Vendor: CheckPoint

Exam Code: 156-215.13

Exam Name: Check Point Certified Security Administrator - GAiA

Version: Demo

Topic 1, Volume A

QUESTION NO: 1

Which of the following are available SmartConsole clients which can be installed from the R76 Windows CD? Read all answers and select the most complete and valid list.

A. SmartView Tracker, CPINFO, SmartUpdate
B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
C. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Answer: A
Explanation:

QUESTION NO: 2

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

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

Answer: D
Explanation:

QUESTION NO: 3

Your bank's distributed R76 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. SmartView Tracker
B. SmartPortal
C. SmartUpdate
D. SmartDashboard

Answer: A
Explanation:

QUESTION NO: 4

When launching SmartDashboard, what information is required to log into R76?

A. User Name, Management Server IP, certificate fingerprint file
B. User Name, Password, Management Server IP
C. Password, Management Server IP
D. Password, Management Server IP, LDAP Server IP

Answer: D
Explanation:

QUESTION NO: 5

Message digests use which of the following?

A. SHA-1 and MD5
B. IDEA and RC4
C. SSL and MD4
D. DES and RC4

Answer: C
Explanation:

QUESTION NO: 6

Which of the following is a hash algorithm?

A. DES
B. IDEA
C. MD5
D. 3DES

Answer: A
Explanation:

QUESTION NO: 7

Which of the following uses the same key to decrypt as it does to encrypt?

A. Asymmetric encryption
B. Symmetric encryption
C. Certificate-based encryption
D. Dynamic encryption

Answer: A
Explanation:

QUESTION NO: 8

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. SmartView Tracker
C. SmartUpdate
D. SmartView Status

Answer: C
Explanation:

QUESTION NO: 9

A digital signature:

A. Provides a secure key exchange mechanism over the Internet.
B. Automatically exchanges shared keys.
C. Guarantees the authenticity and integrity of a message.
D. Decrypts data to its original form.

Answer: B
Explanation:

QUESTION NO: 10

Which component functions as the Internal Certificate Authority for R76?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLSM

Answer: C
Explanation:

QUESTION NO: 11

Which SmartConsole component can Administrators use to track changes to the Rule Base?

A. SmartView Monitor
B. SmartReporter
C. WebUI
D. SmartView Tracker

Answer: D
Explanation:

QUESTION NO: 12

UDP packets are delivered if they are _____.

A. referenced in the SAM related dynamic tables
B. a valid response to an allowed request on the inverse UDP ports and IP
C. a stateful ACK to a valid SYN-SYN/ACK on the inverse UDP ports and IP
D. bypassing the kernel by the forwarding layer of ClusterXL

Answer: B
Explanation:

QUESTION NO: 13

The INSPECT engine inserts itself into the kernel between which two OSI model layers?

A. Physical and Data
B. Session and Transport
C. Data and Network
D. Presentation and Application

Answer: C
Explanation:

QUESTION NO: 14

The customer has a small Check Point installation, which includes one SecurePlatform server working as the SmartConsole, and a second server running Windows 2008 as both Security Management Server and Security Gateway. This is an example of a(n):

A. Distributed Installation
B. Stand-Alone Installation
C. Hybrid Installation
D. Unsupported configuration

Answer: D
Explanation:

QUESTION NO: 15

The customer has a small Check Point installation which includes one Windows 2008 server as the SmartConsole and a second server running SecurePlatform as both Security Management Server and the Security Gateway. This is an example of a(n):

A. Stand-Alone Installation
B. Distributed Installation
C. Unsupported configuration
D. Hybrid Installation

Answer: A
Explanation:

QUESTION NO: 16

The customer has a small Check Point installation which includes one Windows 7 workstation as the SmartConsole, one GAiA device working as Security Management Server, and a third server running SecurePlatform as Security Gateway. This is an example of a(n):

A. Unsupported configuration
B. Stand-Alone Installation
C. Hybrid Installation
D. Distributed Installation

Answer: D
Explanation:

QUESTION NO: 17

The customer has a small Check Point installation which includes one Windows 2008 server as SmartConsole and Security Management Server with a second server running SecurePlatform as Security Gateway. This is an example of a(n):

A. Stand-Alone Installation.
B. Distributed Installation.
C. Hybrid Installation.
D. Unsupported configuration.

Answer: B
Explanation:

QUESTION NO: 18

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

A. SecureClient
B. Security Gateway
C. None, Security Management Server would be installed by itself.
D. SmartConsole

Answer: B
Explanation:

QUESTION NO: 19

Tom has been tasked to install Check Point R76 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does not include a SmartConsole machine in his calculations?

A. Three machines
B. One machine
C. One machine, but it needs to be installed using SecurePlatform for compatibility purposes
D. Two machines

Answer: D
Explanation:

QUESTION NO: 20

Which of the following statements is TRUE about management plug-ins?

A. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
B. The plug-in is a package installed on the Security Gateway.
C. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.
D. Installing a management plug-in is just like an upgrade process.

Answer: A
Explanation:

QUESTION NO: 21

You are installing a Security Management Server. Your security plan calls for three administrators for this particular server. How many can you create during installation?

A. Depends on the license installed on the Security Management Server
B. One

C. As many as you want
D. Only one with full access and one with read-only access

Answer: B
Explanation:

QUESTION NO: 22

During which step in the installation process is it necessary to note the fingerprint for first-time verification?

A. When configuring the Security Gateway object in SmartDashboard
B. When configuring the Security Management Server using cpconfig
C. When establishing SIC between the Security Management Server and the Gateway
D. When configuring the Gateway in the WebUI

Answer: B
Explanation:

QUESTION NO: 23

How can you most quickly reset Secure Internal Communications (SIC) between a Security Management Server and Security Gateway?

A. From the Security Management Server's command line, type fw putkey -p <shared key> <IP Address of Security Gateway>.
B. Run the command fwm sic_reset to reinitialize the Security Management Server Internal Certificate Authority (ICA). Then retype the activation key on the Security Gateway from SmartDashboard.
C. Use SmartUpdate to retype the Security Gateway activation key. This will automatically sync SIC to both the Security Management Server and Gateway.
D. From cpconfig on the Gateway, choose the Secure Internal Communication option and retype the activation key. Next, retype the same key in the Gateway object in SmartDashboard and reinitialize Secure Internal Communications (SIC).

Answer: D
Explanation:

QUESTION NO: 24

How can you recreate the Security Administrator account, which was created during initial Management Server installation on SecurePlatform?

A. Launch cpconfig and delete the Administrator's account. Recreate the account with the same name.
B. Launch SmartDashboard in the User Management screen, and delete the cpconfig administrator.
C. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the Administrator Account portion of the file. You will be prompted to create a new account.
D. Type cpm -a, and provide the existing Administrator's account name. Reset the Security Administrator's password.

Answer: A
Explanation:

QUESTION NO: 25

When Jon first installed his new security system, he forgot to configure DNS servers on his Security Gateway. How could Jon configure DNS servers now that his Security Gateway is in production?

A. Login to the SmartDashboard, edit the firewall Gateway object, select the tab Interfaces > Domain Name Servers.
B. Login to the firewall using SSH and run cpconfig, then select Domain Name Servers.
C. Login to the firewall using SSH and run fwm, then select System Configuration > Domain Name Servers.
D. Login to the firewall using SSH and run sysconfig, then select Domain Name Servers.

Answer: D
Explanation:

QUESTION NO: 26

The London Security Gateway Administrator has just installed the Security Gateway and Management Server. He has not changed any default settings. As he tries to configure the Gateway, he is unable to connect. Which troubleshooting suggestion will NOT help him?

A. Check if some intermediate network device has a wrong routing table entry, VLAN assignment, duplex-mismatch, or trunk issue.

B. Verify that the Rule Base explicitly allows management connections.
C. Test the IP address assignment and routing settings of the Security Management Server, Gateway, and console client.
D. Verify the SIC initialization.

Answer: B
Explanation:

QUESTION NO: 27

You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? (i.e. the command cprestart is not sufficient.)

1. Adding a hot-swappable NIC to the Operating System for the first time.
2. Uninstalling the R75 Power/UTM package.
3. Installing the R75 Power/UTM package.
4. Re-establishing SIC to the Security Management Server.
5. Doubling the maximum number of connections accepted by the Security Gateway.

A. 2, 3 only
B. 3 only
C. 3, 4, and 5 only
D. 1, 2, 3, 4, and 5

Answer: A
Explanation:

QUESTION NO: 28

The Security Gateway is installed on SecurePlatform R76 The default port for the Web User Interface is _____.

A. TCP 443
B. TCP 4433
C. TCP 18211
D. TCP 257

Answer: A

Explanation:

QUESTION NO: 29

Over the weekend, an Administrator without access to SmartDashboard installed a new R76 Security Gateway using GAiA. You want to confirm communication between the Gateway and the Management Server by installing the Security Policy. What might prevent you from installing the Policy?

