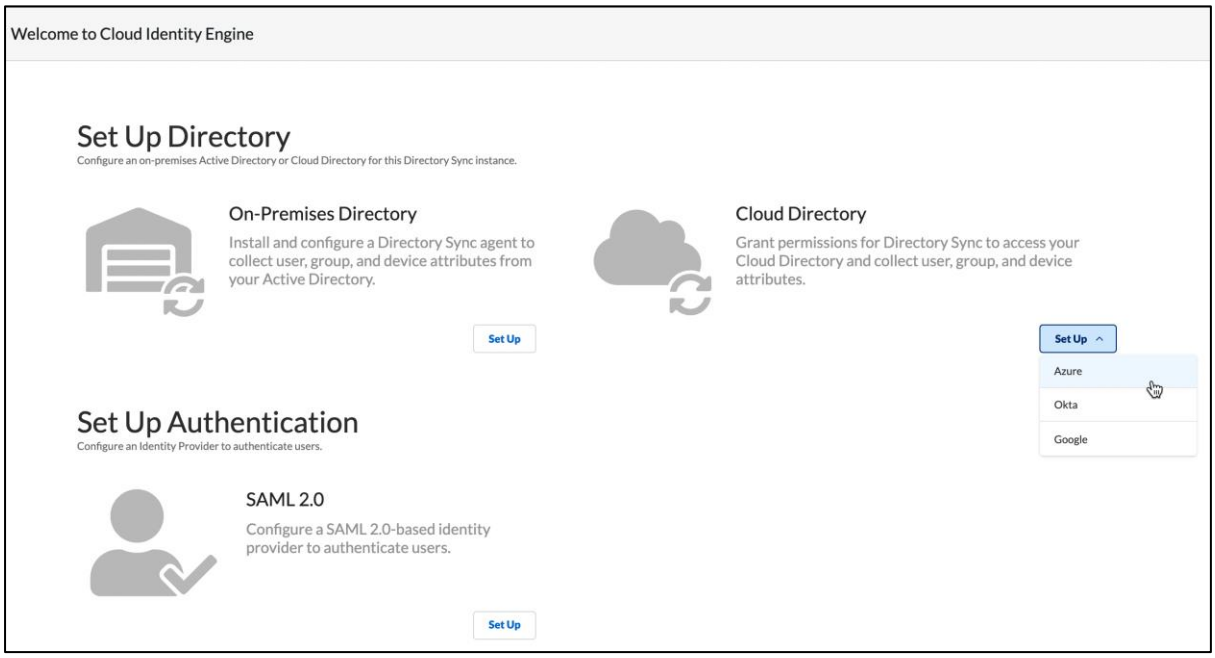

LDAP Server Profile
Profile Name
pangurus
Administrator Use Only
Server List
NAME
LDAP SERVER
PORT
AD001
192.168.0.7
636
Add
Delete
Enter the IP address or FQDN of the LDAP server
Server Settings
Type
active-directory
Base DN
DC=pangurus,DC=com
Bind DN
paloalto@pangurus.com
Password
Confirm Password
Bind Timeout
30
Search Timeout
30
Retry Interval
60
Require SSL/TLS secured connection
Verify Server Certificate for SSL sessions
OK
Cancel

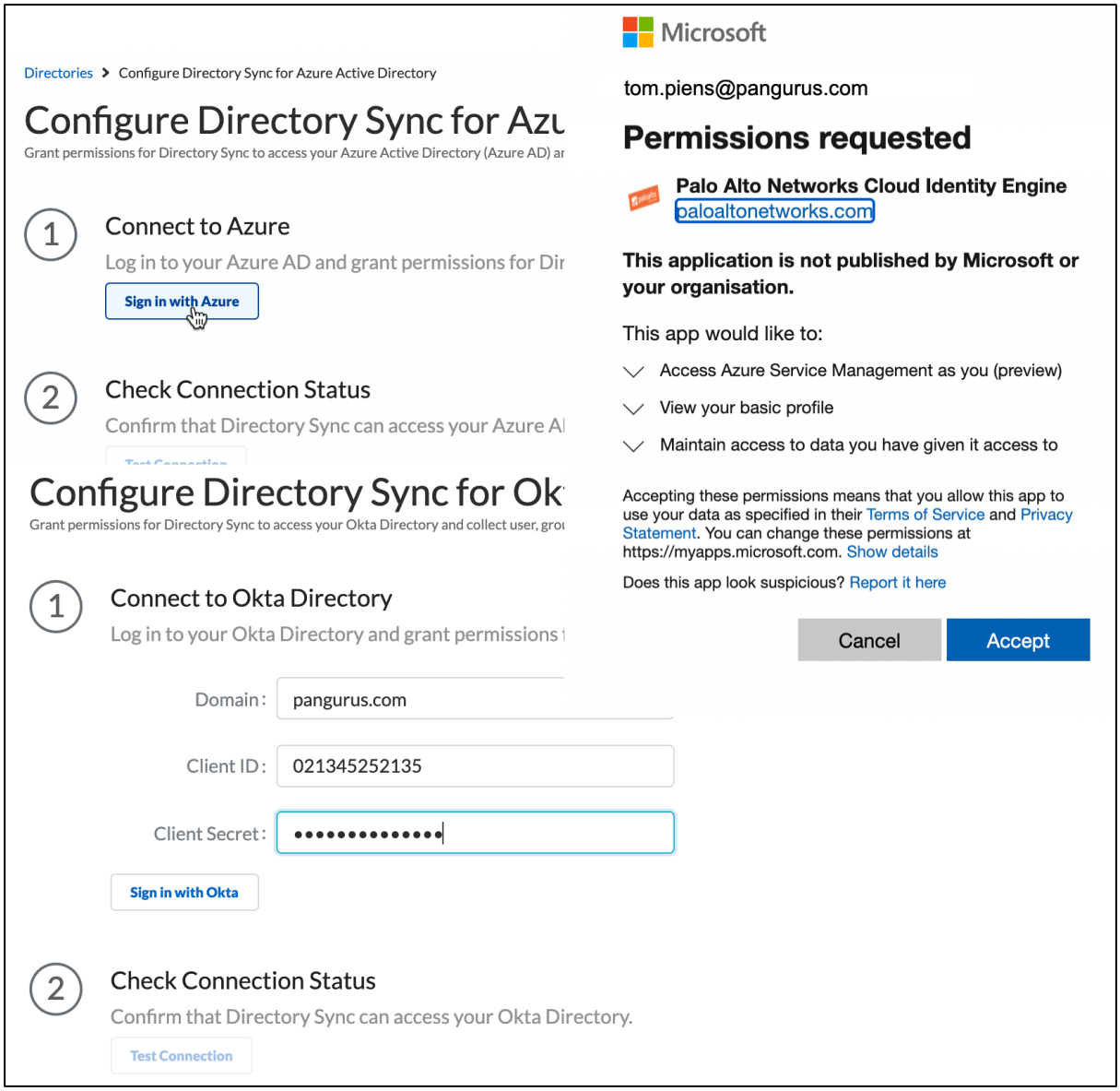

Group Mapping
Name
pangurus
Server Profile
User and Group Attributes
Group Include List
Custom Group
Server Profile
pangurus
Update Interval
[60 - 86400]
Domain Setting
User Domain
pangurus
Group Objects
Search Filter
Object Class
group
User Objects
Search Filter
sAMAccountName
Object Class
person
Enabled
Fetch list of managed devices
OK
Cancel

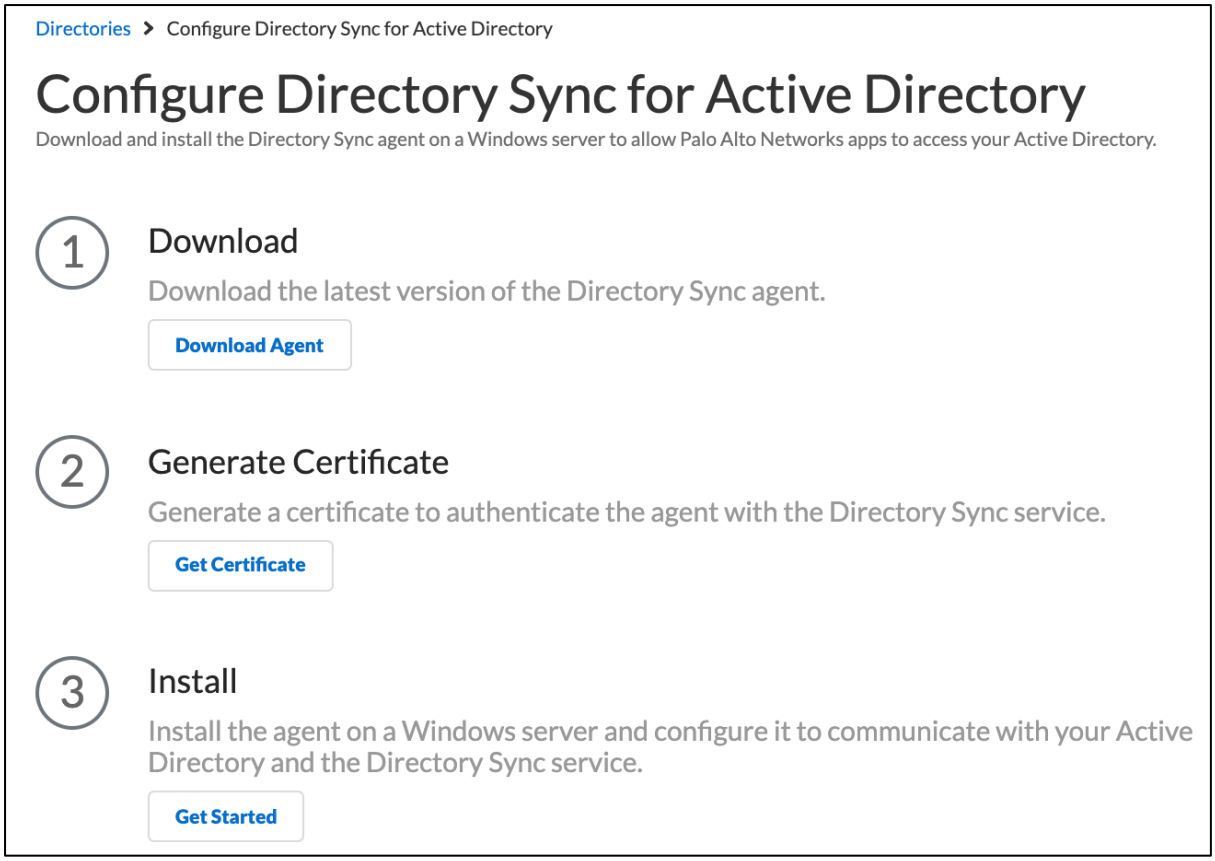


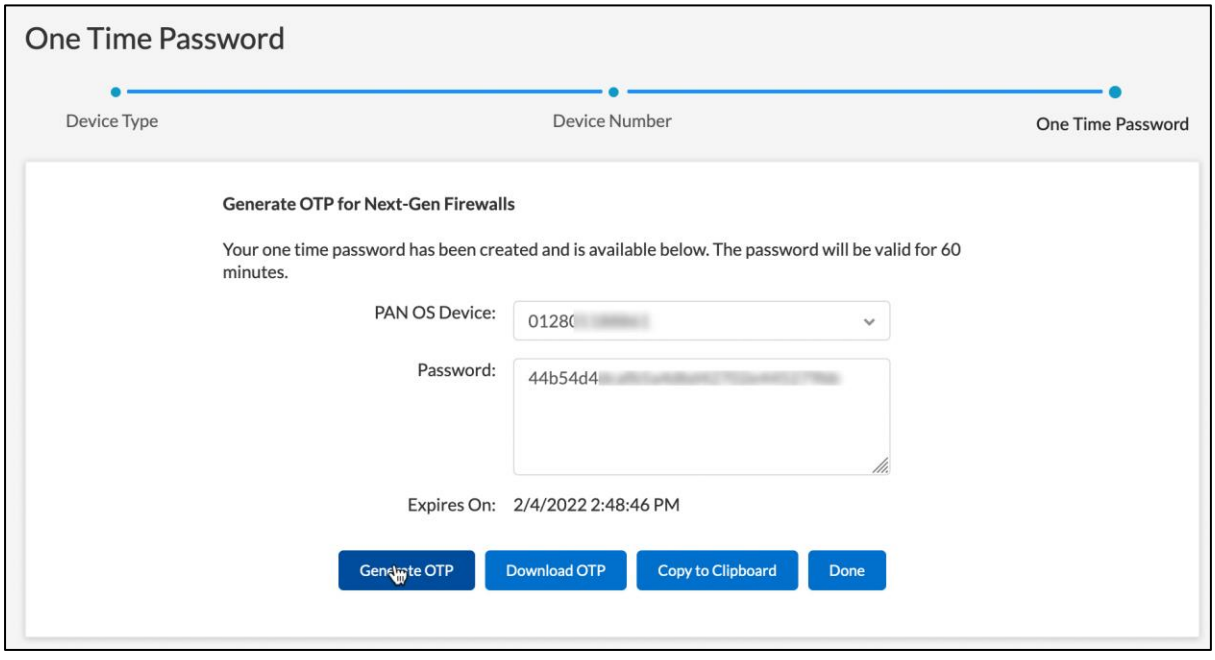
	NAME	TYPE	Source			Destination	
			ZONE	ADDRESS	USER	ZONE	ADDRESS
1	server access	universal	Trust-L3	any	pangurus-users	DMZ	servers
2	internet access users	universal	Trust-L3	any	known-user	Untrust-L3	any

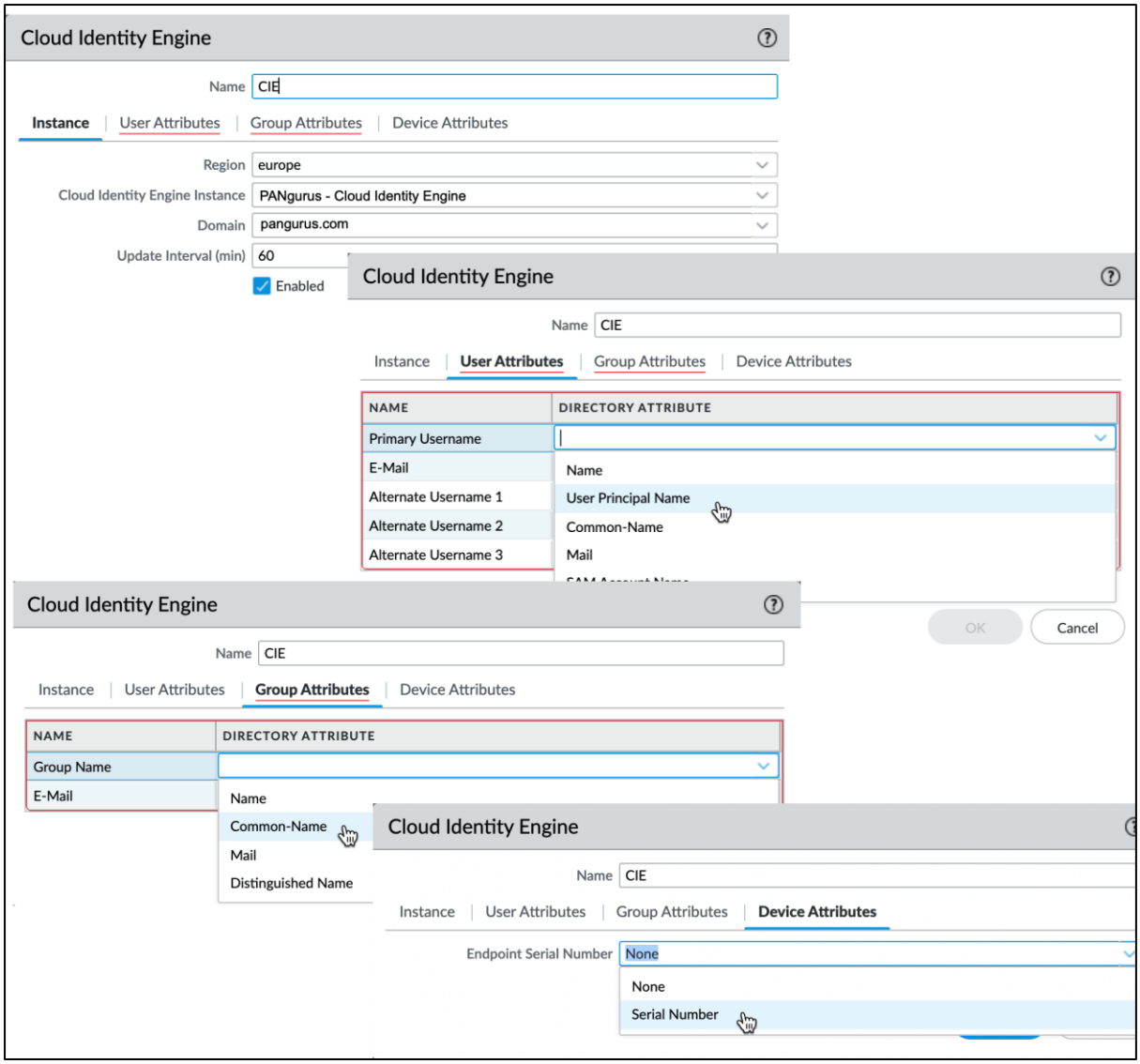

HUB
Have an auth code?
Activate App
Tom Piens
Activate Cloud Identity Engine
Please provide the following information to set up the app.
COMPANY ACCOUNT
PANgurus
Once you activate this app, you cannot move it to a different account. Please change account prior to activation.
NAME
PANgurus - Cloud Identity Engine
DESCRIPTION
REGION
Choose a Region
EULA
Required Field
Cloud Identity Engine
Activate
United States - Americas
Netherlands - Europe
United Kingdom
Singapore
Canada
Japan
Australia
Germany


Welcome to Cloud Identity Engine
Set Up Directory
Configure an on-premises Active Directory or Cloud Directory for this Directory Sync instance.
On-Premises Directory
Install and configure a Directory Sync agent to collect user, group, and device attributes from your Active Directory.
Set Up
Cloud Directory
Grant permissions for Directory Sync to access your Cloud Directory and collect user, group, and device attributes.
Set Up
Azure
Okta
Google
Set Up Authentication
Configure an Identity Provider to authenticate users.
SAML 2.0
Configure a SAML 2.0-based identity provider to authenticate users.
Set Up


Directories > Configure Directory Sync for Azure Active Directory
Configure Directory Sync for Azu
Grant permissions for Directory Sync to access your Azure Active Directory (Azure AD) ar
1
Connect to Azure
Log in to your Azure AD and grant permissions for Dir
Sign in with Azure
2
Check Connection Status
Confirm that Directory Sync can access your Azure Al
Configure Directory Sync for Ok
Grant permissions for Directory Sync to access your Okta Directory and collect user, grou
1
Connect to Okta Directory
Log in to your Okta Directory and grant permissions
Domain:
pangurus.com
Client ID:
021345252135
Client Secret:
Sign in with Okta
2
Check Connection Status
Confirm that Directory Sync can access your Okta Directory.
Test Connection
Microsoft
tom.piens@pangurus.com
Permissions requested
Palo Alto Networks Cloud Identity Engine
paloaltonetworks.com
This application is not published by Microsoft or your organisation.
This app would like to:
Access Azure Service Management as you (preview)
View your basic profile
Maintain access to data you have given it access to
Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details
Does this app look suspicious? Report it here
Cancel
Accept


Directories > Configure Directory Sync for Active Directory
Configure Directory Sync for Active Directory
Download and install the Directory Sync agent on a Windows server to allow Palo Alto Networks apps to access your Active Directory.
1
Download
Download the latest version of the Directory Sync agent.
Download Agent
2
Generate Certificate
Generate a certificate to authenticate the agent with the Directory Sync service.
Get Certificate
3
Install
Install the agent on a Windows server and configure it to communicate with your Active Directory and the Directory Sync service.
Get Started


One Time Password
Device Type
Device Number
One Time Password
Generate OTP for Next-Gen Firewalls
Your one time password has been created and is available below. The password will be valid for 60 minutes.
PAN OS Device:
Password:
Expires On:
2/4/2022 2:48:46 PM
Generate OTP
Download OTP
Copy to Clipboard
Done


Cloud Identity Engine
Name CIE
Instance | User Attributes | Group Attributes | Device Attributes
Region europe
Cloud Identity Engine Instance PANgurus - Cloud Identity Engine
Domain pangurus.com
Update Interval (min) 60
Enabled
Cloud Identity Engine
Name CIE
Instance | User Attributes | Group Attributes | Device Attributes
NAME
DIRECTORY ATTRIBUTE
Primary Username
E-Mail
Alternate Username 1
Alternate Username 2
Alternate Username 3
Name
User Principal Name
Common-Name
Mail
OK
Cancel
Cloud Identity Engine
Name CIE
Instance | User Attributes | Group Attributes | Device Attributes
NAME
DIRECTORY ATTRIBUTE
Group Name
E-Mail
Name
Common-Name
Mail
Distinguished Name
Cloud Identity Engine
Name CIE
Instance | User Attributes | Group Attributes | Device Attributes
Endpoint Serial Number
None
None
Serial Number

Set Up SAML Authentication

Configure the service provider on your identity provider(IdP). Set up and validate an IdP profile.
Click here to learn more about configuring an authentication profile.

1 Configure Cloud Authentication Service (CAS) as your SAML Service Provider

Download the Service Provider (SP) metadata or use the SP Metadata page to configure the SP on your Identity Provider(IdP).

Download SP Metadata

2 Configure your Identity Provider Profile

Enter a Profile Name, select your IdP vendor, and select the method you want to use to provide the metadata.

- PROFILE NAME: Azure
- IDP VENDOR: Azure
- ADD METADATA: Upload Metadata
  - Click to Upload
  - Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service.xml
- IDENTITY PROVIDER ID: https://sts.windows.net/71fbaa2b-5[redacted]
- IDENTITY PROVIDER CERTIFICATE: Microsoft Azure Federated SSO Certificate — Expires in 3 years
- IDENTITY PROVIDER SSO URL: https://login.microsoftonline.com/71fbaa[redacted]
- HTTP BINDING FOR SSO REQUEST TO IDP: (•) HTTP Redirect ( ) HTTP Post
- MAXIMUM CLOCK SKEW (SECONDS) ⓘ: 60
- MFA IS ENABLED ON THE IDP ⓘ: (•) YES ( ) NO

3 Test SAML Setup

Test SAML authentication with the identity provider.

Success

MFA info is detected from the SAML response.

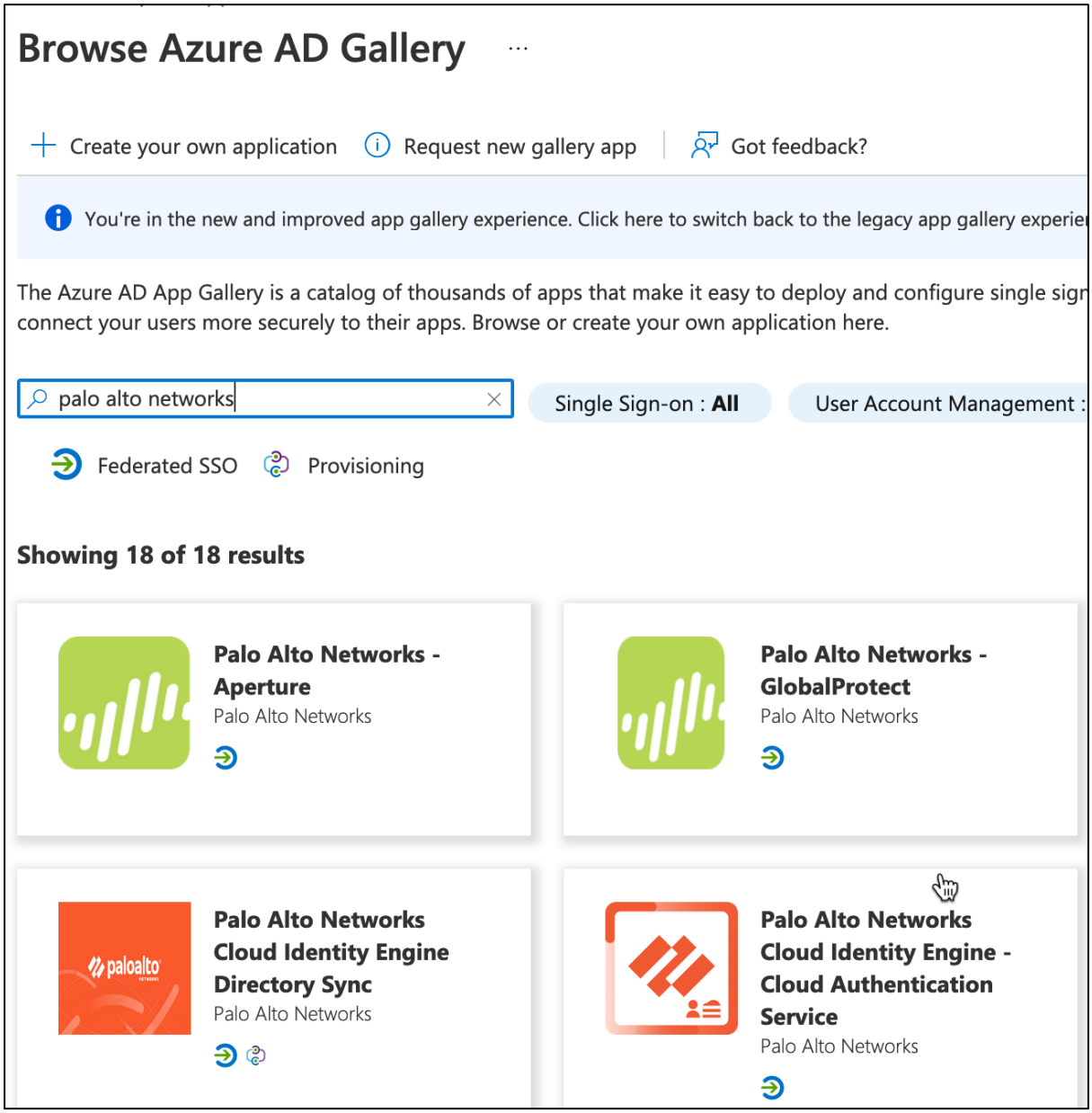
4 SAML Attributes

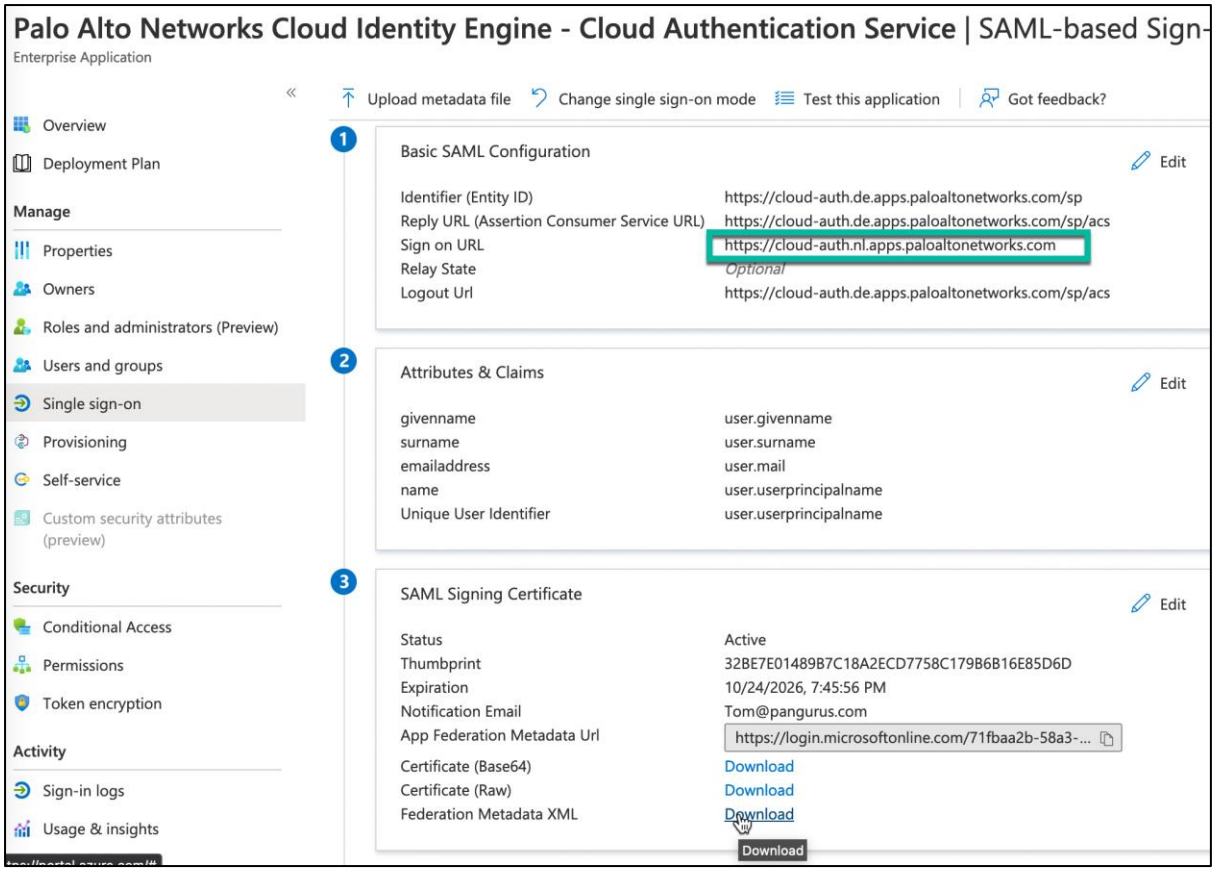
Map your IdP SAML attribute to CAS

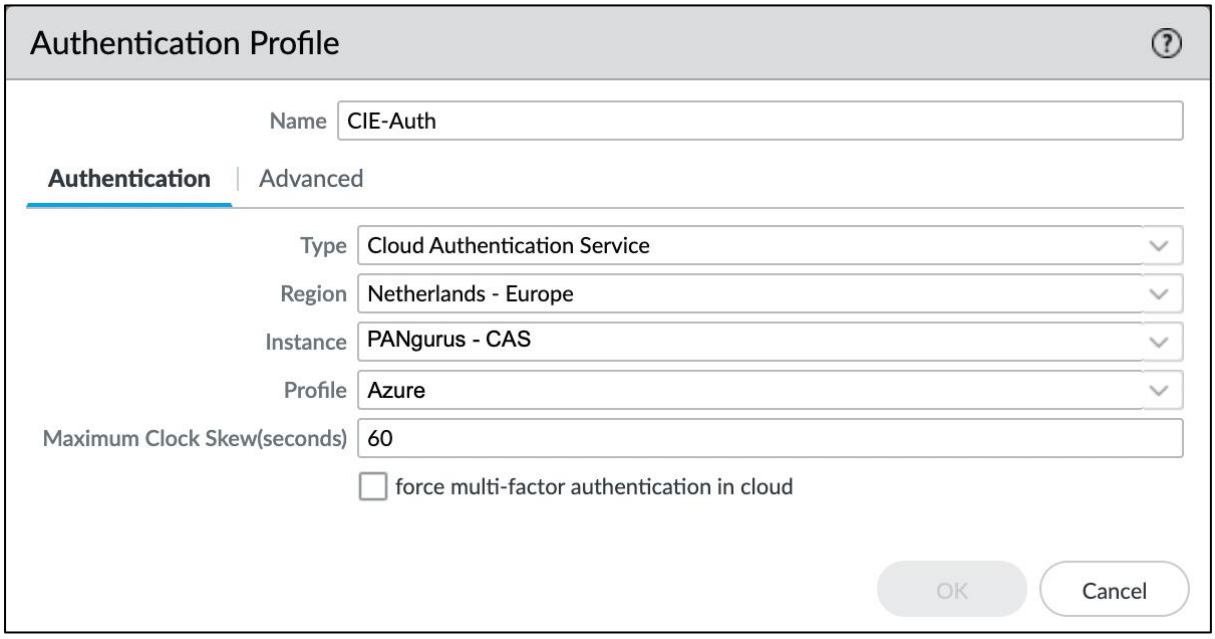
- USERNAME ATTRIBUTE: http://schemas.microsoft.com/identity/claims/displayname
- USERGROUP ATTRIBUTE: Select One
- ACCESS DOMAIN: Select One
- USER DOMAIN: Select One
- ADMIN ROLE: Select One

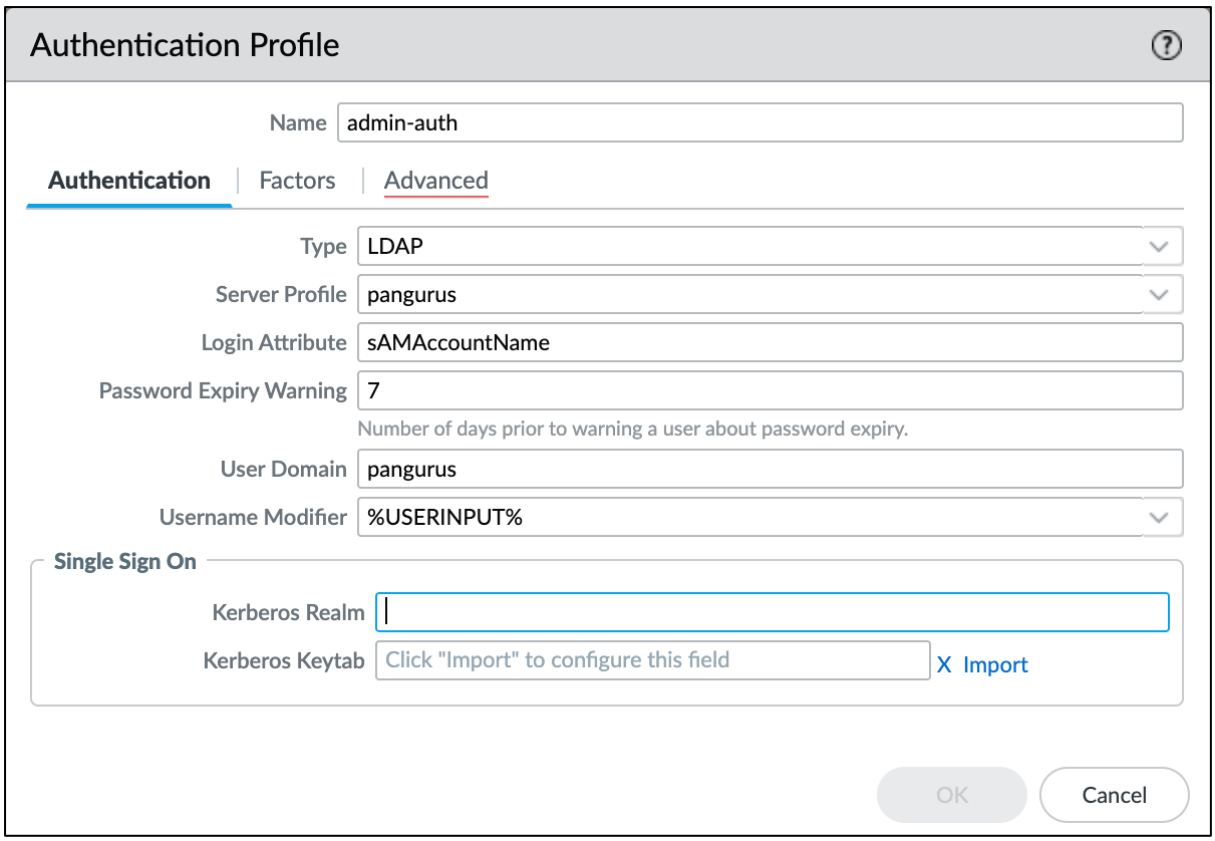
• Required Field

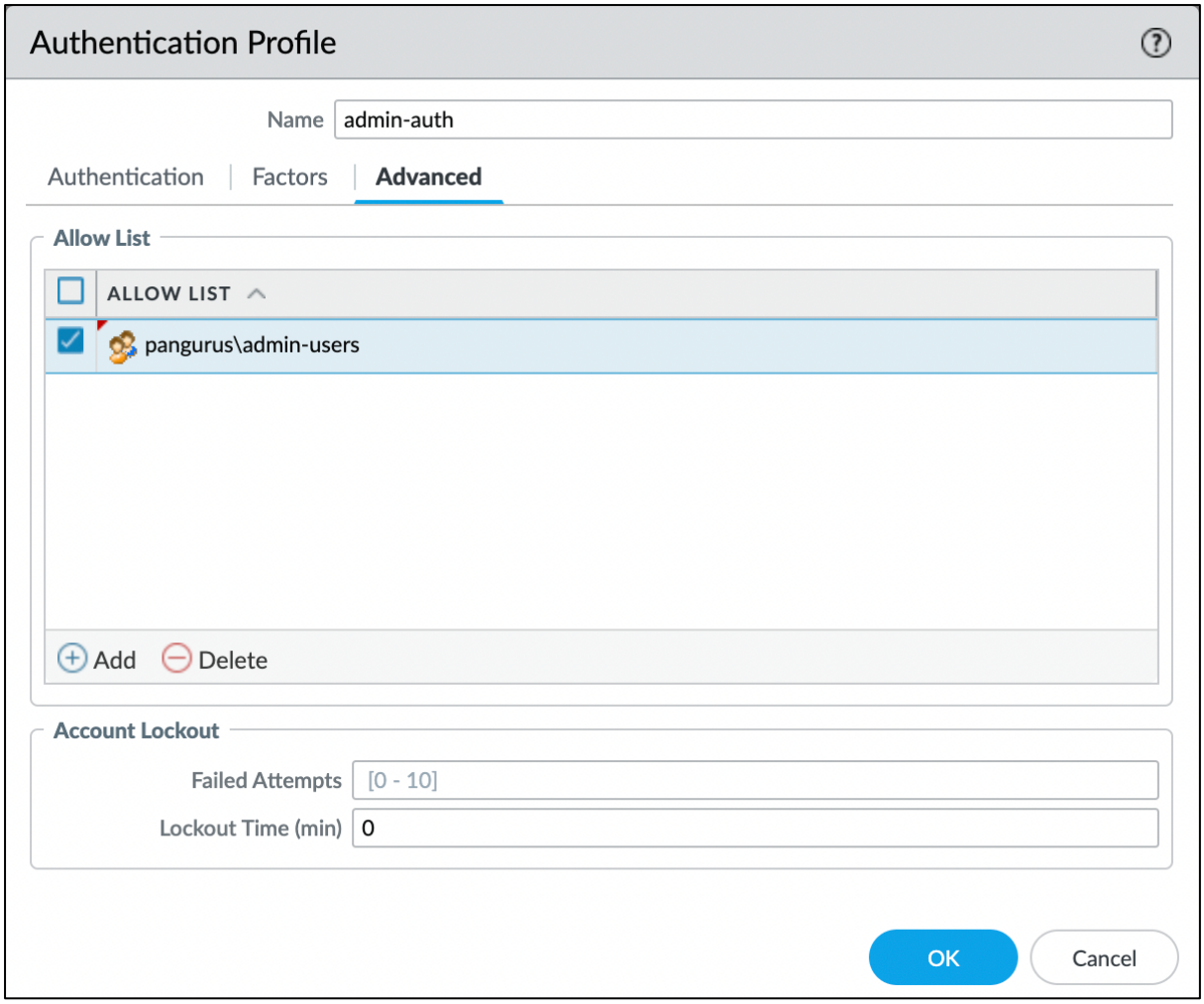
Cancel Submit

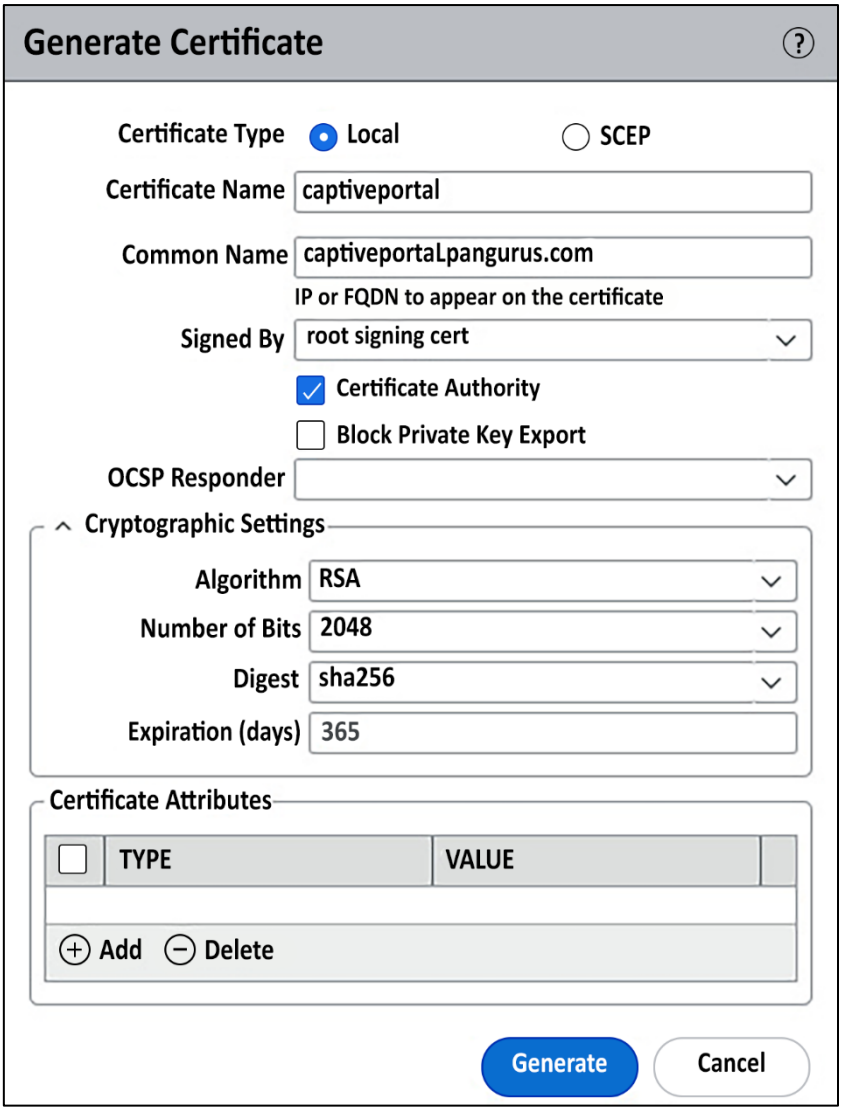

Browse Azure AD Gallery
Create your own application
Request new gallery app
Got feedback?
You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experie
The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign
connect your users more securely to their apps. Browse or create your own application here.
palo alto networks
Single Sign-on : All
User Account Management :
Federated SSO
Provisioning
Showing 18 of 18 results
Palo Alto Networks - Aperture
Palo Alto Networks
Palo Alto Networks - GlobalProtect
Palo Alto Networks
Palo Alto Networks Cloud Identity Engine Directory Sync
Palo Alto Networks
Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service
Palo Alto Networks

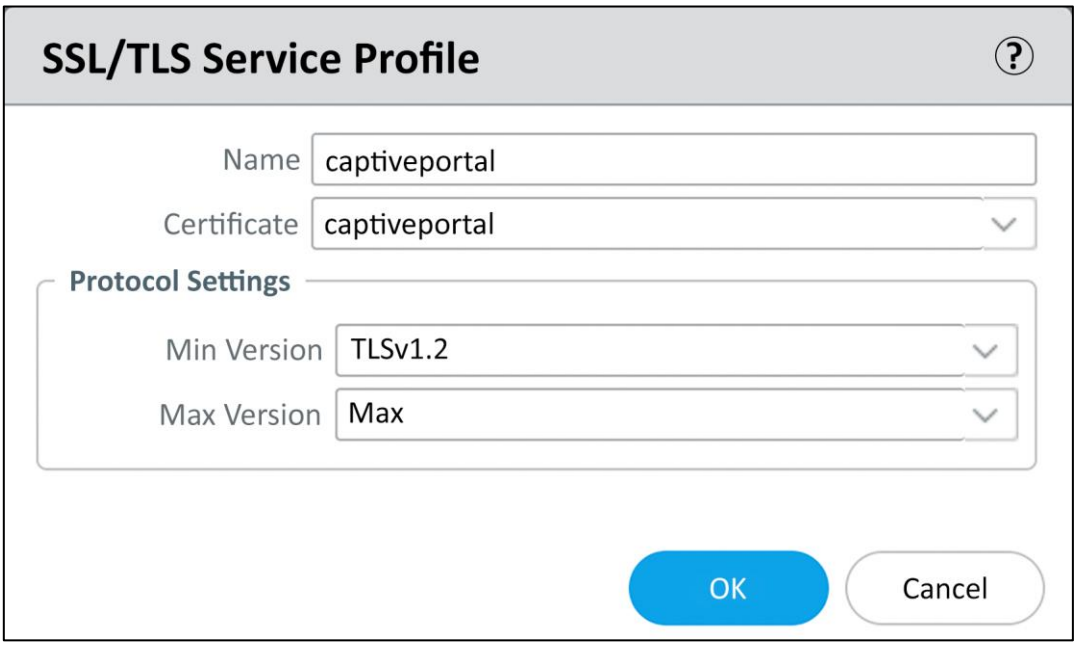

Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service | SAML-based Sign-
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes (preview)
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-in logs
Usage & insights
1
Basic SAML Configuration
Edit
Identifier (Entity ID) https://cloud-auth.de.apps.paloaltonetworks.com/sp
Reply URL (Assertion Consumer Service URL) https://cloud-auth.de.apps.paloaltonetworks.com/sp/acs
Sign on URL https://cloud-auth.nl.apps.paloaltonetworks.com
Relay State Optional
Logout Url https://cloud-auth.de.apps.paloaltonetworks.com/sp/acs
2
Attributes & Claims
Edit
givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname
3
SAML Signing Certificate
Edit
Status Active
Thumbprint 32BE7E01489B7C18A2ECD7758C179B6B16E85D6D
Expiration 10/24/2026, 7:45:56 PM
Notification Email Tom@pangurus.com
App Federation Metadata Url https://login.microsoftonline.com/71fbaa2b-58a3-...
Certificate (Base64) Download
Certificate (Raw) Download
Federation Metadata XML Download
Download

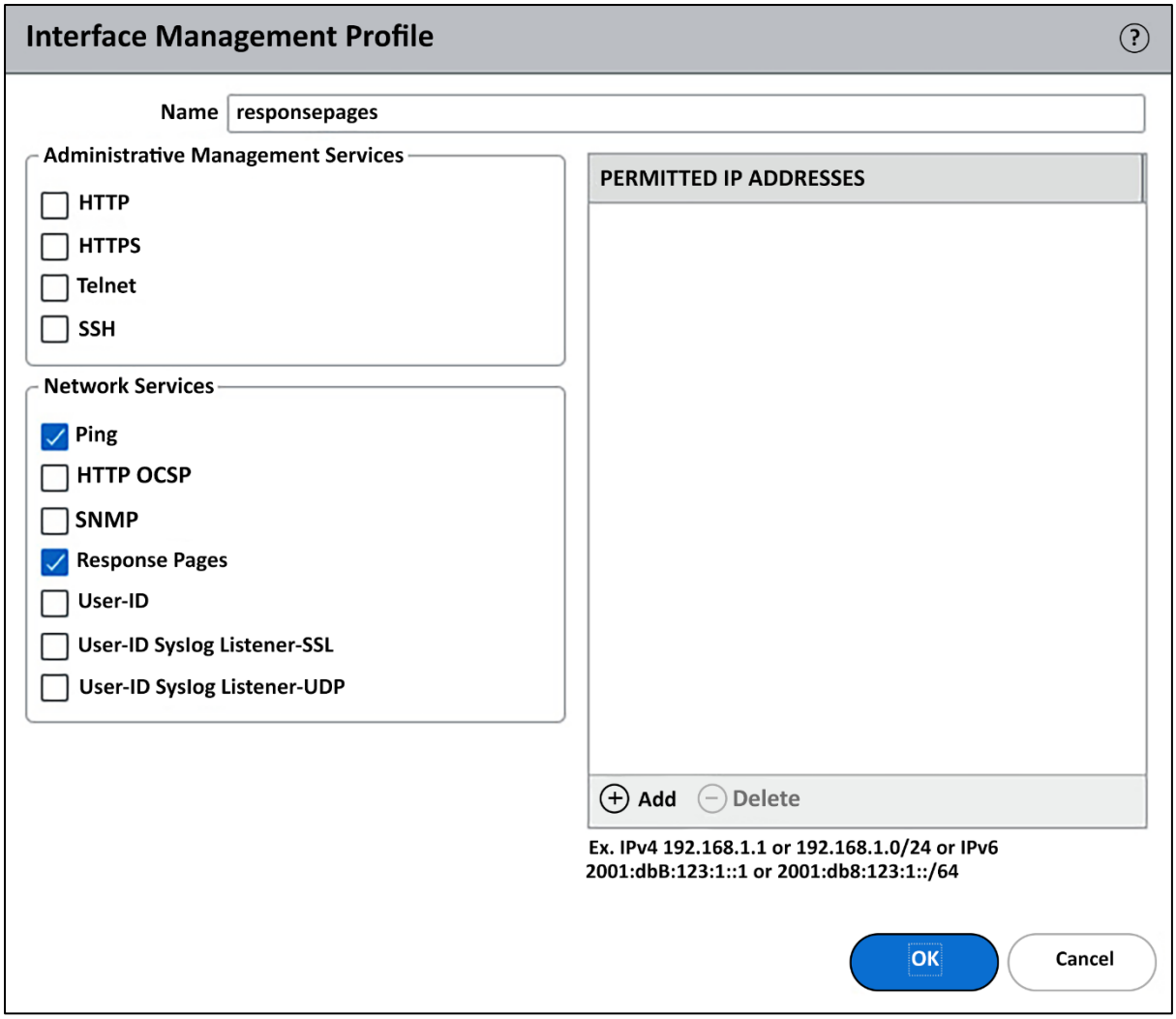

Authentication Profile
Name CIE-Auth
Authentication
Advanced
Type Cloud Authentication Service
Region Netherlands - Europe
Instance PANgurus - CAS
Profile Azure
Maximum Clock Skew(seconds) 60
force multi-factor authentication in cloud
OK
Cancel

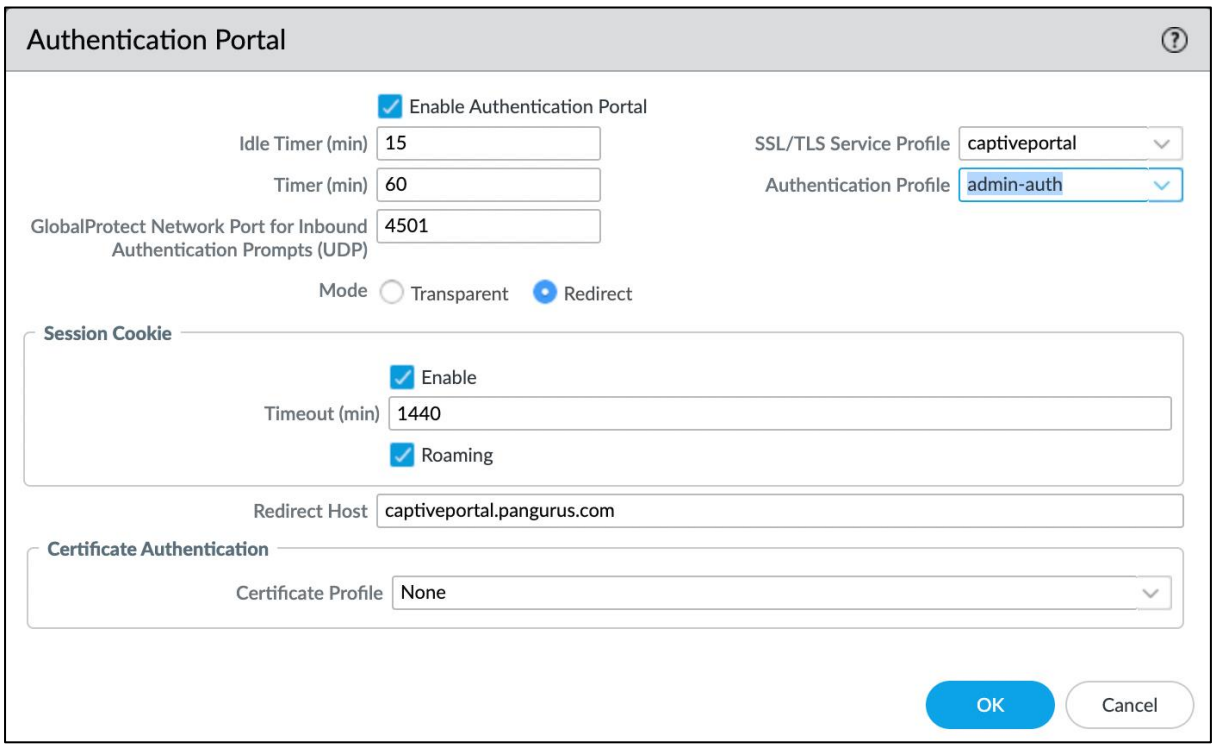

Authentication Profile
Name
admin-auth
Authentication
Factors
Advanced
Type
LDAP
Server Profile
pangurus
Login Attribute
sAMAccountName
Password Expiry Warning
7
Number of days prior to warning a user about password expiry.
User Domain
pangurus
Username Modifier
%USERINPUT%
Single Sign On
Kerberos Realm
Kerberos Keytab
Click "Import" to configure this field
X Import
OK
Cancel

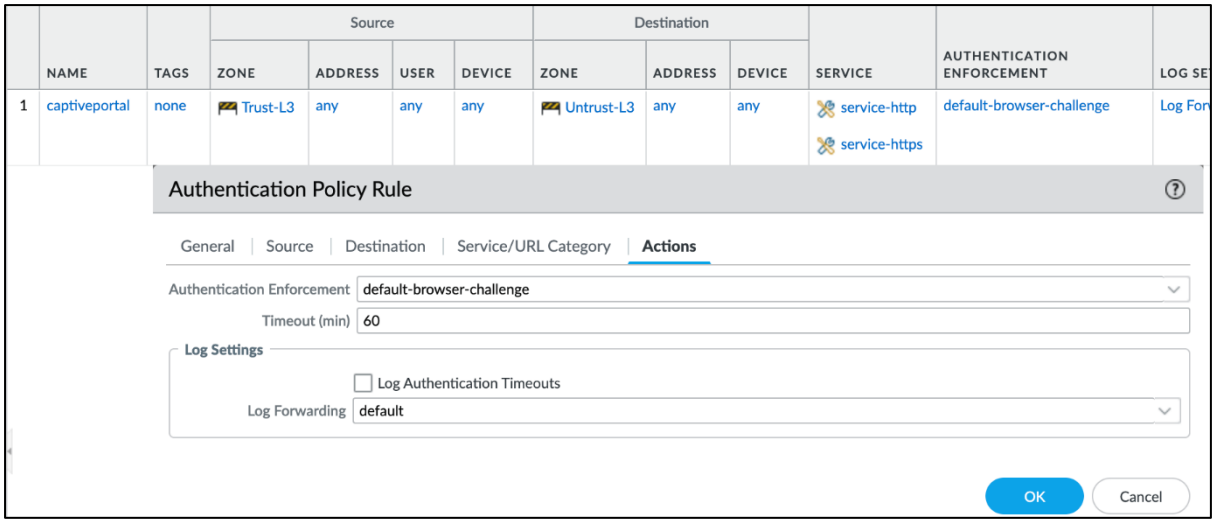

Authentication Profile
Name
admin-auth
Authentication
Factors
Advanced
Allow List
ALLOW LIST
pangurus\admin-users
Add
Delete
Account Lockout
Failed Attempts
[0 - 10]
Lockout Time (min)
0
OK
Cancel

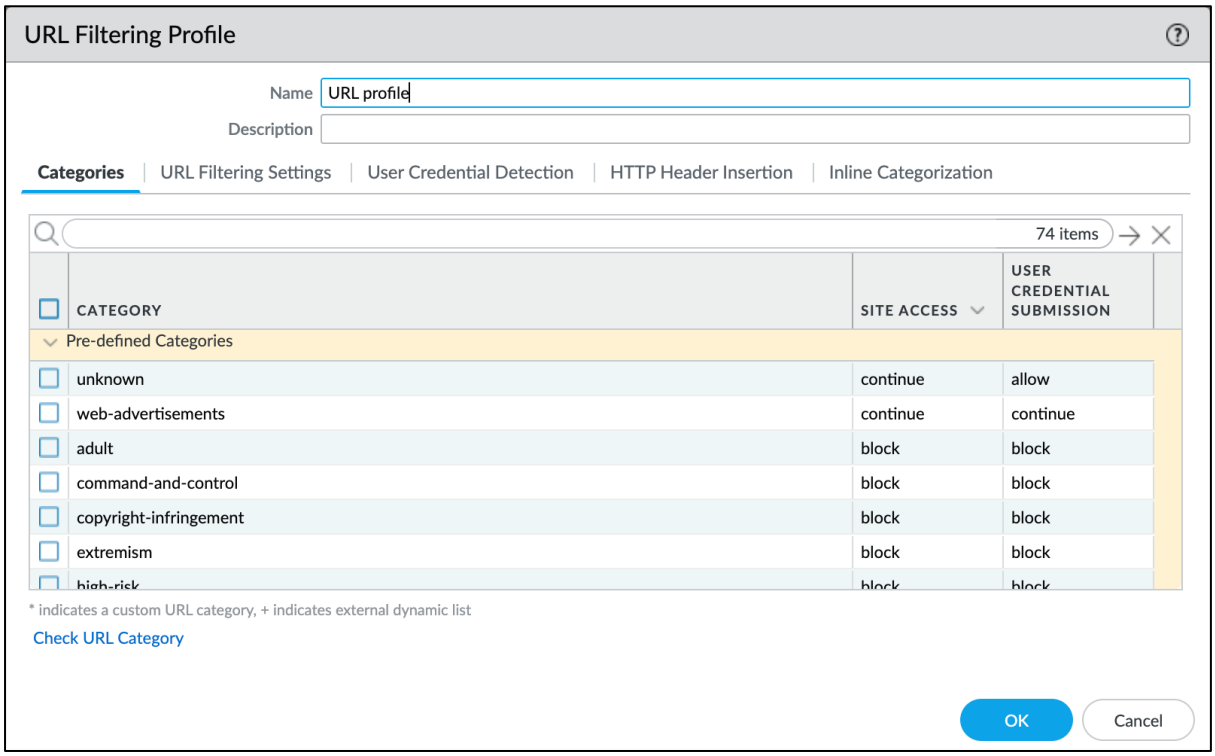

Generate Certificate
Certificate Type
Local
SCEP
Certificate Name
captiveportal
Common Name
captiveportaLpangurus.com
IP or FQDN to appear on the certificate
Signed By
root signing cert
Certificate Authority
Block Private Key Export
OCSP Responder
Cryptographic Settings
Algorithm
RSA
Number of Bits
2048
Digest
sha256
Expiration (days)
365
Certificate Attributes
TYPE
VALUE
Add
Delete
Generate
Cancel

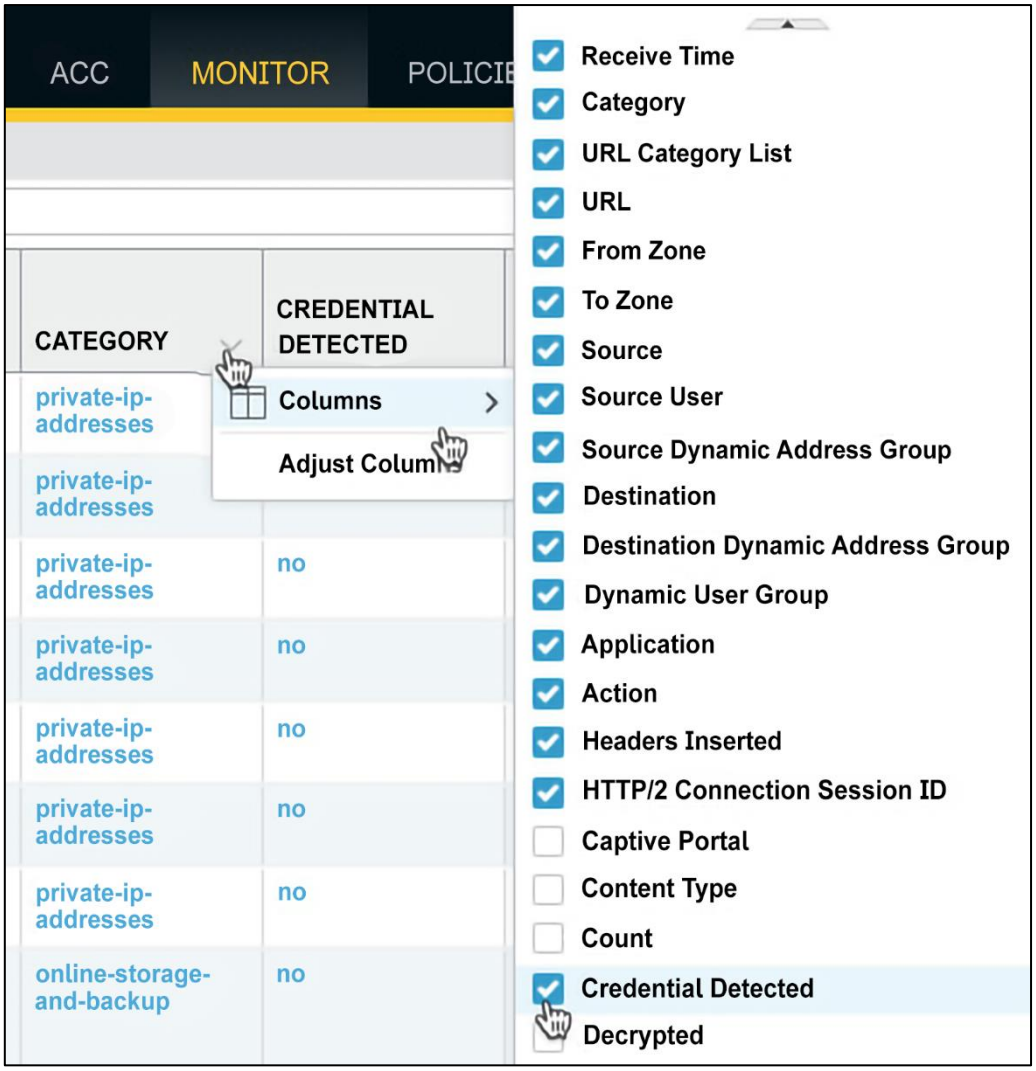

SSL/TLS Service Profile
Name
captiveportal
Certificate
captiveportal
Protocol Settings
Min Version
TLSv1.2
Max Version
Max
OK
Cancel


Interface Management Profile
Name
responsepages
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
PERMITTED IP ADDRESSES
Add
Delete
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:dbB:123:1::1 or 2001:db8:123:1::/64
OK
Cancel

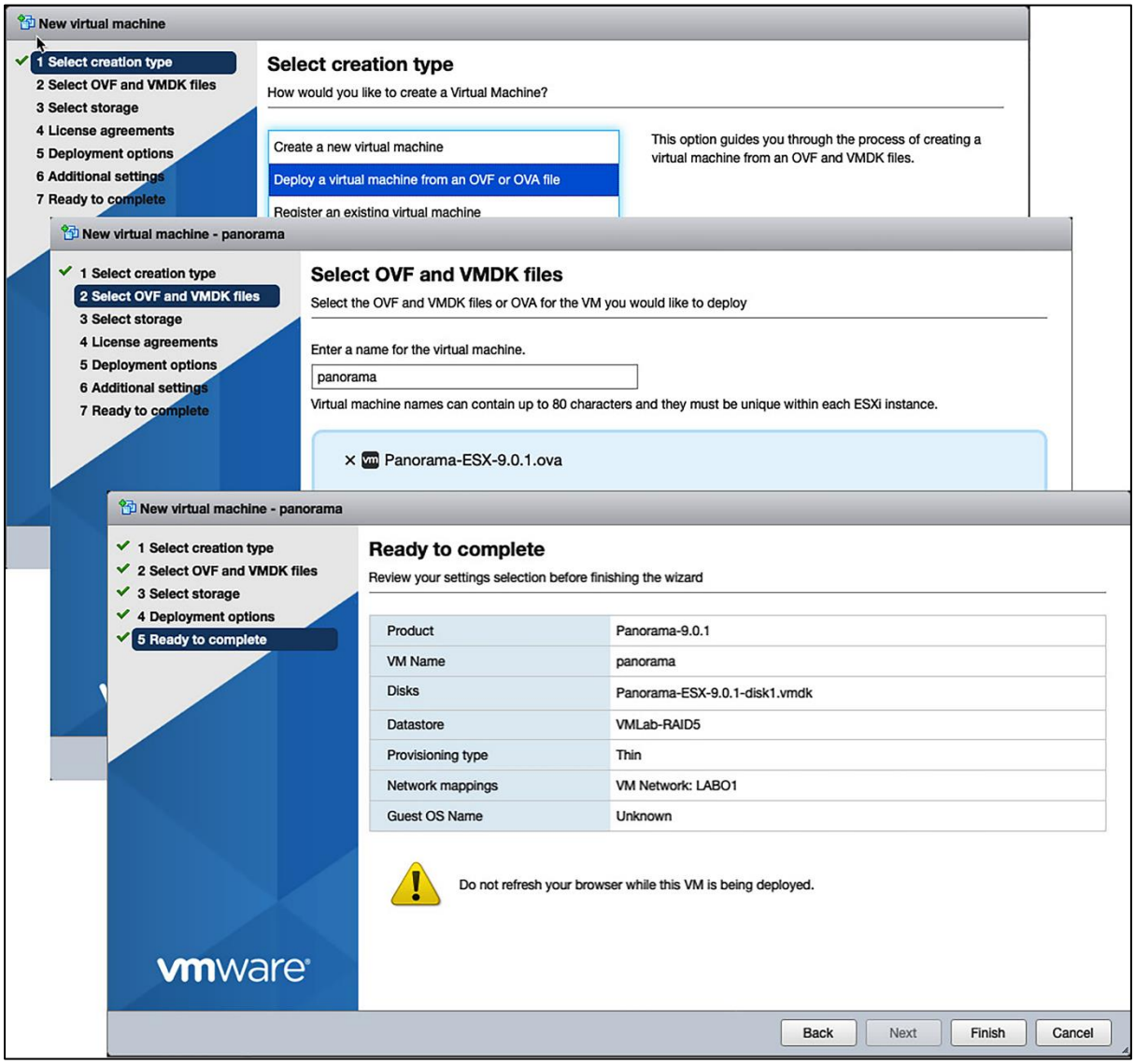

Authentication Portal
Enable Authentication Portal
Idle Timer (min)
15
Timer (min)
60
GlobalProtect Network Port for Inbound Authentication Prompts (UDP)
4501
SSL/TLS Service Profile
captiveportal
Authentication Profile
admin-auth
Mode
Transparent
Redirect
Session Cookie
Enable
Timeout (min)
1440
Roaming
Redirect Host
captiveportal.pangurus.com
Certificate Authentication
Certificate Profile
None
OK
Cancel

