

digitalscepter

# Palo Alto Networks Advanced Troubleshooting

November 17th, 2026

# Agenda

1. Common Firewall Issues
2. Troubleshooting Tools & Techniques
3. Real World Scenarios
4. “Can I Troubleshoot Effectively” Test

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Common Firewall Issues

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Traffic Slowness/Latency

- Users may experience packet loss even when an interface and the firewall is below its bandwidth limit.
- Check packet buffers, descriptors, session creation rates and dataplane utilization.
- Useful commands: *show running resource-monitor* and *show session info*
- Correlate rising drop counters with protection events and the timing of user complaints.

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Traffic Slowness/Latency

- firewall>*show running resource-monitor*

```
zsum@prdfw01a(active)> show running resource-monitor hour last 5

Resource monitoring sampling data (per hour):

CPU load (%) during last 5 hours:
core    0       1       2       3       4       5       6       7
     avg max avg max avg max avg max avg max avg max avg max avg max
       *   *   1   8   1   9   0   9   1  14   1   7   1   6   *   *
       *   *   1  11   1   9   0   9   1   4   1   9   1   8   *   *
       *   *   0   5   1   4   0   4   1   3   1   7   1   7   *   *
       *   *   0   5   1   4   0   3   1   4   1   3   1   4   *   *
       *   *   1   4   1   4   0  12   1   3   1   4   1   5   *   *

Resource utilization (%) during last 5 hours:
session (average):
  0   0   0   0   0
session (maximum):
  0   0   0   0   0
packet buffer (average):
  0   0   0   0   0
packet buffer (maximum):
  0   0   0   0   0
packet descriptor (average):
  0   0   0   0   0
packet descriptor (maximum):
  0   0   0   0   0
sw tags descriptor (average):
  4   4   4   4   4
sw tags descriptor (maximum):
  8   8   7   8   8
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Traffic Slowness/Latency

- firewall>*show session info*

```
zsum@prdfw01a(active)> show session info

target-dp:                                    *.dp0
-------------------------------------------------------------------------------
Number of sessions supported:                 945000
Number of allocated sessions:                 901
Number of active TCP sessions:                390
Number of active UDP sessions:                504
Number of active ICMP sessions:               0
Number of active GTPc sessions:               0
Number of active HTTP2-5gc sessions:          0
Number of active GTPu sessions:               0
Number of pending GTPu sessions:              0
Number of active BCAST sessions:              0
Number of active MCAST sessions:              0
Number of active predict sessions:            0
Number of active SCTP sessions:               0
Number of active SCTP associations:           0
Number of active PFCP sessions:               0
Number of active IMSI sessions:               0
Session table utilization:                    0%
Number of sessions created since bootup:      36531322
Packet rate:                                  696/s
Throughput:                                   2446 kbps
New connection establish rate:                6 cps
-------------------------------------------------------------------------------
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

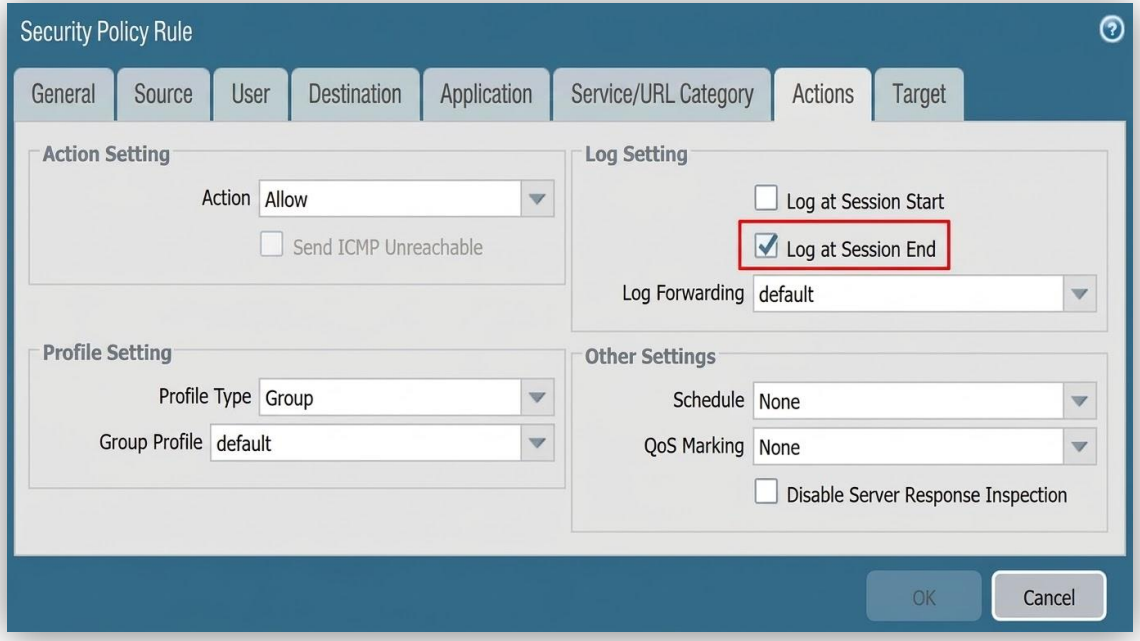
# Traffic Slowness/Latency

- Pay close attention to symptoms
    - New web page has a few seconds of latency then loads fine?
        - Test DNS resolution. Some requests may be timing out
    - Page continuously tries to load, but never does?
        - More likely to be an outage versus a firewall issue
    - Connection immediately fails?
        - Check browser error code. Could be firewall or destination resetting connection. Could be decrypt issue, threat prevention, etc.

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Missing Traffic Logs

- The security policy needs “Log at Session End” enabled

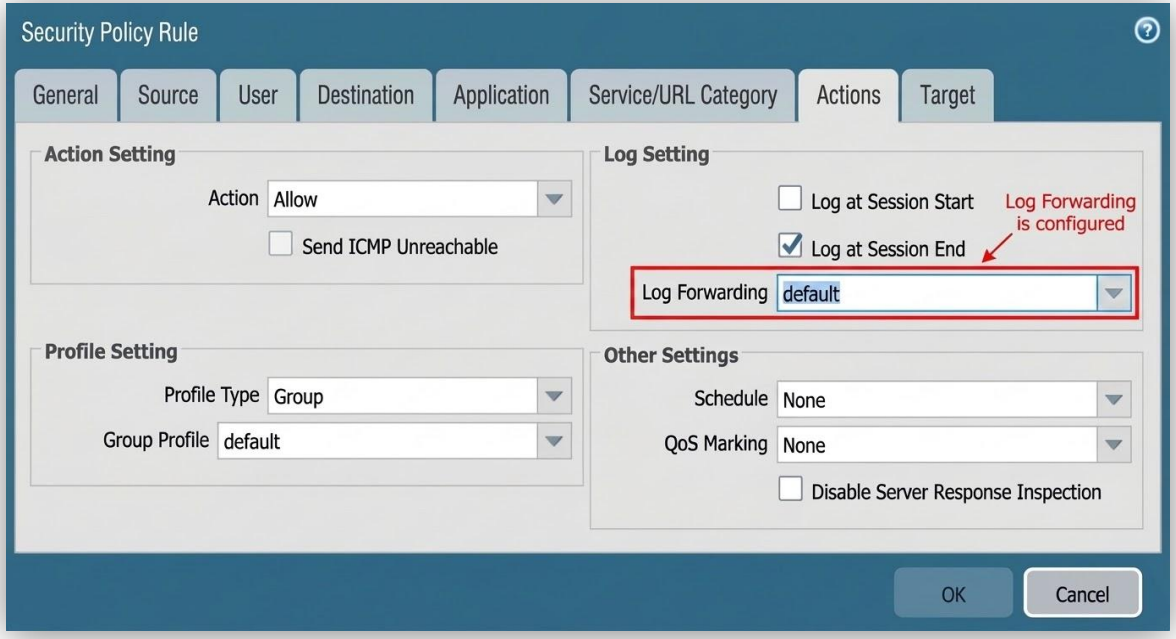



©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Missing Traffic Logs

- If missing in Panorama, the rule may not be configured to forward logs to Panorama

