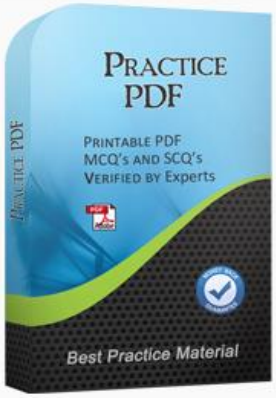
Actual4Cert

Actual4Cert

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

http://www.actual4cert.com/

We are a test cert center to provide the best and valid study material for all of you, and aim to help you pass.

Exam : **156-315.77**

Title : Check Point Certified Security Expert

Vendor : CheckPoint

Version : DEMO

NO.1 What is not available for Express Reports compared to Standard Reports?
A. Filter
B. Period
C. Content
D. Schedule
Answer: A

NO.2 Which type of VPN routing relies on a VPN Tunnel Interface (VTI) to route traffic?
A. Host-based VPN
B. Route-based VPN
C. Domain-based VPN
D. Subnet-based VPN
Answer: B

NO.3 You set up a mesh VPN Community, so your internal networks can access your partner's network, and vice versa. Your Security Policy encrypts only FTP and HTTP traffic through a VPN tunnel. All other traffic among your internal and partner networks is sent in clear text.
How do you configure the VPN Community?
A. Disable "accept all encrypted traffic", and put FTP and HTTP in the Excluded services in the Community object. Add a rule in the Security Policy for services FTP and http, with the Community object in the VPN field.
B. Disable "accept all encrypted traffic" in the Community, and add FTP and HTTP services to the Security Policy, with that Community object in the VPN field.
C. Enable "accept all encrypted traffic", but put FTP and HTTP in the Excluded services in the Community. Add a rule in the Security Policy, with services FTP and http, and the Community object in the VPN field.
D. Put FTP and HTTP in the Excluded services in the Community object. Then add a rule in the Security Policy to allow Any as the service, with the Community object in the VPN field.
Answer: B

NO.4 Which internal user authentication protocols are supported in SSL VPN?
A. Check Point Password, SecurID, LDAP, RADIUS, TACACS
B. Check Point Password, SecurID, L2TP, RADIUS, TACACS
C. Check Point Password, SecurID, Active Directory, RADIUS, TACACS
D. Point Password, SecurID, OS Password, RADIUS, TACACS
Answer: D

NO.5 Which command provides cluster upgrade status?
A. cphaprob status
B. cphaprob ldstat
C. cphaprob fcustat
D. cphaprob tablestat
Answer: C

NO.6 What is Check Point's CoreXL?
A. A way to synchronize connections across cluster members
B. TCP-18190
C. Multiple core interfaces on the device to accelerate traffic
D. Multi Core support for Firewall Inspection
Answer: D

NO.7 What process manages the dynamic routing protocols (OSPF, RIP, etc.) on GAiA?
A. routed
B. There's no separate process, but the Linux default router can take care of that.
C. routerd
D. arouted
Answer: A

NO.8 You are preparing computers for a new ClusterXL deployment.
For your cluster, you plan to use four machines with the following configurations:
Cluster Member 1: OS:Secure Platform, NICs: QuadCard, memory: 1 GB, Security Gateway only, version: R76 Cluster Member 2: OS:Secure Platform, NICs: 4 Intel 3Com, memory: 1 GB, Security Gateway only, version: R76 Cluster Member 3: OS:Secure Platform, NICs: 4 other manufacturers, memory: 512 MB, Security Gateway only, version: R76 Security Management Server: MS Windows 2003, NIC. Intel NIC (1), Security Gateway and primary Security Management Server installed, version: R76 Are these machines correctly configured for a ClusterXL deployment?
A. No, the Security Gateway cannot be installed on the Security Management Pro Server.
B. No, Cluster Member 3 does not have the required memory.
C. Yes, these machines are configured correctly for a ClusterXL deployment.
D. No, the Security Management Server is not running the same operating system as the cluster members.
Answer: C

NO.9 SmartProvisioning uses different types of profiles to manage and provision the gateways. These types are:
A. SmartLSM Security Profiles and Provisioning Profiles
B. Provisioning Profiles and Gateways Profiles
C. SmartLSM Security Profiles and SmartDashboard Profiles
D. SmartConsole Profiles and SmartFilter Profiles
Answer: A

NO.10 When you check Web Server in a host-node object, what happens to the host?
A. The Web server daemon is enabled on the host.
B. More granular controls are added to the host, in addition to Web Intelligence tab settings.
C. You can specify allowed ports in the Web server's node-object properties. You then do not need to list all allowed ports in the Rule Base.
D. IPS Web Intelligence is enabled to check on the host.

Answer: B

NO.11 Which of these four Check Point QoS technologies prevents the transmission of redundant packets when multiple copies of a packet are concurrently queued on the same flow?
A. Weighted Flow Random Early Drop (WFRED)
B. Intelligent Queuing Engine
C. Retransmission Detection Early Drop (RDED)
D. Stateful Inspection
Answer: C

NO.12 What SmartConsole application allows you to change the SmartReporter Policy?
A. SmartDashboard
B. SmartReporter
C. SmartEvent Server
D. SmartUpdate
Answer: A

NO.13 In the following command,
LSMcli [-d] <server><user><pswd><action> "server"
should be replaced with:
A. Hostname of ROBO gateway
B. Hostname DAIP device
C. IP address of the Security Management server
D. GUIclient
Answer: C

NO.14 SmartReporter reports can be used to analyze data from a penetration-testing regimen in all of the following examples, EXCEPT:
A. Analyzing traffic patterns against public resources.
B. Possible worm/malware activity.
C. Analyzing access attempts via social-engineering.
D. Tracking attempted port scans.
Answer: C

NO.15 Which Security Servers can perform Content Security tasks, but CANNOT perform authentication tasks?
A. Telnet
B. FTP
C. SMTP
D. HTTP
Answer: C

NO.16 _____ manages Standard Reports and allows the administrator to specify automatic uploads

of reports to a central FTP server.
A. SmartReporter Database
B. SmartReporter
C. SmartDashboard Log Consolidator
D. Security Management Server
Answer: B

NO.17 Which describes the function of the account unit?
A. An Account Unit is the Check Point account that SmartDirectory uses to access an (LDAP) server
B. An Account Unit is a system account on the Check Point gateway that SmartDirectory uses to access an (LDAP) server
C. An Account Unit is the administration account on the LDAP server that SmartDirectory uses to access to (LDAP) server
D. An Account Unit is the interface which allows interaction between the Security Management server and Security Gateways, and the SmartDirectory (LDAP) server.
Answer: D

NO.18 VPN access control would fall under which VPN component?
A. QoS
B. Performance
C. Management
D. Security
Answer: D

NO.19 Which of the following is a TRUE statement concerning contract verification?
A. Your contract file is stored on the User Center and fetched by the Gateway as needed.
B. Your contract file is stored on the SmartConsole and downloaded to the SmartCenter Server.
C. Your contract file is stored on the SmartConsole and downloaded to the Gateway.
D. Your contract file is stored on the SmartCenter Server and downloaded to the Security Gateway.
Answer: D

NO.20 Your current VPN-1 NG with Application Intelligence (AI) R55 stand-alone VPN-1 Pro Gateway and SmartCenter Server runs on SecurePlatform.
You plan to implement VPN-1 NGX R65 in a distributed environment, where the new machine will be the SmartCenter Server, and the existing machine will be the VPN-1 Pro Gateway only.
You need to migrate the NG with AI R55 SmartCenter Server configuration, including licensing.
How do you handle licensing for this NGX R65 upgrade?
A. Request an NGX R65 SmartCenter Server license, using the new server's IP address.
Request a new central NGX R65 VPN-1 Gateway license also licensed to the new SmartCenter Server's IP address.
B. Leave the current license on the gateway to be upgraded during the software upgrade.
Purchase a new license for the VPN-1 NGX R65 SmartCenter Server.
C. Request an NGX R65 SmartCenter Server license, using the existing gateway machine's IP address.
Request a new local license for the NGX R65 VPN-1 Gateway using the new server's IP address.

D. Request an NGX R65 SmartCenter Server license, using the new server's IP address.
Request a new central NGX R65 VPN-1 Gateway license for the existing gateway server's IP address.
Answer: A

NO.21 You have an internal FTP server, and you allow downloading, but not uploading.
Assume Network Address Translation is set up correctly, and you want to add an inbound rule with:
Source: Any
Destination: FTP server
Service: FTP resources object.
How do you configure the FTP resource object and the action column in the rule to achieve this goal?
A. Enable only the "Get" method in the FTP Resource Properties, and use this method in the rule, with action accept.
B. Enable only the "Get" method in the FTP Resource Properties and use it in the rule, with action drop.
C. Enable both "Put" and "Get" methods in the FTP Resource Properties and use them in the rule, with action drop.
D. Disable "Get" and "Put" methods in the FTP Resource Properties and use it in the rule, with action accept.
E. Enable only the "Put" method in the FTP Resource Properties and use it in the rule, with action accept.
Answer: A

NO.22 How do you block some seldom-used FTP commands, such as CWD, and FIND from passing through the Gateway?
A. Add the restricted commands to the aftpd.conf file in the Security Management Server.
B. Modify the desired profile in the FTP commands under Protection Details in the IPS tab.
C. Configure the restricted FTP commands in the Security Servers screen of the Global Properties.
D. Enable FTP Bounce checking / Application Intelligence / Protocol Protections from the IPS tab.
Answer: B

NO.23 Which of the following does IPSec use during IPSec key negotiation?
A. IPSec SA
B. RSA Exchange
C. ISAKMP SA
D. Diffie-Hellman exchange
Answer: D

NO.24 What can you do to see the current number of kernel instances in a system with CoreXL enabled?
A. Only Check Point support personnel can access that information.
B. Run command cpconfig.
C. Execute SmartDashboard client.
D. Browse to Secure Platform Web GUI.
Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92711.htm

NO.25 A ClusterXL configuration is limited to _____ members.
A. There is no limit.
B. 16
C. 8
D. 2
Answer: C

NO.26 How is change approved for implementation in SmartWorkflow?
A. The change is submitted for approval and is automatically installed by the approver once Approve is clicked.
B. The change is submitted for approval and is automatically installed by the original submitter the next time he logs in after approval of the change.
C. The change is submitted for approval and is manually installed by the original submitter the next time he logs in after approval of the change.
D. The change is submitted for approval and is manually installed by the approver once Approve is clicked.
Answer: C

NO.27 The We-Make-Widgets company has purchased twenty UTM-1 Edge appliances for their remote offices. Kim decides the best way to manage those appliances is to use SmartProvisioning and create a profile they can all use. List the order of steps Kim would go through to add the Dallas Edge appliance to the Remote Office profile using the output below.
1 . Enter the name of the profile called "Remote Offices"
2 . Change the provisioning profile to "Remote Offices"
3 . Click File, then select New, then Provisioning Profile
4 . Click on the Devices Tab
5 . Highlight the Dallas Edge appliance, click Edit, then edit Gateway
6 . Click on the Profiles Tab
A. 6, 3, 1, 4, 5, 2
B. 4, 1, 3, 6, 5, 2
C. 6, 1, 3, 4, 5, 2
D. 4, 3, 1, 6, 5, 2
Answer: A

NO.28 Regarding QoS guarantees and limits, which of the following statements is FALSE?
A. If both a limit and a guarantee per rule are defined in a QoS rule, then the limit must be smaller than the guarantee.
B. If both a rule limit and a per connection limit are defined for a rule, the per connection limit must not be greater than the rule limit.
C. A rule guarantee must not be less than the sum the guarantees defined in its sub-rules.
D. If a guarantee is defined in a sub-rule, then a guarantee must be defined for the rule above it.

Answer: A

NO.29 When you use the Global Properties' default settings on R77, which type of traffic will be dropped if NO explicit rule allows the traffic?

