

ITExamReview

LOGIN / REGISTER | MY CART (5)

ITExamReview HOME CERTIFICATIONS ABOUT FREE DEMO HOW TO PAY? GUARANTEE FAQ

INSTANT DOWNLOAD
FREE UPDATES

ITExamReview- useful and reliable platform for your certification exam

Try before you buy

Download a free sample of any of our exam questions and answers

[Download Demo](#)

- ✓ 24/7 customer support, Secure shopping site
- ✓ Free One year updates to match real exam scenarios
- ✓ If you failed your exam after buying our products we will refund the full amount back to you.

Quality and Value
ITExamReview Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Easy to Pass
If you prepare for the exams using our ITExamReview testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Tested and Approved
We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Try Before Buy
ITExamReview offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

<http://www.itexamreview.com>

Useful and reliable platform for your certification exam

Exam : **156-115.77**

Title : Check Point Certified Security Master

Vendor : CheckPoint

Version : DEMO

NO.1 When VPN user-based authentication fails, which of the following debug logs is essential to understanding the issue?

- A. VPN-1 kernel debug logs
- B. IKE.elg
- C. Vpnd.elg
- D. fw monitor trace

Answer: B

NO.2 How do you set up Port Address Translation?

- A. Since Hide NAT changes to random high ports it is by definition PAT (Port Address Translation).
- B. Create a manual NAT rule and specify the source and destination ports.
- C. Edit the service in SmartDashboard, click on the NAT tab and specify the translated port.
- D. Port Address Translation is not support in Check Point environment

Answer: B

NO.3 You run the command `fw tab -t connections -s` on both members in the cluster. Both members report differing values for "vals" and "peaks". Which may NOT be a reason for this difference?

- A. Synchronization is not working between the two members
- B. SGMs in a 61k environment only sync selective parts of the connections table.
- C. Heavily used short-lived services have had synchronization disabled for performance improvement.
- D. Standby member does not synchronize until a failover is needed.

Answer: D

NO.4 You are trying to troubleshoot a NAT issue on your network, and you use a kernel debug to verify a connection is correctly translated to its NAT address. What flags should you use for the kernel debug?

- A. `fw ctl debug -m fw + conn drop nat vm xlate xltrc`
- B. `fw ctl debug -m fw + conn drop ld`
- C. `fw ctl debug -m nat + conn drop nat xlate xltrc`
- D. `fw ctl debug -m nat + conn drop fw xlate xltrc`

Answer: A

NO.5 Which command should you use to stop kernel module debugging (excluding SecureXL)?

- A. `fw ctl debug 0`
- B. `fw ctl zdebug - all`
- C. `fw debug fwd off; vpn debug off`
- D. `fw debug fwd off`

Answer: A

NO.6 Which command clears all the connection table entries on a Security Gateway?

- A. `fw tab -t connetion -u`
- B. `fw ctl tab -t connetions -u`

- C. fw tab -t connetion -s
- D. fw tab -t connections -x

Answer: D

NO.7 When finished running a debug on the Management Server using the command fw debug fwm on how do you turn this debug off?

- A. fwm debug off
- B. fw ctl debug off
- C. fw debug off
- D. fw debug fwm off

Answer: D

NO.8 Since switching your network to ISP redundancy you find that your outgoing static NAT connections are failing. You use the command _____ to debug the issue.

- A. fwaccel stats misp
- B. fw ctl pstat
- C. fw ctl debug -m fw + nat drop
- D. fw tab -t fwx_alloc -x

Answer: C

NO.9 What is the prefix name for the interface when creating an unnumbered VTI in GAIA?

- A. VTii
- B. tun
- C. vpnt
- D. VTI

Answer: C

NO.10 Where do you configure the file user.def to change the encryption domain of the Security Gateway?

- A. Management Server
- B. Endpoint Client
- C. Security Gateway
- D. interoperable device

Answer: A

NO.11 You are experiencing an issue where Endpoint Connect client connects successfully however, it disconnects every 20 seconds. What is the most likely cause of this issue?

- A. The Accept Remote Access control connections is not enabled in Global Properties > FireWall Implied Rules.
- B. You have selected IKEv2 only in Global Properties > Remote Access > VPN - Authentication and Encryption.
- C. You are not licensed for Endpoint Connect client.
- D. Your remote access community is not configured.

Answer: A

NO.12 In a ClusterXL cluster with delayed synchronization, which of the following is not true?

- A. The length of time for the delay can be edited.
- B. It applies only to TCP services whose Protocol Type is set to HTTP or None.
- C. Delayed Synchronization is disabled if the Track option in the rule is set to Log or Account.
- D. Delayed Synchronization is performed only for connections matching a SecureXL Connection Template.

Answer: A

NO.13 ACME Corp has a cluster consisting of two 13500 appliances. As the Firewall Administrator, you notice that on an output of top, you are seeing high CPU usage of the cores assigned as SNDs, but low CPU usage on cores assigned to individual fw_worker_X processes. What command should you run next to performance tune your cluster?

- A. fw ctl debug -m cluster + all - this will show you all the connections being processed by ClusterXL and explain the high CPU usage on your appliance.
- B. fwaccel off - this will turn off SecureXL, which is causing your SNDs to be running high in the first place.
- C. fwaccel stats -s - this will show you the acceleration profile of your connections and potentially why your SNDs are running high while other cores are running low.
- D. fw tab -t connections -s - this will show you a summary of your connections table, and allow you to determine whether there is too much traffic traversing your firewall.

Answer: C

Explanation:

Topic 8, Enable CoreXL

NO.14 Which file holds global Kernel values to survive reboot in a Check Point R77 gateway?

- A. \$FWDIR/conf/fwkernel.conf
- B. \$FWDIR/boot/modules/fwkernel.conf
- C. \$FWDIR/boot/confkernel.conf
- D. \$FWDIR/boot/fwkernel.conf

Answer: B

NO.15 When troubleshooting and trying to understand which chain is causing a problem on the Security Gateway, you should use the command:

- A. fw ctl zdebug drop
- B. fw tab -t connections
- C. fw monitor -e "accept;" -p all
- D. fw ctl chain

Answer: C

NO.16 Which of the following statements about Full HA support with IPv6 is NOT true?

- A. There is no Dynamic Routing with IPv6.

- B. Mirrored Interfaces must have IPv4 addresses.
- C. Sync traffic must be IPv4.
- D. IPv6 does not support a Secondary Management Server.

Answer: D

Explanation:

Topic 11, Advanced VPN

NO.17 What is the function of the setting "no_hide_services_ports" in the tables.def files?


- A. Preventing the secondary member from hiding its presence by not forwarding any packets.
- B. Allowing management traffic to be accepted in an applied rule ahead of the stealth rule.
- C. Hiding the particular tables from being synchronized to the other cluster member.
- D. Preventing outbound traffic from being hidden behind the cluster IP address.

Answer: D

Explanation:

Topic 4, VPN Troubleshooting

NO.18 Look at the follow Rule Base display. Rule 5 contains a TIME object. What is the effect on the following rules?



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment
<div style="background-color: #ffffcc; padding: 2px;"> Limit Access to Gateways Rule (Rule 1) </div> <div style="background-color: #ffffcc; padding: 2px;"> Rules for Specific Sites (Rules 2-4) </div> <div style="background-color: #ffffcc; padding: 2px;"> Common Rules - All Sites (Rules 5-10) </div>											
5	0	contractor access	Tech-Support	SMTPServer	Any Traffic	ssh	accept	Log	Policy Targets	Work-Hours	TIME object to provide limited a for contractor access.
6	428K	Mail and Web servers	Corporate-inte	Corporate-dmz	Any Traffic	http https smtp	accept	Log	Policy Targets	Any	Mail 4/1/2014 -Delinsky
7	55K	DNS server	Corporate-inte	Corporate-dns	Any Traffic	domain-udp	accept	Log	Policy Targets	Any	Allow domain name queries to external DNS server
8	4K	SMTP	Corporate-mail	Internal-net-gr	Any Traffic	smtp	accept	Log	Policy Targets	Any	Allow outgoing SMTP connectio but don't allow the mail server t initiate connections to the inter networks, in case it is compromi
9	1M	DMZ and Internet	Internal-net-gr	Any	Any Traffic	http https	accept	Log	Policy Targets	Any	User access to DMZ servers and Internet
10	3K	Clean up rule	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Clean up rule - block all other connections

©2014 Check Point Software Technologies Ltd. 6

Checkpoint 156-115.77 Exam

- A. Rule 6 will be eligible but Rule 7 will not.
- B. All subsequent rules below Rule 5 will not be templated, regardless of the rule
- C. No effect. Rules 6 and 7 will be eligible for templating.
- D. The restriction on one rule does not affect later rules with regards to templates.

Answer: B