Vendor: Check Point

Exam Code: 156-215.77

Exam Name: Check Point Certified Security Administrator

Version: Demo

QUESTION 1
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. SmartView Tracker and SmartView Monitor
B. SmartLSM and SmartUpdate
C. SmartDashboard and SmartView Tracker
D. SmartView Monitor and SmartUpdate

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 2
Your bank's distributed R77 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

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 3
When launching SmartDashboard, what information is required to log into R77?

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 4
Message digests use which of the following?

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 5
Which of the following is a hash algorithm?

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 6
Which of the following uses the same key to decrypt as it does to encrypt?

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 7
You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners. Which SmartConsole application should you use to confirm your suspicions?

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 8
A digital signature:

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 9
Which component functions as the Internal Certificate Authority for R77?

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 10
The customer has a small Check Point installation, which includes one GAiA 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. Hybrid Installation
C. Unsupported configuration
D. Stand-Alone Installation

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 11
The customer has a small Check Point installation which includes one Windows 2008 server as the SmartConsole and a second server running GAiA as both Security Management Server and the Security Gateway. This is an example of a(n):

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 12
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. Hybrid Installation
B. Unsupported configuration
C. Stand-Alone Installation
D. Distributed Installation

Correct Answer: D

Explanation

Explanation/Reference:

QUESTION 13
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 GAiA as Security Gateway. This is an example of a(n):

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 14
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 15
Tom has been tasked to install Check Point R77 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. Two machines
D. One machine, but it needs to be installed using SecurePlatform for compatibility purposes

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 16
Which command allows Security Policy name and install date verification on a Security Gateway?

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 17
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. Run fwm dbexport -l filename. Restore the database. Then, run fwm dbimport -l filename to import the users.
B. Run fwm_dbexport to export the user database. Select restore the entire database in the Database Revision screen. Then, run fwm_dbimport.
C. Restore the entire database, except the user database, and then create the new user and user group.
D. Restore the entire database, except the user database.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 18
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. Database Revision Control
B. Policy Package management
C. dbexport/dbimport
D. upgrade_export/upgrade_import

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 19
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 Gateway after reboot?

A. Since the Security Management Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, all traffic is allowed through the Gateway.
B. Since the Security Management Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, no traffic is allowed through the Gateway.
C. The remote Gateway fetches the last installed Security Policy locally and passes traffic normally. The Gateway will log locally, since the Security Management Server is not available.
D. Since the Security Management Server is not available, the remote Gateway uses the local Security Policy, but does not log traffic.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 20
How can you configure an application to automatically launch on the Security Management Server when traffic is dropped or accepted by a rule in the Security Policy?

A. SNMP trap alert script
B. Custom scripts cannot be executed through alert scripts.
C. User-defined alert script
D. Pop-up alert script

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is NOT useful to verify whether or not a Security Policy is active on a Gateway?

A. fw ctl get string active_secpol
B. fw stat
C. cpstat fw -f policy
D. Check the Security Policy name of the appropriate Gateway in SmartView Monitor.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 22
Exhibit:

1. Simplified mode Rule Bases
2. Traditional mode Rule Bases
3. SecurePlatform WebUI Users
4. SIC certificates
5. SmartView Tracker audit logs
6. SmartView Tracker traffic logs
7. Implied Rules
8. IPS Profiles
9. Blocked connections
10. Manual NAT rules
11. VPN communities
12. Gateway route table
13. Gateway licenses

Of the following, what parameters will not be preserved when using Database Revision Control?

A. 2, 4, 7, 10, 11
B. 3, 4, 5, 6, 9, 12, 13
C. 5, 6, 9, 12, 13
D. 1, 2, 8, 10, 11

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 23
You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

A. Manual copies of the directory $FWDIR/conf
B. upgrade_export command
C. Database Revision Control
D. GAiA backup utilities

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 24
Exhibit:

1. `upgrade_export` and `upgrade_import` utilities
2. Database revision control
3. SecurePlatform backup utilities
4. Policy package management
5. Manual copies of the `$CPDIR/conf` directory

You plan to create a backup of the rules, objects, policies, and global properties from an R77 Security Management Server. Which of the following backup and restore solutions can you use?

