

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

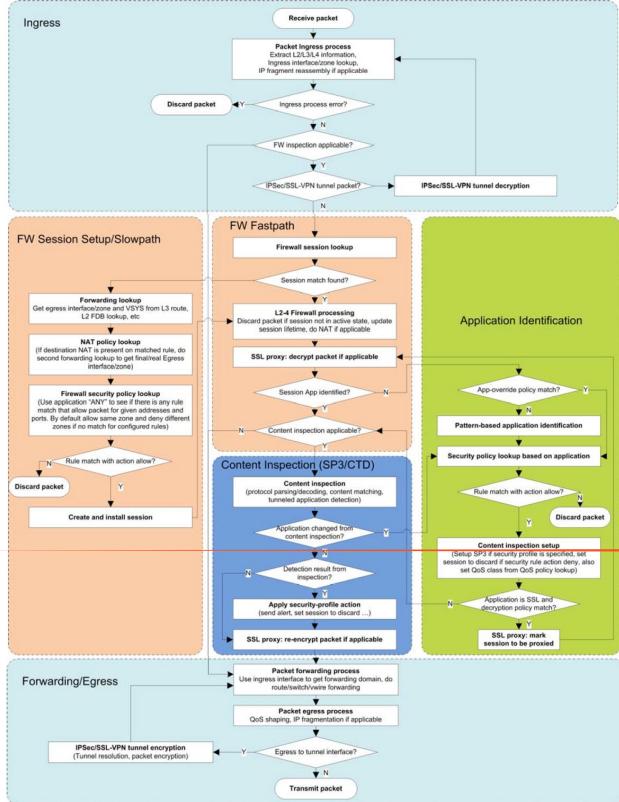
- 5.0 – General Troubleshooting Topics (Flow Basic, Destination NAT, etc.)
- 5.1 - Troubleshoot Site-to-Site tunnels
- 5.2 - Troubleshoot Physical Interfaces
- 5.3 - Troubleshoot SSL Decryption
- 5.4 - Troubleshoot Routing
- 5.5 - Investigate Traffic Patterns on the NGFW or Panorama
- 5.6 - Troubleshoot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

New Features (v10.1)

Section 5.0

General Troubleshooting Topics

Packet Flow Sequence – Reference



Flow Logic and Diagram

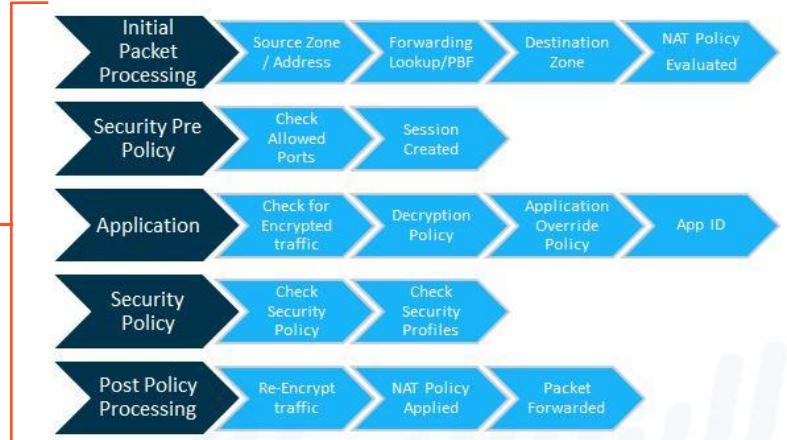
Initial Packet Processing - (Pre NAT)

Security Pre-Policy - (Session Creation)

Application - (App-ID)

Security Policy - (Security Profiles Applied)

Post Policy Processing - (Post NAT)



<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000000ClVHCA0>

GUI Based Troubleshooting tools

The screenshot shows the Palo Alto Networks PA-220 device configuration interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE, with DEVICE selected. The left sidebar contains several categories: Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting (selected), Certificate Management, Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusion, SSH Service Profile, Response Pages, Log Settings, Server Profiles, SNMP Trap, Syslog, Email, HTTP, Netflow, RADIUS, TACACS+, LDAP, Kerberos, SAML Identity Provider, Multi Factor Authentication, Local User Database, Users, and User Groups. The Troubleshooting section is expanded, showing sub-options like Ping, Traceroute, Log Collector Connectivity, and External Dynamic List. The main content area displays the 'Test Configuration' screen for the 'Ping' test. It includes fields for Select Test (Ping), Count (5), Interval ([1 - 2]), Source, Pattern, Size ([0 - 65468]), Tos ([1 - 255]), Ttl ([1 - 255]), and Host. There are also checkboxes for Bypass routing tables and send directly to a host on an attached network, Don't fragment echo request packets (IPv4), Force to IPv6 destination, and Don't attempt to print addresses symbolically. At the bottom are Execute and Reset buttons.

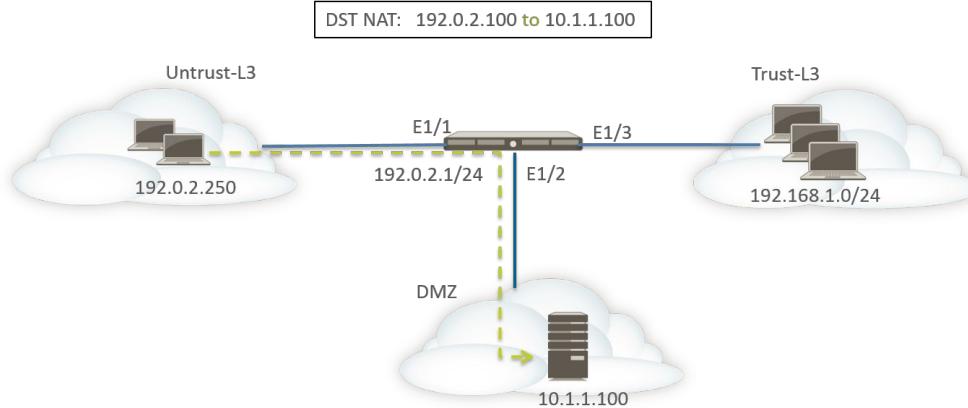
GUI Based Tests:

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).

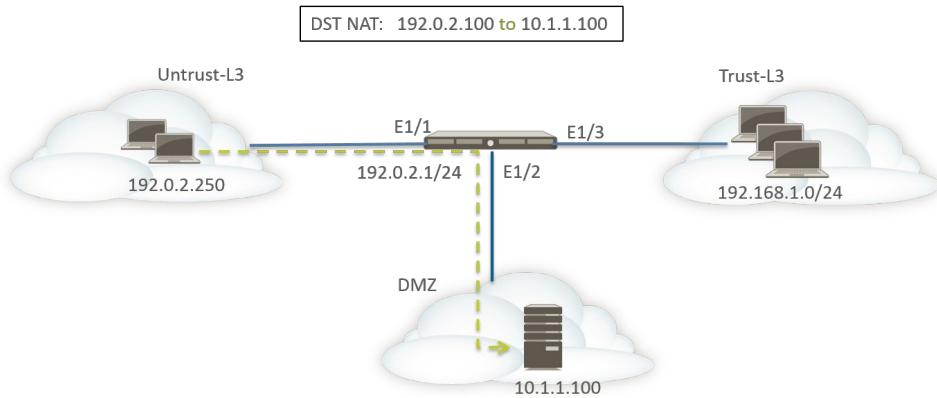
The firewall receives the ARP request packet for destination 192.0.2.100 on the Ethernet1/1 interface and processes the request. The firewall only responds to the ARP request with its own MAC address if DNAT rule is configured.

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:

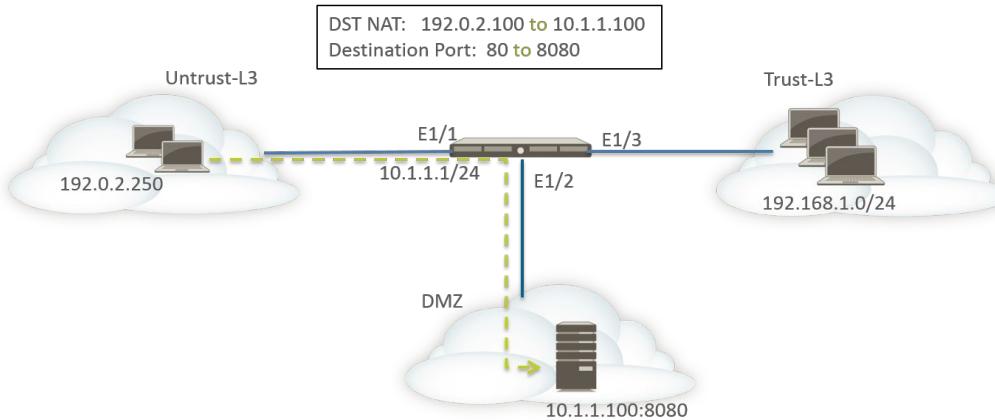
NAME	TAGS	Original Packet						Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	destination-translation address: webserver-private	

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:

NAME	Source		Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
	ZONE	ADDRESS	ZONE	ADDRESS					
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**

NAME	TAGS	Original Packet						Translated Packet			
		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	

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

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

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

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=kA10q000000CIRTCAO>

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)

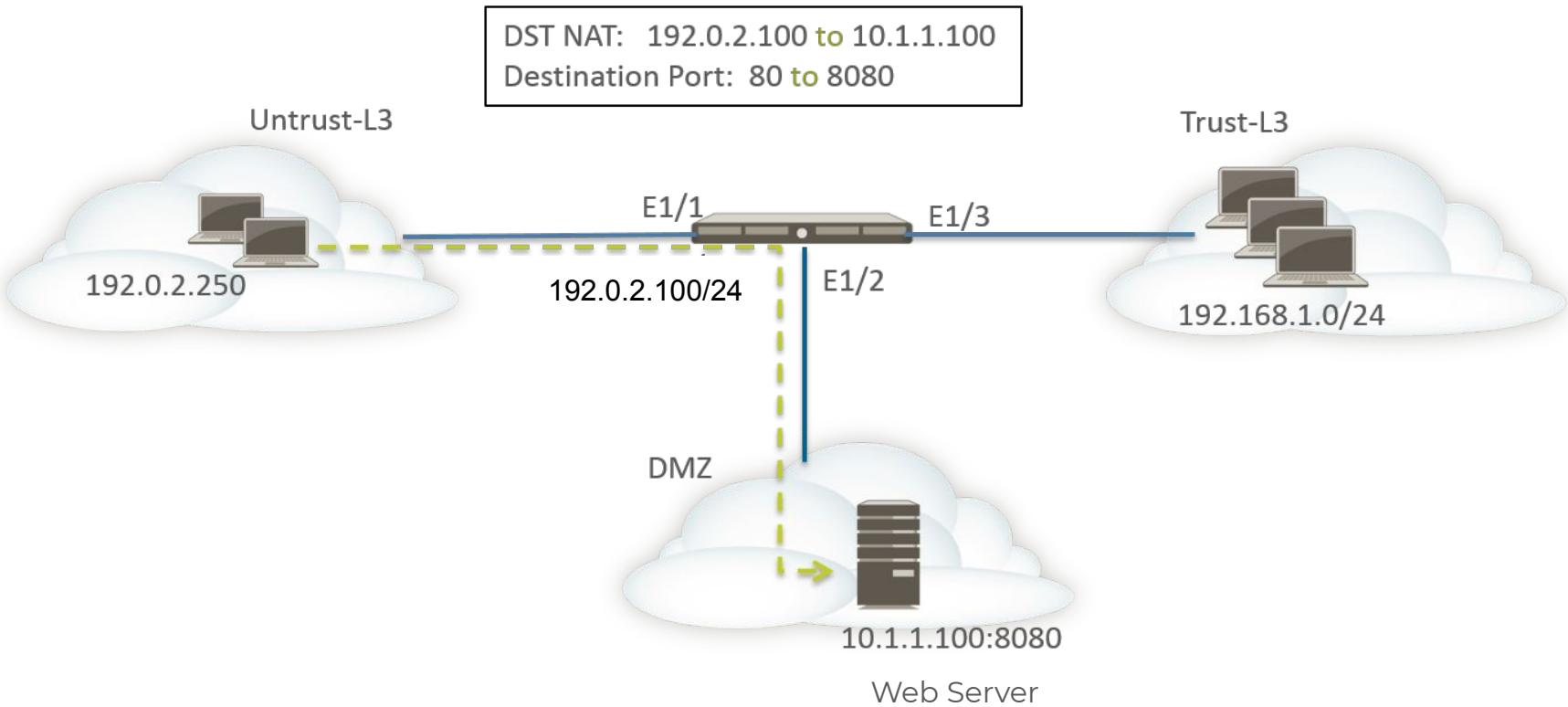
Run the **show running resource-monitor** command (to review dataplane CPU usage)

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=kA10q000000CIRTCAO>

QUIZ
TIME



Section 5.1

Troubleshooting IPSec Tunnels

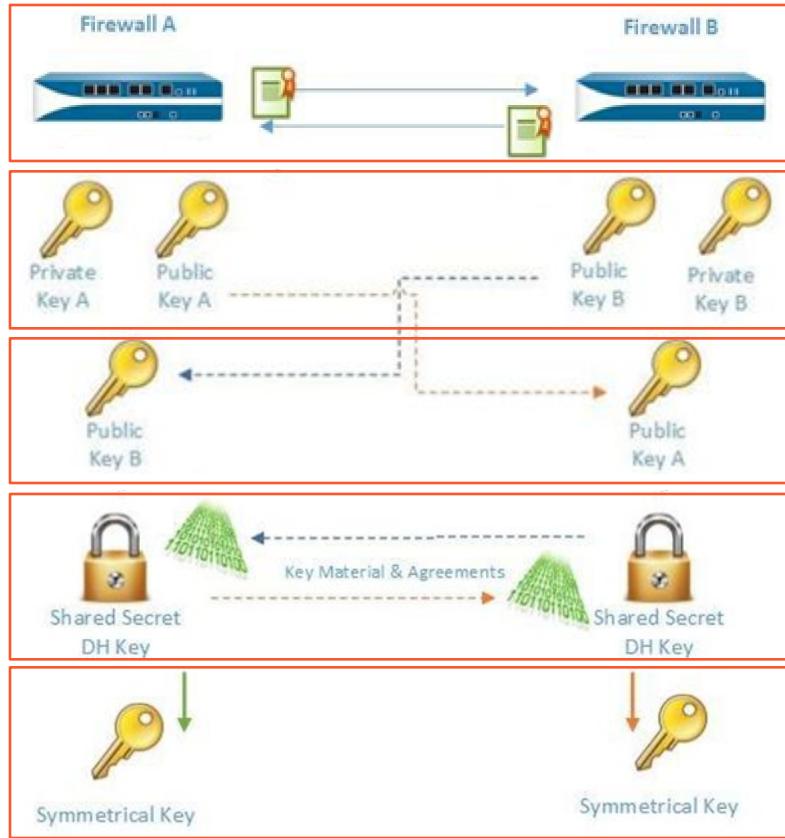
5.1.1 Troubleshooting Site-to-Site Tunnels

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

NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface				
			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...	Up

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 PI done	2	VPN_to_H4B_SOLIHULL_MANU_Primary	1756	759	Init	00000000	00000000	00000000 GetS

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

Q (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:e7007cccb3f4e822:291c2e31bfa78671.
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:f40a0ce4fcc66fd: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		Resp ESP/ DH2/tun1/	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.**

NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface				COMMENT
			INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	
IPSec-Tunnel.3_1.1.2-to-1.1.1	Tunnel Info	Auto Key	ethernet1/3	1.1.2/30	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:
<p>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.</p> <p>or</p> <p>IKE phase 1 negotiation is failed. Couldn't find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]</p>	<ul style="list-style-type: none">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.
<p>Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...</p> <p>or</p> <p>IKE phase-1 negotiation is failed. Unable to process peer's SA payload.</p>	Check the IKE Crypto profile configuration to verify that the proposals on both sides have a common encryption, authentication, and DH Group proposal.
<p>pfs group mismatched:my: 2peer: 0</p> <p>or</p> <p>IKE phase-2 negotiation failed when processing SA payload. No suitable proposal found in peer's SA payload.</p>	<p>Check the IPSec Crypto profile configuration to verify that:</p> <ul style="list-style-type: none">pfs is either enabled or disabled on both VPN peersthe DH Groups proposed by each peer has at least one DH Group in common
<p>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.</p>	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:

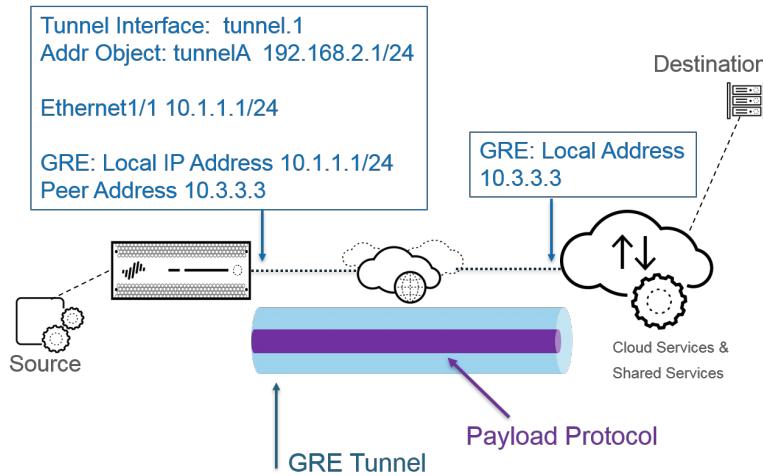
Change IKE Gateway config to use the “default” crypto profile, rather than “IKE-Phase1-MaxCrypto” profile.

IKE Advanced Options						COMMENT
MODE	PASSIVE MODE	NAT TRAVERSAL	CRYPTO PROFILE	DPD	LIVENESS	
auto	<input type="checkbox"/>	<input type="checkbox"/>	IKE-Phase1-MaxCrypto	enabl...		IPSec Tunnel to PA-220-2 in San Francisco

IKE Advanced Options						COMMENT
MODE	PASSIVE MODE	NAT TRAVERSAL	CRYPTO PROFILE	DPD	LIVENESS	
auto	<input type="checkbox"/>	<input type="checkbox"/>	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.

