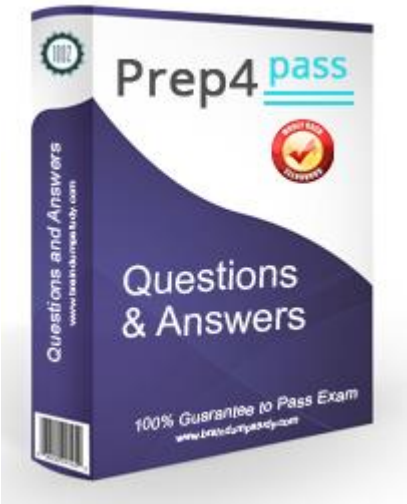
Prep4Pass



Try before you buy

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

- 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.

Choose an exam to sample

Select a vendor...

Select an exam...

Your email address

Download Now

http://www.prep4pass.com

IT certification exam prep provide, High passing rate

Exam : **156-215.77**

Title : Check Point Certified Security Administrator

Vendor : CheckPoint

Version : DEMO

NO.1 When using GAiA, 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?

```
# IP link set eth0 down
# IP link set eth0 addr 00:0C:29:12:34:56
# IP link set eth0 up
```

As expert user, issue these commands:

```
(conf
:(conns
      :(conn
            :hwaddr ("00:0C:29:12:34:56")
```

A. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field

B. As expert user, issue the command:

C. # IP link set eth0 addr 00:0C:29:12:34:56

D. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.

Answer: C

NO.2 In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

A. Rule 0

B. Blank field under Rule Number

C. Rule 1

D. Cleanup Rule

Answer: A

NO.3 Which tool CANNOT be launched from SmartUpdate R77?

A. IP Appliance Voyager

B. snapshot

C. GAiA WebUI

D. cpinfo

Answer: B

NO.4 Which of the following is true of a Stealth Rule?

A. The Stealth rule should not be logged

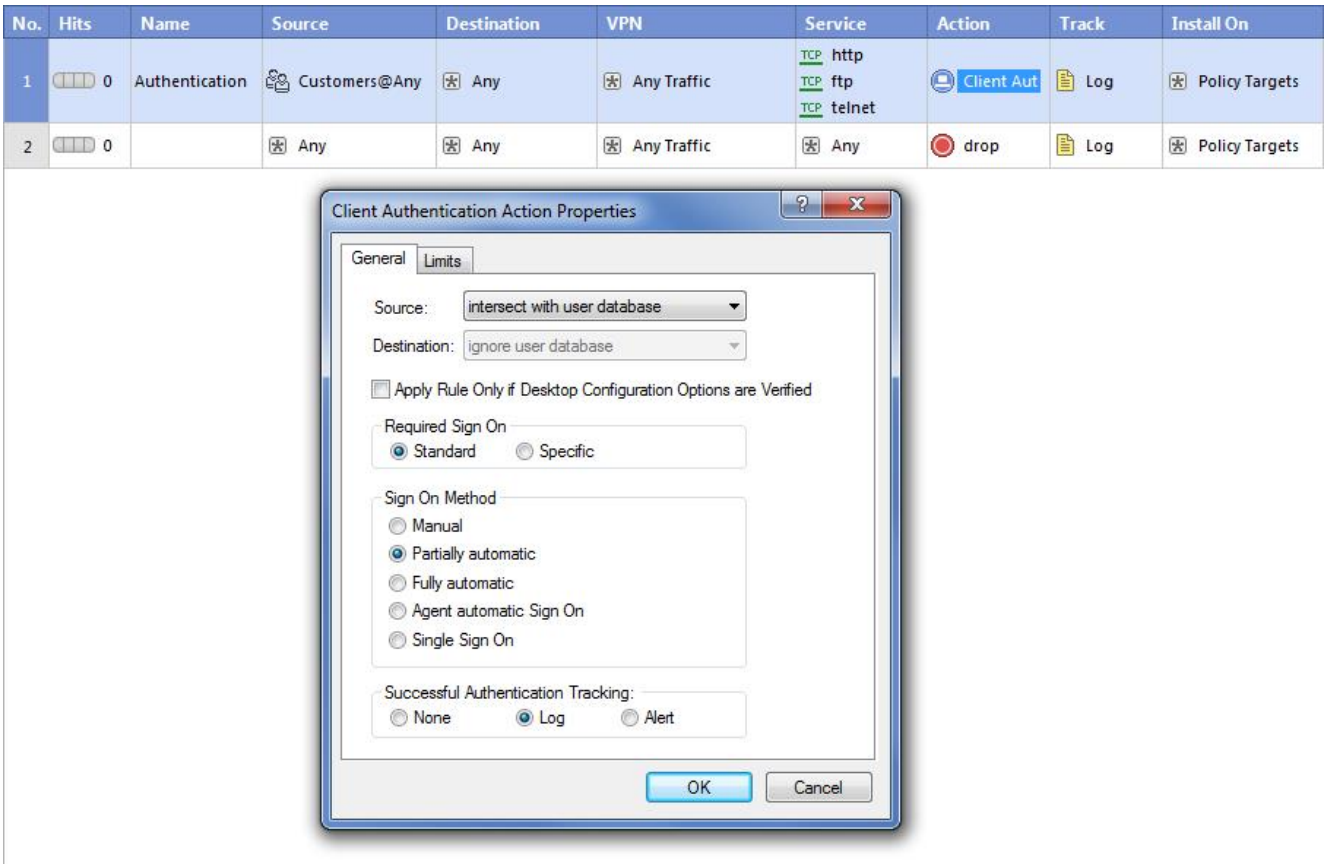
B. The Stealth rule is required for proper firewall protection

C. The Stealth rule should be located just before the Cleanup rule

D. The Stealth rule must be the first rule in a policy

Answer: B

NO.5 Study the Rule base and Client Authentication Action properties screen -



After being authenticated by the Security Gateway, when a user starts an HTTP connection to a Web site, the user tries to FTP to another site using the command line. What happens to the user?

A. user is prompted for authentication by the Security Gateway again.

B. FTP data connection is dropped after the user is authenticated successfully.

C. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client Authentication.

D. FTP connection is dropped by Rule 2.

Answer: C

Explanation:

Manual Users must use either telnet to port 259 on the firewall, or use a Web browser to connect to port 900 on the firewall to authenticate before being granted access.

Partially Automatic If user authentication is configured for the service the user is attempting to access and they pass this authentication, then no further client authentication is required. For example, if HTTP is permitted on a client authentication rule, the user will be able to transparently authenticate since FireWall-1 has a security server for HTTP.Then, if this setting is chosen, users will not have to manually authenticate for this connection. Note that this applies to all services for which FireWall-1 has built-in security servers (HTTP, FTP, telnet, and rlogin).

Fully Automatic If the client has the session authentication agent
installed, then no further client authentication is required (see session authentication below). For HTTP, FTP, telnet, or rlogin, the firewall will authenticate via user authentication, and then session authentication will be used to authenticate all other services.

http://www.syngress.com

Figure 6.19 Client Authentication Action Properties

278 Chapter 6 * Authenticating Users

Agent Automatic Sign On Uses session authentication agent to provide

transparent authentication (see session authentication below).
Single Sign-On System Used in conjunction with UserAuthority servers to provide enhanced application level security. Discussion of UserAuthority is beyond the scope of this book.

NO.6 Which SmartView Tracker mode allows you to read the SMTP e-mail body sent from the Chief Executive Officer (CEO) of a company?

A. This is not a SmartView Tracker feature.

B. Display Capture Action

C. Network and Endpoint Tab

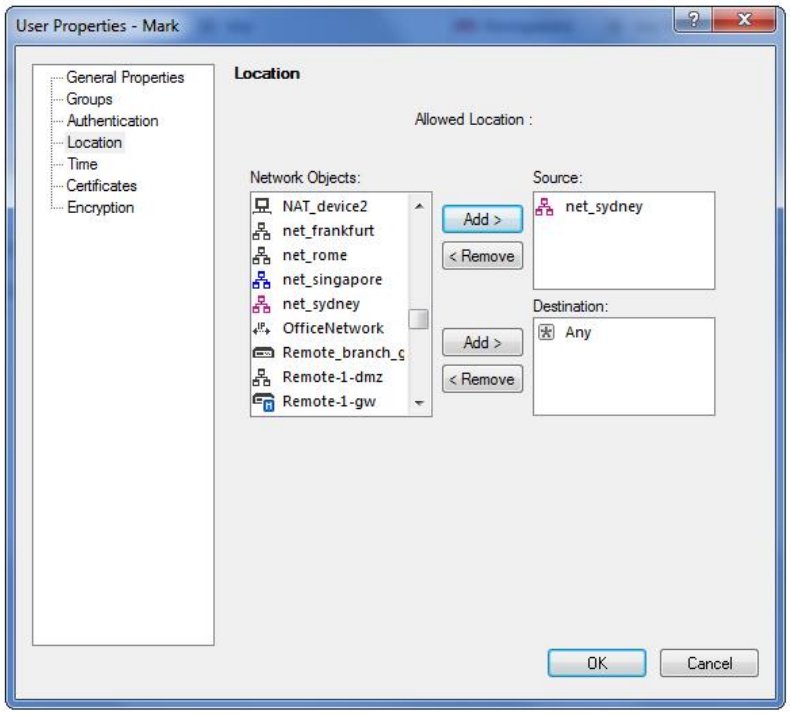
D. Display Payload View

Answer: A

NO.7 Charles requests a Website while using a computer not in the net_singapore network. What is TRUE about his location restriction?

Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None	Policy Targets
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	Log	Policy Targets
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
4	0	Authentication	All Users@net_singapore	Any	Any Traffic	http	User Auth	Log	Policy Targets
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	Any	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	ftp	accept	Log	Policy Targets
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets



A. Source setting in Source column always takes precedence.

B. Source setting in User Properties always takes precedence.

C. As location restrictions add up, he would be allowed from net_singapore and net_sydney.
D. It depends on how the User Auth object is configured; whether User Properties or Source Restriction takes precedence.
Answer: D

NO.8 Which rule is responsible for the installation failure?
Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None	Policy Targets
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None	Policy Targets
3	0	Web Server	Any	webSingapore	Any Traffic	http	Client Aut	Log	Policy Targets
4	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	http	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	http dns icmp-proto ftp https	accept	Log	Policy Targets
7	0	Network Traffic	webSydney	Any	Any Traffic	ftp	reject	Log	Policy Targets
8	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

A. Rule 5
B. Rule 4
C. Rule 3
D. Rule 6
Answer: B

NO.9 You are running a R77 Security Gateway on GAiA. 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. upgrade_export
C. backup
D. snapshot
Answer: D

NO.10 Which of the following items should be configured for the Security Management Server to authenticate using LDAP?
A. Login Distinguished Name and password
B. Windows logon password
C. Check Point Password
D. WMI object
Answer: A

NO.11 Choose the correct statement regarding Implied Rules:
A. To edit Implied rules you go to: Launch Button > Policy > Global Properties > Firewall.

B. Implied rules are fixed rules that you cannot change.
C. You can directly edit the Implied rules by double-clicking on a specific Implicit rule.
D. You can edit the Implied rules but only if requested by Check Point support personnel.
Answer: A

NO.12 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 an IP address 10.0.0.19 via DHCP.
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. 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.
John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?
A. John should install the Identity Awareness Agent
B. The firewall admin should install the Security Policy
C. John should lock and unlock the computer
D. Investigate this as a network connectivity issue
Answer: B

NO.13 Exhibit:

1) Create a new activation key on the Security Gateway, then exit `cpconfig`.
2) Click the **Communication** tab on the Security Gateway object, then click **Reset**.
3) Run the `sysconfig` tool, then select **Secure Internal Communication** to reset.
4) Input the new activation key in the Security Gateway object, then click **Initialize**.
5) Run the `cpconfig` tool, then select **Secure Internal Communication** to reset.

Chris has lost SIC communication with his Security Gateway and he needs to re-establish SIC. What would be the correct order of steps needed to perform this task?
A. 5, 1, 2, 4
B. 5, 1, 4, 2
C. 3, 1, 4, 2
D. 2, 3, 1, 4
Answer: A

NO.14 You are about to test some rule and object changes suggested in an R77 news group.

Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?
A. Manual copies of the directory $FWDIR/conf
B. upgrade_export command
C. Database Revision Control
D. GAiA backup utilities
Answer: C

NO.15 Which of the following tools is used to generate a Security Gateway R77 configuration report?
A. fw cpinfo
B. infoCP
C. cpinfo
D. infoview
Answer: C

NO.16 What statement is true regarding Visitor Mode?
A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
B. Only ESP traffic is tunneled through port TCP 443.
C. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
D. All VPN traffic is tunneled through UDP port 4500.
Answer: A

NO.17 Which of the following R77 SmartView Tracker views will display a popup warning about performance implications on the Security Gateway?
A. All Records Query
B. Account Query
C. Active Tab
D. Audit Tab
Answer: C

NO.18 You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners.
Which SmartConsole application should you use to confirm your suspicions?
A. SmartDashboard
B. SmartUpdate
C. SmartView Status
D. SmartView Tracker
Answer: D