PaloAlto

VM-Series on Orange Flex Engine

Troubleshooting Guide

11th September 2018

version 1.0

Document control

date	version no.	author	change/addition
11th September 2018	1.0	Ahmad Samak	Document Creation

Table of contents

1 Recommendation for Network Troubleshooting Tools

It is useful to have a separate troubleshooting station to capture traffic or inject test packets in the virtualized environment. It can be helpful to build a fresh OS from scratch with common troubleshooting tools installed such as tcpdump, nmap, hping, traceroute, iperf, tcpedit, netcat, etc. This machine can then be powered down and converted to a template. Each time the tools are needed, the troubleshooting client (virtual machine) can be quickly deployed to the virtual switch(es) in question and used to isolate networking problems. When the testing is complete, the instance can simply be discarded and the template used again the next time it is required.

2 Licensing Issues

2.1 Why am I unable to apply the support or feature license?

Have you applied the capacity auth-code on the VM-Series firewall? Before you can activate the support or feature license, you must apply the capacity auth-code so that the device can obtain a serial number. This serial number is required to activate the other licenses on the VM-Series firewall.

2.2 Why does my cloned VM-Series firewall not have a valid license?

VMware assigns a unique UUID to each virtual machine including the VM-Series firewall.So, when a VM-Series firewall is cloned, a new UUID is assigned to it. Because the serial number and license for each instance of the VM-Series firewall is tied to the UUID, cloning a licensed VM-Series firewall will result in a new firewall with an invalid license. You will need a new auth-code to activate the license on the newly deployed firewall. You must apply the capacity auth-code and a new support license in order to obtain full functionality, support, and software upgrades on the VM-Series firewall.

2.3 Will moving the VM-Series firewall cause license invalidation?

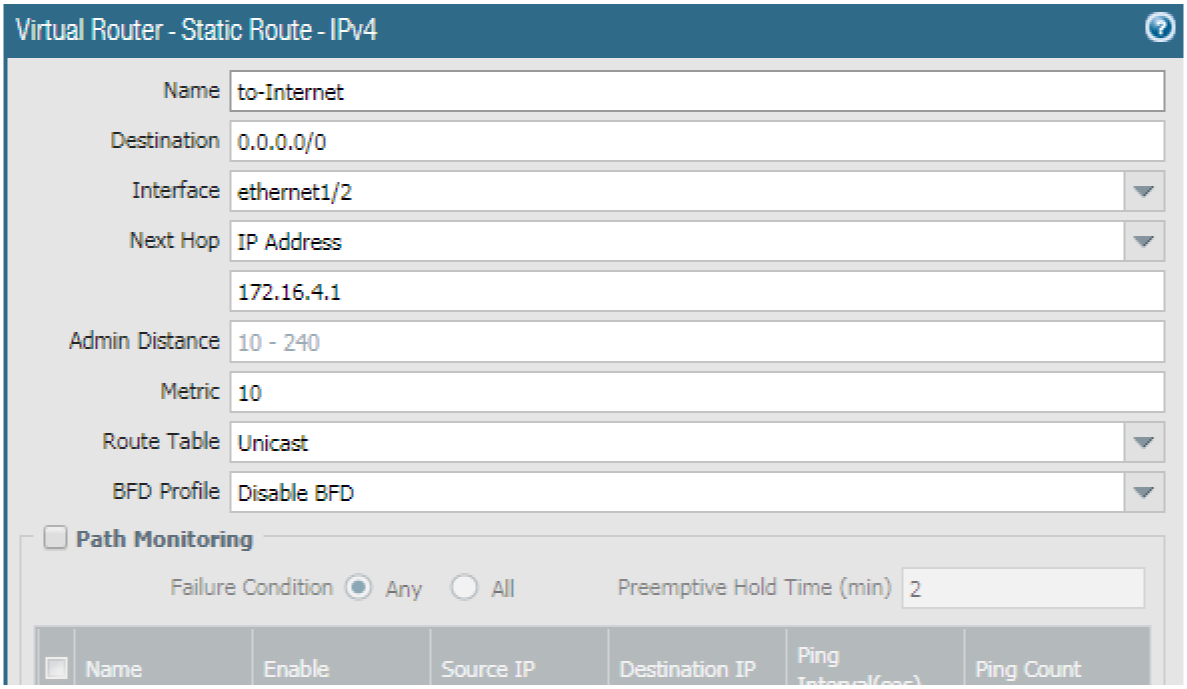
If you are manually moving the VM-Series firewall from one host to another, be sure to select the option, This guest was moved to prevent license invalidation.

3 Connectivity Issues

Before Troubleshooting connectivity issues. You have to make sure that the following configuration has been done correctly :

3.1 Un-trust port is not connected to the Internet

Make sure that the next hop is the gateway of the VPC containing the Palo Alto VM.



Virtual Router - Static Route - IPv4

Name	to-Internet
Destination	0.0.0.0/0
Interface	ethernet1/2
Next Hop	IP Address
	172.16.4.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

Failure Condition ● Any ○ All Preemptive Hold Time (min) 2

□	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

3.2 Why is the VM-Series firewall not receiving any network traffic?

On the VM-Series firewall. check the traffic logs (MonitorLogs). If the logs are empty, use the following CLI command to view the packets on the interfaces of the VM-Series firewall:

```
show counter global filter delta yes
Global counters:
Elapsed time since last sampling: 594.544 seconds
--------------------------------------------------------------------------------
Total counters shown: 0
--------------------------------------------------------------------------------
```

In the vSphere environment, check for the following issues:

- Check the port groups and confirm that the firewall and the virtual machine(s) are on the correct port group

  Make sure that the interfaces are mapped correctly.

  Network adapter 1 = management

Network adapter 2= Ethernet1/1

Network adapter 3 = Ethernet1/2

For each virtual machine, check the settings to verify the interface is mapped to the correct port group.

- Verify that either promiscuous mode is enabled for each port group or for the entire switch or that you have configured the firewall to Hypervisor Assigned MAC Addresses .

  Since the dataplane PAN-OS MAC addresses are different than the VMNIC MAC addresses assigned by vSphere, the port group (or the entire vSwitch) must be in promiscuous mode if not enabled to use the hypervisor assigned MAC address:

  - Check the VLAN settings on vSphere.
    The use of the VLAN setting for the vSphere port group serves two purposes: It determines which port groups share a layer 2 domain, and it determines whether the uplink ports are tagged (802.1Q).

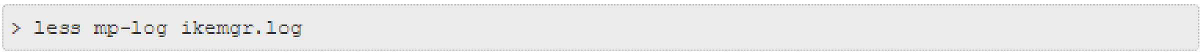
  - Check the physical switch port settings
    If a VLAN ID is specified on a port group with uplink ports, then vSphere will use 802.1Q to tag outbound frames. The tag must match the configuration on the physical switch or the traffic will not pass.
    Check the port statistics if using virtual distributed switches (vDS); Standard switches do not provide any port statistic

3.3 How to Troubleshoot IPSec VPN connectivity issues

These steps are intended to help troubleshoot IPSec VPN connectivity issues. They are divided into two parts, one for each Phase of an IPSec VPN.

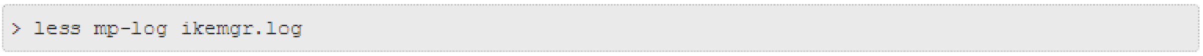
Phase 1

- To rule out ISP-related issues, try pinging the peer IP from the PA external interface. 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. Usually this policy is not required if there is no clean-up rule configured on the box. If a clean-up rule is configured, the policy is configured usually from the external zone to the external zone.
- 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:



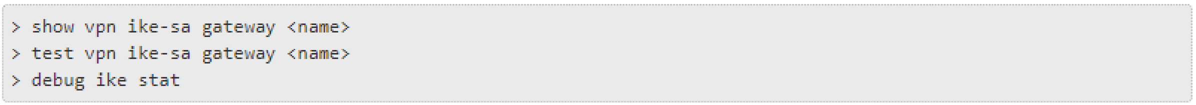
```
> less mp-log ikemgr.log
```

- Check that preshared 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
```

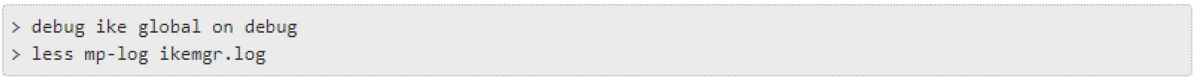
- Take packet captures to analyze the traffic. Use filters to narrow the scope of the captured traffic.
- Useful CLI commands:



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

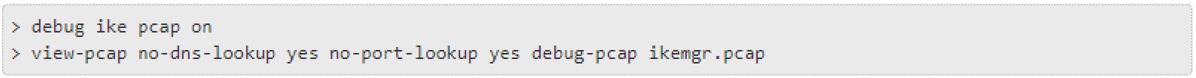
Advanced CLI commands:

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



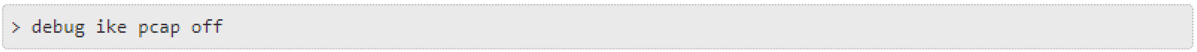
```
> debug ike global on debug
> less mp-log ikemgr.log
```

- 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



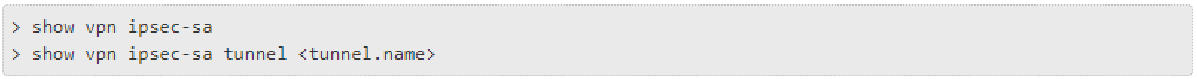
```
> debug ike pcap off
```

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.

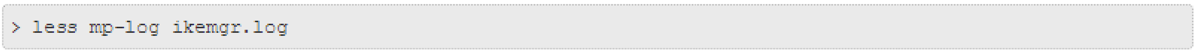
Phase 2

- 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. If incorrect, logs about the mismatch can be found under the system logs under the monitor tab, or by using the following command:



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

- Check if pfs is enabled on both ends. If incorrect, logs about the mismatch can be found under the system logs under the monitor tab, or by using the command:

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

- Check the proxy-id configuration. This is usually not required when the tunnel is between two Palo Alto Networks firewalls, but when the peer is from another vendor, IDs usually need to be configured.
  A mismatch would be indicated under the system logs, or by using the command:

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

- Check the proxy-id configuration. This is usually not required when the tunnel is between two Palo Alto Networks firewalls, but when the peer is from another vendor, IDs usually need to be configured.
  A mismatch would be indicated under the system logs, or by using the command:

```
> 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
```

- 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 translating device in front of PAN that might be dropping the ESP packets.

```
> 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>
```

```
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:

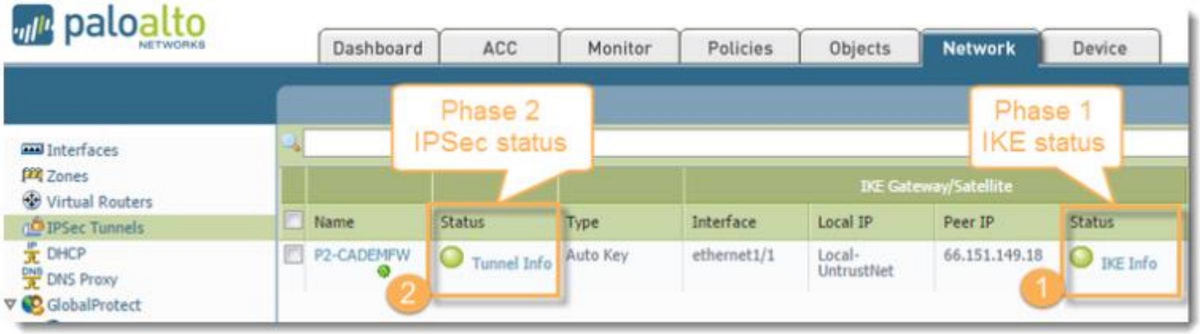
- Check security policy and routing.
- Check for any devices upstream that perform port-and-address-translations. Because ESP is a layer 3 protocol, ESP packets do not have port numbers. When such devices receive ESP packets, there is a high possibility they may silently drop them, because they do not 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.

3.4 VPN IPSec Tunnel Status is Red

When it comes to working with IPSec VPNs, it can be tricky to understand the status properly, which is why I chose this topic to talk about.

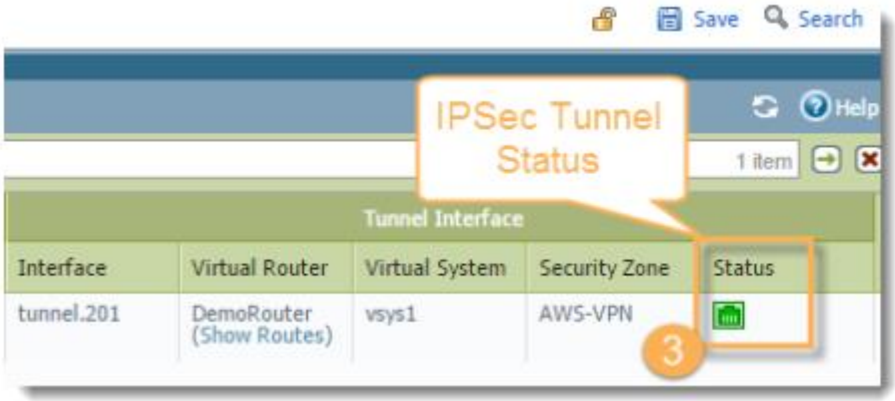
Let's start with the IPSec tunnel status window, which can be accessed from the WebGUI > Network > IPSec Tunnels.

Inside that window, you see the status of all of the IPSec VPN tunnels that you have configured on this firewall.



Name	Status	Type	Interface	Local IP	Peer IP	Status
			IKE Gateway/Satellite			
P2-CADEMFW	● Tunnel Info	Auto Key	ethernet1/1	Local-UntrustNet	66.151.149.18	● IKE Info

IPSec Tunnel status window showing both P1 and P2 status of every tunnel on this device.



Tunnel Interface				
Interface	Virtual Router	Virtual System	Security Zone	Status
tunnel.201	DemoRouter (Show Routes)	vsys1	AWS-VPN	🟩

Detail of the second part of the same window showing the IPSec Tunnel Status.

The confusing part about the IPSec Tunnel status window is that there are actually 3 areas that show the current status. I have detailed the "status" below:

1. **Phase 1 - IKE status** - Green indicates a valid IKE phase-1 SA or IKEv2 IKE SA. Red indicates that IKE phase-1 SA is not available or has expired.
2. **Phase 2 - IPSec status** - Green indicates an IPSec phase-2 security association (SA) tunnel. Red indicates that IPSec phase-2 SA is not available or has expired.
3. **IPSec Tunnel Interface status** - Green indicates that the tunnel interface is up (because tunnel monitor is disabled or because tunnel monitor status is UP and the monitoring IP address is reachable). Red indicates that the tunnel interface is down because the tunnel monitor is enabled and the remote tunnel monitoring IP address is unreachable.

I have personally seen the Phase 2 IPSec showing Green, with Phase 1 IKE showing a Red status, even though the tunnel is showing green, because it is still active. The next time that IKE is to be renegotiated, it may or may not have an issue, but it's good to be aware of.

To get more detailed information on what is going on when the IPSec Tunnel Interface is showing Red, you will need to go into your logs and look for any errors that may help indicate what the problem is. You also can click the "Tunnel Info" and "IKE Info" text to the right of the "bubble" status to get more info. (A window will appear showing the IKE or IPSec info).

3.5 Troubleshooting GlobalProtect

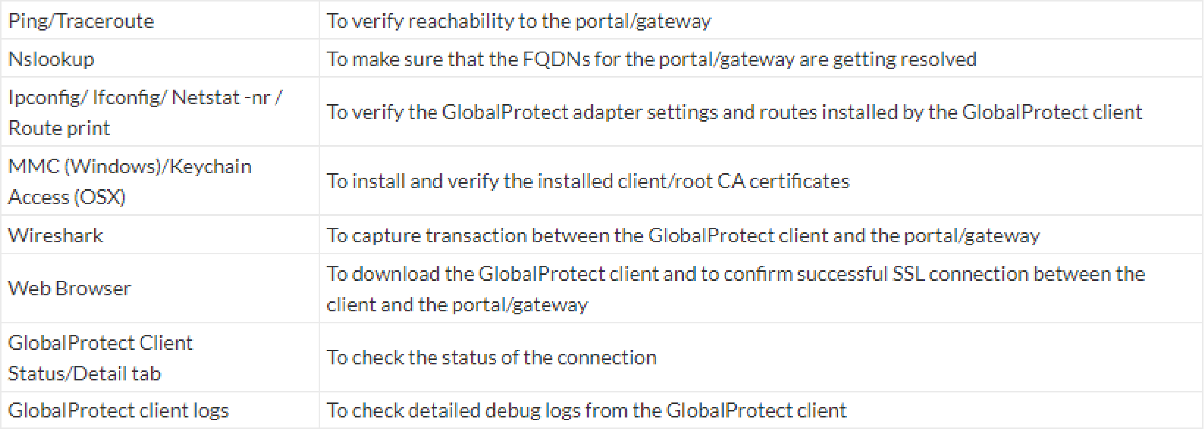
Issues related to GlobalProtect can fall broadly into the following categories:

- GlobalProtect unable to connect to portal or gateway
- GlobalProtect agent connected but unable to access resources
- Miscellaneous

This article lists some of the common issues and methods for troubleshooting GlobalProtect. The article assumes you are aware of the basics of GlobalProtect and its configuration.

Tools used for troubleshooting

Tools and utilities for troubleshooting on the client machine:



Ping/Traceroute	To verify reachability to the portal/gateway
Nslookup	To make sure that the FQDNs for the portal/gateway are getting resolved
Ipconfig/ Ifconfig/ Netstat -nr / Route print	To verify the GlobalProtect adapter settings and routes installed by the GlobalProtect client
MMC (Windows)/Keychain Access (OSX)	To install and verify the installed client/root CA certificates
Wireshark	To capture transaction between the GlobalProtect client and the portal/gateway
Web Browser	To download the GlobalProtect client and to confirm successful SSL connection between the client and the portal/gateway
GlobalProtect Client Status/Detail tab	To check the status of the connection
GlobalProtect client logs	To check detailed debug logs from the GlobalProtect client

Tools used for troubleshooting on the firewall:

1. Packet Captures:

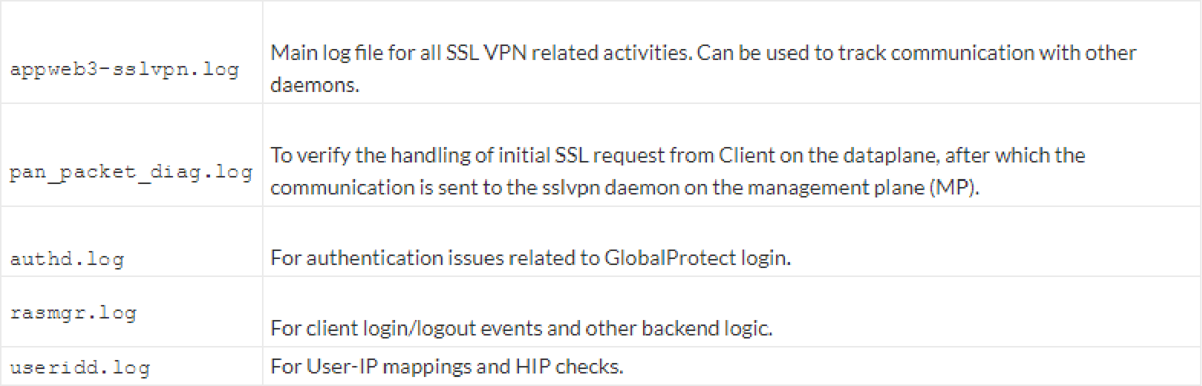
- **Dataplane Captures:**

  For transactions between the client and the portal/gateway. Useful to see if the firewall is dropping any packets on the dataplane. But not very helpful with SSL offload enabled since packets might be missing.