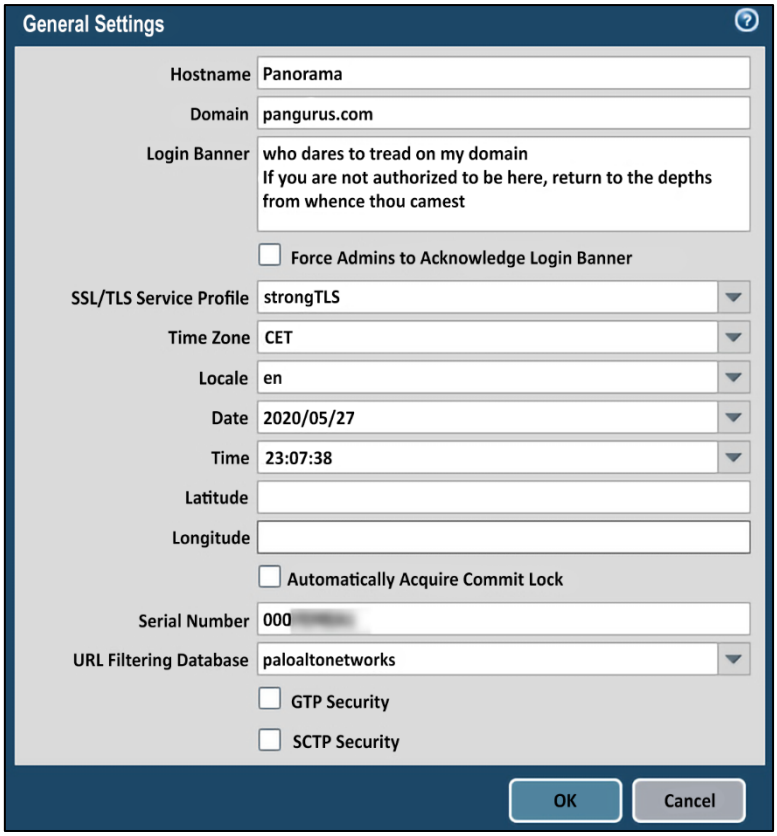

Source
Destination
NAME
TAGS
ZONE
ADDRESS
USER
DEVICE
ZONE
ADDRESS
DEVICE
SERVICE
AUTHENTICATION ENFORCEMENT
LOG SE
1
captiveportal
none
Trust-L3
any
any
any
Untrust-L3
any
any
service-http
service-https
default-browser-challenge
Log For
Authentication Policy Rule
General
Source
Destination
Service/URL Category
Actions
Authentication Enforcement
default-browser-challenge
Timeout (min)
60
Log Settings
Log Authentication Timeouts
Log Forwarding
default
OK
Cancel

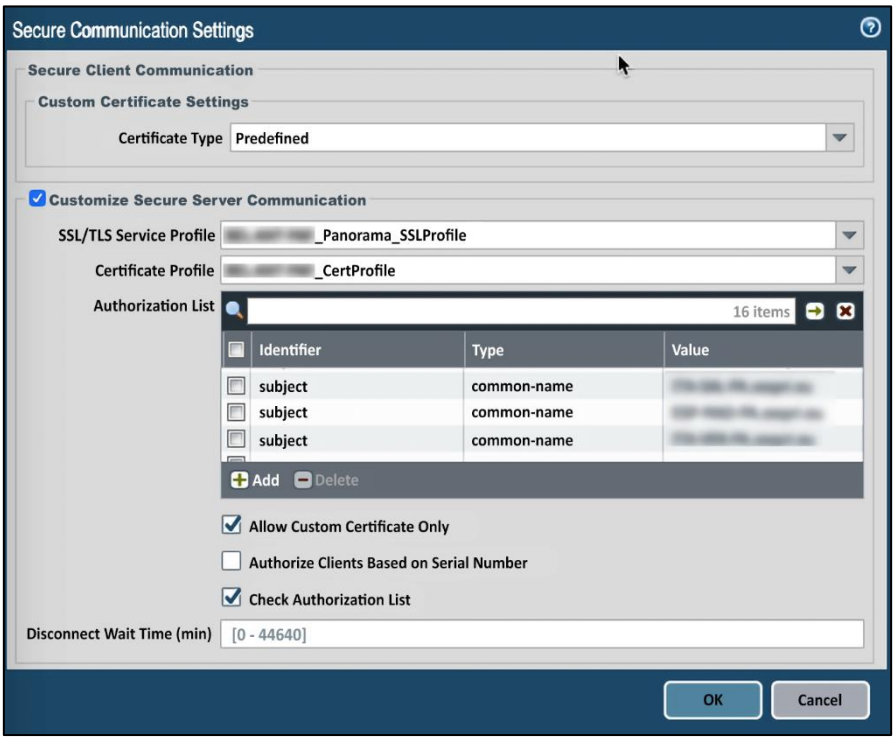

URL Filtering Profile
Name
URL profile
Description
Categories
URL Filtering Settings
User Credential Detection
HTTP Header Insertion
Inline Categorization
74 items
CATEGORY
SITE ACCESS
USER CREDENTIAL SUBMISSION
Pre-defined Categories
unknown
continue
allow
web-advertisements
continue
continue
adult
block
block
command-and-control
block
block
copyright-infringement
block
block
extremism
block
block
high-risk
block
block
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
OK
Cancel

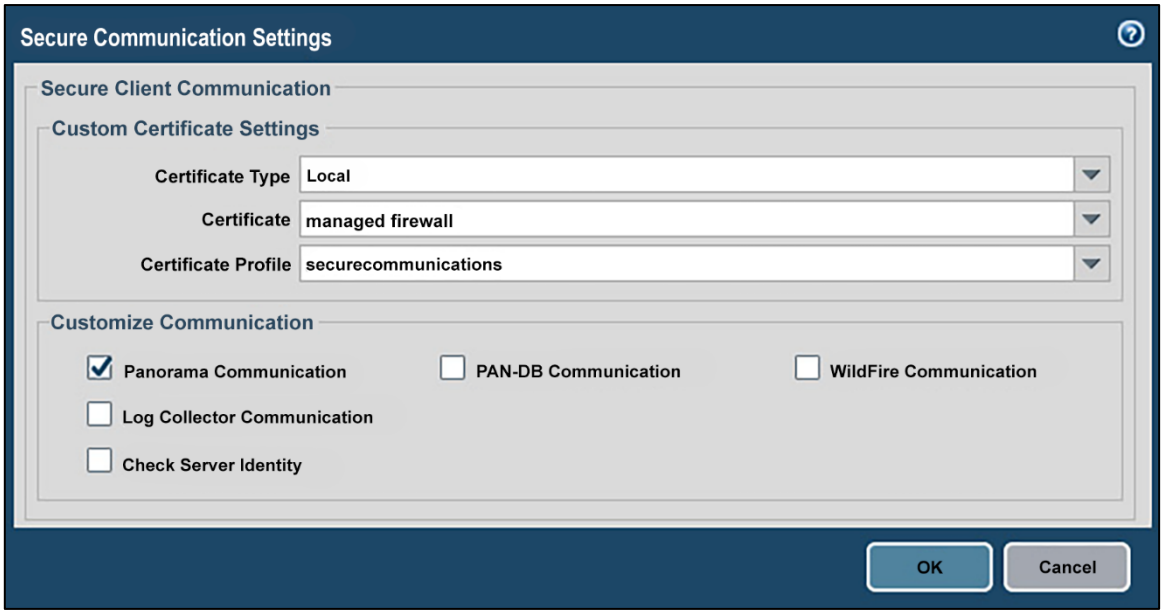

ACC
MONITOR
POLICIE
CATEGORY
CREDENTIAL DETECTED
Columns
Adjust Columns
private-ip-addresses
private-ip-addresses
private-ip-addresses
no
private-ip-addresses
no
private-ip-addresses
no
private-ip-addresses
no
private-ip-addresses
no
online-storage-and-backup
no
Receive Time
Category
URL Category List
URL
From Zone
To Zone
Source
Source User
Source Dynamic Address Group
Destination
Destination Dynamic Address Group
Dynamic User Group
Application
Action
Headers Inserted
HTTP/2 Connection Session ID
Captive Portal
Content Type
Count
Credential Detected
Decrypted

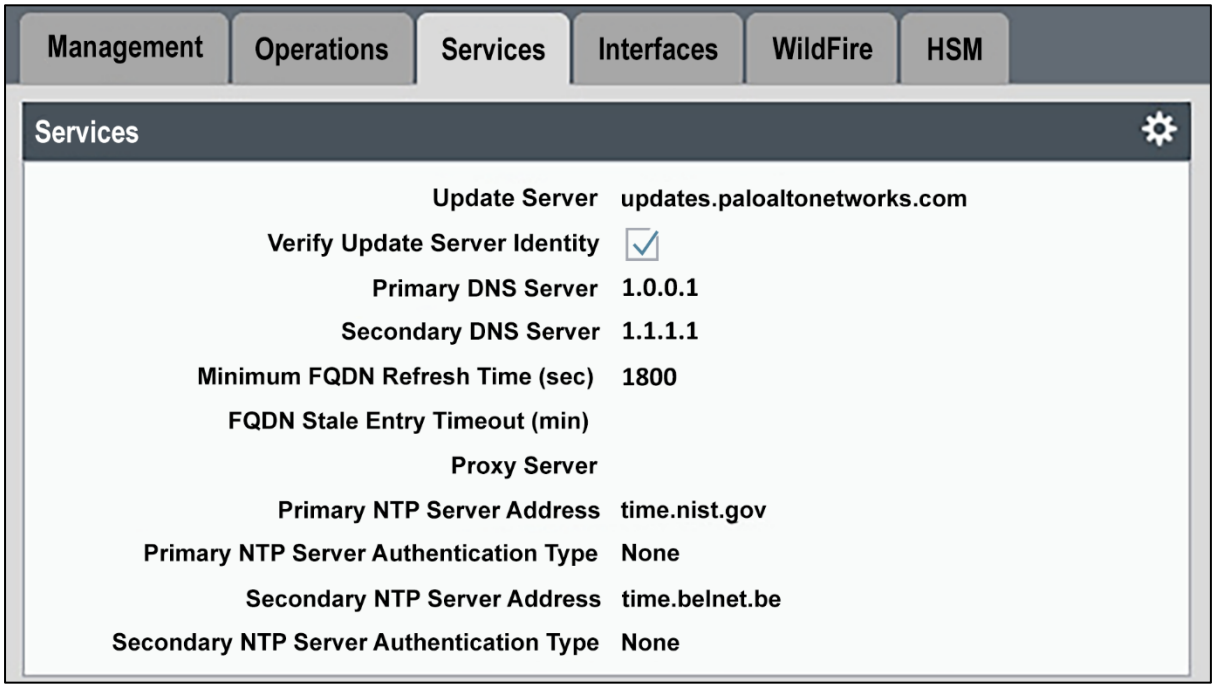
Chapter 7: Managing Firewalls through Panorama

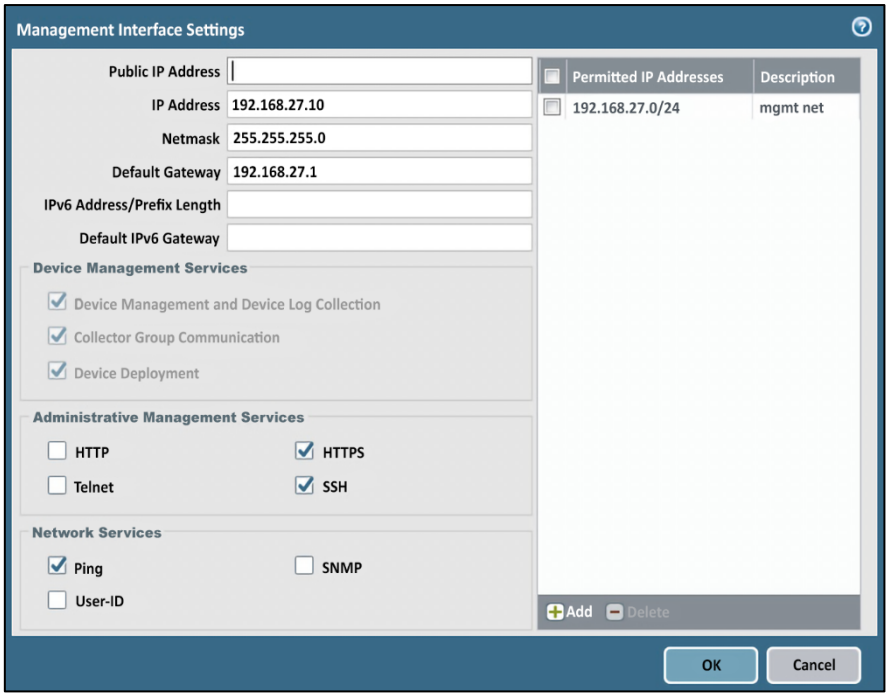


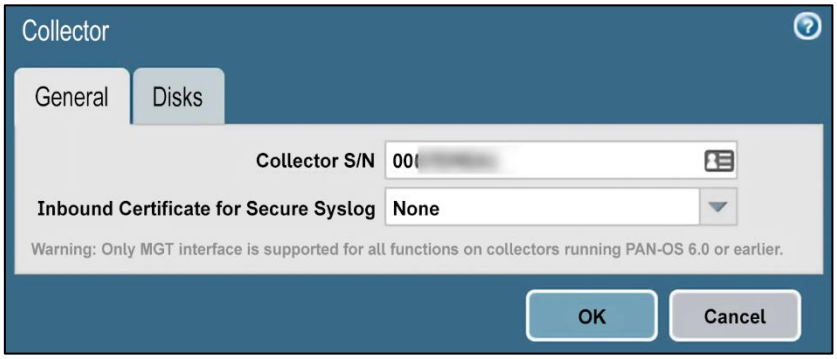

General Settings
Hostname
Panorama
Domain
pangurus.com
Login Banner
who dares to tread on my domain
If you are not authorized to be here, return to the depths
from whence thou camest
Force Admins to Acknowledge Login Banner
SSL/TLS Service Profile
strongTLS
Time Zone
CET
Locale
en
Date
2020/05/27
Time
23:07:38
Latitude
Longitude
Automatically Acquire Commit Lock
Serial Number
000
URL Filtering Database
paloaltonetworks
GTP Security
SCTP Security
OK
Cancel

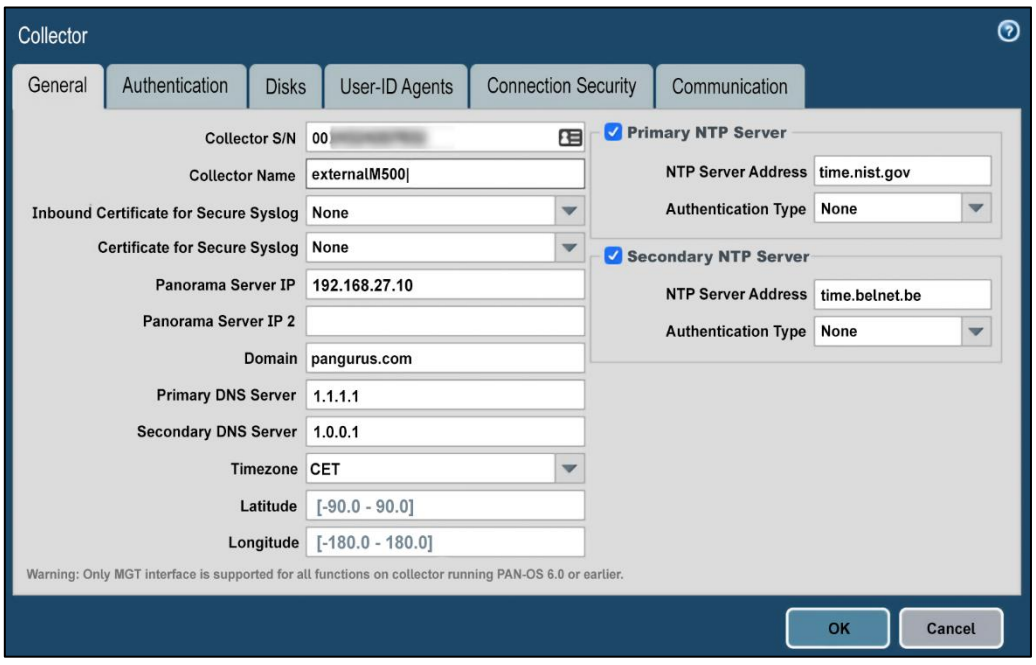

Secure Communication Settings
Secure Client Communication
Custom Certificate Settings
Certificate Type
Predefined
Customize Secure Server Communication
SSL/TLS Service Profile
_Panorama_SSLProfile
Certificate Profile
_CertProfile
Authorization List
16 items
Identifier
Type
Value
subject
common-name
subject
common-name
subject
common-name
Add
Delete
Allow Custom Certificate Only
Authorize Clients Based on Serial Number
Check Authorization List
Disconnect Wait Time (min)
[0 - 44640]
OK
Cancel

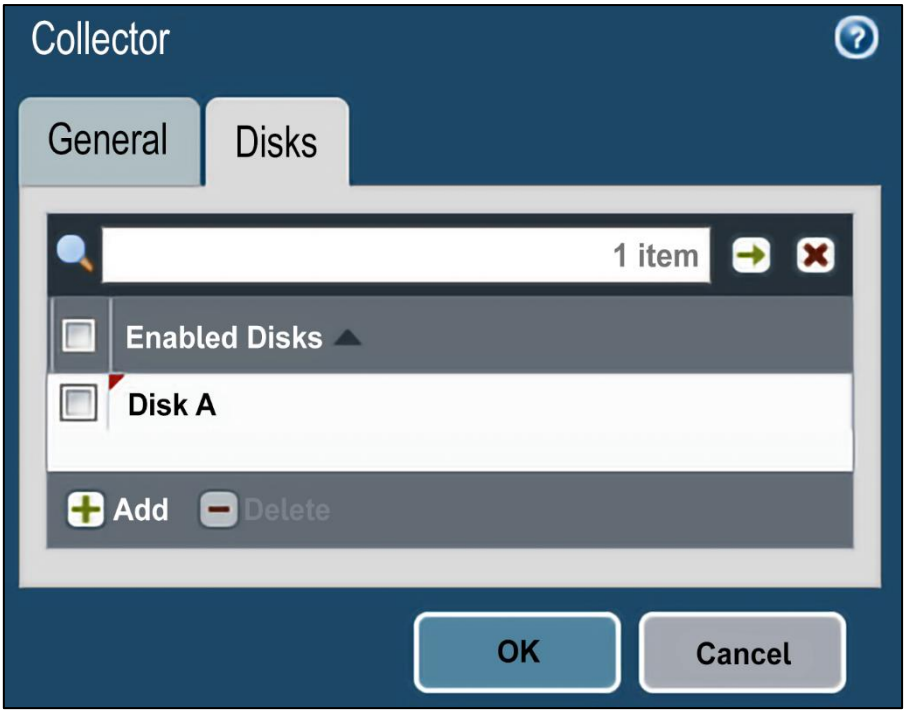

Secure Communication Settings
Secure Client Communication
Custom Certificate Settings
Certificate Type
Local
Certificate
managed firewall
Certificate Profile
securecommunications
Customize Communication
Panorama Communication
PAN-DB Communication
WildFire Communication
Log Collector Communication
Check Server Identity
OK
Cancel

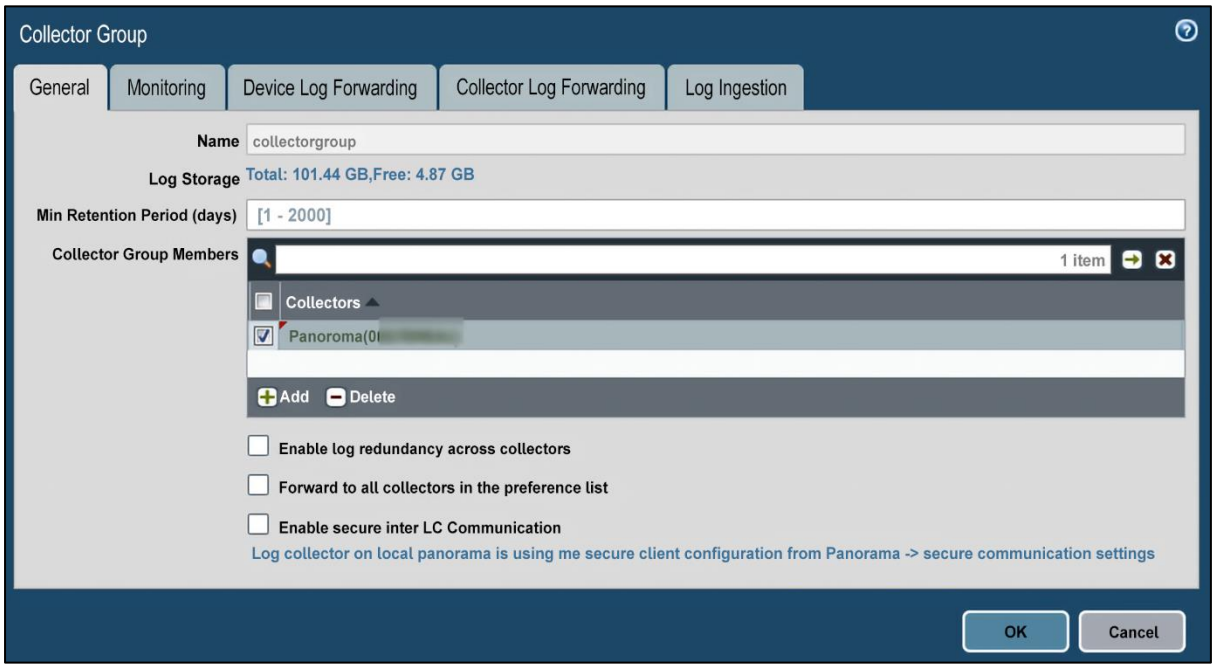

Management
Operations
Services
Interfaces
WildFire
HSM
Services
Update Server
updates.paloaltonetworks.com
Verify Update Server Identity
Primary DNS Server
1.0.0.1
Secondary DNS Server
1.1.1.1
Minimum FQDN Refresh Time (sec)
1800
FQDN Stale Entry Timeout (min)
Proxy Server
Primary NTP Server Address
time.nist.gov
Primary NTP Server Authentication Type
None
Secondary NTP Server Address
time.belnet.be
Secondary NTP Server Authentication Type
None


Management Interface Settings
Public IP Address
IP Address 192.168.27.10
Netmask 255.255.255.0
Default Gateway 192.168.27.1
IPv6 Address/Prefix Length
Default IPv6 Gateway
Device Management Services
Device Management and Device Log Collection
Collector Group Communication
Device Deployment
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
SNMP
User-ID
Permitted IP Addresses
Description
192.168.27.0/24
mgmt net
Add
Delete
OK
Cancel


Collector
General
Disks
Collector S/N
Inbound Certificate for Secure Syslog
None
Warning: Only MGT interface is supported for all functions on collectors running PAN-OS 6.0 or earlier.
OK
Cancel


Collector
General
Authentication
Disks
User-ID Agents
Connection Security
Communication
Collector S/N
Collector Name
externalM500
Inbound Certificate for Secure Syslog
None
Certificate for Secure Syslog
None
Panorama Server IP
192.168.27.10
Panorama Server IP 2
Domain
pangurus.com
Primary DNS Server
1.1.1.1
Secondary DNS Server
1.0.0.1
Timezone
CET
Latitude
[-90.0 - 90.0]
Longitude
[-180.0 - 180.0]
Primary NTP Server
NTP Server Address
time.nist.gov
Authentication Type
None
Secondary NTP Server
NTP Server Address
time.belnet.be
Authentication Type
None
Warning: Only MGT interface is supported for all functions on collector running PAN-OS 6.0 or earlier.
OK
Cancel


Collector
General
Disks
1 item
Enabled Disks
Disk A
Add
Delete
OK
Cancel

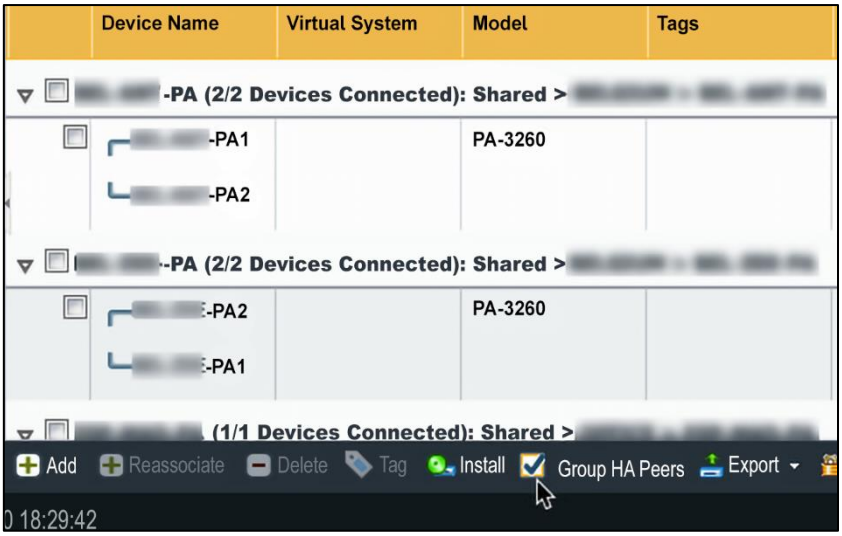

Collector Group
General
Monitoring
Device Log Forwarding
Collector Log Forwarding
Log Ingestion
Name
collectorgroup
Log Storage
Total: 101.44 GB,Free: 4.87 GB
Min Retention Period (days)
[1 - 2000]
Collector Group Members
1 item
Collectors
Panoroma(0
Add
Delete
Enable log redundancy across collectors
Forward to all collectors in the preference list
Enable secure inter LC Communication
Log collector on local panorama is using me secure client configuration from Panorama -> secure communication settings
OK
Cancel

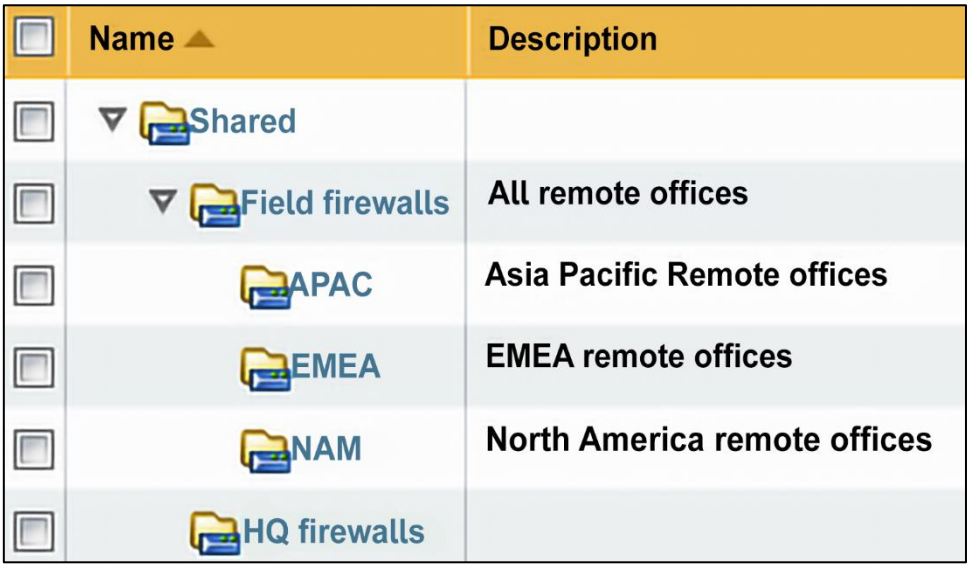
Panorama Settings

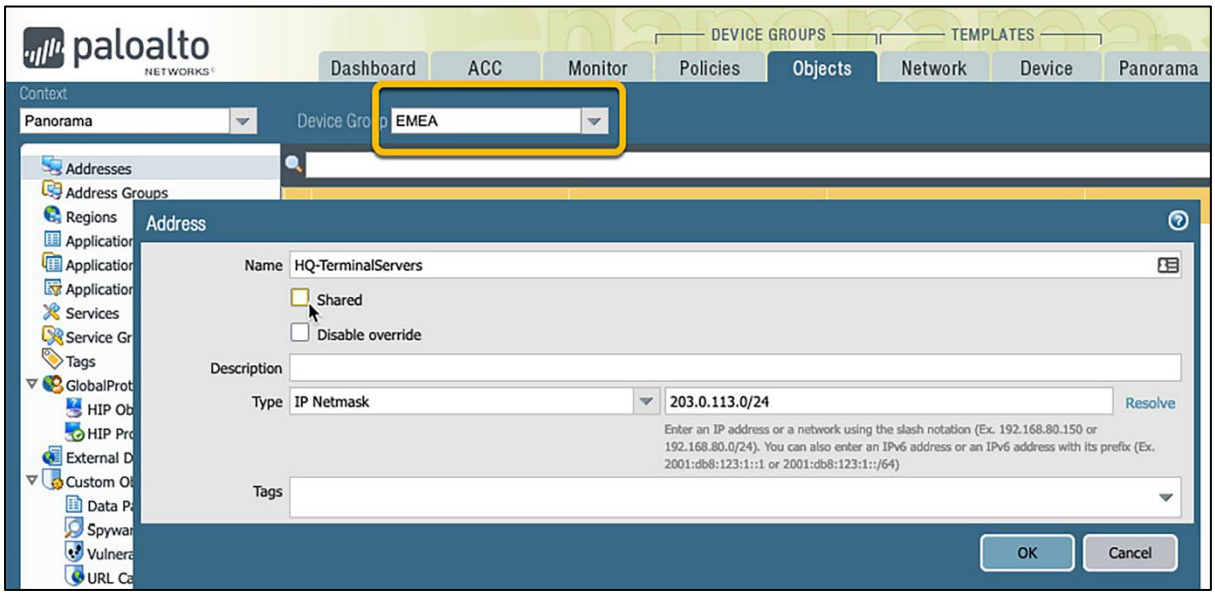
Panorama Servers	192.168.27.10
Enable pushing device monitoring data to Panorama	☑
Receive Timeout for Connection to Panorama (sec)	240
Send Timeout for Connection to Panorama (sec)	240
Retry Count for SSL Send to Panorama	25
Enable automated commit recovery	☑
Number of attempts to check for Panorama connectivity on automated commit recovery	1
Interval between retries (sec) on automated commit recovery	10

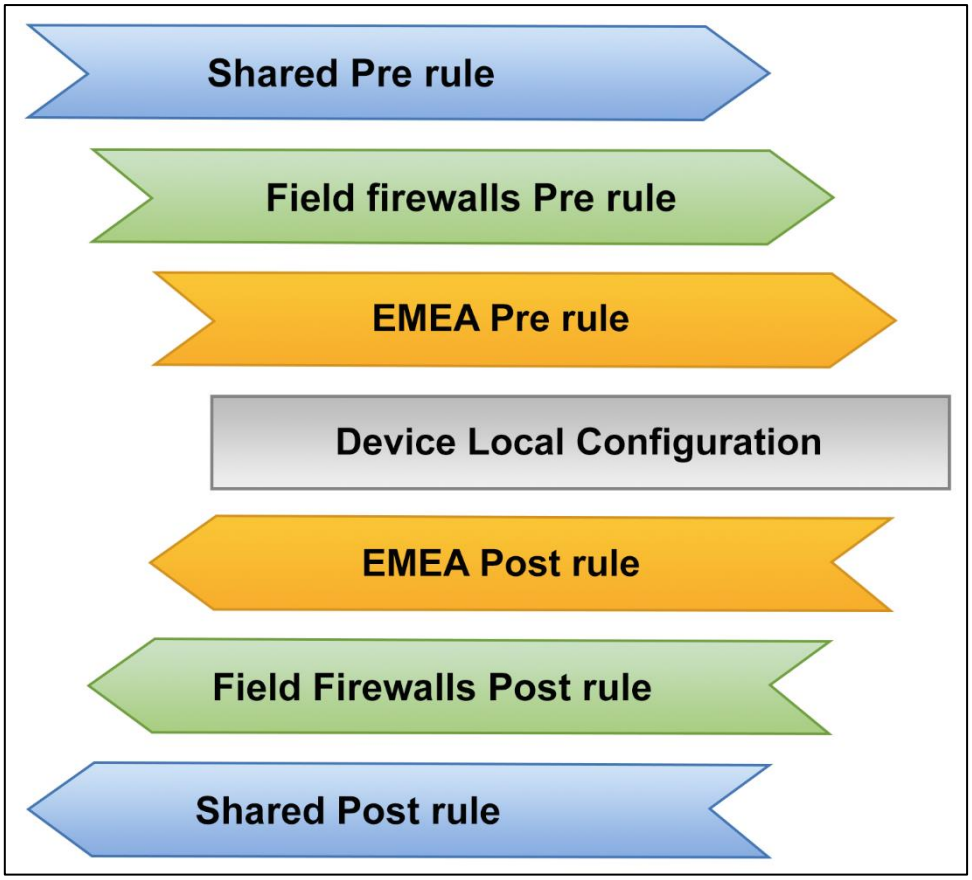
Secure Communication Settings

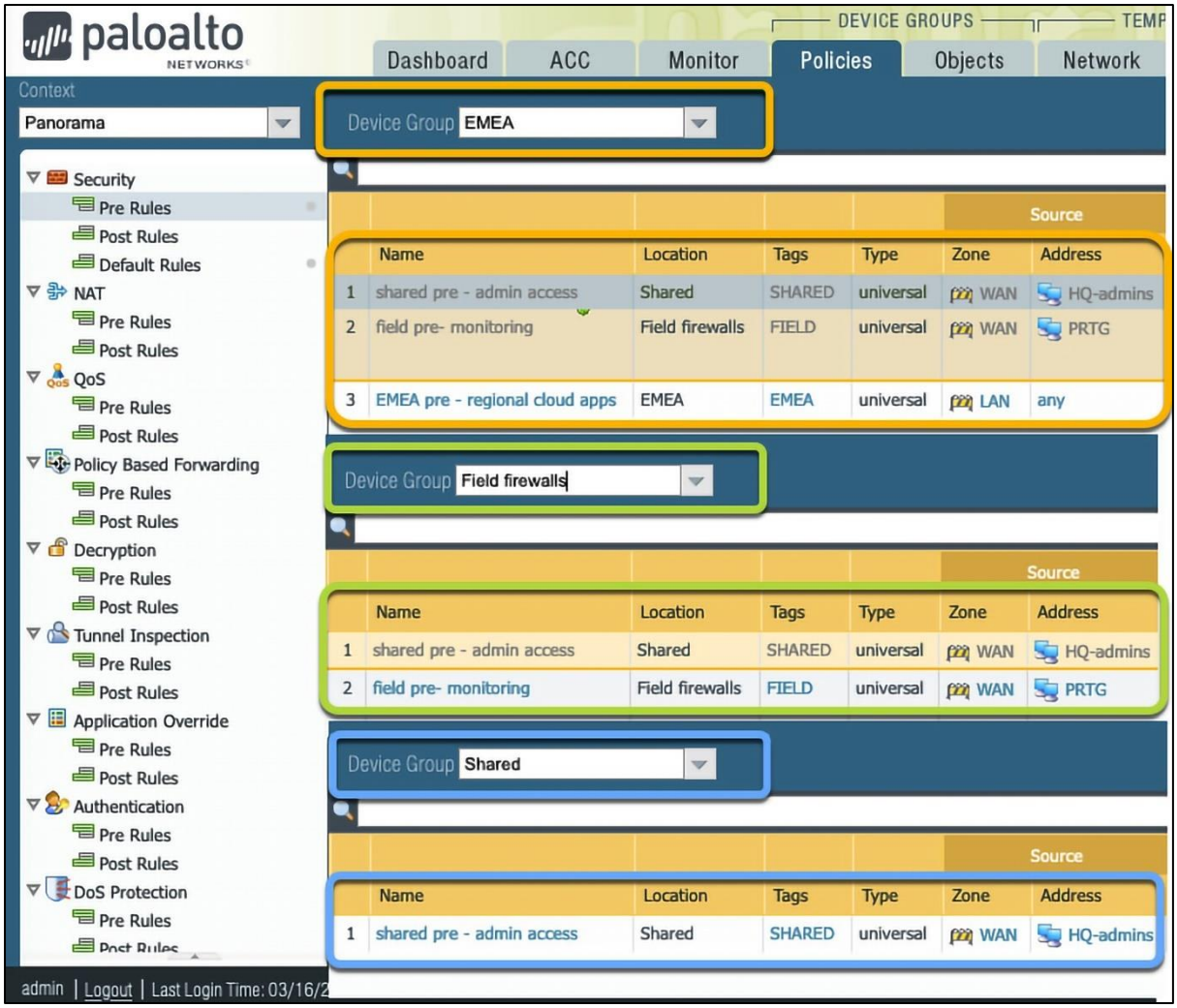
Certificate Type	Local Certificate:managed firewall Certificate Profile:securecommunications
Panorama Communication	☑

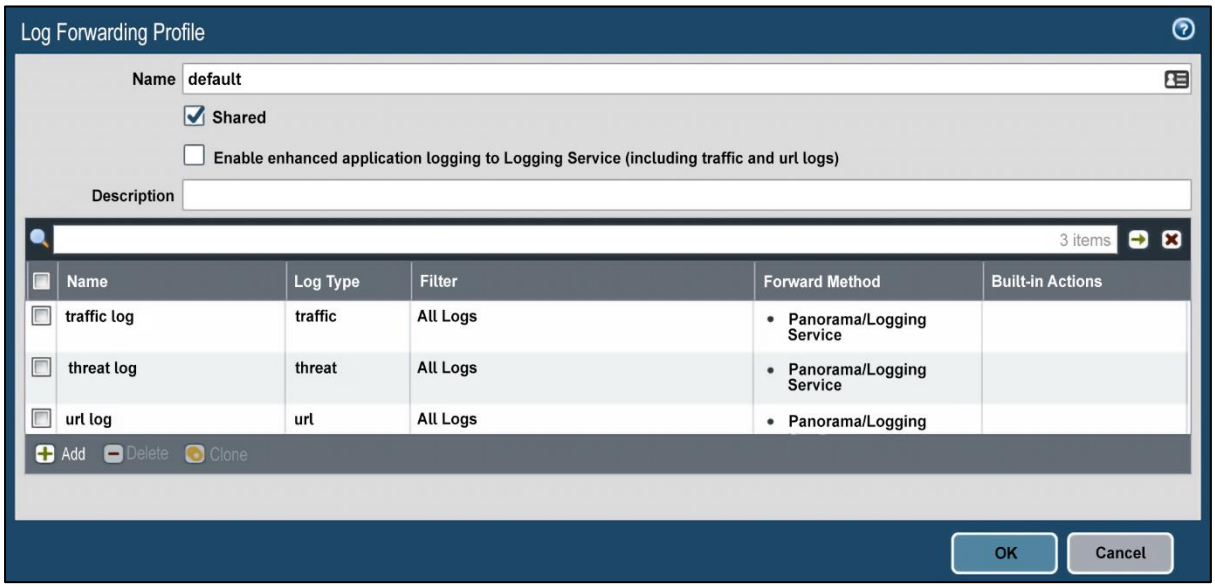

Device Name
Virtual System
Model
Tags
-PA (2/2 Devices Connected): Shared >
-PA1
PA-3260
-PA2
-PA (2/2 Devices Connected): Shared >
-PA2
PA-3260
-PA1
(1/1 Devices Connected): Shared >
Add
Reassociate
Delete
Tag
Install
Group HA Peers
Export
0 18:29:42

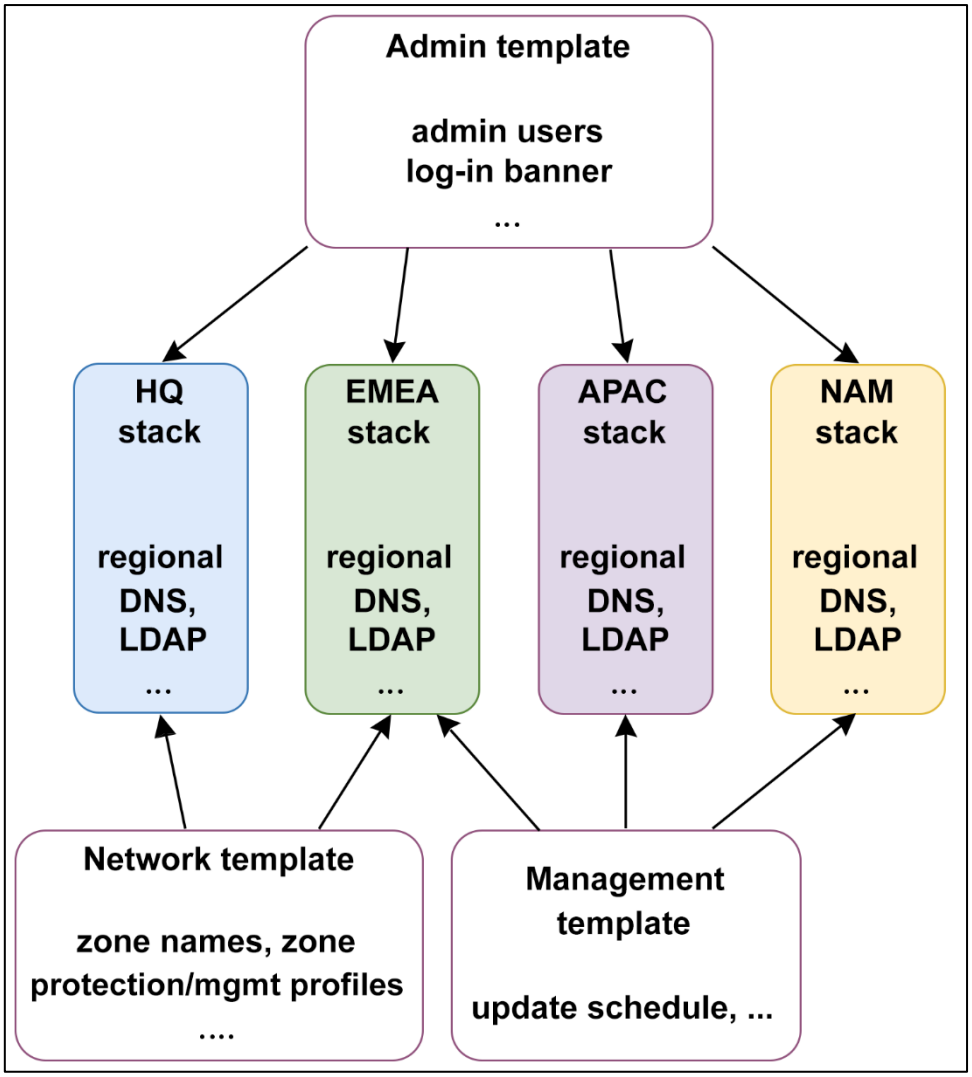

Name
Description
Shared
Field firewalls
All remote offices
APAC
Asia Pacific Remote offices
EMEA
EMEA remote offices
NAM
North America remote offices
HQ firewalls

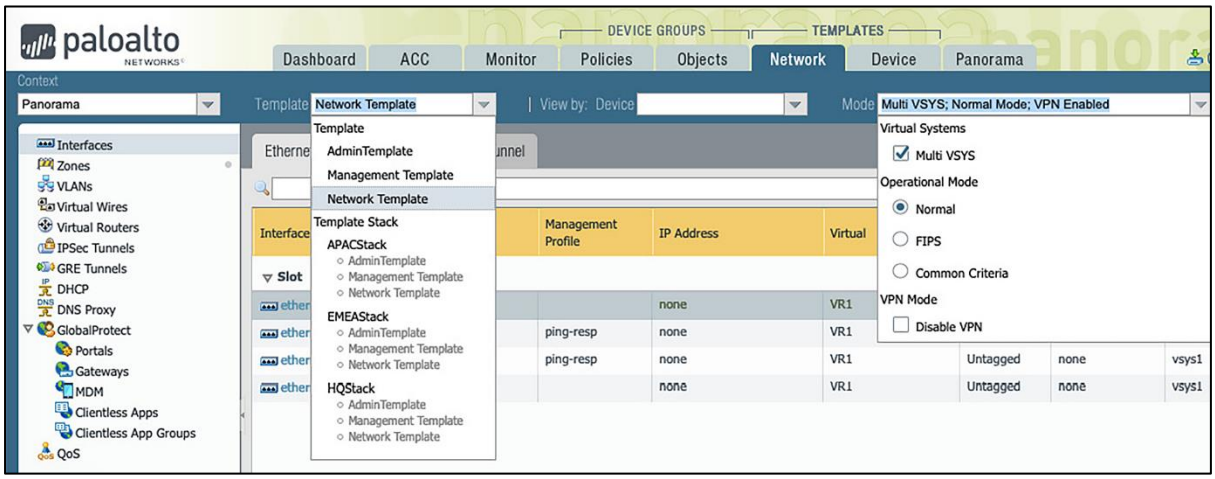

paloalto
NETWORKS
DEVICE GROUPS
TEMPLATES
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Panorama
Context
Panorama
Device Group
EMEA
Addresses
Address Groups
Regions
Services
Tags
Address
Name
HQ-TerminalServers
Shared
Disable override
Description
Type
IP Netmask
203.0.113.0/24
Resolve
Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)
Tags
OK
Cancel

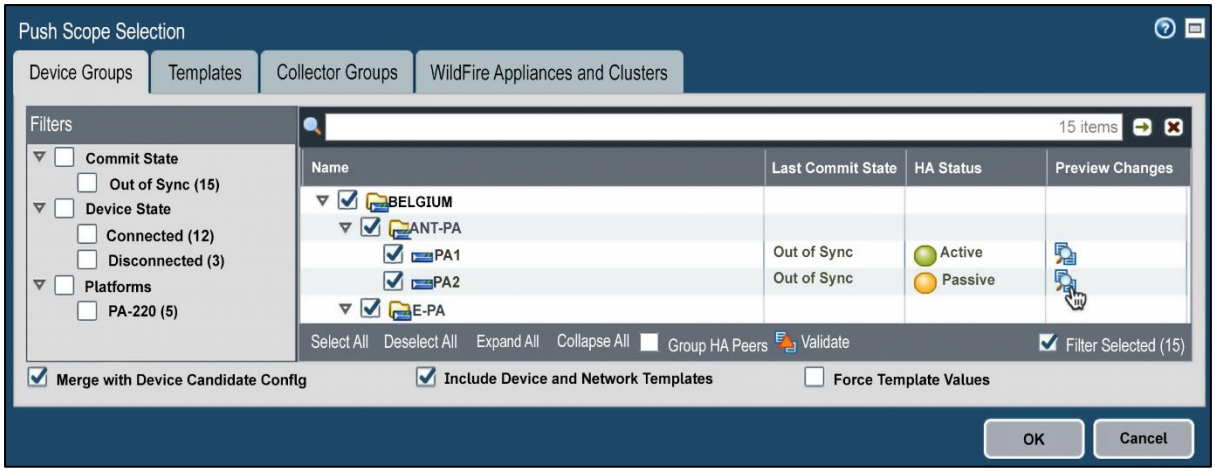

Shared Pre rule
Field firewalls Pre rule
EMEA Pre rule
Device Local Configuration
EMEA Post rule
Field Firewalls Post rule
Shared Post rule

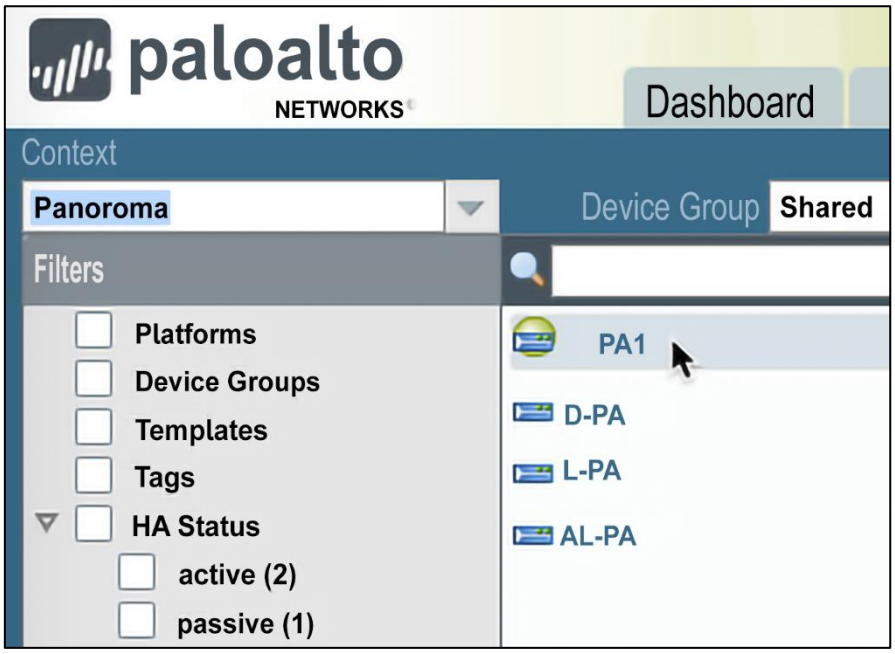

paloalto NETWORKS
DEVICE GROUPS
TEMP
Dashboard
ACC
Monitor
Policies
Objects
Network
Context
Panorama
Device Group EMEA
Security
Pre Rules
Post Rules
Default Rules
NAT
Pre Rules
Post Rules
QoS
Pre Rules
Post Rules
Policy Based Forwarding
Pre Rules
Post Rules
Decryption
Pre Rules
Post Rules
Tunnel Inspection
Pre Rules
Post Rules
Application Override
Pre Rules
Post Rules
Authentication
Pre Rules
Post Rules
DoS Protection
Pre Rules
Post Rules
Source
Name Location Tags Type Zone Address
1 shared pre - admin access Shared SHARED universal WAN HQ-admins
2 field pre- monitoring Field firewalls FIELD universal WAN PRTG
3 EMEA pre - regional cloud apps EMEA EMEA universal LAN any
Device Group Field firewalls
Source
Name Location Tags Type Zone Address
1 shared pre - admin access Shared SHARED universal WAN HQ-admins
2 field pre- monitoring Field firewalls FIELD universal WAN PRTG
Device Group Shared
Source
Name Location Tags Type Zone Address
1 shared pre - admin access Shared SHARED universal WAN HQ-admins
admin | Logout | Last Login Time: 03/16/2

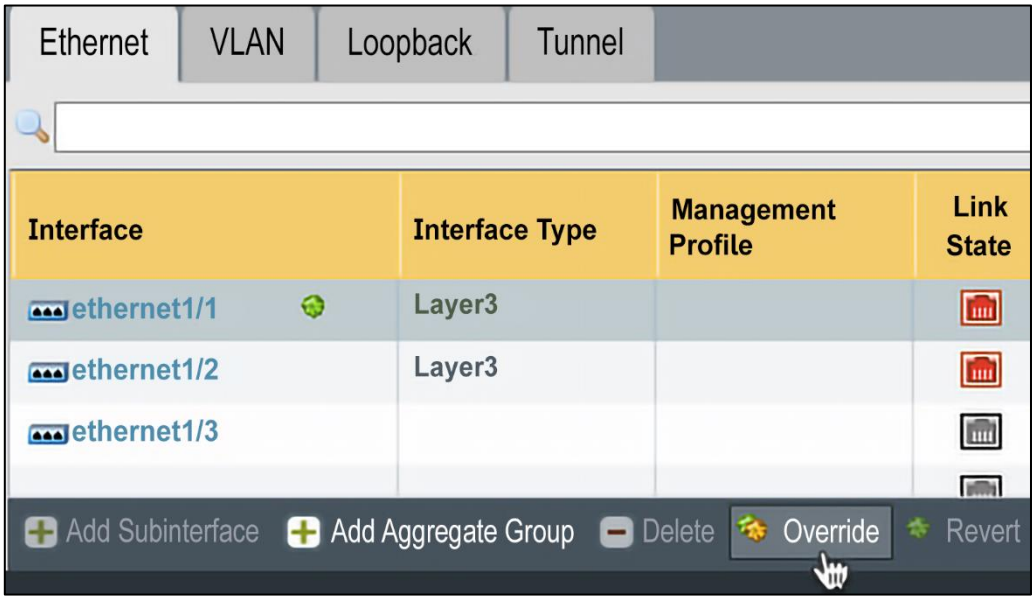

Log Forwarding Profile
Name default
Shared
Enable enhanced application logging to Logging Service (including traffic and url logs)
Description
3 items
Name Log Type Filter Forward Method Built-in Actions
traffic log traffic All Logs Panorama/Logging Service
threat log threat All Logs Panorama/Logging Service
url log url All Logs Panorama/Logging
Add Delete Clone
OK Cancel


Admin template
admin users
log-in banner
...
HQ stack
regional DNS, LDAP
...
EMEA stack
regional DNS, LDAP
...
APAC stack
regional DNS, LDAP
...
NAM stack
regional DNS, LDAP
...
Network template
zone names, zone protection/mgmt profiles
....
Management template
update schedule, ...

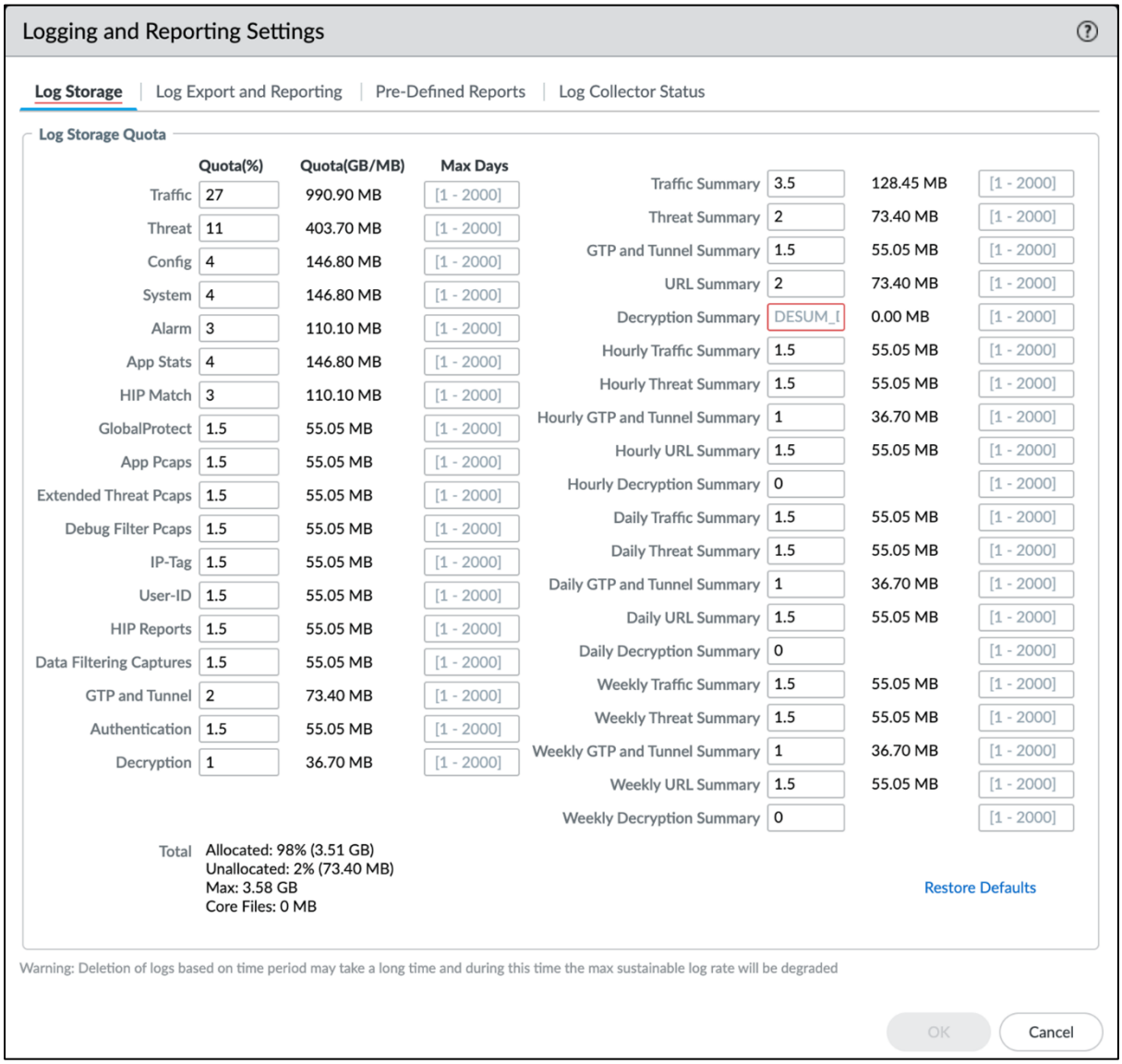

paloalto NETWORKS
DEVICE GROUPS
TEMPLATES
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Panorama
Context
Panorama
Template
Network Template
View by: Device
Mode
Multi VSYS; Normal Mode; VPN Enabled
Template
AdminTemplate
Management Template
Network Template
Template Stack
APACStack
AdminTemplate
Management Template
Network Template
EMEAStack
AdminTemplate
Management Template
Network Template
HQStack
AdminTemplate
Management Template
Network Template
Virtual Systems
Multi VSYS
Operational Mode
Normal
FIPS
Common Criteria
VPN Mode
Disable VPN
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
Interface
Management Profile
IP Address
Virtual
Slot
none
VR1
ping-resp
Untagged
vsys1

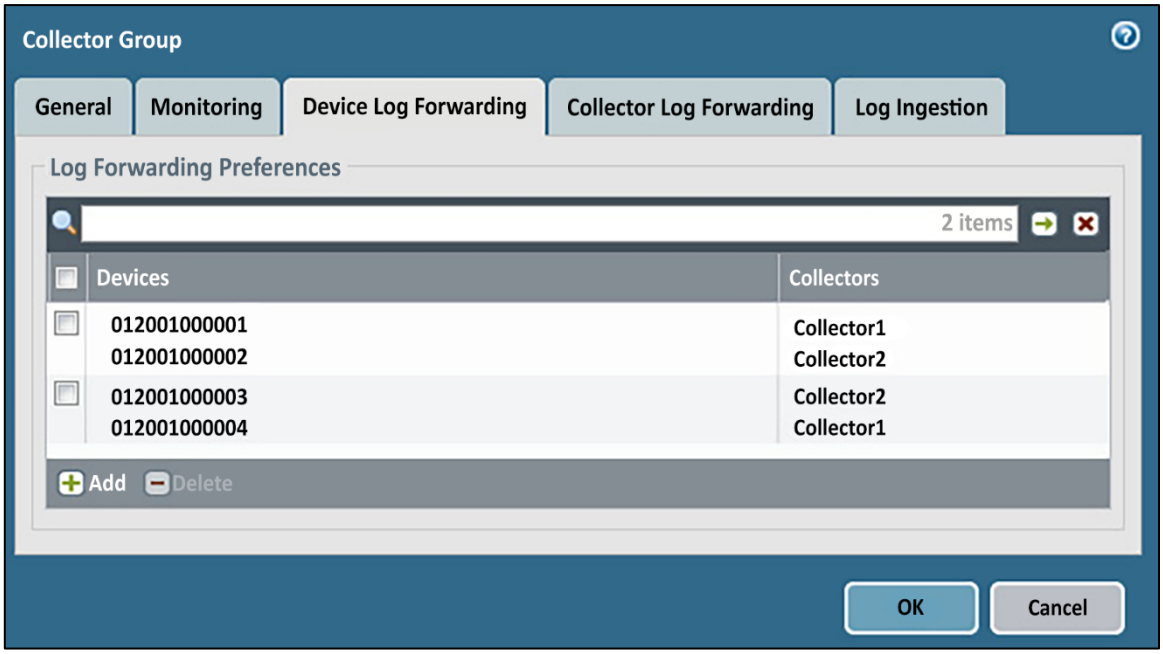

Push Scope Selection
Device Groups
Templates
Collector Groups
WildFire Appliances and Clusters
Filters
Commit State
Out of Sync (15)
Device State
Connected (12)
Disconnected (3)
Platforms
PA-220 (5)
15 items
Name
Last Commit State
HA Status
Preview Changes
BELGIUM
ANT-PA
PA1
Out of Sync
Active
PA2
Out of Sync
Passive
E-PA
Select All
Deselect All
Expand All
Collapse All
Group HA Peers
Validate
Filter Selected (15)
Merge with Device Candidate Config
Include Device and Network Templates
Force Template Values
OK
Cancel

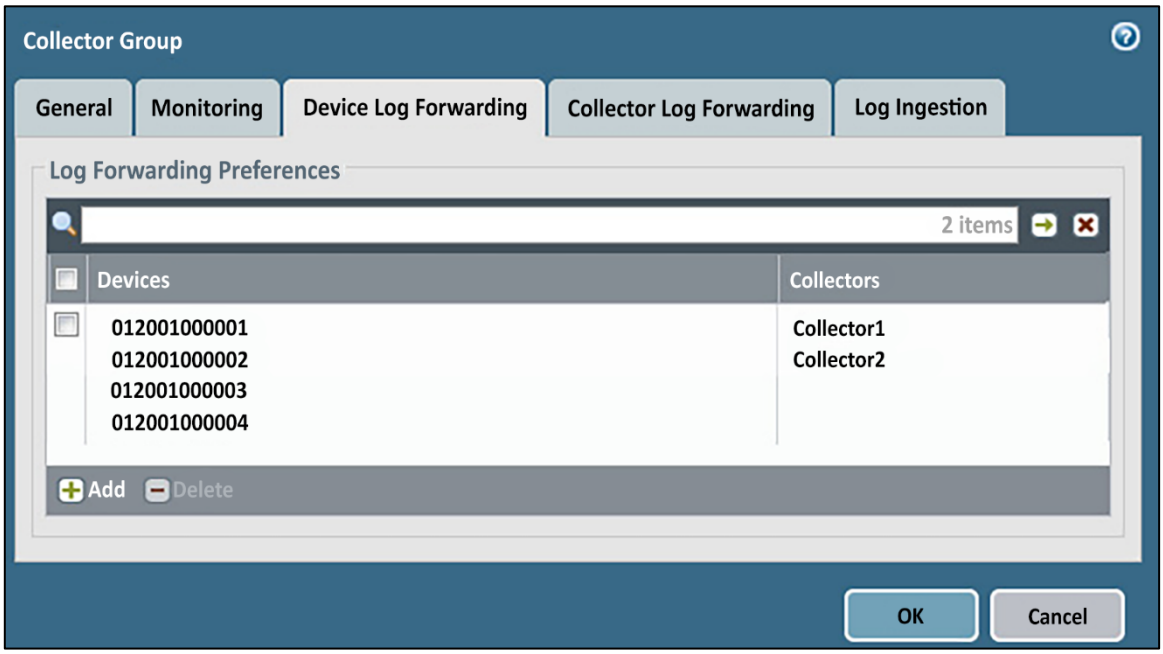

paloalto
NETWORKS
Dashboard
Context
Panoroma
Device Group
Shared
Filters
Platforms
Device Groups
Templates
Tags
HA Status
active (2)
passive (1)
PA1
D-PA
L-PA
AL-PA

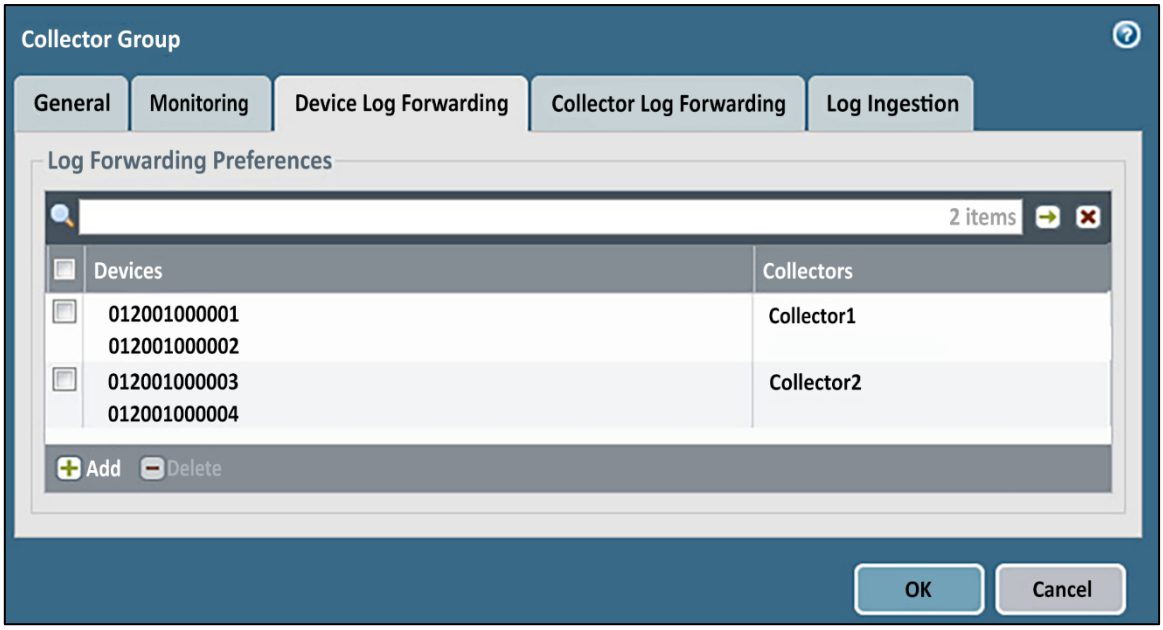

Ethernet
VLAN
Loopback
Tunnel
Interface
Interface Type
Management Profile
Link State
ethernet1/1
Layer3
ethernet1/2
Layer3
ethernet1/3
Add Subinterface
Add Aggregate Group
Delete
Override
Revert

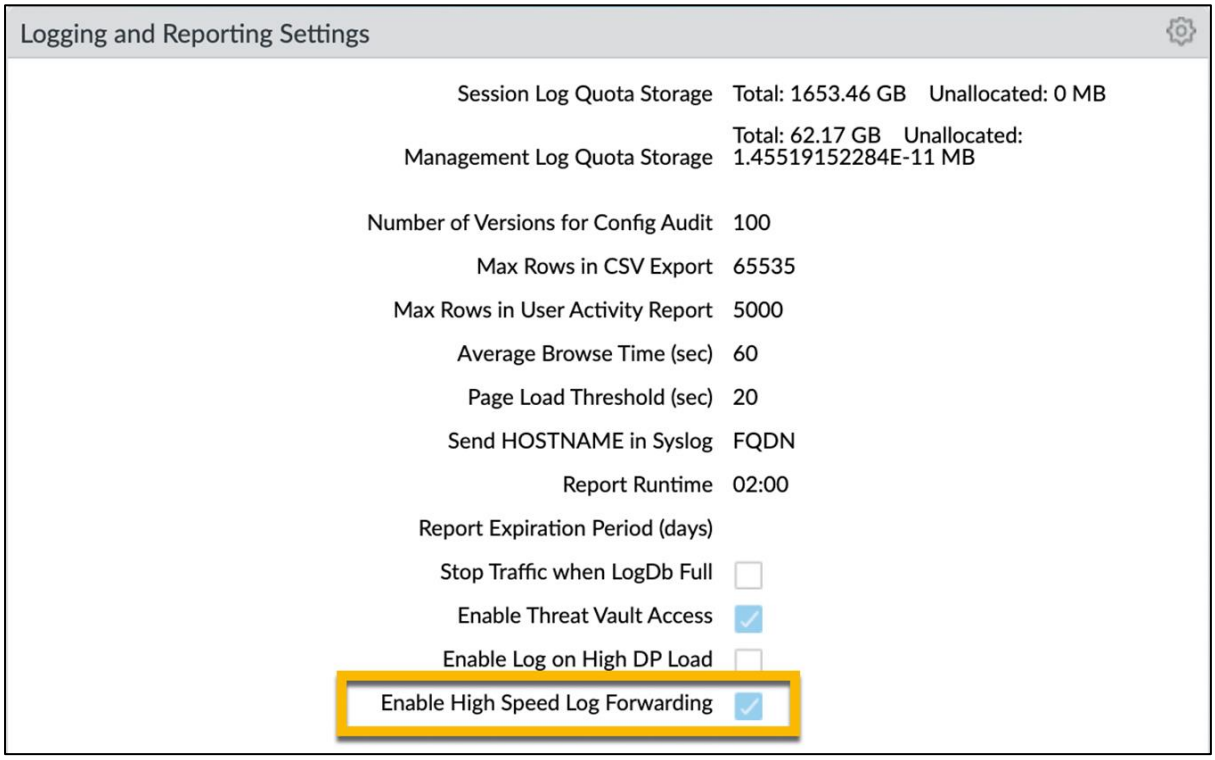
Chapter 9: Logging and Reporting

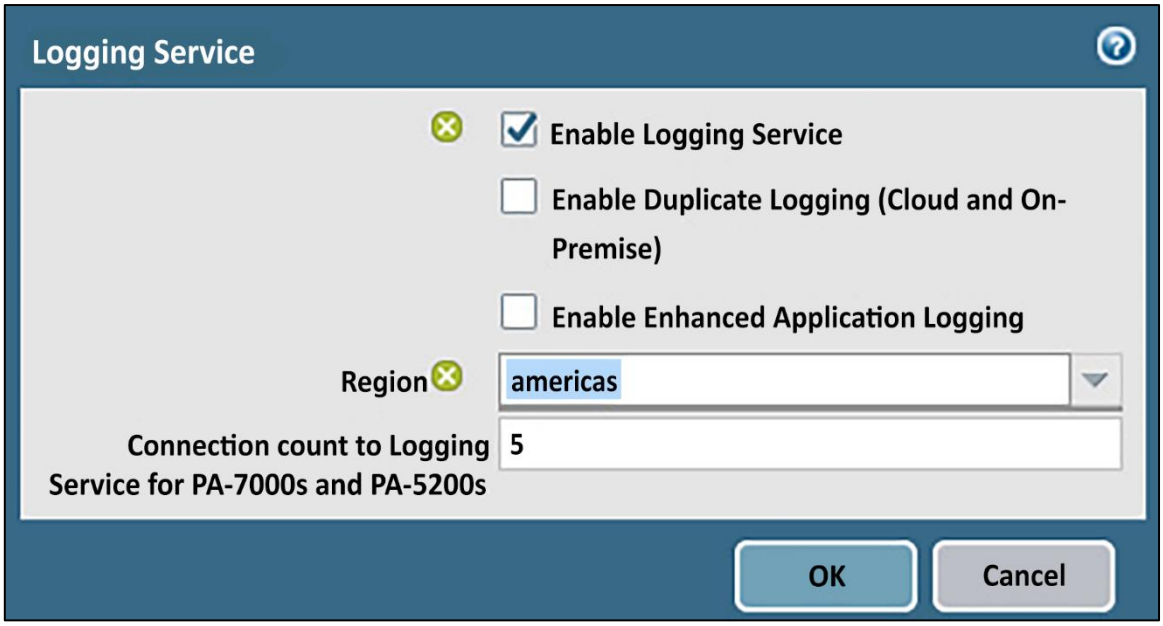


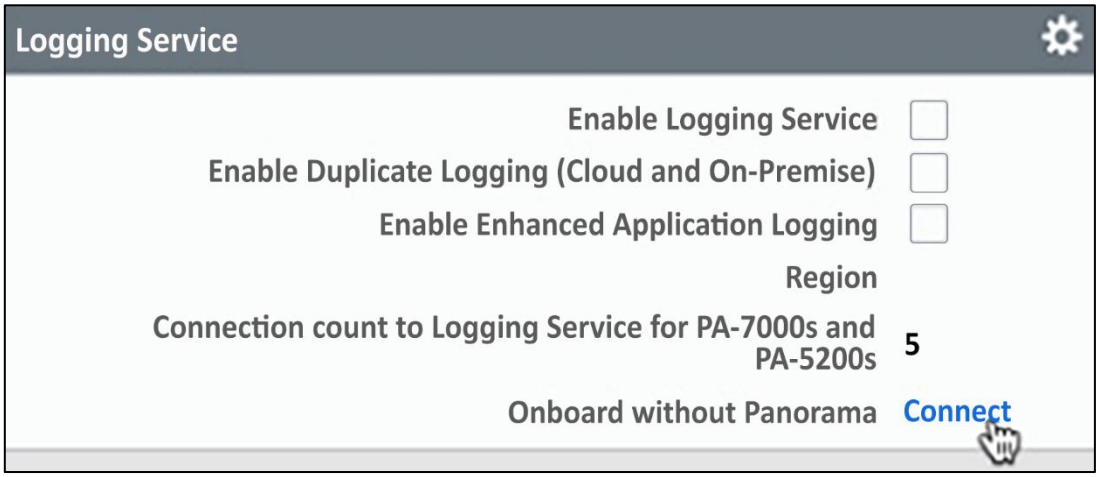

Collector Group
General
Monitoring
Device Log Forwarding
Collector Log Forwarding
Log Ingestion
Log Forwarding Preferences
2 items
Devices
Collectors
012001000001
012001000002
012001000003
012001000004
Collector1
Collector2
Collector2
Collector1
Add
Delete
OK
Cancel

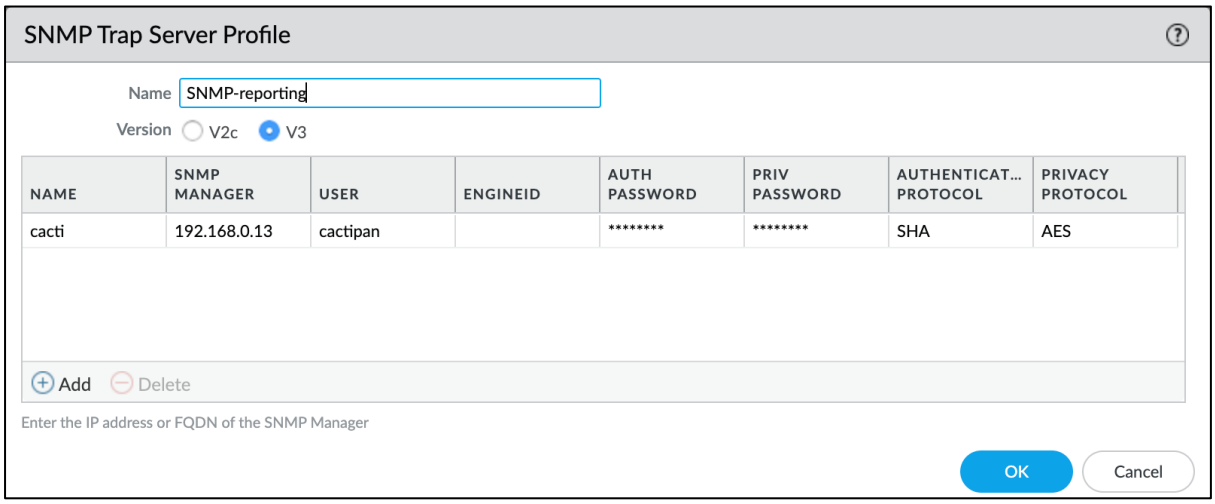

Collector Group
General
Monitoring
Device Log Forwarding
Collector Log Forwarding
Log Ingestion
Log Forwarding Preferences
2 items
Devices
Collectors
012001000001
012001000002
012001000003
012001000004
Collector1
Collector2
Add
Delete
OK
Cancel


Collector Group
General
Monitoring
Device Log Forwarding
Collector Log Forwarding
Log Ingestion
Log Forwarding Preferences
2 items
Devices
Collectors
012001000001
012001000002
Collector1
012001000003
012001000004
Collector2
Add
Delete
OK
Cancel


Logging and Reporting Settings
Session Log Quota Storage
Total: 1653.46 GB Unallocated: 0 MB
Management Log Quota Storage
Total: 62.17 GB Unallocated: 1.45519152284E-11 MB
Number of Versions for Config Audit
100
Max Rows in CSV Export
65535
Max Rows in User Activity Report
5000
Average Browse Time (sec)
60
Page Load Threshold (sec)
20
Send HOSTNAME in Syslog
FQDN
Report Runtime
02:00
Report Expiration Period (days)
Stop Traffic when LogDb Full
Enable Threat Vault Access
Enable Log on High DP Load
Enable High Speed Log Forwarding


Logging Service
Enable Logging Service
Enable Duplicate Logging (Cloud and On-Premise)
Enable Enhanced Application Logging
Region
americas
Connection count to Logging Service for PA-7000s and PA-5200s
5
OK
Cancel

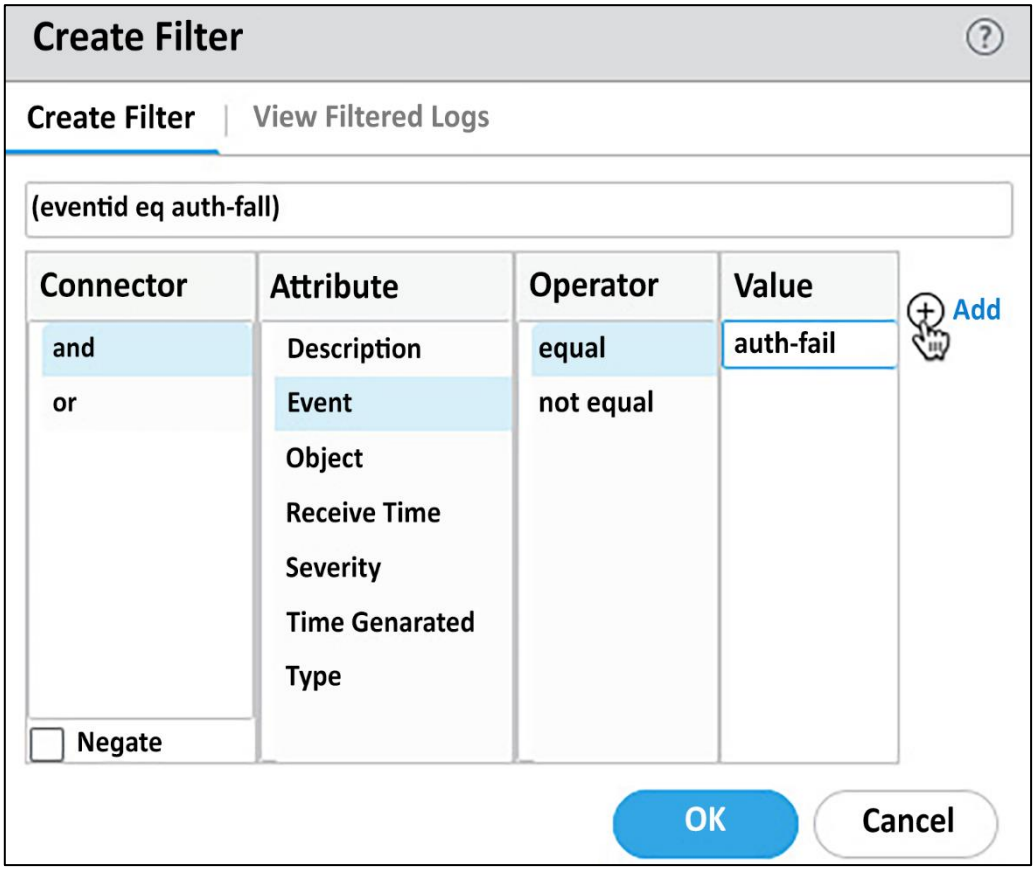

Logging Service
Enable Logging Service
Enable Duplicate Logging (Cloud and On-Premise)
Enable Enhanced Application Logging
Region
Connection count to Logging Service for PA-7000s and PA-5200s
5
Onboard without Panorama
Connect


SNMP Trap Server Profile
Name
SNMP-reporting
Version
V2c
V3
NAME
SNMP MANAGER
USER
ENGINEID
AUTH PASSWORD
PRIV PASSWORD
AUTHENTICAT... PROTOCOL
PRIVACY PROTOCOL
cacti
192.168.0.13
cactipan
****
****
SHA
AES
Add
Delete
Enter the IP address or FQDN of the SNMP Manager
OK
Cancel

System

	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG	HTTP
☐	logs-to-panorama		(severity geq medium)	☑				
☐	alert-OpSecTeam	failed login	(eventid eq auth-fail)	☐		SecTeam-email	splunk	

Add Delete Clone PDF/CSV



Log Forwarding Profile

Name default

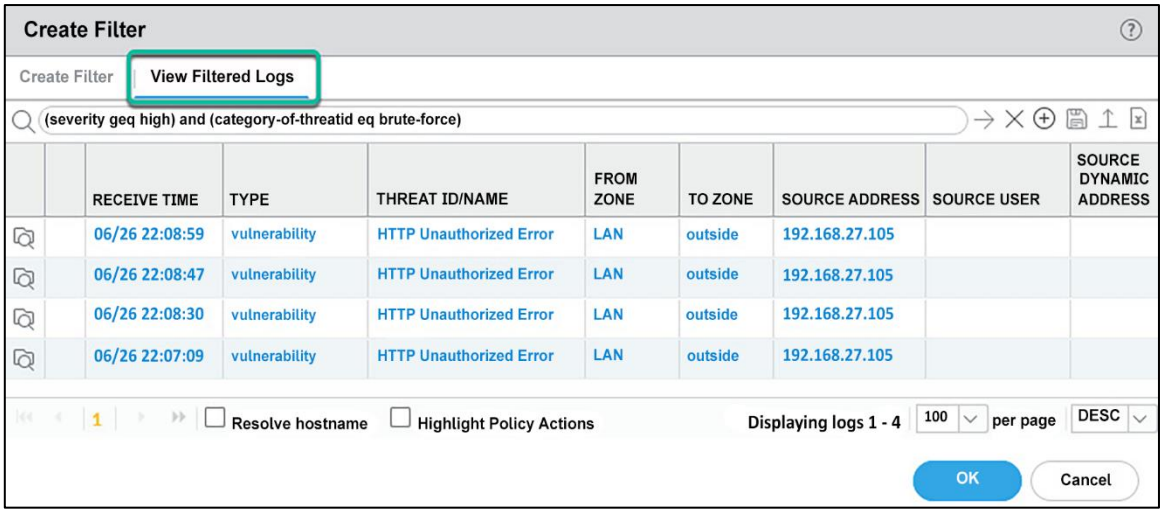
Description

5 items

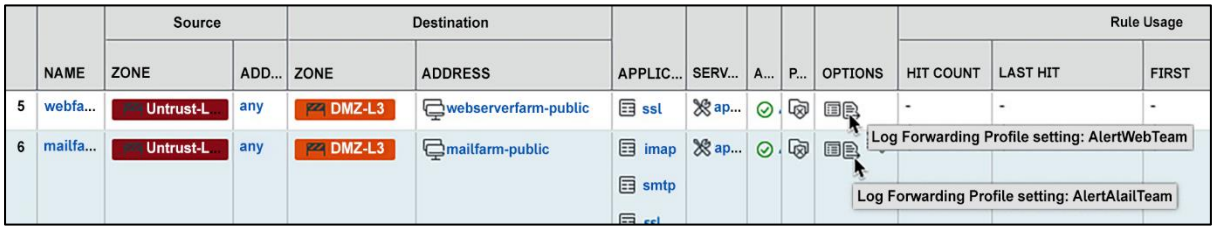
	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
☐	Threat-to-Panorama	threat	All Logs	• Panorama/Logging Service	
☐	Traffic-to-Panorama	traffic	All Logs	• Panorama/Logging Service	
☐	URL-to_Panorama	url	All Logs	• Panorama/Logging Service	
☐	WildFire-to-Panorama	wildfire	All Logs	• Panorama/Logging Service	
☐	Alert-SecTeam	threat	(severity geq high) and (category-of-threatid eq brute-force)	Email • SecTeam-email SysLog • splunk	

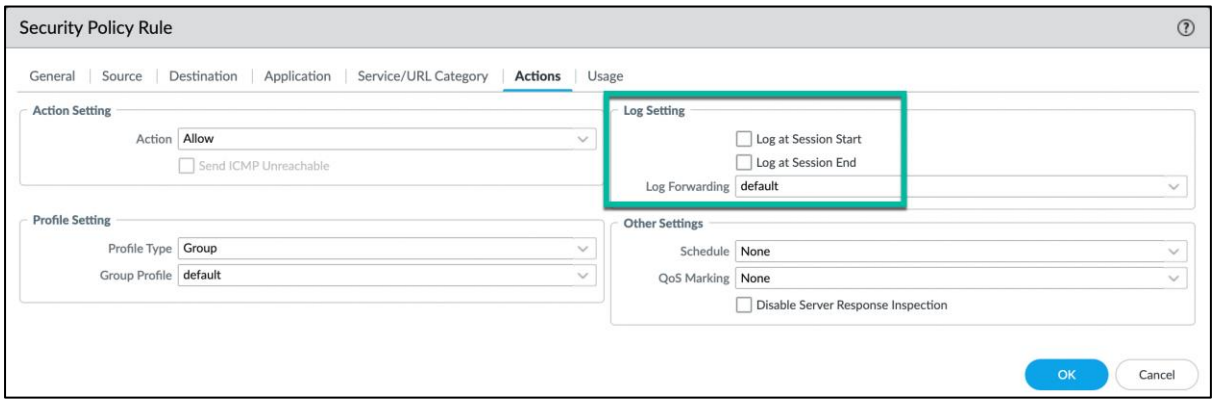
Add Delete Clone

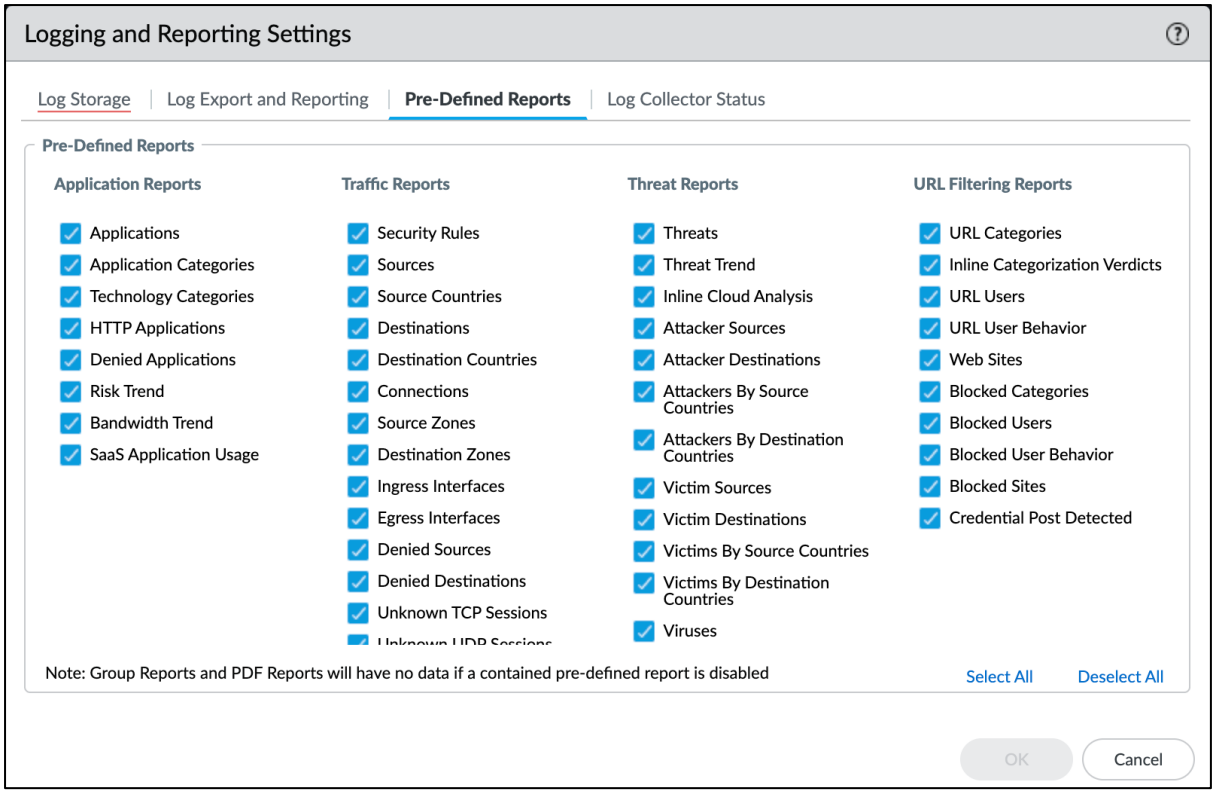
OK Cancel

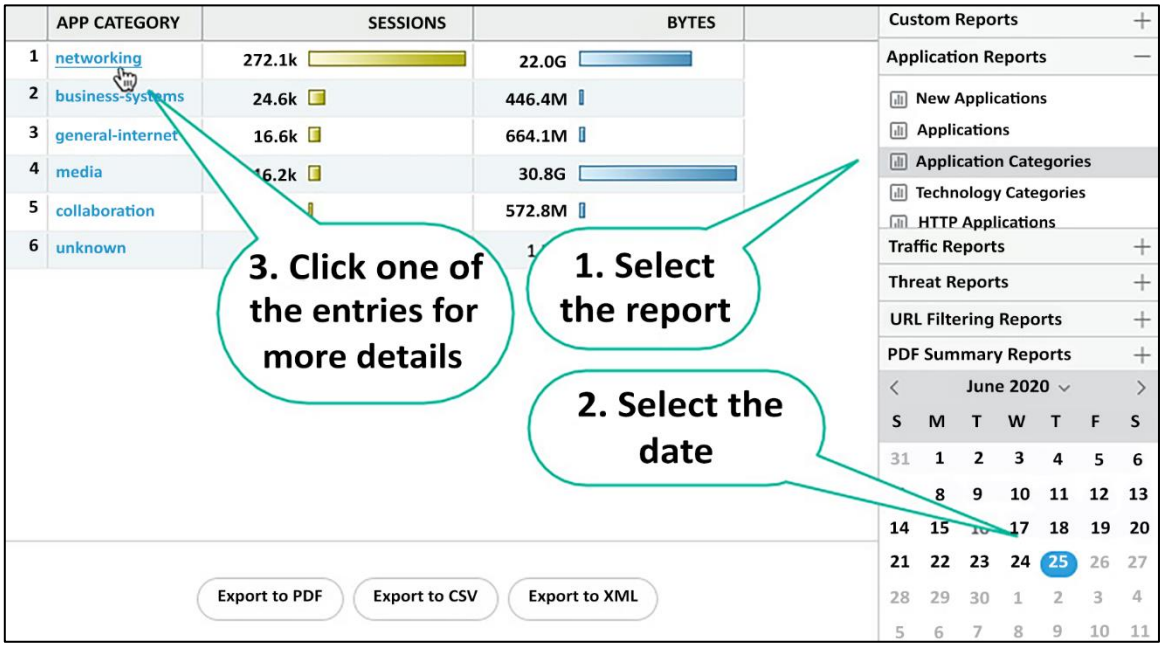


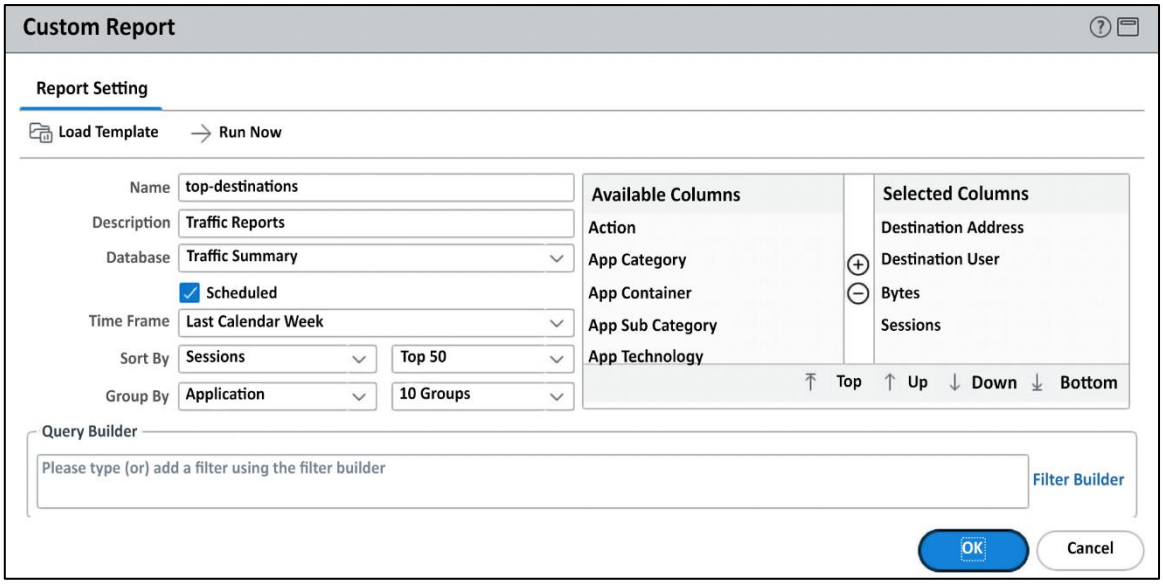
AlertMailTeam	alert mail team on critical events	traffic threat url threat	All Logs All Logs All Logs (severity geq high)	✓ ✓	MailTeam	splunk
AlertWebTeam	alert mail team on critical events	traffic threat url threat	All Logs All Logs All Logs (severity geq high)	✓ ✓	WebTeam	splunk

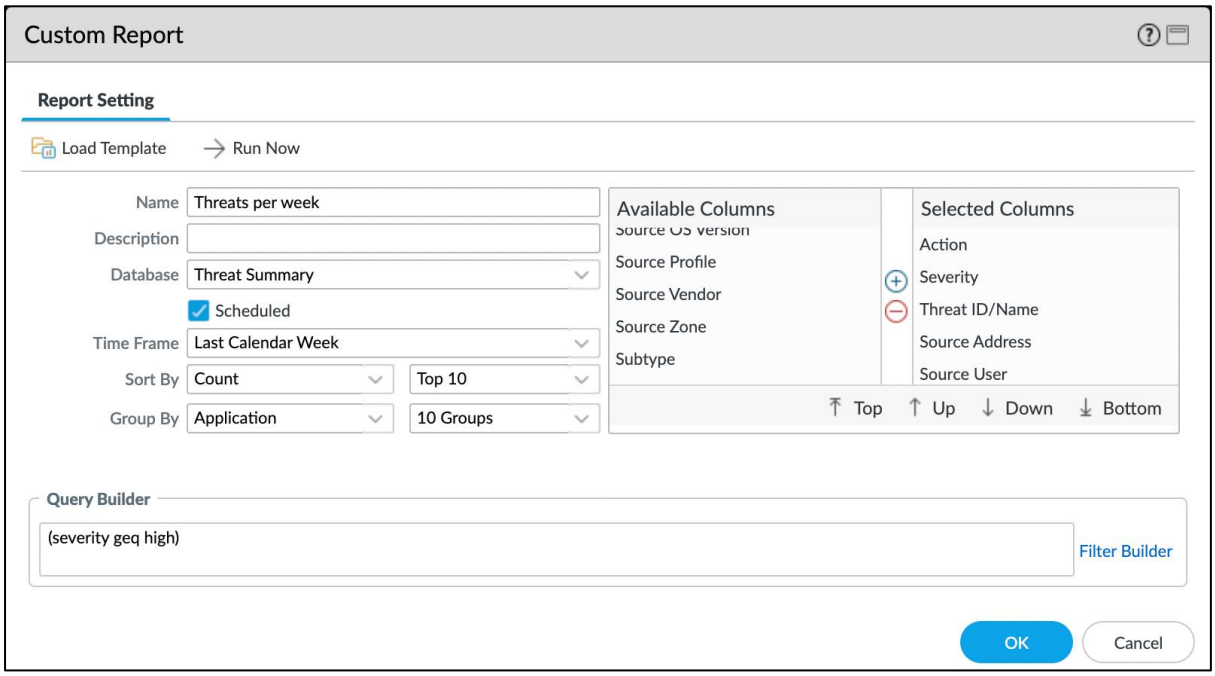


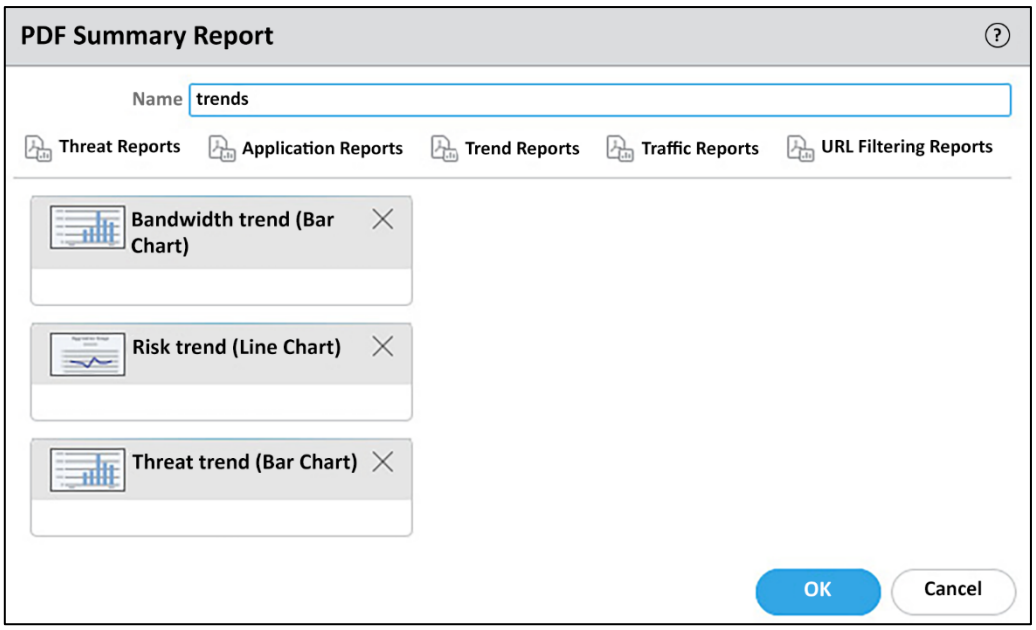


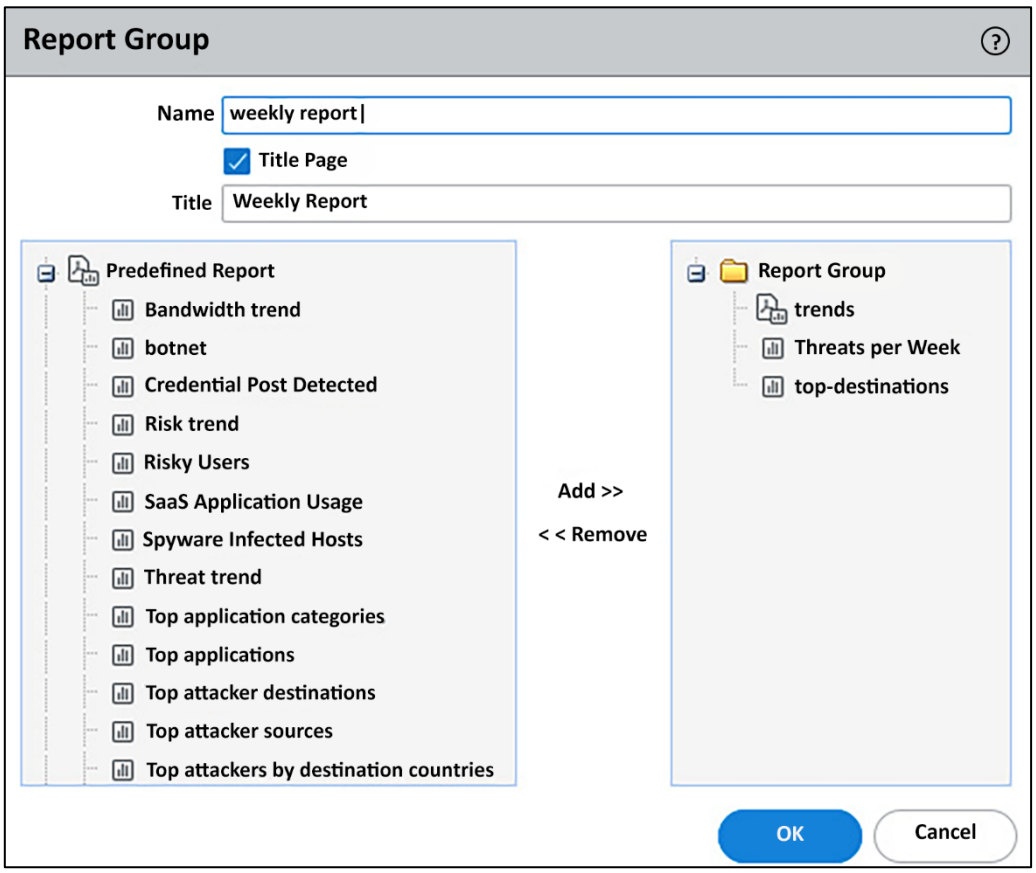

Logging and Reporting Settings
Log Storage
Log Export and Reporting
Pre-Defined Reports
Log Collector Status
Pre-Defined Reports
Application Reports
Applications
Application Categories
Technology Categories
HTTP Applications
Denied Applications
Risk Trend
Bandwidth Trend
SaaS Application Usage
Traffic Reports
Security Rules
Sources
Source Countries
Destinations
Destination Countries
Connections
Source Zones
Destination Zones
Ingress Interfaces
Egress Interfaces
Denied Sources
Denied Destinations
Unknown TCP Sessions
Threat Reports
Threats
Threat Trend
Inline Cloud Analysis
Attacker Sources
Attacker Destinations
Attackers By Source Countries
Attackers By Destination Countries
Victim Sources
Victim Destinations
Victims By Source Countries
Victims By Destination Countries
Viruses
URL Filtering Reports
URL Categories
Inline Categorization Verdicts
URL Users
URL User Behavior
Web Sites
Blocked Categories
Blocked Users
Blocked User Behavior
Blocked Sites
Credential Post Detected
Note: Group Reports and PDF Reports will have no data if a contained pre-defined report is disabled
Select All
Deselect All
OK
Cancel

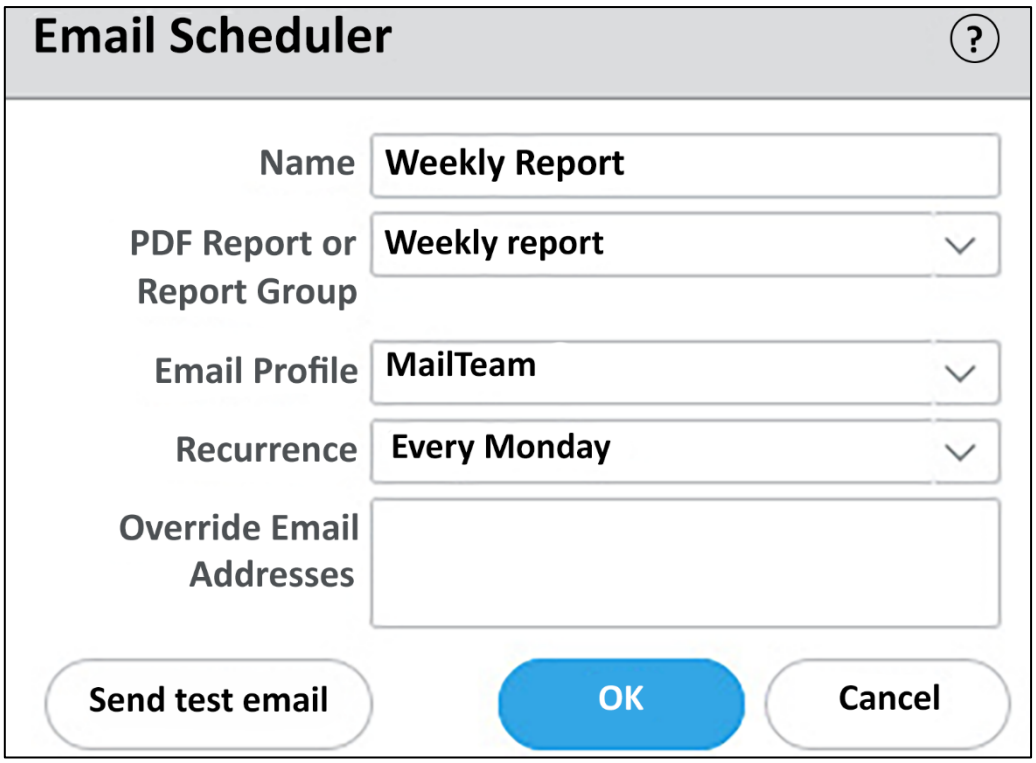

APP CATEGORY
SESSIONS
BYTES
1 networking 272.1k 22.0G
2 business-systems 24.6k 446.4M
3 general-internet 16.6k 664.1M
4 media 16.2k 30.8G
5 collaboration 572.8M
6 unknown
3. Click one of the entries for more details
1. Select the report
2. Select the date
Export to PDF
Export to CSV
Export to XML
Custom Reports
Application Reports
New Applications
Applications
Application Categories
Technology Categories
HTTP Applications
Traffic Reports
Threat Reports
URL Filtering Reports
PDF Summary Reports
June 2020
S M T W T F S
31 1 2 3 4 5 6
8 9 10 11 12 13
14 15 17 18 19 20
21 22 23 24 25 26 27
28 29 30 1 2 3 4
5 6 7 8 9 10 11

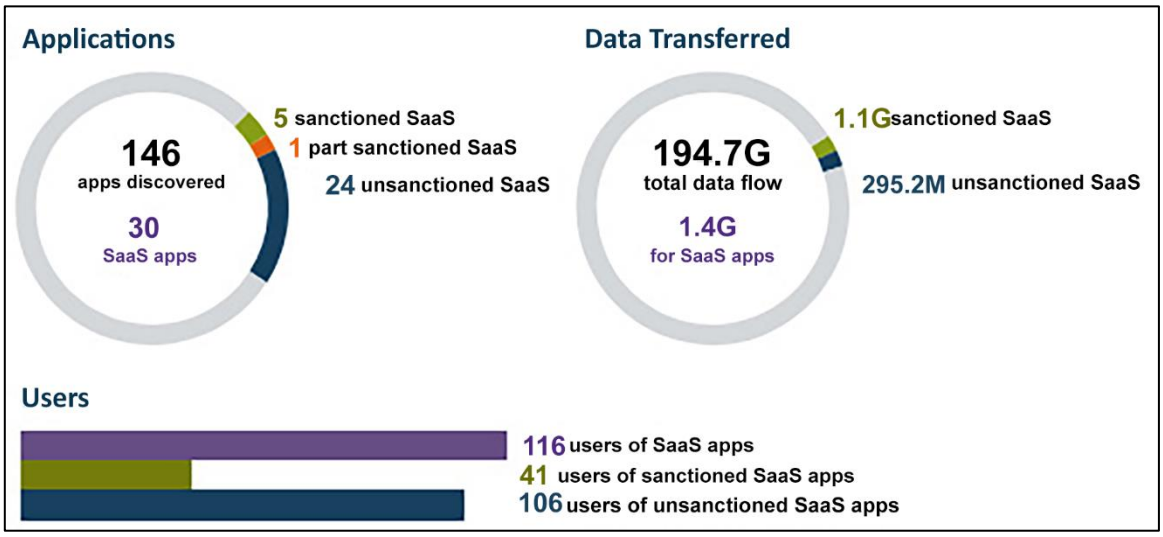

Custom Report
Report Setting
Load Template
Run Now
Name
top-destinations
Description
Traffic Reports
Database
Traffic Summary
Scheduled
Time Frame
Last Calendar Week
Sort By
Sessions
Top 50
Group By
Application
10 Groups
Available Columns
Action
App Category
App Container
App Sub Category
App Technology
Selected Columns
Destination Address
Destination User
Bytes
Sessions
Top
Up
Down
Bottom
Query Builder
Please type (or) add a filter using the filter builder
Filter Builder
OK
Cancel

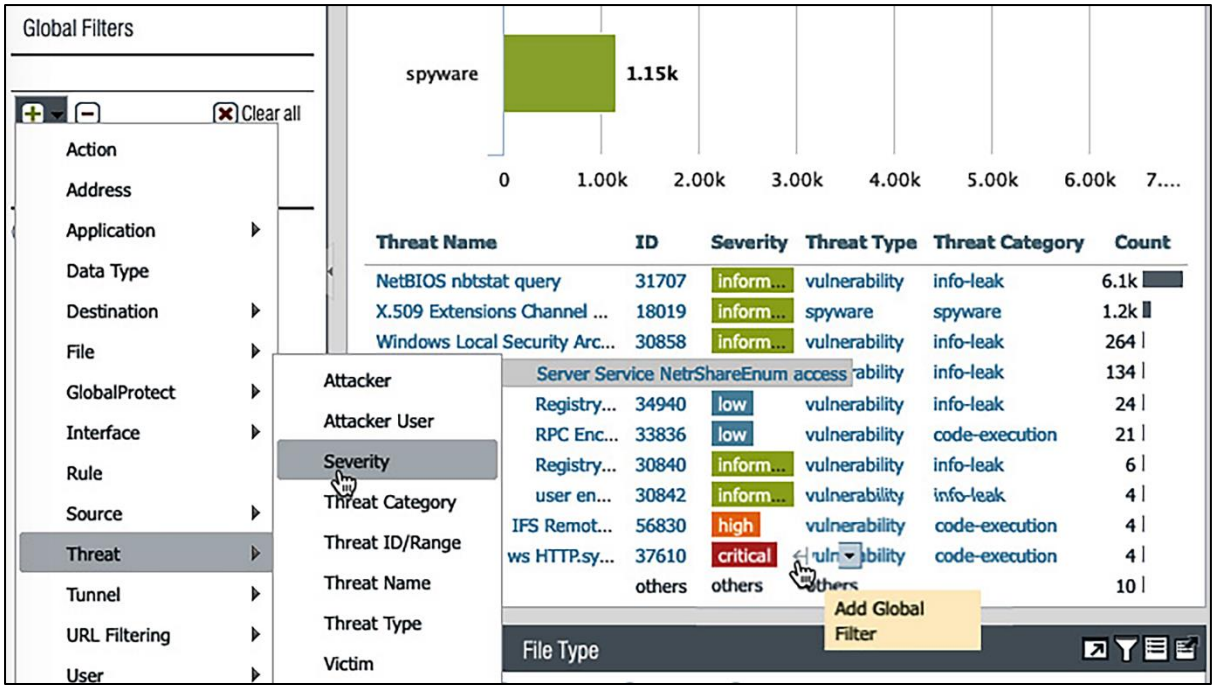

Custom Report
Report Setting
Load Template
Run Now
Name
Threats per week
Description
Database
Threat Summary
Scheduled
Time Frame
Last Calendar Week
Sort By
Count
Top 10
Group By
Application
10 Groups
Available Columns
Source Profile
Source Vendor
Source Zone
Subtype
Selected Columns
Action
Severity
Threat ID/Name
Source Address
Source User
Top
Up
Down
Bottom
Query Builder
(severity geq high)
Filter Builder
OK
Cancel

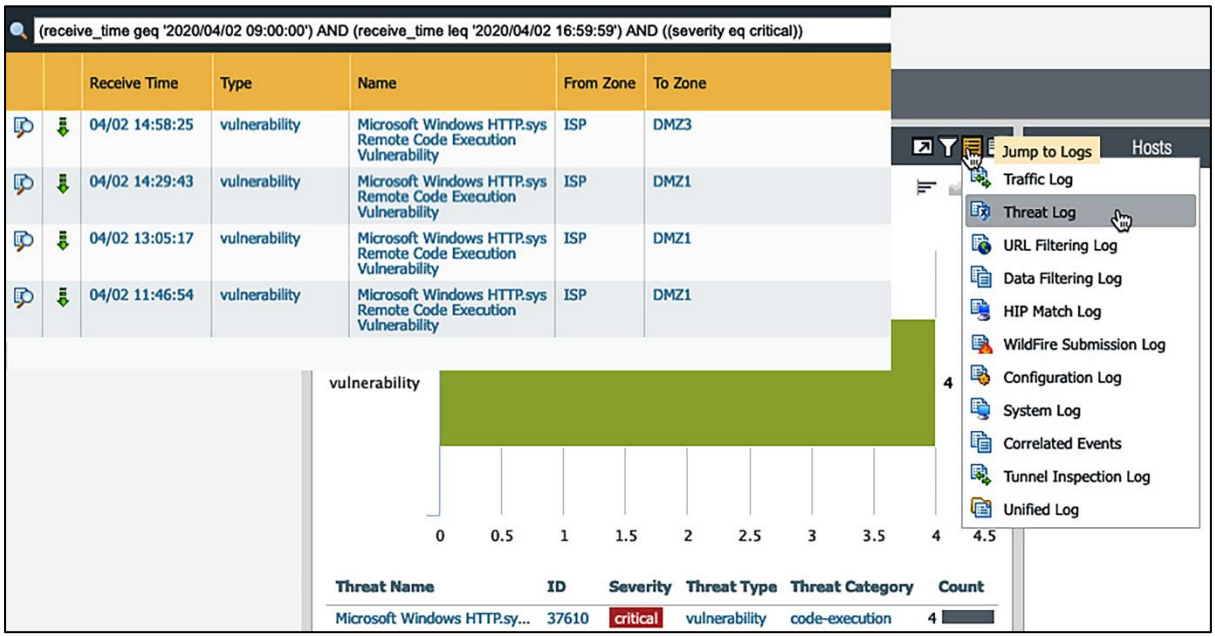

PDF Summary Report
Name
trends
Threat Reports
Application Reports
Trend Reports
Traffic Reports
URL Filtering Reports
Bandwidth trend (Bar Chart)
Risk trend (Line Chart)
Threat trend (Bar Chart)
OK
Cancel

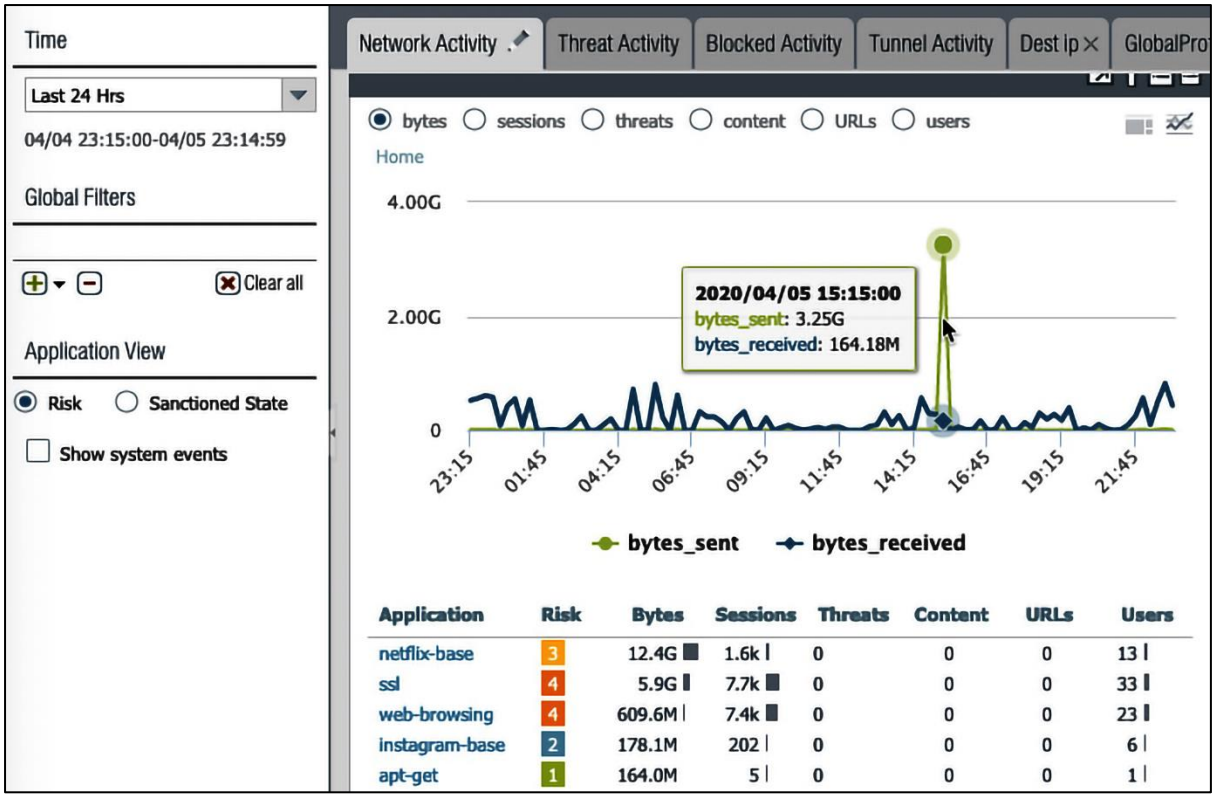

Report Group
Name
weekly report
Title Page
Title
Weekly Report
Predefined Report
Bandwidth trend
botnet
Credential Post Detected
Risk trend
Risky Users
SaaS Application Usage
Spyware Infected Hosts
Threat trend
Top application categories
Top applications
Top attacker destinations
Top attacker sources
Top attackers by destination countries
Add >>
< < Remove
Report Group
trends
Threats per Week
top-destinations
OK
Cancel

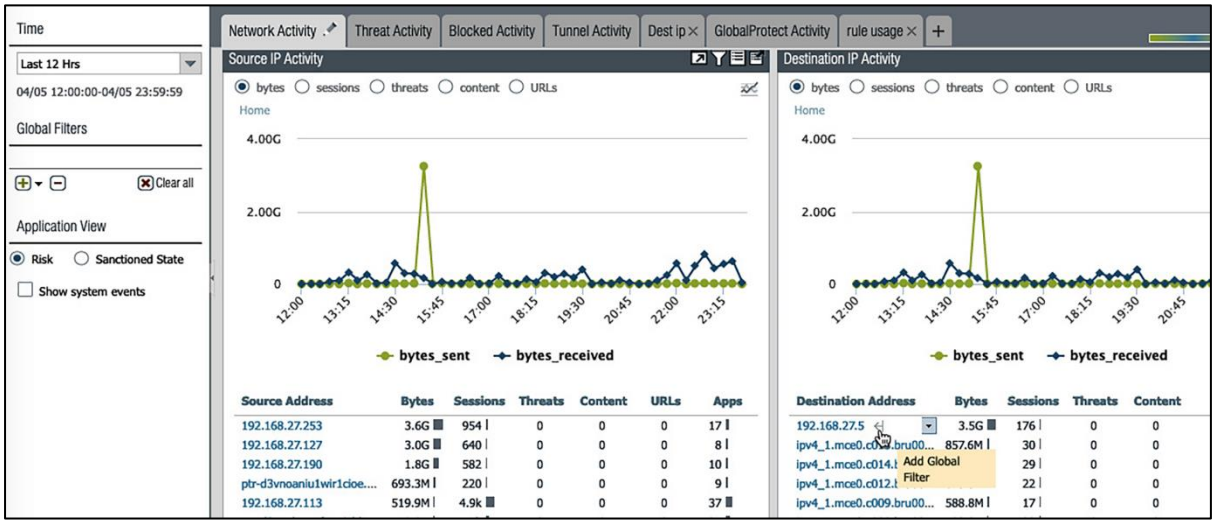

Email Scheduler
?
Name
Weekly Report
PDF Report or Report Group
Weekly report
Email Profile
MailTeam
Recurrence
Every Monday
Override Email Addresses
Send test email
OK
Cancel

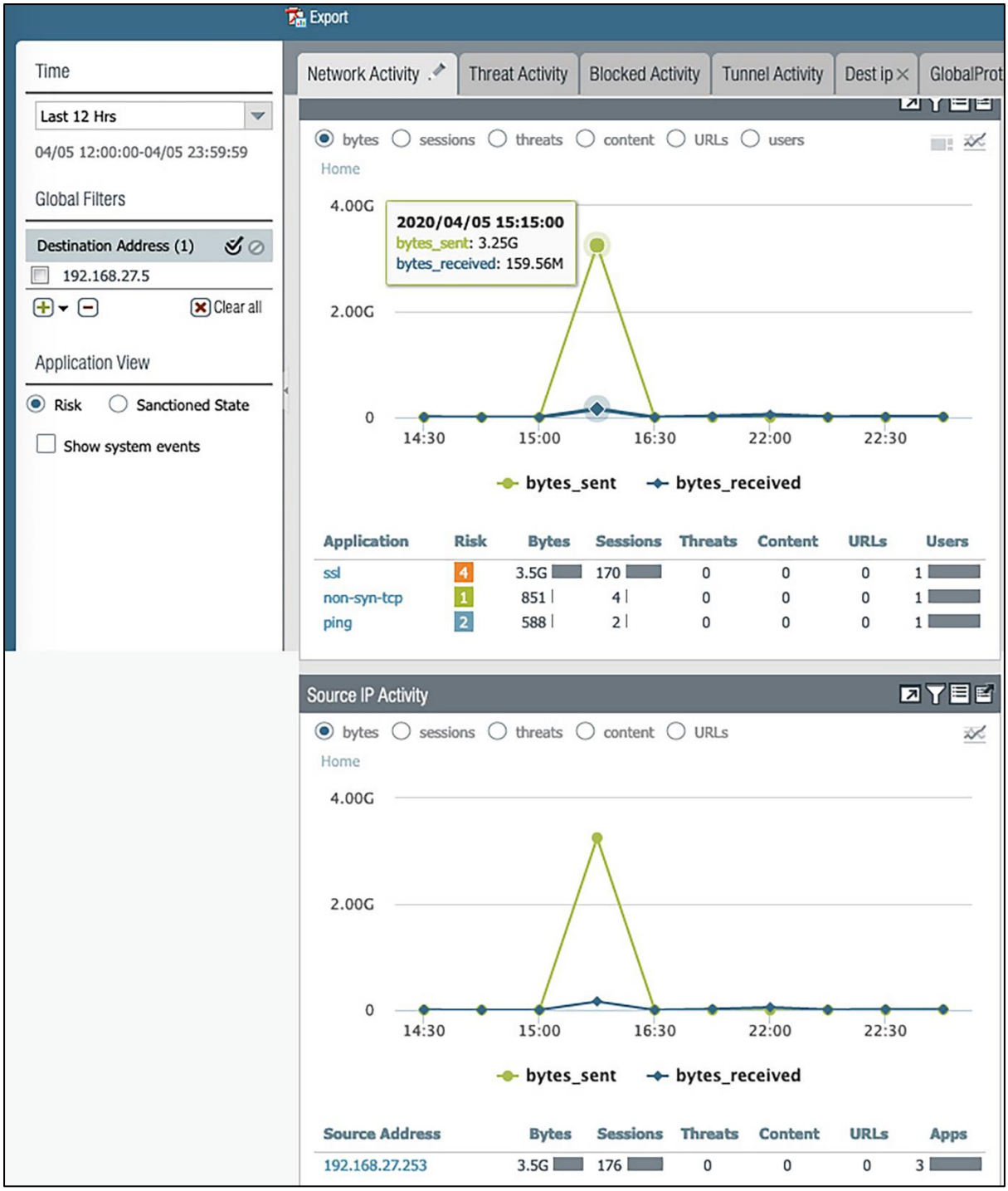

Applications
146
apps discovered
30
SaaS apps
5 sanctioned SaaS
1 part sanctioned SaaS
24 unsanctioned SaaS
Data Transferred
194.7G
total data flow
1.4G
for SaaS apps
1.1G sanctioned SaaS
295.2M unsanctioned SaaS
Users
116 users of SaaS apps
41 users of sanctioned SaaS apps
106 users of unsanctioned SaaS apps

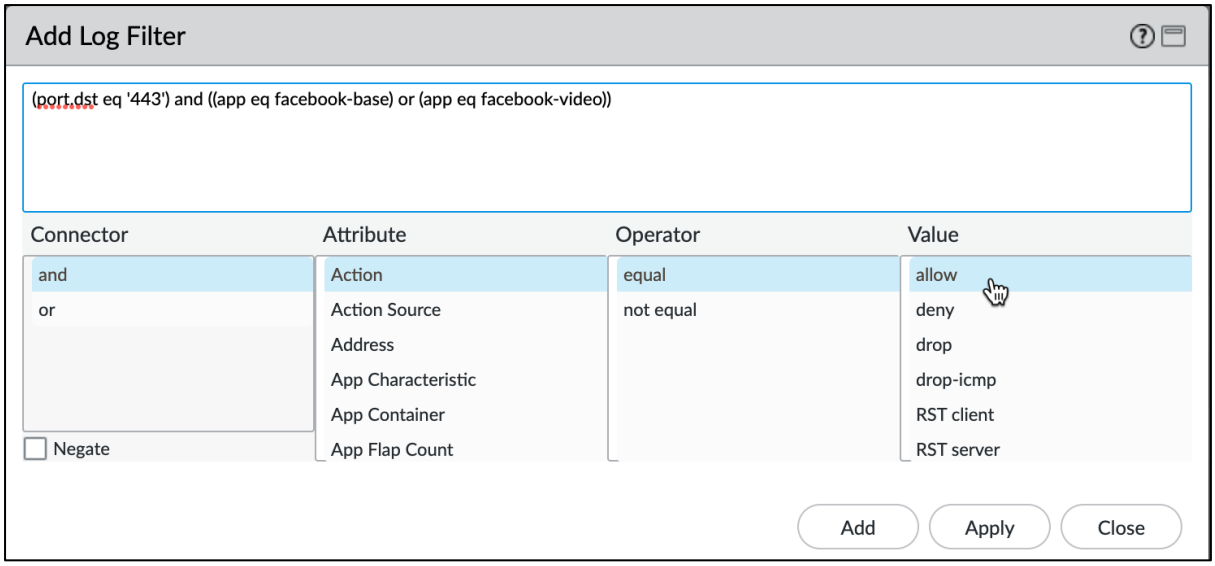

Global Filters
Clear all
Action
Address
Application
Data Type
Destination
File
GlobalProtect
Interface
Rule
Source
Threat
Tunnel
URL Filtering
User
Attacker
Attacker User
Severity
Threat Category
Threat ID/Range
Threat Name
Threat Type
Victim
spyware
1.15k
0
1.00k
2.00k
3.00k
4.00k
5.00k
6.00k
7....
Threat Name
ID
Severity
Threat Type
Threat Category
Count
NetBIOS nbtstat query
31707
inform...
vulnerability
info-leak
6.1k
X.509 Extensions Channel ...
18019
inform...
spyware
spyware
1.2k
Windows Local Security Arc...
30858
inform...
vulnerability
info-leak
264
Server Service NetrShareEnum access
info-leak
134
Registry...
34940
low
vulnerability
info-leak
24
RPC Enc...
33836
low
vulnerability
code-execution
21
Registry...
30840
inform...
vulnerability
info-leak
6
user en...
30842
inform...
vulnerability
info-leak
4
IFS Remot...
56830
high
vulnerability
code-execution
4
ws HTTP.sy...
37610
critical
code-execution
4
others
others
10
Add Global Filter
File Type

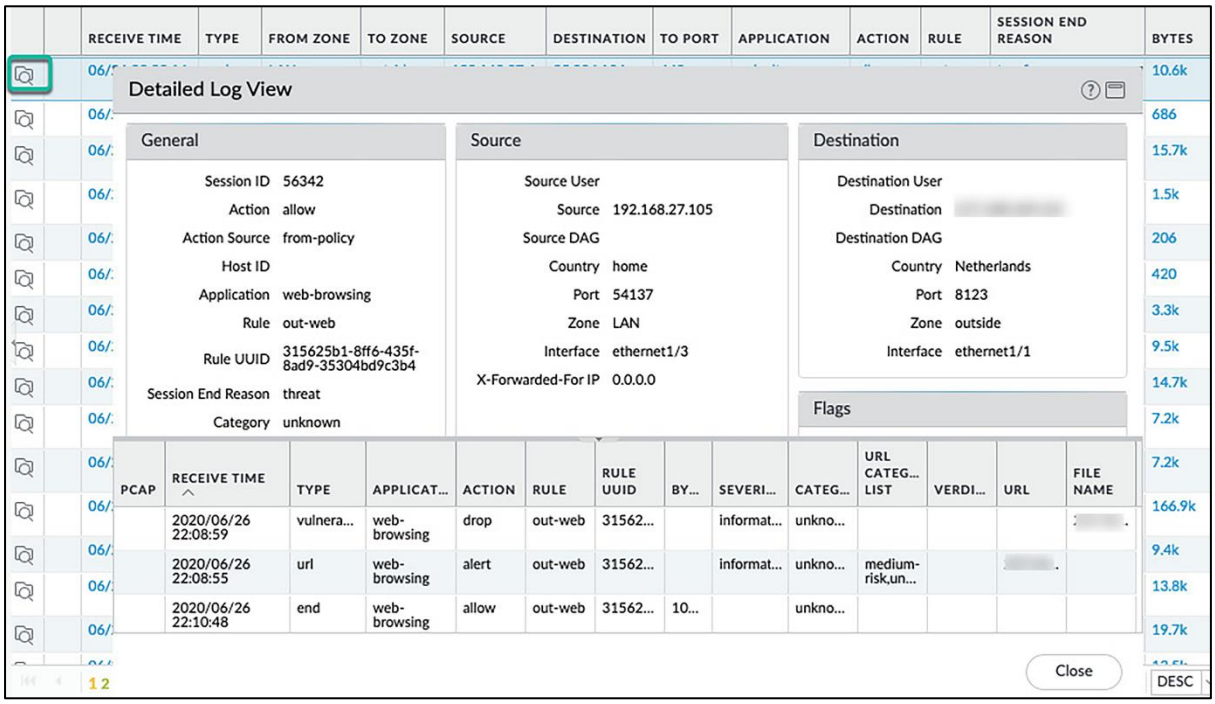

(receive_time geq '2020/04/02 09:00:00') AND (receive_time leq '2020/04/02 16:59:59') AND ((severity eq critical))
Receive Time
Type
Name
From Zone
To Zone
04/02 14:58:25
vulnerability
Microsoft Windows HTTP.sys Remote Code Execution Vulnerability
ISP
DMZ3
04/02 14:29:43
vulnerability
Microsoft Windows HTTP.sys Remote Code Execution Vulnerability
ISP
DMZ1
04/02 13:05:17
vulnerability
Microsoft Windows HTTP.sys Remote Code Execution Vulnerability
ISP
DMZ1
04/02 11:46:54
vulnerability
Microsoft Windows HTTP.sys Remote Code Execution Vulnerability
ISP
DMZ1
Jump to Logs
Hosts
Traffic Log
Threat Log
URL Filtering Log
Data Filtering Log
HIP Match Log
WildFire Submission Log
Configuration Log
System Log
Correlated Events
Tunnel Inspection Log
Unified Log
vulnerability
4
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
Threat Name
ID
Severity
Threat Type
Threat Category
Count
Microsoft Windows HTTP.sy...
37610
critical
vulnerability
code-execution
4

