TECH LEARNIFY

Command Line Interface – CLI

The CLI provides two command modes:

- **Operational**

  —operational mode is used to view information about the firewall and the traffic running through it.

  Operational mode commands are also used to perform operations such as restarting, loading a configuration, shutting down.

- **Configuration**

  —configuration mode is used to view and modify the configuration.

  To switch from operational mode to configuration mode => **configure**
  Switch from configuration mode to operational mode, use either the **quit** or **exit** command
  To enter an operational mode command while in configuration mode, use the **run** command,

General system health

>***show system info*** –provides the system's management IP, serial number and code version
>***show system statistics application/session***– shows the real time throughput on the device
>***show system software status*** – shows whether various system processes are running
>***show jobs processed*** – used to see when commits, downloads, upgrades, etc. are completed
>***show jobs all*** -show any jobs in progress
>***show job id <id#>*** -to show any warning/error in configuration
>***clear job id <id#>*** -to clear a hung job
>***show system disk-space-*** show percent usage of disk partitions
>***show system logdb-quota*** – shows the maximum log file sizes
>***show system state filter cfg.general.max****** - To display the System Limits for objects, profiles, and policies

To monitor CPUs

>***show system resources*** - shows processes running in the management plane similar to "top" command
>***show running resource-monitor*** – used to see the resource utilization in the data plane, such as dataplane CPU utilization
>***less mp-log mp-monitor.log*** – Every 15 minutes the system runs a script to monitor management plane resource usage; output is stored in this file.
>***less dp-log dp-monitor.log*** - Every 15 minutes the system runs a script to monitor dataplane resource usage; output is stored in this file.

TECH LEARNIFY

Dropped packet troubleshooting

>***ping source <IP_addr_src_int> host <IP_addr_host>*** - allows to ping from the specified FW source interface
>***ping host <IP>*** - ping from the MGT interface
>***show session all | match*** – used to show specific sessions in the session table. You can enter any text after the word match. A good example would be a source or destination IP or an application
>***show session all filter destination <IP> dest***- shows all sessions going to a particular dest IP and port <port>- port
>***show session all filter type predict*** – To show any pin-hole applications (e.g.FTP)
>***show session id*** – shows the specifics behind a particular session by entering the ID number after the word "id"
>***show counter interface*** – shows interface counters
>***show counter global | match drop*** – used to troubleshoot dropped packets
>***show counter global filter delta yes*** – show counter changes since last time ran this command
>***show counter global filter delta yes | match [source ip|dest ip| drop | error | frag]*** – show counter changes since last time ran this command, filter on particular keyword
>***show counter global filter packet-filter yes delta yes*** – show counter changes since last time ran this command, filter on debug filter

Routing Debug Commands

>***show routing route*** – displays the routing table
>***test routing fib-lookup virtual-router <VR_name> ip <IP_addr_trying_reach>*** - finds which route in the routing table will be used to reach the IP address that you are testing
>***debug routing global on debug***
>***less mp-log routed.log*** - *To view the log*
>***tail follow yes mp-log routed.log*** - To view the log in real time

Policies

>***show running security-policy*** – shows the current policy set
>***test security-policy-match from <> destination <IP>-*** simulate a packet going through the system, which policy will it match?

Log viewing / deleting

>***show log [system | traffic | threat] direction equal*** *backward* –will take you to the end of the specified log
>***show log [system | traffic | threat] direction equal forward*** – will take you to beginning of the specified log
>***clear log [traffic | threat | acc]*** – clear everything in the specified log
>***show log traffic receive_time*** **in?** - pick a timeframe from the list
>***show log traffic app equal gmail*** - show only gmail traffic in log

TECH LEARNIFY

IPsec Tunnel

To view detailed debug information for IPsec tunnelling*:*

> ***debug ike global on debug***

> ***less mp-log ikemgr.log***

> ***test vpn ike-sa gateway <gw_name>*** - initiates traffic to bring up tunnel

> ***show vpn ike-sa gateway <gw_name>*** - to see if phase 1 is up

> ***show vpn ipsec-sa tunnel <tunnel name>*** *- to see if phase 2 is up*

> ***show vpn flow*** *– to see all active tunnels*

> ***show vpn flow <name> or tunnel-id <id#>*** *-to see detailed info on the tunnel*