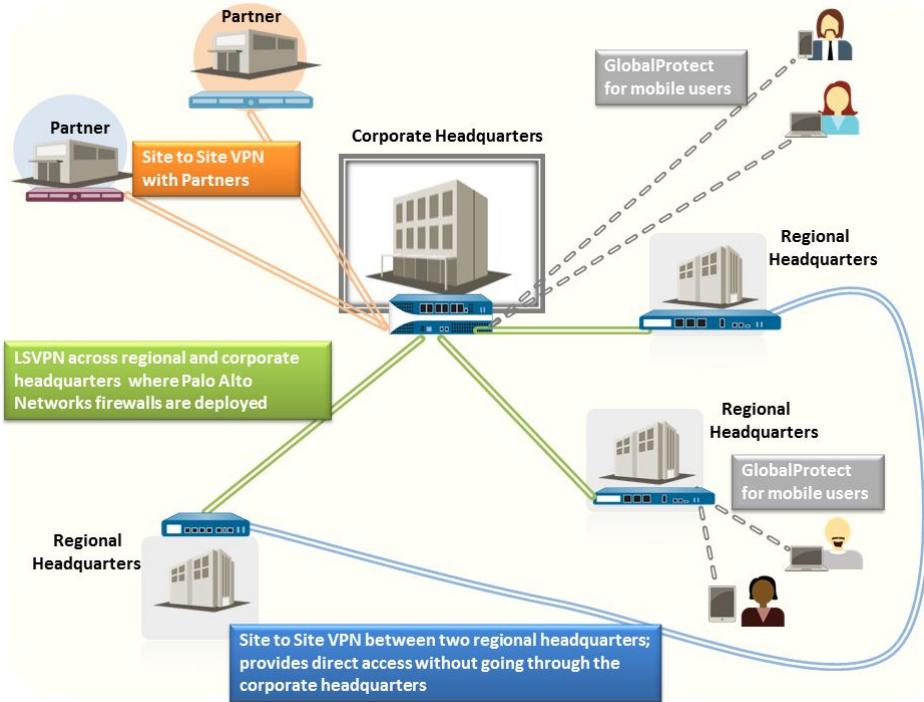
The firewall does not support a single interface acting as both a GRE tunnel endpoint and a decryption broker.

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 (LSPN) or (1-to-Many)

5.1.3 - Types of VPNs and Proxy IDs

Route-Based VPNs

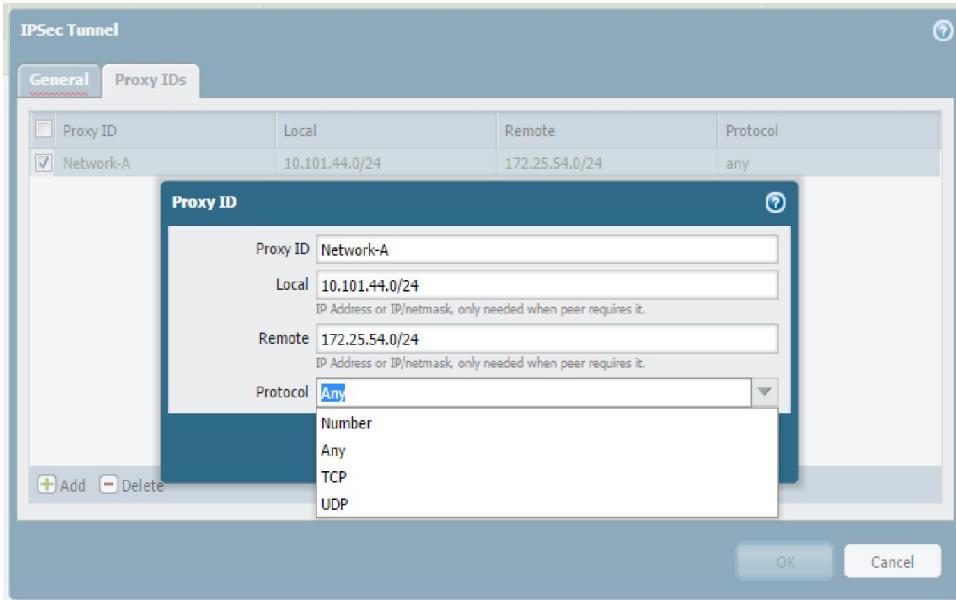
- Firewalls that support route-based VPNs: Palo Alto Firewalls, Juniper SRX, Juniper Netscreen, and Checkpoint.
- IPsec tunnel is invoked during route lookup for remote end of the proxy-ID
- Remote end of the interesting traffic has a route pointing out through the tunnel interface.
- Supports routing (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.
- Policies 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.

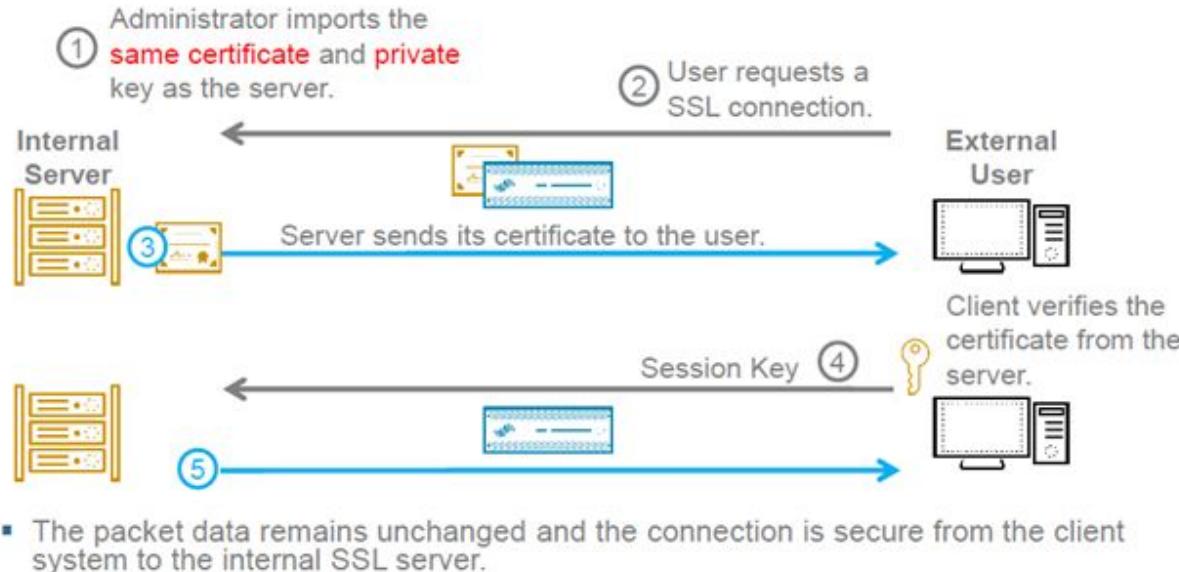
Check for the transceiver transmit light on by using the power meter

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



Common Problems

Unsupported cipher suites

Unsupported EC curves

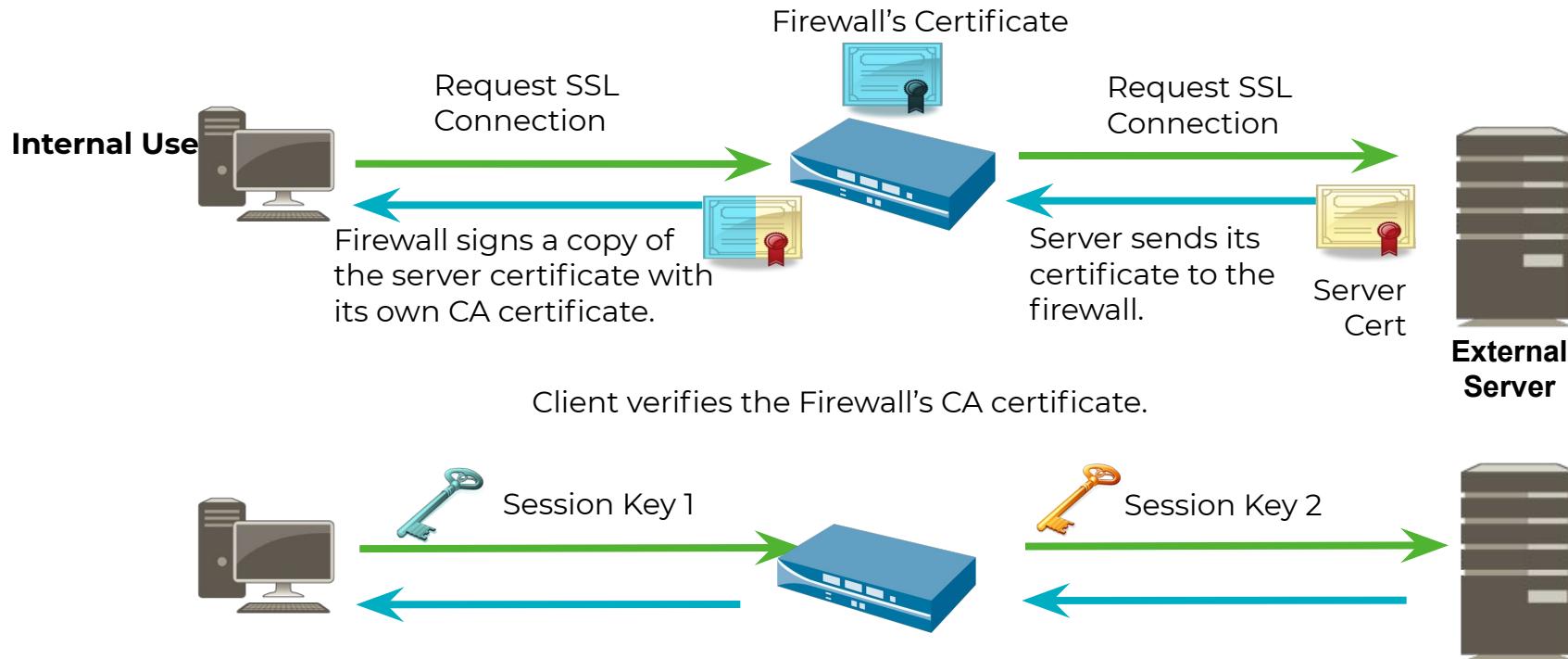
Server using certificate chains

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

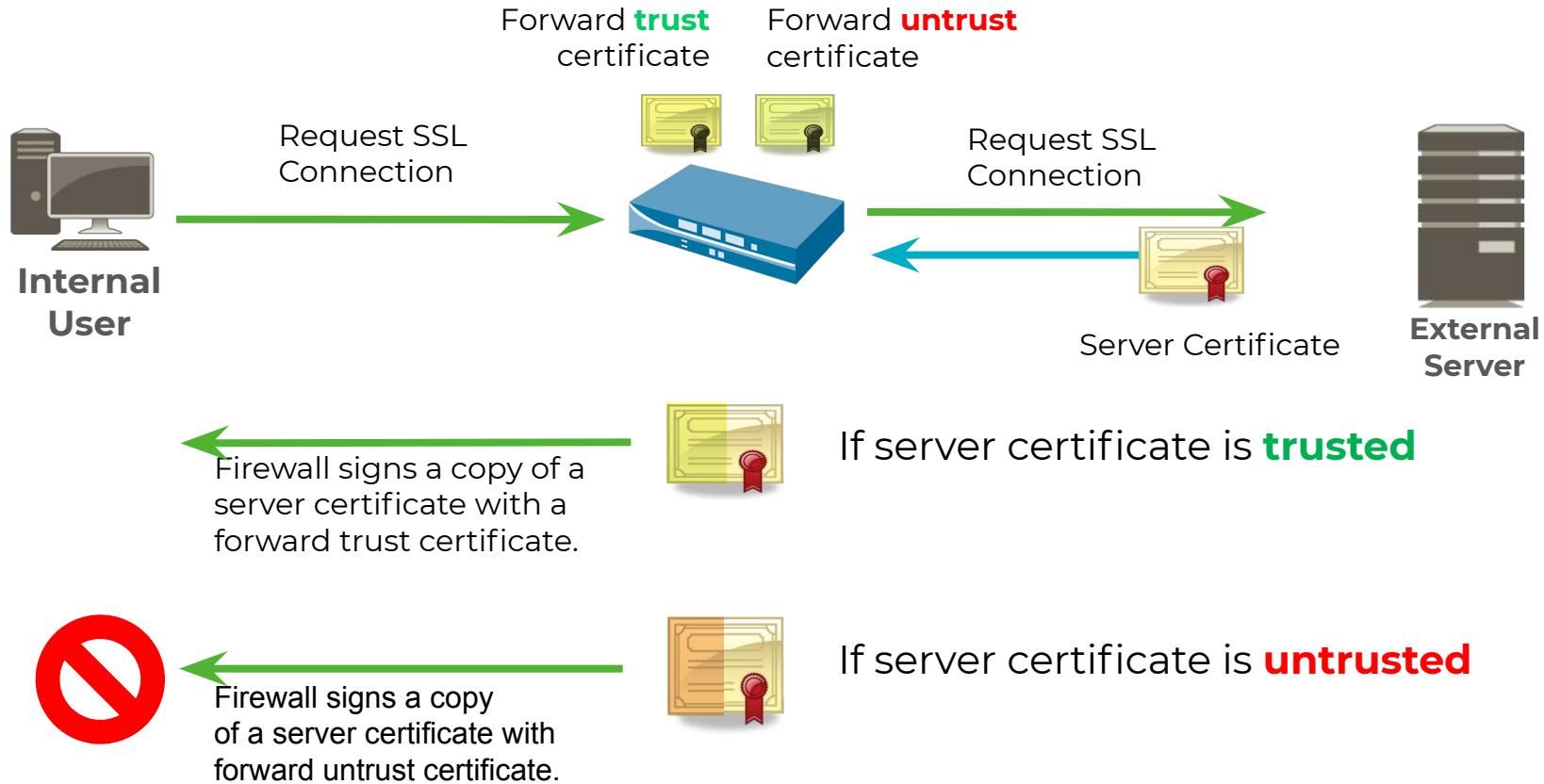
Certificate information

Name	Demo in a Box CA
Subject	/DC=net/DC=demoinabox/CN=DIABCA
Issuer	/DC=net/DC=demoinabox/CN=DIABCA
Not Valid Before	May 2 00:43:26 2020 GMT
Not Valid After	May 2 00:53:26 2030 GMT
Algorithm	RSA
<input checked="" type="checkbox"/> Certificate Authority	
<input checked="" type="checkbox"/> Forward Trust Certificate	
<input type="checkbox"/> Forward Untrust Certificate	
<input checked="" type="checkbox"/> Trusted Root CA	

Certificate information

Name	untrusted-CA
Subject	/CN=untrust.demoinabox.net
Issuer	/CN=untrust.demoinabox.net
Not Valid Before	Feb 21 23:00:32 2020 GMT
Not Valid After	May 1 23:00:32 2022 GMT
Algorithm	RSA
<input checked="" type="checkbox"/> Certificate Authority	
<input type="checkbox"/> Forward Trust Certificate	
<input checked="" type="checkbox"/> Forward Untrust Certificate	
<input type="checkbox"/> Trusted Root CA	

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 displayed 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

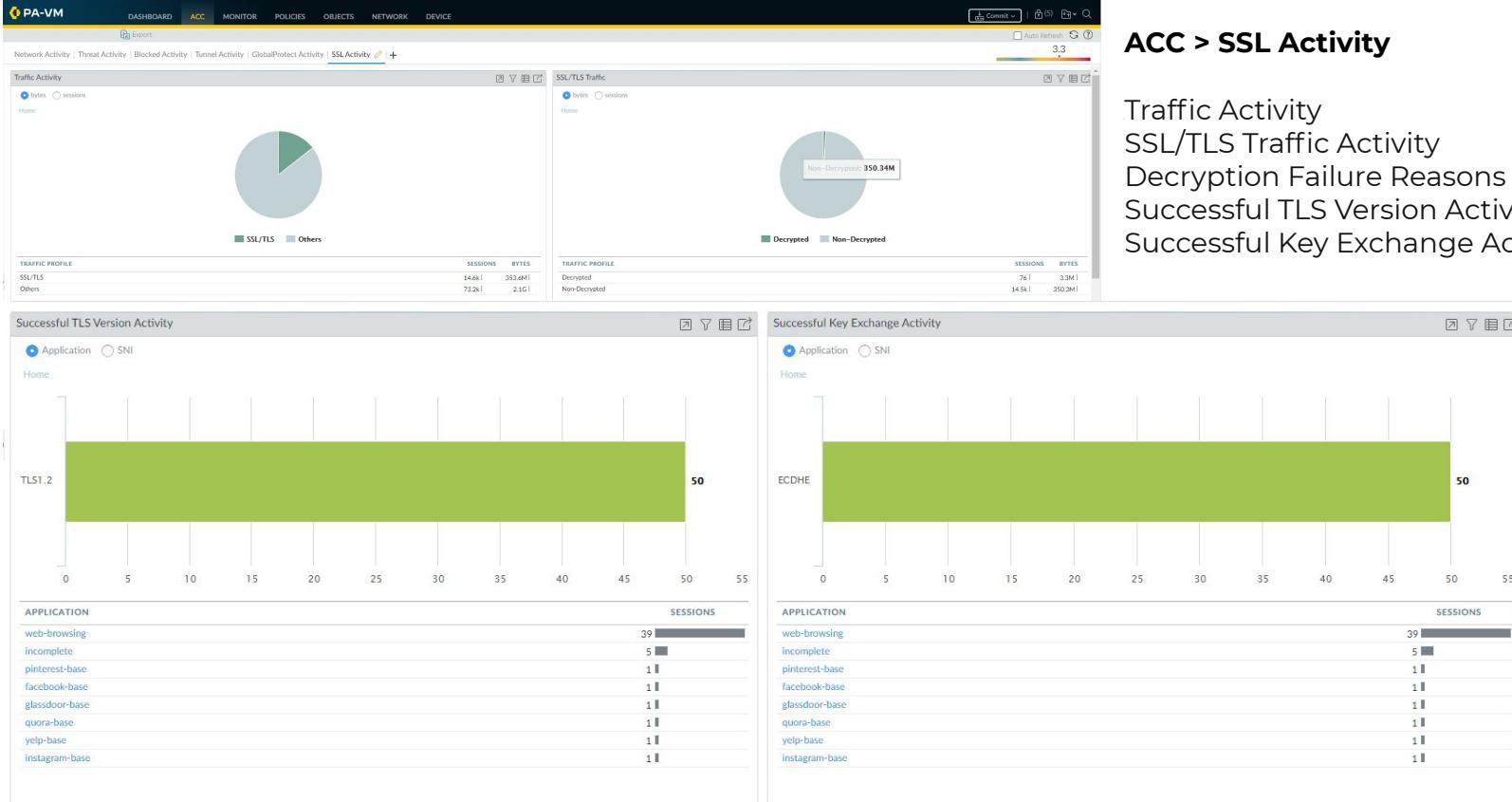
Requirements:

- 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 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 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 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		45.6.131.229	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

The screenshot shows the 'Decryption Policy Rule' configuration window. On the left, under 'Log Settings', two checkboxes are highlighted with a red box: 'Log Successful SSL Handshake' (unchecked) and 'Log Unsuccessful SSL Handshake' (checked). On the right, the 'Log Forwarding Profile Match List' is displayed, showing a single entry named 'decryption-log-forwarding' with a description 'Decryption Logs'. The 'Log Type' is set to 'decryption'. Under 'Forward Method', 'decryption' is selected. At the bottom right are 'OK' and 'Cancel' buttons.