A. You first need to run the command fw unloadlocal on the new Security Gateway.
B. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Server. You must initialize SIC on both the Security Gateway and the Management Server.
C. You first need to initialize SIC in SmartUpdate.
D. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Server. You must initialize SIC on the Security Management Server.

Answer: D
Explanation:

QUESTION NO: 30

An Administrator without access to SmartDashboard installed a new IPSO-based R76 Security Gateway over the weekend. He e-mailed you the SIC activation key. You want to confirm communication between the Security Gateway and the Management Server by installing the Policy. What might prevent you from installing the Policy?

A. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Server. You must initialize SIC on the Security Management Server.
B. You first need to create a new Gateway object in SmartDashboard, establish SIC via the Communication button, and define the Gateway's topology.
C. An intermediate local Security Gateway does not allow a policy install through it to the remote new Security Gateway appliance. Resolve by running the command fw unloadlocal on the local Security Gateway.
D. You first need to run the command fw unloadlocal on the R75 Security Gateway appliance in order to remove the restrictive default policy.

Answer: B
Explanation:

QUESTION NO: 31

How can you reset the Security Administrator password that was created during initial Security Management Server installation on SecurePlatform?

A. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the Password portion of the file. Then log in to the account without a password. You will be prompted to assign a new password.
B. Launch SmartDashboard in the User Management screen, and edit the cpconfig administrator.
C. Type cpm -a, and provide the existing administrator's account name. Reset the Security Administrator's password.
D. As expert user Type fwm -a, and provide the existing administrator's account name. Reset the Security Administrator's password.

Answer: D
Explanation:

QUESTION NO: 32

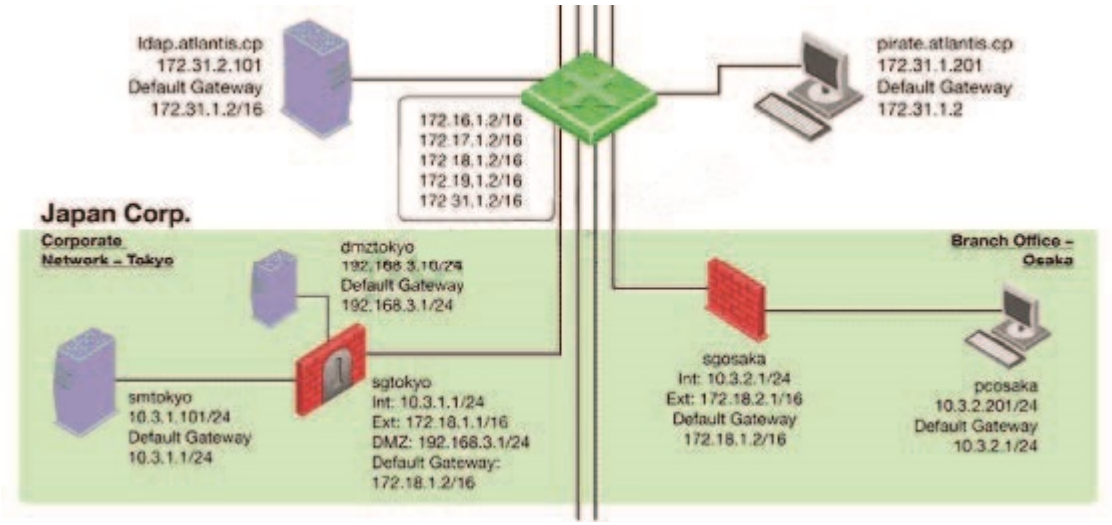
You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

A. Active-X must be allowed on the client.
B. The SNX client application must be installed on the client.
C. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
D. An office mode address must be obtained by the client.

Answer: C
Explanation:

QUESTION NO: 33

The Tokyo Security Management Server Administrator cannot connect from his workstation in Osaka.



Which of the following lists the BEST sequence of steps to troubleshoot this issue?

A. Call Tokyo to check if they can ping the Security Management Server locally. If so, login to sgtokyo, verify management connectivity and Rule Base. If this looks okay, ask your provider if they have some firewall rules that filters out your management traffic.
B. Verify basic network connectivity to the local Gateway, service provider, remote Gateway, remote network and target machine. Then, test for firewall rules that deny management access to the target. If successful, verify that pcosaka is a valid client IP address.
C. Check for matching OS and product versions of the Security Management Server and the client. Then, ping the Gateways to verify connectivity. If successful, scan the log files for any denied management packets.
D. Check the allowed clients and users on the Security Management Server. If pcosaka and your user account are valid, check for network problems. If there are no network related issues, this is likely to be a problem with the server itself. Check for any patches and upgrades. If still unsuccessful, open a case with Technical Support.

Answer: B
Explanation:

QUESTION NO: 34

Match the following commands to their correct function.

Command	Function
C1 `cp_admin_convert`	F1: export and import different revisions of the database.
C2 `cpca_client`	F2: export and import policy packages.
C3 `cp_merge`	F3: transfer Log data to an external database.
C4 `cpwd_admin`	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard.

Each command has one function only listed.

A. C1>F2; C2>F1; C3>F6; C4>F4
B. C1>F4; C2>F6; C3>F3; C4>F2
C. C1>F2; C2>F4; C3>F1; C4>F5
D. C1>F6; C2>F4; C3>F2; C4>F5

Answer: D
Explanation:

QUESTION NO: 35

Which command displays the installed Security Gateway version?

A. fw ver
B. fw stat
C. fw printver
D. cpstat -gw

Answer: A
Explanation:

QUESTION NO: 36

Which command line interface utility allows the administrator to verify the Security Policy name and timestamp currently installed on a firewall module?

A. fw stat

B. fw ctl pstat
C. fw ver
D. cpstat fwd

Answer: A
Explanation:

QUESTION NO: 37

Suppose the Security Gateway hard drive fails and you are forced to rebuild it. You have a snapshot file stored to a TFTP server and backups of your Security Management Server. What is the correct procedure for rebuilding the Gateway quickly?

A. Run the command revert to restore the snapshot. Reinstall any necessary Check Point products. Establish SIC and install the Policy.
B. Reinstall the base operating system (i.e., SecurePlatform). Configure the Gateway interface so that the Gateway can communicate with the TFTP server. Revert to the stored snapshot image, and install the Security Policy.
C. Run the command revert to restore the snapshot, establish SIC, and install the Policy.
D. Reinstall the base operating system (i.e., SecurePlatform). Configure the Gateway interface so that the Gateway can communicate with the TFTP server. Reinstall any necessary Check Point products and previously applied hotfixes. Revert to the stored snapshot image, and install the Policy.

Answer: B
Explanation:

QUESTION NO: 38

Which of the following statements accurately describes the command upgrade_export?

A. Used primarily when upgrading the Security Management Server, upgrade_export stores all object databases and the /conf directories for importing to a newer Security Gateway version.
B. upgrade_export stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.
C. This command is no longer supported in GAiA.
D. upgrade_export is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.

Answer: A
Explanation:

QUESTION NO: 39

What are you required to do before running the command upgrade_export?

A. Run a cpstop on the Security Management Server.
B. Run a cpstop on the Security Gateway.
C. Close all GUI clients.
D. Run cpconfig and set yourself up as a GUI client.

Answer: C
Explanation:

QUESTION NO: 40

A snapshot delivers a complete SecurePlatform backup. The resulting file can be stored on servers or as a local file in /var/CPsnapshot/snapshots. How do you restore a local snapshot named MySnapshot.tgz?

A. As expert user, type the command revert --file MySnapshot.tgz.
B. As expert user, type the command snapshot -r MySnapshot.tgz.
C. As expert user, type the command snapshot - R to restore from a local file. Then, provide the correct file name.
D. Reboot the system and call the start menu. Select the option Snapshot Management, provide the Expert password and select [L] for a restore from a local file. Then, provide the correct file name.

Answer: A
Explanation:

QUESTION NO: 41

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
Explanation:

QUESTION NO: 42

What is the syntax for uninstalling a package using newpkg?

A. -u <pathname of package>
B. newpkg CANNOT be used to uninstall a package
C. -i <full pathname of package>
D. -S <pathname of package>

Answer: B
Explanation:

QUESTION NO: 43

Your primary Security Gateway runs on SecurePlatform. What is the easiest way to back up your Security Gateway R76 configuration, including routing and network configuration files?

A. Using the native SecurePlatform backup utility from command line or in the Web based user interface.
B. Copying the directories $FWDIR/conf and $FWDIR/lib to another location.
C. Using the command upgrade_export.
D. Run the pre_upgrade_verifier and save the .tgz file to the directory /temp.

Answer: A
Explanation:

QUESTION NO: 44

You need to back up the routing, interface, and DNS configuration information from your R76 GAiA Security Gateway. Which backup-and-restore solution do you use?

A. GAiA back up utilities
B. upgrade_export and upgrade_import commands
C. Database Revision Control
D. Manual copies of the directory $FWDIR/conf

Answer: A
Explanation:

QUESTION NO: 45

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
Explanation:

QUESTION NO: 46

Before upgrading SecurePlatform, you should create a backup. To save time, many administrators use the command backup. This creates a backup of the Check Point configuration as well as the system configuration.