Import, Load, and Commit a Configuration File

save config to MyBackup.xml [Config saved to MyBackup.xml]
> tftp export configuration from MyBackup.xml to <tftp>
> tftp import configuration from <tftphost> file <remote>
load config **[**To load a previously saved configuration from the CLI]

How to Troubleshoot Using Counters via the CLI

Counters are a very useful set of indicators for the processes, packet flows and sessions on the PA firewall and can be used to troubleshoot various scenarios.
To troubleshoot dropped packets show counter global filter severity drop can be used. Repeating the command multiple times helps narrow down the drops

> show counter global filter severity drop
> show counter global filter delta yes severity drop
[Packets dropped since the last time the command was issued]

> show counter interface management
> show counter interface ethernet1/1

TCPDUMP - PACKET CAPTURE ON MANAGEMENT INTERFACE

There may be cases where analysis/verification is required to determine whether traffic is being sent/received via the management interface. One such example would be during authentication testing to verify whether requests are being sent from the device to the LDAP or Radius server. Another example would be to determine whether a device is being polled/reachable through a SNMP server. Starting with PAN-OS 5.0 it is possible to know PCAP traffic to/from the management interface. The option is strictly CLI based utilizing **tcpdump**

As captures are strictly/implicitly utilizing the management interface, there is no need to manually specify interfaces as with a traditional tcpdump

> tcpdump filter "host 10.16.0.106 and not port 22"

Note: Filters must be enclosed in quotes, as in:
> tcpdump filter "port 80"
> tcpdump filter "src x.x.x.x"

To view the PCAP on the CLI run the view-pcap command.

> view-pcap mgmt-pcap mgmt.pcap
> **tftp export mgmt-pcap from mgmt.pcap to**

Note: By default, there is a maximum limit of 68 bytes (Snap Length) per packet on PA-200, PA-500 and PA-2000. For the PA-3000, PA-4000 and PA-5000, the default limit is 96 bytes per packet. To extend this limit, use the "snaplen" option

> tcpdump snaplen

Debug Data plane commands

Debug Commands:

>debug dataplane packet-diag show setting - to see if any filters or capture are set
>debug dataplane packet-diag set filter match source x.x.x.x destination x.x.x.x destination-port
>debug dataplane packet-diag set filter on - to turn on filter
>debug dataplane packet-diag set capture stage <receive,drop,firewall,transmit> file <file name>
>debug dataplane packet-diag set capture on - to turn capture on
>view-pcap follow yes <filter-pcap,debug-pcap> - this allows you to view the data real time
>view-pcap filter-pcap <file name>

Clean up Commands:

>debug dataplane packet-diag set capture off - to stop capturing data
>debug dataplane packet-diag set filter off- shut off filter
>delete debug-filter test.pcap - to delete the file

Debug Flow Basic:

>debug dataplane packet-diag filter on
>debug dataplane packet-diag set filter source x.x.x.x dest y.y.y.y
>debug dataplane packet-diag set log on
>less dp0-log pan_packet_diag.log

Clean up Commands:

>debug dataplane packet-diag clear log log
>debug dataplane packet-diag clear filter off
>debug dataplane packet-diag set log off

TECH LEARNIFY

How to Create a Management Profile using the CLI

> Configure
set network profiles interface-management-profile **mgmt-prof** ssh yes
set network profiles interface-management-profile **mgmt-prof** https yes
set network profiles interface-management-profile **mgmt-prof** ping yes
set network interface ethernet **ethernet1/3** layer3 interface-management-profile man
commit

CLI commands to show enable and disable application cache

Command to show running application cache:
> show running application cache

Command to clear the application cache:
> debug dataplane reset appid cache

Command to stop application caching for newly created sessions:
> set application cache no

Command to enable application caching:
> set application cache yes

Command to verify application caching is disabled:
> show running application setting