Decryption Policy Rule

General | Source | Destination | Service/URL Category | Options

Action: No Decrypt
Type: SSL Forward Proxy
Decryption Profile: None

Log Settings

Log Successful SSL Handshake
 Log Unsuccessful SSL Handshake

Log Forwarding: None

Forwarding Profile: None

Log Forwarding Profile Match List

Name	Description	Log Type
decryption-log-forwarding	Decryption Logs	decryption

Forward Method

decryption

SNMP ^
SYSLOG ^
HTTP ^

OK Cancel

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

The screenshot shows the 'Decryption Profile' configuration page for a profile named 'global-trusted'. The 'SSL Decryption' tab is selected. A red box highlights the 'SSL Forward Proxy' tab, which is currently inactive. The 'Unsupported Mode Checks' and 'Failure Checks' sections are also highlighted with a red box. In the 'Unsupported Mode Checks' section, the 'Block sessions with unsupported cipher suites' checkbox is checked. In the 'Failure Checks' section, the 'Block sessions if resources not available' checkbox is checked.

The screenshot shows the 'Decryption Profile' configuration page for a profile named 'global-trusted'. The 'SSH Proxy' tab is selected. A red box highlights the 'Unsupported Mode Checks' and 'Failure Checks' sections. In the 'Unsupported Mode Checks' section, the 'Block sessions with unsupported versions' checkbox is checked. In the 'Failure Checks' section, the 'Block sessions if resources not available' checkbox is checked.

The screenshot shows the 'Decryption Profile' configuration page for a profile named 'global-trusted'. The 'SSL Inbound Inspection' tab is selected. A red box highlights the 'Unsupported Mode Checks' and 'Failure Checks' sections. In the 'Unsupported Mode Checks' section, the 'Block sessions with unsupported cipher suites' checkbox is checked. In the 'Failure Checks' section, both 'Block sessions if resources not available' and 'Block sessions if HSM not available' checkboxes are unchecked.

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**”

The screenshot shows the Palo Alto Networks PA-VM interface. On the left, the navigation menu includes options like Security, NAT, QoS, Policy Based Forwarding, and Decryption. The Decryption section is currently selected. The main table lists four decryption policies:

NAME	TAGS	Decrypt Options				
		ACTION	TYPE	DECRIPTION PROFILE	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
1 temp-no-exp	none	decrypt	ssl-forward-proxy	temp_no_exp	true	true
2 No Decrypt	LIVE INSIDE-2	no-decrypt	ssl-forward-proxy	bp tls1.1-tls1.3_no-blo...	true	true
3 No Decrypt-NoECDHE	LIVE INSIDE-2 TEST	no-decrypt	ssl-forward-proxy	No ECDHE	true	true
4 Big Brother	LIVE	decrypt	ssl-forward-proxy	bp tls1.1-tls1.3-1	true	true

The row for 'Big Brother' is highlighted with a red box. The 'bp tls1.1-tls1.3-1' profile is also highlighted with a red box. To the right, a detailed view of the 'Decryption Profile' for 'bp tls1.1-tls1.3-1' is shown. The 'SSL Protocol Settings' tab is selected. The 'Min Version' is set to 'TLSv1.1' and the 'Max Version' is set to 'TLSv1.3'. Other settings include Key Exchange Algorithms (RSA, DHE, ECDHE), Encryption Algorithms (3DES, RC4, AES128-GCM, AES256-GCM, CHACHA20-POLY1305), and Authentication Algorithms (MD5, SHA1, SHA256, SHA384). A note at the bottom states: "Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead." Buttons for 'OK' and 'Cancel' are at the bottom right.

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')

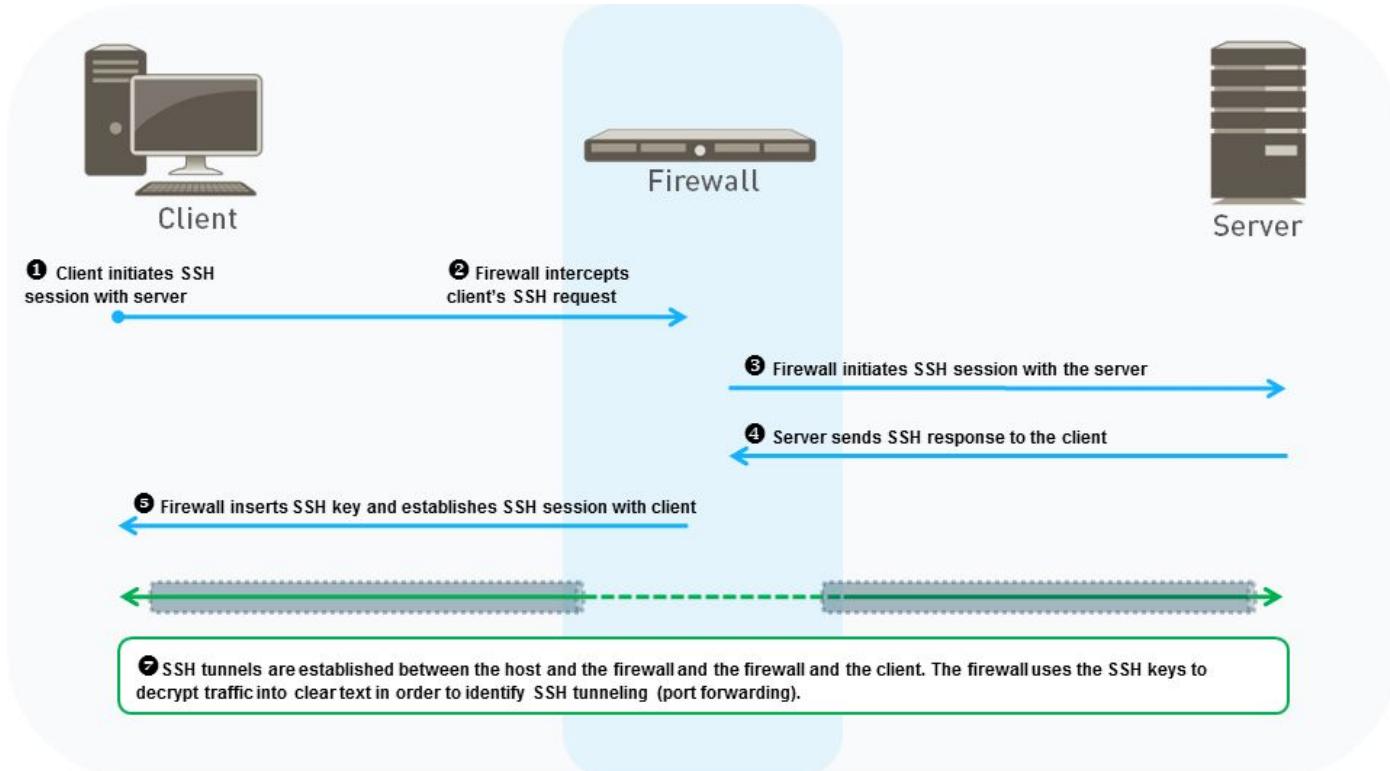
	RECEIVE TIME	APPLICATION	PROXY TYPE	SOURCE ADDRESS	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	TLS VERSION	POLICY NAME
🔗	06/02 11:25:30	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
🔗	06/02 11:16:53	incomplete	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	di-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	di-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 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

Virtual Router - default

Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information

Route Table | Forwarding Table | Static Route Monitoring

Route Table Unicast Multicast Display Address Family IPv4 and IPv6

DESTINATION	NEXT HOP	METRIC	WEIGHT	FLAGS	AGE	INTERFACE
0.0.0.0/0	73.254.100.1	10		AS		ethernet1/1
1.1.0.0/30	1.1.1.1	0		AH		ethernet1/3
1.1.1.1/32	0.0.0.0	0		AH		
73.254.100.0/24	73.254.100.132	0		AH		ethernet1/1
73.254.100.132/32	0.0.0.0	0		AH		
172.16.1.1/32	0.0.0.0	0		AH		
192.168.1.0/24	192.168.1.254	0		AH		vlan
192.168.1.254/32	0.0.0.0	0		AH		
192.168.2.1/32	0.0.0.0	10				tunnel3
192.168.40.0/24	192.168.40.254	0				ethernet1/7.40
192.168.40.254/32	0.0.0.0	0		AH		

Virtual Router - default

Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information

Route Table | **Forwarding Table** | Static Route Monitoring

Display Address Family IPv4 and IPv6

DESTINATION	NEXT HOP	FLAGS	INTERFACE	MTU
0.0.0.0/0	73.254.100.1	ug	ethernet1/1	1500
1.1.0.0/30	0.0.0.0	u	ethernet1/3	1500
1.1.1.1/32	0.0.0.0	uh	ethernet1/3	1500
73.254.100.0/24	0.0.0.0	u	ethernet1/1	1500
73.254.100.132/32	0.0.0.0	uh	ethernet1/1	1500
172.16.1.1/32	0.0.0.0	uh	loopback1	1500
192.168.1.0/24	0.0.0.0	u	vlan	1500
192.168.1.254/32	0.0.0.0	uh	vlan	1500
192.168.2.1/32	0.0.0.0	u	tunnel3	1500
192.168.40.0/24	0.0.0.0	u	ethernet1/7.40	1500
192.168.40.254/32	0.0.0.0	uh	ethernet1/7.40	1500

Refresh u - up, h - host, g - gateway, e- ECMP, * - preferred path

RIB vs. FIB

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
```

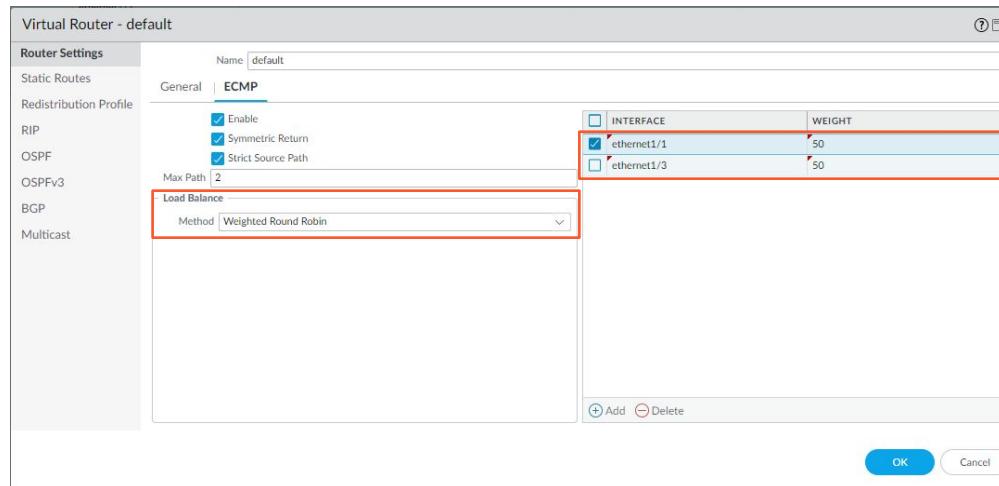
id	destination	nexthop	flags	interface	mtu
45	0.0.0.0/0	73.254.100.1	ug	ethernet1/1	1500
2	1.1.1.0/30	0.0.0.0	u	ethernet1/3	1500
1	1.1.1.1/32	0.0.0.0	uh	ethernet1/3	1500
44	73.254.100.0/24	0.0.0.0	u	ethernet1/1	1500
43	73.254.100.132/32	0.0.0.0	uh	ethernet1/1	1500

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.

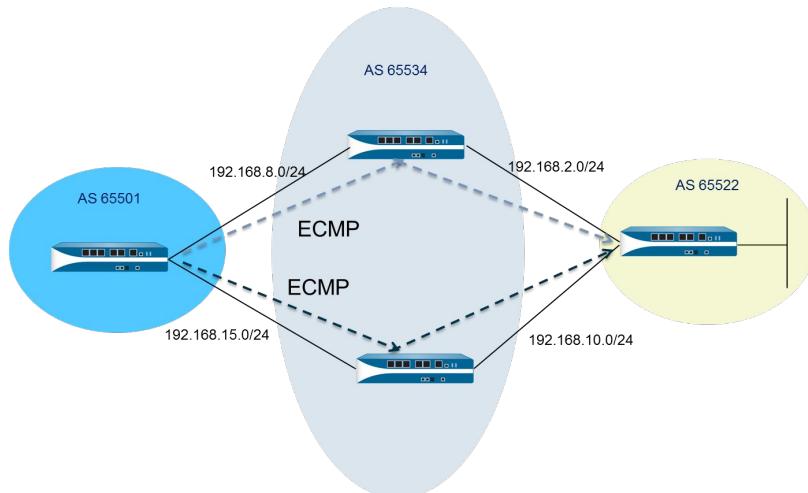
Load balance flows (sessions) to the same destination over multiple equal-cost links to make use of available bandwidth on all links toward the destination, rather than leaving links unused.

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.

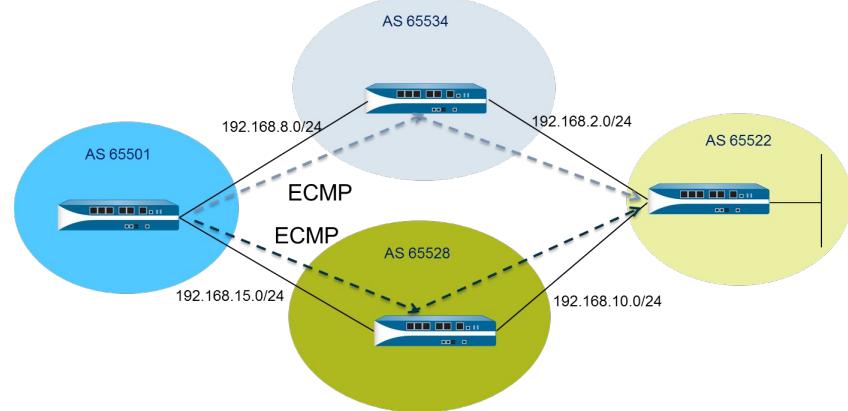


5.4.0 – Equal Cost Multiple Path (ECMP) – Example Deployments

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 systems**.



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

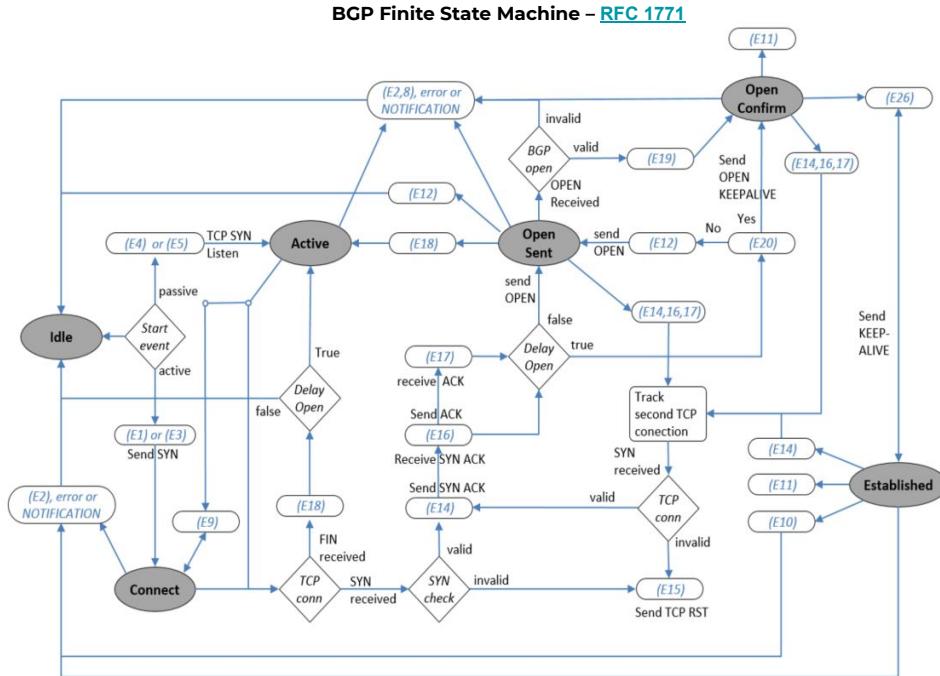
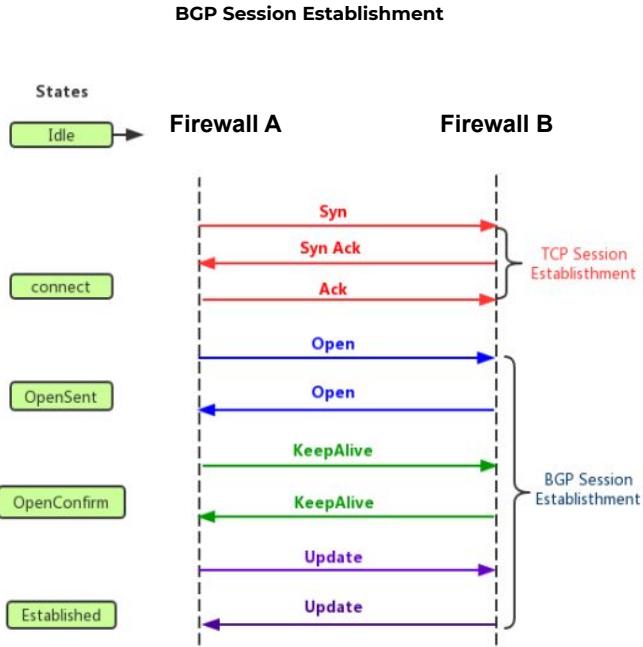
-----
virtual-router name: default
interfaces:
    ethernet1/1 ethernet1/3 ethernet1/7 ethernet1/7.40
    loopback.1 tunnel1.3 vlan

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



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:

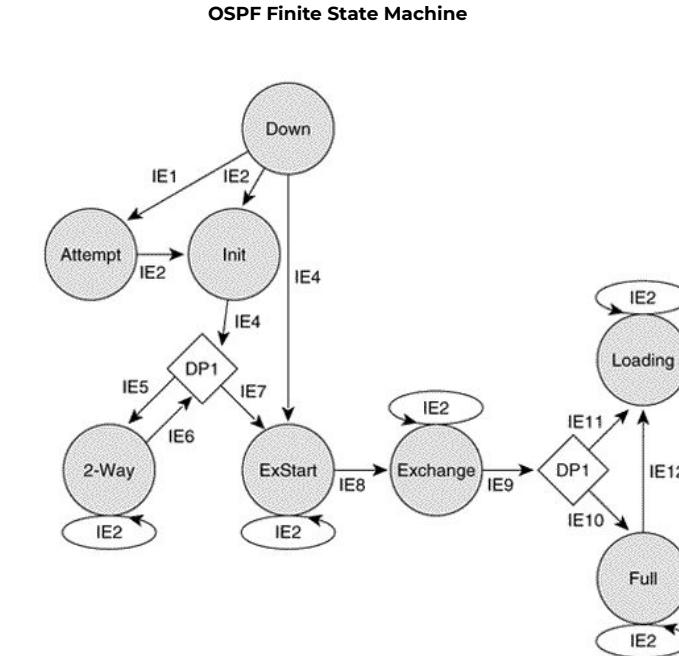
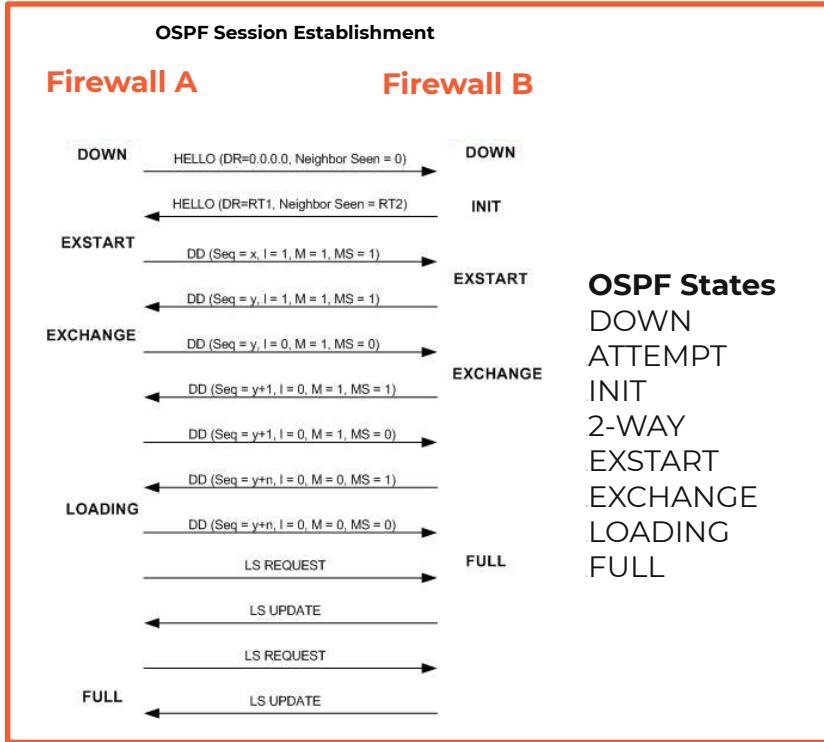
```
test routing bgp virtual-router default restart self      (for restarting BGP connections)  
test routing bgp virtual-router default refresh self     (for refreshing BGP connections)
```

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



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

5.4.1 - CLI Cheat Sheet Networking – Reference, Part 1

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

5.4.1 - CLI Cheat Sheet Networking – Reference, Part 2

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

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:

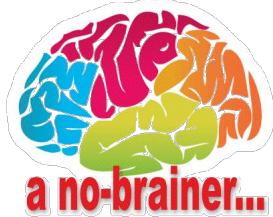
```
debug routing pcap ospf delete
```

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        0       ethernet1/1  Default Route
0.0.0.0/0            73.254.100.1    10     EAS        0       ethernet1/2  Default Route

total routes shown: 2
```

