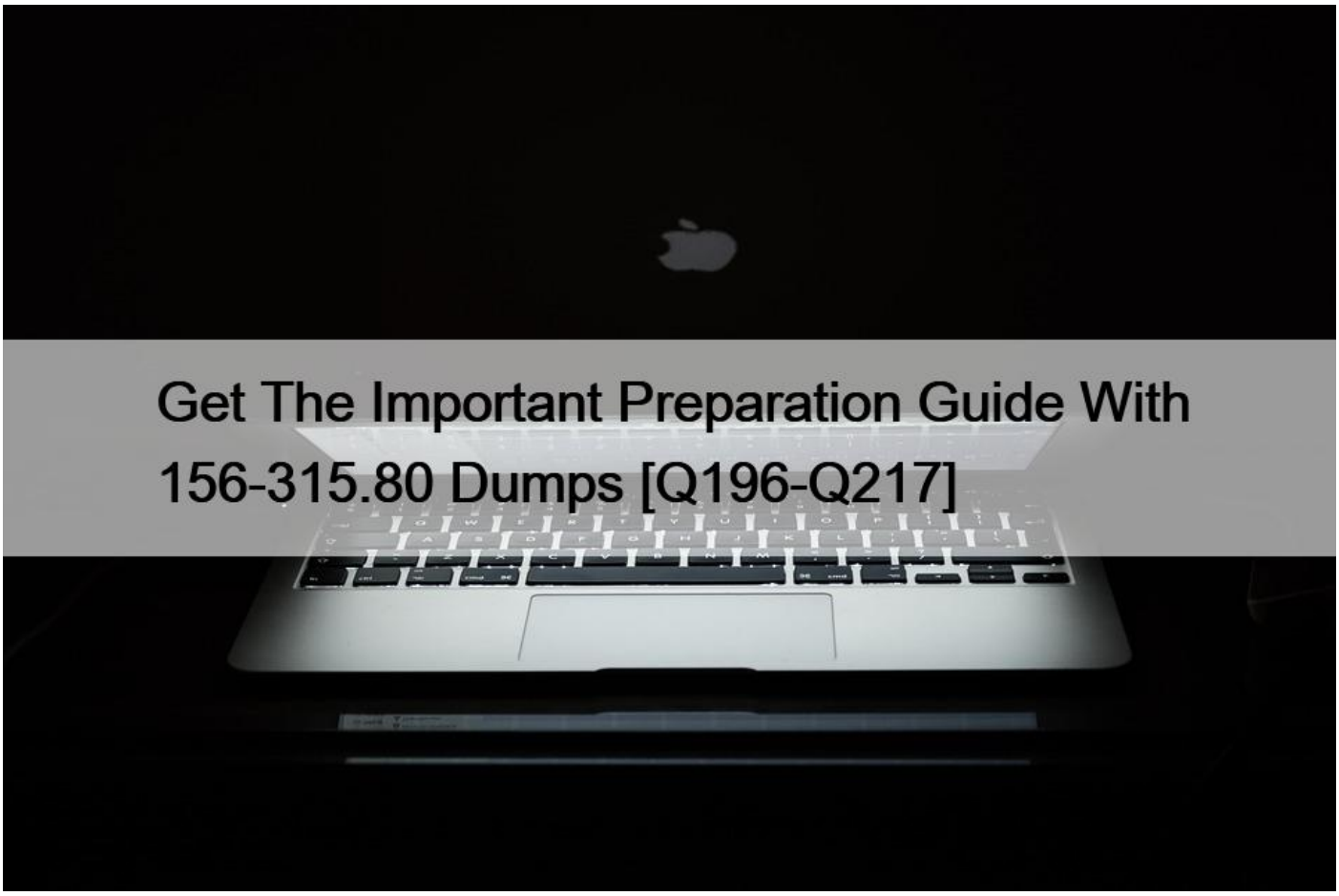
Get The Important Preparation Guide With 156-315.80 Dumps [Q196-Q217



Get The Important Preparation Guide With 156-315.80 Dumps Get Totally Free Updates on 156-315.80 Dumps PDF Questions NO.196 Which Remote Access Client does not provide an Office-Mode Address?

* SecuRemote
* Endpoint Security Suite
* Endpoint Security VPN
* Check Point Mobile

NO.197 SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user’s machine via the web browser. What are the two modes of SNX?