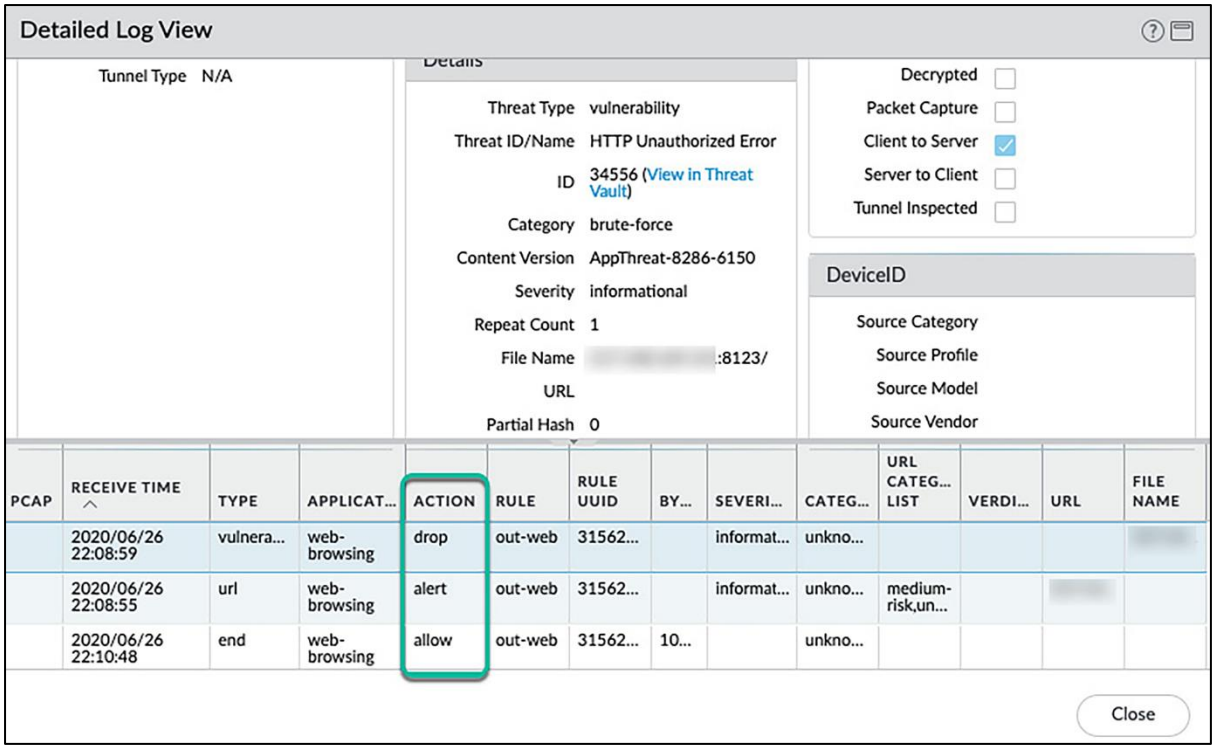

Time
Last 24 Hrs
04/04 23:15:00-04/05 23:14:59
Global Filters
Clear all
Application View
Risk
Sanctioned State
Show system events
Network Activity
Threat Activity
Blocked Activity
Tunnel Activity
Dest ip
GlobalPro
bytes
sessions
threats
content
URLs
users
Home
4.00G
2.00G
0
2020/04/05 15:15:00
bytes_sent: 3.25G
bytes_received: 164.18M
23:15
01:45
04:15
06:45
09:15
11:45
14:15
16:45
19:15
21:45
bytes_sent
bytes_received
Application Risk Bytes Sessions Threats Content URLs Users
netflix-base 3 12.4G 1.6k 0 0 0 13
ssl 4 5.9G 7.7k 0 0 0 33
web-browsing 4 609.6M 7.4k 0 0 0 23
instagram-base 2 178.1M 202 0 0 0 6
apt-get 1 164.0M 5 0 0 0 1

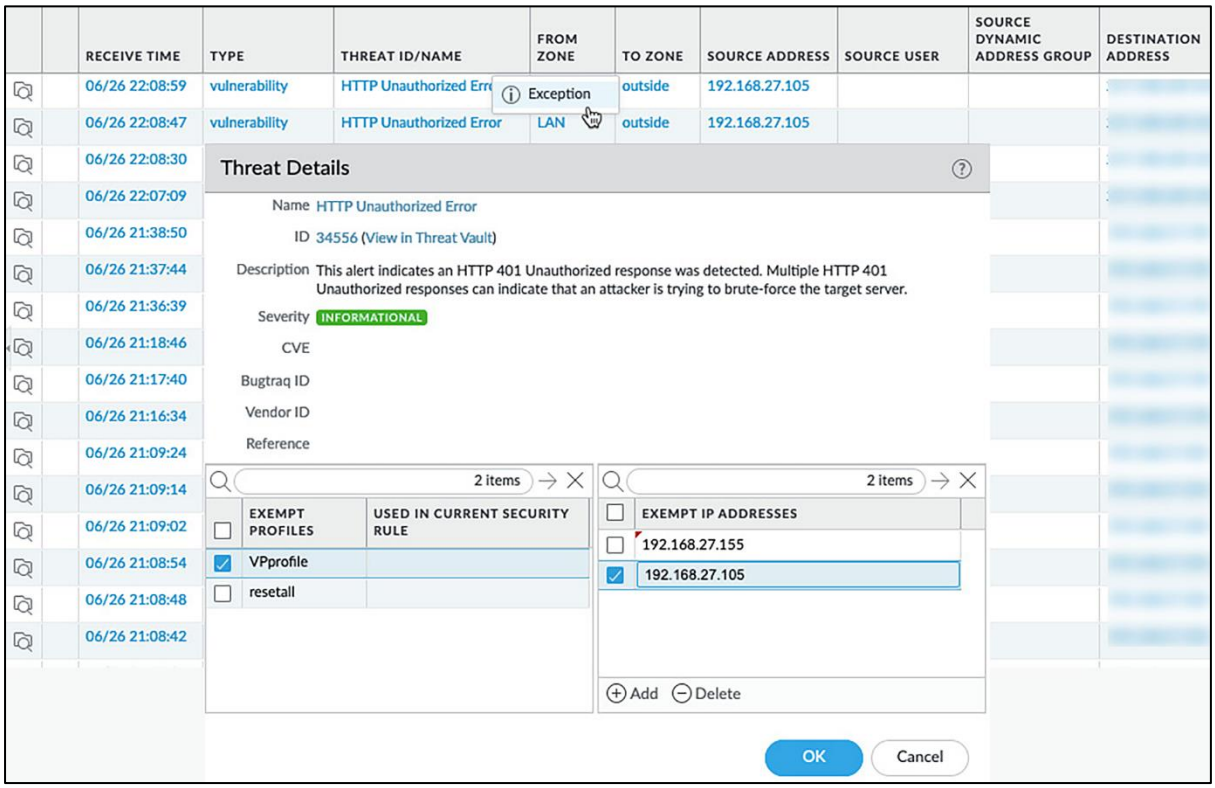

Time
Last 12 Hrs
04/05 12:00:00-04/05 23:59:59
Global Filters
Clear all
Application View
Risk
Sanctioned State
Show system events
Network Activity
Threat Activity
Blocked Activity
Tunnel Activity
Dest ip
GlobalProtect Activity
rule usage
Source IP Activity
Destination IP Activity
bytes
sessions
threats
content
URLs
Home
4.00G
2.00G
0
12:00
13:15
14:30
15:45
17:00
18:15
19:30
20:45
22:00
23:15
bytes_sent
bytes_received
Source Address Bytes Sessions Threats Content URLs Apps
192.168.27.253 3.6G 954 0 0 0 17
192.168.27.127 3.0G 640 0 0 0 8
192.168.27.190 1.8G 582 0 0 0 10
ptr-d3vnoaniu1wir1cioe.... 693.3M 220 0 0 0 9
192.168.27.113 519.9M 4.9k 0 0 0 37
Destination Address Bytes Sessions Threats Content
192.168.27.5 3.5G 176 0 0
ipv4_1.mce0.c009.bru00... 857.6M 30 0 0
Add Global Filter
ipv4_1.mce0.c009.bru00... 588.8M 17 0 0

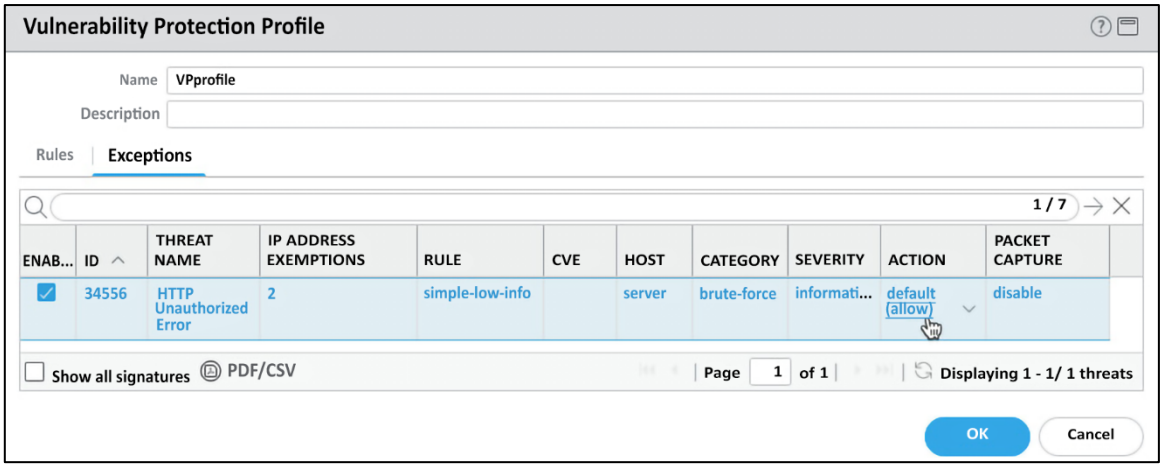

Export
Time
Last 12 Hrs
04/05 12:00:00-04/05 23:59:59
Global Filters
Destination Address (1)
192.168.27.5
Clear all
Application View
Risk
Sanctioned State
Show system events
Network Activity
Threat Activity
Blocked Activity
Tunnel Activity
Dest ip
GlobalProt
bytes
sessions
threats
content
URLs
users
Home
4.00G
2.00G
0
2020/04/05 15:15:00
bytes_sent: 3.25G
bytes_received: 159.56M
14:30
15:00
16:30
22:00
22:30
bytes_sent
bytes_received
Application
Risk
Bytes
Sessions
Threats
Content
URLs
Users
ssl
4
3.5G
170
0
0
0
1
non-syn-tcp
1
851
4
0
0
0
1
ping
2
588
2
0
0
0
1
Source IP Activity
bytes
sessions
threats
content
URLs
Home
4.00G
2.00G
0
14:30
15:00
16:30
22:00
22:30
bytes_sent
bytes_received
Source Address
Bytes
Sessions
Threats
Content
URLs
Apps
192.168.27.253
3.5G
176
0
0
0
3


Add Log Filter
(port.dst eq '443') and ((app eq facebook-base) or (app eq facebook-video))
Connector
and
or
Negate
Attribute
Action
Action Source
Address
App Characteristic
App Container
App Flap Count
Operator
equal
not equal
Value
allow
deny
drop
drop-icmp
RST client
RST server
Add
Apply
Close


RECEIVE TIME
TYPE
FROM ZONE
TO ZONE
SOURCE
DESTINATION
TO PORT
APPLICATION
ACTION
RULE
SESSION END REASON
BYTES
Detailed Log View
General
Session ID 56342
Action allow
Action Source from-policy
Host ID
Application web-browsing
Rule out-web
Rule UUID 315625b1-8ff6-435f-8ad9-35304bd9c3b4
Session End Reason threat
Category unknown
Source
Source User
Source 192.168.27.105
Source DAG
Country home
Port 54137
Zone LAN
Interface ethernet1/3
X-Forwarded-For IP 0.0.0.0
Destination
Destination User
Destination
Destination DAG
Country Netherlands
Port 8123
Zone outside
Interface ethernet1/1
Flags
PCAP
RECEIVE TIME
TYPE
APPLICAT...
ACTION
RULE
RULE UUID
BY...
SEVERI...
CATEG...
URL CATEG... LIST
VERDI...
URL
FILE NAME
2020/06/26 22:08:59 vulnera... web-browsing drop out-web 31562... informat... unkno...
2020/06/26 22:08:55 url web-browsing alert out-web 31562... informat... unkno... medium-risk,un...
2020/06/26 22:10:48 end web-browsing allow out-web 31562... 10... unkno...
Close
DESC


Detailed Log View
Tunnel Type N/A
Details
Threat Type vulnerability
Threat ID/Name HTTP Unauthorized Error
ID 34556 (View in Threat Vault)
Category brute-force
Content Version AppThreat-8286-6150
Severity informational
Repeat Count 1
File Name :8123/
URL
Partial Hash 0
Decrypted
Packet Capture
Client to Server
Server to Client
Tunnel Inspected
DeviceID
Source Category
Source Profile
Source Model
Source Vendor
PCAP
RECEIVE TIME
TYPE
APPLICAT...
ACTION
RULE
RULE UUID
BY...
SEVERI...
CATEG...
URL CATEG... LIST
VERDI...
URL
FILE NAME
2020/06/26 22:08:59 vulnera... web-browsing drop out-web 31562... informat... unkno...
2020/06/26 22:08:55 url web-browsing alert out-web 31562... informat... unkno... medium-risk,un...
2020/06/26 22:10:48 end web-browsing allow out-web 31562... 10... unkno...
Close

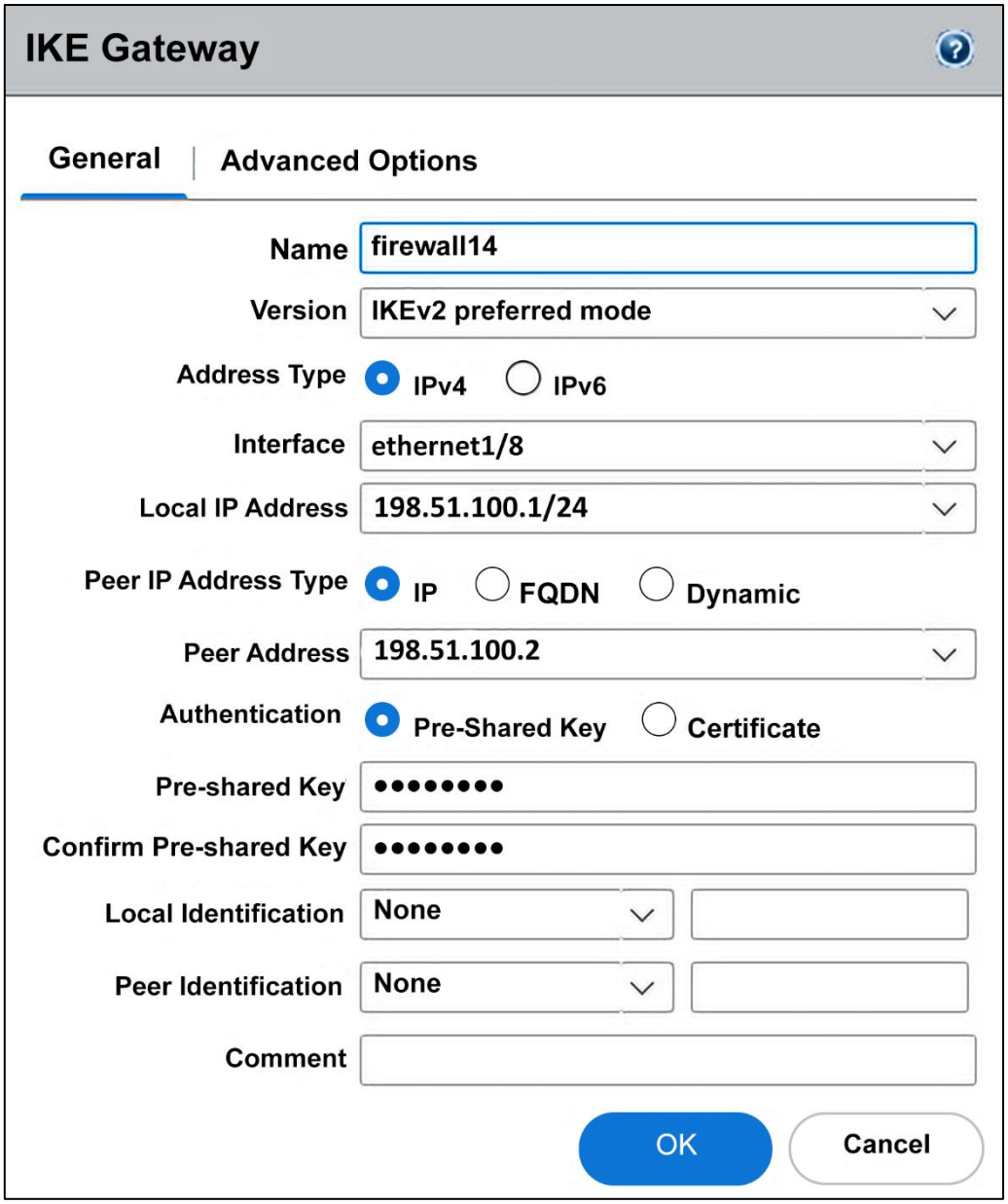

RECEIVE TIME
TYPE
THREAT ID/NAME
FROM ZONE
TO ZONE
SOURCE ADDRESS
SOURCE USER
SOURCE DYNAMIC ADDRESS GROUP
DESTINATION ADDRESS
06/26 22:08:59 vulnerability HTTP Unauthorized Err... outside 192.168.27.105
Exception
06/26 22:08:47 vulnerability HTTP Unauthorized Error LAN outside 192.168.27.105
06/26 22:08:30
06/26 22:07:09
06/26 21:38:50
06/26 21:37:44
06/26 21:36:39
06/26 21:18:46
06/26 21:17:40
06/26 21:16:34
06/26 21:09:24
06/26 21:09:14
06/26 21:09:02
06/26 21:08:54
06/26 21:08:48
06/26 21:08:42
Threat Details
Name HTTP Unauthorized Error
ID 34556 (View in Threat Vault)
Description This alert indicates an HTTP 401 Unauthorized response was detected. Multiple HTTP 401 Unauthorized responses can indicate that an attacker is trying to brute-force the target server.
Severity INFORMATIONAL
CVE
Bugtraq ID
Vendor ID
Reference
2 items
EXEMPT PROFILES
USED IN CURRENT SECURITY RULE
VPprofile
resetall
2 items
EXEMPT IP ADDRESSES
192.168.27.155
192.168.27.105
Add
Delete
OK
Cancel

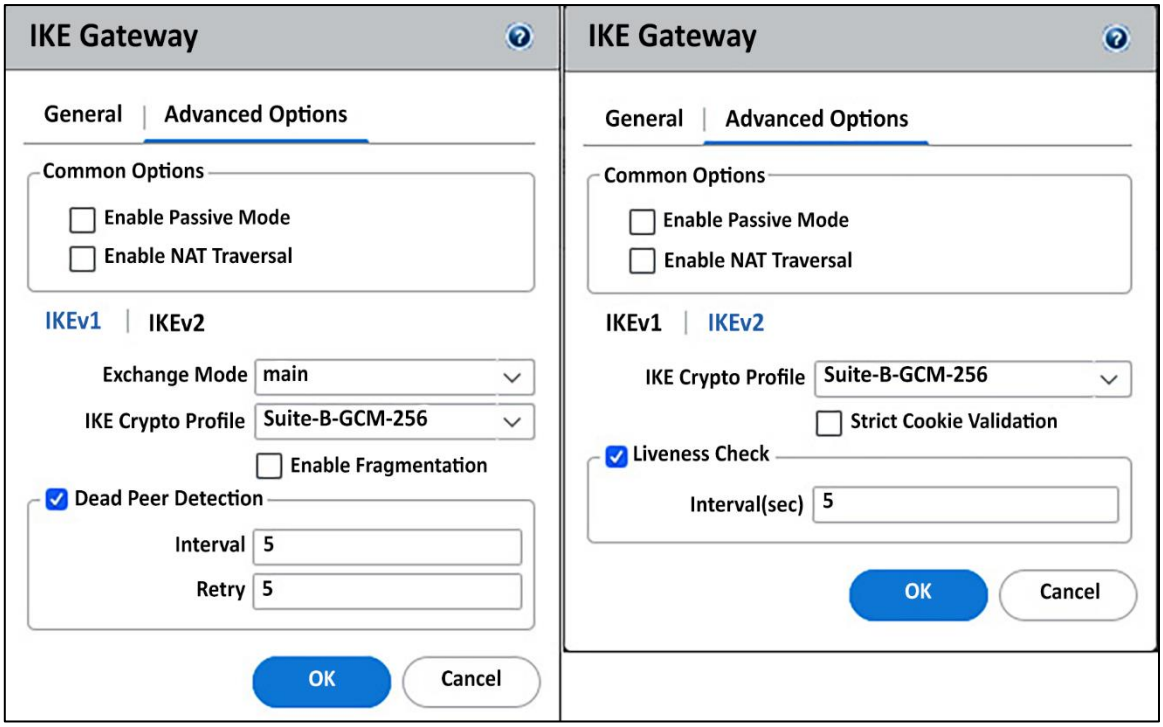


Chapter 10: Virtual Private Networks

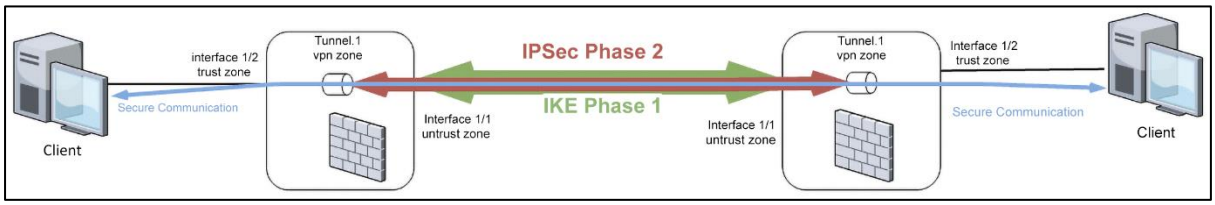
	NAME	ENCRYPTION	AUTHENTICATION	DH GROUP	KEY LIFETIME
☐	default	aes-128-cbc, 3des	sha1	group2	8 hours
☐	Suite-B-GCM-128	aes-128-cbc	sha256	group19	8 hours
☐	Suite-B-GCM-256	aes-256-cbc	sha384	group20	8 hours

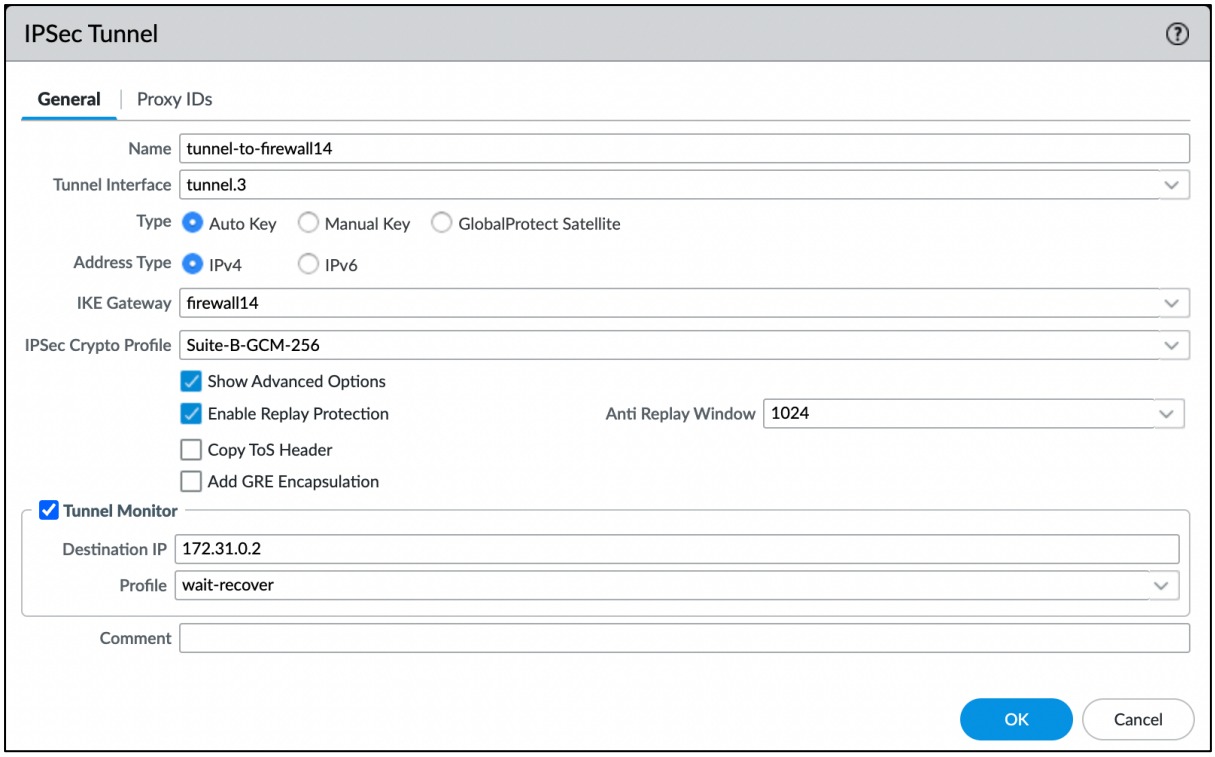
	NAME	ESP/AH	ENCRYPTION	AUTHENTICATION	DH GROUP	LIFETIME	LIFESIZE
☐	default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours	
☐	Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	1 hours	
☐	Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	1 hours	

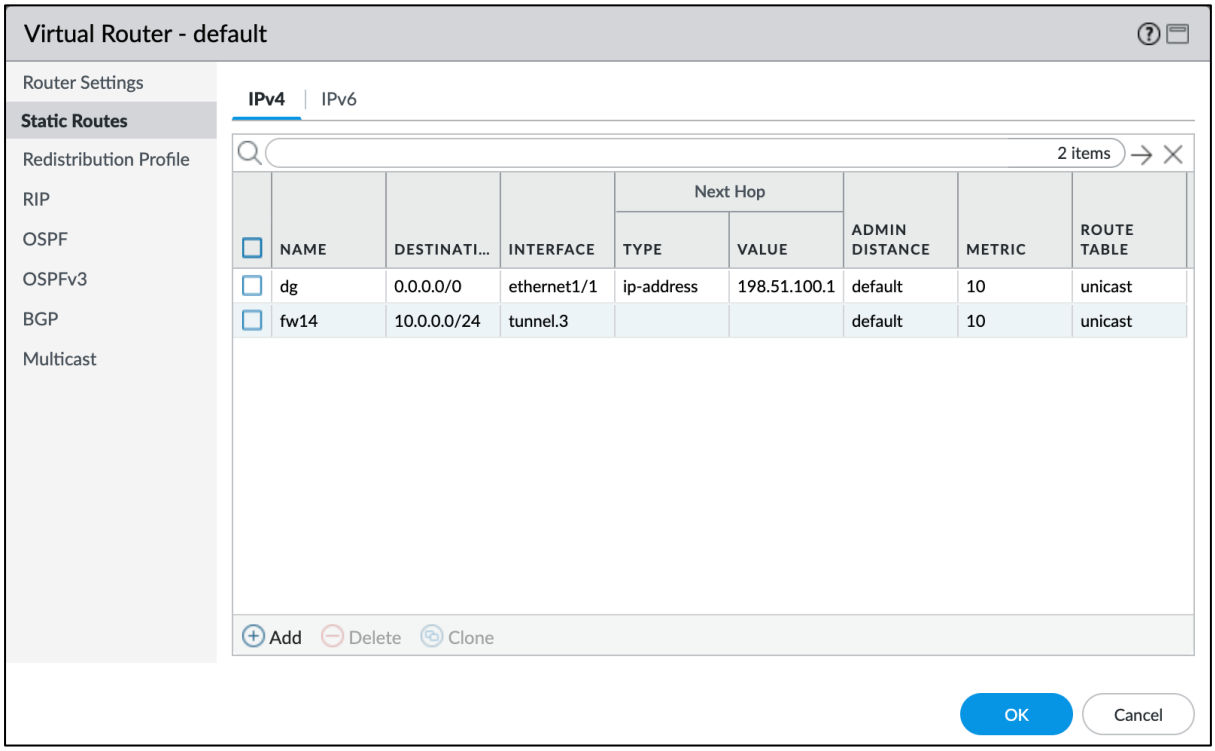

IKE Gateway
General
Advanced Options
Name
firewall14
Version
IKEv2 preferred mode
Address Type
IPv4
IPv6
Interface
ethernet1/8
Local IP Address
198.51.100.1/24
Peer IP Address Type
IP
FQDN
Dynamic
Peer Address
198.51.100.2
Authentication
Pre-Shared Key
Certificate
Pre-shared Key
Confirm Pre-shared Key
Local Identification
None
Peer Identification
None
Comment
OK
Cancel



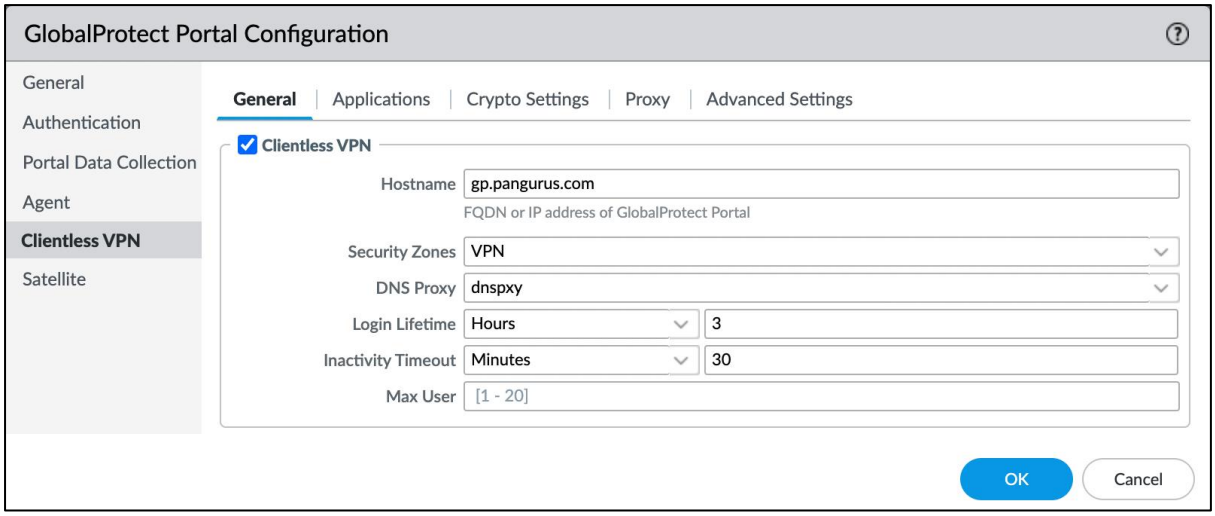
INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VURTUAL ROUTER	SECURITY ZONE	FEATURES
tunnel		none	default	vpn	
tunnel.3	ping	172.31.0.1/30	default	vpn	

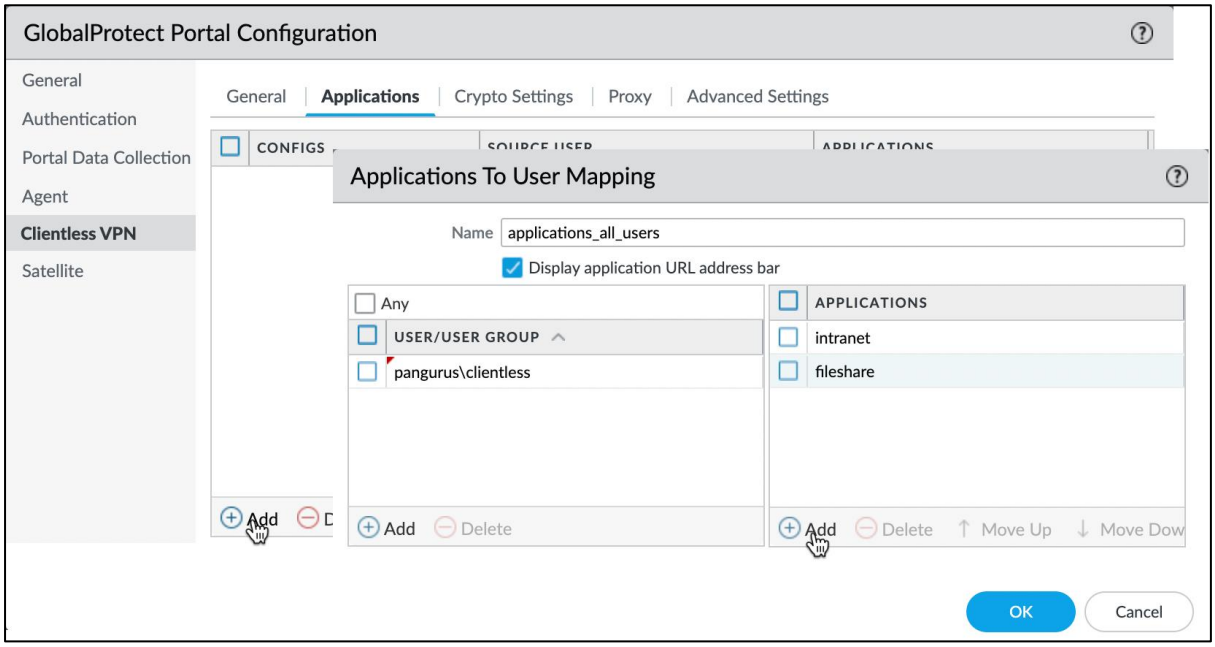


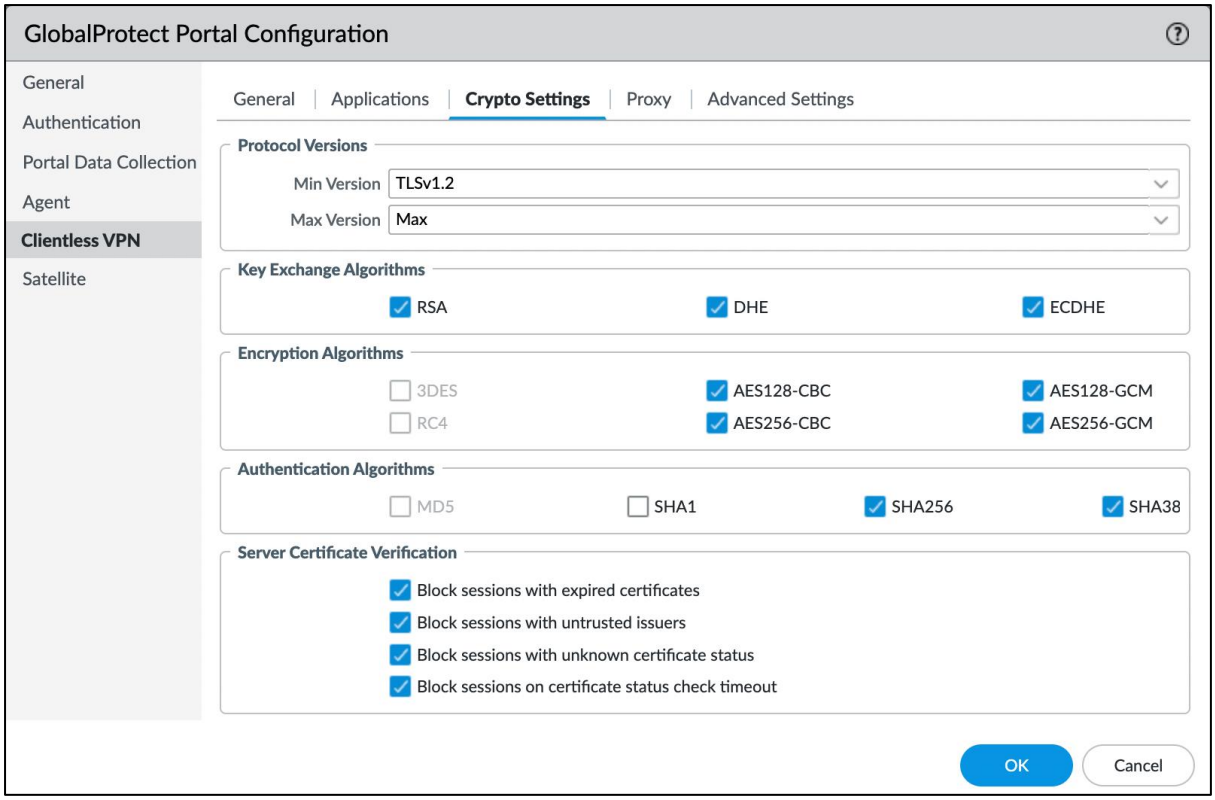


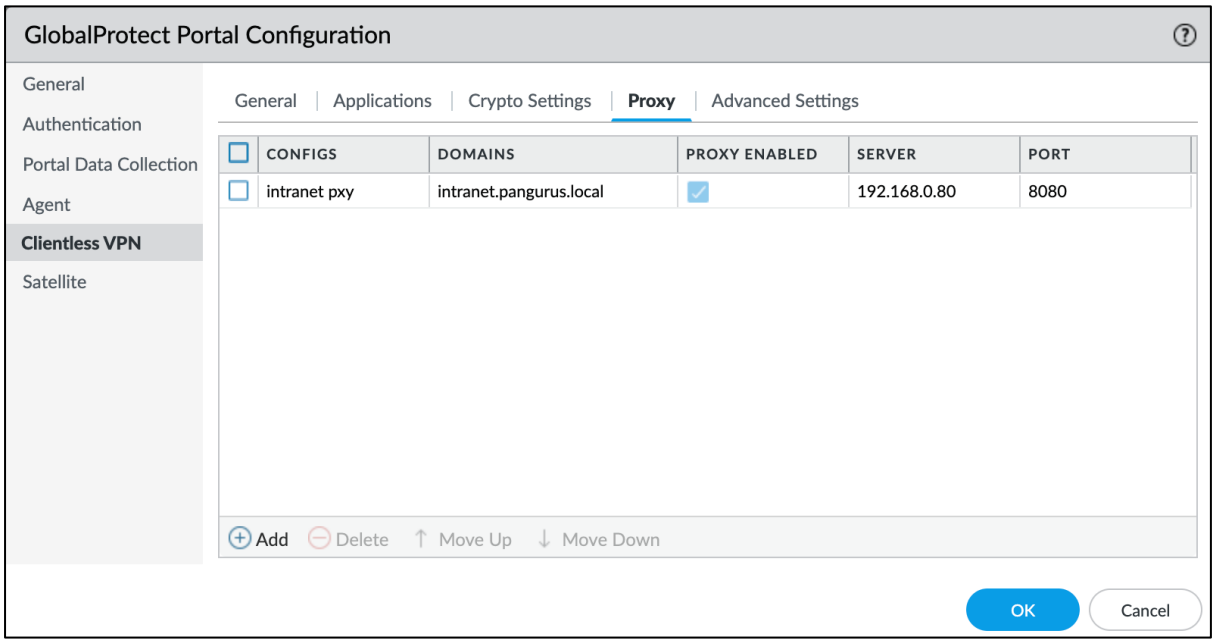


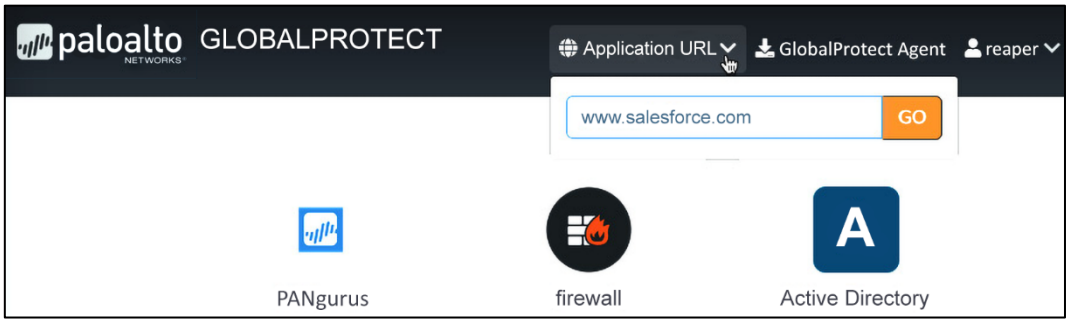
VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION		
5.2.10	99 MB	2021/12/16 14:20:18	✓		Activate	Release Notes	☒
5.2.9	99 MB	2021/11/30 09:57:03			Download	Release Notes	
5.2.8	96 MB	2021/08/04 13:10:27	✓	✓	Reactivate	Release Notes	
5.2.7	94 MB	2021/06/10 14:41:40			Download	Release Notes	

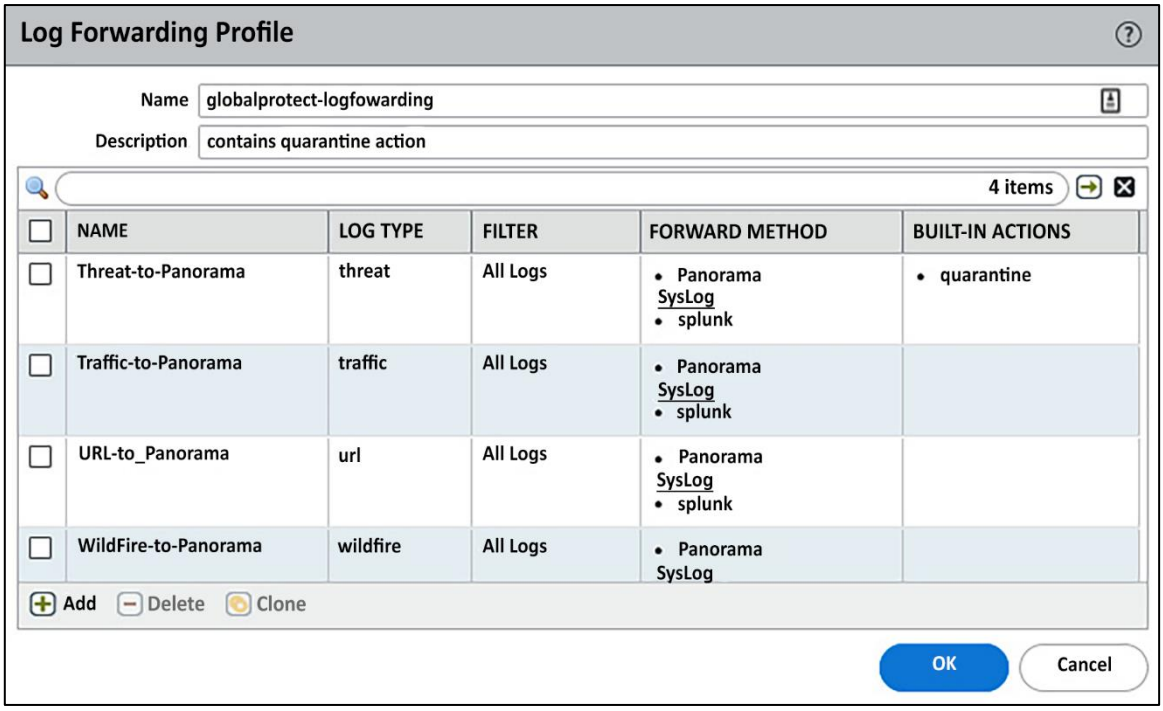

GlobalProtect Portal Configuration
General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite
General
Applications
Crypto Settings
Proxy
Advanced Settings
Clientless VPN
Hostname
gp.pangurus.com
FQDN or IP address of GlobalProtect Portal
Security Zones
VPN
DNS Proxy
dnspxy
Login Lifetime
Hours
3
Inactivity Timeout
Minutes
30
Max User
[1 - 20]
OK
Cancel


GlobalProtect Portal Configuration
General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite
General
Applications
Crypto Settings
Proxy
Advanced Settings
CONFIGS
Applications To User Mapping
Name
applications_all_users
Display application URL address bar
Any
USER/USER GROUP
pangurus\clientless
APPLICATIONS
intranet
fileshare
Add
Delete
Add
Delete
Move Up
Move Dow
OK
Cancel


GlobalProtect Portal Configuration
General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite
General | Applications | Crypto Settings | Proxy | Advanced Settings
Protocol Versions
Min Version TLSv1.2
Max Version Max
Key Exchange Algorithms
RSA DHE ECDHE
Encryption Algorithms
3DES AES128-CBC AES128-GCM
RC4 AES256-CBC AES256-GCM
Authentication Algorithms
MD5 SHA1 SHA256 SHA38
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
OK
Cancel


GlobalProtect Portal Configuration
General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite
General | Applications | Crypto Settings | Proxy | Advanced Settings
CONFIGS DOMAINS PROXY ENABLED SERVER PORT
intranet pxy intranet.pangurus.local 192.168.0.80 8080
Add Delete Move Up Move Down
OK
Cancel


paloalto NETWORKS GLOBALPROTECT
Application URL
GlobalProtect Agent
reaper
www.salesforce.com
GO
PANgurus
firewall
Active Directory

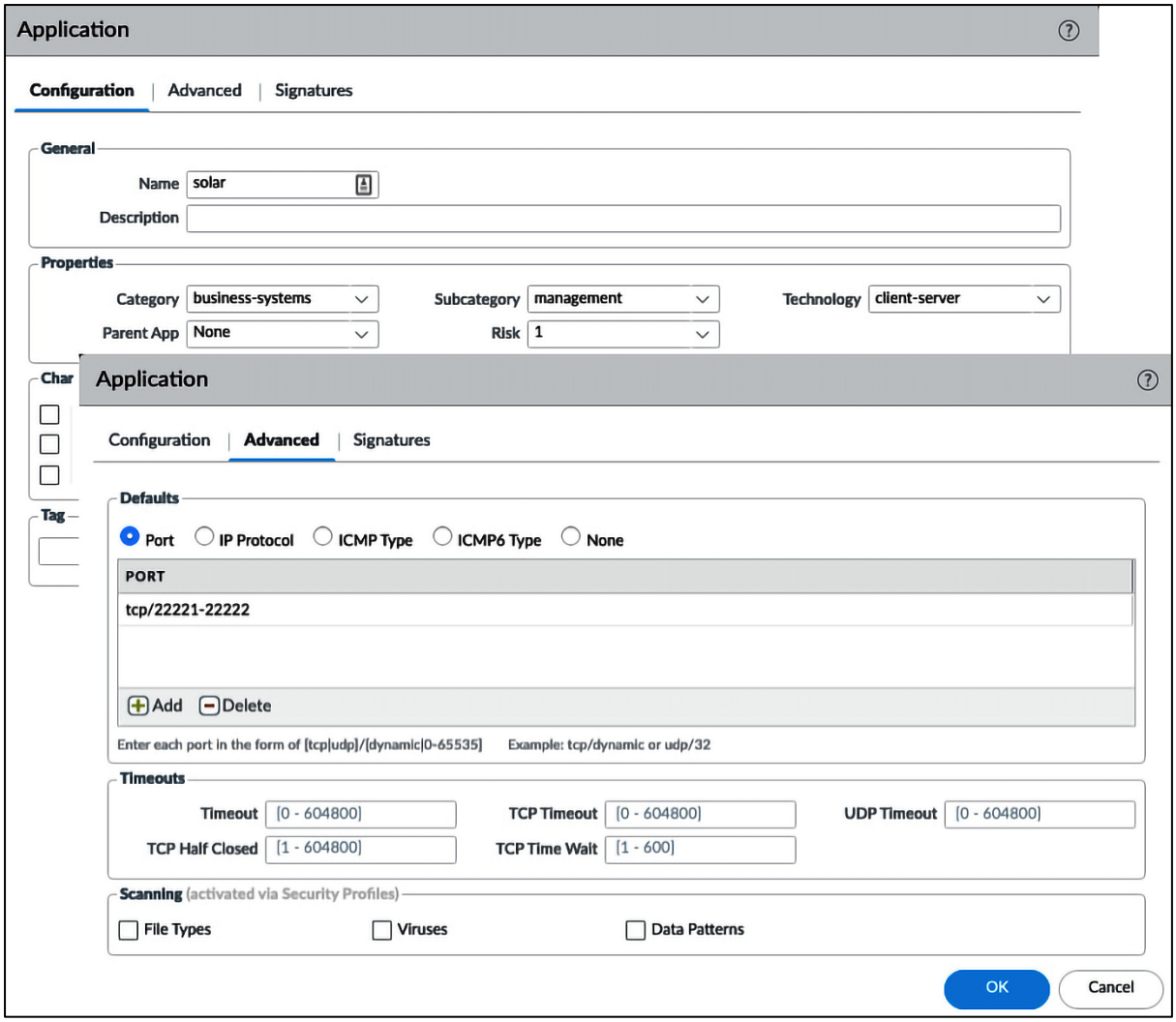


		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION
		06/17 00:57:18	end	LAN	outside	192.168.27.2...	80.	22222	solar	allow
		06/16 19:49:46	end	LAN	outside	192.168.27.2...	80.	22222	solar	allow
		06/16 16:29:25	end	LAN	outside	192.168.27.2...	18	22222	solar	allow

Chapter 11: Advanced Protection

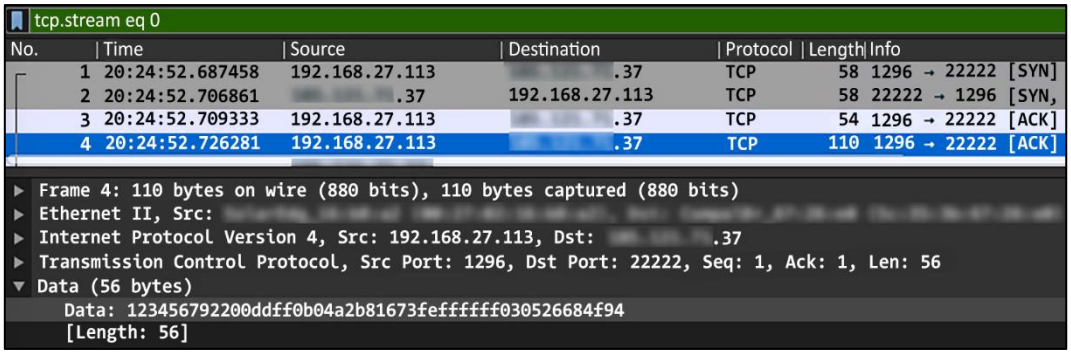
(app eq unknown-tcp) and (addr.src in 192.168.27.4)

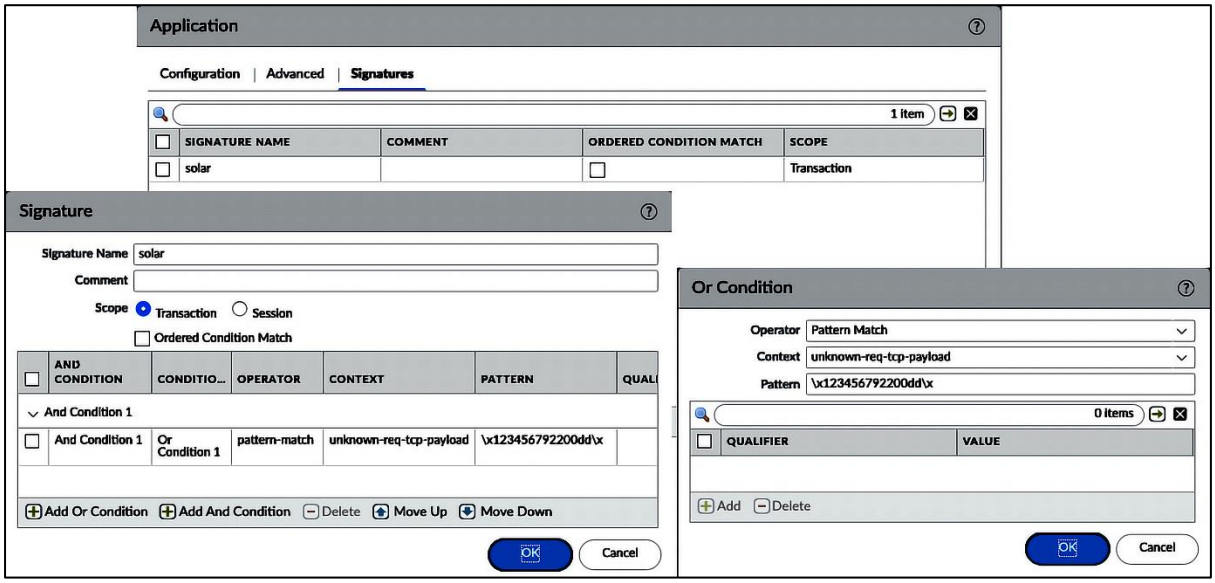
		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATI...	ACTION
		06/14 17:09:28	end	LAN	outside	192.168.27.4	78.	22222	unknown-tcp	allow
		06/14 14:43:08	end	LAN	outside	192.168.27.4	79.	22222	unknown-tcp	allow
		06/14 13:25:23	end	LAN	outside	192.168.27.4	46.	22222	unknown-tcp	allow



	NAME	TAGS	Source		Destination		PROTOC...	PORT	APPLICATI...
			ZONE	ADDRESS	ZONE	ADDRESS			
1	solar override	none	LAN	192.168.27.4	outside	[redacted]	tcp	22221-22222	solar

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION
		06/17 00:57:18	end	LAN	outside	192.168.27.2...	80[redacted]	22222	solar	allow
		06/16 19:49:46	end	LAN	outside	192.168.27.2...	80[redacted]	22222	solar	allow
		06/16 16:29:25	end	LAN	outside	192.168.27.2...	18[redacted]	22222	solar	allow





.	1.3	matches a single character (e.g. 123, 133)
?	dots?	matches string with or without last character (e.g. dot, dots)
*	dots*	matches string with or without last character, and multiple repeats of last character (e.g. dot, dots, dotssss)
+	dots+	matches single or multiple repetitions of the preceding letter (e.g. dots, dotssss)
|	((exe)|(msi))	OR function to match multiple possible strings (e.g. dot.exe, dot.msi)
[ ]	X[abc]	matches preceding string followed by any character between squared brackets (e.g. xa, xb, xc)
-	X[a-z]	matches any character in a range (e.g. xa,xm)
^	X[^AB]	matches any character except the ones listed (e.g. xC, x5)
{ }	X{1,3}	matches anything after x as long as it is 1 to 3 bytes in length (e.g. xl, x123)
\	X\.y	Escape character to exactly match a special character (e.g. www\ pangurus\.com)
&amp		used to match & in a string

Custom Vulnerability Signature

Configuration | Signatures

General

Threat ID: 41000
41000 - 45000 & 6800001 - 6900000
Name: BlockBrowser
Comment:

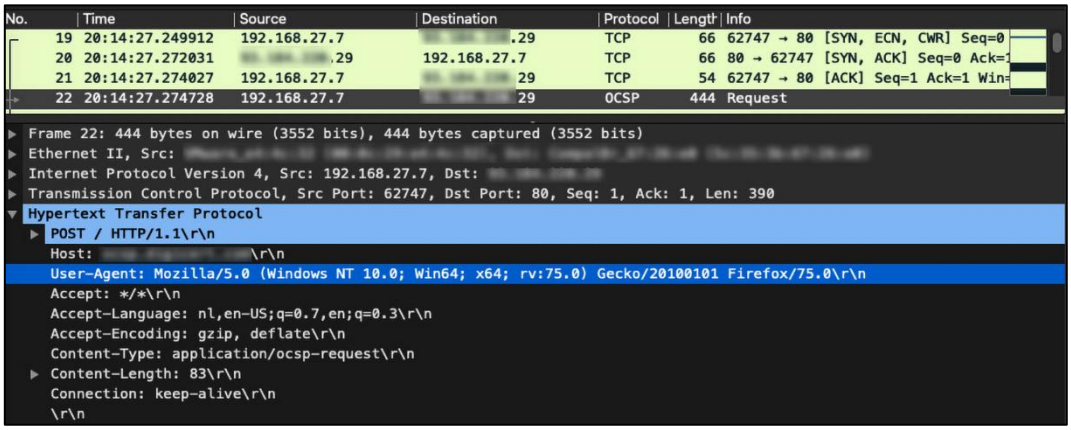
Properties

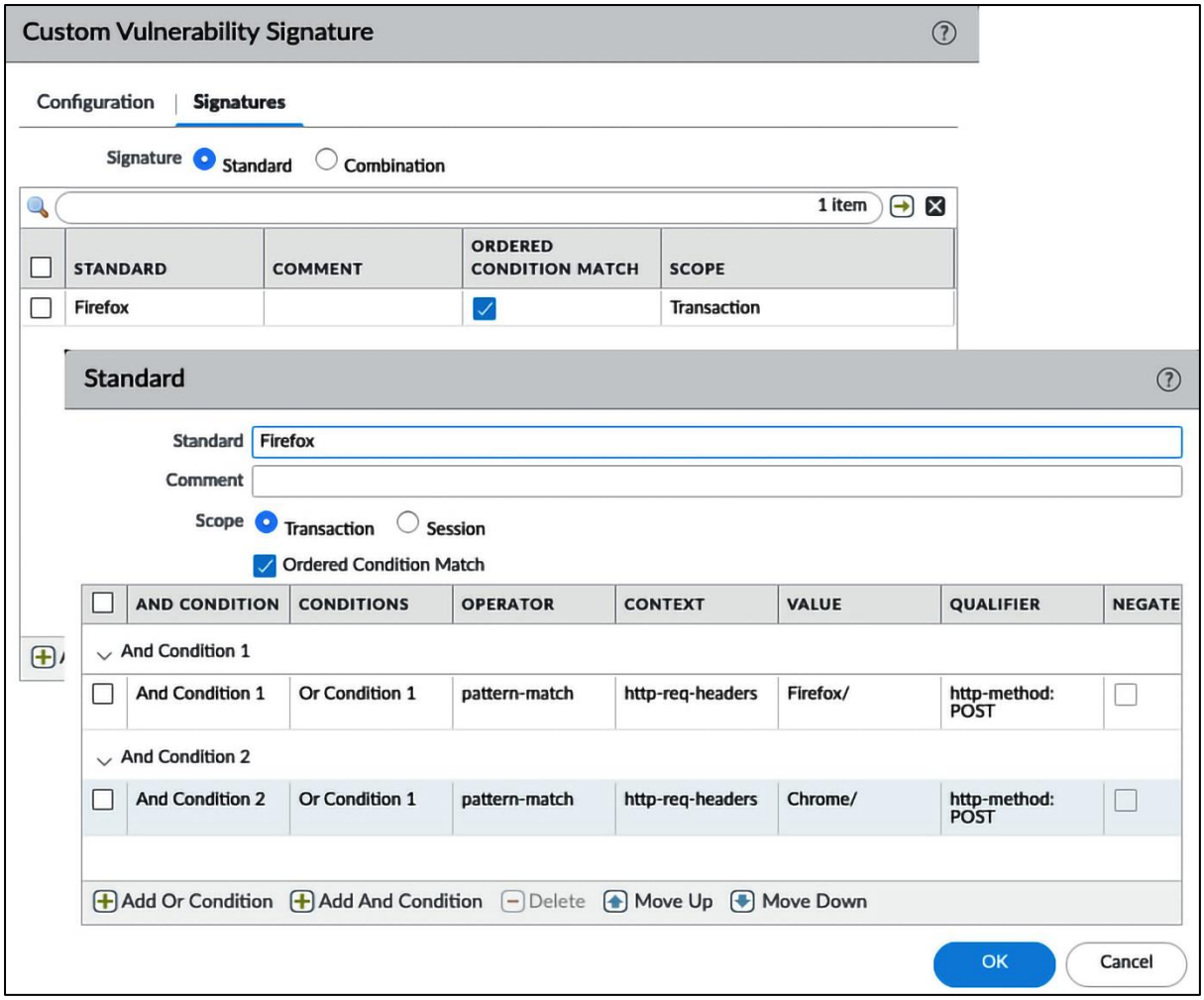
Severity: high
Direction: client2server
Default Action: Reset Client
Affected System: client

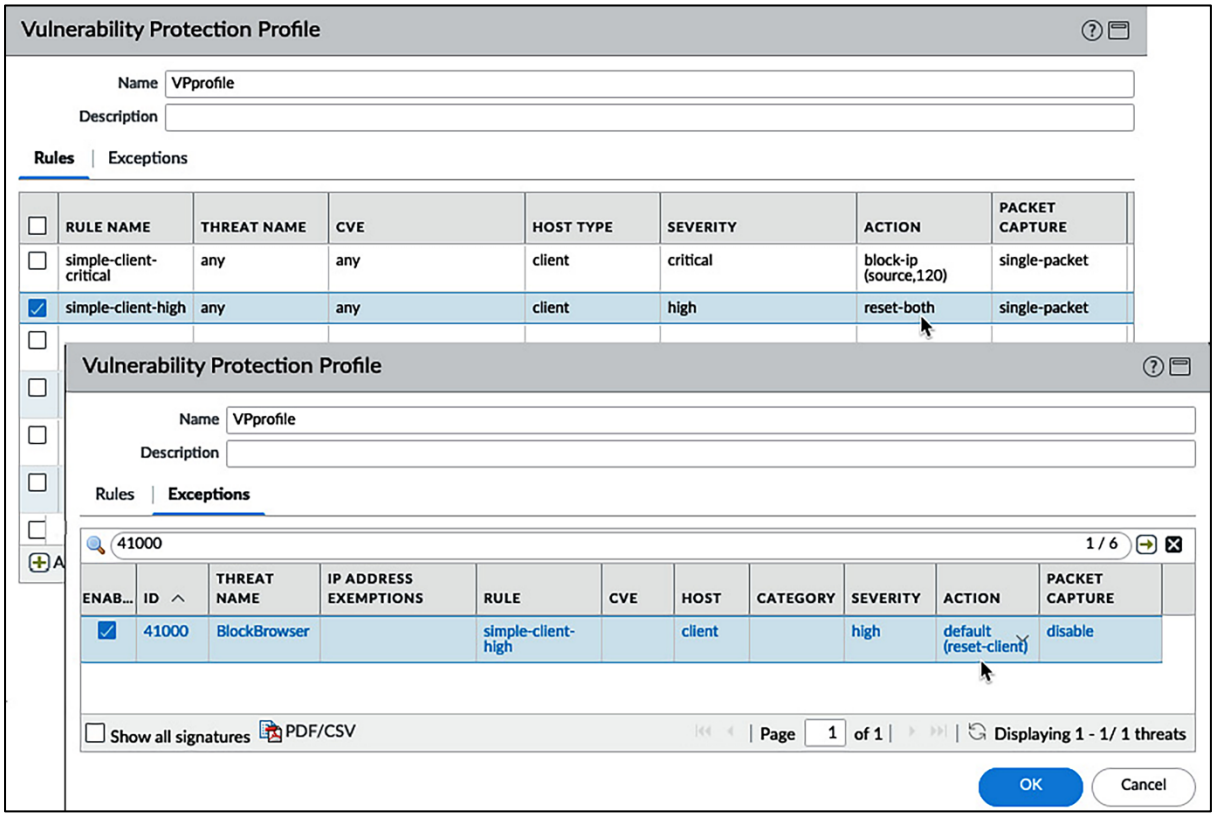
References (one reference per line)

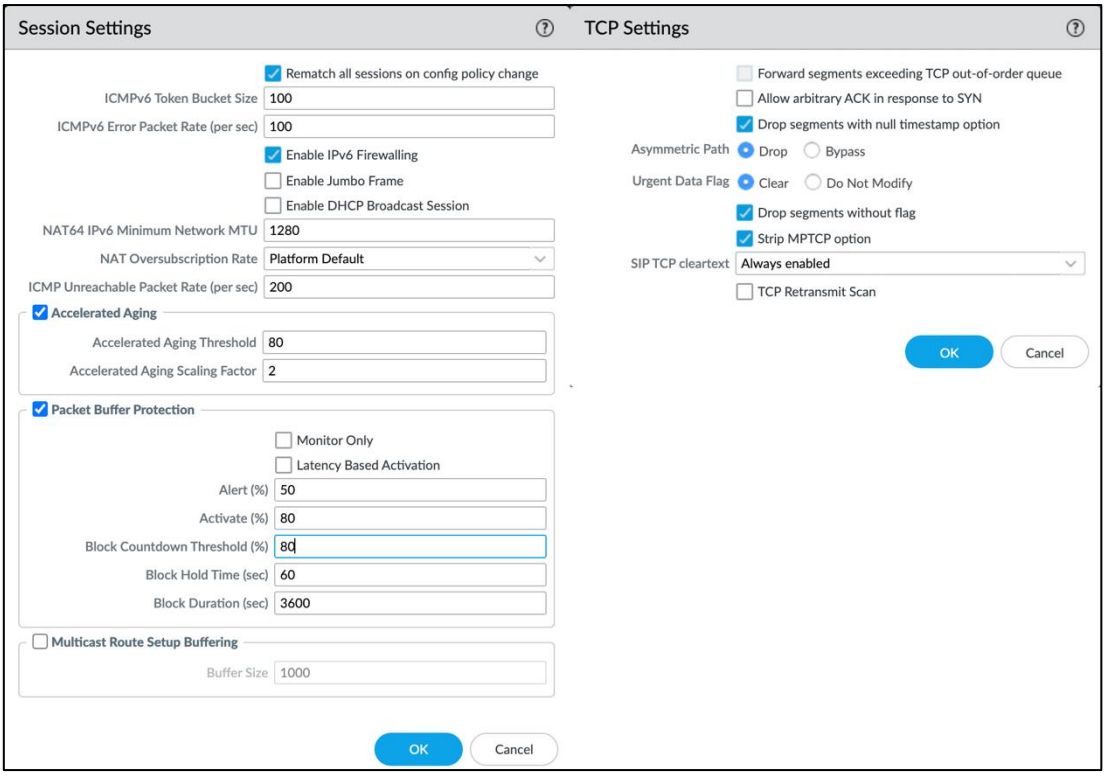
CVE: Example: CVE-1999-0001
Bugtraq: Example: bugtraq id
Vendor: Example: MS03-026
Reference: Example: en.wikipedia.org/wiki/Virus

