Number: 156-585
Passing Score: 800
Time Limit: 120
File Version: 7.0

Exam Code: 156-585

Exam Name: Check Point Certified Troubleshooting Expert

Exam A

QUESTION 1
What command is used to find out which port Multi-Portal has assigned to the Mobile Access Portal?

A. mpclient getdata sslvpn
B. netstat -nap | grep mobile
C. mpclient getdata mobi
D. netstat getdata sslvpn

Correct Answer: D
Section:

QUESTION 2
VPN's allow traffic to pass through the Internet securely by encrypting the traffic as it enters the VPN tunnel and then decrypting the exists. Which process is responsible for Mobile VPN connections?

A. cvpnd
B. vpnd
C. vpnk
D. fwk

Correct Answer: D
Section:

QUESTION 3
Which of the following is contained in the System Domain of the Postgres database?

A. Saved queries for applications
B. Configuration data of log servers
C. Trusted GUI clients
D. User modified configurations such as network objects

Correct Answer: C
Section:

QUESTION 4
Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS. and compiles them together into unified Pattern Matchers?

A. CMI Loader
B. cpas
C. PSL - Passive Signature Loader
D. Context Loader

Correct Answer: A
Section:

QUESTION 5
Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
C. $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/
D. $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

Correct Answer: A
Section:

QUESTION 6
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore you need to add a timestamp to the kernel debug and write the output to a file What is the correct syntax for this?

A. fw ctl kdebug -T -f > filename.debug
B. fw ctl kdebug -T > filename.debug
C. fw ctl debug -T -f > filename.debug
D. fw ctl kdebug -T -f -o filename.debug

Correct Answer: A
Section:

QUESTION 7
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

Correct Answer: A
Section:

QUESTION 8
Which Threat Prevention daemon is the core Threat Emulator, engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd
B. inmsd
C. ted
D. scrub

Correct Answer: C

Section:
Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

QUESTION 9
John has renewed his NGTX License but he gets an error (contract for Anti-Bot expired). He wants to check the subscription status on the CU of the gateway, what command can he use for this?

A. cpstat antimalware -f subscription_status
B. fw monitor license status
C. fwm lie print
D. show license status

Correct Answer: A
Section:

QUESTION 10
During firewall kernel debug with fw ctl zdebug you received less information than expected. You noticed that a lot of messages were lost since the time the debug was started. What should you do to resolve this issue?

A. Increase debug buffer; Use fw ctl debug –buf 32768
B. Redirect debug output to file; Use fw ctl zdebug –o ./debug.elg
C. Increase debug buffer; Use fw ctl zdebug –buf 32768
D. Redirect debug output to file; Use fw ctl debug –o ./debug.elg

Correct Answer: A
Section:
Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/Content/Topics-PTG/Kernel-Debug/Kernel-Debug-Procedure.htm

QUESTION 11
Which process is responsible for the generation of certificates?

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

Correct Answer: B
Section:

QUESTION 12
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 >

Correct Answer: C
Section:

QUESTION 13
When running a debug with fw monitor, which parameter will create a more verbose output?

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

Correct Answer: D
Section:

QUESTION 14
What is connect about the Resource Advisor (RAD) service on the Security Gateways?

A. RAD has a kernel module that looks up the kernel cache, notifies client about hits and misses and forwards a-sync requests to RAD user space module which is responsible for online categorization
B. RAD is completely loaded as a kernel module that looks up URL in cache and if not found connects online for categorization There is no user space involvement in this process
C. RAD functions completely in user space The Pattern Matter (PM) module of the CMI looks up for URLs in the cache and if not found, contact the RAD process in user space to do online categorization
D. RAD is not a separate module, it is an integrated function of the 'fw1 kernel module and does all operations in the kernel space

Correct Answer: C
Section:

QUESTION 15
What are some measures you can take to prevent IPS false positives?

A. Exclude problematic services from being protected by IPS (sip, H 323, etc)
B. Use IPS only in Detect mode
C. Use Recommended IPS profile
D. Capture packets. Update the IPS database, and Back up custom IPS files

Correct Answer: A
Section:

QUESTION 16
RAD is initiated when Application Control and URL Filtering blades are active on the Security Gateway What is the purpose of the following RAD configuration file SFWDIR/conf/rad_settings.C?