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

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 25
Which R77 feature or command allows Security Administrators to revert to earlier Security Policy versions without changing object configurations?

A. upgrade_export/upgrade_import
B. fwm dbexport/fwm dbimport

C. Database Revision Control
D. Policy Package management

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 26
What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security Gateway?

A. In Global Properties > Reporting Tools check the box Enable tracking all rules (including rules marked as None in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
B. Install the View Implicit Rules package using SmartUpdate.
C. Define two log servers on the R77 Gateway object. Enable Log Implied Rules on the first log server. Enable Log Rule Base on the second log server. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits.
D. Check the Log Implied Rules Globally box on the R77 Gateway object.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 27
Which utility allows you to configure the DHCP service on GAiA from the command line?

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 28
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. Type fwm unlock_admin from the Security Management Server command line.
B. Type fwm unlock_admin -u from the Security Gateway command line.
C. Type fwm lock_admin -u <account name> from the Security Management Server command line.
D. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 29
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. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.
B. Reinstall the Security Management Server and restore using upgrade_import.
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.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 30
You are the Security Administrator for ABC-Corp. A Check Point Firewall is installed and in use on GAiA. 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 GAiA. Where can you view them? Give the BEST answer.

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 31
When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

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

As expert user, issue these commands:

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

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

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 32
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. 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.
C. In the menu of SmartDashboard, go to Policy > Policy Installation Targets and select the correct firewall via Specific Targets.
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 on Target.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 33
You have a diskless appliance platform. How do you keep swap file wear to a minimum?

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 34
Your R77 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. On a GAiA Security Management Server, this can only be accomplished by configuring the command fw logswitch via the cron utility.
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. 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.
D. 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.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 35
Which of the following methods will provide the most complete backup of an R77 configuration?

A. Policy Package Management
B. Copying the directories $FWDIR\conf and $CPDIR\conf to another server

C. Execute command upgrade_export
D. Database Revision Control

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 36
Which of the following commands can provide the most complete restoration of a R77 configuration?

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 37
When restoring R77 using the command upgrade_import, which of the following items are NOT restored?

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

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 38
Your organization's disaster recovery plan needs an update to the backup and restore section to reap the new distributed R77 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 R77 components that enforce the Security Policies should be backed up at least once a week.
- Desired ObjectivE. Back up R77 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. Does not meet the required objective.
D. Meets the required objective and both desired objectives.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 39
Your company is running Security Management Server R77 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 SmartDashboard, under Users, select Add New Administrator
B. Using SmartDashboard or cpconfig
C. Using the Web console on GAiA under Product configuration, select Administrators
D. Using cpconfig on the Security Management Server, choose Administrators

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 40
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. You can unlock Peter's account by using the command fwm lock_admin -u Peter on the Security Management Server.
B. You can unlock Peter's account by using the command fwm unlock_admin -u Peter on the Security Management Server
C. It is not possible to unlock Peter's account. You have to install the firewall once again or abstain from Peter's help.
D. You can unlock Peter's account by using the command fwm unlock_admin -u Peter on the Security Gateway.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 41
Where can you find the Check Point's SNMP MIB file?

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 42
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. No action is needed because cpshell has a timeout of one hour by default.
B. Log in as the default user expert and start cpinfo.
C. Log in as admin, switch to expert mode, set the timeout to one hour with the command, idle 60, then start cpinfo.
D. Log in as Administrator, set the timeout to one hour with the command idle 60 and start cpinfo.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 43
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. 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.
D. Right-click on the object representing the specific administrator, and select that Firewall in Policy Targets.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 44
What is the officially accepted diagnostic tool for IP Appliance Support?