OK Cancel

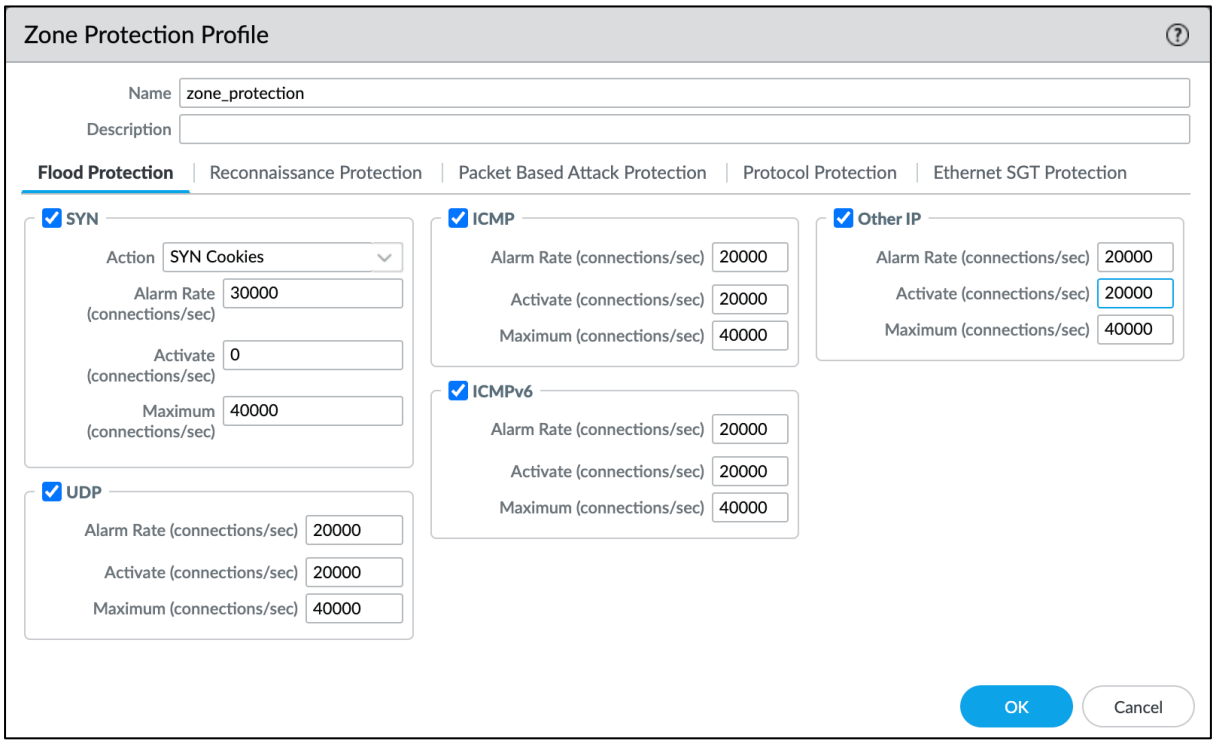


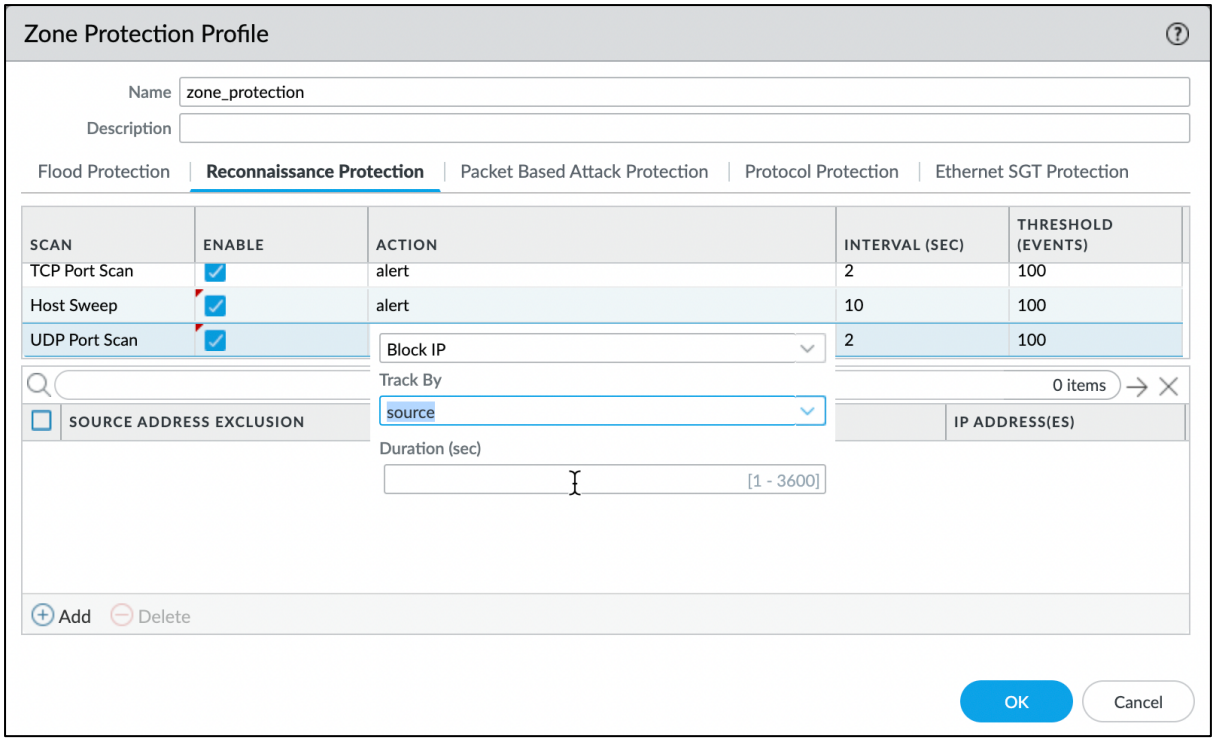

Custom Vulnerability Signature
Configuration
Signatures
Signature
Standard
Combination
1 item
STANDARD
COMMENT
ORDERED CONDITION MATCH
SCOPE
Firefox
Transaction
Standard
Standard
Firefox
Comment
Scope
Transaction
Session
Ordered Condition Match
AND CONDITION
CONDITIONS
OPERATOR
CONTEXT
VALUE
QUALIFIER
NEGATE
And Condition 1
And Condition 1
Or Condition 1
pattern-match
http-req-headers
Firefox/
http-method: POST
And Condition 2
And Condition 2
Or Condition 1
pattern-match
http-req-headers
Chrome/
http-method: POST
Add Or Condition
Add And Condition
Delete
Move Up
Move Down
OK
Cancel

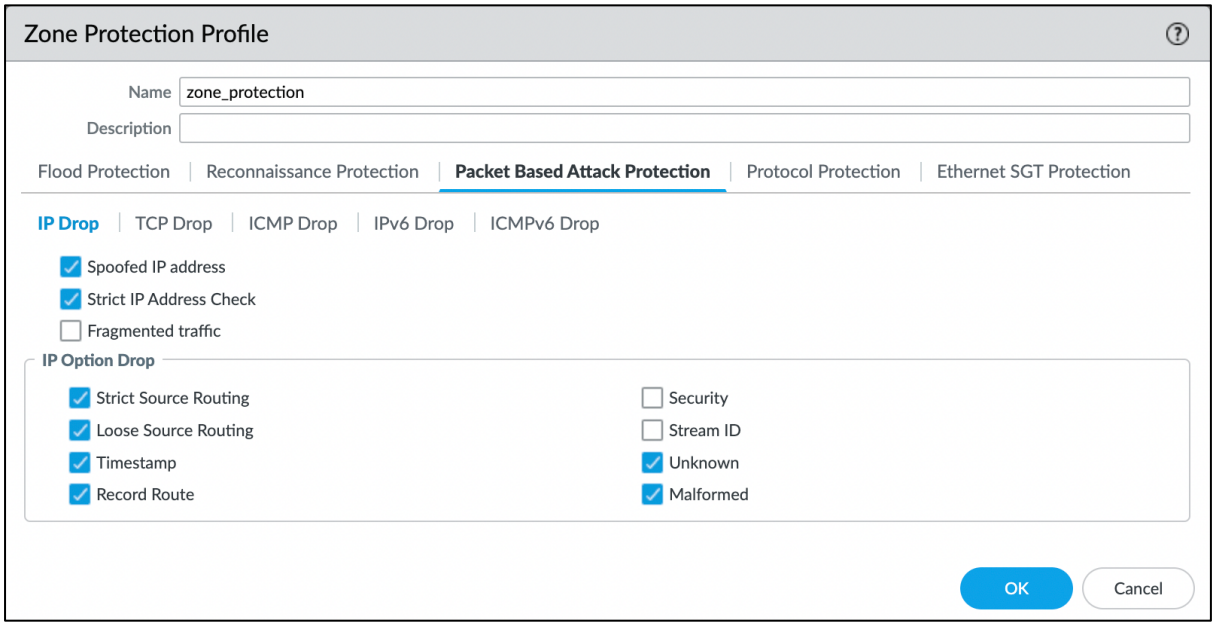

Vulnerability Protection Profile
Name
VPprofile
Description
Rules
Exceptions
RULE NAME
THREAT NAME
CVE
HOST TYPE
SEVERITY
ACTION
PACKET CAPTURE
simple-client-critical
any
any
client
critical
block-ip (source,120)
single-packet
simple-client-high
any
any
client
high
reset-both
single-packet
Vulnerability Protection Profile
Name
VPprofile
Description
Rules
Exceptions
41000
1 / 6
ENAB...
ID
THREAT NAME
IP ADDRESS EXEMPTIONS
RULE
CVE
HOST
CATEGORY
SEVERITY
ACTION
PACKET CAPTURE
41000
BlockBrowser
simple-client-high
client
high
default (reset-client)
disable
Show all signatures
PDF/CSV
Page
1
of 1
Displaying 1 - 1/ 1 threats
OK
Cancel

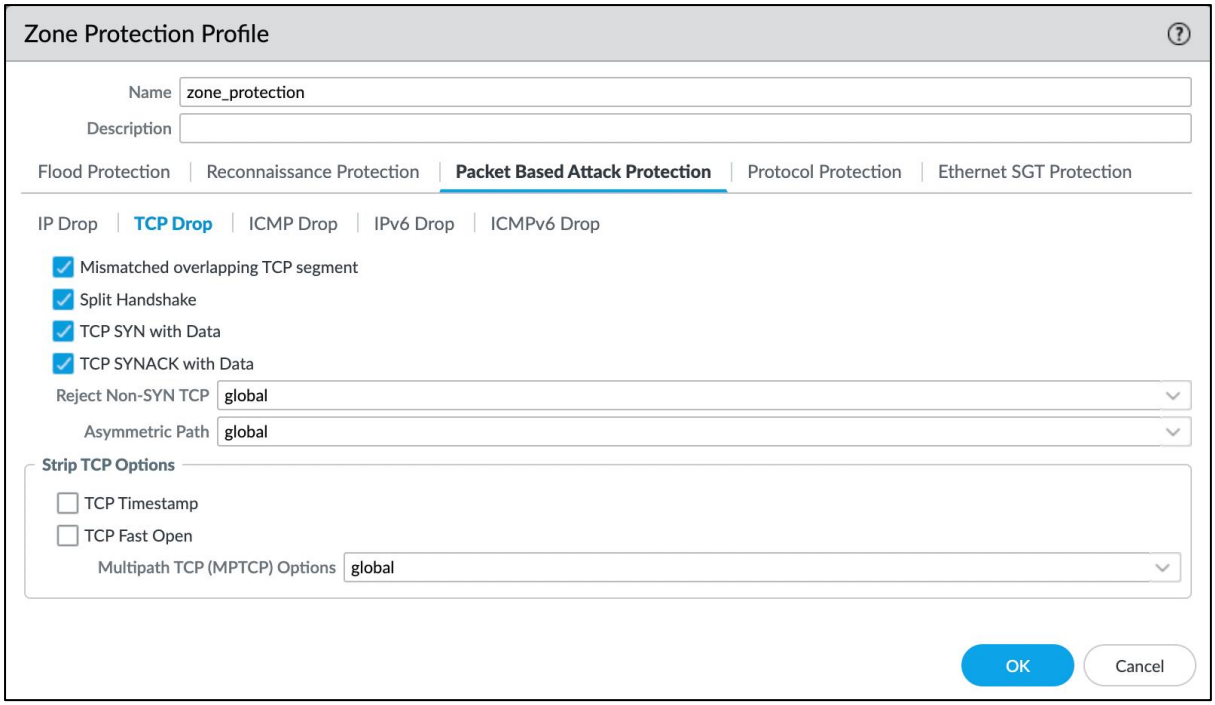


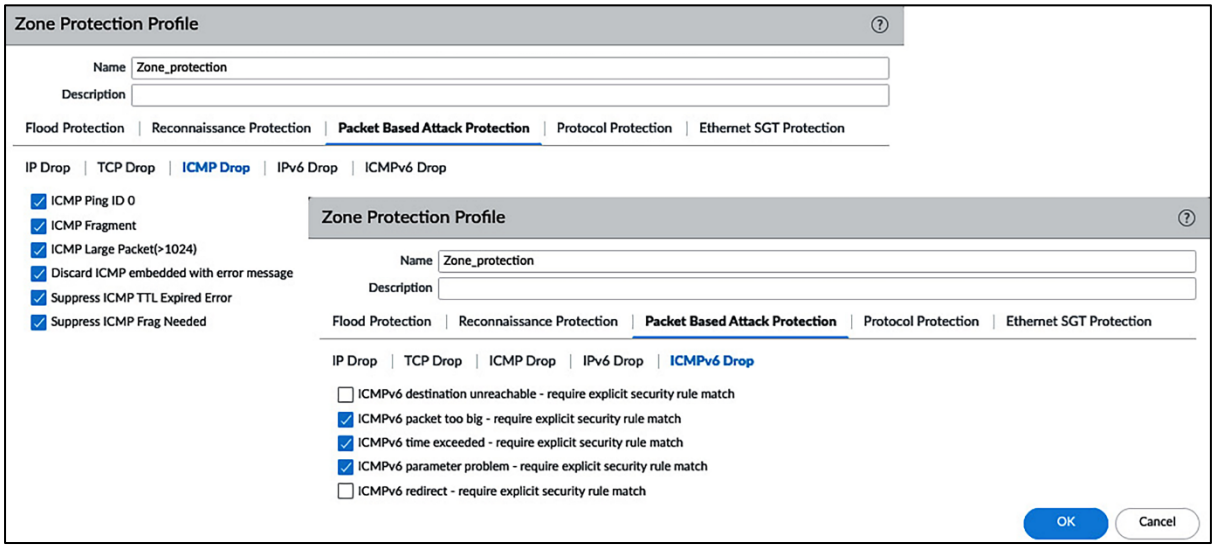
	Receive Time	Type	Name	Direction	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity
	04/29 00:12:21	flood	UDP Flood	client-to-server	LAN	LAN	0.0.0.0	0.0.0.0	0	not-applicable	allow	critical
	04/29 00:12:18	flood	ICMP Flood	client-to-server	LAN	LAN	0.0.0.0	0.0.0.0	0	not-applicable	allow	critical
	04/29 00:07:47	flood	TCP Flood	client-to-server	LAN	LAN	0.0.0.0	0.0.0.0	0	not-applicable	syncookie-sent	critical

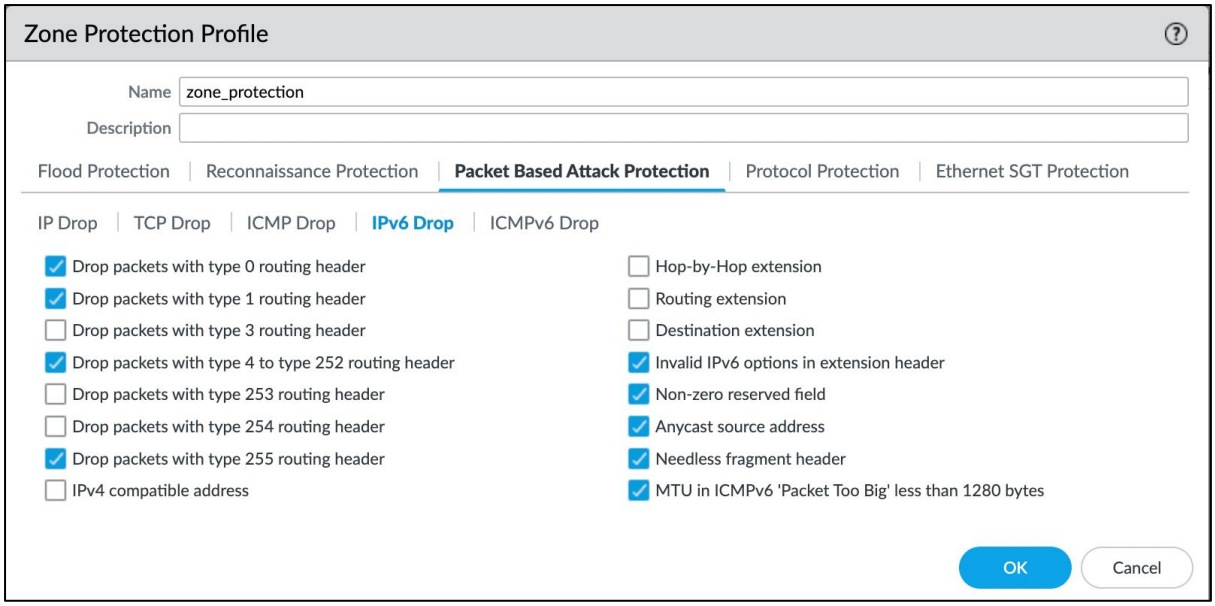


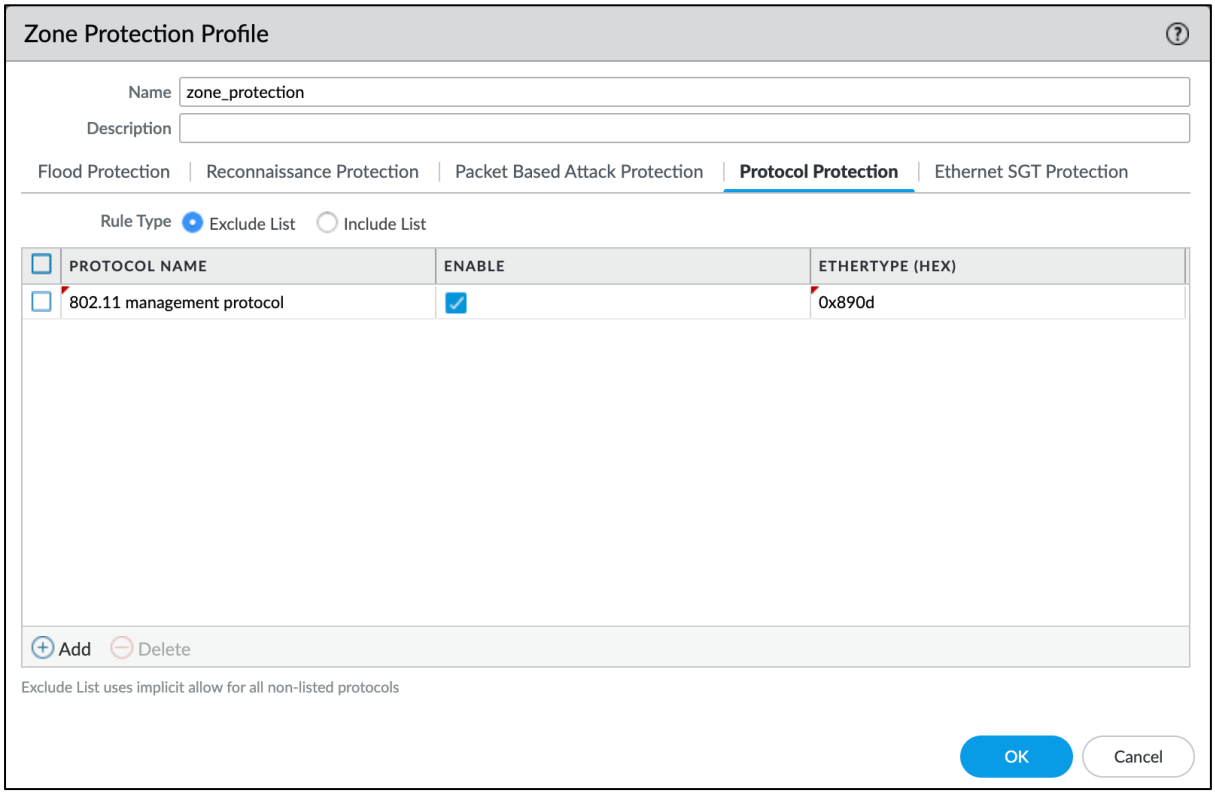

Zone Protection Profile
Name
zone_protection
Description
Flood Protection
Reconnaissance Protection
Packet Based Attack Protection
Protocol Protection
Ethernet SGT Protection
SCAN
ENABLE
ACTION
INTERVAL (SEC)
THRESHOLD (EVENTS)
TCP Port Scan
alert
2
100
Host Sweep
alert
10
100
UDP Port Scan
Block IP
2
100
Track By
source
Duration (sec)
[1 - 3600]
0 items
SOURCE ADDRESS EXCLUSION
IP ADDRESS(ES)
Add
Delete
OK
Cancel

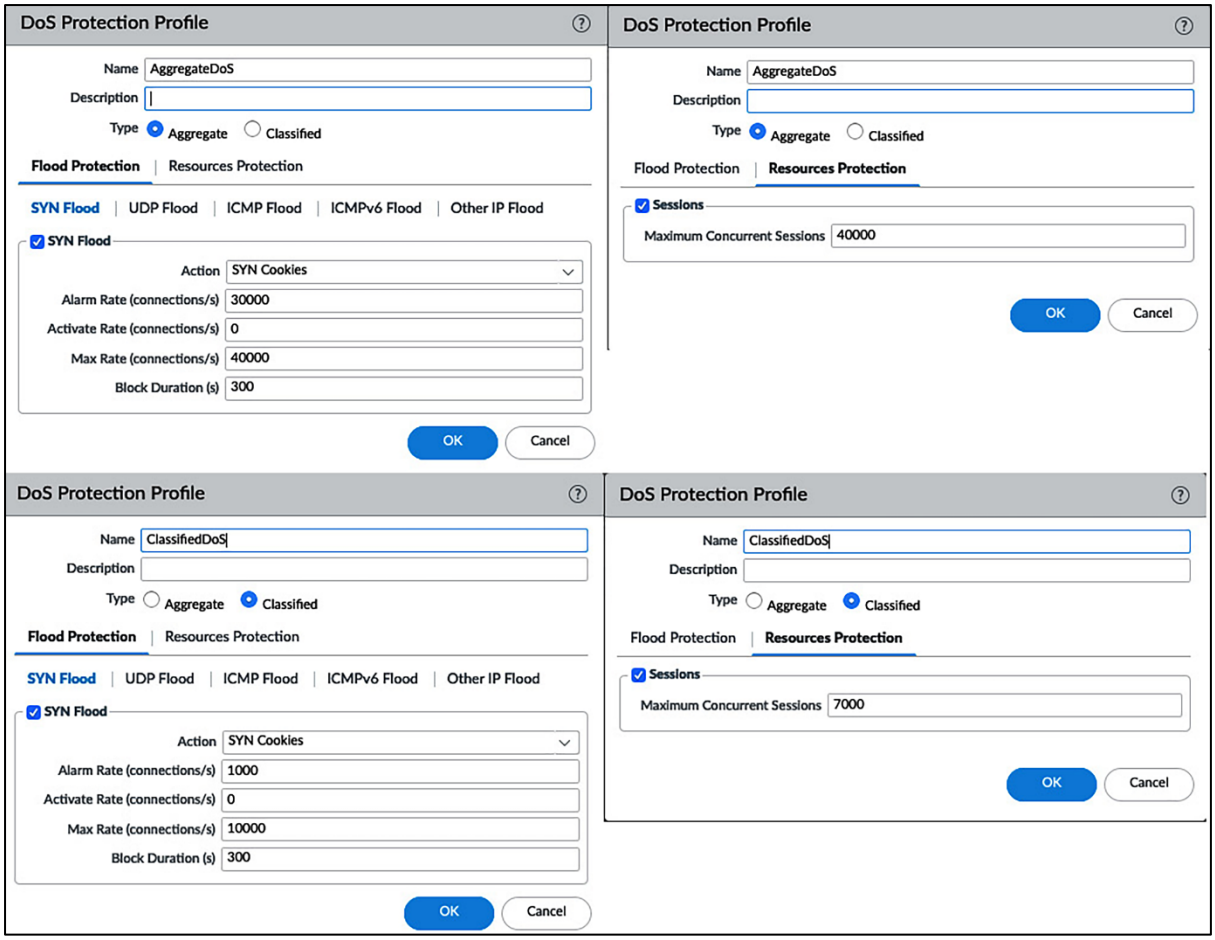

Zone Protection Profile
Name
zone_protection
Description
Flood Protection
Reconnaissance Protection
Packet Based Attack Protection
Protocol Protection
Ethernet SGT Protection
IP Drop
TCP Drop
ICMP Drop
IPv6 Drop
ICMPv6 Drop
Spoofed IP address
Strict IP Address Check
Fragmented traffic
IP Option Drop
Strict Source Routing
Loose Source Routing
Timestamp
Record Route
Security
Stream ID
Unknown
Malformed
OK
Cancel


Zone Protection Profile
Name
zone_protection
Description
Flood Protection
Reconnaissance Protection
Packet Based Attack Protection
Protocol Protection
Ethernet SGT Protection
IP Drop
TCP Drop
ICMP Drop
IPv6 Drop
ICMPv6 Drop
Mismatched overlapping TCP segment
Split Handshake
TCP SYN with Data
TCP SYNACK with Data
Reject Non-SYN TCP
global
Asymmetric Path
global
Strip TCP Options
TCP Timestamp
TCP Fast Open
Multipath TCP (MPTCP) Options
global
OK
Cancel

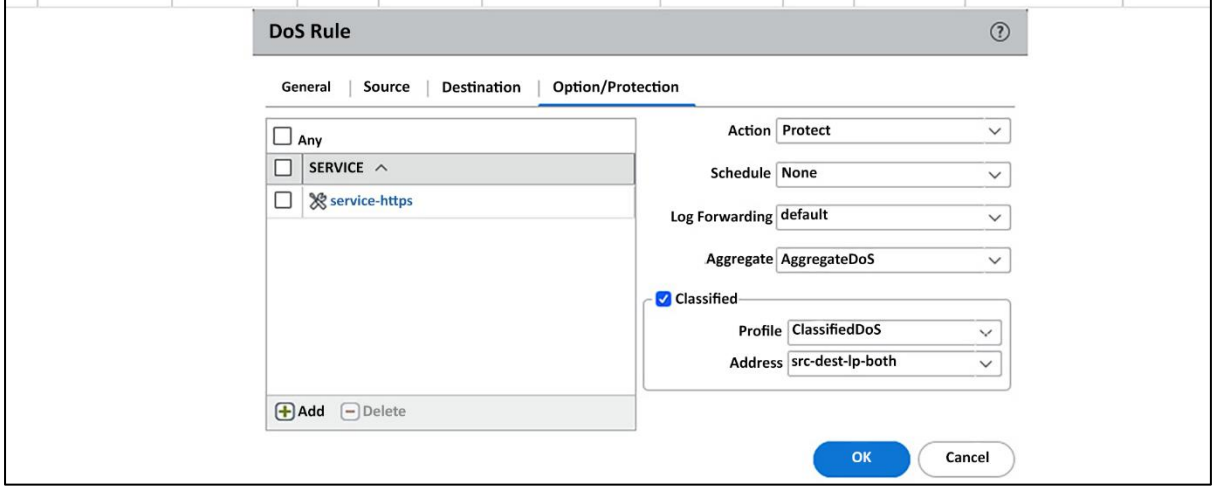

Zone Protection Profile
Name
Zone_protection
Description
Flood Protection
Reconnaissance Protection
Packet Based Attack Protection
Protocol Protection
Ethernet SGT Protection
IP Drop
TCP Drop
ICMP Drop
IPv6 Drop
ICMPv6 Drop
ICMP Ping ID 0
ICMP Fragment
ICMP Large Packet(>1024)
Discard ICMP embedded with error message
Suppress ICMP TTL Expired Error
Suppress ICMP Frag Needed
Zone Protection Profile
Name
Zone_protection
Description
Flood Protection
Reconnaissance Protection
Packet Based Attack Protection
Protocol Protection
Ethernet SGT Protection
IP Drop
TCP Drop
ICMP Drop
IPv6 Drop
ICMPv6 Drop
ICMPv6 destination unreachable - require explicit security rule match
ICMPv6 packet too big - require explicit security rule match
ICMPv6 time exceeded - require explicit security rule match
ICMPv6 parameter problem - require explicit security rule match
ICMPv6 redirect - require explicit security rule match
OK
Cancel


Zone Protection Profile
Name
zone_protection
Description
Flood Protection
Reconnaissance Protection
Packet Based Attack Protection
Protocol Protection
Ethernet SGT Protection
IP Drop
TCP Drop
ICMP Drop
IPv6 Drop
ICMPv6 Drop
Drop packets with type 0 routing header
Drop packets with type 1 routing header
Drop packets with type 3 routing header
Drop packets with type 4 to type 252 routing header
Drop packets with type 253 routing header
Drop packets with type 254 routing header
Drop packets with type 255 routing header
IPv4 compatible address
Hop-by-Hop extension
Routing extension
Destination extension
Invalid IPv6 options in extension header
Non-zero reserved field
Anycast source address
Needless fragment header
MTU in ICMPv6 'Packet Too Big' less than 1280 bytes
OK
Cancel

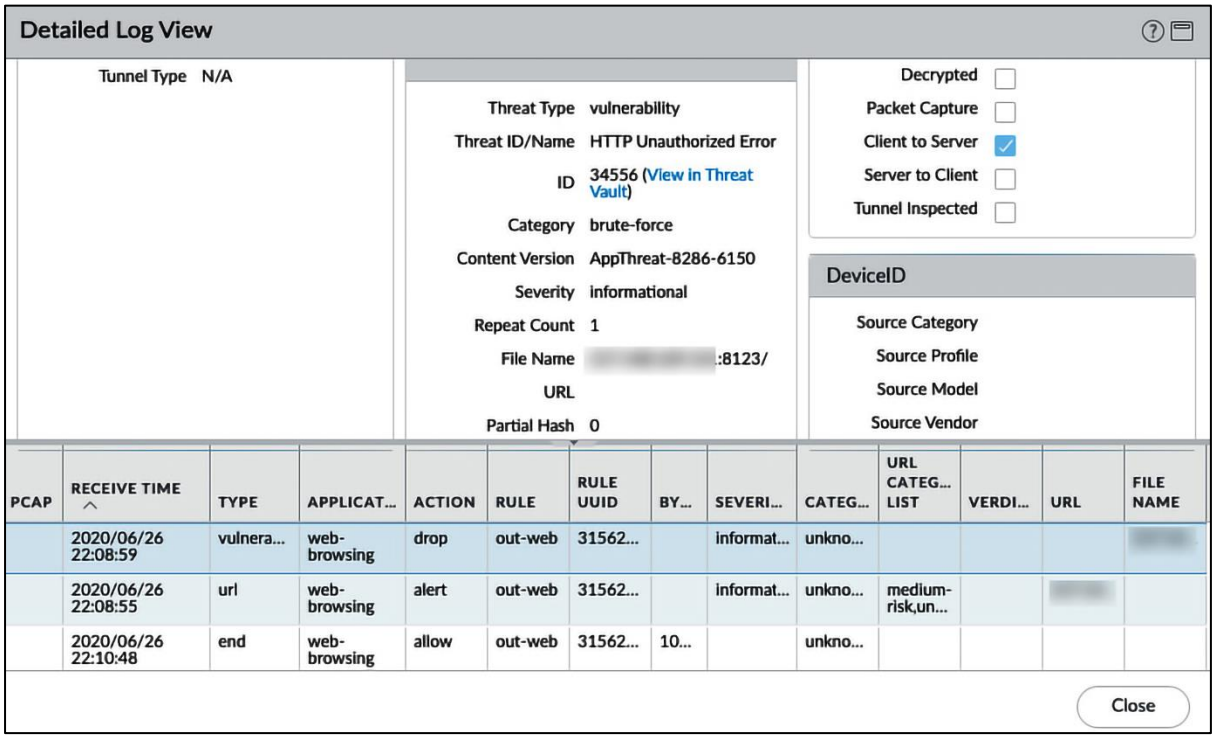

Zone Protection Profile
Name
zone_protection
Description
Flood Protection
Reconnaissance Protection
Packet Based Attack Protection
Protocol Protection
Ethernet SGT Protection
Rule Type
Exclude List
Include List
PROTOCOL NAME
ENABLE
ETHERTYPE (HEX)
802.11 management protocol
0x890d
Add
Delete
Exclude List uses implicit allow for all non-listed protocols
OK
Cancel

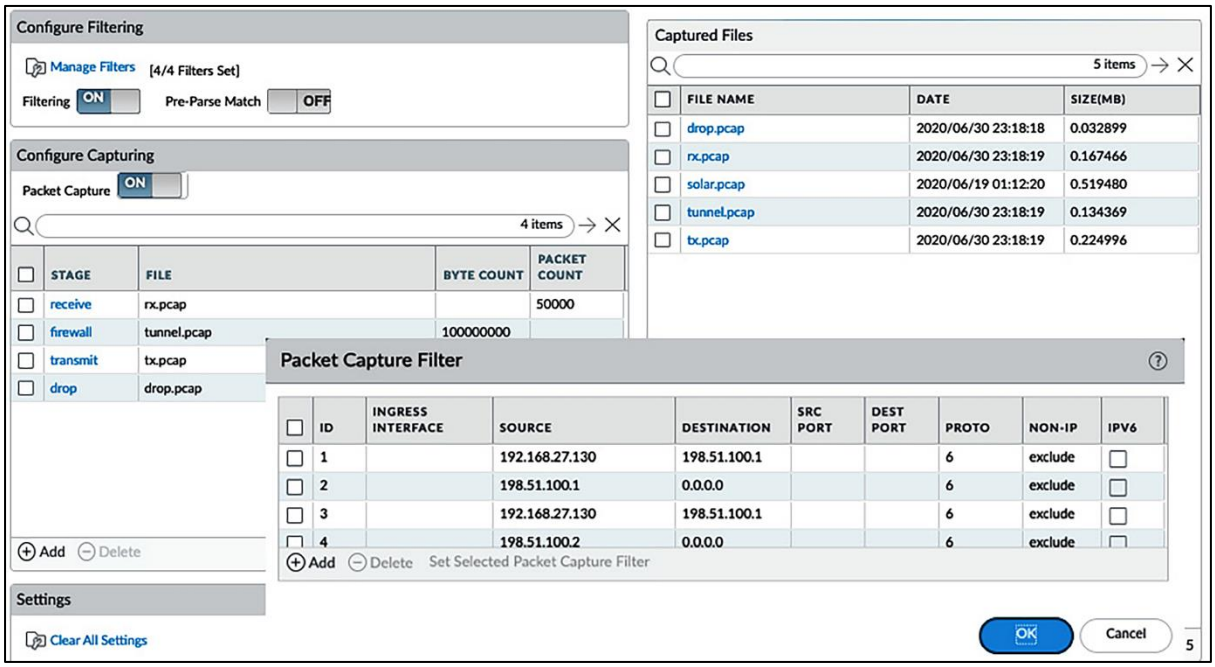


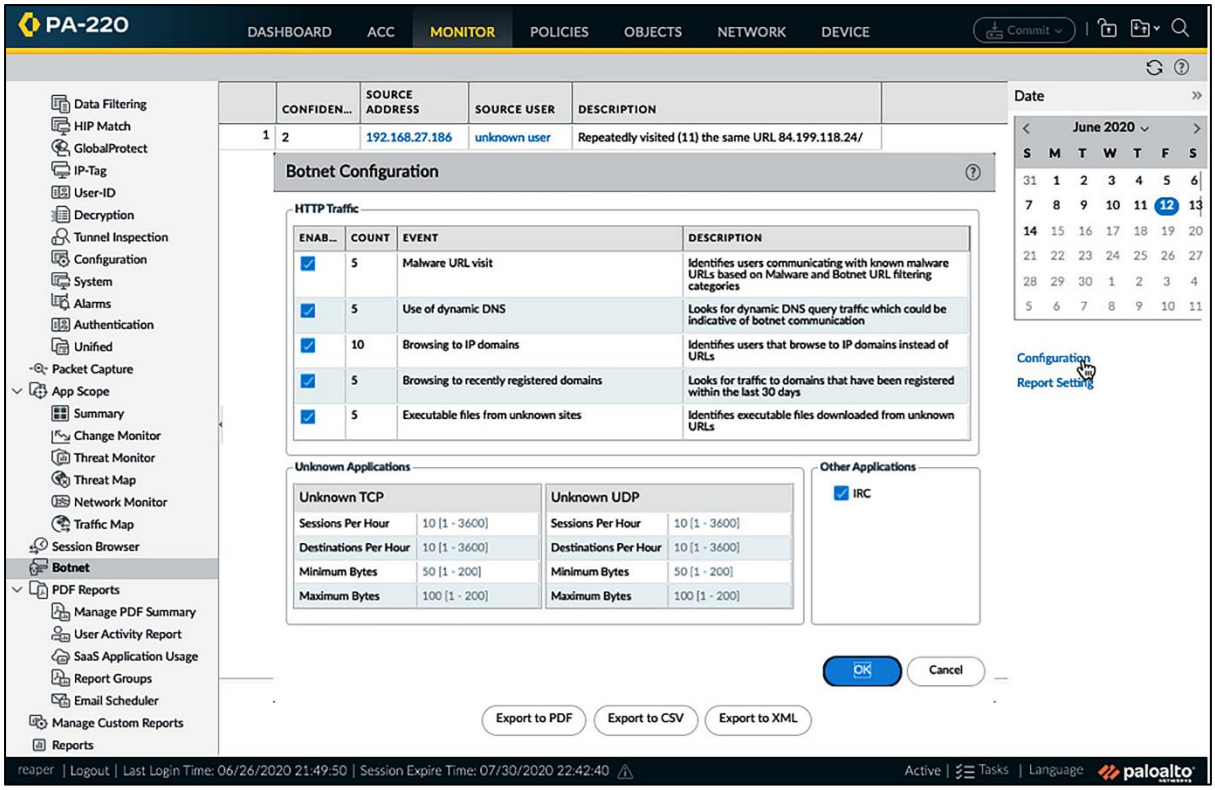
	NAME	Source		Destination		SERVICE	ACTION	Protection		SCHEDULE
		ZONE/INTERFA...	ADDRESS	ZONE/INTE...	ADDRESS			AGGREGATE	CLASSIFIED	
1	protect webserver	ethernet1/1	any	dmz	webserverfarm-public	service-https	protect	AggregateDoS	profile: ClassifiedDoS src-dest-ip-both	none

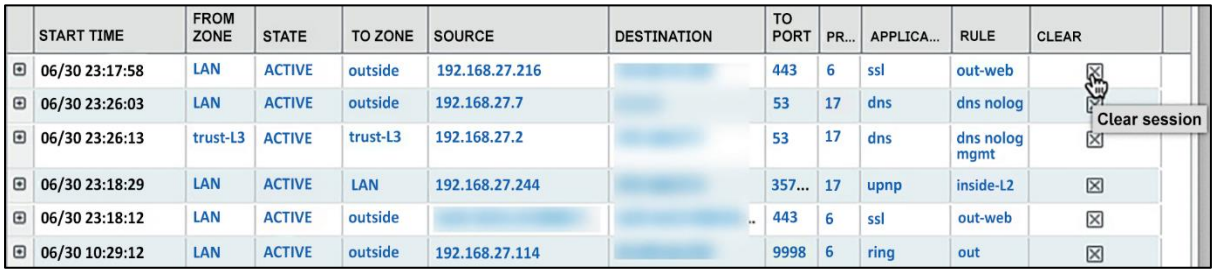


Chapter 12: Troubleshooting Common Session Issues

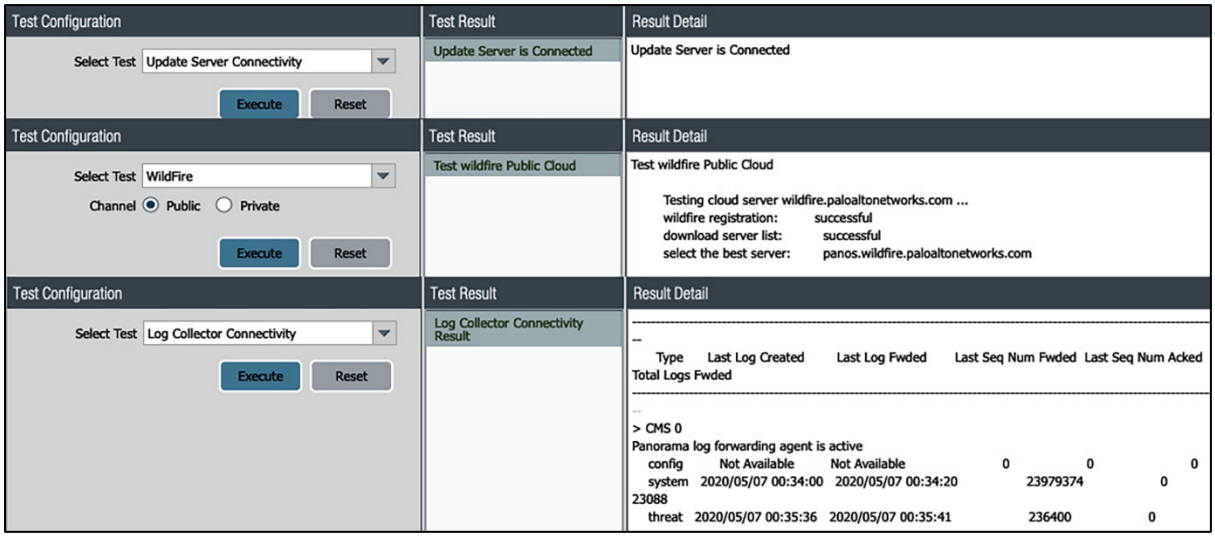


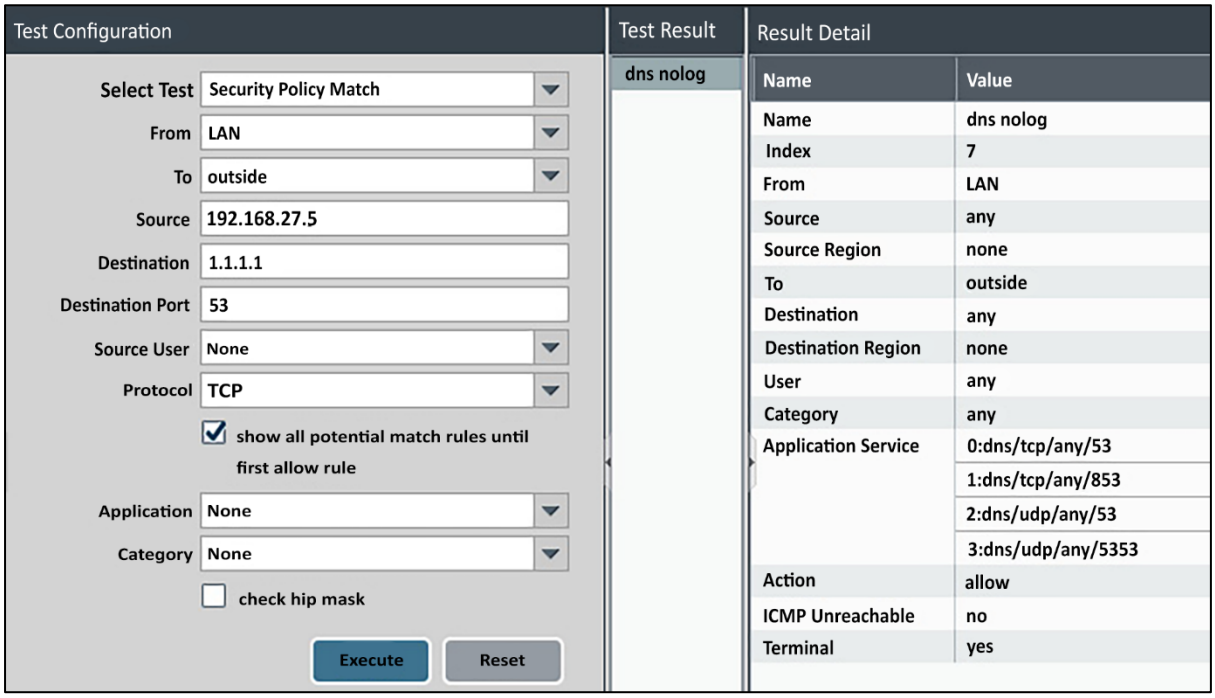


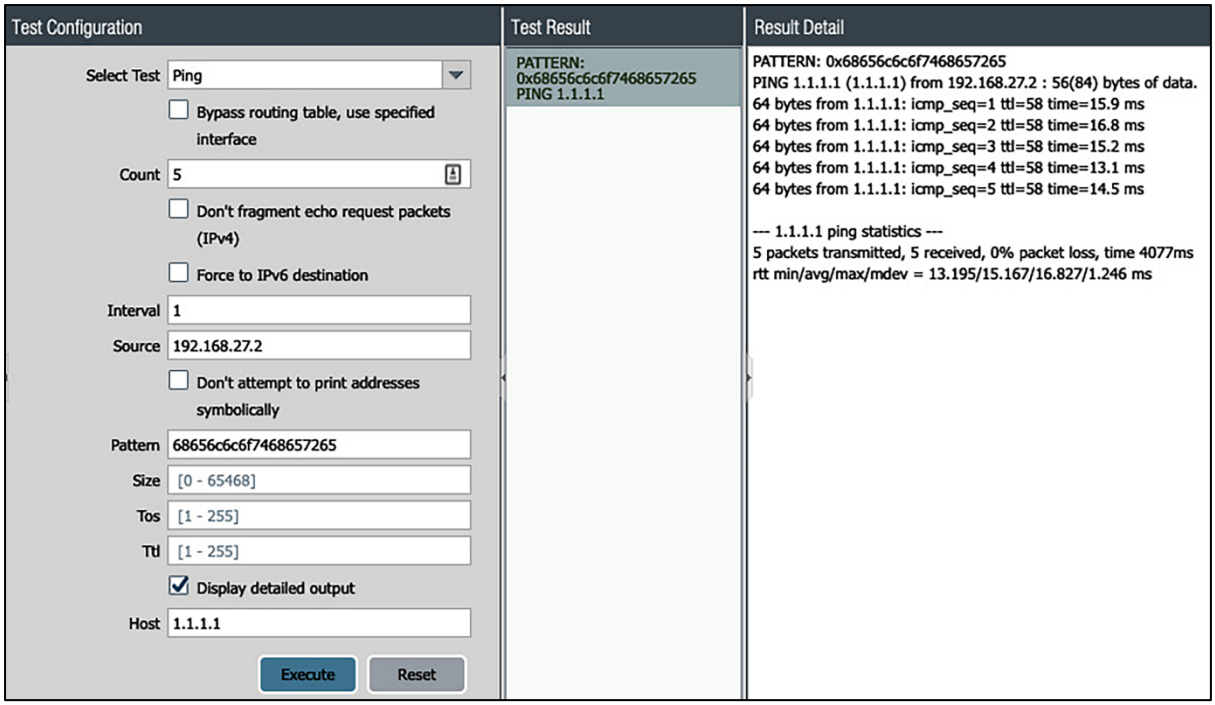


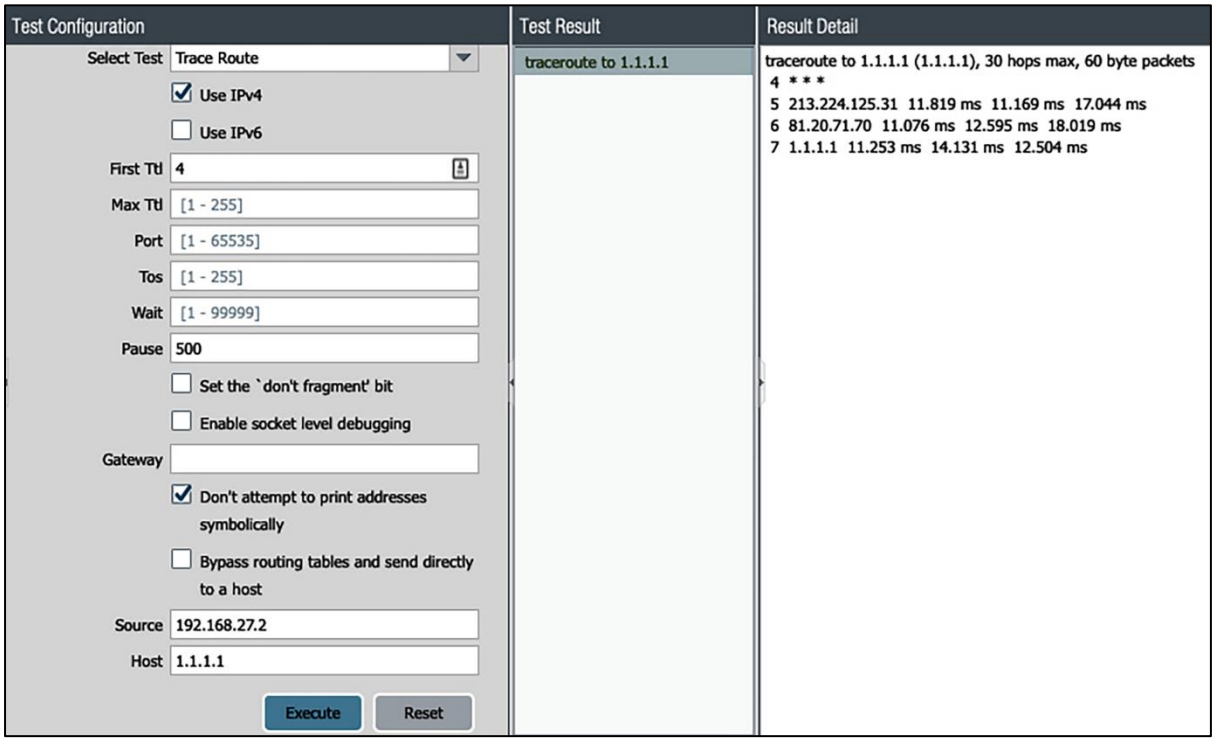


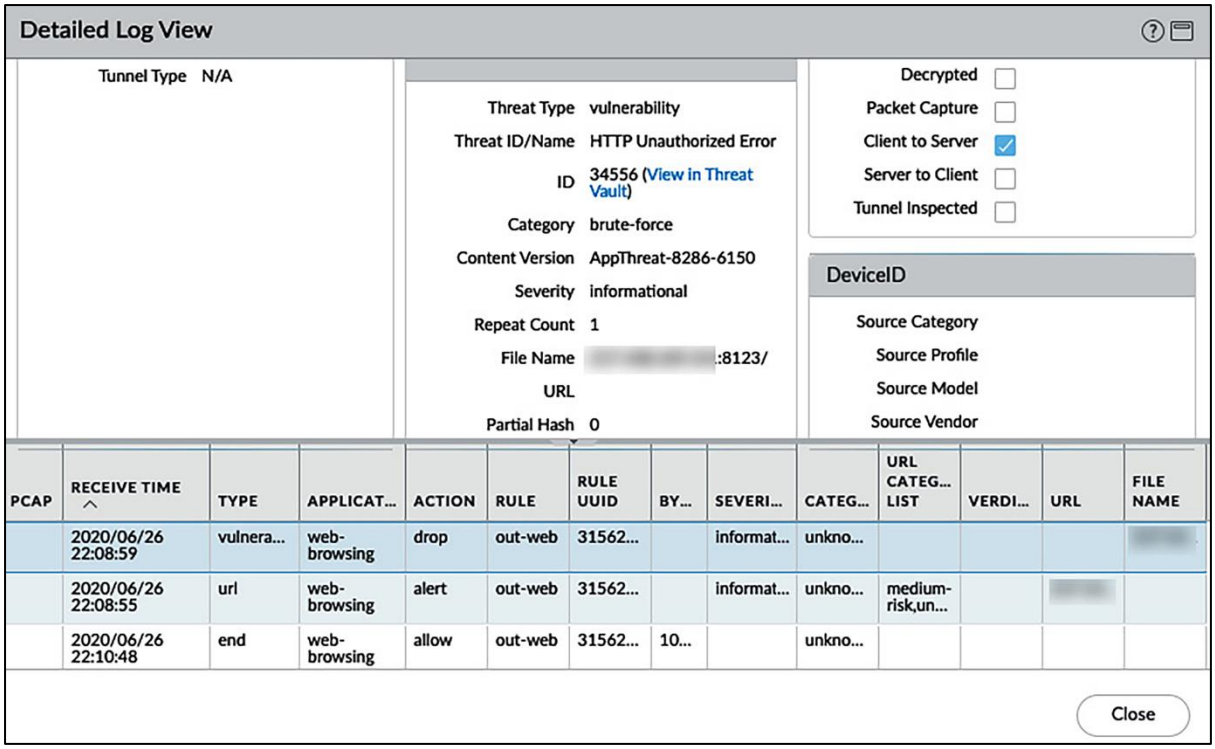

```
reaper@PA-VM> show session all filter protocol 6 nat source from trust type flow state active

--------------------------------------------------------------------------------
ID          Application    State   Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                                          Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------------------------------
261         ss1            ACTIVE  FLOW  NS   10.0.0.8[49915]/trust/6  (192.168.27.251(35448])
vsys1                                         [redacted].122.2[443]/untrust  ([redacted].122.2[443])
353         web-browsing   ACTIVE  FLOW  NS   10.0.0.8[50011)/trust/6  (192.168.27.251(43839])
vsys1                                         [redacted].4.52[80]/untrust  ([redacted].4.52[80])
356         web-browsing   ACTIVE  FLOW  NS   10.0.0.8[500101/trust/6  (192.168.27.251[54552])
vsys1                                         [redacted].4.52[80]/untrust  ([redacted].4.52[80])
253         ss1            ACTIVE  FLOW  NS   10.0.0.8[49918]/trust/6  (192.168.27.251(64354])
vsys1                                         [redacted].37.44[443]/untrust  ([redacted].37.44[443])
267         ss1            ACTIVE  FLOW  NS   10.0.0.8[49919]/trust/6  (192.168.27.251[3751])
vsys1                                         [redacted].38.49[443]/untrust  ([redacted].38.49[443])
231         ss1            ACTIVE  FLOW  NS   10.0.0.8[49917]/trust/6  (192.168.27.251(16008])
vsys1                                         [redacted].121.44[443]/untrust  ([redacted].121.44[443])
```

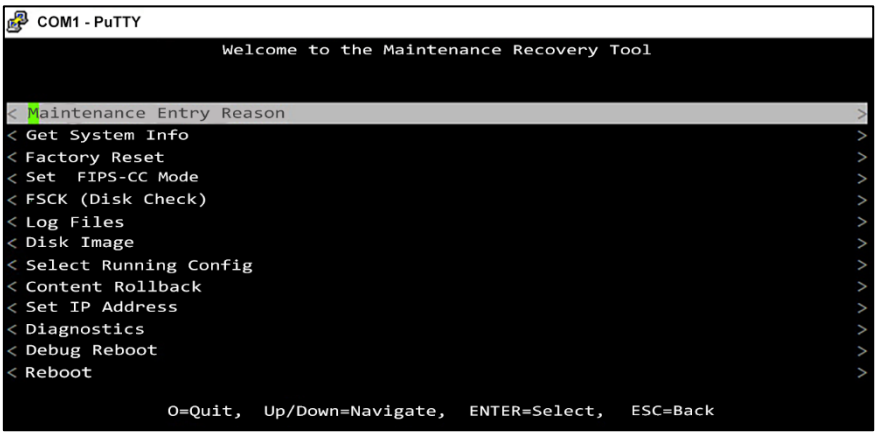

Test Configuration
Select Test
Update Server Connectivity
Execute
Reset
Test Result
Update Server is Connected
Result Detail
Update Server is Connected
Test Configuration
Select Test
WildFire
Channel
Public
Private
Execute
Reset
Test Result
Test wildfire Public Cloud
Result Detail
Test wildfire Public Cloud
Testing cloud server wildfire.paloaltonetworks.com ...
wildfire registration: successful
download server list: successful
select the best server: panos.wildfire.paloaltonetworks.com
Test Configuration
Select Test
Log Collector Connectivity
Execute
Reset
Test Result
Log Collector Connectivity Result
Result Detail
Type Last Log Created Last Log Fwded Last Seq Num Fwded Last Seq Num Acked Total Logs Fwded
> CMS 0
Panorama log forwarding agent is active
config Not Available Not Available 0 0 0
system 2020/05/07 00:34:00 2020/05/07 00:34:20 23979374 0 23088
threat 2020/05/07 00:35:36 2020/05/07 00:35:41 236400 0


Test Configuration
Select Test
Security Policy Match
From
LAN
To
outside
Source
192.168.27.5
Destination
1.1.1.1
Destination Port
53
Source User
None
Protocol
TCP
show all potential match rules until first allow rule
Application
None
Category
None
check hip mask
Execute
Reset
Test Result
dns nolog
Result Detail
Name
Value
Name
dns nolog
Index
7
From
LAN
Source
any
Source Region
none
To
outside
Destination
any
Destination Region
none
User
any
Category
any
Application Service
0:dns/tcp/any/53
1:dns/tcp/any/853
2:dns/udp/any/53
3:dns/udp/any/5353
Action
allow
ICMP Unreachable
no
Terminal
yes


Test Configuration
Select Test
Ping
Bypass routing table, use specified interface
Count
5
Don't fragment echo request packets (IPv4)
Force to IPv6 destination
Interval
1
Source
192.168.27.2
Don't attempt to print addresses symbolically
Pattern
68656c6c6f7468657265
Size
[0 - 65468]
Tos
[1 - 255]
Ttl
[1 - 255]
Display detailed output
Host
1.1.1.1
Execute
Reset
Test Result
PATTERN: 0x68656c6c6f7468657265
PING 1.1.1.1
Result Detail
PATTERN: 0x68656c6c6f7468657265
PING 1.1.1.1 (1.1.1.1) from 192.168.27.2 : 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=58 time=15.9 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=58 time=16.8 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=58 time=15.2 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=58 time=13.1 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=58 time=14.5 ms
--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 13.195/15.167/16.827/1.246 ms


Test Configuration
Select Test
Trace Route
Use IPv4
Use IPv6
First Ttl
4
Max Ttl
[1 - 255]
Port
[1 - 65535]
Tos
[1 - 255]
Wait
[1 - 99999]
Pause
500
Set the `don't fragment' bit
Enable socket level debugging
Gateway
Don't attempt to print addresses symbolically
Bypass routing tables and send directly to a host
Source
192.168.27.2
Host
1.1.1.1
Execute
Reset
Test Result
traceroute to 1.1.1.1
Result Detail
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
4 * * *
5 213.224.125.31 11.819 ms 11.169 ms 17.044 ms
6 81.20.71.70 11.076 ms 12.595 ms 18.019 ms
7 1.1.1.1 11.253 ms 14.131 ms 12.504 ms


Detailed Log View
Tunnel Type N/A
Threat Type vulnerability
Threat ID/Name HTTP Unauthorized Error
ID 34556 (View in Threat Vault)
Category brute-force
Content Version AppThreat-8286-6150
Severity informational
Repeat Count 1
File Name :8123/
URL
Partial Hash 0
Decrypted
Packet Capture
Client to Server
Server to Client
Tunnel Inspected
DeviceID
Source Category
Source Profile
Source Model
Source Vendor
PCAP
RECEIVE TIME
TYPE
APPLICAT...
ACTION
RULE
RULE UUID
BY...
SEVERI...
CATEG...
URL CATEG... LIST
VERDI...
URL
FILE NAME
2020/06/26 22:08:59 vulnera... web-browsing drop out-web 31562... informat... unkno...
2020/06/26 22:08:55 url web-browsing alert out-web 31562... informat... unkno... medium-risk,un...
2020/06/26 22:10:48 end web-browsing allow out-web 31562... 10... unkno...
Close


COM1 - PuTTY
Welcome to the Maintenance Recovery Tool
< Maintenance Entry Reason >
< Get System Info >
< Factory Reset >
< Set FIPS-CC Mode >
< FSCK (Disk Check) >
< Log Files >
< Disk Image >
< Select Running Config >
< Content Rollback >
< Set IP Address >
< Diagnostics >
< Debug Reboot >
< Reboot >
O=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back


Factory Reset
WARNING: Performing a factory reset will remove all logs and configuration.
Using Image:
(x) panos-9.0.0
WARNING: Scrubbing will iteratively write patterns on pancfg, panlogs, and any extra disks to make retrieving the data more difficult.
NOTE: This could take up to 48 hours if selected. Scrubbing is not recommended unless explicitly required.
[ ] Scrub
If scrubbing, select scrub type:
(X) nnsa
( ) dod
< Factory Reset >
< Advanced >
Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back

Chapter 13: A Deep Dive into Troubleshooting

```
reaper@PA-VM> show counter global filter delta yes

Global counters:
Elapsed time since last sampling: 2.476 seconds

name                                    value     rate severity  category  aspect    description
-------------------------------------------------------------------------------
pkt_recv                                    9        3 info      packet    pktproc   packets received
pkt_stp_rcv                                 3        1 info      packet    pktproc   STP BPDU packets received
flow_fwd_l3_bcast_drop                      1        0 drop      flow      forward   Packets dropped: unhandled IP broadcast
flow_fwd_l3_mcast_drop                      1        0 drop      flow      forward   Packets dropped: no route for IP multicast
flow_arp_pkt_rcv                            4        1 info      flow      arp       ARP packets received
flow_arp_rcv_gratuitous                     2        0 info      flow      arp       Gratuitous ARP packets received
-------------------------------------------------------------------------------
Total counters shown: 6
-------------------------------------------------------------------------------

reaper@PA-VM> _
```

```
admin@PA-VM> show counter global filter delta yes severity drop

Global counters:
Elapsed time since last sampling: 27.424 seconds

name                                    value     rate severity  category  aspect    description
-------------------------------------------------------------------------------
flow_ipv6_disabled                         48        1 drop      flow      parse     Packets dropped: IPv6 disabled on interface
flow_fwd_l3_mcast_drop                      7        0 drop      flow      forward   Packets dropped: unhandled IP broadcast
flow_fwd_l3_mcast_drop                     33        1 drop      flow      forward   Packets dropped: no route for IP multicast
-------------------------------------------------------------------------------
Total counters shown: 3
```

```
reaper@PA-VM> debug dataplane packet-diag clear all

Packet diagnosis setting set to default.
reaper@PA-VM> debug dataplane packet-diag clear filter-marked-session all

Unmark All sessions in packet debug
reaper@PA-VM> debug dataplane packet-diag set filter match source 10.0.0.10 destination 194.7.1.4

reaper@PA-VM>
reaper@PA-VM> debug dataplane packet-diag set filter match source 194.7.1.4 destination 198.51.100.2

reaper@PA-VM> debug dataplane packet-diag set filter on

debug packet filter: on
reaper@PA-VM> debug dataplane packet-diag show setting

-------------------------------------------------------------------------------
Packet diagnosis setting:
-------------------------------------------------------------------------------
Packet filter
  Enabled:                  yes
  Match pre-parsed packet:  no
  Index 1: 10.0.0.10/32[0]->194.7.1.4/32[0], proto 0
           ingress-interface any, egress-interface any, exclude non-IP
  Index 2: 194.7.1.4/32(0)->198.51.100.2/32[0], proto 0
           ingress-interface any, egress-interface any, exclude non-IP
-------------------------------------------------------------------------------
Logging
  Enabled:                  no
  Log-throttle:             no
  Sync-log-by-ticks:        yes
  Features:
  Counters:
-------------------------------------------------------------------------------
Packet capture
  Enabled:                  no
  Snaplen:                  0
  Username:
```