- **Management Port Captures**

  For transactions between the firewall and the LDAP server (for authentication)

2. Debug Logs: Might need to enable debug for more detailed information:



`appweb3-sslvpn.log`	Main log file for all SSL VPN related activities. Can be used to track communication with other daemons.
`pan_packet_diag.log`	To verify the handling of initial SSL request from Client on the dataplane, after which the communication is sent to the sslvpn daemon on the management plane (MP).
`authd.log`	For authentication issues related to GlobalProtect login.
`rasmgr.log`	For client login/logout events and other backend logic.
`useridd.log`	For User-IP mappings and HIP checks.

3. CLI commands

4. Traffic logs: To verify connections coming from the client for the portal/gateway and for checking details of sessions from a connected GlobalProtect client to resources.

3.5.1 General Troubleshooting approach:

1. Verify that the configuration has been done correctly as per documents suiting your scenario.
2. On the client, make sure the GlobalProtect client is installed, if this is not the first time you are connecting to GlobalProtect.
3. Use nslookup on the client to make sure the client can resolve the FQDNs for the portal/gateway.
4. Open a web browser and enter the URL : https://<Portal-IP/FQDN> ***and/or*** https://<Gateway-IP/FQDN>. This will make sure that the SSL communication between the client and the portal/gateway is working fine. The web browser easily helps us check the certificate coming from the portal/gateway. If there are certificate issues, browser errors can help isolate those, for example,

- Signing Authority is not trusted
- Common Name in the certificate is different from SNI requested by client, or SAN does not contain proper DNS name
- Certificate validity expired
- Any issues in certificate chain

5. If the browser page above is not loading properly, check with Wireshark to see if the TCP handshake is complete or not. Use filter**`ip.addr==<Portal IP>`** ***or*** **`ip.addr==<gatewayIP>`** as appropriate
.
6. If the SYN packet is going out and no ACK is received, move to the firewall and see if the sessions are getting formed, and if packets are getting dropped. Use dataplane debugs or captures combined with global counters to check the same. Check security policies, NAT, etc. to make sure traffic is not getting dropped.
7. In the above case, sometimes it is also helpful to check if dataplane resources are healthy. Check the following commands to find any resource overutilization:

```
> show running resource-monitor
> debug dataplane pool statistics
```

8. Check **`appweb3-sslvpn.log`** for more information, if packets are not getting dropped on the dataplane.
9. From the browser, if the GlobalProtect login page is loading properly, it might ask for the client certificate if client certificate-based authentication is enabled on the portal.
10. Check whether the proper client certificate is loaded into the machine's certificate store, and the browser’s certificate store.
11. If you are getting the error 'valid Client Certificate is required,' import the client certificate into the browser and the client machine.
'Valid client certificate is required' error accessing portal address on Firefox
Internet Explorer Browser Error: "Valid client certificate required"

12. Try logging in to the GlobalProtect Portal Web page. This will confirm that the authentication is working fine.

13. If unable to log in, check the firewall authd logs to see what is the error. The following document can be helpful if using LDAP authentication: How to Troubleshoot LDAP Authentication

14. If you are able to login in to the Portal Web page, download and install the GlobalProtect client, if not already installed.

15. Open the GlobalProtect client, and enter the required settings (Username/ Password / Portal) and click Apply.

16. Notice the message displayed on the Status tab.

17. Collect the logs on the GlobalProtect client, as mentioned in the tools used section, and open the PanGPS.log file in the zipped folder.

18. Go through the logs, and based on error messages, take corrective action or troubleshoot.

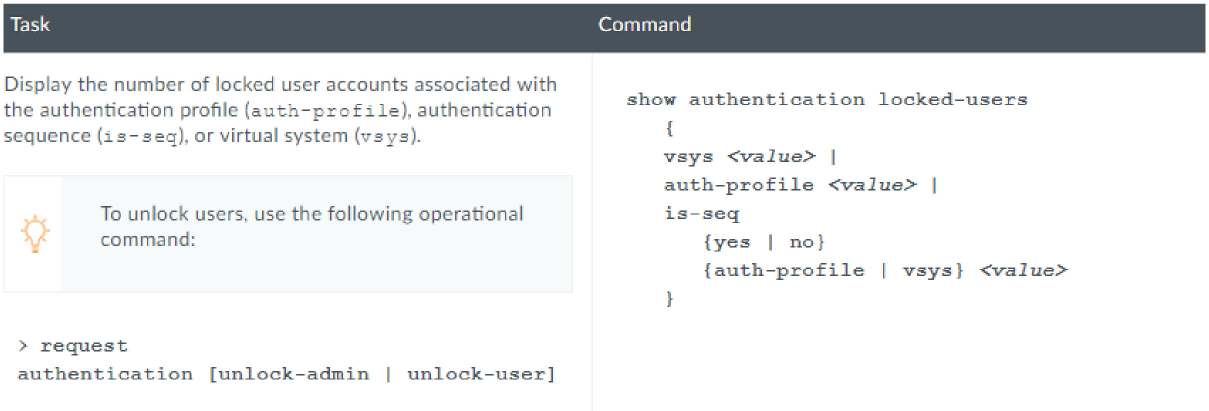
19. Simultaneously, you might be required to check the **`mp-log/appweb3-sslvpn.log`** on the firewall for more information.

