Checkpoint

Exam 156-915.76

Check Point Certified Security Expert Update Blade

Version: 9.0

[Total Questions: 269]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	69

Topic 1, Volume A

Question No : 1 - (Topic 1)

When using SecurePlatform, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active.

How do you configure this change?

A. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field
(conf
: (conns
: (conn
:hwaddr (“00:0c:29:12:34:56”)
B. As expert user, issue these commands:
# IP link set eth0 down
# IP link set eth0 addr 00:0c:29:12:34:56
# IP link set eth0 up
C. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.
D. As expert user, issue the command: # IP link set eth0 addr 00:0C:29:12:34:56

Answer: B

Question No : 2 - (Topic 1)

Which of the following are authentication methods that Security Gateway R76 uses to validate connection attempts? Select the response below that includes the MOST complete list of valid authentication methods.

A. User, Client, Session
B. Proxied, User, Dynamic, Session
C. Connection, User, Client
D. User, Proxied, Session

Answer: A

Question No : 3 - (Topic 1)

You are responsible for the configuration of MegaCorp's Check Point Firewall. You need to allow two NAT rules to match a connection. Is it possible? Give the BEST answer.

A. Yes, it is possible to have two NAT rules which match a connection, but only when using Automatic NAT (bidirectional NAT).
B. Yes, it is possible to have two NAT rules which match a connection, but only in using Manual NAT (bidirectional NAT).
C. Yes, there are always as many active NAT rules as there are connections.
D. No, it is not possible to have more than one NAT rule matching a connection. When the firewall receives a packet belonging to a connection, it compares it against the first rule in the Rule Base, then the second rule, and so on. When it finds a rule that matches, it stops checking and applies that rule.

Answer: A

Question No : 4 - (Topic 1)

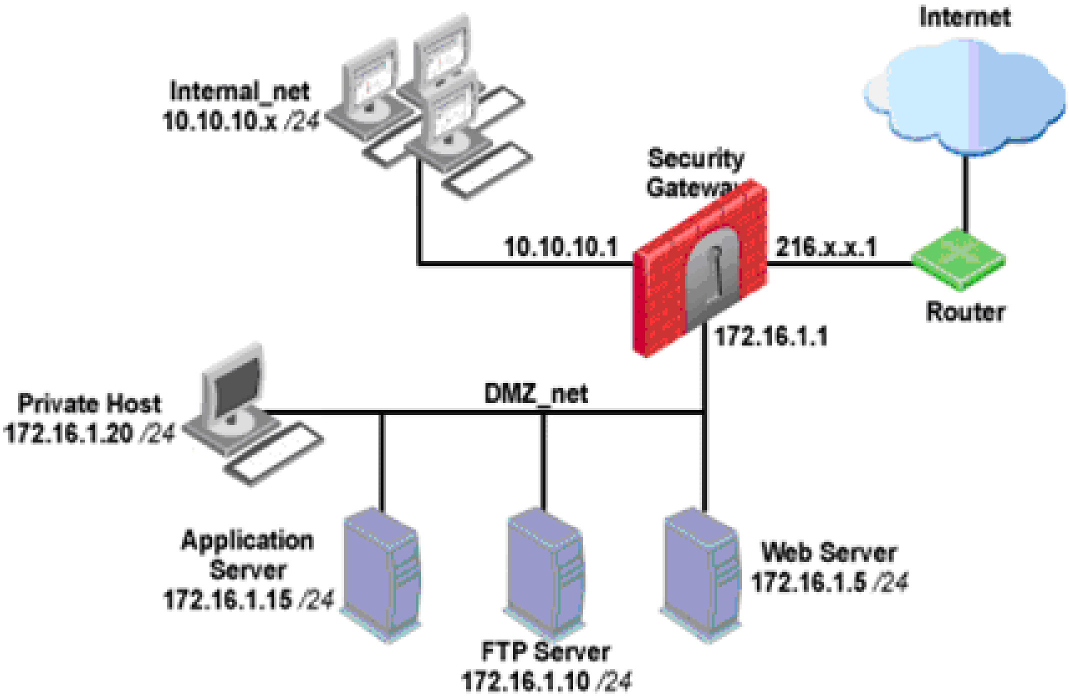
What is the primary benefit of using the command upgrade_export over either backup or snapshot?

A. The commands backup and snapshot can take a long time to run whereas upgrade_export will take a much shorter amount of time.
B. upgrade_export will back up routing tables, hosts files, and manual ARP configurations, where backup and snapshot will not.
C. upgrade_export has an option to back up the system and SmartView Tracker logs while backup and snapshot will not.
D. upgrade_export is operating system independent and can be used when backup or snapshot is not available.