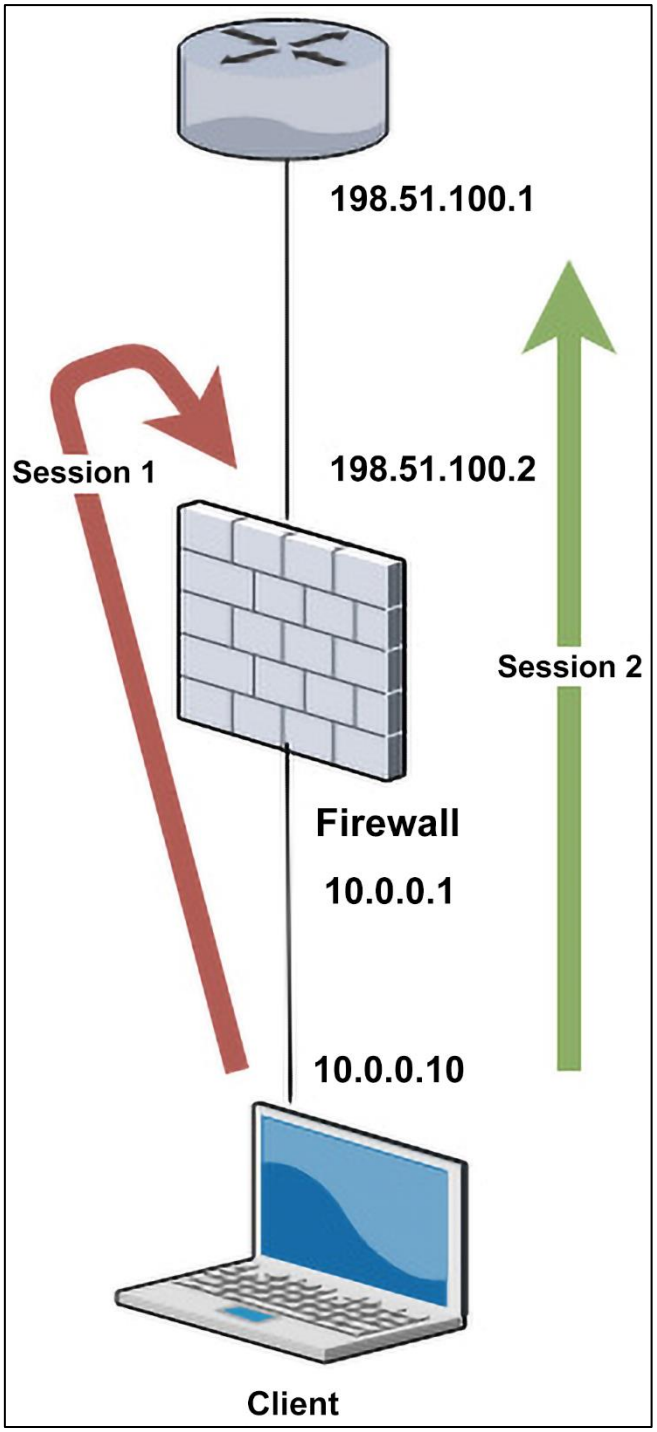
```
reaper@PA-VM> show counter global filter delta yes packet-filter yes

Global counters:
Elapsed time since last sampling: 1.684 seconds

name                                    value     rate severity  category  aspect    description
-------------------------------------------------------------------------------
pkt_sent                                    4        2 info      packet    pktproc   Packets transmitted
session_allocated                           2        1 info      session   resource  sessions allocated
session_installed                           2        1 info      session   resource  sessions installed
flow_ip_cksm_sw_validation                  4        2 info      flow      pktproc   Packets for which IP checksum validation was done in software
appid_ident_by_icmp                         2        1 info      appid     pktproc   Application identified by icmp type
nat_dynamic_port_xlat                       2        1 info      nat       resource  The total number of dynamic_ip_port NAT translate called
dfa_sw                                      4        2 info      dfa       pktproc   The total number of dfa match using software
ctd_pscan_sw                                2        1 info      ctd       pktproc   The total usage of software for pscan
ctd_process                                 2        1 info      ctd       pktproc   session processed by ctd
ctd_pkt_slowpath                            4        2 info      ctd       pktproc   Packets processed by slowpath
-------------------------------------------------------------------------------
Total counters shown: 10
```

```
reaper@PA-VM> show session all filter application ping

--------------------------------------------------------------------------------
ID          Application    State   Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                                          Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------------------------------
6997        ping           ACTIVE  FLOW  NS   10.0.0.10[1109]/trust/1  (198.51.100.2[1109])
vsys1                                         194.7.1.4[1138]/untrust  (194.7.1.4[1138])
6993        ping           ACTIVE  FLOW  NS   10.0.0.10[1109]/trust/1  (198.51.100.2[1109])
vsys1                                         194.7.1.4[1138]/untrust  (194.7.1.4[1134])
6992        ping           ACTIVE  FLOW  NS   10.0.0.10[1109]/trust/1  (198.51.100.2[1109])
vsys1                                         194.7.1.4[1138]/untrust  (194.7.1.4[1133])
```

```
reaper@PA-VM> show counter global filter delta yes packet-filter yes

Global counters:
Elapsed time since last sampling: 2.740 seconds

name                                    value     rate severity  category  aspect    description
-------------------------------------------------------------------------------
session_allocated                           1        0 info      session   resource  Sessions allocated
session_freed                               1        0 info      session   resource  Sessions freed
flow_policy_nat_land                        1        0 drop      flow      session   Session setup: source NAT IP allocation result in LAND attack
nat_dynamic_port_xlat                       1        0 info      nat       resource  The total number of dynamic_ip_port NAT translate called
nat_dynamic_port_release                    2        0 info      nat       resource  The total number of dynamic_ip_port NAT release called
-------------------------------------------------------------------------------
Total counters shown: 5
-------------------------------------------------------------------------------
```

			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SER...	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	U-Turn	none	Trust-L3	Untrust-L3	ethernet1/1	any	198.51.100.2	any	dynamic-ip-and-port ethernet1/3 10.0.0.1/24	destination-translation address: 10.0.0.5 dns-rewrite: reverse
2	inbound SSH server	none	Untrust-L...	Untrust-L3	ethernet1/1	any	109.51.100.2	any	none	destination-translation address: 10.0.0.5
3	dynamic ip-port interface	none	Trust-L3	Untrust-L3	ethernet1/1	dhcpsp...	any	any	dynamic-ip-and-port ethernet1/1 198.51.100.2/24	none

```
[admin@PANgurus> debug dataplane packet-diag set log feature flow
  ager            ager
  all             all
  arp             arp
  basic           basic
  cluster         cluster
  fbo             fbo
  ha              ha
  log             log
  nd              nd
  np              np
  pred            pred
  receive         receive
  sdwan           sdwan
  sdwan_probe     sdwan_probe
  track           track
```


198.51.100.1
Session 1
198.51.100.2
Session 2
Firewall
10.0.0.1
10.0.0.10
Client

```
== 2020-06-04 00:45:37.522 +0200 ==
Packet received at ingress stage, tag 0, type ORDERED
Packet info: len 74 port 17 interface 17 vsys 1
  wqe index 33521 packet 0x0xc0013b0900, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.2, protocol 6
        version 4, ihl 5, tos 0x00, len 60,
        id 41859, frag_off 0x4000, ttl 64, checksum 63842(0x62f9)
TCP:    sport 43100, dport 22, seq 3116136369, ack 0,
        reserved 0, offset 10, window 64240, checksum 24589,
        flags 0x02 ( SYN), urgent data 0, 14 data len 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  69 3f 75 a2 00 00 00 00    ........ i?u.....
00000010: 01 03 03 07                                        ....
Flow lookup, key word0 0x600020016a85c word1 0  word2 0xa00000affff0000 word3 0x0 word4 0x26433c6ffff0000
* Dos Profile NULL (NO) Index (0/0) *
Session setup: vsys 1
No active flow found, enqueue to create session


== 2020-06-04 00:45:37.522 +0200 ==
Packet received at slowpath stage, tag 3223295891, type ATOMIC
Packet info: len 74 port 17 interface 17 vsys 1
  wqe index 33521 packet 0x0xc0013b0900, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.2, protocol 6
        version 4, ihl 5, tos 0x00, len 60,
        id 41859, frag_off 0x4000, ttl 64, checksum 63842(0x62f9)
TCP:    sport 43100, dport 22, seq 3116136369, ack 0,
        reserved 0, offset 10, window 64240, checksum 24589,
        flags 0x02 ( SYN), urgent data 0, 14 data len 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  69 3f 75 a2 00 00 00 00    ........ i?u.....
00000010: 01 03 03 07                                        ....
Session setup: vsys 1
Session setup: ingress interface ethernet1/2 egress interface ethernet1/1 (zone 1)
NAT policy lookup, matched rule index 1
Policy lookup, matched rule index 0,
Allocated new session 265.
set exclude_video in session 265 0xe03cb10780 0 from work 0xe014f40f80 0
Rule: index=1 name=outbound hide, cfg_pool_idx=1 cfg_fallback_pool_idx=0
NAT Rule: name=outbound hide, cfg_pool_idx=1; Session: index=265, nat_pool_idx=1
Packet dropped, vsys 1 NAT rule index 2 result in LAND attack, same SA/DA 198.51.100.2
```

```
== 2020-06-05 00:16:22.030 +0200 ==
Packet received at ingress stage, tag 0, type ORDERED
Packet info: len 74 port 17 interface 17 vsys 1
  wqe index 23554 packet 0x0xc0013fdf40, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.1, protocol 6
        version 4, ihl 5, tos 0x00, len 60,
        id 29076, frag_off 0x4000, ttl 64, checksum 59796(0x94e9)
TCP:    sport 49404, dport 22, seq 4257280317, ack 0,
        reserved 0, offset 10, window 64240, checksum 17082,
        flags 0x02 ( SYN), urgent data 0, 14 data len 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  3d 06 e8 fe 00 00 00 00    ........ =.......
00000010: 01 03 03 07                                        ....
Flow lookup, key word0 0x600020016c0fc word1 0  word2 0xa00000affff0000 word3 0x0 word4 0x16433c6ffff0000
* Dos Profile NULL (NO) Index (0/0) *
Session setup: vsys 1
No active flow found, enqueue to create session


== 2020-06-05 00:16:22.030 +0200 ==
Packet received at slowpath stage, tag 1688519813, type ATOMIC
Packet info: len 74 port 17 interface 17 vsys 1
  wqe index 23554 packet 0x0xc0013fdf40, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.1, protocol 6
        version 4, ihl 5, tos 0x00, len 60,
        id 29076, frag_off 0x4000, ttl 64, checksum 59796(0x94e9)
TCP:    sport 49404, dport 22, seq 4257280317, ack 0,
        reserved 0, offset 10, window 64240, checksum 17082,
        flags 0x02 ( SYN), urgent data 0, 14 data len 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  3d 06 e8 fe 00 00 00 00    ........ =.......
00000010: 01 03 03 07                                        ....
Session setup: vsys 1
PBF lookup (vsys 1) with application none
Session setup: ingress interface ethernet1/2 egress interface ethernet1/1 (zone 1)
NAT policy lookup, matched rule index 1
Policy lookup, matched rule index 0,
TCI_INSPECT: Do TCI lookup policy - appid 0
Allocated new session 941.
set exclude_video in session 941 0xe03cb3ab80 0 from work 0xe014cd2080 0
Rule: index=1 name=outbound hide, cfg_pool_idx=1 cfg_fallback_pool_idx=0
NAT Rule: name=outbound hide, cfg_pool_idx=1; Session: index=941, nat_pool_idx=1
Packet matched vsys 1 NAT rule 'outbound hide' (index 2),
source translation 10.0.0.10/49404 => 198.51.100.2/63571
Created session, enqueue to install. work 0xe014cd2080 exclude_video 0,session 941 0xe03cb3ab80 exclude_video 0
```

```
== 2020-06-05 00:16:22.030 +0200 ==
Packet received at fastpath stage, tag 941, type ATOMIC
Packet info: len 74 port 17 interface 17 vsys 1
  wqe index 23554 packet 0x0xc0013fdf40, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.1, protocol 6
        version 4, ihl 5, tos 0x00, len 60,
        id 29076, frag_off 0x4000, ttl 64, checksum 59796(0x94e9)
TCP:    sport 49404, dport 22, seq 4257280317, ack 0,
        reserved 0, offset 10, window 64240, checksum 17082,
        flags 0x02 ( SYN), urgent data 0, l4 data len 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  3d 06 e8 fe 00 00 00 00    ........ =.......
00000010: 01 03 03 07                                         ....
Flow fastpath, session 941 c2s (set work 0xe014cd2080 exclude_video 0 from sp 0xe03cb3ab80 exclude_video 0)
IP checksum valid
* Dos Profile NULL (NO) Index (0/0) *
* Dos Profile NULL (NO) Index (0/0) *
2020-06-05 00:16:22.030 +0200  pan_flow_process_fastpath(src/pan_flow_proc.c:3928): SESSION-DSCP: set session DSCP: 0x00
NAT session, run address/port translation
Syn Cookie: pan_reass(Init statete): c2s:0 c2s:nxtseq 4257280318 c2s:startseq 4257280318 c2s:win 0 c2s:st 3 c2s:newsyn 0
0 plen 0
CP-DENY TCP non data packet getting through
Forwarding lookup, ingress interface 17
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 198.51.100.1
Route found, interface ethernet1/1, zone 1
Resolve ARP for IP 198.51.100.1 on interface ethernet1/1
ARP entry found on interface 16
Transmit packet size 60 on port 16
```

```
== 2020-06-05 00:16:22.032 +0200 ==
Packet received at ingress stage, tag 0, type ORDERED
Packet info: len 74 port 16 interface 16 vsys 1
  wqe index 23554 packet 0x0xc002c89380, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:7a:5e:82->00:0c:29:7e:38:db, type 0x0800
IP:     198.51.100.1->198.51.100.2, protocol 6
        version 4, ihl 5, tos 0x00, len 60,
        id 0, frag_off 0x4000, ttl 64, checksum 20966(0xe651)
TCP:    sport 22, dport 63571, seq 671986244, ack 4257280318,
        reserved 0, offset 10, window 28960, checksum 36020,
        flags 0x12 ( SYN ACK), urgent data 0, l4 data len 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  07 57 06 99 3d 06 e8 fe    ........ .W..=...
00000010: 01 03 03 07                                         ....
Flow lookup, key word0 0x60001f8530016 word1 0  word2 0x16433c6ffff0000 word3 0x0 word4 0x26433c6ffff0000
Flow 1883 found, state 2, HA 0
Active flow, enqueue to fastpath process, type 0

* Dos Profile NULL (NO) Index (0/0) *

== 2020-06-05 00:16:22.032 +0200 ==
Packet received at fastpath stage, tag 941, type ATOMIC
Packet info: len 74 port 16 interface 16 vsys 1
  wqe index 23554 packet 0x0xc002c89380, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:7a:5e:82->00:0c:29:7e:38:db, type 0x0800
IP:     198.51.100.1->198.51.100.2, protocol 6
        version 4, ihl 5, tos 0x00, len 60,
        id 0, frag_off 0x4000, ttl 64, checksum 20966(0xe651)
TCP:    sport 22, dport 63571, seq 671986244, ack 4257280318,
        reserved 0, offset 10, window 28960, checksum 36020,
        flags 0x12 ( SYN ACK), urgent data 0, l4 data len 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  07 57 06 99 3d 06 e8 fe    ........ .W..=...
00000010: 01 03 03 07                                         ....
Flow fastpath, session 941 s2c (set work 0xe014cd2080 exclude_video 0 from sp 0xe03cb3ab80 exclude_video 0)
IP checksum valid
* Dos Profile NULL (NO) Index (0/0) *
NAT session, run address/port translation
Syn Cookie: pan_reass(Init statete): c2s:1 c2s:nxtseq 4257280318 c2s:startseq 4257280318 c2s:win 28960 c2s:
s2c:newsyn 0 ack 4257280318 nosyn 0 plen 0
CP-DENY TCP non data packet getting through
Forwarding lookup, ingress interface 16
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 10.0.0.10
Route found, interface ethernet1/2, zone 2
Resolve ARP for IP 10.0.0.10 on interface ethernet1/2
ARP entry found on interface 17
Transmit packet size 60 on port 17
```

```
== 2020-06-05 00:16:22.032 +0200 ==
Packet received at ingress stage, tag 0, type ORDERED
Packet info: len 66 port 17 interface 17 vsys 1
  wqe index 23554 packet 0x0xc0013fe900, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.1, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 29077, frag_off 0x4000, ttl 64, checksum 61588(0x94f0)
TCP:    sport 49404, dport 22, seq 4257280318, ack 671986245,
        reserved 0, offset 8, window 502, checksum 33324,
        flags 0x10 ( ACK), urgent data 0, l4 data len 0
TCP option:
00000000: 01 01 08 0a 3d 06 e9 00  07 57 06 99                 ....=... .W..
Flow lookup, key word0 0x600020016c0fc word1 0  word2 0xa00000affff0000 word3 0x0 word4 0x16433c6ffff0000
Flow 1882 found, state 2, HA 0
Active flow, enqueue to fastpath process, type 0

* Dos Profile NULL (NO) Index (0/0) *

== 2020-06-05 00:16:22.032 +0200 ==
Packet received at fastpath stage, tag 941, type ATOMIC
Packet info: len 66 port 17 interface 17 vsys 1
  wqe index 23554 packet 0x0xc0013fe900, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.1, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 29077, frag_off 0x4000, ttl 64, checksum 61588(0x94f0)
TCP:    sport 49404, dport 22, seq 4257280318, ack 671986245,
        reserved 0, offset 8, window 502, checksum 33324,
        flags 0x10 ( ACK), urgent data 0, l4 data len 0
TCP option:
00000000: 01 01 08 0a 3d 06 e9 00  07 57 06 99                 ....=... .W..
Flow fastpath, session 941 c2s (set work 0xe014cd2080 exclude_video 0 from sp 0xe03cb3ab80 exclude_video 0)
IP checksum valid
NAT session, run address/port translation
CP-DENY TCP non data packet getting through
Forwarding lookup, ingress interface 17
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 198.51.100.1
Route found, interface ethernet1/1, zone 1
Resolve ARP for IP 198.51.100.1 on interface ethernet1/1
ARP entry found on interface 16
Transmit packet size 52 on port 16
```

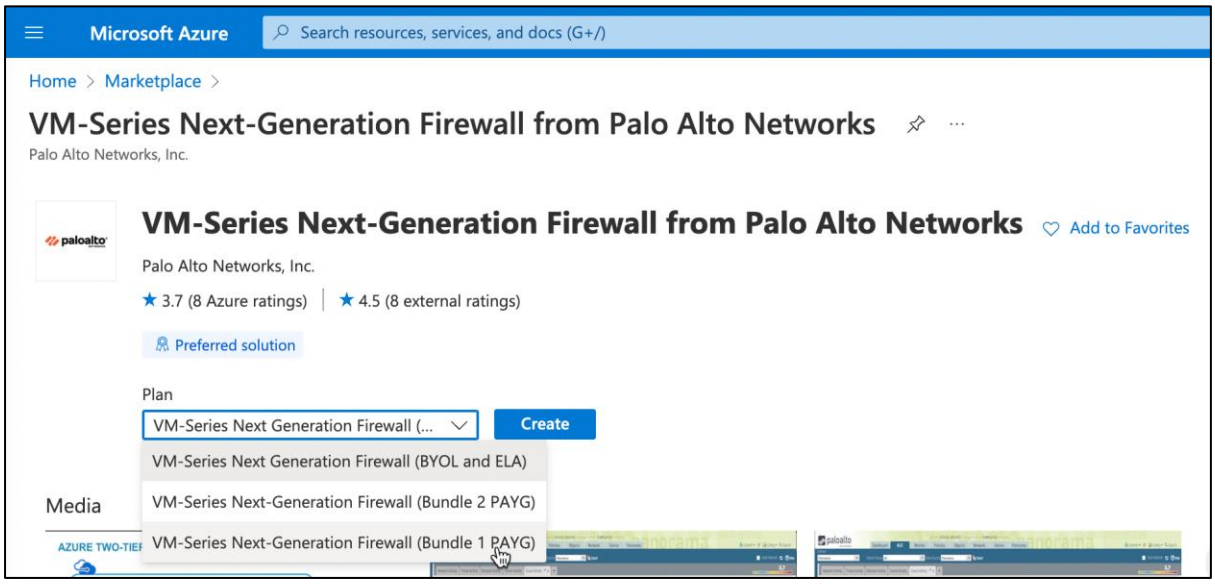
```
== 2020-06-05 00:16:22.032 +0200 ==
Packet received at ingress stage, tag 0, type ORDERED
Packet info: len 107 port 17 interface 17 vsys 1
  wqe index 23554 packet 0x0xc0013ff2c0, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.1, protocol 6
        version 4, ihl 5, tos 0x00, len 93,
        id 29078, frag_off 0x4000, ttl 64, checksum 50836(0x94c6)
TCP:    sport 49404, dport 22, seq 4257280318, ack 671986245,
        reserved 0, offset 8, window 502, checksum 63771,
        flags 0x18 ( ACK PSH), urgent data 0, l4 data len 41
TCP option:
00000000: 01 01 08 0a 3d 06 e9 01  07 57 06 99                 ....=... .W..
Flow lookup, key word0 0x600020016c0fc word1 0  word2 0xa00000affff0000 word3 0x0 word4 0x16433c6ffff0000
Flow 1882 found, state 2, HA 0
Active flow, enqueue to fastpath process, type 0

* Dos Profile NULL (NO) Index (0/0) *
```

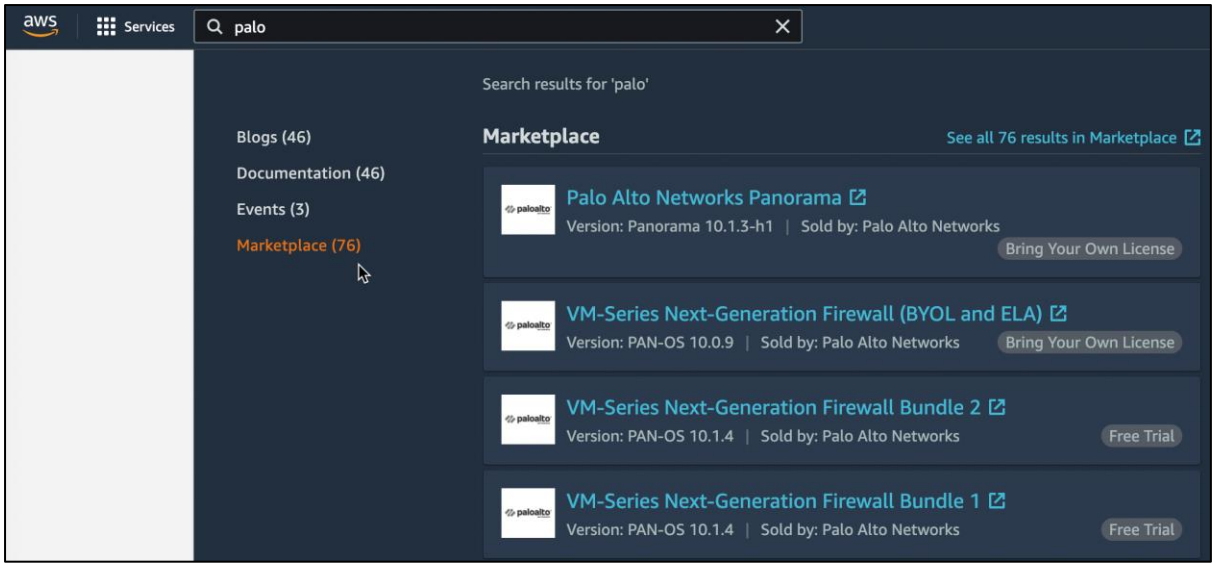
```
== 2020-06-05 00:16:22.032 +0200 ==
Packet received at fastpath stage, tag 941, type ATOMIC
Packet info: len 107 port 17 interface 17 vsys 1
  wqe index 23554 packet 0x0xc0013ff2c0, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:d7:40:22->00:0c:29:7e:38:e5, type 0x0800
IP:     10.0.0.10->198.51.100.1, protocol 6
        version 4, ihl 5, tos 0x00, len 93,
        id 29078, frag_off 0x4000, ttl 64, checksum 50836(0x94c6)
TCP:    sport 49404, dport 22, seq 4257280318, ack 671986245,
        reserved 0, offset 8, window 502, checksum 63771,
        flags 0x18 ( ACK PSH), urgent data 0, l4 data len 41
TCP option:
00000000: 01 01 08 0a 3d 06 e9 01  07 57 06 99                 ....=... .W..
Flow fastpath, session 941 c2s (set work 0xe014cd2080 exclude_video 0 from sp 0xe03cb3ab80 exclude_video 0)
IP checksum valid
NAT session, run address/port translation
session 941 packet sequeunce old 0 new 1
Forwarding lookup, ingress interface 17
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 198.51.100.1
Route found, interface ethernet1/1, zone 1
Resolve ARP for IP 198.51.100.1 on interface ethernet1/1
ARP entry found on interface 16
Transmit packet size 93 on port 16
```

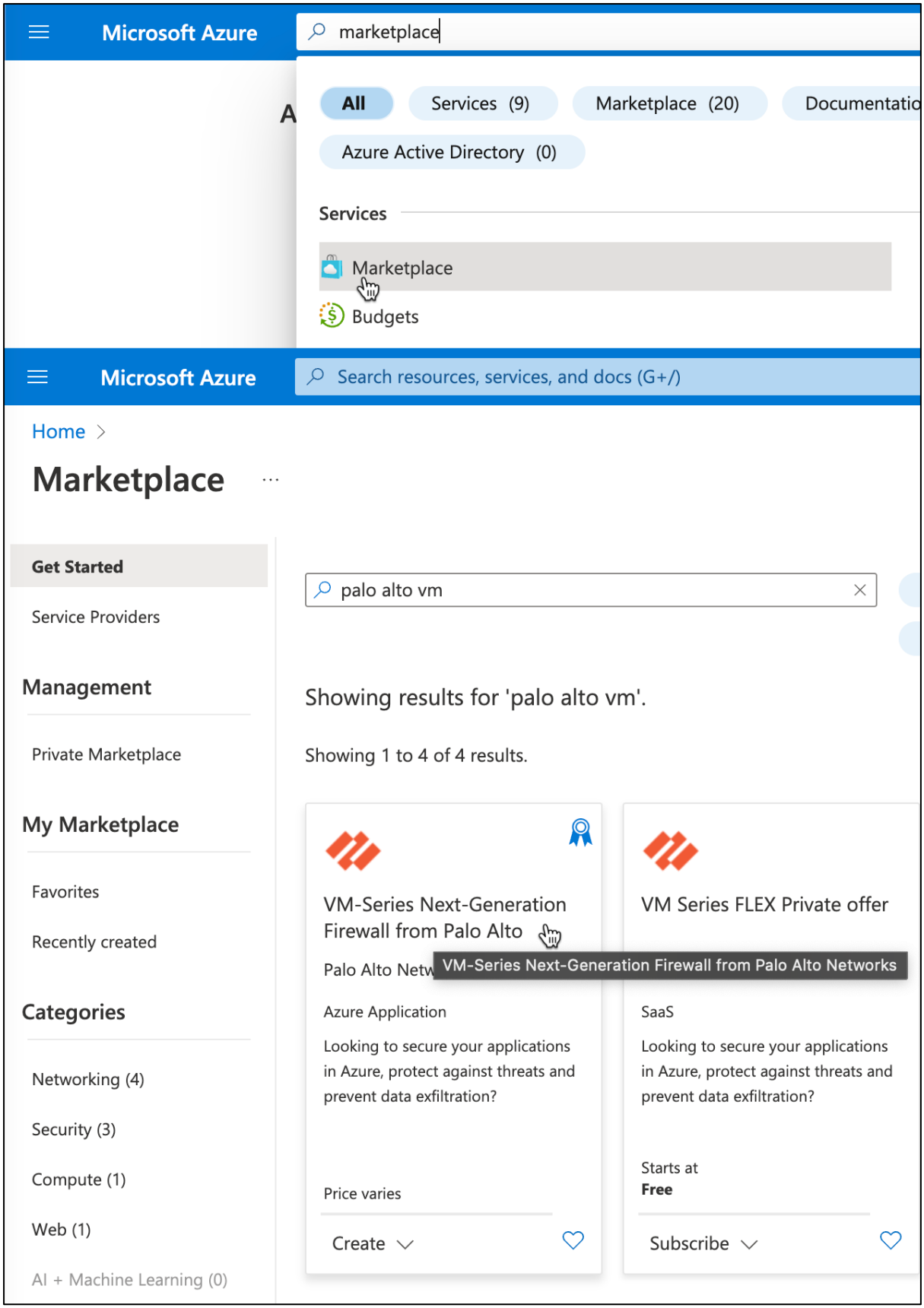
```
== 2020-06-05 00:16:22.034 +0200 ==
Packet received at ingress stage, tag 0, type ORDERED
Packet info: len 66 port 16 interface 16 vsys 1
  wqe index 23554 packet 0x0xc002c83bc0, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:7a:5e:82->00:0c:29:7e:38:db, type 0x0800
IP:     198.51.100.1->198.51.100.2, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 46303, frag_off 0x4000, ttl 64, checksum 31281(0x317a)
TCP:    sport 22, dport 63571, seq 671986245, ack 4257280359,
        reserved 0, offset 8, window 227, checksum 11152,
        flags 0x10 ( ACK), urgent data 0, l4 data len 0
TCP option:
00000000: 01 01 08 0a 07 57 06 9b  3d 06 e9 01                .....W.. =...
Flow lookup, key word0 0x60001f8530016 word1 0  word2 0x16433c6ffff0000 word3 0x0 word4 0x26433c6ffff0000
Flow 1883 found, state 2, HA 0
Active flow, enqueue to fastpath process, type 0

* Dos Profile NULL (NO) Index (0/0) *
```

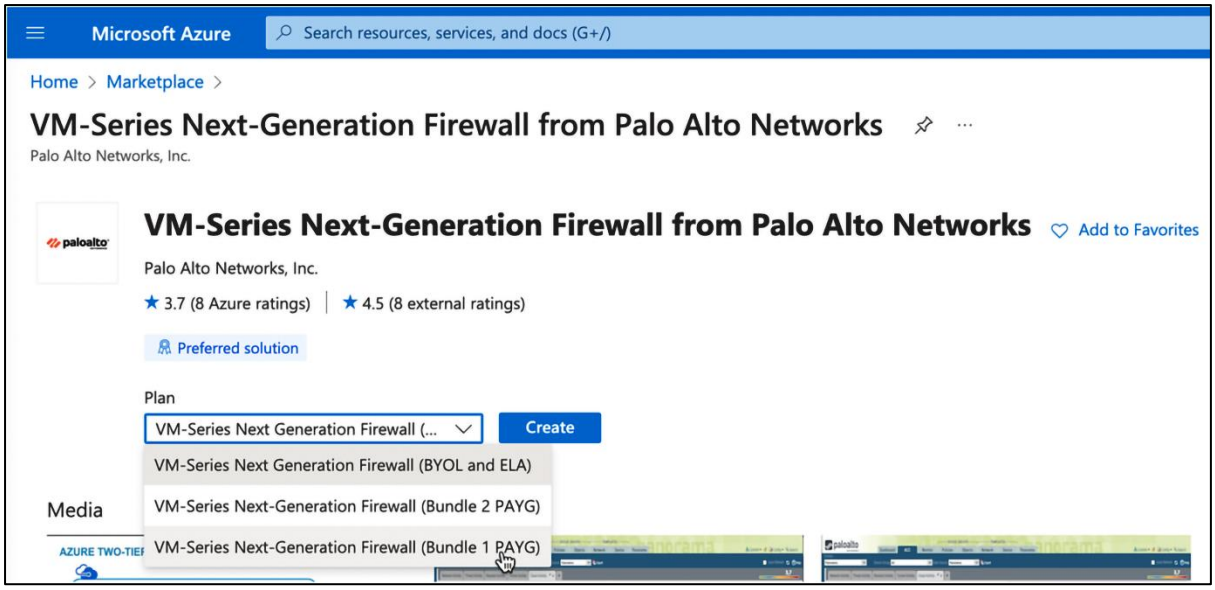
```
== 2020-06-05 00:16:22.034 +0200 ==
Packet received at fastpath stage, tag 941, type ATOMIC
Packet info: len 66 port 16 interface 16 vsys 1
  wqe index 23554 packet 0x0xc002c83bc0, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:7a:5e:82->00:0c:29:7e:38:db, type 0x0800
IP:     198.51.100.1->198.51.100.2, protocol 6
        version 4, ihl 5, tos 0x00, len 52,
        id 46303, frag_off 0x4000, ttl 64, checksum 31281(0x317a)
TCP:    sport 22, dport 63571, seq 671986245, ack 4257280359,
        reserved 0, offset 8, window 227, checksum 11152,
        flags 0x10 ( ACK), urgent data 0, l4 data len 0
TCP option:
00000000: 01 01 08 0a 07 57 06 9b  3d 06 e9 01                .....W.. =...
Flow fastpath, session 941 s2c (set work 0xe014cd2080 exclude_video 0 from sp 0xe03cb3ab80 exclude_video
IP checksum valid
NAT session, run address/port translation
CP-DENY TCP non data packet getting through
Forwarding lookup, ingress interface 16
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 10.0.0.10
Route found, interface ethernet1/2, zone 2
Resolve ARP for IP 10.0.0.10 on interface ethernet1/2
ARP entry found on interface 17
Transmit packet size 52 on port 17
```

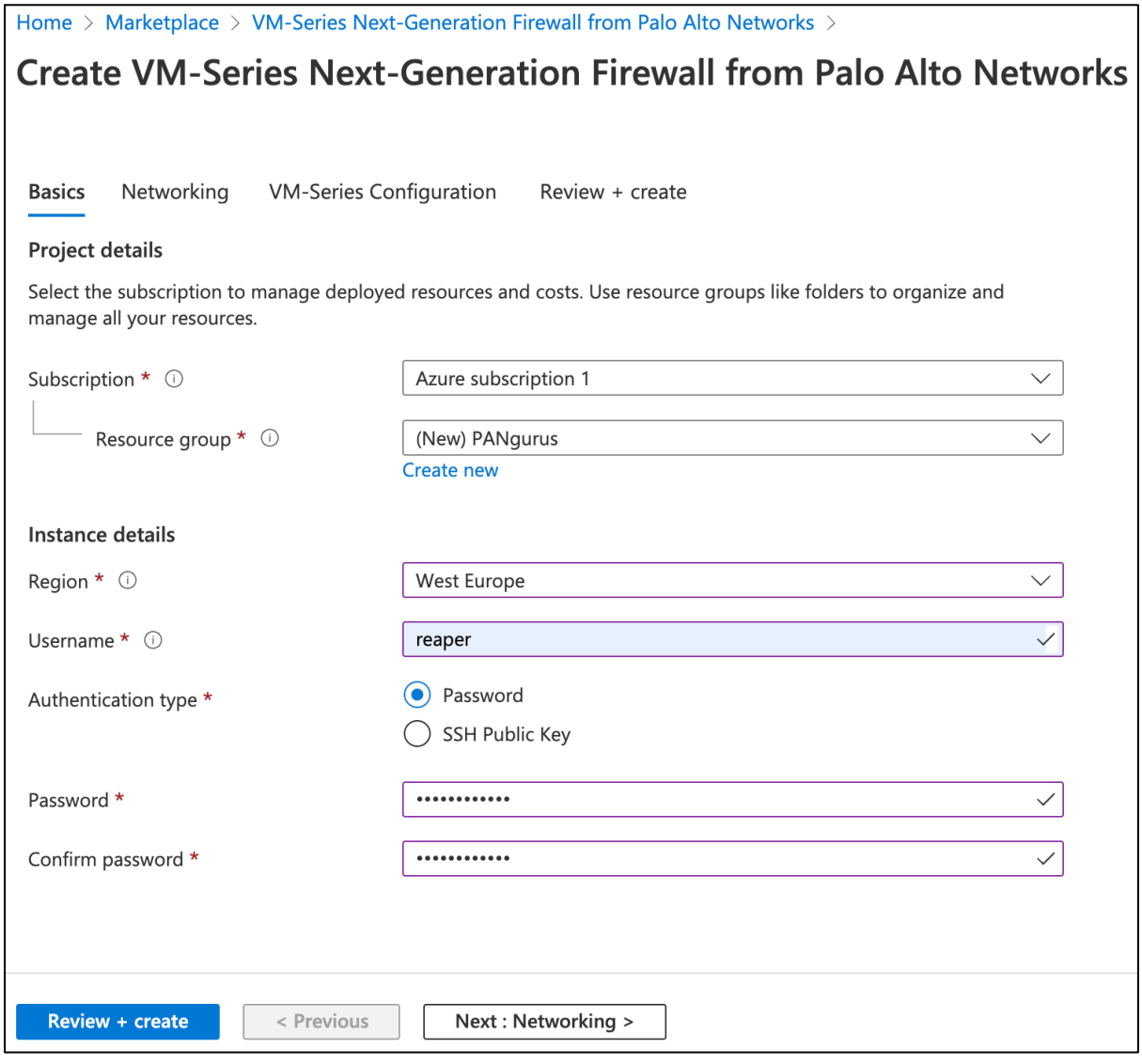
Chapter 14: Cloud-Based Firewall Deployment

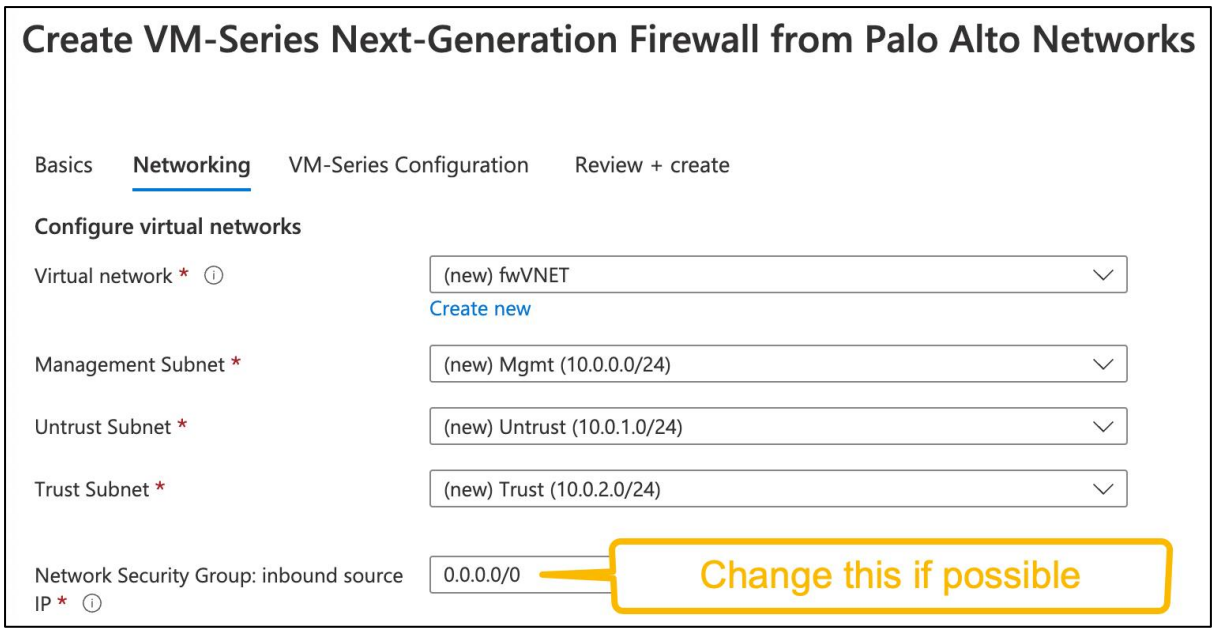


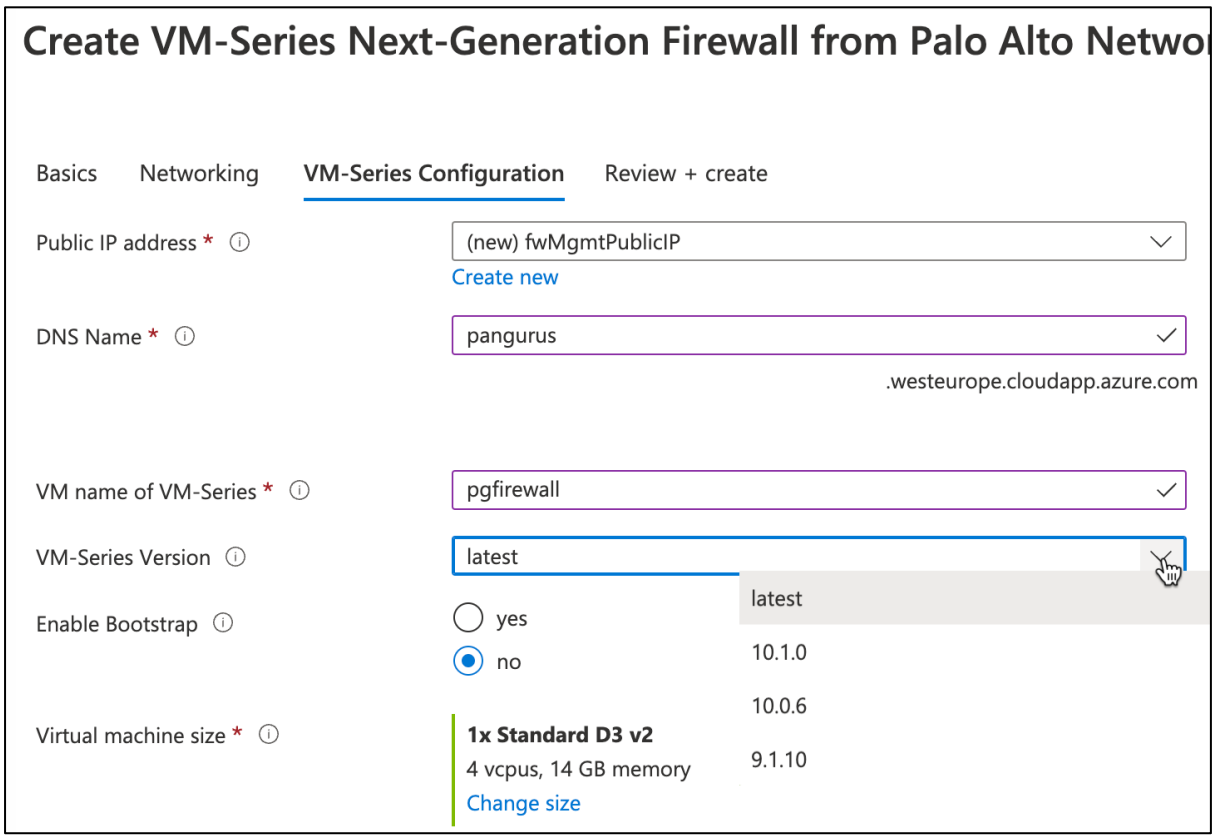

aws
Services
palo
Search results for 'palo'
Blogs (46)
Documentation (46)
Events (3)
Marketplace (76)
Marketplace
See all 76 results in Marketplace
Palo Alto Networks Panorama
Version: Panorama 10.1.3-h1 | Sold by: Palo Alto Networks
Bring Your Own License
VM-Series Next-Generation Firewall (BYOL and ELA)
Version: PAN-OS 10.0.9 | Sold by: Palo Alto Networks
Bring Your Own License
VM-Series Next-Generation Firewall Bundle 2
Version: PAN-OS 10.1.4 | Sold by: Palo Alto Networks
Free Trial
VM-Series Next-Generation Firewall Bundle 1
Version: PAN-OS 10.1.4 | Sold by: Palo Alto Networks
Free Trial


Microsoft Azure
marketplace
All
Services (9)
Marketplace (20)
Azure Active Directory (0)
Services
Marketplace
Budgets
Microsoft Azure
Search resources, services, and docs (G+/)
Home
Marketplace
Get Started
Service Providers
Management
Private Marketplace
My Marketplace
Favorites
Recently created
Categories
Networking (4)
Security (3)
Compute (1)
Web (1)
AI + Machine Learning (0)
palo alto vm
Showing results for 'palo alto vm'.
Showing 1 to 4 of 4 results.
VM-Series Next-Generation Firewall from Palo Alto
VM-Series Next-Generation Firewall from Palo Alto Networks
Azure Application
Looking to secure your applications in Azure, protect against threats and prevent data exfiltration?
Price varies
Create
VM Series FLEX Private offer
SaaS
Looking to secure your applications in Azure, protect against threats and prevent data exfiltration?
Starts at
Free
Subscribe


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Marketplace >
VM-Series Next-Generation Firewall from Palo Alto Networks
Palo Alto Networks, Inc.
VM-Series Next-Generation Firewall from Palo Alto Networks
Add to Favorites
Palo Alto Networks, Inc.
3.7 (8 Azure ratings)
4.5 (8 external ratings)
Preferred solution
Plan
VM-Series Next Generation Firewall (...
Create
VM-Series Next Generation Firewall (BYOL and ELA)
VM-Series Next-Generation Firewall (Bundle 2 PAYG)
VM-Series Next-Generation Firewall (Bundle 1 PAYG)
Media


Home > Marketplace > VM-Series Next-Generation Firewall from Palo Alto Networks >
Create VM-Series Next-Generation Firewall from Palo Alto Networks
Basics
Networking
VM-Series Configuration
Review + create
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure subscription 1
Resource group *
(New) PANgurus
Create new
Instance details
Region *
West Europe
Username *
reaper
Authentication type *
Password
SSH Public Key
Password *
Confirm password *
Review + create
< Previous
Next : Networking >


Create VM-Series Next-Generation Firewall from Palo Alto Networks
Basics
Networking
VM-Series Configuration
Review + create
Configure virtual networks
Virtual network *
(new) fwVNET
Create new
Management Subnet *
(new) Mgmt (10.0.0.0/24)
Untrust Subnet *
(new) Untrust (10.0.1.0/24)
Trust Subnet *
(new) Trust (10.0.2.0/24)
Network Security Group: inbound source IP *
0.0.0.0/0
Change this if possible


Create VM-Series Next-Generation Firewall from Palo Alto Netwo
Basics
Networking
VM-Series Configuration
Review + create
Public IP address *
(new) fwMgmtPublicIP
Create new
DNS Name *
pangurus
.westeurope.cloudapp.azure.com
VM name of VM-Series *
pgfirewall
VM-Series Version
latest
Enable Bootstrap
yes
no
Virtual machine size *
1x Standard D3 v2
4 vcpus, 14 GB memory
Change size
latest
10.1.0
10.0.6
9.1.10

Create VM-Series Next-Generation Firewall from Palo Alto Networks

Validation Passed

Basics | Networking | VM-Series Configuration | **Review + create**

PRODUCT DETAILS

VM-Series Next-Generation Firewall
from Palo Alto Networks
by Palo Alto Networks, Inc.
Terms of use | Privacy policy

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Name	Tom Piens
Preferred e-mail address *	Tom@pangurus.com
Preferred phone number *	[redacted]

Basics

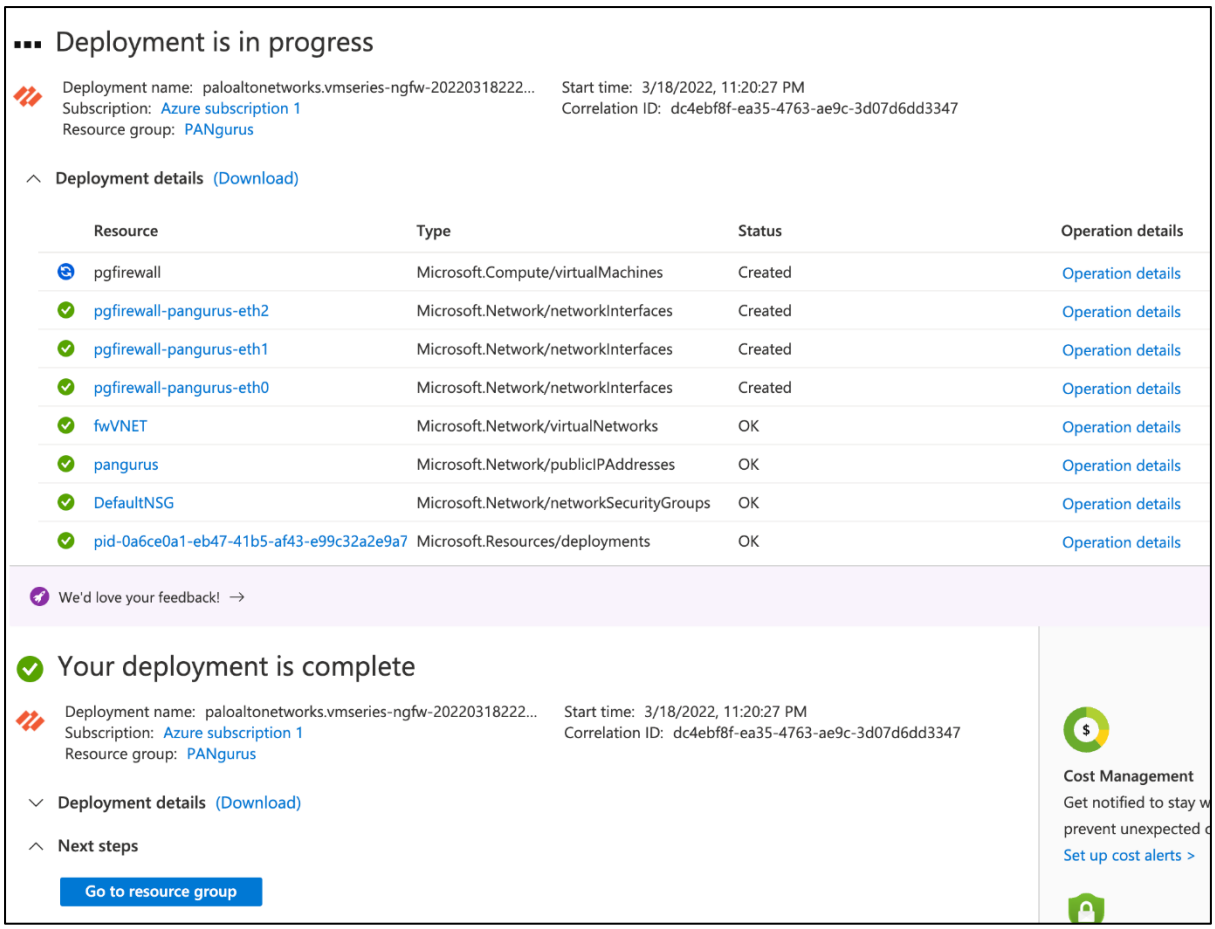
Subscription	Azure subscription 1
Resource group	PANgurus
Region	West Europe
Username	reaper
Password	**********

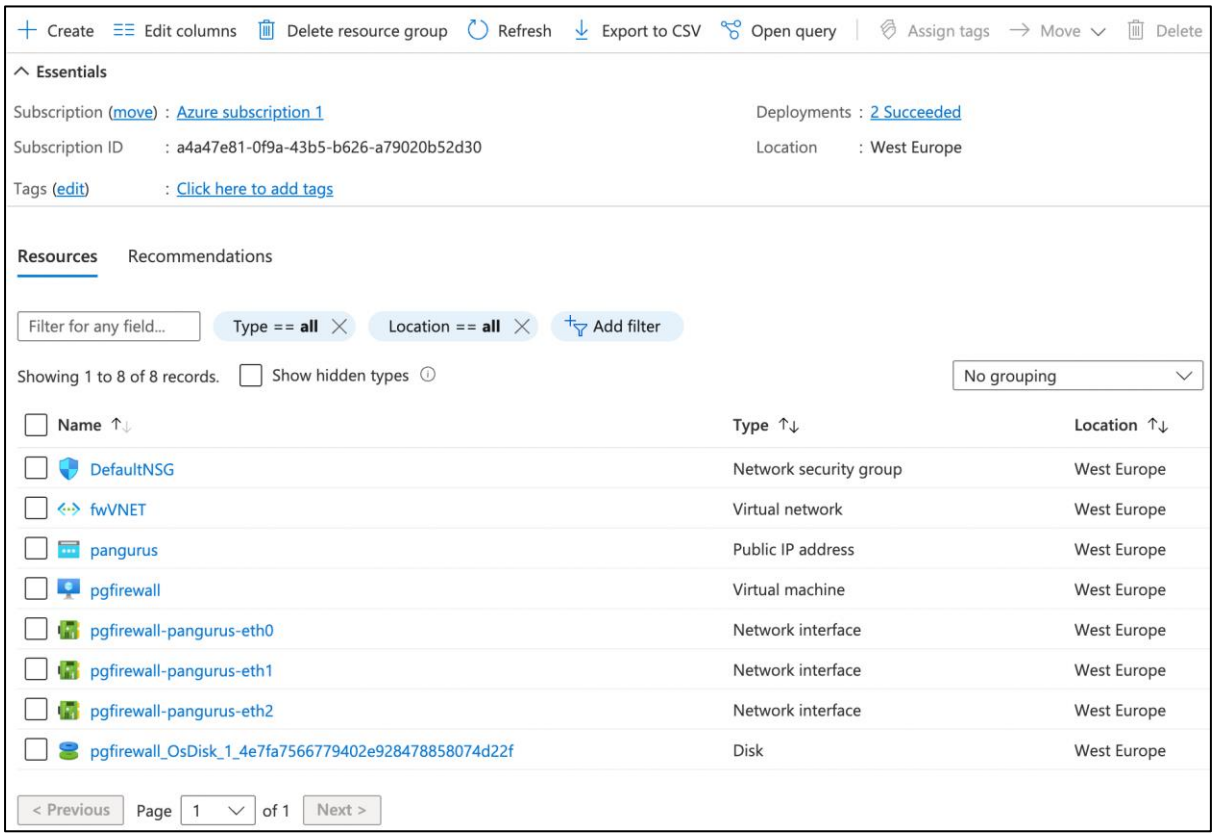
Networking

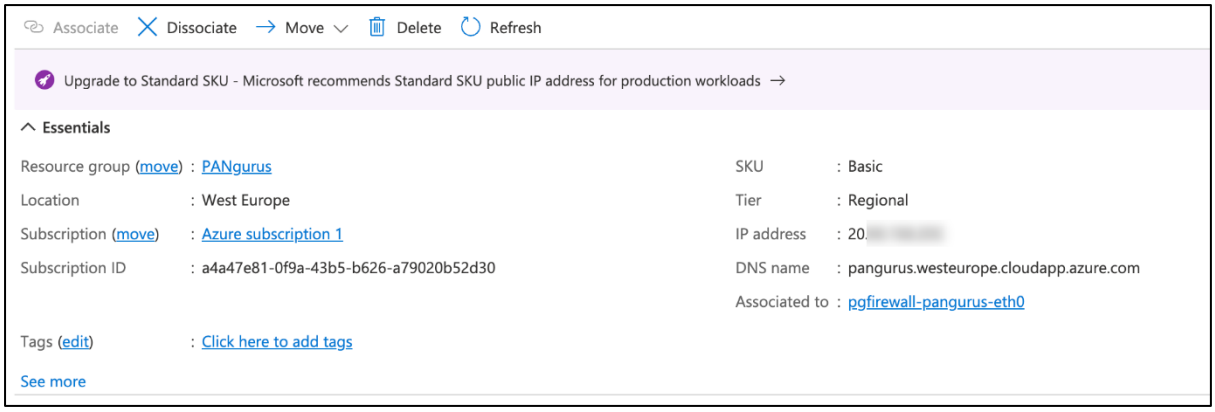
Virtual network	fwVNET
Management Subnet	Mgmt
Address prefix (Management Subnet)	10.0.0.0/24
Untrust Subnet	Untrust
Address prefix (Untrust Subnet)	10.0.1.0/24
Trust Subnet	Trust
Address prefix (Trust Subnet)	10.0.2.0/24
Network Security Group: inbound sourc...	0.0.0.0/0

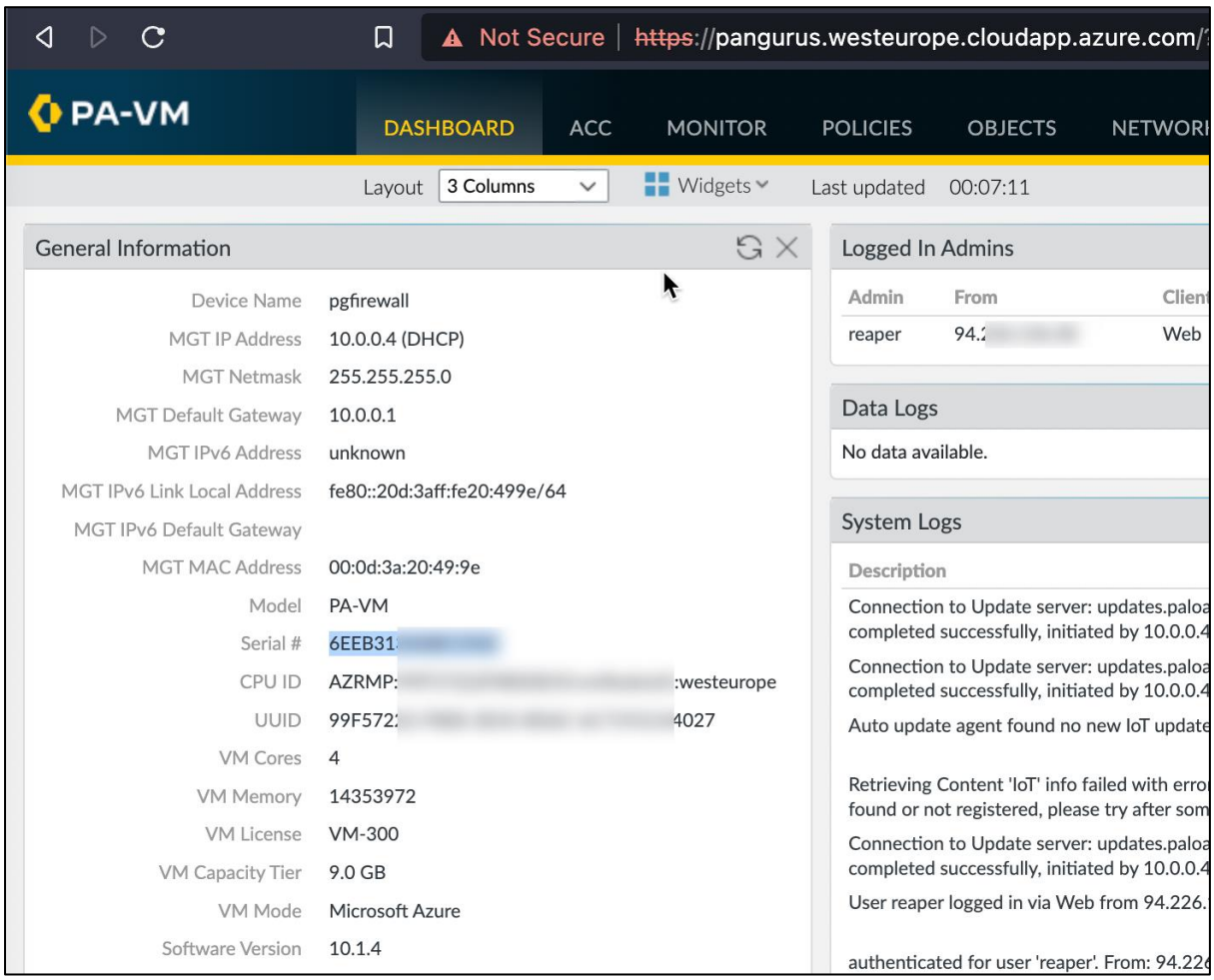
VM-Series Configuration

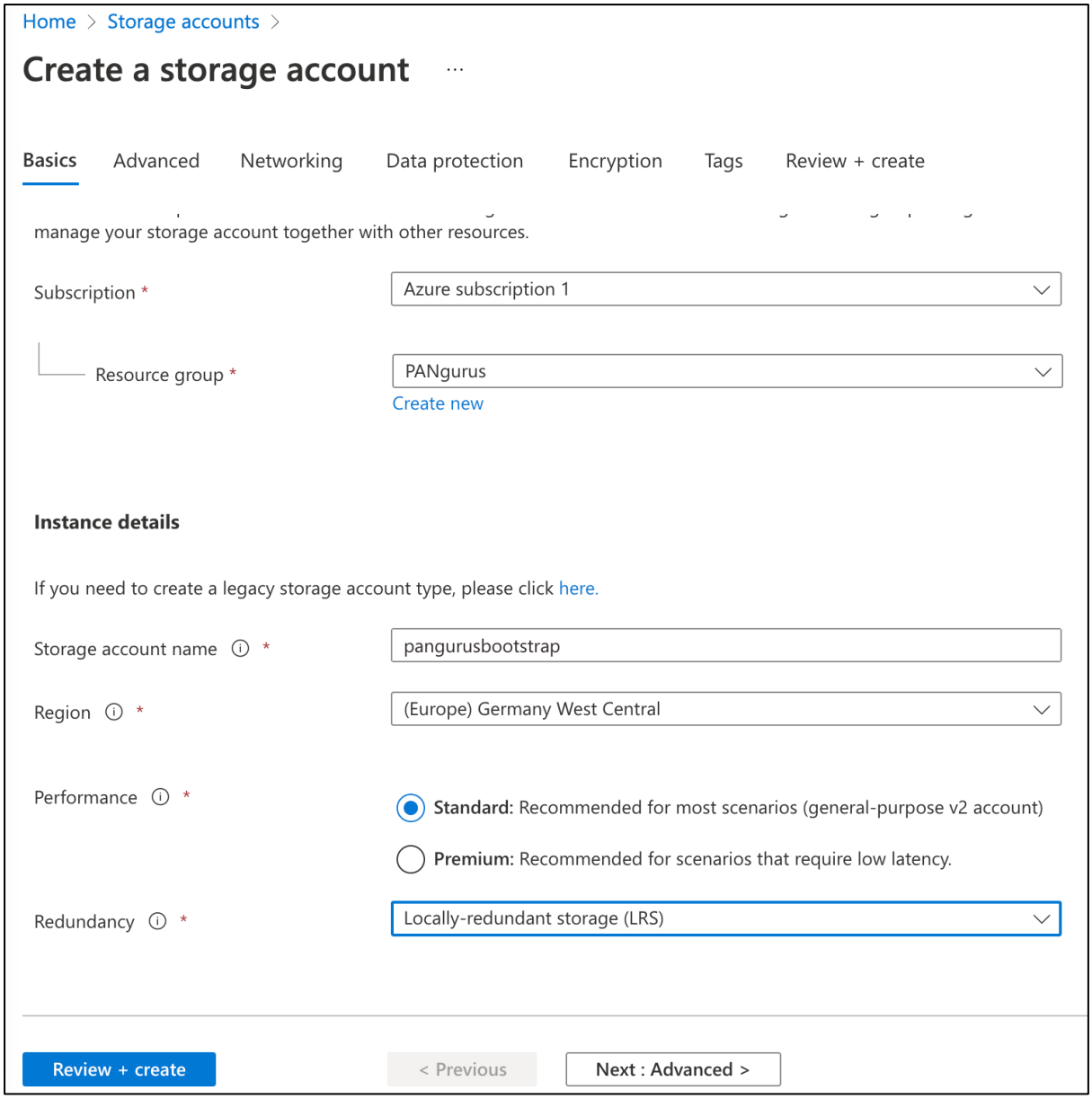
Public IP address	fwMgmtPublicIP
Domain name label	pangurus
VM name of VM-Series	pgfirewall
VM-Series Version	latest
Enable Bootstrap	no
Virtual machine size	Standard_D3_v2

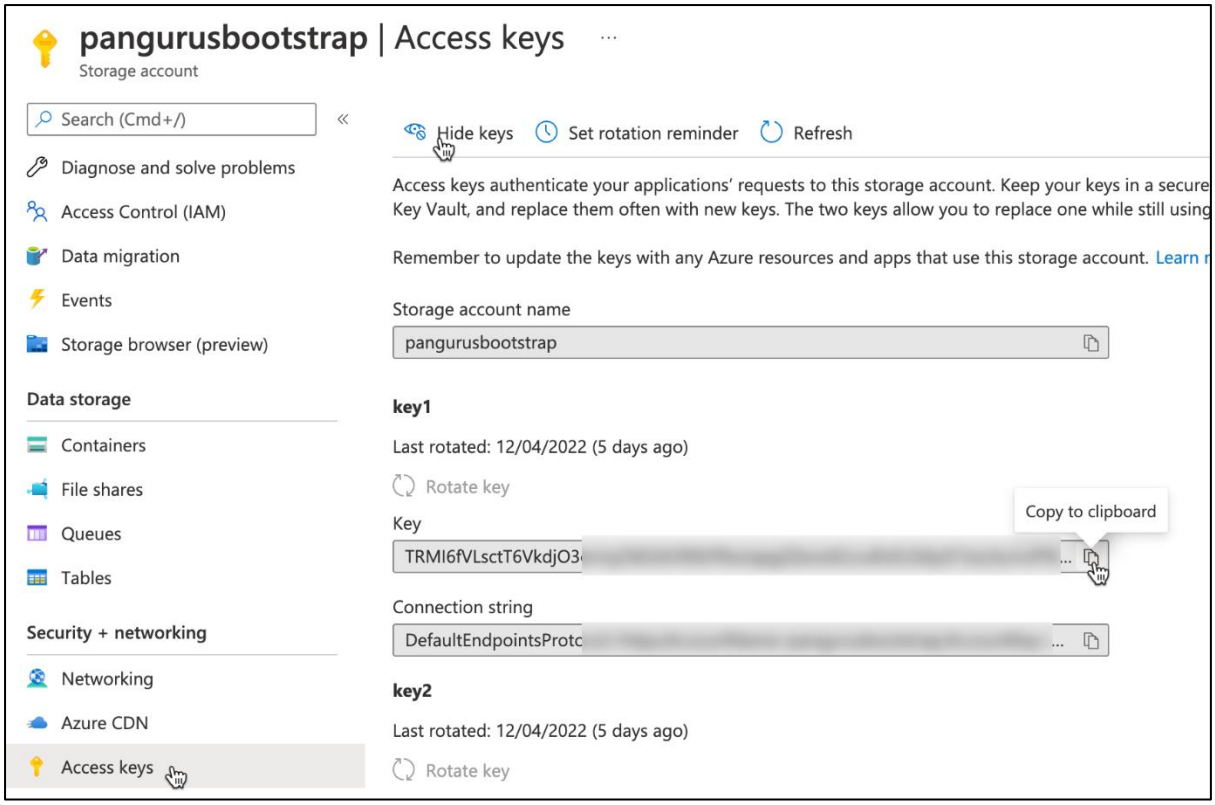

Deployment is in progress
Deployment name: paloaltonetworks.vmseries-ngfw-20220318222...
Subscription: Azure subscription 1
Resource group: PANgurus
Start time: 3/18/2022, 11:20:27 PM
Correlation ID: dc4ebf8f-ea35-4763-ae9c-3d07d6dd3347
Deployment details (Download)
Resource Type Status Operation details
pgfirewall Microsoft.Compute/virtualMachines Created Operation details
pgfirewall-pangurus-eth2 Microsoft.Network/networkInterfaces Created Operation details
pgfirewall-pangurus-eth1 Microsoft.Network/networkInterfaces Created Operation details
pgfirewall-pangurus-eth0 Microsoft.Network/networkInterfaces Created Operation details
fwVNET Microsoft.Network/virtualNetworks OK Operation details
pangurus Microsoft.Network/publicIPAddresses OK Operation details
DefaultNSG Microsoft.Network/networkSecurityGroups OK Operation details
pid-0a6ce0a1-eb47-41b5-af43-e99c32a2e9a7 Microsoft.Resources/deployments OK Operation details
We'd love your feedback!
Your deployment is complete
Deployment name: paloaltonetworks.vmseries-ngfw-20220318222...
Subscription: Azure subscription 1
Resource group: PANgurus
Start time: 3/18/2022, 11:20:27 PM
Correlation ID: dc4ebf8f-ea35-4763-ae9c-3d07d6dd3347
Deployment details (Download)
Next steps
Go to resource group
Cost Management
Get notified to stay w
prevent unexpected c
Set up cost alerts >