5.4.4 - Troubleshooting Route Monitoring

The screenshot shows the 'Virtual Router - default' configuration screen. On the left, a sidebar lists various routing protocols: Router Settings, Static Routes (selected), Redistribution Profile, RIP, OSPF, OSPFv3, BGP, and Multicast. The main area has tabs for IPv4 and IPv6, with IPv4 selected. A search bar at the top right shows '1 item' and a delete icon. Below it is a table for static routes:

NAME	DESTINATION	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	ROUTE TABLE
			TYPE	VALUE			
To 192.168.2.1 Tunnel3	PA-220-2-Trust	tunnel.3		default	10	unicast	

Below this is a modal window titled 'Virtual Router - Static Route - IPv4' containing detailed route information:

Name: To 192.168.2.1 Tunnel3
Destination: PA-220-2-Trust
Interface: tunnel.3
Next Hop: None
Admin Distance: 10 - 240
Metric: 10
Route Table: Unicast

The 'Path Monitoring' section is checked and contains a table:

NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
				Any	All
Path Monitoring for VPN	<input checked="" type="checkbox"/>	DHCP	192.168.2.2	3	5

At the bottom of the modal are 'OK' and 'Cancel' buttons.

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

The dashboard displays several widgets:

- General Information:** Shows device details like Device Name (ux1-gcp), MGT IP Address (100.64.0.50 (IDHCP)), and MGT MAC Address (42:01:64:00:00:32).
- Interfaces:** A grid showing interface status (e.g., 1, 2, 3, 5, 6, 7).
- Logged In Admins:** A list of admins and their session details.
- ACC Risk Factor (Last 60 minutes):** A chart showing a risk factor of 3.7.
- Threat Logs:** A table of threat logs with columns: Name, Severity, and Time.
- Top Applications:** A treemap visualization of application usage.
- System Logs:** A table of system log entries with columns: Description, Client, Session Start, and Idle For.
- Config Logs:** A table of configuration log entries with columns: Command, Path, Admin, and Time.

Information for:

General System

Interfaces

HA Status

Top Applications

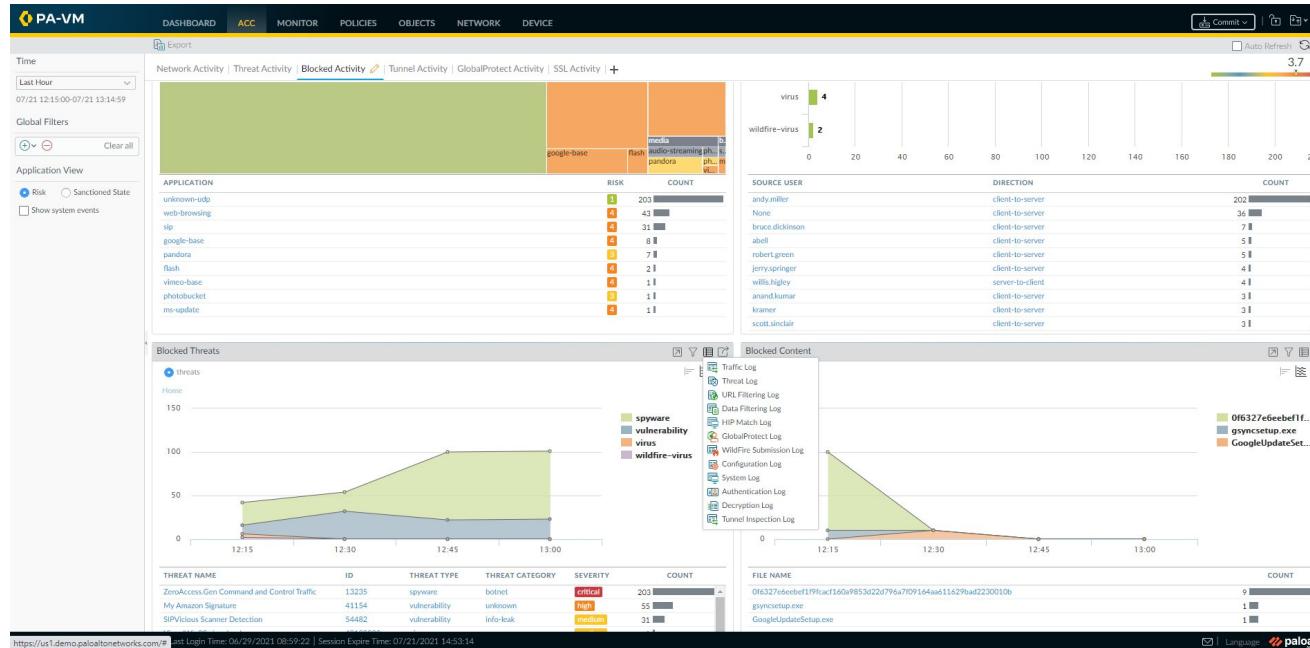
Systems Logs

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

Identical Tabs in NGFW

Switch Device Context

Logging in Panorama

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA

Device Group: us1demo

Panorama

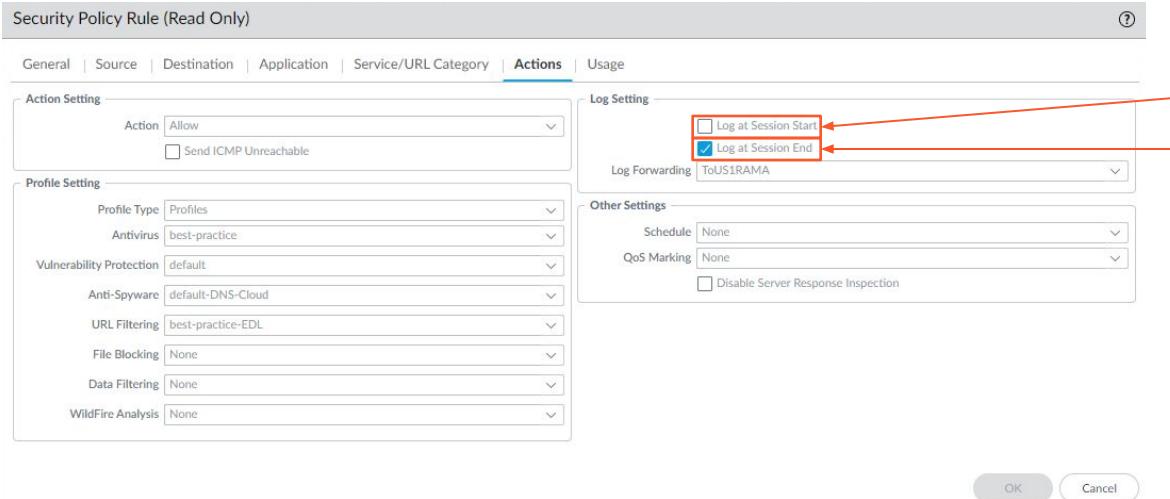
Traffic Logs Threat URL Filtering Wildfire Submissions Data Filtering Data Plane HIP Match GlobalProtect IP-Tag User-ID Decryption Tunnel Inspection Configuration Authentication Unified

Automated Correlation Engine Correlation Objects Correlated Events App Scope Summary Change Monitor Threat Monitor Threat Map Network Monitor Traffic Map PDF Reports Manage PDF Summary User Activity Report SaaS Application Usage Report Groups Email Scheduler Manage Custom Reports Reports

GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	APP FLAP COUNT	DEVICE SN	DEVICE NAME
08/09/09:57:10	end	L3-TAP	L3-TAP	10.154.13.168	pancademo james.collins	216.178.33.48	80	web-browsing	allow	General Web Infrastructure	aged-out	15.2k	0	007058000139888	us1-gcp
08/09/09:57:10	end	L3-TAP	L3-TAP	10.154.13.168	pancademo james.collins	216.178.33.43	80	web-browsing	allow	General Web Infrastructure	aged-out	13.2k	0	007058000139888	us1-gcp
08/09/09:57:10	end	L3-TAP	L3-TAP	10.154.10.176	pancademo josc.garbett	74.125.127.102	80	google-safebrowsing	allow	General Web Infrastructure	aged-out	2.4k	0	007058000139888	us1-gcp
08/09/09:57:10	end	L3-TAP	L3-TAP	10.154.13.168	pancademo james.collins	198.189.255.76	80	flash	allow	General Web Infrastructure	aged-out	27.2k	0	007058000139888	us1-gcp
08/09/09:57:10	end	L3-TAP	L3-TAP	10.154.13.168	pancademo james.collins	207.171.14.119	80	web-browsing	allow	General Web Infrastructure	aged-out	1.8k	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.13.168	pancademo james.collins	216.178.33.42	80	web-browsing	allow	General Web Infrastructure	aged-out	2.3k	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.14.24	pancademo gloria.dionne	198.189.255.89	80	flash	allow	General Web Infrastructure	aged-out	136.9k	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.13.168	pancademo james.collins	74.125.19.157	80	google-base	allow	General Web Infrastructure	aged-out	3.2k	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.13.168	pancademo james.collins	216.178.33.52	80	web-browsing	allow	General Web Infrastructure	aged-out	6.3k	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.10.134	pancademo amanda.peralta	64.95.73.13	80	web-browsing	allow	General Web Infrastructure	aged-out	10.1k	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.14.63	pancademo ignacio.white	74.125.127.113	80	google-base	allow	General Web Infrastructure	aged-out	855	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.14.39	pancademo sharon.harris	69.174.88.90	80	web-browsing	allow	General Web Infrastructure	aged-out	108.5k	0	007058000139888	us1-gcp
08/09/09:57:09	end	L3-TAP	L3-TAP	10.154.14.39	pancademo sharon.harris	69.174.88.90	80	web-browsing	allow	General Web Infrastructure	aged-out	37.9k	0	007058000139888	us1-gcp
08/09/09:57:08	end	L3-TAP	L3-TAP	10.154.6.23	pancademo barbra.jenkins	64.94.125.138	80	web-browsing	allow	General Web Infrastructure	aged-out	15.2k	0	007058000139888	us1-gcp
08/09/09:57:08	end	L3-TAP	L3-TAP	10.154.6.128	pancademo marta.murphy	69.80.200.254	80	web-browsing	allow	General Web Infrastructure	aged-out	926	0	007058000139888	us1-gcp
08/09/09:57:07	end	L3-TAP	L3-TAP	10.154.6.23	pancademo barbra.jenkins	74.125.127.95	80	google-base	allow	General Web Infrastructure	aged-out	15.6k	0	007058000139888	us1-gcp
08/09/09:57:07	end	L3-TAP	L3-TAP	10.154.14.63	pancademo hans.garber	74.125.127.127	80	google-base	allow	General Web Infrastructure	aged-out	2.8k	0	007058000139888	us1-gcp
08/09/09:57:07	end	L3-TAP	L3-TAP	10.154.14.63	pancademo hans.garber	74.125.19.165	80	google-base	allow	General Web Infrastructure	aged-out	4.4k	0	007058000139888	us1-gcp
08/09/09:57:07	end	L3-TAP	L3-TAP	10.154.6.23	pancademo barbra.jenkins	74.125.127.147	80	google-base	allow	General Web Infrastructure	aged-out	1.1k	0	007058000139888	us1-gcp
08/09/09:57:07	end	L3-TAP	L3-TAP	10.154.14.63	pancademo hans.garber	74.125.19.165	80	google-base	allow	General Web Infrastructure	aged-out	3.7k	0	007058000139888	us1-gcp
08/09/09:57:07	end	L3-TAP	L3-TAP	10.154.14.63	pancademo hans.garber	74.125.19.165	80	google-base	allow	General Web Infrastructure	aged-out	25.8k	0	007058000139888	us1-gcp
08/09/09:57:07	end	L3-TAP	L3-TAP	10.154.14.63	pancademo hans.garber	74.125.19.165	80	google-base	allow	General Web Infrastructure	aged-out	5.0k	0	007058000139888	us1-gcp
08/09/09:57:06	end	L3-TAP	L3-TAP	10.154.9.201	pancademo patricia.enrique	121.254.165.1...	80	flash	allow	General Web Infrastructure	aged-out	185.2k	0	007058000139888	us1-gcp
08/09/09:57:06	end	L3-TAP	L3-TAP	10.154.4.188	pancademo mable.weathe...	72.14.213.100	80	google-base	allow	General Web Infrastructure	aged-out	23.1k	0	007058000139888	us1-gcp
08/09/09:57:06	end	L3-TAP	L3-TAP	10.154.2.19	pancademo brian.crawford	66.235.143.118	80	web-browsing	allow	General Web Infrastructure	aged-out	3.3k	0	007058000139888	us1-gcp
08/09/09:57:06	end	L3-TAP	L3-TAP	10.154.7.218	pancademo agnes.freeman	74.125.127.190	80	google-base	allow	General Web Infrastructure	aged-out	72.5k	0	007058000139888	us1-gcp

Displaying logs 1 - 100 100 per page DESC

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)

The screenshot shows the Palo Alto Networks PA-VM interface with the 'MONITOR' tab selected. In the left sidebar, under the 'Logs' section, there is a search bar containing the filter: '(zone.src eq L3-Trust) and (zone.dst eq L3-Untrust) and (flags has proxy)'. The main area displays a table of log entries. One specific entry in the 3rd row is highlighted with a red border, showing details such as RECEIVE TIME (07/21 13:03:14), TYPE (end), FROM ZONE (L3-Trust), TO ZONE (L3-Untrust), SOURCE (192.168.60.250), URL CATEGORY (social-networking), DESTINATION (151.101.0.84), and APPLICATION (pinterest-base). The 'DECRYPTED' column shows 'yes' and the 'TO PORT' column shows '443'. The 'ACTION' column contains 'allow' and the 'RULE' column contains 'Outbound-Trust2'. The 'SESSION END REASON' column shows 'aged-out'. The 'BYTES RECEIVED' column shows '7.4k' and the 'BYTES SENT' column shows '1.1k'. The 'APP FLAG COUNT' column shows '0'. The table also includes columns for 'SESSION ID', 'TIME', 'TYPE', 'FROM ZONE', 'TO ZONE', 'SOURCE', 'URL CATEGORY', 'DESTINATION', 'APPLICATION', 'ACTION', 'RULE', 'SESSION END REASON', 'BYTES RECEIVED', 'BYTES SENT', 'VTPS RECEIVED', 'SDWAN SITE NAME', and 'APP FLAG COUNT'. At the bottom of the table, there are navigation links (1-10) and a 'Displaying logs 1 - 100' message.

