Get 156-315.81 Actual Free Exam Q&As to Prepare for Your CheckPoint Certification [Q348-Q364

Get 156-315.81 Actual Free Exam Q&As to Prepare for Your CheckPoint Certification [Q348-Q364]

Get 156-315.81 Actual Free Exam Q&As to Prepare for Your CheckPoint Certification
CheckPoint Actual Free Exam Questions And Answers

The CheckPoint 156-315.81 exam is designed to test a candidate's understanding of Check Point security products and how they can be deployed to secure enterprise networks. It covers a wide range of topics, including network security, VPN technologies, firewall policies, advanced threat prevention, and security management. 156-315.81 exam is divided into multiple sections, and each section covers a specific topic. Candidates must demonstrate their proficiency in each section to pass the exam.

NEW QUESTION 348

Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?
* Source Address

* Destination Address
* TCP Acknowledgment Number
* Source Port
Explanation

https //sc1.checkpoint.com/documents/R77/CP R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 349

When using the Mail Transfer Agent, where are the debug logs stored?
* $FWDIR/bin/emaild.mta. elg
* $FWDIR/log/mtad elg
* /var/log/mail.mta elg
* $CPDIR/log/emaild elg

NEW QUESTION 350

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
Explanation

For packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are dropped with logs and without sending a negative acknowledgment. Firewall Kernel Inspection is the process of applying security policies and rules to network traffic by the Firewall kernel module. If a packet does not match any rule or matches a rule with an action of Drop or Reject, the packet is dropped by the Firewall kernel module. The difference between Drop and Reject is that Drop silently discards the packet without informing the sender, while Reject discards the packet and sends a negative acknowledgment (such as an ICMP message) to the sender. However, both Drop and Reject actions generate logs that record the details of the dropped packets, such as source, destination, protocol, port, rule number, etc. The other options are either incorrect or describe different scenarios.

NEW QUESTION 351

To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, run the following command in Expert mode then reboot:
* fw ctl multik set_mode 1
* fw ctl Dynamic_Priority_Queue on
* fw ctl Dynamic_Priority_Queue enable
* fw ctl multik set_mode 9
Explanation

Dynamic Dispatcher is a feature that optimizes the performance of Security Gateways with multiple CPU cores by dynamically allocating traffic to different cores based on their load and priority. Firewall Priority Queues is a feature that prioritizes traffic based on its type and importance by assigning it to different queues with different weights and limits. To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, you need to run the following command in Expert mode then reboot:

```
fw ctl multik set_mode 9
```

This command sets the multi-core mode to 9, which means that Dynamic Dispatcher is enabled with Firewall Priority Queues. The other commands are not valid or do not enable both features. References: R81 Performance Tuning Administration Guide

NEW QUESTION 352

SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user&#8217;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
SSL Network Extender (SNX) has two modes of operation: Network Mode and Application Mode. Network Mode provides full network connectivity to the remote user, while Application Mode provides access to specific applications on the corporate network. Reference: [SSL Network Extender]

NEW QUESTION 353

What is false regarding prerequisites for the Central Deployment usage?
* The administrator must have write permission on SmartUpdate
* Security Gateway must have the latest CPUSE Deployment Agent
* No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.
* The Security Gateway must have a policy installed
Establishing SIC between gateways and the management server is a prerequisite for Central Deployment usage, as the CDT tool will not take care of this automatically1. The administrator must have write permission on SmartUpdate, the Security Gateway must have the latest CPUSE Deployment Agent, and the Security Gateway must have a policy installed2. These are the basic requirements for using the Central Deployment Tool (CDT), which is a utility that lets you manage a deployment of software packages from your Management Server to the multiple managed Security gateways and cluster members at the same time2. The CDT can perform various actions, such as installation of software packages, taking snapshots, running shell scripts, pushing/pulling files, and automating the RMA backup and restore process2. The CDT is supported on Check Point Appliances with R80.40 and higher versions2. Reference: How to keep your Security Gateways up to date &#8211; Check Point Software, Central Deployment Tool (CDT) &#8211; Check Point CheckMates.

NEW QUESTION 354

What solution is Multi-queue intended to provide?
* Improve the efficiency of traffic handling by SecureXL SNDs
* Reduce the confusion for traffic capturing in FW Monitor
* Improve the efficiency of CoreXL Kernel Instances
* Reduce the performance of network interfaces

NEW QUESTION 355

In Advanced Permanent Tunnel Configuration, to set the amount of time the tunnel test runs without a response before the peer host is declared &#8216;down&#8217;, you would set the__________?
* life sign polling interval
* life sign timeout
* life_sign_polling_interval

* life_sign_timeout
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?

topic=documents/R77/CP_R77_VPN_AdminGuide/14018

NEW QUESTION 356

What needs to be configured if the NAT property &#8216;Translate destination or client side&#8217; is not enabled in Global Properties?
* A host route to route to the destination IP.
* Use the file local.arp to add the ARP entries for NAT to work.
* Nothing, the Gateway takes care of all details necessary.
* Enabling &#8216;Allow bi-directional NAT&#8217; for NAT to work correctly.
The NAT property &#8216;Translate destination or client side&#8217; is used to determine whether the destination IP address of a packet should be translated on the client side or the server side of a connection. If this property is not enabled, then the destination IP address is translated on the server side, which means that the gateway takes care of all details necessary for NAT to work. The gateway will send an ARP request for the translated IP address and will reply to any ARP requests for that address. Therefore, there is no need to configure a host route, use the local.arp file, or enable bi-directional NAT for NAT to work correctly. Reference: R81 Security Management Administration Guide, page 1010.

NEW QUESTION 357

Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.

What will happen to the changes already made?
* Tom&#8217;s changes will have been stored on the Management when he reconnects and he will not lose any of his work.
* Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
* Tom&#8217;s changes will be lost since he lost connectivity and he will have to start again.
* Tom will have to reboot his SmartConsole computer, clear to cache, and restore changes.
Tom&#8217;s changes will have been stored on the Management when he reconnects and he will not lose any of his work.

This is because SmartConsole has a feature called Concurrent Administration, which allows multiple administrators to work on the same Security Policy simultaneously, without blocking each other or creating conflicts. Concurrent Administration uses a locking mechanism to prevent multiple administrators from modifying the same rule or object at the same time. When an administrator clicks on a rule or an object, it becomes locked and a lock icon appears next to it. The lock icon shows the name of the administrator who is working on that rule or object, and prevents other administrators from editing it until it is unlocked12.

Concurrent Administration also has a feature called Session Persistence, which preserves the changes made by an administrator in case of a network failure or a SmartConsole crash. When an administrator reconnects to the Management Server after a network failure or a SmartConsole crash, they can resume their work from where they left off, without losing any changes. The changes are stored locally on the administrator&#8217;s machine until they are published to the Management Server13.

Therefore, if Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity, his changes will not be lost. They will be stored locally on his machine and he can resume his work when he reconnects to the Management Server.

NEW QUESTION 358

What state is the Management HA in when both members have different policies/databases?

- Synchronized
- Never been synchronized
- Lagging
- Collision

Explanation

The state of the Management HA when both members have different policies/databases is Collision. This state indicates that there is a conflict between the members and they need to be synchronized manually. The other states are not applicable in this scenario. The Synchronized state indicates that both members have identical policies/databases and are ready for failover. The Never been synchronized state indicates that the members have never been synchronized since they were configured as HA pair. The Lagging state indicates that one member has a newer policy/database than the other member and needs to be synchronized automatically.

References: [Management High Availability]

https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/
html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/98838

NEW QUESTION 359

The Event List within the Event tab contains:

- a list of options available for running a query.
- the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list.
- events generated by a query.
- the details of a selected event.

Explanation

The Event List within the Event tab contains events generated by a query. The Event List shows the events that match the query criteria, such as time range, filter, and aggregation. The events can be sorted by different columns, such as severity, time, action, and source3. The other options are either not part of the Event tab or not related to the Event List. References: Check Point R81 Logging and Monitoring Administration Guide

NEW QUESTION 360

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

- Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
- Create a separate Security Policy package for each remote Security Gateway.
- Create network objects that restricts all applicable rules to only certain networks.
- Run separate SmartConsole instances to login and configure each Security Gateway directly.

Explanation

To simplify security administration when working with multiple Security Gateways enforcing an extensive number of rules, you would choose to create a separate Security Policy package for each remote Security Gateway. A Security Policy package is a set of rules and objects that can be assigned to one or more Security Gateways. This allows you to manage different policies for different gateways from the same Management Server1. The other options are either not effective or not feasible for simplifying security administration.

References: Check Point R81 Security Management Administration Guide

NEW QUESTION 361

What is &#8220;Accelerated Policy Installation&#8221;?
* Starting R81, the Desktop Security Policy installation process is accelerated thereby reducing the duration of the process significantly
* Starting R81, the QoS Policy installation process is accelerated thereby reducing the duration of the process significantly
* Starting R81, the Access Control Policy installation process is accelerated thereby reducing the duration of the process significantly
* Starting R81, the Threat Prevention Policy installation process is accelerated thereby reducing the duration of the process significantly

NEW QUESTION 362

What are the attributes that SecureXL will check after the connection is allowed by Security Policy?
* Source address, Destination address, Source port, Destination port, Protocol
* Source MAC address, Destination MAC address, Source port, Destination port, Protocol
* Source address, Destination address, Source port, Destination port
* Source address, Destination address, Destination port, Protocol
The attributes that SecureXL will check after the connection is allowed by Security Policy are Source address, Destination address, Source port, Destination port, Protocol. These are the five tuple parameters that define a connection and are used by SecureXL to accelerate the traffic. The other options are either missing some of the parameters or include irrelevant ones, such as MAC addresses1. Reference: Check Point R81 SecureXL Administration Guide

NEW QUESTION 363

Which blades and or features are not supported in R81?
* SmartEvent Maps
* SmartEvent
* Identity Awareness
* SmartConsole Toolbars
According to the Check Point website, SmartEvent Maps is a feature that was supported in previous versions of SmartEvent, but is not supported in R81. SmartEvent Maps displayed a graphical representation of security events on a world map. The other options are either supported or not valid features in R81. Reference: SmartEvent Maps

NEW QUESTION 364

When simulating a problem on ClusterXL cluster with cphaprob -d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?
* cphaprob -d STOP unregister
* cphaprob STOP unregister
* cphaprob unregister STOP
* cphaprob -d unregister STOP
esting a failover in a controlled manner using following command;

```
# cphaprob -d STOP -s problem -t 0 register
```

This will register a problem state on the cluster member this was entered on; If you then run;

```
# cphaprob list
```

this will show an entry named STOP.

to remove this problematic register run following;

```
# cphaprob -d STOP unregister
```

156-315.81 Questions Truly Valid For Your CheckPoint Exam:
https://www.examslabs.com/CheckPoint/Check-Point-Certified-Security-Expert/best-156-315.81-exam-dumps.html]