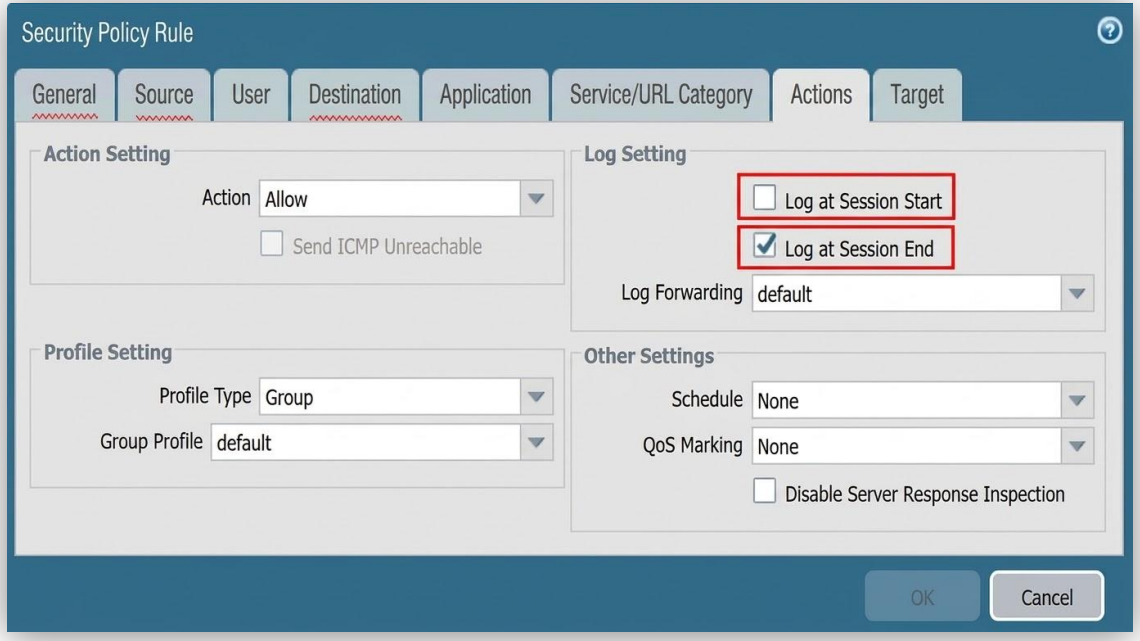



©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Missing Traffic Logs

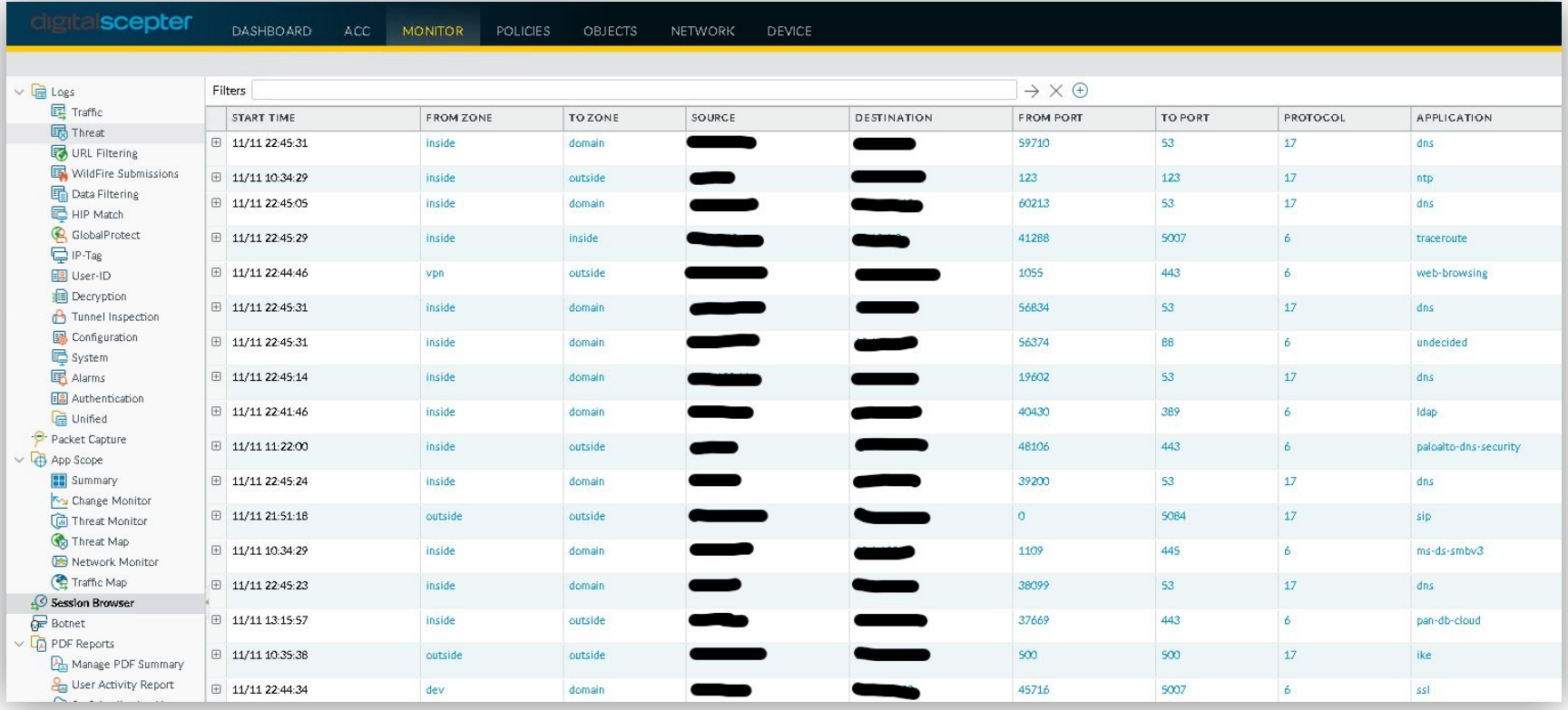
- The session is still active with default log settings configured




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Missing Traffic Logs




| START TIME | FROM ZONE | TO ZONE | SOURCE | DESTINATION | FROM PORT | TO PORT | PROTOCOL | APPLICATION |
|---|---|---|---|---|---|---|---|---|
| 11/11 22:45:31 | inside | domain | [redacted] | [redacted] | 59710 | 53 | 17 | dns |
| 11/11 10:34:29 | inside | outside | [redacted] | [redacted] | 123 | 123 | 17 | ntp |
| 11/11 22:45:05 | inside | domain | [redacted] | [redacted] | 60213 | 53 | 17 | dns |
| 11/11 22:45:29 | inside | inside | [redacted] | [redacted] | 41288 | 9007 | 6 | traceroute |
| 11/11 22:44:46 | vpn | outside | [redacted] | [redacted] | 1055 | 443 | 6 | web-browsing |
| 11/11 22:45:31 | inside | domain | [redacted] | [redacted] | 56834 | 53 | 17 | dns |
| 11/11 22:45:31 | inside | domain | [redacted] | [redacted] | 56374 | 88 | 6 | undecided |
| 11/11 22:45:14 | inside | domain | [redacted] | [redacted] | 19602 | 53 | 17 | dns |
| 11/11 22:41:46 | inside | domain | [redacted] | [redacted] | 40430 | 389 | 6 | ldap |
| 11/11 11:22:00 | inside | outside | [redacted] | [redacted] | 48106 | 443 | 6 | paloalto-dns-security |
| 11/11 22:45:24 | inside | domain | [redacted] | [redacted] | 39200 | 53 | 17 | dns |
| 11/11 21:51:18 | outside | outside | [redacted] | [redacted] | 0 | 5084 | 17 | sip |
| 11/11 10:34:29 | inside | domain | [redacted] | [redacted] | 1109 | 445 | 6 | ms-ds-smbv3 |
| 11/11 22:45:23 | inside | domain | [redacted] | [redacted] | 38099 | 53 | 17 | dns |
| 11/11 13:15:57 | inside | outside | [redacted] | [redacted] | 37669 | 443 | 6 | pan-db-cloud |
| 11/11 10:35:38 | outside | outside | [redacted] | [redacted] | 500 | 500 | 17 | ike |
| 11/11 22:44:34 | dev | domain | [redacted] | [redacted] | 45716 | 9007 | 6 | ssl |

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Missing Traffic Logs

- Silent Drops (packets discarded without a corresponding Traffic log)

- Examples include drops before or after Security policy evaluation:
  - Zone Protection, DoS Protection, or Packet Buffer Protection
  - IP block list enforcement (DoS or Vulnerability Protection)
  - Missing route or discard route
  - Failed next-hop ARP resolution
  - Invalid/asymmetric packets, or session/resource allocation failures

***How do you find them?***

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Silent Drops

- Silent drops can be seen via the cli using the below command:
  **firewall>** *show counter global filter severity drop*
  - Add "*delta yes*" to show counters since the command was last ran
  - Add "*packet-filter yes*" to filter counters to a specific flow
- Threat logs can sometimes have entries that can explain missing traffic logs

```
zsum@prdfw01a(active)> show counter global filter severity drop delta yes

Global counters:
Elapsed time since last sampling: 10.414 seconds

name                                value     rate severity  category  aspect    description
------------------------------------------------------------------------------------------
flow_rcv_dot1q_tag_err                 10        0 drop      flow      parse     Packets dropped: 802.1q tag not configured
flow_no_interface                      10        0 drop      flow      parse     Packets dropped: invalid interface
flow_ipv6_disabled                      1        0 drop      flow      parse     Packets dropped: IPv6 disabled on interface
flow_policy_deny                       21        2 drop      flow      session   Session setup: denied by policy
flow_tcp_non_syn_drop                   2        0 drop      flow      session   Packets dropped: non-SYN TCP without session match
flow_fwd_l3_mcast_drop                  9        0 drop      flow      forward   Packets dropped: no route for IP multicast
flow_fwd_l3_ttl_zero                    2        0 drop      flow      forward   Packets dropped: IP TTL reaches zero
flow_fwd_l3_noarp                       7        0 drop      flow      forward   Packets dropped: no ARP
flow_action_close                       2        0 drop      flow      pktproc   TCP sessions closed via injecting RST
flow_host_service_unknown               1        0 drop      flow      mgmt      Session discarded: unknown application to control plane
------------------------------------------------------------------------------------------
Total counters shown: 10
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Packet Capture: Missing Packets

- Packet capture filters need to account for each direction of a particular flow
- Pre-NAT and post-NAT addresses should be included in filters
- Captures are done in four stages:

**RECEIVE**

Sees the packet at ingress. If missing, check upstream forwarding and your capture filter.

**FIREWALL**

Shows packets during dataplane processing. Correlate with policy, NAT and session state.

**TRANSMIT**

Confirms the packet leaves the egress path. If missing, inspect routing and drops.

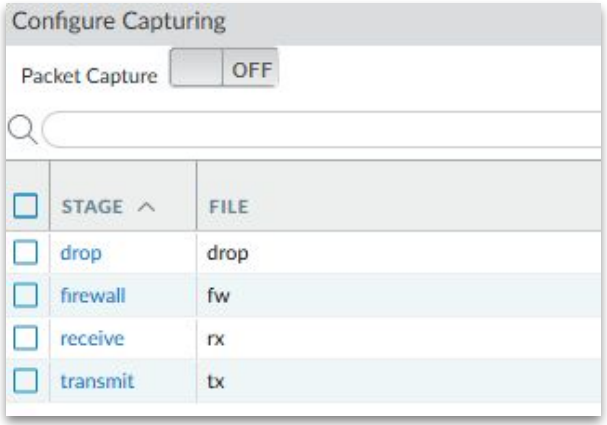
**DROP**

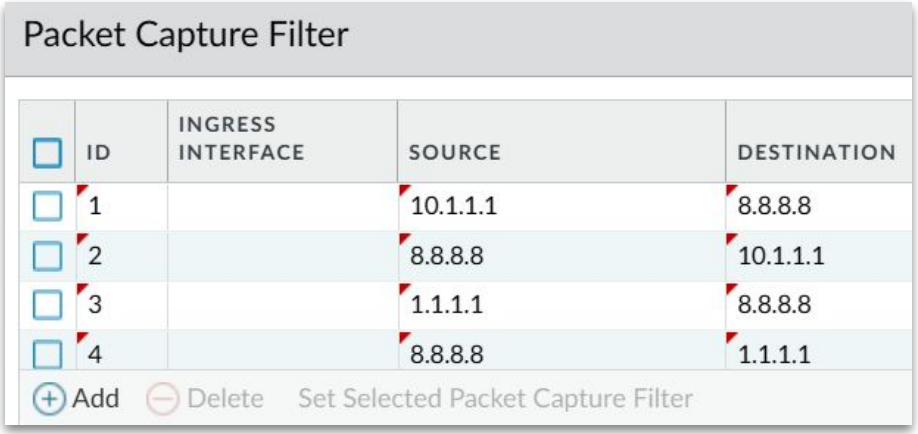
Shows packets discarded by the dataplane. Match captures with global drop counters.

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Packet Capture: Missing Packets

- Let's review a scenario where we want to capture traffic for a host on our network:
  - Source: 10.1.1.1
  - Source NAT: 1.1.1.1
  - Destination: 8.8.8.8



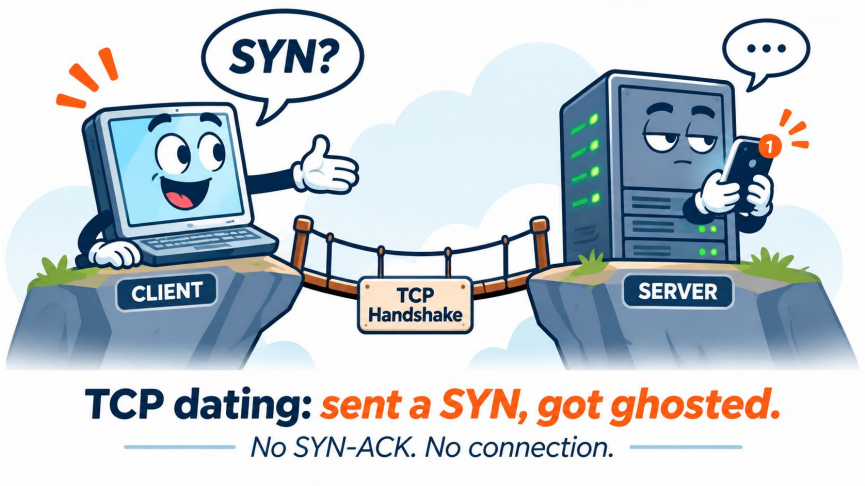

Don't forget to turn your packet capture off

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Incomplete Traffic

- In Traffic logs, an application of 'incomplete' means the TCP three-way handshake did not finish, or it finished without application data.
- For example, the firewall sees the client's SYN but no SYN-ACK returns; an idle connection with no payload can also appear as incomplete.
- Use packet captures and sent/received byte counters to see where communication stopped.



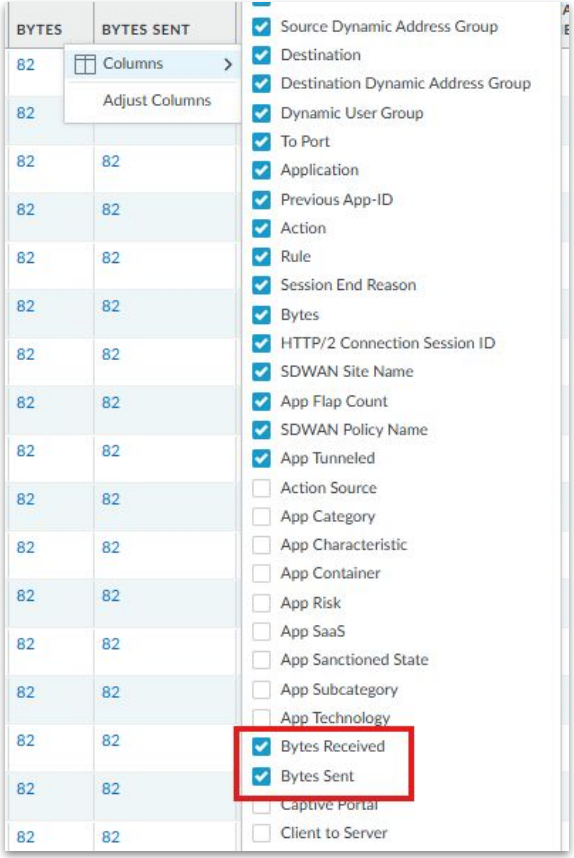

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Incomplete Traffic

- Add the bytes received and bytes sent column in your traffic log view
- Zero server-to-client bytes suggests no reply was seen by the firewall. Verify with session counters and captures; it does not prove the server never replied.

| TO PORT | APPLICATION | PREVIOUS APP-ID | ACTION | RULE | SESSION END REASON | BYTES | BYTES SENT | BYTES RECEIVED |
|---|---|---|---|---|---|---|---|---|
| 179 | incomplete | | allow | intrazone-default | aged-out | 312 | 312 | 0 |
| 179 | incomplete | | allow | intrazone-default | aged-out | 312 | 312 | 0 |
| 179 | incomplete | | allow | intrazone-default | aged-out | 312 | 312 | 0 |
| 179 | incomplete | | allow | intrazone-default | aged-out | 312 | 312 | 0 |
| 179 | incomplete | | allow | intrazone-default | aged-out | 312 | 312 | 0 |




©2026 Digital Scepter. All rights reserved. digitalscepter.com

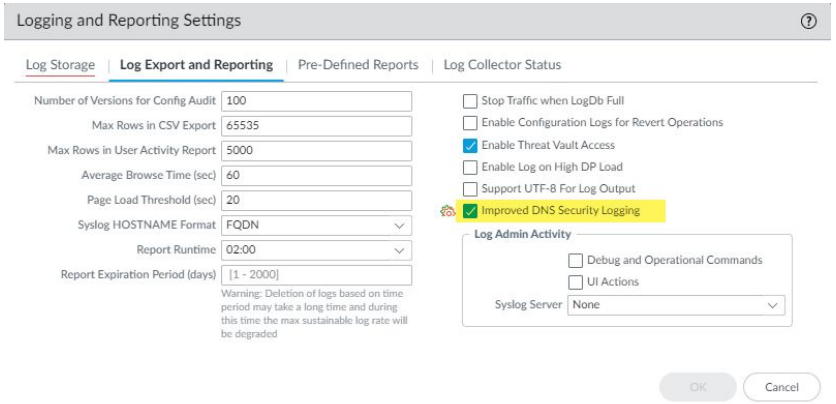
digitalscepter

# Troubleshooting Tools & Techniques

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# DNS Troubleshooting: New Log View

- On PAN-OS 12.1.2 or later, inspect DNS queries in Monitor > Logs > DNS Security.
- Enable Improved DNS Security Logging in Device > Setup > Management > Logging and Reporting Settings.
- Check query, response, action, severity and DNS threat details in the log detail pane.
- Use client IP and queried domain plus time range to tie a DNS failure to the user.




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Transceivers

- New links not coming up? Check transceiver support using these commands The below examples are for slot 1 port 19. If you are on a fixed model, everything is slot 1.
  - show transceiver-detail ethernet1/19