An administrator has installed the latest HFA on the system for fixing traffic problem after creating a backup file. There is a mistake in the very complex static routing configuration. The Check Point configuration has not been changed. Can the administrator use a restore to fix the errors in static routing?

A. The restore is done by selecting Snapshot Management from the boot menu of GAiA.
B. A backup cannot be restored, because the binary files are missing.
C. The restore can be done easily by the command restore and selecting the file netconf.C.
D. The restore is not possible because the backup file does not have the same build number (version).

Answer: C
Explanation:

QUESTION NO: 47

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

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

Answer: A
Explanation:

QUESTION NO: 48

You intend to upgrade a Check Point Gateway from R71 to R76. Prior to upgrading, you want to back up the Gateway should there be any problems with the upgrade. Which of the following allows for the Gateway configuration to be completely backed up into a manageable size in the least amount of time?

A. upgrade_export
B. snapshot
C. backup
D. database revision

Answer: C
Explanation:

QUESTION NO: 49

Your network is experiencing connectivity problems and you want to verify if routing problems are present. You need to disable the firewall process but still allow routing to pass through the Gateway running on an IP Appliance running IPSO. What command do you need to run after stopping the firewall service?

A. ipsofwd on admin
B. ipsofwd slowpath

C. fw fwd routing
D. fw load routed

Answer: A
Explanation:

QUESTION NO: 50

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

A. cpconfig
B. ifconfig
C. dhcp_cfg
D. sysconfig

Answer: D
Explanation:

QUESTION NO: 51

The third-shift Administrator was updating Security Management Server access settings in Global Properties and testing. He managed to lock himself out of his account. How can you unlock this account?

A. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.
B. Type fwm lock_admin -u <account name> from the Security Management Server command line.
C. Type fwm unlock_admin -u from the Security Gateway command line.
D. Type fwm unlock_admin from the Security Management Server command line.

Answer: B
Explanation:

QUESTION NO: 52

The third-shift Administrator was updating Security Management Server access settings in Global Properties. He managed to lock all administrators out of their accounts. How should you unlock these accounts?

A. Reinstall the Security Management Server and restore using upgrade_import.
B. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.
C. Type fwm lock_admin -ua from the Security Management Server command line.
D. Login to SmartDashboard as the special cpconfig_admin user account; right-click on each administrator object and select unlock.

Answer: C
Explanation:

QUESTION NO: 53

You are the Security Administrator for ABC-Corp. A Check Point Firewall is installed and in use on SecurePlatform. You are concerned that the system might not be retaining your entries for the interfaces and routing configuration. You would like to verify your entries in the corresponding file(s) on SecurePlatform. Where can you view them? Give the BEST answer.

A. /etc/conf/route.C
B. /etc/sysconfig/network-scripts/ifcfg-ethx
C. /etc/sysconfig/netconf.C
D. /etc/sysconfig/network

Answer: C
Explanation:

QUESTION NO: 54

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
B. As expert user, issue these commands:
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
Explanation:

QUESTION NO: 55

Several Security Policies can be used for different installation targets. The Firewall protecting Human Resources' servers should have its own Policy Package. These rules must be installed on this machine and not on the Internet Firewall. How can this be accomplished?

A. A Rule Base is always installed on all possible targets. The rules to be installed on a Firewall are defined by the selection in the Rule Base row Install On.
B. A Rule Base can always be installed on any Check Point Firewall object. It is necessary to select the appropriate target directly after selecting Policy > Install on Target.
C. When selecting the correct Firewall in each line of the Rule Base row Install On, only this Firewall is shown in the list of possible installation targets after selecting Policy > Install on Target.
D. In the menu of SmartDashboard, go to Policy > Policy Installation Targets and select the correct firewall via Specific Targets.

Answer: D
Explanation:

QUESTION NO: 56

Where is the IPSO Boot Manager physically located on an IP Appliance?

A. On the platform's BIOS
B. In the directory /nvram
C. On an external jump drive
D. On built-in compact Flash memory

Answer: D
Explanation:

QUESTION NO: 57

How is wear on the flash storage device mitigated on diskless appliance platforms?

A. The external PCMCIA-based flash extension has the swap file mapped to it, allowing easy replacement.
B. A RAM drive reduces the swap file thrashing which causes fast wear on the device.
C. Issue FW-1 bases its package structure on the Security Management Server, dynamically loading when the firewall is booted.
D. PRAM flash devices are used, eliminating the longevity.

Answer: B
Explanation:

QUESTION NO: 58

Your R76 primary Security Management Server is installed on GAiA. You plan to schedule the Security Management Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. Create a time object, and add 48 hours as the interval. Select that time object's Global Properties > Logs and Masters window, to schedule a logswitch.
B. Create a time object, and add 48 hours as the interval. Open the primary Security Management Server object's Logs and Masters window, enable Schedule log switch, and select the Time object.
C. On a SecurePlatform Security Management Server, this can only be accomplished by configuring the command fw logswitch via the cron utility.
D. Create a time object, and add 48 hours as the interval. Open the Security Gateway object's Logs and Masters window, enable Schedule log switch, and select the Time object.

Answer: B
Explanation:

QUESTION NO: 59

Which of the following methods will provide the most complete backup of an R75 configuration?

A. Execute command upgrade_export
B. Database Revision Control
C. Policy Package Management
D. Copying the directories $FWDIR\conf and $CPDIR\conf to another server

Answer: A
Explanation:

QUESTION NO: 60

Which of the following commands can provide the most complete restoration of a R76 configuration?

A. cpinfo -recover
B. fwm dbimport -p <export file>
C. upgrade_import
D. cpconfig

Answer: C
Explanation:

QUESTION NO: 61

When restoring R76 using the command upgrade_import, which of the following items are NOT restored?

A. Licenses
B. SIC Certificates
C. Global properties
D. Route tables

Answer: D
Explanation:

QUESTION NO: 62

Your organization's disaster recovery plan needs an update to the backup and restore section to reap the new distributed R76 installation benefits. Your plan must meet the following required and desired objectives:

Required ObjectivE. The Security Policy repository must be backed up no less frequently than every 24 hours.

Desired ObjectivE. The R76 components that enforce the Security Policies should be backed up at least once a week.

Desired ObjectivE. Back up R76 logs at least once a week.

Your disaster recovery plan is as follows:

- Use the cron utility to run the command upgrade_export each night on the Security Management Servers.

- Configure the organization's routine back up software to back up the files created by the

command upgrade_export.

- Configure the GAiA back up utility to back up the Security Gateways every Saturday night.

- Use the cron utility to run the command upgrade_export each Saturday night on the log servers.

- Configure an automatic, nightly logswitch.

- Configure the organization's routine back up software to back up the switched logs every night.

Upon evaluation, your plan:

A. Meets the required objective and only one desired objective.
B. Meets the required objective but does not meet either desired objective.
C. Meets the required objective and both desired objectives.
D. Does not meet the required objective.

Answer: C
Explanation:

QUESTION NO: 63

Your company is running Security Management Server R76 on GAiA, which has been migrated through each version starting from Check Point 4.1. How do you add a new administrator account?

A. Using cpconfig on the Security Management Server, choose Administrators
B. Using SmartDashboard, under Users, select Add New Administrator
C. Using the Web console on SecurePlatform under Product configuration, select Administrators
D. Using SmartDashboard or cpconfig

Answer: B
Explanation:

QUESTION NO: 64

Peter is your new Security Administrator. On his first working day, he is very nervous and enters the wrong password three times. His account is locked. What can be done to unlock Peter's account? Give the BEST answer.

A. It is not possible to unlock Peter's account. You have to install the firewall once again or abstain

from Peter's help.
B. You can unlock Peter's account by using the command fwm unlock_admin -u Peter on the Security Gateway.
C. You can unlock Peter's account by using the command fwm lock_admin -u Peter on the Security Management Server.
D. You can unlock Peter's account by using the command fwm unlock_admin -u Peter on the Security Management Server

Answer: C
Explanation:

QUESTION NO: 65

Where can you find the Check Point's SNMP MIB file?

A. $CPDIR/lib/snmp/chkpt.mib
B. There is no specific MIB file for Check Point products.
C. $FWDIR/conf/snmp.mib
D. It is obtained only by request from the TAC.

Answer: A
Explanation:

QUESTION NO: 66

You want to generate a cpinfo file via CLI on a system running GAiA. This will take about 40 minutes since the log files are also needed. What action do you need to take regarding timeout?

A. Log in as Administrator, set the timeout to one hour with the command idle 60 and start cpinfo.
B. Log in as the default user expert and start cpinfo.
C. No action is needed because cpshell has a timeout of one hour by default.
D. Log in as admin, switch to expert mode, set the timeout to one hour with the command, idle 60, then start cpinfo.

Answer: A
Explanation:

QUESTION NO: 67

Many companies have defined more than one administrator. To increase security, only one administrator should be able to install a Rule Base on a specific Firewall. How do you configure this?