Answer: D

Question No : 5 - (Topic 1)

You have three servers located in a DMZ, using private IP addresses. You want internal users from 10.10.10.x to access the DMZ servers by public IP addresses. Internal_net 10.10.10.x is configured for Hide NAT behind the Security Gateway's external interface.



What is the best configuration for 10.10.10.x users to access the DMZ servers, using the DMZ servers' public IP addresses?

A. When connecting to the Internet, configure manual Static NAT rules to translate the DMZ servers.
B. When connecting to internal network 10.10.10.x, configure Hide NAT for the DMZ network behind the Security Gateway DMZ interface.
C. When the source is the internal network 10.10.10.x, configure manual static NAT rules to translate the DMZ servers.
D. When trying to access DMZ servers, configure Hide NAT for 10.10.10.x behind the DMZ's interface.

Answer: C

Question No : 6 - (Topic 1)

You enable Automatic Static NAT on an internal host node object with a private IP address of 10.10.10.5, which is NATed into 216.216.216.5. (You use the default settings in Global Properties / NAT.)

When you run fw monitor on the R76 Security Gateway and then start a new HTTP connection from host 10.10.10.5 to browse the Internet, at what point in the monitor output will you observe the HTTP SYN-ACK packet translated from 216.216.216.5 back into 10.10.10.5?

A. O=outbound kernel, after the virtual machine
B. i=inbound kernel, before the virtual machine
C. I=inbound kernel, after the virtual machine
D. o=outbound kernel, before the virtual machine

Answer: C

Question No : 7 - (Topic 1)

MultiCorp has bought company OmniCorp and now has two active AD domains. How would you deploy Identity Awareness in this environment?

A. Identity Awareness can only manage one AD domain.
B. Only Captive Portal can be used.
C. Only one ADquery is necessary to ask for all domains.
D. You must run an ADquery for every domain.

Answer: D

Question No : 8 - (Topic 1)

The connection to the first ClusterXL member breaks. The first ClusterXL member leaves the cluster. Afterwards the switch admin set on port to second ClusterXL member to down. What will happen?

A. Second ClusterXL member still stays active as last member.
B. Both ClusterXL members share load equally.
C. Second ClusterXL member also left the cluster.

D. First ClusterXL member is asked to come back to cluster.

Answer: A

Question No : 9 - (Topic 1)

Which Check Point address translation method allows an administrator to use fewer ISP-assigned IP addresses than the number of internal hosts requiring Internet connectivity?

A. Static Source
B. Static Destination
C. Dynamic Destination
D. Hide

Answer: D

Question No : 10 - (Topic 1)

How do you verify the Check Point kernel running on a firewall?

A. fw ctl get kernel
B. fw ctl pstat
C. fw kernel
D. fw ver -k

Answer: D

Question No : 11 - (Topic 1)

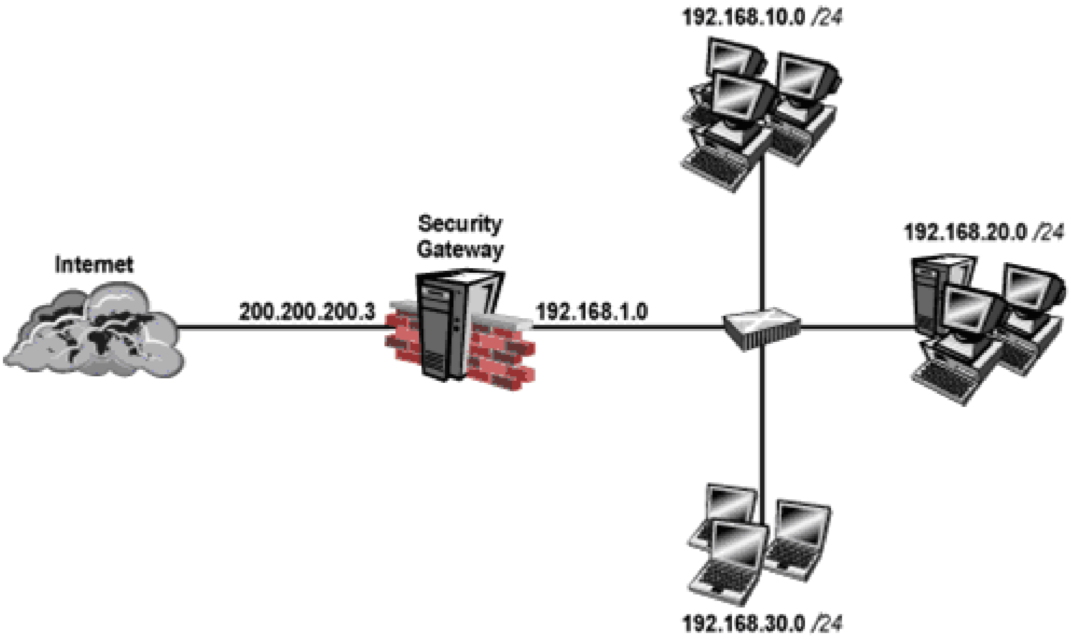
Which command will only show the number of entries in the connection table?

