paloalto NETWORKS

PCNSE

PCNSE Bootcamp v10.1

Exam Domain 5 – Troubleshooting

Nick Burrows, CISSP

Free Digital Learning and Instructor-Led Training

Digital Learning

Next-Generation Firewall Feature Overview
Firewall Deployment
Firewall Tuning
Utilize Firewall as a Platform
Utilize Security Subscriptions
Panorama Deployment

Instructor Led

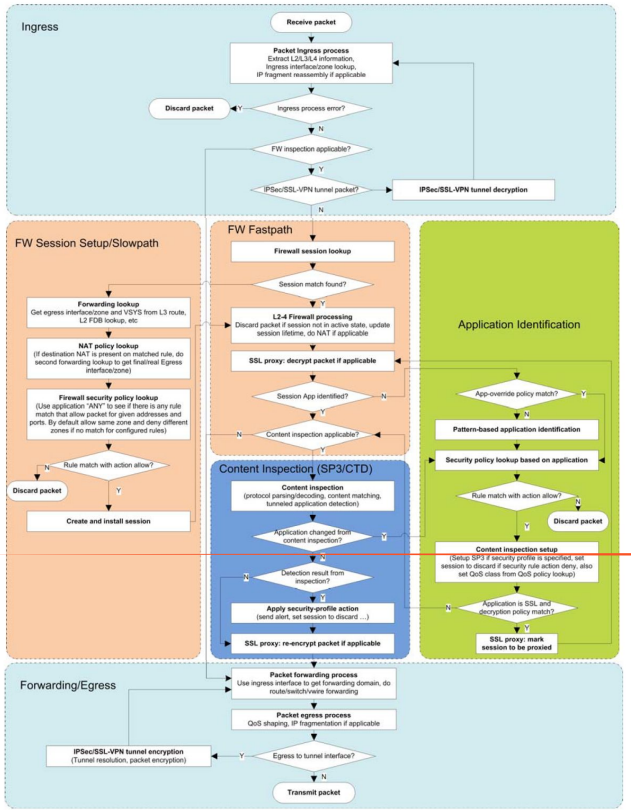
(EDU-210) Firewall 10.1 Essentials: Configuration and Management
(EDU-214) Firewall 10.1: Improving Security Posture and Hardening PAN-OS
(EDU-220) Panorama 10.1: Managing Firewalls at Scale
(EDU-330) Firewall 10.1: Troubleshooting – **Recommended!**

Topics

- 5.0 – General Troubleshooting Topics (Flow Basic, Destination NAT, etc.)
- 5.1 - Troubleshoot Site-to-Site tunnels
- 5.2 - Troubleshoot Physical Interfaces
- 5.3 - Troubleshoot SSL Decryption
- 5.4 - Troubleshoot Routing
- 5.5 - Investigate Traffic Patterns on the NGFW or Panorama
- 5.6 - Troubleshoot Zone Protection, Packet Buffer Protection and DDoS protection
- 5.7 - Troubleshoot GlobalProtect
- 5.8 - Troubleshooting PAN-OS-based SD-WAN

Section 5.0
General Troubleshooting Topics

Packet Flow Sequence – Reference



Flow Logic and Diagram

Initial Packet Processing - (Pre NAT)

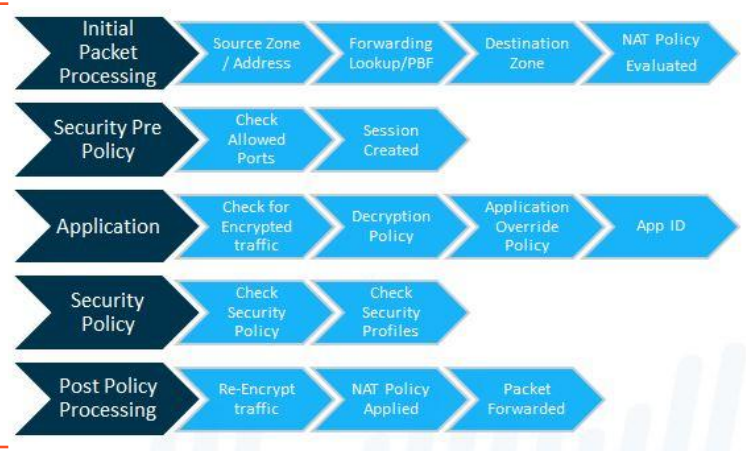
Security Pre-Policy - (Session Creation)

Application - (App-ID)

Security Policy - (Security Profiles Applied)

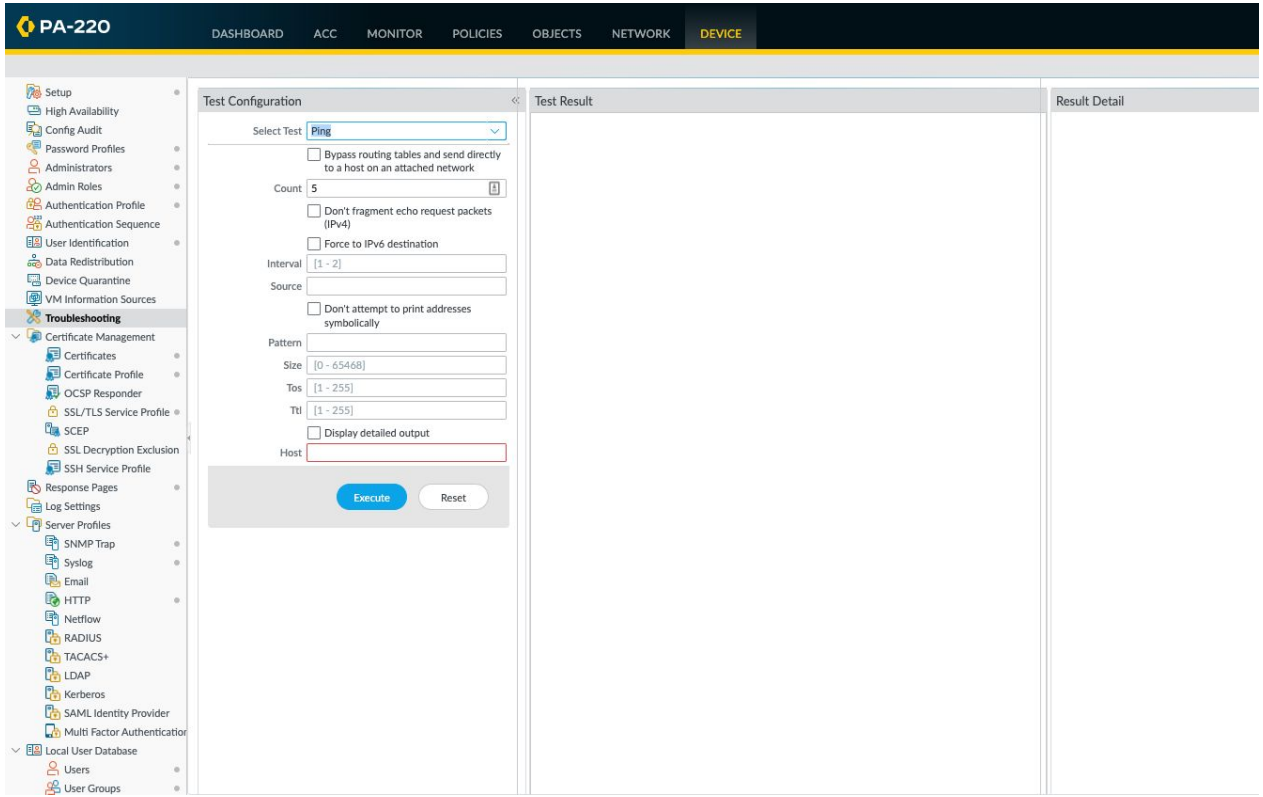
Post Policy Processing - (Post NAT)

5 Steps



https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

GUI Based Troubleshooting tools



GUI Based Tests:

Security Policy Match

QoS Policy Match

Authentication Policy Match

Decryption Policy Match

NAT Policy Match

PBF Policy Match

DoS Policy Match

Routing

Threat Vault

Ping

Trace Route

Log Collector Connectivity

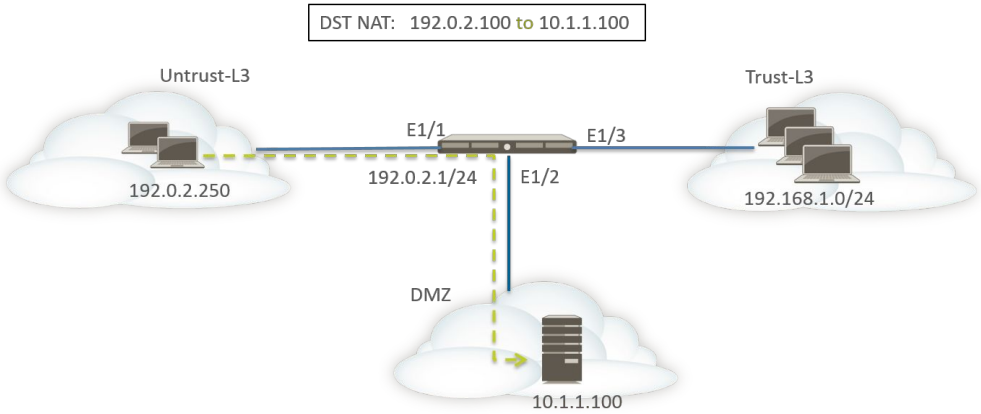
External Dynamic List

Update Server Connectivity

Essentially a GUI based version of the `test` command!

Troubleshooting Destination NAT

5.0.1 - Understanding Destination NAT



Sequence of Events:
The Host at 192.0.2.250 sends an ARP request for the address 192.0.2.100 (the public address of the destination server).

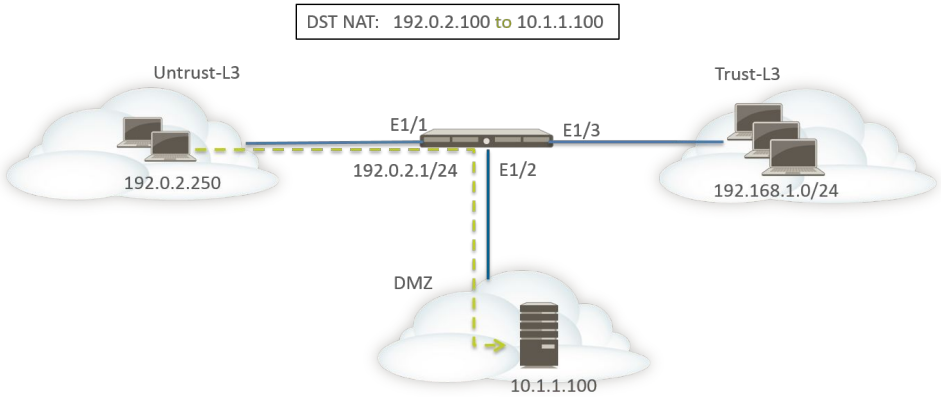
The firewall receives the ARP request packet for destination 192.0.2.100 on the Ethernet1/1 interface and processes the request. The firewall only responds to the ARP request with its own MAC address if DNAT rule is configured.

The NAT rules are then evaluated for a match. For the destination IP address to be translated, **a destination NAT rule from zone Untrust-L3 to zone Untrust-L3 must be created to translate the destination IP of 192.0.2.100 to 10.1.1.100.**

After determining the translated address, the firewall performs a route lookup for destination 10.1.1.100 to determine the egress interface.

In this example, the egress interface is Ethernet1/2 in zone DMZ. The firewall performs a security policy lookup to see if the traffic is permitted from zone Untrust-L3 to DMZ.

5.0.1 - Destination NAT Configuration and Security Policy



The firewall forwards the packet to the server out egress interface Ethernet1/2. The destination address is changed to 10.1.1.100 as the packet leaves the firewall. For this example, address objects are configured for webserver-private (10.1.1.100) and Webserver-public (192.0.2.100). The configured NAT rule would look like this:

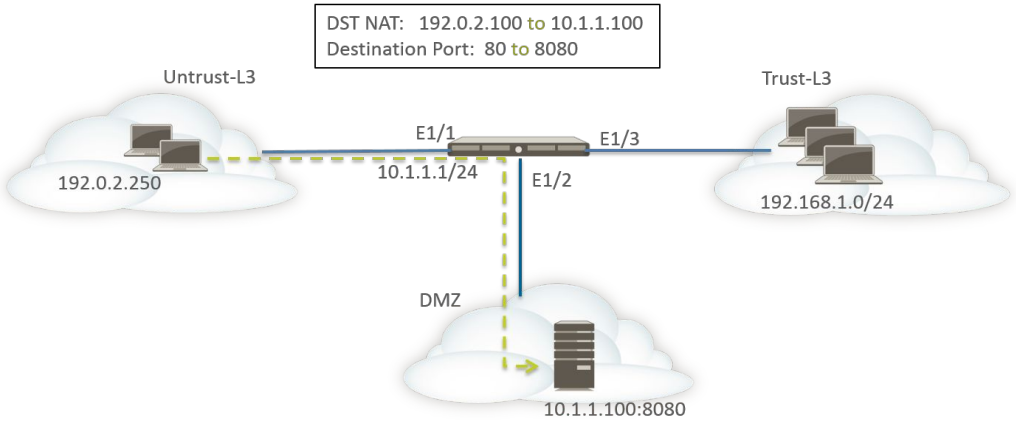
		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

The direction of the NAT rules is based on the result of route lookup. The configured security policy to provide access to the server from the Untrust-L3 zone would look like this:

	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

Reference: DNAT

5.0.2 - Understanding Destination NAT and PAT



Same sequence of events for this scenario, with a couple of exceptions.
In this example, the web server is configured to listen for HTTP traffic on port 8080.
The clients access the web server using the IP address 192.0.2.100:80 (TCP Port 80). The destination NAT rule is configured to translate **both IP address and port from 192.0.2.250:80 to 10.1.1.100:8080**

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	any	none	destination-translation address: webserver-private port: 8080

			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

Port Address Translation – translates port 80 (Untrust) to 8080 (Trust)

```
show session all | match 8080
OR
show session all | match 80
```


Troubleshooting Performance Issues

Troubleshooting High DP-CPU

One of the hardest (and most frustrating) things to troubleshoot!

Several factors that need to be identified before taking action:

- Is some, all, or no traffic through the firewall affected?
- Are users experiencing high latency, and if so, does latency affect all traffic or just certain applications?
- If issues are being reported, are these reports coinciding with specific peak times of the day, at regular intervals, or at totally random moments?

READ THIS!!!!!!

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRTCA0

Troubleshooting High DP-CPU

Are you simply trying to do more than the box is capable of?

`show session info`

Or is it something else?

- Data Plane (DP) CPU
- Packet Buffers
- Session
- Management Plane (MP)

Generate a tech support file while the issue is occurring (DEVICE > Support > Tech Support File > Generate Tech Support File)

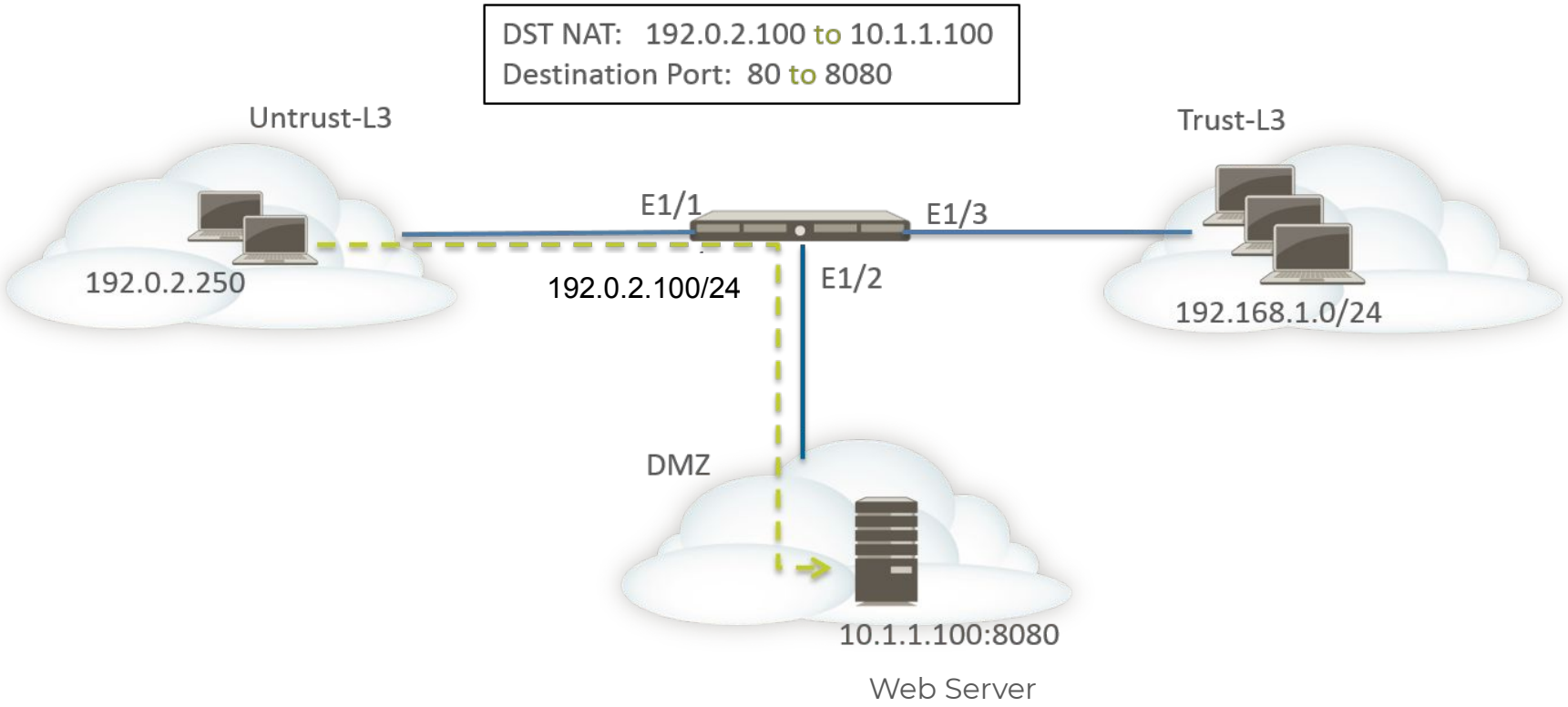
Run the **`show running resource-monitor`** command (to review dataplane CPU usage)

Run the **`debug dataplane pool statistics`** command (returns the status of all the buffers being used by the system and their status)

Run the **`show counter global filter delta yes`** command (returns a snapshot of the global counters triggered during the timeframe between the current and previous iteration, and could expose unusual numbers of discarded packets)

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRTCA0


QUIZ
TIME



Section 5.1
Troubleshooting IPSec Tunnels

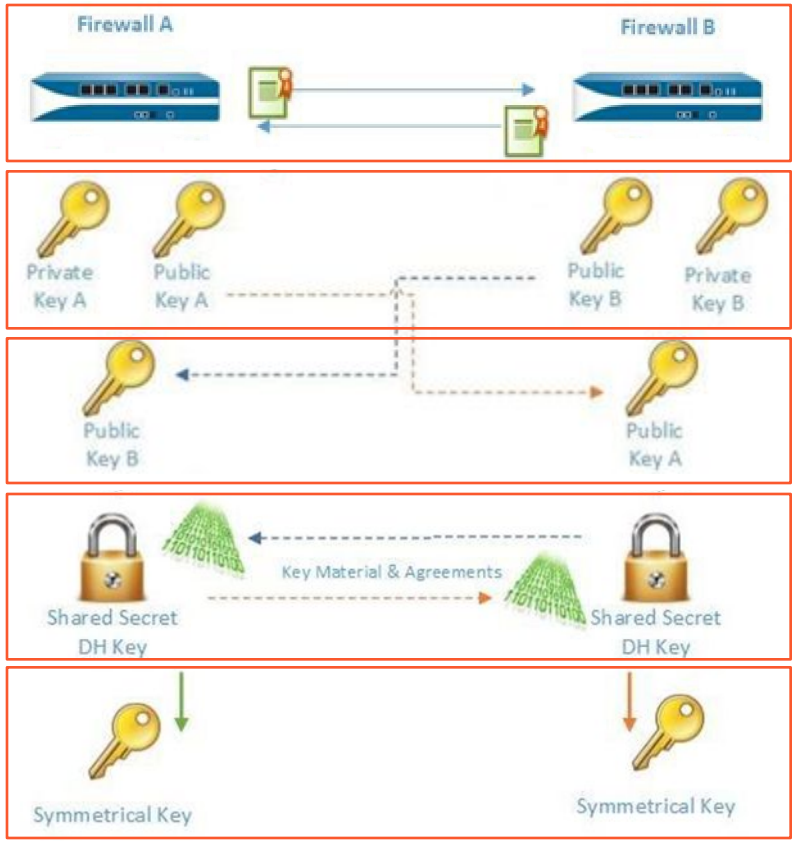
5.1.1 Troubleshooting Site-to-Site Tunnels

5.1.1 - Fundamentals of IPSEC - Reference

- **IKE Phase 1 -** In this phase, the firewalls use the parameters defined in the IKE Gateway configuration and the IKE Crypto profile to authenticate each other and set up a secure control channel.
  - ✔ IKE Phase supports the use of pre-shared keys or digital certificates (which use public key infrastructure, PKI) for mutual authentication of the VPN peers.
  - ✔ Digital certificates can be more convenient for larger networks or implementations that require stronger authentication security.
- **IKE Phase 2 -** After the tunnel is secured and authenticated, in Phase 2 the channel is further secured for the transfer of data between the networks.
  - ✔ IKE Phase 2 uses the keys that were established in Phase 1 of the process and the IPSec Crypto profile, which defines the IPSec protocols and keys used for the SA in IKE Phase 2.
- **The IPSEC uses the following protocols to enable secure communication:**
  - ✔ **Encapsulating Security Payload (ESP) -** Allows you to encrypt the entire IP packet and authenticate the source and verify integrity of the data. While ESP requires that you encrypt and authenticate the packet, you can choose to only encrypt or only authenticate by setting the encryption option to Null; using encryption without authentication is discouraged. AH operates directly on top of IP, using **IP protocol number 50.**
  - ✔ **Authentication Header (AH) -** Authenticates the source of the packet and verifies data integrity. AH does not encrypt the data payload and is unsuited for deployments where data privacy is important. AH is commonly used when the main concern is to verify the legitimacy of the peer, and data privacy is not required. AH operates directly on top of IP, using **IP protocol number 51.**

IP protocol Numbers

5.1.1 - Internet Key Exchange (IKE) - Reference



IKE Process

IKE Peers authenticate with PKI certificates or a pre-shared key (PSK).

Diffie-Hellman (DH) Private key is generated from random seed bits. DH Public key is generated from its DH private key.

Firewalls exchange their public keys.

Each firewall creates a shared secret from their private key and the other peer's public key. The shared secret produces the DH key.

The DH key is used to exchange key material. The encryption and Integrity agreement is formed for IKE Phase 2. Each firewall, and then generates its own symmetrical key from the DH key and the material is exchanged.

5.1.1 - Network > IPSec Tunnels

				IKE Gateway/Satellite				Tunnel Interface				
	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS
☐	VPN_to_H4B_SOLIHULL_MANU_Primary	Tunnel Info	Auto Key	ethernet1/3.10	192.168.10.60...	192.168.10.70	IKE Info	tunnel.10	default (Show Routes)	vsys1	H4B_SOLIHUL...	

```
BearAdmin@H4B_NGFW_1> show vpn ike-sa

There is no IKEv1 phase-1 SA found.

There is no IKEv1 phase-2 SA found.

IKEv2 SAs
Gateway ID      Peer-Address          Gateway Name                                    Role SN      Algorithm           Established     Expiration      Xt Child  ST

----------      ------------          ------------                                    ---- --      ---------           -----------     ----------      -- -----  --

1               192.168.10.70         VPN_to_H4B_SOLIHULL_MANU_Primary                Init 759     PSK/    /    /                                  5  1      INIT sent


IKEv2 IPSec Child SAs
Gateway Name                                    TnID     Tunnel                                    ID       Parent    Role SPI(in)  SPI(out) MsgID    ST

------------                                    ----     ------                                    --       ------    ---- --------  -------- -----    --

VPN_to_H4B_SOLIHULL_MANU_Primary                2        VPN_to_H4B_SOLIHULL_MANU_Primary          1756     759       Init 00000000 00000000 00000000 GetS
PI done

Show IKEv2 SA: Total 1 gateways found. 1 ike sa found.


BearAdmin@H4B_NGFW_1> show vpn ipsec-sa

There is no IPSec SA found.

BearAdmin@H4B_NGFW_1>
```


5.1.1 - Monitor > Logs > System

(subtype eq vpn) and (description contains 'failed')

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
07/26 12:52:34	vpn	informational	ikev2-nego-ike-fail	IKE2-Phase1-Gateway	IKEv2 IKE SA negotiation is failed as responder, non-rekey. Failed SA: 1.1.1.1[500]-1.1.1.2[500] SPI:e7007cceb3f4e822:291c2e31bfa78671.
07/26 12:52:34	vpn	informational	ikev2-nego-child-ts-bad	IKE2-Phase1-Gateway	IKEv2 child SA negotiation failed when processing traffic selector. cannot find matching IPSec tunnel for received traffic selector. received local TS: 192.168.1.1-192.168.1.1 protocol 0 port 0-65535, received remote TS: 192.168.2.1-192.168.2.1 protocol 0 port 0-65535.
07/26 12:52:29	vpn	informational	ikev2-nego-ike-fail	IKE2-Phase1-Gateway	IKEv2 IKE SA negotiation is failed as responder, non-rekey. Failed SA: 1.1.1.1[500]-1.1.1.2[500] SPI:0de826c007192f0b:34ea17005e8d9243.
07/26 12:52:29	vpn	informational	ikev2-nego-child-ts-bad	IKE2-Phase1-Gateway	IKEv2 child SA negotiation failed when processing traffic selector. cannot find matching IPSec tunnel for received traffic selector. received local TS: 192.168.1.1-192.168.1.1 protocol 0 port 0-65535, received remote TS: 192.168.2.1-192.168.2.1 protocol 0 port 0-65535.
07/26 12:52:22	vpn	informational	ikev2-nego-ike-fail	IKE2-Phase1-Gateway	IKEv2 IKE SA negotiation is failed as initiator, non-rekey. Failed SA: 1.1.1.1[500]-1.1.1.2[500] SPI:fef3fa4ba7731bf3:3750aebe34c66c0b.
07/26 12:52:19	vpn	informational	ikev2-nego-ike-fail	IKE2-Phase1-Gateway	IKEv2 IKE SA negotiation is failed as initiator, non-rekey. Failed SA: 1.1.1.1[500]-1.1.1.2[500] SPI:d8ea3b23f2bb52d6:6c08d77f9ffbc018.
07/26 11:42:07	vpn	informational	ike-config-p1-failed		IKE daemon configuration load phase-1 failed.
07/26 01:10:13	vpn	informational	ike-nego-p1-fail	IKE-GW	IKE phase-1 negotiation is failed as initiator, aggressive mode. Failed SA: 1.1.1.1[500]-1.1.1.2[500] cookie:8d9efe6450780aee:0000000000000000. Due to timeout.
07/26 01:09:41	vpn	informational	ike-generic-event		IKE_SA_INIT retransmission failed for gateway IKE-GW SN 1, trying IKEv1.
07/25 11:27:26	vpn	informational	ike-nego-p1-fail	IKE-GW	IKE phase-1 negotiation is failed as initiator, aggressive mode. Failed SA: 1.1.1.1[500]-1.1.1.2[500] cookie:77759c24bacad20d:0000000000000000. Due to timeout.
07/25 11:26:53	vpn	informational	ike-nego-p1-fail	IKE-GW	IKE phase-1 negotiation is failed as initiator, aggressive mode. Failed SA: 1.1.1.1[500]-1.1.1.2[500] cookie:f40a0ce4fcc66fdd:0000000000000000. Due to timeout.
04/29 19:24:51	vpn	informational	ike-nego-p2-fail	IPSEC-to-PA-220-2	IKE phase-2 negotiation is failed as initiator, quick mode. Failed SA: 1.1.1.1[500]-1.1.1.2[500] message id:0x142D640C. Due to negotiation timeout.
04/29 19:20:31	vpn	informational	ike-nego-p2-fail	IPSEC-to-PA-220-2	IKE phase-2 negotiation is failed as initiator, quick mode. Failed SA: 1.1.1.1[500]-1.1.1.2[500] message id:0x4CDC8883. Due to negotiation timeout.
04/29 19:12:56	vpn	informational	ike-nego-p2-fail	IPSEC-to-PA-220-2	IKE phase-2 negotiation is failed as initiator, quick mode. Failed SA: 1.1.1.1[500]-1.1.1.2[500] message id:0xE2DF049F. Due to negotiation timeout.

System filters to identify a VPN failure

```
( subtype eq vpn )  and ( description contains 'failed' )
```


5.1.1 - Troubleshooting IPSec (IKE Phase 1) – Part 1

To rule out ISP-related issues, try pinging the peer IP from the PA external interface.

ping source <external IP> **host** <peer IP>

NOTE: Ensure that pings are enabled on the peer's external interface. If pings have been blocked per security requirements, see if the other peer is responding to the main/aggressive mode messages, or the DPDs.

Check for the responses of the "Are you there?" messages from the peer in the system logs under the Monitor tab or under ikemgr logs.

Check that the IKE identity is configured correctly.

Check that the policy is in place to permit IKE and IPSec applications.

5.1.1 - Troubleshooting IPSec (IKE Phase 1) – Part 2

- **Check that proposals are correct.**
  If incorrect, logs about the mismatch can be found under the system logs, or by using the following CLI command:
  >less mp-log ikemgr.log

- **Check that pre-shared key is correct.**
  If incorrect, logs about the mismatch can be found under the system logs, or by using the following CLI command:
  >less mp-log ikemgr.log

if you open a log file

- *shift+g will take you to the end of the file (regular 'g' will take you to start of file)*
- */<keyword> to search , while in search use 'n' to go to the next or 'N' (shift+n) to go to the previous*
- *only use arrow keys to scroll up or down*

Take packet captures to analyze the traffic. Use filters to narrow the scope of the captured traffic.

- **>show vpn ike-sa gateway <name>**
- **>test vpn ike-sa gateway <name>**
- **>debug ike stat ?**

```
admin@PA-220-1> show vpn ike-sa gateway IKE-Phase1-Gateway

IKEv1 phase-1 SAs
GwID/client IP  Peer-Address           Gateway Name           Role Mode Algorithm             Established     Expiration      V  ST Xt Phase2
--------------  ------------           ------------           ---- ---- ---------             -----------     ----------      -  -- -- ------
1               1.1.1.2                IKE-Phase1-Gateway     Resp Aggr PSK/ DH2/A256/SHA512  Aug.11 17:39:35 Aug.12 01:39:35 v1 13 1  2

Show IKEv1 IKE SA: Total 1 gateways found. 1 ike sa found.


IKEv1 phase-2 SAs
Gateway Name           TnID     Tunnel                 GwID/IP          Role Algorithm          SPI(in)  SPI(out) MsgID    ST Xt
------------           ----     ------                 -------          ---- ---------          -------  -------- -----    -- --
IKE-Phase1-Gateway     1        IPSec-Tunnel.3_1.1.1.1 1                Resp ESP/ DH2/tunl/     C7E4DE93 9347DE6A 238D6F49 9  1

Show IKEv1 phase2 SA: Total 1 gateways found. 1 ike sa found.
```


5.1.1 - Advanced CLI Commands (IKE Phase 1) - Reference

- **For detailed logging, turn on the logging level to debug:**

```
debug ike global on debug
less mp-log ikemgr.log
```

- **To view the main/aggressive and quick mode negotiations, it is possible to turn on pcaps for capturing these negotiations. Messages 5 and 6 onwards in the main mode and all the packets in the quick mode have their data payload encrypted:**

```
debug ike pcap on
        view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap
```

- **Turn off debugs**

```
debug ike pcap off
```

- **Configuring packet filter and captures restricts pcaps only to the one worked on, debug IKE pcap on shows pcaps for all VPN traffic.**
- **To check if NAT-T is enabled, packets will be on port 4500 instead of 500 from the 5th and 6th messages of main mode.**
- **Check if vendor id of the peer is supported on the Palo Alto Networks device and vice-versa.**

5.1.1 - Troubleshooting IPSec (IKE Phase 2) - Part 1

- **Check if the firewalls are negotiating the tunnels, and ensure that 2 unidirectional SPIs exist:**

```
show vpn ipsec-sa
show vpn ipsec-sa tunnel <tunnel.name>
```

- **Check if proposals are correct.**
- **Check if pfs is enabled on both ends.**
- **Check the proxy-id configuration.**

```
less mp-log ikemgr.log
```

- **Useful CLI commands:**

```
show vpn flow name <tunnel.id/tunnel.name>
show vpn flow name <tunnel.id/tunnel.name> | match bytes
```


5.1.1 - Troubleshooting IPSec (IKE Phase 2) - Part 2

- **Check if encapsulation and decapsulation bytes are increasing. If the firewall is passing traffic, then both values should be increasing.**

```
show vpn flow name <tunnel.id/tunnel.name> | match bytes
```

- If encapsulation bytes are increasing and decapsulation is constant, then the firewall is sending, but not receiving packets.
- **Check to see if a policy is dropping the traffic, or if a port translation device in front of our firewall is dropping the ESP packets.**

```
show vpn flow name <tunnel.id/tunnel.name> | match bytes
```

Check to see if a policy is dropping the traffic:

```
test routing fib-lookup virtual-router default ip <destination IP>
```

```
------------------------------------------------
runtime route lookup
------------------------------------------------
virtual-router:  default
destination:     10.5.1.1
result:          interface tunnel.1
```

```
show routing route
test vpn ipsec-sa tunnel <name>
```


5.1.1 - Advanced CLI Commands (IKE Phase 2) - Reference

- **Advanced CLI Commands:**
  - `debug ike global on debug`
  - `less mp-log ikemgr.log`
  - `debug ike pcap on`
  - `view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap`
  - `debug ike pcap off`

- **If tunnels are up but traffic is not passing through the tunnel:**
  - **Check security policy and routing.**
  - **Check for any devices upstream that perform port-and-address-translations.**
    Because ESP is a layer 3 protocol, ESP packets do not have port numbers. When such devices receive ESP packets, there is a high possibility they may silently drop them, because they do not see the port numbers to translate.
  - **Apply debug packet filters, captures or logs, if necessary, to isolate the issue where the traffic is getting dropped.**

				IKE Gateway/Satellite				Tunnel Interface					
	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS	COMMENT
☑	IPSec-Tunnel.3_1.1.1.2-to-1.1.1.1	Tunnel Info	Auto Key	ethernet1/3	1.1.1.2/30	1.1.1.1	IKE Info	tunnel.3	default (Show Routes)	vsys1	VPN		IPSec Tunnel to PA-220-1 in Seattle

5.1.1 - Common VPN Error Messages - Reference

If Error is this:	Try This:
IKE phase-1 negotiation is failed as initiator, main mode. Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout. **or** **IKE phase 1 negotiation is failed. Couldn't find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]**	• Verify that the public IP address for each VPN peer is accurate in the IKE Gateway configuration. • Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure.
Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored... **or** **IKE phase-1 negotiation is failed. Unable to process peer's SA payload.**	Check the IKE Crypto profile configuration to verify that the proposals on both sides have a common encryption, authentication, and DH Group proposal.
pfs group mismatched:my: 2peer: 0 **or** **IKE phase-2 negotiation failed when processing SA payload. No suitable proposal found in peer's SA payload.**	Check the IPSec Crypto profile configuration to verify that: • pfs is either enabled or disabled on both VPN peers • the DH Groups proposed by each peer has at least one DH Group in common
IKE phase-2 negotiation failed when processing Proxy ID. Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.	The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto Networks firewall.

5.1.1 - Common VPN Error Messages - Reference

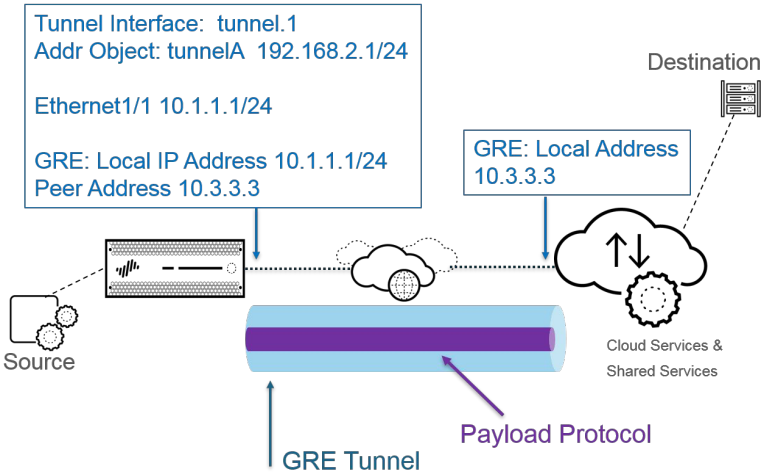
Test in Lab and validate in Logs > System:
Change IKE Gateway config to use the “default” crypto profile, rather than “IKE-Phase1-MaxCrypto” profile.

IKE Advanced Options						
MODE	PASSIVE MODE	NAT TRAVERSAL	CRYPTO PROFILE	DPD	LIVENESS	COMMENT
auto	☐	☐	IKE-Phase1-MaxCrypto	enabl...		IPSec Tunnel to PA-220-2 in San Francisco

IKE Advanced Options						
MODE	PASSIVE MODE	NAT TRAVERSAL	CRYPTO PROFILE	DPD	LIVENESS	COMMENT
auto	☐	☐	default	enabl...		IPSec Tunnel to PA-220-1 in Seattle

5.1.1 - Fundamentals of GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network. GRE packets that are encapsulated within IP use IP protocol type 47



The firewall does not support routing a GRE or IPSec tunnel to a GRE tunnel, but you can route a GRE tunnel to an IPSec tunnel.

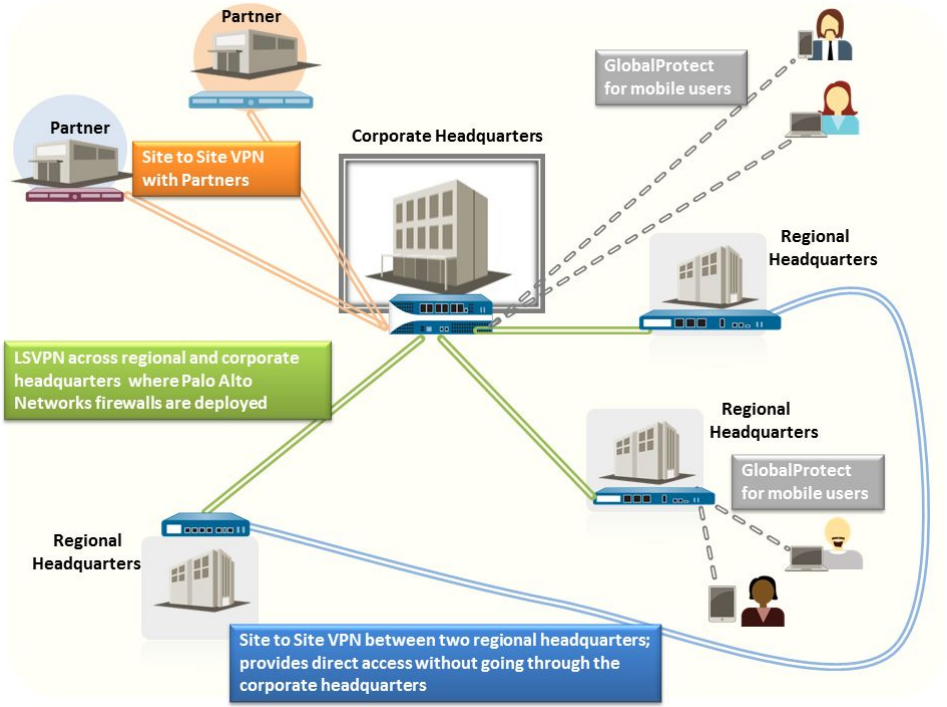
Additionally:
A GRE tunnel does not support QoS.

The firewall does not support a single interface acting as both a GRE tunnel endpoint and a decryption broker.

GRE tunneling **does not** support NAT between GRE tunnel endpoints.

5.1.2
Troubleshooting One-to-One and One to Many Tunnels

5.1.1 - Types of VPNs Supported



- **Site-to-Site VPN**
- **Remote User-to-Site VPN**
- **Large Scale VPN (LSVPN) or (1-to-Many)**

5.1.3 - Types of VPNs and Proxy IDs

Route-Based VPNs

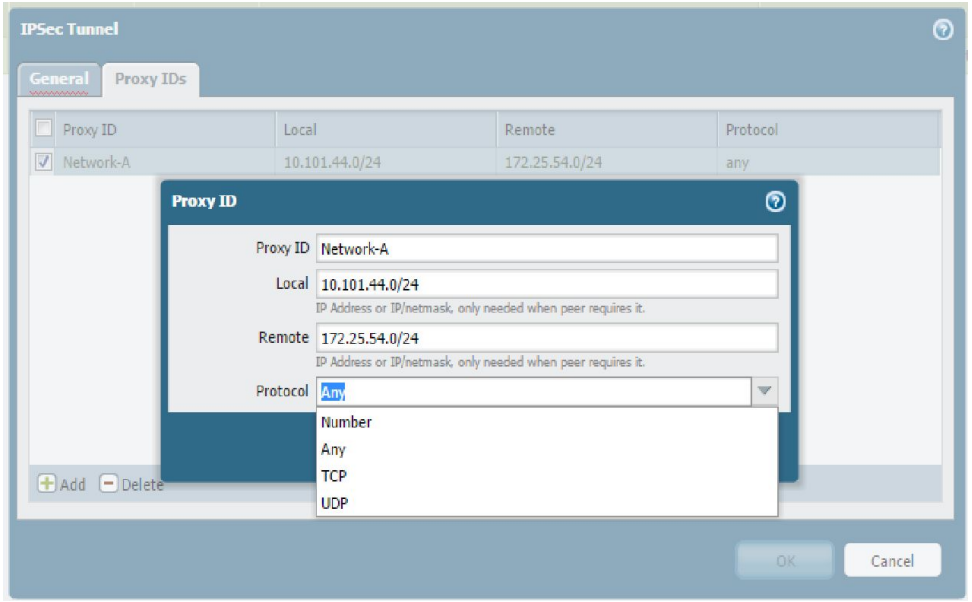
- Firewalls that support route-based VPNs: Palo Alto Firewalls, Juniper SRX, Juniper Netscreen, and Checkpoint.
- IPSec tunnel is invoked during route lookup for remote end of the proxy-ID
- Remote end of the interesting traffic has a route pointing out through the tunnel interface.
- Supports routing (static, dynamic) over VPNs.
- Proxy-IDs are configured as part of the VPN setup.

Policy-Based VPNs

- **Firewalls that support policy-based VPNs:** Juniper SRX, Juniper Netscreen, **Cisco ASA**, and Checkpoint.
- The IPSEC tunnel is invoked during policy lookup for policy-based matching the interesting traffic.
- No tunnel interfaces. The remote has a route pointed out through the default gateway.
- No tunnel interfaces = No routing over VPNs.
- Polices and ACLs configured for the interesting traffic serve as the proxy-IDs for the tunnels.

Key Takeaway: The most important take away is to just understand that Proxy IDs are **REQUIRED** when the other end of the tunnel is configured to use policy-based VPN (Cisco) in comparison the route-based VPN (Palo Alto Networks).

5.1.3 - Proxy ID's



Proxy ID's – Must define proxy IDs when connecting to peers that support policy-based VPN.

IKE Versions:

IKEv1 supports only Proxy-ID exact match.

IKEv2, there is support traffic selector narrowing when the proxy ID setting is different on the two VPN gateways.


QUIZ
TIME

5.2 Troubleshoot Physical Interfaces

5.2.1 - Copper and Fiber Ports - Reference

Copper:
The status of the link light should be **solid green** if the link is up.

IF link is **not up** or the LED is not solid green **THEN**:
- Check for the Physical damage on the cable
- Check cable type: CAT5/6
- Replace with Known-Good cable.
- If using a patch panel, try different patch interfaces.
- Verify speed/duplex settings on both sides of the link.
- Check if the distance specification of the cable. :

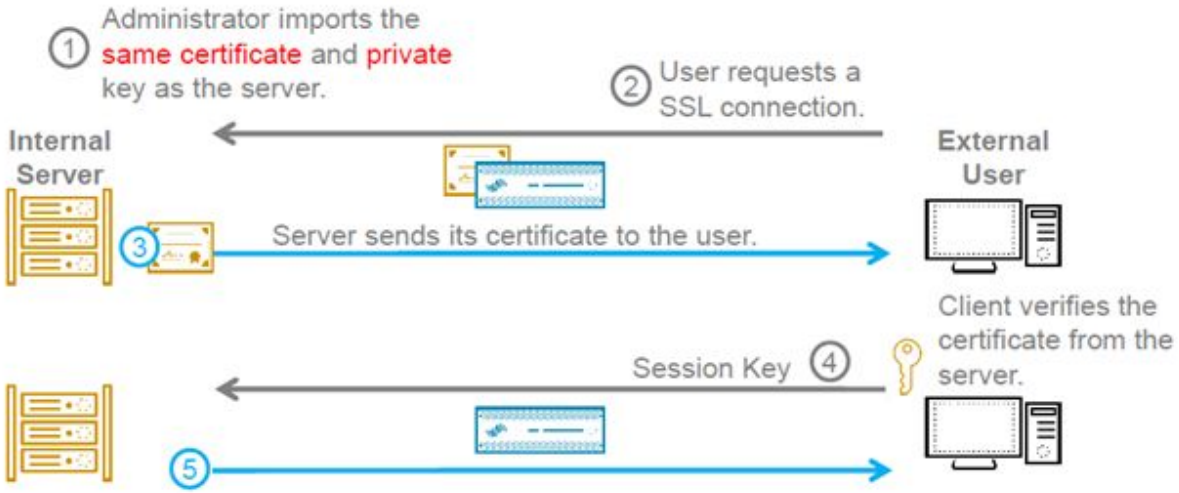
Fiber ports:

IF the connection is Fiber, **THEN**
- Ensure fiber connections are clean
- Try another transceiver and cable if fiber(SM or MM)
- Check power levels for fiber links to ensure the cable does not have signal loss
- Is it the correct type of transceiver? GBIC, SFP, XFP, SFP+, QSFP, QSFP+, etc.
- Check for the transceiver transmit light on by using the power meter
- Verify of the optics are supported by Palo Alto. A list of supported optics can be found here.


QUIZ
TIME

5.3 Troubleshoot SSL Decryption

5.3.5 - SSL Inbound Decryption

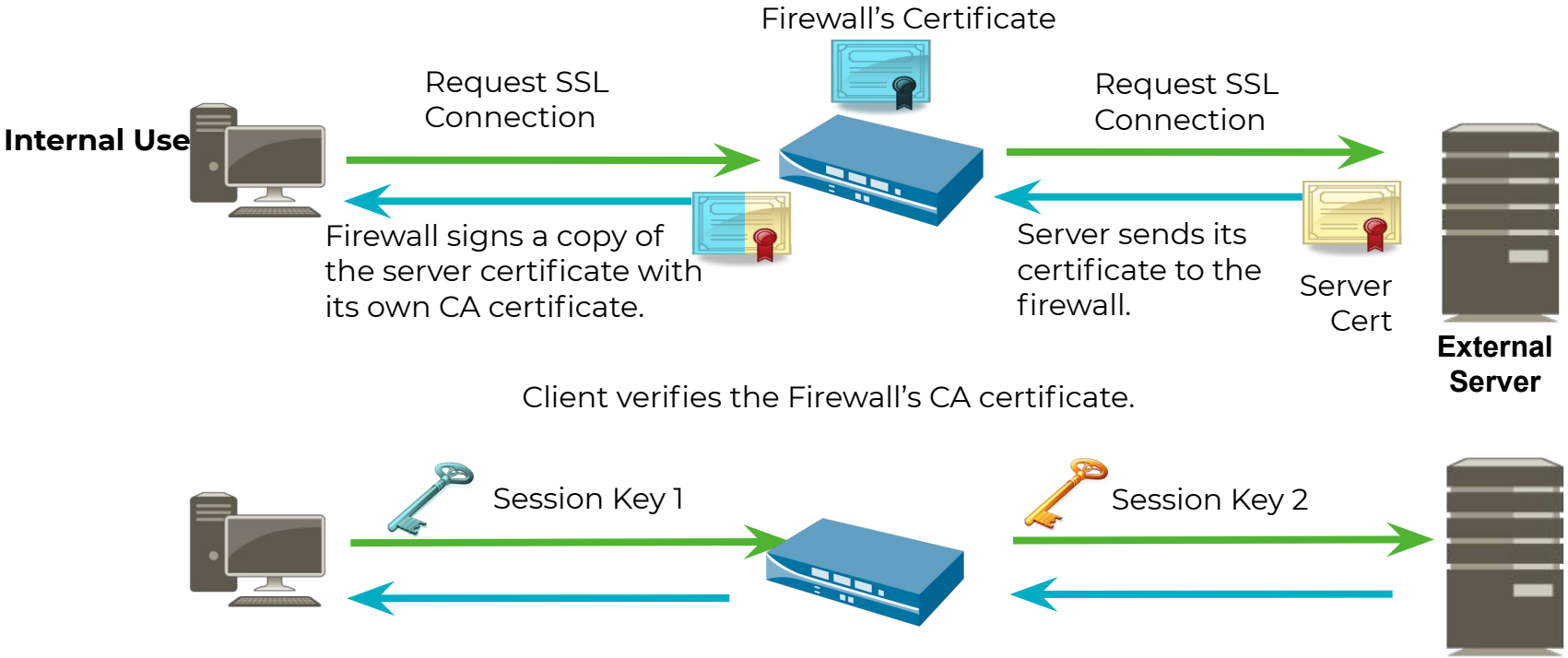


- The packet data remains unchanged and the connection is secure from the client system to the internal SSL server.

Common Problems

Unsupported cipher suites
Unsupported EC curves
Server using certificate chains
Server sending client certificate verify
Server Configured with client certificate authentication
Client sending SSL alert due to unknown certificate or bad certificate.

5.3.6 - How SSL Forward Proxy Works (Outbound) - Reference



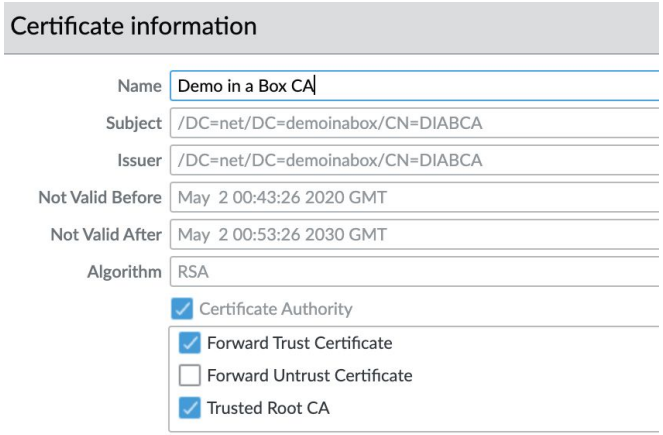
Note: By default firewall generates a cert with same Key size as the certificate the external server presented.
Note: TLS 1.3 improves upon this by doing key exchange on initial cert negotiation.

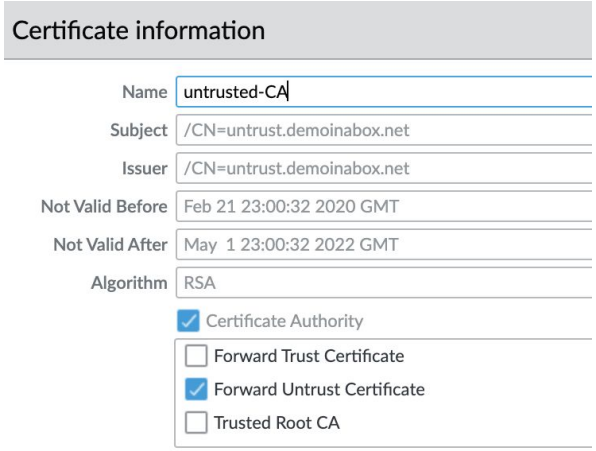
5.3.6 - Forward Trust / Forward Untrust Certificate

Certificates need to be assigned two roles:

- **Forward Trust Certificate** - a trusted certificate is presented to the endpoint when the firewall is able to successfully validate the site the endpoint is connecting to

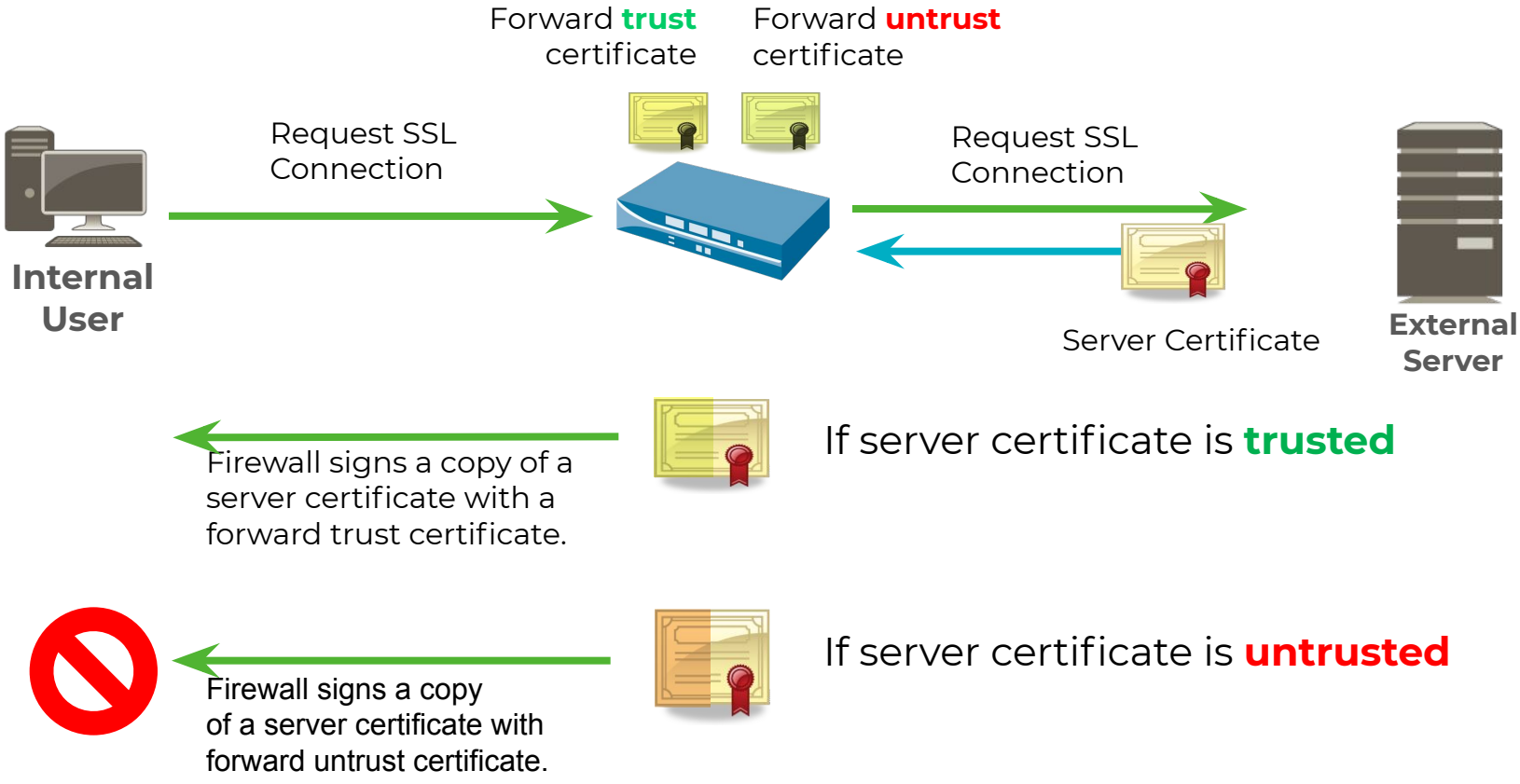
- **Forward Untrust Certificate** - an untrusted certificate is presented to the endpoint when the firewall is unable to validate the site the endpoint is connecting to, i.e., the certificate is expired or otherwise invalid.