A. Define a permission profile in SmartDashboard with read/write privileges, but restrict it to all other firewalls by placing them in the Policy Targets field. Then, an administrator with this permission profile cannot install a policy on any Firewall not listed here.
B. Put the one administrator in an Administrator group and configure this group in the specific Firewall object in Advanced > Permission to Install.
C. Right-click on the object representing the specific administrator, and select that Firewall in Policy Targets.
D. In the object General Properties representing the specific Firewall, go to the Software Blades product list and select Firewall. Right-click in the menu, select Administrator to Install to define only this administrator.

Answer: B
Explanation:

QUESTION NO: 68

What is the officially accepted diagnostic tool for IP Appliance Support?

A. ipsoinfo
B. cpinfo
C. uag-diag
D. CST

Answer: D
Explanation:

QUESTION NO: 69

ALL of the following options are provided by the SecurePlatform sysconfig utility, EXCEPT:

A. Export setup
B. Time & Date
C. DHCP Server configuration
D. GUI Clients

Answer: D

Explanation:

QUESTION NO: 70

Which of the following options is available with the SecurePlatform cpconfig utility?

A. Time & Date
B. GUI Clients
C. DHCP Server configuration
D. Export setup

Answer: B
Explanation:

QUESTION NO: 71

Which command would provide the most comprehensive diagnostic information to Check Point Technical Support?

A. cpstat - date.cpstat.txt
B. fw cpinfo
C. cpinfo -o date.cpinfo.txt
D. diag

Answer: C
Explanation:

QUESTION NO: 72

Which of the following statements accurately describes the command snapshot?

A. snapshot creates a Security Management Server full system-level backup on any OS.
B. snapshot stores only the system-configuration settings on the Gateway.
C. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server.
D. snapshot creates a full OS-level backup, including network-interface data, Check Point product information, and configuration settings during an upgrade of a SecurePlatform Security Gateway.

Explanation:

Answer: D

Explanation:

QUESTION NO: 73

How do you recover communications between your Security Management Server and Security Gateway if you lock yourself out through a rule or policy mis-configuration?

A. fw delete all.all@localhost
B. fw unload policy
C. fwm unloadlocal
D. fw unloadlocal

Answer: D

Explanation:

QUESTION NO: 74

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

Explanation:

QUESTION NO: 75

Which command allows you to view the contents of an R76 table?

A. fw tab -s <tablename>
B. fw tab -t <tablename>
C. fw tab -x <tablename>
D. fw tab -a <tablename>

Answer: B

Explanation:

QUESTION NO: 76

Which of the following tools is used to generate a Security Gateway R76 configuration report?

A. infoCP
B. cpinfo
C. infoview
D. fw cpinfo

Answer: B
Explanation:

QUESTION NO: 77

Which of the following is a CLI command for Security Gateway R76?

A. fw merge
B. fw tab -u
C. fw shutdown
D. fwm policy_print <policyname>

Answer: B
Explanation:

QUESTION NO: 78

You are the Security Administrator for MegaCorp. A Check Point firewall is installed and in use on a platform using GAiA. You have trouble configuring the speed and duplex settings of your Ethernet interfaces. Which of the following commands can be used in Expert Mode to configure the speed and duplex settings of an Ethernet interface and will survive a reboot? Give the BEST answer.

A. eth_set
B. mii_tool
C. ifconfig -a
D. ethtool

QUESTION NO: 79

Which command enables IP forwarding on IPSO?

A. echo 1 > /proc/sys/net/ipv4/ip_forward
B. ipsofwd on admin
C. echo 0 > /proc/sys/net/ipv4/ip_forward
D. clish -c set routing active enable

Answer: B
Explanation:

QUESTION NO: 80

When you change an implicit rule's order from Last to First in Global Properties, how do you make the change take effect?

A. Run fw fetch from the Security Gateway.
B. Select Install Database from the Policy menu.
C. Reinstall the Security Policy.
D. Select Save from the File menu.

Answer: C
Explanation:

QUESTION NO: 81

How does the button Get Address, found on the Host Node Object > General Properties page retrieve the address?

A. Route Table
B. Address resolution (ARP, RARP)
C. Name resolution (hosts file, DNS, cache)
D. SNMP Get

Answer: C
Explanation:

QUESTION NO: 82

Anti-Spoofing is typically set up on which object type?

A. Network
B. Security Management object
C. Host
D. Security Gateway

Answer: D
Explanation:

QUESTION NO: 83

Spoofing is a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Making packets appear as if they come from an authorized IP address.
C. Detecting people using false or wrong authentication logins.
D. Hiding your firewall from unauthorized users.

Answer: B
Explanation:

QUESTION NO: 84

How can you activate the SNMP daemon on a Check Point Security Management Server?

A. Using the command line, enter snmp_install.
B. Any of these options will work.
C. In SmartDashboard, right-click a Check Point object and select Activate SNMP.
D. From cpconfig, select SNMP extension.

Answer: D

Explanation:

QUESTION NO: 85

Which of the following describes the default behavior of an R76 Security Gateway?

A. Traffic is filtered using controlled port scanning.
B. IP protocol types listed as secure are allowed by default, i.e. ICMP, TCP, UDP sessions are inspected.
C. All traffic is expressly permitted via explicit rules.
D. Traffic not explicitly permitted is dropped.

Answer: D
Explanation:

QUESTION NO: 86

When you use the Global Properties' default settings on R76, which type of traffic will be dropped if NO explicit rule allows the traffic?

A. Firewall logging and ICA key-exchange information
B. RIP traffic
C. Outgoing traffic originating from the Security Gateway
D. SmartUpdate connections

Answer: B
Explanation:

QUESTION NO: 87

You have installed a R76 Security Gateway on GAiA. To manage the Gateway from the enterprise Security Management Server, you create a new Gateway object and Security Policy. When you install the new Policy from the Policy menu, the Gateway object does not appear in the Install Policy window as a target. What is the problem?

A. The new Gateway's temporary license has expired.
B. The object was created with Node > Gateway.
C. The Gateway object is not specified in the first policy rule column Install On.

D. No Masters file is created for the new Gateway.

Answer: B
Explanation:

QUESTION NO: 88

Certificates for Security Gateways are created during a simple initialization from _____.

A. The ICA management tool
B. SmartUpdate
C. sysconfig
D. SmartDashboard

Answer: D
Explanation:

QUESTION NO: 89

Which of the below is the MOST correct process to reset SIC from SmartDashboard?

A. Run cpconfig, and click Reset.
B. Click the Communication button for the firewall object, then click Reset. Run cpconfig and type a new activation key.
C. Click Communication > Reset on the Gateway object, and type a new activation key.
D. Run cpconfig, and select Secure Internal Communication > Change One Time Password.

Answer: B
Explanation:

QUESTION NO: 90

You installed Security Management Server on a computer using GAiA in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second SecurePlatform computer, which you plan to ship to another Administrator at a MegaCorp hub office. What is the correct order for pushing SIC certificates to the Gateway before shipping it?

A. 2, 1, 3, 4, 5

B. 2, 3, 4, 5, 1
C. 1, 3, 2, 4, 5
D. 2, 3, 4, 1, 5

Answer: A
Explanation:

QUESTION NO: 91

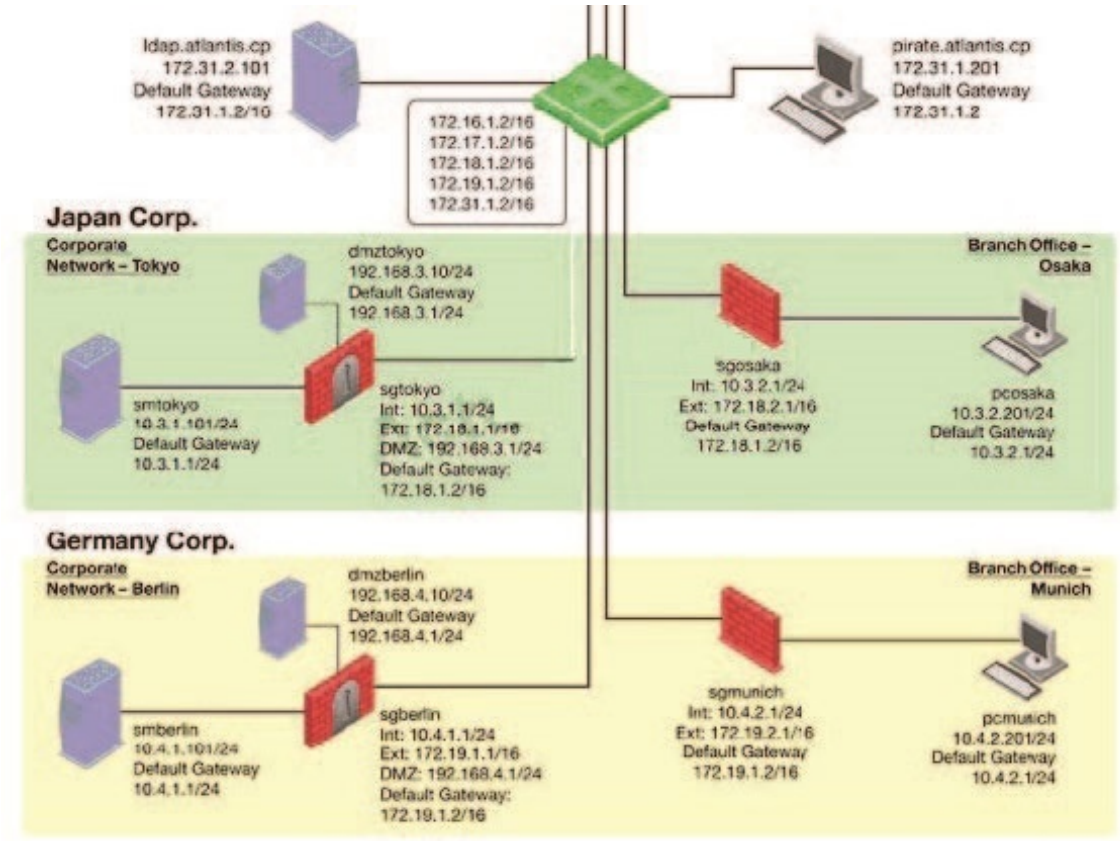
Although SIC was already established and running, Joe reset SIC between the Security Management Server and a remote Gateway. He set a new activation key on the Gateway's side with the command cpconfig and put in the same activation key in the Gateway's object on the Security Management Server. Unfortunately, SIC cannot be established. What is a possible reason for the problem?

