Latest Version: 6.0

Question: 1

Office mode means that:

A. SecureID client assigns a routable MAC address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
B. Users authenticate with an Internet browser and use secure HTTPS connection.
C. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
D. Allows a security gateway to assign a remote client an IP address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

Explanation:
Office Mode enables a Security Gateway to assign internal IP addresses to SecureClient users. This IP address will not be exposed to the public network, but is encapsulated inside the VPN tunnel between the client and the Gateway. The IP to be used externally should be assigned to the client in the usual way by the Internet Service provider used for the Internet connection. This mode allows a Security Administrator to control which addresses are used by remote clients inside the local network and makes them part of the local network. The mechanism is based on an IKE protocol extension through which the Security Gateway can send an internal IP address to the client.

Question: 2

Administrator wishes to update IPS from SmartConsole by clicking on the option “update now” under the IPS tab. Which device requires internet access for the update to work?

A. Security Gateway
B. Device where SmartConsole is installed
C. SMS
D. SmartEvent

Answer: B

Explanation:
Updating IPS Manually
You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website. You can only manually update IPS if a proxy is defined in Internet Explorer settings.
To obtain updates of all the latest protections from the IPS website:
The LAN Settings window opens.
The settings for the Internet Explorer proxy server are configured.

If you chose to automatically mark new protections for Follow Up, you have the option to open the Follow Up page directly to see the new protections.

Question: 3

Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?

A. Create a text-file with mgmt_cli script that creates all objects and policies. Open the file in SmartConsole Command Line to run it.
B. Create a text-file with Gaia CLI -commands in order to create all objects and policies. Run the file in CLISH with command load configuration.
C. Create a text-file with DBEDIT script that creates all objects and policies. Run the file in the command line of the management server using command dbedit -f.
D. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.

Answer: A

Explanation:
Did you know: mgmt_cli can accept csv files as inputs using the --batch option.
The first row should contain the argument names and the rows below it should hold the values for these parameters.
So an equivalent solution to the powershell script could look like this:
data.csv:

name	ip v4-address	color
host1	192.168.35.1	black
host2	192.168.35.2	red
host3	192.168.35.3	blue

mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server>
This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

Question: 4

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

A. RADIUS
B. Remote Access and RADIUS

C. AD Query
D. AD Query and Browser-based Authentication

Answer: D

Explanation:
Identity Awareness gets identities from these acquisition sources:

Question: 5

Which of the following is NOT a back up method?

A. Save backup
B. System backup
C. snapshot
D. Migrate

Answer: A

Explanation:
The built-in Gaia backup procedures:
Check Point provides three different procedures for backing up (and restoring) the operating system and networking parameters on your appliances.