English

CCDC Palo Alto Playbook V2.0

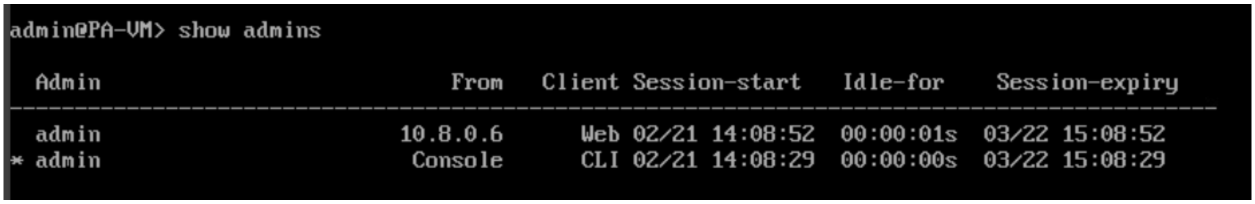
** Create a saved configuration snapshot often incase HTF **

General Hardening:

1. Change admin passwords
2. Logout logged in administrators
3. Disable insecure services on management interface
4. Remove management profiles on external interfaces
5. Create security policies

Incident Response:

Use show admins to check for remote sessions to both console and webUI.



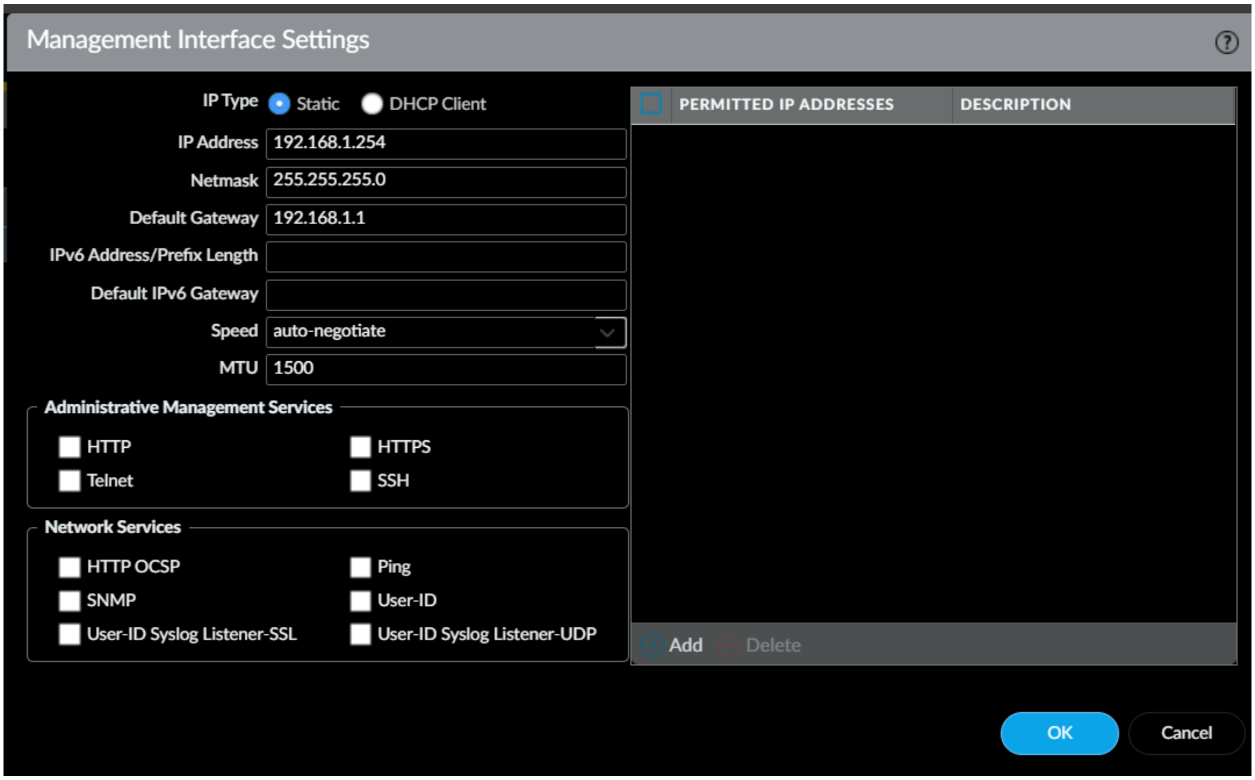
```
admin@PA-VM> show admins

  Admin                              From   Client Session-start   Idle-for    Session-expiry
---------------------------------------------------------------------------------------------
  admin                          10.8.0.6      Web 02/21 14:08:52  00:00:01s  03/22 15:08:52
* admin                           Console      CLI 02/21 14:08:29  00:00:00s  03/22 15:08:29
```