```
zsum@prdfw01a(active)> show transceiver-detail ethernet1/19

----------------------------------------------------------------------------
Detailed Transceiver Information
----------------------------------------------------------------------------
Interface:                              ethernet1/19
Vendor Name:                            CISCO-MOLEX
Vendor Part Number:                     74752-9047       Rev 07
Vendor Serial Number:                   MOC14384932
Pan Supported Optics:                   No
Link Length for copper:                 5 m
Copper cable attenuation:               0 m
Diagnostic Monitor Information:
----------------------------------------------------------------------------
                                    Alarms                  Warnings
                                High          Low         High        Low
----------------------------------------------------------------------------
Temperature           n/a
Voltage               n/a
Current               n/a
TX Power              n/a
RX Power              n/a
----------------------------------------------------------------------------
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Transceivers

- New links not coming up? Check transceiver support using these commands The below examples are for slot 1 port 19. If you are on a fixed model, everything is slot 1.
  - show transceiver-detail ethernet1/19
  - show system state | match sys.s1.p19.phy

```
zsum@prdfw01a(active)> show system state | match sys.s1.p19.phy
sys.s1.p19.phy: { 'link-partner': { 'ability_1000base_t_fdx': False, 'ability_1000base_t_hdx': False, 'ability_100
base_t4': False, 'ability_100base_x_fdx': False, 'ability_100base_x_hdx': False, 'ability_10base_t_fdx': False, 'a
bility_10base_t_hdx': False, 'acknowledge': False, 'asymmetric_pause': False, 'next_page_present': False, 'remote_
fault': False, 'symmetric_pause': False, 'valid': False, }, 'media': SFP-Plus-Copper, 'sfp': { 'Raw-eeprom':
peer.sys.s1.p19.phy: { 'link-partner': { 'ability_1000base_t_fdx': False, 'ability_1000base_t_hdx': False, 'abilit
y_100base_t4': False, 'ability_100base_x_fdx': False, 'ability_100base_x_hdx': False, 'ability_10base_t_fdx': Fals
e, 'ability_10base_t_hdx': False, 'acknowledge': False, 'asymmetric_pause': False, 'next_page_present': False, 're
mote_fault': False, 'symmetric_pause': False, 'valid': False, }, 'media': SFP-Plus-Copper, 'sfp': { 'Raw-eeprom':
zsum@prdfw01a(active)>
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# ARP

- Layer 2 issues can be easily verified by utilizing commands on the firewall CLI
  - “**show arp all**” *or* “**show arp** *<interface-name>*”
  - **ping source** *<interface-ip>* **host** *<host-ip>*
  - **test arp gratuitous interface** *<int-name>* **ip** *<ip-address>*

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# ARP

- “show arp all” *or* “show arp <*interface-name*>”

```
zsum@prdfw01a(active)> clear arp interface ae1.1654

All ARP entries for interface ae1.1654 are cleared.
zsum@prdfw01a(active)> show arp ae1.1654

maximum of entries supported :      3000
default timeout:                    1800 seconds
total ARP entries in table :        0
total ARP entries shown :           0
status: s - static, c - complete, e - expiring, i - incomplete

interface               ip address      hw address        port              status   ttl
-------------------------------------------------------------------------------

zsum@prdfw01a(active)>
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# ARP

- ping source <*interface-ip*> host <*host-ip*>

```
zsum@prdfw01a(active)> ping source 10.1.64.113 host 10.1.64.115
PING 10.1.64.115 (10.1.64.115) from 10.1.64.113 : 56(84) bytes of data.
64 bytes from 10.1.64.115: icmp_seq=1 ttl=128 time=0.912 ms
64 bytes from 10.1.64.115: icmp_seq=2 ttl=128 time=0.814 ms
^C
--- 10.1.64.115 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 62ms
rtt min/avg/max/mdev = 0.814/0.863/0.912/0.049 ms
zsum@prdfw01a(active)>
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# ARP

- Now we will run “show arp <*interface-name*>” again to see if we have a valid or incomplete arp entry

```
zsum@prdfw01a(active)> show arp ae1.1654

maximum of entries supported :      3000
default timeout:                    1800 seconds
total ARP entries in table :        1
total ARP entries shown :           1
status: s - static, c - complete, e - expiring, i - incomplete

interface               ip address      hw address        port              status   ttl
-------------------------------------------------------------------------------------
ae1.1654                10.1.64.115     00:50:56:96:35:ab ae1                       c      1742
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# ARP

- The test arp gratuitous command will send a gratuitous ARP for the specified IP address from the specified interface. The IP address must be on the subnet of that interface
  - test arp gratuitous interface *<int-name>* ip *<ip-address>*