A. fw tab
B. fw tab -t connections -s
C. fw tab -t connections -u
D. fw tab -t connections

Answer: B

Question No : 12 - (Topic 1)

Your perimeter Security Gateway’s external IP is 200.200.200.3. Your network diagram shows:



Required. Allow only network 192.168.10.0 and 192.168.20.0 to go out to the Internet, using 200.200.200.5.

The local network 192.168.1.0/24 needs to use 200.200.200.3 to go out to the Internet.

Assuming you enable all the settings in the NAT page of Global Properties, how could you achieve these requirements?

A. Create a network object 192.168.0.0/16. Enable Hide NAT on the NAT page. Enter

200.200.200.5 as the hiding IP address. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
B. Create network objects for 192.168.10.0/24 and 192.168.20.0/24. Enable Hide NAT on both network objects, using 200.200.200.5 as hiding IP address. Add an ARP entry for 200.200.200.3 for the MAC address of 200.200.200.5.
C. Create an Address Range object, starting from 192.168.10.1 to 192.168.20.254. Enable Hide NAT on the NAT page of the address range object. Enter Hiding IP address 200.200.200.5. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
D. Create two network objects: 192.168.10.0/24 and 192.168.20.0/24. Add the two network objects to a group object. Create a manual NAT rule like the following: Original source - group object; Destination - any; Service - any; Translated source - 200.200.200.5; Destination - original; Service - original.

Answer: C

Question No : 13 - (Topic 1)

As a Security Administrator, you must refresh the Client Authentication authorization time-out every time a new user connection is authorized. How do you do this? Enable the Refreshable Timeout setting:

A. In the user object's Authentication screen.
B. In the Gateway object's Authentication screen.
C. In the Global Properties Authentication screen.
D. In the Limit tab of the Client Authentication Action Properties screen.

Answer: D

Question No : 14 - (Topic 1)

You are running a R76 Security Gateway on SecurePlatform. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What back up method could be used to quickly put the secondary firewall into production?

A. manual backup
B. snapshot
C. upgrade_export
D. backup

Answer: B

Question No : 15 - (Topic 1)

How can you check whether IP forwarding is enabled on an IP Security Appliance?

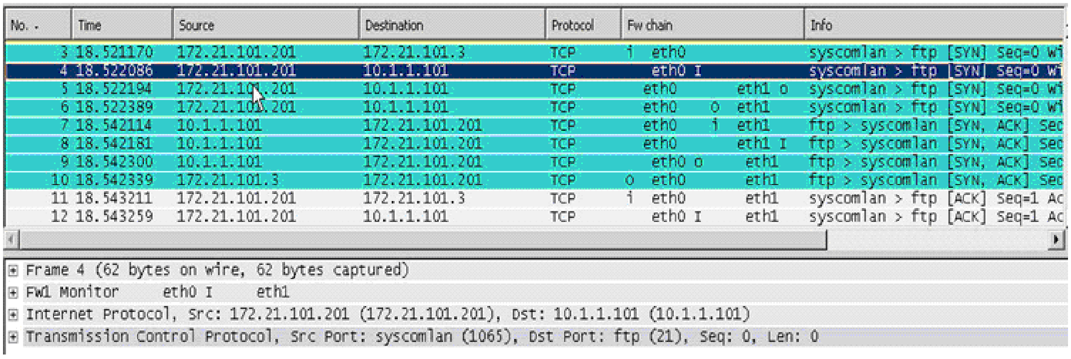
A. clish -c show routing active enable
B. ipsofwd list
C. cat /proc/sys/net/ipv4/ip_forward
D. echo 1 > /proc/sys/net/ipv4/ip_forward

Answer: B

Question No : 16 - (Topic 1)

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

Exhibit:



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.