digitalscepter

Palo Alto Networks Advanced Troubleshooting

November 20th, 2025

Agenda

1. Common Operational Issues
2. Troubleshooting Tips
3. Q&A

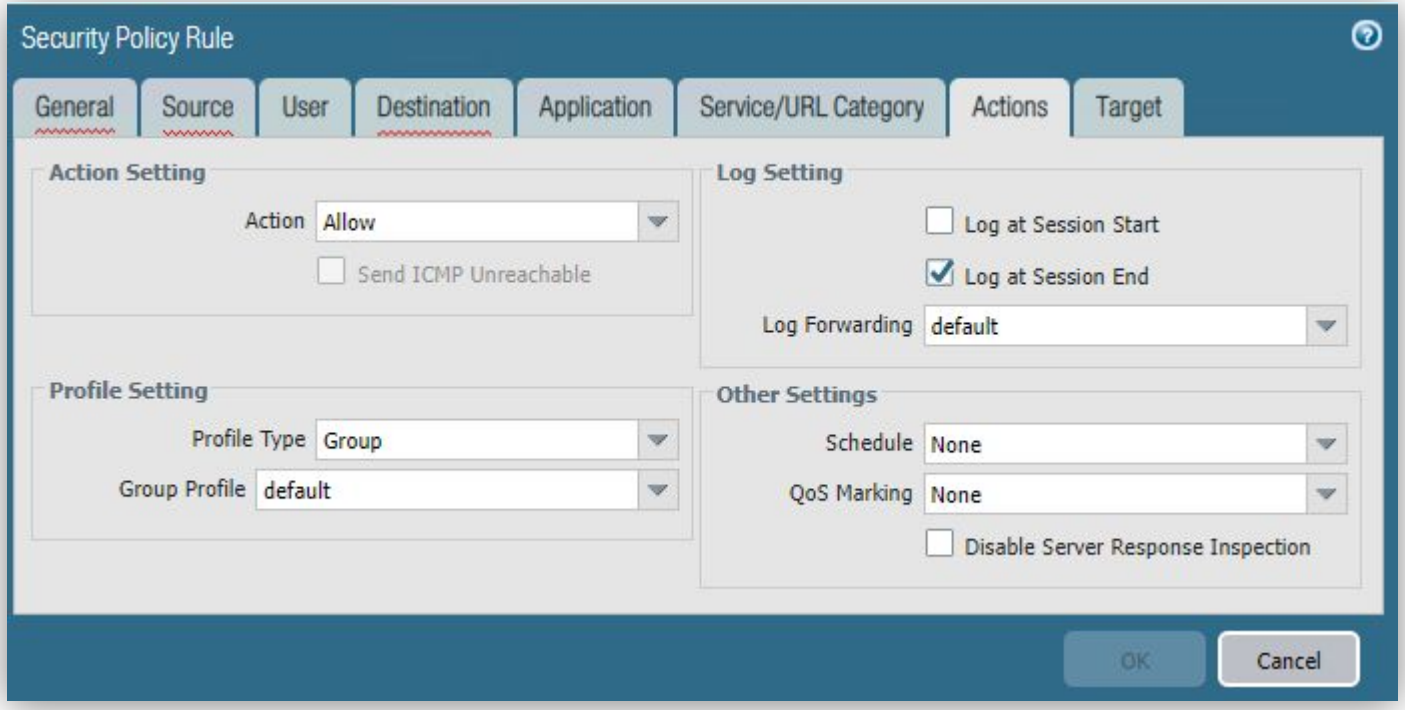
digitalscepter

Common Operational Issues

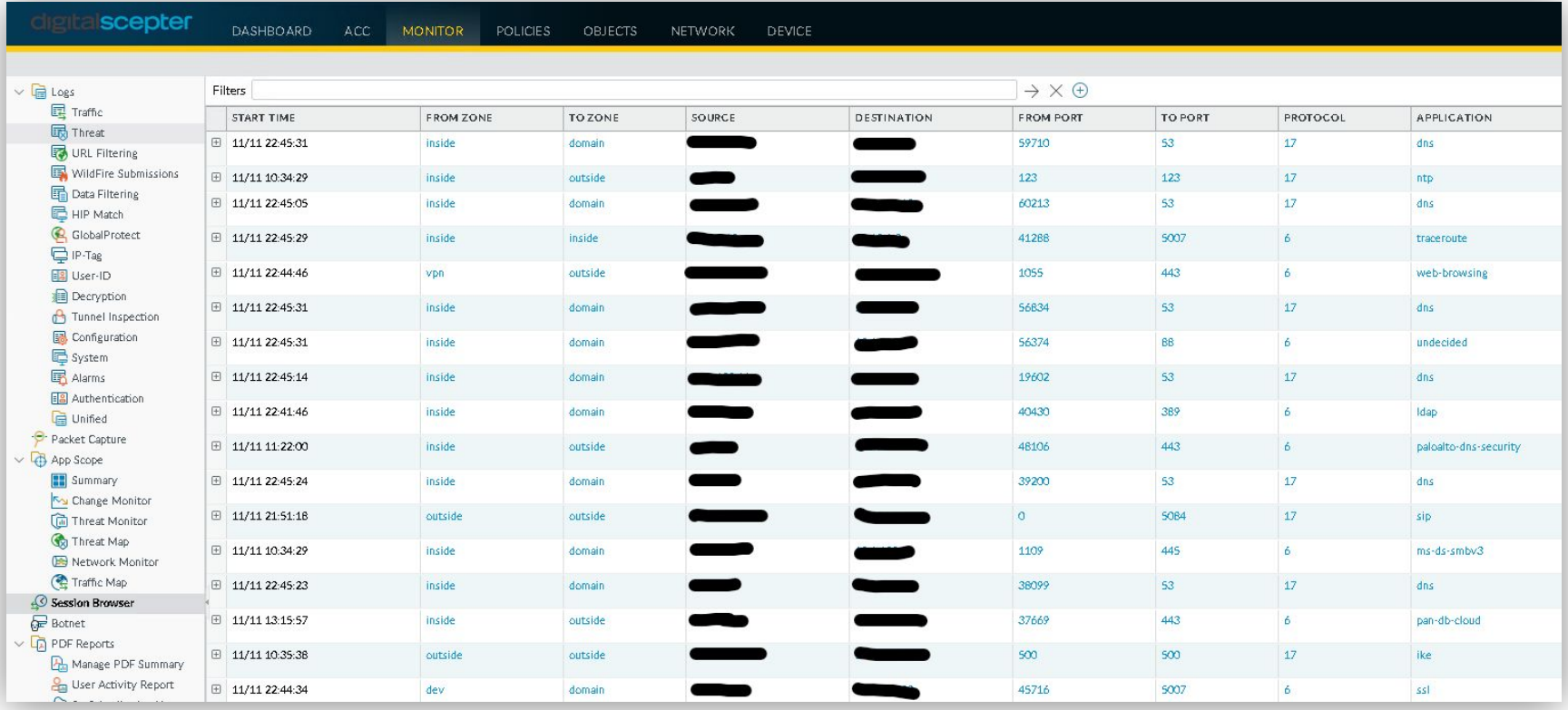
Missing Traffic Logs

- The security policy does not have logging enabled
- If in Panorama, the rule is not configured to forward logs to Panorama
- Default logging is at session end and the session isn't closed yet
- Silent Drops (traffic was dropped prior to security policy match)

Missing Traffic Logs



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

Silent Drops

- Some reasons the firewall may drop traffic without generating a traffic log:
  - Zone Protection Profiles, PBP, DOS Protection
  - IP Block list
  - No route to destination
  - No ARP
  - Etc.

How do you find them?

