

# 156-215.65 : Check Point Security Administrator NGX R70

1

Select the correct statement about Secure Internal Communications (SIC) Certificates? SIC Certificates:

- A. for NGX Security Gateways are created during the SmartCenter Server installation.
- B. for the SmartCenter Server are created during the SmartCenter Server installation.
- C. are used for securing internal network communications between the SmartView Tracker and an OPSEC device.
- D. decrease network security by securing administrative communication among the SmartCenter Servers and the Security Gateway.
- E. uniquely identify Check Point enabled machines; they have the same function as Authentication Certificates.

2

Jill is about to test some rule and object changes suggested in an NGX newsgroup. Which backup and restore solution should Jill use, to ensure she can most easily restore her Security Policy to its previous configuration, after testing the changes?

- A. SecurePlatform backup utilities
- B. Manual copies of the `$FWDIR/conf` directory
- C. `upgrade_export` and `upgrade_import` commands
- D. Policy Package management
- E. Database Revision Control

3

Your organization's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How would you request and apply the license? Request a central license:

- A. using the remote Gateway's IP address. Apply the license locally with the `cplic put` command.
- B. for the Gateways' IP addresses. Apply the licenses on the SmartCenter Server with the `cplic put` command.
- C. using the remote Gateway's IP address. Attach the license to the remote Gateway via SmartUpdate.
- D. using your SmartCenter Server's IP address. Attach the license to the remote Gateway via SmartUpdate.
- E. using the SmartCenter Server's IP address. Apply the license locally on the remote Gateway with the `cplic put` command.

4

Sarah is the Security Administrator for a sporting-goods manufacturer. Sarah has configured SmartDefense to block the `CMD` and `FIND` commands. Sarah installs the Security Policy, but the Security Gateway continues to pass the commands. Which of the following could be the cause of the problem?

- A. The Rule Base includes a rule accepting FTP to any source, and from any destination.
- B. The SmartDefense > Application Intelligence > FTP Security Server screen does not have the radio button set to "Configurations apply to all connections".
- C. The FTP Service Object > Advanced > Blocked FTP Commands list does not include `CMD` and `FIND`.
- D. The Web Intelligence > Application Layer > FTP Settings list is configured to allow, rather than exclude, `CMD` and `FIND` commands.
- E. The Global Properties > Security Server > "Control FTP Commands" box is not checked.

5

Herman is attempting to configure a site-to-site VPN with one of his firm's business partners. Herman thinks Phase 2 negotiations are failing. Which SmartConsole application should Herman use to confirm his suspicions?

- A. SmartUpdate
- B. SmartView Tracker
- C. SmartView Monitor
- D. SmartDashboard
- E. SmartView Status

6

How can you unlock an administrator's account, which was been locked due to SmartCenter Access settings in Global Properties?

- A. Type `fwm lock_admin -ua` from the command line of the SmartCenter Server.
- B. Clear the "locked" box of the user's General Properties in SmartDashboard.
- C. Type `fwm unlock_admin -ua` from the command line of the SmartCenter Server.
- D. Type `fwm unlock_admin -ua` from the command line of the Security Gateway.
- E. Delete the file `admin.lock` in the `$FWDIR/tmp/` directory of the SmartCenter Server.

7

Which encryption scheme provides "in-place" encryption?

- A. IKE
- B. Manual IPSec
- C. DES
- D. SKIP
- E. AES

8

You are setting up a Virtual Private Network, and must select an encryption scheme. Your data is extremely business sensitive and you want maximum security for your data communications. Which encryption scheme would you select?

- A. Tunneling mode encryption
- B. In-place encryption
- C. Either one will work without compromising performance

9

How do you view a Security Administrator's activities, using SmartConsole tools? With:

- A. User Monitor
- B. SmartView Monitor using the Administrator Activity filter
- C. SmartView Tracker in Log mode
- D. SmartView Tracker in Audit mode
- E. SmartView Status

10

Your internal Web server in the DMZ has IP address 172.16.10.1/24. A particular network from the Internet tries to access this Web server. You need to set up some type of Network Address Translation (NAT), so that NAT occurs only for the HTTP service, and only from the remote network as the source. The public IP address for the Web server is 200.200.200.1. All properties in the NAT screen of Global Properties are enabled.

Select the correct NAT rules, so NAT happens ONLY between "web\_dallas" and the remote network.

- A.
  1. Create another node object named "web\_dallas\_valid", and enter "200.200.200.1" in the General Properties screen.
  2. Create two manual NAT rules above the automatic Hide NAT rules for the 172.16.10.0 network.
  3. Select "HTTP" in the Service column of both manual NAT rules.
  4. Enter an ARP entry and route on the Security Gateway's OS.
- B.
  1. Enable NAT on the web\_dallas object, select "static", and enter "200.200.200.1" in the General Properties screen.
  2. Specify "HTTP" in the automatic Static Address Translation rules.
  3. Create incoming and outgoing rules for the web\_dallas server, for the HTTP service only.
- C.
  1. Enable NAT on the web\_dallas object, select "hide", and enter "200.200.200.1" for the Hide NAT IP address.
  2. Specify "HTTP" in the Address Translation rules that are generated automatically.
  3. Create incoming and outgoing rules for the web\_dallas server, for the HTTP service only.
- D.
  1. Create another node object named "web\_dallas\_valid", and enter "200.200.200.1" in the General Properties screen.
  2. Create two manual NAT rules below the Automatic Hide NAT rule for network 172.16.10.0, in the Address Translation Rule Base.
  3. Select "HTTP" in the Service column of both manual NAT rules.
  4. Enter an ARP entry and route on the Security Gateway's OS.