A. Joe forgot to exit from cpconfig.
B. The installed policy blocks the communication.
C. The old Gateway object should have been deleted and recreated.
D. Joe forgot to reboot the Gateway.

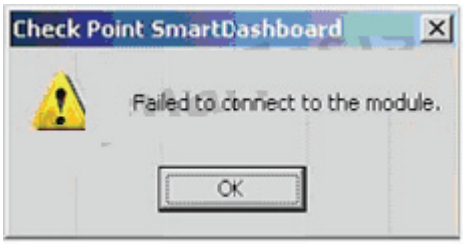
Answer: A
Explanation:

QUESTION NO: 92

You want to reset SIC between smberlin and sgosaka.



In SmartDashboard, you choose sgosaka, Communication, Reset. On sgosaka, you start cpconfig, choose Secure Internal Communication and enter the new SIC Activation Key. The screen reads The SIC was successfully initialized and jumps back to the cpconfig menu. When trying to establish a connection, instead of a working connection, you receive this error message:



What is the reason for this behavior?

A. The Gateway was not rebooted, which is necessary to change the SIC key.
B. The Check Point services on the Gateway were not restarted because you are still in the cpconfig utility.
C. You must first initialize the Gateway object in SmartDashboard (i.e., right-click on the object, choose Basic Setup > Initialize).
D. The activation key contains letters that are on different keys on localized keyboards. Therefore, the activation can not be typed in a matching fashion.

Answer: B
Explanation:

QUESTION NO: 93

John is the Security Administrator in his company. He installs a new R76 Security Management Server and a new R76 Gateway. He now wants to establish SIC between them. After entering the activation key, he gets the following message in SmartDashboard -

"Trust established"

SIC still does not seem to work because the policy won't install and interface fetching does not work. What might be a reason for this?

A. It always works when the trust is established
B. This must be a human error.
C. SIC does not function over the network.
D. The Gateway's time is several days or weeks in the future and the SIC certificate is not yet valid.

Answer: D
Explanation:

QUESTION NO: 94

The SIC certificate is stored in the directory _____.

A. $CPDIR/conf
B. $FWDIR/database
C. $CPDIR/registry
D. $FWDIR/conf

Answer: A
Explanation:

QUESTION NO: 95

You run cpconfig to reset SIC on the Security Gateway. After the SIC reset operation is complete, the policy that will be installed is the:

A. Default filter.
B. Last policy that was installed.
C. Standard policy.
D. Initial policy.

Answer: D
Explanation:

QUESTION NO: 96

Chris has lost SIC communication with his Security Gateway and he needs to re-establish SIC.

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.

What would be the correct order of steps needed to perform this task?

A. 3, 1, 4, 2
B. 2, 3, 1, 4
C. 5, 1, 2, 4
D. 5, 1, 4, 2

Answer: C
Explanation:

QUESTION NO: 97

Which rule position in the Rule Base should hold the Cleanup Rule? Why?

A. Last. It explicitly drops otherwise accepted traffic.
B. First. It explicitly accepts otherwise dropped traffic.
C. Last. It serves a logging function before the implicit drop.
D. Before last followed by the Stealth Rule.

Answer: C
Explanation:

QUESTION NO: 98

The _____and _____Rules are the two basic rules which should be used by all Security Administrators?

A. Cleanup; Stealth
B. Administrator Access; Stealth
C. Cleanup; Administrator Access
D. Network Traffic; Stealth

Answer: A
Explanation:

QUESTION NO: 99

Which item below in a Security Policy would be enforced first?

A. Network Address Translation
B. Security Policy First rule
C. Administrator-defined Rule Base
D. IP spoofing/IP options

Answer: D
Explanation:

QUESTION NO: 100

When you hide a rule in a Rule Base, how can you then disable the rule?

A. Right-click on the hidden rule place-holder bar and uncheck Hide, then right-click and select

Disable Rule(s); re-hide the rule.
B. Right-click on the hidden rule place-holder bar and select Disable Rule(s).
C. Use the search utility in SmartDashboard to view all hidden rules. Select the relevant rule and click Disable Rule(s).
D. Hidden rules are already effectively disabled from Security Gateway enforcement.

Answer: A
Explanation:

Topic 2, Volume B

QUESTION NO: 101

A Cleanup rule.

A. drops packets without logging connections that would otherwise be dropped and logged by default.
B. logs connections that would otherwise be accepted without logging by default.
C. drops packets without logging connections that would otherwise be accepted and logged by default.
D. logs connections that would otherwise be dropped without logging by default.

Answer: D
Explanation:

QUESTION NO: 102

Which statement is TRUE about implicit rules?

A. You create them in SmartDashboard.
B. The Gateway enforces implicit rules that enable outgoing packets only.
C. Changes to the Security Gateway's default settings do not affect implicit rules.
D. They are derived from Global Properties and explicit object properties.

Answer: D
Explanation:

QUESTION NO: 103

You have included the Cleanup Rule in your Rule Base. Where in the Rule Base should the

Accept ICMP Requests implied rule have no effect?

A. After Stealth Rule
B. First
C. Before Last
D. Last

Answer: D
Explanation:

QUESTION NO: 104

All of the following are Security Gateway control connections defined by default implied rules, EXCEPT:

A. Exclusion of specific services for reporting purposes.
B. Specific traffic that facilitates functionality, such as logging, management, and key exchange.
C. Acceptance of IKE and RDP traffic for communication and encryption purposes.
D. Communication with server types, such as RADIUS, CVP, UFP, TACACS, and LDAP.

Answer: A
Explanation:

QUESTION NO: 105

In a distributed management environment, the administrator has removed all default check boxes from the Policy > Global Properties > Firewall tab. In order for the Security Gateway to send logs to the Security Management Server, an explicit rule must be created to allow the Security Gateway to communicate to the Security Management Server on port _____.

A. 257
B. 256
C. 259
D. 900

Answer: A
Explanation:

QUESTION NO: 106

A Security Policy has several database versions. What configuration remains the same no matter which version is used?

A. Objects_5_0.C
B. fwauth.NDB
C. Rule Bases_5_0.fws
D. Internal Certificate Authority (ICA) certificate

Answer: D
Explanation:

QUESTION NO: 107

You are working with multiple Security Gateways that enforce an extensive number of rules. To simplify security administration, which one of the following would you choose to do?

A. Create network objects that restrict all applicable rules to only certain networks.
B. Run separate SmartConsole instances to login and configure each Security Gateway directly.
C. Create a separate Security Policy package for each remote Security Gateway.
D. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.

Answer: C
Explanation:

QUESTION NO: 108

Which rules are not applied on a first-match basis?

A. Client Authentication
B. Session Authentication
C. User Authentication
D. Cleanup

Answer: C
Explanation:

QUESTION NO: 109

Installing a policy usually has no impact on currently existing connections. Which statement is TRUE?

A. All connections are reset, so a policy install is recommended during announced downtime only.
B. Users being authenticated by Client Authentication have to re-authenticate.
C. Site-to-Site VPNs need to re-authenticate, so Phase 1 is passed again after installing the Security Policy.
D. All FTP downloads are reset; users have to start their downloads again.

Answer: B
Explanation:

QUESTION NO: 110

Several Security Policies can be used for different installation targets. The firewall protecting Human Resources' servers should have a unique Policy Package. These rules may only be installed on this machine and not accidentally on the Internet firewall. How can this be configured?

A. A Rule Base is always installed on all possible targets. The rules to be installed on a firewall are defined by the selection in the row Install On of the Rule Base.
B. When selecting the correct firewall in each line of the row Install On of the Rule Base, only this firewall is shown in the list of possible installation targets after selecting Policy > Install.
C. In the SmartDashboard policy, select the correct firewall to be the Specific Target of the rule.
D. A Rule Base can always be installed on any Check Point firewall object. It is necessary to select the appropriate target directly after selecting Policy > Install.