4 Authentication Issues

When users fail to authenticate to a Palo Alto Networks firewall or Panorama, or the Authentication process takes longer than expected, analyzing authentication-related information can help you determine whether the failure or delay resulted from:

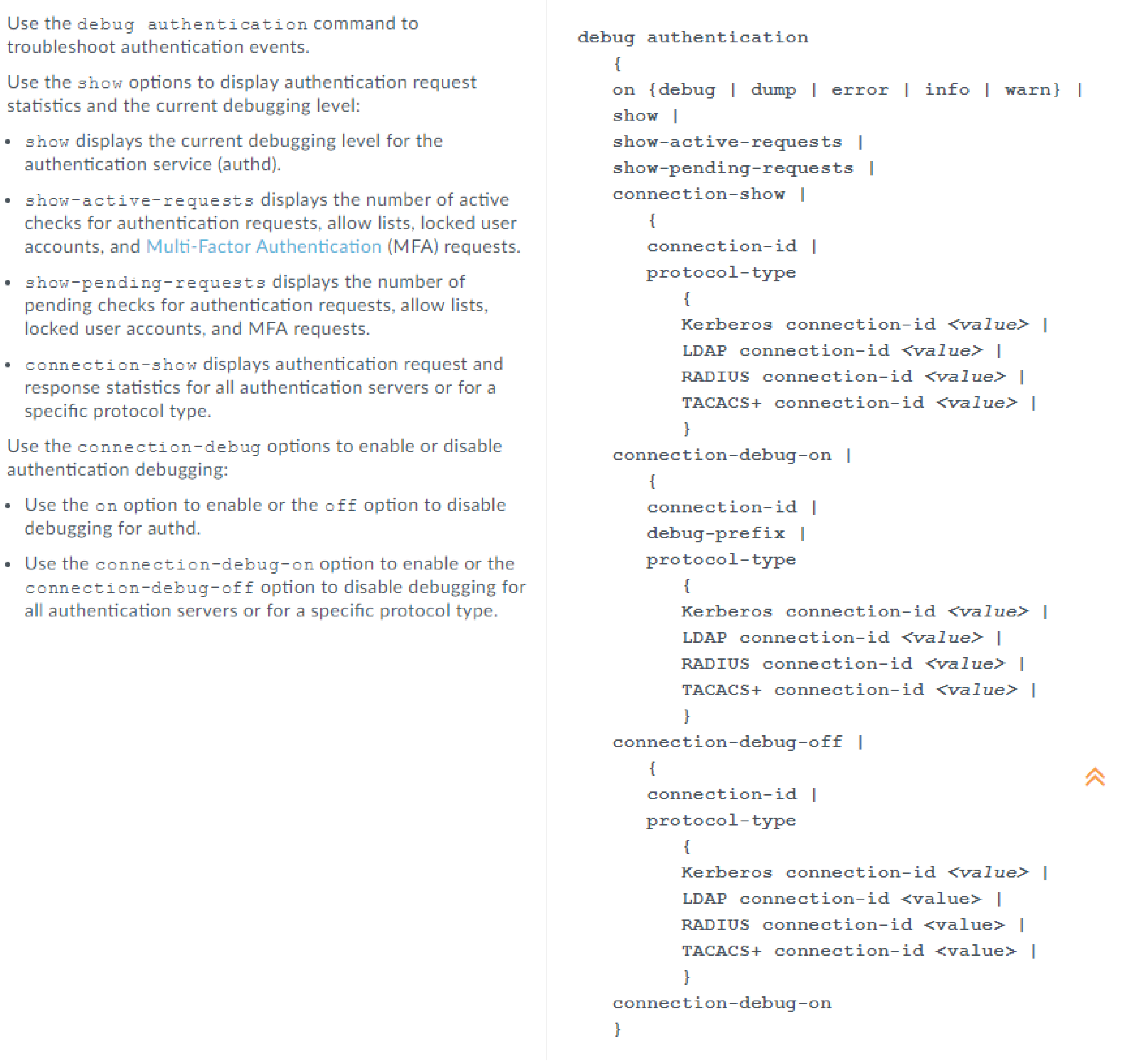
- **User behavior**—For example, users are locked out after entering the wrong credentials or a high volume of users are simultaneously attempting access.
- **System or network issues**—For example, an authentication server is inaccessible.
- **Configuration issues**—For example, the Allow List of an authentication profile doesn't have all the users it should have.

The following CLI commands display information that can help you troubleshoot these issues:



Task	Command

Display the number of locked user accounts associated with the authentication profile (`auth-profile`), authentication sequence (`is-seq`), or virtual system (`vsys`).
To unlock users, use the following operational command:
`> request authentication [unlock-admin | unlock-user]`
	`show authentication locked-users`
	`{`
	`vsys <value> |`
	`auth-profile <value> |`
	`is-seq`
	`{yes | no}`
	`{auth-profile | vsys} <value>`
	`}`



Use the `debug authentication` command to troubleshoot authentication events.

