

Checkpoint

Exam 156-515-65

Check Point Certified Security Expert Plus NGX R65

Version: 3.0

[Total Questions: 70]

Question No : 1

NGX Wire Mode allows:

- A. Peer gateways to establish a VPN connection automatically from predefined presharedsecrets.
- B. Administrators to verify that each VPN-1 SecureClient is properly configured, before allowing it access to the protected domain.
- C. Peer gateways to fail over existing VPN traffic, by avoiding Stateful Inspection.
- D. Administrators to monitor VPN traffic for troubleshooting purposes.
- E. Administrators to limit the number of simultaneous VPN connections, to reduce the traffic load passing through a Security Gateway.

Answer: C

Question No : 2

To stop the sr_service debug process, you must first stop VPN-1 SecureClient, delete which of the following files, and restart SecureClient?

- A. sr_auth.all
- B. sr_topo.all
- C. sr_tde.all
- D. sr_service.all
- E. sr_users.all

Answer: C

Question No : 3

When Network Address Translation is used:

- A. VLAN tagging cannot be defined for any hosts protected by the Gateway
- B. It is not necessary to add a static route to the Gateway's routing table.
- C. The Security Gateway's ARP file must be modified.
- D. The Gateway's Imhosts file must be modified.
- E. It is necessary to add a static route to the Gateway's routing table.

Answer: B

Question No : 4

How can you view cpinfo on a SecurePlatform Pro machine?

- A. snoop -i
- B. infotab
- C. tcpdump
- D. Text editor, such as vi
- E. infoview

Answer: D

Question No : 5

After a sudden spike in traffic, you receive this system log file message:

"kernel: FW-1: Log buffer is full".

Which is NOT a solution?

- A. Increase the log buffer size.
- B. Disable logging.
- C. Reconfigure the minimum disk space "stop logging" threshold.
- D. Decrease the amount of logging.

Answer: C

Question No : 6

When you verify IP forwarding on SecurePlatform Pro using the command more

/proc/sys/net/ipv4/ip_forward, what value should be stored in the resulting file?

- A. Y
- B. P
- C. 1
- D. 0
- E. 4

Answer: C

Question No : 7

If you run only fw monitor without any parameters, where does the output display?

- A. In /tmp/log/monitor.out
- B. In \$FWDIR/bin
- C. In /var/log/monitor.out
- D. On the console
- E. In /var/adm/monitor.out

Answer: D

Question No : 8

fw monitor packets are collected from the kernel in a buffer. What happens if the buffer becomes full?

- A. The information in the buffer is saved and packet capture continues, with new data stored in the buffer.
- B. Older packet information is dropped as new packet information is added.
- C. Packet capture stops.
- D. All packets in it are deleted, and the buffer begins filling from the beginning.

Answer: D

Question No : 9

Which file provides the data for the host_table output, and is responsible for keeping a record of all internal IPs passing through the internal interfaces of a restricted hosts licensed Security Gateway?

- A. hosts.h
- B. external.if
- C. hosts
- D. fwd.h
- E. fwconn.h

Answer: D

Question No : 10

You have installed SecurePlatform R60 as Security Gateway operating system. As company requirements changed, you need the VTI features of NGX. What should you do?

- A. In SmartDashboard click on the OS drop down menu and choose SecurePlatform Pro. You have to reboot the Security Gateway in order for the change to take effect
- B. Only IPSO 3.9 supports VTI feature, so you have to replace your Security Gateway with Nokia appliances
- C. You have to re-install your Security Gateway with SecurePlatform Pro R60, as SecurePlatform R60 does not support VTIs
- D. Nothing, because SPLAT R60 does support VTIs
- E. Type "pro enable" on your Security Gateway and reboot it

Answer: E

Question No : 11

Each module within the NGX kernel contains specific debugging flags. Which of the statements is true concerning kernel-debug flags?

- A. Debugging flags are universal across all modules.
- B. Debug flags cannot be disabled.
- C. Debugging flags can be configured to produce varying levels of information.
- D. Debug flags require an administrator to set them.
- E. Each flag is generic and cannot be modified to produce varying levels of information.

Answer: C

Question No : 12

Policy Server login and Desktop Policy installation will kill which of the following processes on the

client machine?