Answer: C
Explanation:

QUESTION NO: 111

A _____rule is used to prevent all traffic going to the R75 Security Gateway.

A. Cleanup
B. Stealth
C. Reject
D. IPS

Answer: B

Explanation:

QUESTION NO: 112

In a distributed management environment, the administrator has removed the default check from Accept Control Connections under the Policy > Global Properties > FireWall tab. In order for the Security Management Server to install a policy to the Firewall, an explicit rule must be created to allow the server to communicate to the Security Gateway on port _____.

A. 259
B. 256
C. 80
D. 900

Answer: B
Explanation:

QUESTION NO: 113

To check the Rule Base, some rules can be hidden so they do not distract the administrator from the unhidden rules. Assume that only rules accepting HTTP or SSH will be shown. How do you accomplish this?

A. This cannot be configured since two selections (Service, Action) are not possible.
B. Ask your reseller to get a ticket for Check Point SmartUse and deliver him the Security Management Server cpinfo file.
C. In SmartDashboard menu, select Search > Rule Base Queries. In the window that opens, create a new Query, give it a name (e.g. "HTTP_SSH") and define a clause regarding the two services HTTP and SSH. When having applied this, define a second clause for the action Accept and combine them with the Boolean operator AND.
D. In SmartDashboard, right-click in the column field Service > Query Column. Then, put the services HTTP and SSH in the list. Do the same in the field Action and select Accept here.

Answer: C
Explanation:

QUESTION NO: 114

What CANNOT be configured for existing connections during a policy install?

A. Reset all connections
B. Re-match connections
C. Keep all connections
D. Keep data connections

Answer: A
Explanation:

QUESTION NO: 115

What is the purpose of a Stealth Rule?

A. To permit implied rules.
B. To drop all traffic to the management server that is not explicitly permitted.
C. To prevent users from connecting directly to the gateway.
D. To permit management traffic.

Answer: C
Explanation:

QUESTION NO: 116

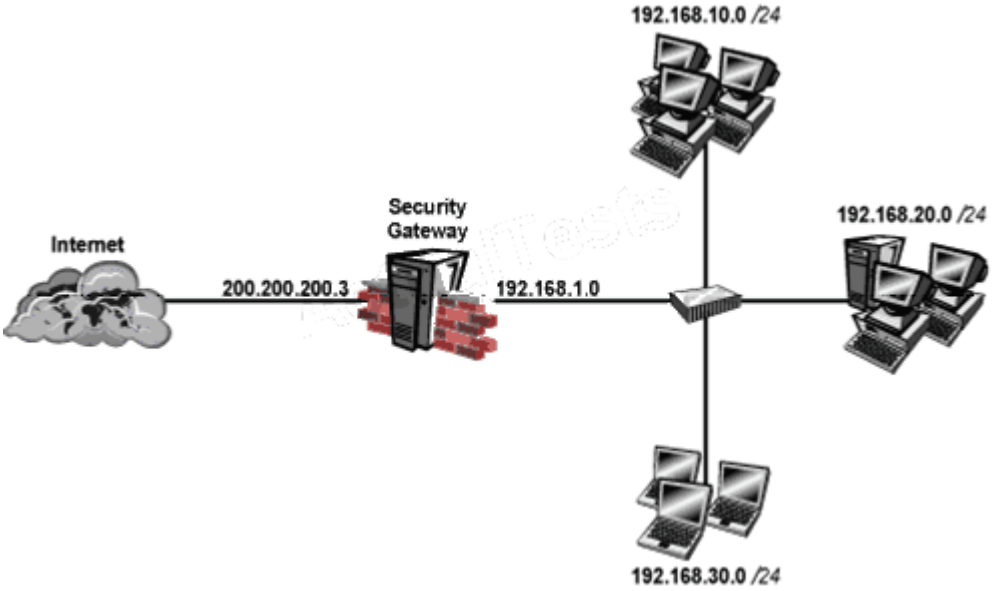
Which of these Security Policy changes optimize Security Gateway performance?

A. Use Automatic NAT rules instead of Manual NAT rules whenever possible.
B. Using domain objects in rules when possible.
C. Using groups within groups in the manual NAT Rule Base.
D. Putting the least-used rule at the top of the Rule Base.

Answer: A
Explanation:

QUESTION NO: 117

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 - groupobject; Destination - any; Service - any; Translated source - 200.200.200.5; Destination - original; Service - original.

Answer: C
Explanation:

QUESTION NO: 118

Because of pre-existing design constraints, you set up manual NAT rules for your HTTP server. However, your FTP server and SMTP server are both using automatic NAT rules. All traffic from your FTP and SMTP servers are passing through the Security Gateway without a problem, but traffic from the Web server is dropped on rule 0 because of anti-spoofing settings. What is causing this?

A. Allow bi-directional NAT is not checked in Global Properties.
B. Translate destination on client side is not checked in Global Properties under Manual NAT Rules.
C. Manual NAT rules are not configured correctly.
D. Routing is not configured correctly.

Answer: B
Explanation:

QUESTION NO: 119

You enable Hide NAT on the network object, 10.1.1.0 behind the Security Gateway's external interface. You browse to from host, 10.1.1.10 successfully. You enable a log on the rule that allows 10.1.1.0 to exit the network. How many log entries do you see for that connection in SmartView Tracker?

A. Two, one for outbound, one for inbound
B. Only one, inbound
C. Only one, outbound
D. Two, both outbound, one for the real IP connection and one for the NAT IP connection

Answer: C
Explanation:

QUESTION NO: 120

Which of the following statements BEST describes Check Point's Hide Network Address Translation method?

A. Translates many source IP addresses into one source IP address
B. Many-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Source and Destination IP address translation
C. Translates many destination IP addresses into one destination IP address
D. One-to-one NAT which implements PAT (Port Address Translation) for accomplishing both

Source and Destination IP address translation

Answer: A
Explanation:

QUESTION NO: 121

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
Explanation:

QUESTION NO: 122

NAT can NOT be configured on which of the following objects?

A. Host
B. HTTP Logical Server
C. Address Range
D. Gateway

Answer: B
Explanation:

QUESTION NO: 123

Which Check Point address translation method is necessary if you want to connect from a host on the Internet via HTTP to a server with a reserved (RFC 1918) IP address on your DMZ?

A. Hide Address Translation
B. Static Destination Address Translation
C. Port Address Translation

D. Dynamic Source Address Translation

Answer: B
Explanation:

QUESTION NO: 124

You want to implement Static Destination NAT in order to provide external, Internet users access to an internal Web Server that has a reserved (RFC 1918) IP address. You have an unused valid IP address on the network between your Security Gateway and ISP router. You control the router that sits between the firewall external interface and the Internet.

What is an alternative configuration if proxy ARP cannot be used on your Security Gateway?

A. Publish a proxy ARP entry on the ISP router instead of the firewall for the valid IP address.
B. Publish a proxy ARP entry on the internal Web server instead of the firewall for the valid IP address.
C. Place a static host route on the firewall for the valid IP address to the internal Web server.
D. Place a static ARP entry on the ISP router for the valid IP address to the firewall's external address.

Answer: D
Explanation:

QUESTION NO: 125

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 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.
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 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.

Answer: D Explanation:

QUESTION NO: 126

Which NAT option applicable for Automatic NAT applies to Manual NAT as well?

A. Translate destination on client-side
B. Enable IP Pool NAT
C. Allow bi-directional NAT
D. Automatic ARP configuration

Answer: A
Explanation:

QUESTION NO: 127

Your main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. You also have a small network 10.10.20.0/24 behind the internal router. You want 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 the Internet?

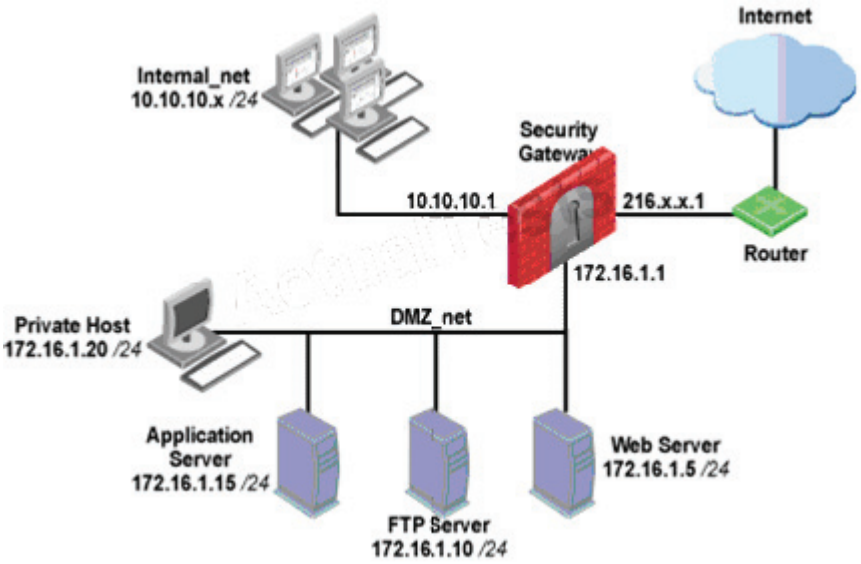
A. Configure Automatic Static NAT on network 10.10.20.0/24.
B. Configure Automatic Hide NAT on network 10.10.20.0/24 and then edit the Service column in the NAT Rule Base on the automatic rule.
C. Configure one Manual Hide NAT rule for HTTP, FTP, and SMTP services for network 10.10.20.0/24.
D. Configure three Manual Static NAT rules for network 10.10.20.0/24, one for each service.

