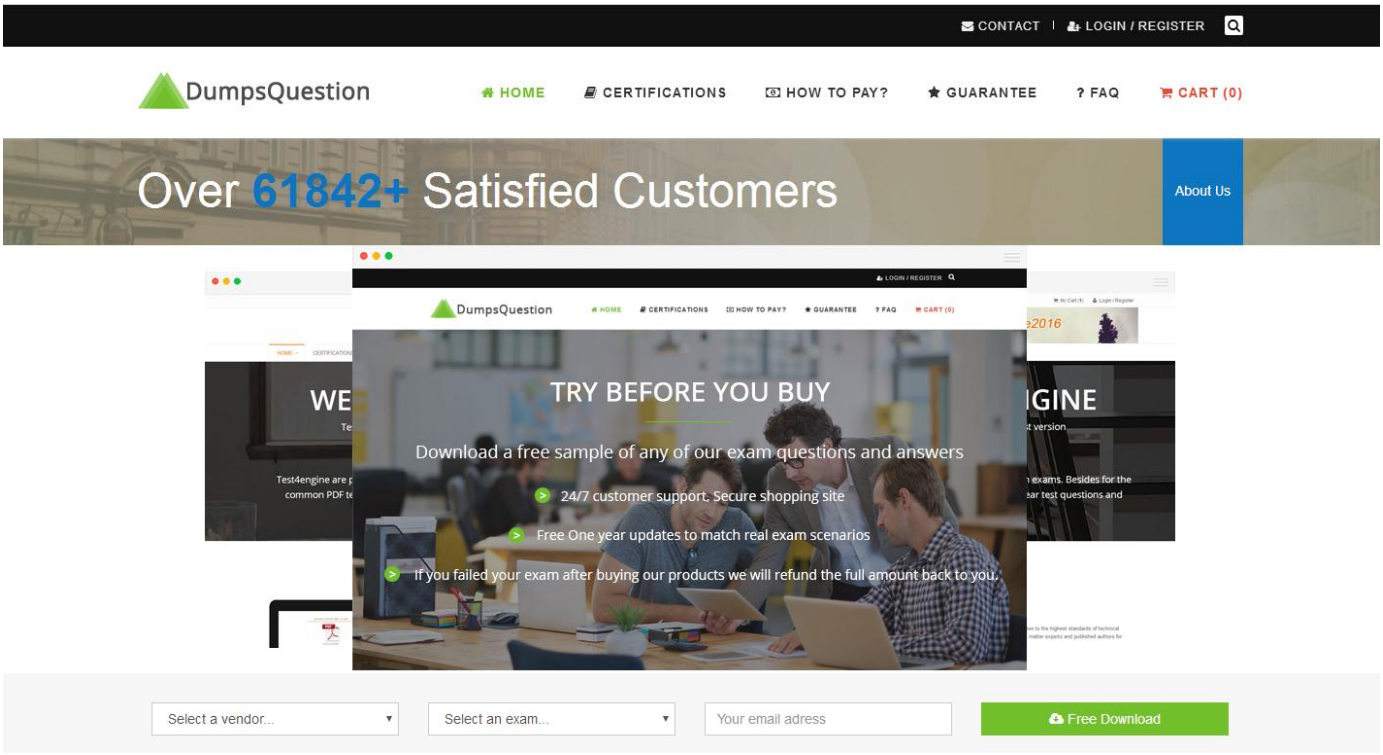
DumpsQuestion



What Clients Say About Us

Disclaimer Policy: The site does not guarantee the content of the comments. Because of the different time and the changes in the scope of the exam, it can produce different effect. Before you purchase the dump, please carefully read the product introduction from the page. In addition, please be advised the site will not be responsible for the content of the comments and contradictions between users.

"Good things should be shared together. I pass the HPE0-J75. The dumps is good for examination."

Honey

"Do not hesitate about the dumps. It is very good valid dumps. Yes, I am sure it is vald for this times. Worthy it."