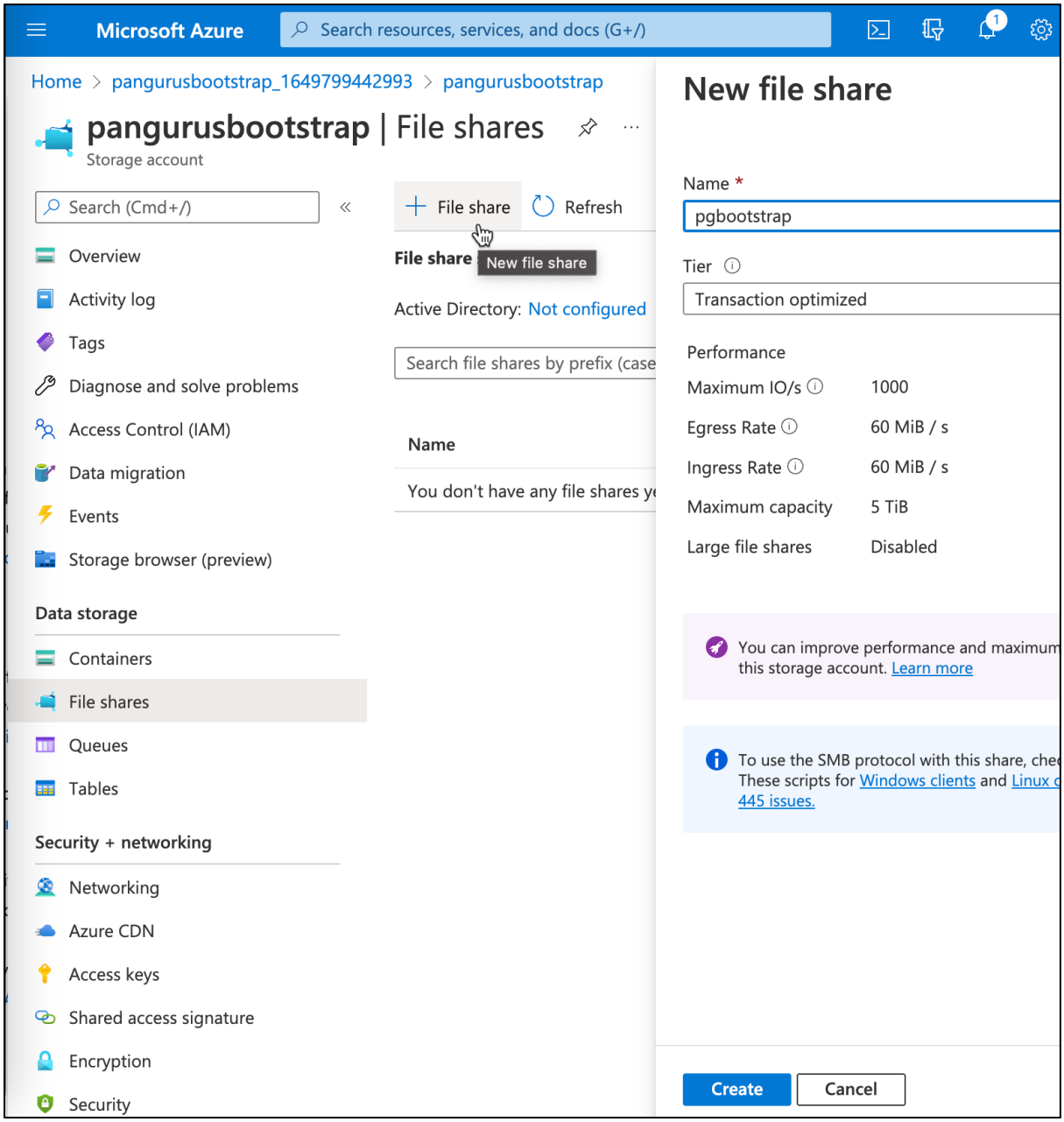

Create
Edit columns
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Delete
Essentials
Subscription (move) : Azure subscription 1
Subscription ID : a4a47e81-0f9a-43b5-b626-a79020b52d30
Tags (edit) : Click here to add tags
Deployments : 2 Succeeded
Location : West Europe
Resources
Recommendations
Filter for any field...
Type == all
Location == all
Add filter
Showing 1 to 8 of 8 records.
Show hidden types
No grouping
Name
Type
Location
DefaultNSG Network security group West Europe
fwVNET Virtual network West Europe
pangurus Public IP address West Europe
pgfirewall Virtual machine West Europe
pgfirewall-pangurus-eth0 Network interface West Europe
pgfirewall-pangurus-eth1 Network interface West Europe
pgfirewall-pangurus-eth2 Network interface West Europe
pgfirewall_OsDisk_1_4e7fa7566779402e928478858074d22f Disk West Europe
< Previous
Page 1 of 1
Next >

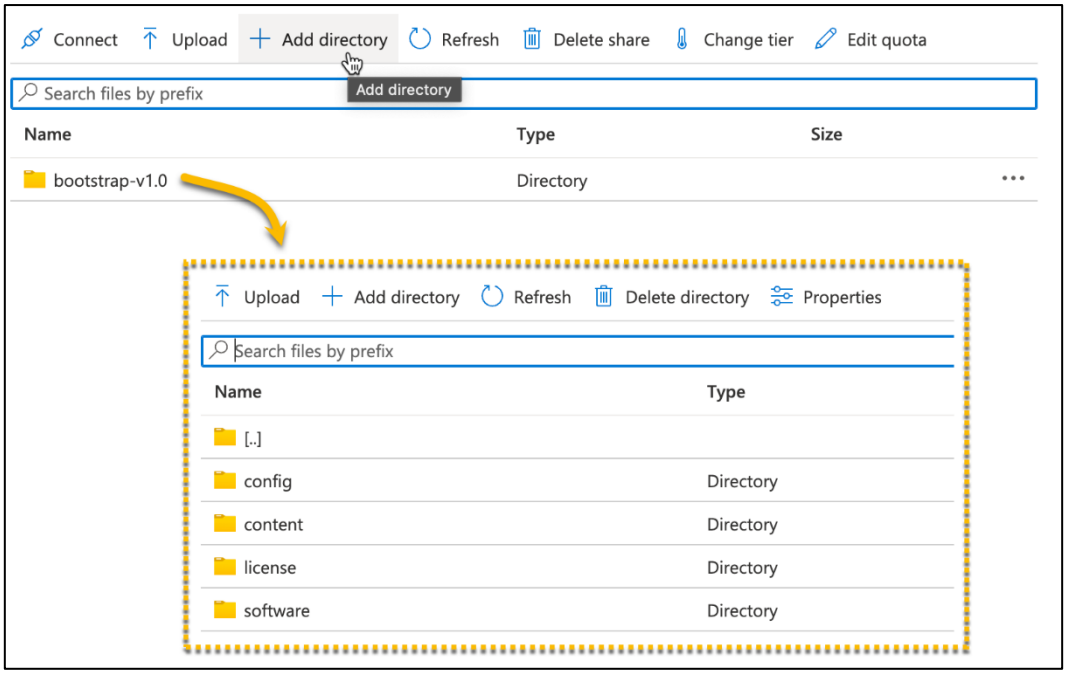

Associate
Dissociate
Move
Delete
Refresh
Upgrade to Standard SKU - Microsoft recommends Standard SKU public IP address for production workloads →
Essentials
Resource group (move) : PANgurus
Location : West Europe
Subscription (move) : Azure subscription 1
Subscription ID : a4a47e81-0f9a-43b5-b626-a79020b52d30
Tags (edit) : Click here to add tags
SKU : Basic
Tier : Regional
IP address : 20.
DNS name : pangurus.westeurope.cloudapp.azure.com
Associated to : pgfirewall-pangurus-eth0
See more


Not Secure
https://pangurus.westeurope.cloudapp.azure.com/
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORI
Layout
3 Columns
Widgets
Last updated
00:07:11
General Information
Device Name pgfirewall
MGT IP Address 10.0.0.4 (DHCP)
MGT Netmask 255.255.255.0
MGT Default Gateway 10.0.0.1
MGT IPv6 Address unknown
MGT IPv6 Link Local Address fe80::20d:3aff:fe20:499e/64
MGT IPv6 Default Gateway
MGT MAC Address 00:0d:3a:20:49:9e
Model PA-VM
Serial # 6EEB31
CPU ID AZRMP: :westeurope
UUID 99F572 4027
VM Cores 4
VM Memory 14353972
VM License VM-300
VM Capacity Tier 9.0 GB
VM Mode Microsoft Azure
Software Version 10.1.4
Logged In Admins
Admin From Client
reaper 94. Web
Data Logs
No data available.
System Logs
Description
Connection to Update server: updates.paloa completed successfully, initiated by 10.0.0.4
Connection to Update server: updates.paloa completed successfully, initiated by 10.0.0.4
Auto update agent found no new IoT update
Retrieving Content 'IoT' info failed with erro found or not registered, please try after som
Connection to Update server: updates.paloa completed successfully, initiated by 10.0.0.4
User reaper logged in via Web from 94.226.
authenticated for user 'reaper'. From: 94.22


Home > Storage accounts >
Create a storage account ...
Basics Advanced Networking Data protection Encryption Tags Review + create
manage your storage account together with other resources.
Subscription *
Azure subscription 1
Resource group *
PANgurus
Create new
Instance details
If you need to create a legacy storage account type, please click here.
Storage account name *
pangurusbootstrap
Region *
(Europe) Germany West Central
Performance *
Standard: Recommended for most scenarios (general-purpose v2 account)
Premium: Recommended for scenarios that require low latency.
Redundancy *
Locally-redundant storage (LRS)
Review + create
< Previous
Next : Advanced >


pangurusbootstrap | Access keys
Storage account
Search (Cmd+/)
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser (preview)
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Azure CDN
Access keys
Hide keys
Set rotation reminder
Refresh
Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure
Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using
Remember to update the keys with any Azure resources and apps that use this storage account. Learn
Storage account name
pangurusbootstrap
key1
Last rotated: 12/04/2022 (5 days ago)
Rotate key
Key
Copy to clipboard
Connection string
key2
Last rotated: 12/04/2022 (5 days ago)
Rotate key


Microsoft Azure
Search resources, services, and docs (G+/)
Home > pangurusbootstrap_1649799442993 > pangurusbootstrap
pangurusbootstrap | File shares
Storage account
Search (Cmd+/)
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser (preview)
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
Security
File share
Refresh
New file share
File share
Active Directory: Not configured
Search file shares by prefix (case
Name
You don't have any file shares y
New file share
Name *
pgbootstrap
Tier
Transaction optimized
Performance
Maximum IO/s 1000
Egress Rate 60 MiB / s
Ingress Rate 60 MiB / s
Maximum capacity 5 TiB
Large file shares Disabled
You can improve performance and maximum
this storage account. Learn more
To use the SMB protocol with this share, chec
These scripts for Windows clients and Linux c
445 issues.
Create
Cancel


Connect
Upload
Add directory
Refresh
Delete share
Change tier
Edit quota
Add directory
Search files by prefix
Name
Type
Size
bootstrap-v1.0
Directory
Upload
Add directory
Refresh
Delete directory
Properties
Search files by prefix
Name
Type
[..]
config
Directory
content
Directory
license
Directory
software
Directory

Basics Networking VM-Series Configuration Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ — Azure subscription 1

Resource group * ⓘ — PANgurus

Create new

Instance details

Region * ⓘ — West Europe

Username * ⓘ — reaper

Authentication type * — (•) Password ( ) SSH Public Key

Password * — ••••••••••••

Confirm password * — ••••••••••••

Basics **Networking** VM-Series Configuration Review + create

Configure virtual networks

Virtual network * ⓘ — (new) fwVNET

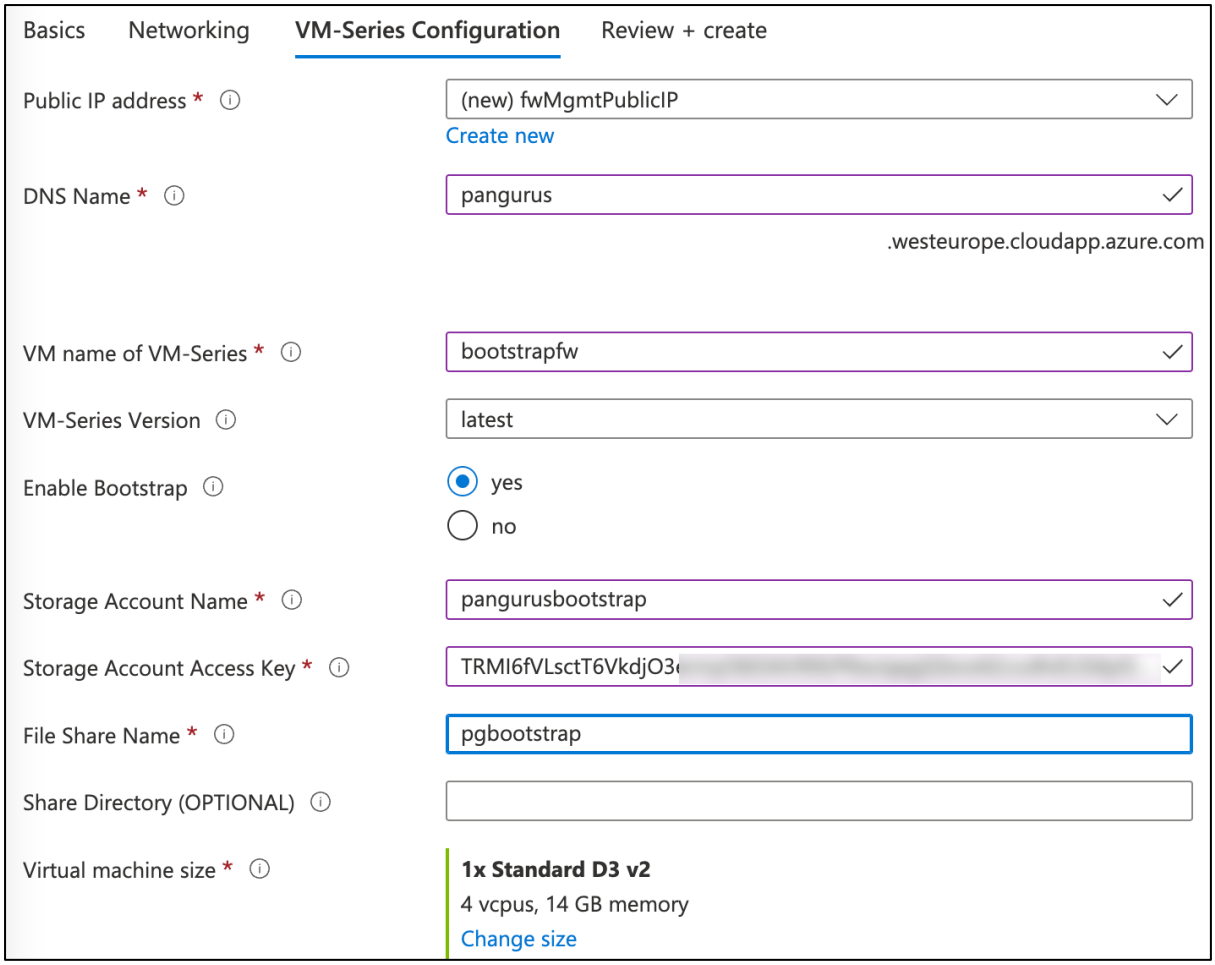
Create new

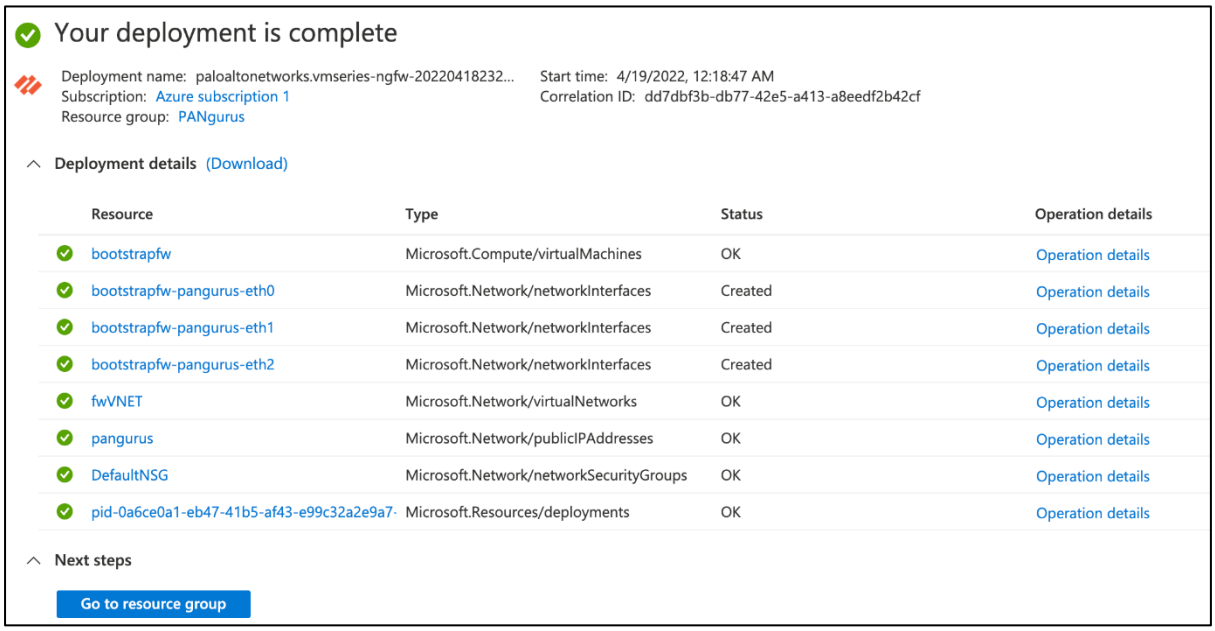
Management Subnet * — (new) Mgmt (10.1.0.0/24)

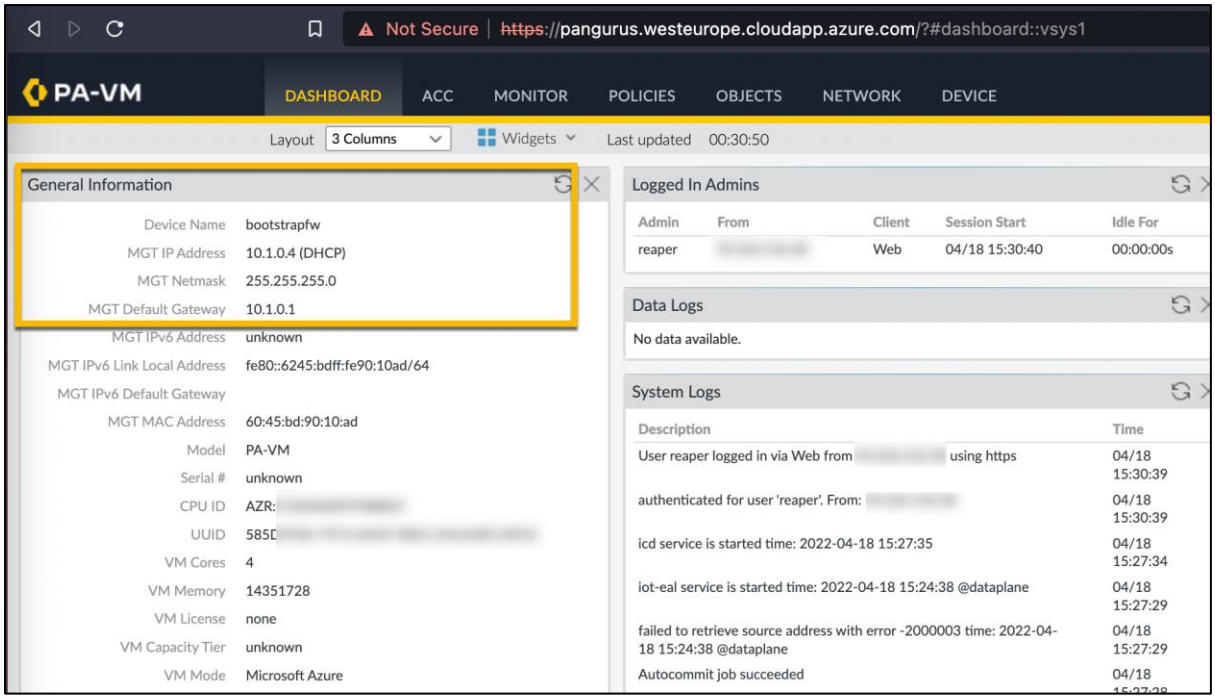
Untrust Subnet * — (new) Untrust (10.1.1.0/24)

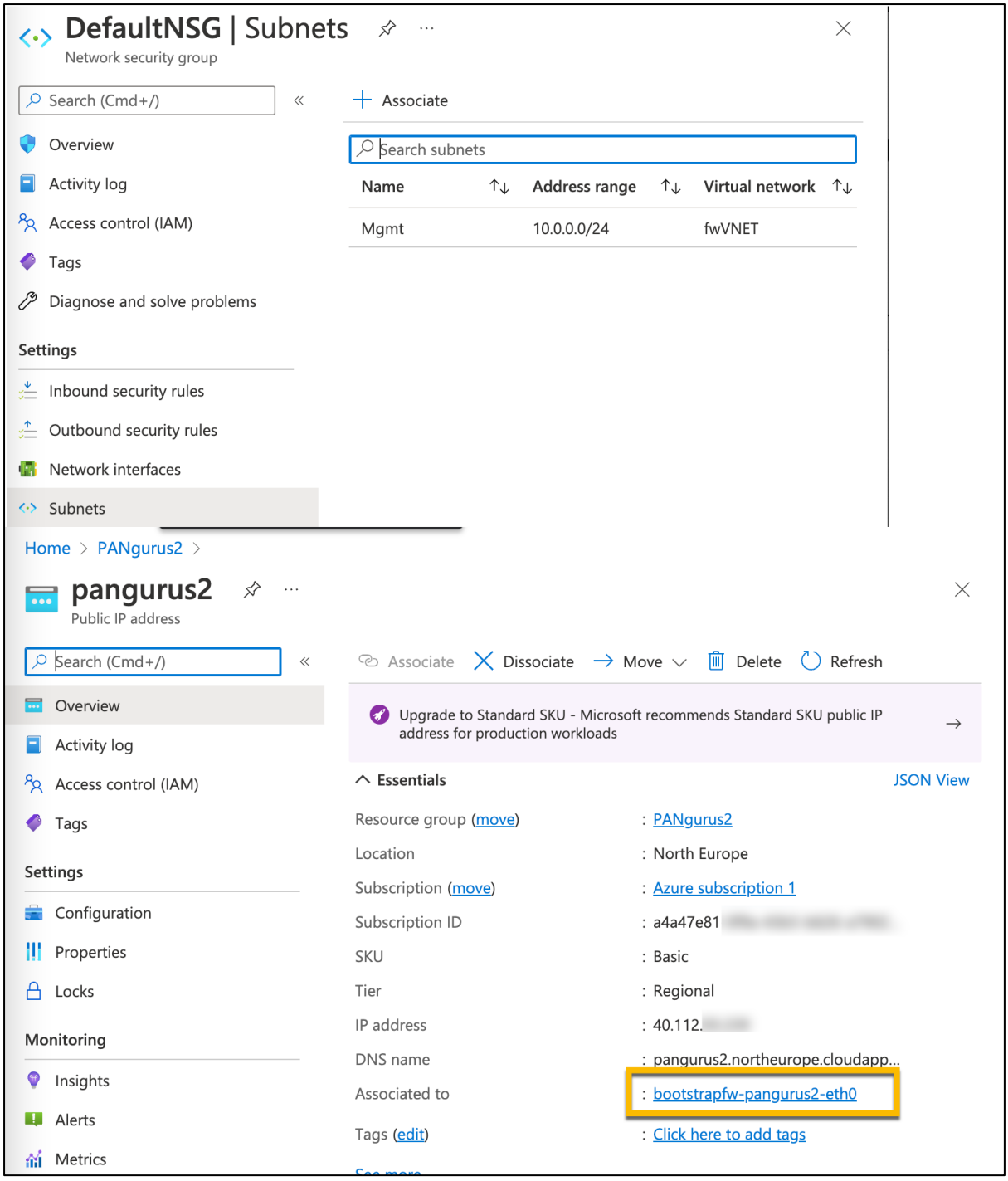
Trust Subnet * — (new) Trust (10.1.2.0/24)

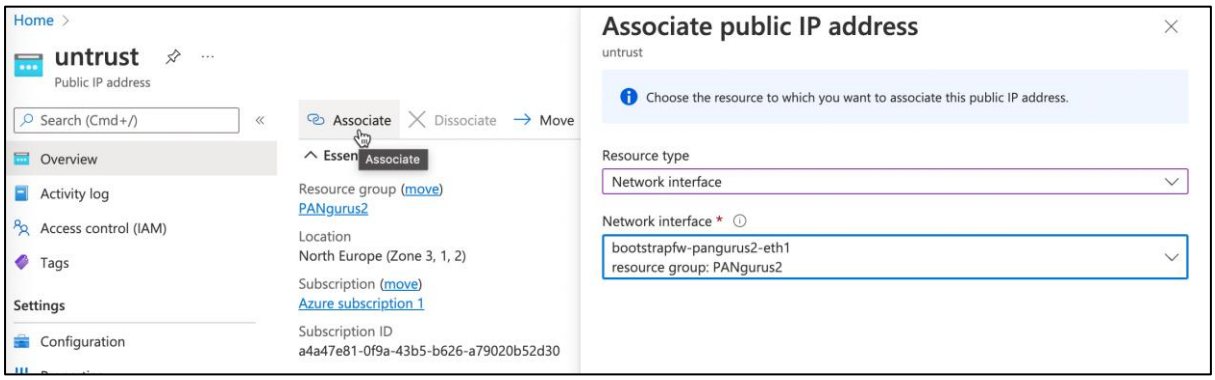
Network Security Group: inbound source IP * ⓘ — 193.158.100.5/32

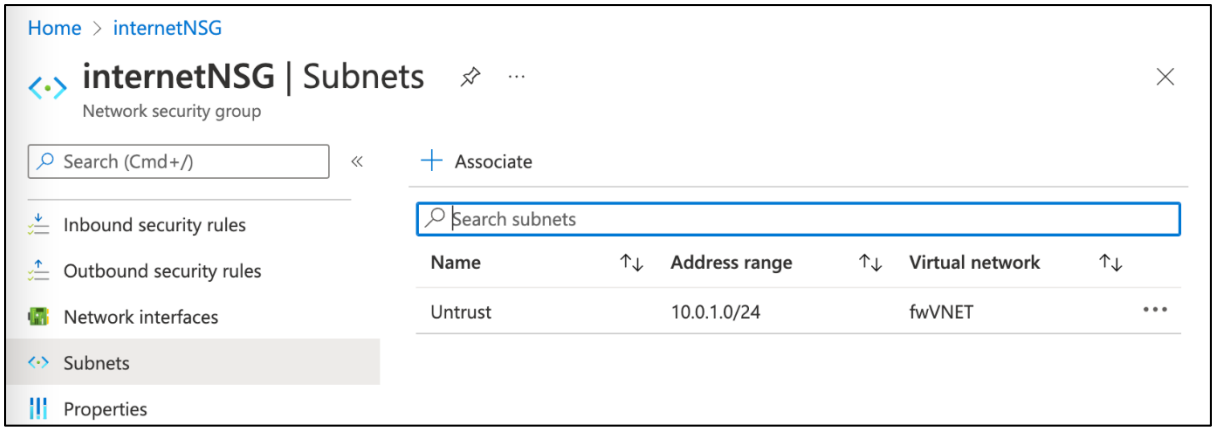

Basics
Networking
VM-Series Configuration
Review + create
Public IP address *
(new) fwMgmtPublicIP
Create new
DNS Name *
pangurus
.westeurope.cloudapp.azure.com
VM name of VM-Series *
bootstrapfw
VM-Series Version
latest
Enable Bootstrap
yes
no
Storage Account Name *
pangurusbootstrap
Storage Account Access Key *
TRMI6fVLsctT6VkdjO3
File Share Name *
pgbootstrap
Share Directory (OPTIONAL)
Virtual machine size *
1x Standard D3 v2
4 vcpus, 14 GB memory
Change size

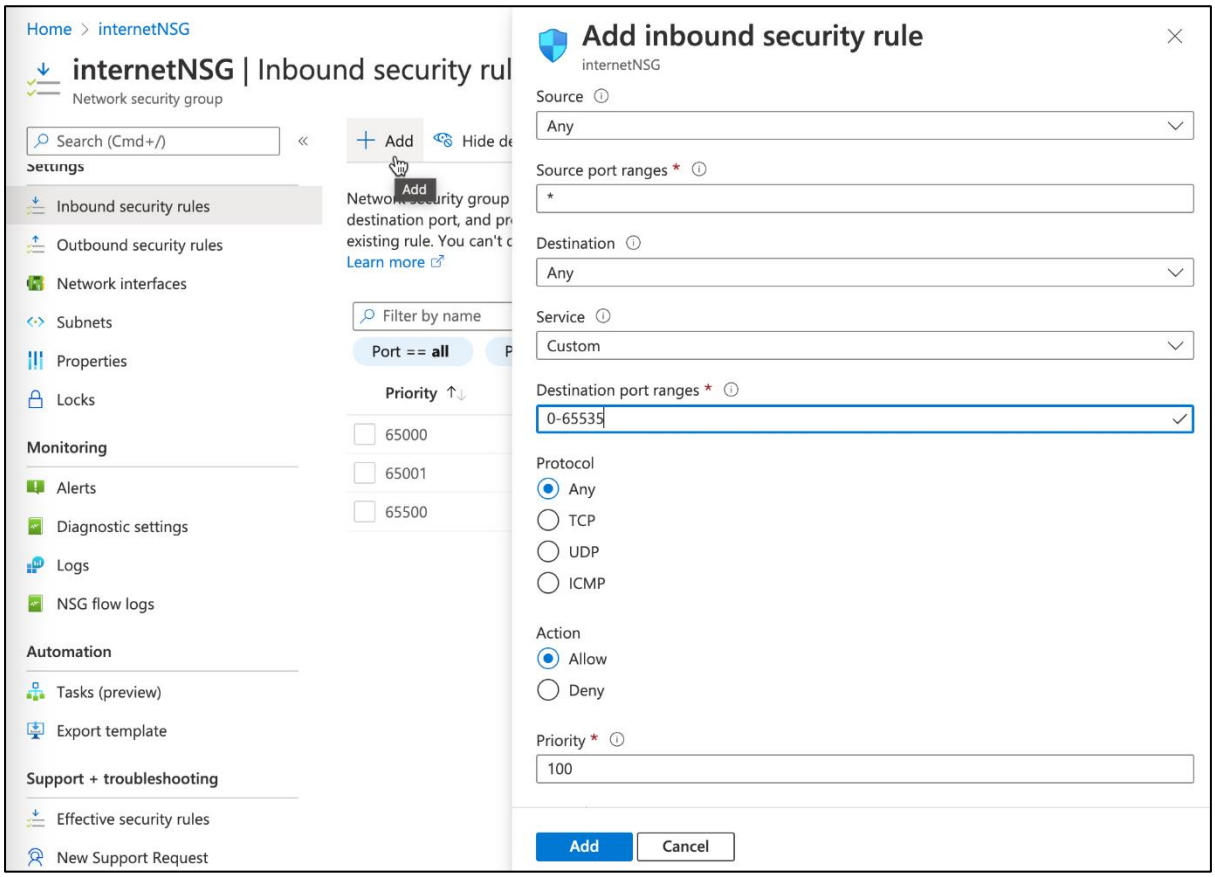

Your deployment is complete
Deployment name: paloaltonetworks.vmseries-ngfw-20220418232...
Subscription: Azure subscription 1
Resource group: PANgurus
Start time: 4/19/2022, 12:18:47 AM
Correlation ID: dd7dbf3b-db77-42e5-a413-a8eedf2b42cf
Deployment details (Download)
Resource
Type
Status
Operation details
bootstrapfw
Microsoft.Compute/virtualMachines
OK
Operation details
bootstrapfw-pangurus-eth0
Microsoft.Network/networkInterfaces
Created
Operation details
bootstrapfw-pangurus-eth1
Microsoft.Network/networkInterfaces
Created
Operation details
bootstrapfw-pangurus-eth2
Microsoft.Network/networkInterfaces
Created
Operation details
fwVNET
Microsoft.Network/virtualNetworks
OK
Operation details
pangurus
Microsoft.Network/publicIPAddresses
OK
Operation details
DefaultNSG
Microsoft.Network/networkSecurityGroups
OK
Operation details
pid-0a6ce0a1-eb47-41b5-af43-e99c32a2e9a7-
Microsoft.Resources/deployments
OK
Operation details
Next steps
Go to resource group

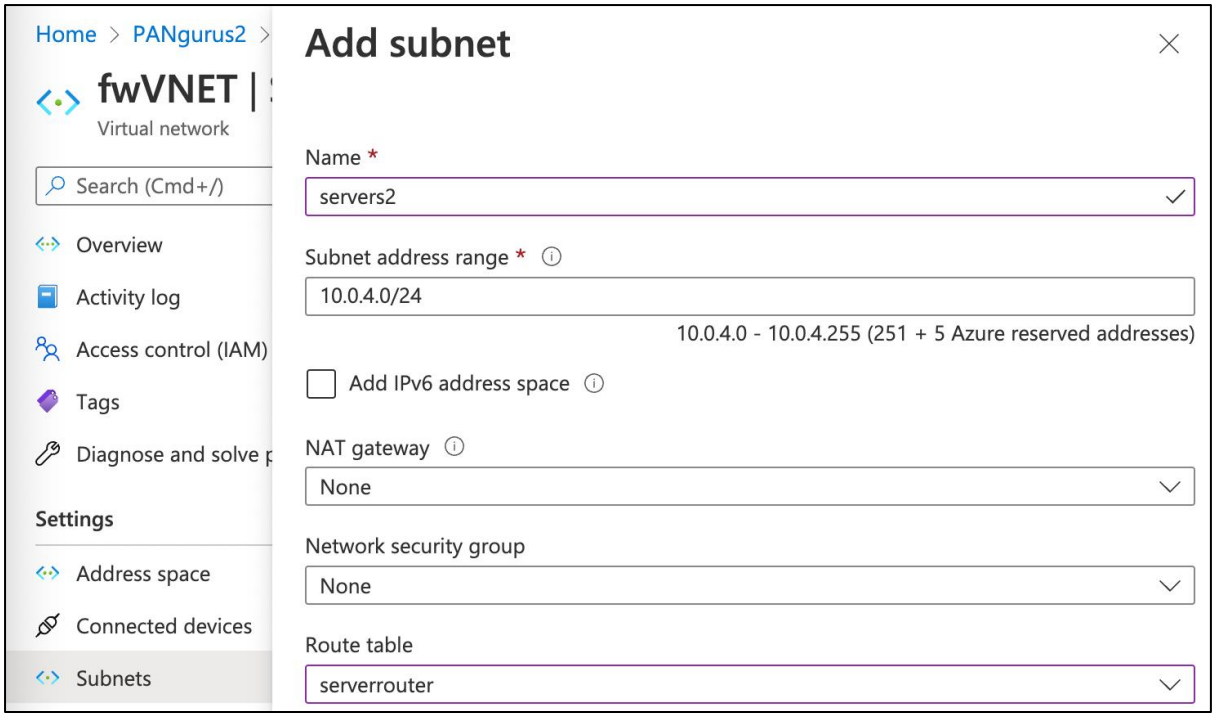

Not Secure | https://pangurus.westeurope.cloudapp.azure.com/?#dashboard::vsys1
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Layout 3 Columns
Widgets
Last updated 00:30:50
General Information
Device Name bootstrapfw
MGT IP Address 10.1.0.4 (DHCP)
MGT Netmask 255.255.255.0
MGT Default Gateway 10.1.0.1
MGT IPv6 Address unknown
MGT IPv6 Link Local Address fe80::6245:bdff:fe90:10ad/64
MGT IPv6 Default Gateway
MGT MAC Address 60:45:bd:90:10:ad
Model PA-VM
Serial # unknown
CPU ID AZR:
UUID 585D
VM Cores 4
VM Memory 14351728
VM License none
VM Capacity Tier unknown
VM Mode Microsoft Azure
Logged In Admins
Admin From Client Session Start Idle For
reaper Web 04/18 15:30:40 00:00:00s
Data Logs
No data available.
System Logs
Description Time
User reaper logged in via Web from using https 04/18 15:30:39
authenticated for user 'reaper'. From: 04/18 15:30:39
icd service is started time: 2022-04-18 15:27:35 04/18 15:27:34
iot-eal service is started time: 2022-04-18 15:24:38 @dataplane 04/18 15:27:29
failed to retrieve source address with error -2000003 time: 2022-04-18 15:24:38 @dataplane 04/18 15:27:29
Autocommit job succeeded 04/18

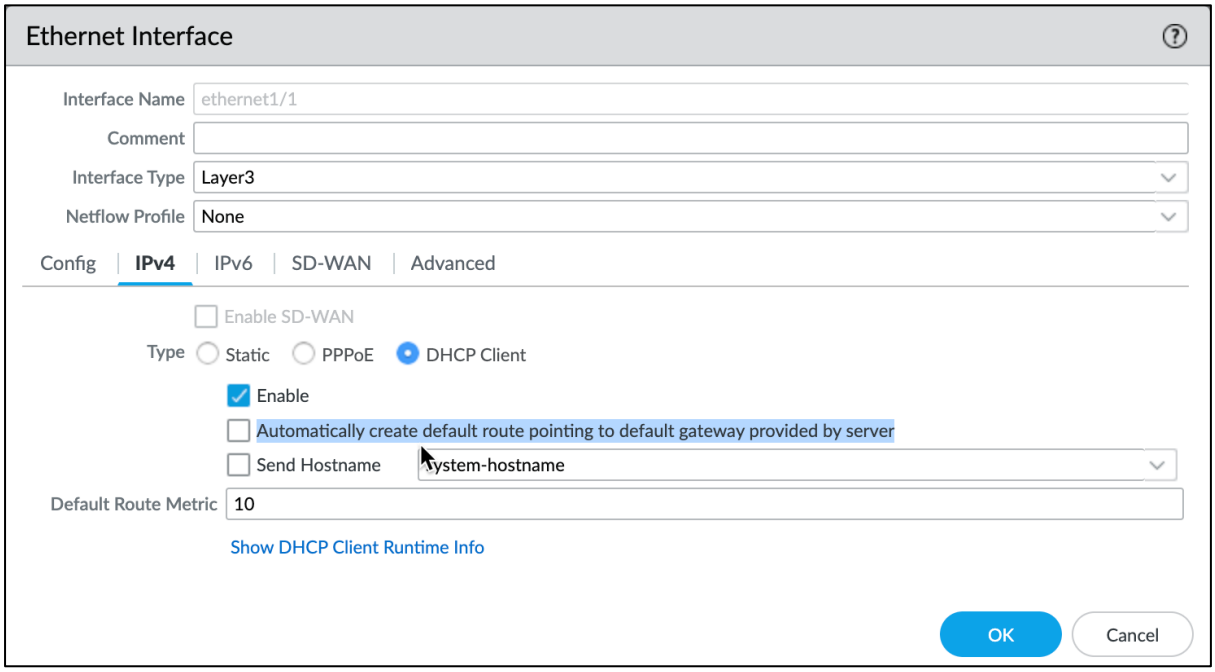

DefaultNSG | Subnets
Network security group
Search (Cmd+/)
Associate
Search subnets
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Name
Address range
Virtual network
Mgmt
10.0.0.0/24
fwVNET
Home > PANgurus2 >
pangurus2
Public IP address
Search (Cmd+/)
Associate
Dissociate
Move
Delete
Refresh
Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Monitoring
Insights
Alerts
Metrics
Upgrade to Standard SKU - Microsoft recommends Standard SKU public IP address for production workloads
Essentials
JSON View
Resource group (move) : PANgurus2
Location : North Europe
Subscription (move) : Azure subscription 1
Subscription ID : a4a47e81
SKU : Basic
Tier : Regional
IP address : 40.112.
DNS name : pangurus2.northeurope.cloudapp...
Associated to : bootstrapfw-pangurus2-eth0
Tags (edit) : Click here to add tags

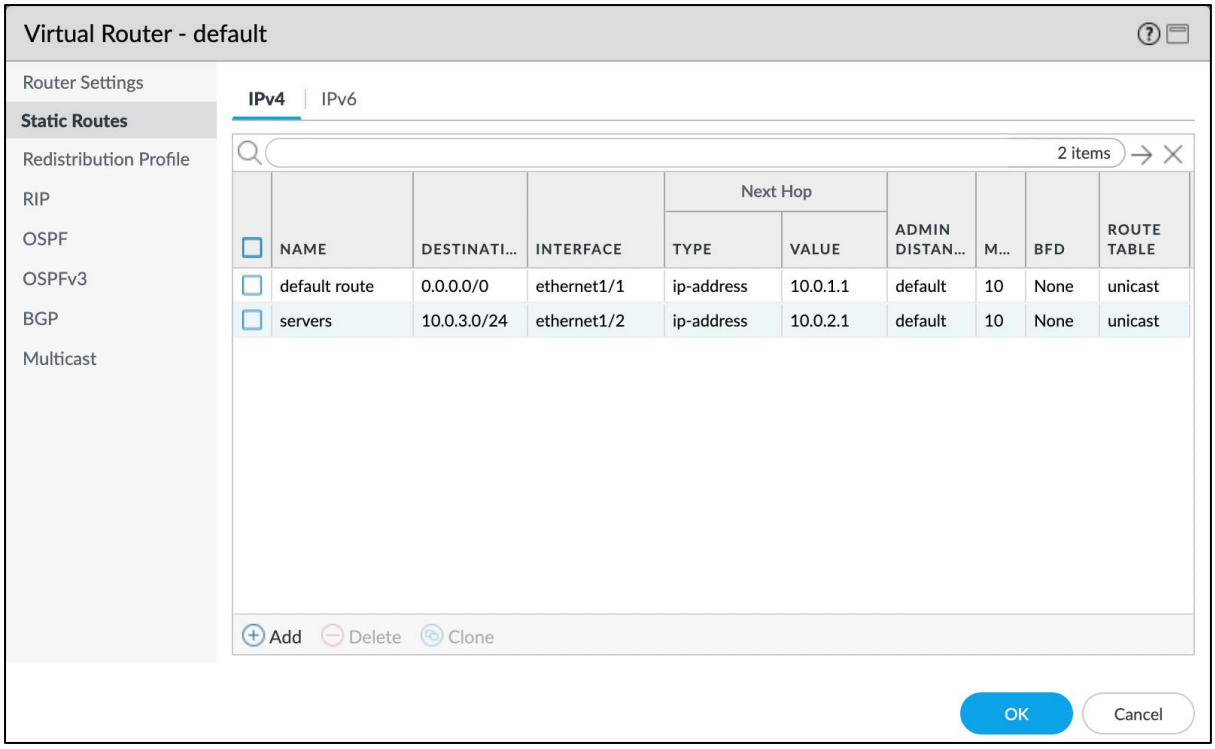

Home >
untrust
Public IP address
Search (Cmd+/)
Associate
Dissociate
Move
Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Associate
Resource group (move)
PANgurus2
Location
North Europe (Zone 3, 1, 2)
Subscription (move)
Azure subscription 1
Subscription ID
a4a47e81-0f9a-43b5-b626-a79020b52d30
Associate public IP address
untrust
Choose the resource to which you want to associate this public IP address.
Resource type
Network interface
Network interface *
bootstrapfw-pangurus2-eth1
resource group: PANgurus2

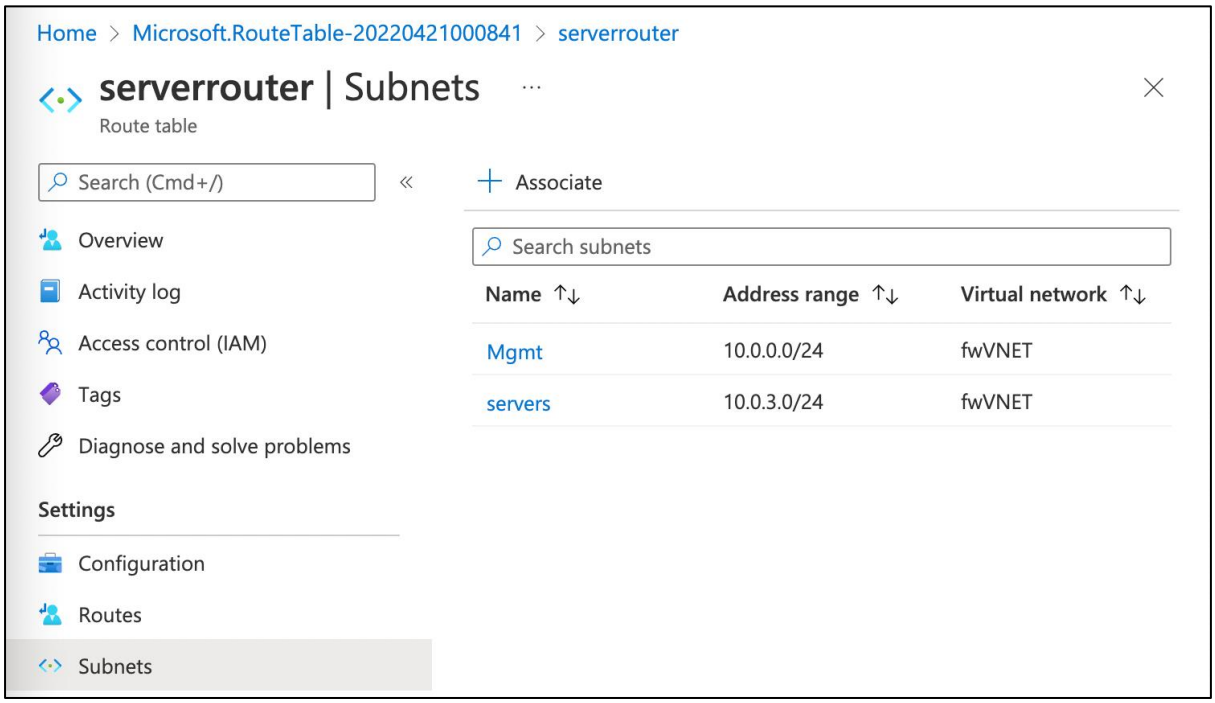

Home > internetNSG
internetNSG | Subnets
Network security group
Search (Cmd+/)
Associate
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Search subnets
Name
Address range
Virtual network
Untrust
10.0.1.0/24
fwVNET

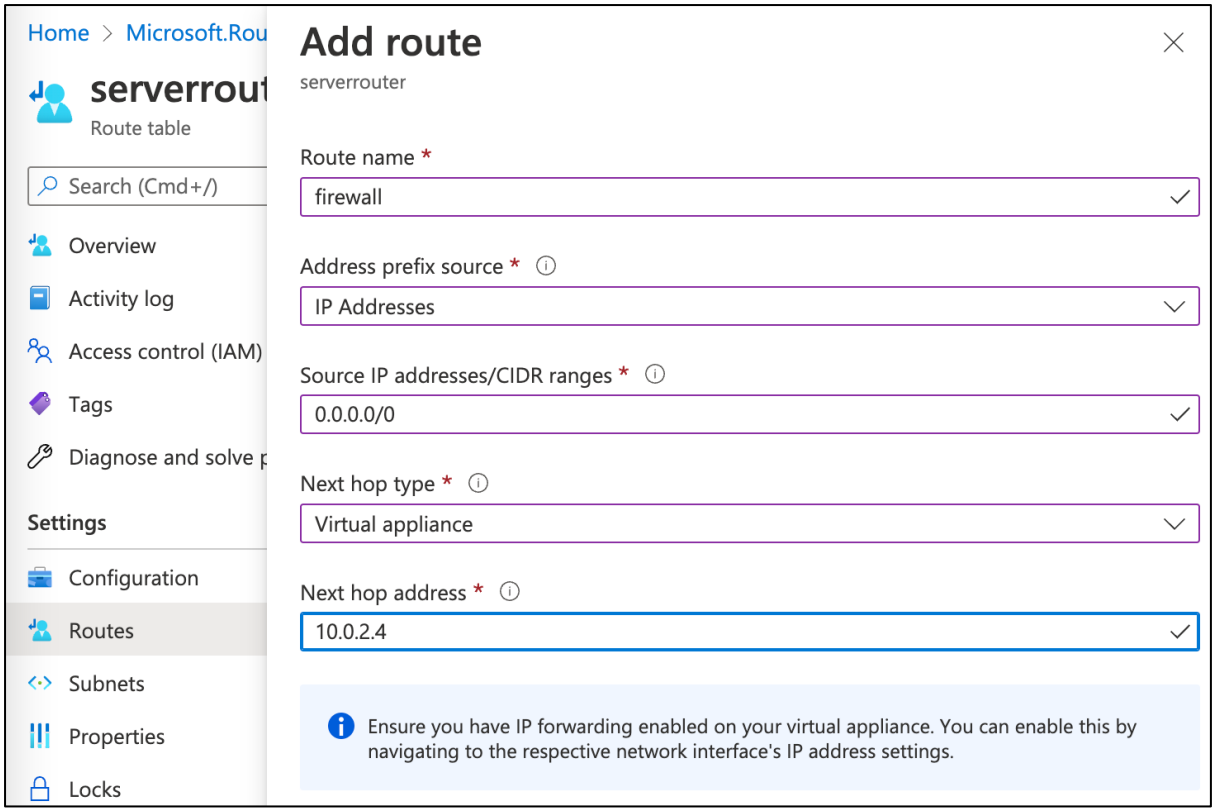

Home > internetNSG
internetNSG | Inbound security rul
Network security group
Search (Cmd+/)
Add
Hide de
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Alerts
Diagnostic settings
Logs
NSG flow logs
Automation
Tasks (preview)
Export template
Support + troubleshooting
Effective security rules
New Support Request
Learn more
Filter by name
Port == all
Priority
65000
65001
65500
Add inbound security rule
internetNSG
Source
Any
Source port ranges *
*
Destination
Any
Service
Custom
Destination port ranges *
0-65535
Protocol
Any
TCP
UDP
ICMP
Action
Allow
Deny
Priority *
100
Add
Cancel

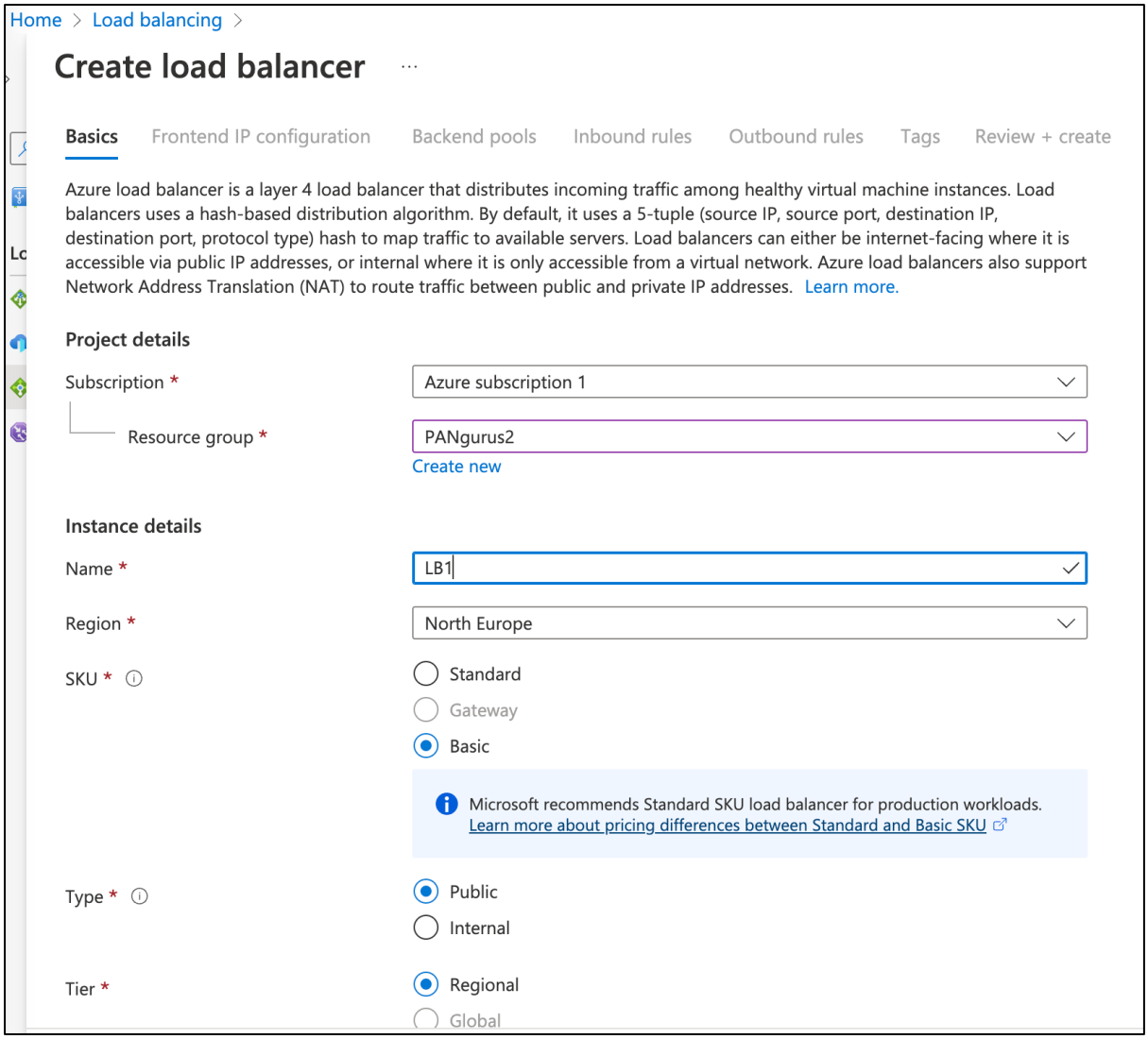

Home > PANgurus2 >
fwVNET |
Virtual network
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve p
Settings
Address space
Connected devices
Subnets
Add subnet
Name *
servers2
Subnet address range *
10.0.4.0/24
10.0.4.0 - 10.0.4.255 (251 + 5 Azure reserved addresses)
Add IPv6 address space
NAT gateway
None
Network security group
None
Route table
serverrouter

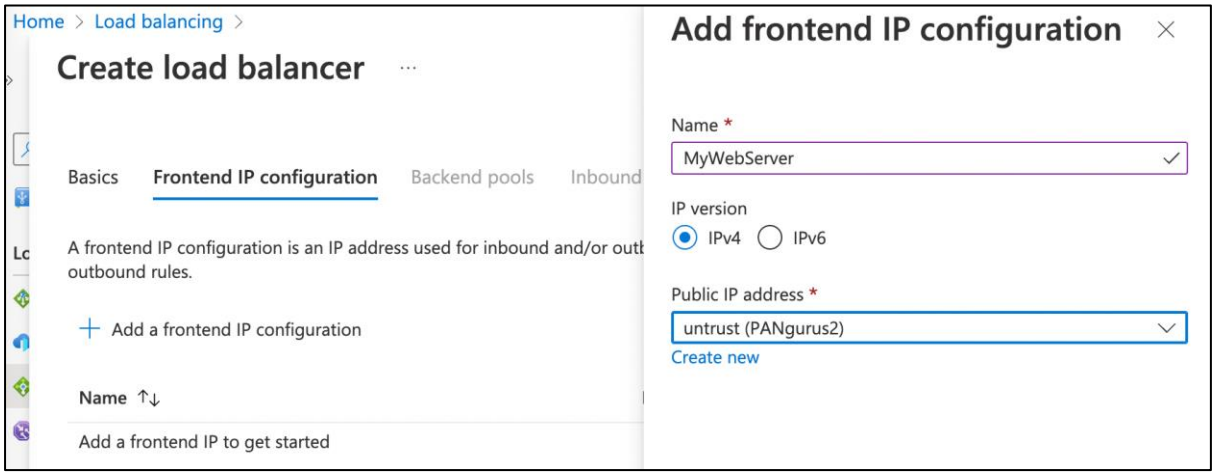

Ethernet Interface
Interface Name
ethernet1/1
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
SD-WAN
Advanced
Enable SD-WAN
Type
Static
PPPoE
DHCP Client
Enable
Automatically create default route pointing to default gateway provided by server
Send Hostname
system-hostname
Default Route Metric
10
Show DHCP Client Runtime Info
OK
Cancel

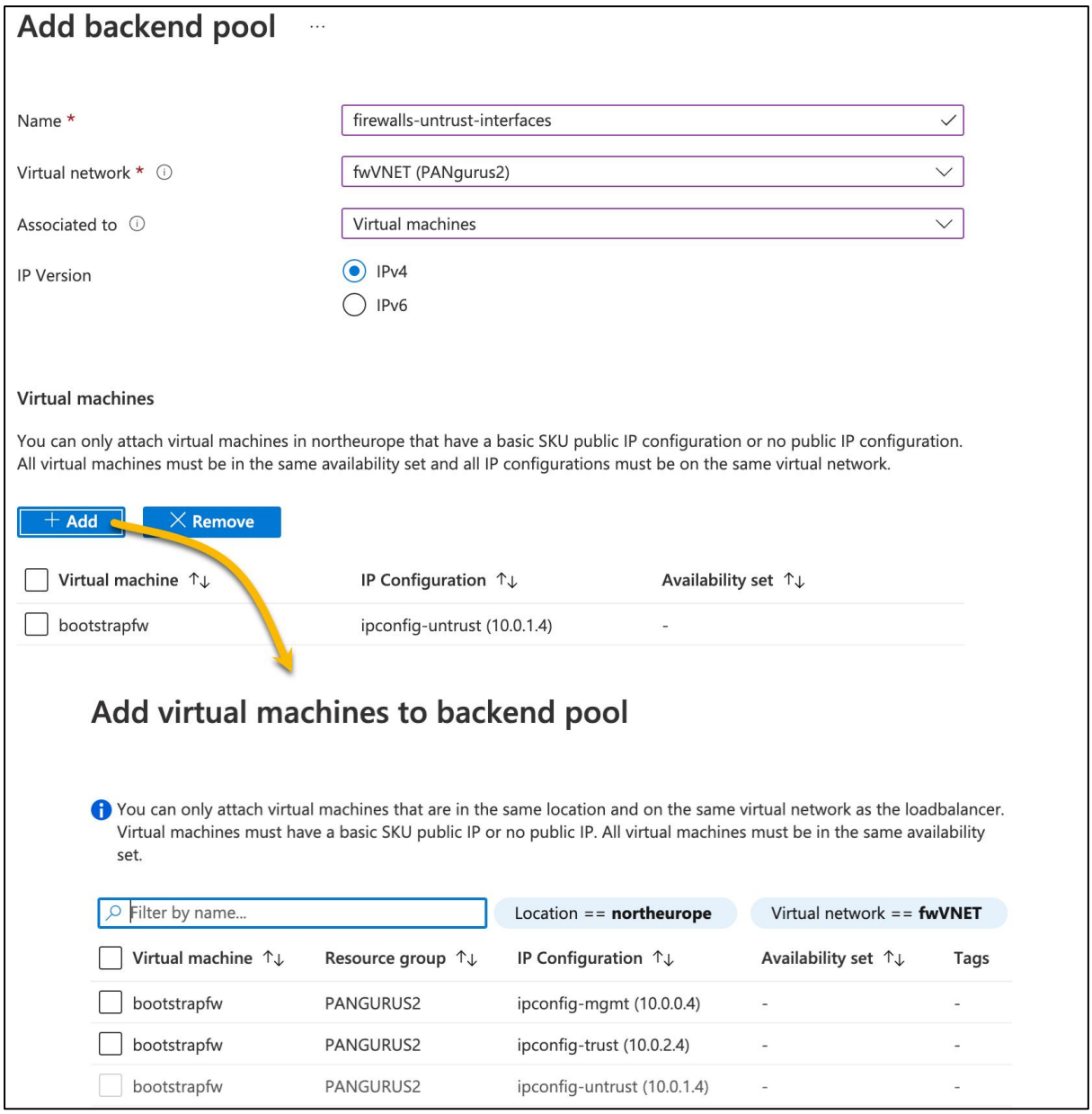

Virtual Router - default
Router Settings
Static Routes
Redistribution Profile
RIP
OSPF
OSPFv3
BGP
Multicast
IPv4
IPv6
2 items
NAME
DESTINATI...
INTERFACE
Next Hop
TYPE
VALUE
ADMIN DISTAN...
M...
BFD
ROUTE TABLE
default route
0.0.0.0/0
ethernet1/1
ip-address
10.0.1.1
default
10
None
unicast
servers
10.0.3.0/24
ethernet1/2
ip-address
10.0.2.1
default
10
None
unicast
Add
Delete
Clone
OK
Cancel

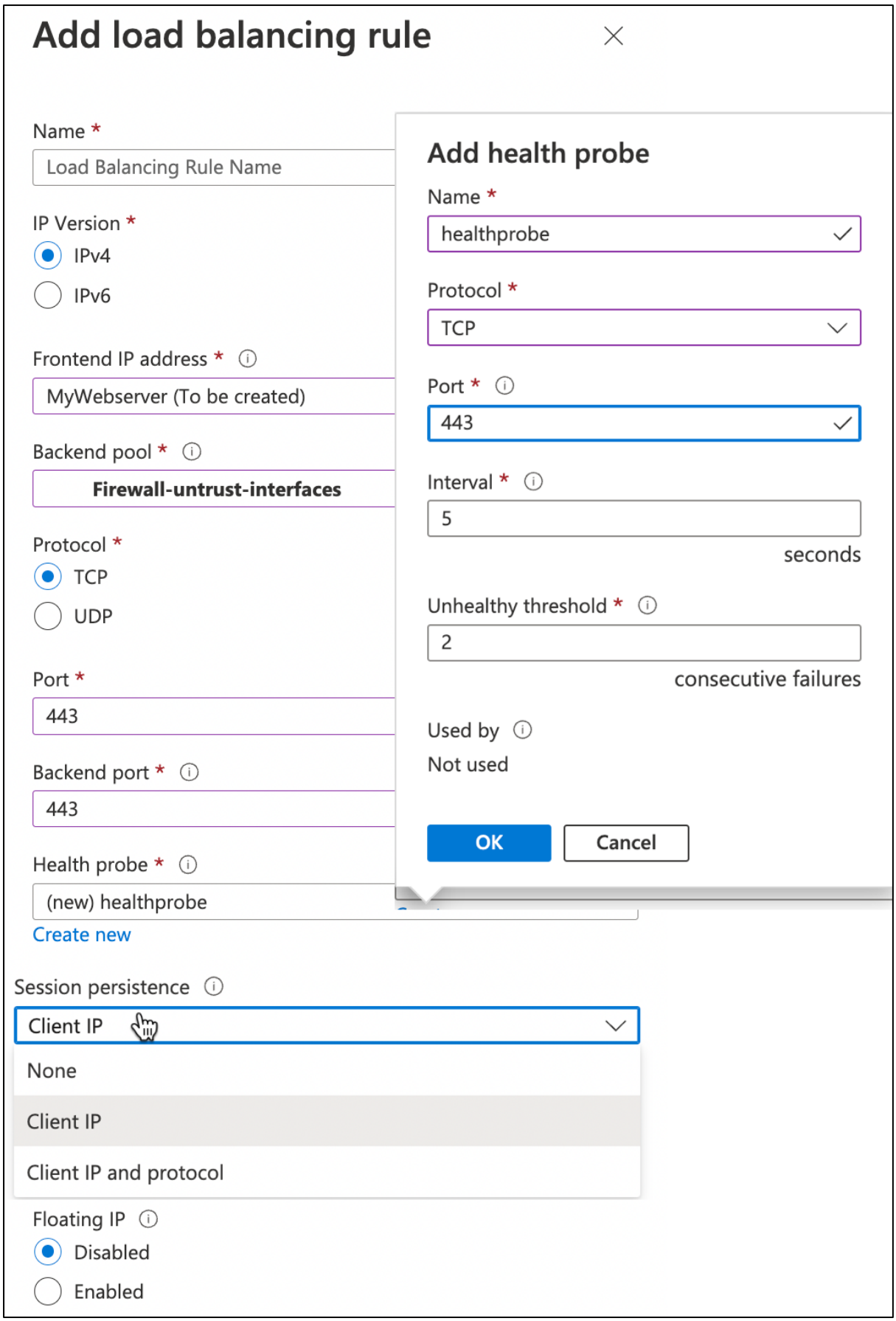

Home
Microsoft.RouteTable-20220421000841
serverrouter
serverrouter | Subnets
Route table
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Subnets
Associate
Search subnets
Name
Address range
Virtual network
Mgmt
10.0.0.0/24
fwVNET
servers
10.0.3.0/24
fwVNET


Home > Microsoft.Rou
serverrout
Route table
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve p
Settings
Configuration
Routes
Subnets
Properties
Locks
Add route
serverrouter
Route name *
firewall
Address prefix source *
IP Addresses
Source IP addresses/CIDR ranges *
0.0.0.0/0
Next hop type *
Virtual appliance
Next hop address *
10.0.2.4
Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.