Remove all sessions: ‘> delete admin-sessions ’

> delete admin-sessions username <username>

Regaining GUI Access:

If you committed something like this by accident:



Management Interface Settings

IP Type	● Static ○ DHCP Client
IP Address	192.168.1.254
Netmask	255.255.255.0
Default Gateway	192.168.1.1
IPv6 Address/Prefix Length	
Default IPv6 Gateway	
Speed	auto-negotiate
MTU	1500

Administrative Management Services

□ HTTP □ HTTPS
□ Telnet □ SSH

Network Services

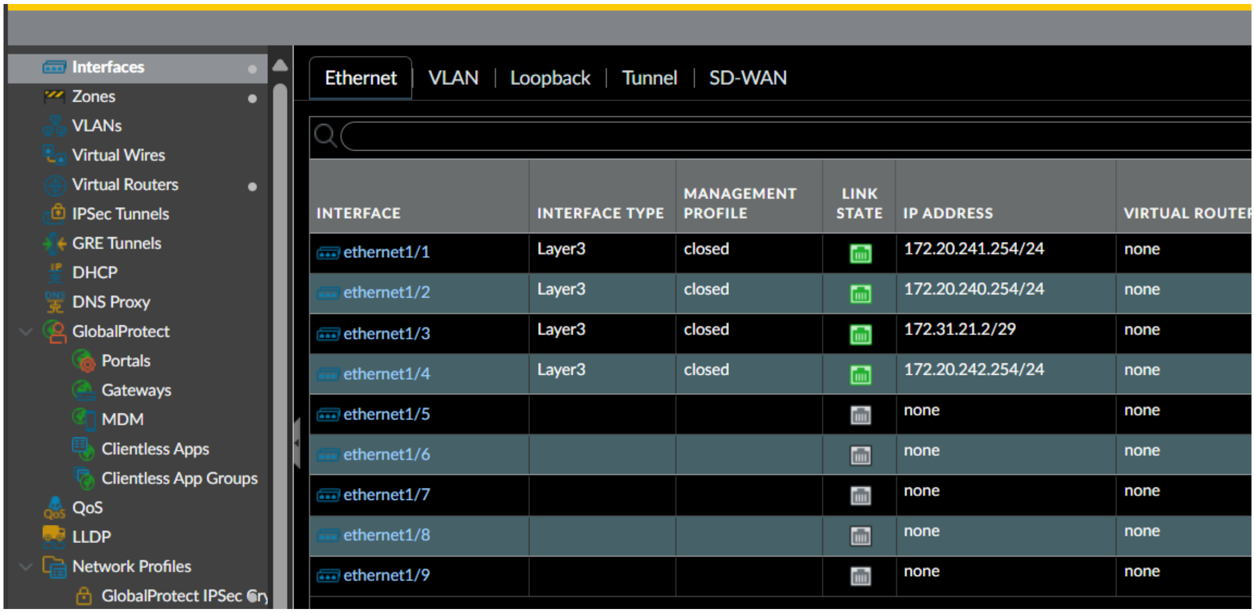
□ HTTP OCSP □ Ping
□ SNMP □ User-ID
□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION

# Set deviceconfig system service disable-https no

# commit

If you configured all your interfaces to block outside administration.

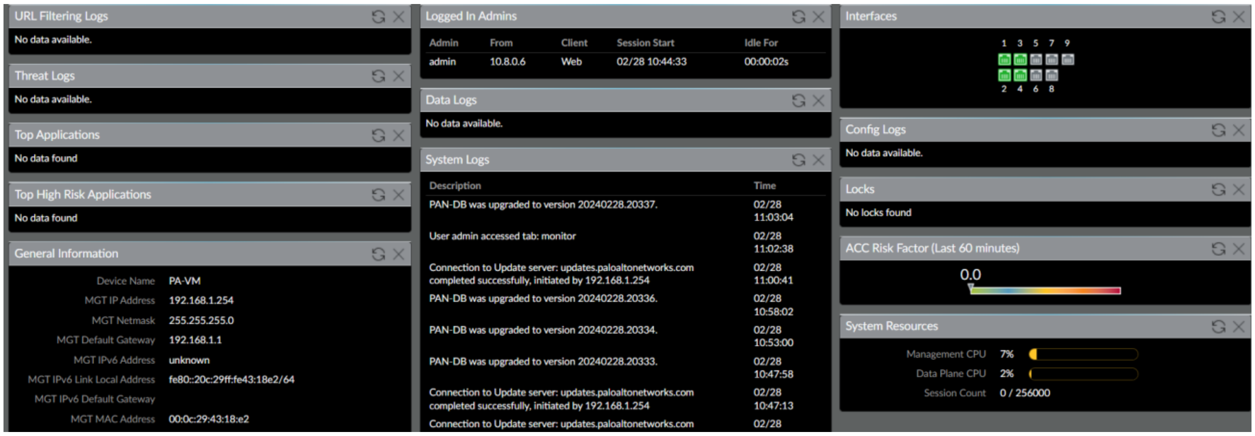


INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER
ethernet1/1	Layer3	closed	🟩	172.20.241.254/24	none
ethernet1/2	Layer3	closed	🟩	172.20.240.254/24	none
ethernet1/3	Layer3	closed	🟩	172.31.21.2/29	none
ethernet1/4	Layer3	closed	🟩	172.20.242.254/24	none
ethernet1/5			▨	none	none
ethernet1/6			▨	none	none
ethernet1/7			▨	none	none
ethernet1/8			▨	none	none
ethernet1/9			▨	none	none

# set network interface ethernet ethernet1/4 layer3 interface-management-profile open-mgmt

Troubleshooting Steps

1. Dashboard Tab



URL Filtering Logs

No data available.

Threat Logs

No data available.

Top Applications

No data found

Top High Risk Applications

No data found

General Information

Device Name	PA-VM
MGT IP Address	192.168.1.254
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.1.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::20c:29ff:fe43:18e2/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:0c:29:43:18:e2

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	10.8.0.6	Web	02/28 10:44:33	00:00:02s

Data Logs

No data available.

System Logs

Description	Time
PAN-DB was upgraded to version 20240228.20337.	02/28 11:03:04
User admin accessed tab: monitor	02/28 11:02:38
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	02/28 11:00:41
PAN-DB was upgraded to version 20240228.20336.	02/28 10:58:02
PAN-DB was upgraded to version 20240228.20334.	02/28 10:53:00
PAN-DB was upgraded to version 20240228.20333.	02/28 10:47:58
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	02/28 10:47:13
Connection to Update server: updates.paloaltonetworks.com	02/28

Interfaces

Config Logs

No data available.