## 11

How are cached usernames and passwords cleared from the memory of an NGX Security Gateway?

- A. Usernames and passwords only clear from memory after they time out.
- B. By retrieving LDAP user information, using the `fw fetchldap` command
- C. By using the Clear User Cache button in SmartDashboard
- D. By installing a Security Policy
- E. By pushing new user information from the LDAP server

## 12

Ivan's main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. Ivan also has a small network 10.10.20.0/24 behind the internal router. Ivan wants to configure the kernel to translate the source address only when network 10.10.20.0 tries to access the Internet for HTTP, SMTP, and FTP services.

Which of the following configurations will allow this network to access Internet?

- A. Automatic Static NAT on network 10.10.20.0/24
- B. Manual Hide NAT rules for HTTP, FTP, and SMTP services for network 10.10.20.0/24
- C. Manual Static NAT rules for network 10.10.20.0/24
- D. Automatic Hide NAT for network 10.10.20.0/24
- E. No change is necessary

## 13

You have just started a new job as the Security Administrator for Widgets Inc. Your boss has asked you to ensure that peer-to-peer file sharing is not allowed past the corporate Security Gateway. Where should you configure this?

- A. SmartDashboard > SmartDefense
- B. SmartDashboard > WebDefense
- C. By editing the file `$FWDIR/conf/application_intelligence.C`
- D. SmartDashboard > Policy > Global Properties > Malicious Activity Detection
- E. SmartDashboard > Web Intelligence

## 14

Jeremy manages sites in Tokyo, Calcutta and Dallas, from his office in Chicago. He is trying to create a report for management, detailing the current software level of each Security Gateway. He also wants to create a proposal outline, listing the most cost-effective way to upgrade his Gateways. Which two SmartConsole applications should Jeremy use, to create his report and outline?

- A. SmartLSM and SmartUpdate
- B. SmartDashboard and SmartLSM
- C. SmartDashboard and SmartView Tracker
- D. SmartView Monitor and SmartUpdate
- E. SmartView Tracker and SmartView Monitor

## 15

Your internal network is using 10.1.1.0/24. This network is behind your perimeter NGX VPN-1 Gateway, which connects to your ISP provider. How do you configure the Gateway to allow this network to go out to the Internet?

- A. Use automatic Static NAT for network 10.1.1.0/24.
- B. Use Hide NAT for network 10.1.1.0/24 behind the internal interface of your perimeter Gateway.
- C. Use manual Static NAT on the client side for network 10.1.1.0/24.
- D. Use Hide NAT for network 10.1.1.0/24 behind the external IP address of your perimeter Gateway.
- E. Do nothing, as long as 10.1.1.0 network has the correct default Gateway.

16

Your primary SmartCenter Server runs on SecurePlatform. What is the easiest way to back up your NGX configuration, including routing and network configuration files?

- A. Using the `upgrade_export` command in the `$FWDIR\bin` directory
- B. Running a `conf_merge` with an `objects_5_0.c` from a new NGX installation
- C. Copying the contents of `$FWDIR` to another location
- D. Copying the `$FWDIR\conf` and `$FWDIR\lib` directory to another location
- E. Using the native SecurePlatform backup utility from command line or in Web based interface

17

Anna is working in a large hospital, together with three other Security Administrators. Which SmartConsole tool should she use to check changes to rules or object properties other administrators made?

- A. SmartDashboard
- B. SmartView Tracker
- C. Eventia Tracker
- D. Eventia Monitor
- E. SmartView Monitor

18

Mary is the IT auditor for a bank. One of her responsibilities is reviewing the Security Administrator activity and comparing it to the change log. Which application should Mary use to view Security Administrator activity?

- A. NGX cannot display Security Administrator activity
- B. SmartView Tracker in Real-Time Mode
- C. SmartView Tracker in Audit Mode
- D. SmartView Tracker in Log Mode
- E. SmartView Tracker in Active Mode

19

Which NGX configuration setting forces the Client Authentication authorization time-out to refresh, each time a new user is authenticated? Choose ONE. The:

- A. "Time" properties, adjusted on the user objects for each user, in the source of the Client Authentication rule
- B. Time object, with hours restricted and renewable, in the Time field of the Client Authentication rule
- C. SmartDefense > Application Intelligence > Client Authentication > Refresh User Timeout option enabled
- D. Global Properties > Authentication parameters, adjusted to allow for "Regular Client Refreshment"
- E. "Refreshable Timeout" setting, in the Limit tab of the Client Authentication Action properties screen

20

A user attempts authentication using SecureClient. The user's password is rejected, even though it is correctly defined in the LDAP directory. Which of the following is a valid cause?

- A. The LDAP server has insufficient memory.
- B. The LDAP and Security Gateway databases are not synchronized.
- C. The SmartCenter Server cannot communicate with the LDAP server.
- D. The user has defined the wrong encryption scheme.
- E. The user is defined in both the NGX user database and the LDAP directory.