Answer: C
Explanation:

QUESTION NO: 128

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.

Answer: D Explanation:



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
Explanation:

QUESTION NO: 129

An internal host initiates a session to and is set for Hide NAT behind the Security Gateway. The initiating traffic is an example of _____.

A. None of these
B. source NAT
C. destination NAT
D. client side NAT

Answer: B Explanation:

QUESTION NO: 130

A host on the Internet initiates traffic to the Static NAT IP of your Web server behind the Security Gateway. With the default settings in place for NAT, the initiating packet will translate the _____.

A. source on client side
B. source on server side
C. destination on client side
D. destination on server side

Answer: C
Explanation:

QUESTION NO: 131

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

Answer: D
Explanation:

QUESTION NO: 132

When translation occurs using automatic Hide NAT, what also happens?

A. The destination port is modified.
B. Nothing happens.

Answer: B Explanation:C.
The destination is modified.
D. The source port is modified.

Answer: D
Explanation:

QUESTION NO: 133

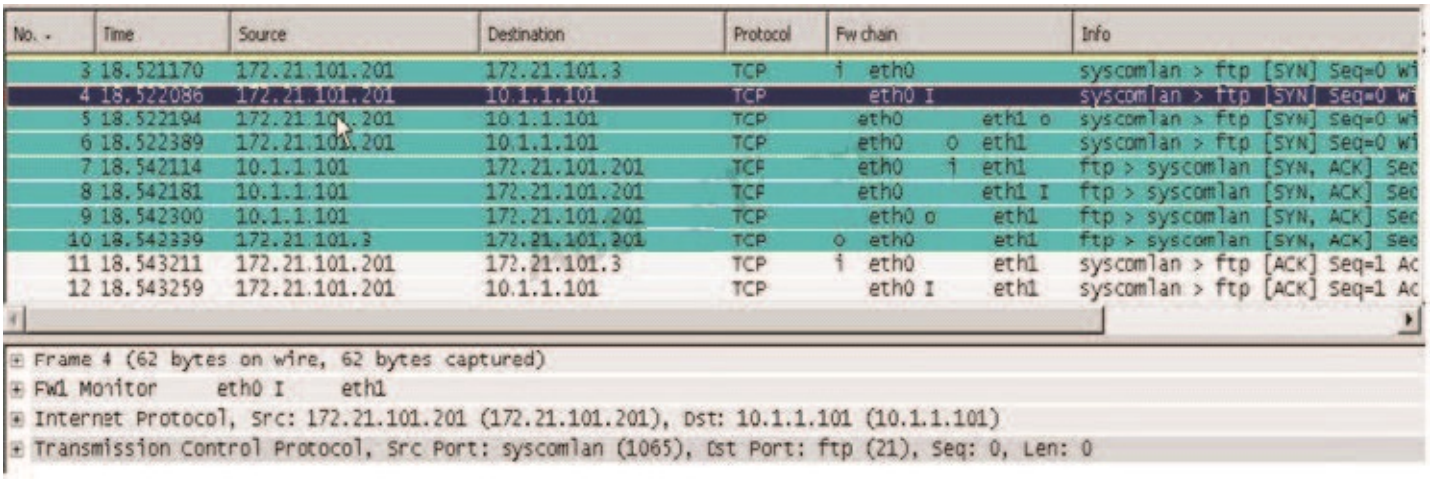
The fw monitor utility is used to troubleshoot which of the following problems?

A. Address translation
B. Log Consolidation Engine
C. User data base corruption
D. Phase two key negotiation

Answer: A
Explanation:

QUESTION NO: 134

Looking at the SYN packets in the Wireshark output,



select the statement that is true about NAT.

A. This is an example of Hide NAT.
B. This is an example of Static NAT and Translate destination on client side unchecked in Global Properties.

C. There is not enough information provided in the Wireshark capture to determine the NAT settings.

D. This is an example of Static NAT and Translate destination on client side checked in Global Properties.

Answer: D
Explanation:

QUESTION NO: 135

In SmartDashboard, Translate destination on client side is checked in Global Properties. When Network Address Translation is used:

A. VLAN tagging cannot be defined for any hosts protected by the Gateway.
B. The Security Gateway's ARP file must be modified.
C. It is not necessary to add a static route to the Gateway's routing table.
D. It is necessary to add a static route to the Gateway's routing table.

Answer: C
Explanation:

QUESTION NO: 136

Secure Internal Communications (SIC) is completely NAT-tolerant because it is based on:

A. SIC names.
B. MAC addresses.
C. IP addresses.
D. SIC is not NAT-tolerant.

Answer: A
Explanation:

QUESTION NO: 137

Static NAT connections, by default, translate on which firewall kernel inspection point?

A. Post-inbound
B. Eitherbound
C. Inbound

D. Outbound

Answer: C
Explanation:

QUESTION NO: 138

You are MegaCorp's Security Administrator. There are various network objects which must be NATed. Some of them use the Automatic Hide NAT method, while others use the Automatic Static NAT method. What is the rule order if both methods are used together? Give the best answer.

A. The Administrator decides the rule order by shifting the corresponding rules up and down.
B. The Hide NAT rules have priority over the Static NAT rules and the NAT on a node has priority over the NAT on a network or an address range.
C. The Static NAT rules have priority over the Hide NAT rules and the NAT on a node has priority over the NAT on a network or an address range.
D. The rule position depends on the time of their creation. The rules created first are placed at the top; rules created later are placed successively below the others.

Answer: C
Explanation:

QUESTION NO: 139

Which answers are TRUE? Automatic Static NAT CANNOT be used when:

1) NAT decision is based on the destination port.

2) Both Source and Destination IP's have to be translated.

3) The NAT rule should only be installed on a dedicated Gateway.

4) NAT should be performed on the server side.

A. 2 and 3
B. 1, 3, and 4
C. 1 and 2
D. 2 and 4

Answer: C
Explanation:

QUESTION NO: 140

In order to have full control, you decide to use Manual NAT entries instead of Automatic NAT rules. Which of the following is NOT true?

A. When using Static NAT, you must enter ARP entries for the Gateway on all hosts that are using the NAT Gateway with that Gateway's internal interface IP address.
B. When using Static NAT, you must add proxy ARP entries to the Gateway for all hiding addresses.
C. If you chose Automatic NAT instead, all necessary entries are done for you.
D. When using Dynamic Hide NAT with an address that is not configured on a Gateway interface, you need to add a proxy ARP entry for that address.

Answer: A
Explanation:

QUESTION NO: 141

After filtering a fw monitor trace by port and IP, a packet is displayed three times; in the i, I, and o inspection points, but not in the O inspection point. Which is the likely source of the issue?

A. A SmartDefense module has blocked the packet.
B. It is due to NAT.
C. An IPSO ACL has blocked the packet's outbound passage.
D. The packet has been sent out through a VPN tunnel unencrypted.

Answer: B
Explanation:

QUESTION NO: 142

Your internal network is configured to be 10.1.1.0/24. This network is behind your perimeter R76 Gateway, which connects to your ISP provider. How do you configure the Gateway to allow this network to go out to the Internet?

A. Do nothing, as long as 10.1.1.0 network has the correct default Gateway.
B. Use Hide NAT for network 10.1.1.0/24 behind the internal interface of your perimeter Gateway.
C. Use automatic Static NAT 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.

Answer: D
Explanation:

QUESTION NO: 143

You are a Security Administrator who has installed Security Gateway R76 on your network. You need to allow a specific IP address range for a partner site to access your intranet Web server. To limit the partner's access for HTTP and FTP only, you did the following:

1) Created manual Static NAT rules for the Web server.

2) Cleared the following settings in the Global Properties > Network Address Translation screen:

- Allow bi-directional NAT

- Translate destination on client side

Do the above settings limit the partner's access?

A. No. The first setting is not applicable. The second setting will reduce performance.
B. Yes. This will ensure that traffic only matches the specific rule configured for this traffic, and that the Gateway translates the traffic after accepting the packet.
C. Yes. Both of these settings are only applicable to automatic NAT rules.
D. No. The first setting is only applicable to automatic NAT rules. The second setting will force translation by the kernel on the interface nearest to the client.