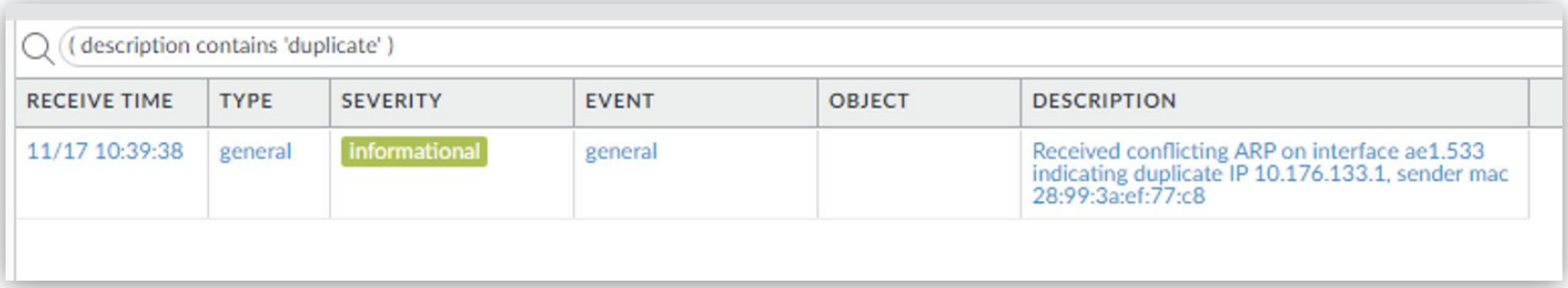
```
zsum@prdfw01a(active)> test arp gratuitous interface ae1.1654 ip 10.1.64.113

1 ARPs were sent
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Duplicate IP Addresses

- System logs will show duplicate IP addresses
- If unsure, change the IP of one of the devices in question while still pinging the IP. If it still pings or shows up in ARP table, it was a duplicate IP.

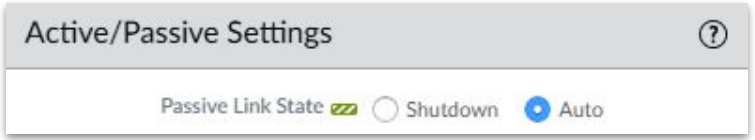


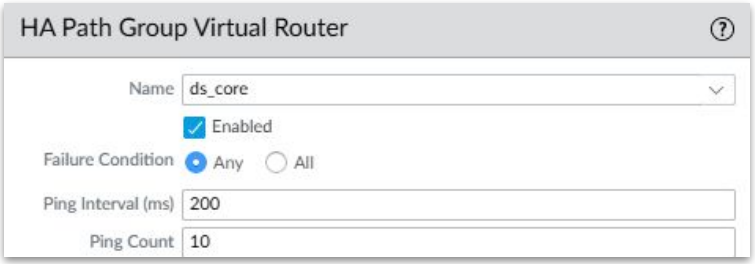

©2026 Digital Scepter. All rights reserved. digitalscepter.com

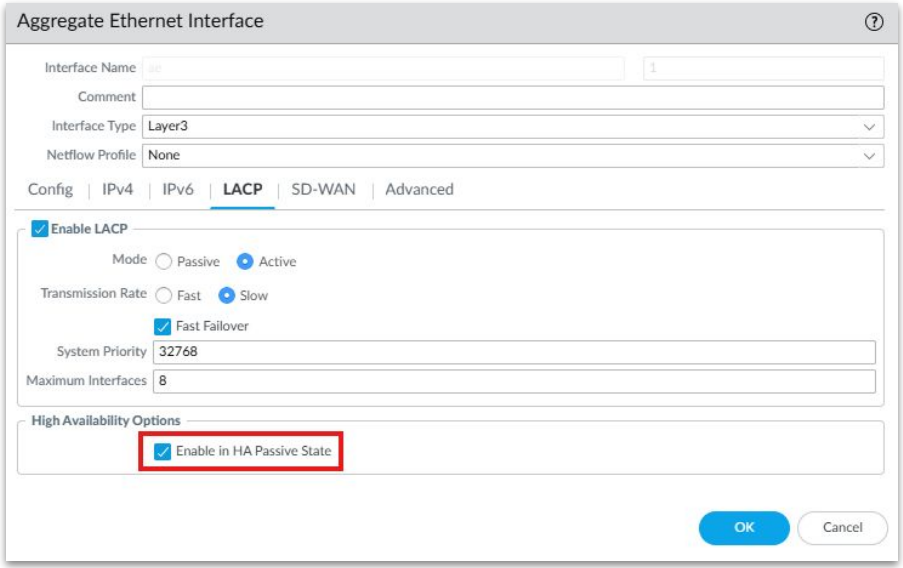
digitalscepter

# Slow HA Failover

- Some common reasons for slow HA failovers from the firewall side
  - Standby interfaces are set to shutdown
  - You are using LACP, but the aggregate is not configured to keep LACP interfaces up on the passive firewall
  - Path monitoring timers




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

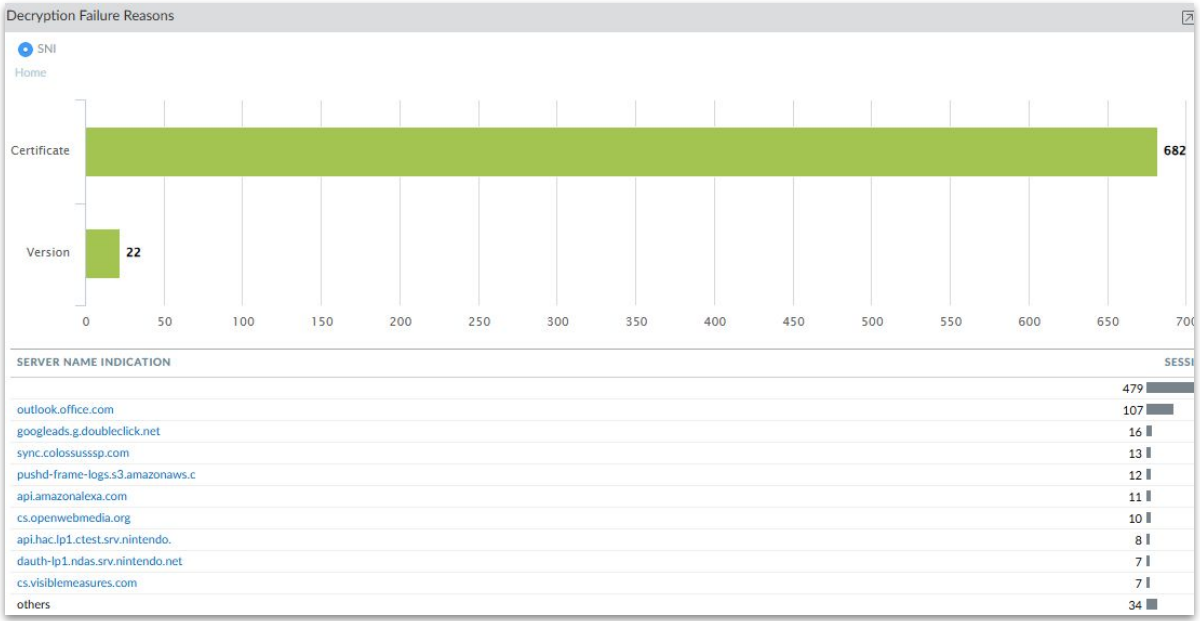
# IPSec VPN: Useful CLI Commands

- show vpn ike-sa — View IKE (Phase 1) security associations
- show vpn ipsec-sa — View IPSec (Phase 2) security associations
- show vpn flow — Check tunnel state and packet counters
- clear vpn ike-sa — Clear an IKE SA to renegotiate
- clear vpn ipsec-sa — Clear an IPSec SA to renegotiate
- test vpn ike-sa — Initiate or test IKE negotiation
- test vpn ipsec-sa — Initiate or test IPSec negotiation
- tail follow yes mp-log ikemgr.log — Follow IKE events
- tail follow yes mp-log ikemgr-ng.log — IKE log on 11.2+

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Decryption Errors

- ACC > SSL Activity > Decryption Failure Reasons
  - Can proactively check for domains failing to be decrypted
  - Choose to create exceptions, or leave them be if the domains are not required




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Decryption Errors

- Monitor > Logs > Decryption.
  - Filter: (err_index neq None) — add source IP or SNI to narrow results.
- Read the Error field and open log details to see why TLS failed.

err_index neq none

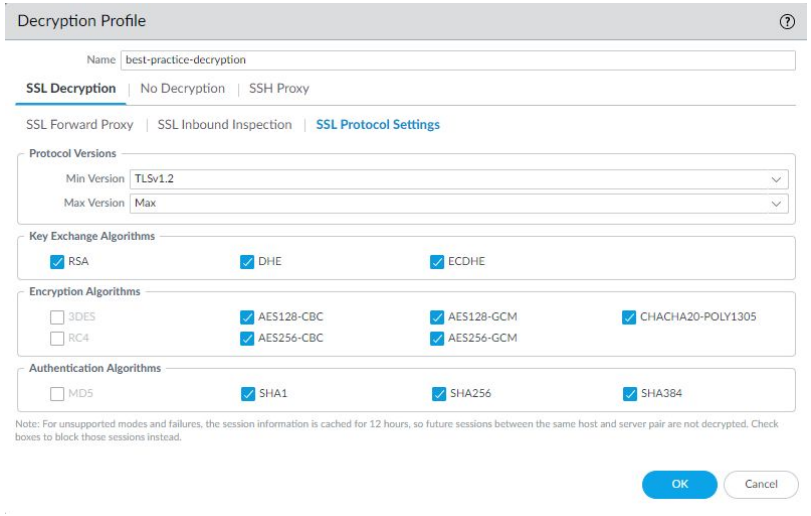
| RECEIVE TIME | APPLICATION | POLICY NAME | SOURCE ZONE | DESTINA... ZONE | PROXY TYPE | SOURCE ADDRESS | SOURCE USER | DESTINATION ADDRESS | SERVER NAME INDICATION | ERROR | ERROR INDEX | DECRYPTION STATUS | DECRYPTION STATUS REASON |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11/16 19:40:22 | incomplete | Decrypt Outbound - IP | inside | outside | Forward | 10.1.3.10 | | 172.215.188.232 | settings-win.data.microso... | TLS Handshake Failure | Protocol | Failed | Not Applicable (No Decrypt; Handshake Failed; Blocked; Succeeded) |
| 11/16 19:40:22 | incomplete | Decrypt Outbound - IP | inside | outside | Forward | 10.1.3.10 | | 172.215.188.232 | settings-win.data.microso... | TLS Handshake Failure | Protocol | Failed | Not Applicable (No Decrypt; Handshake Failed; Blocked; Succeeded) |
| 11/16 19:40:22 | incomplete | Decrypt Outbound - IP | inside | outside | Forward | 10.1.3.10 | | 172.215.188.232 | settings-win.data.microso... | TLS Handshake Failure | Protocol | Failed | Not Applicable (No Decrypt; Handshake Failed; Blocked; Succeeded) |
| 11/16 19:31:22 | incomplete | Decrypt Outbound - IP | inside | outside | Forward | 10.1.3.10 | | 4.150.223.107 | v10.events.data.... | TLS Handshake Failure | Protocol | Failed | Not Applicable (No Decrypt; Handshake Failed; Blocked; Succeeded) |

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Fix TLS or Create a Narrow Exception

- Certificate issue? Repair trust/chain or renew the certificate.
- Version or cipher mismatch? Check the applied Decryption Profile.
- Pinning or client-auth incompatibility? Test a specific no-decrypt rule.
- Retest the workflow; document and review any exception.

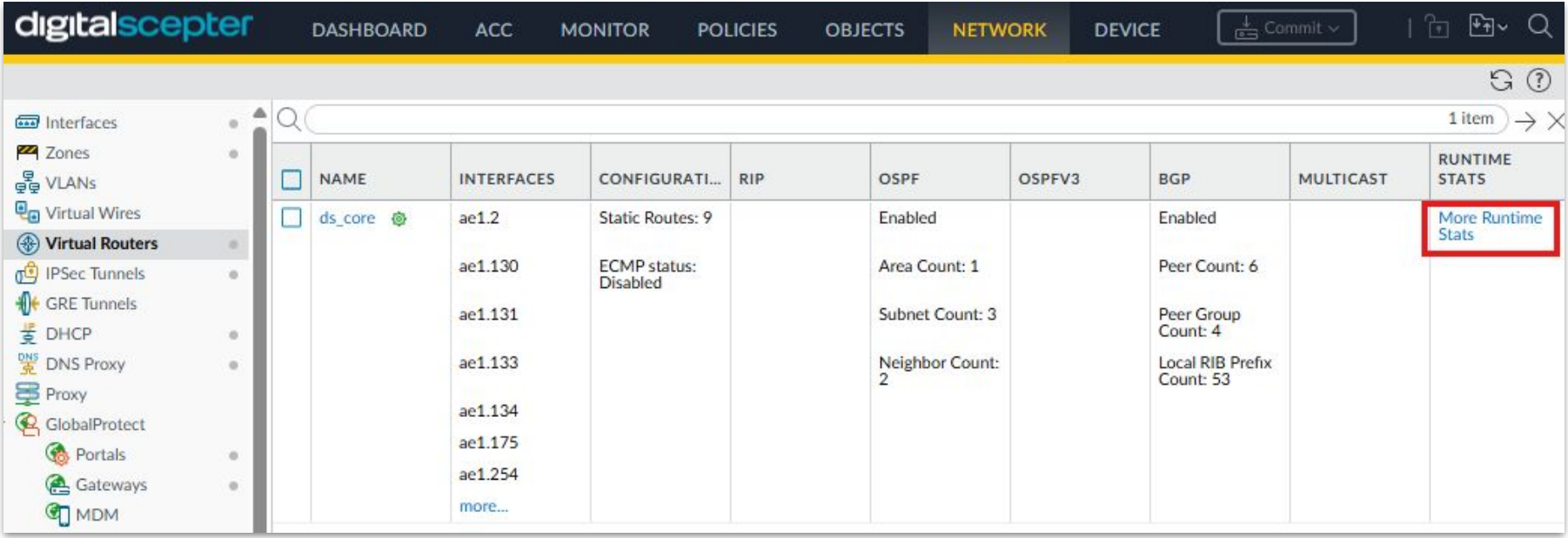



©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Routing Problems

- Start in the correct virtual router or logical router. Verify the destination route, next hop and egress interface in both the route table and forwarding table.

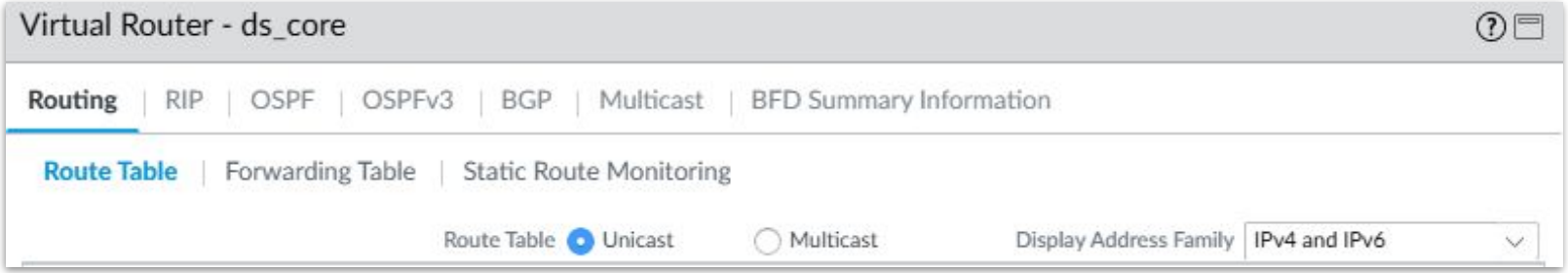



©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Routing Problems

- A learned route is not necessarily the installed forwarding path.
  - The routing table contains connected, static and learned routing information.
  - The forwarding table contains installed routes used for packet forwarding.




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Routing Problems

- Route table versus Forwarding Table

Some examples where the forwarding table will **not** include all routes from the route table:

| Situation | Route Table | Forwarding Table |
|---|---|---|
| Multiple candidate routes | Shows all | Only the best one(s) |
| Admin distance makes one worse | Shows both | Only installs the winning route |
| Next-hop ARP unresolved | Shows route | Not installed in forwarding table |
| Dynamic route learned but overridden by static | Both appear | Only static appears |

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Routing Problems

- Watch for adjacency changes in system logs. Filter: *subtype eq routing*
