Cheat Sheet – General

Palo Alto Networks
for PANOS 10.1

The cheat sheet from BOLL. Here you can find helpful guidance for the operation and troubleshooting of Palo Alto Firewalls running PANOS.

Links

General Links	
docs.paloaltonetworks.com	Manuals, release notes, best practice guides and more.
knowledgebase.paloaltonetworks.com	Knowledgebase
live.paloaltonetworks.com	Live community
support.paloaltonetworks.com	Customer support portal
fuelusergroup.com	Fuel user group

Service Links	
apps.paloaltonetworks.com	Cloud Hub
applipedia.paloaltonetworks.com	Application lookup
threatvault.paloaltonetworks.com	Threat lookup (login required)
urlfiltering.paloaltonetworks.com	URL category lookup
status.paloaltonetworks.com	Cloud service status
de.wildfire.paloaltonetworks.com eu.wildfire.paloaltonetworks.com wildfire.paloaltonetworks.com	Wildfire Portals (login required)
updates.paloaltonetworks	Update servers from content updates

System

Default device information	
admin / admin	Default login. Password must be changed on first login
192.168.1.1	Default IP on MGMT interface
9600/8-N-1 hardware flow control disabled	Default serial console settings
set deviceconfig system type dhcp-client	Configure the management interface as a DHCP client.

Maintenance Mode	
Type “maint” when prompted	Enter maintenance mode while bootup process
debug system maintenance-mode	Enter maintenance mode after bootup process
MA1NT	Password if prompted
Maintenance Mode settings	Get system information Factory reset Disk check (fsck) Configuration and image management Set management IP address Diagnostics Reboot

Reboot and shutdown	
request restart system	Restart the device.
request shutdown system	Shutdown the device

Tech Support File

Tech support file (webUI)	
Device > Support > Tech Support File	Download Tech support file. The Tech support file can be extracted and contains various information.

Tech support file (CLI)	
tftp export tech-support to <tftp host>	Export tech support file via TFTP
scp export tech-support to <username@host:path>	Export tech support file via SCP

/var/log/pan/dp-monitor.log /var/log/pan/mp-monitor.log	Data and Management plane information
/opt/pancfg/mgmt/saved-configs/	Running configuration
/usr/local/bin/remove- private-info.sh	Script to remove private information from log files
/tmp/cli/techsupport_...	Support file contains all commands which have been run to generate Tech support file
/var/cores/crashinfo	Backtraces files for service crahses

CLI Basics

Configuration Mode	
configure	Enter configuration mode
exit	Exit configuration mode
set cli config-output-format <default | json | set | xml>	Run the command to change the output format

Find CLI commands	
find command	Use command without any parameters to display the entire command hierarchy in the current command mode
find command keyword <keyword>	Use command to locate all commands that have a specified keyword
/command Type n for next search result	Highlights specific string in find command output
+ option * option	Optional option Mandatory option

Jobs and commit

Job Management	
show jobs pending	Display pending jobs
show jobs processed	Display finished jobs
show jobs id <number>	Display info for specific job

Commit	
check pending-changes	Check for any uncommitted changes to the candidate configuration
validate full	Validate commit. Validate command creates a job with a job ID
show jobs id <id>	View the validation results using the job ID
commit	Commit the entire configuration
commit partial ?	Commit part of the configuration
show system last-commit-info	Display last commit information

Cheat Sheet – Session

Palo Alto Networks
for PANOS 10.1

Session

Session information	
show session info	Summary of session-based statistics
show session all	Display session information for all active sessions

NS = Source NAT
ND = Destination NAT
NB = Both NAT
* = Session was decrypted
	Flags used in the session information

show session id <number>	Display detailed session info for a specific session.
Clear session id <number>	Clear a specific session
Monitor > Session Browser	Display real-time session data (WebUI)
Device > Troubleshooting	Diagnostic Tools for Policy and Connectivity Analysis (WebUI)

Session states	
Init	Session begins the initialization state (stable state).
Active	Active session matching a traffic flow (stable state).
Discard	Traffic denied because of security policy or threat detection (stable state).
Opening, Closed, Closing, Free	Transient session states, rare to see because the firewall quickly transitions session state to one of the stable states.

Traffic Log	
show log traffic	Display all traffic log entries
show log traffic ?	Use? To show available filters to filter traffic log

Flow basic

Flow basic Logs	
debug dataplane packet-diag set log feature flow basic	Flow basic provides detailed output for individual packets. Should be used in combination with packet capture.
1. debug dataplane packet-diag show setting	Show configured settings
2. debug dataplane packet-diag clear all	Clear existing filter
3. debug dataplane packet-diag set filter	Add up to four filter
4. debug dataplane packet-diag set filter on	Enable filter
5. debug dataplane packet-diag set log feature flow basic	Enable flow basic debugging and run traffic
6. debug dataplane packet-diag aggregate-logs	Aggregate all packet-diag logs into a single file
7a. less dp-log pan_packet_diag.log	View flow basic logs
8b. less mp-log pan_packet_diag.log	View flow basic logs for smaller models without management plane
8. tftp export log-file management-plane to <username@host:path>	Export collected logs to a TFTP or SCP destination.

Offloading Traffic	
set session offload no / yes	Termporary, non-persistent offloading setting
set deviceconfig setting session offload no / yes	Persistent offloading configuration

Packet Capture

Packet capture (CLI)	
debug dataplane packet-diag show setting	Show configured capture settings
1. debug dataplane packet-diag clear all	Delete existing filters
2. debug dataplane packet-diag clear log log	Delete existing log files.
3. > debug dataplane packet-diag set filter index <1-4> match destination <a.a.a.a> destination-port <bb> ingress-interface ethernet1/1 source <d.d.d.d> protocol <17> non-ip exclude	Add up to four filters
4. debug dataplane packet-diag set filter on	Enable Filters
5. debug dataplane packet-diag set capture stage <receive | firewall | drop | transmit> file <filename>	Assign a name for the output file for each stage
6. debug dataplane packet-diag set capture on	Enable packet capture to start packet capture
7. show counter global filter delta yes packet-filter yes	Check if any packets were captured (run command twice)
8. debug dataplane packet-diag set capture off	Stop capture, refresh page and download pcap files
9. view-pcap no-dns-lookup yes filter-pcap <filename><tftp | scp> export filter-pcap from <filename> to <tftp-ip | user@ip-address>	Download packet capture files for further analysis
10. debug dataplane packet-diag clear capture stage <receive | firewall | drop | transmit> file <filename>	Delete files after download

Packet capture (webUI)	
Monitor > Packet capture	Add, filter and download packet captures (webUI)
1. Clear All Settings	Delete existing filters
2. Manage Filters	Add up to four filters
3. Filtering → On	Enable Filters
4. Define packet stages	Assign a name for the output file for each stage
5. Packet Capture → On	Enable packet capture to start packet capture
6. CLI: show counter global filter delta yes packet-filter yes	Check if any packets were captures (run command twice)
7. Packet Capture → Off	Stop capture, refresh page and download pcap files
8. Download Captured Files	Download packet capture files for further analysis
9. Delete Captured Files	Delete files after download

Network tools	
ping host <destination-ip-address>	Ping from the management (MGT) interface to a destination IP address
ping source <ip-address-on-dp> host <destination-ip>	Ping from a dataplane interface to a destination IP address
traceroute <interface><destination-ip-	Print the route taken by packets to a destination
dig <interface><server address> <hostname>	Query DNS servers
show netstat statistics yes	Show network statistics

Cheat Sheet – Services

Palo Alto Networks
for PANOS 10.1

Services

View service logs	
less mp-log <log-name>	Service log listing for service logs as listed below:
tail follow yes mp-log	End of service log with automatic refresh
grep mp-log <log-name> pattern <value>	Search for specific pattern in service logs

Change debug level	
debug software logging-level show level service all-services	Show current log levels
debug software logging-level set level <level> service <service-name>	Set log level for specific service
debug software logging-level set level default service <service-name>	Reset log level for specific service to default
0 = Off 1 = Error 2 = Warn 3 = Info (or normal) 4 = Debug 5 = Dump (use with caution)	Debug levels

Listing of service logs	
authd.log	All firewall and authentication policy initiated authentications
devsrvr.log	Device Server for configuration push and communication with data plane
ha-agent.log	High availability status
Ikemgr.log keymgr.log	Contains ISAKMP and IPSec service logs
logcvr.log	Records traffic logs sent from the data plane
mgmt_httpd_access.log mgmt._httpd_error.log	Management user interface and XML APi requests
ms.log	Management Server for configuration management
rasmgr.log	Provides logs for GlobalProtect remote access
routed.log	Provides static and dynamic routing service information
sslvpn-acces.log sslvpn_error.log	Service log for GlobalProtect web-based features
syslog-ng.log	Handles log forwarding
userid.log	Manages User-ID features
varcvr.log	Records URL logs and pcaps sent from the data plane

Restart processes	
debug software restart process <process-name>	Restart process
show system software status | match <service-name>	Check if process is running

File and Disk	
show system logdb-quota	Show the maximum log file size.
show system disk-space files	Show percent usage of disk partitions
show running logging	Show log and packet logging rate

General system health

General system information	
show system info	Show general system health information
show system software status	Show running processes
show system resources follow	Show processes running in the management plane Press h for help Press 1 to toggle CPU Press M to sort by Memory
show running resource-monitor second last 60	Show resource utilization in the data plane for the last 60 seconds
request license info	Show the licenses installed on the device.

Administrators	
show admins	Show the administrators who are currently logged in to the web interface, CLI, or API.
Show admins all	Show the administrators who can access the web interface, CLI, or API, regardless of the login status.

User-ID

Agent status	
show user user-id-agent state all	See all configured Windows-based agents
show user server-monitor state all	See if the PAN-OS-integrated agent is configured

User-ID	
show user ip-user-mapping all	View all user mappings on the Palo Alto Networks device
show user ip-user-mapping all | match <domain>\\<username-string>	Show user mappings filtered by a username string (if the string includes the domain name, use two backslashes before the username)
show user ip-user-mapping ip <ip-address>	Show user mappings for a specific IP address
show user user-ids	Show usernames
show log userid datasource equal <datasource>	View mappings learned using a particular type of user mapping

Group mapping	
show user group-mapping statistics	Show group mapping statistics
show user group-mapping state all	Show all group mappings
show user group list	Lista ll groups
show user group name <group-name>	Show group members for a specific group

User Cache	
clear user-cache all	Clear the User-ID cache
clear user-cache ip <ip-address/netmask>	Clear a User-ID mapping for a specific IP address

Cheat Sheet – Features

High Availability

High Availability	
show high-availability cluster all	View all HA cluster configuration content
show high-availability cluster flap-statistics	View HA cluster flap statistics.
show high-availability cluster session-synchronization	View information about the type and number of synchronized messages to or from an HA cluster.
show high-availability cluster state	View HA cluster state and configuration information.
show high-availability cluster statistics	View HA cluster statistics, such as counts received messages and dropped packets for various reasons.
clear high-availability cluster statistics	Clear HA cluster statistics.
request high-availability cluster clear-cache	Clear session cache.
request high-availability cluster sync-from	Request full session cache synchronization.

Routing

Route lookup	
show routing route	Display the routing table
test routing fib virtual-router <name> | match <x.x.x.x/Y>	Test routing lookup for a specific destination

NAT

NAT Policies and Pool	
show running nat-policy	Show the NAT policy table
test nat-policy-match	Test the NAT policy
show running ippool show running global-ippool	Show NAT pool utilization

IPSEC

Show VPN information	
show vpn flow	Show IPSec counters
show vpn flow tunnel-id <id>	Show details for a specific tunnel
show vpn gateway	Display list of IKE gateway configurations
show vpn tunnel	Display list of auto-key IPSec tunnel configurations
show vpn ike-sa	Show IKE phase 1 SAs
show vpn ipsec-sa	Show IKE phase 2 SAs
show session all filter protocol 50	Show sessions for ESP packets

Test VPN connection	
test vpn ike-sa gateway <gateway-name>	Initiate Phase 1 for a specific gateway
test vpn ipsec sa tunnel <tunnel-name>	Initiate Phase 2 for a specific tunnel without generating traffic

Clear VPN connection	
clear vpn flow tunnel-id <tunnel-id-number>	Clear IPSEC counters
clear vpn ike-sa gateway <gateway-name>	Clear IKE phase 1 SAs
clear vpn ipsec-sa tunnel <tunnel-name>	Clear IKE phase 2 SAs

IPSEC (cont.)

Debug IPSEC VPN	
debug ike pcap on	Activate pcap for all IKE traffic
view-pcap <options debug-pcap ikemgr.pcap	Display the pcap in CLI
debug ike pcap off	Turn off packet capture
scp export debug-pcap <filename<	Copy the pcap off the firewall
debug ike pcap delete	Remove the ikemgr.pcap file

SSL Decryption

SSL Decryption	
show system setting ssl-decrypt setting	Show SSL Decryption settings
show system setting ssl-decrypt certificate	Display which certificates are loaded on the data plane
show system setting ssl-decrypt exclude-cache	Display destinations actively excluded from SSL decryption
debug dataplane reset ssl-decrypt exclude-cache application <application-name>	Reset application from the exclude cache
debug dataplane reset ssl-decrypt exclude-cache server <IP-address:port>	Reset IP address from the exclude cache

URL filtering

Test URL	
test url <url or IP>	Test the categorization of a URL on the device
test url-info-cloud <url>	Test the categorization of a URL in the cloud

Status and Cache	
show log url direction equal backward	Display the URL log, most recent entries first
show url-cloud status	Check URL cloud status
debug dataplane show url-cache statistic	Display statistics on the URL cache
clear url-cache all	Clear URL cache
clear url-cache url <value>	Clear specific entry from cache

Wildfire

Test URL	
debug wildfire upload-log show	Verify file submission

VSYS

VSYS	
show system info | match vsys	Find out if the firewall is in multi-vsys mode
set system setting target-vsys	View a list of virtual systems configured on the firewall
set system setting target-vsys <vsys-name>	Switch to a particular vsys so that you can issue commands and view data specific to that vsys
set system setting target-vsys none	Return to configuring the firewall globally

Cheat Sheet – Features

Palo Alto Networks
for PANOS 10.1

Licenses, Software and Updates

Software	
debug swm status	Show status of PAN Software Manager
debug swm info	Display info on current or specified image
debug swm history	Show history of software install operations
debug swm revert	Revert back to previous running software packages

Dynamic Updates	
request content upgrade info	Show information about available threat packages
request content upgrade install version latest	Installs most recently downloaded threat package
request anti-virus upgrade info	Show information about available antivirus packages
request anti-virus upgrade install version latest	Installs most recently downloaded antivirus package
debug swm rebuild-content-db	Rebuild content databas

Panorama

Panorama Mode	
show system info | match system-mode	Display the current operational mode.
request system system-mode logger	Switch from Panorama mode to Log Collector mode.
request system system-mode panorama	Switch the Panorama virtual appliance from Legacy mode to Panorama mode.
request system system-mode legacy	Switch the Panorama virtual appliance from Panorama mode to Legacy mode.

Device and Template information on firewall	
set panorama [off | on]	Enable or disable the connection between a firewall and Panorama. You must enter this command from the firewall CLI.
show config pushed-shared-policy	Show all the policy rules and objects pushed from Panorama to a firewall.
show config pushed-template	Show all the network and device settings pushed from Panorama to a firewall.

Device and Template information on Panorama	
show devicegroups name <device-group-name>	Show the history of device group commits, status of the connection to Panorama and other information
show templates name <template-name	Show the history of template commits, status of the connection to Panorama and other information

Log Collector on firewall	
show logging-status	The output shows how many logs the firewall has forwarded to Panorama.

Panorama (cont)

Log Collector on Panorama	
debug log-collector log-collection-stats show incoming-logs	Show the current rate at which the Panorama management server or a Dedicated Log Collector receives firewall logs
debug log-collector log-collection-stats show log-forwarding-stats	Show the quantity and status of logs that Panorama or a Dedicated Log Collector forwarded to external servers
show logging-status device <firewall-serial-number>	Show status information for log forwarding to the Panorama management server or a Dedicated Log Collector from a particular firewall.
clear log [acc | alarm | config | hipmatch | system]	Clear logs by type.