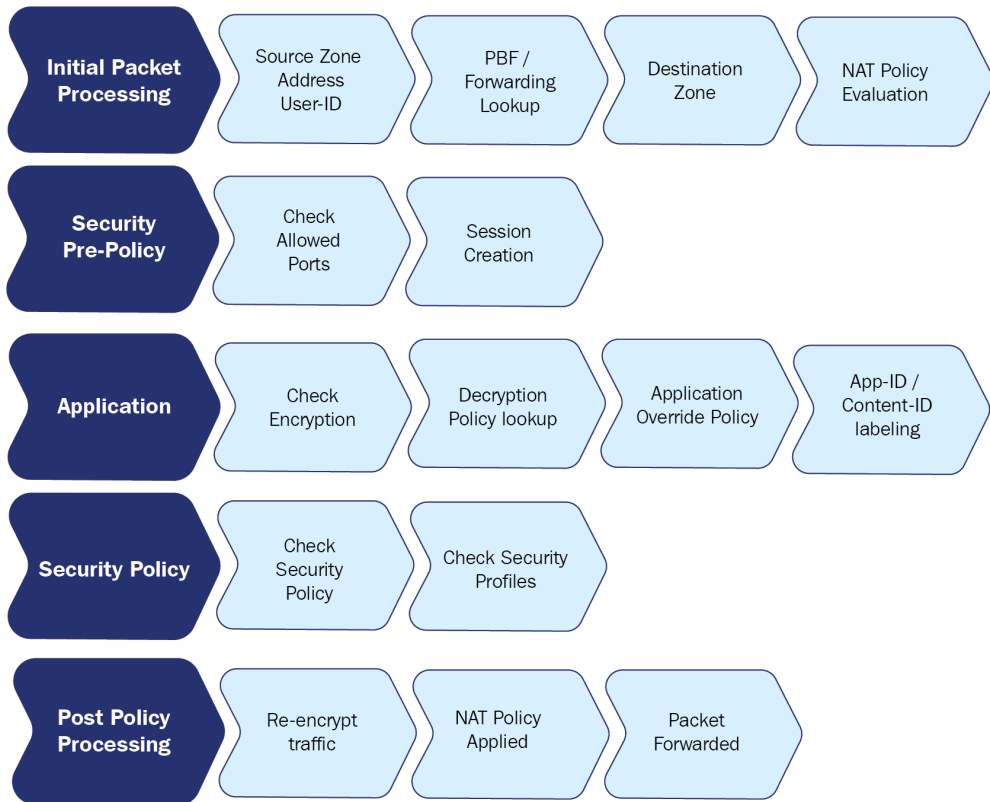
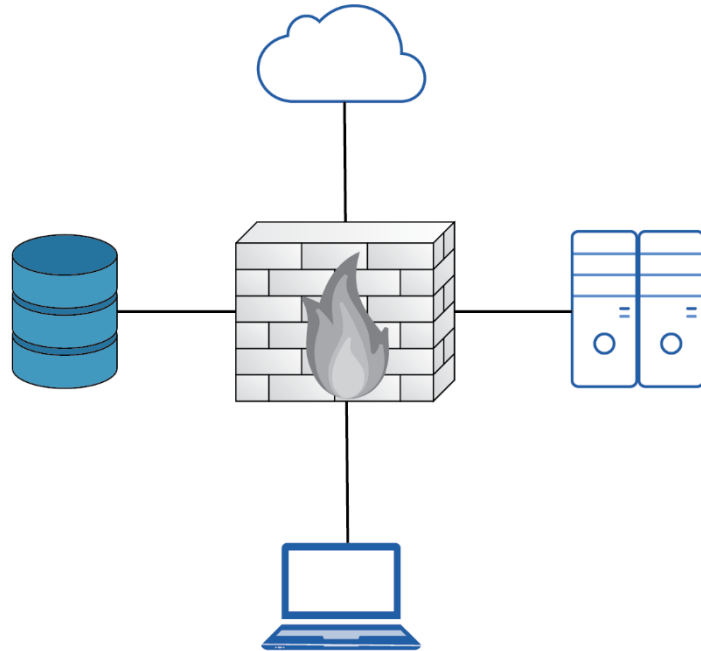
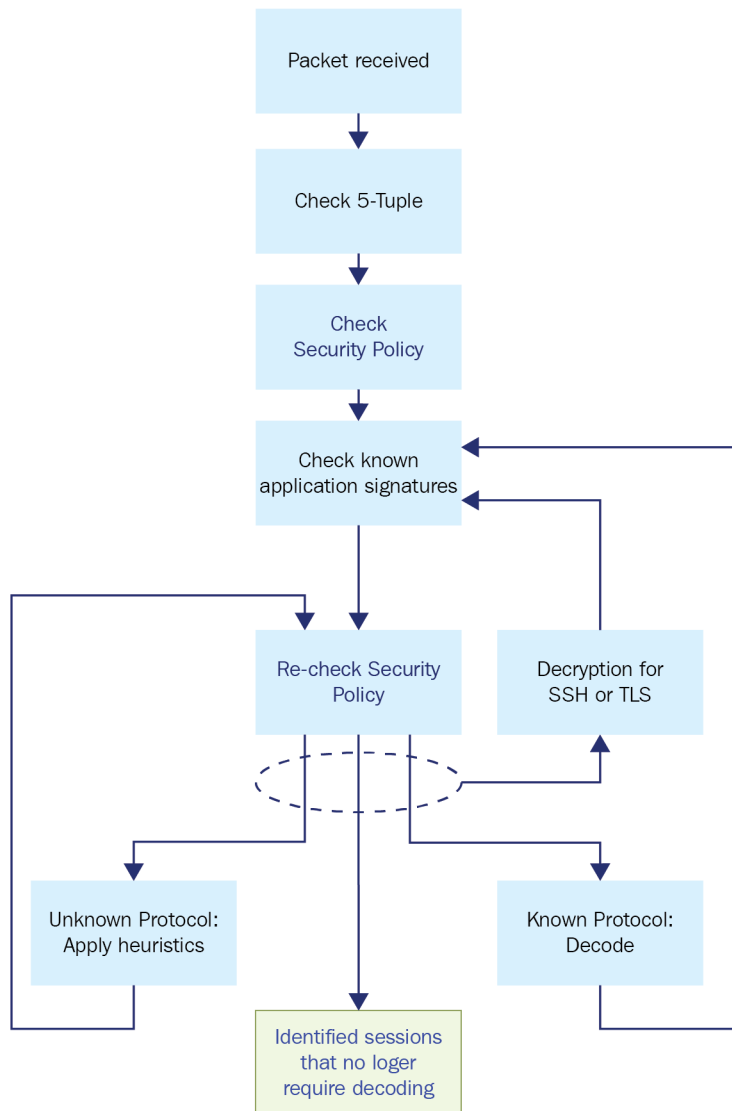
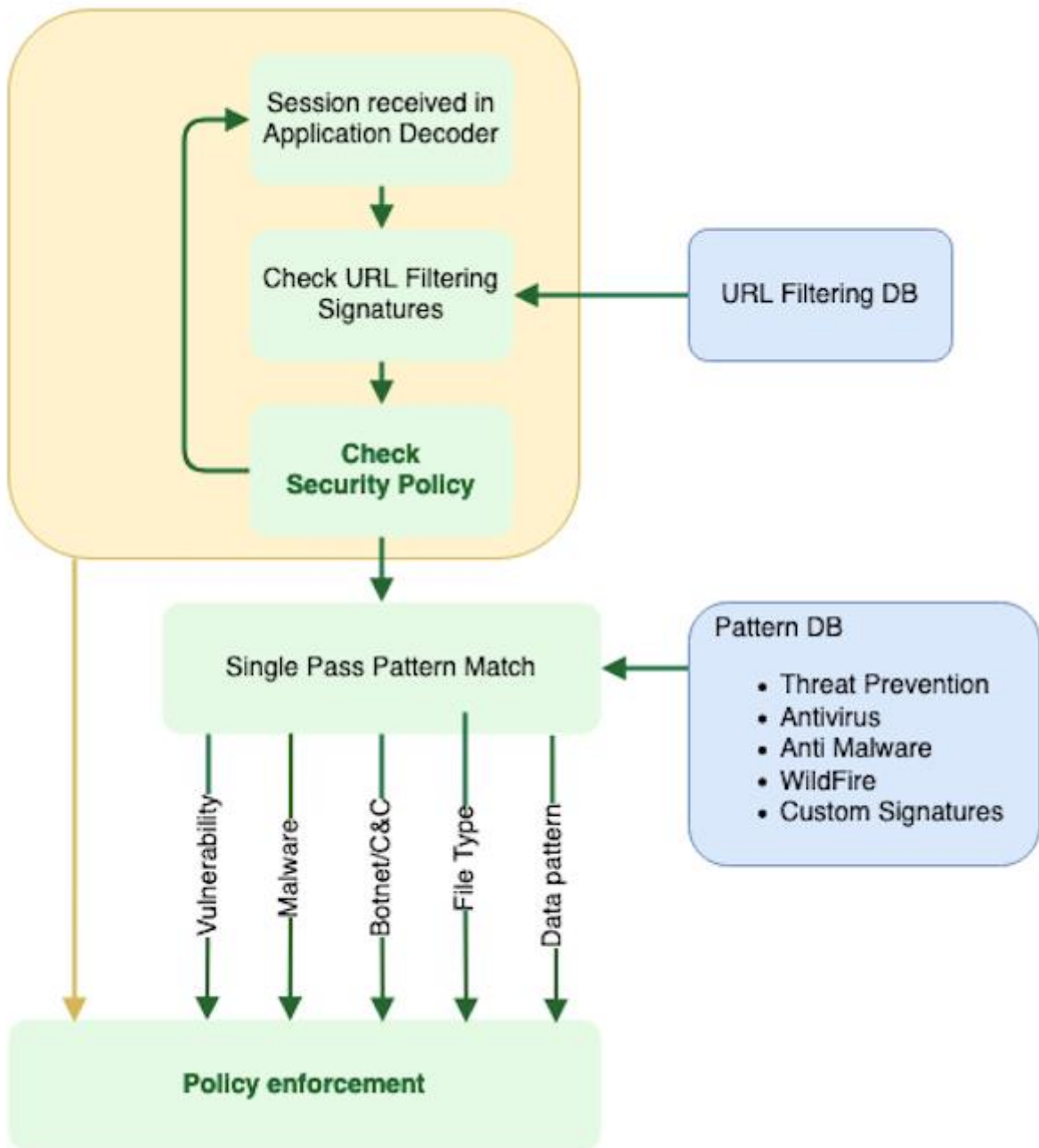


# Chapter 1: Understanding the Core Technologies

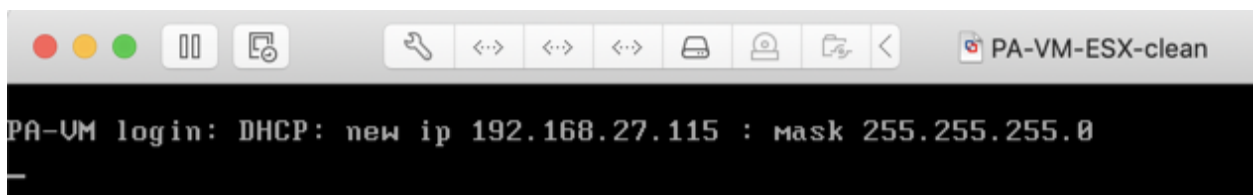
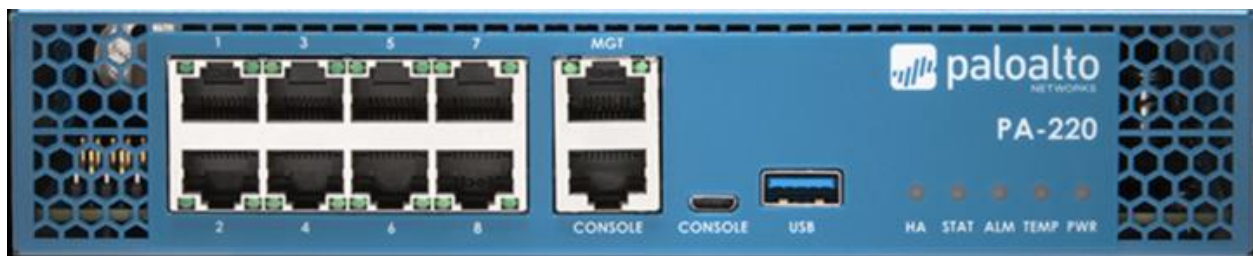
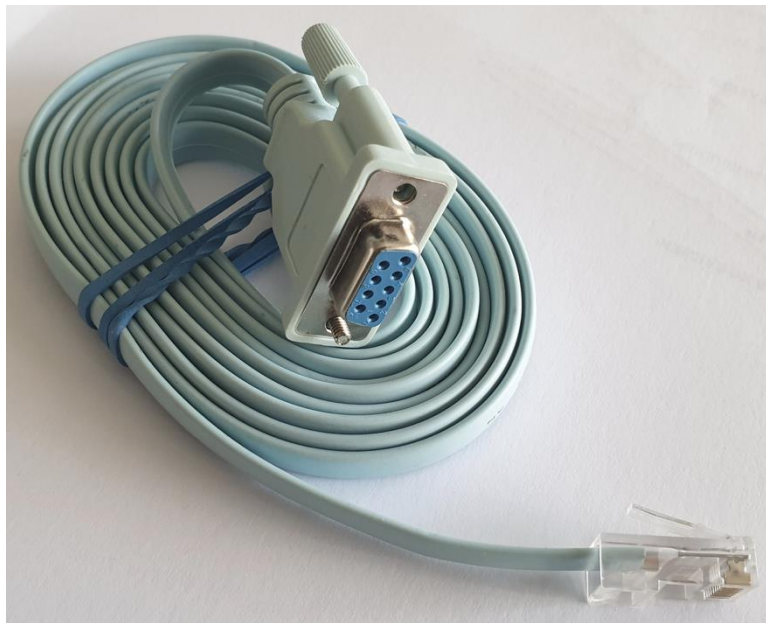


|    | NAME              | TYPE      | Source     |         | Destination |         | APPLICATION      | SERVICE             | ACTION | PROFILE | OPTIONS |
|----|-------------------|-----------|------------|---------|-------------|---------|------------------|---------------------|--------|---------|---------|
|    |                   |           | ZONE       | ADDRESS | ZONE        | ADDRESS |                  |                     |        |         |         |
| 1  | intrazone         | intrazone | dmz<br>lan | any     | (intrazone) | any     | allowed web apps | application-default | Allow  |         |         |
| 2  | interzone         | interzone | dmz<br>lan | any     | dmz<br>lan  | any     | allowed web apps | application-default | Allow  |         |         |
| 3  | universal         | universal | dmz<br>lan | any     | dmz<br>lan  | any     | allowed web apps | application-default | Allow  |         |         |
| 9  | intrazone-default | intrazone | any        | any     | (intrazone) | any     | any              | any                 | Allow  | none    | none    |
| 10 | interzone-default | interzone | any        | any     | any         | any     | any              | any                 | Deny   | none    | none    |





## Chapter 2: Setting Up a New Device







### 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 pages 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 192.168.27.115 \(unsafe\)](#)



### 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 480748849bf2e9c604324a8de84853c2a1be652f0a3203367791c9227706feff.

Error code: SEC\_ERROR\_UNKNOWN\_ISSUER

[View Certificate](#)

Go Back (Recommended)

Accept the Risk and Continue

#### General Information



|                                      |                          |
|--------------------------------------|--------------------------|
| Device Name                          | Reaper-PA-220            |
| MGT IP Address                       | 192.168.27.115           |
| MGT Netmask                          | 255.255.255.0            |
| MGT Default Gateway                  | 192.168.27.1             |
| MGT IPv6 Address                     | unknown                  |
| MGT IPv6 Link Local Address          | unknown                  |
| MGT IPv6 Default Gateway             |                          |
| MGT MAC Address                      | 08:30:6b:7b:6e:00        |
| Model                                | PA-220                   |
| Serial #                             | 0                        |
| Software Version                     | 10.0                     |
| GlobalProtect Agent                  | 5.1.3                    |
| Application Version                  | 8284-6141 (06/17/20)     |
| Threat Version                       | 8284-6141 (06/17/20)     |
| Antivirus Version                    | 3386-3897 (06/21/20)     |
| Device Dictionary Version            | 1-202                    |
| WildFire Version                     | 464843-467778 (06/21/20) |
| URL Filtering Version                | 20200621.20331           |
| GlobalProtect Clientless VPN Version | 86-182 (04/23/20)        |
| Time                                 | Mon Jun 22 00:04:06 2020 |
| Uptime                               | 5 days, 22:39:44         |
| Device Certificate Status            | None                     |

#### General Information



|                                      |                          |
|--------------------------------------|--------------------------|
| Device Name                          | 9dot2                    |
| MGT IP Address                       | 192.168.27.14            |
| MGT Netmask                          | 255.255.255.0            |
| MGT Default Gateway                  | 192.168.27.1             |
| MGT IPv6 Address                     | unknown                  |
| MGT IPv6 Link Local Address          | fe80::                   |
| MGT IPv6 Default Gateway             |                          |
| MGT MAC Address                      | 00:0c::                  |
| Model                                | PA-VM                    |
| Serial #                             | 01                       |
| CPU ID                               | ESX:                     |
| UUID                                 | 5641                     |
|                                      | 8531                     |
| VM License                           | VM-50                    |
| VM Mode                              | VMware ESXI              |
| Software Version                     | 10.0                     |
| GlobalProtect Agent                  | 0.0.0                    |
| Application Version                  | 8250-6008                |
| Device-ID Version                    | 1-202                    |
| URL Filtering Version                | 0000.00.00.000           |
| GlobalProtect Clientless VPN Version | 0                        |
| Time                                 | Mon Jun 22 00:07:46 2020 |
| Uptime                               | 0 days, 0:04:37          |
| Plugin VM series                     | vm_series-2.0.0-c36      |
| Device Certificate Status            | None                     |

# 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:    | <input type="text" value="Tom"/>      | * | Last Name:     | <input type="text" value="Piens"/>         | * |
| Title:         | <input type="text"/>                  |   | Phone:         | <input type="text" value="555-123456"/>    | * |
| Address Line1: | <input type="text" value="Mystreet"/> | * | Address Line2: | <input type="text"/>                       |   |
| City:          | <input type="text" value="MyTown"/>   | * | Country:       | <input type="text" value="United States"/> | * |
|                |                                       |   | Region/State:  | <input type="text" value="California"/>    | * |
|                |                                       |   | Postal Code:   | <input type="text" value="95050"/>         | * |

## Create UserID and Password

|   |   |   |
|---|---|---|
| Display Name:   | <input type="text" value="MyDisplayName"/>      | * |
| Your Email Address:   | <input type="text" value="myname@example.com"/> | * |
| Confirm Email Address:  | <input type="text" value="myname@example.com"/> | * |
| Password:   | <input type="password" value="....."/>          | * |
| (Minimum of 8 characters in length. Contains 3 of the following: uppercase letter, lowercase letter, number, symbol.) |   |   |
| Confirm Password:   | <input type="password" value="....."/>          | * |

|                                    |                      |   |
|------------------------------------|----------------------|---|
| Device Serial Number or Auth Code: | <input type="text"/> | * |
| Sales Order Number or Customer Id: | <input type="text"/> | * |

[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

Company Account

Members

Groups

Assets

Devices

Export To CSV

| Serial Number | Model Name | Device Name | Group | License                   | Actions | Auth Code | Expiration Date |
|---------------|------------|-------------|-------|---------------------------|---------|-----------|-----------------|
| 0             | PAN-PA-220 | PA220       |       | Software warranty Support |         | F         | 9/28/2019       |

1 50 items per page

## Device Licenses



### Device Licenses

Serial Number: 0 [REDACTED]

Model: PAN-PA-220

Device Name: PA220

| Feature Name              | Authorization Code | Expiration Date   | Actions |
|---------------------------|--------------------|-------------------|---------|
| Software warranty Support | F: [REDACTED]      | <b>09/28/2019</b> |         |

To activate the license feature for DNS Security, the OS version for the firewall must be 9.0 or above and have a valid Threat Prevention license.

### Activate Licenses

- Activate Auth-Code
- Activate Trial License
- Activate Feature License

### Auth-Code Activation

Authorization Code:

### EULA

By clicking "Agree and Submit" below, you agree to the terms and conditions of our [END USER LICENSE AGREEMENT](#) and [SUPPORT AGREEMENT](#) .

Agree and Submit

Refuse

|            |             |          |                           |              |            |
|------------|-------------|----------|---------------------------|--------------|------------|
| [REDACTED] | PAN-PA-3260 | PERIM 01 | Threat Prevention ▾       | 4 [REDACTED] | 4/23/2023  |
|            |             |          | PAN-DB URL Filtering ▾    | 8 [REDACTED] | 4/23/2023  |
|            |             |          | GlobalProtect Portal ▾    | 2 [REDACTED] | 11/11/2023 |
|            |             |          | Premium Partner Support ▾ | 6 [REDACTED] | 4/23/2023  |
|            |             |          | WildFire License ▾        | 9 [REDACTED] | 4/23/2023  |

- Multi Factor Authentication
- Local User Database
  - Users
  - User Groups
- Scheduled Log Export
- Software
- GlobalProtect Client
- Dynamic Updates
- Plugins
- VM-Series
- Licenses**
- Support

**License Management**

- [Retrieve license keys from license server](#)
- [Activate feature using authorization code](#)
- [Manually upload license key](#)
- [Deactivate VM](#)
- [Upgrade VM capacity](#)

**Update License** ?

Authorization Code

**AutoFocus Device License**

Date Issued February 25, 2020  
 Date Expires February 11, 2034  
 Description AutoFocus Device License

**Decryption Port Mirror**

Date Issued May 15, 2020  
 Date Expires Never  
 Description Decryption Port Mirror  
 Active Yes

**GlobalProtect Gateway**

Date Issued September 30, 2019  
 Date Expires September 28, 2022  
 Description GlobalProtect Gateway License

**GlobalProtect Portal**

Date Issued September 05, 2018  
 Date Expires Never  
 Description GlobalProtect Portal License

**PAN-DB URL Filtering**

Date Issued September 30, 2019  
 Date Expires September 28, 2022  
 Description Palo Alto Networks URL Filtering License  
 Active Yes

**SD WAN**

Date Issued December 17, 2019  
 Date Expires December 17, 2020  
 Description License to enable SD WAN feature

**Standard**

Date Issued September 30, 2019  
 Date Expires September 28, 2022  
 Description 10 x 5 phone support; repair and replace hardware service

**Threat Prevention**

Date Issued September 30, 2019  
 Date Expires September 28, 2022  
 Description Threat Prevention

**WildFire License**

Date Issued September 30, 2019  
 Date Expires September 28, 2022  
 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](#)

**PA-220** DASHBOARD ACC MONITOR POLICIES

- Multi Factor Authentication
- Local User Database
  - Users
  - User Groups
- Scheduled Log Expo
- Software
- GlobalProtect Client
- Dynamic Updates
- Licenses
- Support**
- Master Key and Diag
- Policy Recommendation

Support

[Activate support using authorization code](#)

**Update License** ?

Authorization Code

OK Cancel

**PA-220** DASHBOARD ACC MONITOR POLICIES OBJECTS

- Multi Factor Authentication
- Local User Database
  - Users
  - User Groups
- Scheduled Log Export
- Software
- GlobalProtect Client
- Dynamic Updates**
- Licenses
- Support
- Master Key and Diagnostics
- Policy Recommendation

| VERSION | FILE NAME                    | FEATURES            | TYPE           | SIZE | SHA256 |
|---------|------------------------------|---------------------|----------------|------|--------|
| >       | GlobalProtect Clientless VPN | Last checked: Never | Schedule: None |      |        |
| >       | GlobalProtect Data File      | Schedule: None      |                |      |        |

reaper | Logout | Last Login Time: 06/19/2020 13:52:16 | Session Expire Time: 07/21/2020 23:41:30

| VERSION  | FILE NAME                      | FEATURES      | TYPE | SIZE  | RELEASE DATE             | DOW... | CURR... INST... | ACTION                   | DOCUMENTATION                 |
|--|--------------------------------|---------------|------|-------|--------------------------|--------|-----------------|--------------------------|-------------------------------|
| Applications and Threats Last checked: 2020/06/22 00:03:11 CEST Schedule: Every Wednesday at 01:02 (Download only) |                                |               |      |       |                          |        |                 |                          |                               |
| 8276-6104  | panupv2-all-contents-8276-6104 | Apps, Threats | Full | 50 MB | 2020/05/22 04:59:18 CEST |        |                 | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 8277-6107  | panupv2-all-contents-8277-6107 | Apps, Threats | Full | 50 MB | 2020/05/23 03:11:27 CEST |        |                 | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 8278-6109  | panupv2-all-contents-8278-6109 | Apps, Threats | Full | 50 MB | 2020/05/28 02:51:13 CEST |        |                 | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 8279-6115  | panupv2-all-contents-8279-6115 | Apps, Threats | Full | 50 MB | 2020/06/03 01:06:06 CEST |        |                 | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 8280-6121  | panupv2-all-contents-8280-6121 | Apps, Threats | Full | 50 MB | 2020/06/05 00:14:35 CEST |        |                 | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 8281-6129  | panupv2-all-contents-8281-6129 | Apps, Threats | Full | 50 MB | 2020/06/09 19:08:18 CEST |        |                 | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 8282-6133  | panupv2-all-contents-8282-6133 | Apps, Threats | Full | 50 MB | 2020/06/12 00:53:26 CEST |        |                 | <a href="#">Download</a> | <a href="#">Release Notes</a> |

| VERSION ^                      | FILE NAME                              | FEATURES | TYPE   | SIZE | RELEASE DATE | DOW... | CURR... INST... |
|--------------------------------|--|----------|--|------|--------------|--------|-----------------|
| > Antivirus                    | Last checked: 2020/06/22 00:03:11 CEST |          | Schedule: None (Manual)                            |      |              |        |                 |
| > Applications and Threats     | Last checked: 2020/06/22 00:03:11 CEST |          | Schedule: Every Wednesday at 01:02 (Download only) |      |              |        |                 |
| > GlobalProtect Clientless VPN | Last checked: 2020/06/21 02:00:23 CEST |          | Schedule: None (Manual)                            |      |              |        |                 |
| > GlobalProtect Data File      | Schedule: None (Manual)                |          |  |      |              |        |                 |
| > WildFire                     | Last checked: 2020/06/22 00:30:10 CEST |          | Schedule: None (Manual)                            |      |              |        |                 |

### Antivirus Update Schedule

Recurrence: Hourly

Minutes Past Hour: 15

Action: download-and-install

Threshold (hours): 5

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: 34

Action: download-and-install

Disable new apps in content update

Threshold (hours): 5

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): 24

Delete Schedule
OK
Cancel

**Operation Failed**

No update information available

Close

| VERSION ▾ | SIZE   | RELEASE DATE        | AVAILABLE  | CURRENTLY INSTALLED | ACTION                   |                               |
|-----------|--------|---------------------|------------|---------------------|--------------------------|-------------------------------|
| 9.1.2-h1  | 277 MB | 2020/04/29 08:01:29 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 9.1.2     | 277 MB | 2020/04/08 10:49:11 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 9.1.1     | 277 MB | 2020/02/10 14:10:23 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 9.1.0     | 421 MB | 2019/12/13 12:51:48 | Downloaded |                     | <a href="#">Install</a>  | <a href="#">Release Notes</a> |
| 9.0.8     | 358 MB | 2020/04/16 13:29:06 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 9.0.7     | 356 MB | 2020/03/17 13:50:11 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |
| 9.0.6     | 356 MB | 2020/01/27 14:28:15 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |

| VERSION ▾ | SIZE   | RELEASE DATE        | AVAILABLE  | CURRENTLY INSTALLED | ACTION                   |                               |                          |
|-----------|--------|---------------------|------------|---------------------|--------------------------|-------------------------------|--------------------------|
| 9.1.2-h1  | 277 MB | 2020/04/29 08:01:29 | Downloaded |                     | <a href="#">Install</a>  | <a href="#">Release Notes</a> | <input type="checkbox"/> |
| 9.1.2     | 277 MB | 2020/04/08 10:49:11 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |                          |
| 9.1.1     | 277 MB | 2020/02/10 14:10:23 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |                          |
| 9.1.0     | 421 MB | 2019/12/13 12:51:48 | Downloaded |                     | <a href="#">Install</a>  | <a href="#">Release Notes</a> | <input type="checkbox"/> |
| 9.0.8     | 358 MB | 2020/04/16 13:29:06 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |                          |
| 9.0.7     | 356 MB | 2020/03/17 13:50:11 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |                          |
| 9.0.6     | 356 MB | 2020/01/27 14:28:15 |            |                     | <a href="#">Download</a> | <a href="#">Release Notes</a> |                          |

## Reboot Device



The device needs to be rebooted for the new software to be effective.

Do you want to reboot it now?

Yes

No



# Management Interface Settings



IP Type  Static  DHCP Client

IP Address

Netmask

Default Gateway

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed

MTU

### 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

| <input type="checkbox"/> | PERMITTED IP ADDRESSES | DESCRIPTION |
|--------------------------|------------------------|-------------|
| <input type="checkbox"/> | 192.168.27.0/24        | mgmt net    |
| <input type="checkbox"/> | 10.15.15.37            | remote mgmt |

OK

Cancel

## Interface Management Profile



Name

### 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

10.15.15.37

192.168.27.0/24

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

Comment

Interface Type

Netflow Profile

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

### Link Settings

Link Speed  Link Duplex  Link State

**Other info** | ARP Entries | ND Entries | NDP Proxy | LLDP | DDNS

Management Profile

MTU

Adjust TCP MSS

IPv4 MSS Adjustment

IPv6 MSS Adjustment

Untagged Subinterface

OK

Cancel

## Service Route Configuration



## Service Route Configuration



Use Management Interface for all  Customize

IPv4 | IPv6 | Destination

| <input type="checkbox"/> | SERVICE                 | SOURCE INTERFACE | SOURCE ADDRESS  |
|--------------------------|-------------------------|------------------|-----------------|
| <input type="checkbox"/> | AutoFocus               | ethernet1/8      | 198.51.100.1/24 |
| <input type="checkbox"/> | CRL Status              | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | Dataplane               | ethernet1/8      | 198.51.100.1/24 |
| <input type="checkbox"/> | DDNS                    | ethernet1/8      | 198.51.100.1/24 |
| <input type="checkbox"/> | Panorama pushed updates | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | DNS                     | ethernet1/8      | 198.51.100.1/24 |
| <input type="checkbox"/> | External Dynamic Lists  | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | Email                   | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | HTTP                    | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | IoT                     | ethernet1/8      | 198.51.100.1/24 |
| <input type="checkbox"/> | Kerberos                | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | LDAP                    | vlan             | 192.168.27.2/24 |

Set Selected Service Routes

Use Management Interface for all  Customize

IPv4 | IPv6 | Destination

| <input type="checkbox"/> | DESTINATION                | SOURCE INTERFACE | SOURCE ADDRESS  |
|--------------------------|----------------------------|------------------|-----------------|
| <input type="checkbox"/> | 192.168.27.7               | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | wildfire.paloaltonetwo...  | ethernet1/8      | 198.51.100.1/24 |
| <input type="checkbox"/> | panos.wildfire.paloalto... | ethernet1/8      | 198.51.100.1/24 |
| <input type="checkbox"/> | 192.168.27.4               | vlan             | 192.168.27.2/24 |
| <input type="checkbox"/> | 192.168.27.242             | vlan             | 192.168.27.2/24 |

+ Add - Delete Set Selected Service Routes


OK


Cancel

OK


Cancel


### Administrator ?

Name  

Authentication Profile  


Use only client certificate authentication (Web)


Password  

Confirm Password  


Use Public Key Authentication (SSH)

Administrator Type  Dynamic  Role Based



Password Profile  

### Password Profiles ?

Name  

Required Password Change Period (days)

Expiration Warning Period (days)

Post Expiration Admin Login Count

Post Expiration Grace Period (days)

## Minimum Password Complexity



Enabled

### Password Format Requirements

|                            |                                 |
|----------------------------|---------------------------------|
| Minimum Length             | <input type="text" value="12"/> |
| Minimum Uppercase Letters  | <input type="text" value="1"/>  |
| Minimum Lowercase Letters  | <input type="text" value="1"/>  |
| Minimum Numeric Letters    | <input type="text" value="1"/>  |
| Minimum Special Characters | <input type="text" value="1"/>  |
| Block Repeated Characters  | <input type="text" value="2"/>  |

Block Username Inclusion (including reversed)

### Functionality Requirements

|  |  |
|--|--|
| New Password Differs By Characters     | <input type="text" value="8"/>   |
|  | <input checked="" type="checkbox"/> Require Password Change on First Login |
| Prevent Password Reuse Limit           | <input type="text" value="6"/>   |
| Block Password Change Period (days)    | <input type="text" value="2"/>   |
| Required Password Change Period (days) | <input type="text" value="180"/>   |
| Expiration Warning Period (days)       | <input type="text" value="20"/>  |
| Post Expiration Admin Login Count      | <input type="text" value="1"/>   |
| Post Expiration Grace Period (days)    | <input type="text" value="10"/>  |

Functionality requirements can be overridden by password profiles

OK

Cancel

## Admin Role Profile



Name

Description

**Web UI**

XMLAPI

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:

Description:

Web UI | **XMLAPI** | 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:

Description:

Web UI | XMLAPI | 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

Legend:  Enable  Read Only  Disable

### Admin Role Profile ?

Name:

Description:

Web UI | XMLAPI | **Command Line** | REST API

- None
- superuser
- superreader
- deviceadmin
- devicereader

## TACACS+ Server Profile



Profile Name



Administrator Use Only

### Server Settings

Timeout (sec)

Authentication Protocol



Use single connection for all authentication

### Servers

| NAME | TACACS+ SERVER | SECRET | PORT |
|------|----------------|--------|------|
| TAC1 | 192.168.27.33  | *****  | 49   |

Enter the IP address or FQDN of the TACACS+ server

OK

Cancel

## LDAP Server Profile



Profile Name



Administrator Use Only

### Server List

| NAME     | LDAP SERVER ^ | PORT |
|----------|---------------|------|
| ADserver | 192.168.27.7  | 636  |

Enter the IP address or FQDN of the LDAP server

### Server Settings

Type

Base DN

Bind DN

Password



Confirm Password



Bind Timeout

Search Timeout

Retry Interval

Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

OK

Cancel



## RADIUS Server Profile



Profile Name



Administrator Use Only

### Server Settings

Timeout (sec)

Retries

Authentication Protocol

Allow users to change passwords after expiry

Make Outer Identity Anonymous

Certificate Profile

### Servers

| NAME    | RADIUS SERVER | SECRET | PORT |
|---------|---------------|--------|------|
| RADIUS1 | 192.168.27.45 | *****  | 1812 |

Enter the IP address or FQDN of the RADIUS server

OK

Cancel

## Certificate Profile



Name



Username Field

User Domain

CA Certificates

| <input type="checkbox"/> | NAME     | DEFAULT OCSP URL       | OCSP VERIFY CERTIFICATE | TEMPLATE NAME/OID |
|--------------------------|----------|------------------------|-------------------------|-------------------|
| <input type="checkbox"/> | RADIUSca | http://ca.pangurus.com | rootypines              |                   |

Default OCSP URL (must start with http:// or https://)

Use CRL

CRL Receive Timeout (sec)

Use OCSP

OCSP Receive Timeout (sec)

OCSP takes precedence over CRL

Certificate Status Timeout (sec)

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



Administrator Use Only

### Identity Provider Configuration

Identity Provider ID

Identity Provider Certificate

Select the certificate that IDP uses to sign SAML messages

Identity Provider SSO URL

Identity Provider SLO URL

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)

OK

Cancel

## Multi Factor Authentication Server Profile



Profile Name

Certificate Profile

### Server Settings

MFA Vendor

| NAME            | VALUE        |
|-----------------|--------------|
| API Host        |              |
| Integration Key |              |
| Secret Key      |              |
| Timeout (sec)   | 30 [5 - 600] |
| Base URI        | /auth/v2     |

OK

Cancel

## Authentication Profile



Profile Name

**Authentication** | Factors | Advanced

Type

Server Profile

Login Attribute

Password Expiry Warning   
Number of days prior to warning a user about password expiry.

User Domain

Username Modifier

### Single Sign On

Kerberos Realm

Kerberos Keytab  [X Import](#)

OK

Cancel

## Authentication Profile



Profile Name

Authentication | **Factors** | Advanced

Enable Additional Authentication Factors  
The factors below are used only for Authentication Policy

|                                      |                |
|--------------------------------------|----------------|
| <input type="checkbox"/>             | <b>FACTORS</b> |
| <input type="checkbox"/>             | mfa-okta       |
| + Add - Delete ↑ Move Up ↓ Move Down |                |

OK

Cancel

## Authentication Profile



Profile Name

Authentication | Factors | **Advanced**

### Allow List

ALLOW LIST ^

all

- all
- smokeypines\pangurus
- tpiens
- vpn-reaper

+ Add - Delete

### Account Lockout

Failed Attempts

Lockout Time (min)

OK

Cancel

## Administrator



Name

Authentication Profile

Use only client certificate authentication (Web)

Use Public Key Authentication (SSH)

Administrator Type  Dynamic  Role Based

Profile

OK

Cancel

## Ethernet Interface



Interface Name

Comment

Interface Type

Netflow Profile

**Config** | Advanced

### Assign Interface To

Virtual Wire

Security Zone

- None
- New Zone

## Virtual Wire



Profile Name

Interface1

Interface2

Tag Allowed

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

Comment

Interface Type

Netflow Profile

**Config** | IPv4 | IPv6 | SD-WAN | Advanced

### Assign Interface To

Virtual Router

Security Zone

OK

Cancel

## Ethernet Interface



Interface Name

Comment

Interface Type

Netflow Profile

Config | **IPv4** | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type  Static  PPPoE  DHCP Client

|                                      |                 |
|--------------------------------------|-----------------|
| <input type="checkbox"/>             | IP              |
| <input type="checkbox"/>             | 198.51.100.1/24 |
| + Add - Delete ↑ Move Up ↓ Move Down |                 |

IP address/netmask. Ex. 192.168.2.254/24

Config | **IPv4** | SD-WAN | Advanced

Enable SD-WAN

Type  Static  PPPoE  DHCP Client

**General** | Advanced

Enable

Username

Password

Confirm Password

[Show PPPoE Client Runtime Info](#)

Enable SD-WAN

Type  Static  PPPoE  DHCP Client

General | **Advanced**

Authentication

Static Address

automatically create default route pointing to peer

Default Route Metric

Access Concentrator

Service

Passive

OK

Cancel

### Virtual Router - default



#### Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

Profile Name

General | **ECMP**

- INTERFACES ^
  - loopback
  - tunnel
  - tunnel.2
  - tunnel.3
  - tunnel.4
  - vlan
- 

#### Administrative Distances

Static

Static IPv6

OSPF Int

OSPF Ext

OSPFv3 Int

OSPFv3 Ext

IBGP

EBGP

RIP

OK

Cancel

**Virtual Router - Static Route - IPv4** ?

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

Path Monitoring

Failure Condition  Any  All      Preemptive Hold Time (min)

| <input type="checkbox"/> | NAME        | ENABLE                              | SOURCE IP        | DESTINATION IP | PING INTERVAL(SEC) | PING COUNT |
|--------------------------|-------------|-------------------------------------|------------------|----------------|--------------------|------------|
| <input type="checkbox"/> | PathMonitor | <input checked="" type="checkbox"/> | 198.51.100.10... | 198.51.100.1   | 3                  | 5          |

**VLAN** ?

Profile Name

VLAN Interface

Static MAC Configuration

| <input type="checkbox"/> | INTERFACES ^ | MAC ADDRESS | INTERFACE |
|--------------------------|--------------|-------------|-----------|
| <input type="checkbox"/> | ethernet1/1  |             |           |
| <input type="checkbox"/> | ethernet1/2  |             |           |
| <input type="checkbox"/> | ethernet1/3  |             |           |
| <input type="checkbox"/> | ethernet1/4  |             |           |



### VLAN Interface ?

Interface Name

Comment

Netflow Profile

**Config** | IPv4 | IPv6 | Advanced

Assign Interface To

VLAN

Virtual Router

Security Zone

### VLAN Interface ?

Interface Name

Comment

Netflow Profile

**Config** | **IPv4** | IPv6 | Advanced

Type  Static  DHCP Client

| <input type="checkbox"/> | IP              |
|--------------------------|-----------------|
| <input type="checkbox"/> | 192.168.27.2/24 |

### Loopback Interface ?

Interface Name  .

Comment

Netflow Profile

**Config** | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router

Security Zone

### Virtual Router - Static Route - IPv4 ?

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

### Tunnel Interface ?

Interface Name  .

Comment







Netflow Profile

**Config** | IPv4 | IPv6 | Advanced

**Assign Interface To**

Virtual Router

Security Zone

| INTERFACE  | INTERFACE TYPE | LINK STATE  | IP ADDRESS       | MAC ADDRESS       | VIRTUAL ROUTER | SECURITY ZONE |
|--|----------------|---|------------------|-------------------|----------------|---------------|
|  ethernet1/3    | Layer3         |  | none             | 00:1b:17:00:32:12 | none           | none          |
|  ethernet1/3.10 | Layer3         |  | 172.16.0.1/24    |                   | default        | finance       |
|  ethernet1/3.20 | Layer3         |  | 192.168.27.1/... |                   | default        | trust-L3      |

### Aggregate Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

Config | IPv4 | IPv6 | **LACP** | Advanced

**Enable LACP**

Mode  Passive  Active

Transmission Rate  Fast  Slow

Fast Failover

System Priority

Maximum Interfaces

**High Availability Options**

Enable in HA Passive State

Same System MAC Address For Active-Passive HA

MAC Address

Select system generated MAC or enter a valid MAC

### Ethernet Interface ?

Interface Name

Comment

Interface Type

Aggregate Group

**Advanced**

**Link Settings**

Link Speed  Link Duplex  Link State

LACP Port Priority

### Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

**Config** | **Advanced**

**Assign Interface To**

Security Zone

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

|    |                |        |                        |    |            |
|----|----------------|--------|------------------------|----|------------|
| 01 | PAN-PA-850-NFR | PA-850 | NFR Bundle             | 2  | 10/29/2020 |
|    |                |        | Threat Prevention      |    | 10/29/2020 |
|    |                |        | PAN-DB URL Filtering   |    | 10/29/2020 |
|    |                |        | Decryption Port Mirror | 13 | Perpetual  |
|    |                |        | DNS Security           |    | 10/29/2020 |
|    |                |        | GlobalProtect Gateway  |    | 10/29/2020 |

**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 to the [AGREEMENT](#) and [SUPPORT AGREEMENT](#).

## Chapter 3: Building Strong Policies

### Antivirus Profile ?

Name  📄

Description

**Action** | Virus Exception | Dynamic Classification

Enable Packet Capture

**Decoders**

| DECODER ^ | ACTION               | WILDFIRE ACTION      | DYNAMIC CLASSIFICATION ACTION |
|-----------|----------------------|----------------------|-------------------------------|
| http      | default (reset-both) | default (reset-both) | default (reset-both)          |
| http2     | default (reset-both) | default (reset-both) | default (reset-both)          |
| imap      | default (alert)      | default (alert)      | default (alert)               |
| pop3      | default (alert)      | default (alert)      | default (alert)               |
| smb       | default (reset-both) | default (reset-both) | default (reset-both)          |

**Application Exception**

🔍  0 items → ✕

| <input type="checkbox"/> | APPLICATION | ACTION |
|--------------------------|-------------|--------|
|--------------------------|-------------|--------|

⊕ Add ⊖ Delete

OK Cancel

## Anti-Spyware Profile



Name ASprofile

Description

**Signature Policies** | Signature Exceptions | DNS Policies | DNS Exceptions

| <input type="checkbox"/> | POLICY NAME     | SEVERITY             | ACTION                | PACKET CAPTURE |
|--------------------------|-----------------|----------------------|-----------------------|----------------|
| <input type="checkbox"/> | simple-critical | critical             | block-ip (source,120) | single-packet  |
| <input type="checkbox"/> | simple-high     | high                 | reset-both            | single-packet  |
| <input type="checkbox"/> | simple-medium   | medium               | reset-both            | single-packet  |
| <input type="checkbox"/> | simple-low-info | low<br>informational | default               | disable        |

+ Add - Delete ↑ Move Up ↓ Move Down @ Clone 🔍 Find Matching Signatures

OK

Cancel

## Anti-Spyware Policy



Policy Name simple-critical

Threat Name any

Used to match any signature containing the entered text as part of the signature name

Category any

Action adware

Track By any

Duration autogen

Packet Capture backdoor

Severity

any (All

critical

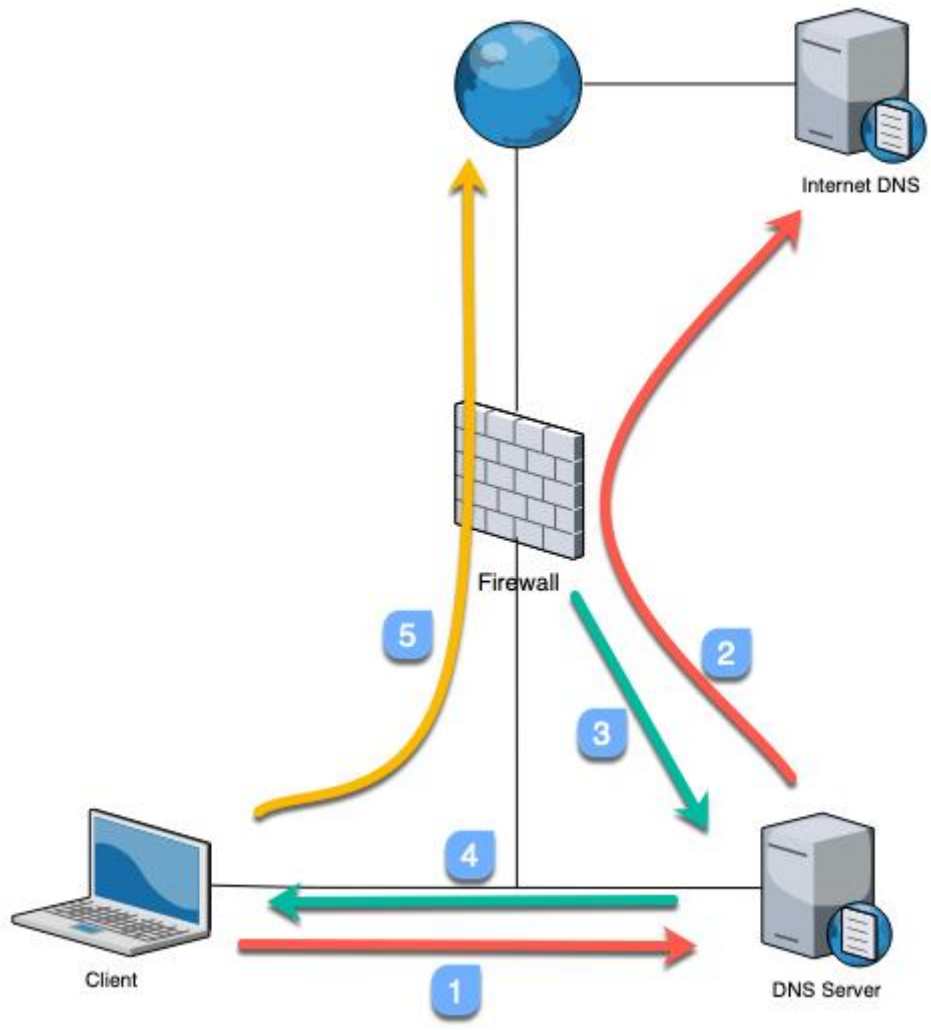
high

medium

low

informati

botnet  
browser-hijack  
command-and-control  
cryptominer  
data-theft  
dns  
dns-benign  
dns-c2  
dns-ddns



# Anti-Spyware Profile



Name

Description

[Signature Policies](#) | [Signature Exceptions](#) | **[DNS Policies](#)** | [DNS Exceptions](#)

## DNS Policies

| <input type="checkbox"/>       | SIGNATURE SOURCE            | LOG SEVERITY     | POLICY ACTION   | PACKET CAPTURE |
|--------------------------------|-----------------------------|------------------|-----------------|----------------|
| ∨ : Palo Alto Networks Content |                             |                  |                 |                |
| <input type="checkbox"/>       | default-paloalto-dns        | high             | sinkhole        | disable        |
| ∨ : DNS Security               |                             |                  |                 |                |
| <input type="checkbox"/>       | Benign Domains              | default (none)   | default (allow) | disable        |
| <input type="checkbox"/>       | Command and Control Domains | default (high)   | sinkhole        | disable        |
| <input type="checkbox"/>       | Dynamic DNS Hosted Domains  | default (medium) | default (allow) | disable        |
| <input type="checkbox"/>       | Malware Domains             | default (high)   | sinkhole        | disable        |
| <input type="checkbox"/>       | Recently Registered Domains | default (medium) | default (block) | disable        |

## DNS Sinkhole Settings

Sinkhole IPv4

Sinkhole IPv6





# Interface Management Profile



Name

## 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

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

# URL Filtering Profile



Name

Description

**Categories** | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Dynamic Classification

73 items → ×

| <input type="checkbox"/> | CATEGORY               | SITE ACCESS ▾ | USER CREDENTIAL SUBMISSION |
|--------------------------|------------------------|---------------|----------------------------|
| <input type="checkbox"/> | unknown                | continue      | allow                      |
| <input type="checkbox"/> | web-advertisements     | continue      | allow                      |
| <input type="checkbox"/> | adult                  | block         | block                      |
| <input type="checkbox"/> | command-and-control    | block         | block                      |
| <input type="checkbox"/> | copyright-infringement | block         | block                      |
| <input type="checkbox"/> | extremism              | block         | block                      |
| <input type="checkbox"/> | malware                | block         | block                      |

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

[Check URL Category](#)

**OK** Cancel

| SITE ACCESS ▾ | USER CREDENTIAL SUBMISSION |
|---------------|----------------------------|
| continue      |                            |
| continue      |                            |
| block         |                            |
| block         |                            |
| block         |                            |
| block         |                            |
| block         |                            |

- ↑ A Z Sort Ascending
- ↑ A Z Sort Descending
- Columns >
- Set All Actions >
- Set Selected Actions >
- Adjust Columns

allow  
alert  
block  
continue  
override

## URL Filtering Profile



Name

Description

Categories | **URL Filtering Settings** | User Credential Detection | HTTP Header Insertion | Dynamic Classification

- Log container page only
- Safe Search Enforcement

### HTTP Header Logging

- User-Agent
- Referer
- X-Forwarded-For

OK

Cancel

## HTTP Header Insertion



Name

Type

Domains

|                      |
|----------------------|
| DOMAINS              |
| *.google.com         |
| gmail.com            |
| <input type="text"/> |
| <input type="text"/> |

Headers

| <input type="checkbox"/>            | HEADER                     | VALUE                | LOG                                 |
|-------------------------------------|----------------------------|----------------------|-------------------------------------|
| <input checked="" type="checkbox"/> | X-GooGApps-Allowed-Domains | pangurus             | <input checked="" type="checkbox"/> |
| <input type="checkbox"/>            | <input type="text"/>       | <input type="text"/> | <input type="checkbox"/>            |

OK

Cancel

strict file blocking Predefin...

/22/2020 21:34:31 | Session

### File Blocking Profile

Name:

Description:

Search:

| <input type="checkbox"/>            | NAME ^                     | APPLICATIONS | FILE  |
|-------------------------------------|----------------------------|--------------|---|
| <input checked="" type="checkbox"/> | Block all risky file types | any          | <ul style="list-style-type: none"> <li><input type="checkbox"/> encrypted-7z</li> <li><input type="checkbox"/> encrypted-doc</li> <li><input type="checkbox"/> encrypted-docx</li> <li><input type="checkbox"/> encrypted-office</li> <li><input type="checkbox"/> encrypted-pdf</li> <li><input checked="" type="checkbox"/>   <input type="text"/></li> </ul> |

+ Add - Delete

| DIRECTION | ACTION |
|-----------|--------|
| both      | block  |

3 items → ×

OK Cancel

### WildFire Analysis Profile

Name:

Description:

Search:

| <input type="checkbox"/> | NAME      | APPLICATIONS | FILE TYPES | DIRECTION | ANALYSIS      |
|--------------------------|-----------|--------------|------------|-----------|---------------|
| <input type="checkbox"/> | pdf       | any          | pdf        | upload    | private-cloud |
| <input type="checkbox"/> | all files | any          | any        | both      | public-cloud  |

+ Add - Delete

2 items → ×

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

Vendor  Example: MS03-026

Bugtraq  Example: bugtraq id

Reference  Example: en.wikipedia.org/wiki/Virus

OK

Cancel

**Configuration** | **Signatures**

Signature  Standard  Combination

## Standard



Standard

Comment

Scope  Transaction  Session

Ordered Condition Match

AND CONDITI
NEGATE

New And Condition - Or Condition ?

Operator

Context

Pattern

QUALIFIER

- ftp-rsp-message
- ftp-rsp-protocol-payload
- gdbremote-req-context
- gdbremote-rsp-context
- giop-req-message-body
- giop-rsp-message-body
- gtpv2-req-pco-realm
- gtpv2-rsp-pco-realm
- h225-payload
- http-req-boxnet-enterprise-subdomain
- http-req-cookie
- http-req-headers
- http-req-host-header

|       |               |   |
|-------|---------------|---|
| .     | 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. x1, 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 request URI: http://www.example.com/]

[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: ww.  |
| 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 OS 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:

Description:

Data Capture

| DATA PATTERN                             | APPLICATIONS | FILE TYPE | DIRECTION | ALERT THRESHOLD | BLOCK THRESHOLD | LOG SEVERITY |
|--|--------------|-----------|-----------|-----------------|-----------------|--------------|
| <input type="checkbox"/> sensitive files | any          | Any       | both      | 1               | 2               | critical     |

#### Data Patterns

Name:

Description:

Pattern Type:

| NAME                                  | FILE TYPE            | FILE PROPERTY  | PROPERTY VALUE    |
|---------------------------------------|----------------------|----------------|-------------------|
| <input type="checkbox"/> pdf class    | Adobe PDF            | Classification | secret            |
| <input type="checkbox"/> pp sensitive | Microsoft PowerPoint | Sensitivity    | sensitive         |
| <input type="checkbox"/> rich text    | Rich Text Format     | Keywords/Tags  | internal use only |

### Security Profile Group

Name:

Antivirus Profile:

Anti-Spyware Profile:

Vulnerability Protection Profile:

URL Filtering Profile:

File Blocking Profile:

Data Filtering Profile:

WildFire Analysis Profile:

|    | NAME              | TYPE      | Source |         | Destination |         | APPLICATION | SERVICE | ACTION  | PROFILE | OPTIONS |
|----|-------------------|-----------|--------|---------|-------------|---------|-------------|---------|---------|---------|---------|
|    |                   |           | ZONE   | ADDRESS | ZONE        | ADDRESS |             |         |         |         |         |
| 10 | intrazone-default | intrazone | any    | any     | (intrazone) | any     | any         | any     | 🟢 Allow | none    | none    |
| 11 | interzone-default | interzone | any    | any     | any         | any     | any         | any     | 🔴 Deny  | none    | none    |

## Security Policy Rule

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

|  |  |   |
|--|--|---|
| <input type="checkbox"/> Any                   | <input type="checkbox"/> Any   | any                                       |
| <input type="checkbox"/> SOURCE ZONE ^         | <input type="checkbox"/> SOURCE ADDRESS ^                              | <input type="checkbox"/> SOURCE USER ^    |
| <input checked="" type="checkbox"/> Untrust-L3 | <input type="checkbox"/> Palo Alto Networks - Bulletproof IP addresses |   |
|  | <input type="checkbox"/> Palo Alto Networks - High risk IP addresses   |   |
|  | <input checked="" type="checkbox"/>                                    |   |
|  | <b>External Dynamic List</b>   |   |
|  | Minemeld feed  |   |
|  | Palo Alto Networks - Bulletproof IP addresses                          |   |
|  | Palo Alto Networks - High risk IP addresses                            |   |
|  | Palo Alto Networks - Known malicious IP addresses                      |   |
|  | <b>Region</b>  |   |
|  | 0.0.0.0-0.255.255  | External Dynamic List: panw-known-ip-list |
|  | 10.0.0.0-10.255.255 (Reserved)   |   |
| (+) Add (-) Delete                             | (+) Add (-) Delete   | (-) Delete                                |

## Security Policy Rule

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

|   |  |
|---|--|
| select                                      | <input checked="" type="checkbox"/> Any        |
| <input type="checkbox"/> DESTINATION ZONE ^ | <input type="checkbox"/> DESTINATION ADDRESS ^ |
| <input type="checkbox"/> Untrust-L3         |  |
| <input type="checkbox"/> dmz                |  |

## Security Policy Rule

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

|  |   |
|--|---|
| <b>Action Setting</b>                          | <b>Log Setting</b>  |
| Action: Drop                                   | <input type="checkbox"/> Log at Session Start               |
| <input type="checkbox"/> Send ICMP Unreachable | <input checked="" type="checkbox"/> Log at Session End      |
|  | Log Forwarding: default                                     |
| <b>Profile Setting</b>                         | <b>Other Settings</b>                                       |
| Profile Type: Group                            | Schedule: None  |
| Group Profile: default                         | QoS Marking: None   |
|  | <input type="checkbox"/> Disable Server Response Inspection |

OK

Cancel

Security Policy Rule ?

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

|  |   |  |  |
|--|---|--|--|
| <input type="checkbox"/> Any           | <input checked="" type="checkbox"/> Any   | any                                    | any                                      |
| <input type="checkbox"/> SOURCE ZONE ^ | <input type="checkbox"/> SOURCE ADDRESS ^ | <input type="checkbox"/> SOURCE USER ^ | <input type="checkbox"/> SOURCE DEVICE ^ |
| <input type="checkbox"/> dmz           |   |  |  |
| <input type="checkbox"/> trust-L3      |   |  |  |

Security Policy Rule ?

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

|   |  |   |
|---|--|---|
| select                                      | <input type="checkbox"/> Any   | any   |
| <input type="checkbox"/> DESTINATION ZONE ^ | <input type="checkbox"/> DESTINATION ADDRESS ^   | <input type="checkbox"/> DESTINATION DEVICE ^ |
| <input type="checkbox"/> untrust-L3         | <input type="checkbox"/> Palo Alto Networks - Bulletproof IP addresses<br><input type="checkbox"/> Palo Alto Networks - High risk IP addresses<br><input type="checkbox"/> Palo Alto Networks - Known malicious IP addresses |   |

|    |                   |           |     |     |             |     |     |     |                     |       |      |      |
|----|-------------------|-----------|-----|-----|-------------|-----|-----|-----|---------------------|-------|------|------|
| 12 | catchall          | universal | any | any | any         | any | any | any | application-default | Drop  |      |      |
| 13 | catchall-any      | universal | any | any | any         | any | any | any | any                 | Drop  |      |      |
| 14 | intrazone-default | intrazone | any | any | (intrazone) | any | any | any | any                 | Allow | none | none |
| 15 | interzone-default | interzone | any | any | any         | any | any | any | any                 | Deny  | none | none |

Application Group ?

Name  ?

9 items → ×

|                          |                              |
|--------------------------|------------------------------|
| <input type="checkbox"/> | <b>APPLICATIONS</b>          |
| <input type="checkbox"/> | ssl                          |
| <input type="checkbox"/> | dns                          |
| <input type="checkbox"/> | ntp                          |
| <input type="checkbox"/> | paloalto-updates             |
| <input type="checkbox"/> | paloalto-wildfire-cloud      |
| <input type="checkbox"/> | paloalto-gp-mfa-notification |
| <input type="checkbox"/> | paloalto-logging-service     |

## Application Filter



NAME

Apply to New App-IDs only

421 matching applications

| CATEGORY ^            | SUBCATEGORY ^            | RISK ^ | TAGS ^               | CHARACTERISTIC ^         |
|-----------------------|--------------------------|--------|----------------------|--------------------------|
| 1278 business-systems | 45 erp-crm               | 184 1  | 28 Enterprise VoIP   | 9 Data Breaches          |
| 636 collaboration     | 198 general-business     | 137 2  | 0 G Suite            | 79 Evasive               |
| 510 general-internet  | 464 ics-protocols        | 100 3  | 7 Palo Alto Networks | 47 Excessive Bandwidth   |
| 323 media             | 146 instant-messaging    | 50 4   | 349 Web App          | 11 FEDRAMP               |
| 505 networking        | 76 internet-conferencing | 5 5    | 0 block              | 27 HIPAA                 |
| 2 unknown             | 279 management           |        |                      | 30 IP Based Restrictions |
|                       | 11 marketing             |        |                      | 115 No Certifications    |

| NAME                      | CATEGORY         | SUBCATEGORY      | RISK | TAGS                  | STANDARD PORTS  | EXCLUDE                  |
|---------------------------|------------------|------------------|------|-----------------------|-----------------|--------------------------|
| adobe-connectnow (1 out)  |                  |                  |      |                       |                 | <input type="checkbox"/> |
| adobe-connectnow-base     | collaboration    | internet-confer  | 2    | Enterprise... Web App | tcp/80,443,1935 | <input type="checkbox"/> |
| adobe-cq                  | business-systems | general-business | 1    | Web App               | tcp/4502,4503   | <input type="checkbox"/> |
| adobe-creative-cloud      |                  |                  |      |                       |                 | <input type="checkbox"/> |
| adobe-creative-cloud-base | business-systems | general-business | 2    |                       | tcp/443, 80     | <input type="checkbox"/> |

Page 1 of 13 | Displaying 1 - 40 of 496

Show Technology Column

OK

Cancel

## Application Filter



NAME

Apply to New App-IDs only

76 matching applications

| CATEGORY ^          | SUBCATEGORY ^            | RISK ^ | TAGS ^               | CHARACTERISTIC ^        |
|---------------------|--------------------------|--------|----------------------|-------------------------|
| 1 business-systems  | 17 file-sharing          | 20 1   | 76 Enterprise VoIP   | 18 Evasive              |
| 50 collaboration    | 1 infrastructure         | 28 2   | 0 G Suite            | 38 Excessive Bandwidth  |
| 17 general-internet | 4 instant-messaging      | 14 3   | 0 Palo Alto Networks | 3 FEDRAMP               |
| 4 media             | 25 internet-conferencing | 13 4   | 62 Web App           | 18 HIPAA                |
| 4 networking        | 1 management             | 1 5    | 0 block              | 8 IP Based Restrictions |
|                     | 4 photo-video            |        |                      | 20 No Certifications    |
|                     | 3 remote-access          |        |                      | 7 PCI                   |

| NAME                 | CATEGORY         | SUBCATEGORY     | RISK | TAGS                  | STANDARD PORTS           | EXCLUDE                  |
|----------------------|------------------|-----------------|------|-----------------------|--------------------------|--------------------------|
| gotowebinar          |                  |                 |      |                       |                          | <input type="checkbox"/> |
| gotowebinar-base     | collaboration    | internet-confer | 1    | Enterprise... Web App | 1853,443,80,8200,tcp,udp | <input type="checkbox"/> |
| gotowebinar-download | general-internet | file-sharing    | 2    | Enterprise... Web App | 443,tcp                  | <input type="checkbox"/> |
| gotowebinar-upload   | general-internet | file-sharing    | 2    | Enterprise... Web App | 443,tcp                  | <input type="checkbox"/> |

Page 1 of 3 | Displaying 1 - 40 of 89

Show Technology Column

OK

Cancel

# Security Policy Rule



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

|   |   |  |   |
|---|---|--|---|
| <input type="checkbox"/> Any                          | <input type="checkbox"/> APPLICATIONS ^ | <input type="checkbox"/> enterprise VoIP | <input checked="" type="checkbox"/> allowed |
| <b>Application Group</b><br>allowed mgmt applications |   | <b>DEPENDS ON</b> ^                      |   |
| <b>Application Filter</b><br>allowed web apps         |   | adobe-flash-socketpolicy-server          |   |
| New Application Filter Application Group              |   | amazon-cloud-drive-base                  |   |
|   |   | amazon-cloud-drive-uploading             |   |
|   |   | boxnet-base                              |   |
|   |   | citrix                                   |   |
|   |   | citrix-jedi                              |   |
|   |   | evernote-base                            |   |

+ Add - Delete

21 items → X

Add To Current Rule Add To Existing Rule

OK Cancel

# Security Policy Rule



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

|                              |   |  |                                    |
|------------------------------|---|--|------------------------------------|
| <input type="checkbox"/> Any | <input type="checkbox"/> APPLICATIONS ^ | <input type="checkbox"/> ms-sms            | <input type="checkbox"/> ms-update |
|                              |   | <input checked="" type="checkbox"/> ssl    |                                    |
|                              |   | <input type="checkbox"/> web-browsing      |                                    |
|                              |   | <input checked="" type="checkbox"/> webdav |                                    |

+ Add - Delete


4 items → X


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

### Actions

**Log Setting**

Log at Session Start

Log at Session End

Log Forwarding


**Other Settings**

Schedule


QoS Marking



Disable Server Response Inspection

### Schedule

Name  

Recurrence

| START TIME |   |
|------------|---|
| 00:00      | Daily  |
| 12:00      | Weekly  |
| 18:00      | Non-recurring   |
| 23:59      |   |

 Add  Delete

PA-220 DASHBOARD ACC MONITOR **POLICIES** OBJECTS NETWORK DEVICE Commit

Security NAT QoS

Policy Optimizer

- No App Specified 0
- Unused Apps 0
- Rule Usage
  - Unused in 30 days 0
  - Unused in 90 days 1
  - Unused 1

| NAME              | ENABLED                             | HITS | LAST HIT | ACTION            | TAGS | GROUP | TYPE      | ZONE | ADDRESS | ZONES      |
|-------------------|-------------------------------------|------|----------|-------------------|------|-------|-----------|------|---------|------------|
| allow-byod        | <input checked="" type="checkbox"/> | 7    | 1-3      | allow-byod        | vpn  | vpn   | universal | vpn  | ippool  | DMZ        |
| allow-all-AV      | <input checked="" type="checkbox"/> | 8    | 5-10     | allow-all-AV      | vpn  | vpn   | universal | vpn  | ippool  | DMZ        |
| allow-all-opensvn | <input checked="" type="checkbox"/> | 9    | 11-14    | allow-all-opensvn | vpn  | vpn   | universal | vpn  | ippool  | DMZ        |
| Internet access   | <input checked="" type="checkbox"/> |      |          | Internet access   | vpn  | vpn   | universal | vpn  | ippool  | Untrust-L3 |

Object: A Zone Override Revert Enable Disable Move PDF/CSV Highlight Unused Rules View Rulebase as Groups Reset Rule Hit Counter Group

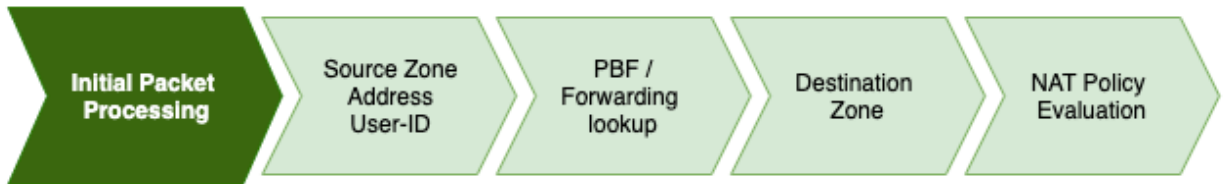
reaper Logout Last Login Time: 06/23/2020 00:05:07 Session Expire Time: 07/23/2020 22:09:27 Active Tasks Language

Tags to mark security rules

Tags to identify zones

Tags to group security rules

| 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

|  |   |  |  |
|--|---|--|--|
| <input type="checkbox"/> Any   | <b>Destination Zone</b><br>Untrust-L3       | <input checked="" type="checkbox"/> Any                                      | <input type="checkbox"/> Any   |
| <input type="checkbox"/> SOURCE ZONE ^                                       |   | <input type="checkbox"/> SOURCE ADDRESS ^                                    | <input type="checkbox"/> DESTINATION ADDRESS ^                               |
| <input type="checkbox"/> Untrust-L3  | <b>Destination Interface</b><br>ethernet1/1 |  | <input type="checkbox"/> 109.51.100.2  |
|  | <b>Service</b><br>any                       |  |  |
| <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> |   | <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> | <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> |

# NAT Policy Rule



General | Original Packet | **Translated Packet**

**Source Address Translation**

Translation Type:

**Destination Address Translation**

Translation Type:

Translated Address:

Translated Port:

Enable DNS Rewrite

Direction:

# NAT Policy Rule



General | **Original Packet** | Translated Packet

|  |  |  |  |
|--|--|--|--|
| <input type="checkbox"/> Any   | Destination Zone                         | <input type="checkbox"/> Any   | <input checked="" type="checkbox"/> Any                                      |
| <input type="checkbox"/> SOURCE ZONE ^                                       | <input type="text" value="Untrust-L3"/>  | <input type="checkbox"/> SOURCE ADDRESS ^                                    | <input type="checkbox"/> DESTINATION ADDRESS ^                               |
| <input type="checkbox"/> Trust-L3  | Destination Interface                    | <input type="checkbox"/> dhcpspace   |  |
|  | <input type="text" value="ethernet1/1"/> |  |  |
|  | Service                                  |  |  |
|  | <input type="text" value="any"/>         |  |  |
| <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> |  | <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> | <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> |

General | Original Packet | **Translated Packet**

**Source Address Translation**

Translation Type:

Address Type:

Interface:

IP Address:

General | Original Packet | **Translated Packet**

**Source Address Translation**

Translation Type:

Address Type:

|   |
|---|
| <input type="checkbox"/> TRANSLATED ADDRESS ^       |
| <input type="checkbox"/> 198.51.100.3               |
| <input type="checkbox"/> 198.51.100.5-198.51.100.38 |
| <input type="checkbox"/> 198.51.100.128/29          |



## NAT Policy Rule

General | Original Packet | **Translated Packet**

### Source Address Translation

Translation Type **Dynamic IP**

|                          |                      |
|--------------------------|----------------------|
| <input type="checkbox"/> | TRANSLATED ADDRESS ^ |
| <input type="checkbox"/> | 198.51.100.0/24      |
| <input type="checkbox"/> | 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

|  |                       |   |  |
|--|-----------------------|---|--|
| <input type="checkbox"/> Any           | Destination Zone      | <input type="checkbox"/> Any              | <input checked="" type="checkbox"/> Any        |
| <input type="checkbox"/> SOURCE ZONE ^ | Untrust-L3            | <input type="checkbox"/> SOURCE ADDRESS ^ | <input type="checkbox"/> DESTINATION ADDRESS ^ |
| <input type="checkbox"/> Trust-L3      | Destination Interface | <input type="checkbox"/> serverfarm       |  |
|  | ethernet1/1           |   |  |
|  | Service               |   |  |
|  | any                   |   |  |
| + Add - Delete                         |                       | + Add - Delete                            | + Add - Delete                                 |

OK

Cancel

## NAT Policy Rule

General | Original Packet | **Translated Packet**

|  |  |
|--|--|
| <b>Source Address Translation</b>                  | <b>Destination Address Translation</b> |
| Translation Type <b>Static IP</b>                  | Translation Type <b>None</b>           |
| Translated Address <b>serverfarm-public</b>        |  |
| <input checked="" type="checkbox"/> Bi-directional |  |

OK

Cancel

# NAT Policy Rule



General | **Original Packet** | Translated Packet

|  |                       |  |  |
|--|-----------------------|--|--|
| <input type="checkbox"/> Any   | Destination Zone      | <input checked="" type="checkbox"/> Any                                      | <input type="checkbox"/> Any   |
| <input type="checkbox"/> SOURCE ZONE ^                                       | Untrust-L3            | <input type="checkbox"/> SOURCE ADDRESS ^                                    | <input type="checkbox"/> DESTINATION ADDRESS ^                               |
| <input type="checkbox"/> Trust-L3  |                       |  | <input type="checkbox"/> 198.51.100.2  |
|  | Destination Interface |  |  |
|  | ethernet1/1           |  |  |
|  | Service               |  |  |
|  | any                   |  |  |
| <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> |                       | <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> | <input type="button" value="+ Add"/> <input type="button" value="- Delete"/> |

# NAT Policy Rule



General | Original Packet | **Translated Packet**

|                                       |   |
|---------------------------------------|---|
| <b>Source Address Translation</b>     | <b>Destination Address Translation</b>      |
| Translation Type: Dynamic IP And Port | Translation Type: Static IP                 |
| Address Type: Interface Address       | Translated Address: 10.0.0.5                |
| Interface: ethernet1/3                | Translated Port: [1 - 65535]                |
| IP Address: 10.0.0.1/24               | <input type="checkbox"/> Enable DNS Rewrite |
|                                       | Direction: reverse                          |

|  |             |
|--|-------------|
| Translated Address                                     | 10.0.0.5    |
| Translated Port  | [1 - 65535] |
| <input checked="" type="checkbox"/> Enable DNS Rewrite |             |
| Direction  | reverse     |
|  | reverse     |
|  | forward     |

**Destination Address Translation**

Translation Type **Dynamic IP (with session distribution)** ▾

Translated Address **serverfarm** ▾

Translated Port **[1 - 65535]**

Session Distribution Method **Round Robin** ▾

- Round Robin**
- Source IP Hash
- IP Modulo
- IP Hash
- Least Sessions

# Chapter 4: Taking Control of Sessions

**Actions** | Usage

---

**Log Setting**

Log at Session Start

Log at Session End

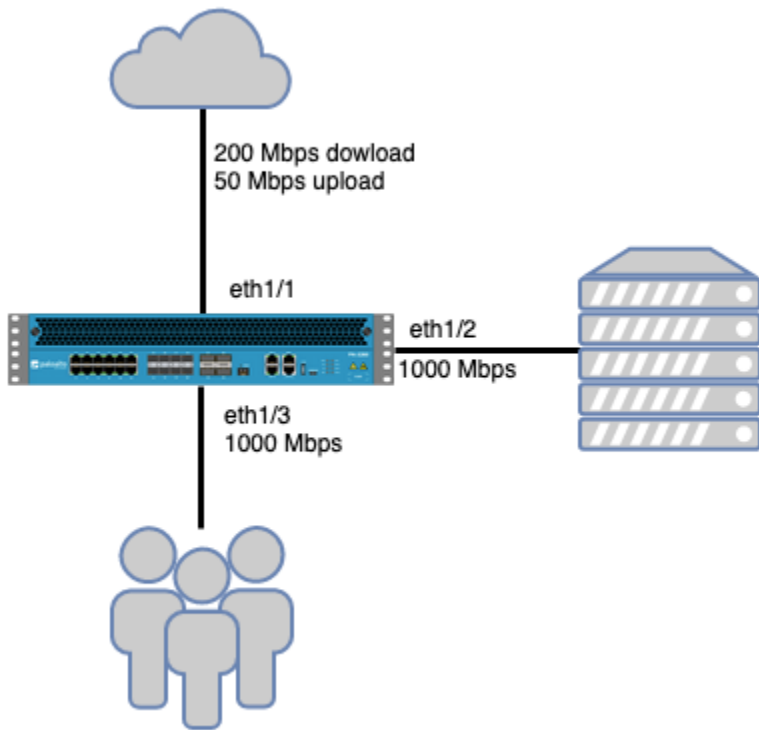
Log Forwarding: default

**Other Settings**

Schedule: None

QoS Marking: **None**

- IP DSCP
- IP Precedence
- Follow Client-to-Server Flow
- None



### QoS Profile

**Profile**

Profile Name:

Egress Max:

Egress Guaranteed:

**Classes**

Class Bandwidth Type:  Mbps  Percentage

| <input type="checkbox"/> | CLASS  | PRIORITY ^ | EGRESS MAX (MBPS) | EGRESS GUARANTEED (MBPS) |
|--------------------------|--------|------------|-------------------|--------------------------|
| <input type="checkbox"/> | class5 | medium     | 50                | 0                        |
| <input type="checkbox"/> | class1 | real-time  | 0                 | 20                       |

### QoS Profile

**Profile**

Profile Name:

Egress Max:

Egress Guaranteed:

**Classes**

Class Bandwidth Type:  Mbps  Percentage

| <input type="checkbox"/> | CLASS  | PRIORITY ^ | EGRESS MAX (MBPS) | EGRESS GUARANTEED (MBPS) |
|--------------------------|--------|------------|-------------------|--------------------------|
| <input type="checkbox"/> | class1 | real-time  | 0                 | 20                       |

### QoS Profile

**Profile**

Profile Name:

Egress Max:

Egress Guaranteed:

**Classes**

Class Bandwidth Type:  Mbps  Percentage

| <input type="checkbox"/> | CLASS  | PRIORITY ^ | EGRESS MAX (MBPS) | EGRESS GUARANTEED (MBPS) |
|--------------------------|--------|------------|-------------------|--------------------------|
| <input type="checkbox"/> | class4 | medium     | 0                 | 20                       |

### QoS Profile

**Profile**

Profile Name:

Egress Max:

Egress Guaranteed:

**Classes**

Class Bandwidth Type:  Mbps  Percentage

| <input type="checkbox"/> | CLASS  | PRIORITY ^ | EGRESS MAX (MBPS) | EGRESS GUARANTEED (MBPS) |
|--------------------------|--------|------------|-------------------|--------------------------|
| <input type="checkbox"/> | class8 | low        | 300               | 0                        |

## QoS Interface ?

**Physical Interface**
Clear Text Traffic
Tunneled Traffic

Interface Name:

Egress Max (Mbps):

Turn on QoS feature on this interface

**Default Profile**

Clear Text:

Tunnel Interface:

OK
Cancel

## QoS Interface



**Physical Interface** | Clear Text Traffic | Tunneled Traffic

Interface Name

Egress Max (Mbps)

Turn on QoS feature on this interface

### Default Profile

Clear Text

Tunnel Interface

## QoS Interface



Physical Interface | **Clear Text Traffic** | Tunneled Traffic

Egress Guaranteed (Mbps)

Egress Max (Mbps)

| <input type="checkbox"/> | NAME       | QOS PROFILE       | SOURCE INTERFACE | SOURCE SUBNET |
|--------------------------|------------|-------------------|------------------|---------------|
| <input type="checkbox"/> | userupload | internal          | ethernet1/3      | any           |
| <input type="checkbox"/> | internet   | internet-download | ethernet1/1      | any           |

OK

Cancel

## QoS Interface



**Physical Interface** | Clear Text Traffic | Tunneled Traffic

Interface Name

Egress Max (Mbps)

Turn on QoS feature on this interface

### Default Profile

Clear Text

Tunnel Interface

## QoS Interface



Physical Interface | **Clear Text Traffic** | Tunneled Traffic

Egress Guaranteed (Mbps)

Egress Max (Mbps)

| <input type="checkbox"/> | NAME             | QOS PROFILE       | SOURCE INTERFACE | SOURCE SUBNET |
|--------------------------|------------------|-------------------|------------------|---------------|
| <input type="checkbox"/> | userupload       | internal          | ethernet1/2      | any           |
| <input type="checkbox"/> | internetdownload | internet-download | ethernet1/1      | any           |

OK

Cancel

**QoS Policy Rule** ⓘ

General | **Source** | QoS Policy Rule ⓘ

Any  
 SOURCE ZONE ^  
 DMZ-L3  
 Trust-L3

DESTINATION ZONE ^  
 Untrust-L3

Any  
 APPLICATIONS ^  
 enterprise VoIP

**QoS Policy Rule** ⓘ

General | Source | Destination | **Application** | Service/URL Category | DSCP/ToS | Other Settings

Class 1

Schedule None

**QoS Policy Rule** ⓘ

General | **Source** | QoS Policy Rule ⓘ

Any  
 SOURCE ZONE ^  
 Untrust-L3

DESTINATION ZONE ^  
 DMZ-L3  
 Trust-L3

Any  
 APPLICATIONS ^  
 enterprise VoIP

**QoS Policy Rule** ⓘ

General | Source | Destination | **Application** | Service/URL Category | DSCP/ToS | Other Settings

Class 1

Schedule None

### QoS Policy Rule

General | **Source** | QoS Policy Rule

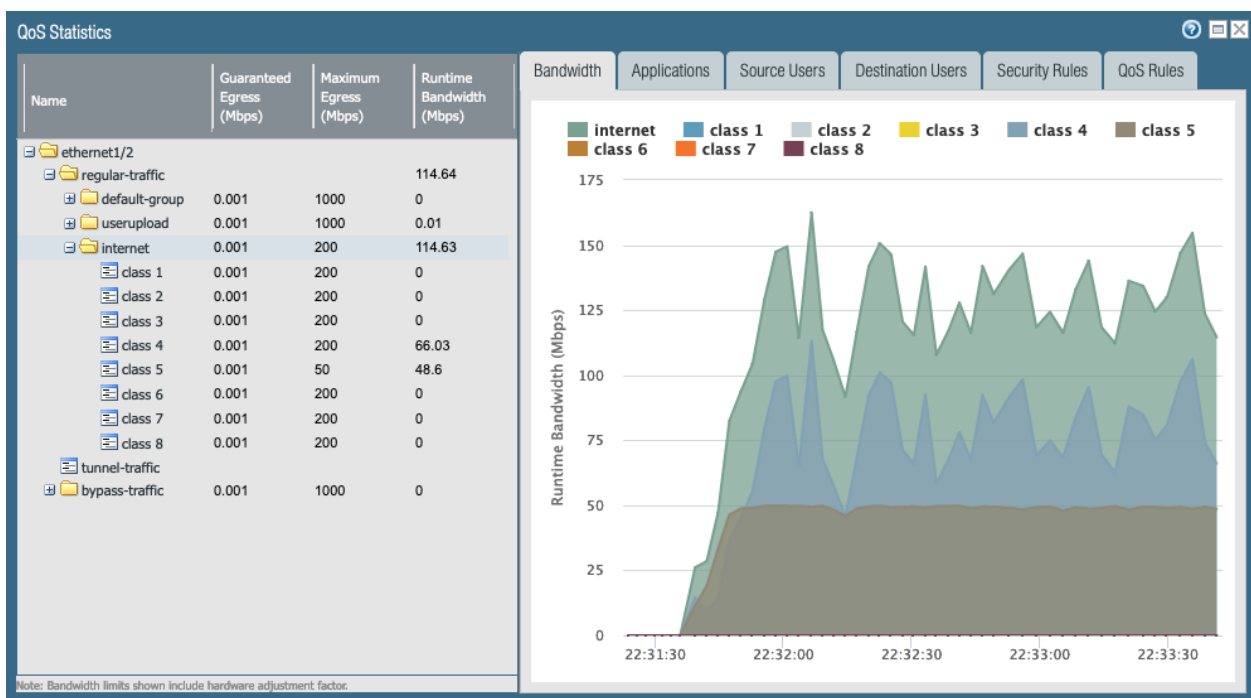
Any  
 SOURCE ZONE ^  
 Trust-L3

DESTINATION ZONE ^  
 DMZ-L3

Any  
 APPLICATIONS ^  
 ftp  
 ms-ds-smb  
 scps

Any  
 APPLICATIONS ^  
 ftp  
 ms-ds-smb  
 scps

Class: 8  
 Schedule: None





### Generate Certificate

Certificate Type:  Local  SCEP

Certificate Name:

Common Name:

Signed By:

Certificate Authority  
 Block Private Key Export

OCSF Responder:

**Cryptographic Settings**

Algorithm:

Number of Bits:

Digest:

Expiration (days):

**Certificate Attributes**

| TYPE   | VALUE             |
|--|-------------------|
| <input type="checkbox"/> Country = "C" from "Subject" field      | BE                |
| <input type="checkbox"/> Organization = "O" from "Subject" field | example.com       |
| <input type="checkbox"/> Email = "emailAddress" part             | certs@example.com |

### Generate Certificate

Certificate Type:  Local  SCEP

Certificate Name:

Common Name:

Signed By:

Certificate Authority  
 Block Private Key Export

OCSF Responder:

**Cryptographic Settings**

Algorithm:

Number of Bits:

Digest:

Expiration (days):

**Certificate Attributes**

| TYPE   | VALUE                |
|--|----------------------|
| <input type="checkbox"/> Country = "C" from "Subject" field      | BE                   |
| <input type="checkbox"/> Organization = "O" from "Subject" field | example.com          |
| <input type="checkbox"/> Email = "emailAddress" part             | helpdesk@example.com |

### Generate Certificate

Certificate Type:  Local  SCEP

Certificate Name:

Common Name:

Signed By:

Certificate Authority  
 Block Private Key Export

OCSF Responder:

**Cryptographic Settings**

Algorithm:

Number of Bits:

Digest:

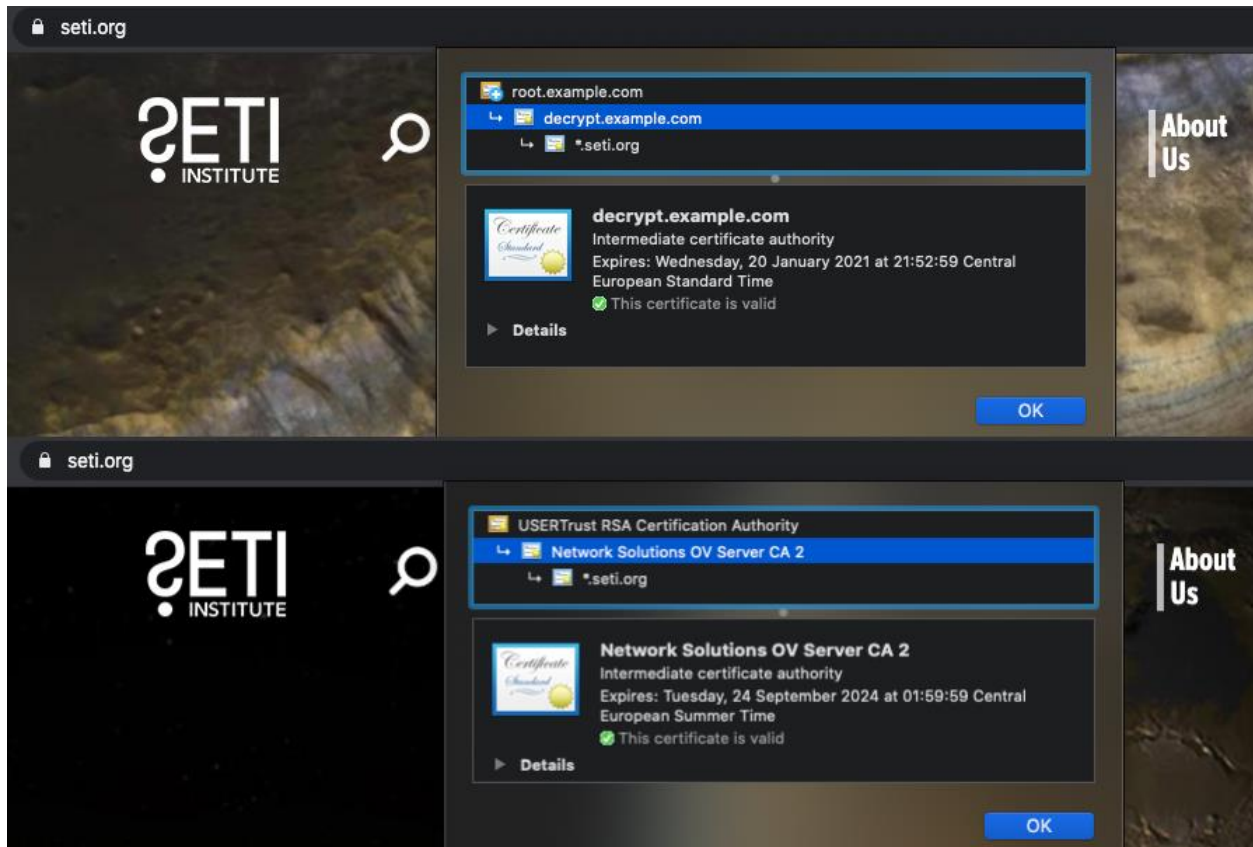
Expiration (days):

**Certificate Attributes**

| TYPE  | VALUE                 |
|---|-----------------------|
| <input type="checkbox"/> Email = "emailAddress" part of "Subject" CN field (CN=CommonName/emailA... | Incidents@example.com |

| <input type="checkbox"/>            | NAME                   | EXPIRES                   | SUBJECT                             |
|-------------------------------------|------------------------|---------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> | root signing cert      | Jan 20 20:50:19 2021 G... | C = BE, O = example.com, CN = ro... |
| <input type="checkbox"/>            | decryption subordinate | Jan 20 20:52:59 2021 G... | C = BE, O = example.com, CN = de... |

/23/2020 00:05:07 | Session Expire Time: 07/23/2020 22:09:27



### Import Certificate ?

Certificate Type  Local  SCEP

Certificate Name

Certificate File  [Browse...](#)

File Format  ▼

Private key resides on Hardware Security Module

Import Private Key

Block Private Key Export

Key File  [Browse...](#)

Passphrase

Confirm Passphrase

|                          |                                  |                                     |                                     |                                     |                                     |
|--------------------------|----------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | ▼ DigiCert Global Root CA        | CN = DigiCert Global Root CA        | CN = DigiCert Global Root CA        | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> | ▼ DigiCert SHA2 Secure Server CA | CN = DigiCert SHA2 Secure Server CA | CN = DigiCert Global Root CA        | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> | www.example.com                  | CN = www.example.com                | CN = DigiCert SHA2 Secure Server CA | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

**Policy Based Forwarding Rule** ?

General | **Source** | Destination/Application/Service | Forwarding

Type Zone  Any any

|                                   |   |  |
|-----------------------------------|---|--|
| <input type="checkbox"/> ZONE ^   | <input type="checkbox"/> SOURCE ADDRESS ^ | <input type="checkbox"/> SOURCE USER ^ |
| <input type="checkbox"/> Trust-L3 | <input type="checkbox"/> 192.168.27.0/24  |  |

**Policy Based Forwarding Rule** ?

General | Source | **Destination/Application/Service** | Forwarding

|  |   |  |
|--|---|--|
| <input checked="" type="checkbox"/> Any        | <input checked="" type="checkbox"/> Any | <span>select</span>                    |
| <input type="checkbox"/> DESTINATION ADDRESS ^ | <input type="checkbox"/> APPLICATIONS ^ | <input type="checkbox"/> SERVICE ^     |
|  |   | <input type="checkbox"/> service-https |

**Policy Based Forwarding Rule** ?

General | Source | Destination/Application/Service | **Forwarding**

Monitor

Action Forward

Egress Interface ethernet1/8

Next Hop IP Address

198.51.100.2

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:

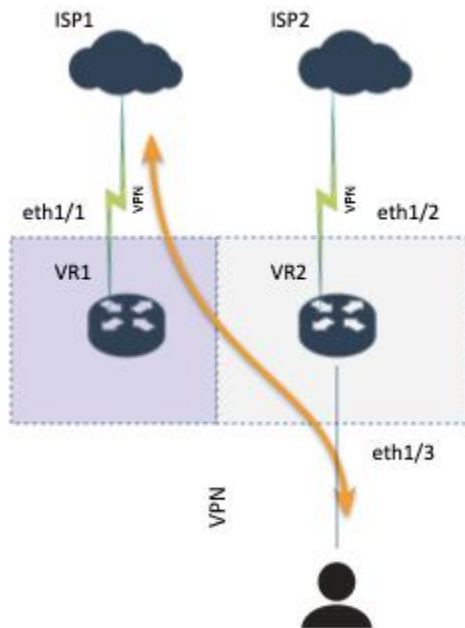
Disable this rule if nexthop/monitor ip is unreachable

IP Address:

Enforce Symmetric Return

| NEXT HOP ADDRESS LIST |
|-----------------------|
| 203.0.113.1           |

Schedule: None



# 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

| <input type="checkbox"/> | INTERFACE   | WEIGHT |
|--------------------------|-------------|--------|
| <input type="checkbox"/> | ethernet1/4 | 50     |
| <input type="checkbox"/> | ethernet1/1 | 100    |

+ Add - Delete

OK

Cancel

## Chapter 5: Services and Operational Modes

### Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

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

Default Route Metric

[Show DHCP Client Runtime Info](#)

## DHCP Server



Interface

Mode

Lease | Options

Ping IP when allocating new IP

Lease  Unlimited  Timeout

Days  Hours  Minutes

| IP POOLS ^               |                   | RESERVED ADDRESS | MAC ADDRESS       | DESCRIPTION |
|--------------------------|-------------------|------------------|-------------------|-------------|
| <input type="checkbox"/> | 192.168.27.128/25 | 192.168.27.4     |                   |             |
|                          |                   | 192.168.27.5     | 64:76:ba:94:f1:22 | laBtop      |

## DHCP Server



Interface

Mode



Lease | Options

Inheritance Source

[Check inheritance source status](#)

Gateway

Subnet Mask

Primary DNS

Secondary DNS

### Custom DHCP options

| <input type="checkbox"/> | NAME | CODE | TYPE | VALUE |
|--------------------------|------|------|------|-------|
|                          |      |      |      |       |

## DHCP Relay



Interface

IPv4

### DHCP SERVER IP ADDRESS

192.168.27.4

IPv6

| DHCP SERVER IPV6 ADDRESS | INTERFACE |
|--------------------------|-----------|
|                          |           |

Specify outgoing interface when using an IPv6 multicast address for your DHCPv6 server

OK

Cancel



## DNS Proxy ?

Enable

Name

Inheritance Source  Check inheritance source status

Primary

Secondary

INTERFACE ^

ethernet1/2

ethernet1/3

+ Add - Delete

DNS Proxy Rules | **Static Entries** | Advanced

| NAME        | CACHEABLE                           | DOMAIN NAME | PRIMARY      | SECONDARY    |
|-------------|-------------------------------------|-------------|--------------|--------------|
| example.com | <input checked="" type="checkbox"/> | example.com | 192.168.27.6 | 192.168.27.7 |

DNS Proxy Rules | **Static Entries** | Advanced

| NAME       | FQDN             | ADDRESS   |
|------------|------------------|-----------|
| mailserver | mail.example.com | 10.0.0.25 |

DNS Proxy Rules | Static Entries | **Advanced**

TCP Queries

Max Pending Requests

UDP Queries Retries

Interval (sec)

Attempts

Cache

Enable TTL

Time to Live (sec)

Cache EDNS Responses

OK Cancel

## Setup ?

Enable HA

Group ID

Description

Mode  Active Passive  Active Active

Enable Config Sync

Peer HA1 IP Address

Backup Peer HA1 IP Address

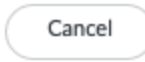
OK Cancel

## Active/Passive Settings



Passive Link State  Shutdown  Auto

Monitor Fail Hold Down Time (min)



## Aggregate Ethernet Interface



Interface Name

Comment

Interface Type

Netflow Profile

Config | IPv4 | IPv6 | **LACP** | Advanced

Enable LACP

Mode  Passive  Active

Transmission Rate  Fast  Slow

Fast Failover

System Priority

Maximum Interfaces

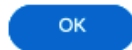
High Availability Options

Enable in HA Passive State

Same System MAC Address For Active-Passive HA

MAC Address

Select system generated MAC or enter a valid MAC



Config | IPv4 | IPv6 | LACP | **Advanced**

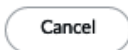
Other Info | ARP Entries | ND Entries | NDP Proxy | **LLDP** | DDNS

Enable LLDP

LLDP Profile

High Availability Options

Enable in HA Passive State



Import HA Key Export HA Key

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

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

## HA Virtual Address ?

Interface: ethernet1/8

IPv4 | IPv6

|                          | ADDRESS       | TYPE             | Floating                            |                   |                   |                       | ARP Load Sharing |           |
|--------------------------|---------------|------------------|-------------------------------------|-------------------|-------------------|-----------------------|------------------|-----------|
|                          |               |                  | BIND TO ACTIVE PRIMARY              | DEVICE 0 PRIORITY | DEVICE 1 PRIORITY | FAILOVER ON LINK DOWN | TYPE             | SEED      |
| <input type="checkbox"/> | 198.51.100.15 | floating         | <input type="checkbox"/>            | 10                | 100               | true                  |                  |           |
| <input type="checkbox"/> | 198.51.100.16 | floating         | <input type="checkbox"/>            | 100               | 10                | true                  |                  |           |
| <input type="checkbox"/> | 198.51.100.17 | floating         | <input checked="" type="checkbox"/> |                   |                   | true                  |                  |           |
| <input type="checkbox"/> | 198.51.100.18 | arp-load-sharing | <input type="checkbox"/>            |                   |                   |                       | ip-modulo        |           |
| <input type="checkbox"/> | 198.51.100.19 | arp-load-sharing | <input type="checkbox"/>            |                   |                   |                       | ip-hash          | 254313245 |

IPv4 ?

IPv4 Address: 198.51.100.15

Type:  Floating  ARP Load Sharing

Floating IP bound to the Active-Primary device

Device 0 Priority: 10

Device 1 Priority: 100

Failover address if link state is down

OK

Cancel

IPv4 ?

IPv4 Address: 198.51.100.18

Type:  Floating  ARP Load Sharing

Device Selection Algorithm:  IP Modulo  IP Hash

OK

Cancel

## NAT Policy Rule ?

General | Original Packet | Translated Packet | **Active/Active HA Binding**

Active/Active HA Binding: primary

primary

both

0

1

### 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

Virtual System

ID 2

Allow forwarding of decrypted content

Name Beta environment

General Resource

Sessions Limit [1 - 262144]

**Policy Limits**

Security Rules [0 - 2500]

NAT Rules [0 - 3000]

Decryption Rules [0 - 250]

QoS Rules [0 - 1000]

Application Override Rules [0 - 250]

Policy Based Forwarding Rules [0 - 500]

Authentication Rules [0 - 1000]

DoS Protection Rules [0 - 1000]

**VPN Limits**

Site to Site VPN Tunnels [0 - 1024]

Concurrent SSL VPN Tunnels [0 - 1024]

**Inter-Vsys User-ID Data Sharing**

Make this vsys a User-ID data hub  
User-ID data on the User-ID hub is available to all other virtual systems

OK Cancel

|                          | Name       | Interfaces                 | Configuration                                  | RIP |
|--------------------------|------------|----------------------------|--|-----|
| <input type="checkbox"/> | default    | ethernet1/1<br>ethernet1/2 | Virtual System: vsys1<br>ECMP status: Disabled |     |
| <input type="checkbox"/> | v2-default | ethernet1/7<br>ethernet1/8 | Virtual System: none<br>ECMP status: Disabled  |     |

| 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   |

**Administrator**

Name: vsys2admin

Authentication Profile: authprofile

Use only client certificate authentication (Web)

Use Public Key Authentication (SSH)

Administrator Type:  Dynamic  Role Based

Virtual system administrator

Virtual System

- Beta environment (vsys2)
  - Superuser
  - Superuser (read-only)
  - Device administrator
  - Device administrator (read-only)
  - Virtual system administrator
  - Virtual system administrator (read-only)

**paloalto** NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

+ Add - Delete

Zones

- GlobalProtect
- Portals
- Gateways
- MDM
- Device Block List
- Clientless Apps
- Clientless App Groups
- SD-WAN Interface Profile

2 items

|                          | Name          | Location                 | Type   | Interfaces / Virtual Systems | Z... P... P... | P... B... P...           | L... S... | User-ID                  |            |                |
|--------------------------|---------------|--------------------------|--------|------------------------------|----------------|--------------------------|-----------|--------------------------|------------|----------------|
|                          |               |                          |        |                              |                |                          |           | E...                     | In... N... | Excl... Net... |
| <input type="checkbox"/> | L3-trust-V2   | Beta environment (vsys2) | layer3 | ethernet1/8                  |                | <input type="checkbox"/> |           | <input type="checkbox"/> | any        | none           |
| <input type="checkbox"/> | L3-untrust-V2 | Beta environment (vsys2) | layer3 | ethernet1/7                  |                | <input type="checkbox"/> |           | <input type="checkbox"/> | any        | n...           |

+ Add - Delete PDF/CSV

vsys2admin | Logout | Last Login Time: 02/13/2020 22:25:22

Tasks | Language

### Admin Role Profile

Name: vsysadminrole

Description:

Role:  Device  Virtual System

Web UI | XML/REST API | Command Line

- Dashboard
- ACC
- Monitor
- Logs
  - Traffic
  - Threat
  - URL Filtering
  - WildFire Sub
  - Data Filtering
  - HIP Match
  - GlobalProtect
  - IP-Tag
  - User-ID
  - Tunnel Inspe
  - Authenticatio

Legend: ✔ Enable ⊘

### Administrator

Name: vsysrole

Authentication Profile: auth

Use only client certificate authentication (Web)

Use Public Key Authentication (SSH)

Administrator Type:  Dynamic  Role Based

Profile: vsysadminrole

Virtual System

- Beta environment (vsys2)

paloalto NETWORKS

Monitor | Policies | Objects | Network

Commit | Config | Search

Virtual System: Beta environment (vsys2)

Manual | Help

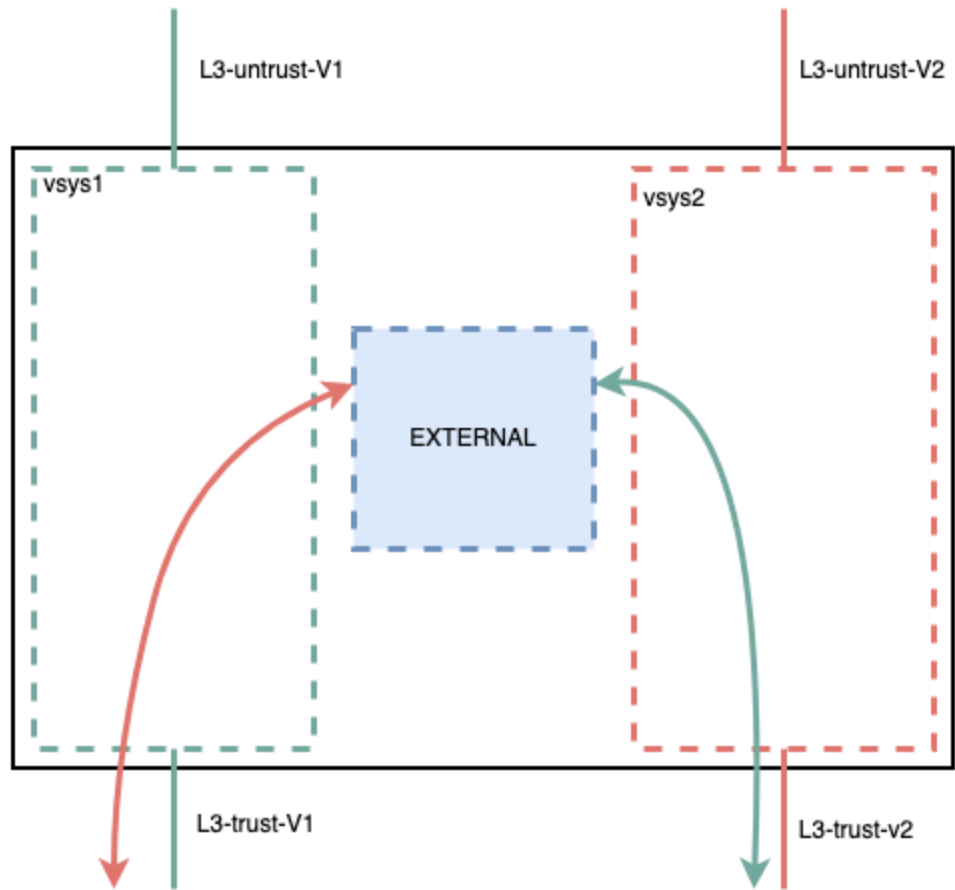
| Receive Time | Type | From Zone | To Zone | Source | Source User |
|--------------|------|-----------|---------|--------|-------------|
|              |      |           |         |        |             |

Resolve hostname  Highlight Policy Actions

20 per page DESC

vsysrole | Logout | Last Login Time: 02/13/2020 22:43:34

Tasks | Language



Device Certificates | Default Trusted Certificate Authorities

| 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... | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 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... | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Forward Trust Certificate   |
| portal                 | Apr 16 21:10:19 2021 GMT | CN = portal.example.com             | C = BE, O = example.co... | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                             |
| captiveportal          | May 1 23:24:32 2021 GMT  | CN = captiveportal.pangurus.com     | C = BE, O = example.co... | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                             |
| gateway                | Jun 24 22:35:47 2021 GMT | CN = gateway.example.com            | C = BE, O = example.co... | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                             |
| webservers             | Jun 24 22:37:12 2021 GMT | C = BE, CN = www.example.com, e...  | C = BE, O = example.co... | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                             |
| firewall               | Jun 24 22:37:35 2021 GMT | CN = firewall.example.com           | C = BE, O = example.co... | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                             |
| untrusted cert         | Jan 20 20:57:29 2021 GMT | CN = DangerWillRobinson, emailA...  | CN = DangerWillRobins...  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Forward Untrust Certificate |



## Certificate Profile



Name

Username Field   Email  Principal Name

User Domain

CA Certificates

| <input type="checkbox"/> | NAME                | DEFAULT OCSP URL         | OCSP VERIFY CERTIFICATE | TEMPLATE NAME/OID |
|--------------------------|---------------------|--------------------------|-------------------------|-------------------|
| <input type="checkbox"/> | client signing cert | https://ocsp.example.com | root signing cert       |                   |

Default OCSP URL (must start with http:// or https://)

Use CRL  CRL Receive Timeout (sec)

Use OCSP  OCSP Receive Timeout (sec)

OCSP takes precedence over CRL

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

## SSL/TLS Service Profile



Name

Certificate

**Protocol Settings**

Min Version

Max Version

## SCEP Configuration



Name

### One Time Password (Challenge)

SCEP Challenge

Server URL

Username

Password

### Configuration

Server URL

CA-IDENT Name

Subject

Subject Alternative Name Type

### Cryptographic Settings

Number of Bits

Digest for CSR

Use as digital signature

Use for key encipherment

CA Certificate Fingerprint

### SCEP Server SSL Authentication

CA Certificate

Client Certificate

## Generate Certificate



Certificate Type  Local  SCEP

Certificate Name

SCEP Profile

Generate

Cancel

OK

Cancel

## Generate Certificate



Certificate Type  Local  SCEP

Certificate Name

Common Name

IP or FQDN to appear on the certificate

Signed By

Certificate Authority

Block Private Key Export

OCSP Responder

### Cryptographic Settings

#### Certificate Attributes

| <input type="checkbox"/> | TYPE   | VALUE                 |
|--------------------------|--|-----------------------|
| <input type="checkbox"/> | Country = "C" from "Subject" field   | BE                    |
| <input type="checkbox"/> | Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailA... | webmaster@example.com |

Generate

Cancel

## Chapter 6: Identifying Users and Controlling Access

**Zone**

Name

Log Setting

Type

INTERFACES ^

- ethernet1/2
- ethernet1/3.20
- ethernet1/4
- vlan

**Zone Protection**

Zone Protection Profile

Enable Packet Buffer Protection

**User Identification ACL**

Enable User Identification

INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

# 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)

Enable Session

Server Session Read Frequency (sec)

## Novell eDirectory Monitoring

Novell eDirectory Query Interval (sec)

## Syslog Listener Settings

Syslog Service Profile

**OK** Cancel

# Palo Alto Networks User ID Agent Setup



Authentication | Server Monitor | Client Probing | Cache | Agent Service | eDirectory | **Syslog**

Syslog Service Port

Enable Syslog Service

## Syslog filters

| Name                               | Type  | User                       | IP                       |
|------------------------------------|-------|----------------------------|--------------------------|
| <input type="checkbox"/> Cisco ISE | Regex | User-Name=([a-zA-Z0-9]\... | Framed-IP-Address=( [... |

Add

## Palo Alto Networks User ID Agent Syslog Parse Profile



Profile Name

Description

Type  Regex  Field

Event Regex

Username Regex

Address Regex

**OK** Cancel

### User-ID Agent

Name:

Add an Agent Using  Serial Number  Host and Port

Host:

Port:

Use as LDAP Proxy

Use for NTLM Authentication

User-ID Collector Name:

User-ID Collector Pre-Shared Key:

Confirm User-ID Collector Pre-Shared Key:

Enabled

HIP Report

Palo Alto Networks Terminal Server Agent

File Help

### Terminal Server Agent

- Configure
- Monitor
- Server Certificate

System Source Port Allocation Range:

System Reserved Source Ports:

---

Listening Port:

Source Port Allocation Range:  -

Reserved Source Ports:

Port Allocation Start Size Per User:

Port Allocation Maximum Size Per User:

Domain Override:

Fail port binding when available ports are used up

Detach agent driver at shutdown

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\administrator | 20000-20399 |            |

Terminal Server Agent

Name:

Host:

Port:

Alternative Hosts

|                          |              |
|--------------------------|--------------|
| <input type="checkbox"/> | Host List ▲  |
| <input type="checkbox"/> | 172.16.25.65 |

Enabled

User Identification Monitored Server

Name:

Description:

Enabled

Type:

Transport Protocol:

Network Address:

---

User Identification Monitored Server

Name:

Description:

Enabled

Type:

Transport Protocol:

Network Address:

---

User Identification Monitored Server

Name:

Description:

Enabled

Type:

Network Address:

Connection Type:  UDP  SSL

Filter

| <input type="checkbox"/>            | SYSLOG PARSE PROFILE                          | EVENT TYPE |
|-------------------------------------|---|------------|
| <input checked="" type="checkbox"/> |   | login      |
| <input type="checkbox"/>            | Aerohive AP v1.0.0                            |            |
| <input type="checkbox"/>            | BlueCoat Log Main Format Proxy Authentication |            |
| <input type="checkbox"/>            | BlueCoat Proxy SG Proxy Log                   |            |
| <input type="checkbox"/>            | BlueCoat Squid Web Proxy Authentication       |            |
| <input type="checkbox"/>            | Cisco ASA Any Connect v1.0.0                  |            |
| <input type="checkbox"/>            | Cisco ASA IPsec v1.0.0                        |            |
| <input type="checkbox"/>            | Citrix Access Gateway v1.0.0                  |            |
| <input type="checkbox"/>            | Juniper IC v1.0.0                             |            |
| <input type="checkbox"/>            | Juniper SA Net Connect v1.0.0                 |            |
| <input type="checkbox"/>            | Squid Web Proxy Authentication                |            |
| <input type="checkbox"/>            | SSH Authentication                            |            |
| <input type="checkbox"/>            | Unix PAM Authentication                       |            |

Default Domain Name:

]

## Palo Alto Networks User-ID Agent Setup



**Server Monitor Account** | Server Monitor | Client Probing | Cache | Syslog Filters | Ignore User List

Username

Domain's DNS Name

Password

Confirm Password

Kerberos Server Profile

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)

Enable Session

Server Session Read Frequency (sec)

### Novell eDirectory Monitoring

Novell eDirectory Query Interval (sec)

### Syslog Listener Settings

Syslog Service Profile

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

NetBIOS domain name for NTLM domain

Admin User Name

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 → ×

| <input type="checkbox"/> | SYSLOG PARSE PROFILE          | TYPE             | USER   | IP   |
|--------------------------|-------------------------------|------------------|--|--|
| <input type="checkbox"/> | Citrix Access Gateway v1.0.0  | regex-identifier | User ([a-zA-Z0-9\_]+)  | Nat_ip ([A-F0-9a-f.]+)                                 |
| <input type="checkbox"/> | Aerohive AP v1.0.0            | regex-identifier | username ([a-zA-Z0-9\_]+)                                    | ip ([A-F0-9a-f.]+)                                     |
| <input type="checkbox"/> | 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.]+)) |
| <input type="checkbox"/> | 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.]+)) |
| <input type="checkbox"/> | Juniper SA Net Connect v1.0.0 | regex-identifier | (?:\ \\,)\s([a-zA-Z0-9\_]+)                                  | IP ([A-F0-9a-f.]+)                                     |
| <input type="checkbox"/> | Juniper IC v1.0.0             | regex-identifier | user=([a-zA-Z0-9\_]+)  | src=([A-F0-9a-f.]+)                                    |
| <input type="checkbox"/> | 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 |

OK

Cancel

## LDAP Server Profile



Profile Name

Administrator Use Only

### Server List

| NAME     | LDAP SERVER ^ | PORT |
|----------|---------------|------|
| ADserver | 192.168.27.7  | 636  |

Enter the IP address or FQDN of the LDAP server

### Server Settings

Type

Base DN

Bind DN

Password

Confirm Password

Bind Timeout

Search Timeout

Retry Interval

Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

OK

Cancel

## Group Mapping



Name

### Server Profile

User and Group Attributes

Group Include List

Custom Group

Server Profile

Update Interval

### Domain Setting

User Domain

### Group Objects

Search Filter

Object Class

### User Objects

Search Filter

Object Class

Enabled

Fetch list of managed devices

OK

Cancel










## Group Mapping ?

Name





[Server Profile](#) | 
 [User and Group Attributes](#) | 
 **[Group Include List](#)** | 
 [Custom Group](#)

**Available Groups**

→ ×




-  cn=key admins
-  cn=labusers
-  cn=pangurus
-  cn=protected users
-  cn=ras and ias servers
-  cn=read-only domain controllers
-  cn=schema admins
-  **cn=supervpnusers**
-  cn=vpnusers

**Included Groups**

-  pangurus\pangurus
-  pangurus\vpnusers
-  pangurus\clientless
-  panguruss\admins

+  
-

OK
Cancel

|    | NAME      | TAGS <span style="font-size: small;">v</span> | TYPE      | Source   |         |  | Destination  |   |
|----|-----------|---|-----------|--|---------|--|--|---|
|    |           |   |           | ZONE   | ADDRESS | USER   | ZONE   | ADDRESS   |
| 11 | hr access | users   | universal | <span style="background-color: #70ad47; color: white; padding: 2px;">Trust-L3</span> | any     |  smokeypines\pangurus | <span style="background-color: #e69d00; color: white; padding: 2px;">DMZ-L3</span>       |  hr-server |
| 12 | all users | users   | universal | <span style="background-color: #70ad47; color: white; padding: 2px;">Trust-L3</span> | any     |  known-user           | <span style="background-color: #c00000; color: white; padding: 2px;">Untrust-L...</span> | any   |

## Authentication Profile



Name

**Authentication** | Factors | Advanced

Type

Server Profile

Login Attribute

Password Expiry Warning

Number of days prior to warning a user about password expiry.

User Domain

Username Modifier

### Single Sign On

Kerberos Realm

Kerberos Keytab  [X Import](#)

OK

Cancel

## Authentication Profile



Name

Authentication | Factors | **Advanced**

### Allow List

- ALLOW LIST ^
  - all
- [+ Add](#) [- Delete](#)

### Account Lockout

Failed Attempts

Lockout Time (min)

OK

Cancel

## Generate Certificate



Certificate Type  Local  SCEP

Certificate Name

Common Name

IP or FQDN to appear on the certificate

Signed By

Certificate Authority

Block Private Key Export

OCSP Responder

### ^ Cryptographic Settings

Algorithm

Number of Bits

Digest

Expiration (days)

### Certificate Attributes

| <input type="checkbox"/> | TYPE | VALUE |
|--------------------------|------|-------|
| + Add - Delete           |      |       |

Generate

Cancel

## SSL/TLS Service Profile



Name

Certificate

### Protocol Settings

Min Version

Max Version

OK

Cancel

# Interface Management Profile



Name

### 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

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



# Captive Portal



Enable Captive Portal

Idle Timer (min)

Timer (min)

GlobalProtect Network Port for Inbound Authentication Prompts (UDP)

SSL/TLS Service Profile

Authentication Profile

Mode  Transparent  Redirect

**Session Cookie**

Enable

Timeout (min)

Roaming

Redirect Host

**Certificate Authentication**

Certificate Profile

**NTLM Authentication**

Attempts

Timeout (sec)

Reversion Time (sec)

|   | NAME          | TAGS | Source   |         |      |        | Destination  |         |        | SERVICE                       | AUTHENTICATION ENFORCEMENT | LOG SETTINGS            |
|---|---------------|------|----------|---------|------|--------|--------------|---------|--------|-------------------------------|----------------------------|-------------------------|
|   |               |      | ZONE     | ADDRESS | USER | DEVICE | ZONE         | ADDRESS | DEVICE |                               |                            |                         |
| 1 | CaptivePortal | none | Trust-L3 | any     | any  | any    | Untrust-L... | any     | any    | service-http<br>service-https | default-browser-challenge  | Log Forwarding: default |

**Authentication Policy Rule**

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

Authentication Enforcement

Timeout (min)

**Log Settings**

Log Authentication Timeouts

Log Forwarding

# URL Filtering Profile



Name

Description

**Categories** | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Dynamic Classification

73 items → ×

| <input type="checkbox"/> | CATEGORY               | SITE ACCESS | USER CREDENTIAL SUBMISSION ▾ |
|--------------------------|------------------------|-------------|------------------------------|
| ▾                        | Pre-defined Categories |             |                              |
| <input type="checkbox"/> | unknown                | continue    | continue                     |
| <input type="checkbox"/> | web-advertisements     | continue    | continue                     |
| <input type="checkbox"/> | adult                  | block       | block                        |
| <input type="checkbox"/> | command-and-control    | block       | block                        |
| <input type="checkbox"/> | copyright-infringement | block       | block                        |
| <input type="checkbox"/> | extremism              | block       | block                        |

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

[Check URL Category](#)

| ACC                       | MONITOR             | POLICIE |
|---------------------------|---------------------|---------|
|                           |                     |         |
|                           |                     |         |
| CATEGORY                  | CREDENTIAL DETECTED |         |
| private-ip-addresses      | Columns >           |         |
| private-ip-addresses      | Adjust Columns      |         |
| private-ip-addresses      | no                  |         |
| 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

**New virtual machine**

1 Select creation type  
2 Select OVF and VMDK files  
3 Select storage  
4 License agreements  
5 Deployment options  
6 Additional settings  
7 Ready to complete

### Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine  
**Deploy a virtual machine from an OVF or OVA file**  
Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

---

**New virtual machine - panorama**

1 Select creation type  
**2 Select OVF and VMDK files**  
3 Select storage  
4 License agreements  
5 Deployment options  
6 Additional settings  
7 Ready to complete

### Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.  
panorama

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× Panorama-ESX-9.0.1.ova

---

**New virtual machine - panorama**

1 Select creation type  
2 Select OVF and VMDK files  
3 Select storage  
4 Deployment options  
**5 Ready to complete**

### Ready to complete

Review your settings selection before finishing the wizard

|                   |                               |
|-------------------|-------------------------------|
| Product           | Panorama-9.0.1                |
| VM Name           | panorama                      |
| Disks             | Panorama-ESX-9.0.1-disk1.vmdk |
| Datastore         | VMLab-RAID5                   |
| Provisioning type | Thin                          |
| Network mappings  | VM Network: LAB01             |
| Guest OS Name     | Unknown                       |

Do not refresh your browser while this VM is being deployed.

vmware

Back Next Finish Cancel

## General Settings



Hostname

Domain

Login Banner

Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile

Time Zone

Locale

Date

Time

Latitude

Longitude

Automatically Acquire Commit Lock

Serial Number

URL Filtering Database

GTP Security

SCTP Security

OK

Cancel

## Secure Communication Settings



### Secure Client Communication

#### Custom Certificate Settings

Certificate Type

#### Customize Secure Server Communication

SSL/TLS Service Profile

Certificate Profile

Authorization List

| <input type="checkbox"/> | Identifier | Type        | Value |
|--------------------------|------------|-------------|-------|
| <input type="checkbox"/> | subject    | common-name |       |
| <input type="checkbox"/> | subject    | common-name |       |
| <input type="checkbox"/> | subject    | common-name |       |

Allow Custom Certificate Only

Authorize Clients Based on Serial Number

Check Authorization List

Disconnect Wait Time (min)

OK

Cancel

## Secure Communication Settings



### Secure Client Communication

#### Custom Certificate Settings

Certificate Type

Certificate

Certificate Profile

#### 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

| <input type="checkbox"/> | Permitted IP Addresses | Description |
|--------------------------|------------------------|-------------|
| <input type="checkbox"/> | 192.168.27.0/24        | mgmt net    |

 Add  Delete

OK Cancel

### Collector

General Disks

Collector S/N 001 [icon]

Inbound Certificate for Secure Syslog None [dropdown]

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 001 [icon]

Collector Name externalM500

Inbound Certificate for Secure Syslog None [dropdown]

Certificate for Secure Syslog None [dropdown]

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 [dropdown]

Latitude [-90.0 - 90.0]

Longitude [-180.0 - 180.0]

Primary NTP Server

NTP Server Address time.nist.gov

Authentication Type None [dropdown]

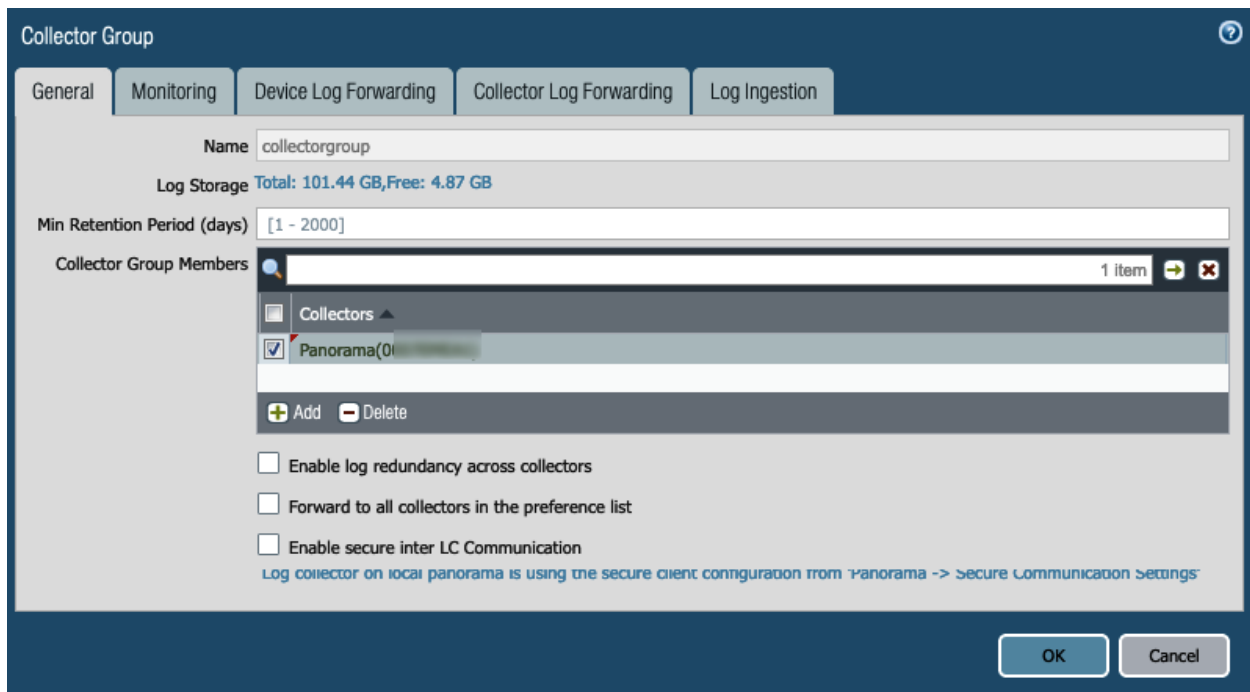
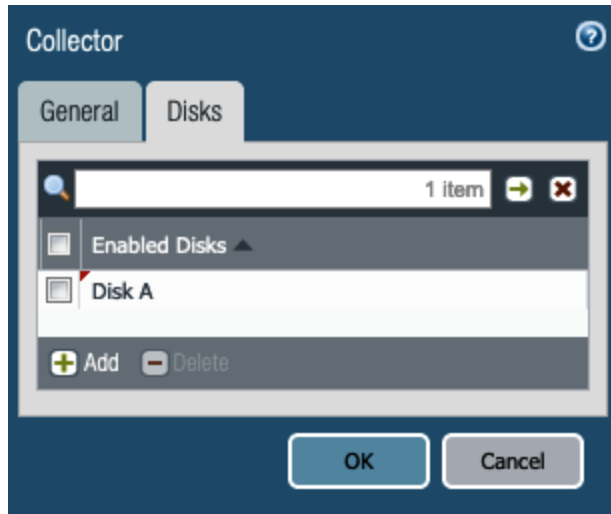
Secondary NTP Server

NTP Server Address time.belnet.be

Authentication Type None [dropdown]

Warning: Only MGT interface is supported for all functions on collectors running PAN-OS 6.0 or earlier.

OK Cancel



The screenshot shows the 'Add Device' dialog box in the Palo Alto Networks management console. The background interface includes a left-hand navigation menu with categories like Setup, High Availability, Config Audit, Managed WildFire Clusters, Password Profiles, Administrators, Admin Roles, Access Domain, Authentication Profile, Authentication Sequence, User Identification, Managed Devices, Summary, Health, Troubleshooting, Templates, Device Groups, and Managed Collectors. The main content area displays a table with the following data:

| Device Name   |
|---------------|
| Reaper-PA-220 |

The 'Add Device' dialog box contains the following elements:

- Title:** Add Device
- Serial:** A text input field containing '000'.
- Instructions:** "Please enter one or more device serial numbers. Enter one entry per row, separating the rows with a newline."
- Associate Devices:** An unchecked checkbox.
- Buttons:** 'Import', 'OK', and 'Cancel'.

The screenshot displays two configuration sections:

### 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 |
|--|----------------|---------|------|
| ▼ <input type="checkbox"/> [blurred]-PA (2/2 Devices Connected): Shared > [blurred]                          |                |         |      |
| <input type="checkbox"/> [blurred]-PA1   |                | PA-3260 |      |
| <input type="checkbox"/> [blurred]-PA2   |                |         |      |
| ▼ <input type="checkbox"/> [blurred]-PA (2/2 Devices Connected): Shared > [blurred]                          |                |         |      |
| <input type="checkbox"/> [blurred]-PA2   |                | PA-3260 |      |
| <input type="checkbox"/> [blurred]-PA1   |                |         |      |
| ▼ <input type="checkbox"/> [blurred] (1/1 Devices Connected): Shared > [blurred]                             |                |         |      |
| + Add   + Reassociate   - Delete   Tag   Install <input checked="" type="checkbox"/> 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      |                              |

Dashboard   ACC   Monitor   Policies   **Objects**   Network   Device   Panorama

Context: Panorama   Device Group: **EMEA**

**Address**

Name: HQ-TerminalServers

Shared  
 Disable override

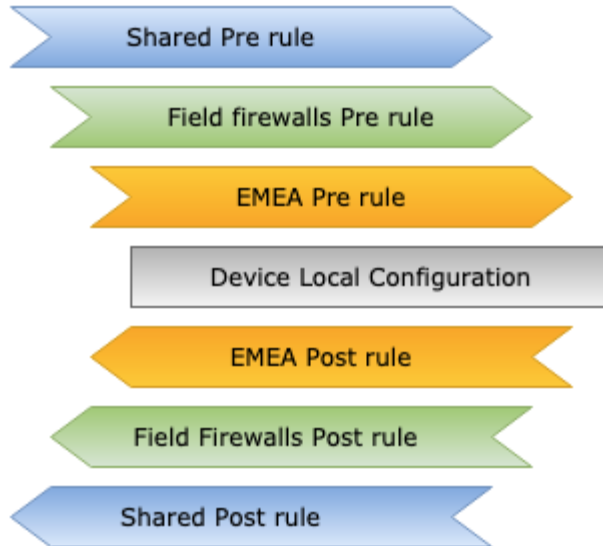
Description: \_\_\_\_\_

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: \_\_\_\_\_





pano Palo Alto NETWORKS

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

| 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

| 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

| Name                        | Location | Tags   | Type      | Zone | Address   |
|-----------------------------|----------|--------|-----------|------|-----------|
| 1 shared pre - admin access | Shared   | SHARED | universal | WAN  | HQ-admins |

admin | Logout | Last Login Time: 03/16/2020

**Log Forwarding Profile**

Name: default

Shared

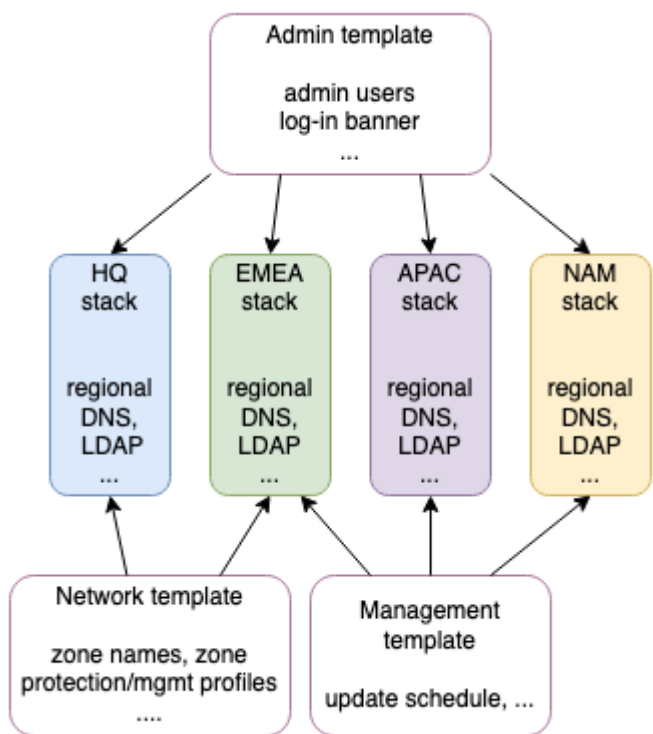
Enable enhanced application logging to Logging Service (including traffic and url logs)

Description:

| 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 Service |                  |

+ Add - Delete Clone

OK Cancel



**paloalto NETWORKS**

Dashboard ACC Monitor Policies Objects **Network** Device Panorama

Context: Panorama

Template: Network Template

View by: Device Mode: Multi VSYS; Normal Mode; VPN Enabled

Virtual Systems:  Multi VSYS

Operational Mode:  Normal  FIPS  Common Criteria

VPN Mode:  Disable VPN

| Management Profile | IP Address | Virtual |  |          |            |
|--------------------|------------|---------|--|----------|------------|
|                    | none       | VR1     |  |          |            |
| ping-resp          | none       | VR1     |  | Untagged | none vsys1 |
| ping-resp          | none       | VR1     |  | Untagged | none vsys1 |
|                    | none       | VR1     |  | Untagged | none vsys1 |

**Push Scope Selection**

Device Groups Templates Collector Groups WildFire Appliances and Clusters

Filters: 15 items

- Commit State
  - Out of Sync (15)
- Device State
  - Connected (12)
  - Disconnected (3)
- Platforms
  - PA-220 (5)

| Name  | Last Commit State | HA Status                                     | Preview Changes |
|---|-------------------|---|-----------------|
| <input checked="" type="checkbox"/> BELGIUM |                   |   |                 |
| <input checked="" type="checkbox"/> ANT-PA  |                   |   |                 |
| <input checked="" type="checkbox"/> PA1     | Out of Sync       | <span style="color: green;">●</span> Active   |                 |
| <input checked="" type="checkbox"/> PA2     | Out of Sync       | <span style="color: orange;">●</span> Passive |                 |
| <input checked="" type="checkbox"/> 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: Panorama

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

## Logging and Reporting Settings



Log Storage | Log Export and Reporting | Pre-Defined Reports | Log Collector Status

### Log Storage Quota

|                         | Quota(%)                         | Quota(GB/MB) | Max Days                                |                               |                                      |           |   |
|-------------------------|----------------------------------|--------------|---|-------------------------------|--------------------------------------|-----------|---|
| Traffic                 | <input type="text" value="27"/>  | 1.21 GB      | <input type="text" value="[1 - 2000]"/> | Traffic Summary               | <input type="text" value="3.5"/>     | 161.25 MB | <input type="text" value="[1 - 2000]"/> |
| Threat                  | <input type="text" value="11"/>  | 506.77 MB    | <input type="text" value="[1 - 2000]"/> | Threat Summary                | <input type="text" value="2"/>       | 92.14 MB  | <input type="text" value="[1 - 2000]"/> |
| Config                  | <input type="text" value="4"/>   | 184.28 MB    | <input type="text" value="[1 - 2000]"/> | GTP and Tunnel Summary        | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| System                  | <input type="text" value="4"/>   | 184.28 MB    | <input type="text" value="[1 - 2000]"/> | URL Summary                   | <input type="text" value="2"/>       | 92.14 MB  | <input type="text" value="[1 - 2000]"/> |
| Alarm                   | <input type="text" value="3"/>   | 138.21 MB    | <input type="text" value="[1 - 2000]"/> | Decryption Summary            | <input type="text" value="DESUM_1"/> | 0.00 MB   | <input type="text" value="[1 - 2000]"/> |
| App Stats               | <input type="text" value="4"/>   | 184.28 MB    | <input type="text" value="[1 - 2000]"/> | Hourly Traffic Summary        | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| HIP Match               | <input type="text" value="3"/>   | 138.21 MB    | <input type="text" value="[1 - 2000]"/> | Hourly Threat Summary         | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| GlobalProtect           | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Hourly GTP and Tunnel Summary | <input type="text" value="1"/>       | 46.07 MB  | <input type="text" value="[1 - 2000]"/> |
| App Pcaps               | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Hourly URL Summary            | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| Extended Threat Pcaps   | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Hourly Decryption Summary     | <input type="text" value="0"/>       | 0.00 MB   | <input type="text" value="[1 - 2000]"/> |
| Debug Filter Pcaps      | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Daily Traffic Summary         | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| IP-Tag                  | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Daily Threat Summary          | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| User-ID                 | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Daily GTP and Tunnel Summary  | <input type="text" value="1"/>       | 46.07 MB  | <input type="text" value="[1 - 2000]"/> |
| HIP Reports             | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Daily URL Summary             | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| Data Filtering Captures | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Daily Decryption Summary      | <input type="text" value="0"/>       | 0.00 MB   | <input type="text" value="[1 - 2000]"/> |
| GTP and Tunnel          | <input type="text" value="2"/>   | 92.14 MB     | <input type="text" value="[1 - 2000]"/> | Weekly Traffic Summary        | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| Authentication          | <input type="text" value="1.5"/> | 69.11 MB     | <input type="text" value="[1 - 2000]"/> | Weekly Threat Summary         | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
| Decryption              | <input type="text" value="1"/>   | 46.07 MB     | <input type="text" value="[1 - 2000]"/> | Weekly GTP and Tunnel Summary | <input type="text" value="1"/>       | 46.07 MB  | <input type="text" value="[1 - 2000]"/> |
|                         |                                  |              |   | Weekly URL Summary            | <input type="text" value="1.5"/>     | 69.11 MB  | <input type="text" value="[1 - 2000]"/> |
|                         |                                  |              |   | Weekly Decryption Summary     | <input type="text" value="0"/>       | 0.00 MB   | <input type="text" value="[1 - 2000]"/> |

Total Allocated: 98% (4.41 GB)  
 Unallocated: 2% (92.14 MB)  
 Max: 4.50 GB  
 Core Files: 0 MB

[Restore Defaults](#)

Warning: Deletion of logs based on time period may take a long time and during this time the max sustainable log rate will be degraded

Collector Group ?

General Monitoring Device Log Forwarding **Collector Log Forwarding** Log Ingestion

**Log Forwarding Preferences**

2 items ➔ ✕

| Devices   | Collectors               |
|---|--------------------------|
| <input type="checkbox"/> 012001000001<br>012001000002 | Collector1<br>Collector2 |
| <input type="checkbox"/> 012001000003<br>012001000004 | Collector2<br>Collector1 |

+ Add - Delete

OK Cancel

Collector Group ?

General Monitoring Device Log Forwarding **Collector Log Forwarding** Log Ingestion

**Log Forwarding Preferences**

2 items ➔ ✕

| Devices   | Collectors               |
|---|--------------------------|
| <input type="checkbox"/> 012001000001<br>012001000002<br>012001000003<br>012001000004 | Collector1<br>Collector2 |

+ Add - Delete

OK Cancel

### Collector Group

General | Monitoring | Device Log Forwarding | **Collector Log Forwarding** | Log Ingestion

#### Log Forwarding Preferences

2 items

| Devices  | Collectors |
|--|------------|
| <input type="checkbox"/> 012001000001<br><input type="checkbox"/> 012001000002 | Collector1 |
| <input type="checkbox"/> 012001000003<br><input type="checkbox"/> 012001000004 | Collector2 |

+ Add - Delete

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:

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

Version  V2c  V3

| NAME  | SNMP MANAGER  | USER     | ENGINEID | AUTH PASSWORD | PRIV PASSWORD |
|-------|---------------|----------|----------|---------------|---------------|
| cacti | 192.168.27.13 | cactipan |          | *****         | *****         |

Enter the IP address or FQDN of the SNMP Manager

## System

| <input type="checkbox"/> | NAME             | DESCRIPTION  | FILTER                 | PANORAMA                            | SNMP TRAP | EMAIL         | SYSLOG | HTTP |
|--------------------------|------------------|--------------|------------------------|-------------------------------------|-----------|---------------|--------|------|
| <input type="checkbox"/> | logs-to-panorama |              | (severity geq medium)  | <input checked="" type="checkbox"/> |           |               |        |      |
| <input type="checkbox"/> | alert-OpSecTeam  | failed login | (eventid eq auth-fail) | <input type="checkbox"/>            |           | SecTeam-email | splunk |      |

## Create Filter



**Create Filter** | [View Filtered Logs](#)

| Connector | Attribute      | Operator  | Value     |
|-----------|----------------|-----------|-----------|
| and       | Description    | equal     | auth-fail |
| or        | Event          | not equal |           |
|           | Object         |           |           |
|           | Receive Time   |           |           |
|           | Severity       |           |           |
|           | Time Generated |           |           |
|           | Type           |           |           |

Negate



## Log Forwarding Profile



Name

Description

5 items → ×

| <input type="checkbox"/> | NAME                 | LOG TYPE | FILTER  | FORWARD METHOD   | BUILT-IN ACTIONS ^ |
|--------------------------|----------------------|----------|---|--|--------------------|
| <input type="checkbox"/> | Threat-to-Panorama   | threat   | All Logs  | • Panorama/Logging Service                                   |                    |
| <input type="checkbox"/> | Traffic-to-Panorama  | traffic  | All Logs  | • Panorama/Logging Service                                   |                    |
| <input type="checkbox"/> | URL-to-panorama      | url      | All Logs  | • Panorama/Logging Service                                   |                    |
| <input type="checkbox"/> | WildFire-to-Panorama | wildfire | All Logs  | • Panorama/Logging Service                                   |                    |
| <input type="checkbox"/> | Alert-SecTeam        | threat   | (severity geq high) and (category-of-threatid eq brute-force) | <b>Email</b><br>• SecTeam-email<br><b>SysLog</b><br>• splunk |                    |

+ Add - Delete ↺ Clone

OK

Cancel

## Create Filter



Create Filter

**View Filtered Logs**

(severity geq high) and (category-of-threatid eq brute-force) → × + 📄 ↑ ✕

|   | RECEIVE TIME   | TYPE          | THREAT ID/NAME          | FROM ZONE | TO ZONE | SOURCE ADDRESS | SOURCE USER | SOURCE DYNAMIC ADDRESS |
|---|----------------|---------------|-------------------------|-----------|---------|----------------|-------------|------------------------|
| 🗨 | 06/26 22:08:59 | vulnerability | HTTP Unauthorized Error | LAN       | outside | 192.168.27.105 |             |                        |
| 🗨 | 06/26 22:08:47 | vulnerability | HTTP Unauthorized Error | LAN       | outside | 192.168.27.105 |             |                        |
| 🗨 | 06/26 22:08:30 | vulnerability | HTTP Unauthorized Error | LAN       | outside | 192.168.27.105 |             |                        |
| 🗨 | 06/26 22:07:09 | vulnerability | HTTP Unauthorized Error | LAN       | outside | 192.168.27.105 |             |                        |

⏪ < 1 > ⏩  Resolve hostname  Highlight Policy Actions

Displaying logs 1 - 4 100 per page DESC

OK

Cancel

|                          |                      |                                    |         |                     |                                     |          |        |
|--------------------------|----------------------|------------------------------------|---------|---------------------|-------------------------------------|----------|--------|
| <input type="checkbox"/> | <b>AlertMailTeam</b> | alert mail team on critical events | traffic | All Logs            | <input checked="" type="checkbox"/> |          |        |
|                          |                      |                                    | threat  | All Logs            | <input checked="" type="checkbox"/> |          |        |
|                          |                      |                                    | url     | All Logs            |                                     |          |        |
|                          |                      |                                    | threat  | (severity geq high) |                                     | MailTeam | splunk |
| <input type="checkbox"/> | <b>AlertWebTeam</b>  | alert mail team on critical events | traffic | All Logs            | <input checked="" type="checkbox"/> |          |        |
|                          |                      |                                    | threat  | All Logs            | <input checked="" type="checkbox"/> |          |        |
|                          |                      |                                    | url     | All Logs            |                                     |          |        |
|                          |                      |                                    | threat  | (severity geq high) |                                     | WebTeam  | splunk |

|   | NAME      | Source    |        | Destination |                      | APPLIC...           | SERV... | A... | P... | OPTIONS | Rule Usage |          |       |
|---|-----------|-----------|--------|-------------|----------------------|---------------------|---------|------|------|---------|------------|----------|-------|
|   |           | ZONE      | ADD... | ZONE        | ADDRESS              |                     |         |      |      |         | HIT COUNT  | LAST HIT | FIRST |
| 5 | webfa...  | Untrust-L | any    | DMZ-L3      | webserverfarm-public | ssl                 | ap...   | ✓    |      |         | -          | -        | -     |
| 6 | mailfa... | Untrust-L | any    | DMZ-L3      | mailfarm-public      | imap<br>smtp<br>rel | ap...   | ✓    |      |         |            |          |       |

Log Forwarding Profile setting: AlertWebTeam  
Log Forwarding Profile setting: AlertMailTeam

### Security Policy Rule

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

**Action Setting**

Action: Allow

Send ICMP Unreachable

**Profile Setting**

Profile Type: Group

Group Profile: default

**Log Setting**

Log at Session Start

Log at Session End

Log Forwarding: default

**Other Settings**

Schedule: None

QoS Marking: None

Disable Server Response Inspection

OK Cancel

### Logging and Reporting Settings

Log Storage | Log Export and Reporting | **Pre-Defined Reports** | Log Collector Status

**Pre-Defined Reports**

|  |  |  |  |
|--|--|--|--|
| <p><b>Application Reports</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Applications</li> <li><input checked="" type="checkbox"/> Application Categories</li> <li><input checked="" type="checkbox"/> Technology Categories</li> <li><input checked="" type="checkbox"/> HTTP Applications</li> <li><input checked="" type="checkbox"/> Denied Applications</li> <li><input checked="" type="checkbox"/> Risk Trend</li> <li><input checked="" type="checkbox"/> Bandwidth Trend</li> <li><input checked="" type="checkbox"/> SaaS Application Usage</li> </ul> | <p><b>Traffic Reports</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Security Rules</li> <li><input checked="" type="checkbox"/> Sources</li> <li><input checked="" type="checkbox"/> Source Countries</li> <li><input checked="" type="checkbox"/> Destinations</li> <li><input checked="" type="checkbox"/> Destination Countries</li> <li><input checked="" type="checkbox"/> Connections</li> <li><input checked="" type="checkbox"/> Source Zones</li> <li><input checked="" type="checkbox"/> Destination Zones</li> <li><input checked="" type="checkbox"/> Ingress Interfaces</li> <li><input checked="" type="checkbox"/> Egress Interfaces</li> <li><input checked="" type="checkbox"/> Denied Sources</li> <li><input checked="" type="checkbox"/> Denied Destinations</li> <li><input checked="" type="checkbox"/> Unknown TCP Sessions</li> </ul> | <p><b>Threat Reports</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Threats</li> <li><input checked="" type="checkbox"/> Threat Trend</li> <li><input checked="" type="checkbox"/> Attacker Sources</li> <li><input checked="" type="checkbox"/> Attacker Destinations</li> <li><input checked="" type="checkbox"/> Attackers By Source Countries</li> <li><input checked="" type="checkbox"/> Attackers By Destination Countries</li> <li><input checked="" type="checkbox"/> Victim Sources</li> <li><input checked="" type="checkbox"/> Victim Destinations</li> <li><input checked="" type="checkbox"/> Victims By Source Countries</li> <li><input checked="" type="checkbox"/> Victims By Destination Countries</li> <li><input checked="" type="checkbox"/> Viruses</li> <li><input checked="" type="checkbox"/> Spyware</li> </ul> | <p><b>URL Filtering Reports</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> URL Categories</li> <li><input checked="" type="checkbox"/> URL Users</li> <li><input checked="" type="checkbox"/> URL User Behavior</li> <li><input checked="" type="checkbox"/> Web Sites</li> <li><input checked="" type="checkbox"/> Blocked Categories</li> <li><input checked="" type="checkbox"/> Blocked Users</li> <li><input checked="" type="checkbox"/> Blocked User Behavior</li> <li><input checked="" type="checkbox"/> Blocked Sites</li> <li><input checked="" type="checkbox"/> Credential Post Detected</li> </ul> |
|--|--|--|--|

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 | <a href="#">networking</a>       | 272.1k   | 22.0G  |  |
| 2 | <a href="#">business-systems</a> | 24.6k    | 446.4M |  |
| 3 | <a href="#">general-internet</a> | 16.6k    | 664.1M |  |
| 4 | <a href="#">media</a>            | 16.2k    | 30.8G  |  |
| 5 | <a href="#">collaboration</a>    |          | 572.8M |  |
| 6 | <a href="#">unknown</a>          |          |        |  |

| June 2020 |    |    |    |    |    |    |
|-----------|----|----|----|----|----|----|
| S         | M  | T  | W  | T  | F  | S  |
| 31        | 1  | 2  | 3  | 4  | 5  | 6  |
|           | 8  | 9  | 10 | 11 | 12 | 13 |
| 14        | 15 | 16 | 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 |

Export to PDF    Export to CSV    Export to XML

3. Click one of the entries for more details

1. Select the report

2. Select the date

**Custom Report** ? ☰

**Report Setting**

Load Template    Run Now

|   |   |  |  |
|---|---|--|--|
| Name  | <input type="text" value="top-destinations"/> | Available Columns  | Selected Columns                                     |
| Description                                   | <input type="text" value="Traffic Reports"/>  | Action   | Destination Address                                  |
| Database                                      | Traffic Summary                               | App Category   | <input checked="" type="checkbox"/> Destination User |
| <input checked="" type="checkbox"/> Scheduled |   | App Container  | <input type="checkbox"/> Bytes                       |
| Time Frame                                    | Last Calendar Week                            | App Sub Category   | Sessions   |
| Sort By                                       | Sessions                                      | App Technology   |  |
| Group By                                      | Application                                   | <input type="checkbox"/> Top <input type="checkbox"/> Up <input type="checkbox"/> Down <input type="checkbox"/> Bottom |  |
|   | Top 50  |  |  |
|   | 10 Groups                                     |  |  |

**Query Builder**

Please type (or) add a filter using the filter builder Filter Builder

## Custom Report



### Report Setting

Load Template → Run Now

|   |   |                   |   |
|---|---|-------------------|---|
| Name  | <input type="text" value="Threats per Week"/>   | Available Columns | Selected Columns                        |
| Description                                   | <input type="text"/>                            | App Category      | Action                                  |
| Database                                      | <input type="text" value="Threat Summary"/>     | App Container     | <input type="checkbox"/> Severity       |
| <input checked="" type="checkbox"/> Scheduled |   | App Sub Category  | <input type="checkbox"/> Threat ID/Name |
| Time Frame                                    | <input type="text" value="Last Calendar Week"/> | App Technology    | Source Address                          |
| Sort By                                       | <input type="text" value="Count"/>              | Application       | Source User                             |
| Group By                                      | <input type="text" value="Application"/>        |                   |   |
|   | <input type="text" value="Top 10"/>             |                   |   |
|   | <input type="text" value="10 Groups"/>          |                   |   |

### Query Builder

(severity geq high)

[Filter Builder](#)



Cancel

## PDF Summary Report



Name

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

Title Page

Title

- 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

- Report Group
  - trends
  - Threats per Week
  - top-destinations

Add >>  
<< Remove

## Email Scheduler ?

Name

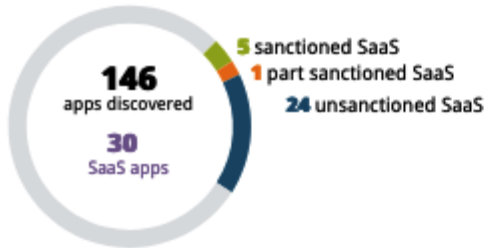
PDF Report or Report Group

Email Profile

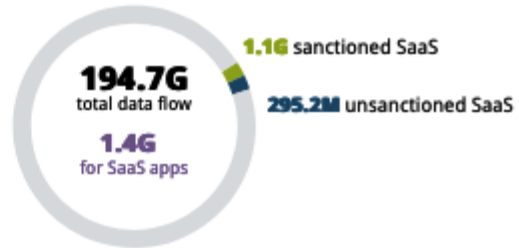
Recurrence

Override Email Addresses

### Applications



### Data Transferred



### Users



Global Filters

- Action
- Address
- Application
- Data Type
- Destination
- File
- GlobalProtect
- Interface
- Rule
- Source
- Threat
- Tunnel
- URL Filtering
- User

spyware 1.15k

| 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 |       |           | ability       | 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  | vulnerability | code-execution  | 4     |
| others                              |       | others    | others        |                 | 10    |

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

- 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

| Threat Name                   | ID    | Severity | Threat Type   | Threat Category | Count |
|-------------------------------|-------|----------|---------------|-----------------|-------|
| Microsoft Windows HTTP.sys... | 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 x GlobalPro

bytes sessions threats content URLs users

| 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 x GlobalProtect Activity rule usage x +

### Source IP Activity

bytes sessions threats content URLs

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 IP Activity

bytes sessions threats content URLs

4.00G

2.00G

0

12:00 13:15 14:30 15:45 17:00 18:15 19:30 20:45

bytes\_sent bytes\_received

| 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       |
| ipv4_1.mce0.c014.l        | 29     | 0        | 0       | 0       |
| ipv4_1.mce0.c012.l        | 22     | 0        | 0       | 0       |
| ipv4_1.mce0.c009.bru00... | 588.8M | 17       | 0       | 0       |



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

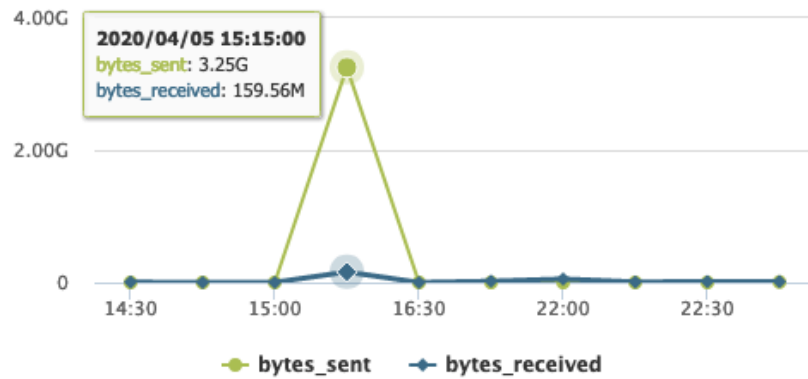
Risk  Sanctioned State

Show system events

Network Activity Threat Activity Blocked Activity Tunnel Activity Dest ip x GlobalProt

bytes  sessions  threats  content  URLs  users

Home

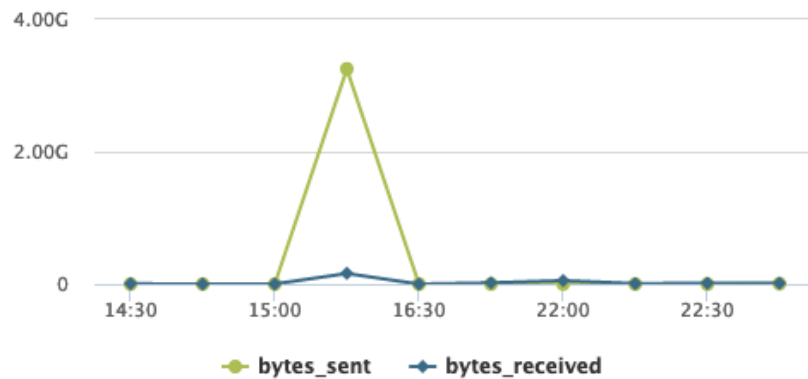


| Application | Risk | Bytes | Sessions | Threats | Content | URLs | Users |
|-------------|------|-------|----------|---------|---------|------|-------|
| ssl         | 4    | 3.5G  | 170      | 0       | 0       | 0    | 1     |
| non-syn-tcp | 1    | 851   | 4        | 0       | 0       | 0    | 1     |
| ping        | 2    | 588   | 2        | 0       | 0       | 0    | 1     |

Source IP Activity

bytes  sessions  threats  content  URLs

Home



| Source Address | Bytes | Sessions | Threats | Content | URLs | Apps |
|----------------|-------|----------|---------|---------|------|------|
| 192.168.27.253 | 3.5G  | 176      | 0       | 0       | 0    | 3    |

Search: (port.dst eq 443) and ((app eq facebook-base) or (app eq facebook-video))

| RECEIVE TIME | TYPE | FROM ZONE | TO ZONE | SOURCE | DESTINATION | TO PORT | APPLICATION | ACTION |
|--------------|------|-----------|---------|--------|-------------|---------|-------------|--------|
|--------------|------|-----------|---------|--------|-------------|---------|-------------|--------|

### Add Log Filter

(port.dst eq 443) and ((app eq facebook-base) or (app eq facebook-video))

| Connector | Attribute                  | Operator  | Value      |
|-----------|----------------------------|-----------|------------|
| and       | Action                     | equal     | allow      |
| or        | Action Source              | not equal | deny       |
|           | Address                    |           | drop       |
|           | App Flap Count             |           | drop-icmp  |
|           | Application                |           | RST client |
|           | Application Characteristic |           | RST server |

Negate

Buttons: 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   | Source  | Destination  |
|---|---|--|
| Session ID 56342<br>Action allow<br>Action Source from-policy<br>Host ID<br>Application web-browsing<br>Rule out-web<br>Rule UUID 315625b1-8ff6-435f-8ad9-35304bd9c3b4<br>Session End Reason threat<br>Category unknown | Source User<br>Source 192.168.27.105<br>Source DAG<br>Country home<br>Port 54137<br>Zone LAN<br>Interface ethernet1/3<br>X-Forwarded-For IP 0.0.0.0 | Destination User<br>Destination [REDACTED]<br>Destination DAG<br>Country Netherlands<br>Port 8123<br>Zone outside<br>Interface ethernet1/1 |

Flags

| PCAP | RECEIVE TIME        | TYPE       | APPLICAT...  | ACTION | RULE    | RULE UUID | BY... | SEVERI...   | CATEG... | URL CATEG... LIST | VERDI... | URL | FILE NAME  | BYTES  |
|------|---------------------|------------|--------------|--------|---------|-----------|-------|-------------|----------|-------------------|----------|-----|------------|--------|
|      | 2020/06/26 22:08:59 | vulnera... | web-browsing | drop   | out-web | 31562...  |       | informat... | unkno... |                   |          |     | [REDACTED] | 166.9k |
|      | 2020/06/26 22:08:55 | url        | web-browsing | alert  | out-web | 31562...  |       | informat... | unkno... | medium-risk,un... |          |     | [REDACTED] | 9.4k   |
|      | 2020/06/26 22:10:48 | end        | web-browsing | allow  | out-web | 31562...  | 10... |             | unkno... |                   |          |     | [REDACTED] | 13.8k  |
|      |                     |            |              |        |         |           |       |             |          |                   |          |     | [REDACTED] | 19.7k  |

Buttons: Close, DESC

Detailed Log View



| Tunnel Type N/A |                     | <b>Details</b><br>Threat Type vulnerability<br>Threat ID/Name HTTP Unauthorized Error<br>ID 34556 (View in Threat Vault)<br>Category brute-force<br>Content Version AppThreat-8286-6150<br>Severity informational<br>Repeat Count 1<br>File Name :8123/<br>URL<br>Partial Hash 0 |              |        |         |           |       | Decrypted <input type="checkbox"/><br>Packet Capture <input type="checkbox"/><br>Client to Server <input checked="" type="checkbox"/><br>Server to Client <input type="checkbox"/><br>Tunnel Inspected <input type="checkbox"/> |          |                   |          |     |           |
|-----------------|---------------------|--|--------------|--------|---------|-----------|-------|---|----------|-------------------|----------|-----|-----------|
|                 |                     |  |              |        |         |           |       | <b>DeviceID</b><br>Source Category<br>Source Profile<br>Source Model<br>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 Error | Exception | outside | 192.168.27.105 |             |                              |                     |
|  | 06/26 22:08:47 | vulnerability | HTTP Unauthorized Error | LAN       | outside | 192.168.27.105 |             |                              |                     |

**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

EXEMPT PROFILES USED IN CURRENT SECURITY RULE

VPprofile

resetall

EXEMPT IP ADDRESSES

192.168.27.155

192.168.27.105

+ Add - Delete

OK Cancel

## Vulnerability Protection Profile



Name VPprofile

Description

Rules | **Exceptions**

1 / 7 → ×

| ENAB...                             | ID ^  | THREAT NAME             | IP ADDRESS EXEMPTIONS | RULE            | CVE | HOST   | CATEGORY    | SEVERITY     | ACTION            | PACKET CAPTURE |
|-------------------------------------|-------|-------------------------|-----------------------|-----------------|-----|--------|-------------|--------------|-------------------|----------------|
| <input checked="" type="checkbox"/> | 34556 | HTTP Unauthorized Error | 2                     | simple-low-info |     | server | brute-force | informati... | default (allow) ↓ | disable        |

Show all signatures @ PDF/CSV

Page 1 of 1 | Displaying 1 - 1 / 1 threats

OK

Cancel

# Chapter 10: VPN and Advanced Protection

| <input type="checkbox"/> | NAME            | ENCRYPTION        | AUTHENTICATION | DH GROUP | KEY LIFETIME |
|--------------------------|-----------------|-------------------|----------------|----------|--------------|
| <input type="checkbox"/> | default         | aes-128-cbc, 3des | sha1           | group2   | 8 hours      |
| <input type="checkbox"/> | Suite-B-GCM-128 | aes-128-cbc       | sha256         | group19  | 8 hours      |
| <input type="checkbox"/> | Suite-B-GCM-256 | aes-256-cbc       | sha384         | group20  | 8 hours      |

| <input type="checkbox"/> | NAME            | ESP/AH | ENCRYPTION        | AUTHENTICATION | DH GROUP | LIFETIME | LIFESIZE |
|--------------------------|-----------------|--------|-------------------|----------------|----------|----------|----------|
| <input type="checkbox"/> | default         | ESP    | aes-128-cbc, 3des | sha1           | group2   | 1 hours  |          |
| <input type="checkbox"/> | Suite-B-GCM-128 | ESP    | aes-128-gcm       | none           | group19  | 1 hours  |          |
| <input type="checkbox"/> | Suite-B-GCM-256 | ESP    | aes-256-gcm       | none           | group20  | 1 hours  |          |

### IKE Gateway ?

---

**General** | **Advanced Options**

Name

Version

Address Type  IPv4  IPv6

Interface

Local IP Address

Peer IP Address Type  IP  FQDN  Dynamic

Peer Address

Authentication  Pre-Shared Key  Certificate

Pre-shared Key

Confirm Pre-shared Key

Local Identification

Peer Identification

Comment

### IKE Gateway

General | **Advanced Options**

**Common Options**

Enable Passive Mode

Enable NAT Traversal

**IKEv1 | IKEv2**

Exchange Mode: main

IKE Crypto Profile: Suite-B-GCM-256

Enable Fragmentation

**Dead Peer Detection**

Interval: 5

Retry: 5

OK Cancel

### IKE Gateway

General | **Advanced Options**

**Common Options**

Enable Passive Mode

Enable NAT Traversal

**IKEv1 | IKEv2**

IKE Crypto Profile: Suite-B-GCM-256

Strict Cookie Validation

**Liveness Check**

Interval (sec): 5

OK Cancel

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



# IPSec Tunnel



## General | Proxy IDs

Name:

Tunnel Interface:

Type:  Auto Key  Manual Key  GlobalProtect Satellite

Address Type:  IPv4  IPv6

IKE Gateway:

IPSec Crypto Profile:

Show Advanced Options

Enable Replay Protection

Copy ToS Header

Add GRE Encapsulation

Tunnel Monitor

Destination IP:

Profile:

Comment:

# Virtual Router - default



## Router Settings

### Static Routes

#### Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

## IPv4 | IPv6

2 items

|                          | NAME | DESTINATION | INTERFACE | Next Hop   |              | ADMIN DISTANCE | METRIC | ROUTE TABLE |
|--------------------------|------|-------------|-----------|------------|--------------|----------------|--------|-------------|
|                          |      |             |           | TYPE       | VALUE        |                |        |             |
| <input type="checkbox"/> | dg   | 0.0.0.0/0   | vlan      | ip-address | 192.168.27.1 | default        | 10     | unicast     |
| <input type="checkbox"/> | fw14 | 10.0.0.0/24 | tunnel.3  |            |              | default        | 10     | unicast     |

OK

Cancel

www.salesforce.com

GO



PANgurus



firewall



Active Directory

### Log Forwarding Profile ?

Name

Description

4 items

| <input type="checkbox"/> | NAME                 | LOG TYPE | FILTER   | FORWARD METHOD  | BUILT-IN ACTIONS   |
|--------------------------|----------------------|----------|----------|---|--|
| <input type="checkbox"/> | Threat-to-Panorama   | threat   | All Logs | <ul style="list-style-type: none"> <li>Panorama SysLog</li> <li>splunk</li> </ul> | <ul style="list-style-type: none"> <li>quarantine</li> </ul> |
| <input type="checkbox"/> | Traffic-to-Panorama  | traffic  | All Logs | <ul style="list-style-type: none"> <li>Panorama SysLog</li> <li>splunk</li> </ul> |  |
| <input type="checkbox"/> | URL-to_panorama      | url      | All Logs | <ul style="list-style-type: none"> <li>Panorama SysLog</li> <li>splunk</li> </ul> |  |
| <input type="checkbox"/> | WildFire-to-Panorama | wildfire | All Logs | <ul style="list-style-type: none"> <li>Panorama SysLog</li> </ul>                 |  |

Add Delete Clone

OK

Cancel

| NAME                 | TYPE      | Source |         |                   |            | Destination |                    | APPLICATION   | SERVICE             | ACTION |
|----------------------|-----------|--------|---------|-------------------|------------|-------------|--------------------|---|---------------------|--------|
|                      |           | ZONE   | ADDRESS | USER              | DEVICE     | ZONE        | ADDRESS            |   |                     |        |
| 1 device quarantine  | universal | vpn    | lppool  | pangurus\vpnusers | quarantine | dmz         | remediation server | <ul style="list-style-type: none"> <li>ms-update</li> <li>ssh</li> <li>ssl</li> <li>symantec-av-update</li> <li>web-browsing</li> </ul> | application-default | Allow  |
| 2 allow-corp-devices | universal | vpn    | lppool  | pangurus\vpnuser  | corp       | dmz         | firewall           | <ul style="list-style-type: none"> <li>ssh</li> <li>ssl</li> </ul>  | application-default | Allow  |
| 3 allow-byod         | universal | vpn    | lppool  | pangurus\vpnuser  | byod       | dmz         | synology           | <ul style="list-style-type: none"> <li>ms-ds-smb-base</li> <li>ms-ds-smbv3</li> </ul>   | application-default | Allow  |
| 4 allow-all-AV       | universal | vpn    | lppool  | pangurus\vpnuser  | any        | dmz         | symantec           | <ul style="list-style-type: none"> <li>symantec-av-update</li> <li>symantec-endpoint...</li> </ul>                                      | application-default | Allow  |
| 5 allow-all-openvpn  | universal | vpn    | lppool  | pangurus\vpnuser  | no-hip     | dmz         | webserverfarm-p... | <ul style="list-style-type: none"> <li>ssl</li> <li>web-browsing</li> </ul>   | application-default | Allow  |



( 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 | 78.0.0.0    | 22222   | unknown-tcp  | allow  |
|  |  | 06/14 14:43:08 | end  | LAN       | outside | 192.168.27.4 | 79.0.0.0    | 22222   | unknown-tcp  | allow  |
|  |  | 06/14 13:25:23 | end  | LAN       | outside | 192.168.27.4 | 46.0.0.0    | 22222   | unknown-tcp  | allow  |

## Application ?

**Configuration** | Advanced | Signatures

### General

Name

Description

### Properties

Category  Subcategory  Technology

Parent App  Risk

## Application ?

**Configuration** | **Advanced** | Signatures

- Char
- 
- 
- 

### Tag

### Defaults

Port  IP Protocol  ICMP Type  ICMP6 Type  None

#### PORT

tcp/22221-22222

Add Delete

Enter each port in the form of [tcp/udp]/[dynamic|0-65535] Example: tcp/dynamic or udp/32

### Timeouts

Timeout  TCP Timeout  UDP Timeout

TCP Half Closed  TCP Time Wait

### Scanning (activated via Security Profiles)

File Types  Viruses  Data Patterns

OK

Cancel

|   | NAME           | TAGS | Source |              | Destination |         | PROTOC... | PORT        | APPLICATI... |
|---|----------------|------|--------|--------------|-------------|---------|-----------|-------------|--------------|
|   |                |      | ZONE   | ADDRESS      | ZONE        | ADDRESS |           |             |              |
| 1 | solar override | none | LAN    | 192.168.27.4 | outside     |         | 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... | 80.239.175.38 | 22222   | solar       | allow  |
|  |  | 06/16 19:49:46 | end  | LAN       | outside | 192.168.27.2... | 80.239.175.38 | 22222   | solar       | allow  |
|  |  | 06/16 16:29:25 | end  | LAN       | outside | 192.168.27.2... | 185.121.71.38 | 22222   | solar       | allow  |

tcp.stream eq 0

| No. | Time            | Source         | Destination    | Protocol | Length | Info               |
|-----|-----------------|----------------|----------------|----------|--------|--------------------|
| 1   | 20:24:52.687458 | 192.168.27.113 | .37            | TCP      | 58     | 1296 → 22222 [SYN] |
| 2   | 20:24:52.706861 | .37            | 192.168.27.113 | TCP      | 58     | 22222 → 1296 [SYN, |
| 3   | 20:24:52.709333 | 192.168.27.113 | .37            | TCP      | 54     | 1296 → 22222 [ACK] |
| 4   | 20:24:52.726281 | 192.168.27.113 | .37            | TCP      | 110    | 1296 → 22222 [ACK] |

▶ Frame 4: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)  
 ▶ Ethernet II, Src:  
 ▶ Internet Protocol Version 4, Src: 192.168.27.113, Dst:  
 ▶ Transmission Control Protocol, Src Port: 1296, Dst Port: 22222, Seq: 1, Ack: 1, Len: 56  
 ▼ Data (56 bytes)  
 Data: 123456792200ddff0b04a2b81673fefefffff030526684f94...  
 [Length: 56]

**Application** ?

Configuration | Advanced | **Signatures**

1 item

| <input type="checkbox"/> | SIGNATURE NAME | COMMENT | ORDERED CONDITION MATCH  | SCOPE       |
|--------------------------|----------------|---------|--------------------------|-------------|
| <input type="checkbox"/> | solar          |         | <input type="checkbox"/> | Transaction |

**Signature** ?

Signature Name: solar

Comment:

Scope:  Transaction  Session

Ordered Condition Match

| <input type="checkbox"/> | AND CONDITION   | CONDITIO...    | OPERATOR      | CONTEXT                 | PATTERN            | QUAL |
|--------------------------|-----------------|----------------|---------------|-------------------------|--------------------|------|
| <input type="checkbox"/> | And Condition 1 | Or Condition 1 | pattern-match | unknown-req-tcp-payload | \x123456792200dd\x |      |

**Or Condition** ?

Operator: Pattern Match

Context: unknown-req-tcp-payload

Pattern: \x123456792200dd\x

0 items

| <input type="checkbox"/> | QUALIFIER | VALUE |
|--------------------------|-----------|-------|
|--------------------------|-----------|-------|

|       |               |   |
|-------|---------------|---|
| .     | 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. x1, 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  Name   
41000 - 45000 & 6800001 - 6900000  
Comment

### Properties

Severity  Direction   
Default Action  Affected System

### References (one reference per line)

CVE  Bugtraq   
Vendor  Reference

OK

Cancel

| No. | Time            | Source        | Destination   | Protocol | Length | Info                              |
|-----|-----------------|---------------|---------------|----------|--------|-----------------------------------|
| 19  | 20:14:27.249912 | 192.168.27.7  | 192.168.27.29 | TCP      | 66     | 62747 → 80 [SYN, ECN, CWR] Seq=0  |
| 20  | 20:14:27.272031 | 192.168.27.29 | 192.168.27.7  | TCP      | 66     | 80 → 62747 [SYN, ACK] Seq=0 Ack=1 |
| 21  | 20:14:27.274027 | 192.168.27.7  | 192.168.27.29 | TCP      | 54     | 62747 → 80 [ACK] Seq=1 Ack=1 Win= |
| 22  | 20:14:27.274728 | 192.168.27.7  | 192.168.27.29 | OCSP     | 444    | Request                           |

```
▶ Frame 22: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0
▶ Ethernet II, Src: Intel(R) Ethernet Controller (3:9:5:3:3:3), Dst: Intel(R) Ethernet Controller (3:9:5:3:3:3)
▶ Internet Protocol Version 4, Src: 192.168.27.7, Dst: 192.168.27.29
▶ Transmission Control Protocol, Src Port: 62747, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
▼ Hypertext Transfer Protocol
  ▶ POST / HTTP/1.1\r\n
    Host: \r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
    Accept: */*\r\n
    Accept-Language: nl,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/ocsp-request\r\n
    ▶ Content-Length: 83\r\n
    Connection: keep-alive\r\n
  \r\n
```

# Custom Vulnerability Signature



Configuration | **Signatures**

Signature  Standard  Combination

1 item

| <input type="checkbox"/> | STANDARD | COMMENT | ORDERED<br>CONDITION MATCH          | SCOPE       |
|--------------------------|----------|---------|-------------------------------------|-------------|
| <input type="checkbox"/> | Firefox  |         | <input checked="" type="checkbox"/> | Transaction |

## Standard



Standard

Comment

Scope  Transaction  Session

Ordered Condition Match

| <input type="checkbox"/>  | AND CONDITION   | CONDITIONS     | OPERATOR      | CONTEXT          | VALUE    | QUALIFIER            | NEGATE                   |
|---|-----------------|----------------|---------------|------------------|----------|----------------------|--------------------------|
| ∨ And Condition 1   |                 |                |               |                  |          |                      |                          |
| <input type="checkbox"/>  | And Condition 1 | Or Condition 1 | pattern-match | http-req-headers | Firefox/ | http-method:<br>POST | <input type="checkbox"/> |
| ∨ And Condition 2   |                 |                |               |                  |          |                      |                          |
| <input type="checkbox"/>  | And Condition 2 | Or Condition 1 | pattern-match | http-req-headers | Chrome/  | http-method:<br>POST | <input type="checkbox"/> |
| Add Or Condition  Add And Condition  Delete  Move Up  Move Down |                 |                |               |                  |          |                      |                          |

OK

Cancel

## Vulnerability Protection Profile

Name

Description

Rules | Exceptions

| <input type="checkbox"/>            | RULE NAME              | THREAT NAME | CVE | HOST TYPE | SEVERITY | ACTION                | PACKET CAPTURE |
|-------------------------------------|------------------------|-------------|-----|-----------|----------|-----------------------|----------------|
| <input type="checkbox"/>            | simple-client-critical | any         | any | client    | critical | block-ip (source,120) | single-packet  |
| <input checked="" type="checkbox"/> | simple-client-high     | any         | any | client    | high     | reset-both            | single-packet  |

### Vulnerability Protection Profile

Name

Description

Rules | **Exceptions**

1 / 6

| ENAB...                             | ID ^  | THREAT NAME  | IP ADDRESS EXEMPTIONS | RULE               | CVE | HOST   | CATEGORY | SEVERITY | ACTION                 | PACKET CAPTURE |
|-------------------------------------|-------|--------------|-----------------------|--------------------|-----|--------|----------|----------|------------------------|----------------|
| <input checked="" type="checkbox"/> | 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

## Session Settings

Rematch all sessions on config policy change

ICMPv6 Token Bucket Size

ICMPv6 Error Packet Rate (per sec)

Enable IPv6 Firewalling

Enable Jumbo Frame

Enable DHCP Broadcast Session

NAT64 IPv6 Minimum Network MTU

NAT Oversubscription Rate

ICMP Unreachable Packet Rate (per sec)

Accelerated Aging

Accelerated Aging Threshold

Accelerated Aging Scaling Factor

Packet Buffer Protection

Latency Based Activation

Alert (%)

Activate (%)

Block Countdown Threshold (%)

Block Hold Time (sec)

Block Duration (sec)

Multicast Route Setup Buffering

Buffer Size

OK

Cancel

## TCP Settings

Forward segments exceeding TCP out-of-order queue

Allow arbitrary ACK in response to SYN

Drop segments with null timestamp option

Asymmetric Path  Drop  Bypass

Urgent Data Flag  Clear  Do Not Modify

Drop segments without flag

Strip MPTCP option

SIP TCP cleartext

TCP Retransmit Scan

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

Description

**Flood Protection** | Reconnaissance Protection | Packet Based Attack Protection | Protocol Protection | Ethernet SGT Protection

**SYN**

Action:

Alarm Rate (connections/sec):

Activate (connections/sec):

Maximum (connections/sec):

**ICMP**

Alarm Rate (connections/sec):

Activate (connections/sec):

Maximum (connections/sec):

**Other IP**

Alarm Rate (connections/sec):

Activate (connections/sec):

Maximum (connections/sec):

**UDP**

Alarm Rate (connections/sec):

Activate (connections/sec):

Maximum (connections/sec):

**ICMPv6**

Alarm Rate (connections/sec):

Activate (connections/sec):

Maximum (connections/sec):

## Zone Protection Profile ?

Name

Description

Flood Protection | **Reconnaissance Protection** | Packet Based Attack Protection | Protocol Protection | Ethernet SGT Protection

| SCAN          | ENABLE                              | ACTION                                | INTERVAL (SEC) | THRESHOLD (EVENTS) |
|---------------|-------------------------------------|---------------------------------------|----------------|--------------------|
| TCP Port Scan | <input checked="" type="checkbox"/> | block-ip                              | 2              | 100                |
| UDP Port Scan | <input checked="" type="checkbox"/> | block                                 | 2              | 100                |
| Host Sweep    | <input checked="" type="checkbox"/> | <input type="text" value="Block IP"/> | 10             | 100                |

Track By  1 item

|   | IP ADDRESS(ES) |
|---|----------------|
| <input type="checkbox"/> SOURCE ADDRESS EXCLUSION | 192.168.27.155 |
| <input type="checkbox"/> nmap                     |                |

Duration (sec)

## Zone Protection Profile



Name

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

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Strict Source Routing | <input type="checkbox"/> Security             |
| <input checked="" type="checkbox"/> Loose Source Routing  | <input type="checkbox"/> Stream ID            |
| <input checked="" type="checkbox"/> Timestamp             | <input checked="" type="checkbox"/> Unknown   |
| <input checked="" type="checkbox"/> Record Route          | <input checked="" type="checkbox"/> Malformed |

OK

Cancel

## Zone Protection Profile



Name

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

Asymmetric Path

### Strip TCP Options

- TCP Timestamp
- TCP Fast Open

Multipath TCP (MPTCP) Options

OK

Cancel

## Zone Protection Profile



Name

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

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

Description

Flood Protection | Reconnaissance Protection | **Packet Based Attack Protection** | Protocol Protection | Ethernet SGT Protection

IP Drop | TCP Drop | ICMP Drop | **IPv6 Drop** | ICMPv6 Drop

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Drop packets with type 0 routing header             | <input type="checkbox"/> Hop-by-Hop extension   |
| <input checked="" type="checkbox"/> Drop packets with type 1 routing header             | <input type="checkbox"/> Routing extension  |
| <input type="checkbox"/> Drop packets with type 3 routing header                        | <input type="checkbox"/> Destination extension  |
| <input checked="" type="checkbox"/> Drop packets with type 4 to type 252 routing header | <input checked="" type="checkbox"/> Invalid IPv6 options in extension header            |
| <input type="checkbox"/> Drop packets with type 253 routing header                      | <input checked="" type="checkbox"/> Non-zero reserved field                             |
| <input type="checkbox"/> Drop packets with type 254 routing header                      | <input checked="" type="checkbox"/> Anycast source address                              |
| <input checked="" type="checkbox"/> Drop packets with type 255 routing header           | <input checked="" type="checkbox"/> Needless fragment header                            |
| <input type="checkbox"/> IPv4 compatible address  | <input checked="" type="checkbox"/> MTU in ICMPv6 'Packet Too Big' less than 1280 bytes |

OK

Cancel



## Zone Protection Profile



Name

Description

Flood Protection | Reconnaissance Protection | Packet Based Attack Protection | **Protocol Protection** | Ethernet SGT Protection

Rule Type  Exclude List  Include List

| <input type="checkbox"/> | PROTOCOL NAME              | ENABLE                              | ETHERTYPE (HEX) |
|--------------------------|----------------------------|-------------------------------------|-----------------|
| <input type="checkbox"/> | 802.11 management protocol | <input checked="" type="checkbox"/> | 0x890d          |

Exclude List uses implicit allow for all non-listed protocols



Cancel

## DoS Protection Profile



Name

Description

Type  Aggregate  Classified

**Flood Protection** | Resources Protection

**SYN Flood** | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

SYN Flood

Action

Alarm Rate (connections/s)

Activate Rate (connections/s)

Max Rate (connections/s)

Block Duration (s)

OK

Cancel

## DoS Protection Profile



Name

Description

Type  Aggregate  Classified

Flood Protection | **Resources Protection**

Sessions

Maximum Concurrent Sessions

OK

Cancel

## DoS Protection Profile



Name

Description

Type  Aggregate  Classified

**Flood Protection** | Resources Protection

**SYN Flood** | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

SYN Flood

Action

Alarm Rate (connections/s)

Activate Rate (connections/s)

Max Rate (connections/s)

Block Duration (s)

OK

Cancel

## DoS Protection Profile



Name

Description

Type  Aggregate  Classified

Flood Protection | **Resources Protection**

Sessions

Maximum Concurrent Sessions

OK

Cancel

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

**DoS Rule** ?

General | Source | Destination | **Option/Protection**

Any  
 SERVICE ^  
 service-https

Action:

Schedule:

Log Forwarding:

Aggregate:

**Classified**

Profile:

Address:

# Chapter 11: Troubleshooting Common Session Issues

**Detailed Log View** ? [ ]

|                 |  |   |
|-----------------|--|---|
| Tunnel Type N/A | Threat Type vulnerability<br>Threat ID/Name HTTP Unauthorized Error<br>ID 34556 ( <a href="#">View in Threat Vault</a> )<br>Category brute-force<br>Content Version AppThreat-8286-6150<br>Severity informational<br>Repeat Count 1<br>File Name [REDACTED]:8123/<br>URL<br>Partial Hash 0 | Decrypted <input type="checkbox"/><br>Packet Capture <input type="checkbox"/><br>Client to Server <input checked="" type="checkbox"/><br>Server to Client <input type="checkbox"/><br>Tunnel Inspected <input type="checkbox"/> |
|-----------------|--|---|

**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... |                   |          |            | [REDACTED] |
|      | 2020/06/26 22:08:55 | url        | web-browsing | alert  | out-web | 31562...  |       | informat... | unkno... | medium-risk,un... |          | [REDACTED] |            |
|      | 2020/06/26 22:10:48 | end        | web-browsing | allow  | out-web | 31562...  | 10... |             | unkno... |                   |          |            |            |

Close

**Configure Filtering**  
 Manage Filters [4/4 Filters Set]  
 Filtering  ON Pre-Parse Match  OFF

**Configure Capturing**  
 Packet Capture  ON

| STAGE                    | FILE                 | BYTE COUNT | PACKET COUNT |
|--------------------------|----------------------|------------|--------------|
| <input type="checkbox"/> | receive rx.pcap      |            | 50000        |
| <input type="checkbox"/> | firewall tunnel.pcap | 100000000  |              |
| <input type="checkbox"/> | transmit tx.pcap     |            |              |
| <input type="checkbox"/> | drop drop.pcap       |            |              |

+ Add - Delete

**Settings**  
[Clear All Settings](#)

**Captured Files**  
 5 items → ×

| FILE NAME                            | DATE                | SIZE(MB) |
|--------------------------------------|---------------------|----------|
| <input type="checkbox"/> drop.pcap   | 2020/06/30 23:18:18 | 0.032899 |
| <input type="checkbox"/> rx.pcap     | 2020/06/30 23:18:19 | 0.167466 |
| <input type="checkbox"/> solar.pcap  | 2020/06/19 01:12:20 | 0.519480 |
| <input type="checkbox"/> tunnel.pcap | 2020/06/30 23:18:19 | 0.134369 |
| <input type="checkbox"/> tx.pcap     | 2020/06/30 23:18:19 | 0.224996 |

**Packet Capture Filter**

| ID                         | INGRESS INTERFACE | SOURCE         | DESTINATION  | SRC PORT | DEST PORT | PROTO | NON-IP  | IPV6                     |
|----------------------------|-------------------|----------------|--------------|----------|-----------|-------|---------|--------------------------|
| <input type="checkbox"/> 1 |                   | 192.168.27.130 | 198.51.100.1 |          |           | 6     | exclude | <input type="checkbox"/> |
| <input type="checkbox"/> 2 |                   | 198.51.100.1   | 0.0.0.0      |          |           | 6     | exclude | <input type="checkbox"/> |
| <input type="checkbox"/> 3 |                   | 192.168.27.130 | 198.51.100.1 |          |           | 6     | exclude | <input type="checkbox"/> |
| <input type="checkbox"/> 4 |                   | 198.51.100.2   | 0.0.0.0      |          |           | 6     | exclude | <input type="checkbox"/> |

+ Add - Delete Set Selected Packet Capture Filter

OK

Cancel

PA-220 DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit

Date >>

< June 2020 >

| S  | M  | T  | W  | T  | F  | S  |
|----|----|----|----|----|----|----|
| 31 | 1  | 2  | 3  | 4  | 5  | 6  |
| 7  | 8  | 9  | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 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 |

Configuration Report Setting

CONFIDEN... SOURCE ADDRESS SOURCE USER DESCRIPTION

1 2 192.168.27.186 unknown user Repeatedly visited (11) the same URL 84.199.118.24/

### Botnet Configuration

HTTP Traffic

| ENAB...                             | COUNT | EVENT                                   | DESCRIPTION   |
|-------------------------------------|-------|---|---|
| <input checked="" type="checkbox"/> | 5     | Malware URL visit                       | Identifies users communicating with known malware URLs based on Malware and Botnet URL filtering categories |
| <input checked="" type="checkbox"/> | 5     | Use of dynamic DNS                      | Looks for dynamic DNS query traffic which could be indicative of botnet communication                       |
| <input checked="" type="checkbox"/> | 10    | Browsing to IP domains                  | Identifies users that browse to IP domains instead of URLs  |
| <input checked="" type="checkbox"/> | 5     | Browsing to recently registered domains | Looks for traffic to domains that have been registered within the last 30 days                              |
| <input checked="" type="checkbox"/> | 5     | Executable files from unknown sites     | Identifies executable files downloaded from unknown URLs  |

Unknown Applications

| Unknown TCP           |               | Unknown UDP           |               |
|-----------------------|---------------|-----------------------|---------------|
| Sessions Per Hour     | 10 [1 - 3600] | Sessions Per Hour     | 10 [1 - 3600] |
| Destinations Per Hour | 10 [1 - 3600] | Destinations Per Hour | 10 [1 - 3600] |
| Minimum Bytes         | 50 [1 - 200]  | Minimum Bytes         | 50 [1 - 200]  |
| Maximum Bytes         | 100 [1 - 200] | Maximum Bytes         | 100 [1 - 200] |

Other Applications

IRC

OK Cancel

Export to PDF Export to CSV Export to XML

reaper | Logout | Last Login Time: 06/26/2020 21:49:50 | Session Expire Time: 07/30/2020 22:42:40 | Active | Tasks | Language paloalto

|  | START TIME     | FROM ZONE | STATE  | TO ZONE  | SOURCE         | DESTINATION | TO PORT | PR... | APPLICA... | RULE           | CLEAR                               |
|--|----------------|-----------|--------|----------|----------------|-------------|---------|-------|------------|----------------|-------------------------------------|
|  | 06/30 23:17:58 | LAN       | ACTIVE | outside  | 192.168.27.216 |             | 443     | 6     | ssl        | out-web        | <input checked="" type="checkbox"/> |
|  | 06/30 23:26:03 | LAN       | ACTIVE | outside  | 192.168.27.7   |             | 53      | 17    | dns        | dns nolog      | <input checked="" type="checkbox"/> |
|  | 06/30 23:26:13 | trust-L3  | ACTIVE | trust-L3 | 192.168.27.2   |             | 53      | 17    | dns        | dns nolog mgmt | <input checked="" type="checkbox"/> |
|  | 06/30 23:18:29 | LAN       | ACTIVE | LAN      | 192.168.27.244 |             | 357...  | 17    | upnp       | inside-L2      | <input checked="" type="checkbox"/> |
|  | 06/30 23:18:12 | LAN       | ACTIVE | outside  |                |             | 443     | 6     | ssl        | out-web        | <input checked="" type="checkbox"/> |
|  | 06/30 10:29:12 | LAN       | ACTIVE | outside  | 192.168.27.114 |             | 9998    | 6     | ring       | out            | <input checked="" type="checkbox"/> |

Clear session

```
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])     | Dst[Dport]/Zone (translated IP[Port]) |
|-----|--------------|--------|------|------|---|---------------------------------------|
| 261 | ssl          | ACTIVE | FLOW | NS   | 10.0.0.8[49915]/trust/6 (192.168.27.251[35448]) | .122.2[443]/untrust (.122.2[443])     |
| 353 | web-browsing | ACTIVE | FLOW | NS   | 10.0.0.8[50011]/trust/6 (192.168.27.251[43839]) | .4.52[80]/untrust (.4.52[80])         |
| 356 | web-browsing | ACTIVE | FLOW | NS   | 10.0.0.8[50010]/trust/6 (192.168.27.251[54552]) | .4.52[80]/untrust (.4.52[80])         |
| 253 | ssl          | ACTIVE | FLOW | NS   | 10.0.0.8[49918]/trust/6 (192.168.27.251[64354]) | .37.44[443]/untrust (.37.44[443])     |
| 267 | ssl          | ACTIVE | FLOW | NS   | 10.0.0.8[49919]/trust/6 (192.168.27.251[3751])  | .38.49[443]/untrust (.38.49[443])     |
| 231 | ssl          | ACTIVE | FLOW | NS   | 10.0.0.8[49917]/trust/6 (192.168.27.251[16008]) | .121.44[443]/untrust (.121.44[443])   |

| Test Configuration   | Test Result                       | Result Detail   |
|--|-----------------------------------|---|
| Select Test: Update Server Connectivity<br><input type="button" value="Execute"/> <input type="button" value="Reset"/>   | Update Server is Connected        | Update Server is Connected  |
| Select Test: WildFire<br>Channel: <input checked="" type="radio"/> Public <input type="radio"/> Private<br><input type="button" value="Execute"/> <input type="button" value="Reset"/> | Test wildfire Public Cloud        | Test wildfire Public Cloud<br><br>Testing cloud server wildfire.paloaltonetworks.com ...<br>wildfire registration: successful<br>download server list: successful<br>select the best server: panos.wildfire.paloaltonetworks.com  |
| Select Test: Log Collector Connectivity<br><input type="button" value="Execute"/> <input type="button" value="Reset"/>   | Log Collector Connectivity Result | <pre> --   Type      Last Log Created   Last Log Fwded   Last Seq Num Fwded   Last Seq Num Acked Total Logs Fwded ----- &gt; 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           </pre> |

| Test Configuration   | Test Result        | Result Detail  |      |       |      |           |       |   |      |     |        |     |               |      |    |         |             |     |                    |      |      |     |          |     |                     |                  |  |                   |  |                  |  |                    |        |       |                  |    |          |     |
|--|--------------------|--|------|-------|------|-----------|-------|---|------|-----|--------|-----|---------------|------|----|---------|-------------|-----|--------------------|------|------|-----|----------|-----|---------------------|------------------|--|-------------------|--|------------------|--|--------------------|--------|-------|------------------|----|----------|-----|
| Select Test: Security Policy Match<br>From: LAN<br>To: outside<br>Source: 192.168.27.5<br>Destination: 1.1.1.1<br>Destination Port: 53<br>Source User: None<br>Protocol: TCP<br><input checked="" type="checkbox"/> show all potential match rules until first allow rule<br>Application: None<br>Category: None<br><input type="checkbox"/> check hip mask<br><input type="button" value="Execute"/> <input type="button" value="Reset"/> | dns nolog          | <table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr><td>Name</td><td>dns nolog</td></tr> <tr><td>Index</td><td>7</td></tr> <tr><td>From</td><td>LAN</td></tr> <tr><td>Source</td><td>any</td></tr> <tr><td>Source Region</td><td>none</td></tr> <tr><td>To</td><td>outside</td></tr> <tr><td>Destination</td><td>any</td></tr> <tr><td>Destination Region</td><td>none</td></tr> <tr><td>User</td><td>any</td></tr> <tr><td>Category</td><td>any</td></tr> <tr><td>Application Service</td><td>0:dns/tcp/any/53</td></tr> <tr><td></td><td>1:dns/tcp/any/853</td></tr> <tr><td></td><td>2:dns/udp/any/53</td></tr> <tr><td></td><td>3:dns/udp/any/5353</td></tr> <tr><td>Action</td><td>allow</td></tr> <tr><td>ICMP Unreachable</td><td>no</td></tr> <tr><td>Terminal</td><td>yes</td></tr> </tbody> </table> | 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 |
| 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   | Test Result   | Result Detail  |
|--|---|--|
| <p>Select Test: <b>Ping</b></p> <p><input type="checkbox"/> Bypass routing table, use specified interface</p> <p>Count: <b>5</b></p> <p><input type="checkbox"/> Don't fragment echo request packets (IPv4)</p> <p><input type="checkbox"/> Force to IPv6 destination</p> <p>Interval: <b>1</b></p> <p>Source: <b>192.168.27.2</b></p> <p><input type="checkbox"/> Don't attempt to print addresses symbolically</p> <p>Pattern: <b>68656c6c6f7468657265</b></p> <p>Size: <b>[0 - 65468]</b></p> <p>Tos: <b>[1 - 255]</b></p> <p>Ttl: <b>[1 - 255]</b></p> <p><input checked="" type="checkbox"/> Display detailed output</p> <p>Host: <b>1.1.1.1</b></p> <p><b>Execute</b> <b>Reset</b></p> | <p>PATTERN:<br/>0x68656c6c6f7468657265<br/>PING 1.1.1.1</p> | <p>PATTERN: 0x68656c6c6f7468657265<br/>PING 1.1.1.1 (1.1.1.1) from 192.168.27.2 : 56(84) bytes of data.<br/>64 bytes from 1.1.1.1: icmp_seq=1 ttl=58 time=15.9 ms<br/>64 bytes from 1.1.1.1: icmp_seq=2 ttl=58 time=16.8 ms<br/>64 bytes from 1.1.1.1: icmp_seq=3 ttl=58 time=15.2 ms<br/>64 bytes from 1.1.1.1: icmp_seq=4 ttl=58 time=13.1 ms<br/>64 bytes from 1.1.1.1: icmp_seq=5 ttl=58 time=14.5 ms</p> <p>-- 1.1.1.1 ping statistics --<br/>5 packets transmitted, 5 received, 0% packet loss, time 4077ms<br/>rtt min/avg/max/mdev = 13.195/15.167/16.827/1.246 ms</p> |

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

```
GNU GRUB version 0.97 (638K lower / 3143616K upper memory)

PANOS (maint-other)
PANOS (maint)
PANOS (sysroot0)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS or 'p' to enter a
password to unlock the next set of features.
```

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 >

Q=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 12: 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_rcv              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_bcast_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  2      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[1134]/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[1133]/untrust (194.7.1.4[1133])
-----

```

```

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

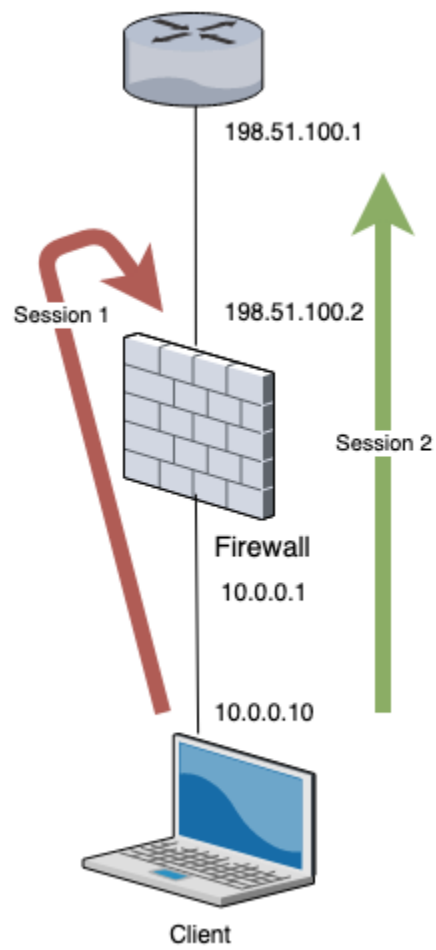
Global counters:
Elapsed time since last sampling: 2.740 seconds

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

```

| NAME                        | TAGS | Original Packet |                  |                       |                |                     |        | Translated Packet                                     |  |
|-----------------------------|------|-----------------|------------------|-----------------------|----------------|---------------------|--------|---|--|
|                             |      | 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<br>ethernet1/3<br>10.0.0.1/24     | destination-translation<br>address: 10.0.0.5<br>dns-rewrite: reverse |
| 2 inbound SSH server        | none | Untrust-L3      | Untrust-L3       | ethernet1/1           | any            | 109.51.100.2        | any    | none  | destination-translation<br>address: 10.0.0.5                         |
| 3 dynamic ip-port interface | none | Trust-L3        | Untrust-L3       | ethernet1/1           | dhcp...        | any                 | any    | dynamic-ip-and-port<br>ethernet1/1<br>198.51.100.2/24 | none   |

```
[reaper@PA-VM> debug dataplane packet-diag set log feature flow
  ager          ager
  all           all
  arp           arp
  basic         basic
  cluster       cluster
  ha            ha
  log           log
  nd            nd
  netx         netx
  np            np
  pred          pred
  receive       receive
  sdwan         sdwan
  sdwan_probe  sdwan_probe
  track        track
```



```
== 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 0x0000
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 0x0000
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 0xa0000affff0000 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, 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 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, 14 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 0x16433c6ffff000 word3 0x0 word4 0x26433c6ffff000
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, 14 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, 14 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, 14 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, 14 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, 14 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 sequence 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, 14 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, 14 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 0)
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
```

| Command  | Function  |
|--|---|
| find command keyword <keyword>                           | Lets you find any command as long as you know what you're looking for.                            |
| match <value>  | Filters the output of a command and only returns the line that has a positive match.              |
| except <value>   | Filters the output of a command and returns everything except the lines that match the value.     |
| tcpdump snaplen 0 filter "not port 22"                   | Captures all sessions on the management interface except sessions on port 22.                     |
| view-pcap debug-pcap filter-pcap mgmt-pcap no-dns-lookup | Shows packet captures taken on daemons, via packet-diag or tcpdump.                               |
| show admins  | Shows currently logged-in admins.   |
| delete admin-sessions username <user>                    | Terminates an admin's session.  |
| set system setting target-vsyz <vsyz>                    | Changes operational commends to a vsyz perspective.   |
| show authentication allowlist                            | Shows the allow list for all authentication profiles.   |
| show system environmentals                               | Shows system core temperatures and power levels.  |
| scp tftp export <thing> to user@destination:/path/       | Many things can be exported from the system, including log files, packet captures, or core files. |

| Basic system information    | Function  |
|-----------------------------|---|
| show system info            | Returns basic device information, such as serial, IP, installed content, and software versions.             |
| show system software status | Shows whether all processes are running properly.   |
| show system logdb-quota     | Returns the LogDB usage.  |
| show system disk-space      | Returns disk volume information.  |
| show jobs all/id            | Returns the status of all commit, download, install, and qfdn jobs, and additional details on specific IDs. |
| show system files           | Shows whether any core dump files have been created due to a process crash.                                 |
| request license fetch/info  | Retrieves and shows currently active licenses.  |
| show netstat all yes        | Shows all listening and established connections on the management plane, per process.                       |
| show chassis-ready          | Shows whether the dataplane is ready to process sessions.   |
| show panorama-status        | Verifies connectivity with panorama.  |

| High availability                                       | Function   |
|---|--|
| show high-availability state                            | Shows a quick rundown of the local peer's HA condition.  |
| show high-availability all                              | Summary of all HA runtime.   |
| show high-availability state-synchronization            | Displays statistics about sent and received sync messages.   |
| request high-availability sessions-reestablish force    | Re-establishes HA1 link if link was lost; use 'force' if HA1 backup is not configured.   |
| show high-availability session-reestablish-status       | Shows when HA1 and HA1-backup links were last re-established.  |
| request high-availability sync-to-remote running-config | Manually syncs running configuration to peer, in case automatic sync failed or if status is out-of-sync.   |
| request high-availability state functional suspend      | Suspends or activates local device.  |
| request high-availability state peer functional suspend | Suspends or activates peer device.   |
| show high-availability transitions                      | Indicates how many times a device has transitioned between HA states.  |
| show high-availability flap statistics                  | Details about preemptions 'flaps' (preemption activates device, error encountered again, device non-funct, recovers, preempt activates, error encountered again, and so on). |
| show high-availability control-link statistics          | Detailed information about HA1 messages.   |

| Performance information                    | Function   |
|--|--|
| show system resources                      | Shows management plane resource usage, similar to top in linux.  |
| show running resource-monitor              | Shows data plane CPU core utilization and buffer usage.  |
| debug dataplane pool statistics            | Shows software buffer pool usage.  |
| show session info                          | Shows number of active sessions, packets per second, throughput, and other session-related parameters.             |
| debug log-receiver statistics              | Information on log volume per second and any errors while writing or forwarding log.                               |
| show system statistics application session | Shows live statistics about top applications, or system throughput.  |
| show report jobs                           | Indicates whether reports are currently being generated (this could have an impact on management plane CPU usage). |

| DNS operations                            | Function   |
|---|--|
| show system setting ssl-decrypt dns-cache | Shows SSL decryption DNS cache.                          |
| show dns-proxy cache all                  | Shows the DNS proxy cache.                               |
| show system setting ssl-decrypt memory    | Shows SSL decryption memory usage.                       |
| show dns-proxy fqdn all                   | Shows all FQDN objects with their resolved IP addresses. |
| request system fqdn refresh               | Refreshes all FQDN objects.                              |
| debug dataplane internal vif link         | Returns statistics on the internal hardware interfaces.  |



| Packet flow  | Function   |
|--|--|
| show counter global filter delta yes                       | Shows global counters.   |
| show session all filter <filters>                          | Shows active, discard, and predict sessions matching the filter (or 'all' sessions). |
| set session offload yes no                                 | Enables and disables session offloading to hardware.                                 |
| set session tcp-reject-non-syn yes no                      | Disables dropping TCP ACK packets coming in without a proper handshake.              |
| # set deviceconfig setting tcp asymmetric-path bypass drop | Disables dropping packets that arrive out of window or out of sync.                  |

| Layers 2 and 3                             | Function   |
|--|--|
| show routing route                         | Outputs the routing table (Routing Information Base, or rib).  |
| show routing fib                           | Shows the forwarding table (Forwarding Information Base).  |
| show arp all                               | Shows the content of the ARP table (layer 3).  |
| show mac all                               | Shows the content of the MAC table (layer 2).  |
| show routing protocol ospf bgp rip summary | Returns a summary of the OSPF, BGP or RIP status.  |
| show routing resource                      | Verifies the number of routes is not reaching the system limits.   |
| debug routing pcap ospf bgp rip on off     | Enables/disables packet captures on the routing engine for the routing protocol. Use for troubleshooting only. |

| Policies  | Function  |
|---|---|
| show running nat-policy   | Shows all active NAT rules.   |
| show running nat-rule-ippool rule <rulename>                        | Shows memory usage, over-subscription ratio, and allocations per rule.      |
| show running global-ippool  | Shows runtime statistics for global dynamic source NAT.                     |
| show running ippool   | Shows overall source NAT statistics.  |
| show session all filter qos-class [1-8]                             | Displays all sessions that match a specific QoS class.                      |
| show qos interface <interface> counter                              | Shows general counter on QoS configured on an interface.                    |
| show qos interface <interface> throughput <Qid as seen in counters> | Returns actual throughput for a Qid on an interface.                        |
| show zone-protection zone <zone>                                    | Shows zone protection statistics for the zone.                              |
| show dos-protection rule <rulename> statistics                      | Shows statistics for a dos-protection rule.                                 |
| show dos-protection zone <zone> blocked source                      | Shows which IP addresses are currently being blocked due to DoS protection. |

| URL filtering                          | Function   |
|--|--|
| test url-info-cloud <url>              | Shows the category for a URL via cloud lookup.                                 |
| test url-info-host <url>               | Shows the category for a URL in the management plane cache.                    |
| show running url                       | Shows the category for a URL in the dataplane cache.                           |
| request url-filtering update url <url> | Refreshes the management plane cache entry for a URL with a cloud lookup.      |
| show running url-cache all             | Outputs the URL cache to mp-log dp_url_DB.log.                                 |
| show running url-cache statistics      | Shows memory usage of the URL cache.   |
| show url-cloud status                  | Returns connectivity information for URL lookup cloud connections.             |
| clear url-cache all url <url>          | Clears a single URL from cache, or the entire cache from the dataplane.        |
| delete url-database all url            | Clears a single URL from cache, or the entire cache from the management plane. |

| Panorama  | Function   |
|---|--|
| show logging-status device <serial>                                   | Returns log forwarding information for a device logging to Panorama.   |
| debug log-collector log-collection-stats show incoming-logs           | Shows incoming log statistics, including the current log rate.   |
| show system raid detail   | Shows RAID array information on an M appliance.  |
| show system disk details  | Shows disk status information on a VM appliance.   |
| replace old <serial> new <serial>                                     | Replaces a managed device's serial with a new one after an RMA. This loads all the configuration previously associated with one device with a new one without needing to go in and assign configuration to the new serial (it removes the old serial). |
| request log-fwd-ctrl action latest start-from-lastack device <serial> | Starts log forwarding from device from the last log last acked log.  |
| request log-fwd-ctrl start stop latest device <serial>                | Starts or stops log forwarding from a device to panorama with buffering.   |
| request log-fwd-ctrl action live device <serial>                      | Starts log forwarding without buffering (this could cause a large flood of inbound logs).  |

| IPSec   | Function  |
|---|---|
| show running tunnel flow info                 | Shows basic statistics about all VPN tunnels.             |
| test vpn ike-sa gateway <gateway>             | Initiates an IKE negotiation with the designated gateway. |
| test vpn ipsec-sa tunnel <tunnel>             | Initiates an IPSec negotiation for the designated tunnel. |
| clear vpn ike-sa gateway <gateway>            | Clears the IKE SA for a given gateway.                    |
| clear vpn ipsec-sa tunnel <tunnel>            | Clears the IPSec SA for a given tunnel.                   |
| show vpn ike-sa gateway <gateway>             | Shows the IKE SA for a given gateway.                     |
| show vpn ipsec-sa tunnel <tunnel>             | Shows the IPSec SA for a given tunnel.                    |
| show global-protect-gateway current-satellite | Shows currently connected satellites to GlobalProtect.    |
| show global-protect-gateway current-user      | Shows currently connected users to GlobalProtect.         |

| User-ID   | Function  |
|---|---|
| show user ip-user-mapping all   ip              | Shows all mapped users or the mapped user(s) for a specific IP on the dataplane.        |
| show user ip-user-mapping-mp all   ip           | Shows all mapped users or the mapped user(s) for a specific IP on the management plane. |
| debug user-id refresh group-mapping all         | Refreshes group-mapping memberships.  |
| show user group list                            | Shows all groups used in group-mapping.   |
| show user group name <group>                    | Shows all members of a group.   |
| show user group-mapping state all               | Shows the state of all group-mapping profiles.  |
| show user group-mapping statistics              | Shows last/next refresh of group mapping.   |
| show user user-id-agent statistics   state all  | Shows user-ID agent state and statistics.   |
| show user ts-agent statistics   state all       | Shows terminal server agent state and statistics.                                       |
| show user server-monitor statistics   state all | Shows the state of the agentless user-ID agent.   |
| show user ip-port-user-mapping all              | Shows user-to-port mapping for terminal server agents or a specific server IP.          |

| WildFire                   | Function                                       |
|----------------------------|--|
| show wildfire status       | Shows connection status to the WildFire cloud. |
| show wildfire statistics   | Shows file transfer statistics.                |
| test wildfire registration | Tests connectivity to the WildFire cloud.      |

| DHCP  | Function  |
|---|---|
| show dhcp server lease all  | Shows all DHCP leases.  |
| clear dhcp lease interface <interface> ip   mac   expiredonly <value> | Clears a lease for an IP or MAC address, or all the expired ones. |
| debug dhcpd pcap on   off   | Enables packet capture of DHCP transactions on the daemon.        |
| show dhcp client state <interface>                                    | Shows DHCP information for an interface that is a DHCP client.    |
| request dhcp client release   renew <interface>                       | Releases or renews DHCP client lease for a DHCP client interface. |

| Device state                              | Function  |
|---|---|
| show system state                         | This command returns the state of the entire device.                        |
| show system state filter env.*            | Shows system core temperatures and power levels.                            |
| show system state   match fan             | Searches the system state for any line containing 'fan' to find fan speeds. |
| show system state   match cfg.general.max | Returns the maximum number of configurable objects the system supports.     |
| show system state filter-pretty sys.s1.*  | Shows information about all the interfaces in slot 1.                       |

# Chapter 13: Supporting Tools

The screenshot shows the Splunk Enterprise interface. At the top left, the logo reads "splunk>enterprise". Below it is a sidebar with "Apps" and a gear icon. The sidebar contains a green arrow icon labeled "Search & Reporting" and a "+ Find More Apps" button. The main content area is titled "Explore Splunk Enterprise" and features two cards: "Product Tours" with a binoculars icon and the text "New to Splunk? Take a tour to help you on your way.", and "Add Data" with a server rack icon and a plus sign, with the text "Add or f Add Data ata to Splunk Enterprise. Afterwards, you may extract fields." The bottom navigation bar shows "splunk>enterprise", "Apps", and "Administrator" with an info icon.

## What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources



Data from every product in the Palo Alto Networks Next-generation Security Platform, including Firewalls, Panorama, Traps Endpoints...

[Configure now](#)

## Palo Alto Networks



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



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



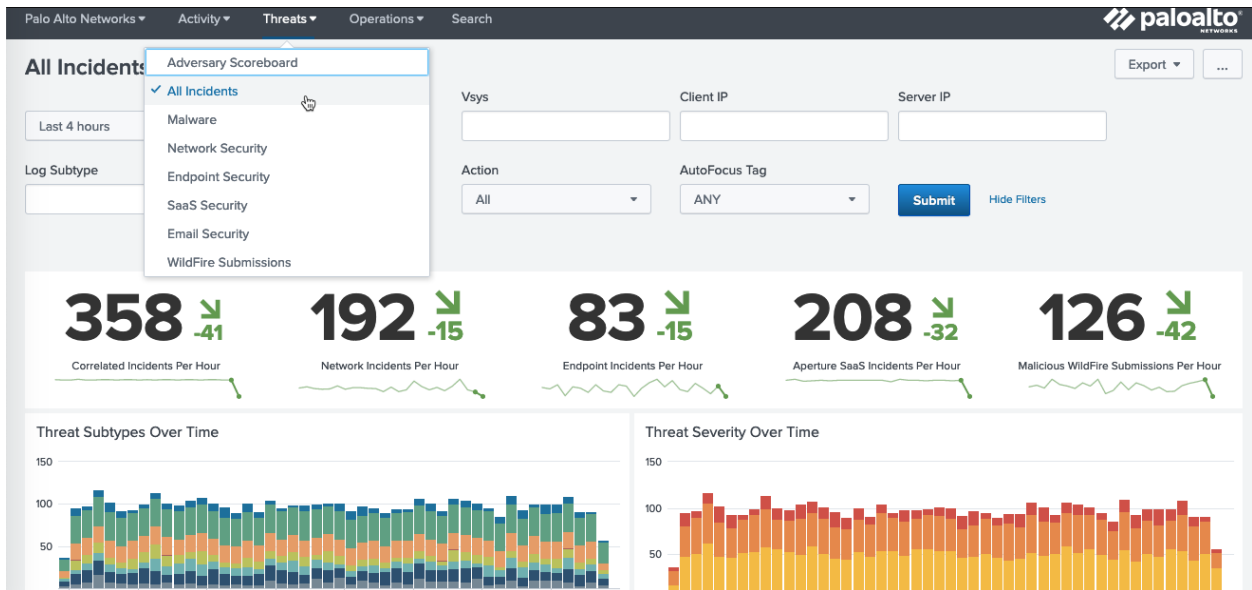
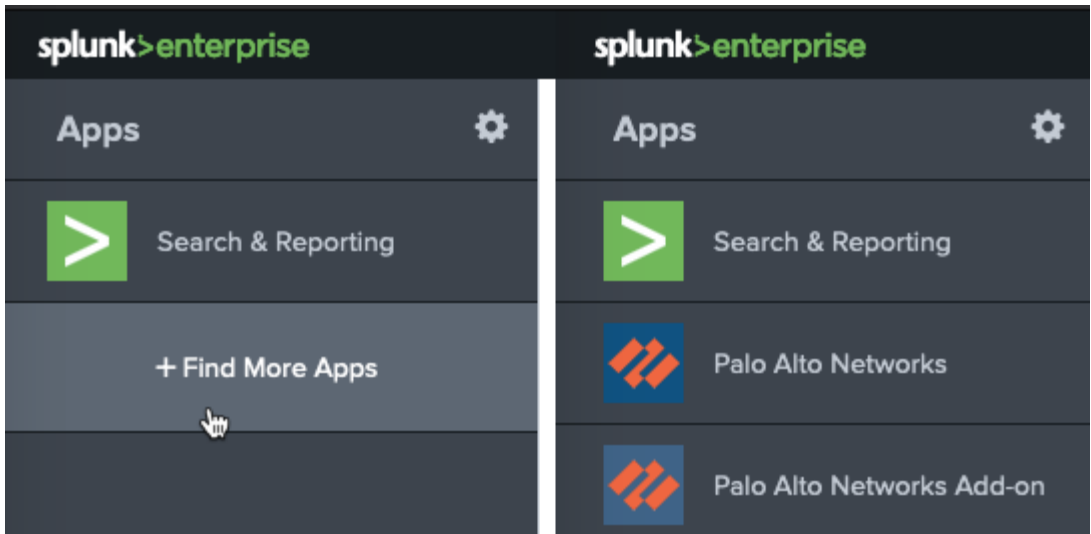
< Back Finish

### 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](#) [\[2\]](#) , enter the query below.

```
| tstats count where index=* AND (sourcetype="pan:*") by sourcetype, index
```



# Log Forwarding Profile



Name

Description

4 items → ×

| <input type="checkbox"/> | NAME                | LOG TYPE | FILTER   | FORWARD METHOD  | BUILT-IN ACTIONS |
|--------------------------|---------------------|----------|----------|---|------------------|
| <input type="checkbox"/> | Threat-to-Panorama  | threat   | All Logs | <ul style="list-style-type: none"><li>• Panorama <b>SysLog</b></li><li>• splunk</li></ul> |                  |
| <input type="checkbox"/> | Traffic-to-Panorama | traffic  | All Logs | <ul style="list-style-type: none"><li>• Panorama <b>SysLog</b></li><li>• splunk</li></ul> |                  |
| <input type="checkbox"/> | URL-to-Panorama     | url      | All Logs | <ul style="list-style-type: none"><li>• Panorama</li></ul>                                |                  |

+ Add - Delete 🔄 Clone

OK

Cancel

### System

| <input type="checkbox"/> | NAME           | DESCRI... | FILTER   | PANORAMA                            | SNMP TRAP | EMAIL | SYSLOG | HTTP |
|--------------------------|----------------|-----------|----------|-------------------------------------|-----------|-------|--------|------|
| <input type="checkbox"/> | Forward System |           | All Logs | <input checked="" type="checkbox"/> |           |       | splunk |      |

[+](#) Add [-](#) Delete [🔄](#) Clone [📄](#) PDF/CSV

### Configuration

| <input type="checkbox"/> | NAME                  | DE... | FILTER   | PANORAMA                            | SNMP TRAP | EMAIL | SYSLOG | HTTP |
|--------------------------|-----------------------|-------|----------|-------------------------------------|-----------|-------|--------|------|
| <input type="checkbox"/> | Forward Configuration |       | All Logs | <input checked="" type="checkbox"/> |           |       | splunk |      |

[+](#) Add [-](#) Delete [🔄](#) Clone [📄](#) PDF/CSV

### User-ID

| <input type="checkbox"/> | NAME            | DESCR... | FILTER   | PANORA...                           | SNMP TRAP | EMAIL | SYSLOG | HTTP | BUILT-IN ACTIONS |
|--------------------------|-----------------|----------|----------|-------------------------------------|-----------|-------|--------|------|------------------|
| <input type="checkbox"/> | Forward User-ID |          | All Logs | <input checked="" type="checkbox"/> |           |       | splunk |      |                  |

[+](#) Add [-](#) Delete [🔄](#) Clone [📄](#) PDF/CSV

### HIP Match

| <input type="checkbox"/> | NAME              | DE... | FILTER   | PANORA...                           | SNMP TRAP | EM... | SYSLOG | HT... | QU...                    | BUILT-IN ACTIONS |
|--------------------------|-------------------|-------|----------|-------------------------------------|-----------|-------|--------|-------|--------------------------|------------------|
| <input type="checkbox"/> | Forward HIP-match |       | All Logs | <input checked="" type="checkbox"/> |           |       | splunk |       | <input type="checkbox"/> |                  |

[+](#) Add [-](#) Delete [🔄](#) Clone [📄](#) PDF/CSV

### GlobalProtect

| <input type="checkbox"/> | NAME                  | DESCRIPTI... | FILTER   | PANORAMA                            | SNMP TRAP | EMAIL | SYSLOG | HTTP |
|--------------------------|-----------------------|--------------|----------|-------------------------------------|-----------|-------|--------|------|
| <input type="checkbox"/> | Forward GlobalProtect |              | All Logs | <input checked="" type="checkbox"/> |           |       | splunk |      |

[+](#) Add [-](#) Delete [🔄](#) Clone [📄](#) PDF/CSV



chrome web store



XXXXXXXXXX

🔍 pan(w)achrome x

## Extensions

[More extensions](#)

« Home

- Extensions
- Themes

#### Features

- Runs Offline



### Pan(w)achrome

Offered by: Luigi Mori

PANW extension for Chrome

★★★★★ 51 Productivity

[Add to Chrome](#)

Pan(w)achrome | chrome-extension://eopilnegkknidcicegemfhei... ☆

Devices

+ Add - Delete

| Name                | Status | Model | Serial | Version | URL |
|---------------------|--------|-------|--------|---------|-----|
| No device monitored |        |       |        |         |     |

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 |





DASHBOARDS

Overview

Resources

Traffic Details

DP Details

Counters

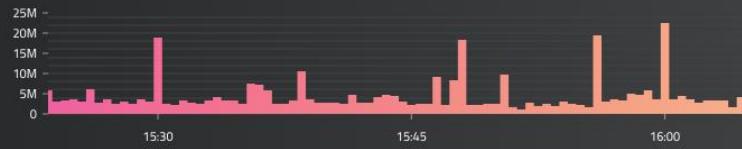
DEEP DIVES

+ Add Deep Dive

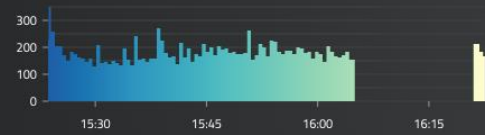
Ingress Traffic (bps)



Egress Traffic (bps)



Active Sessions



Connections Per Second (cps)



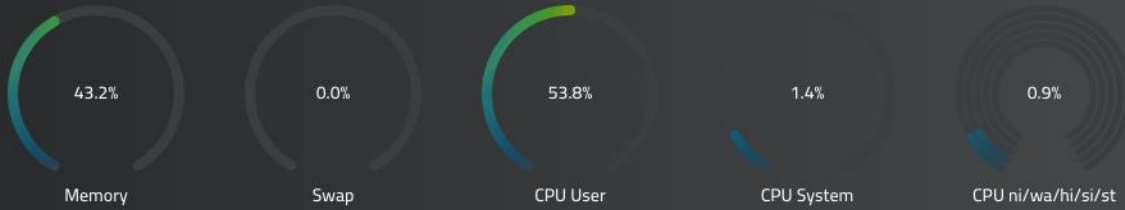
### Counter Global

| Name                                 | Category | Aspect   | Severity | Value     | Rate |
|--------------------------------------|----------|----------|----------|-----------|------|
| <a href="#">pkt_rcv</a>              | packet   | pktproc  | info     | 257370123 | 661  |
| <a href="#">pkt_rcv_zero</a>         | packet   | pktproc  | info     | 257370123 | 661  |
| <a href="#">pkt_flow_np</a>          | packet   | resource | info     | 248465422 | 641  |
| <a href="#">pkt_sent</a>             | packet   | pktproc  | info     | 252298152 | 640  |
| <a href="#">flow_qos_pkt_enqueue</a> | flow     | qos      | info     | 252254549 | 640  |
| <a href="#">flow_qos_pkt_dequeue</a> | flow     | qos      | info     | 252254549 | 640  |
| <a href="#">ctd_pscan_sw</a>         | ctd      | pktproc  | info     | 21362913  | 168  |
| <a href="#">dfa_sw</a>               | dfa      | pktproc  | info     | 20034769  | 167  |
| <a href="#">ctd_pkt_slowpath</a>     | ctd      | pktproc  | info     | 22098423  | 167  |

### Logical Interfaces

| Name                        | Info                          | Bitrate                        | Packets                     | Errors  | Drops   |
|-----------------------------|-------------------------------|--------------------------------|-----------------------------|---------|---------|
| <a href="#">ethernet1/1</a> | <a href="#">vsys1/outside</a> | in 419 Kbps +<br>out 38 Kbps + | in 47 pps +<br>out 44 pps + | 0 pps = | 0 pps = |
| <a href="#">ethernet1/2</a> | <a href="#">vsys1/LAN</a>     | in 600 bps -<br>out 3 Kbps -   | in < 1 pps -<br>out 2 pps - | 0 pps = | 0 pps = |
| <a href="#">ethernet1/3</a> | <a href="#">vsys1/LAN</a>     | in 35 Kbps +<br>out 568 Kbps + | in 39 pps +<br>out 72 pps + | 0 pps = | 0 pps = |

### Management Plane Load



### DPO Load Maximum



evices > Reaper-PA-220

DASHBOARDS

- Overview
- Resources
- Traffic Details
- DP Details
- Counters**

DEEP DIVES

- Active Sessions Overview
- + Add Deep Dive**

Deep Dive

Zone Traffic

outside

Ingress Traffic

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

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

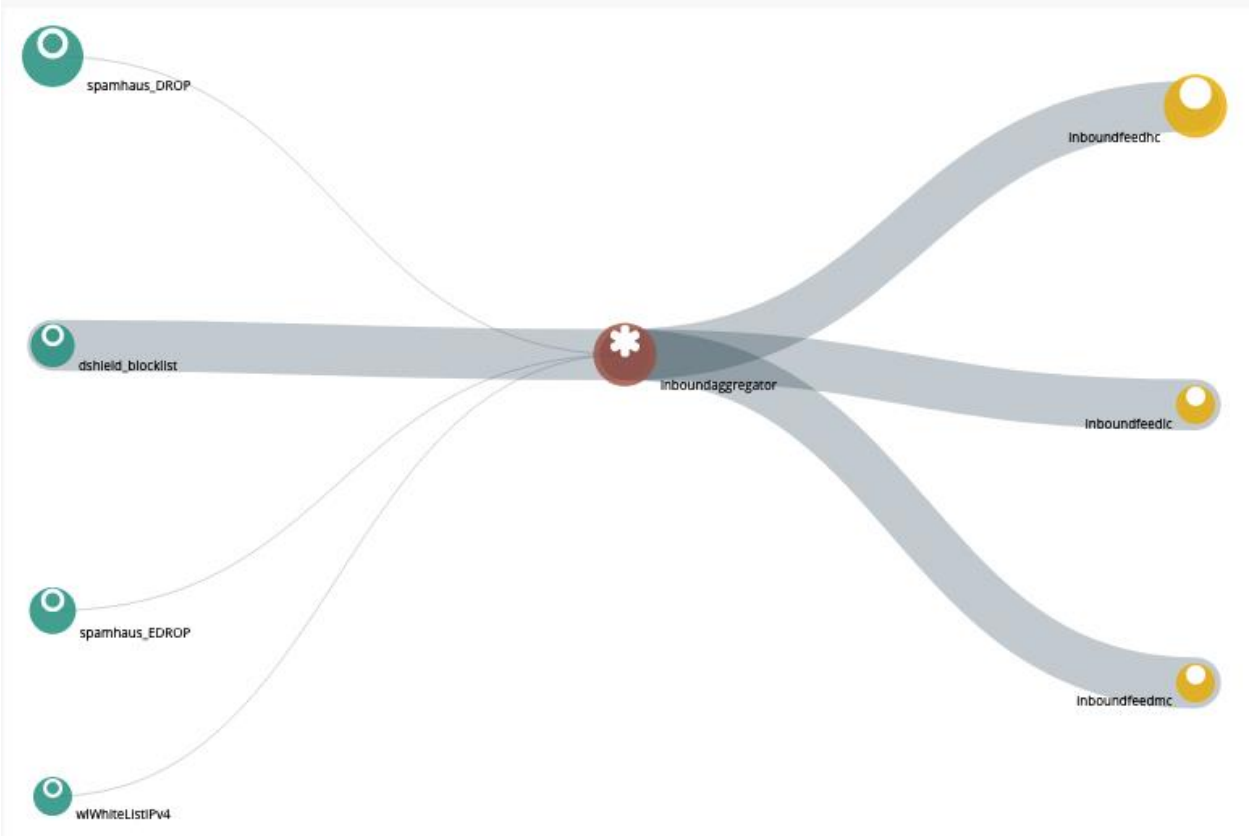
200 ADDED

200 REMOVED

**# OF INDICATORS (LAST 24h)**

ADDED/REMOVED (LAST 24h)

CONNECTION GRAPH



MINEMELD

| NAME              | TYPE   | STATE   | INDICATORS | ADD/REM/AO             | UPDATES                        | WITHDRAWS                      |
|-------------------|--------|---------|------------|------------------------|--------------------------------|--------------------------------|
| dshield_blocklist | MINER  | STARTED | 20         | ADDED: 0<br>REMOVED: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 |
| spamhaus_DROP     | MINER  | STARTED | 790        | ADDED: 0<br>REMOVED: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 |
| spamhaus_EDROP    | MINER  | STARTED | 95         | ADDED: 0<br>REMOVED: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 |
| wlWhiteListIPv4   | MINER  | STARTED | 0          | ADDED: 0<br>REMOVED: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 |
| inboundfeedhc     | OUTPUT | STARTED | 909        | ADDED: 0<br>REMOVED: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 | RX: 0<br>PROCESSED: 0<br>TX: 0 |
| inboundfeedlc     | OUTPUT | STARTED | 0          | ADDED: 0               | RX: 0                          | RX: 0                          |

# dshield\_blocklist NODE

## STATUS



|              |                               |                |  |
|--------------|-------------------------------|----------------|--|
| CLASS        | minemeld.ft.http.HttpFT       |                |  |
| PROTOTYPE    | <a href="#">dshield_block</a> |                |  |
| STATE        | <b>STARTED</b>                |                |  |
| LAST RUN     | 2020-06-17 00:14:24 +0200     | <b>SUCCESS</b> |  |
| # 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

**MINER** **STABLE**

ABOUT cloudflare

CLONE NEW

COMMIT

REVERT LOAD IMPORT EXPORT

Search:

NAME

|                    |  |                               |  |
|--------------------|--|-------------------------------|--|
| cloudflare4        | inboundagggregator                                   |                               |  |
| dshield_blocklist  | INPUTS   |                               |  |
| spamhaus_DROP      | spamhaus_DROP x spamhaus_EDROP x dshield_blocklist x |                               |  |
| spamhaus_EDROP     | wWhiteListIPv4 x                                     |                               |  |
| wWhiteListIPv4     | MINER  |                               |  |
|                    | cloudflare4  |                               |  |
| inboundfeedhc      | OUTPUT   | stdlib.feedHCGreen            | inboundagggregator x   |
| inboundfeedlc      | OUTPUT   | stdlib.feedLCGreen            | inboundagggregator x   |
| inboundfeedmc      | OUTPUT   | stdlib.feedMCGreen            | inboundagggregator x   |
| inboundagggregator | PROCESSOR  | stdlib.agggregatorIPv4Inbound | spamhaus_DROP<br>spamhaus_EDROP<br>dshield_blocklist<br>wWhiteListIPv4 x |

# inboundfeedhc NODE

STATUS

|               |  |        |                    |
|---------------|--|--------|--------------------|
| CLASS         | minemeld.ft.redis.RedisSet                 | OUTPUT | DISABLED           |
| PROTOTYPE     | stdlib.feedHCGreen                         | INPUTS | inboundagggregator |
| STATE         | STARTED                                    |        |                    |
| FEED BASE URL | https://192.168.27.242/feeds/inboundfeedhc |        |                    |
| TAGS          |  |        |                    |
| # INDICATORS  | 909  |        |                    |

### External Dynamic Lists ?

Name

**Create List** | List Entries And Exceptions

Type

Description

Source

**Server Authentication**

Certificate Profile

Check for updates

### External Dynamic Lists ?

Name

**Create List** | **List Entries And Exceptions**

**List Entries**

|                          | LIST ENTRIES                  |
|--------------------------|-------------------------------|
| <input type="checkbox"/> | 1.10.16.0-1.10.31.255         |
| <input type="checkbox"/> | 1.19.0.0-1.19.255.255         |
| <input type="checkbox"/> | 1.32.128.0-1.32.191.255       |
| <input type="checkbox"/> | 101.134.0.0-101.135.255.255   |
| <input type="checkbox"/> | 101.192.0.0-101.195.255.255   |
| <input type="checkbox"/> | 101.202.0.0-101.202.255.255   |
| <input type="checkbox"/> | 101.203.128.0-101.203.159.255 |

**Manual Exceptions**

|  | LIST ENTRIES |
|--|--------------|
|  |              |

# Admin Role Profile



Name

Description

Web UI | **XMLAPI**

- Report
- Log
- Configuration
- Operational Requests
- Commit
- User-ID Agent
- IoT Agent
- Export
- Import

Legend:  Enable  Read

## Admin Role Profile



Name

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