SESSION ID	TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	URL CATEGORY	DESTINATION	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES RECEIVED	BYTES SENT	VTPS RECEIVED	SDWAN SITE NAME	APP FLAG COUNT		
1	07/21 13:03:14	end	L3-Trust	L3-Untrust	192.168.60.250	social-networking	151.101.0.84	pinterest-base	allow	Outbound-Trust2	aged-out	7.4k	1.1k	6.4k	Branch1	0		
2	07/21 13:03:14	end	L3-Trust	L3-Untrust	192.168.60.250	games	a23-74-153-152.deploy.static.akamaitechnologie...	yes	443	web-browsing	allow	Outbound-Trust2	threat	7.2k	1.2k	6.1k	Branch1	0
3	07/21 13:03:14	end	L3-Trust	L3-Untrust	192.168.60.250	online-storage-and-backup	187.29.190.35.bc.googleusercontent.com	yes	443	google-app-engine	allow	Outbound-Trust2	tcp-fin	94.0k	3.4k	90.7k	Branch1	0
4	07/21 13:03:14	end	L3-Trust	L3-Untrust	192.168.60.250	computer-and-internet-info	w2src.vip.gq1.yahoo.com	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	12.1k	1.3k	10.7k	Branch1	0
5	07/21 13:03:14	end	L3-Trust	L3-Untrust	192.168.60.250	news	192.0.6.2	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	7.2k	1.1k	6.1k	Branch1	0
6	07/21 13:03:13	end	L3-Trust	L3-Untrust	192.168.60.250	shopping	7.26.192.104.bc.googleusercontent.com	yes	443	web-browsing	allow	Outbound-Trust2	aged-out	7.1k	1.3k	5.8k	Branch1	0
7	07/21 13:03:13	end	L3-Trust	L3-Untrust	192.168.60.250	training-and-tools	104.17.73.91	yes	443	web-browsing	allow	Outbound-Trust2	aged-out	6.3k	1.2k	5.1k	Branch1	0
8	07/21 13:03:13	end	L3-Trust	L3-Untrust	192.168.60.250	shopping	a104-100-58-222.deploy.static.akamaitechnologie...	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	7.1k	1.3k	5.8k	Branch1	0
9	07/21 13:03:13	end	L3-Trust	L3-Untrust	192.168.60.250	entertainment-and-arts	104.16.6.49	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	5.2k	1.1k	4.1k	Branch1	0
10	07/21 13:03:13	end	L3-Trust	L3-Untrust	192.168.60.250	computer-and-internet-info	bily.com	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	67.0k	3.3k	63.7k	Branch1	0
11	07/21 13:03:12	end	L3-Trust	L3-Untrust	192.168.60.250	reference-and-research	104.26.5.237	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	5.1k	1.1k	3.9k	Branch1	0
12	07/21 13:03:12	end	L3-Trust	L3-Untrust	192.168.60.250	health-and-medicine	207.231.204.56	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	9.6k	1.3k	8.3k	Branch1	0
13	07/21 13:03:12	end	L3-Trust	L3-Untrust	192.168.60.250	society	104.26.4.246	yes	443	web-browsing	allow	Outbound-Trust2	aged-out	73.4k	2.5k	70.8k	Branch1	0
14	07/21 13:03:11	end	L3-Trust	L3-Untrust	192.168.60.250	business-and-economy	178.250.0.187	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	4.8k	1.2k	3.5k	Branch1	0
15	07/21 13:03:10	end	L3-Trust	L3-Untrust	192.168.60.250	search-engines	#929-23.members.linode.com	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	6.9k	1.1k	5.8k	Branch1	0
16	07/21 13:03:10	end	L3-Trust	L3-Untrust	192.168.60.250	business-and-economy	101.120.192.35.bc.googleusercontent.com	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	73.1k	1.3k	71.8k	Branch1	0
17	07/21 13:03:10	end	L3-Trust	L3-Untrust	192.168.60.250	business-and-economy	151.101.2.137	yes	443	web-browsing	allow	Outbound-Trust2	aged-out	6.8k	1.1k	5.7k	Branch1	0
18	07/21 13:03:10	end	L3-Trust	L3-Untrust	192.168.60.250	computer-and-internet-info	ph-in-f105.c100.net	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	7.2k	1.2k	6.0k	Branch1	0
19	07/21 13:03:09	end	L3-Trust	L3-Untrust	192.168.60.250	business-and-economy	172.67.74.92	yes	443	web-browsing	allow	Outbound-Trust2	aged-out	5.2k	1.3k	3.9k	Branch1	0
20	07/21 13:03:09	end	L3-Trust	L3-Untrust	192.168.60.250	computer-and-internet-info	198.185.159.176	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	6.9k	1.2k	5.7k	Branch1	0
21	07/21 13:03:09	end	L3-Trust	L3-Untrust	192.168.60.250	shareware-and-freeware	104.18.20.183	yes	443	web-browsing	allow	Outbound-Trust2	threat	4.0k	1.1k	3.0k	Branch1	0
22	07/21 13:03:09	end	L3-Trust	L3-Untrust	192.168.60.250	news	172.67.33.204	yes	443	web-browsing	allow	Outbound-Trust2	aged-out	317.8k	4.7k	313.1k	Branch1	0
23	07/21 13:03:08	end	L3-Trust	L3-Untrust	192.168.60.250	computer-and-internet-info	13.91.95.74	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	7.5k	1.2k	6.4k	Branch1	0
24	07/21 13:03:08	end	L3-Trust	L3-Untrust	192.168.60.250	online-storage-and-backup	104.16.202.237	yes	443	mediafire	allow	Outbound-Trust2	aged-out	7.7k	1.2k	6.5k	Branch1	0
25	07/21 13:03:07	end	L3-Trust	L3-Untrust	192.168.60.250	government	151.101.64.144	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	5.8k	1.1k	4.7k	Branch1	0
26	07/21 13:03:03	end	L3-Trust	L3-Untrust	192.168.60.250	search-engines	vandrx.ru	yes	443	web-browsing	allow	Outbound-Trust2	tcp-fin	31.9k	1.1k	30.8k	Branch1	0