Silent Drops

- > Show counter global filter severity drop
  - Optional parameters:
    - Delta yes
    - Packet-filter yes
- Threat logs (sometimes)

```
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
```

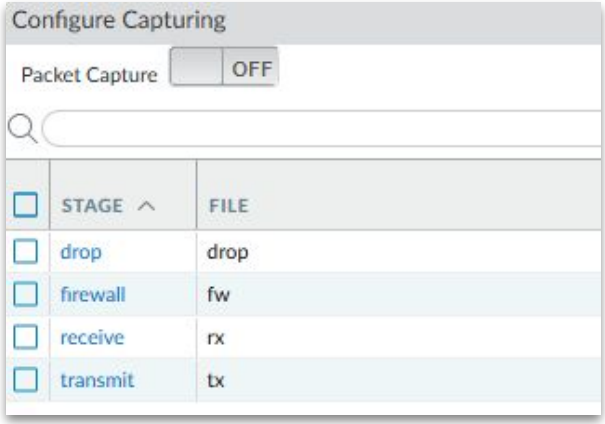
Packet Capture - Missing Packets

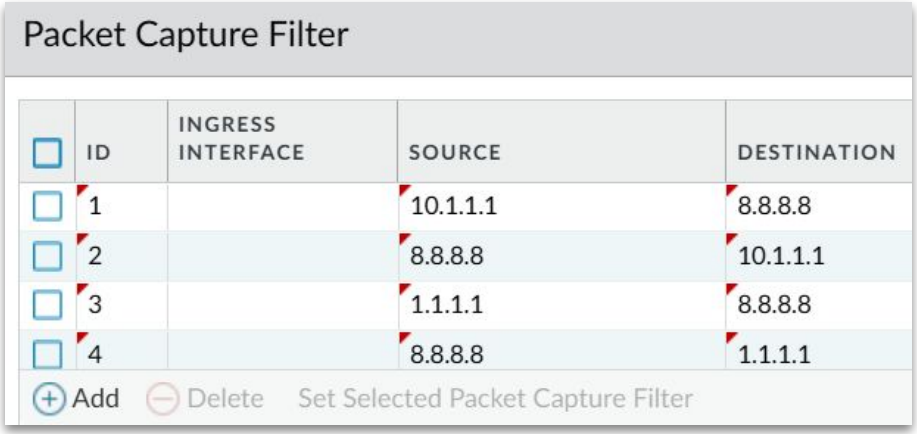
- Packet capture filters need to account for each direction of a particular flow
- NAT also needs to be accounted for
- Captures are done in four stages
  - Transmit
  - Receive
  - Firewall
  - Drop

} These can be combined

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





Packet Capture - Missing Packets

Don’t forget to turn your packet capture off

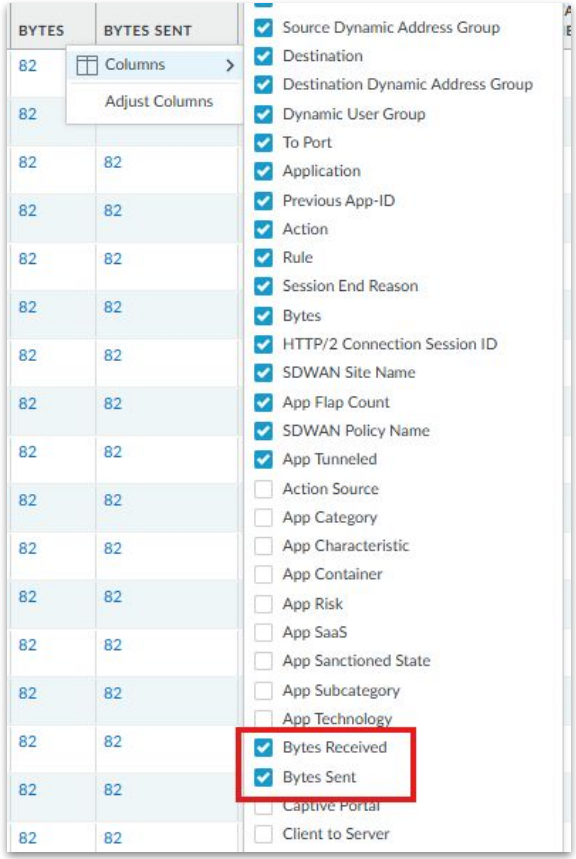
Incomplete Traffic

- It is common to see traffic logs where the application shows as incomplete
- This means a TCP three way handshake either did not complete, or completed and then no other traffic was sent
- Often seen when remote server is not responding or the traffic is dropped upstream of the firewall