* Application and Client Service
* Network and Application
* Network and Layers
* Virtual Adapter and Mobile App

Explanation/Reference: https://supportcenter.checkpoint.com/supportcenter/portal?

eventSubmit_doGoviewsolutiondetails=&solutionid=sk67820

NO.198 Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace

the existing single core CPU. After installation, is the administrator required to perform any additional tasks?
* Go to clash-Run cpstop | Run cpstart
* Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
* Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores
* Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

NO.199 SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user’s machine via the web browser. What are the two modes of SNX?
* Application and Client service
* Network and Application
* Network and Layers
* Virtual Adapter and Mobile App
Explanation

SSL Network Extender (SNX) is a thin SSL VPN on-demand client installed automatically on the user’s machine via a web browser. It supplies access to all types of corporate resources. SSL Network Extender (SNX) has two modes:

*Network Mode: Users can access all application types (Native-IP-based and Web-based) in the internal network. To install the Network Mode client, users must have administrator privileges on the client computer.

*Application Mode: Users can access most application types (Native-IP-based and Web-based) in the internal network, including most TCP applications. The user does not require administrator privileges on the endpoint machine.

NO.200 Which process handles connection from SmartConsole R80?
* fwd
* cpmd
* cpm
* cpd

NO.201 You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don’t have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priorities Queues and fully enable Dynamic Dispatcher. How can you enable them?
* fw ctl multik dynamic_dispatching on
* fw ctl multik dynamic_dispatching set_mode 9
* fw ctl multik set_mode 9
* fw ctl multik pq enable
Reference:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk105261

NO.202 Which of the following is NOT a valid type SecureXL template?
* Accept Template
* Deny template
* Drop Template
* NAT Template

NO.203 What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?
* 4 Interfaces – an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.

* 3 Interfaces – an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
* 1 Interface – an interface leading to the organization and the Internet, and configure for synchronization.
* 2 Interfaces – a data interface leading to the organization and the Internet, a second interface for synchronization.

Explanation/Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Mobile_Access_WebAdmin/41723.htm

NO.204 Which is NOT an example of a Check Point API?
* Gateway API
* Management API
* OPSC SDK
* Threat Prevention API

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R80/APIs/#introduction%20

NO.205 Which statement is not TRUE about Default synchronization?
* Using UDP Multicast Broadcast on port 8161
* Using UDP Multicast on port 8116
* Quicker than Full sync
* Transfer changes in the kernel tables between cluster members

NO.206 What kind of information would you expect to see using the sim affinity command?
* The VMACs used in a Security Gateway cluster
* The involved firewall kernel modules in inbound and outbound packet chain
* Overview over SecureXL templated connections
* Network interfaces and core distribution used for CoreXL

NO.207 Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?
* Synchronized
* Never been synchronized
* Lagging
* Collision

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?

topic=documents/R80/CP_R80_SecMGMT/120712

NO.208 What SmartEvent component creates events?
* Consolidation Policy
* Correlation Unit
* SmartEvent Policy
* SmartEvent GUI

NO.209 What is the command to check the status of the SmartEvent Correlation Unit?
* fw ctl get int cpsead_stat
* cpstat cpsead
* fw ctl stat cpsemd
* cp_conf get_stat cpsemd

Explanation/Reference: https://supportcenter.checkpoint.com/supportcenter/portal?

eventSubmit_doGoviewsolutiondetails=&solutionid=sk113265

NO.210 For Management High Availability, which of the following is NOT a valid synchronization status?
* Collision
* Down
* Lagging
* Never been synchronized

References:

NO.211 Fill in the blank: The R80 utilityfw monitoris used to troubleshoot _____.
* User data base corruption
* LDAP conflicts
* Traffic issues
* Phase two key negotiations

Check Point’s FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark Reference: https://supportcenter.checkpoint.com/supportcenter/portal?

eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

NO.212 During Inspection of your Threat Prevention logs you find four different computers having one event each with a critical Severity. Which of those host should you try to remediate first?
* Host having critical event found by Threat Emulation IS.
* Host having critical event found by IPS
* Host having critical event found by Antivirus
* Host having critical event found by Anti-Bot

NO.213 An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret and cannot be enabled.

Why does it not allow him to specify the pre-shared secret?
* IPsec VPN blade should be enabled on both Security Gateway.
* Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
* Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
* The Security Gateways are pre-R75.40.

NO.214 When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:
* All UDP packets
* All IPv6 Traffic
* All packets that match a rule whose source or destination is the Outside Corporate Network
* CIFS packets

NO.215 Which is NOT an example of a Check Point API?
* Gateway API
* Management API
* OPSC SDK

* Threat Prevention API

References:

NO.216 What will SmartEvent automatically define as events?

* Firewall
* VPN
* IPS
* HTTPS

NO.217 To ensure that VMAC mode is enabled, which CLI command should you run on all cluster members?

* fw ctl set int fwha vmac global param enabled
* fw ctl get int vmac global param enabled; result of command should return value 1
* cphaprob-a if
* fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm