Vendor: CheckPoint

Exam Code:156-115.77

Exam Name: Check Point Certified Security Master

Version: Demo

QUESTION 1

"Tuning" IPS protections to suit the specific needs of an environment can be accomplished by all of the following EXCEPT:

A. Focusing on high confidence level protections.

B. Focusing on low capacity protections.

C. Focusing on low performance impact protections.

D. Focusing on high severity protections.

Correct Answer: B

QUESTION 2

In a VPN configuration, the following mode can be used to increase throughput by bypassing firewall enforcement.

A. Virtual Tunnel Interface (VTI) Mode can bypass firewall for all encrypted traffic

B. Hub Mode can be used to bypass stateful inspection

C. There is no such mode that can bypass firewall enforcement

D. Wire mode can be used to bypass stateful inspection

Correct Answer: D

QUESTION 3

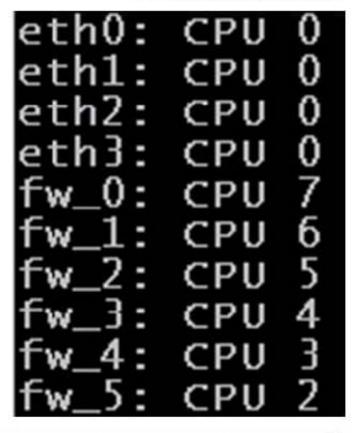Where would an administrator set an email alert for a specific permanent VPN tunnel?

A. Edit the file vpnconf.

B. Run sysconfig.

C. In the Tunnel Properties select Mail Alert.

D. You can only enable logging or SNMP traps.

Correct Answer: C

QUESTION 4

Your customer has a well optimized Rule Base with most traffic accelerated by SecureXL. They are still seeing slow performance. They are using an 8 core machine. They see the following output from fw ctl affinity -l. What could be done to improve performance with this deployment?

A. Increase the number of cores dedicated to logging.

B. Increase the number of Secure Network Dispatchers as the accelerated traffic is not passed to a worker core.

C. Add more CPU resources to the hardware.

D. Upgrade to SAM hardware.

Correct Answer: B

QUESTION 5

What is the command to check how many connections the firewall has detected for the SecureXL device?

A. fw tab t connections s

B. fw tab -t cphwd_db s

C. fw tab t connection s | grep template

D. fwaccel conns

Correct Answer: B

QUESTION 6

What debug file would you check to see what IKE version is being used?

A. fwpnd.elg

B. vpn.txt

C. debug.txt

D. vpnd.elg

Correct Answer: D

QUESTION 7

What would be considered Best Practice to determine which IPS protections you can safely disable for your environment?

A. You should use vulnerability tools to perform an assessment of your environment.

B. Work through turning on each protection to see which signatures get alerts.

C. You should set all protections to "Detect".

D. You should not disable any IPS protections.

Correct Answer: A

QUESTION 8

Which of the following is a valid synchronization status as an output to fw ctl pstat?

A. Unable to receive sync packets

B. Sync member down

C. Synchronized

D. Communicating

Correct Answer: A

QUESTION 9

Which command would a troubleshooter use to verify table connection info (peak, concurrent) and verify information about cluster synchronization state?
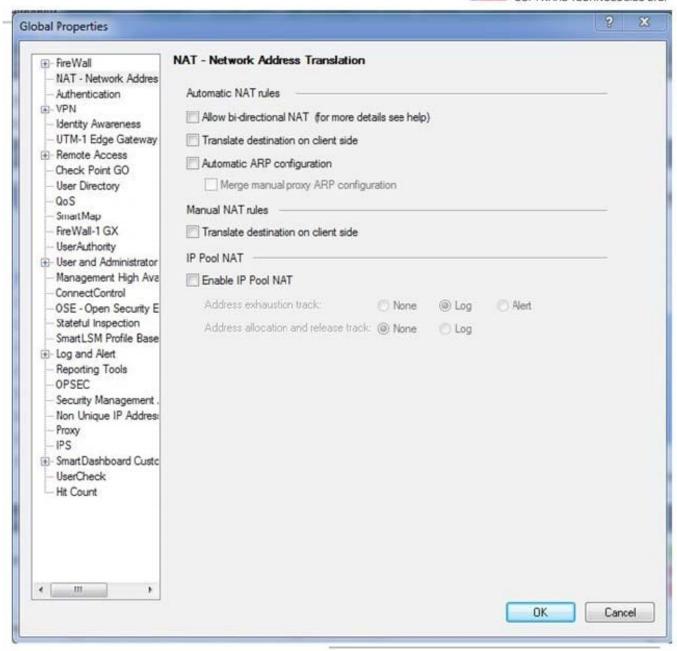
A. fw tab t connections s

B. fw ctl pstat

C. fw ctl multik stat

D. Show info all

Correct Answer: D

QUESTION 10

Which command displays FireWall internal statistics about memory and traffic?

A. fw getifs

B. cpstat os f memory

C. fw ctl pstat

D. cpstat os f cpu

Correct Answer: C

QUESTION 11

Tom has a Web server for which he has created a manual NAT rule. The rule is not working. He tries to initiate a connection from the external network to a DMZ server using the public IP which the firewall translates to the actual IP of the server. He analyzes the captured packets using Wireshark and observes that the destination IP is being changed as required by the firewall but does not see the packet leave the internal interface. Which box in Global Properties should be checked?

Global Properties   ? X

NAT – Network Address Translation

- FireWall
- NAT - Network Addres
- Authentication
- VPN
- Identity Awareness
- UTM-1 Edge Gateway
- Remote Access
- Check Point GO
- User Directory
- QoS
- SmartMap
- FireWall-1 GX
- UserAuthority
- User and Administrator
- Management High Ava
- ConnectControl
- OSE - Open Security E
- Stateful Inspection
- SmartLSM Profile Base
- Log and Alert
- Reporting Tools
- OPSEC
- Security Management .
- Non Unique IP Address
- Proxy
- IPS
- SmartDashboard Custc
- UserCheck
- Hit Count

Automatic NAT rules

- ☐ Allow bi-directional NAT (for more details see help)
- ☐ Translate destination on client side
- ☐ Automatic ARP configuration
    - ☐ Merge manual proxy ARP configuration

Manual NAT rules

- ☐ Translate destination on client side

IP Pool NAT

- ☐ Enable IP Pool NAT

  Address exhaustion track: ○ None   ◉ Log   ○ Alert
  Address allocation and release track: ◉ None   ○ Log

OK   Cancel

A. Automatic NAT rules > Allow bi-directional NAT

B. Automatic NAT rules > Automatic ARP Configuration

C. Automatic NAT rules > Translate destination on client side

D. Manual NAT rules > Translate destination on client side

Correct Answer: D

QUESTION 12

You have spent time configuring the IPS profile on your primary gateway firewall. You want to ensure that this profile can be applied to all gateway firewalls in your environment. How can you share this information between firewalls?

A. From the command line, run: ips_export [-o] [-p].

B. IPS profiles must be manually configured on each gateway.

C. From the Smart Dashboard IPS tab select export IPS profiles and select the gateway to send this export to.

D. From the command line, run: ips_export_import export [-o] [-p].

Correct Answer: D