Incomplete Traffic

- Add the bytes received and bytes sent column in your traffic log view
- Bytes received = 0 means the firewall never received a reply (some caveats, but generally this is the case)

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



digitalscepter

Troubleshooting Tips

Transceivers

- New links not coming up? Check if the transceiver is supported using a few different commands The below examples are for slot 1 port 19. If you are on a fixed model, everything is slot 1:
  - show transceiver-detail ethernetx1/19
  - show system state | match sys.s1.p19.phy

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>*

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)>
```

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)>
```

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
```

ARP

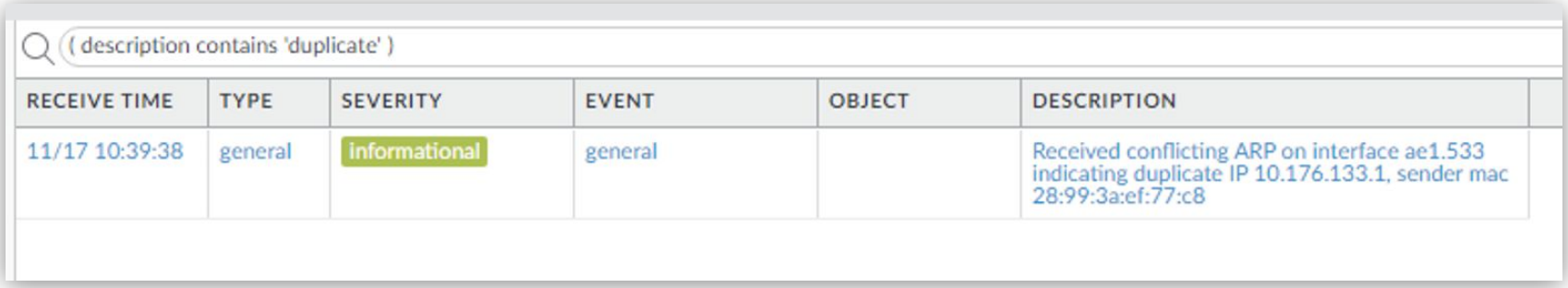
- The test arp gratuitous command will send a gratuitous ARP for the specified IP address from the specified interface. The IP address must be on the subnet of that interface
  - test arp gratuitous interface *<int-name>* ip *<ip-address>*

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

1 ARPs were sent
```

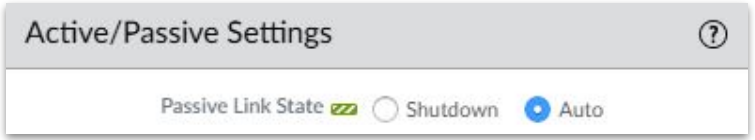
Duplicate IP Addresses

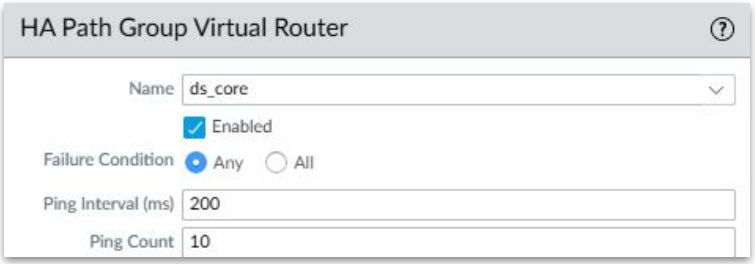
- System logs will show duplicate IP addresses

