PAN Cheat Sheet

Palo Alto Networks
for PANOS 11.1

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
knowledgebase.paloaltonetworks.com	Knowledgebase
live.paloaltonetworks.com	Live community
support.paloaltonetworks.com	Customer support portal
beacon.paloaltonetworks.com	Learning Center
live.paloaltonetworks.com Search: Software Release Guidance	Preferred software releases (login required)

Service Links	
apps.paloaltonetworks.com	Cloud Hub
applipedia.paloaltonetworks.com	Application lookup
updates.paloaltonetworks.com	Update servers for content updates
urlfiltering.paloaltonetworks.com	URL category lookup
security.paloaltonetworks.com	Security Advisories for PAN products
threatvault.paloaltonetworks.com	Threat lookup (login required)
wildfire.paloaltonetworks.com with ch. / de. / eu subdomains	Wildfire Portals (login required)

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	
choose maint-sysroot in menu	Enter maintenance mode while bootup process
debug system maintenance-mode	Enter maintenance mode after bootup process
MA1NT	Maintenance password
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 > Generate Tech Support File	Generate and download Tech support file. 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

Useful information in the extracted Tech support file	
/var/log/pan/dp-monitor.log /var/log/pan/mp-monitor.log	Data and Management plane ressource information
/opt/pancfg/mgmt/saved-configs/	Running configuration
/tmp/cli/techsupport_...	Support file contains all commands which have been run to generate Tech support file
/var/cores/crashinfo	Backtrace files for service crashes

CLI Basics

Configuration Mode	
configure	Enter configuration mode. All commands in configuration mode are marked with (#)
exit (#)	Exit configuration mode
set cli config-output-format <default | json | set | xml>	Run the command to change the output format
command ? + option command ? * option	Optional option in command Mandatory option in command

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

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

PAN Cheat Sheet

Palo Alto Networks
for PANOS 11.1

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 in WebUI (max 1024 entries)
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

Packet capture and flow basic

Notes	
Packet capture and flow basic commands are often used together to troubleshoot traffic problems in detail.	
Packet capture	Capture packets in different firewall stages. Download as pcap possible.
Flow basic	Flow basic provides detailed output for individual packets.

Offloading Traffic	
Offloaded traffic is not included in the packet capture. To capture full traffic, disable offloading. Take care that disabling offloading will increase the dataplane CPU!	
set session offload no / yes	Termporary, non-persistent offloading setting
set deviceconfig setting session offload no / yes (#)	Persistent offloading configuration

Packet capture and flow basic filter
Log filters apply equally to the packet capture and the flow basic and only need to be set once. Filters can be set in the WebUI and in the CLI.

1a Filter Settings in WebUI	
Monitor > Packet capture	1. Show configured capture settings
Clear All Settings	2. Delete existing filters
Delete Captured Files	3. Delete existing files
Manage Filters	4. Add up to four filters
Filtering → On	5. Enable Filters

1b Filter Settings in CLI	
debug dataplane packet-diag show setting	1. Show configured capture settings
debug dataplane packet-diag clear all	2. Delete existing filters
debug dataplane packet-diag clear log log	3. Delete existing files.
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>	4. Add up to four filters (A few examples of filters are listed on the left. More filtering options with ?)
debug dataplane packet-diag set filter on	5. Enable filters

2a Start packet capture in webUI	
Set and enable filters	6. Check “Filter Settings in WebUI”
Define packet stages	7. Assign a name for the output file for each stage
Packet Capture → On	8. Enable packet capture to start packet capture
CLI: show counter global filter delta yes packet-filter yes	9. Check if any packets were captures (run command twice)
Packet Capture → Off	10. Stop capture and refresh page
Download Captured Files	11. Download packet capture files for further analysis
Delete Captured Files	12. Delete files after download

2b Start packet capture in CLI	
Set and enable filters	6. Check “Filter Settings in CLI”
debug dataplane packet-diag set capture stage <receive | firewall | drop | transmit> file <filename>	7. Assign a name for the output files for each stage
debug dataplane packet-diag set capture on	8. Enable packet capture to start packet capture
show counter global filter delta yes packet-filter yes	9. Check if any packets were captured (run command twice)
debug dataplane packet-diag set capture off	10. Stop capture
view-pcap no-dns-lookup yes filter-pcap <filename><tftp | scp> export filter-pcap from <filename> to <tftp-ip | user@ip-address>	11. Download packet capture files for further analysis
debug dataplane packet-diag clear capture stage <receive | firewall | drop | transmit> file <filename>	12. Delete files after download

Flow basic Logs (CLI commands only)	
Set and enable filters	1. Check “Filter Settings in WebUI / CLI”
debug dataplane packet-diag set log feature flow basic	2. Enable flow basic debugging
debug dataplane packet-diag set log on	3. Enable flow basic logging and run traffic
debug dataplane packet-diag aggregate-logs	4. Aggregate all packet-diag logs into a single file
less dp-log pan_packet_diag.log less mp-log pan_packet_diag.log	5. View flow basic logs (smaller models without management plane)
tftp / scp export log-file data-plane / management-plane to	6. Export collected logs to a TFTP or SCP destination

PAN Cheat Sheet

Palo Alto Networks
for PANOS 11.1

General system information

General system information	
show system info	Show general system health information
show system software status	Show running processes
show system resources	Show processes running in the management plane
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

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 source <ip-address-on-dp> host <destination-ip>	Print the route taken by packets to a destination
show netstat statistics yes / no	Show network statistics

User-ID

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

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 all	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	List all 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

Services

View service logs	
less mp-log <log-name>	Service log listing for service logs as listed below
tail follow yes mp-log <log-name>	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	
show system software status | match <process-name>	Check if specific process is running
debug software restart process <process-name>	Restart process

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

PAN Cheat Sheet

Palo Alto Networks
for PANOS 11.1

High Availability

High Availability	
show high-availability all	Show high-availability pair information
show high-availability flap-statistics	HA cluster flap statistics
show high-availability state	HA cluster state information
show high-availability state-synchronization	HA pair state synchronization statistics
show high-availability link-monitoring / path-monitoring	Link and path monitoring states
clear high-availability cluster control-link 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> ip <ip>	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 ESP sessions

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 follow yes debug-pcap ikemgr.pcap	Display the pcap in CLI
debug ike pcap off	Turn off packet capture
scp export debug-pcap from <filename> to <host>	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 (SNI or CName) actively excluded from SSL decryption
debug dataplane reset ssl-decrypt <cache>	Reset different SSL caches
certificate-cache certificate-status dns-cache gp-cookie-cache	Certificate cache Certificate CRL status DNS cache GlobalProtect cookie 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 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
show 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

PAN Cheat Sheet

Palo Alto Networks
for PANOS 11.1

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

Panorama

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

Device information	
show devices all	Show detailed information about connected firewall devices
show panorama status	(Firewall) Show Panorama status on firewall

Device and Template information on firewall	
set panorama [off | on]	Enable or disable the connection between a firewall and Panorama
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

Something missing?

Please contact us for comments, corrections or ideas regarding our cheat sheet at support@boll.ch

BOLL