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

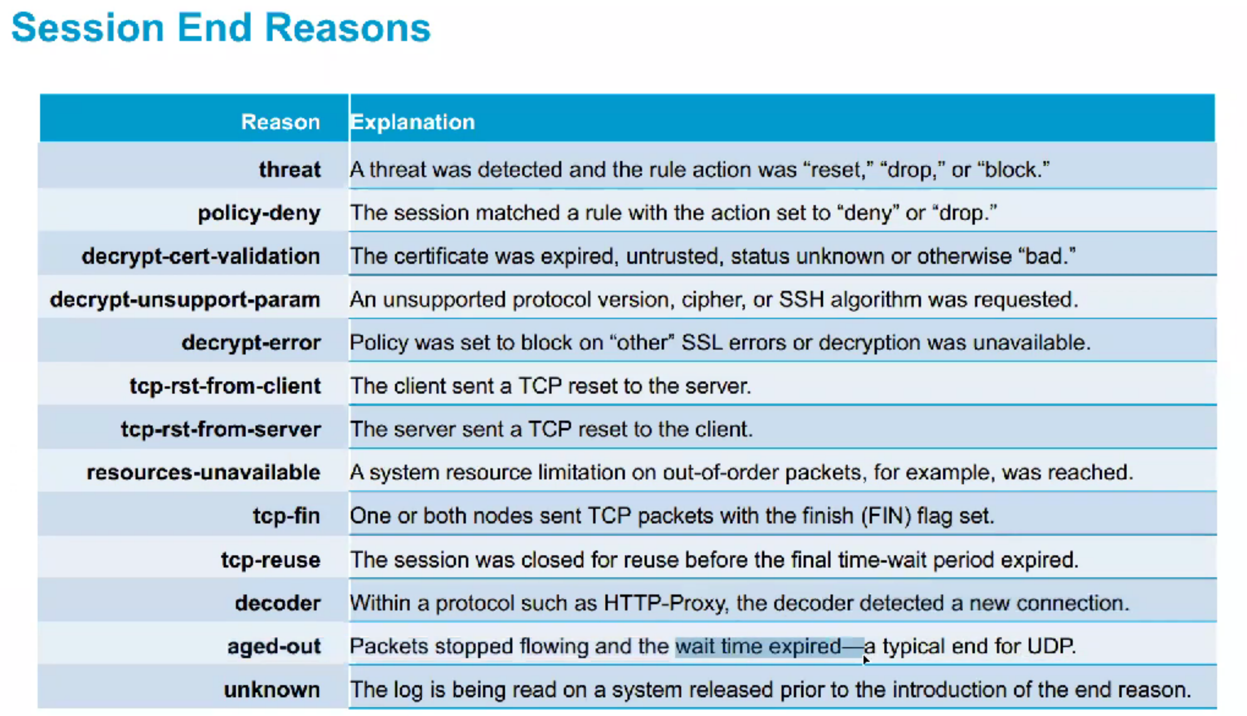
System Resources

Management CPU	7%
Data Plane CPU	2%
Session Count	0 / 256000

Various widgets allow for quick display of interfaces up/down and some logs

2. Monitor Tab - Threat and Traffic

It is typical for UDP traffic to display end-reason 'aged=out'



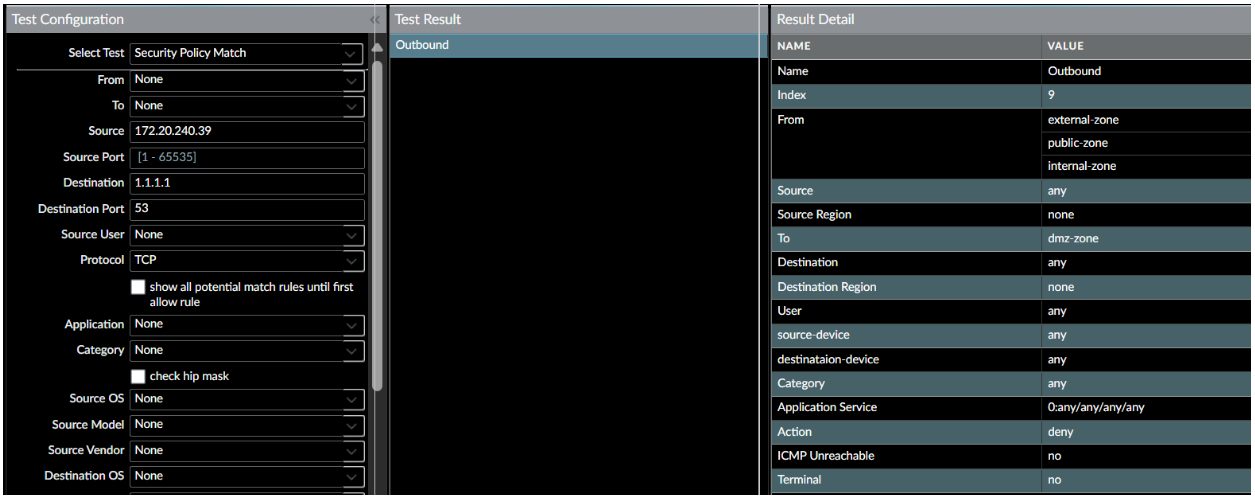
Session End Reasons

Reason	Explanation
threat	A threat was detected and the rule action was "reset," "drop," or "block."
policy-deny	The session matched a rule with the action set to "deny" or "drop."
decrypt-cert-validation	The certificate was expired, untrusted, status unknown or otherwise "bad."
decrypt-unsupport-param	An unsupported protocol version, cipher, or SSH algorithm was requested.
decrypt-error	Policy was set to block on "other" SSL errors or decryption was unavailable.
tcp-rst-from-client	The client sent a TCP reset to the server.
tcp-rst-from-server	The server sent a TCP reset to the client.
resources-unavailable	A system resource limitation on out-of-order packets, for example, was reached.
tcp-fin	One or both nodes sent TCP packets with the finish (FIN) flag set.
tcp-reuse	The session was closed for reuse before the final time-wait period expired.
decoder	Within a protocol such as HTTP-Proxy, the decoder detected a new connection.
aged-out	Packets stopped flowing and the wait time expired—a typical end for UDP.
unknown	The log is being read on a system released prior to the introduction of the end reason.

3. Ping

Ping command available via cli or through GUI

4. Test Matching Security Policies



Test Configuration

Select Test	Security Policy Match
From	None
To	None
Source	172.20.240.39
Source Port	[1 - 65535]
Destination	1.1.1.1
Destination Port	53
Source User	None
Protocol	TCP
	□ show all potential match rules until first allow rule
Application	None
Category	None
	□ check hip mask
Source OS	None
Source Model	None
Source Vendor	None
Destination OS	None

Test Result

Outbound

Result Detail

NAME	VALUE
Name	Outbound
Index	9
From	external-zone public-zone internal-zone
Source	any
Source Region	none
To	dmz-zone
Destination	any
Destination Region	none
User	any
source-device	any
destinataion-device	any
Category	any
Application Service	0:any/any/any/any
Action	deny
ICMP Unreachable	no
Terminal	no

5. Packet Capture

CLI packet capture

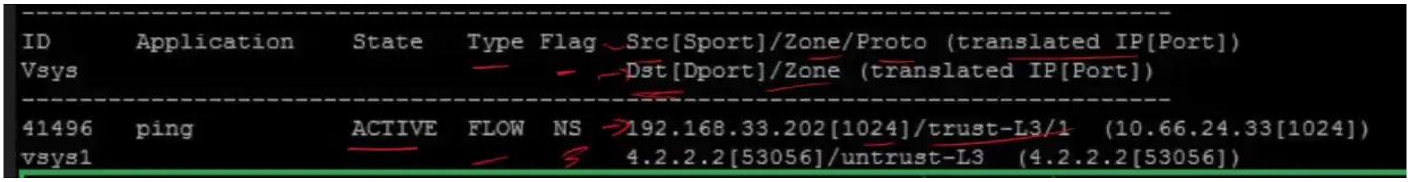
> tcpdump – capture packets on management interface

> view-pcap – view packet capture files generated on the firewall

Display current sessions

> show sessions all filter [?]

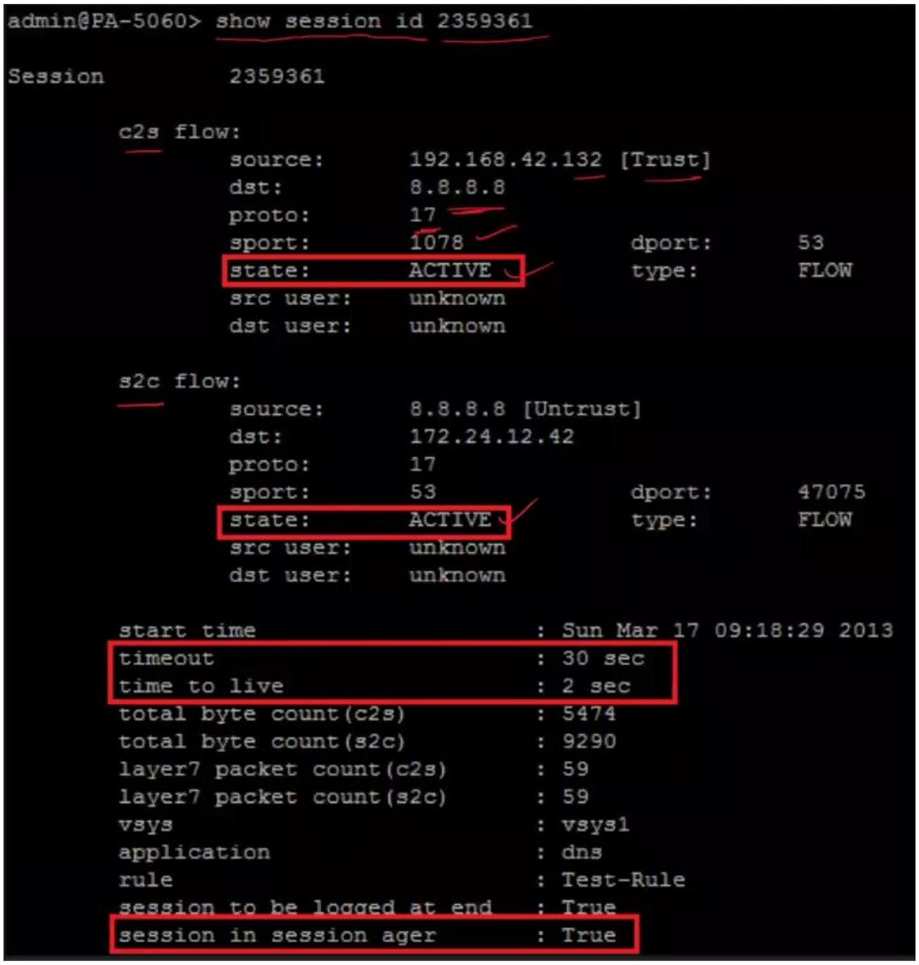
Will display all current sessions matching enter filter. Filters are similar to filtering in GUI:



```
--------------------------------------------------------------------------------
ID      Application    State    Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                                       Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------------------------------
41496   ping           ACTIVE   FLOW  NS   192.168.33.202[1024]/trust-L3/1   (10.66.24.33[1024])
vsys1                                      4.2.2.2[53056]/untrust-L3   (4.2.2.2[53056])
```

> show session id [id #]

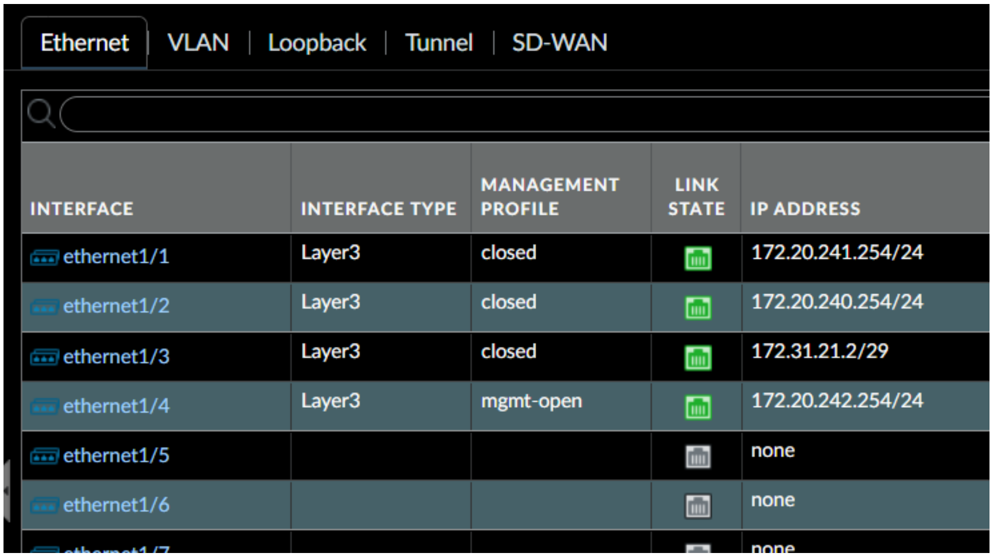
Displays all information about a session.



```
admin@PA-5060> show session id 2359361

Session          2359361

        c2s flow:
                source:      192.168.42.132 [Trust]
                dst:         8.8.8.8
                proto:       17
                sport:       1078             dport:      53
                state:       ACTIVE           type:       FLOW
                src user:    unknown
                dst user:    unknown

        s2c flow:
                source:      8.8.8.8 [Untrust]
                dst:         172.24.12.42
                proto:       17
                sport:       53               dport:      47075
                state:       ACTIVE           type:       FLOW
                src user:    unknown
                dst user:    unknown

        start time                    : Sun Mar 17 09:18:29 2013
        timeout                       : 30 sec
        time to live                  : 2 sec
        total byte count(c2s)         : 5474
        total byte count(s2c)         : 9290
        layer7 packet count(c2s)      : 59
        layer7 packet count(s2c)      : 59
        vsys                          : vsys1
        application                   : dns
        rule                          : Test-Rule
        session to be logged at end   : True
        session in session ager       : True
```

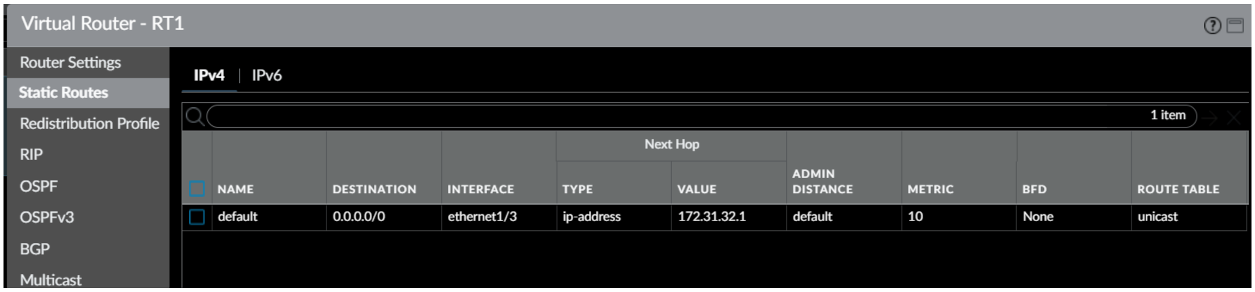
6. **Check network configuration if network can't reach out to internet:**

Ethernet IP Addresses:



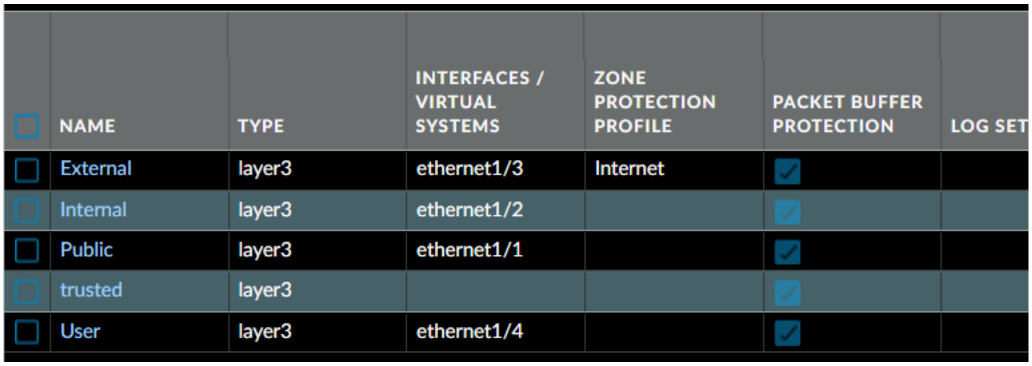
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Layer3	closed	🟩	172.20.241.254/24
ethernet1/2	Layer3	closed	🟩	172.20.240.254/24
ethernet1/3	Layer3	closed	🟩	172.31.21.2/29
ethernet1/4	Layer3	mgmt-open	🟩	172.20.242.254/24
ethernet1/5			⬜	none
ethernet1/6			⬜	none
ethernet1/7			⬜	none

Virtual Router > Static Routes



				Next Hop					
□	NAME	DESTINATION	INTERFACE	TYPE	VALUE	ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE
□	default	0.0.0.0/0	ethernet1/3	ip-address	172.31.32.1	default	10	None	unicast

Ensure the zones are assigned to the correct interfaces



□	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SET
□	External	layer3	ethernet1/3	Internet	☑	
□	Internal	layer3	ethernet1/2		☑	
□	Public	layer3	ethernet1/1		☑	
□	trusted	layer3			☑	
□	User	layer3	ethernet1/4		☑	

7. **If all else fails, just reload to previous configuration snapshot instead of remaining red.**