A. This file contains the location information tor Application Control and/or URL Filtering entitlements
B. This file contains the information on how the Security Gateway reaches the Security Managers RAD service for Application Control and URL Filtering
C. This file contains RAD proxy settings
D. This file contains all the host name settings for the online application detection engine

Correct Answer: C
Section:

QUESTION 17
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

Correct Answer: A
Section:

QUESTION 18
What is the buffer size set by the fw ctl zdebug command?

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

Correct Answer: A
Section:

QUESTION 19
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

Correct Answer: A
Section:

QUESTION 20
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 deamon 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 cant be debugged

Correct Answer: D
Section:

QUESTION 21
Which of the following daemons is used for Threat Extraction?

A. scrubd
B. extractd
C. tex
D. tedex

Correct Answer: A
Section:

QUESTION 22
You are upgrading your NOC Firewall (on a Check Point Appliance) from R77 to R80 30 but you did not touch the security policy After the upgrade you can't connect to the new R80 30 SmartConsole of the upgraded Firewall anymore What is a possible reason for this?

A. new new console port is 19009 and a access rule ts missing
B. the license became invalig and the firewall does not start anymore
C. the upgrade process changed the interfaces and IP adresses and you have to switch cables
D. the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall

Correct Answer: D
Section:

QUESTION 23
What are the main components of Check Point's Security Management architecture?

A. Management server, management database, log server, automation server
B. Management server, Security Gateway. Multi-Domain Server, SmartEvent Server
C. Management Server. Log Server. LDAP Server, Web Server
D. Management server Log server, Gateway server. Security server

Correct Answer: A
Section:

QUESTION 24
What does SIM handle?

A. Accelerating packets
B. FW kernel to SXL kernel hand off
C. OPSEC connects to SecureXL
D. Hardware communication to the accelerator

Correct Answer: D
Section:

QUESTION 25
VPN issues may result from misconfiguration, communication failure, or incompatible default configurations between peers Which basic command syntax needs to be used for troubleshooting Site-to-Site VPN Issues?

A. vpn debug truncon
B. fw debug truncon

C. cp debug truncon
D. vpn truncon debug

Correct Answer: A
Section:

QUESTION 26
Select the technology that does the following actions
- provides reassembly via streaming for TCP
- handles packet reordering and congestion
- handles payload overlap
- provides consistent stream of data to protocol parsers

A. Passive Streaming Library
B. Context Management
C. Pre-Protocol Parser
D. fwtcpstream

Correct Answer: A
Section:

QUESTION 27
What is the kernel process for Content Awareness that collects the data from the contexts received from the CMI and decides if the file is matched by a data type?

A. dlpda
B. dlpu
C. cntmgr
D. cntawmod

Correct Answer: A
Section:

QUESTION 28
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 *

Correct Answer: D
Section:

QUESTION 29
What is the purpose of the Hardware Diagnostics Tool?

A. Verifying that Check Point Appliance hardware is functioning correctly

B. Verifying the Security Management Server hardware is functioning correctly
C. Verifying that Security Gateway hardware is functioning correctly
D. Verifying that Check Point Appliance hardware is actually broken

Correct Answer: A
Section:
Explanation:
https://support.checkpoint.com/results/sk/sk97251

QUESTION 30
What table does the command "fwaccel conns" pull information from?

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

Correct Answer: A
Section:

QUESTION 31
Check Point Threat Prevention policies can contain multiple policy layers and each layer consists of its own Rule Base Which Threat Prevention daemon is used for Anti-virus?

A. in.emaild.mta
B. in.msd
C. ctasd
D. in emaild

Correct Answer: D
Section:

QUESTION 32
Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0, choose the correct answer.

A. fw monitor –po -0x1ffffe0
B. fw monitor –p0 ox1ffffe0
C. fw monitor –po 1ffffe0
D. fw monitor –p0 –ox1ffffe0

Correct Answer: A
Section:
Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/Content/Topics-PTG/CLI/fw-monitor.htm

QUESTION 33
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 problem
Pre-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 problem
Pre-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 problem
Pre-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

Correct Answer: B
Section:

QUESTION 34
Your fwm constantly crashes and is restarted by the watchdog. You can't find any coredumps related to this process, so you need to check If coredumps are enabled at all How can you achieve that?

