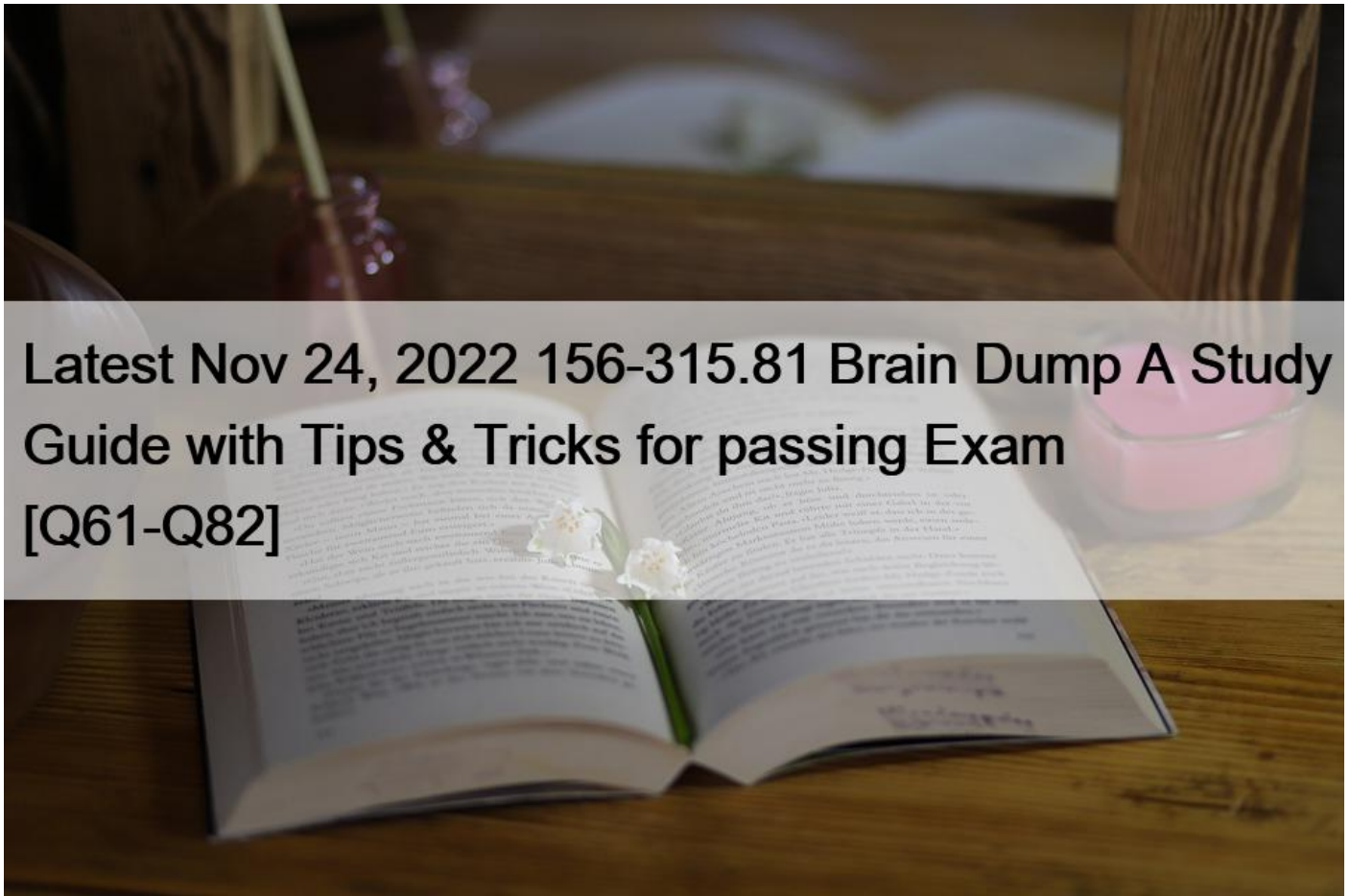


## Latest Nov 24, 2022 156-315.81 Brain Dump A Study Guide with Tips & Tricks for passing Exam [Q61-Q82]



## Latest Nov 24, 2022 156-315.81 Brain Dump A Study Guide with Tips & Tricks for passing Exam [Q61-Q82]

Latest Nov 24, 2022 156-315.81 Brain Dump: A Study Guide with Tips & Tricks for passing Exam  
156-315.81 Question Bank: Free PDF Download Recently Updated Questions

### NEW QUESTION 61

Which of the following authentication methods ARE NOT used for Mobile Access?

- \* RADIUS server
- \* Username and password (internal, LDAP)
- \* SecurID
- \* TACACS+

### NEW QUESTION 62

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- \* SND is a feature to accelerate multiple SSL VPN connections
- \* SND is an alternative to IPsec Main Mode, using only 3 packets
- \* SND is used to distribute packets among Firewall instances

- \* SND is a feature of fw monitor to capture accelerated packets

### NEW QUESTION 63

Which one of the following is true about Threat Emulation?

- \* Takes less than a second to complete
- \* Works on MS Office and PDF files only
- \* Always delivers a file
- \* Takes minutes to complete (less than 3 minutes)

### NEW QUESTION 64

Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

- \* cpwd
- \* fwd
- \* cpd
- \* fwm

Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that require direct GUI access, such as SmartEvent, It provides the following:

&#8211; GUI Client communication

&#8211; Database manipulation

&#8211; Policy Compilation

&#8211; Management HA sync

### NEW QUESTION 65

What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?

- \* Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.
- \* Security Gateway failover as well as Security Management Server failover is a manual procedure.
- \* Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
- \* Security Gateway failover as well as Security Management Server failover is an automatic procedure.

### NEW QUESTION 66

Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.