Use the `show` options to display authentication request statistics and the current debugging level:

- `show` displays the current debugging level for the authentication service (authd).
- `show-active-requests` displays the number of active checks for authentication requests, allow lists, locked user accounts, and Multi-Factor Authentication (MFA) requests.
- `show-pending-requests` displays the number of pending checks for authentication requests, allow lists, locked user accounts, and MFA requests.
- `connection-show` displays authentication request and response statistics for all authentication servers or for a specific protocol type.

Use the `connection-debug` options to enable or disable authentication debugging:

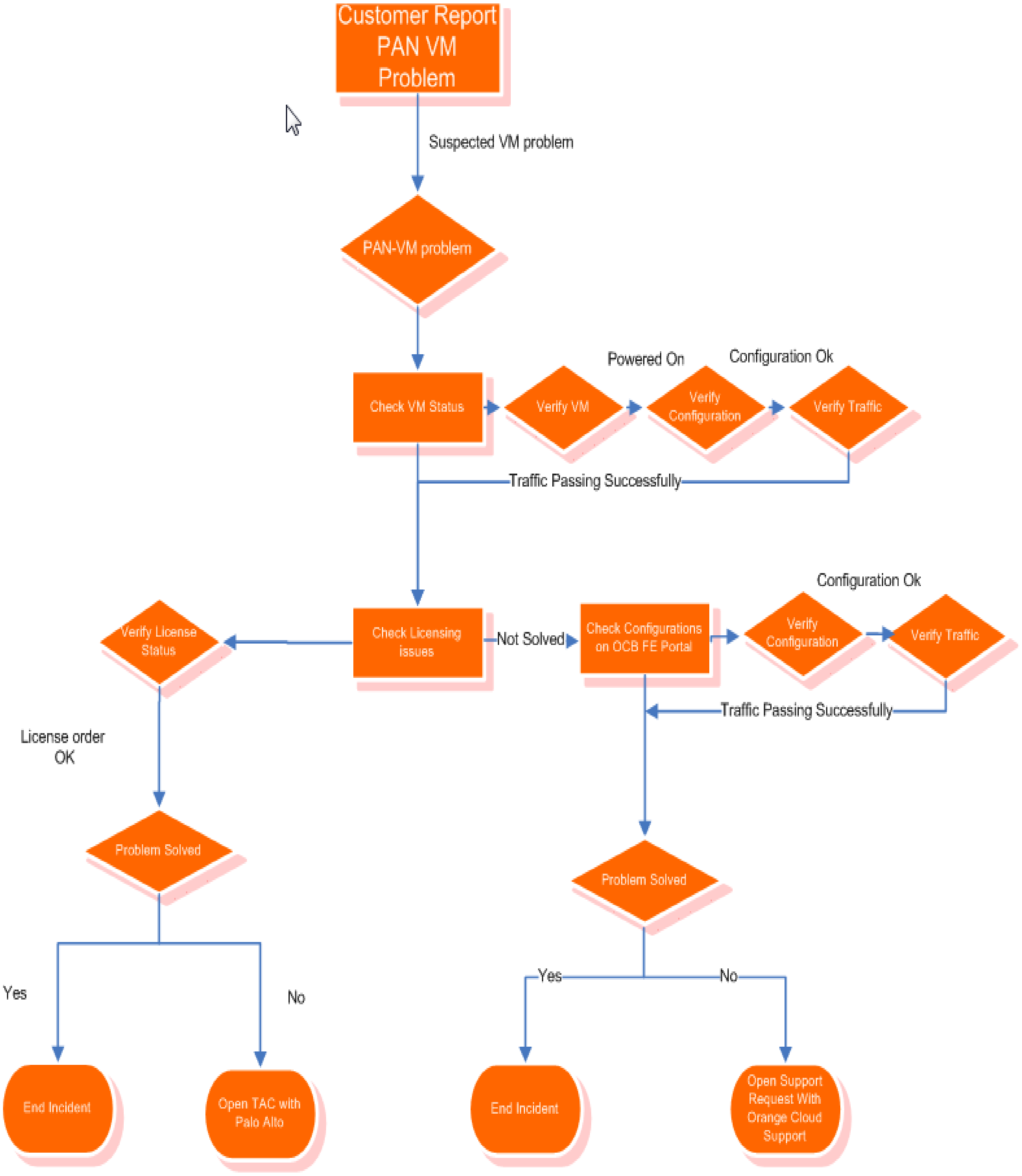
- Use the `on` option to enable or the `off` option to disable debugging for authd.
- Use the `connection-debug-on` option to enable or the `connection-debug-off` option to disable debugging for all authentication servers or for a specific protocol type.

```
debug authentication
   {
   on {debug | dump | error | info | warn} |
   show |
   show-active-requests |
   show-pending-requests |
   connection-show |
      {
      connection-id |
      protocol-type
         {
         Kerberos connection-id <value> |
         LDAP connection-id <value> |
         RADIUS connection-id <value> |
         TACACS+ connection-id <value> |
         }
   connection-debug-on |
      {
      connection-id |
      debug-prefix |
      protocol-type
         {
         Kerberos connection-id <value> |
         LDAP connection-id <value> |
         RADIUS connection-id <value> |
         TACACS+ connection-id <value> |
         }
   connection-debug-off |
      {
      connection-id |
      protocol-type
         {
         Kerberos connection-id <value> |
         LDAP connection-id <value> |
         RADIUS connection-id <value> |
         TACACS+ connection-id <value> |
         }
   connection-debug-on
   }
```

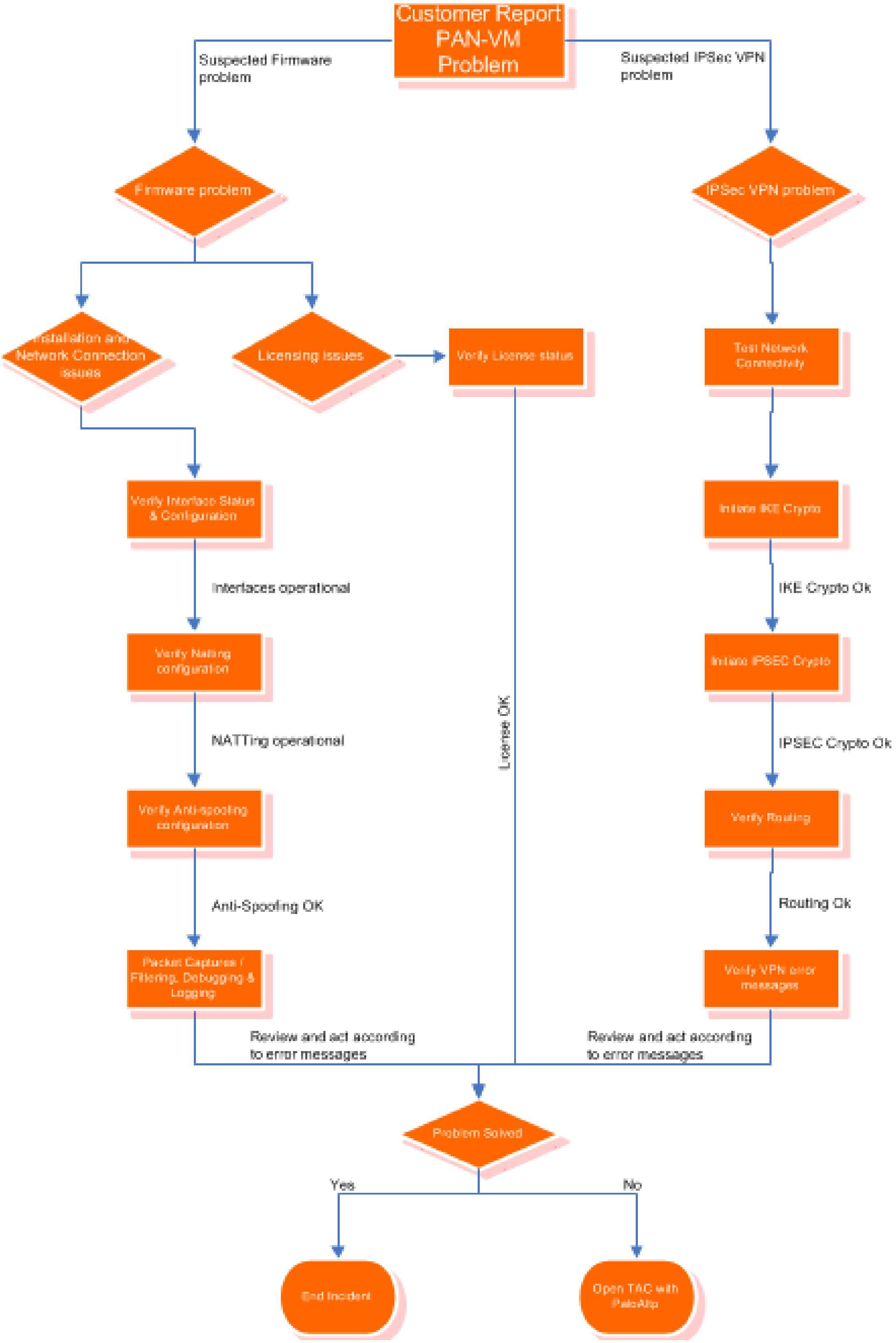
5 Troubleshooting Decision Tree

5.1 Troubleshooting Decision Diagram

PaloAlto – VM-SERIES
Troubleshooting Decision Diagram (VM-Series + Orange Flex Engine)



5.2 Troubleshooting Decision Diagram (PN-VM + IPSEC VPN)


Customer Report PAN-VM Problem
Suspected Firmware problem
Suspected IPSec VPN problem
Firmware problem
IPSec VPN problem
Installation and Network Connection issues
Licensing issues
Verify License status
Test Network Connectivity
Verify Interface Status & Configuration
Initiate IKE Crypto
Interfaces operational
IKE Crypto Ok
Verify Natting configuration
Initiate IPSEC Crypto
License OK
NATTing operational
IPSEC Crypto Ok
Verify Anti-spoofing configuration
Verify Routing
Anti-Spoofing OK
Routing Ok
Packet Captures / Filtering, Debugging & Logging
Verify VPN error messages
Review and act according to error messages
Review and act according to error messages
Problem Solved
Yes
No
End Incident
Open TAC with PaloAlto