Hardy

http://www.dumpsquestion.com

Professional Dump Collection & Excellent Exam Questions & Latest Questions

Exam : **156-215.80**

Title : Check Point Certified Security Administrator R80

Vendor : CheckPoint

Version : DEMO

NO.1 Session unique identifiers are passed to the web api using which http header option?
A. Proxy-Authorization
B. X-chkp-sid
C. Application
D. Accept-Charset
Answer: A

NO.2 What object type would you use to grant network access to an LDAP user group?
A. Access Role
B. SmartDirectory Group
C. User Group
D. Group Template
Answer: C

NO.3 You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100
Web Filtering Categories	☐	100
Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
Special properties	☐	100

A. XlateDst

B. XlateDPort

C. XlateSPort
D. XlateSrc
Answer: C

NO.4 When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?
A. Log, send snmp trap, email
B. Log, allow packets, email
C. Drop packet, alert, none
D. Log, alert, none
Answer: D
Explanation
Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected:

NO.5 Which of the following are types of VPN communicates?
A. Pentagon, star, and combination
B. Combined and star
C. Meshed, star, and combination
D. Star, octagon, and combination
Answer: C

NO.6 Using ClusterXL, what statement is true about the Sticky Decision Function?
A. Is only relevant when using SecureXL
B. All connections are processed and synchronized by the pivot
C. Can only be changed for Load Sharing implementations
D. Is configured using cpconfig
Answer: C

NO.7 Where do you verify that UserDirectory is enabled?
A. Verify that Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked.
B. Verify that Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
C. Verify that Security Gateway > General Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.
D. Verify that Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.
Answer: D

NO.8 Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?
A. The two algorithms do not have the same key length and so don't work together. You will get the

error
... No proposal chosen...
B. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs performance and does not add security due to a shorter key in phase 1.
C. All is fine and can be used as is.
D. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.
Answer: B

NO.9 Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?
A. External-user group
B. LDAP group
C. A group with a genetic user
D. All Users
Answer: B

NO.10 R80 Security Management Server can be installed on which of the following operating systems?
A. Gaia, SPLAT, Windows Server only
B. Gaia, SPLAT, Windows Server and IPSO only
C. Gaia only
D. Gaia and SPLAT only
Answer: C
Explanation
R80 can be installed only on GAIA OS.
Supported Check Point Installations All R80 servers are supported on the Gaia Operating System:
* Security Management Server
* Multi-Domain Security Management Server
* Log Server
* Multi-Domain Log Server
* SmartEvent Server

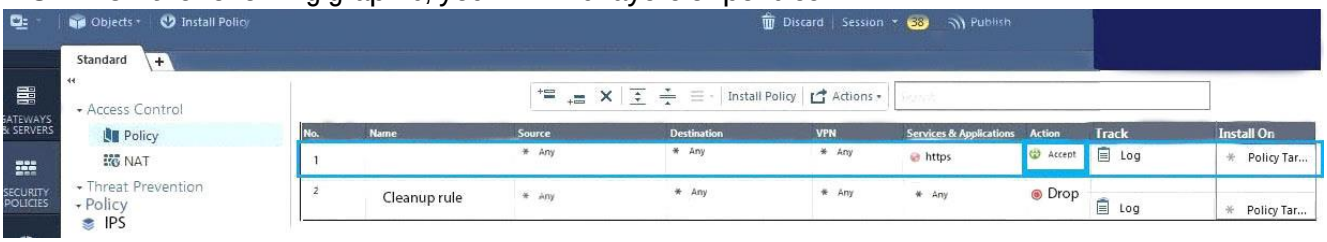
NO.11 Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD?
Read all answers and select the most complete and valid list.
A. Security Policy Editor, Log Viewer, Real Time Monitor GUI
B. SmartView Tracker, CPINFO, SmartUpdate
C. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
D. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
Answer: B

NO.12 Anti-Spoofing is typically set up on which object type?

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

NO.13 The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?
A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
B. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
C. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.
D. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with UID 0 and assign role to the user.
Answer: A

NO.14 On the following graphic, you will find layers of policies.