What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

- \* Pamela should check SecureXL status on DMZ Security gateway and if it's turned ON. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.

- \* Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OFF. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
- \* Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
- \* Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

### NEW QUESTION 67

Which process is used mainly for backward compatibility of gateways in R81.X? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.

- \* cpm
- \* fwd
- \* cpd
- \* fwm

D18912E1457D5D1DDCBD40AB3BF70D5D

### NEW QUESTION 68

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- \* Symmetric routing
- \* Failovers
- \* Asymmetric routing
- \* Anti-Spoofing

### NEW QUESTION 69

Which of the following statements about SecureXL NAT Templates is true?

- \* NAT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are enabled by default and work only if Accept Templates are enabled.
- \* DROP Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are disabled by default and work only if NAT Templates are disabled.
- \* NAT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are disabled by default and work only if Accept Templates are disabled.
- \* ACCEPT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are disabled by default and work only if NAT Templates are disabled.

### NEW QUESTION 70

During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

- \* Dropped without sending a negative acknowledgment
- \* Dropped without logs and without sending a negative acknowledgment
- \* Dropped with negative acknowledgment
- \* Dropped with logs and without sending a negative acknowledgment

### NEW QUESTION 71

Fill in the blank: The command \_\_\_\_\_ provides the most complete restoration of a R81 configuration.

- \* upgrade\_import
- \* cpconfig
- \* fwm dbimport -p <export file>
- \* cpinfo -recover

### NEW QUESTION 72

Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is \_\_\_\_\_ .

- \* Sent to the Internal Certificate Authority.
- \* Sent to the Security Administrator.
- \* Stored on the Security Management Server.
- \* Stored on the Certificate Revocation List.

### NEW QUESTION 73

Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R81.10 SmartConsole application?

- \* IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.
- \* Firewall, IPS, Threat Emulation, Application Control.
- \* IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.
- \* Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.

### NEW QUESTION 74

Capsule Connect and Capsule Workspace both offer secured connection for remote users who are using their mobile devices. However, there are differences between the two.

Which of the following statements correctly identify each product's capabilities?

- \* Workspace supports ios operating system, Android, and WP8, whereas Connect supports ios operating system and Android only
- \* For compliance/host checking, Workspace offers the MDM cooperative enforcement, whereas Connect offers both jailbreak/root detection and MDM cooperative enforcement.
- \* For credential protection, Connect uses One-time Password login support and has no SSO support, whereas Workspace offers both One-Time Password and certain SSO login support.
- \* Workspace can support any application, whereas Connect has a limited number of application types which it will support.

### NEW QUESTION 75

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

### NEW QUESTION 76

At what point is the Internal Certificate Authority (ICA) created?

- \* Upon creation of a certificate.
- \* During the primary Security Management Server installation process.

- \* When an administrator decides to create one.
- \* When an administrator initially logs into SmartConsole.

#### NEW QUESTION 77

The Hit count feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits if the Track option is set to None?;

- \* No, it will work independently. Hit Count will be shown only for rules Track option set as Log or alert.
- \* Yes it will work independently as long as analyze all rules; tick box is enabled on the Security Gateway.
- \* No, it will not work independently because hit count requires all rules to be logged.
- \* Yes it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways.

#### NEW QUESTION 78

Which Check Point daemon monitors the other daemons?

- \* fwm
- \* cpd
- \* cpwd
- \* fwssd

#### NEW QUESTION 79

Which one of the following is true about Capsule Connect?

- \* It is a full layer 3 VPN client
- \* It offers full enterprise mobility management
- \* It is supported only on iOS phones and Windows PCs
- \* It does not support all VPN authentication methods

#### NEW QUESTION 80

Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?

- \* Security Gateway Clusters in Load Sharing mode
- \* Dedicated Log Server
- \* Dedicated SmartEvent Server
- \* Security Gateways/Clusters in ClusterXL HA new mode

#### NEW QUESTION 81

After the initial installation on Check Point appliance, you notice that the Management-interface and default gateway are incorrect.

Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

- \* `set interface Mgmt ipv4-address 192.168.80.200 mask-length 24`  
`set static-route default nexthop gateway address 192.168.80.1`  
`onsave config`
- \* `set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0`  
`add static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1`  
`onsave config`
- \* `set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0`  
`set static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1`  
`onsave config`
- \* `set interface Mgmt ipv4-address 192.168.80.200 mask-length 24`  
`add static-route default nexthop gateway address 192.168.80.1`  
`onsave config`

#### NEW QUESTION 82

VPN Link Selection will perform the following when the primary VPN link goes down?

- \* The Firewall will drop the packets.
- \* The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
- \* The Firewall will send out the packet on all interfaces.
- \* The Firewall will inform the client that the tunnel is down.

What should I know before taking the CheckPoint 156-315.81 Exam?

If you are looking for a certification that will help you get a job in the cyber security industry, then Check Point Certified Security Expert (CCSE) is the right certification for you.

The CCSE certification is designed to help individuals understand and apply best practices for protecting IT systems from threats and vulnerabilities. This includes understanding how to protect your organization's networks from cyberattacks, as well as being able to create a strategy to mitigate risk.

The CCSE certification has three levels: Level 1 - CCSE-155-001, Level 2 - CCSE-155-002, and Level 3 - CCSE-155-003.

Level 1 is focused on the basics of network security, while Level 2 covers advanced topics such as vulnerability management and incident response techniques. These are both required for passing the exam at Level 3.

If you want to become a strong candidate for getting hired by your company or other organizations who require security professionals with this level of expertise, then you need to put in some time studying and preparing yourself before taking this exam.

**CheckPoint 156-315.81 exam dumps** will help you get the most out of your preparation.

**New 156-315.81 Exam Dumps with High Passing Rate:** <https://www.validbraindumps.com/156-315.81-exam-prep.html>