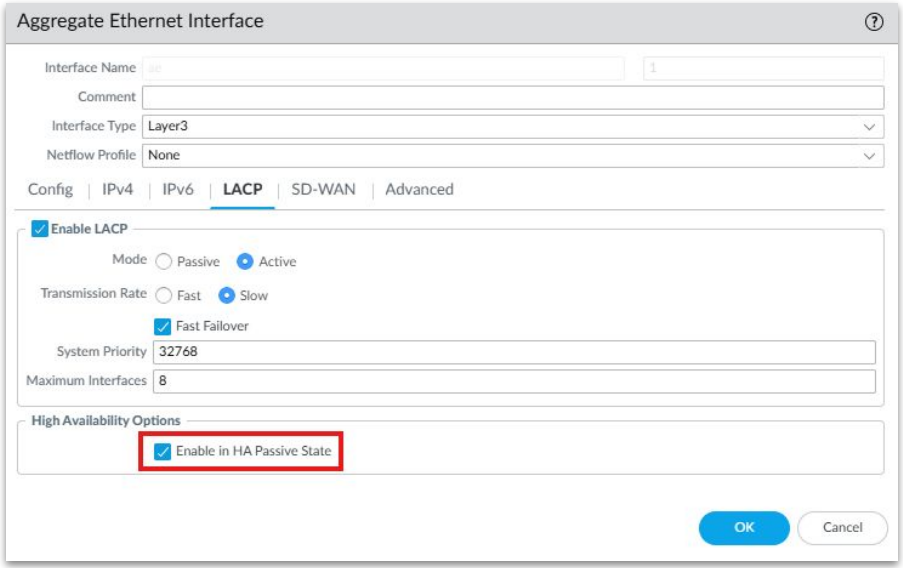


Slow HA Failover

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





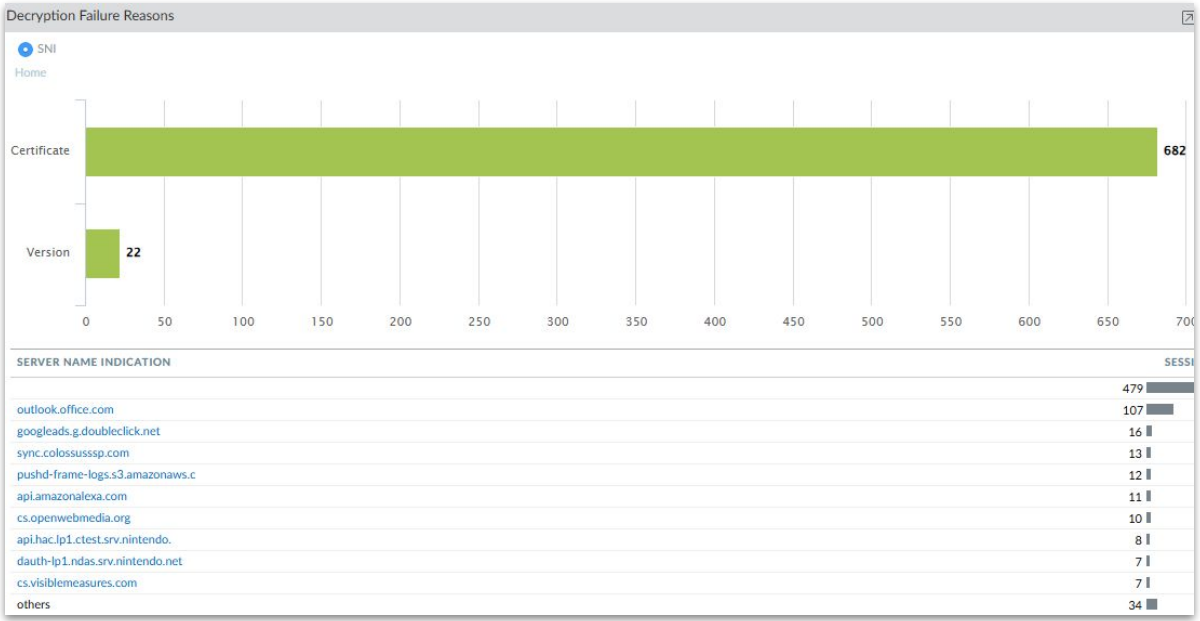


VPN Tunnels

- Clear vpn ike-sa
- Clear vpn ipsec-sa
- Test vpn ike-sa
- Test vpn ipsec-sa
- Tail follow yes mp-log ikemgr.log
- tail follow yes mp-log ikemgr-ng.log (PAN-OS 11.2+)

Decryption Errors

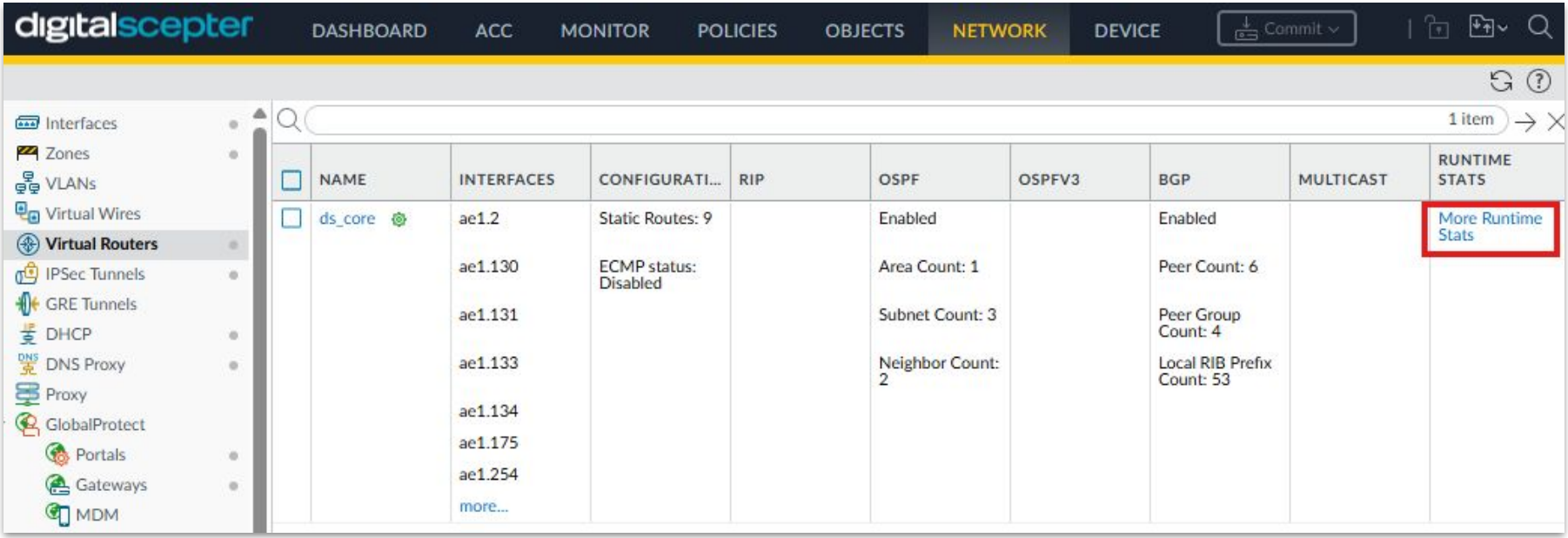
- ACC > SSL Activity > Decryption Failure Reasons
  - Can proactively check for domains failing to be decrypted
  - Choose to create exceptions, or leave them be if the domains are not required



