

The background of the slide is a photograph of a modern interior space. It features a white ceiling with several long, rectangular, illuminated light fixtures hanging from it. The ceiling has a complex, angular design. In the background, there are dark structural elements and some spotlights. The overall lighting is soft and modern.

digitalscepter

Palo Alto Networks Advanced Troubleshooting

November 20th, 2025

Agenda

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

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

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Target

Action Setting

Action: Allow

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: default

Profile Setting

Profile Type: Group

Group Profile: default

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

OK Cancel

Missing Traffic Logs

digital scepter										
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE										
Logs	Filters → × +									
	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	
Traffic	11/11 22:45:31	inside	domain	██████████	██████████	59710	53	17	dns	
Threat	11/11 10:34:29	inside	outside	██████████	██████████	123	123	17	ntp	
URL Filtering	11/11 22:45:05	inside	domain	██████████	██████████	60213	53	17	dns	
WildFire Submissions	11/11 22:45:29	inside	inside	██████████	██████████	41288	5007	6	traceroute	
Data Filtering	11/11 22:44:46	vpn	outside	██████████	██████████	1055	443	6	web-browsing	
HIP Match	11/11 22:45:31	inside	domain	██████████	██████████	56834	53	17	dns	
GlobalProtect	11/11 22:45:31	inside	domain	██████████	██████████	56374	88	6	undecided	
IP-Tag	11/11 22:45:14	inside	domain	██████████	██████████	19602	53	17	dns	
User-ID	11/11 22:41:46	inside	domain	██████████	██████████	40430	389	6	ldap	
Decryption	11/11 22:00	inside	outside	██████████	██████████	48106	443	6	paloalto-dns-security	
Tunnel Inspection	11/11 22:45:24	inside	domain	██████████	██████████	39200	53	17	dns	
Configuration	11/11 21:51:18	outside	outside	██████████	██████████	0	5084	17	sip	
System	11/11 10:34:29	inside	domain	██████████	██████████	1109	445	6	ms-ds-smbv3	
Alarms	11/11 22:45:23	inside	domain	██████████	██████████	38099	53	17	dns	
Authentication	11/11 13:15:57	inside	outside	██████████	██████████	37669	443	6	pan-db-cloud	
Unified	11/11 10:35:38	outside	outside	██████████	██████████	500	500	17	ike	
Packet Capture	11/11 22:44:34	dev	domain	██████████	██████████	45716	5007	6	ssl	
App Scope										
Summary										
Change Monitor										
Threat Monitor										
Threat Map										
Network Monitor										
Traffic Map										
Session Browser										
Botnet										
PDF Reports										
Manage PDF Summary										
User Activity Report										

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 } These can be combined
 - Firewall
 - Drop

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

Configure Capturing

Packet Capture ☐ OFF

☐	STAGE ^	FILE
☐	drop	drop
☐	firewall	fw
☐	receive	rx
☐	transmit	tx

Packet Capture Filter				
☐	ID	INGRESS INTERFACE	SOURCE	DESTINATION
☐	1		10.1.1.1	8.8.8.8
☐	2		8.8.8.8	10.1.1.1
☐	3		1.1.1.1	8.8.8.8
☐	4		8.8.8.8	1.1.1.1
+ Add - Delete Set Selected Packet Capture Filter				

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



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

Q (description contains 'duplicate')						
RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION	
11/17 10:39:38	general	informational	general		Received conflicting ARP on interface ae1.533 indicating duplicate IP 10.176.133.1, sender mac 28:99:3a:ef:77:c8	

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

Active/Passive Settings

Passive Link State ☒ Shutdown ☐ Auto ☒

HA Path Group Virtual Router

Name ds_core

☒ Enabled

Failure Condition ☒ Any ☐ All

Ping Interval (ms) 200

Ping Count 10

Aggregate Ethernet Interface

Interface Name 1

Comment

Interface Type Layer3

Netflow Profile None

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

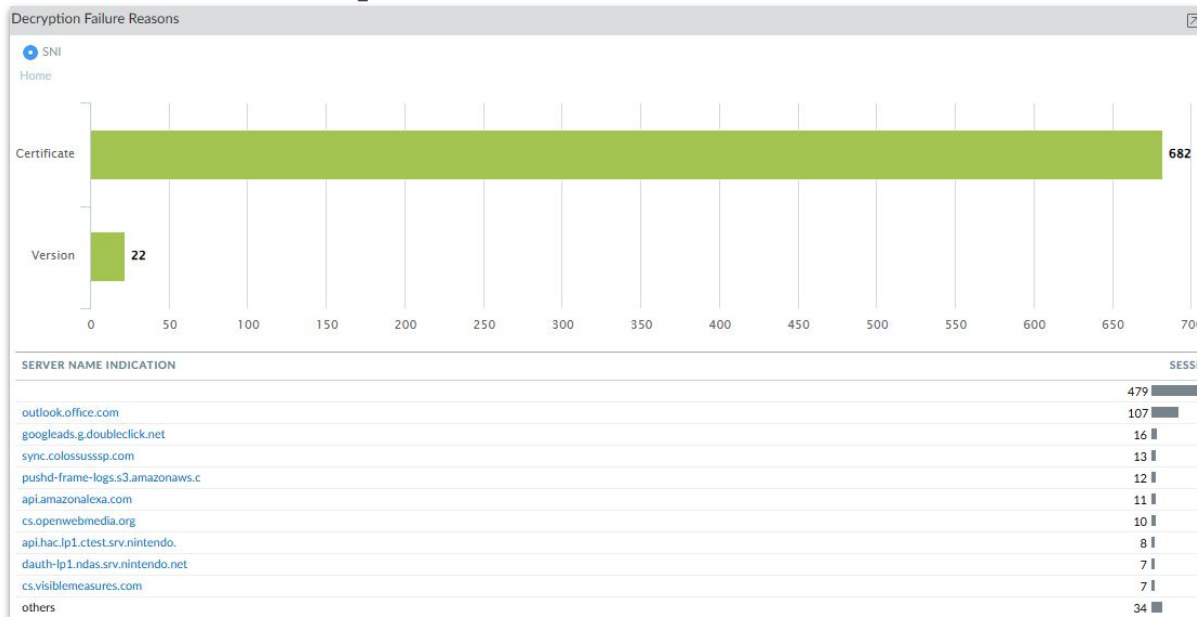
OK Cancel

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+)

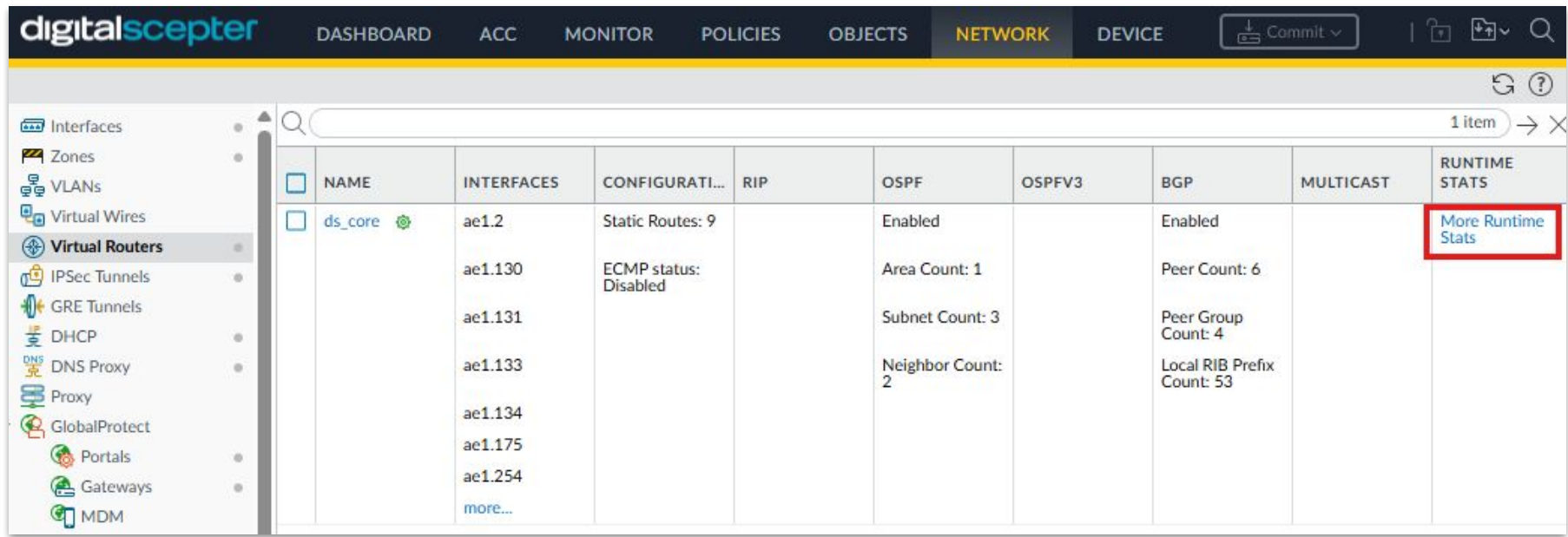
Decryption Errors

- 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



Routing Problems

- Can check route table from GUI or CLI

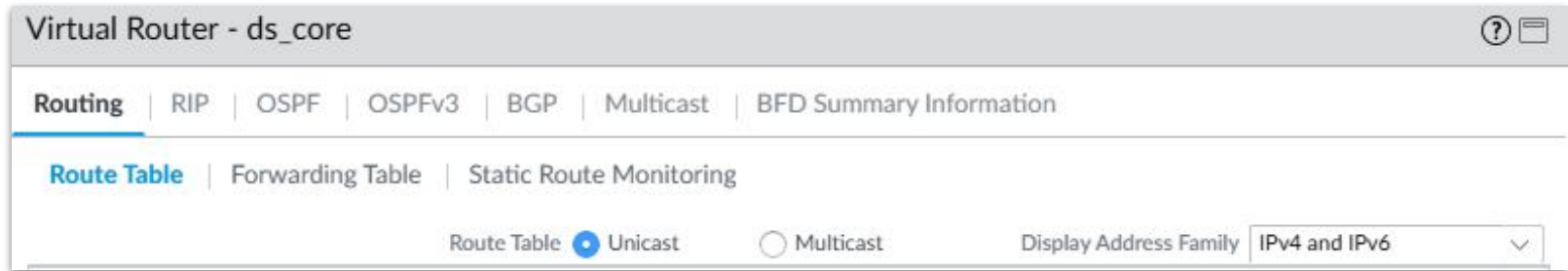


The screenshot displays the DigitalScepter Network configuration interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (active), and DEVICE. A 'Commit' button is visible on the right. The left sidebar lists various network components, with 'Virtual Routers' selected. The main table lists the configuration for the 'ds_core' virtual router, showing its interfaces, configuration status, and runtime statistics. A red box highlights the 'More Runtime Stats' link in the 'RUNTIME STATS' column.

	NAME	INTERFACES	CONFIGURATI...	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
☐	ds_core	ae1.2	Static Routes: 9		Enabled		Enabled		More Runtime Stats
		ae1.130	ECMP status: Disabled		Area Count: 1		Peer Count: 6		
		ae1.131			Subnet Count: 3		Peer Group Count: 4		
		ae1.133			Neighbor Count: 2		Local RIB Prefix Count: 53		
		ae1.134							
		ae1.175							
		ae1.254							
		more...							

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

Q (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



Troubleshooting

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

Test Configuration	Test Result
Select Test: Security Policy Match	Allow Outbound DNS
From: None	
To: None	
Source: 10.1.130.10	
Source Port: [1 - 65535]	
Destination: 8.8.8.8	
Destination Port: 53	
Source User: None	
Protocol: UDP	
☐ show all potential match rules until first allow rule	
Application: dns	
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	
Execute	Reset

Test Configuration	Test Result
Select Test: Security Policy Match	No Rule Matched
From: vpn	
To: outside	
Source: 10.9.1.15	
Source Port: [1 - 65535]	
Destination: 8.8.8.8	
Destination Port: 53	
Source User: None	
Protocol: UDP	
☐ show all potential match rules until first allow rule	
Application: dns	
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	
Execute	Reset

"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

NAME	Source			Destination			APPLICATION	SERVICE
	ZONE	ADDRESS	USER	ZONE	ADDRESS	DEVICE		
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

Anti-Spyware Profile

Name:

Description:

☒ Shared

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions | Inline Cloud Analysis

DNS Policies

12 items → ×

☐	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
▼	Palo Alto Networks Content			
☐	default-paloalto-dns		sinkhole	single-packet
▼	DNS Security			
☐	Ad Tracking Domains	default (informational)	default (allow)	disable

DNS Zone Misconfigurations

0 items → ×

DOMAIN ^	DESCRIPTION
----------	-------------

+ Add - Delete

DNS Sinkhole Settings

Sinkhole IPv4:

Sinkhole IPv6:

Block DNS Record Types

☒ SVCB ☒ HTTPS ☐ ANY

Q&A

Thanks for attending

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

A photograph of a modern interior space, possibly a museum or gallery, with a teal color overlay. The scene features several long, rectangular light fixtures hanging from the ceiling, and a few spotlights are visible on the right side. The overall aesthetic is clean and contemporary.

digitalscepter

sales@digitalscepter.com
(888) 299-3718

digitalscepter.com