Home > Load balancing >
Create load balancer
Basics
Frontend IP configuration
Backend pools
Inbound rules
Outbound rules
Tags
Review + create
Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. Learn more.
Project details
Subscription *
Azure subscription 1
Resource group *
PANgurus2
Create new
Instance details
Name *
LB1
Region *
North Europe
SKU *
Standard
Gateway
Basic
Microsoft recommends Standard SKU load balancer for production workloads.
Learn more about pricing differences between Standard and Basic SKU
Type *
Public
Internal
Tier *
Regional
Global


Home > Load balancing >
Create load balancer
Basics
Frontend IP configuration
Backend pools
Inbound
A frontend IP configuration is an IP address used for inbound and/or outb
outbound rules.
Add a frontend IP configuration
Name
Add a frontend IP to get started
Add frontend IP configuration
Name *
MyWebServer
IP version
IPv4
IPv6
Public IP address *
untrust (PANgurus2)
Create new


Add backend pool
Name *
firewalls-untrust-interfaces
Virtual network *
fwVNET (PANgurus2)
Associated to
Virtual machines
IP Version
IPv4
IPv6
Virtual machines
You can only attach virtual machines in northeurope that have a basic SKU public IP configuration or no public IP configuration. All virtual machines must be in the same availability set and all IP configurations must be on the same virtual network.
Add
Remove
Virtual machine
IP Configuration
Availability set
bootstrapfw
ipconfig-untrust (10.0.1.4)
-
Add virtual machines to backend pool
You can only attach virtual machines that are in the same location and on the same virtual network as the loadbalancer. Virtual machines must have a basic SKU public IP or no public IP. All virtual machines must be in the same availability set.
Filter by name...
Location == northeurope
Virtual network == fwVNET
Virtual machine
Resource group
IP Configuration
Availability set
Tags
bootstrapfw
PANGURUS2
ipconfig-mgmt (10.0.0.4)
-
-
bootstrapfw
PANGURUS2
ipconfig-trust (10.0.2.4)
-
-
bootstrapfw
PANGURUS2
ipconfig-untrust (10.0.1.4)
-
-


Add load balancing rule
Name *
Load Balancing Rule Name
IP Version *
IPv4
IPv6
Frontend IP address *
MyWebserver (To be created)
Backend pool *
Firewall-untrust-interfaces
Protocol *
TCP
UDP
Port *
443
Backend port *
443
Health probe *
(new) healthprobe
Create new
Session persistence
Client IP
None
Client IP
Client IP and protocol
Floating IP
Disabled
Enabled
Add health probe
Name *
healthprobe
Protocol *
TCP
Port *
443
Interval *
5
seconds
Unhealthy threshold *
2
consecutive failures
Used by
Not used
OK
Cancel

Add inbound NAT rule

LBin

An inbound NAT rule forwards incoming traffic sent to a selected IP address and port combination to a specific virtual machine.

Name *

Inbound NAT Rule name

Target virtual machine

bootstrapfw
ResourceGroup: PANGURUS2, AvailabilitySet: -

Network IP configuration

ipconfig-untrust (10.0.1.4)

Frontend IP address *

MyWebserver (To be created)

Frontend Port *

2222

Service Tag *

SSH

Backend port *

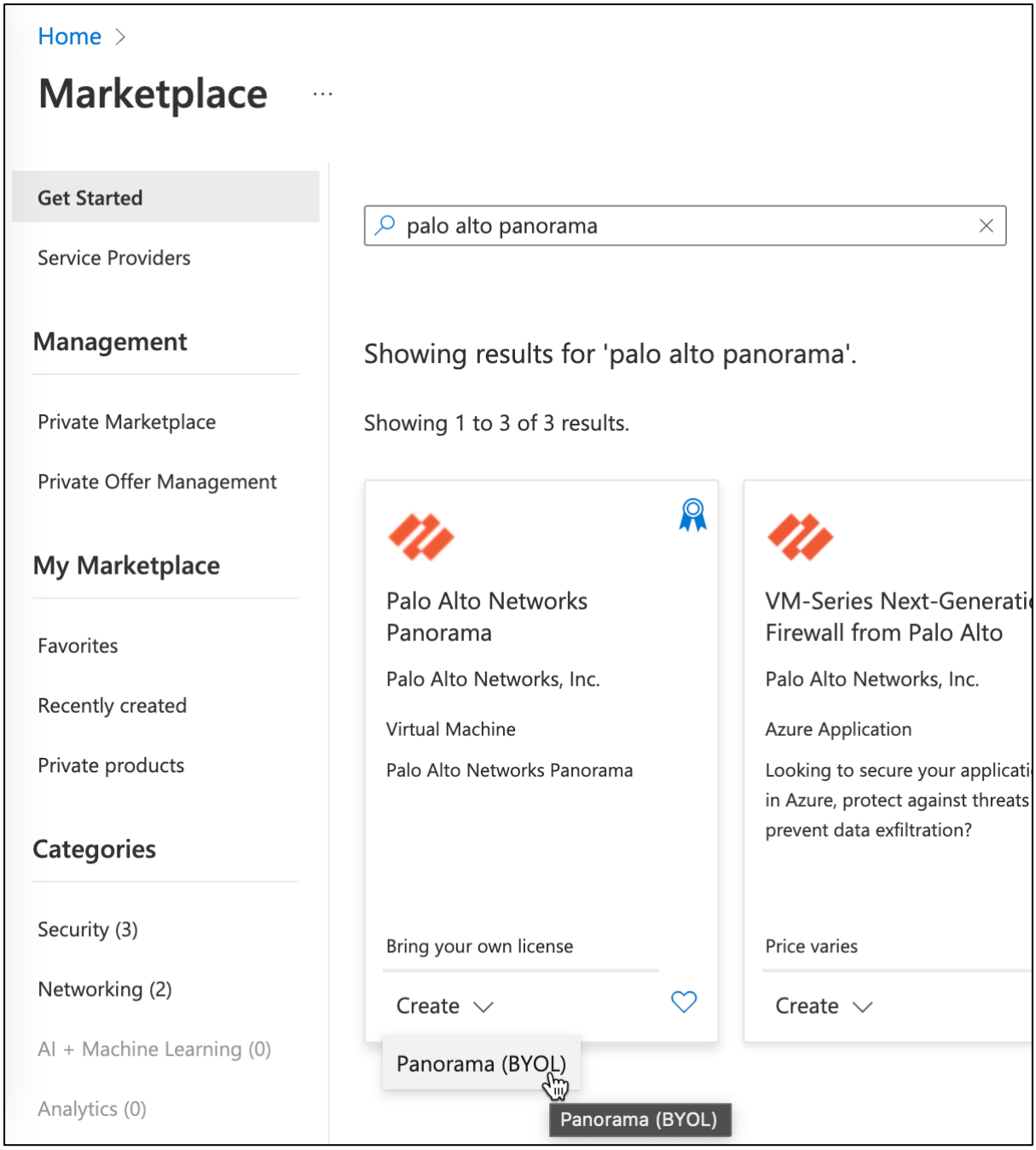
22

Protocol

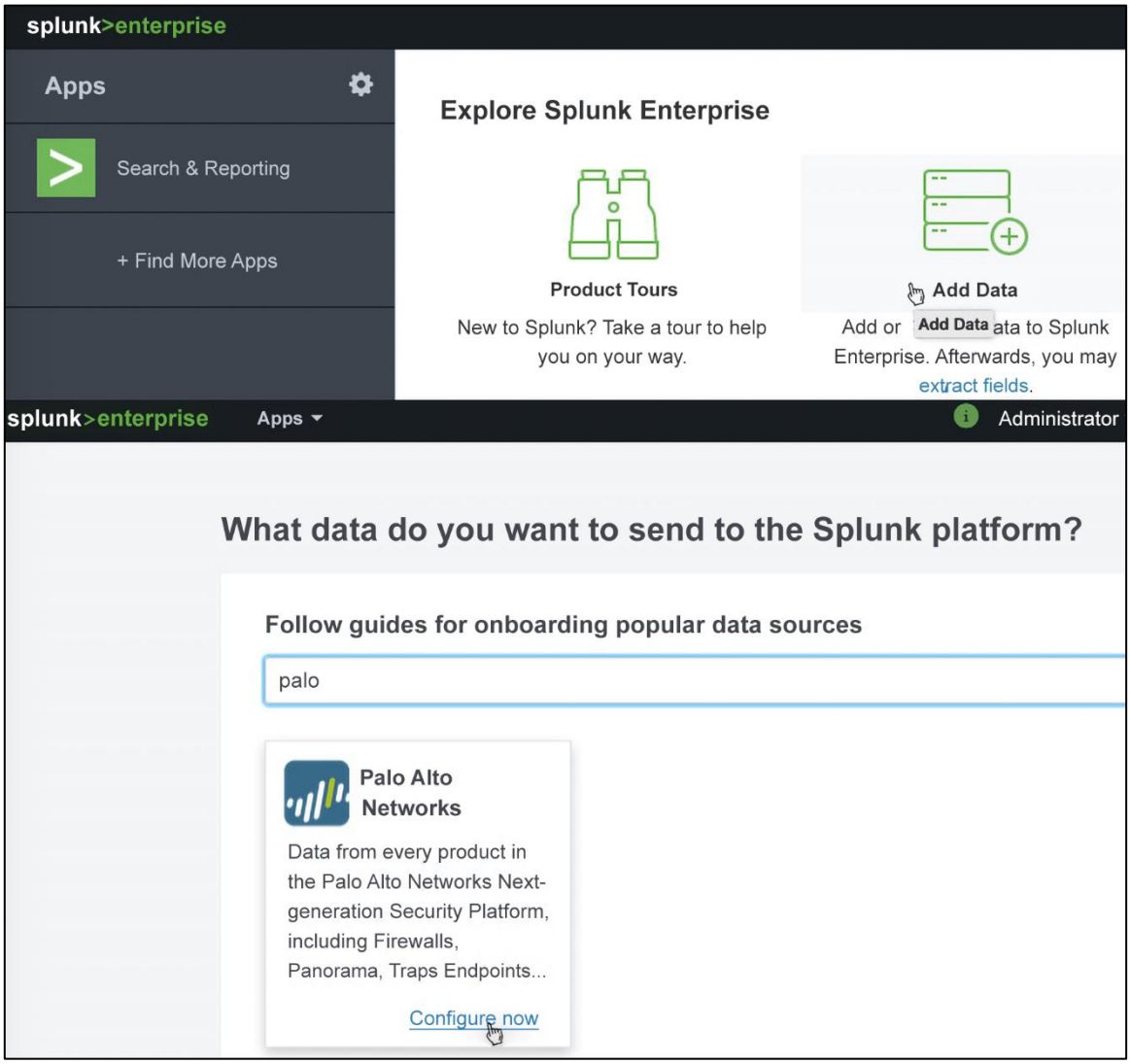
- (•) TCP
- ( ) UDP

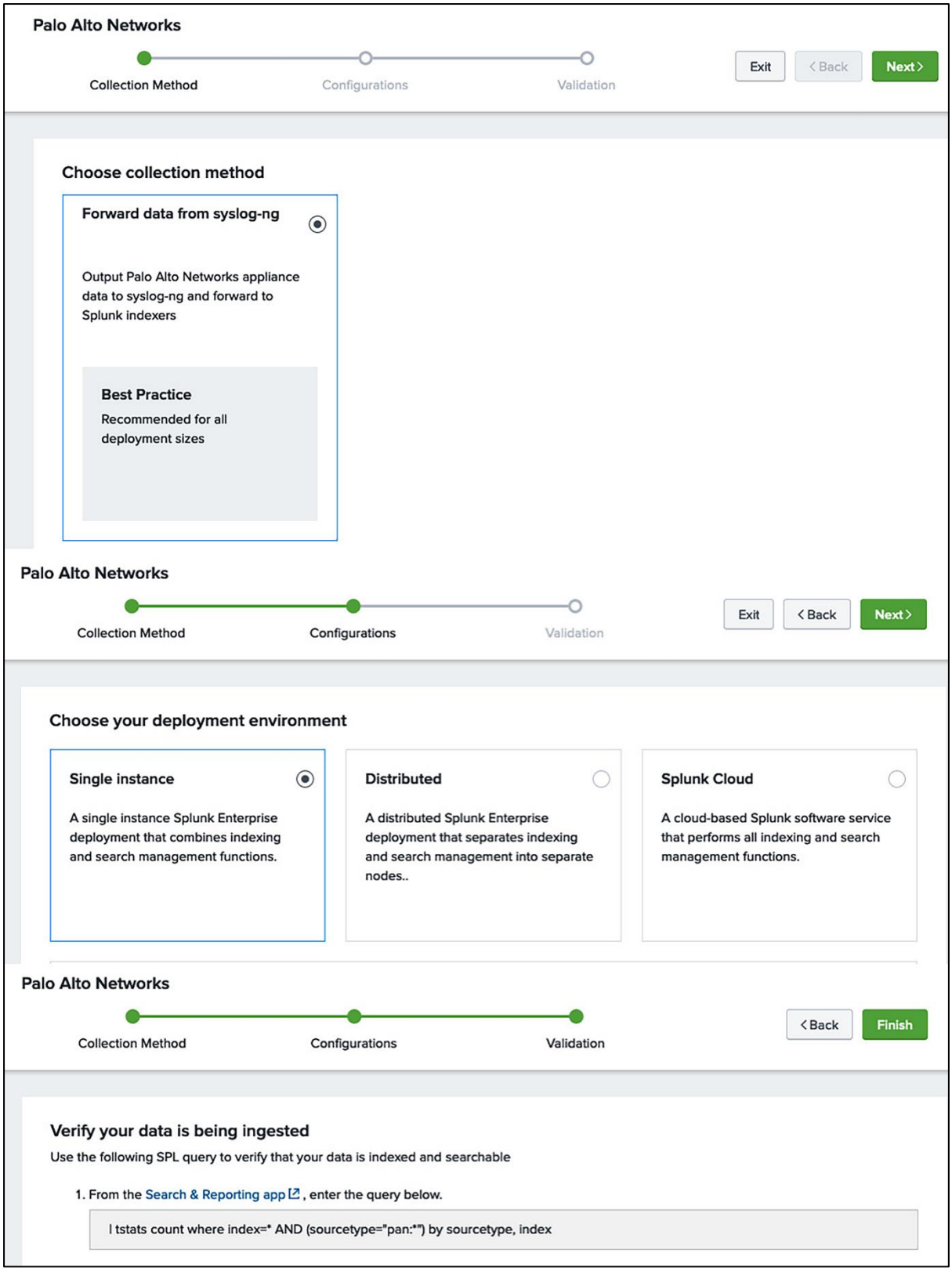
Idle timeout (minutes)

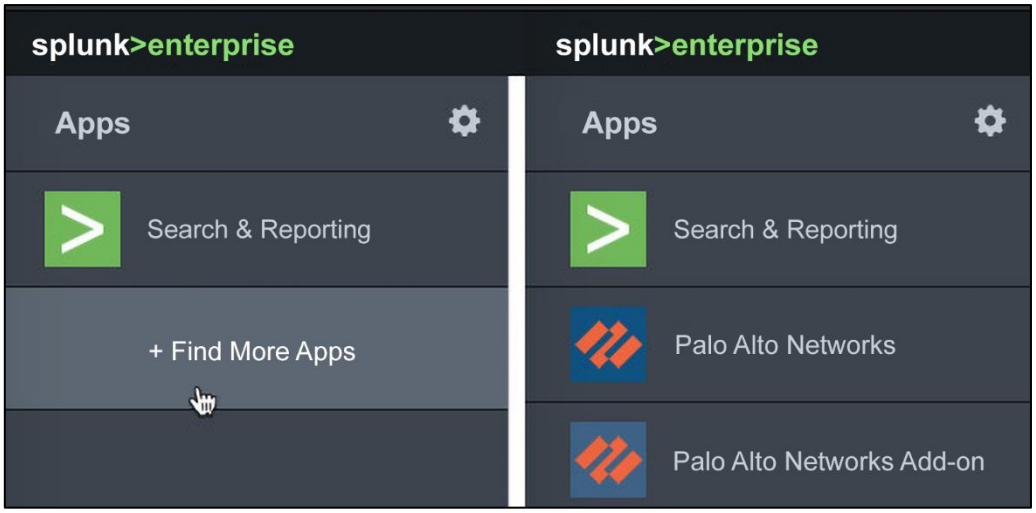
4

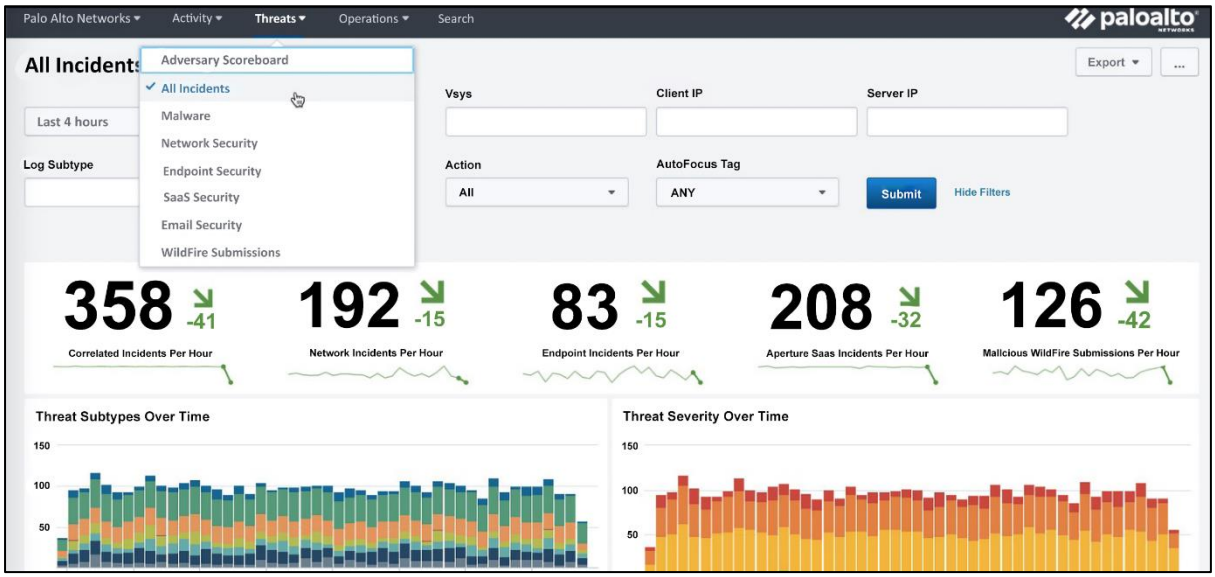

Home
Marketplace
Get Started
Service Providers
Management
Private Marketplace
Private Offer Management
My Marketplace
Favorites
Recently created
Private products
Categories
Security (3)
Networking (2)
AI + Machine Learning (0)
Analytics (0)
palo alto panorama
Showing results for 'palo alto panorama'.
Showing 1 to 3 of 3 results.
Palo Alto Networks Panorama
Palo Alto Networks, Inc.
Virtual Machine
Palo Alto Networks Panorama
Bring your own license
Create
VM-Series Next-Generati
Firewall from Palo Alto
Palo Alto Networks, Inc.
Azure Application
Looking to secure your applicati
in Azure, protect against threats
prevent data exfiltration?
Price varies
Create
Panorama (BYOL)
Panorama (BYOL)

Chapter 15: Supporting Tools




Palo Alto Networks
Collection Method
Configurations
Validation
Exit
Back
Next
Choose collection method
Forward data from syslog-ng
Output Palo Alto Networks appliance data to syslog-ng and forward to Splunk indexers
Best Practice
Recommended for all deployment sizes
Palo Alto Networks
Collection Method
Configurations
Validation
Exit
Back
Next
Choose your deployment environment
Single instance
A single instance Splunk Enterprise deployment that combines indexing and search management functions.
Distributed
A distributed Splunk Enterprise deployment that separates indexing and search management into separate nodes..
Splunk Cloud
A cloud-based Splunk software service that performs all indexing and search management functions.
Palo Alto Networks
Collection Method
Configurations
Validation
Back
Finish
Verify your data is being ingested
Use the following SPL query to verify that your data is indexed and searchable
1. From the Search & Reporting app , enter the query below.
| tstats count where index=* AND (sourcetype="pan:*") by sourcetype, index





Log Forwarding Profile

Name: default

Description:

4 items

NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
Threat-to-Panorama	threat	All Logs	• Panorama SysLog • splunk	
Traffic-to-Panorama	traffic	All Logs	• Panorama SysLog • splunk	
URL-to-Panorama	url	All Logs	• Panorama	

Add Delete Clone

OK Cancel

System

	NAME	DESCRI...	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG	HTTP
☐	Forward System		All Logs	☑			splunk	

Add Delete Clone PDF/CSV

Configuration

	NAME	DE...	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG	HTTP
☐	Forward Configuration		All Logs	☑			splunk	

Add Delete Clone PDF/CSV

User-ID

	NAME	DESCR...	FILTER	PANORA...	SNMP TRAP	EMAIL	SYSLOG	HTTP	BUILT-IN ACTIONS
☐	Forward User-ID		All Logs	☑			splunk		

Add Delete Clone PDF/CSV

HIP Match

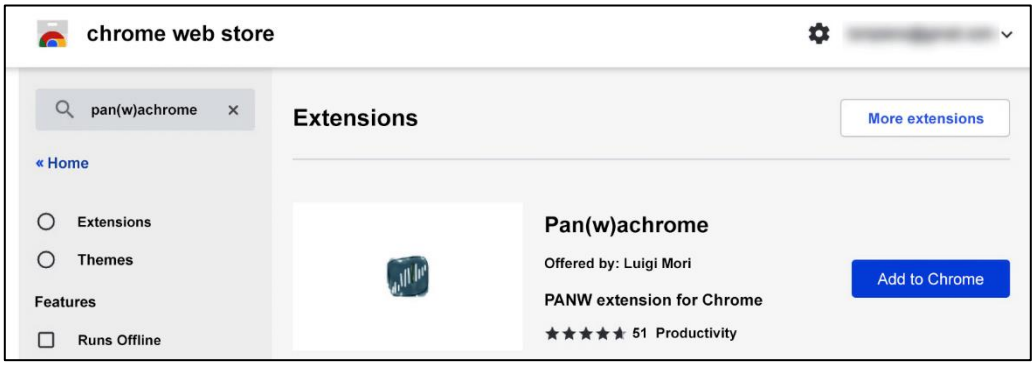
	NAME	DE...	FILTER	PANORA...	SNMP TRAP	EM...	SYSLOG	HT...	QU...	BUILT-IN ACTIONS
☐	Forward HIP-match		All Logs	☑			splunk		☐	

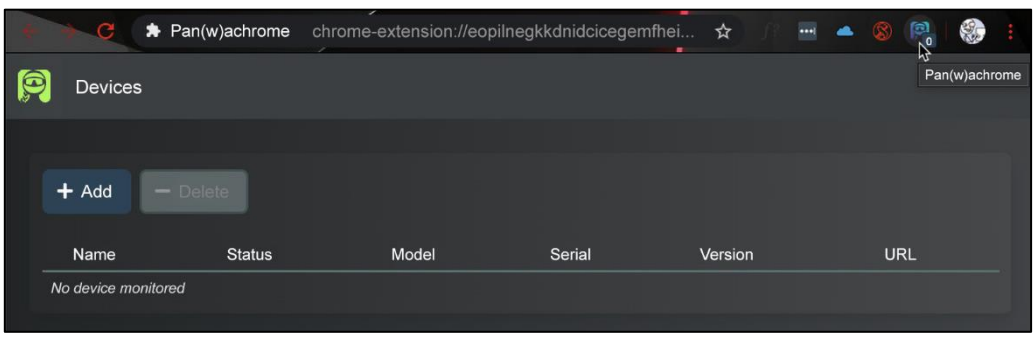
Add Delete Clone PDF/CSV

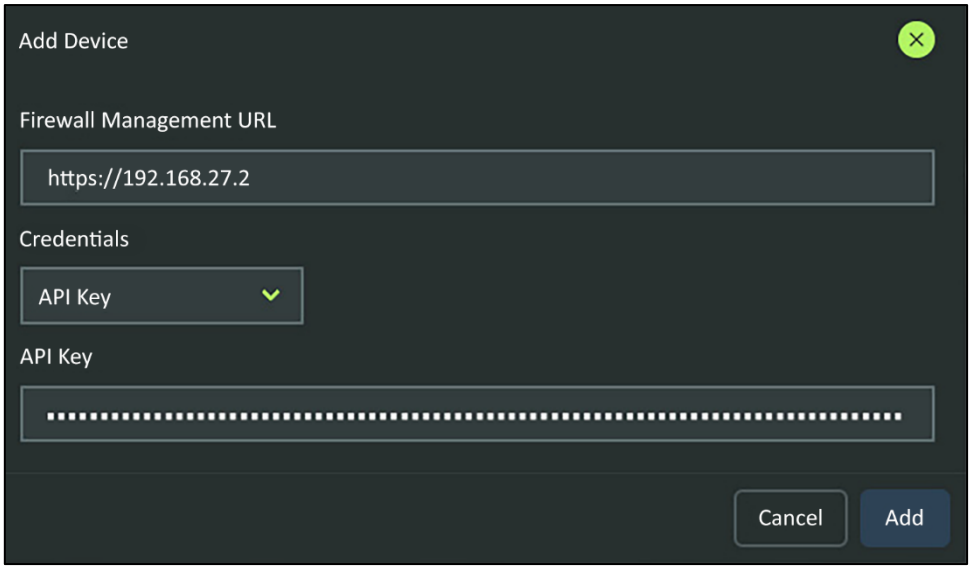
GlobalProtect

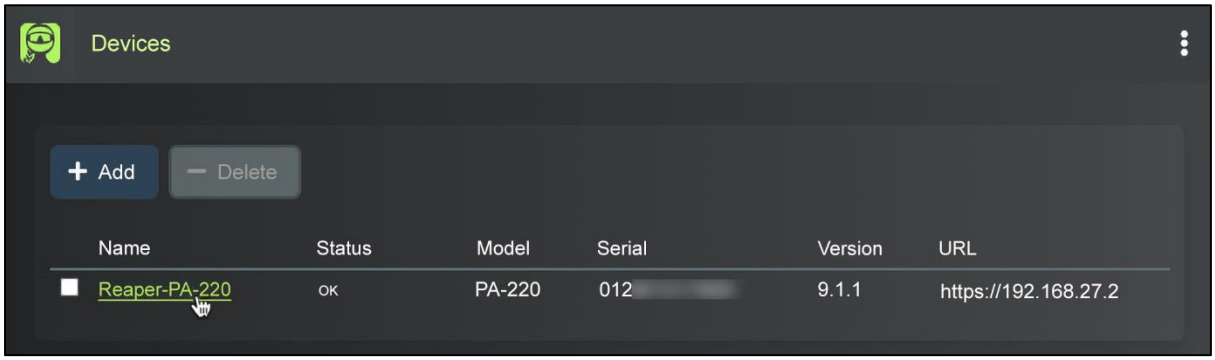
	NAME	DESCRIPTI...	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG	HTTP
☐	Forward GlobalProtect		All Logs	☑			splunk	

Add Delete Clone PDF/CSV

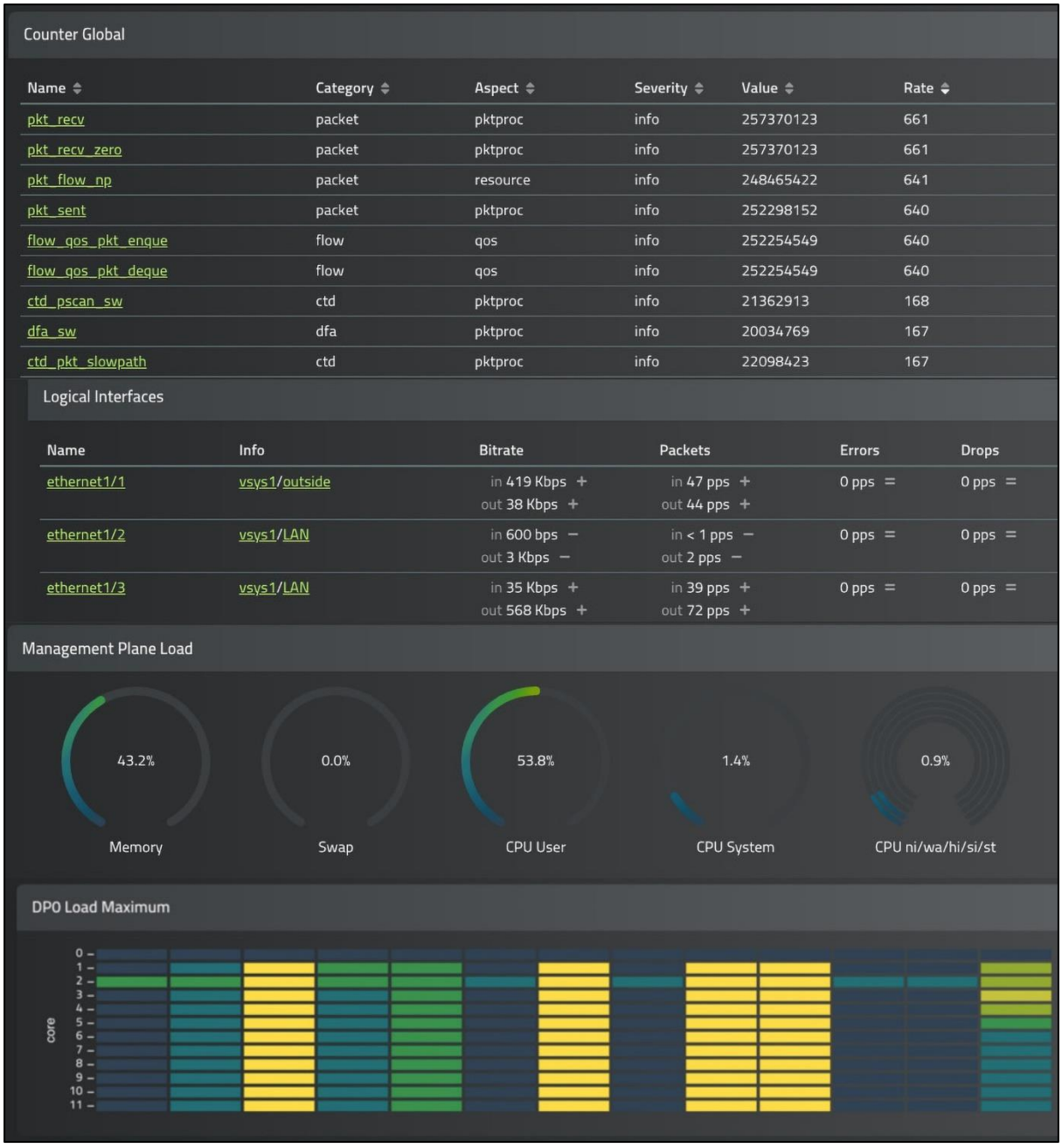


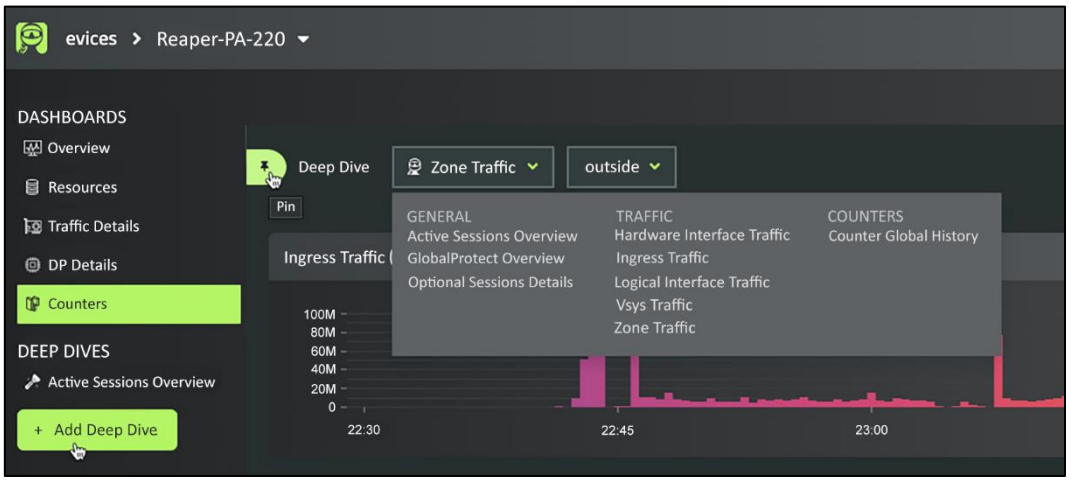


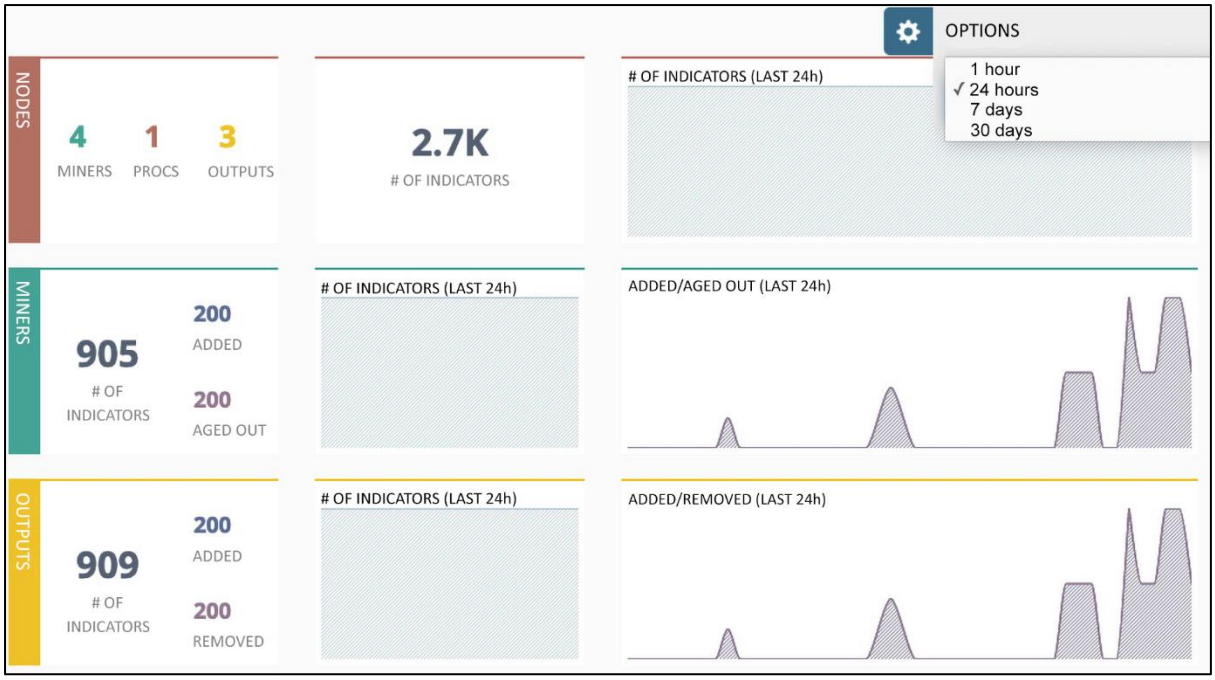

Add Device
Firewall Management URL
https://192.168.27.2
Credentials
API Key
API Key
Cancel
Add

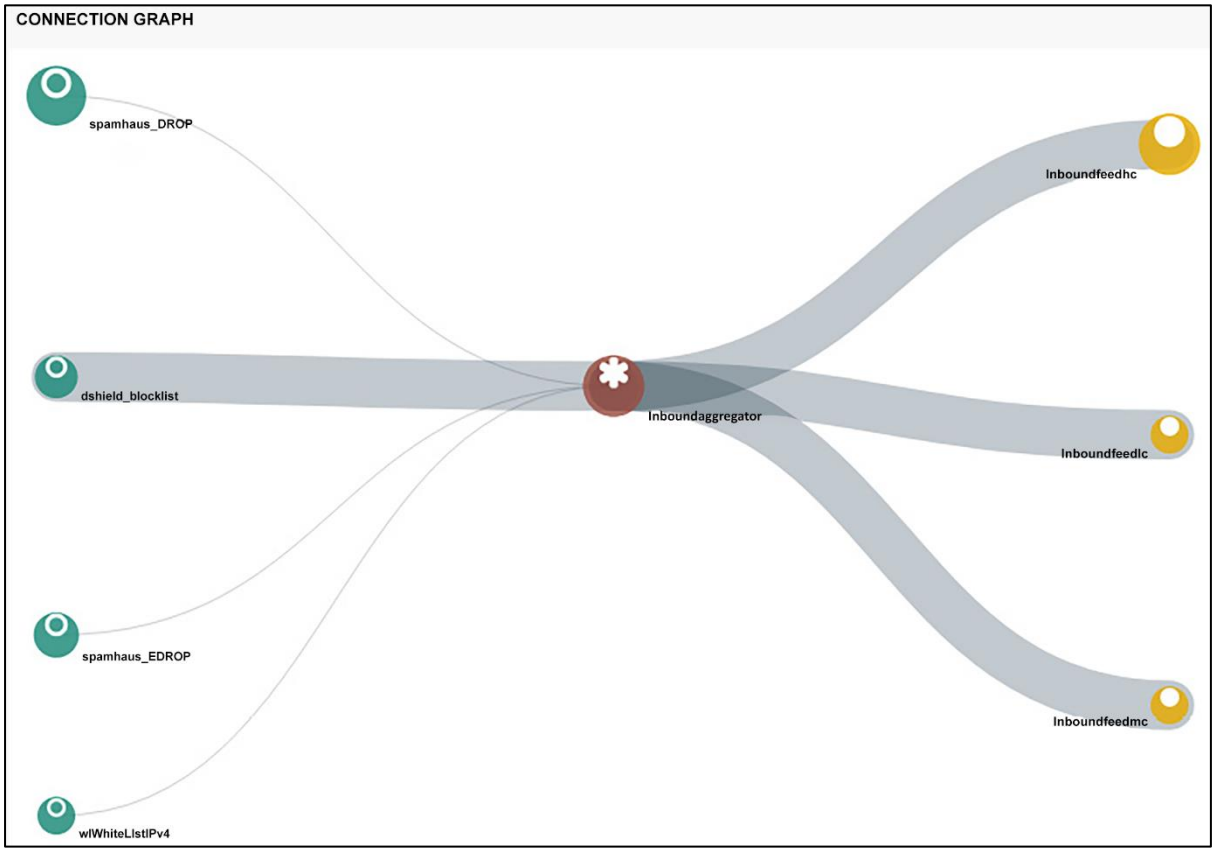

Devices
Add
Delete
Name
Status
Model
Serial
Version
URL
Reaper-PA-220
OK
PA-220
012
9.1.1
https://192.168.27.2

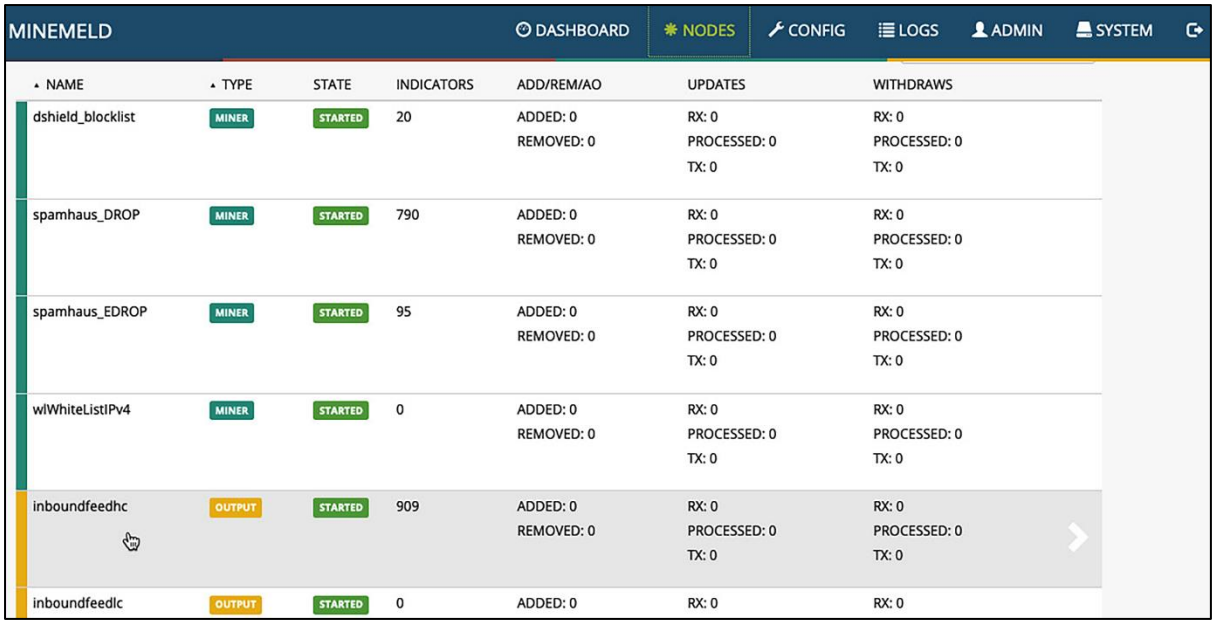

Devices
Reaper-PA-220
DASHBOARDS
Overview
Resources
Traffic Details
DP Details
Counters
DEEP DIVES
+ Add Deep Dive
Ingress Traffic (bps)
20M
15M
10M
5M
0
15:30
15:45
16:00
Egress Traffic (bps)
25M
20M
15M
10M
5M
0
15:30
15:45
16:00
Active Sessions
300
200
100
0
15:30
15:45
16:00
16:15
Connections Per Second (cps)
40
30
20
10
0
15:30
15:45
16:00

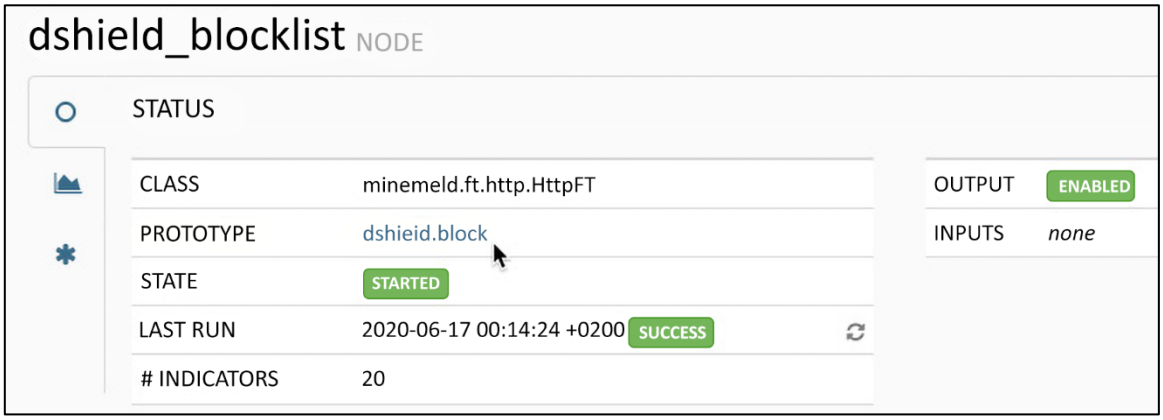

Counter Global
Name
Category
Aspect
Severity
Value
Rate
pkt_recv packet pktproc info 257370123 661
pkt_recv_zero packet pktproc info 257370123 661
pkt_flow_np packet resource info 248465422 641
pkt_sent packet pktproc info 252298152 640
flow_qos_pkt_enque flow qos info 252254549 640
flow_qos_pkt_deque flow qos info 252254549 640
ctd_pscan_sw ctd pktproc info 21362913 168
dfa_sw dfa pktproc info 20034769 167
ctd_pkt_slowpath ctd pktproc info 22098423 167
Logical Interfaces
Name
Info
Bitrate
Packets
Errors
Drops
ethernet1/1 vsys1/outside in 419 Kbps + out 38 Kbps + in 47 pps + out 44 pps + 0 pps = 0 pps =
ethernet1/2 vsys1/LAN in 600 bps − out 3 Kbps − in < 1 pps − out 2 pps − 0 pps = 0 pps =
ethernet1/3 vsys1/LAN in 35 Kbps + out 568 Kbps + in 39 pps + out 72 pps + 0 pps = 0 pps =
Management Plane Load
43.2%
Memory
0.0%
Swap
53.8%
CPU User
1.4%
CPU System
0.9%
CPU ni/wa/hi/si/st
DPO Load Maximum
core
0
1
2
3
4
5
6
7
8
9
10
11

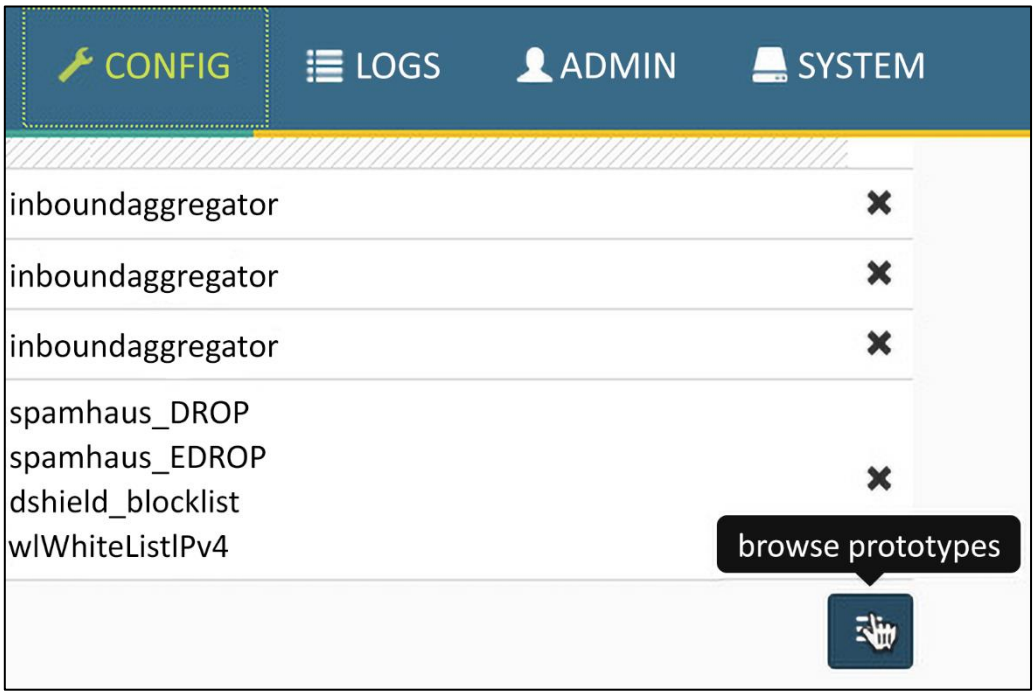

evices
Reaper-PA-220
DASHBOARDS
Overview
Resources
Traffic Details
DP Details
Counters
DEEP DIVES
Active Sessions Overview
+ Add Deep Dive
Deep Dive
Pin
Zone Traffic
outside
GENERAL
Active Sessions Overview
GlobalProtect Overview
Optional Sessions Details
TRAFFIC
Hardware Interface Traffic
Ingress Traffic
Logical Interface Traffic
Vsys Traffic
Zone Traffic
COUNTERS
Counter Global History
Ingress Traffic
100M
80M
60M
40M
20M
0
22:30
22:45
23:00

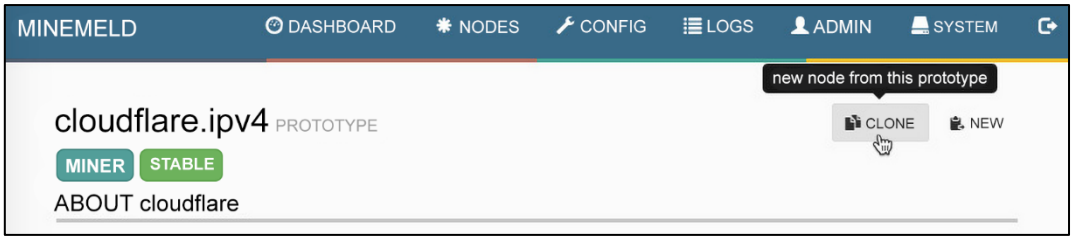

OPTIONS
1 hour
✓ 24 hours
7 days
30 days
NODES
4
MINERS
1
PROCS
3
OUTPUTS
2.7K
OF INDICATORS
OF INDICATORS (LAST 24h)
MINERS
905
OF INDICATORS
200
ADDED
200
AGED OUT
OF INDICATORS (LAST 24h)
ADDED/AGED OUT (LAST 24h)
OUTPUTS
909
OF INDICATORS
200
ADDED
200
REMOVED
OF INDICATORS (LAST 24h)
ADDED/REMOVED (LAST 24h)

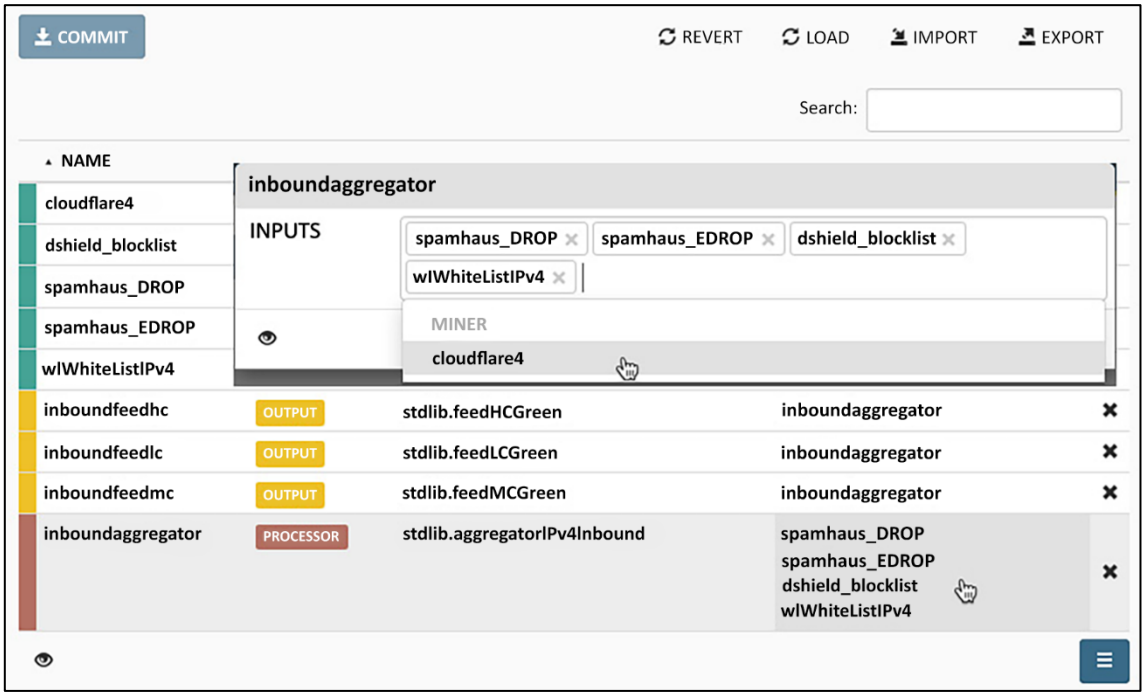

CONNECTION GRAPH
spamhaus_DROP
dshield_blocklist
spamhaus_EDROP
wlWhiteLIstIPv4
Inboundaggregator
Inboundfeedhc
Inboundfeedlc
Inboundfeedmc

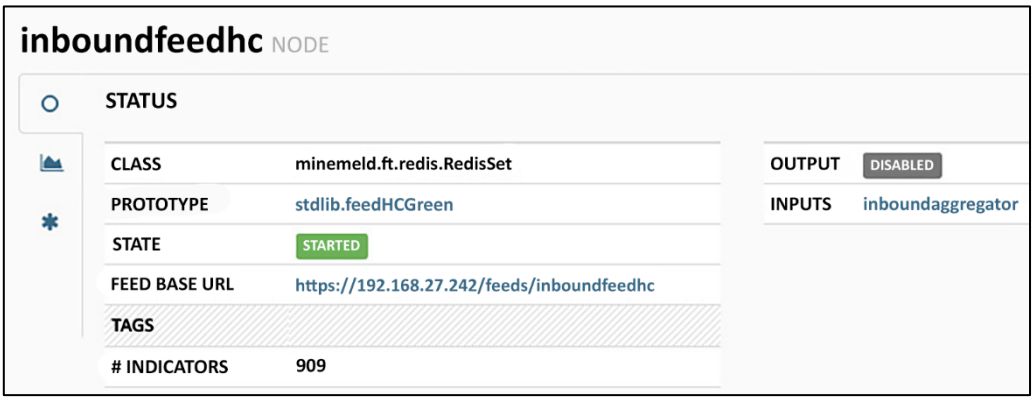

MINEMELD
DASHBOARD
NODES
CONFIG
LOGS
ADMIN
SYSTEM
NAME
TYPE
STATE
INDICATORS
ADD/REM/AO
UPDATES
WITHDRAWS
dshield_blocklist
MINER
STARTED
20
ADDED: 0
REMOVED: 0
RX: 0
PROCESSED: 0
TX: 0
RX: 0
PROCESSED: 0
TX: 0
spamhaus_DROP
MINER
STARTED
790
ADDED: 0
REMOVED: 0
RX: 0
PROCESSED: 0
TX: 0
RX: 0
PROCESSED: 0
TX: 0
spamhaus_EDROP
MINER
STARTED
95
ADDED: 0
REMOVED: 0
RX: 0
PROCESSED: 0
TX: 0
RX: 0
PROCESSED: 0
TX: 0
wlWhiteListIPv4
MINER
STARTED
0
ADDED: 0
REMOVED: 0
RX: 0
PROCESSED: 0
TX: 0
RX: 0
PROCESSED: 0
TX: 0
inboundfeedhc
OUTPUT
STARTED
909
ADDED: 0
REMOVED: 0
RX: 0
PROCESSED: 0
TX: 0
RX: 0
PROCESSED: 0
TX: 0
inboundfeedlc
OUTPUT
STARTED
0
ADDED: 0
RX: 0
RX: 0

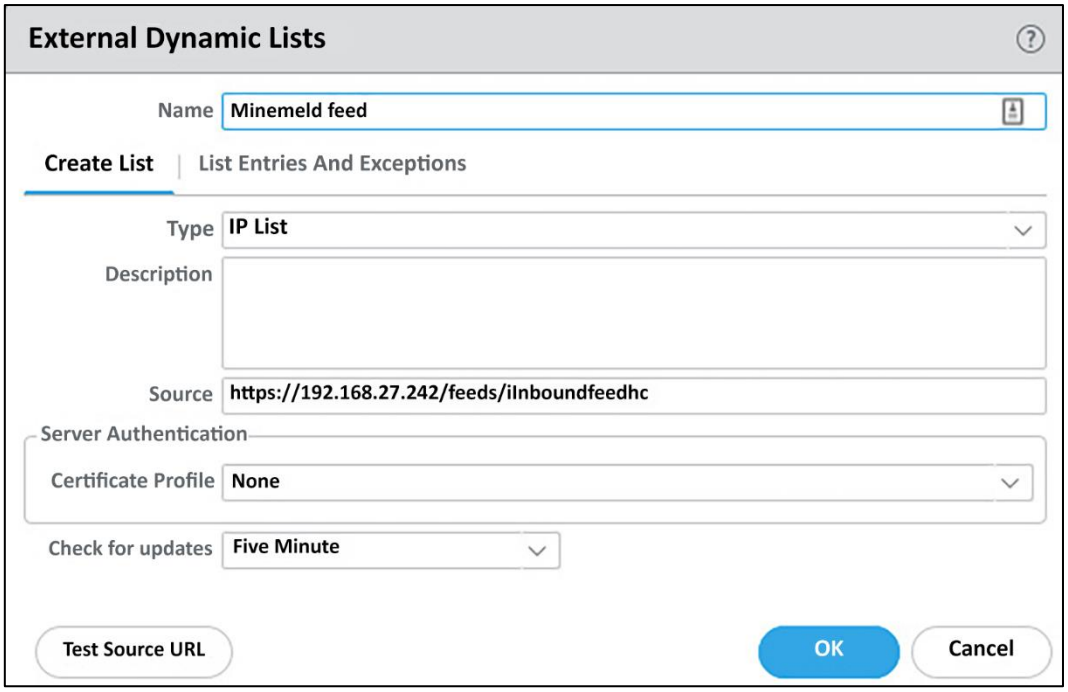

dshield_blocklist NODE
STATUS
CLASS
minemeld.ft.http.HttpFT
PROTOTYPE
dshieid.block
STATE
STARTED
LAST RUN
2020-06-17 00:14:24 +0200
SUCCESS
INDICATORS
20
OUTPUT
ENABLED
INPUTS
none

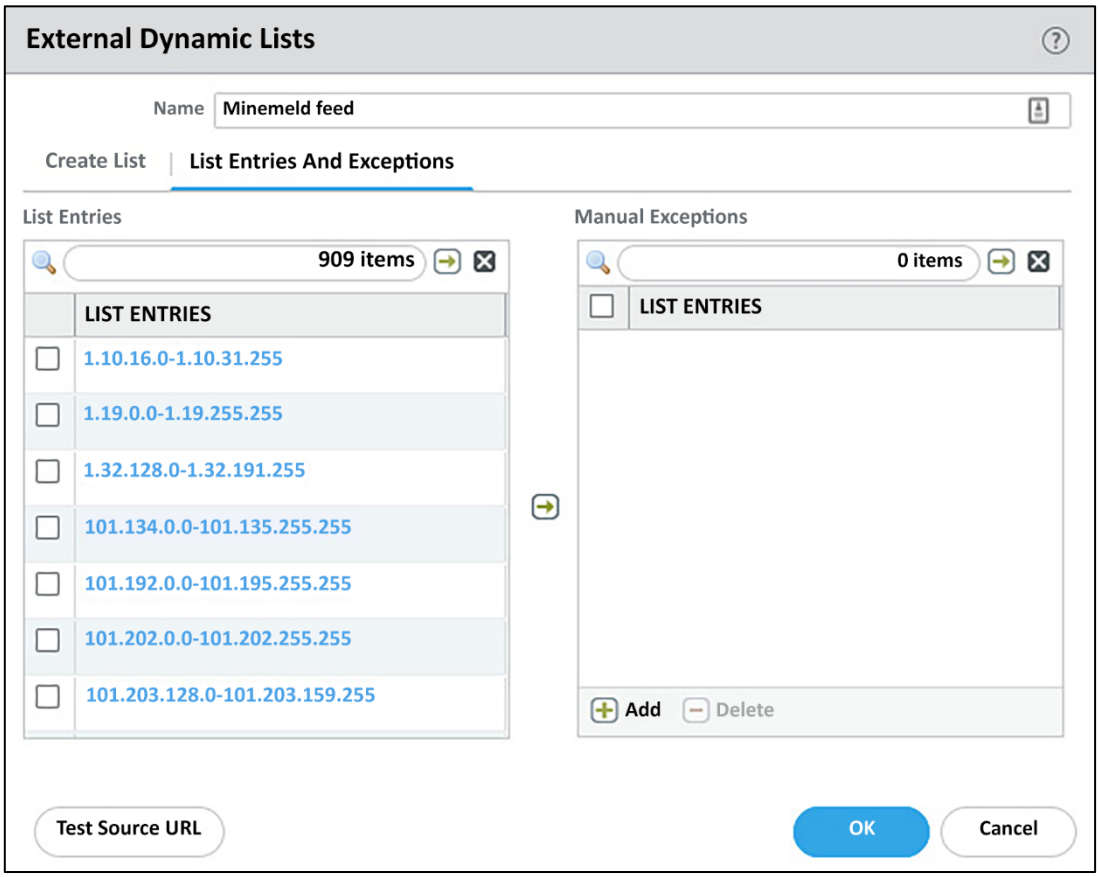

CONFIG
LOGS
ADMIN
SYSTEM
inboundaggregator
inboundaggregator
inboundaggregator
spamhaus_DROP
spamhaus_EDROP
dshield_blocklist
wlWhiteListIPv4
browse prototypes

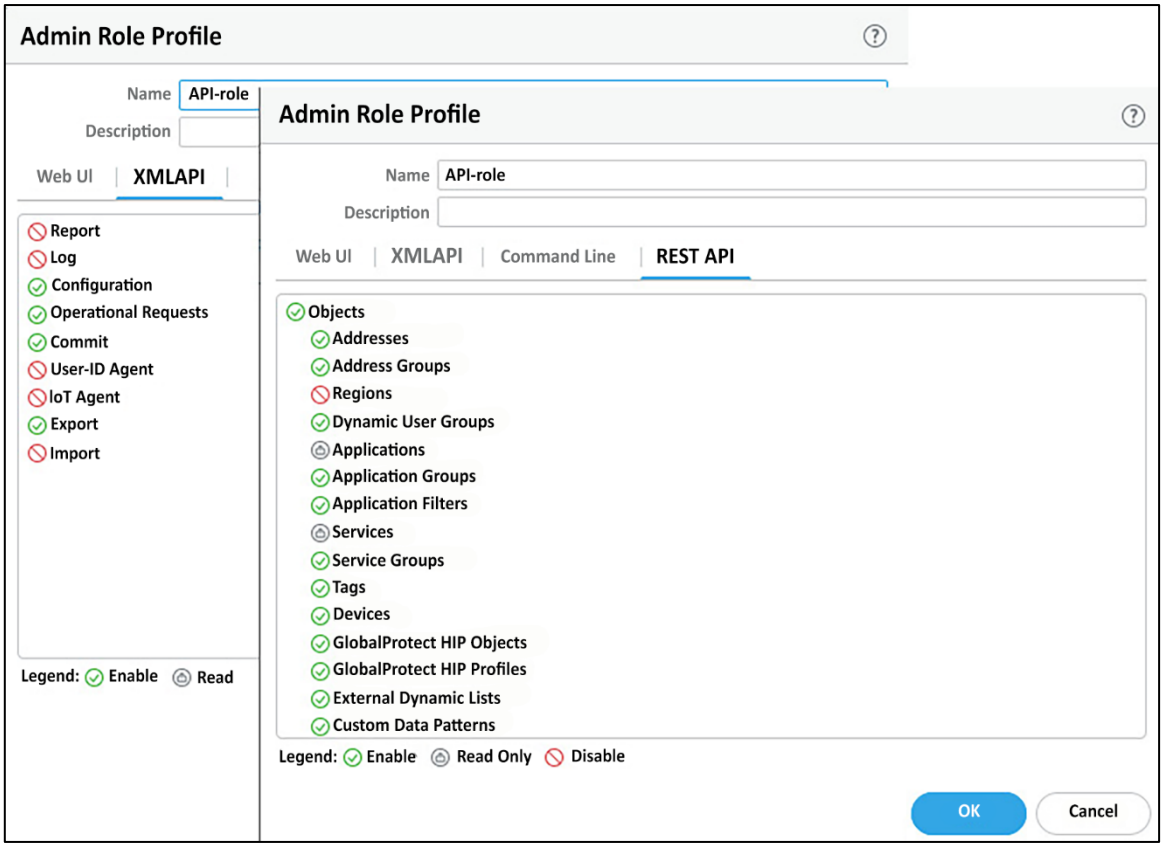

MINEMELD
DASHBOARD
NODES
CONFIG
LOGS
ADMIN
SYSTEM
new node from this prototype
cloudflare.ipv4 PROTOTYPE
CLONE
NEW
MINER
STABLE
ABOUT cloudflare


COMMIT
REVERT
LOAD
IMPORT
EXPORT
Search:
NAME
cloudflare4
dshield_blocklist
spamhaus_DROP
spamhaus_EDROP
wlWhiteListIPv4
inboundaggregator
INPUTS
spamhaus_DROP
spamhaus_EDROP
dshield_blocklist
wlWhiteListIPv4
MINER
cloudflare4
inboundfeedhc OUTPUT stdlib.feedHCGreen inboundaggregator
inboundfeedlc OUTPUT stdlib.feedLCGreen inboundaggregator
inboundfeedmc OUTPUT stdlib.feedMCGreen inboundaggregator
inboundaggregator PROCESSOR stdlib.aggregatorIPv4Inbound
spamhaus_DROP
spamhaus_EDROP
dshield_blocklist
wlWhiteListIPv4


inboundfeedhc NODE
STATUS
CLASS minemeld.ft.redis.RedisSet
PROTOTYPE stdlib.feedHCGreen
STATE STARTED
FEED BASE URL https://192.168.27.242/feeds/inboundfeedhc
TAGS
INDICATORS 909
OUTPUT DISABLED
INPUTS inboundaggregator


External Dynamic Lists
Name
Minemeld feed
Create List
List Entries And Exceptions
Type
IP List
Description
Source
https://192.168.27.242/feeds/iInboundfeedhc
Server Authentication
Certificate Profile
None
Check for updates
Five Minute
Test Source URL
OK
Cancel


External Dynamic Lists
Name
Minemeld feed
Create List
List Entries And Exceptions
List Entries
909 items
LIST ENTRIES
1.10.16.0-1.10.31.255
1.19.0.0-1.19.255.255
1.32.128.0-1.32.191.255
101.134.0.0-101.135.255.255
101.192.0.0-101.195.255.255
101.202.0.0-101.202.255.255
101.203.128.0-101.203.159.255
Manual Exceptions
0 items
LIST ENTRIES
Add
Delete
Test Source URL
OK
Cancel


Admin Role Profile
Name
API-role
Description
Web UI
XMLAPI
Report
Log
Configuration
Operational Requests
Commit
User-ID Agent
IoT Agent
Export
Import
Legend: Enable Read
Admin Role Profile
Name
API-role
Description
Web UI
XMLAPI
Command Line
REST API
Objects
Addresses
Address Groups
Regions
Dynamic User Groups
Applications
Application Groups
Application Filters
Services
Service Groups
Tags
Devices
GlobalProtect HIP Objects
GlobalProtect HIP Profiles
External Dynamic Lists
Custom Data Patterns
Legend: Enable Read Only Disable
OK
Cancel