Checkpoint

Exam 156-915.77

Check Point Certified Security Expert Update

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Deployment Platforms Obj 1	1
Topic 4: Network Address Translation	3
Topic 7: Identity Awareness Obj 1	1
Topic 10: Identity Awareness Obj 4	1
Topic 11: Advanced Firewall	1
Topic 12: Advanced upgrading	1
Topic 15: IPSEC VPN and Remote Access	1
Topic 16: SmartReporting and SmartEvent	1

Topic 1, Deployment Platforms Obj 1

Question No : 1 - (Topic 1)

Which operating systems are supported by a Check Point Security Gateway on an open server? Select MOST complete list.

A. Sun Solaris, Red Hat Enterprise Linux, Check Point SecurePlatform, IPSO, Microsoft Windows
B. Check Point GAiA and SecurePlatform, and Microsoft Windows
C. Check Point GAiA, Microsoft Windows, Red Hat Enterprise Linux, Sun Solaris, IPSO
D. Check Point GAiA and SecurePlatform, IPSO, Sun Solaris, Microsoft Windows

Answer: B

Topic 4, Network Address Translation

Question No : 2 - (Topic 4)

After implementing Static Address Translation to allow Internet traffic to an internal Web Server on your DMZ, you notice that any NATed connections to that machine are being dropped by anti-spoofing protections. Which of the following is the MOST LIKELY cause?

A. The Global Properties setting Translate destination on client side is unchecked. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mask. Check the Global Properties setting Translate destination on client side.
B. The Global Properties setting Translate destination on client side is unchecked. But the topology on the external interface is set to Others +. Change topology to External.
C. The Global Properties setting Translate destination on client side is checked. But the topology on the external interface is set to External. Change topology to Others +.
D. The Global Properties setting Translate destination on client side is checked. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mask. Uncheck the Global Properties setting Translate destination on client side.

Answer: A

Question No : 3 - (Topic 4)

A Web server behind the Security Gateway is set to Automatic Static NAT. Client side NAT is not checked in the Global Properties. A client on the Internet initiates a session to the

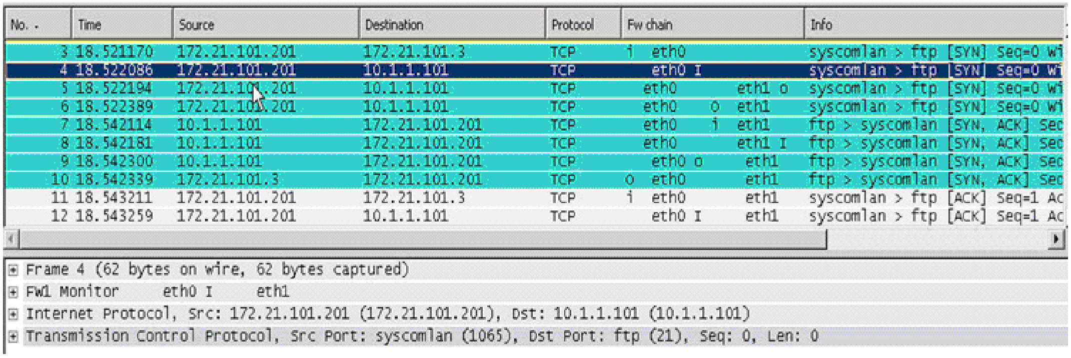
Web Server. Assuming there is a rule allowing this traffic, what other configuration must be done to allow the traffic to reach the Web server?

A. Automatic ARP must be unchecked in the Global Properties.
B. Nothing else must be configured.
C. A static route must be added on the Security Gateway to the internal host.
D. A static route for the NAT IP must be added to the Gateway's upstream router.