- Use email or SNMP alerts for high-severity routing events so intermittent flaps are not missed. Filter: (*subtype eq routing and severity geq high)*

( subtype eq routing )

| RECEIVE TIME | TYPE | SEVERITY | EVENT | OBJECT | DESCRIPTION |
|---|---|---|---|---|---|
| 11/17 10:36:57 | routing | high | routed-OSPF-neighbor-down | vr_core | OSPF adjacency with neighbor has gone down. interface ae1.921, neighbor router ID 10.252.0.2, neighbor IP address 10.252.2.4. |
| 11/17 10:36:52 | routing | high | routed-OSPF-neighbor-down | vr_core | OSPF adjacency with neighbor has gone down. interface ae1.921, neighbor router ID 10.252.0.2, neighbor IP address 10.252.2.4. |
| 11/17 10:36:47 | routing | high | routed-OSPF-neighbor-down | vr_core | OSPF adjacency with neighbor has gone down. interface ae1.921, neighbor router ID 10.252.0.2, neighbor IP address 10.252.2.4. |
| 11/17 10:36:46 | routing | high | routed-BGP-peer-left-established | vr_core | BGP peer session left established state.peer name: prdarista01a, peer IP: 10.252.0.1. |
| 11/17 10:36:44 | routing | high | routed-BGP-peer-left-established | vr_core | BGP peer session left established state.peer name: prdarista01b, peer IP: 10.252.0.2. |

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Panorama > Managed Devices > Health

- This often overlooked feature of Panorama provides historical metrics similar to what you'd get from SNMP monitoring
  - Throughput
  - Session utilization
  - Connections per second
  - Dataplane/management plane utilization
  - Packet Buffer/Descriptor utilization
  - etc.

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Panorama > Managed Devices > Health

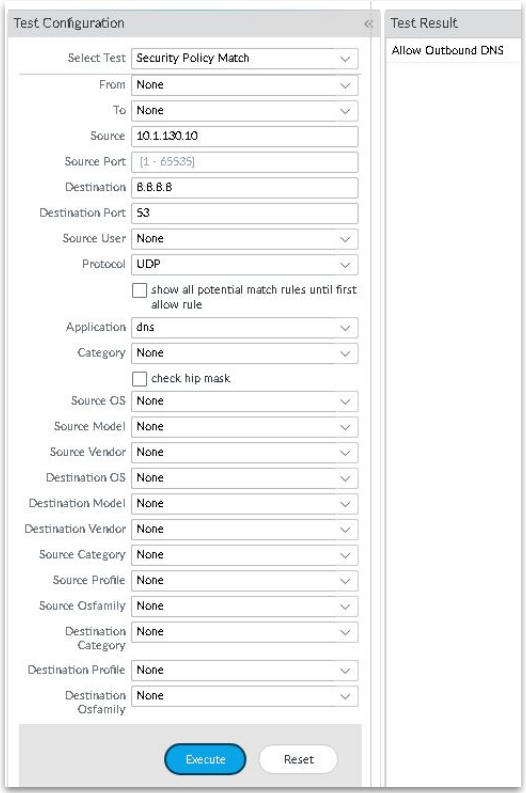


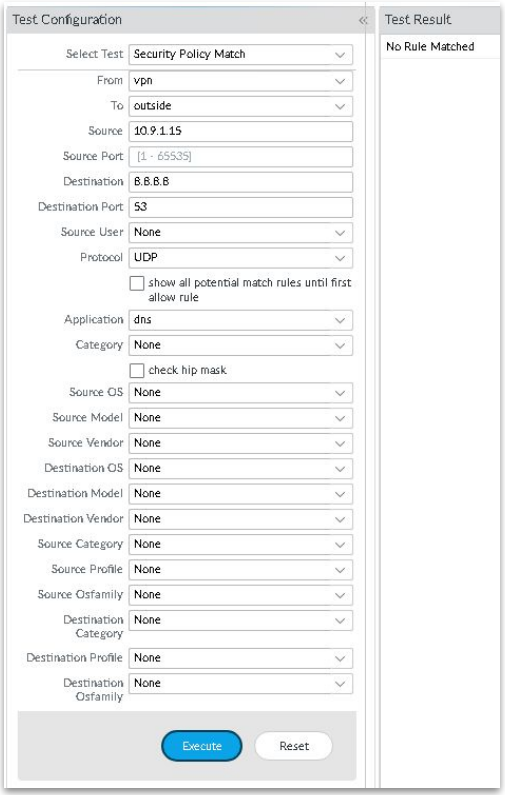

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Testing Policy Matches From the Firewall

- Use the firewall's GUI troubleshooting tools to test security policy, NAT, and PBF matches with a defined flow. Check the selected virtual router and route, then validate the result with a live session or packet capture.



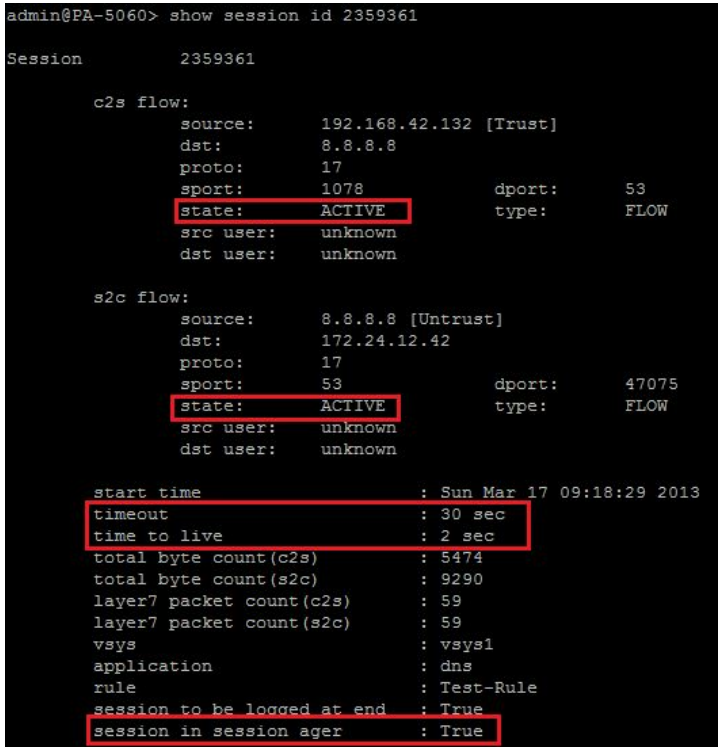




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Use the Session Table to Trace Traffic

- Traffic logs show what happened; the session table shows current flow state and NAT translations.
- Find a user's active sessions with: show session all filter source 10.1.1.1
- Inspect the flow in detail with: show session id <session-id>
- Compare packets in both directions to determine whether replies reach the firewall.




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Real World Scenarios

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# “I can’t get to the website”

- Start in URL Filtering logs: Monitor > Logs > URL Filtering
  - Get their IP Address
  - Query: addr.src in *<users_ip>* and url contains *‘digitalscepter.com’*
  - Action allow? Application look right? Session end reason?
- If there are no logs
  - Can the user resolve the domain?
  - Are there policy denies from the user’s IP address to the internet? (in traffic logs)
- Check session end reason–sometimes everything looks ok, but session-end reason may clue you in to a problem

| GENERATE TIME | TYPE | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | TO PORT | APPLICATION | PREVIOUS APP-ID | ACTION | RULE | SESSION END REASON |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 09/02 08:11:22 | end | outside | outside | 20.171.207.254 | | 199.255.27.72 | 443 | web-browsing | | allow | Allow Internet to GP | resources-unavailable |
| 09/02 05:50:18 | end | outside | outside | 104.248.114.90 | | 199.255.27.72 | 80 | web-browsing | | allow | Allow Internet to GP | resources-unavailable |
| 08/30 00:51:05 | end | outside | outside | 20.171.207.254 | | 199.255.27.72 | 443 | web-browsing | | allow | Allow Internet to GP | resources-unavailable |

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# “I can get to this site, but it should be blocked”

- Start in URL Filtering logs: Monitor > Logs > URL Filtering
  - Get their IP Address
  - Query: addr.src in *<users_ip>* and url contains ‘*digitalscepter.com*’
  - Missing URL logs do not automatically mean traffic is allowed or uninspected. QUIC, ECH, policy settings and decryption can limit URL visibility. Correlate Traffic and Decryption logs before testing a targeted QUIC/ECH control.
  - If a URL log is present, verify the category and custom URL pattern. To match both the base domain and subdomains, include these entries:
    - digitalscepter.com
    - *.digitalscepter.com

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# “I can get to this site, but it should be blocked”

- To block QUIC

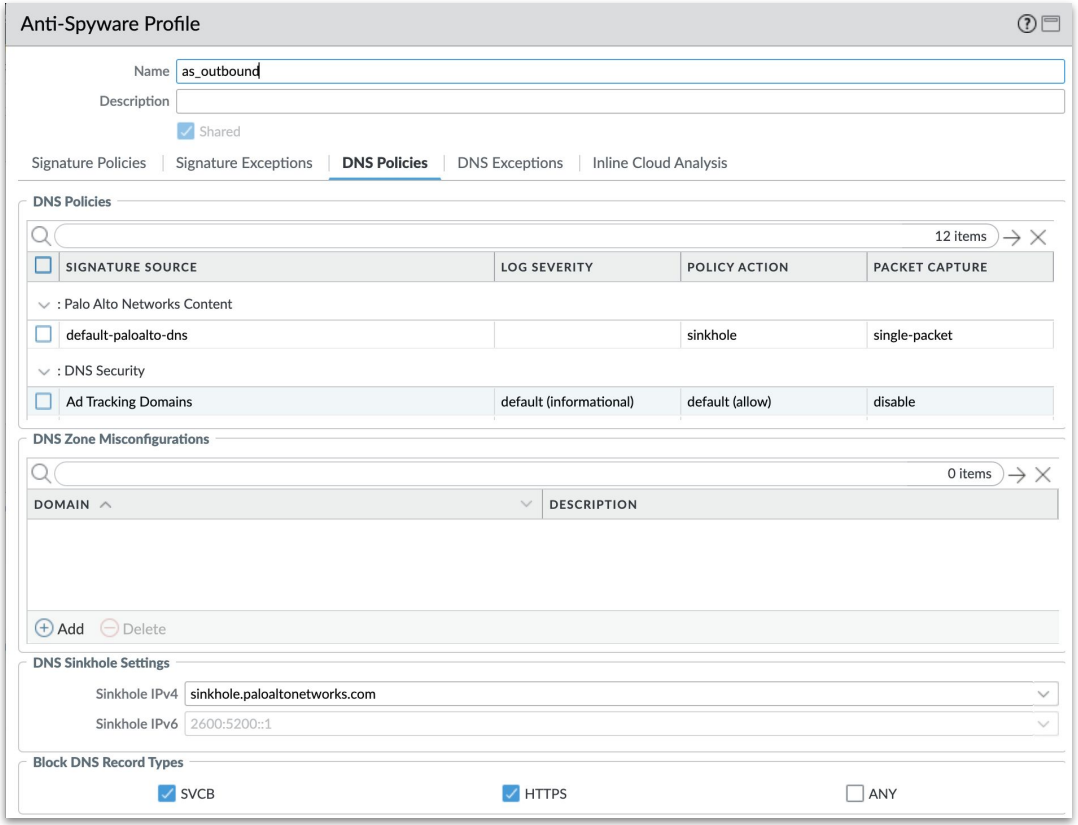
| | Source | | | Destination | | | | |
|---|---|---|---|---|---|---|---|---|
| NAME | ZONE | ADDRESS | USER | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE |
| Block Quic | any | INTERNAL_NETWORKS | any | outside | any | any | quic | any |

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# “I can get to this site, but it should be blocked”

- To block ECH




©2026 Digital Scepter. All rights reserved. digitalscepter.com

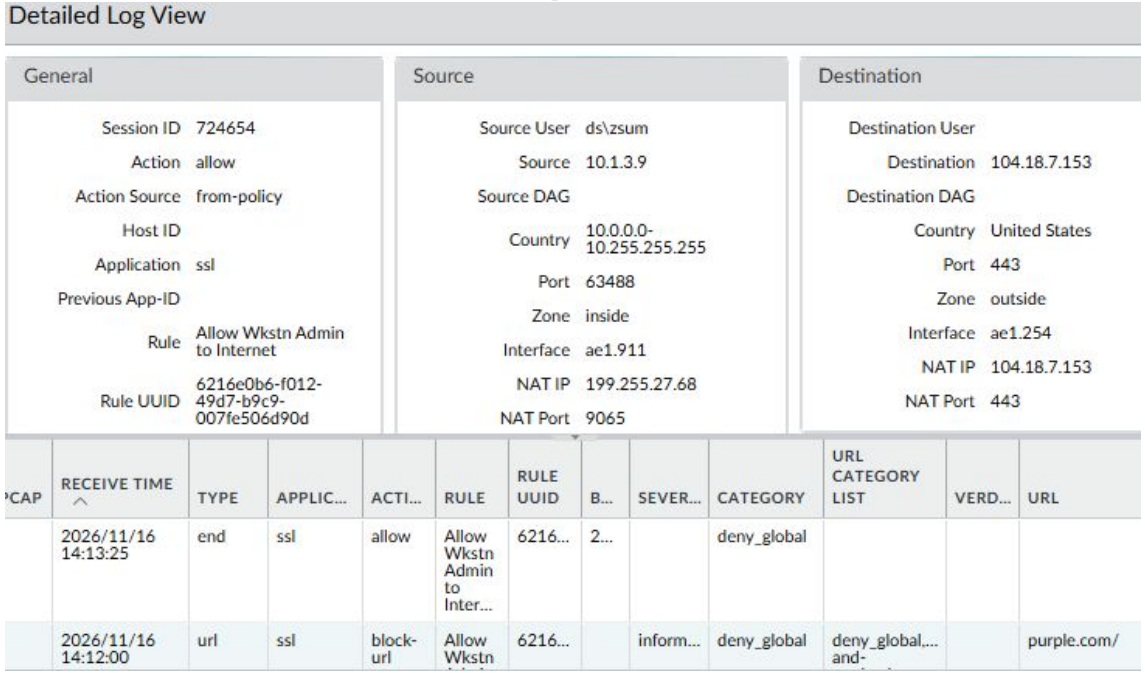
digitalscepter

# Can I Troubleshoot Effectively Test (CITE Test)

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Question 1

- A school user cannot open a website, yet the traffic log shows Allow. Based on the screenshot below, why can the user not get to the website?



Detailed Log View

**General**

| | |
|---|---|
| Session ID | 724654 |
| Action | allow |
| Action Source | from-policy |
| Host ID | |
| Application | ssl |
| Previous App-ID | |
| Rule | Allow Wkstn Admin to Internet |
| Rule UUID | 6216e0b6-f012-49d7-b9c9-007fe506d90d |

**Source**

| | |
|---|---|
| Source User | ds\zsum |
| Source | 10.1.3.9 |
| Source DAG | |
| Country | 10.0.0.0-10.255.255.255 |
| Port | 63488 |
| Zone | inside |
| Interface | ae1.911 |
| NAT IP | 199.255.27.68 |
| NAT Port | 9065 |

**Destination**

| | |
|---|---|
| Destination User | |
| Destination | 104.18.7.153 |
| Destination DAG | |
| Country | United States |
| Port | 443 |
| Zone | outside |
| Interface | ae1.254 |
| NAT IP | 104.18.7.153 |
| NAT Port | 443 |

| PCAP | RECEIVE TIME | TYPE | APPLIC... | ACTI... | RULE | RULE UUID | B... | SEVER... | CATEGORY | URL CATEGORY LIST | VERD... | URL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2026/11/16 14:13:25 | end | ssl | allow | Allow Wkstn Admin to Inter... | 6216... | 2... | | deny_global | | | |
| | 2026/11/16 14:12:00 | url | ssl | block-url | Allow Wkstn | 6216... | | inform... | deny_global | deny_global,... and- | | purple.com/ |

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

## General

| | |
|---|---|
| Session ID | 724654 |
| Action | allow |
| Action Source | from-policy |
| Host ID | |
| Application | ssl |
| Previous App-ID | |
| Rule | Allow Wkstn Admin to Internet |
| Rule UUID | 6216e0b6-f012-49d7-b9c9-007fe506d90d |

## Source

| | |
|---|---|
| Source User | ds\zsum |
| Source | 10.1.3.9 |
| Source DAG | |
| Country | 10.0.0.0-10.255.255.255 |
| Port | 63488 |
| Zone | inside |
| Interface | ae1.911 |
| NAT IP | 199.255.27.68 |
| NAT Port | 9065 |

## Destination

| | |
|---|---|
| Destination User | |
| Destination | 104.18.7.153 |
| Destination DAG | |
| Country | United States |
| Port | 443 |
| Zone | outside |
| Interface | ae1.254 |
| NAT IP | 104.18.7.153 |
| NAT Port | 443 |

| PCAP | RECEIVE TIME | TYPE | APPLIC... | ACTI... | RULE | RULE UUID | B... | SEVER... | CATEGORY | URL CATEGORY LIST | VERD... | URL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2026/11/16 14:13:25 | end | ssl | allow | Allow Wkstn Admin to Inter... | 6216... | 2... | | deny_global | | | |
| | 2026/11/16 14:12:00 | url | ssl | block-url | Allow Wkstn | 6216... | | inform... | deny_global | deny_global,... and- | | purple.com/ |

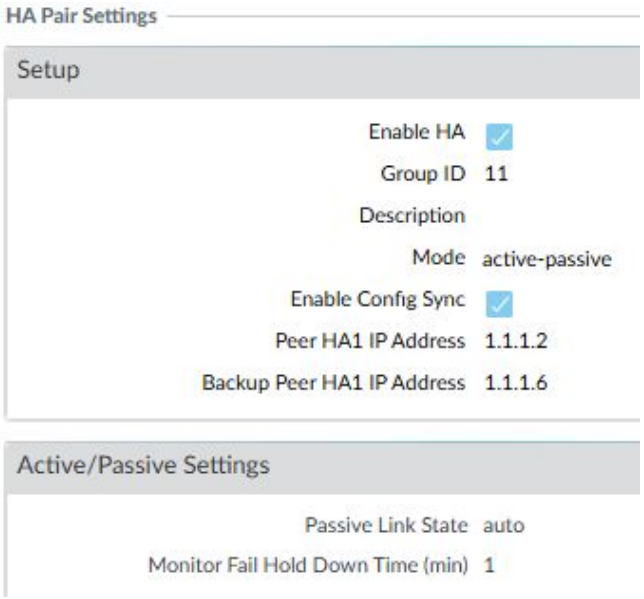
# Answer 1

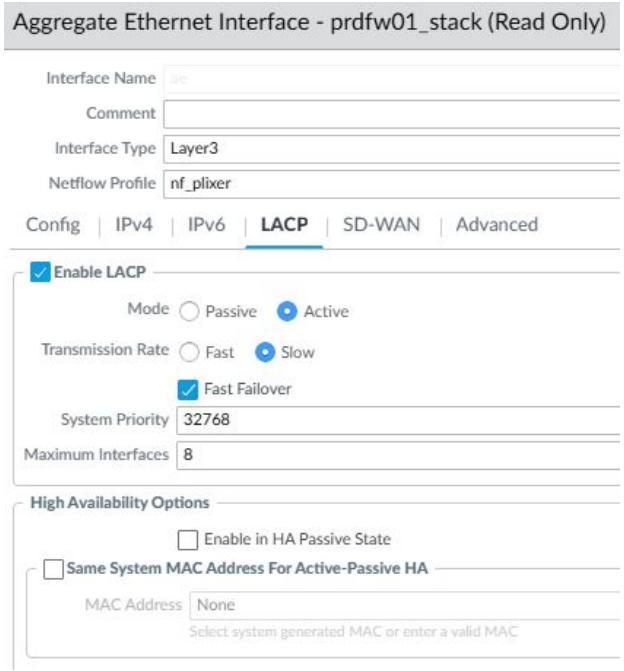
- URL Filtering blocked the URL
- The screenshot shows it being a part of the deny_global custom URL category.
- Fix: If miscategorized, remove the URL from the deny_global custom URL category. Also, confirm predefined URL category action for this URL is not set to block.

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Question 2

- A school district loses internet for approximately 30 seconds during a planned active/passive HA failover. What explains the 30 second outage?




©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

## HA Pair Settings

### Setup

| | |
|---|---|
| Enable HA | ☑ |
| Group ID | 11 |
| Description | |
| Mode | active-passive |
| Enable Config Sync | ☑ |
| Peer HA1 IP Address | 1.1.1.2 |
| Backup Peer HA1 IP Address | 1.1.1.6 |

### Active/Passive Settings

| | |
|---|---|
| Passive Link State | auto |
| Monitor Fail Hold Down Time (min) | 1 |

## Aggregate Ethernet Interface - prdfw01_stack (Read Only)

| | |
|---|---|
| Interface Name | ae |
| Comment | |
| Interface Type | Layer3 |
| Netflow Profile | nf_plixer |

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

☑ **Enable LACP**

| | |
|---|---|
| Mode | ○ Passive ◉ Active |
| Transmission Rate | ○ Fast ◉ Slow |
| | ☑ Fast Failover |
| System Priority | 32768 |
| Maximum Interfaces | 8 |

**High Availability Options**

☐ Enable in HA Passive State

☐ **Same System MAC Address For Active-Passive HA**

MAC Address: None

Select system generated MAC or enter a valid MAC

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Answer 2

- LACP should be enabled in HA Passive state
- This checkbox allows the passive firewall to send and respond to LACPDUs allowing LACP negotiation while in a passive state.
- Fix: Check the box “Enable in HA Passive State”
    - Before applying this change ensure each firewall connects to a unique lag/port-channel on the connected switches. E.g. firewall-1 connects to switch using port-channel1, firewall-2 connects to switch using port-channel2

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Question 3

- Internet works for most classrooms, but intermittent new sessions fail at peak times. Based on the below counters, what is the cause?

```
admin@school-fw01> show counter global filter severity drop

Global counters:
Elapsed time since last sampling: 14.390 seconds

name                          value   rate    severity category aspect    description
flow_policy_deny              9643    652     drop     flow     policy    Session denied by policy
flow_policy_nat               7284    487     drop     flow     session   Session setup: source NAT IP/port allocation error
flow_rcv_dot1q_tag_err        51      0       drop     flow     packet    Received packet with invalid 802.1Q tag
flow_fwd_l3_mcast_drop        3925    261     drop     flow     fwd       Dropped multicast packet (not permitted)
flow_host_service_deny        147     0       drop     flow     host      Packet denied by host service
flow_ipv6_disabled            77      0       drop     flow     packet    IPv6 packet dropped (IPv6 disabled)
flow_no_interface             23      0       drop     flow     fwd       No egress interface for packet
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

```
admin@school-fw01> show counter global filter severity drop

Global counters:
Elapsed time since last sampling: 14.390 seconds

name                      value   rate  severity  category  aspect   description
------------------------------------------------------------------------------------------------
flow_policy_deny           9643    652  drop      flow      policy   Session denied by policy
flow_policy_nat            7284    487  drop      flow      session  Session setup: source NAT IP/port allocation error
flow_rcv_dot1q_tag_err       51      0  drop      flow      packet   Received packet with invalid 802.1Q tag
flow_fwd_l3_mcast_drop     3925    261  drop      flow      fwd      Dropped multicast packet (not permitted)
flow_host_service_deny      147      0  drop      flow      host     Packet denied by host service
flow_ipv6_disabled           77      0  drop      flow      packet   IPv6 packet dropped (IPv6 disabled)
flow_no_interface            23      0  drop      flow      fwd      No egress interface for packet
```

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Answer 3

- Source NAT port exhaustion
- The flow_policy_nat counter indicates the Dynamic IP and Port pool cannot allocate another usable source-port mapping at peak concurrency.
- Fix: Expand or redistribute the public-IP pool, adjust NAT design, and verify failure counters stop rising.

©2026 Digital Scepter. All rights reserved. digitalscepter.com

# Q&A

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter

# Thanks for attending

- Digital Scepter can be reached at digitalscepter.com or via email at sales@digitalscepter.com

©2026 Digital Scepter. All rights reserved. digitalscepter.com

digitalscepter




sales@digitalscepter.com
(888) 299-3718

digitalscepter.com