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

Correct Answer: D
Explanation

Explanation/Reference:

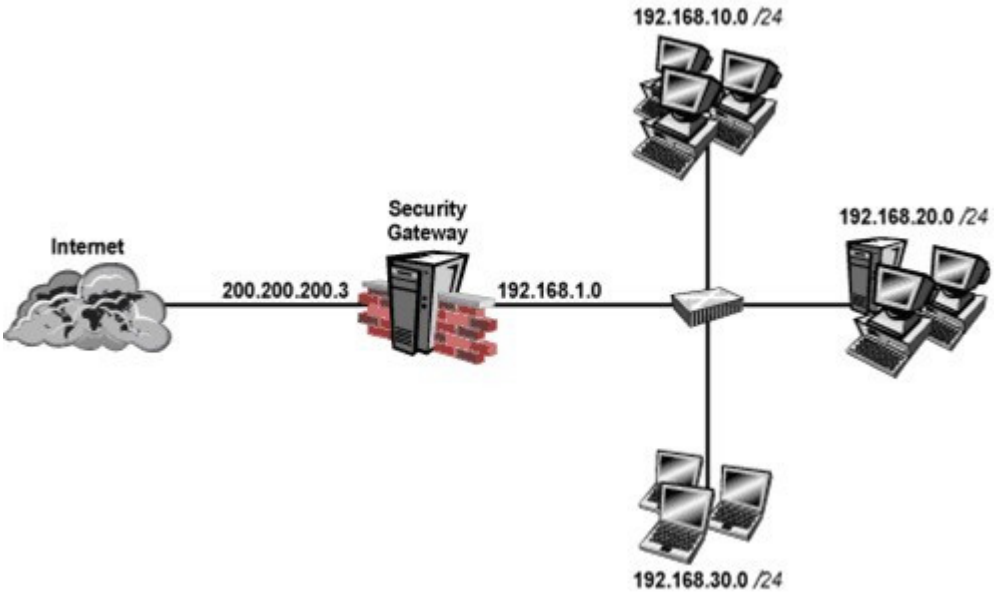
QUESTION 45
Which of these Security Policy changes optimize Security Gateway performance?

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 46
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 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.
B. 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.
C. 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.
D. Create two network objects: 192.168.10.0/24 and 192.168.20.0/24. Add the two network objects to a group object. Create a manual NAT rule like the following: Original source - group object; Destination - any; Service - any; Translated source - 200.200.200.5; Destination - original; Service - original.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 47
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. Manual NAT rules are not configured correctly.
B. Allow bi-directional NAT is not checked in Global Properties.

C. Routing is not configured correctly.
D. Translate destination on client side is not checked in Global Properties under Manual NAT Rules.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 48
You enable Hide NAT on the network object, 10.1.1.0 behind the Security Gateway's external interface. You browse to the Google Website 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, outbound
C. Two, both outbound, one for the real IP connection and one for the NAT IP connection
D. Only one, inbound

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 49
Which of the following statements BEST describes Check Point's Hide Network Address Translation method?

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

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 50
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. Hide
B. Static Destination
C. Static Source
D. Dynamic Destination

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 51
NAT can NOT be configured on which of the following objects?

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 52
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. Dynamic Source Address Translation
B. Hide Address Translation
C. Port Address Translation
D. Static Destination Address Translation

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 53
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. Place a static ARP entry on the ISP router for the valid IP address to the firewall's external address.
C. Publish a proxy ARP entry on the internal Web server instead of the firewall for the valid IP address.
D. Place a static host route on the firewall for the valid IP address to the internal Web server.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 54
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 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.
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 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.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 55
Which NAT option applicable for Automatic NAT applies to Manual NAT as well?

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

Correct Answer: C
Explanation

Explanation/Reference:

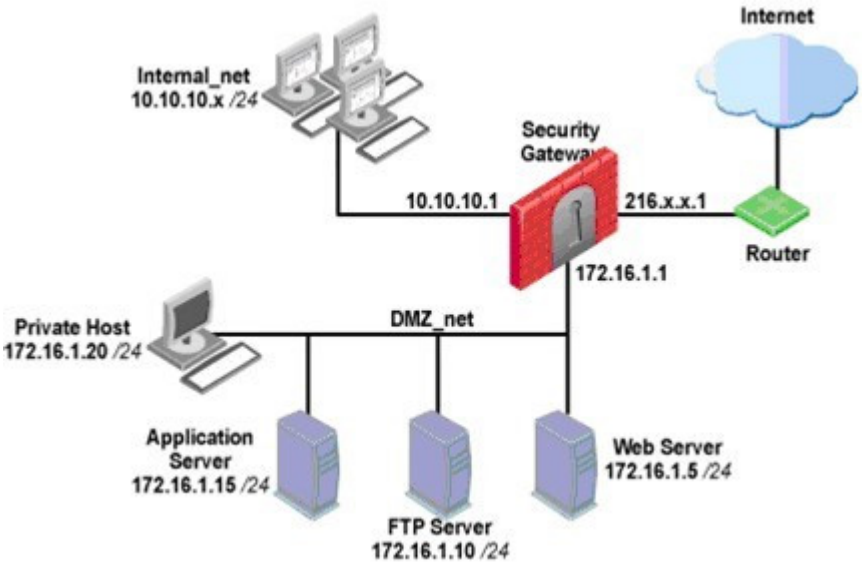
QUESTION 56
Your main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. You also have a small network 10.10.20.0/24 behind the internal router. You want to configure the kernel to translate the source address only when network 10.10.20.0 tries to access the Internet for HTTP, SMTP, and FTP services. Which of the following configurations will allow this network to access the Internet?

A. Configure three Manual Static NAT rules for network 10.10.20.0/24, one for each service.
B. Configure Automatic Static NAT on network 10.10.20.0/24.
C. Configure one Manual Hide NAT rule for HTTP, FTP, and SMTP services for network 10.10.20.0/24.
D. 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.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 57
You have three servers located in a DMZ, using private IP addresses. You want internal users from 10.10.10.x to access the DMZ servers by public IP addresses. Internal_net 10.10.10.x is configured for Hide NAT behind the Security Gateway's external interface.



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

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 58
An internal host initiates a session to the Google.com website and is set for Hide NAT behind the Security Gateway. The initiating traffic is an example of _____.

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 59
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. destination on server side
B. source on server side
C. source on client side
D. destination on client side

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 60
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. Automatic ARP must be unchecked in the Global Properties.
B. Nothing else must be configured.
C. A static route must be added on the Security Gateway to the internal host.
D. A static route for the NAT IP must be added to the Gateway's upstream router.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 61
When translation occurs using automatic Hide NAT, what also happens?

A. Nothing happens.
B. The destination is modified.
C. The destination port is modified.
D. The source port is modified.

Correct Answer: D
Explanation

Explanation/Reference:

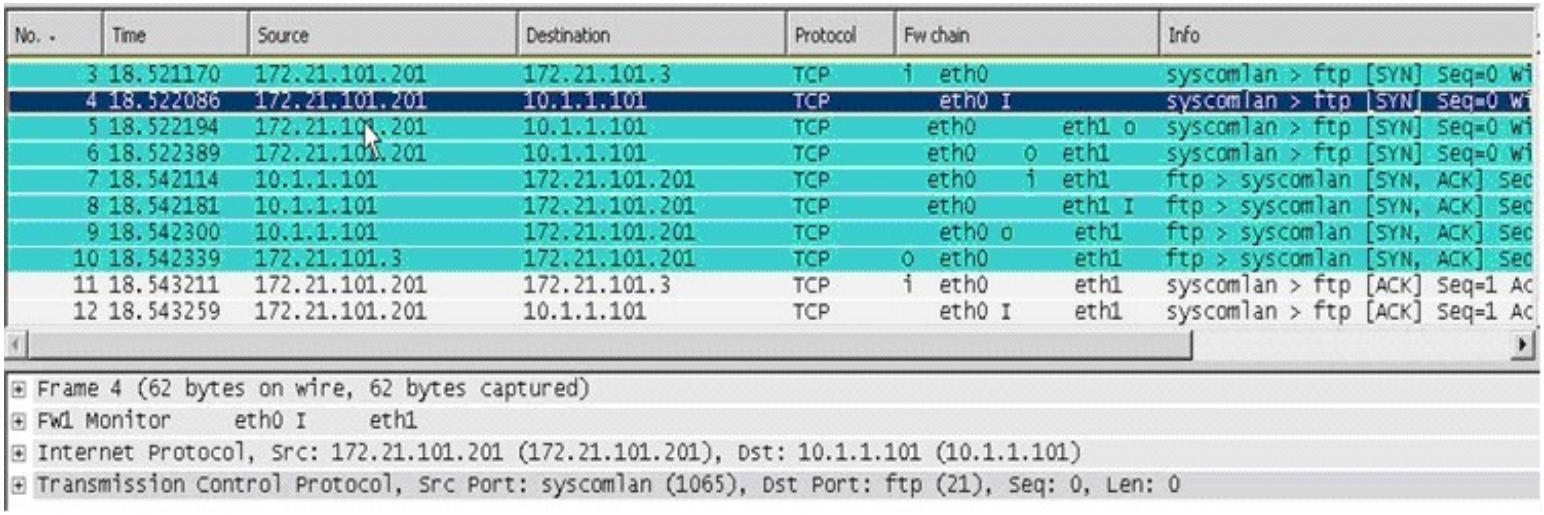
QUESTION 62
The fw monitor utility is used to troubleshoot which of the following problems?

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 63
Looking at the SYN packets in the Wireshark output, select the statement that is true about NAT.
Exhibit:



A. This is an example of Hide NAT.
B. There is not enough information provided in the Wireshark capture to determine the NAT settings.
C. This is an example of Static NAT and Translate destination on client side unchecked in Global Properties.
D. This is an example of Static NAT and Translate destination on client side checked in Global Properties.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 64
In SmartDashboard, Translate destination on client side is checked in Global Properties. When Network Address Translation is used:

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 65
Secure Internal Communications (SIC) is completely NAT-tolerant because it is based on:

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

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 66

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

A. Inbound
B. Outbound
C. Post-inbound
D. Eitherbound

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 67
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 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.
C. 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.
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.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 68
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. 1 and 2
B. 2 and 4
C. 1, 3, and 4
D. 2 and 3

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 69
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. The packet has been sent out through a VPN tunnel unencrypted.
B. An IPSO ACL has blocked the packet's outbound passage.
C. A SmartDefense module has blocked the packet.
D. It is due to NAT.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 70
Your internal network is configured to be 10.1.1.0/24. This network is behind your perimeter R77 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 Hide NAT for network 10.1.1.0/24 behind the external IP address of your perimeter 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. Do nothing, as long as 10.1.1.0 network has the correct default Gateway.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 71
You are a Security Administrator who has installed Security Gateway R77 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. 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.
B. No. The first setting is not applicable. The second setting will reduce performance.
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.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 72
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 R77 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, before the virtual machine
B. I=inbound kernel, after the virtual machine
C. O=outbound kernel, after the virtual machine
D. i=inbound kernel, before the virtual machine

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 73
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. No extra configuration is needed.
B. A proxy ARP entry, to ensure packets destined for the public IP address will reach the Security Gateway's external interface.
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.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 74
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:
SourcE. Any || Destination: web_public_IP || ServicE. Any || Translated SourcE. original || Translated Destination: web_private_IP || ServicE. Original ? is the node object that represents the new Web server's public IP address.
"web_public_IP
? is the node object that represents the new Web site's private IP address. You "web_private_IP
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 ?. Which of the following is NOT a possible reason? displayed

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 75
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. 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.
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. Yes, it is possible to have two NAT rules which match a connection, but only when using Automatic NAT (bidirectional NAT).

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 76
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. What is TRUE about the new package's NAT rules?
Exhibit:

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	websydney	Any	Any	websydney (Hid	Original	Original	fwsydney
2	net_singapore	net_singapore	Any	Original	Original	Original	All
3	net_singapore	Any	Any	net_singapore (H	Original	Original	All
4	Any	websydney	Any	Original	websydney	Original	Policy Targets
5	Any	websignapore	HTTP_and_HTTPS	Original	Original	http	Policy Targets

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 77
What is the default setting when you use NAT?

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

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 78
Select the TRUE statements about the Rule Base shown? Exhibit:

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

1) HTTP traffic from webrome to websingapore will be encrypted.
2) HTTP traffic from websingapore to webrome will be encrypted.
3) HTTP traffic from webrome to websingapore will be authenticated.
4) HTTP traffic from websingapore to webrome will be blocked.

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

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 79
Which rule is responsible for the client authentication failure? Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log
4	0	User Auth	Any	webSingapore	Any Traffic	http	User Auth	Log
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	http	accept	Log
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	http dns icmp-proto ftp https	accept	Log
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 80
You receive a notification that long-lasting Telnet connections to a mainframe are dropped after an hour of inactivity. Reviewing SmartView Tracker shows the packet is dropped with the error:
Unknown established connection
How do you resolve this problem without causing other security issues? Choose the BEST answer.

A. Increase the service-based session timeout of the default Telnet service to 24-hours.
B. Ask the mainframe users to reconnect every time this error occurs.
C. Increase the TCP session timeout under Global Properties > Stateful Inspection.
D. Create a new TCP service object on port 23 called Telnet-mainframe. Define a service-based session timeout of 24-hours. Use this new object only in the rule that allows the Telnet connections to the mainframe.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 81
Which SmartConsole tool would you use to see the last policy pushed in the audit log?

A. SmartView Tracker
B. None, SmartConsole applications only communicate with the Security Management Server.
C. SmartView Status
D. SmartView Server

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 82
SmartView Tracker logs the following Security Administrator activities, EXCEPT:

A. Object creation, deletion, and editing
B. Tracking SLA compliance
C. Administrator login and logout
D. Rule Base changes

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 83
What happens when you select File > Export from the SmartView Tracker menu?

A. Current logs are exported to a new *.log file.
B. Exported log entries are not viewable in SmartView Tracker.
C. Logs in fw.log are exported to a file that can be opened by Microsoft Excel.
D. Exported log entries are deleted from fw.log.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 84
By default, when you click File > Switch Active File in SmartView Tracker, the Security Management Server:

A. Saves the current log file, names the log file by date and time, and starts a new log file.
B. Purges the current log file, and starts a new log file.
C. Prompts you to enter a filename, and then saves the log file.
D. Purges the current log file, and prompts you for the new log's mode.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 85
You are working with three other Security Administrators. Which SmartConsole component can be used to monitor changes to rules or object properties made by the other administrators?

A. Eventia Tracker
B. SmartView Monitor
C. Eventia Monitor
D. SmartView Tracker

Correct Answer: D

Explanation

Explanation/Reference:

QUESTION 86
Which SmartView Tracker mode allows you to read the SMTP e-mail body sent from the Chief Executive Officer (CEO) of a company?

A. This is not a SmartView Tracker feature.
B. Display Capture Action
C. Network and Endpoint Tab
D. Display Payload View

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 87
You can include External commands in SmartView Tracker by the menu Tools > Custom Commands. The Security Management Server is running under GAiA, and the GUI is on a system running Microsoft Windows. How do you run the command traceroute on an IP address?

A. There is no possibility to expand the three pre-defined options Ping, Whois, and Nslookup.
B. Go to the menu Tools > Custom Commands and configure the Windows command tracert.exe to the list.
C. Use the program GUIdbedit to add the command traceroute to the Security Management Server properties.
D. Go to the menu, Tools > Custom Commands and configure the Linux command traceroute to the list.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 88
Where is the easiest and BEST place to find information about connections between two machines?

A. All options are valid.
B. On a Security Gateway using the command fw log.
C. On a Security Management Server, using SmartView Tracker.
D. On a Security Gateway Console interface; it gives you detailed access to log files and state table information.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 89
Which of the following can be found in cpinfo from an enforcement point?

A. Everything NOT contained in the file r2info
B. VPN keys for all established connections to all enforcement points
C. The complete file objects_5_0.c

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

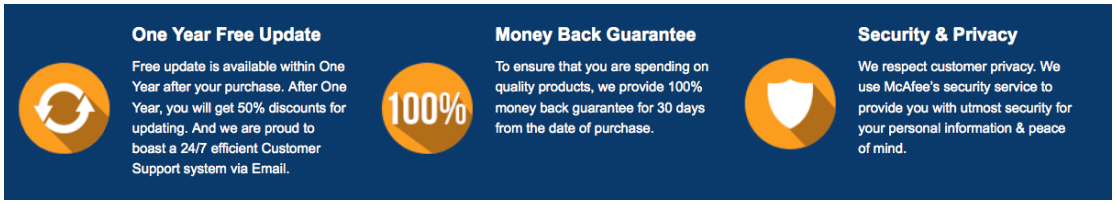
★ Average **99.9%** Success Rate

★ 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