Answer: C

Question No : 4 - (Topic 4)

Looking at the SYN packets in the Wireshark output, select the statement that is true about NAT.



```
No. -  Time       Source            Destination       Protocol  Fw chain              Info
    3  18.521170  172.21.101.201    172.21.101.3      TCP       i  eth0               syscomlan > ftp [SYN] Seq=0 Wi
    4  18.522086  172.21.101.201    10.1.1.101        TCP          eth0 I             syscomlan > ftp [SYN] Seq=0 Wi
    5  18.522194  172.21.101.201    10.1.1.101        TCP         eth0       eth1 o   syscomlan > ftp [SYN] Seq=0 Wi
    6  18.522389  172.21.101.201    10.1.1.101        TCP         eth0     o eth1     syscomlan > ftp [SYN] Seq=0 Wi
    7  18.542114  10.1.1.101        172.21.101.201    TCP         eth0     i eth1     ftp > syscomlan [SYN, ACK] Sec
    8  18.542181  10.1.1.101        172.21.101.201    TCP         eth0       eth1 I   ftp > syscomlan [SYN, ACK] Sec
    9  18.542300  10.1.1.101        172.21.101.201    TCP          eth0 o     eth1    ftp > syscomlan [SYN, ACK] Sec
   10  18.542339  172.21.101.3      172.21.101.201    TCP       o  eth0       eth1    ftp > syscomlan [SYN, ACK] Sec
   11  18.543211  172.21.101.201    172.21.101.3      TCP       i  eth0       eth1    syscomlan > ftp [ACK] Seq=1 Ac
   12  18.543259  172.21.101.201    10.1.1.101        TCP          eth0 I     eth1    syscomlan > ftp [ACK] Seq=1 Ac

⊞ Frame 4 (62 bytes on wire, 62 bytes captured)
⊞ FW1 Monitor      eth0 I      eth1
⊞ Internet Protocol, Src: 172.21.101.201 (172.21.101.201), Dst: 10.1.1.101 (10.1.1.101)
⊞ Transmission Control Protocol, Src Port: syscomlan (1065), Dst Port: ftp (21), Seq: 0, Len: 0
```

A. This is an example of Hide NAT.
B. There is not enough information provided in the Wireshark capture to determine the NAT settings.
C. This is an example of Static NAT and Translate destination on client side unchecked in Global Properties.
D. This is an example of Static NAT and Translate destination on client side checked in Global Properties.

Answer: D

Topic 7, Identity Awareness Obj 1

Question No : 5 - (Topic 7)

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.

2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

What should John do when he cannot access the web server from a different personal computer?

A. John should lock and unlock his computer
B. Investigate this as a network connectivity issue
C. The access should be changed to authenticate the user instead of the PC
D. John should install the Identity Awareness Agent

Answer: C

Topic 10, Identity Awareness Obj 4

Question No : 6 - (Topic 10)

What command syntax would you use to turn on PDP logging in a distributed environment?

A. pdp track=1
B. pdp tracker on
C. pdp logging on
D. pdp log=1

Answer: B

Topic 11, Advanced Firewall

Question No : 7 - (Topic 11)

You are troubleshooting a HTTP connection problem. You've started fw monitor -o http.pcap. When you open http.pcap with Wireshark there is only one line. What is the most likely reason?

A. fw monitor was restricted to the wrong interface.
B. Like SmartView Tracker only the first packet of a connection will be captured by fw monitor.
C. By default only SYN pakets are captured.
D. Acceleration was turned on and therefore fw monitor sees only SYN.

Answer: D

Topic 12, Advanced upgrading

Question No : 8 CORRECT TEXT - (Topic 12)

In a zero downtime firewall cluster environment, what command syntax do you run to avoid switching problems around the cluster for command cphaconf?

Answer: set_ccp broadcast

Topic 15, IPSEC VPN and Remote Access

Question No : 9 - (Topic 15)

Which Check Point tool allows you to open a debug file and see the VPN packet exchange details.

A. PacketDebug.exe
B. VPNDebugger.exe
C. IkeView.exe
D. IPSECDebug.exe

Answer: C

Topic 16, SmartReporting and SmartEvent

Question No : 10 - (Topic 16)

When migrating the SmartEvent data base from one server to another, the first step is to back up the files on the original server. Which of the following commands should you run to back up the SmartEvent data base?

A. migrate export
B. eva_db_backup
C. snapshot
D. backup

Answer: B