Note: Know how to identify type of certificate, Self-Signed, CA Signed, etc...
Note: Must use CA certificate for SSL Forward Proxy

5.3.6 - Forward Trust and Untrust Certificates (Outbound) - Reference



5.3.6 - Decryption Failure Reasons - Reference

- **decrypt-cert-validation -** The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when the session uses client authentication or when the session uses a server certificate with any of the following conditions: expired, untrusted issuer, unknown status, or status verification time-out.

- **This session end reason also displays when the server certificate produces a fatal error alert of type:** bad_certificate, unsupported_certificate, certificate_revoked, access_denied, or no_certificate_RESERVED (SSLv3 only).

- **decrypt-unsupport-param -** The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when the session uses an unsupported protocol version, cipher, or SSH algorithm. This session end reason is displays when the session produces a fatal error alert of type: unsupported_extension, unexpected_message, or handshake_failure.

- **decrypt-error -** The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when firewall resources or the hardware security module (HSM) were unavailable. This session end reason is also displayed when you configured the firewall to block SSL traffic that has SSH errors or that produced any fatal error alert other than those listed for the **decrypt-cert-validation** and **decrypt-unsupport-param** end reasons.

References:
Decryption Overview
Implement and Test SSL Decryption

Troubleshoot and Monitor Decryption

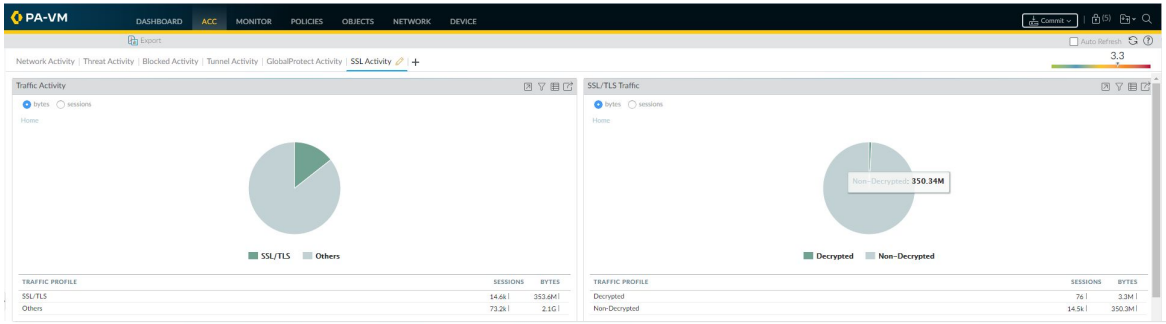
Requirements:

- Identify traffic that causes decryption failures by Service Name Identification (SNI) and application.
- Identify traffic that uses weak protocols and algorithms.
- Examine successful and unsuccessful decryption activity in the network.
- View detailed information about individual sessions.
- Profile decryption usage and patterns.

Monitor detailed decryption statistics and information about adoption, failures, versions, algorithms using the following tools:

- ACC > SSL Activity > Decryption Failure Reasons
- Monitor > Logs > Decryption (also the ‘Decrypted’ column in Monitor > Logs > Traffic)
- Local Decryption Exclusion Cache
- Custom Report Templates for Decryption

5.3.1 - Decryption using ACC Widgets



ACC > SSL Activity

Traffic Activity
SSL/TLS Traffic Activity
Decryption Failure Reasons
Successful TLS Version Activity
Successful Key Exchange Activity

5.3.1 - Monitor > Logs > Decryption

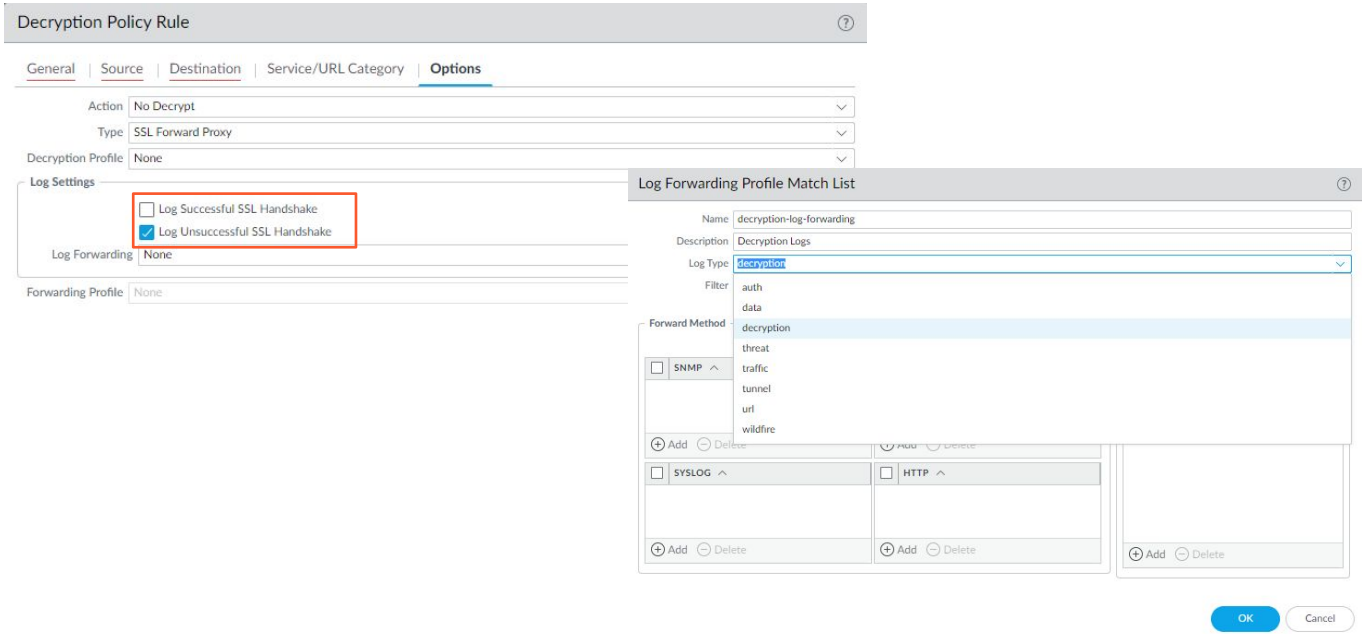
Provides comprehensive information about sessions that match a decryption policy.
Firewall doesn't log network traffic unless it matches a Decryption Policy rule.

RECEIVE TIME	APPLICATION	POLICY NAME	SOURCE ZONE	DESTINATION ZONE	PROXY TYPE	SOURCE ADDRESS	SOURCE USER	DESTINATION ADDRESS	ROOT COMMON NAME	ROOT STATUS	SUBJECT COMMON NAME	ISSUER COMMON NAME	CERTIFICATE START DATE
08/01 18:03:47	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		98.136.103.23	DigiCert High Assurance EV Root CA	trusted	src6.yahoo.com	DigiCert SHA2 High Assurance Server CA	2021/07/12 17:00:00
08/01 18:03:46	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		192.0.66.2	ISRG Root X1	trusted	mercurynews.com	R3	2021/07/08 13:45:12
08/01 18:03:45	pinterest-base	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		151.101.0.84	DigiCert Global Root CA	trusted	*.pinterest.com	DigiCert TLS RSA SHA256 2020 CA1	2021/07/26 17:00:00
08/01 18:03:44	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.86.90.179	DigiCert Global Root CA	trusted	groupon.com	DigiCert TLS RSA SHA256 2020 CA1	2021/01/31 16:00:00
08/01 18:03:44	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.17.74.91	Baltimore CyberTrust Root	trusted	sni.cloudflaressl.com	Cloudflare Inc ECC CA-3	2021/07/03 17:00:00
08/01 18:03:43	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.196.26.7	ISRG Root X1	trusted	shopify.com	R3	2021/07/28 04:56:01
08/01 18:03:43	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.16.6.49	Baltimore CyberTrust Root	trusted	patreon.com	Cloudflare Inc ECC CA-3	2021/06/07 17:00:00
08/01 18:03:42	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.26.9.237	Baltimore CyberTrust Root	trusted	doi.org	Cloudflare Inc ECC CA-3	2021/07/07 17:00:00
08/01 18:03:37	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.26.5.246	Baltimore CyberTrust Root	trusted	sni.cloudflaressl.com	Cloudflare Inc ECC CA-3	2021/06/14 17:00:00
08/01 18:02:44	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		35.190.29.187	DigiCert Global Root CA	trusted	*.evernote.com	DigiCert SHA2 Secure Server CA	2020/09/01 17:00:00
08/01 18:02:43	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		67.199.248.14	DigiCert Global Root CA	trusted	*.bitly.com	DigiCert TLS RSA SHA256 2020 CA1	2021/06/23 17:00:00
08/01 18:02:39	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		162.159.129.81	Baltimore CyberTrust Root	trusted	sni.cloudflaressl.com	Cloudflare Inc ECC CA-3	2021/05/17 17:00:00
08/01 18:02:39	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.21.11.58	Baltimore CyberTrust Root	trusted	sni.cloudflaressl.com	Cloudflare Inc ECC CA-3	2021/07/03 17:00:00
08/01 18:02:02	glassdoor-base	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		104.17.91.51	Baltimore CyberTrust Root	trusted	glassdoor.com	Cloudflare Inc ECC CA-3	2021/06/05 17:00:00
08/01 18:02:02	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		45.60.131.229	DigiCert High Assurance EV Root CA	trusted	www.digicert.com	DigiCert SHA2 Extended Validation Server CA	2021/04/25 17:00:00
08/01 18:02:00	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		77.88.55.60	Certum Trusted Network CA	trusted	yandex.ru	Yandex CA	2021/03/18 06:58:41
08/01 18:01:59	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		5.57.16.220	DigiCert Global Root CA	trusted	*.booking.com	DigiCert ECC Secure Server CA	2020/10/13 17:00:00
08/01 18:01:59	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		182.22.59.229	Security Communication RootCA2	trusted	edge01.yahoo.co.jp	Cybertrust Japan SureServer CA G4	2021/05/23 18:00:59
08/01 18:01:58	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		128.30.52.100	USERTrust RSA Certification Authority	trusted	*.w3.org	Gandi Standard SSL CA 2	2021/06/01 17:00:00
08/01 18:01:58	web-browsing	Decrypt-HTTP2	L3-Trust	L3-Untrust	Forward	192.168.60.250		125.209.222.141	DigiCert Global Root CA	trusted	www.naver.net	DigiCert SHA2 Secure Server CA	2020/06/02 17:00:00

5.3.1 - Decryption Logging

- **Log successful SSL handshakes** and **unsuccessful SSL handshakes** to gain visibility into as much decrypted traffic as your device's available resources permit (don't decrypt private or sensitive traffic; follow decryption best practices and decrypt as much traffic as you can)

- Create a **Log Forwarding profile** to forward Decryption logs to Log Collectors



5.3.2 - Identifying Encrypted Traffic using CLI

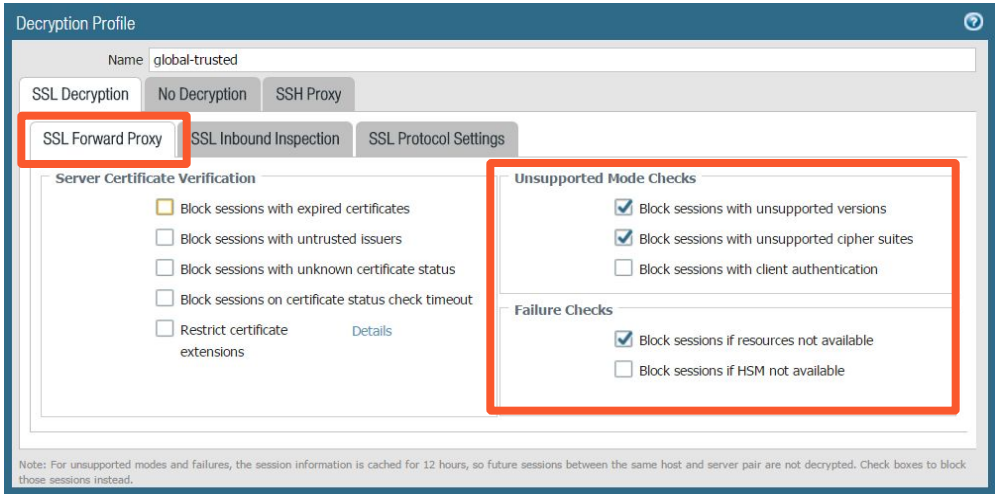
```
admin@PA-220-1> show session all filter ssl-decrypt yes

OR

admin@PA-220-1> show session all | match "*NS"

--------------------------------------------------------------------------------
ID          Application     State   Type Flag  Src[Sport]/Zone/Proto (traNS*lated IP[Port])
Vsys                                           Dst[Dport]/Zone (traNS*lated IP[Port])
--------------------------------------------------------------------------------
21187       DNS*            ACTIVE  FLOW *NS   192.168.1.18[65483]/Trust-L3/17  (73.254.100.132[11558])
vsys1                                          8.8.8.8[53]/Untrust-L3  (8.8.8.8[53])
56897       google-base     ACTIVE  FLOW *NS   192.168.1.19[18928]/Trust-L3/6  (73.254.100.132[24384])
vsys1                                          74.125.195.188[5228]/Untrust-L3  (74.125.195.188[5228])
19739       DNS*            ACTIVE  FLOW *NS   192.168.1.13[64424]/Trust-L3/17  (73.254.100.132[63878])
vsys1                                          8.8.8.8[53]/Untrust-L3  (8.8.8.8[53])
47649       google-base     ACTIVE  FLOW *NS   192.168.1.25[51084]/Trust-L3/6  (73.254.100.132[6849])
vsys1                                          108.177.98.188[5228]/Untrust-L3  (108.177.98.188[5228])
15343       rtcp            ACTIVE  FLOW *NS   192.168.1.11[53199]/Trust-L3/17  (73.254.100.132[37040])
vsys1                                          213.179.212.235[50004]/Untrust-L3  (213.179.212.235[50004])
17299       google-base     ACTIVE  FLOW *NS   192.168.1.29[53919]/Trust-L3/6  (73.254.100.132[1328])
vsys1                                          74.125.142.188[5228]/Untrust-L3  (74.125.142.188[5228])
```

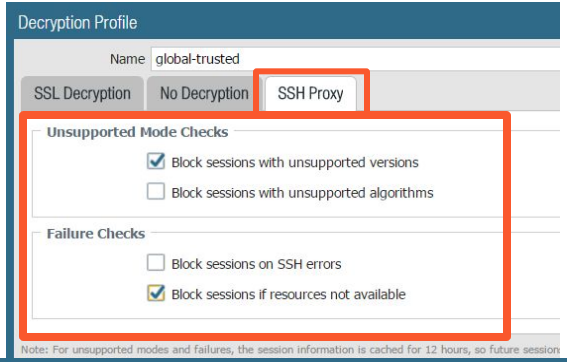
The session flag options are NS, ND, NB and refer to NAT - Source, Destination or Both. Nothing in the flag field means there is no NAT in the session.

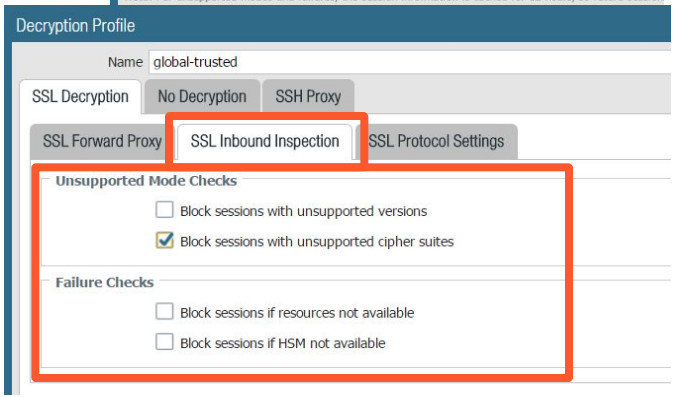
NOTE: The (*) asterisk indicates that the traffic is decrypted

5.3.3 - Unsupported Mode and Failure Checks

Objects > Decryption Profile



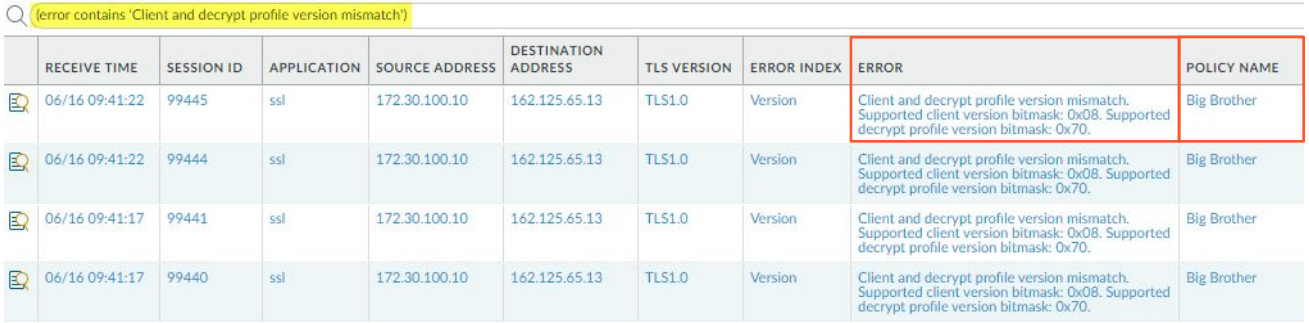




Are there any blocked sessions, if so:
View the configuration to determine the firewalls response to unsupported modes and failure checks.

5.3.3 - Troubleshoot Unsupported Cipher Suites

In the Decryption log (**Monitor Logs Decryption**), use the query **(error contains 'Client and decrypt profile mismatch'** to identify all cipher suite version mismatches.
The hexadecimal codes **(0x70)** identify the exact version that the client supports and the exact version that the Decryption profile supports.
The errors show a client and Decryption profile mismatch. The supported client bitmask is 0x08 and the supported Decryption profile bitmask is 0x70:


(error contains 'Client and decrypt profile version mismatch')

	RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
	06/16 09:41:22	99445	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:22	99444	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:17	99441	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:17	99440	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother

For Example:

```
admin@VM-1> debug dataplane show ssl-decrypt bitmask-version0x08
TLSv1.0

admin@VM-1> debug dataplane show ssl-decrypt bitmask-version0x70
TLSv1.1
TLSv1.2
TLSv1.3
```

References: Unsupported Cipher Suites

5.3.3 - Remediating Unsupported Cipher Suites

There are multiple ways to address this issue.

Update the client so that it accepts a more secure TLS version. **(Preferred)**

If the client requires TLSv1.0 for some reason, you can continue to let the firewall block the traffic. **(Preferred, but not ideal)**

Update the Decryption profile to allow all TLSv1.0 traffic **(Not Recommended)**

Create a decryption policy and profile that allow TLSv1.0 and apply it only to the client devices that must use TLSv1.0 and cannot support a more secure protocol. **(Compromise)**

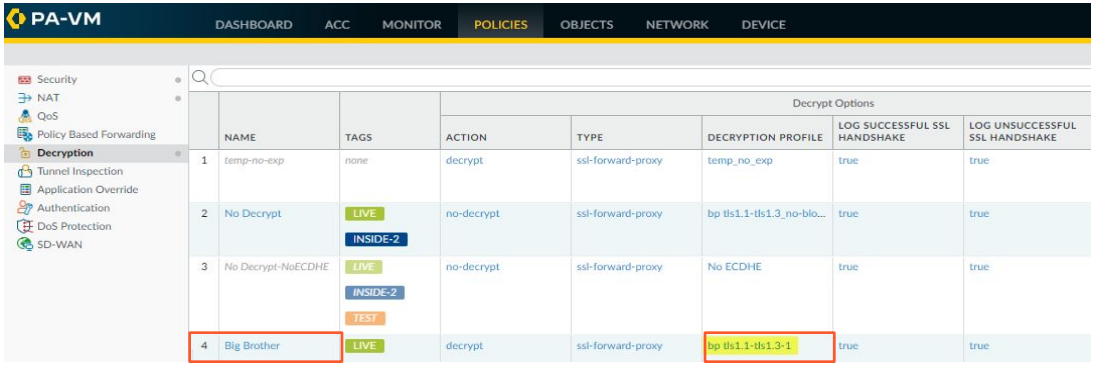
References:
Decryption Overview
Implement and Test SSL Decryption

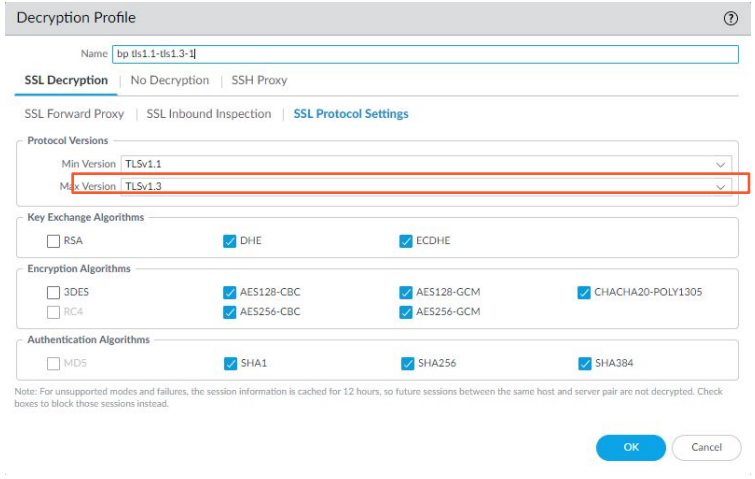
5.3.3 - Remediating Unsupported Cipher Suites

Create a decryption policy and profile that allow TLSv1.0 and apply it only to the client devices that must use TLSv1.0 and cannot support a more secure protocol.