What is a precedence of traffic inspection for the defined polices?
A. A packet arrives at the gateway, it is checked against the rules in IPS policy layer and then it comes next to the Network policy layer and then after accepting the packet it passes to Threat Prevention layer.
B. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if implicit Drop Rule drops the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer.
C. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to Threat Prevention layer and then after accepting the packet it passes to IPS layer.
D. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer
Answer: D
Explanation
To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.
For example, when you upgrade to R80 from earlier versions:
When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

All layers are evaluated in parallel

NO.15 When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:
A. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
B. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.
C. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
D. The entire Management Database and all sessions and other administrators can connect only as Read-only.
Answer: B

NO.16 Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is _____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.
A. Accept; drop
B. Accept; redirect
C. Drop; accept
D. Redirect; drop
Answer: C

NO.17 What is true about the IPS-Blade?
A. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same
B. in R80, IPS is managed by the Threat Prevention Policy
C. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
D. in R80, IPS Exceptions cannot be attached to "all rules"
Answer: B

NO.18 In SmartEvent, what are the different types of automatic reactions that the administrator can configure?
A. Mail, Block Source, Block Destination, External Script, SNMP Trap
B. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
C. Mail, Block Source, Block Destination, Block Services, SNMP Trap
D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap
Answer: B

NO.19 Which authentication scheme requires a user to possess a token?
A. SecurID
B. TACACS
C. RADIUS

D. Check Point password
Answer: A
Explanation
SecurID
SecurID requires users to both possess a token authenticator and to supply a PIN or password

NO.20 What CLI utility allows an administrator to capture traffic along the firewall inspection chain?
A. tcpdump
B. fw monitor
C. tcpdump /snoop
D. show interface (interface) -chain
Answer: B

NO.21 How many packets does the IKE exchange use for Phase 1 Main Mode?
A. 1
B. 3
C. 6
D. 12
Answer: C

NO.22 What is the default shell for the command line interface?
A. Clish
B. Normal
C. Admin
D. Expert
Answer: A
Explanation
The default shell of the CLI is called clish

NO.23 Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment. Which details she need to fill in System Restore window before she can click OK button and test the backup?
A. Server, SCP, Username, Password, Path, Comment, Member
B. Server, Protocol, Username, Password, Path, Comment, All Members
C. Server, TFTP, Username, Password, Path, Comment, All Members
D. Server, Protocol, Username, Password, Path, Comment, Member
Answer: B

NO.24 Which of the following is NOT a tracking log option in R80.x?
A. Full Log
B. Extended Log
C. Log

D. Detailed Log
Answer: D

NO.25 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?
A. As expert user, issue the command:# IP link set eth0 addr 00:0C:29:12:34:56
B. As expert user, issue these commands:# IP link set eth0 down# IP link set eth0 addr 00:0C:29:12:34:56# IP link set eth0 up
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. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field(conf:(conns:(conn:hwaddr ("00:0C:29:12:34:56")
Answer: A

NO.26 While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?
1)Select Active Mode tab in SmartView Tracker.
2) Select Tools > Block Intruder.
3) Select Log Viewing tab in SmartView Tracker.
4) Set Blocking Timeout value to 60 minutes.
5) Highlight connection that should be blocked.
A. 1, 5, 2, 4
B. 1, 2, 5, 4
C. 3, 2, 5, 4
D. 3, 5, 2, 4
Answer: A

NO.27 The SmartEvent R80 Web application for real-time event monitoring is called:
A. SmartView Monitor
B. There is no Web application for SmartEvent
C. SmartView
D. SmartEventWeb
Answer: D

NO.28 What data MUST be supplied to the SmartConsole System Restore window to restore a backup?
A. Username, Password, Path, Version
B. Server, Username, Password, Path, Version
C. Server, Protocol, Username, Password, Path
D. Server, Protocol, Username, Password, Destination Path
Answer: C

NO.29 What needs to be configured if the NAT property 'Translate destination on client side' is not enabled in Global properties?

A. A host route to route to the destination IP

B. Use the file local.arp to add the ARP entries for NAT to work

C. Nothing, the Gateway takes care of all details necessary

D. Enabling 'Allow bi-directional NAT' for NAT to work correctly

Answer: C

NO.30 MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway.
How do you apply the license?

A. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.

B. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.

C. Using each of the Gateway's IP addresses, and applying the licenses on the Security Management Server with the command cprlic put.

D. Using the remote Gateway's IP address, and applying the license locally with command cplic put.

Answer: A