Question #1 *Topic 1*

What are SmartEvent Features and Capabilities?

A. 300+ Check Point Security Best Practices, Monitoring in real time policy changes, Regulatory standards Best Practices

B. Full threat visibility, Real-time forensics, Immediate response

C. SmartDashboards, SmartLogs, SmartEvents

D. Compliance Reports, Events Logs and Reports, Best Practices Tests

Suggested Answer: *B*

greeklover84 3 weeks, 1 day ago

Selected Answer: B

yes B makes sense in comparison to the rest.

upvoted 1 times

Question #2 *Topic 1*

John wants to execute a command on all members of an ElasticXL Cluster, which command line should he use?

A. expert

B. clish

C. gclish

D. global api

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

What is the correct statement about requirement of a JSON configuration file when upgrading a Security Management / Log / SmartEvent Server using CPUSE?

A. A JSON configuration file is required to upgrade any Check Point device prior to R80.20 when upgrading to R82 or above release

B. There is no such requirement of a JSON configuration file when using CPUSE. The CPUSE upgrade is completely automatic

C. A JSON configuration file is required only if there is a change of IP address on an of the Security Management / Log / SmartEvent servers

D. A JSON configuration is always required when upgrading a Security Management / Log / SmartEvent server to R82 or above release

Suggested Answer: *D*

Community vote distribution

C (100%)

victorpardo21 2 months, 1 week ago

Selected Answer: C

C. A JSON configuration file is required only if there is a change of IP address on an of the Security Management / Log / SmartEvent servers.

upvoted 1 times

9dfb7ac 3 months ago

Selected Answer: C

JSON is only required if there is an IP address change

upvoted 2 times

Question #4 *Topic 1*

What is Modern Dump?

A. It's database dump with information stored without pre-generated code that require further verification but does not require compilation before transfer to the Security Gateway

B. It's database dump with information stored with pre-generated code that require further compilation or verification before transfer to the Security Gateway

C. It's database dump with information stored without pre-generated code that does not require further compilation or verification before transfer to the Security Gateway

D. It's database dump with information stored with pre-generated code that does not require further compilation or verification before transfer to the Security Gateway

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Which command will allow an administrator to manually load policy files on the gateway?

A. fw fetch

B. fw load

C. fw install

D. fw policy

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Which statement concerning Network Feeds is most correct?

A. Network Feeds are the objects manually created in the SmartConsole with a name but no IP address. They are used in security policies and resolve to an IP address locally on each Security Gateway

B. Network Feeds are generated on external HTTP/HTTPS servers that provides an ability to add custom cyber intelligence feeds into the Access Control engine

C. Network Feeds are external services like Zoom, Office365. Ips are maintained on the Check Point Cloud and objects are automatically synced with the cloud at regular intervals

D. Network Feeds are generated on external HTTP/HTTPS servers that are fetched by Security Gateways

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

In SmartEvent Settings & Policy App, Severity contains which options?

A. Informational, Warning, Low, Medium, High

B. Low, Medium, High

C. Low, Medium, High, Critical

D. Informational, Low, Medium, High, Critical

Suggested Answer: *D*

Community vote distribution

D (100%)

greeklover84 3 weeks, 1 day ago

Selected Answer: D

In the Check Point SmartEvent Policy tab, the Severity settings, used to categorize events, include Informational, Low, Medium, High, and Critical. These options allow administrators to filter, prioritize, and define automatic reactions (like alerts or blocks) based on the severity level of the event.

upvoted 1 times

Question #8 *Topic 1*

Where does an administrator need to navigate to in the SmartConsole to carry out a Central Deployment upgrade?

A. COMMAND LINE

B. GATEWAYS & SERVERS

C. MANAGE & SETTINGS

D. INFINITY SERVICES

Suggested Answer: *C*

Community vote distribution

B (100%)

greeklover84 3 weeks, 1 day ago

Selected Answer: B

yes I would go for B.

upvoted 1 times

victorpardo21 2 months, 1 week ago

Selected Answer: B

B. GATEWAYS & SERVERS is the correct answer.

upvoted 1 times

9dfb7ac 3 months ago

Selected Answer: B

Manage and settings is where the deployment images are stored. But deploying updates is done directly from Gateways and servers

upvoted 2 times

Question #9 *Topic 1*

What is true about the magg1 and Sync interfaces on an ElasticXL Cluster?

A. magg1 is a bonded interface, Sync is also a bonded interface

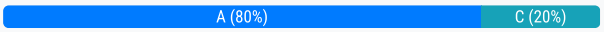
B. magg1 is a secondary interface of the Mgmt Port, Sync is the Sync port

C. magg1 is a bonded interface, Sync is an individual Sync Port

D. magg1 is only available in Maestro and is a disabled and unused port in ElasticXL. Sync is the Sync Port

Suggested Answer: *A*

Community vote distribution



caf7705 2 weeks, 2 days ago

Selected Answer: A

navigate to page 435, ElasticXL Cluster interfaces

upvoted 1 times

Armrest9955 1 month, 1 week ago

Selected Answer: A

Both magg1 and Sync are bonded. Answer is A

upvoted 1 times

liorp1 2 months ago

Selected Answer: C

magg1 interface = management aggregation interface

It is implemented as a bonded interface by default, you do not change that.

whereas Sync interface is the traditional ClusterXL sync and is dedicated physical interface (not bonded by default but can be changed by admin)

upvoted 1 times

victorpardo21 2 months, 1 week ago

Selected Answer: A

A. magg1 is a bonded interface, Sync is also a bonded

upvoted 1 times

elekt 2 months, 2 weeks ago

Selected Answer: A

magg1 is a dedicated and bonded interface responsible for Management traffic.

sync interface: dedicated interface responsible for synchronization between cluster members, ensuring all nodes have consistent state information.

This is a bonded interface that is hidden in SmartConsole. The Sync port is assigned automatically. So correct answer is A

upvoted 1 times

Question #10 *Topic 1*

VTI in Site-2-Site VPN stands for_____ .

A. Virtual Tunnel Interface

B. VPN Transfer Interface

C. Virtual Transfer Interface

D. VPN Tunnel Interface

Suggested Answer: *A*

Community vote distribution

A (100%)

greeklover84 3 weeks, 1 day ago

Selected Answer: A

no doubt. A.

upvoted 1 times

Question #11 *Topic 1*

Alice & Bob are tasked to integrate a Check Point IPSEC VPN Solution. Which of the following statements is true?

A. Confidentiality - Uses standard authentication methods

B. Integrity - All VPN data is encrypted

C. Authenticity - All VPN data is encrypted

D. Confidentiality - All VPN data is encrypted

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

In the Management HA environment how many synchronization methods are supported?

A. 1

B. 4

C. 3

D. 2

Suggested Answer: *D*

Community vote distribution

D (100%)

57433db 2 months, 3 weeks ago

Selected Answer: D

Automatic and manual synchronization

upvoted 2 times

Question #13 *Topic 1*

Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently in “Active” state. Alice uses the Check Point SmartConsole tool. Which Check Point Console is needed to lookup for the Management High Availability status?

A. SmartView Tracker -> Log Search “Mgmt HA Status”

B. SmartUpdate -> Package Repository -> Management High Availability

C. Gaia Portal -> Overall View -> Management High Availability

D. Check Point SmartConsole -> Applications Menu -> Management High Availability

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

What is collision mode in Management HA?

A. This situation is with two Management Servers - 1st set as Active, 2nd set as Standby

B. This situation is with three Management Servers - 1st set as Active, 2nd and 3rd set as Standby

C. This situation is with two Management Servers - 1st set as Standby, 2nd set as Standby

D. This situation is with two Management Servers - both set as Active

Suggested Answer: *D*

Community vote distribution

D (100%)

greeklover84 3 weeks, 1 day ago

Selected Answer: D

yes both think are Primary.

upvoted 1 times

Question #15 *Topic 1*

When it comes to manual synchronization, what statement is true?

A. You can only initiate a Full Synchronization via Manual Sync.

B. You can only initiate a Delta Synchronization via Manual Sync.

C. You can choose whether to perform a Full Sync or Delta Sync when it comes to do a Manual Sync.

D. Manual Sync is only done at the very beginning to force a Cluster Join after having installed the Secondary Management Server.

Suggested Answer: *C*

Community vote distribution

A (100%)

Armrest9955 1 month, 1 week ago

Selected Answer: A

Manual synchronization is a full synchronization that overwrites all data on the peers.

Best Practice - Use this option with caution, and only in cases of synchronization error. We recommend that you publish changes before initiating full sync.

upvoted 1 times

9dfb7ac 3 months ago

Selected Answer: A

manual sync always performs a full database synchronisation

upvoted 3 times

Question #16 *Topic 1*

Network Feed objects are used as a Source or Destination in Access Control, HTTPS Inspection, and Threat Prevention Policies. What file formats are supported for download in Network Feed objects?

A. Flat list only

B. Flat list and XML

C. JSON only

D. Flat list or JSON

Suggested Answer: *D*

Community vote distribution

D (100%)

Armrest9955 1 month, 1 week ago

Selected Answer: D

Flat list and JSON

upvoted 1 times

03e280a 2 months, 2 weeks ago

Selected Answer: D

Format - Configure the content structure in the feed, so the Security Gateway knows how to parse the feed. The supported formats are Flat list and JSON.

upvoted 1 times

Question #17 *Topic 1*

During Conversion of the Security Policy, the compiled code is stored in which directory?

A. In the $FWDIR/state/<Gateway Name>/FW1 directory of the Gateway

B. In the /etc/fw.boot/modules/ Directory of the Management Server.

C. In the $FWDIR/state/<Gateway Name>/FW1 directory of the Management Server

D. In the $CPDIR/state/<Gateway Name>/FW1 directory of the Management Server

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

When installing policy, which process is responsible for Verification / conversion?

A. CPD

B. CPM

C. FWM

D. FWD

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

When the CPM process does a Modern Dump, what is happening?

A. CPM is using a new version of Postgre SQL to optimize the policy installation, and allow it to happen faster.

B. When doing backups in Gaia CPM uses Modern Dump and is able to export the database faster in R8x version than previous versions.

C. Using pre-generated code does not require further compilation or verification before transfer to the Security Gateway.

D. CPM can bypass FWM and install updated and new rules directly to the Security Gateway.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

In Management HA the failover is:

A. Always manual

B. Automatic by default, but can be changed to manual

C. Manual by default, can be changed to automatic

D. Always automatic

Suggested Answer: *C*

Armrest9955 1 month, 1 week ago

Selected Answer: A

PG 24 Failover is Manual

upvoted 1 times

9dfb7ac 3 months ago

Selected Answer: A

Failover in Check Point Management HA is always manual

upvoted 3 times

Question #21 *Topic 1*

Which process is responsible for the code generation and compilation of legacy dump files?

A. FWM

B. CPM

C. Stateful Compiler

D. Inspect Engine

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

To which directory does CPTA transfer policy files to the Security Gateway?

A. $FWDIR/state/_tmp/FW1

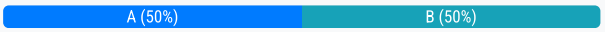
B. $FWDIR/state/local/FW1

C. $CPDIR/state/tmp/FW1

D. $FWDIR/state/_tmp/FW1

Suggested Answer: *A*

Community vote distribution



Armrest9955 1 month, 1 week ago

Selected Answer: A

It Transfers to $FWDIR/state/__tmp/FW1, Note its double _ After installation its stored in $FWDIR/state/local/FW1

upvoted 2 times

besik 1 week, 4 days ago

I agree also it is saying transfer

1. CPM → receives install request
2. FWM → verifies + compiles
3. CPTA → transfers files to gateway
4. CPD → receives files
5. Files stored temporarily in:

$FWDIR/state/_tmp/FW1

6. CPD runs fw fetchlocal → loads policy
7. Files copied to:

$FWDIR/state/local/FW1

upvoted 1 times

03e280a 2 months, 2 weeks ago

Selected Answer: B

Security Gateway, or Cluster Member stores the installed Access Control Policy in these directories:

$FWDIR/state/__tmp/FW1/

$FWDIR/state/local/FW1/

$FWDIR/state/<Name of Cluster Object>/FW1/

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_CLI_ReferenceGuide/208173

upvoted 2 times

Question #23 *Topic 1*

Which part of the installation process is responsible for checking potential conflict between rules?

A. verification

B. legacy dump

C. transfer

D. conversion

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

During the policy installation, the CPM process needs to make a decision for Full Installation Policy or Fast Installation Policy. Depending on the decision the CPM process decides what kind of dump will be used. Which statement is true for the Fast Installation Policy?

A. Modern Dump always combines the Legacy Dump in which the pre-verified and pre-generated code is included

B. Modern Dump files never include the pre-verified and pre-generated code

C. Modern Dump files are sent to the FWM (Firewall) process, which is responsible for code generation and compilation

D. Modern Dump files already include the pre-verified and pre-generated code

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which daemon makes the decision if Modern Dump or Legacy Dump should be used during Policy Installation?

A. FWM (Firewall Management)

B. CPTA (Check Point Transfer Agent)

C. CPD (Check Point Daemon)

D. CPM (Check Point Management)

Suggested Answer: *D*

Community vote distribution

A (100%)

greeklover84 3 weeks ago

Selected Answer: A

The FWM (Firewall Management) daemon on the Check Point Management Server is responsible for managing the policy database, converting it, and determining whether to use a "Modern Dump" (new format) or "Legacy Dump" (old format) during the policy installation process.

upvoted 1 times

Question #26 *Topic 1*

What is crucial in translating services (destination ports) in a NAT rule?

A. This can only be accomplished with the Automatic NAT Rule with “Translate Destination on Server Side” enabled

B. This can only be accomplished with Automatic NAT Rule in conjunction with Bi-Directional NAT

C. This can only be accomplished with the Automatic NAT Rule with “Automatic ARP Configuration” enabled.

D. This has to be done with a Manual NAT Rule.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

What does the CPTA (Check Point Transfer Agent) do?

A. CPTA communicates with the ThreatCloud to transfer anonymized attack log data and download new signatures.

B. CPTA transfers the policy files from the Security Management Server to the Security Gateway for policy installation.

C. CPTA is the agent built into Gaia that downloads new software updates, including JHFAs and major version installation packages.

D. CPTA is the process that finds and downloads licenses and contracts from the UserCenter to the Security Management Server.

Suggested Answer: *B*

Community vote distribution

B (100%)

greeklover84 3 weeks ago

Selected Answer: B

The Check Point Transfer Agent (CPTA) is a specialized component within the Check Point management architecture responsible for securely transferring compiled security policies from the Management Server to target Security Gateways.

upvoted 1 times

Question #28 *Topic 1*

Which Management Server Process receives an install command if it comes to install a policy?

A. The CPM process is involved in installing a policy to the gateway.

B. The CPWD process invokes the install function.

C. The FWM process is involved in installing the policy.

D. The FWD process is involved in installing a policy.

Suggested Answer: *A*

Chikku221 1 week, 5 days ago

Selected Answer: A

Phase 1clearly mentioned the statement The CPM process on the security management server receives an installed command .

upvoted 2 times

besik 1 week, 4 days ago

I agree

1. SmartConsole → sends install command
2. CPM → receives the command
3. CPM → forwards to FWM
4. FWM → verification + compilation
5. CPTA → transfer
6. CPD → receives on gateway

upvoted 1 times

Armrest9955 1 month, 1 week ago

Selected Answer: C

Phase 4 of policy installation pg 89

upvoted 1 times

9dfb7ac 3 months ago

Selected Answer: C

fwm (Firewall Management Process)

upvoted 2 times

Question #29 *Topic 1*

According to the policy installation flow, the transfer state (CPTA) is invoked by the FWM (Firewall) process which initiates the Transfer/Commit phase. On the Security Gateway side a process receives them and first stores them into a temporary directory. Which directory for the Transfer is correct for receiving these files?

A. $FWDIR/state/local/FW1

B. $FWDIR/state/_tmp/FW1

C. $FWDIR/state/_tmp/FW-1

D. $CPDIR/state/_tmp/FWM1

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Which Management Server is Primary?

A. It's the Management Server with the highest firmware version and JHF

B. It's the current Active Management Server

C. It's the every Management Server that is not Standby

D. It's the first installed Management Server

Suggested Answer: *D*

Community vote distribution

D (100%)

greeklover84 3 weeks ago

Selected Answer: D

Key Aspects of the Primary Management Server:

- Installation Order: It is defined during the initial installation.