Answer: D
Explanation:

QUESTION NO: 144

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
Explanation:

QUESTION NO: 145

You have configured Automatic Static NAT on an internal host-node object. You clear the box Translate destination on client site from Global Properties > NAT. Assuming all other NAT settings in Global Properties are selected, what else must be configured so that a host on the Internet can initiate an inbound connection to this host?

A. A proxy ARP entry, to ensure packets destined for the public IP address will reach the Security Gateway's external interface.
B. No extra configuration is needed.
C. The NAT IP address must be added to the external Gateway interface anti-spoofing group.
D. A static route, to ensure packets destined for the public NAT IP address will reach the Gateway's internal interface.

Answer: D
Explanation:

QUESTION NO: 146

Source:	Any
Destination:	web_public_IP
Service:	Any
Translated Source:	original
Translated Destination:	web_private_IP
Service:	original

You just installed a new Web server in the DMZ that must be reachable from the Internet. You create a manual Static NAT rule as follows:

"web_public_IP" is the node object that represents the new Web server's public IP address. "web_private_IP" is the node object that represents the new Web site's private IP address. You enable all settings from Global Properties > NAT.

When you try to browse the Web server from the Internet you see the error "page cannot be displayed". Which of the following is NOT a possible reason?

A. There is no route defined on the Security Gateway for the public IP address to the Web server's private IP address.
B. There is no ARP table entry for the protected Web server's public IP address.
C. There is no Security Policy defined that allows HTTP traffic to the protected Web server.
D. There is no NAT rule translating the source IP address of packets coming from the protected Web server.

Answer: D
Explanation:

QUESTION NO: 147

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
Explanation:

QUESTION NO: 148

You have created a Rule Base for firewall, websydney. Now you are going to create a new policy package with security and address translation rules for a second Gateway.

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

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1	NetBIOS Rule	Any	Any	Any Traffic	NBT	drop	None	Policy Targets
2	Mgmt Rule	websignapore	fwsingapore	Any Traffic	ssh https	accept	None	Policy Targets
3	Web Server Rule	Any	websignapore	Any Traffic	http	Client Auth	Log	Policy Targets
4	Stealth Rule	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
5	Partner City Rule	net_singapore net_rome	net_singapore net_rome	Rome_Singapore	http	accept	Log	Policy Targets
6	Network Traffic Rule	net_singapore net_sydney	Any	Any Traffic	dns icmp-proto ftp https http	accept	Log	Policy Targets
7	Network Traffic Rule	websydney	Any	Any Traffic	ftp	reject	Log	Policy Targets
8	Cleanup Rule	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

What is TRUE about the new package's NAT rules?

A. NAT rules will be empty in the new package.
B. Rules 4 and 5 will appear in the new package.
C. Rules 1, 2, 3 will appear in the new package.
D. Only rule 1 will appear in the new package.

Answer: C
Explanation:

QUESTION NO: 149

What is the default setting when you use NAT?

A. Source Translated on Client side
B. Source Translated on both sides
C. Destination Translated on Client side
D. Destination Translated on Server side

Answer: C
Explanation:

QUESTION NO: 150

A marketing firm's networking team is trying to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks you to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should you use to check these objects and rules?

A. SmartView Tracker
B. SmartView Monitor
C. SmartDashboard
D. SmartView Status

Answer: C
Explanation:

QUESTION NO: 151

Which statement below describes the most correct strategy for implementing a Rule Base?

A. Place a network-traffic rule above the administrator access rule.
B. Limit grouping to rules regarding specific access.
C. Place the most frequently used rules at the top of the Policy and the ones that are not frequently used further down.
D. Add the Stealth Rule before the last rule.

Answer: C
Explanation:

QUESTION NO: 152

Which of the following is a viable consideration when determining Rule Base order?

A. Grouping authentication rules with address-translation rules
B. Grouping rules by date of creation
C. Grouping reject and drop rules after the Cleanup Rule

D. Grouping functionally related rules together

Answer: D
Explanation:

QUESTION NO: 153

Which of the following is a viable consideration when determining Rule Base order?

A. Adding SAM rules at the top of the Rule Base
B. Placing frequently accessed rules before less frequently accessed rules
C. Grouping rules by date of creation
D. Grouping IPS rules with dynamic drop rules

Answer: B
Explanation:

QUESTION NO: 154

Which of the following is a viable consideration when determining Rule Base order?

A. Grouping IPS rules with dynamic drop rules
B. Grouping reject and drop rules after the Cleanup Rule
C. Placing more restrictive rules before more permissive rules
D. Grouping authentication rules with QOS rules

Answer: C
Explanation:

QUESTION NO: 155

You would use the Hide Rule feature to:

A. View only a few rules without the distraction of others.
B. Hide rules from read-only administrators.
C. Hide rules from a SYN/ACK attack.
D. Make rules invisible to incoming packets.

in the Install On check box. What should you look for?

Answer: A

Explanation:

QUESTION NO: 156

You are a Security Administrator using one Security Management Server managing three different firewalls. One firewall does NOT show up in the dialog box when attempting to install a Security Policy. Which of the following is a possible cause?

A. The firewall has failed to sync with the Security Management Server for 60 minutes.
B. The firewall object has been created but SIC has not yet been established.
C. The firewall is not listed in the Policy Installation Targets screen for this policy package.
D. The license for this specific firewall has expired.

Answer: C

Explanation:

QUESTION NO: 157

Your shipping company uses a custom application to update the shipping distribution database. The custom application includes a service used only to notify remote sites that the distribution database is malfunctioning. The perimeter Security Gateway's Rule Base includes a rule to accept this traffic. Since you are responsible for multiple sites, you want notification by a text message to your cellular phone, whenever traffic is accepted on this rule. Which of the following would work BEST for your purpose?

A. SmartView Monitor Threshold
B. SNMP trap
C. Logging implied rules
D. User-defined alert script

Answer: D

Explanation:

QUESTION NO: 158

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear

in the Install On check box. What should you look for?

A. Secure Internal Communications (SIC) not configured for the object.
B. A Gateway object created using the Check Point > Security Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.
C. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
D. Anti-spoofing not configured on the interfaces on the Gateway object.

Answer: C
Explanation:

QUESTION NO: 159

A Security Policy installed by another Security Administrator has blocked all SmartDashboard connections to the stand-alone installation of R76. After running the command fw unloadlocal, you are able to reconnect with SmartDashboard and view all changes. Which of the following change is the most likely cause of the block?

A. A Stealth Rule has been configured for the R76 Gateway.
B. The Gateway Object representing your Gateway was configured as an Externally Managed VPN Gateway.
C. The Security Policy installed to the Gateway had no rules in it.
D. The Allow Control Connections setting in Policy > Global Properties has been unchecked.

Answer: D
Explanation:

QUESTION NO: 160

When configuring anti-spoofing on the Security Gateway object interfaces, which of the following is NOT a valid R76 topology configuration?

A. Specific
B. External
C. Not Defined
D. Any

Answer: D
Explanation:

in the Install On check box. What should you look for?

QUESTION NO: 161

You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

A. The POP3 rule is disabled.
B. The POP3 rule is hidden.
C. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R75.
D. POP3 is accepted in Global Properties.

Answer: B
Explanation:

QUESTION NO: 162

Which rule is responsible for the installation failure?

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

Answer: C
Explanation:

QUESTION NO: 163

Which command allows Security Policy name and install date verification on a Security Gateway?

A. fw ver -p
B. fw stat -l
C. fw show policy
D. fw ctl pstat -policy

Answer: B

Explanation:

QUESTION NO: 164

You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After awhile, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

A. Restore the entire database, except the user database, and then create the new user and user group.
B. Run fwm_dbexport to export the user database. Select restore the entire database in the Database Revision screen. Then, run fwm_dbimport.
C. Run fwm dbexport -l filename. Restore the database. Then, run fwm dbimport -l filename to import the users.
D. Restore the entire database, except the user database.

Answer: D
Explanation:

QUESTION NO: 165

Which feature or command provides the easiest path for Security Administrators to revert to earlier versions of the same Security Policy and objects configuration?

A. upgrade_export/upgrade_import
B. dbexport/dbimport
C. Database Revision Control
D. Policy Package management

Answer: C
Explanation:

QUESTION NO: 166

Your Security Management Server fails and does not reboot. One of your remote Security Gateways managed by the Security Management Server reboots. What occurs with the remote

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

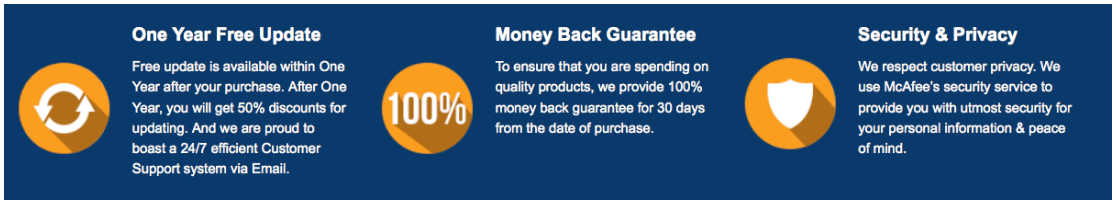
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions