



**156-210.4**

Check Point NG with Application Intelligence - Management I

Q&A

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

This Study guide has been carefully written and compiled by chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

## **Study Tips**

This guide will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedbacks help us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing Chinatag products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**Item: 1** (Ref:Cert-156-210.9.1.5)

By default, which of the following directories are typically used as the VPN-1/FireWall-1 installation directory? Select three choices.

- /fw1
- /etc/fw
- C:\FW1
- /opt/CPfw1-50
- C:\WINNT\FW1\NG

Answer:

**/etc/fw**  
**/opt/CPfw1-50**  
**C:\WINNT\FW1\NG**

---

**Explanation:**

By default, the **\$FWDIR** directory on Windows NT and Windows 2000 computers is located at the following path: **C:\WINNT\FW1\NG**. On Solaris and Linux computers, the default location of the **\$FWDIR** directory is **/opt/CPfw1-50**, which can also be accessed within **/etc/fw**.

The **/fw1** and **C:\FW1** directories are not used as the VPN-1/FireWall-1 installation directory by default.

The VPN-1/FireWall-1 installation directory is usually referred to as **\$FWDIR**.

The **\$FWDIR/lib** directory contains library files. These files should be backed up regularly.

The **\$FWDIR/log** directory contains log files. Log files have a **.log** extension. Because the log files can become quite large, they should be deleted periodically. Although you can back up the log files, you are not required to do so.

The **\$FWDIR/conf** directory contains the Rule Base and should also be backed up regularly. In addition, it contains objects and the Check Point Users Database. Files in the **\$FWDIR/conf** directory include **objects\_5\_0.C**, **rulebases\_5\_0.fws**, and **.W** files. The **objects\_5\_0.C** file includes all defined objects. Files with the **.W** extension are individual Security Policies that have been created in SmartDashboard. The **rulebases\_5\_0.fws** file contains all of the **.W** file policies in one file. The **fwauth.ndb** database file contains all users and groups.

**Objective:**

VPN-1/FireWall-1 NG Upgrades

**Sub-Objective:**

Install and upgrade the VPN-1/FireWall-1 NG software

**References:**

CCSA NG Study Guide, Chapter 10, Backing Up VPN-1/FireWall-1, p. 605.

**Item: 2 (Ref:Cert-156-210.2.1.6)**

You restart an existing Enforcement module.

If the Enforcement module cannot contact the SmartCenter server, which of the following will protect the Enforcement module and the network behind the firewall?

- nothing
- the initial policy
- the default filter
- the locally cached policy
- the Security Policy stored on the SmartCenter server

Answer:

**the locally cached policy**

---

**Explanation:**

If the Enforcement module cannot contact the SmartCenter server, then the locally cached policy will protect the Enforcement module and the network behind the firewall. The locally cached Security Policy is the most recent Security Policy that has been installed on the Enforcement module. Logging will occur locally until communication is established with the SmartCenter server.

The default filter initially protects the Enforcement module. The default policy blocks all traffic until a Security Policy can be enforced. IP forwarding is also blocked while an Enforcement module starts.

The initial Security Policy consists of implicit rules. The initial policy is loaded only the first time the Enforcement module is started; it is loaded after the default filter is applied and before a Security Policy is installed. Once a Security Policy has been installed, the initial Security Policy will not be loaded again.

If the Enforcement module cannot contact the SmartCenter server, the Security Policy stored on the SmartCenter server cannot be installed on the Enforcement module.

**Objective:**

The Security Policy

**Sub-Objective:**

Explain the function and operation of a Security Policy

**References:**

Check Point NG/AI Study Guide, Chapter 4, Default and Initial Policies, pp. 228-230.

**Item: 3** (Ref:Cert-156-210.7.3.4)

Your firewall is configured to perform Hide NAT. A reply packet is received by the firewall.

What information does the firewall use to determine which internal client should receive the packet?

- sequence number
- source IP address
- source port number
- destination IP address
- destination port number

Answer:

**destination port number**

---

**Explanation:**

The firewall uses the destination port number to determine which internal client should receive the packet.

Hide NAT, which is also known as Dynamic NAT, is used to hide multiple internal IP addresses behind one or more registered IP addresses. When a packet is sent from an internal client through the firewall, the source address of the packet is changed, usually to the registered address that is assigned to the firewall's external interface. The packet's source port is modified to a dynamically assigned port number. The dynamic port number is used by the firewall to keep track of which internal device sent each packet.

After the packet reaches its destination, any replies will be sent by using the original packet's source IP address and source port as the new packet's destination IP address and destination port. When the firewall receives the packet, it checks the packet's destination port to determine which internal device should receive the reply packet.

The source IP address of a reply packet will be the IP address of the sending device. Therefore, the source IP address cannot be used to determine which internal client should receive the packet.

The destination IP address of a reply packet will typically be the IP address of the firewall's external interface. Therefore, the destination IP address cannot be used to determine which internal client should receive the packet.

The source port number of a reply packet is assigned by the sending device. Therefore, the source port number cannot be used to determine which internal client should receive the packet.

Sequence numbers are used to order packets that arrive out of sequential order. Sequence numbers are not used to determine which internal client should receive the packet.

**Objective:**

Network Address Translation

**Sub-Objective:**

Demonstrate how to set up Hide NAT

**References:**

Check Point Courseware, Chapter 9, Dynamic NAT, pp. 266-268.

**Item: 4 (Ref:Cert-156-210.6.6.7)**

Which of the following authentication methods uses TCP port 261?

- User authentication
- Client authentication
- Session authentication
- User and Client authentication
- Client and Session authentication

Answer:

**Session authentication**

---

**Explanation:**

Session authentication uses TCP port 261. Session authentication requires a Session Authentication Agent, which listens on TCP port 261 for authentication requests from Enforcement modules.

When Session authentication is used, the user initiates a connection directly to the destination. The Enforcement module will intercept the request and ask the Session Authentication Agent for authorization on TCP port 261.

User authentication uses port 80 for authentication.

Client authentication uses port 259 and port 900 when Manual Sign On is used. A user who manually connects to a firewall by using Client authentication over Telnet will connect through TCP port 259. A user who manually connects to a firewall by using Client authentication over Hypertext Transfer Protocol (HTTP) will connect through TCP port 900.

**Objective:**

Authentication

**Sub-Objective:**

Demonstrate how to implement Client Authentication

**References:**

CCSA NG Study Guide, Chapter 7, Session Authentication, pp. 454-457.

**Item: 5 (Ref:Cert-156-210.2.5.11)**

You have two Check Point gateway objects configured on your SmartCenter server. The gateways are named Door and Portal.

Your Security Policy contains several rules. The **Install On** column of each rule specifies **Policy Targets**.

You attempt to install the Security Policy, but only Door appears in the **Install Policy** dialog box.

Which of the following could cause this behavior? Select two choices.

- Communication with Portal has been lost.
- The **Install On** column is not configured for **Gateways**.
- Portal was created as an externally managed Check Point gateway.
- The **Install On** column is not configured with the name of each gateway.
- The **Specific Modules** radio button has been selected on the **Select Installation Targets** dialog box, and only Door has been added to the **In Installation Targets** list.

Answer:

**Portal was created as an externally managed Check Point gateway.  
The Specific Modules radio button has been selected on the Select Installation Targets dialog box, and only Door has been added to the In Installation Targets list.**

---

**Explanation:**

If Portal is missing from the **Install Policy** dialog box, then Portal might have been created as an externally managed Check Point gateway. A SmartCenter server cannot install a Security Policy on a gateway that is not managed by the SmartCenter server.

If Portal was not created as an externally managed gateway, then perhaps the **Specific Modules** radio button has been selected on the **Select Installation Targets** dialog box, and only Door has been added to the **In Installation Targets** list. Portal would then appear in the **Not In Installation Targets** list. To enable Portal to appear in the **Install Policy** dialog box, you should either add Portal to the **In Installation Targets** list or select the **All internal modules** radio button.

Portal would still appear in the **Install Policy** dialog box even if communication with Portal were lost. The installation would fail, but the option to install the policy on Portal would be available.

Regardless of what is configured for the **Install On** column of each rule, all configured gateways will be listed in the **Install Policy** dialog box. The **Install On** column specifies the gateways on which the rule will be enforced, not installed. **Policy Targets** specifies that the rule will be enforced on all targets. **Gateways** specifies that the rule will be enforced only on gateways. Individually named targets can also be specified in the **Install On** column. Therefore, Door and Portal could be named individually. Therefore, if only Door were specified in the **Install On** column of a rule, the Security Policy would still be installed on Portal, but that rule would not be enforced on Portal.

**Objective:**

The Security Policy

**Sub-Objective:**

Show how to install and uninstall a Security Policy

**References:**

CCSA NG Study Guide, Chapter 3, Configuring Security Objects, pp. 119-137.

CCSA NG Study Guide, Chapter 3, Understanding the Security Rule Base, pp. 148-163.

<b>Item: 6</b> (Ref:Cert-156-210.2.1.19)
--

Consider the following Rule Base:

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
-	 DAG module	* Any	 dhcp_request	 accept	- None
1	* Any	 MainFireWall	* Any	 drop	- None
2	 MainFireWall	* Any	* Any	 accept	- None
3	* Any	* Any	* Any	 drop	 Log
4	* Any	* Any	* Any	 drop	- None

Which of the following are implied rules?

- rule 1
- rules 1, 3 and 4
- rules 1, 2, 3 and 4
- the rule marked with a dash instead of a number
- rules 1, 2, 3, 4, and the rule marked with a dash instead of a number

Answer:

**the rule marked with a dash instead of a number**

### Explanation:

The rule marked with a dash instead of a number is an implied rule. Implied rules, which are also called implicit rules, are not displayed in the Rule Base by default and cannot be modified directly; they must be configured in **Global Properties**. Each implicit rule can be set to **First**, **Before Last** or **Last**.

Rules 1, 2, 3 and 4 are all explicit rules.

Rule 1 is the Stealth rule. The Stealth rule prohibits direct communication with the firewall. The Stealth rule is usually located at the top of the Rule Base. However, Client authentication rules should be placed before the Stealth rule in the Rule Base because authentication rules require access to the firewall in order to perform authentication.

Rule 2 is a normal explicit rule. This explicit rule is configured to allow all traffic that is sent directly from the firewall itself.

Rule 3 is the Cleanup rule. The Cleanup rule is also known as the "none-of-the-above" rule because it is used to log connections that do not match any rules that appear above it in the Rule Base. The Cleanup rule is used to log connections that are dropped or rejected because no other rule applies. The Cleanup rule is an explicit rule and must be defined by an administrator.

Rule 4 is the Default rule. Whenever a rule is added to the Rule Base, the default rule is added. The Default rule is similar to the Cleanup rule; however, no logging is performed.

### Objective:

The Security Policy

### Sub-Objective:

156-210.4

Explain the function and operation of a Security Policy

**References:**

Check Point Courseware, Chapter 4, Creating the Rule Base, pp. 105-107.

**Item: 7 (Ref:Cert-156-210.7.3.9)**

You are responsible for configuring NAT on your network. You select **Hide Nat**, click the button beside **Hide behind IP Address**, and type 0.0.0.0.

What does the address 0.0.0.0 represent?

- the address of the host PCs
- the address of the destination server
- the address of the SmartCenter server
- the internal interface of the Enforcement Module
- the external interface of the Enforcement Module

Answer:

**the external interface of the Enforcement Module**

---

**Explanation:**

The address 0.0.0.0 represents the external interface of the Enforcement Module.

Any of the following addresses can be used to hide internal IP addresses when Hide NAT is used:

- 0.0.0.0
- the external IP address of the Enforcement module
- any IP address that is owned by the company and routable to the Enforcement module

When Hide NAT is selected, two options are available: **Hide behind Gateway** and **Hide behind IP Address**. Selecting **Hide behind Gateway** will configure the Enforcement module to use the external IP address of the Enforcement module. Selecting **Hide behind IP Address** will enable the administrator to configure the IP address to be used. Any IP address that is both owned by the company and routable to the Enforcement module can be used.

The address 0.0.0.0 does not represent the address of the host PCs, the destination server, the SmartCenter server, or the internal interface of the Enforcement module.

**Objective:**

Network Address Translation

**Sub-Objective:**

Demonstrate how to set up Hide NAT

**References:**

CCSA NG Study Guide, Chapter 9, Using the Hide behind the interface of the Install on Gateway Option (0.0.0.0) for Hide NAT, pp. 554-555.

**Item: 8 (Ref:Cert-156-210.2.3.28)**

You have created a Rule Base in which a Stealth rule and a Cleanup rule are placed in the recommended positions within the inspection order. You want to insert an implied rule that accepts outgoing packets that originate from the gateway; the implied rule should be placed above the Stealth rule.

Which of the following options should you select in order to place the new implied rule in the desired position?

**Last**

**First**

**After First**

**Before Last**

**Before First**

Answer:

**First**

---

**Explanation:**

In order to insert the implied rule above the Stealth rule, which is typically one of the first explicit rules in the Rule Base, you should select the **First** option in the drop-down box for that implied rule on the **Global Properties** page. When the **First** option is chosen for an implied rule, that rule will be the first rule enforced after anti-spoofing rules are applied, but before the other rules in the Rule Base are applied. When the inspection order of the Rule Base is changed, the order in which the rules are enforced also changes.

Implied rules can also be moved within the inspection order by choosing the **Before Last** option in the drop-down box of an implied rule. When the **Before Last** selection is chosen for an implied rule, that rule will be enforced immediately before the last rule in the Rule Base is enforced. Because the Cleanup Rule is typically the last rule in the Rule Base, you would select the **Before Last** option to insert an implied rule above the Cleanup Rule.

When the **Last** option is chosen in the drop-down box of an implied rule, that rule will be enforced after all other rules within the Rule Base are enforced.

The **Before First** and **After First** options are not valid.

**Objective:**

The Security Policy

**Sub-Objective:**

Demonstrate the setup and operation of an active Security Policy

**References:**

Check Point Courseware, Chapter 4, Implicit and Explicit Rules, pp. 119-123.

<b>Item: 9</b> (Ref:Cert-156-210.6.1.11)
--

Consider the following Rule Base:

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	* Any	* Any	TCP http	User Auth	Account
2	* Any	* Any	TCP ftp	Client Auth	Log
3	HR	Server1	TCP smtp	Session Auth	Mail
4	HR	Server1	TCP ftp	User Auth	None
5	* Any	* Any	TCP ftp TCP smtp	drop	Alert
6	* Any	* Any	* Any	drop	Log

Which of the following statements are most accurate? Select two choices.

- All FTP connections require Client authentication.
- All HTTP connections require User authentication.
- All Telnet connections require User authentication.
- All SMTP connections require Session authentication.
- No connections from members of the HR group require Client authentication.

Answer:

**All FTP connections require Client authentication.**  
**All HTTP connections require User authentication.**

### Explanation:

All FTP connections require Client authentication, and all HTTP connections require User authentication.

Rules in a Rule Base are processed sequentially from top to bottom. The first rule that matches the source, destination and service will be applied. The required authentication method can be different for each rule.

All FTP connections are handled by rule 2. Therefore, all FTP connections require Client authentication. HR users who access FTP services on Server1 are handled by rule 2, not rule 4.

All HTTP connections are handled by rule 2. Therefore, all HTTP connections require User authentication.

Because rules 1 through 5 do not handle Telnet connections, all Telnet connections are dropped by rule 6. Therefore, Telnet connections do not require authentication.

SMTP connections from HR users require Session authentication. However, SMTP connections from other users are dropped. Therefore, not all SMTP connections require Session authentication.

HR users who access FTP services on Server1 are handled by rule 2. Therefore, Client authentication is required for FTP connections by HR users.

### Objective:

Authentication

156-210.4

**Sub-Objective:**

Demonstrate how to implement authentication

**References:**

CCSA NG Study Guide, Chapter 4, Understanding the Security Rule Base, pp. 148-163.

**Item: 10 (Ref:Cert-156-210.2.6.1)**

You support a network that uses hundreds of individual host IP addresses. The same rules should apply to all hosts. The addresses fall within a contiguous range.

Which of the following objects should you use when creating rules in order to minimize the time that is required for the Security Policy to load?

- a single host object
- individual host objects
- a single dynamic object
- multiple objects for each host
- a single address range object

Answer:

**a single address range object**

---

**Explanation:**

In order to minimize the time that is required for the Security Policy to load, you should use a single address range object when creating rules. Because all of your host addresses fall within a contiguous range, and because the same rules should apply to all hosts, you can use a single address range object to group all of your host addresses as a single entity and create rules that apply to the address range object. This will result in far fewer rules than if you were to create rules for individual host objects. Because using an address range object requires fewer rules, the Security Policy will load faster.

In this scenario, you cannot create the appropriate rules by using a single host object.

A dynamic object is an object whose name is resolved to a different IP address for each FireWall-1 NG computer. In this scenario, you cannot create the appropriate rules by using a single dynamic object.

You should not create multiple objects for each host.

**Objective:**

The Security Policy

**Sub-Objective:**

List the guidelines for improving VPN-1/FireWall-1 NG performance using a Security Policy

**References:**

Check Point Courseware, Chapter 5, Improving VPN-1/Firewall-1 Performance, pp. 134-135.