Vendor: Check Point

Exam Code: 156-583

Exam Name: Check Point Certified Troubleshooting Administrator - R82 (CCTA)

Version: DEMO

QUESTION 1
You want to print the status of WatchDog-monitored processes. What command best meets your needs?

A. cpwd_admin list
B. tcpdump
C. cppcap
D. cpplic print

Answer: A
Explanation:
The cpwd_admin list command is used to display the status of processes monitored by the WatchDog service in Check Point. WatchDog ensures that critical processes are running and restarts them if they fail, maintaining the stability and security of the gateway.

QUESTION 2
The Check Point FW Monitor tool captures and analyzes incoming packets at multiple points in the traffic inspections. Which of the following is the correct inspection flow for traffic?

A. (i) - pre-inbound, (I) - post-inbound, (o) - pre-outbound, (O) - post-outbound
B. (o) - pre-outbound, (O) - post-inbound, (i) - pre-inbound, (I) - post-inbound
C. (O) - post-outbound, (o) - pre-outbound, (I) - post-inbound, (i) - pre-inbound
D. (1) - pre-inbound, (i) - post-inbound, (O) - pre-outbound, (o) - post-outbound

Answer: A
Explanation:
The correct inspection flow using fw monitor is:

(i) - pre-inbound: Before the packet enters the inbound processing path.
(I) - post-inbound: After the inbound processing.
(o) - pre-outbound: Before the packet enters the outbound processing path.
(O) - post-outbound: After the outbound processing.

This sequence ensures that packets are captured and analyzed at all critical points during their traversal through the firewall.

QUESTION 3
What does the FWD daemon instruct the gateway to do when communication issues between the gateway and SMS/Log Server occur?

A. It instructs the gateway to continue forwarding logs to SMS/Log Server and the logs will be stored in a holding queue for the server until communication is restored.
B. It instructs the gateway to stop logging until it can restore communication.
C. It instructs the gateway to store logs locally as it continues to try to restore communication.
D. It instructs the gateway to only log a specified number of logs as defined in the Security Policy.

Answer: C
Explanation:
When there are communication issues between the Security Gateway and the Security Management Server (SMS)/Log Server, the FWD daemon directs the gateway to store logs locally. This ensures that logging continues without interruption, and the logs are queued until communication with the SMS/Log Server is re-established, preventing any loss of log data.

QUESTION 4
You tested the connection from source to destination and you are not able to find logs in your Security Management. What is the best possible reason?

A. The FWM process crashed on Security Management, therefore logging will not work.
B. There is not enough storage in Security Management, so the logs can't be stored.
C. The logging blade was not enabled on Security Gateway.
D. The gateway is logging locally.

Answer: C
Explanation:
If logs are not appearing in the Security Management despite successful traffic flow, the most likely reason is that the logging blade is not enabled on the Security Gateway. Without enabling the logging functionality, the gateway will not send logs to the Security Management Server, even though the traffic itself is passing through successfully.

QUESTION 5
You need to switch the active log file on the Security Gateway. What is the correct command?

A. fw -p -o <log file> switch
B. fw logswitch
C. Install security policy
D. fw switchlog

Answer: B
Explanation:
The fw logswitch command is used to switch the active log file on a Check Point Security Gateway. This command forces the gateway to start writing logs to a new file, which is useful for log management and troubleshooting purposes. Other options listed are either incorrect or do not perform the log-switching function.

QUESTION 6
What is the port for the Log Collection on Security Management Server?

A. 18191
B. 443
C. 258
D. 257

Answer: D
Explanation:
Port 257 is used for log collection on the Security Management Server. This port facilitates the transmission of log data from Security Gateways to the Management Server, ensuring that logs are centralized for monitoring, analysis, and reporting.

QUESTION 7
Which command forces a Security Gateway to retrieve the policy from the Management Server?

A. fw fetch

B. fw load
C. fw stat -l
D. cpstart

Answer: A
Explanation:
The fw fetch command instructs the gateway to pull the last installed policy from the specified management server or from its local state. It is useful for verifying policy retrieval independently of a full policy installation from SmartConsole.

QUESTION 8
Which command removes the security policy from the local gateway, leaving it without policy enforcement?

A. fw unloadlocal
B. fw fetch local
C. cpstop
D. fw ctl uninstall

Answer: A
Explanation:
The fw unloadlocal command removes the currently installed policy from the gateway. Because it leaves the gateway unprotected and accepting traffic, it should only be used during controlled troubleshooting with console access available.

QUESTION 9
Which command displays the currently installed policy name and the time it was installed?

A. fw stat
B. fw ver
C. cpstat os
D. fw ctl get policy

Answer: A
Explanation:
The fw stat command reports the policy name, installation timestamp, and the interfaces it is enforced on. A policy name of "Default Filter" or an unexpected timestamp is an immediate sign that policy installation did not complete as expected.

QUESTION 10
Where are user mode process core dumps stored on a Gaia system by default?

A. /var/log/dump/usermode
B. /var/crash
C. $FWDIR/log/dump
D. /tmp/cores

Answer: A
Explanation:
Core dumps generated by crashing user mode Check Point processes are written to

/var/log/dump/usermode. Finding recent files in this directory usually correlates with WatchDog restarts observed in cpwd_admin list.

QUESTION 11
Which command switches the active log file on a gateway or management server and starts a new one?

A. fw logswitch
B. fw repairlog
C. fw log -n
D. fwm logexport

Answer: A
Explanation:
The fw logswitch command closes the active fw.log, renames it with a timestamp, and opens a new empty log file. It is often used before reproducing an issue so that only the relevant records appear in the new file.

QUESTION 12
Which command repairs a corrupted log file and rebuilds its pointer file?

A. fw repairlog
B. fw logswitch -r
C. fw log -f
D. log_indexer -rebuild

Answer: A
Explanation:
The fw repairlog command rebuilds the pointer file associated with a log file so that it can be read again by log viewers. Corruption commonly follows an abrupt shutdown or a disk space exhaustion event on the log server.

QUESTION 13
Which process indexes log files so that SmartConsole Logs and Monitor views return fast search results?

A. log_indexer
B. fwd
C. cpd
D. cpsead

Answer: A
Explanation:
The log_indexer process reads log files and builds the index used for searching in the Logs and Monitor view. If logs are visible in the raw files but searches return nothing, the indexer is a primary suspect.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**