A. in dish run show core-dump status
B. in expert mode run show core-dump status
C. in dish run set core-dump status
D. in dish run show coredumb status

Correct Answer: A
Section:
Explanation:
https://support.checkpoint.com/results/sk/sk92764

QUESTION 35
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

Correct Answer: B
Section:

QUESTION 36
John works for ABC Corporation. They have enabled CoreXL on their firewall John would like to identify the cores on which the SND runs and the cores on which the firewall instance is running.
Which command should John run to view the CPU role allocation?

A. fw ctl affinity -v
B. fwaccel stat -l
C. fw ctl affinity -l
D. fw ctl cores

Correct Answer: C

Section:

QUESTION 37
Which of the following is NOT a valid "fwaccel" parameter?

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

Correct Answer: D
Section:
Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk41397

QUESTION 38
Which Daemon should be debugged for HTTPS Inspection related issues?

A. FWD
B. HTTPD
C. WSTLSO
D. VPND

Correct Answer: C
Section:

QUESTION 39
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

Correct Answer: A
Section:

QUESTION 40
Which of the following inputs is suitable for debugging HTTPS inspection issues?

A. vpn debug cptls on
B. fw ctl debug –m fw + conn drop cptls
C. fw diag debug tls enable
D. fw debug tls on TDERROR_ALL_ALL=5

Correct Answer: B
Section:

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

QUESTION 41
What is the correct syntax to turn a VPN debug on and create new empty debug files?

A. vpn debug truncon
B. vpndebug trunc on
C. vpn kdebug on
D. vpn debug trunkon

Correct Answer: A
Section:

QUESTION 42
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

Correct Answer: A
Section:

QUESTION 43
Check Point Access Control Daemons contains several daemons for Software Blades and features Which Daemon is used for Application & Control URL Filtering?

A. rad
B. cprad
C. pepd
D. pdpd

Correct Answer: A
Section:

QUESTION 44
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

Correct Answer: A

Section:

QUESTION 45
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'

Correct Answer: A
Section:

QUESTION 46
What acceleration mode utlizes multi-core processing to assist with traffic processing?

A. CoreXL
B. SecureXL
C. HyperThreading
D. Traffic Warping

Correct Answer: C
Section:

QUESTION 47
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

Correct Answer: D
Section:

QUESTION 48
The Check Pom! Firewall Kernel is the core component of the Gaia operating system and an integral part of the traffic inspection process There are two procedures available for debugging the firewall kernel Which procedure/command is used for troubleshooting packet drops and other kernel activites while using minimal resources (1 MB buffer)?

A. fw ctl zdebug
B. fw ctl debug/kdebug
C. fwk ctl debug
D. fw debug ctl

Correct Answer: A
Section:

QUESTION 49
If you run the command "fw monitor -e accept src=10.1.1.201 or src=172.21.101.10 or src=192.0.2.10;" from the cli sh What will be captured?

A. Packets from 10 1 1 201 going to 192.0 2.10
B. Packets destined to 172 21 101 10 from 10.1.1.101
C. Only packet going to 192.0.2.10
D. fw monitor only works in expert mode so no packets will be captured

Correct Answer: C
Section:

QUESTION 50
When a User Mode process suddenly crashes it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash? i Program Counter ii Stack Pointer ii. Memory management information iv Other Processor and OS flags / information

A. i, ii, lii and iv
B. i and n only
C. iii and iv only
D. D Only iii

Correct Answer: C
Section:

QUESTION 51
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

Correct Answer: A
Section:
Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk62848&partition=Advanced&product=IPS

QUESTION 52
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>

Correct Answer: C
Section:

QUESTION 53
Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. core dump
B. CPMIL dump
C. fw monitor
D. tcpdump

Correct Answer: A
Section:

QUESTION 54
The two procedures available for debugging in the firewall kernel are i fw ctl zdebug ii fw ctl debug/kdebug Choose the correct statement explaining the differences in the two

A. (i) Is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to get an output via command line whereas (11) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line
B. (i) is used to debug the access control policy only, however (n) can be used to debug a unified policy
C. (i) is used to debug only issues related to dropping of traffic, however (n) can be used for any firewall issue including NATing, clustering etc.
D. (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server

Correct Answer: C
Section:

QUESTION 55
What is the name of the VPN kernel process?

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

Correct Answer: A
Section:

QUESTION 56
You are running R80.XX on an open server and you see a high CPU utilization on your 12 CPU cores You now want to enable Hyperthreading to get more cores to gain some performance. What is the correct way to achieve this?

A. Hyperthreading is not supported on open servers, on on Check Point Appliances
B. just turn on HAT in the bios of the server and boot it
C. just turn on HAT in the bios of the server and after it has booted enable it in cpconfig
D. in dish run set HAT on

Correct Answer: A

Section:

QUESTION 57
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

Correct Answer: A
Section:

QUESTION 58
Which daemon governs the Mobile Access VPN blade and works with VPND to create Mobile Access VPN connections? It also handles interactions between HTTPS and the Multi-Portal Daemon.

A. Connectra VPN Daemon - cvpnd
B. Mobile Access Daemon - MAD
C. mvpnd
D. SSL VPN Daemon - sslvpnd

Correct Answer: A
Section:

QUESTION 59
You are trying to establish a VPN tunnel between two Security Gateways but fail. What initial steps will you make to troubleshoot the issue

A. capture traffic on both tunnel members and collect debug of IKE and VPND daemon
B. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags, then collect debug of IKE and VPND daemon
C. collect debug of IKE and VPND daemon and collect kernel debug for fw module with vm, crypt, conn and drop flags
D. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags

Correct Answer: A
Section:

QUESTION 60
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

Correct Answer: D
Section:

QUESTION 61
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

Correct Answer: B
Section:

QUESTION 62
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

Correct Answer: A
Section:

QUESTION 63
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

Correct Answer: D
Section:

QUESTION 64
Which command can be run in Expert mode to verify the core dump settings?

A. grep cdm /config/db/coredump
B. grep cdm /config/db/initial
C. grep $FWDIR/config/db/initial
D. cat /etc/sysconfig/coredump/cdm.conf

Correct Answer: C
Section:

QUESTION 65
What process is responsible for sending and receiving logs in the management server?

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

Correct Answer: A
Section:

QUESTION 66
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

Correct Answer: B
Section:

QUESTION 67
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

Correct Answer: D
Section:

QUESTION 68
What process monitors, terminates, and restarts critical Check Point processes as necessary?

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

Correct Answer: A
Section:

QUESTION 69
The Check Point Firewall Kernel is the core component of the Gala operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

A. fw ctl debug/kdebug

B. fw ctl zdebug
C. fw debug/kdebug
D. fw debug/kdebug ctl

Correct Answer: B
Section:

QUESTION 70
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 site. 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
B. Tunnel fails on partner site. 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.
C. Tunnel fails on Joey's site, because he misconfigured IP address of VPN peer.
D. Tunnel falls on partner site. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

Correct Answer: B
Section:

QUESTION 71
Which kernel process is used by Content Awareness to collect the data from contexts?

A. dlpda
B. PDP
C. cpemd
D. CMI

Correct Answer: D
Section:

QUESTION 72
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore, you need to add a timestamp to the kernel debug and write the output to a file but you can't afford to fill up all the remaining disk space and you only have 10 GB free for saving the debugs. What is the correct syntax for this?

A. fw ctl kdebug -T -f -m 10 -s 1000000 -o debugfilename
B. fw ctl kdebug -T -f -m 10 -s 1000000 > debugfilename
C. fw ctl kdebug -T -m 10 -s 1000000 -o debugfilename
D. fw ctl debug -T -f -m 10 -s 1000000 -o debugfilename

Correct Answer: D
Section:

QUESTION 73
Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

A. cpstat
B. CPstat
C. CPview
D. fwstat

Correct Answer: A
Section:

QUESTION 74
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

Correct Answer: D
Section:

QUESTION 75
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

Correct Answer: A
Section:

QUESTION 76
What is the most efficient way to view large fw monitor captures and run filters on the file?

A. wireshark
B. CLISH
C. CLI
D. snoop

Correct Answer: A
Section:

QUESTION 77
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

Correct Answer: C
Section:

QUESTION 78
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

Correct Answer: B
Section:

QUESTION 79
What is the correct syntax to set all debug flags for Unified Policy related issues?

A. fw ctl debug -m UP all
B. fw ctl debug -m up all
C. fw ctl kdebug -m UP all
D. fw ctl debug -m fw all

Correct Answer: A
Section:

QUESTION 80

Some users from your organization have been reported 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 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 -pl 5 -e <filterexpression>
B. fw monitor -pi 5 -e <filterexpression>
C. tcpdump -eni any <filterexpression>
D. fw monitor -pl asm <filterexpression>

Correct Answer: A
Section: