CheckPoint

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

NEW QUESTION 1
How can you start debug of the Unified Policy with all possible flags turned on?

A. fw ctl debug -m UP all
B. fw ctl debug -m UnifiedPolicy all
C. fw ctl debug -m fw + UP
D. fw ctl debug -m UP *

Answer: D

NEW QUESTION 2
You have configured IPS Bypass Under Load function with additional kernel parameters ids_tolerance_no_stress=15 and ids_tolerance_stress-15 For configuration you used the *fw ctl set' command After reboot you noticed that these parameters returned to their default values What do you need to do to make this configuration work immediately and stay permanent?

A. Set these parameters again with “fw ctl set” and edit appropriate parameters in $FWDIR/boot/modules/ fwkern.conf
B. Use script $FWDIR/bin IpsSetBypass.sh to set these parameters
C. Set these parameters again with “fw ctl set” and save configuration with “save config”
D. Edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf

Answer: A

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 3
What does CMI stand for in relation to the Access Control Policy?

A. Content Matching Infrastructure
B. Content Management Interface
C. Context Management Infrastructure
D. Context Manipulation Interface

Answer: C

NEW QUESTION 4
What is the difference in debugging a S2S or C2S (using Check Point VPN Client) VPN?

A. there is no difference
B. the C2S VPN uses a different VPN daemon and there a second VPN debug
C. the C2S VPN can not be debugged as it uses different protocols for the key exchange
D. the C2S client uses Browser based SSL vpn and can’t be debugged

Answer: D

NEW QUESTION 5
What is the main SecureXL database for tracking the acceleration status of traffic?

A. cphwd_db
B. cphwd_tmp1
C. cphwd_dev_conn_table
D. cphwd_dev_identity_table

Answer: D

NEW QUESTION 6
What is the buffer size set by the fw ctl zdebug command?

A. 1 MB
B. 1 GB
C. 8MB
D. 8GB

Answer: A

NEW QUESTION 7
Jenna has to create a VPN tunnel to a CISCO ASA but has to set special property to renegotiate the Phase 2 tunnel after 10 MB of transferee1 data. This can not be configured in the smartconsole, so how can she modify this property?

A. using GUIDBEDIT located in same directory as Smartconsole on the Windows client
B. she need to install GUIDBEDIT which can be downloaded from the Usercenter
C. she need to run GUIDBEDIT from CLISH which opens a graphical window on the smartcenter
D. this cant be done anymore as GUIDBEDIT is not supported in R80 anymore

Answer: C

NEW QUESTION 8
Which process is responsible for the generation of certificates?

A. cpm
B. cpca
C. dbsync
D. fwm

Answer: B

NEW QUESTION 9
Which of the following is NOT a vpn debug command used for troubleshooting?

A. fw ctl debug -m fw + conn drop vm crypt
B. vpn debug trunc
C. pclient getdata sslvpn
D. vpn debug on TDERROR_ALL_ALL=5

Answer: C

NEW QUESTION 10
What are four main database domains?

A. System, Global, Log, Event
B. System, User, Host, Network
C. Local, Global, User, VPN
D. System, User, Global, Log

Answer: D

NEW QUESTION 10
If IPS protections that prevent SecureXL from accelerating traffic, such as Network Quota, Fingerprint Scrambling. TTL Masking etc, have to be used, what is a recommended practice to enhance the performance of the gateway?

A. Use the IPS exception mechanism
B. Disable all such protections
C. Disable SecureXL and use CoreXL
D. Upgrade the hardware to include more Cores and Memory

Answer: C

NEW QUESTION 12
Some users from your organization have been reporting some connection problems with CIFS since this morning You suspect an IPS issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS chain module (position 4 in the chain) to check If the packets pass the IPS. What command do you need to run?

A. fw monitor -ml -pi 5 -e <filterexperession>
B. fw monitor -pi 5 -e <filterexptession>
C. tcpdump -eni any <filterexpression>
D. fw monitor -pi asm <filtefexpfession>

Answer: C

NEW QUESTION 16
What are the maximum kernel debug buffer sizes, depending on the version

A. 8MB or 32MB
B. 8GB or 64GB
C. 4MB or 8MB
D. 32MB or 64MB

Answer: A

NEW QUESTION 17
The customer is using Check Point appliances that were configured long ago by third-party administrators. Current policy includes different enabled IPS protections and Bypass Under Load function. Bypass Under Load is configured to disable IPS inspections of CPU and Memory usage is higher than 80%. The Customer reports that IPS protections are not working at all regardless of CPU and Memory usage.
What is the possible reason of such behavior?