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' )
```

Detailed Log View

The screenshot shows the Palo Alto Networks Unified Log View interface. It displays a detailed log entry with various sections: General, Source, Destination, Flags, and DeviceID. Red arrows point from specific fields to labels: 'Action' points to the 'Action' field in the General section; 'Rule' points to the 'Rule' field in the General section; 'Geographical' points to the 'Country' field in the Source section; 'Threat Information' points to the 'Details' section; 'Decrypted, No (FTP)' points to the 'Decrypted' checkbox in the Flags section; and 'Packet Capture, Yes' points to the 'Packet Capture' checkbox in the Flags section. A red arrow also points from the PCAP icon in the bottom left to the PCAP column in the log table.

General

- Session ID: 221718
- Action: reset-both
- Host ID: Watch Risky Apps
- Application: ftp
- Rule: Watch Risky Apps
- Rule UUID: a6bc1731-cf53-4da0-8e79-c75d96748bab
- Device SN: 007058000139888
- IP Protocol: tcp
- Log Action: T0US1RAMA
- Generated Time: 2021/07/22 06:43:02
- Receive Time: 2021/07/22 06:43:02
- Tunnel Type: N/A

Source

- Source User: 61136.188.83
- Source DAG: China
- Port: 45410
- Zone: L3-TAP
- Interface: ethernet1/4
- X-Forwarded-For IP: 0.0.0.0

Destination

- Destination User: pancademo/dawn.davis
- Destination: 10.154.2.26
- Destination DAG: 10.0.0.0-10.255.255.255
- Port: 21
- Zone: L3-TAP
- Interface: ethernet1/4

Flags

- Captive Portal:
- Proxy Transaction:
- Decrypted: (highlighted)
- Packet Capture: (highlighted)
- Client to Server:
- Server to Client:
- Tunnel Inspected:

DeviceID

- Source Device Category
- Source Device Profile
- Source Device Model
- Source Device Vendor
- Source Device OS Family
- Source Device OS Version

PCAP

PCAP	RECEIVE TIME ^	TYPE	APPLICATION	ACTION	RULE	RULE UUID	FILE URL	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT	URL
	2021/07/22 06:44:39	end	ftp	allow	Watch Risky Apps	a6bc1731-cf53-4da0-8e79-c75d96748bab		1829		any			
	2021/07/22 06:43:02	vulnerability	ftp	reset-both	Watch Risky Apps	a6bc1731-cf53-4da0-8e79-c75d96748bab			high	any			

5.5.1 - Troubleshooting Security Policy and Connectivity Issues

Test Configuration

Select Test: Security Policy Match

From: L3-TAP
To: L3-TAP
Source: 10.154.2.33
Source Port: [1-65535]
Destination: 69.81.76.194
Destination Port: 80
Source User: None
Protocol: TCP
 show all potential match rules until first allow rule

Application: None
Category: None
 check hip mask

Source OS: None
Source Model: None
Source Vendor: None
Destination OS: None
Destination Model: None
Destination Vendor: None
Source Category: None
Source Profile: None
Source Osfamily: None
Destination Category: None
Destination Profile: None
Destination Osfamily: None

Test Result

IT Sanctioned SaaS Apps

Result Detail

NAME	VALUE
Name	IT Sanctioned SaaS Apps
Index	35
From	any
Source	any
Source Region	none
To	any
Destination	any
Destination Region	none
User	known-user
source-device	any
destination-device	any
Category	any
Application Service	any

0:salesforce-base/tcp/any/80
1:salesforce-base/tcp/any/443
2:salesforce-base/tcp/any/4309
3:boxnet-base/tcp/any/80
4:boxnet-base/tcp/any/443
5:concur-base/tcp/any/80
6:concur-base/https/any/443

Test Configuration

Select Test: Ping

Bypass routing table, use specified interface
 Count: 5
 Don't fragment echo request packets (IPv4)
 Force to IPv6 destination
 Interval: [1 - 2]
 Source:
 Don't attempt to print addresses symbolically
 Pattern:
 Size: [0 - 65468]
 Tos: [1 - 255]
 Ttl: [1 - 255]
 Display detailed output
Host: 8.8.8.8

Test Result

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

64 bytes from 8.8.8.8 icmp_seq=1 ttl=115 time=0.797 ms
64 bytes from 8.8.8.8 icmp_seq=2 ttl=115 time=0.798 ms
64 bytes from 8.8.8.8 icmp_seq=3 ttl=115 time=0.767 ms
64 bytes from 8.8.8.8 icmp_seq=4 ttl=115 time=0.798 ms
64 bytes from 8.8.8.8 icmp_seq=5 ttl=115 time=0.803 ms

... 8.8.8.8 ping statistics ...
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.698/0.749/0.803/0.043 ms

Security Policy Match
(addr.src in 192.168.60.250) and (addr.dst in 172.67.72.147) and (flags has proxy)

Diagnostic Tools:
Device > Troubleshooting

In-Context:
[Toolbar] > Test Policy Match

Hit Counters

Rule Usage filtering

Applications Seen

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-unsupported-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 displayed 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-unsupported-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

Logging and Reporting Settings

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

Number of Versions for Config Audit: 100
Max Rows in CSV Export: 65535
Max Rows in User Activity Report: 5000
Average Browse Time (sec): 60
Page Load Threshold (sec): 20
Syslog HOSTNAME Format: FQDN
Report Runtime: 02:00
Report Expiration Period (days): [1 - 2000]

Stop Traffic when LogDb Full
 Enable Threat Vault Access
 Enable Log on High DP Load
 Support UTF-8 For Log Output

Logging and Reporting Settings

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

Pre-Defined Reports

Application Reports	Traffic Reports	Threat Reports	URL Filtering Reports
<input checked="" type="checkbox"/> Applications <input checked="" type="checkbox"/> Application Categories <input checked="" type="checkbox"/> Technology Categories <input checked="" type="checkbox"/> HTTP Applications <input checked="" type="checkbox"/> Denied Applications <input checked="" type="checkbox"/> Risk Trend <input checked="" type="checkbox"/> Bandwidth Trend <input checked="" type="checkbox"/> SaaS Application Usage	<input checked="" type="checkbox"/> Security Rules <input checked="" type="checkbox"/> Sources <input checked="" type="checkbox"/> Source Countries <input checked="" type="checkbox"/> Destinations <input checked="" type="checkbox"/> Destination Countries <input checked="" type="checkbox"/> Connections <input checked="" type="checkbox"/> Source Zones <input checked="" type="checkbox"/> Destination Zones <input checked="" type="checkbox"/> Ingress Interfaces <input checked="" type="checkbox"/> Egress Interfaces <input checked="" type="checkbox"/> Denied Sources <input checked="" type="checkbox"/> Denied Destinations <input checked="" type="checkbox"/> Unknown TCP Sessions <input checked="" type="checkbox"/> Unknown HTTP Sessions	<input checked="" type="checkbox"/> Threats <input checked="" type="checkbox"/> Threat Trend <input checked="" type="checkbox"/> Attacker Sources <input checked="" type="checkbox"/> Attacker Destinations <input checked="" type="checkbox"/> Attackers By Source Countries <input checked="" type="checkbox"/> Attackers By Destination Countries <input checked="" type="checkbox"/> Victim Sources <input checked="" type="checkbox"/> Victim Destinations <input checked="" type="checkbox"/> Victims By Source Country <input checked="" type="checkbox"/> Victims By Destination Countries <input checked="" type="checkbox"/> Viruses <input checked="" type="checkbox"/> Spyware	<input checked="" type="checkbox"/> URL Categories <input checked="" type="checkbox"/> URL Users <input checked="" type="checkbox"/> URL User Behavior <input checked="" type="checkbox"/> Web Sites <input checked="" type="checkbox"/> Blocked Categories <input checked="" type="checkbox"/> Blocked Users <input checked="" type="checkbox"/> Blocked User Behavior <input checked="" type="checkbox"/> Blocked Sites <input checked="" type="checkbox"/> Credential Post Detected

Note: Group Reports and PDF Reports will have no data if a contained pre-defined report is disabled

Select All | Deselect All

OK | Cancel

Predefined Reports

5.5.2 - Reporting Types

SOURCE ADDRESS	SOURCE HOST NAME	SOURCE EDL	SOURCE USER	DESTINATION ADDRESS	DESTINATION HOST NAME	DESTINATION EDL	DESTINATION USER	SOURCE DYNAMIC ADDRESS	DESTINATION GROUP	Application Reports
1 10.154.10.1	10.154.10.10		pancademo/jerry.bowery	67.192.17.93 ^Q		67.192.17.93 ^Q				Traffic Reports
2 10.154.196.169 ^Q	10.154.196.169 ^Q		pancademo/jordan.bowery	96.17.144.46 ^Q	a96-17-144-46.deploy.static.akamaitechnologies.com ^Q					
3 10.154.2.22 ^Q	10.154.2.22 ^Q		pancademo/forest.flx	137.145.204.10 ^Q	137.145.204.10 ^Q					
4 10.154.196.169 ^Q	10.154.196.169 ^Q		pancademo/jordan.bowery	137.145.93.30 ^Q	8.69-17-144-200.deploy.static.akamaitechnologies.com ^Q					
5 10.154.10.88	10.154.10.88 ^Q		pancademo/angela.tapia	137.145.204.10 ^Q	137.145.204.10 ^Q					
6 10.154.196.169	10.154.196.169 ^Q		pancademo/jordan.bowery	96.17.144.200 ^Q	a96-17-144-200.deploy.static.akamaitechnologies.com ^Q					
7 10.154.14.13 ^Q	10.154.14.13 ^Q		pancademo/jane.goffney	72.164.152.203 ^Q						
8 10.42.7.101	10.42.7.101 ^Q		pancademo/amy.fowler	10.4.27.4 ^Q	10.4.27.4 ^Q					
9 10.154.1.106	10.154.1.106 ^Q		pancademo/country.karma	64.191.193.124 ^Q						
10 10.154.3.108	10.154.3.108 ^Q		pancademo/david.edwards	65.49.19.178 ^Q						
11 10.154.10.88	10.154.10.88 ^Q		pancademo/angela.tapia	130.150.102.20 ^Q	130.150.102.20 ^Q					
12 10.154.5.47 ^Q	10.154.5.47 ^Q		pancademo/jeff.pennen	137.145.204.10 ^Q	137.145.204.10 ^Q					
13 10.154.196.169 ^Q	10.154.196.169 ^Q		pancademo/jordan.bowery	10.4.27.4 ^Q	10.4.27.4 ^Q					
14 10.154.196.169 ^Q	10.154.196.169 ^Q		pancademo/brenda.boutin	208.111.148.6 ^Q	208.111.148.6 ^Q					
15 10.154.196.169 ^Q	10.154.196.169 ^Q		pancademo/jordan.bowery	216.239.34.10 ^Q	m2.google.com ^Q					
16 74.85.15.50	none:redshift.com ^Q			10.154.4.195 ^Q	10.154.4.195 ^Q					
17 49.110.2.189	ad6-69-110-2-189.osiptr13.pvtcbt.re ^Q		pancademo/martha.wirck	10.154.14.145 ^Q	10.154.14.145 ^Q					
18 10.154.10.58	Lie.Dekopok ^Q			128.149.22.72 ^Q	128.149.22.72 ^Q					
19 99.138.5.88	ad6-99-138-5-181.osiptr13.pvtcbt.re ^Q			10.154.186.34 ^Q	10.154.186.34 ^Q					
20 200.144.174.205	209.144.176-205.statecasenet.co.th ^Q			10.154.168.185 ^Q	10.154.168.185 ^Q					
21 76.233.232.2 ^Q				10.154.7.14 ^Q	10.154.7.14 ^Q					
22 10.154.172.134 ^Q			pancademo/steven.reid	198.189.255.201 ^Q	a198-189-255-201.deploy.akamaitechnologies.com ^Q					
23 10.154.196.169	10.154.196.169 ^Q		pancademo/jordan.bowery	96.17.144.41 ^Q	a96-17-144-41.deploy.static.akamaitechnologies.com ^Q					
24 10.154.0.203	10.154.0.203 ^Q		pancademo/anthony.parker	198.189.255.73 ^Q	loss3-smart-1.ericc.net ^Q					
25 10.154.229.157	10.154.229.157 ^Q		pancademo/rojinson	184.72.29.32 ^Q	ec2-184-72-29-32.us-west-1.compute.amazonaws.com ^Q					
26 67.170.203.50	e-67-170-203-50.hfd.ca.concast.net ^Q			10.154.7.14 ^Q	10.154.7.14 ^Q					
27 10.154.9.167	10.154.9.167 ^Q		pancademo/justin.wilkic	137.145.204.10 ^Q	137.145.204.10 ^Q					

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

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Logs Traffic Threat URL Filtering Wildfire Submissions Data Filtering HIP Match GlobalProtect IP-Tag User-ID Decryption Tunnel Inspection Configuration System Alarms Authentication Unified Packet Capture App Scope Summary Change Monitor Threat Monitor Threat Map Network Monitor Traffic Map Session Browser Botnet PDF Reports Manage PDF Summary User Activity Report SaaS Application Usage

Filters START TIME FROM ZONE TO ZONE SOURCE DESTINATION FROM PORT TO PORT PROTOCOL APPLICATION RULE

07/21 13:37:35	L3-TAP	L3-TAP	10.154.10.176	75.183.15.179	24650	17619	17	bittorrent	Watch Risky Apps
07/21 13:38:09	L3-TAP	L3-TAP	10.154.3.13	82.3.196.25	41100	61785	17	bittorrent	Watch Risky Apps
07/21 13:44:49	L3-TAP	L3-TAP	10.154.10.88	198.189.255.76	58227	80	6	web-browsing	General Web Infrastructure
07/21 13:38:53	L3-TAP	L3-TAP	24.4.194.119	10.154.7.7	42746	443	6	ssl	Unknown User SSL and Web
07/21 13:30:30	L3-TAP	L3-TAP	10.154.14.30	89.229.140.76	24074	46975	17	bittorrent	Watch Risky Apps
07/21 13:31:31	L3-TAP	L3-TAP	10.154.1.84	83.55.100.172	43711	44814	17	bittorrent	Watch Risky Apps
07/21 13:37:43	L3-TAP	L3-TAP	10.154.4.74	70.50.196.114	14696	19000	17	bittorrent	Watch Risky Apps
07/21 13:32:15	L3-TAP	L3-TAP	98.207.246.161	10.154.7.14	35260	80	6	undecided	Required Infrastructure
07/21 13:38:55	L3-TAP	L3-TAP	10.154.15.105	206.125.47.50	1814	80	6	web-browsing	General Web Infrastructure
07/21 13:37:18	L3-TAP	L3-TAP	10.154.10.176	76.27.212.188	24650	27853	17	bittorrent	Watch Risky Apps
07/21 13:31:44	L3-TAP	L3-TAP	10.154.8.155	198.189.255.76	1355	80	6	web-browsing	General Web Infrastructure
07/21 13:32:37	L3-TAP	L3-TAP	10.154.13.113	174.36.40.212	52362	80	6	web-browsing	General Web Infrastructure

Detail

Session ID	26504
Timeout	1800
Time To Live	767
Virtual System	vsys1
Application	web-browsing
Protocol	6
Security Rule	General Web Infrastructure
URL Category	entertainment-and-arts, low-risk
QoS Rule	N/A
QoS Class	4
Created By Syn Cookie	False
To Host Session	False
Traverse Tunnel	False
Captive Portal	False
Session End Log	True
Session In Ager	True
Session From HA	False
End Reason	unknown

Flow 1

Direction	From Zone	Source	Destination	From Port	To Port	Protocol	Application	Rule
c2s	L3-TAP	10.154.13.113	174.36.40.212	52362	80	6	web-browsing	General Web Infrastructure

Flow 2

Direction	From Zone	Source	Destination	From Port	To Port	Protocol	Application	Rule
s2c	L3-TAP	174.36.40.212	10.154.13.113	80	52362	6	web-browsing	General Web Infrastructure

Filters Destination eq 174.36.40.212

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM	CLEAR
07/21 13:32:37	L3-TAP	L3-TAP	10.154.13.113	174.36.40.212	52362	80	6	web-browsing	General Web Infrastructure	ethernet1/4	ethernet1/4	39521	vsys1	<input checked="" type="checkbox"/>
07/21 13:32:37	L3-TAP	L3-TAP	10.154.13.113	174.36.40.212	52363	80	6	web-browsing	General Web Infrastructure	ethernet1/4	ethernet1/4	31594	vsys1	<input checked="" type="checkbox"/>
07/21 13:32:37	L3-TAP	L3-TAP	10.154.13.113	174.36.40.212	52365	80	6	web-browsing	General Web Infrastructure	ethernet1/4	ethernet1/4	29105	vsys1	<input checked="" type="checkbox"/>
07/21 13:32:37	L3-TAP	L3-TAP	10.154.13.113	174.36.40.212	52364	80	6	web-browsing	General Web Infrastructure	ethernet1/4	ethernet1/4	37601	vsys1	<input checked="" type="checkbox"/>
07/21 13:32:37	L3-TAP	L3-TAP	10.154.13.113	174.36.40.212	52361	80	6	web-browsing	General Web Infrastructure	ethernet1/4	ethernet1/4	78440	vsys1	<input checked="" type="checkbox"/>
07/21 13:32:37	L3-TAP	L3-TAP	10.154.13.113	174.36.40.212	52359	80	6	web-browsing	General Web Infrastructure	ethernet1/4	ethernet1/4	66376	vsys1	<input checked="" type="checkbox"/>

Filter displays all communication to the DST at 174.36.40.212.

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

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

The screenshot shows the Palo Alto Networks PA-220 device configuration interface. The left sidebar navigation includes sections like Logs, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection, Configuration, System, Alarms, Authentication, and Unired. Under the **Packet Capture** section, there are sub-options for App Scope, Session Browser, PDF Reports, Manage PDF Summary, User Activity Report, SaaS Application Usage, Report Groups, Email Scheduler, and Manage Custom Reports.

The main configuration area displays the following sections:

- Configure Filtering:** Shows 1/4 Filters Set. Buttons for Manage Filters, Filtering ON, Pre-Parse Match OFF.
- Configure Capturing:** Shows a table for Packet Capture OFF:

STAGE	FILE	BYTE COUNT	PACKET COUNT
receive	RX		
firewall	FW		
transmit	TX		
drop	DROP		

Buttons for Add and Delete.
- Settings:** Includes a link to Clear All Settings, which is highlighted with a red box and a red arrow pointing to the text **!!! BE MINDFUL !!!**.
- Packet Capture Filter:** Shows a table with one row selected (ID 1):

ID	INGRESS INTERFACE	SOURCE	DESTINATION	SRC PORT	DEST PORT	PROTO	NON-IP	IPV6
1		192.168.1.11	0.0.0.0		443		exclude	<input type="checkbox"/>

Buttons for +Add, -Delete, and Set Selected Packet Capture Filter. Buttons for OK and Cancel.
- Captured Files:** A table listing captured files:

FILE NAME	DATE	SIZE(MB)
FW	2021/07/24 23:35:17	2.667505
RX	2021/07/24 23:35:17	11.941750
TX	2021/07/24 23:35:17	9.299304

Buttons for Page, Delete, and a note indicating 3 items.

Packet Capture Traffic for:

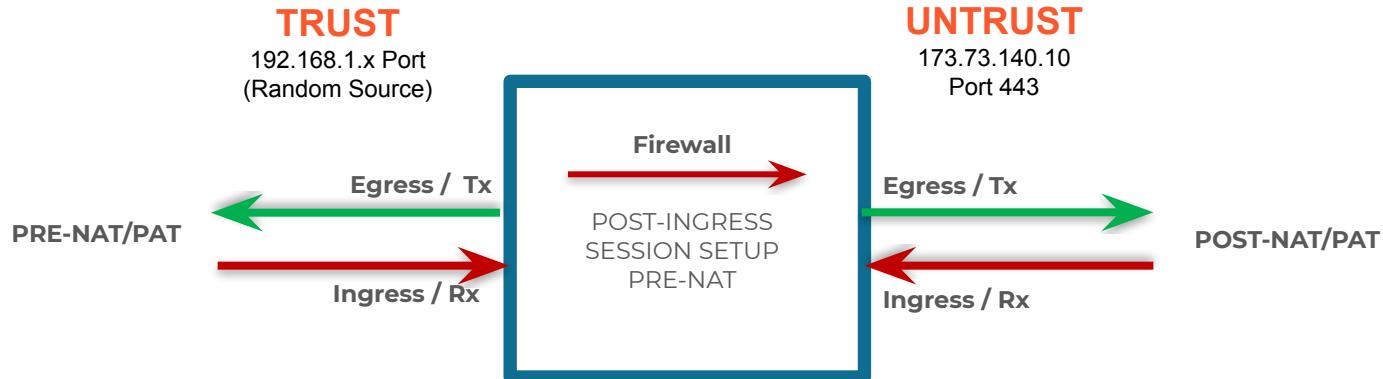
SRC: 192.168.1.11

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.

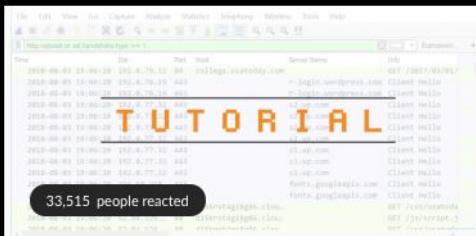


Which stage is right for me? - Reference

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`

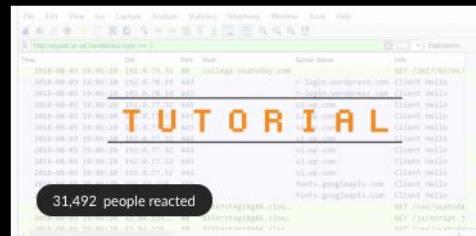


Wireshark Tutorial: Wireshark Workshop Videos Now Available

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

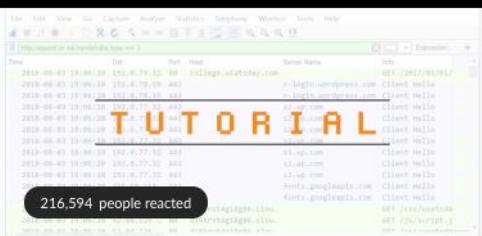
Updated: New Evidence Emerges to Suggest WatchDog Was Behind Crypto Campaign



Wireshark Tutorial: Decrypting



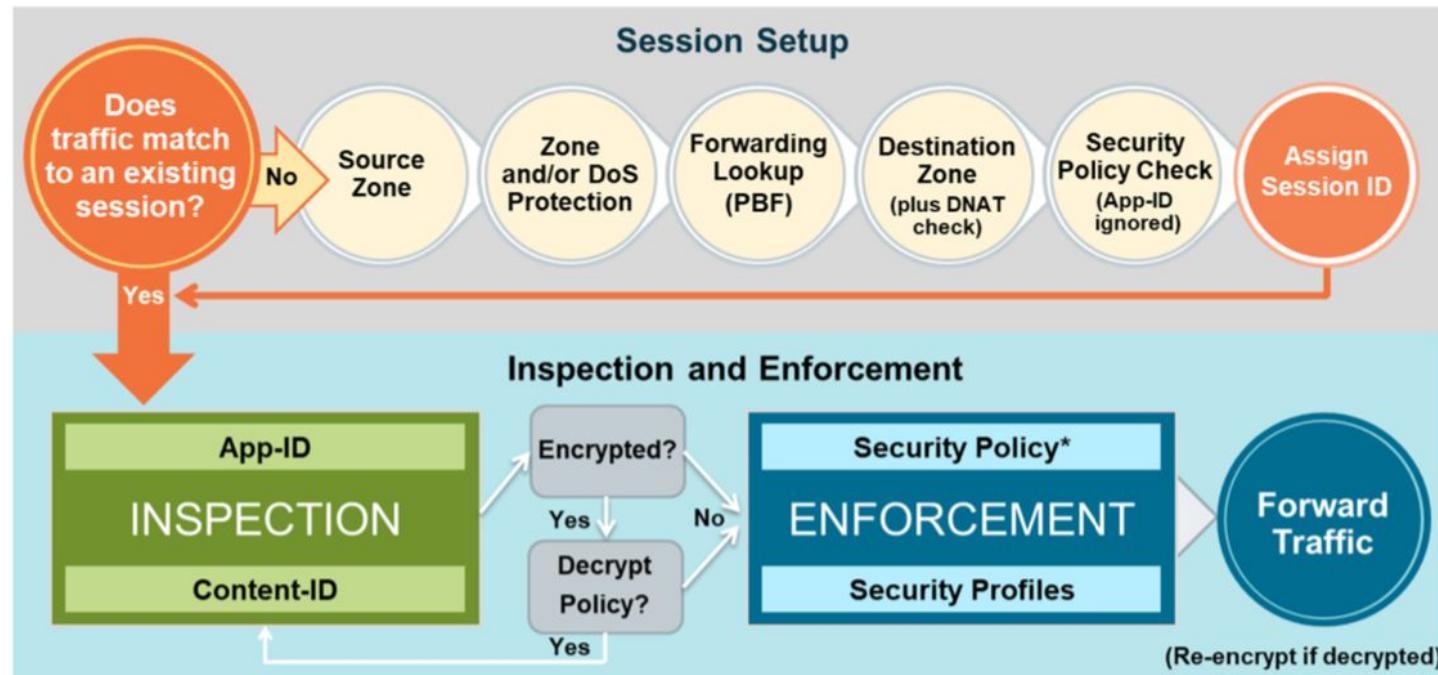
Wireshark Tutorial: Examining



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

Zone Protection Profile

Name: Ingress Zone Protection
Description: Protection against L3/L4 packet-based attacks

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

SYN

Action: Random Early Drop
Alarm Rate (connections/sec): 10000
Activate (connections/sec): 10000
Maximum (connections/sec): 40000

ICMP

Alarm Rate (connections/sec): 10000
Activate (connections/sec): 10000
Maximum (connections/sec): 40000

Other IP

Alarm Rate (connections/sec): 10000
Activate (connections/sec): 10000
Maximum (connections/sec): 40000

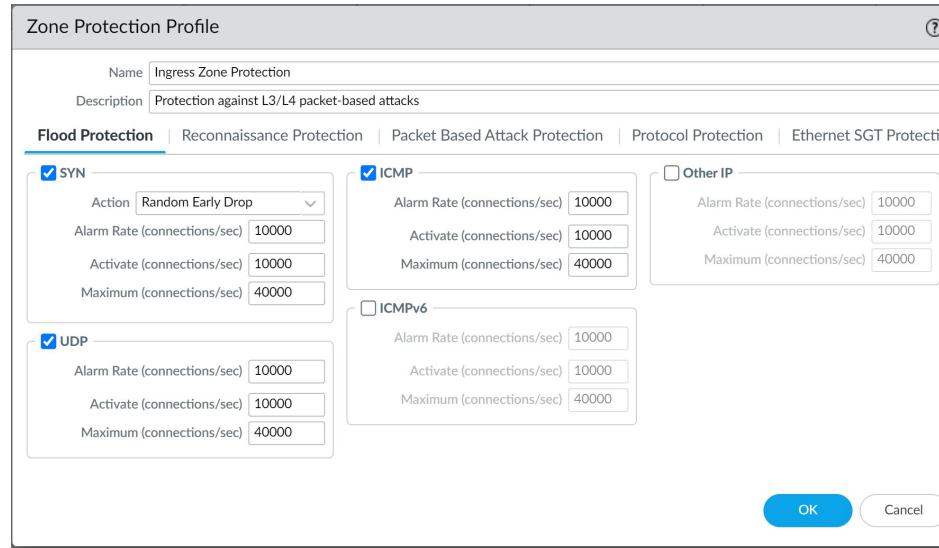
UDP

Alarm Rate (connections/sec): 10000
Activate (connections/sec): 10000
Maximum (connections/sec): 40000

ICMPv6

Alarm Rate (connections/sec): 10000
Activate (connections/sec): 10000
Maximum (connections/sec): 40000

OK Cancel



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.

The screenshot shows the Palo Alto VM (PA-VM) interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR (which is currently selected), POLICIES, OBJECTS, NETWORK, and DEVICE. On the left, a sidebar menu is open under the 'Logs' section, showing options like URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, and IP-Tag. The 'Threat' option is highlighted with a red box. The main pane displays a table of threat logs with the following columns: RECEIVE TIME, TYPE, THREAT ID/NAME, FROM ZONE, TO ZONE, SOURCE ADDRESS, DESTINATION ADDRESS, TO PORT, APPLICATION, ACTION, and SEVERITY. There are four log entries listed, all categorized as 'flood' and 'ICMP Flood', originating from 'Untrust-L3' and destined to 'Untrust-L3'. All entries have a severity of 'critical'.

	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	not-applicable	allow	critical
	07/15 05:57:47	flood	ICMP Flood	Untrust-L3	Untrust-L3	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	not-applicable	allow	critical
	07/15 05:57:15	flood	ICMP Flood	Untrust-L3	Untrust-L3	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

DoS Protection Profile

Name	DoS Protection Profile
Description	DoS protection for web servers
Type	<input type="radio"/> Aggregate <input checked="" type="radio"/> Classified
Flood Protection Resources Protection	
SYN Flood UDP Flood ICMP Flood ICMPv6 Flood Other IP Flood	
<input checked="" type="checkbox"/> SYN Flood	
Action	Random Early Drop
Alarm Rate (connections/s)	10000
Activate Rate (connections/s)	10000
Max Rate (connections/s)	40000
Block Duration (s)	300

OK **Cancel**

DoS Rule

General Source Destination Option/Protection	
<input type="checkbox"/> Any	Action Protect
<input checked="" type="checkbox"/> SERVICE ^	Schedule None
<input checked="" type="checkbox"/> service- http	Log Forwarding None
<input checked="" type="checkbox"/> service- https	Aggregate None
<input checked="" type="checkbox"/> Classified	
Profile DoS Protection Profile	
Address destination-ip-only	

OK **Cancel**

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 SZONE SRC      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):

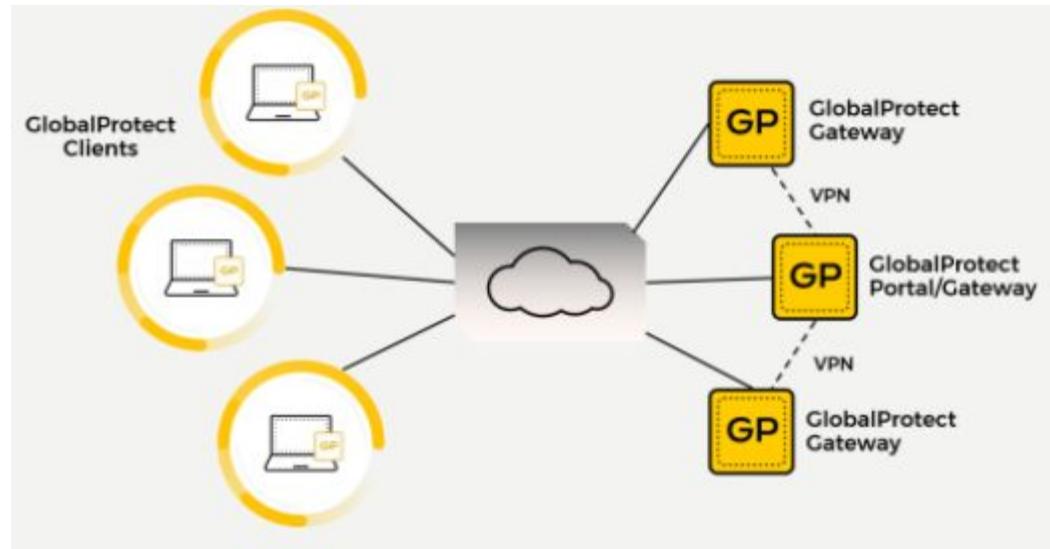
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClcvCAC>

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

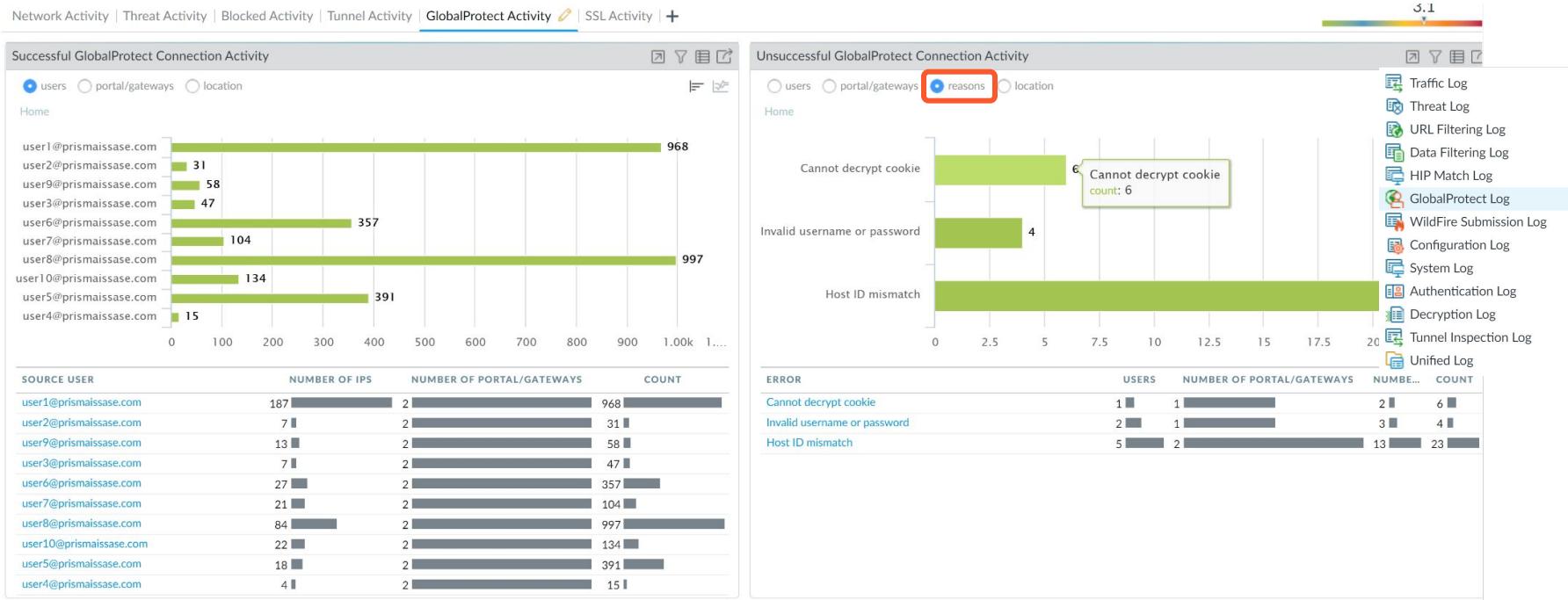
GlobalProtect Deployment Activity: deployment summary based on authentication method, GlobalProtect app version, and operating system version

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

The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR (which is highlighted in yellow), POLICIES, OBJECTS, NETWORK, and DEVICE. On the left, a sidebar menu lists categories like Logs, Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect (which is highlighted with a red box), IP-Tag, User-ID, Decryption, Tunnel Inspection, and Configuration. The main content area displays a table of logs. A search bar at the top of the table area contains the query: '(receive_time geq '2021/01/01 00:00:00') AND (receive_time leq '2021/07/26 15:44:59') AND ((error eq 'Cannot decrypt cookie'))'. The table has columns for RECEIVE TIME, PORTAL/GATE..., STATUS, STAGE, EVENT, SOURCE USER, HOST NAME, AUTH METHOD, and ERROR. The data in the table is as follows:

RECEIVE TIME	PORTAL/GATE...	STATUS	STAGE	EVENT	SOURCE USER	HOST NAME	AUTH METHOD	ERROR
02/11 01:14:21	DiaBGWInternal	failure	login	gateway-auth	chewie@demoin...	MSFT-W10	Cookie	Cannot decrypt cookie
02/05 20:21:27	DiaBGWInternal	failure	login	gateway-auth	chewie@demoin...	MSFT-W10	Cookie	Cannot decrypt cookie
02/05 20:16:23	DiaBGWInternal	failure	login	gateway-auth	chewie@demoin...	MSFT-W10	Cookie	Cannot decrypt cookie
02/04 22:07:46	DaiBGP	failure	login	portal-auth	chewie@demoin...	MSFT-W10	Cookie	Cannot decrypt cookie
02/03 22:07:44	DaiBGP	failure	login	portal-auth	chewie@demoin...	MSFT-W10	Cookie	Cannot decrypt cookie

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>

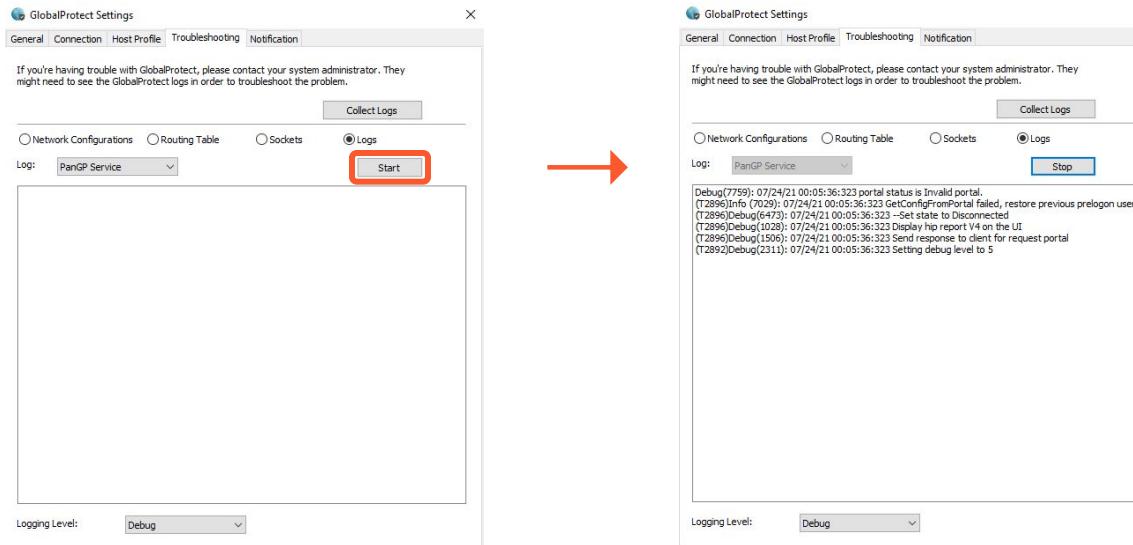
- > show global-protect-gateway flow

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

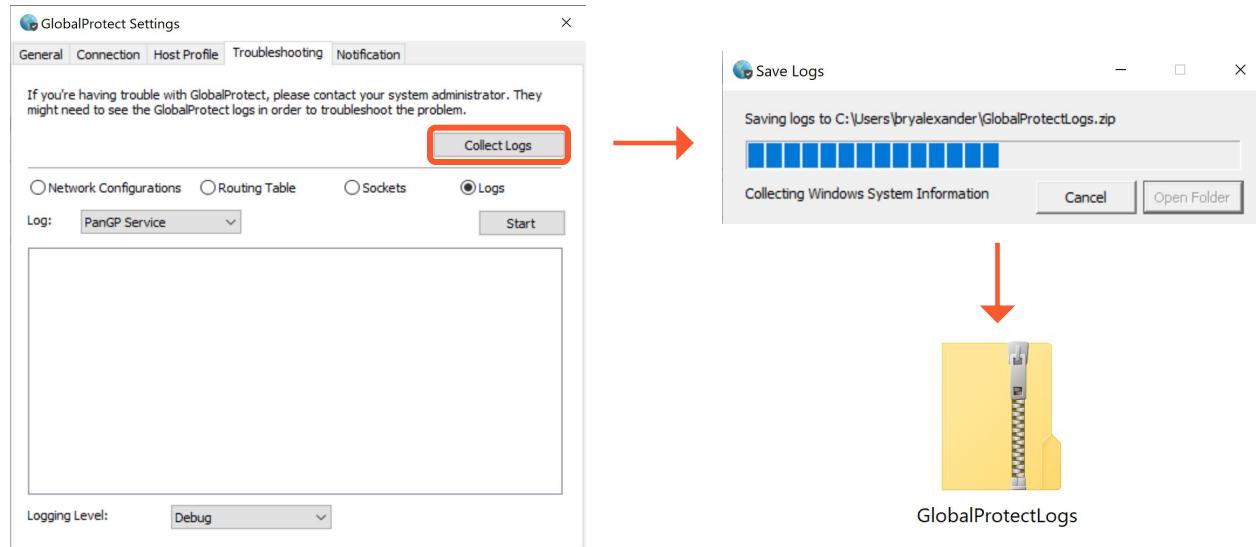


5.7.4 Troubleshoot GP client

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=3574388&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=kA10g000000CIYGCA0>

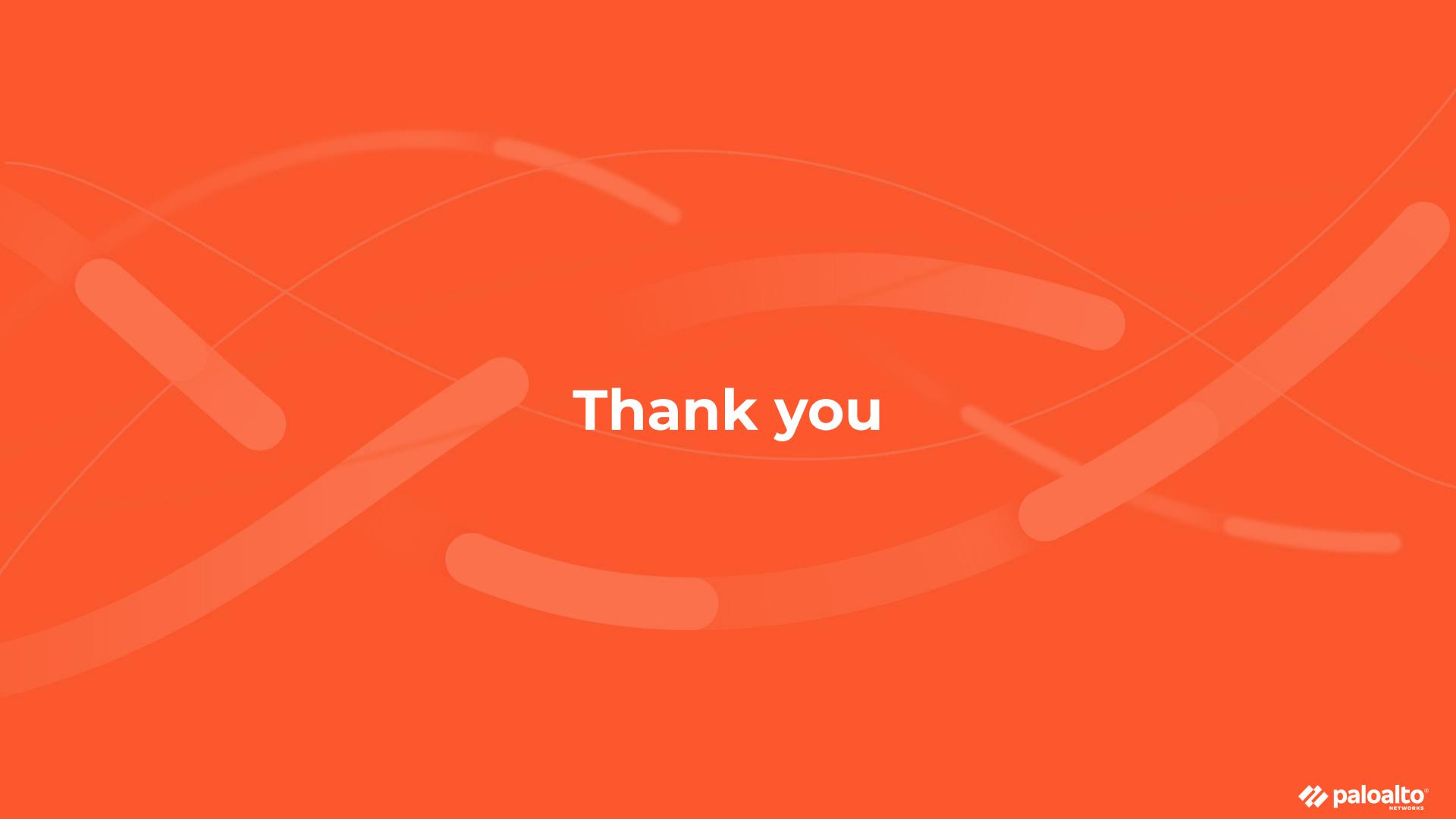
GlobalProtect Users and Internal Resources:

<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

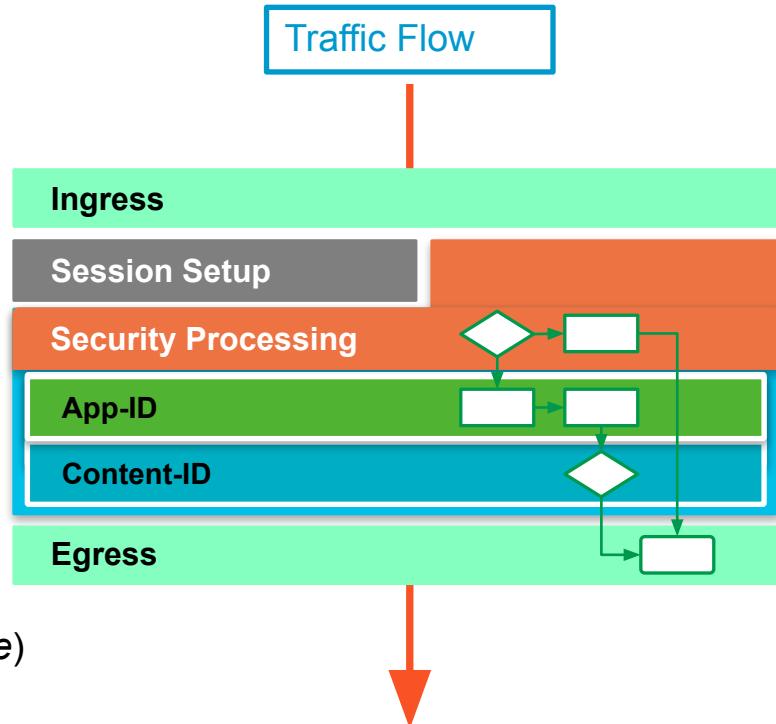
Egress

- QoS (Shaping, Rate Limiting)

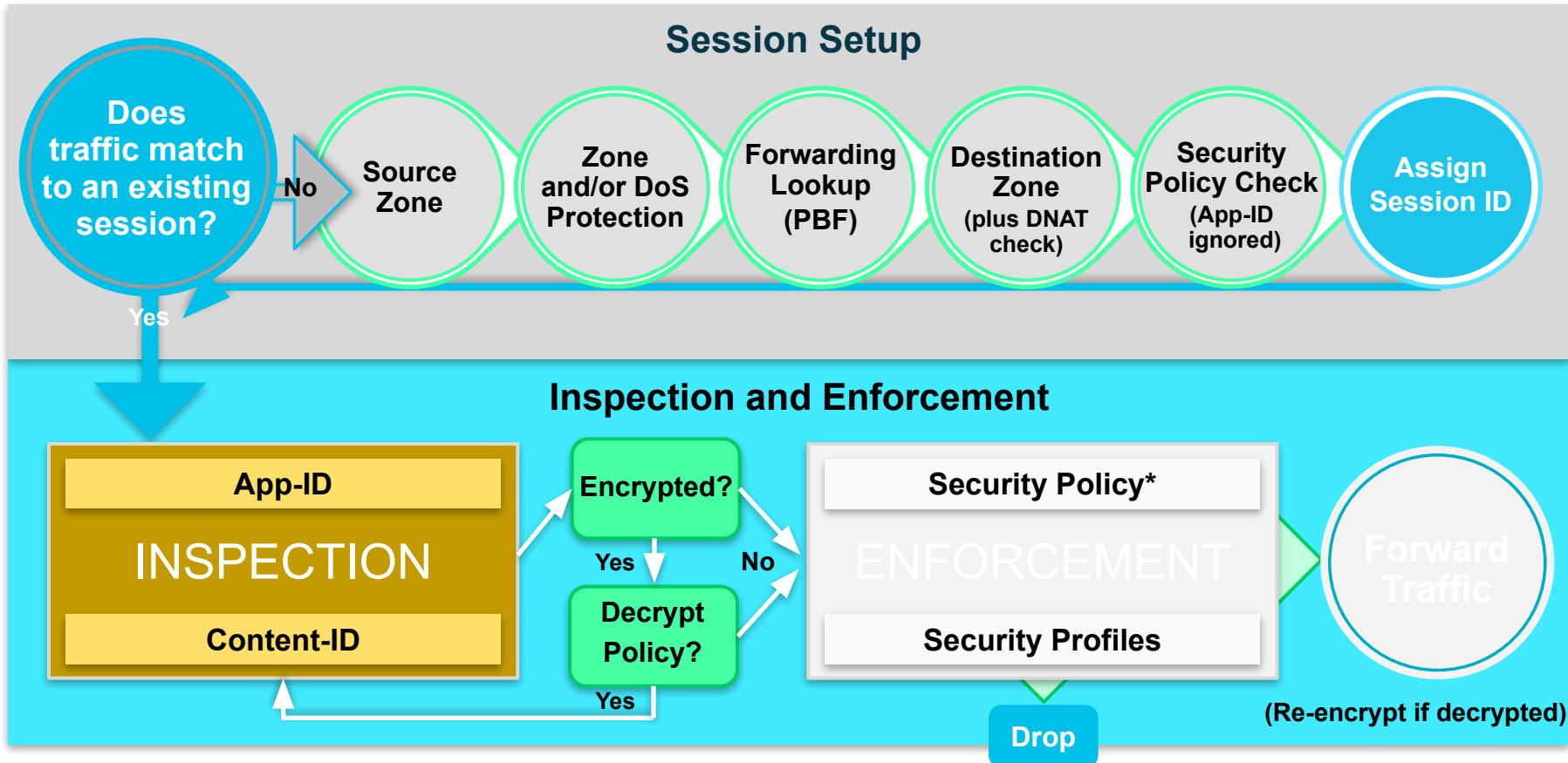
- Fragmentation

- VPN encapsulation

Session Offload = cut-through traffic (*requires hardware*)

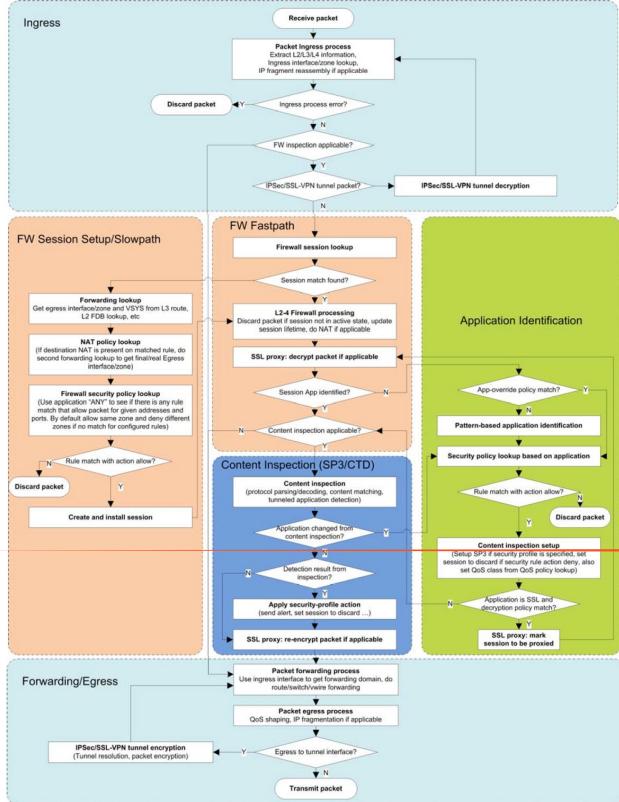


Session Setup, Inspection and Enforcement



* Policy check relies on pre-NAT IP addresses

Packet Flow Sequence – Reference



Flow Logic and Diagram

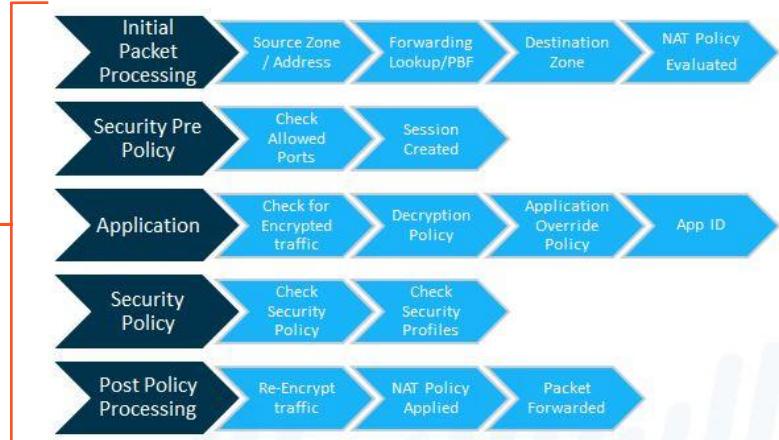
Initial Packet Processing - (Pre NAT)

Security Pre-Policy - (Session Creation)

Application - (App-ID)

Security Policy - (Security Profiles Applied)

Post Policy Processing - (Post NAT)



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, ← Numbered from 0, skips disabled rules
TCI INSPECT: Do TCI lookup policy - appid 0 ← AS profile, DNS Security (tunneling)
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
```

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 0x0c005303580, 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 QoS
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
```

Flow Basic (Egress Stage) - Reference

```
== 2019-07-28 05:46:49.699 -0600 ==
Packet received at forwarding stage, tag 55327, type ATOMIC
Packet info: len 75 port 17 interface 16 vsys 1
wqe index 44269 packet 0x0xc005303580, HA: 0, IC: 0
Packet decoded dump:
L2:      00:1b:17:fa:99:b2->00:50:e8:04:10:1a, type 0x0800
IP:      172.20.9.225->8.8.4.4, protocol 17
         version 4, ihl 5, tos 0x00, len 61,
         id 3353, frag off 0x4000, ttl 63, checksum 38508(0x6c96)
UDP:      sport 35326, dport 53, len 41, checksum 18617
Transmit packet size 61 on port 16
```

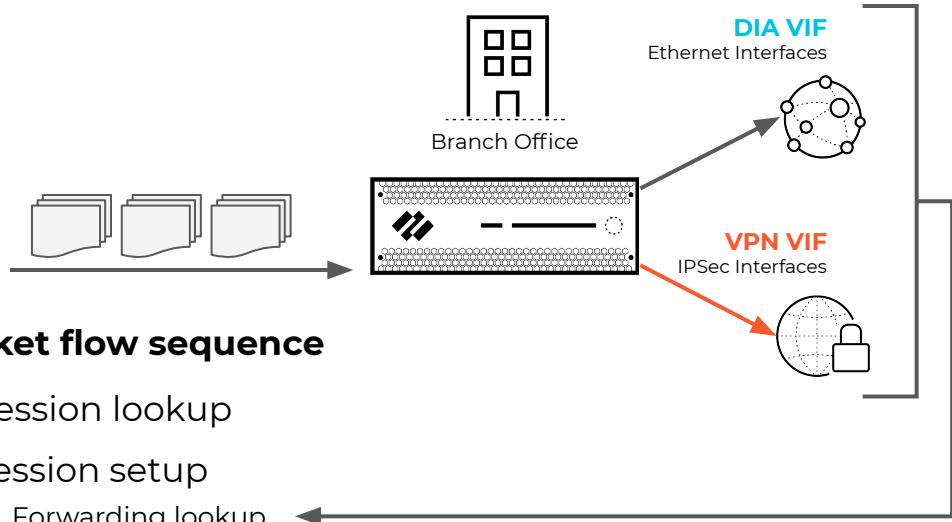
Session ID

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

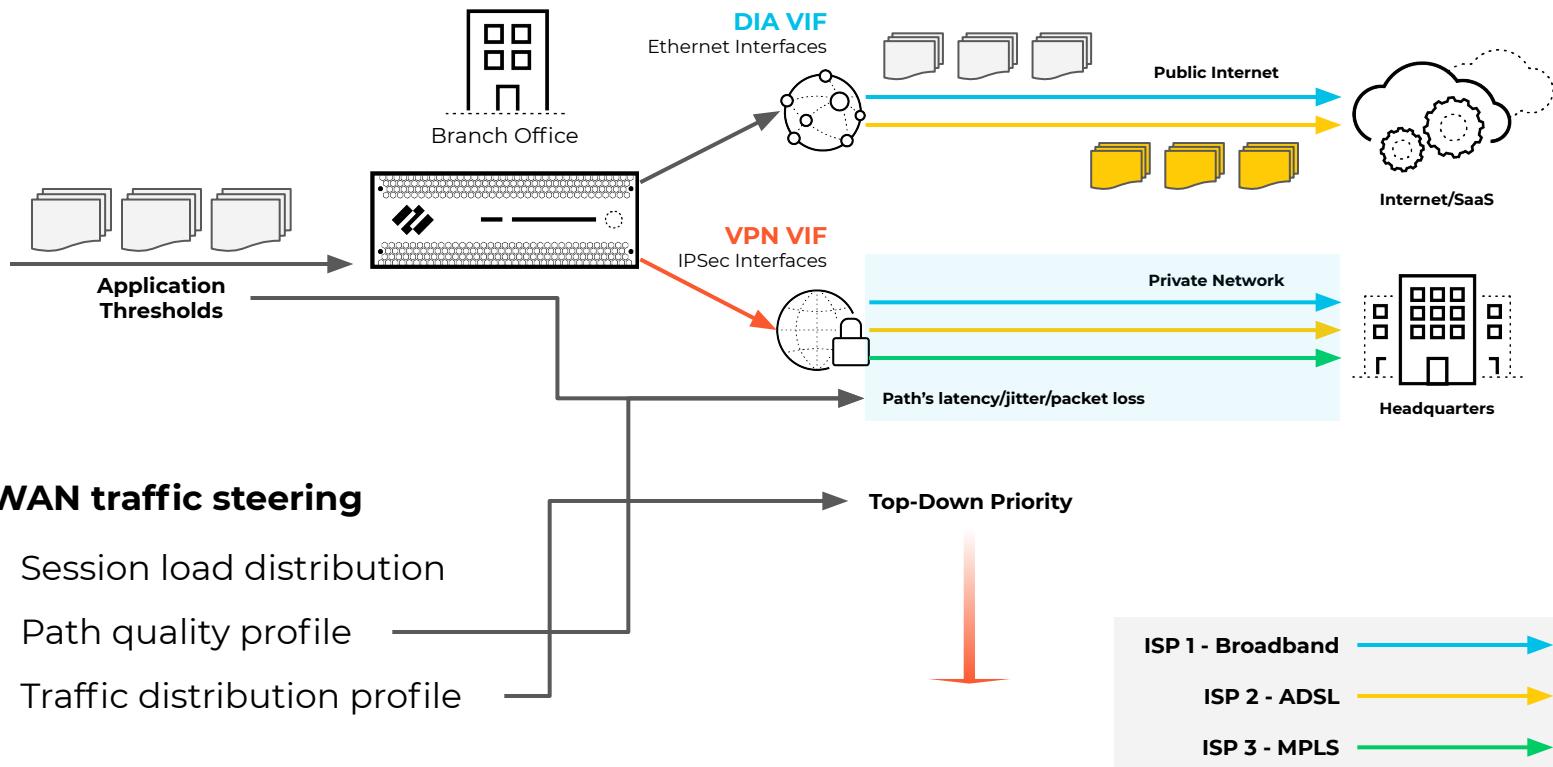


Egress interface is identified from Layer 3 route table lookup

Packet flow sequence

- 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

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

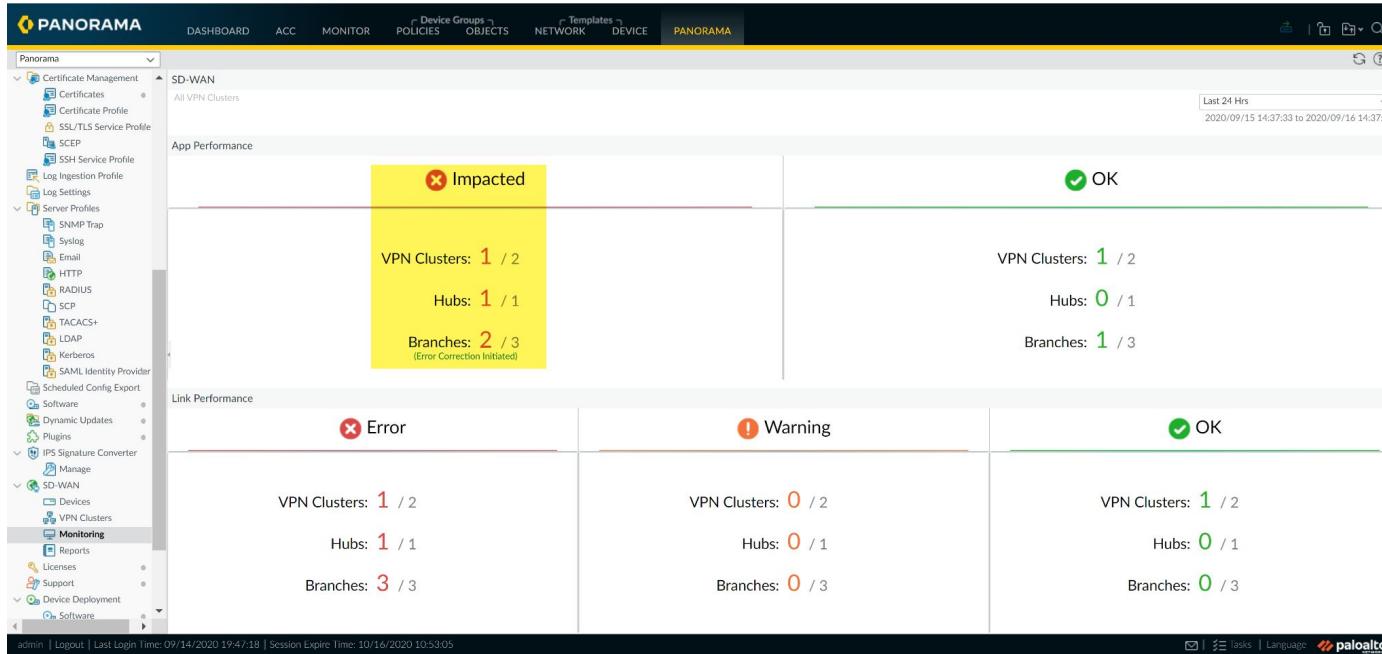
Troubleshoot issues by viewing VPN Cluster information and by drilling down into detailed statistics to isolate the problematic sites, applications, and links

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

The screenshot shows the Palo Alto Networks Panorama web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, and PANORAMA. The left sidebar contains a tree view of configuration sections like Certificate Management, SD-WAN, Server Profiles, and Monitoring. The main content area displays two tables: 'App Performance' and 'Link Performance'.

App Performance Table:
Columns: APP, SD-WAN POLICIES, SAAS MONITORING, APP HEALTH, ERROR CORRECTION APPLIED, BYTES, ERROR CORRECTED SESSIONS / IMPACTED SESSIONS / TOTAL SESSIONS, LINK TAGS.
Data:

APP	SD-WAN POLICIES	SAAS MONITORING	APP HEALTH	ERROR CORRECTION APPLIED	BYTES	ERROR CORRECTED SESSIONS / IMPACTED SESSIONS / TOTAL SESSIONS	LINK TAGS
ssh	Tunnel_SCP	Disabled	● Impacted	-	339.08 GB	0 / 4 / 12	BroadBand1 BroadBand2
bgp		Disabled	● Impacted	-	18.68 MB	0 / 1 / 1	BroadBand1 BroadBand2
alipay	DIA test-rule	Disabled	● OK	-	1.79 MB	0 / 0 / 14k	BroadBand1 BroadBand2
tumblr-base	DIA	Disabled	● OK	-	1.15 MB	0 / 0 / 14k	BroadBand1

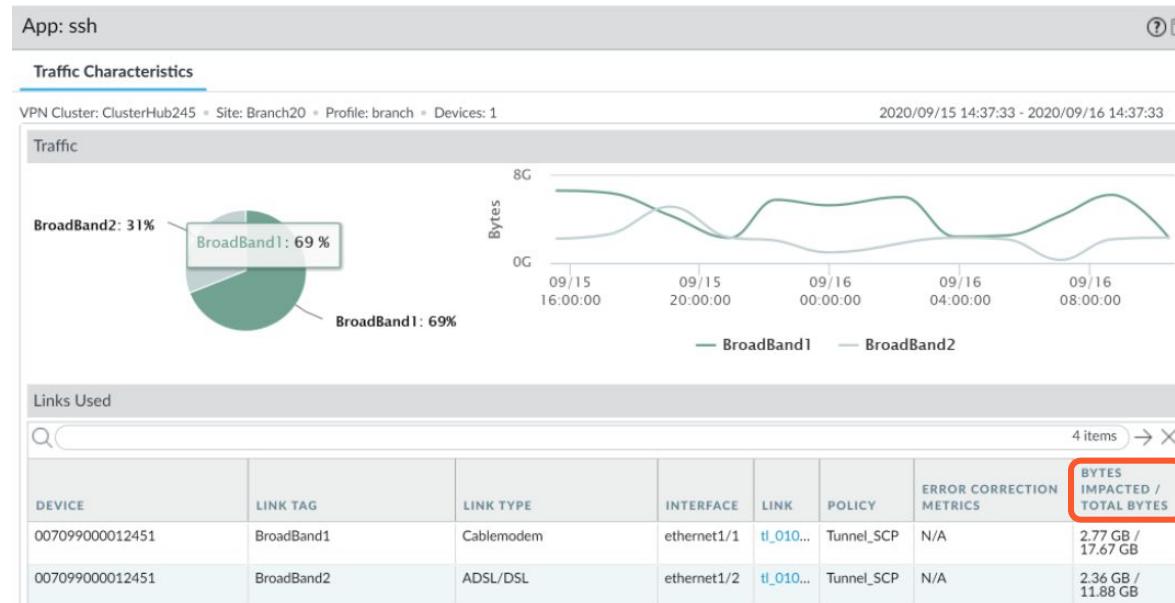
Link Performance Table:
Columns: DEVICE, LINK TAG, LINK TYPE, INTERFACE, LINK, ERROR CORRECTION APPLIED, LINK NOTIFICATIONS, LATENCY, JITTER, PACKET LOSS.
Data:

DEVICE	LINK TAG	LINK TYPE	INTERFACE	LINK	ERROR CORRECTION APPLIED	LINK NOTIFICATIONS	LATENCY	JITTER	PACKET LOSS
Branch20-2	BroadBand1	Cablemodem	ethernet1/1	ethernet1/1	-	● 0	● Warning	● Warning	● Warning
Branch20-2	BroadBand1	Cablemodem	ethernet1/1	IL_0101_00709900001237...	FEC	● 1	● Warning	● Warning	● Warning
Branch20-2	BroadBand1	Cablemodem	ethernet1/1	IL_0101_00709900001237...	FEC	● 2	● Warning	● Warning	● Warning
Branch20-2	BroadBand2	ADSL/DSL	ethernet1/2	ethernet1/2	-	● 0	● Warning	● Warning	● Warning
Branch20-2	BroadBand2	ADSL/DSL	ethernet1/2	IL_0102_00709900001237...	FEC	● 1	● Warning	● Warning	● Warning
Branch20-2	MPLS	MPLS	ethernet1/4	ethernet1/4	-	● 0	● Warning	● Warning	● Warning
Branch20-2	BroadBand2	ADSL/DSL	ethernet1/2	IL_0102_00709900001237...	FEC	● 2	● Warning	● Warning	● Warning
Branch20-2	No Data	No Data	No Data	IL_0104_00709900001237...	-	● 0	● Warning	● Warning	● Warning

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>