A. Firewall logging and ICA key-exchange information

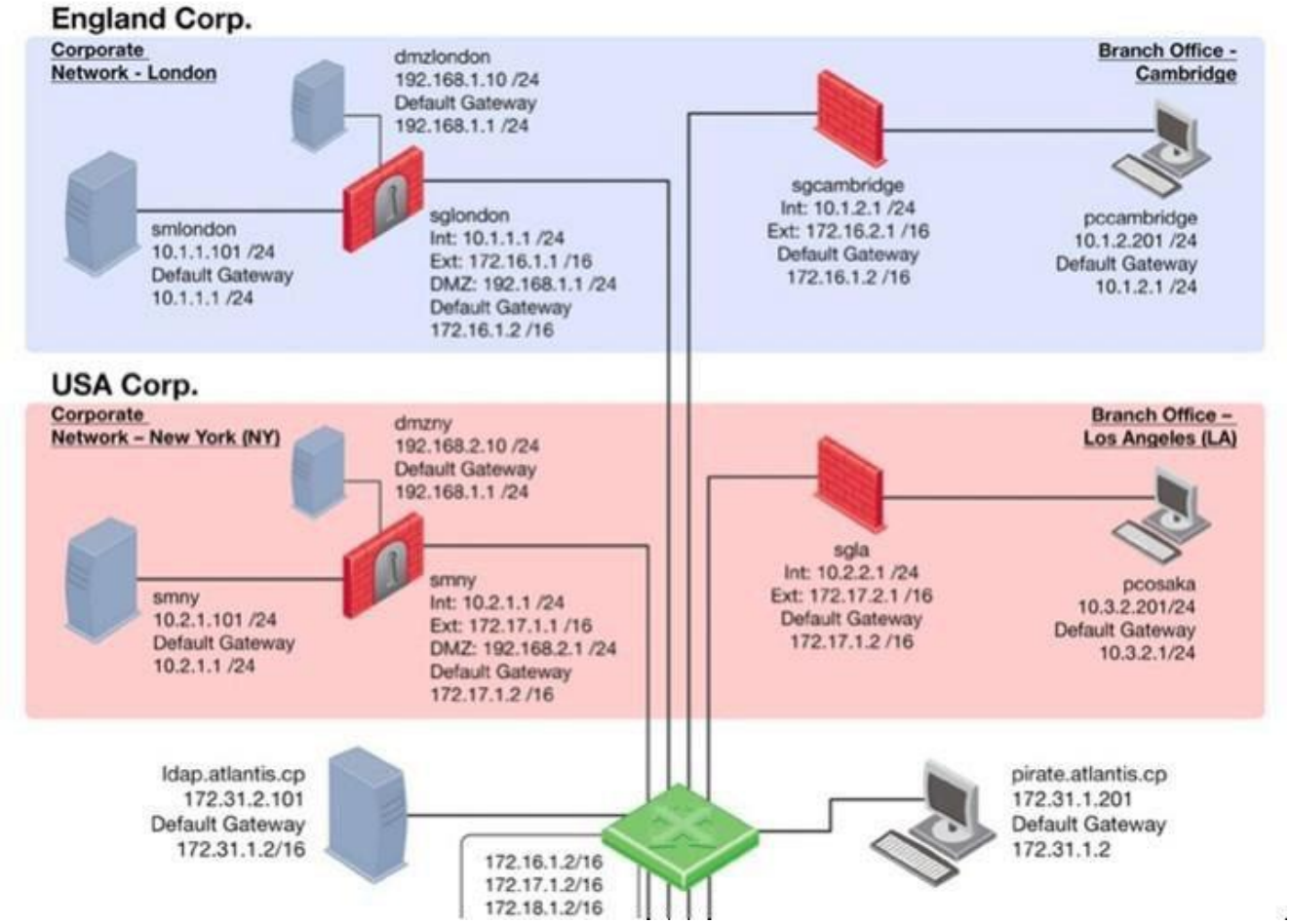
B. RIP traffic

C. Outgoing traffic originating from the Security Gateway

D. SmartUpdate connections

Answer: B

NO.30 Refer to the to the network topology below.



You have IPS software Blades active on security Gateways sglondon, sgla, and sgny, but still experience attacks on the Web server in the New York DMZ. How is this possible?

A. All of these options are possible.

B. The attacker may have used a bunch of evasion techniques like using escape sequences instead of clear text commands. It is also possible that there are entry points not shown in the network layout, like rouge access points.

C. Since other Gateways do not have IPS activated, attacks may originate from their networks without any noticing.

D. An IPS may combine different detection technologies, but is dependent on regular signature updates and well-tuned anomaly algorithms. Even if this is accomplished, no technology can offer

100% protection.
Answer: A

NO.31 What utility would you use to configure route-based VPNs?
A. vpn shell
B. vpn tu
C. vpn sw_topology
D. vpn set_slim_server
Answer: A

NO.32 Which Check Point tool allows you to open a debug file and see the VPN packet exchange details.
A. PacketDebug.exe
B. VPNDebugger.exe
C. IkeView.exe
D. IPSECDebug.exe
Answer: C

NO.33 In a UNIX environment, SmartReporter Data Base settings could be modified in:
A. $CPDIR/Database/conf/conf.C
B. $RTDIR/Database/conf/my.cnf
C. $ERDIR/conf/my.cnf
D. $FWDIR/Eventia/conf/ini.C
Answer: B

NO.34 Which of the following tools is used to generate a Security Gateway R77 configuration report?
A. infoCP
B. cpinfo
C. infoview
D. fw cpinfo
Answer: B

NO.35 John is the MegaCorp Security Administrator, and is using Check Point R71. Malcolm is the Security Administrator of a partner company and is using a different vendor's product and both have to build a VPN tunnel between their companies. Both are using clusters with Load Sharing for their firewalls and John is using ClusterXL as a Check Point clustering solution.
While trying to establish the VPN, they are constantly noticing problems and the tunnel is not stable and then Malcolm notices that there seems to be 2 SPIs with the same IP from the Check Point site. How can they solve this problem and stabilize the tunnel?
A. This can be solved by running the command Sticky VPN on the Check Point CLI. This keeps the VPN Sticky to one member and the problem is resolved.
B. This is surely a problem in the ISPs network and not related to the VPN configuration.
C. This can be solved when using clusters; they have to use single firewalls.

D. This can easily be solved by using the Sticky decision function in ClusterXL.
Answer: D

NO.36 You are establishing a ClusterXL environment, with the following topology:
VIP internal cluster IP = 172.16.10.3; VIP external cluster IP = 192.168.10.3 Cluster Member 1: 4 NICs, 3 enabled. hme0: 192.168.10.1/24, hme1: 10.10.10.1/24, qfe2:
172.16.10.1/24
Cluster Member 2: 5 NICs, 3 enabled; hme3: 192.168.10.2/24, hme1: 10.10.10.2/24, hme2:
1 72.16.10.2/24
External interfaces 192.168.10.1 and 192.168.10.2 connect to a VLAN switch. The upstream router connects to the same VLAN switch. Internal interfaces 172.16.10.1 and
172.16.10.2 connect to a hub. 10.10.10.0 is the synchronization network. The Security Management Server is located on the internal network with IP 172.16.10.3. What is the problem with this configuration?
A. The Cluster interface names must be identical across all cluster members.
B. Cluster members cannot use the VLAN switch. They must use hubs.
C. The Security Management Server must be in the dedicated synchronization network, not the internal network.
D. There is an IP address conflict.
Answer: D

NO.37 In a Cluster, some features such as VPN only function properly when:
A. all cluster members have the same number of interfaces configured.
B. all cluster members' clocks are synchronized.
C. all cluster members have the same policy.
D. all cluster members have the same Hot Fix Accumulator pack installed.
Answer: B

NO.38 Each entry in SmartDirectory has a unique _____.
A. Container
B. Distinguished Name
C. Organizational Unit
D. Schema
Answer: B

NO.39 What is the lowest possible version a Security Gateway may be running in order to use it as an LSM enabled Gateway?
A. NG-AI R55 HFAJ7
B. NGX R60
C. NGXR65HFA_50
D. NGX R71
Answer: A

NO.40 Check Point support has asked Tony for a firewall capture of accepted packets. What would

be the correct syntax to create a capture file to a filename called monitor.out?

A. Run fw monitor -e "accept;" -f monitor.out

B. Run fw monitor -e "accept;" -c monitor.out

C. Run fw monitor -e "accept;" -o monitor.out

D. Run fw monitor -e "accept;" -m monitor.out

Answer: C