A. The kernel parameter ids_assume_stress is set to 0
B. The kernel parameter ids_assume_stress is set to 1
C. The kernel parameter ids_tolerance_no_stress is set to 10
D. The kernel parameter ids_tolerance_stress is set to 10

Answer: D

NEW QUESTION 20
Troubleshooting issues with Mobile Access requires the following:

A. Standard VPN debugs, packet captures, and debugs of cvpnd' process on Security Gateway
B. Standard VPN debugs and packet captures on Security Gateway, debugs of "cvpnd' process on Security Management
C. 'ma_vpnd' process on Secunty Gateway
D. Debug logs of FWD captured with the command - 'fw debug fwd on TDERROR_MOBILE_ACCESS=5'

Answer: A

NEW QUESTION 21
Which of the following is NOT a valid "fwaccel" parameter?

A. stat
B. stats
C. templates
D. packets

Answer: D

NEW QUESTION 26
How does the URL Filtering Categorization occur in the kernel?
* 1. RAD provides the status of the search to the client.
* 2. The a-sync request is forwarded to the RAD User space via the RAD kernel for online categorization.
* 3. The online detection service responds with categories and the kernel cache is updated.
* 4. The kernel cache notifies the RAD kernel of hits and misses.
* 5. URL lookup initiated by the client.
* 6. URL lookup occurs in the kernel cache.
* 7. The client sends an a-sync request back to RAD If the URL was not found.

A. 5, 6, 7, 1, 3, 2, 4
B. 5, 6, 2, 4, 1, 7, 3
C. 5, 6, 4, 1, 7, 2, 3
D. 5, 6, 3, 1, 2, 4, 7

Answer: C

NEW QUESTION 29
PostgreSQL is a powerful, open source relational database management system Check Point offers a command for viewing the database to interact with Postgres interactive shell Which command do you need to enter the PostgreSQL interactive shell?

A. psql_client cpm postgres
B. mysql_client cpm postgres
C. psql_c!ieni postgres cpm
D. mysql -u root

Answer: A

NEW QUESTION 34
In Security Management High Availability, if the primary and secondary managements, running the same version of R80.x, are in a state of ‘Collision’, how can this be resolved?

A. Administrator should manually synchronize the servers using SmartConsole
B. The Collision state does not happen in R80.x as the synchronizing automatically on every publish action
C. Reset the SIC of the secondary management server
D. Run the command ‘fw send synch force’ on the primary server and ‘fw get sync quiet’ on the secondary server

Answer: A

NEW QUESTION 39
Where will the usermode core files be located?

A. /var/log/dump/usermode
B. /var/suroot
C. SFWDIR/var'log/dump/usermode
D. SCPDIR/var/log/dump/usermode

Answer: A

NEW QUESTION 40
What is the function of the Core Dump Manager utility?

A. To generate a new core dump for analysis

B. To limit the number of core dump files per process as well as the total amount of disk space used by core files
C. To determine which process is slowing down the system
D. To send crash information to an external analyzer

Answer: B

NEW QUESTION 42
Joey is configuring a site-to-site VPN with his business partner. On Joey's site he has a Check Point R80.10 Gateway and his partner uses Cisco ASA 5540 as a gateway.
Joey's VPN domain on the Check Point Gateway object is manually configured with a group object that contains two network objects:
VPN_Domain3 = 192.168.14.0/24 VPN_Domain4 = 192.168.15.0/24
Partner's site ACL as viewed from "show run"
access-list JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.14.0 255.255.255.0
access-list JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.15.0 255.255.255.0 When they try to establish VPN tunnel, it fails. What is the most likely cause of the failure given the
information provided?

A. Tunnel falls on partner sit
B. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation.Check Point continues to present its own encryption domain as 192.168.14.0/24 and 192.168.15.0/24, but the peer expects the one network 192.168.14.0/23
C. Tunnel fails on partner sit
D. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation.Check Point continues to present its own encryption domain as 192.168.14.0/23, but the peer expects the two distinct networks 192.168.14.0/24 and 192.168.15.0/24.
E. Tunnel fails on Joey's site, because he misconfigured IP address of VPN peer.
F. Tunnel falls on partner sit
G. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

Answer: B

NEW QUESTION 45
Vanessa is reviewing ike.elg file to troubleshoot failed site-to-site VPN connection After sending Mam Mode Packet 5 the response from the peer is PAYLOAD-MALFORMED"
What is the reason for failed VPN connection?

A. The authentication on Phase 1 is causing the problem.Pre-shared key on local gateway encrypted by the hash algorithm created in Packet 3 and Packet 4 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
B. The authentication on Phase 2 is causing the problemPre-shared key on local gateway encrypted by the hash algorithm created in Packets 1 and 2 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
C. The authentication on Quick Mode is causing the problemPre-shared key on local gateway encrypted by the hash algorithm created in Packets 3 and 4 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
D. The authentication on Phase 1 is causing the problemPre-shared key on local gateway encrypted by the hash algorithm doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key created in Packet 1 and Packet 2

Answer: B

NEW QUESTION 49
Which command(s) will turn off all vpn debug collection?

A. vpn debug off
B. vpn debug -a off
C. vpn debug off and vpn debug ikeoff
D. fw ctl debug 0

Answer: C

NEW QUESTION 53
What is the simplest and most efficient way to check all dropped packets in real time?

A. fw ctl zdebug * drop in expert mode
B. Smartlog
C. cat /dev/fwTlog in expert mode
D. tail -f SFWDIR/log/fw log |grep drop in expert mode

Answer: D

NEW QUESTION 55
URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required"

A. RAD Kernel Space
B. URLF Kernel Client
C. URLF Online Service
D. RAD User Space

Answer: B

NEW QUESTION 56

What process monitors, terminates, and restarts critical Check Point processes as necessary?

A. CPWD
B. CPM
C. FWD
D. FWM

Answer: A

NEW QUESTION 57
What table does the command "fwaccel conns" pull information from?

A. fwxl_conns
B. SecureXLCon
C. cphwd_db
D. sxl_connections

Answer: A

NEW QUESTION 58
Which Threat Prevention Daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd
B. in.msd
C. ted
D. scrub

Answer: C

NEW QUESTION 63
Where do Protocol parsers register themselves for IPS?

A. Passive Streaming Library
B. Other handlers register to Protocol parser
C. Protections database
D. Context Management Infrastructure

Answer: A

NEW QUESTION 65
What is the best way to resolve an issue caused by a frozen process?

A. Reboot the machine
B. Restart the process
C. Kill the process
D. Power off the machine

Answer: B

NEW QUESTION 70
How can you increase the ring buffer size to 1024 descriptors?

A. set interface eth0 rx-ringsize 1024
B. fw ctl int rx_ringsize 1024
C. echo rx_ringsize=1024>>/etc/sysconfig/sysctl.conf
D. dbedit>modify properties firewall_properties rx_ringsize 1024

Answer: A

NEW QUESTION 72
Which situation triggers an IPS bypass under load on a 24-core Check Point appliance?

A. any of the CPU cores is above the threshold for more than 10 seconds
B. all CPU core most be above the threshold for more than 10 seconds
C. a single CPU core must be above the threshold for more than 10 seconds, but is must be the same core during this time
D. the average cpu utilization over all cores must be above the threshold for 1 second

Answer: A

NEW QUESTION 77
When debugging is enabled on firewall kernel module using the ‘fw ctl debug’ command with required options, many debug messages are provided by the kernel that help the administrator to identify issues. Which of the following is true about these debug messages generated by the kernel module?

A. Messages are written to a buffer and collected using ‘fw ctl kdebug’
B. Messages are written to console and also /var/log/messages file

C. Messages are written to /etc/dmesg file
D. Messages are written to $FWDIR/log/fw.elg

Answer: B

NEW QUESTION 79
What is the name of the VPN kernel process?

A. VPNK
B. VPND
C. CVPND
D. FWK

Answer: A

NEW QUESTION 84
When running a debug with fw monitor, which parameter will create a more verbose output?

A. -i
B. -i
C. -0
D. -d

Answer: D

NEW QUESTION 86
What is the benefit of running "vpn debug trunc over "vpn debug on"?

A. "vpn debug trunc" purges ike.elg and vpnd elg and creates limestarnp while starting ike debug and vpn debug
B. "vpn debug trunc* truncates the capture hence the output contains minimal capture
C. "vpn debug trunc* provides verbose capture
D. No advantage one over the other

Answer: A

NEW QUESTION 89
What are the four ways to insert an FW Monitor into the firewall kernel chain?

A. Relative position using location, relative position using alias, absolute position, all positions
B. Absolute position using location, absolute position using alias, relative position, all positions
C. Absolute position using location, relative position using alias, general position, all positions
D. Relative position using geolocation, relative position using inertial navigation, absolute position, all positions

Answer: D

NEW QUESTION 92
What command sets a specific interface as not accelerated?

A. noaccel-s<interface1>
B. fwaccel exempt state <interface1>
C. nonaccel -s <interface1>
D. fwaccel -n <intetface1 >

Answer: C

NEW QUESTION 94
To check the current status of hyper-threading, which command would you execute in expert mode?

A. cat /proc/hypert_status
B. cat /proc/smt_status
C. cat /proc/hypert_stat
D. cat /proc/smt_stat

Answer: B

NEW QUESTION 99
What is the main SecureXL database for tracking acceleration status of traffic?

A. cphwd_db
B. cphwd_tmp1
C. cphwd_dev_conn_table
D. cphwd_dev_identity_table

Answer: B

NEW QUESTION 102
An administrator receives reports about issues with log indexing and text searching regarding an existing Management Server. In trying to find a solution she wants to check if the process responsible for this feature is running correctly. What is true about the related process?

A. fwm manages this database after initialization of the ICA
B. cpd needs to be restarted manual to show in the list
C. fwssd crashes can affect therefore not show in the list
D. solr is a child process of cpm

Answer: D

NEW QUESTION 106
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

156-585 Practice Exam Features:

* 156-585 Questions and Answers Updated Frequently

* 156-585 Practice Questions Verified by Expert Senior Certified Staff

* 156-585 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-585 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year