For Example:

Identify the Decryption policy name, which is “**Big Brother**”
Identify the Decryption profile name, which is “**bp tls1.1-tls1.3-1**”

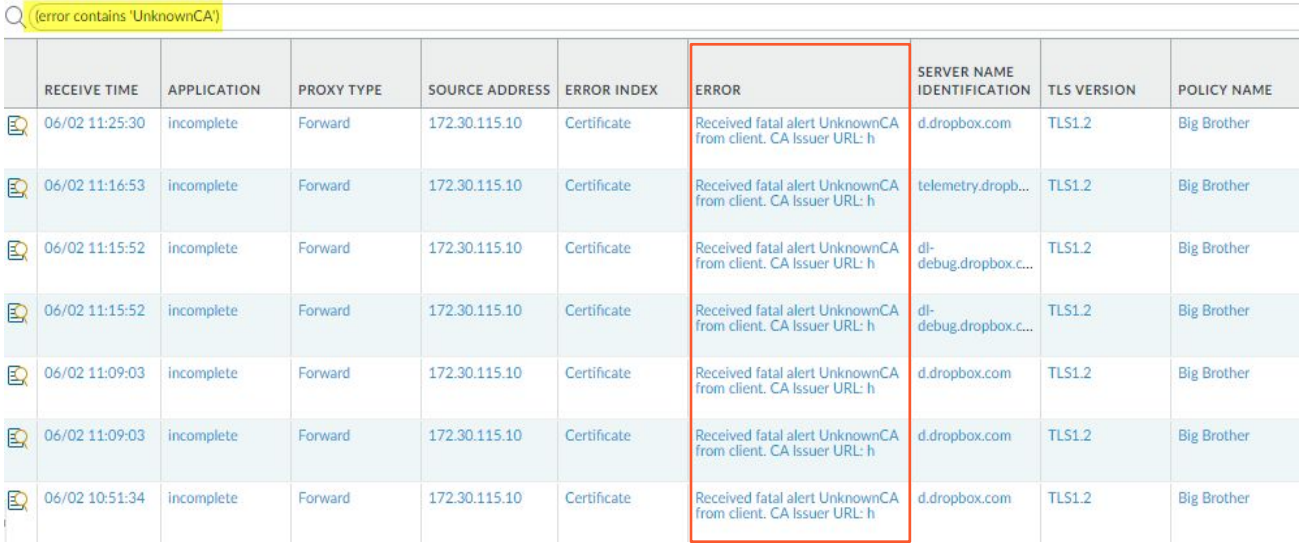




Select the **bp tls1.1-tls1.3-1** decryption profile and click the **SSL Protocol Settings** tab.
The minimum TLS protocol version **(Min Version)** that the profile supports is TLSv1.1. To allow the traffic that the version mismatch blocks, you could change the Min Version to **TLSv1.0.**

5.3.4 - Troubleshoot Pinned Certificates

Monitor > Logs > Decryption
to locate pinned certificates using the filter:
`(error contains 'UnknownCA') or (error contains 'BadCertificate')`


(error contains 'UnknownCA')

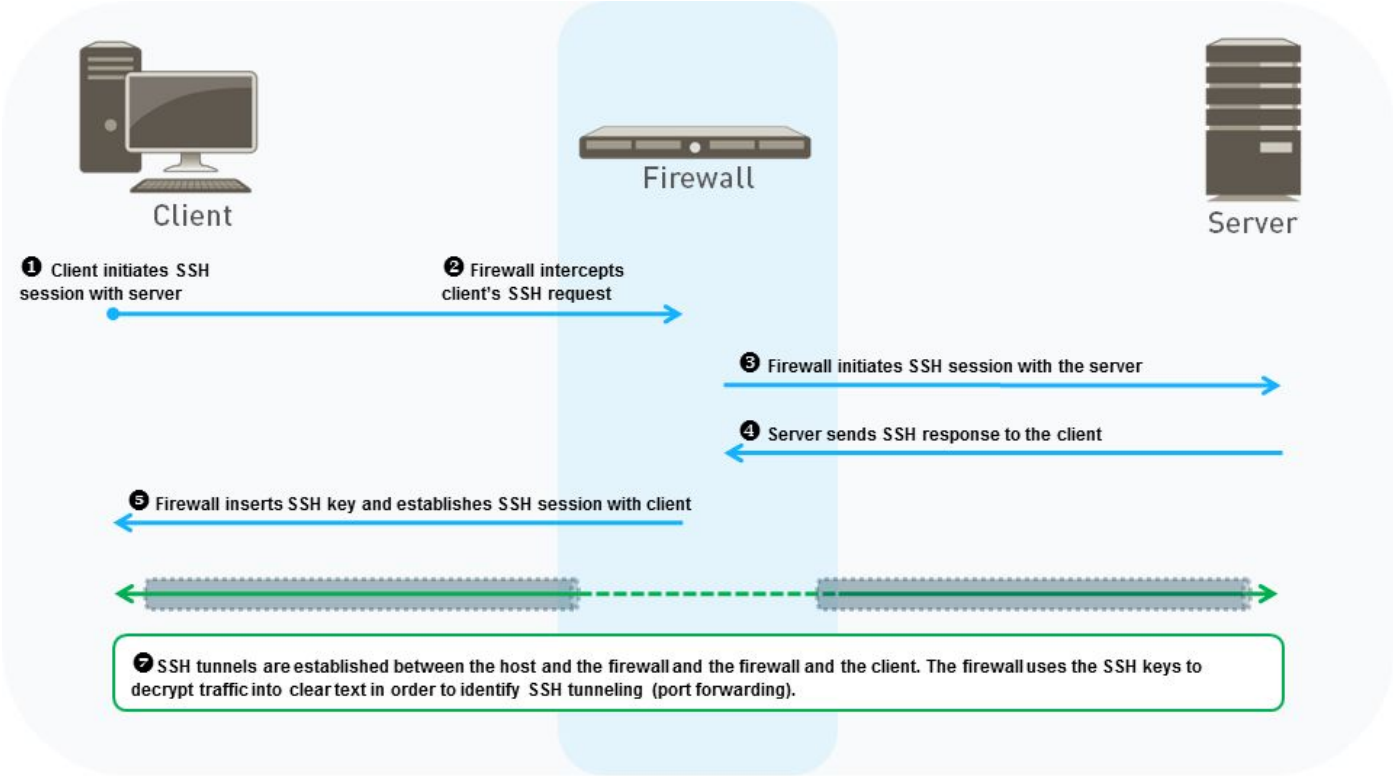
	RECEIVE TIME	APPLICATION	PROXY TYPE	SOURCE ADDRESS	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	TLS VERSION	POLICY NAME
	06/02 11:25:30	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
	06/02 11:16:53	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	telemetry.dropb...	TLS1.2	Big Brother
	06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
	06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
	06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
	06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
	06/02 10:51:34	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother

Important Note: A TLS error will be generated when it the firewall fails to verify the server's certificate. Different applications may use different error codes to indicate a pinned certificate. The most common error indicators for pinned certificates are Unknown CA and Bad Certificate

If necessary you can add a SSL Decryption Exclusion - **Device > Certificate Management > SSL Decryption Exclusions**

References: Certificate Pinning

5.3.7 - Troubleshooting SSH Proxy

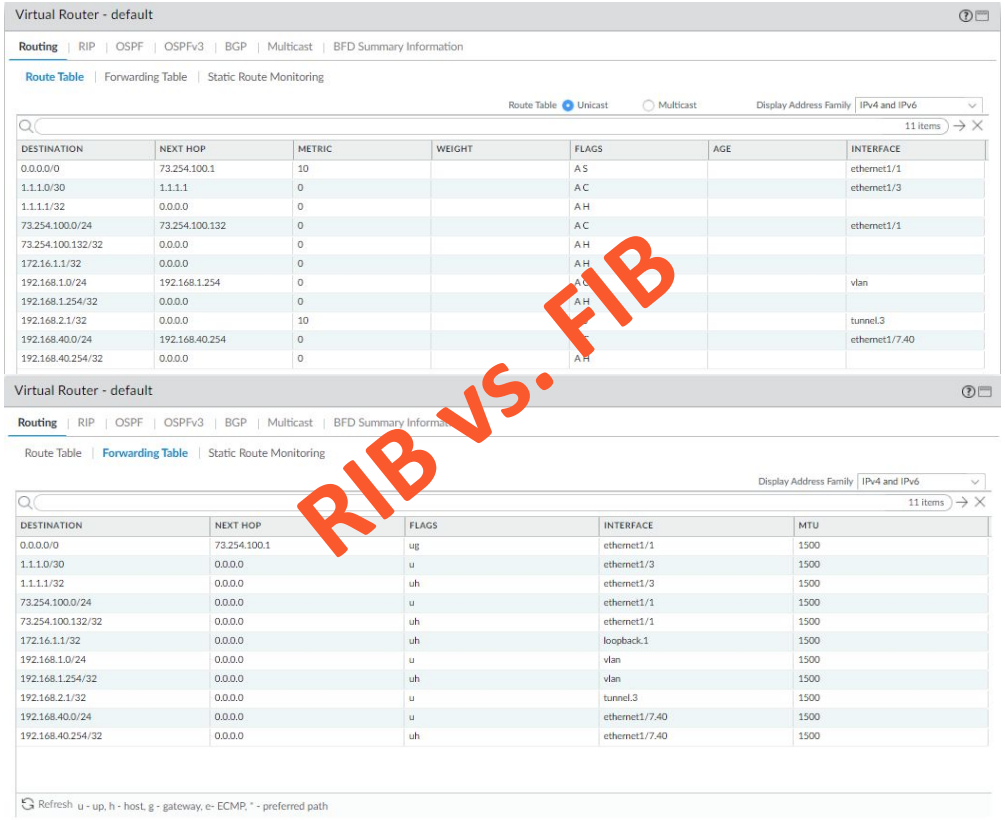



QUIZ
TIME


Break

5.3 Troubleshoot Routing

5.4.1 – Routing and Forwarding Information Base



Palo Alto NGFWs allow you to use multiple virtual routers (VRFs). Interfaces are then attached to the routers in order to facilitate the routing of packets.

FIB - Forwarding Information Base
RIB - Routing Information Base

Under **runtime stats**, there is both a FIB and a RIB.

Virtual Routers and Runtime Statistics
Static Routes
RIP
OSPF
BGP

5.4.1 – Virtual Routers – View RIB in CLI

```
admin@PA-220-1> show routing route

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2, E:ecmp, M:multicast

VIRTUAL ROUTER: default (id 1)
  ==========
destination                              nexthop                              metric flags      age   interface
next-AS
0.0.0.0/0                                73.254.100.1                         10     A S              ethernet1/1
1.1.1.0/30                               1.1.1.1                              0      A C              ethernet1/3
1.1.1.1/32                               0.0.0.0                              0      A H
73.254.100.0/24                          73.254.100.132                       0      A C              ethernet1/1
73.254.100.132/32                        0.0.0.0                              0      A H
172.16.1.1/32                            0.0.0.0                              0      A H
192.168.1.0/24                           192.168.1.254                        0      A C              vlan
192.168.1.254/32                         0.0.0.0                              0      A H
192.168.2.1/32                           0.0.0.0                              10     A S              tunnel.3
192.168.40.0/24                          192.168.40.254                       0      A C              ethernet1/7.40
192.168.40.254/32                        0.0.0.0                              0      A H
total routes shown: 11
```

5.4.0 – Virtual Routers – View FIB in CLI

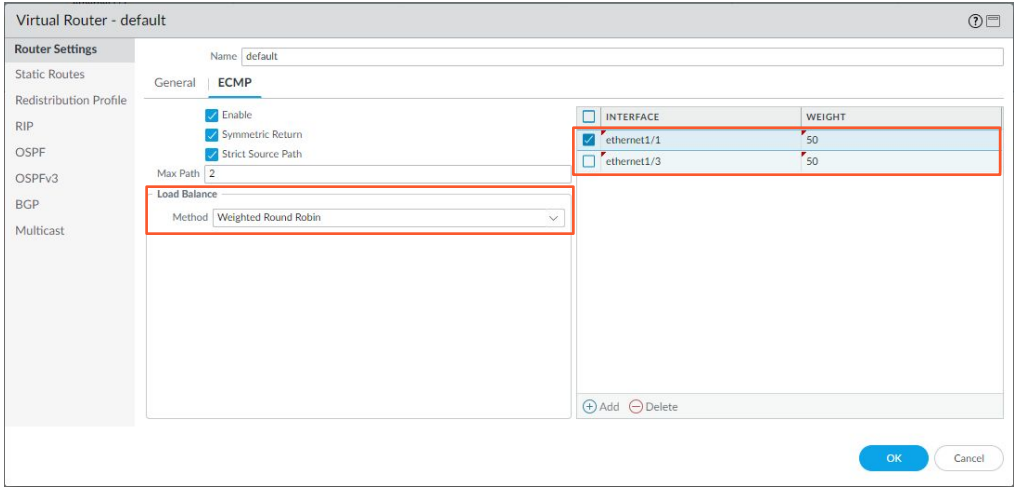
```
admin@PA-220-1> show routing fib

total virtual-router shown :              1
--------------------------------------------------------------------------------
virtual-router name: default
interfaces:
   ethernet1/1 ethernet1/3 ethernet1/7 ethernet1/7.40
   loopback.1 tunnel.3 vlan

route table:
flags: u - up, h - host, g - gateway, e - ecmp, * - preferred path

maximum of fib entries for device:                 10000
maximum of IPv4 fib entries for device:            10000
maximum of IPv6 fib entries for device:            2500
number of fib entries for device:                  11
maximum of fib entries for this fib:               10000
number of fib entries for this fib:                11
number of fib entries shown:                       11

id      destination           nexthop            flags  interface          mtu
--------------------------------------------------------------------------------
45      0.0.0.0/0             73.254.100.1       ug     ethernet1/1        1500
2       1.1.1.0/30            0.0.0.0            u      ethernet1/3        1500
1       1.1.1.1/32            0.0.0.0            uh     ethernet1/3        1500
44      73.254.100.0/24       0.0.0.0            u      ethernet1/1        1500
43      73.254.100.132/32     0.0.0.0            uh     ethernet1/1        1500
--------------------------------------------------------------------------------
```

5.4.0 – Equal Cost Multiple Path (ECMP)

ECMP processing is a networking feature that enables the firewall to use up to four equal-cost routes to the same destination.

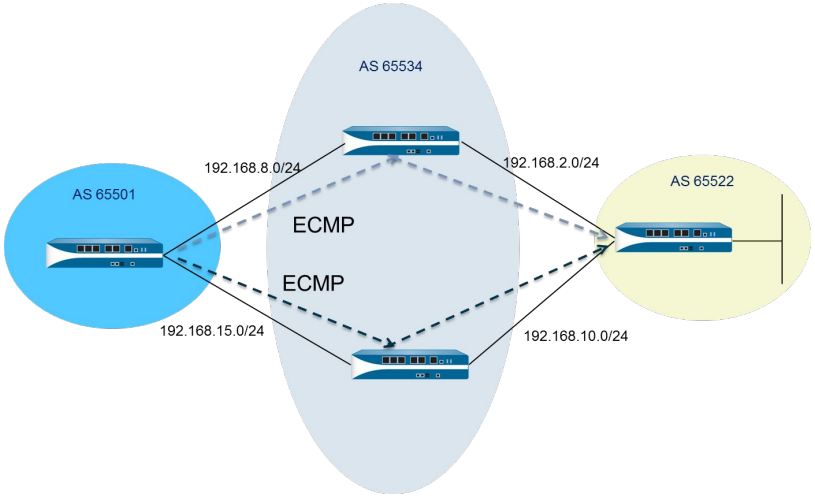
Load balance flows (sessions) to the same destination over multiple equal-cost links to make use of available bandwidth on all links toward the destination, rather than leaving links unused.

Dynamically shifts traffic to another ECMP member to the same destination when a link fails, rather than waiting for the routing protocol or RIB table to elect an alternative path. This reduces time and eliminates the need for the routing protocol to reconverge.

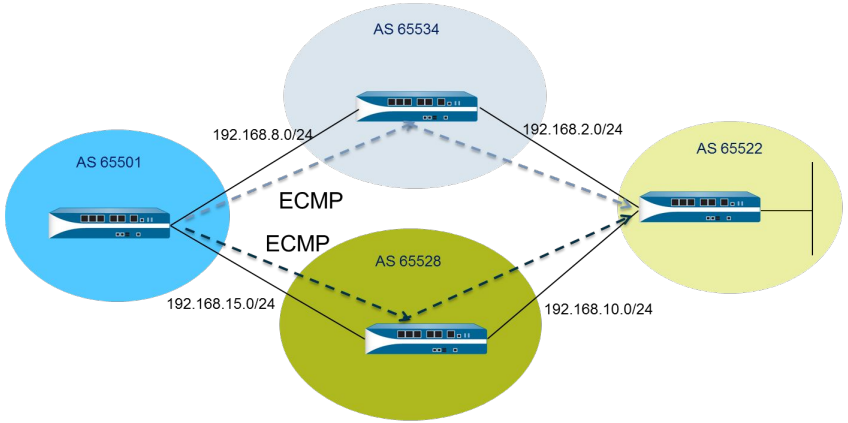


5.4.0 – Equal Cost Multiple Path (ECMP) – Example Deployments

Two ECMP paths to a destination go through two firewalls belonging to a **single ISP in a single BGP autonomous system.**



Two ECMP paths to a destination go through two firewalls belonging to two **different ISPs in different BGP autonomous system.**



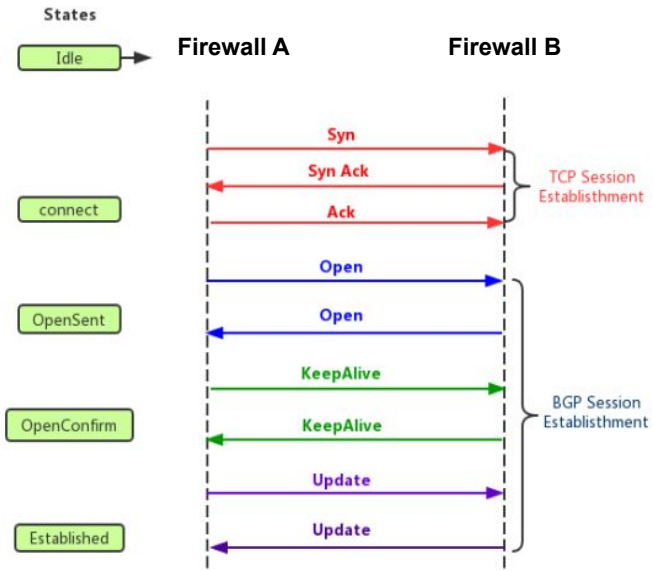
5.4.0 – Equal Cost Multiple Path (ECMP) – CLI

- **Evaluating the FIB for ECMP Group Members to the same or different ISPs.**

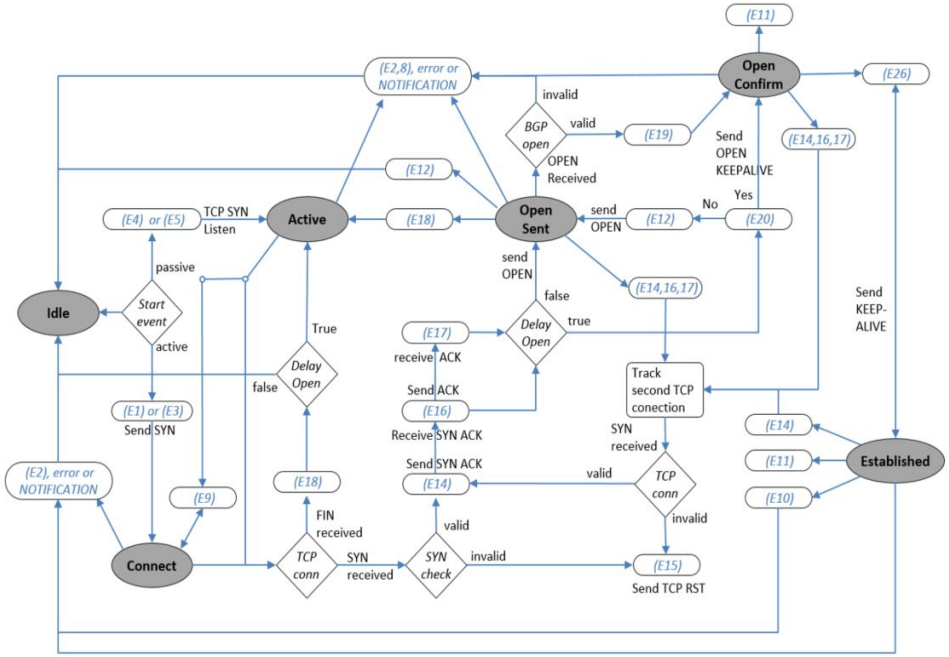
```
admin@PA-220-1> show routing fib

total virtual-router shown :              1

--------------------------------------------------------------------------------
virtual-router name: default
interfaces:
   ethernet1/1 ethernet1/3 ethernet1/7 ethernet1/7.40
   loopback.1 tunnel.3 vlan

route table:
flags: u - up, h - host, g - gateway,  e - ecmp, * - preferred path

maximum of fib entries for device:                10000
maximum of IPv4 fib entries for device:           10000
maximum of IPv6 fib entries for device:           2500
number of fib entries for device:                 11
maximum of fib entries for this fib:              10000
number of fib entries for this fib:               11
number of fib entries shown:                      11

id      destination           nexthop            flags  interface          mtu
--------------------------------------------------------------------------------
40 0.0.0.0/0             73.254. 100.1                *eug     ethernet1/1        1500  □ ISP 1
41 0.0.0.0/0             73.254. 100.1                *eug     ethernet1/2        1500  □ ISP 1
42 0.0.0.0/0             73.254. 101.1           eug     ethernet1/3        1500  □ ISP 2
43 0.0.0.0/0             73.254. 101.1           eug     ethernet1/4        1500  □ ISP 2


--------------------------------------------------------------------------------
```

5.4.1 - Understanding BGP Session Establishment and FSM

BGP Session Establishment



BGP Finite State Machine – RFC 1771



References: Finite State Machine (FSM)

5.4.1 - Common Alerts and Alarms for BGP - Reference

Routing level issues include routing protocol configurations issues, BGP neighbor establishment issues, static routing or misconfigured static routes, or issues with prefix learning or advertisement.

For BGP session establishment issues - check if there is an incorrect AS# or global parameters, an incorrect BGP peer IP, or check if BGP multi-hop is required.

For BGP peer type issues (data center only) - check if the right peer type is selected, core, edge, or classic peer type. The edge peer only learns prefixes.

For static routing issues - check the configuration for administrative distance, next hop (interface, IP, self), local or global scope to block or allow the advertisement into the Prisma SD-WAN fabric.

For prefix learning and advertisement issues - check the route map configurations on Prisma SD-WAN and BGP peer devices, check for interactions with other routing protocols in the enterprise network, and check for split or no-split prefix scenarios.

5.4.1 - Restart / Refresh BGP using CLI

Restarting a BGP session will build the BGP routing table from scratch (intrusive). Refreshing the session will only fetch / look out for new routes (non-intrusive).

To restart/refresh BGP sessions, run the following commands:

For self initiation:

```
test routing bgp virtual-router default restart self   (for restarting BGP connections)
test routing bgp virtual-router default refresh self   (for refreshing BGP connections)
```

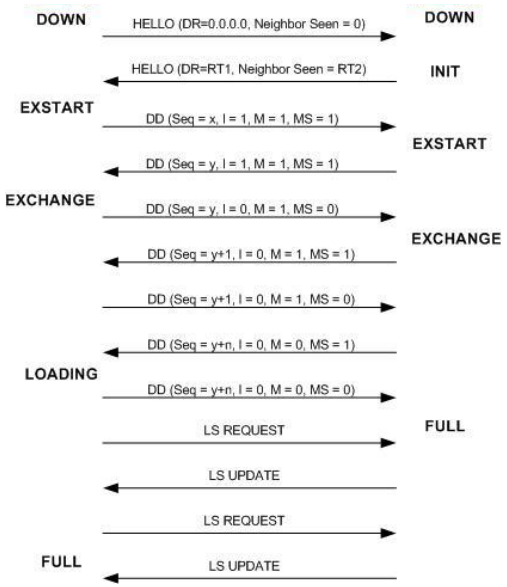
From Peer side:

```
test routing bgp virtual-router default restart peer <BGP peer>  (for restarting BGP connections)
test routing bgp virtual-router default refresh peer <BGP peer>  (for refreshing BGP connections)
```

Note: Depending on where the connection needs to be restarted/refreshed, it may require running the commands in privilege mode.

5.4.1 - Understanding OSPF Session Establishment and FSM

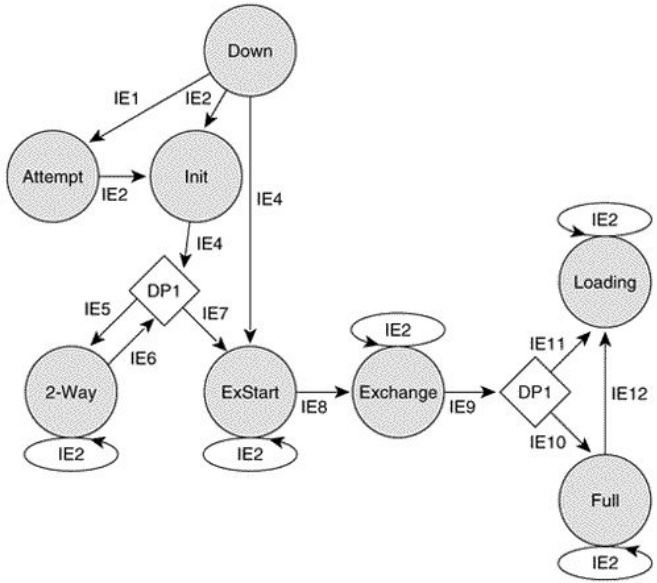
OSPF Session Establishment



OSPF States

DOWN
ATTEMPT
INIT
2-WAY
EXSTART
EXCHANGE
LOADING
FULL

OSPF Finite State Machine



References:

5.4.1 - Troubleshooting Common OSPF Issues - Reference

Reason for Neighbor Adjacency Problem	Diagnosing the Problem (Cisco CLI)	Diagnosing the Problem (PAN-OS CLI)
OSPF is not configured on one of the routers.	`show ip ospf`	`show routing protocol ospf summary`
OSPF is not enabled on an interface where it is needed.	`show ip ospf interface`	`show routing protocol ospf interface virtual-router [virtual-router]`
OSPF HELLO or Dead timer interval values are mismatched.	`show ip ospf interface`	`show routing protocol ospf interface virtual-router [virtual-router] | match hello` `show routing protocol ospf interface virtual-router [virtual-router] | match dead`
ip ospf network-type mismatch on the adjoining interfaces.	`show ip ospf interface`	`show routing protocol ospf interface virtual-router [virtual-router]`
MTU mismatch between neighboring interfaces.	`show interface <int-type/num>`	`show interface [ethernet1/x] | match MTU`
OSPF area-type is stub on one neighbor, but the adjoining neighbor in the same area is not configured for stub.	`show running-config` `show ip ospf interface`	`show routing protocol ospf interface virtual-router [virtual-router]`
OSPF neighbors have duplicate Router IDs.	`show ip ospf` `show ip ospf interface`	`show routing protocol ospf summary` `show routing protocol ospf interface virtual-router [virtual-router]`
OSPF is configured on the secondary network of the neighbor, but not on the primary network. This is an illegal configuration which prevents OSPF from being enabled on the interface.	`show ip ospf interface` `show running-config`	`show routing protocol ospf summary` `show config running`
OSPF HELLOs are not processed due to a lack of resources, such as high CPU utilization or not enough memory.	`show memory summary` `show memory processor`	`show routing protocol ospf summary`
An underlying Layer problem prevents OSPF HELLOs from being received.	`show interface`	`show routing protocol ospf interface virtual-router default | match  interface`

5.4.1 - CLI Cheat Sheet Networking – Reference, Part 1

IF YOU WANT TO . . .	USE . . .
GENERAL ROUTING COMMANDS	
Display the routing table	**> show routing route**
Look at routes for a specific destination	**> show routing fib virtual-router <name> | match <x.x.x.x/Y>**
Change the ARP cache timeout setting from the default of 1800 seconds.	**> set system setting arp-cache-timeout <60-65536>**
View the ARP cache timeout setting.	**> show system setting arp-cache-timeout**
GENERAL BGP COMMANDS	
	> show routing protocol bgp ? > loc-rib Show BGP local-rib > loc-rib-detail Show BGP local-rib > peer Show BGP peer status > peer-group Show BGP peer group status > policy Show BGP route-map status > rib-out Show BGP routes sent to BGP peer > rib-out-detail Show BGP routes sent to BGP peer > summary Show BGP summary information
GENERAL OSPF COMMANDS	
	> show routing protocol ospf > area Show OSPF area status > dumplsdb Show OSPF LS database status with all details > graceful-restart Show OSPF graceful restart status > interface Show OSPF interface status > lsdb Show OSPF LS database status > neighbor Show OSPF neighbor status > summary Show OSPF summary information > virt-link Show OSPF virtual link status > virt-neighbor Show OSPF virtual neighbor status

5.4.1 - CLI Cheat Sheet Networking – Reference, Part 2

IF YOU WANT TO . . .	USE . . .
BI-DIRECTIONAL FORWARDING (BFD)	
Show BFD profiles	`> show routing bfd active-profile [<name>]`
Show BFD details	`> show routing bfd details [interface <name>] [local-ip <ip>] [multihop][peer-ip <ip>] [session-id] [virtual-router <name> ]`
Show BFD statistics on dropped sessions	`> show routing bfd drop-counters session-id <session-id>`
Show counters of transmitted, received, and dropped BFD packets	`> show counter global | match bfd`
Clear counters of transmitted, received, and dropped BFD packets	`> clear routing bfd counters session-id all | <1-1024>`
Clear BFD sessions for debugging purposes	`> clear routing bfd session-state session-id all | <1-1024>`
GENERAL TROUBLESHOOTING	
Ping from the management (MGT) interface to a destination IP address	`> ping host <destination-ip-address>`
Ping from a dataplane interface to a destination IP address	`> ping source <ip-address-on-dataplane> host <destination-ip-address>`
Show network statistics	`> show netstat statistics yes`

References:

5.4.1 - Advanced Packet Captures from CLI for OSPF and BGP - Reference

For troubleshooting purposes it may be necessary to collect the PCAPs of the OSPF and BGP traffic that the Palo Alto Networks device is processing. The quickest way to perform troubleshooting is through the CLI.

Details

- **To start the OSPF capture, use the following CLI command:**

```
debug routing pcap ospf on
```

- **To start the BGP capture, use the following CLI command:**

```
debug routing pcap bgp on
```

- **To stop the OSPF capture:**

```
debug routing pcap ospf off
```

- **To stop the BGP capture:**

```
debug routing pcap bgp off
```

- **To view the OSPF data on the device without the need to export:**

```
debug routing pcap ospf view
```

- **To view the BGP data on the device without the need to export:**

```
debug routing pcap bgp view
```

- **If needed, files can be exported using the following commands:**

```
scp export debug-pcap from "file name" to username@host:path
```

OR

```
tftp export debug-pcap from "file name" to "tftp host"
```

- **Use the following command to delete old captures related to OSPF:**

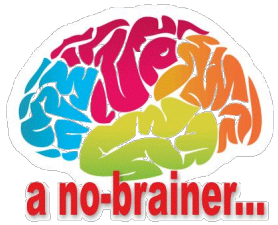
```
debug routing pcap ospf delete
```

- **Use the following command to delete old captures related to BGP:**

```
debug routing pcap bgp delete
```

References:

5.4.3 - Troubleshooting Static Routes

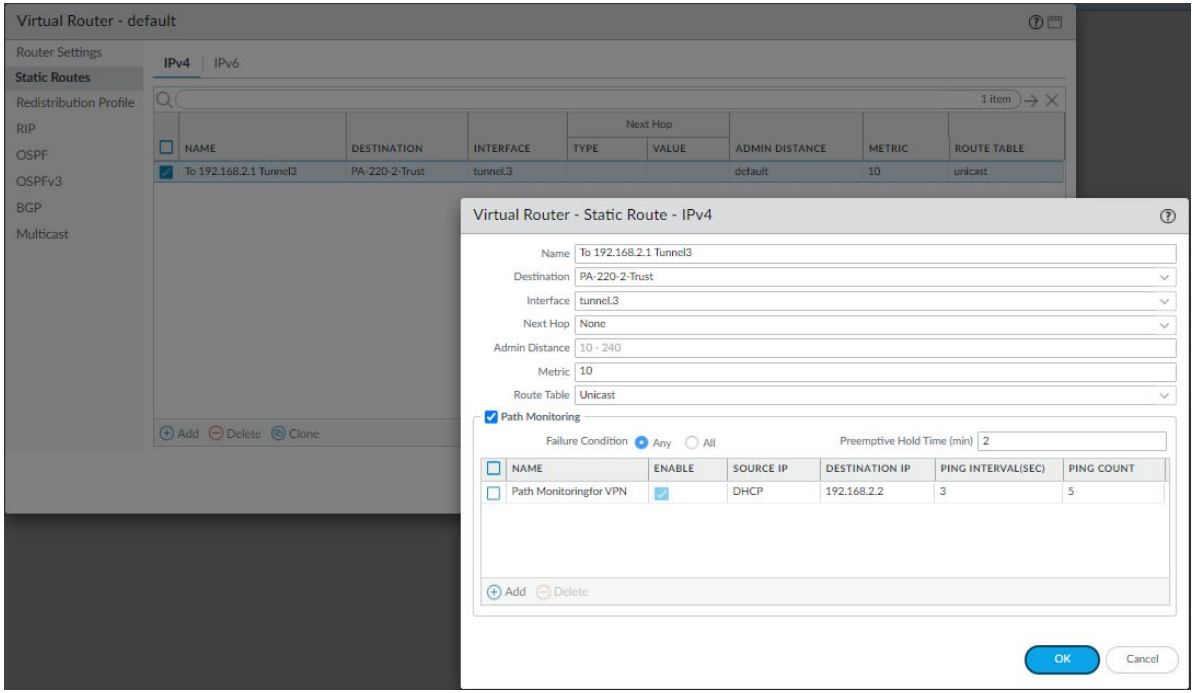



```
admin@PA-220-1> ping source 192.168.1.254 host 73.254.100.1  Ping Gateway
PING 73.254.100.1 (73.254.100.1) from 192.168.1.254 : 56(84) bytes of data.
64 bytes from 73.254.100.1: icmp_seq=1 ttl=255 time=23.3 ms
64 bytes from 73.254.100.1: icmp_seq=2 ttl=254 time=17.5 ms
^C

admin@PA-220-1> ping source 192.168.1.254 host 8.8.8.8  Ping Destination (Google DNS)
PING 8.8.8.8 (8.8.8.8) from 192.168.1.254 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=24.1 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=24.1 ms
```

If you're unable to ping from a valid source address, validate that a static route exists for the destination.

```
admin@PA-220-1> show routing route type static

flags: A:active, ?:loose, C:connect, H:host,S:static, ~:internal, R:rip,O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2;ecmp, M:multicast


VIRTUAL ROUTER: default (id 1)
  ==========
destination                              nexthop                              metric flags      age    interface           next-AS
0.0.0.0/0                                73.254.100.1                         10     EAS                ethernet1/1     Default Route
0.0.0.0/0                                73.254.100.1                         10     EAS                ethernet1/2     Default Route


total routes shown: 2
```

5.4.4 - Troubleshooting Route Monitoring



Destination IP
The destination IP address should belong to a reliable endpoint.
Always use more than a single endpoint for path monitoring.

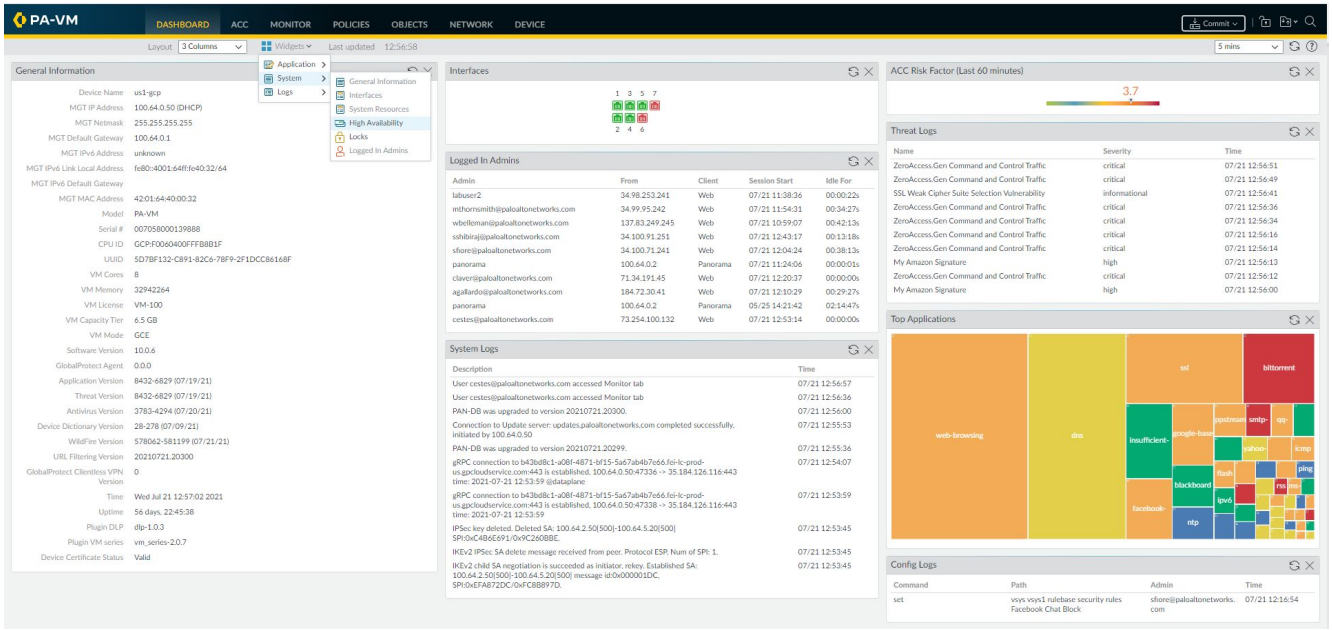
Failure Condition
Select All to avoid the possibility of any single monitored destination signaling a route failure.

References: Path Monitoring


QUIZ
TIME

5.5 Investigate Traffic Patterns on the NGFW or Panorama

5.5.0 - Dashboard – NGFW and Panorama



Information for:

General System

Interfaces

HA Status

Top Applications

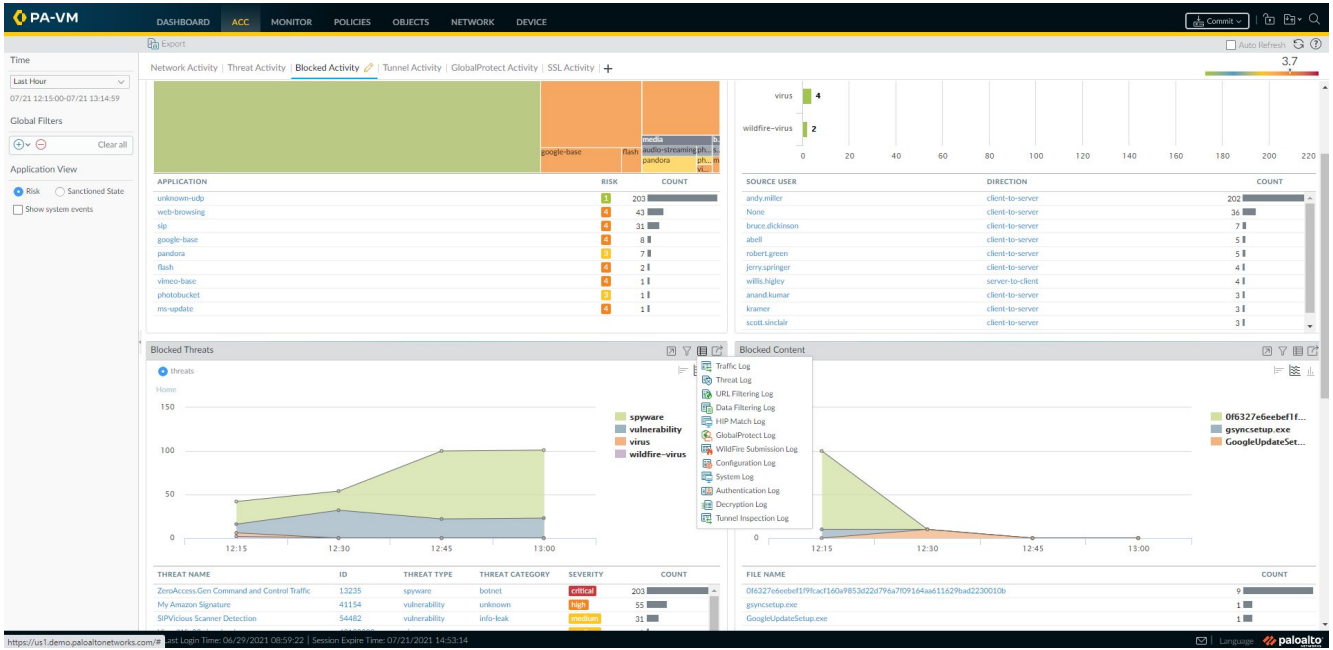
Systems Logs

Threat Logging

ACC Risk Factor

The dashboard supports customizable widgets, and the view is role based on both the NGFW and in Panorama.

5.5.0 - Application Command Center (ACC) – NGFW and Panorama



Displays Activity for:

Network Traffic

Threats

Blocked Users

Tunnels

Global Protect

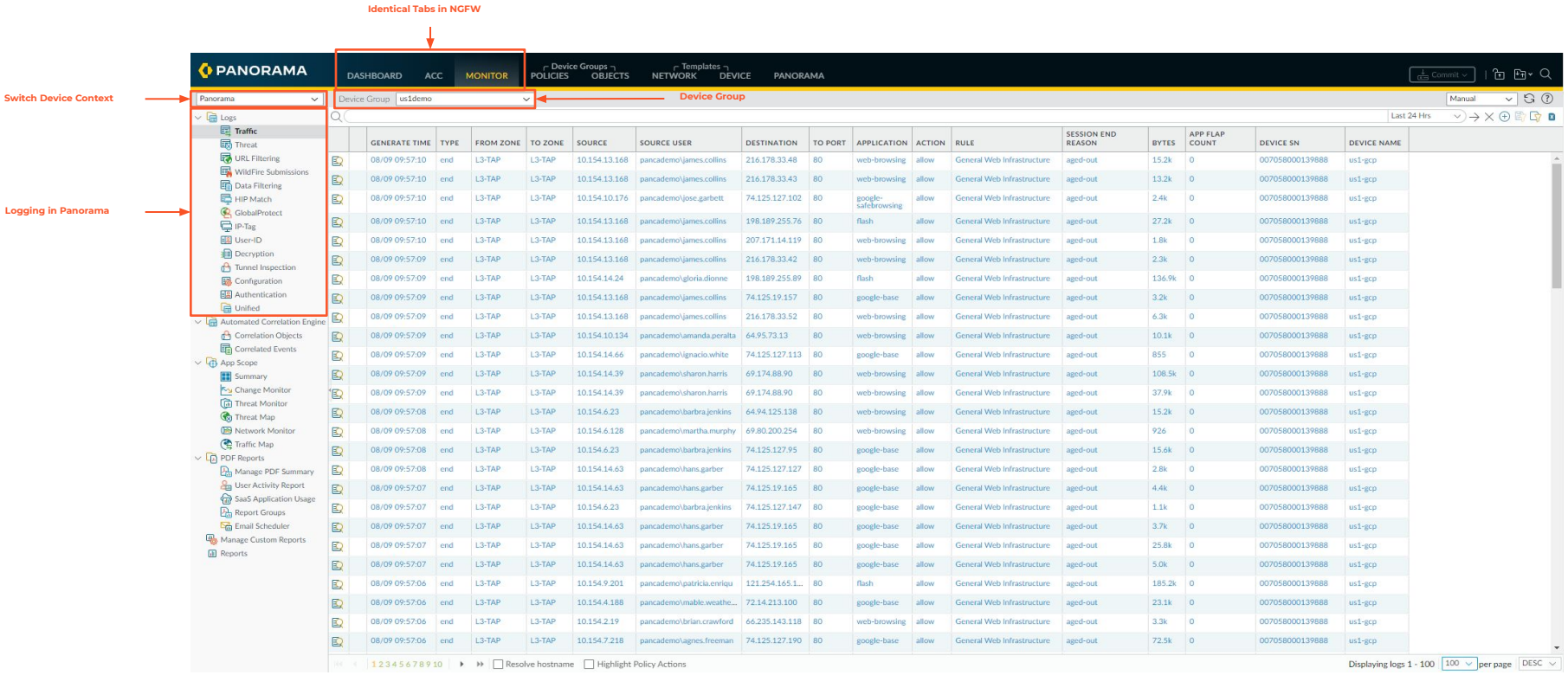
SSL Sessions

Widget's support:

Allows filtering and selection of information for more granular troubleshooting.

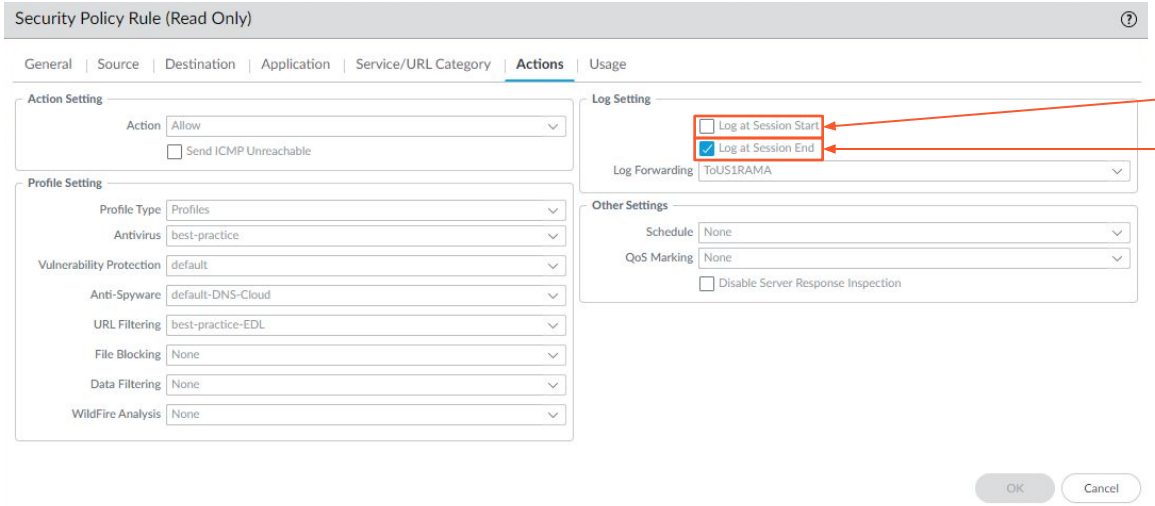
Jumping to logs and exporting information to CSV format.

5.5.0 - Monitor Tab – Panorama



 |

5.5.1 - Prerequisites for Traffic Logging



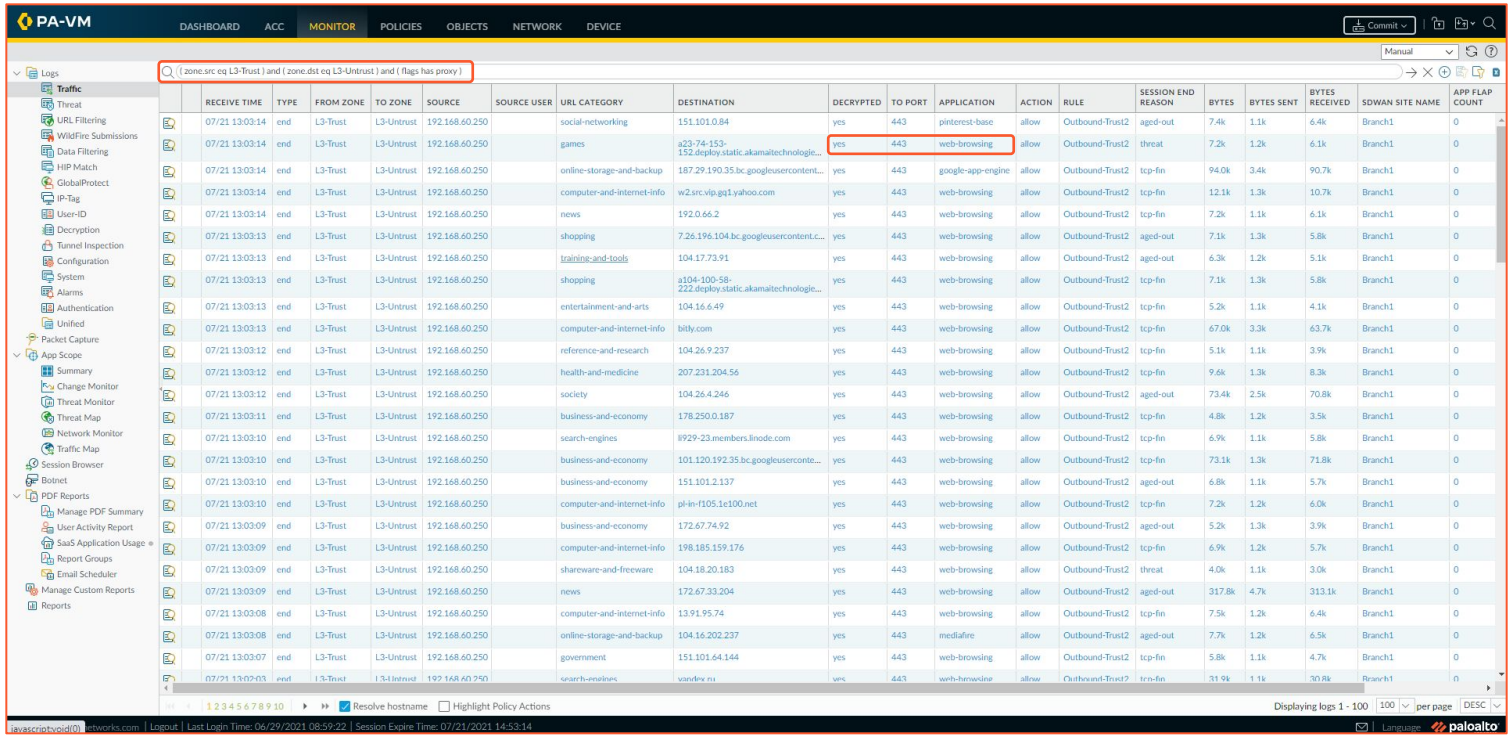
Logging - Self Explanatory?

- Session ID - (Active Session)
- Session ID - (Closed Session)

5.5.1 - Monitor > Logs > Traffic (Example 1 - Decryption)

Demo Filters:

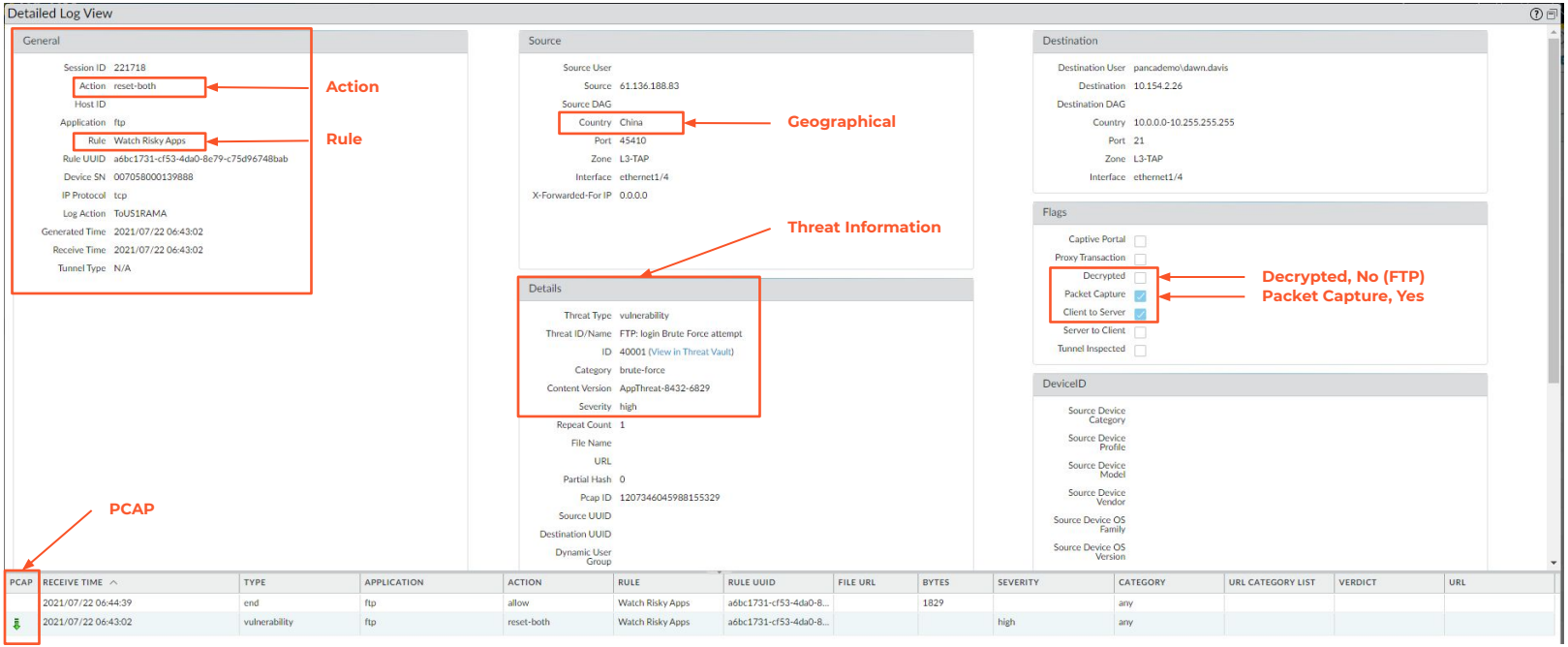
```
( zone.src eq L3-Trust ) and ( zone.dst eq L3-Untrust ) and ( flags has proxy )
```



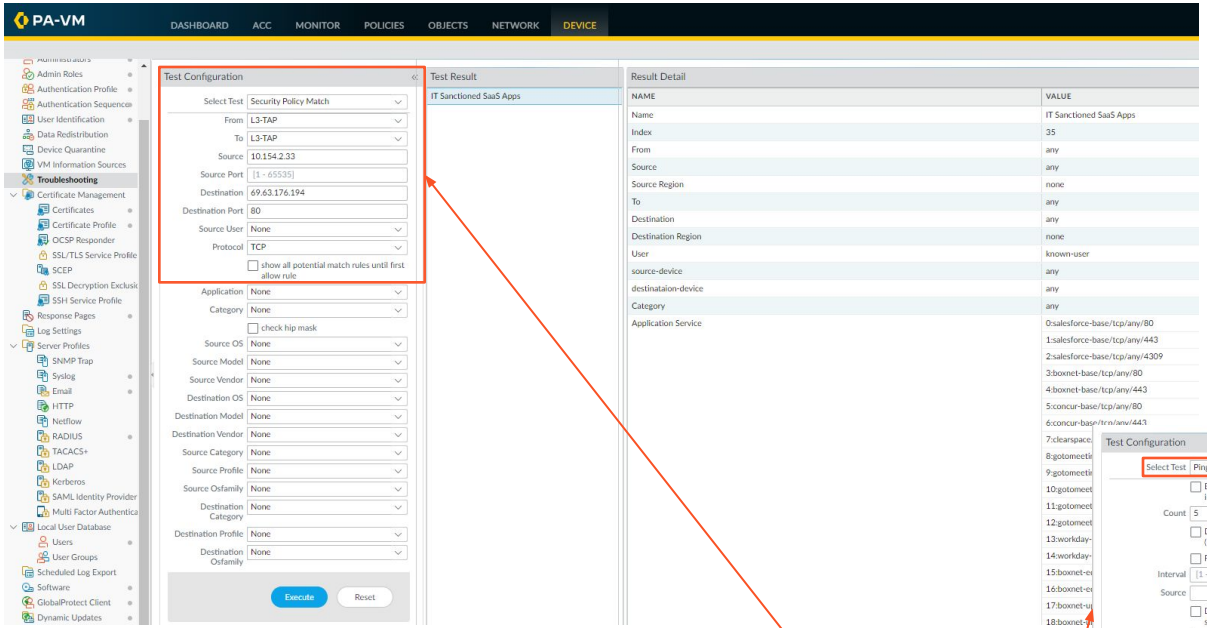
5.5.1 - Monitor > Logs > Unified (Example 2 - Threats)

Demo Filters:

```
( severity eq high )
( severity eq high ) and ( threat_name eq 'FTP: login Brute Force attempt' )
```



5.5.1 - Troubleshooting Security Policy and Connectivity Issues



Diagnostic Tools:

Device > Troubleshooting

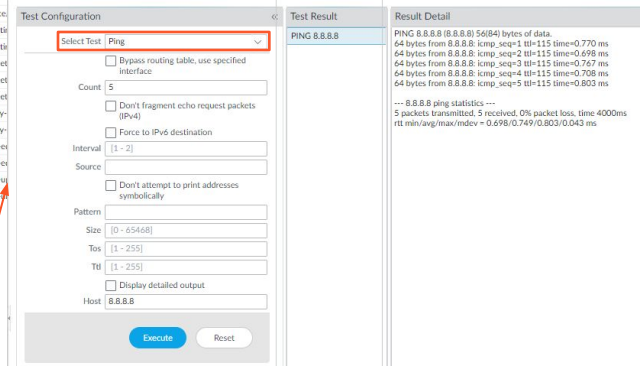
In-Context:

[Toolbar] > Test Policy Match

Hit Counters

Rule Usage filtering

Applications Seen



Security Policy Match
Ping from GUI

Security Policy Match:

```
( addr.src in 192.168.60.250 ) and ( addr.dst in 172.67.72.147 ) and ( flags has proxy )
```


5.5.1 - Application Recognition (App-ID) or lack thereof

- **incomplete:** Either the **TCP handshake (SYN, SYN-ACK, ACK) did not complete**, or the **TCP handshake did complete but there was no data after the handshake to identify the application.**

  - ✔ **For Example:** If a client sends a server a TCP SYN packet and the Palo Alto Networks device creates a session for that SYN packet, but the server never sends a SYN ACK packet back to the client, then that session is "**incomplete**." **Hint:** Look at Bytes Sent vs. Received on FW

- **insufficient data:** Not enough data to identify the application.

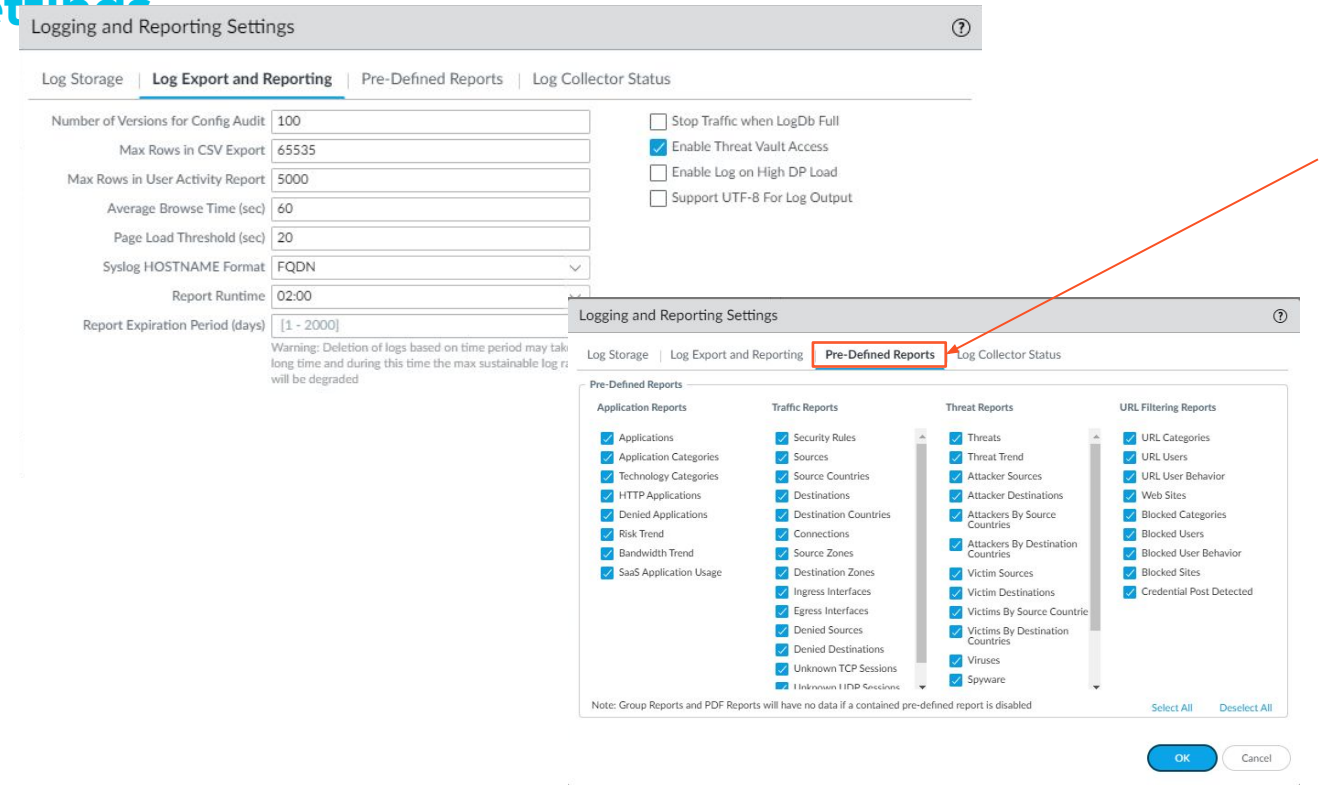
  - ✔ **For Example**: If the three-way TCP handshake completed and there was one data packet after the handshake but there was not enough data to match any signature, then the user will see "**insufficient data**" in the **Application** field of the Traffic log.
  - ✔ `Filter: ( app eq insufficient-data )`

- **unknown-tcp:** The firewall captured the three-way TCP handshake, but the application was not identified, perhaps because of the use of a custom application for which the firewall does not have signatures. **Hint:** Investigate, all applications in use should be known.
- **unknown-udp:** Unknown UDP traffic

5.5.1 - Session End Reason – Reference

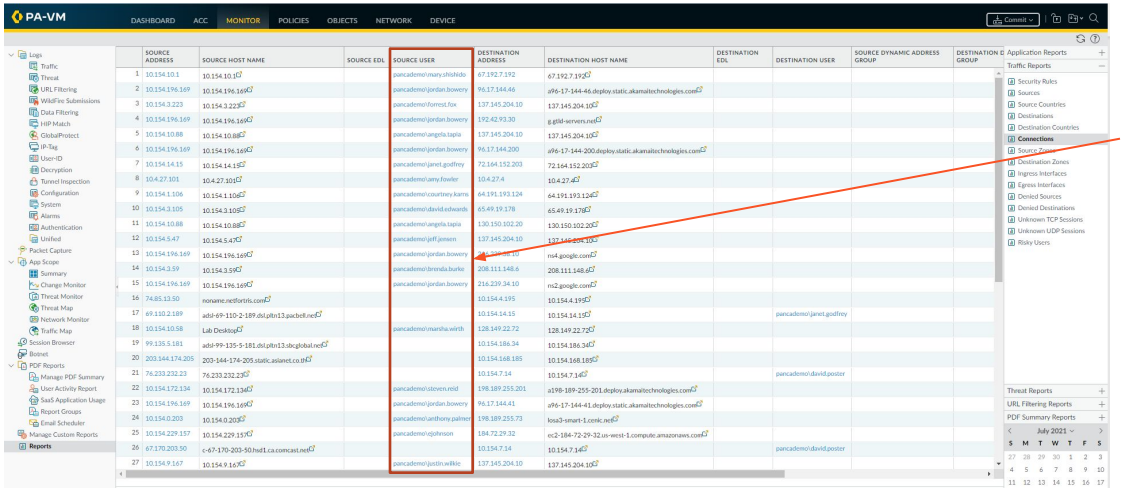
1. **threat -** The firewall detected a threat associated with a reset, drop, or block (IP address) action.
2. **policy-deny -** The session matched a security rule with a deny or drop action.
3. **decrypt-cert-validation -** The session terminated because the firewall was configured to block SSL forward proxy decryption or SSL inbound inspection when the session uses client authentication or when the session uses a server certificate with any of the following conditions: expired, untrusted issuer, unknown status, or status verification time-out. **This session end reason also displays when the server certificate produces a fatal error alert of type:** bad_certificate, unsupported_certificate, certificate_revoked, access_denied, or no_certificate_RESERVED (SSLv3 only).
4. **decrypt-unsupport-param -** The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when the session uses an unsupported protocol version, cipher, or SSH algorithm. **This session end reason is displays when the session produces a fatal error alert of type:** unsupported_extension, unexpected_message, or handshake_failure.
5. **decrypt-error -** The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when firewall resources or the hardware security module (HSM) were unavailable. This session end reason is also displayed when you configured the firewall to block SSL traffic that has SSL errors or that produced any fatal error alert other than those listed for the decrypt-cert-validation and decrypt-unsupport-param end reasons.
6. **tcp-rst-from-client -** The client sent a TCP reset to the server.
7. **tcp-rst-from-server -** The server sent a TCP reset to the client.
8. **tcp-fin -** Both hosts in the connection sent a TCP FIN message to close the session.
9. **tcp-reuse -** A session is reused and the firewall closes the previous session.
10. **decoder -** The decoder detects a new connection within the protocol (such as HTTP-Proxy) and ends the previous connection.
11. **aged-out -** The session aged out.

5.5.2 - Device > Setup > Management > Logging and Reporting Settings



Predefined Reports

5.5.2 - Reporting Types



Reports items link back to ACC

Application Reports
Denied Applications

Traffic Reports
- Source Countries
- **Connections**
- Denied Sources
- Unknown TCP Sessions
- Risky Users

Threat Reports
- **All** are IMPORTANT
- Botnet, Threats, Viruses, Spyware, and Vulnerabilities

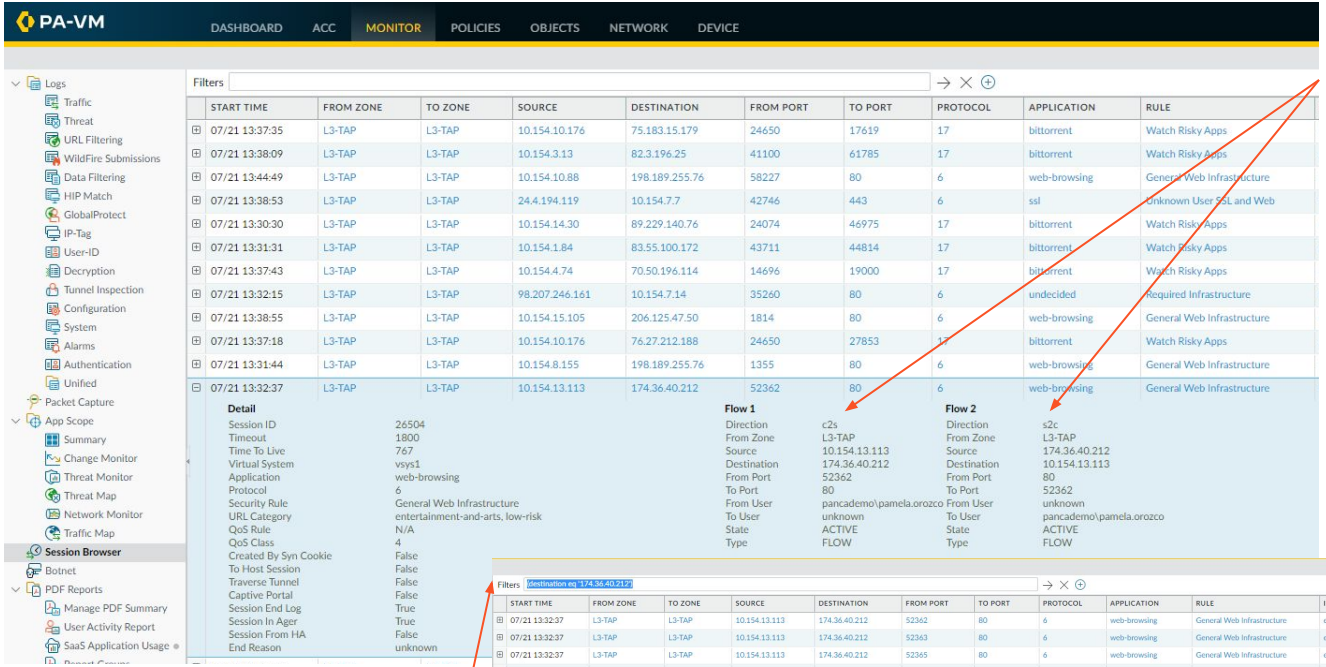
URL Reports
- **All** are IMPORTANT
- Blocked categories, users, user behavior, blocked sites, and AD Credential Theft Detection

PDF Summary Reports
- Depends upon what you're troubleshooting.

5.5.3 - If Traffic Logs are unavailable

- **Did traffic match a security policy with logging enabled?**
- Log on session end is enabled by default in a policy, but can be disabled.
- **Did it match any security policy?**
- The Default action match will not generate traffic log.
- Intra-zone traffic by default is allowed (Same Subnet).
- **Is the session still active?**
- Log on session end is enabled by default.
- Can enable on session start, but this will increase logging rates.
- **Is traffic reaching the firewall?**
- Can enable **packet-diag filters** and **show global counters**.
- Can enable **packet-captures** and/or **flow basic debugging**.

5.5.3 - Troubleshooting Active Flows using Session Browser



Direction:

c2s – Client to Server

s2c – Server to Client

Displays TO / FROM Info:

Zones

IP Addresses and Ports

User-ID

Matching Security Policy

URL Categories

QoS Class and Rate

Filter displays all communication to the DST at 174.36.40.212.


QUIZ
TIME

Understanding Packet Captures

Packet Captures – Why?

Visibility
- Identify TCP 3-way handshake
- Validate SRC, DST IP and Port Information (Pre/Post-NAT), QoS Marking, Sequence #'s, etc.

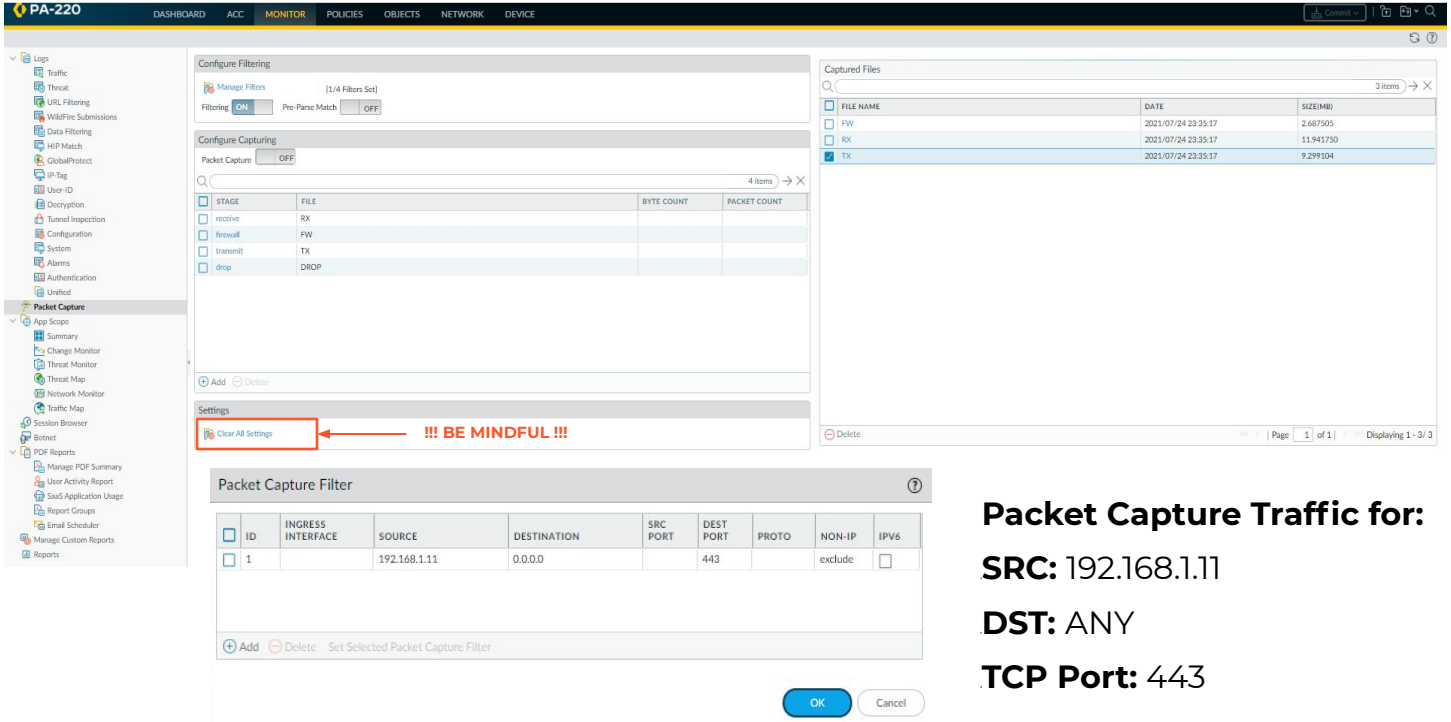
Connectivity
- Validate Security Policy Drops
- Identify Routing Issues
- Identify Missing (SYN-ACK) or Retransmitted Packets

Performance
- Client-Server latency
- Firewall Latency
- Application Behavior

Types of Packet Captures

- **Custom Packet Captures -** The firewall captures packets for all traffic or for specific traffic based on filters that you define.
- **Threat-based Packet Captures -** The firewall captures packets when it detects a virus, spyware, or vulnerability.
- **Application Packet Captures -** The firewall captures packets based on a specific application and filters that you define. These are **enabled** by default.
- **Validate in CLI:**
  - ✔ `show running application setting | match "Unknown capture"`
- If the unknown capture setting option is off, enable it:
  - ✔ `set application dump-unknown yes`
- **Management Interface Packet Captures -** The firewall captures packets on the management interface (MGT) using **tcpdump.**
  - ✔ `tcpdump filter "net 10.5.104.0/24 and not port 22" snaplen 0`
- **GTP Event Packet Capture -** The firewall captures a single GTP event, such as GTP-in-GTP, end user IP spoofing, and abnormal GTP messages, to make GTP troubleshooting easier for mobile network operators (MNOs).

Custom Packet Captures – On the Data Plane



Packet Capture Traffic for:

SRC: 192.168.1.11

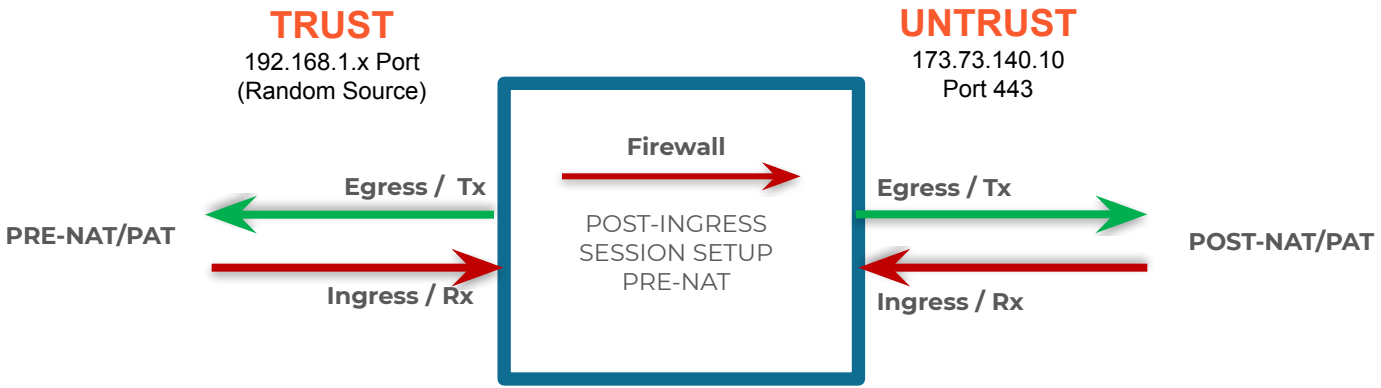
DST: ANY

TCP Port: 443

 |

Packet Captures Stages

- **Drop Stage -** is where packets get discarded.
- **Receive Stage -** captures the packets as they ingress the firewall before they go into the firewall engine. If NAT is configured, these packets will be **pre-NAT.**
- **Transmit Stage -** captures packets how they egress out of the firewall engine. If NAT is configured, these will be **post-NAT.**
- **Firewall Stage -** captures packets in the firewall stage.



Which stage is right for me? - Reference

Traffic visibility use-cases	You need:
Internal flow on the firewall	Firewall-stage and drop-stage captures
Sessions as they were on the wire	Merge receive and transmit captures
Transit time across the firewall	Assess timestamps from receive to transmit
Ingress packets matched to egress	Compare receive and transmit stages
Firewall-generated responses	Examine transmit stage
Dropped packets	Examine drop stage

Packet Captures – Some additional things to know!

- Up to **four filters** can be added with a variety of attributes.
- Packet captures are session based, so a single filter can capture both **client2server (c2s) and server2client (s2c).**
- Packets are captured on the **dataplane** vs **the interface.** (this explains the next bullet)
- Pre-parse Match?
- When filtering is enabled, **only new sessions** can be captured. Existing sessions will not be seen by the Capture filter and need to re-initiated to see match the filter.
- Offloaded sessions can't be captured so offloading may need to be disabled temporarily. An offloaded session will display **'layer7 processing : completed'** in the show session details.
- To disable session offload, you can use the following commands in the CLI.

```
Disable: set session offload no
```


Wireshark Tutorial: Wireshark Workshop Videos Now Available

By Brad Duncan
October 1, 2021 at 6:00 AM

55 2 min. read

Wireshark Tutorial: Examining Traffic from Hancitor Infections

By Brad Duncan
April 7, 2021 at 6:00 AM

19 20 min. read

Trending

1. Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer
2. Finding Azurescape – Cross-Account Container Takeover in Azure Container Instances
3. A Peek into Top-Level Domains and Cybercrime
4. Case Study: From BazarLoader to Network Reconnaissance
5. Updated: New Evidence Emerges to Suggest WatchDog Was Behind Crypto Campaign

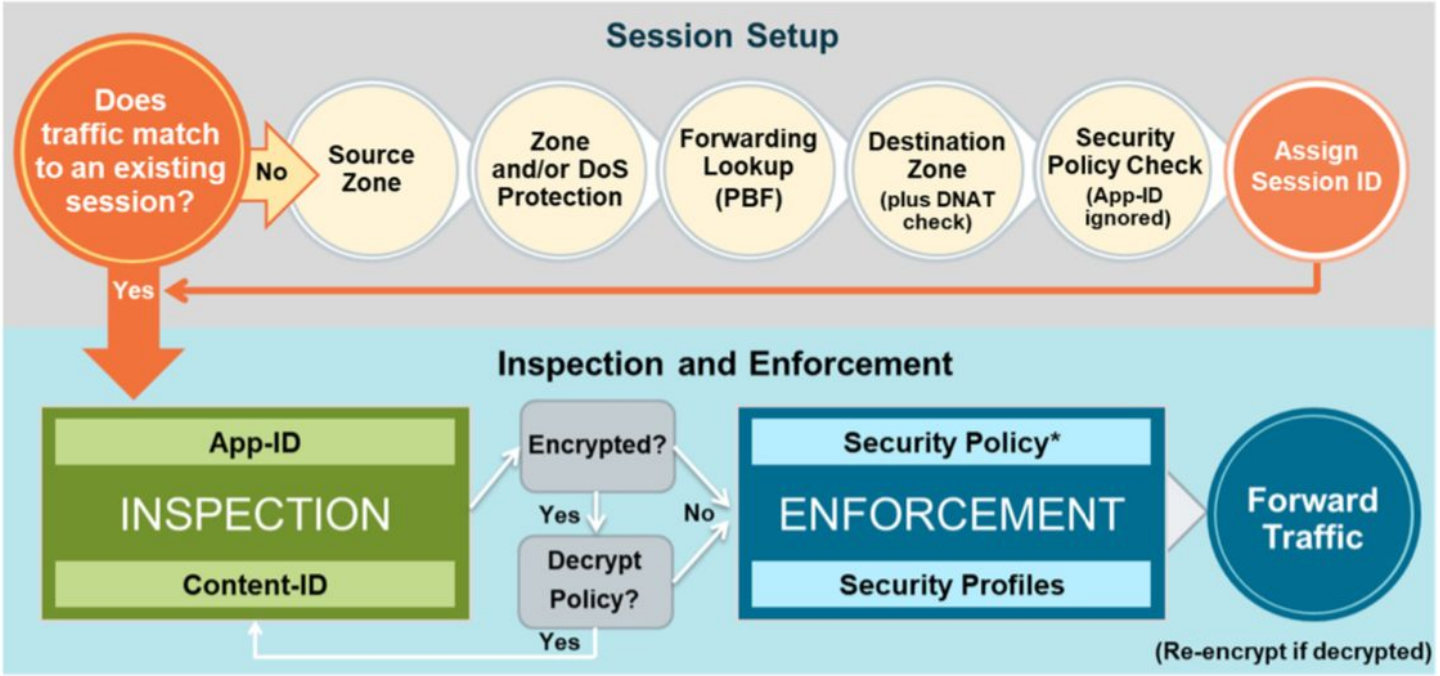
Wireshark Tutorial: Decrypting

Wireshark Tutorial: Examining

Wireshark Tutorial: Decrypting

5.6 Troubleshoot zone protection, packet buffer protection and DoS protection

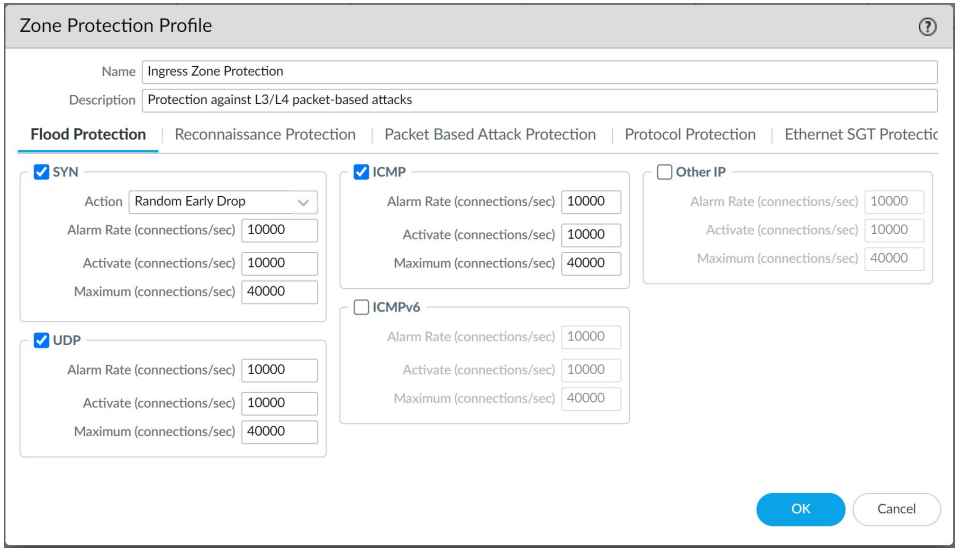
Packet Flow Sequence



PACKET FLOW SEQUENCE IN PAN-OS
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

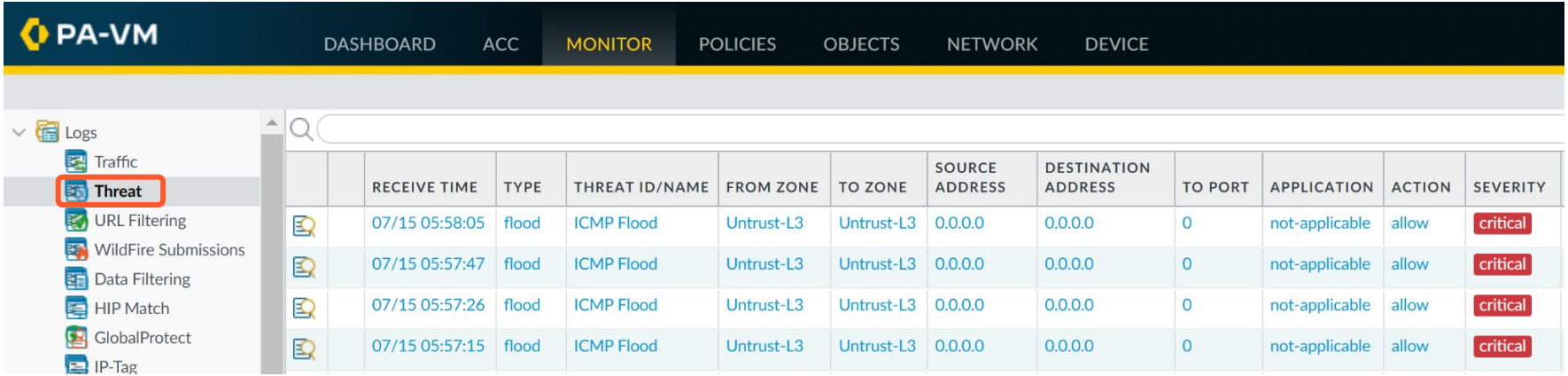
5.6.1 Troubleshoot zone protection profiles

- Zone Protections are always applied on the ingress zone
- Protects networks against common flood, reconnaissance attacks, and other packet-based attacks
- Configure Alarm Rate, Activate and Maximum thresholds



5.6.1 Troubleshoot zone protection profiles

- Threat log generated if any configured flood threshold is crossed
- Log entries show the zone name for which the profile was triggered in the source and destination zone fields.

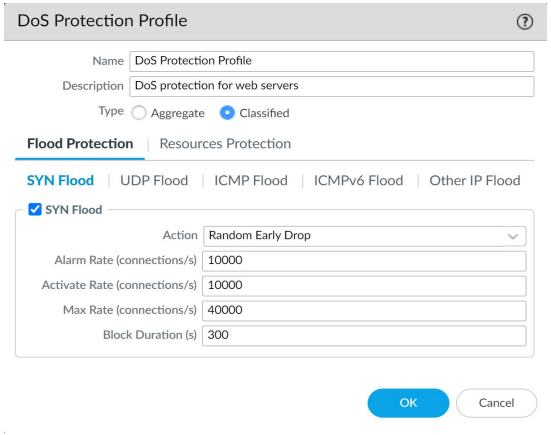


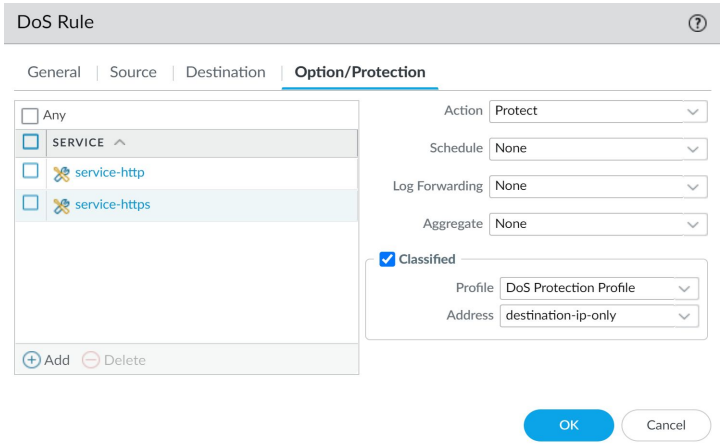
RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY
07/15 05:58:05	flood	ICMP Flood	Untrust-L3	Untrust-L3	0.0.0.0	0.0.0.0	0	not-applicable	allow	critical
07/15 05:57:47	flood	ICMP Flood	Untrust-L3	Untrust-L3	0.0.0.0	0.0.0.0	0	not-applicable	allow	critical
07/15 05:57:26	flood	ICMP Flood	Untrust-L3	Untrust-L3	0.0.0.0	0.0.0.0	0	not-applicable	allow	critical
07/15 05:57:15	flood	ICMP Flood	Untrust-L3	Untrust-L3	0.0.0.0	0.0.0.0	0	not-applicable	allow	critical

5.6.2 Troubleshoot denial-of-service protections

DoS Protection Profiles are designed to work with Zone Protection Profiles.

- A Zone Protection Profile protects an ingress zone, and a DoS Protection policy and DoS Protection Profile protect a destination zone or destination host
- Both provide protection against denial-of-service attacks
- Major difference: DoS Protection can be classified or aggregate. Zone Protection can only be aggregate





5.6.2 Troubleshoot denial-of-service protections

- Troubleshooting requires monitoring the session table:
  - Session table becomes full after DoS traffic is allowed by the firewall policies
  - *> show session all*
    - Identify any source IP or targetted IP that stands out
  - Restrict security policy accordingly and enable DoS Protection and Zone Protection profiles to mitigate future occurrences

5.6.3 Troubleshoot packet buffer protections

- Troubleshooting Packet Buffer / Packet Descriptors Full
  - Occurs in DoS attacks when there's a high rate of new connections or high packet rate on existing sessions
  - *> show session all filter min-kb 5000*
    - Identify sessions transferring more data than usual
  - > show running resource-monitor ingress-backlogs
    - Identify sessions consuming more than 2% of packet descriptor

```
admin@PA-7050> show running resource-monitor ingress-backlogs
-- SLOT:s1, DP:dp1 -- USAGE - ATOMIC: 92%  TOTAL: 93%
TOP SESSIONS:SESS-ID      PCT   GRP-ID   COUNT
6            92%   1        156                  7        1732
SESSION DETAILS SESS-ID PROTO SZONESRC       SPORT  DST       DPORT  IGR-IF    EGR-IF       APP
6    6     trust 192.168.2.35 55653  10.1.8.89 80  ethernet1/21 ethernet1/22 undecided
```


5.6 References

Zone Protection Recommendations (KB article):
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVkCAK

Zone Protection Profiles (KB article):
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clm9CAC

Zone Protection Profiles (Tech docs):
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles.html

Troubleshooting DOS Attacks (KB article):
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClWLCA0

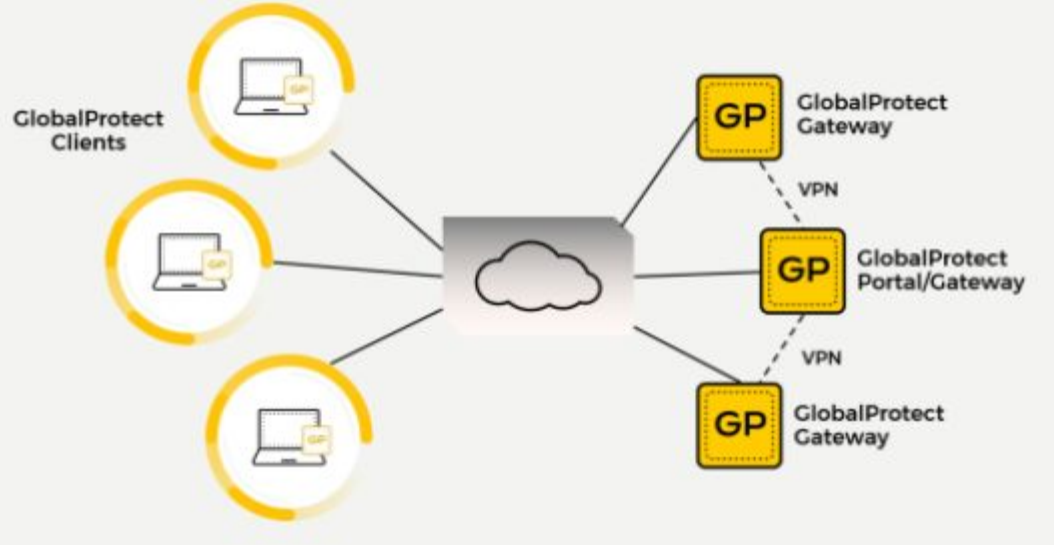
Tips & Tricks: How to Use the Application Command Center (ACC):
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClcvCAC


QUIZ
TIME

5.7 Troubleshoot GlobalProtect

5.7 Troubleshooting GlobalProtect

GlobalProtect has three major components: Portal, Gateways, Client software.



5.7.1 & 5.7.2 Troubleshoot connection problems to Portal/Gateway

The ACC is a great place to start for troubleshooting GlobalProtect connection issues

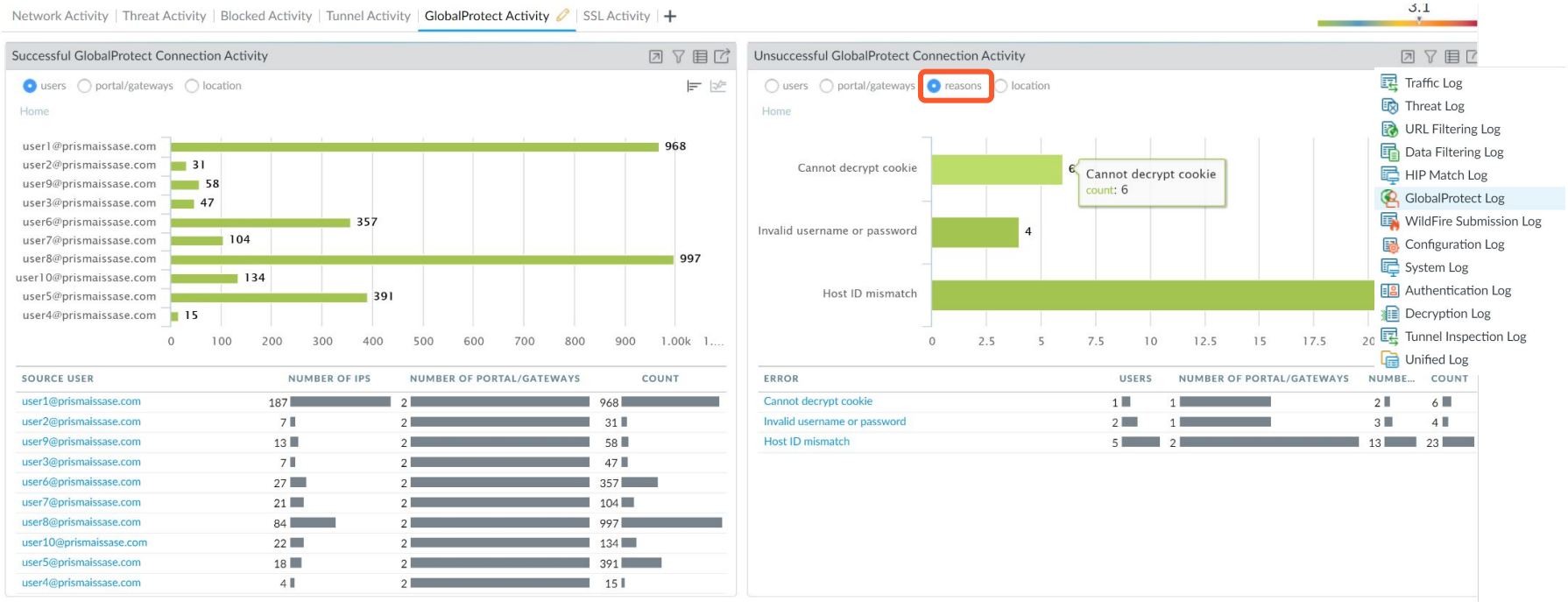
The following ACC charts are available out of the box:

- Successful GlobalProtect Connection Activity: successful connection statistics by users, portals and gateways, and location
- Unsuccessful GlobalProtect Connection Activity: unsuccessful connection statistics by users, portals and gateways, location and reason. This chart indicates the error, source user, public IP address and other information to help you identify and quickly resolve the issue
- GlobalProtect Deployment Activity: deployment summary based on authentication method, GlobalProtect app version, and operating system version
- GlobalProtect Host Information: displays the state of endpoints based on HIP data collected by the GlobalProtect App. This widget is under the Network Activity ACC tab

Jump directly to GlobalProtect logs from the ACC

5.7.1 & 5.7.2 Troubleshoot connection problems to Portal/Gateway

Successful/Unsuccessful GlobalProtect Connection Activity widgets:

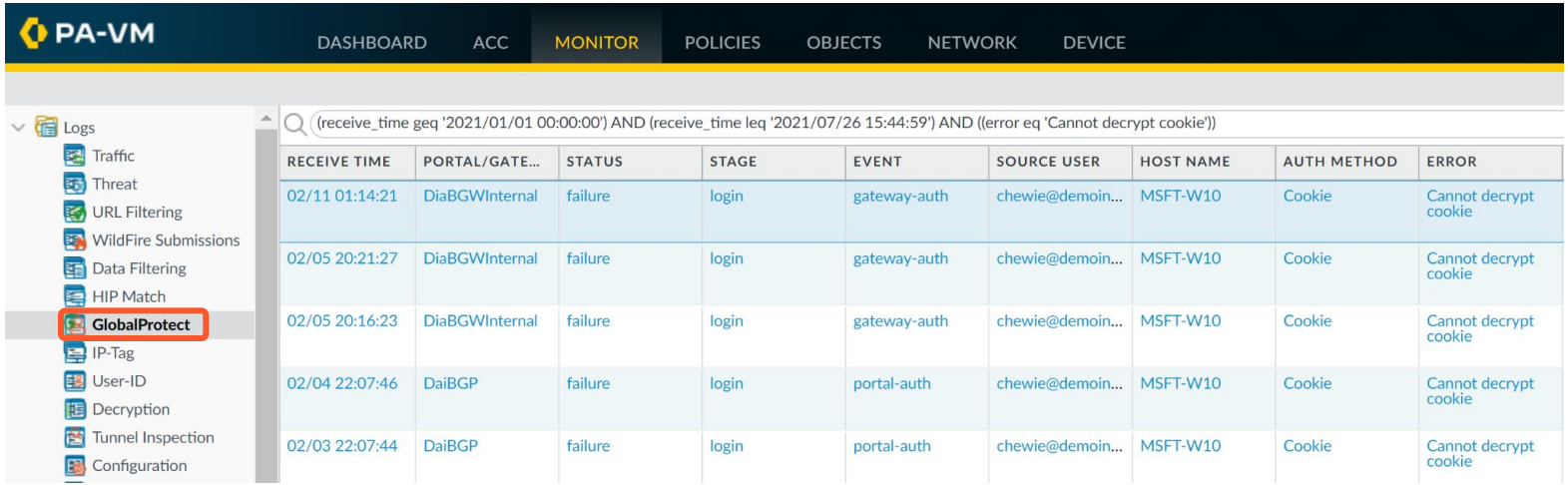


5.7.1 & 5.7.2 Troubleshoot connection problems to Portal/Gateway

GlobalProtect logs are found on a dedicated page in Monitor > Logs.

Examples of GlobalProtect logs:

- GlobalProtect Portal and Gateway Logs
- Clientless VPN logs
- LSVPN and satellite events



5.7.3 Troubleshoot connection problems to the provided resources

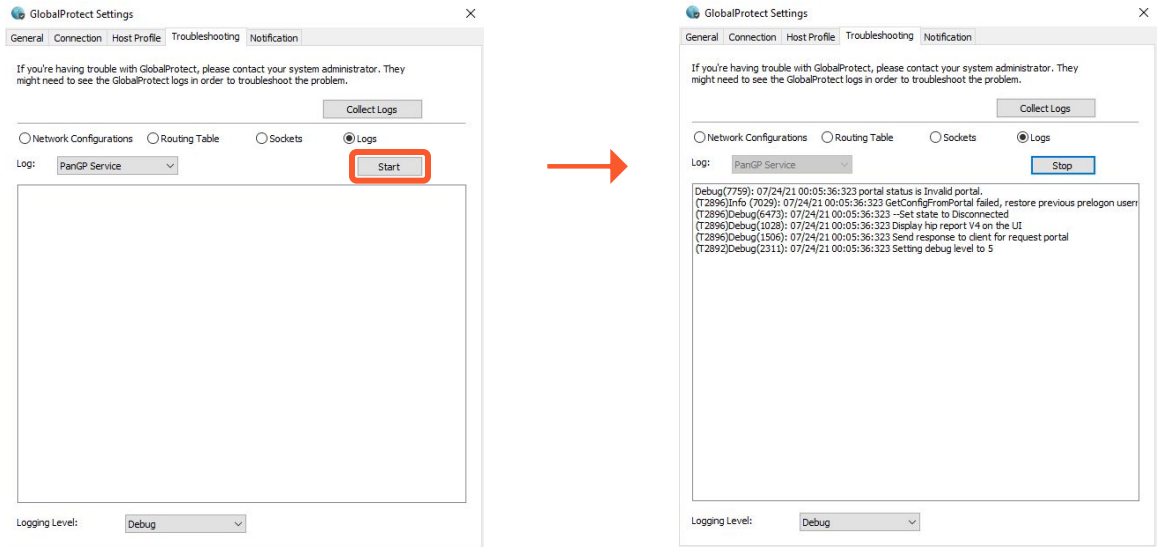
- Scenario where your configuration appears correct but users are unable to access internal resources
- Typically related to one of the following issues:
  - PANGP Virtual Ethernet Adapter
  - Misconfigured security policies
  - Routing
  - IP address-to-username mapping
- Verify GlobalProtect client connection on the firewall and mapping source:
  - > show global-protect-gateway current-user
  - > show user ip-user-mapping ip <ip-address>
  - > show global-protect-gateway flow

5.7.4 Troubleshoot GP client

Collect GlobalProtect Client logs

GlobalProtect App -> Settings -> Troubleshooting

Examine log entries to determine where the connection may be failing

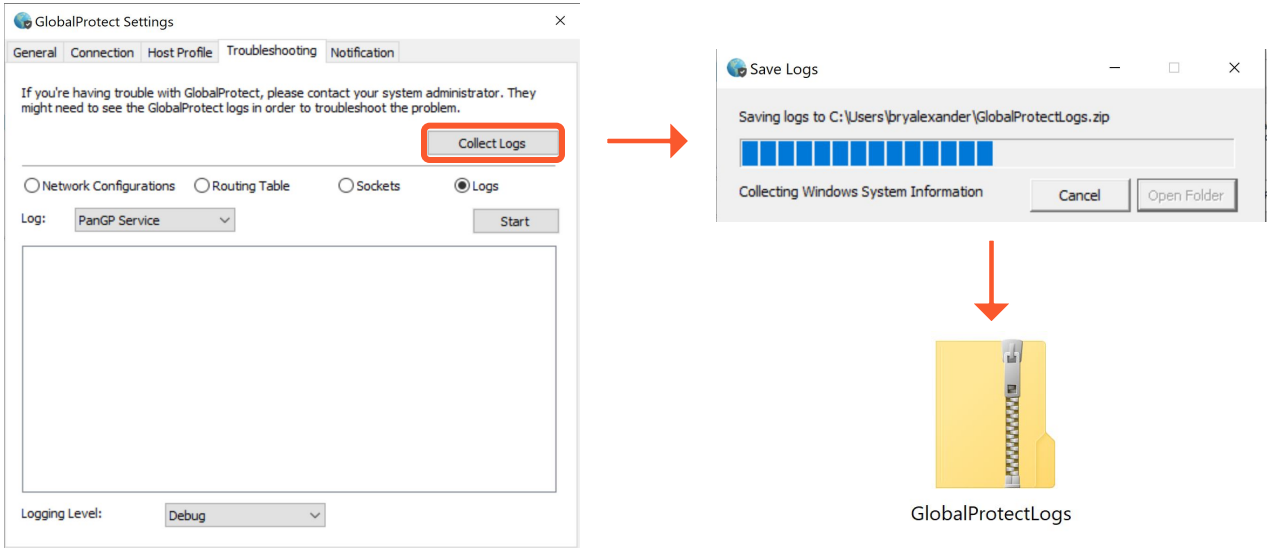


5.7.4 Troubleshoot GP client

Collect GlobalProtect Client logs

GlobalProtect App -> Settings -> Troubleshooting

Examine log entries to determine where the connection may be failing



5.7 References

GlobalProtect Remote User Security:
https://beacon.paloaltonetworks.com/student/path/774588-globalprotect-remote-user-security?sid=35743888&sid_i=0

GlobalProtect Resource List on Configuring and Troubleshooting (KB article):
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfXCAS

Troubleshooting GlobalProtect (KB article):
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClkBCAS

Common Issues with GlobalProtect:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClYGCA0

GlobalProtect Users and Internal Resources:
https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000ClaB

DOTW - GlobalProtect Troubleshooting Tips:
https://live.paloaltonetworks.com/t5/blogs/dotw-globalprotect-troubleshooting-tips/ba-p/383911

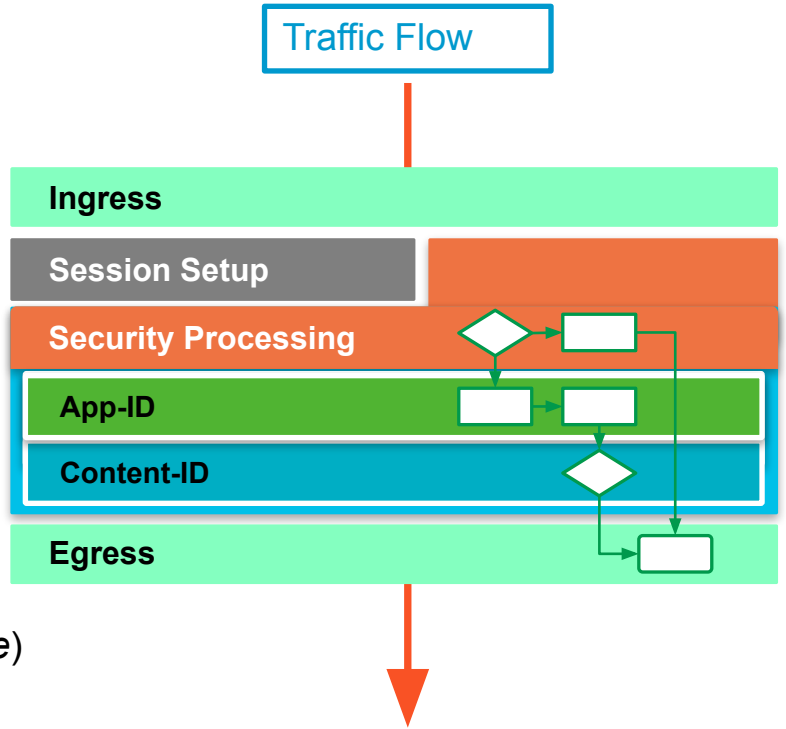

QUIZ
TIME

Thank you

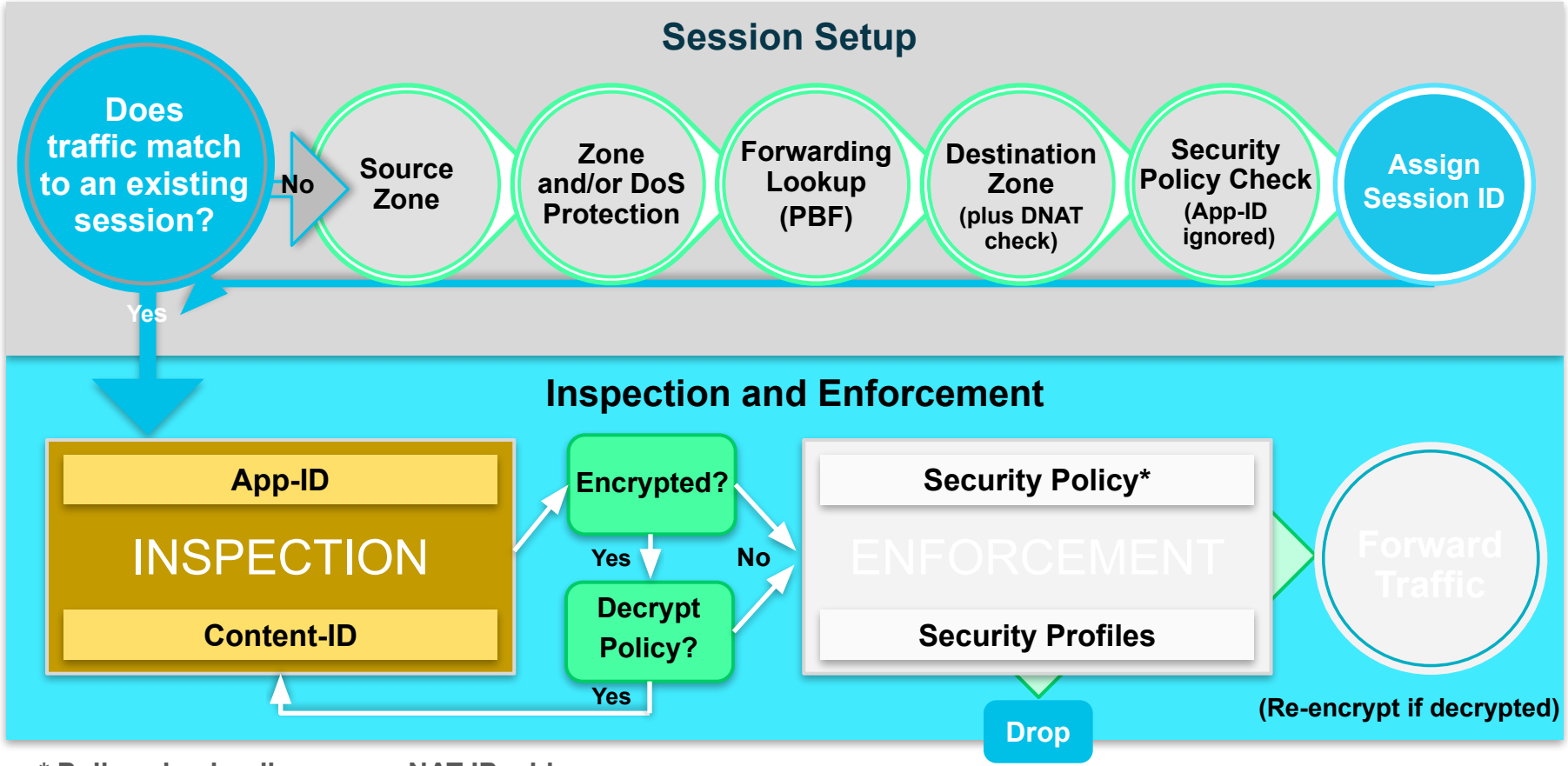
Special Section
Important Troubleshooting Skills

High-Level Packet Processing Logic

- Ingress
  - Packet Processing
  - Defragmentation
  - VPN decapsulation
- Session Setup (“*slowpath*”)
- Security Processing (“fastpath”)
  - Inspection & Enforcement
- Egress
  - QoS (Shaping, Rate Limiting)
  - Fragmentation
  - VPN encapsulation
- Session Offload = cut-through traffic (*requires hardware*)

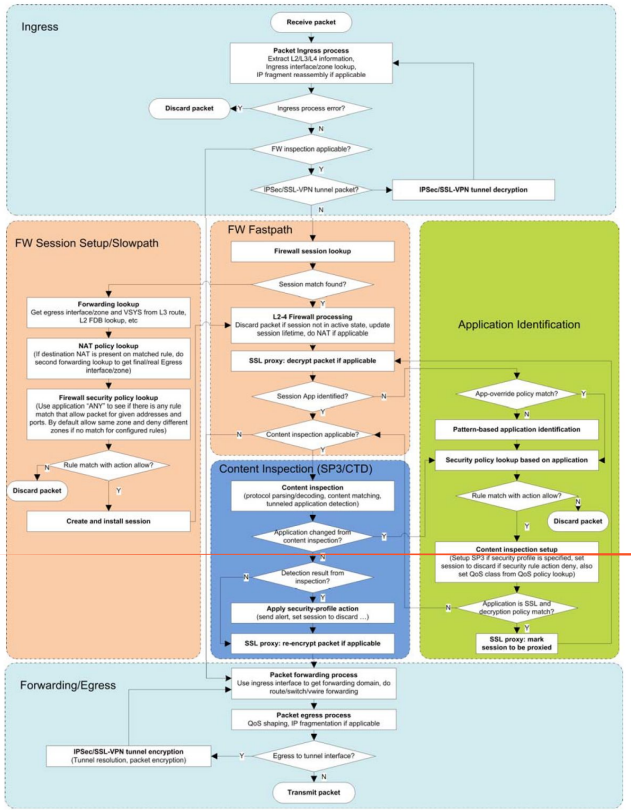


Session Setup, Inspection and Enforcement



* Policy check relies on pre-NAT IP addresses

Packet Flow Sequence – Reference



Flow Logic and Diagram

Initial Packet Processing - (Pre NAT)

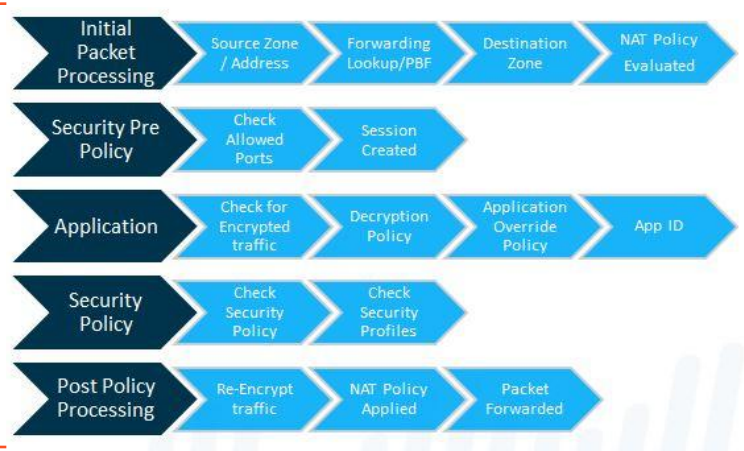
Security Pre-Policy - (Session Creation)

Application - (App-ID)

Security Policy - (Security Profiles Applied)

Post Policy Processing - (Post NAT)

5 Steps



 |

Flow Basic (Ingress Stage) - Reference

```
== 2019-07-28 05:46:49.698 -0600 ==
Packet received at ingress stage, tag 0, type ORDERED
Packet info: len 75 port 17 interface 17 vsys 1
  wqe index 44269 packet 0x0xc005303580, HA: 0, IC: 0
Packet decoded dump:
L2:      00:0c:29:36:8c:a2->00:0c:29:fa:99:bc, type 0x0800
IP:      10.0.0.3->8.8.4.4, protocol 17
         version 4, ihl 5, tos 0x00, len 61,
         id 3353, frag off 0x4000, ttl 64, checksum 35095(0x1789)
UDP:     sport 60945, dport 53, len 41, checksum 37016
Flow lookup, key word0 0x1100080035ee11 word1 0  word2 0x300000afffC
Session setup: vsys 1
No active flow found, enqueue to create session
```

Flow Basic (Session Setup Stage) - Reference

```
== 2019-07-28 05:46:49.698 -0600 ==
Packet received at slowpath stage, tag 1117685237, type ATOMIC
Packet info: len 75 port 17 interface 17 vsys 1
  wqe index 44269 packet 0x0xc005303580, HA: 0, IC: 0
Packet decoded dump:
L2:     00:0c:29:36:8c:a2->00:0c:29:fa:99:bc, type 0x0800
IP:     10.0.0.3->8.8.4.4, protocol 17
        version 4, ihl 5, tos 0x00, len 61,
        id 3353, frag_off 0x4000, ttl 64, checksum 35095(0x1789)
UDP:    sport 60945, dport 53, len 41, checksum 37016
Session setup: vsys 1
PBF lookup (vsys 1) with application none
Session setup: ingress interface ethernet1/2 egress interface ethernet1/1 (zone 9)
NAT policy lookup, matched rule index 0
Policy lookup, matched rule index 8,
TCI INSPECT: Do TCI lookup policy - appid 0
Allocated new session 55327.
set exclude_video in session 55327 0xe03d849d80 0 from work 0xe0151bcb80 0
Rule: index=0 name=SrcNAT-Out, cfg_pool_idx=1 cfg_fallback_pool_idx=0
NAT Rule: name=SrcNAT-Out, cfg_pool_idx=1; Session: index=55327, nat_pool_idx=1
Packet matched vsys 1 NAT rule 'SrcNAT-Out' (index 1),
source translation 10.0.0.3/60945 => 172.20.9.225/35326
Created session, enqueue to install  work 0xe0151bcb80 exclude_video 0,session 55327
```

Numbered from 0, skips disabled rules

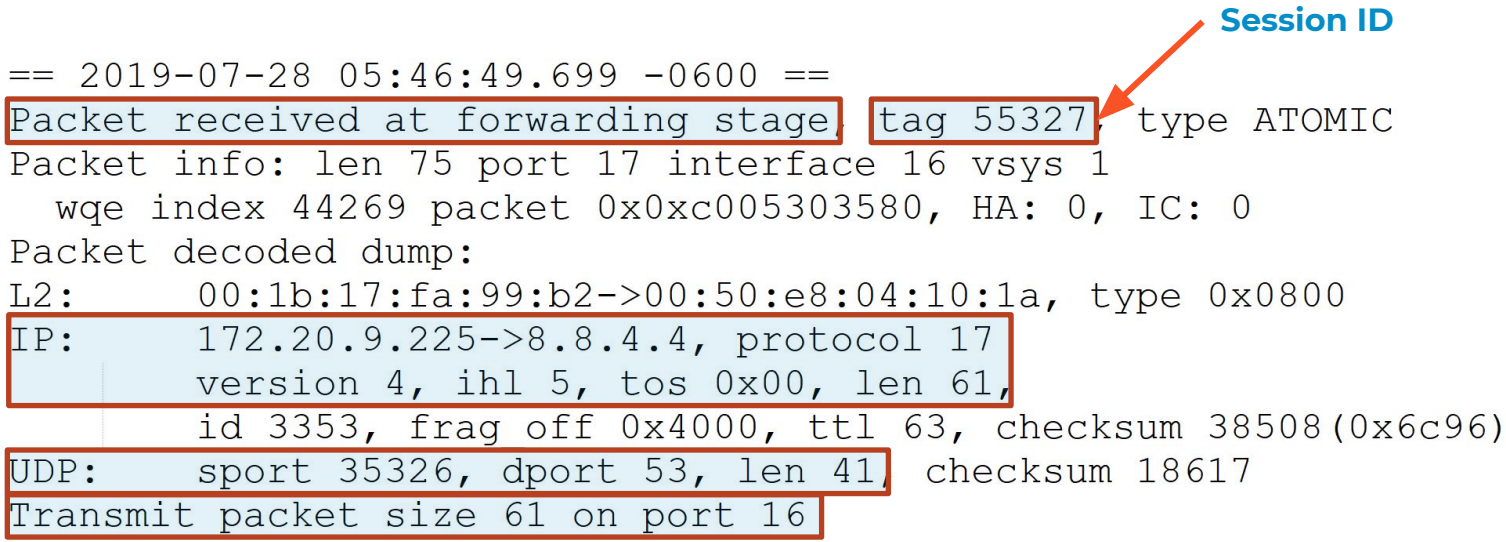
AS profile, DNS Security (tunneling)

Flow Basic (Inspection & Enforcement Stage)- Reference

```
== 2019-07-28 05:46:49.699 -0600 ==
Packet received at fastpath stage, tag 55327, type ATOMIC
Packet info: len 75 port 17 interface 17 vsys 1
  wqe index 44269 packet 0x0xc005303580, HA: 0, IC: 0
Packet decoded dump:
L2:      00:0c:29:36:8c:a2->00:0c:29:fa:99:bc, type 0x0800
IP:      10.0.0.3->8.8.4.4, protocol 17
         version 4, ihl 5, tos 0x00, len 61,
         id 3353, frag off 0x4000, ttl 64, checksum 35095(0x1789)
UDP:     sport 60945, dport 53, len 41, checksum 37016
Flow fastpath, session 55327 (set work 0xe0151bcb80 exclude_video 0 from sp 0
IP checksum valid
2019-07-28 05:46:49.699 -0600  pan_flow_process_fastpath(src/pan_flow_proc.c:
DSCP: 0x00
NAT session, run address/port translation
Forwarding lookup, ingress interface 17
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 8.8.4.4
Route found, interface ethernet1/1, zone 9, nexthop 172.20.0.1
Resolve ARP for IP 172.20.0.1 on interface ethernet1/1
ARP entry found on interface 16
```

Qo
S

Flow Basic (Egress Stage) - Reference

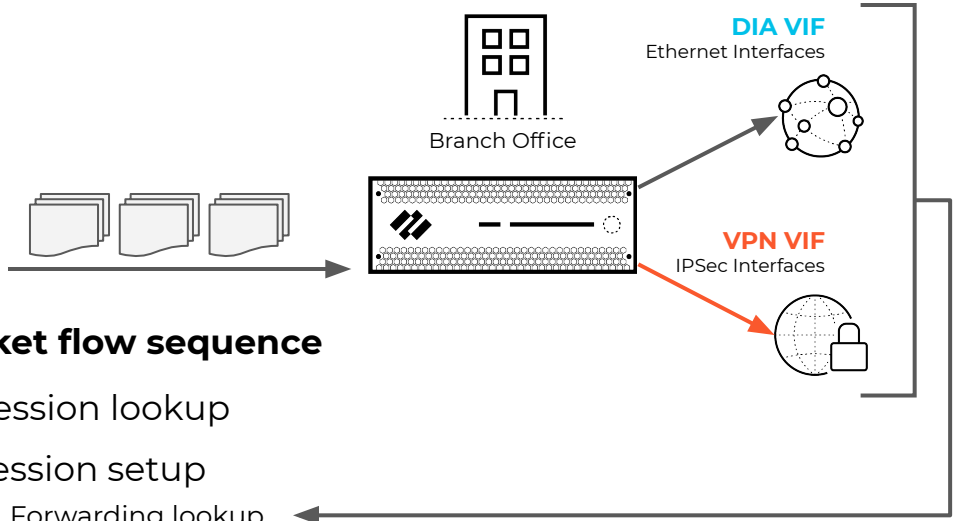


Packet Diagnostic Logging Options

```
admin@TravelFirewall> debug dataplane packet-diag set log feature
> all             all
> appid           appid
> base            base
> cfg             cfg
> ctd             ctd
> flow            flow
> http2           http2
> misc            misc
> module          module
> pow             pow
> proxy           proxy
> ssl             ssl
> tcp             tcp
> tdb             tdb
> tunnel          tunnel
> url_trie        url_trie
> zip             zip
```

5.8 Troubleshoot PAN-OS-based SDWAN

5.8 PAN-OS-based SDWAN

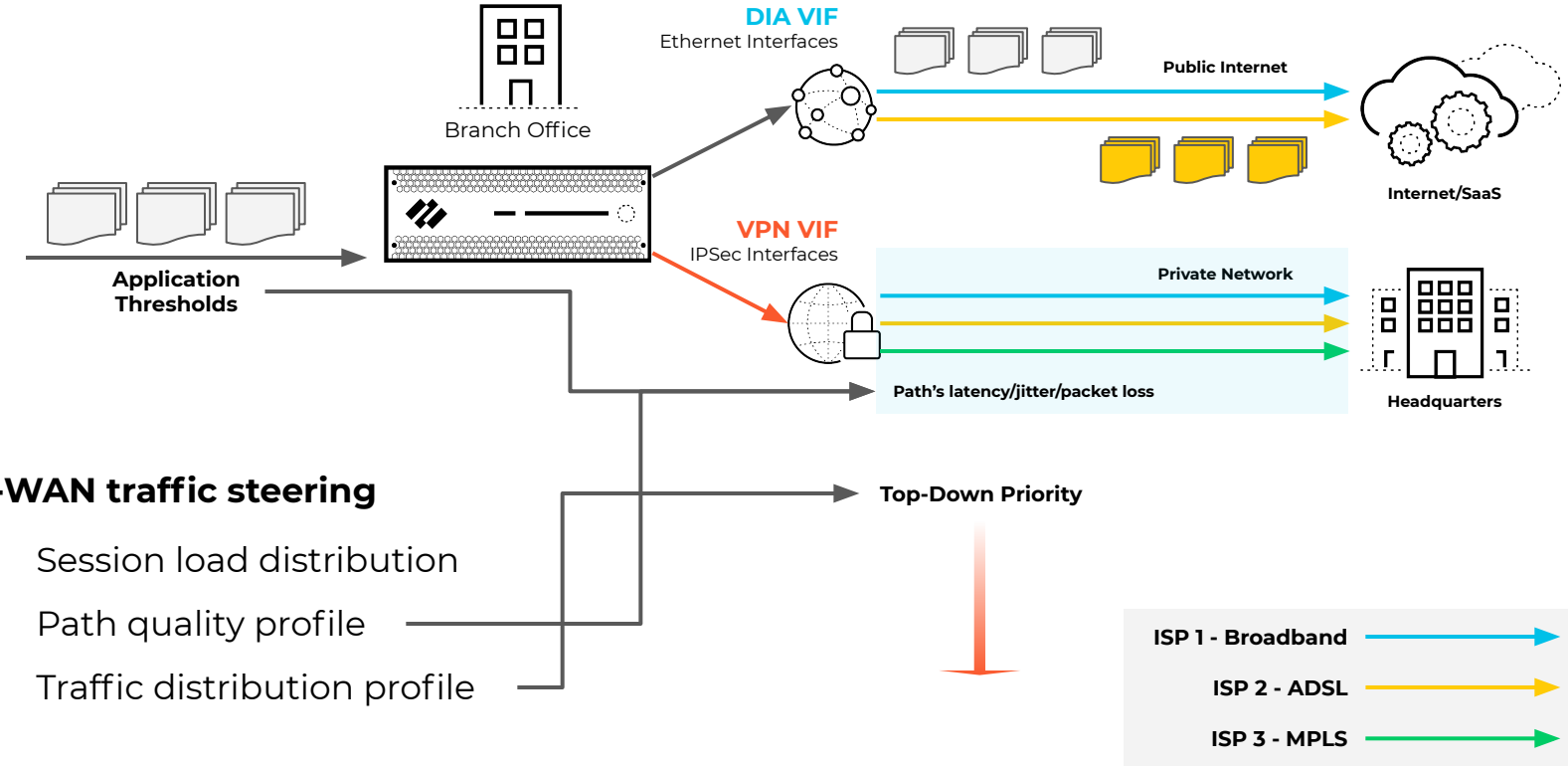


Packet flow sequence

1. Session lookup
2. Session setup
   - Forwarding lookup
   - NAT policy lookup
   - Security policy lookup
3. Content inspection
4. Forwarding/egress ← SD-WAN logic applied
5. Transmit packet

Egress interface is identified from Layer 3 route table lookup

5.8 PAN-OS-based SDWAN



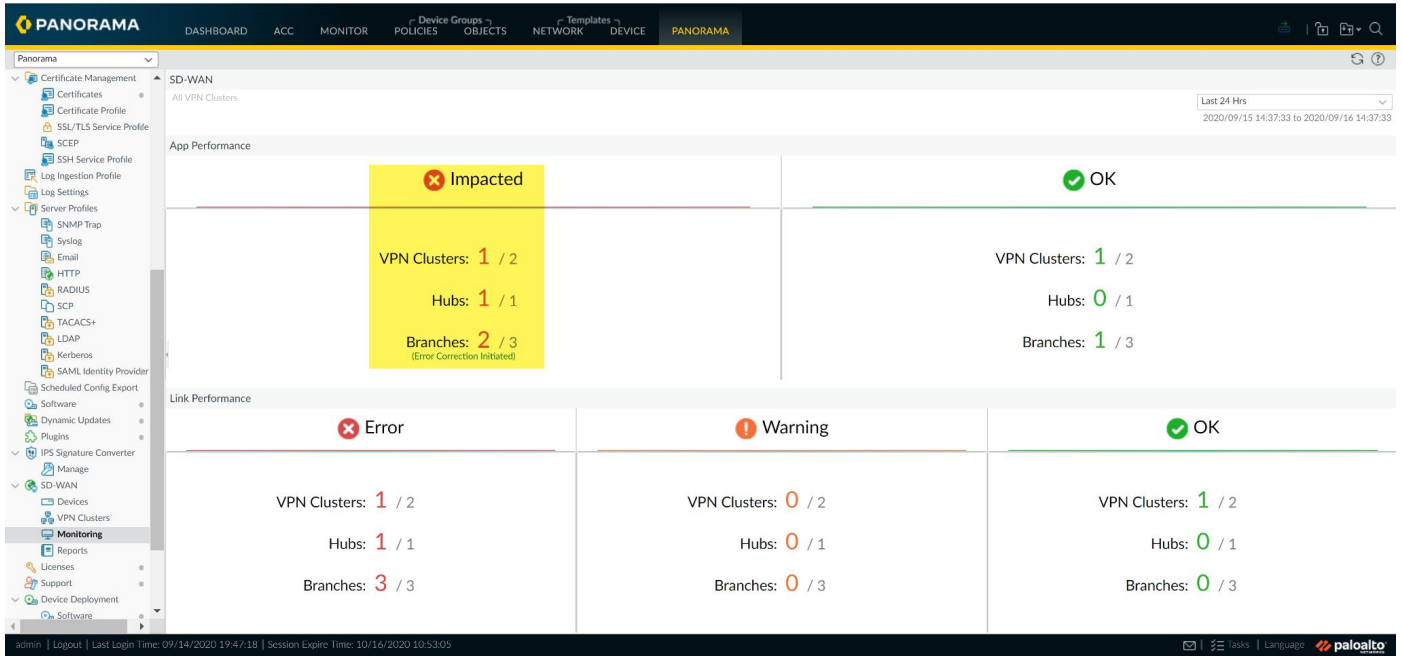
5.8.1 & 5.8.2 Troubleshoot App and Link Performance via Panorama Monitoring

- The Panorama Monitoring tab displays the application and link performance of your VPN clusters
  - Panorama > SD-WAN > Monitoring
- A VPN cluster is just a functional group of branch and hub firewalls that communicate with each other
- Troubleshoot issues by viewing VPN Cluster information and by drilling down into detailed statistics to isolate the problematic sites, applications, and links
- For the PCNSE exam, understand the high level workflow for determining an SD-WAN path failure

5.8.1 & 5.8.2 Troubleshoot App and Link Performance via Panorama Monitoring

Goal is to understand what is causing degraded performance for your apps and services

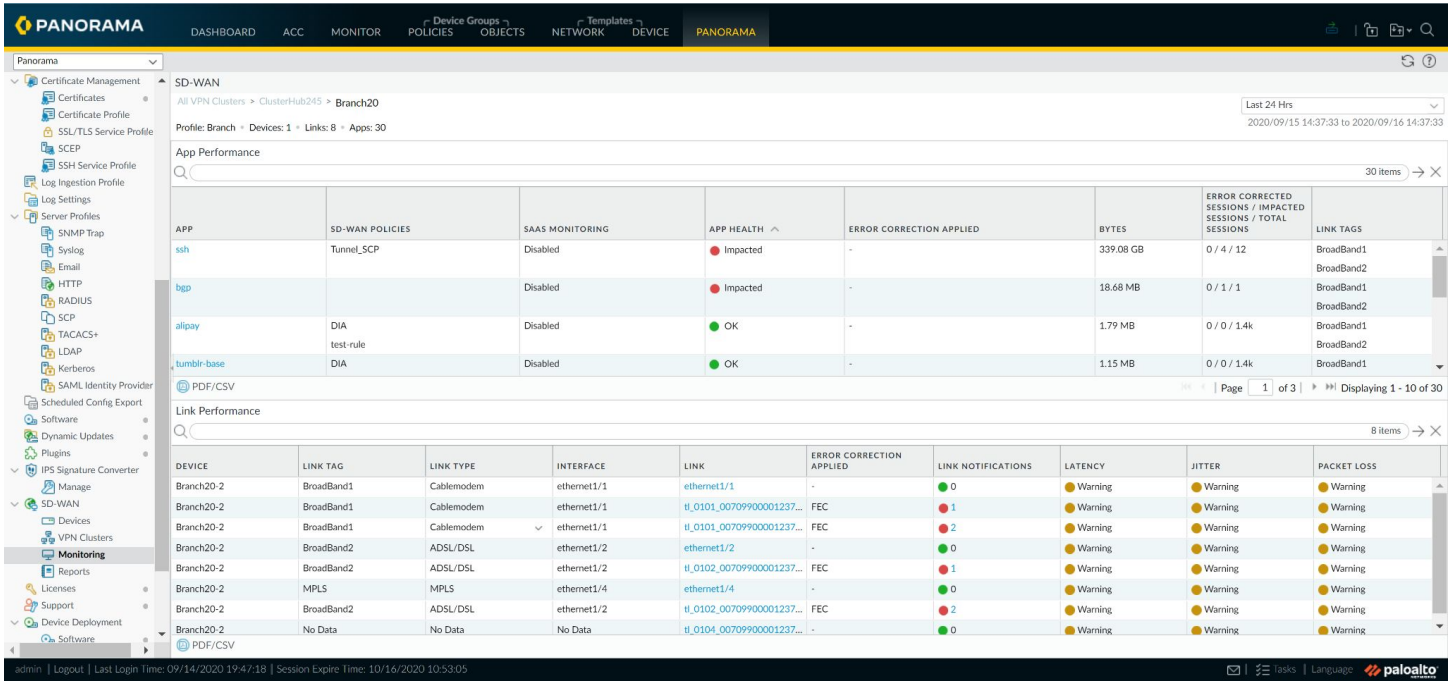
Start by identifying why VPN clusters are impacted and application traffic failed over to different links



5.8.1 & 5.8.2 Troubleshoot App and Link Performance via Panorama Monitoring

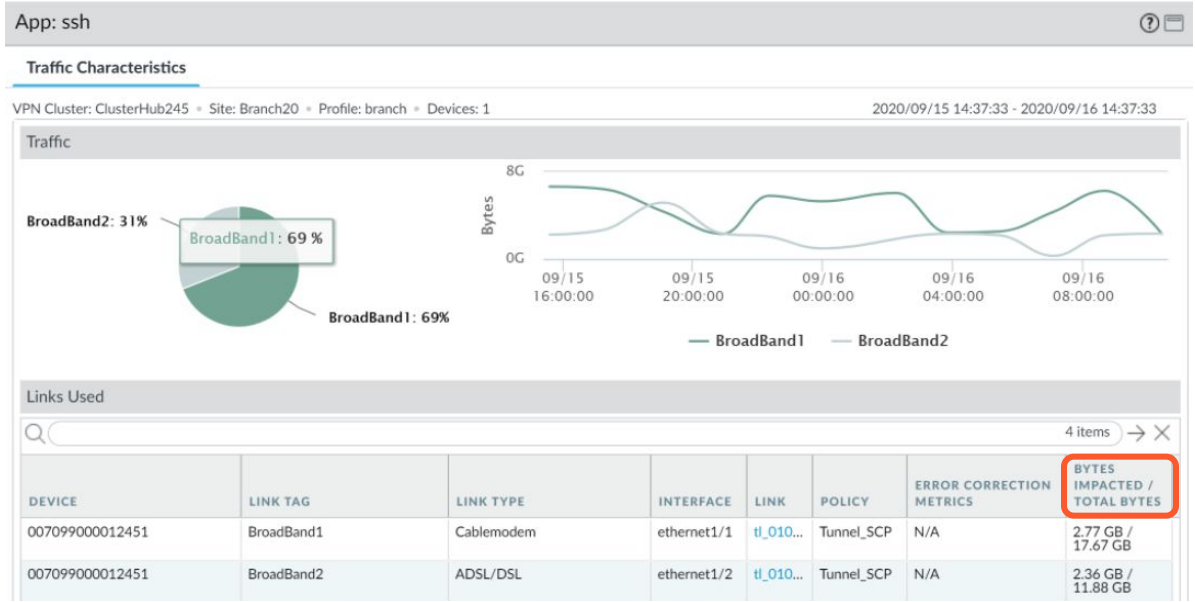
Drill down into your VPN clusters and filter for the site in question

View the impacted apps and the corresponding link performance



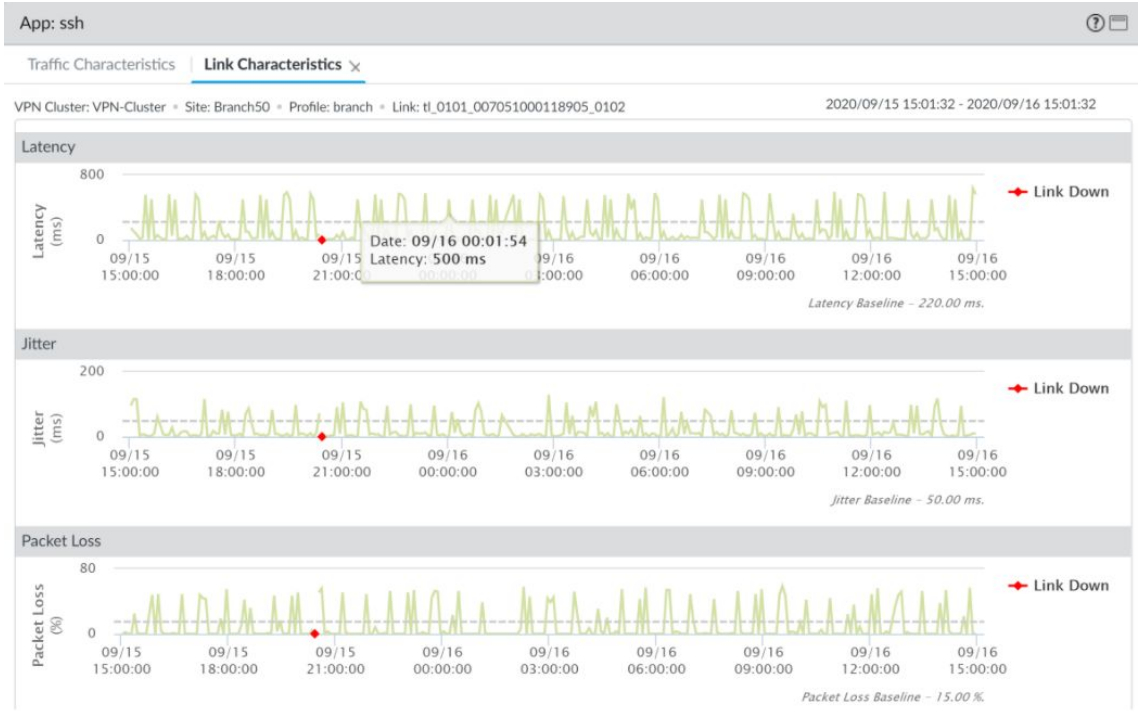
5.8.1 & 5.8.2 Troubleshoot App and Link Performance via Panorama Monitoring

- You can click any application listed and view detailed breakdown of traffic across your internet services
- View the bytes of data transferred and how many of those bytes were impacted on each link used



5.8.1 & 5.8.2 Troubleshoot App and Link Performance via Panorama Monitoring

Identify the health metric that caused the app to swap links



5.8.1 & 5.8.2 Troubleshoot App and Link Performance via Panorama Monitoring

After you have identified the health metric that caused the app performance to degrade, consider the following options:

- Adding additional links to the Traffic Distribution Profile
- Reconfiguring the health thresholds in your Path Quality Profile
- Consulting your internet service provider (ISP) to determine if there are impacts to your network outside of your control that can be resolved

5.8 References

Troubleshoot Link Performance:
https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/troubleshooting/troubleshoot-link-performance.html

Troubleshoot App Performance:
https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/troubleshooting/troubleshoot-app-performance.html

Monitor SD-WAN Application and Link Performance:
https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/monitoring-and-reporting/monitor-sd-wan-application-and-link-performance.html