digitalscepter

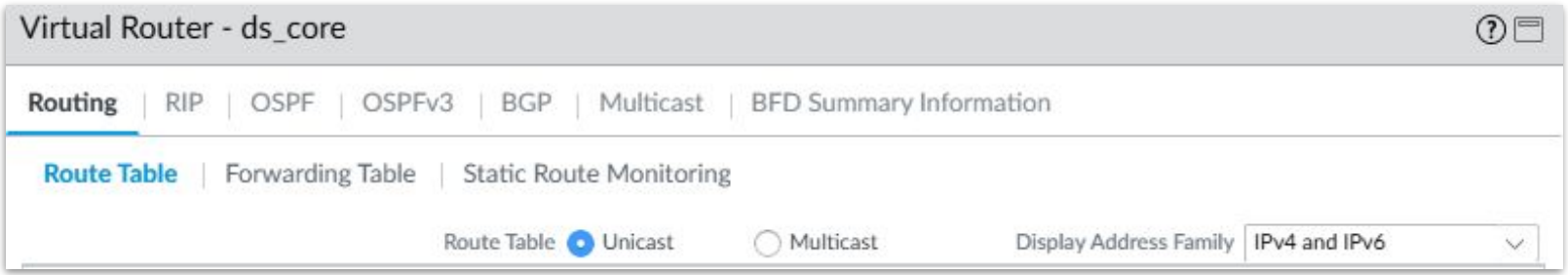
Routing Problems

- Can check route table from GUI or CLI



Routing Problems

- Route table versus Forwarding Table
  - Route table will show all available routes
  - Forwarding table will have the best route that has been installed



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

Routing Problems

- Watch for adjacency changes in system logs
  - Filter: subtype eq routing
- Consider email or snmp alerting on high and critical routing logs

(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.

Panorama > Managed Devices > Health

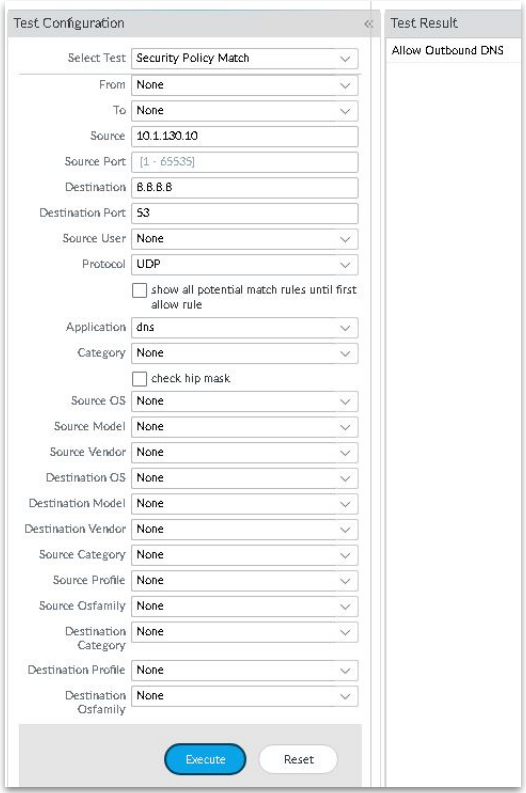
- This often overlooked feature of Panorama provides historical metrics similar to what you'd get from SNMP monitoring
  - Throughput
  - Session utilization
  - Connections per second
  - Dataplane/management plane utilization
  - Packet Buffer/Descriptor utilization
  - etc.

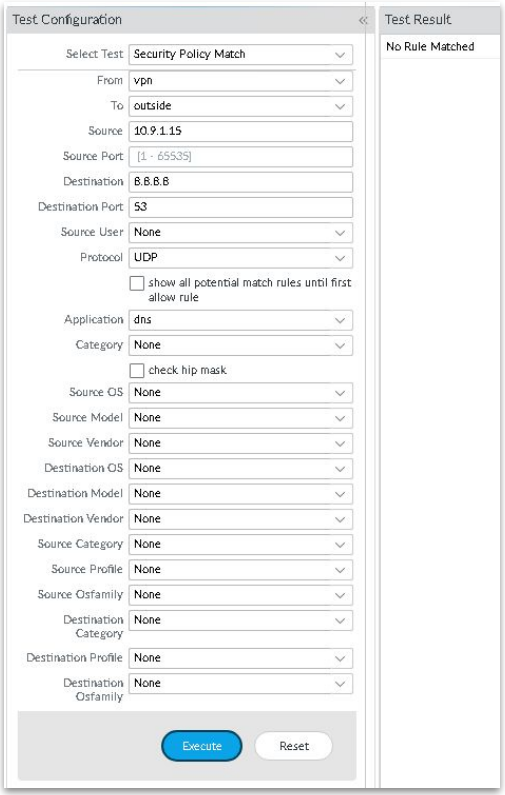
Panorama > Managed Devices > Health

digitalscepter

Troubleshooting

- This feature lets you simulate traffic through the firewall to check for policy matches such as security, nat, pbf and even check routes and send pings/traceroutes–all from the GUI





digitalscepter

“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

“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*’
  - No log? The destination server may be using QUIC or ECH. If so, no URL logs will be generated for that traffic as PAN can not see the http request. Block QUIC and ECH and test again.
  - If log is there, check the URL Categories–if it’s not matching a custom category it may be how it’s formatted. For each URL you want 2 urls in your custom category. Using digitalscepter.com as an example you would have the following:
    - digitalscepter.com
    - *.digitalscepter.com

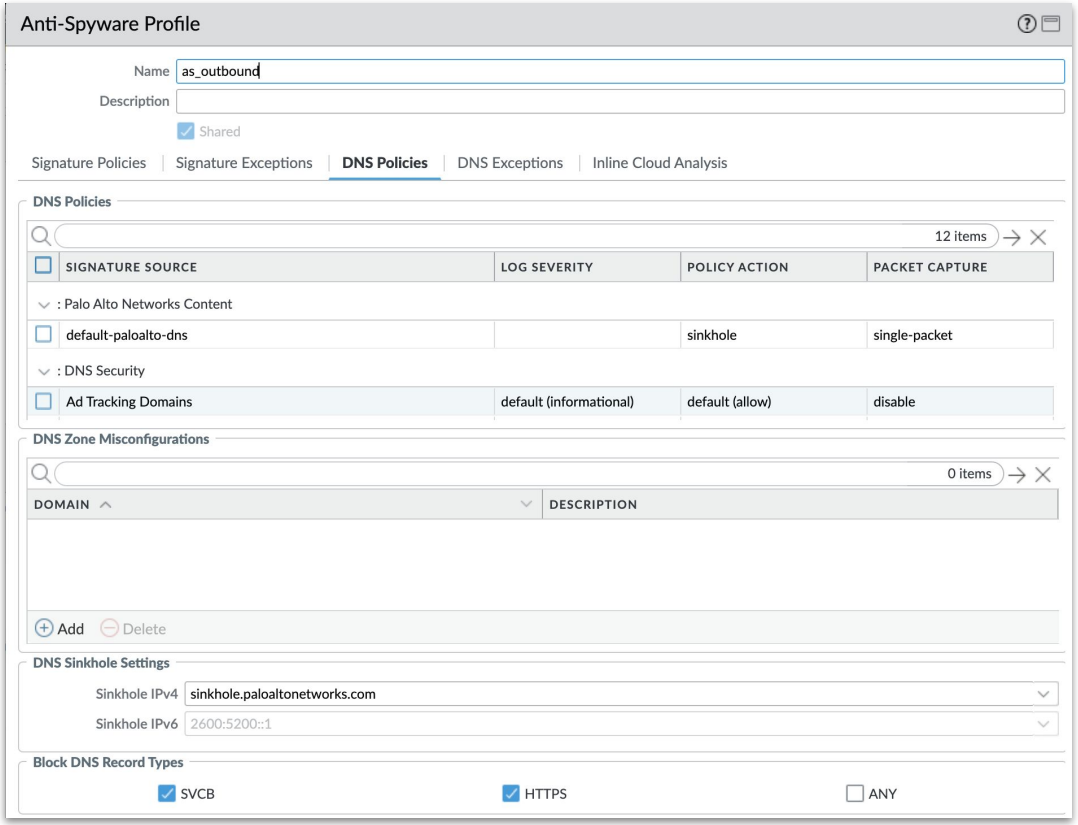
“I can get to this site, but it should be blocked”

- 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

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

- To block ECH



Q&A

digitalscepter

Thanks for attending

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

digitalscepter

sales@digitalscepter.com
(888) 299-3718

digitalscepter.com