- Active Role: While either server can act as "Active" or "Standby," the Primary acts as the synchronization master.

- Synchronization: If the primary is down, secondary servers cannot synchronize databases until one is promoted to primary.

- Changeover: Switching from primary to secondary is manual, not automatic.

upvoted 1 times

Question #31 *Topic 1*

In Management HA, changes in policy and object are performed through the active server. What happens if the active server fails or is taken offline?

A. One of the standby servers must be promoted to Primary Management Server to make it active

B. The standby server with the highest priority set by the administrator automatically becomes active

C. A changeover can be initiated manually to make a standby server become active

D. The closest standby server will immediately become active within 3 seconds

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

According to the policy installation, the transfer state (CPTA) is invoked by the FWM (Firewall) process which initiates the Transfer/Commit phase. On the Security Gateway side a process receives them and first stores them into a temporary directory. Which process is true for receiving these files?

A. FWD

B. CPD

C. FWM

D. RAD

Suggested Answer: *A*

Community vote distribution

B (100%)

Armrest9955 1 month, 1 week ago

Selected Answer: B

The CPD (CheckPoint Daemon) process stores the files in a temporary directory on the SecurityGateway:$FWDIR/state/__tmp/FW1 (two underscores)

upvoted 1 times

dustinsach 2 months, 3 weeks ago

Selected Answer: B

See page 89 CCSE Book

upvoted 4 times

Question #33 *Topic 1*

Alice & Bob are concurrently logged in to the SmartConsole under Logs & Servers to check for the IKE “Key Install” between a working VPN Site-to-Site Tunnel between site Alpha and site Bravo. Which of the following IKE versions are available?

A. IKE

B. IKEv1 & IKEv3

C. IKEv1 & IKEv2

D. IKEv2 & IKEv4

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Internet Key Exchange (IKE) a standard key management protocol that is used to do what exactly?

A. Renew both Phase 1 and Phase 2 IPSec keys when they expire.

B. Renew the Phase 2 key when it expires, after 60 minutes by default.

C. Update the VPN Domain information and renew expired keys when they expire.

D. Create the VPN tunnels by, Authenticating peers, agreeing on keys and methods to be used for encryption.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

Can a VPN Gateway be a member of more than one VPN community?

A. No, it could be used only in one VPN Community.

B. Yes, it is possible, but with correct modifications of vpn_route.conf file on each VPN Gateway

C. Yes, if it doesn't pair with another VPN Gateway in more than one VPN Community.

D. Yes, it could be used in more than one VPN Community, if all VPN Gateways are managed with the same Security Management.

Suggested Answer: *D*

Community vote distribution

C (100%)

dustinsach 2 months, 3 weeks ago

Selected Answer: C

See page 195 CCSEbook

upvoted 4 times

Question #36 *Topic 1*

What is true regarding the number of involved Management Servers in a Management HA environment?

A. You can have one Primary Management Server and one or more Secondary Management Server(s).

B. You can have multiple Primary Management Servers in a Load Sharing Mode HA Environment.

C. You can have one Primary Management Server and one Secondary Management Server.

D. You can have multiple Primary Management Servers behind a Load Balancer, such as the Logical Server, but in this scenario, you can only use Round Robin as the Distribution Mechanism.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

To form a tunnel IKEv2 uses two exchange types - IKE_SA_INIT and IKE_AUTH. How many packets are transferred between the VPN peer gateways during the two exchanges?

A. Each exchange involves two messages, making a total of 4 packets.

B. For a site-to-site VPN on Check Point using IKEv2, the normal exchange is indeed nine packets

C. 9 packets unless legacy peers are included in the VPN community, which uses just 6 packets, 3 per exchange.

D. 6 packets. There are 4 in the SA_INIT exchange because of the Diffie Hellman process.

Suggested Answer: *A*

Community vote distribution

A (100%)

greeklover84 3 weeks ago

Selected Answer: A

A is correct. no doubt !!!

upvoted 1 times

Question #38 *Topic 1*

The Gateways has to mutually authenticate during the IPSec negotiation phase. There are two methods for this, namely:

A. Pre-shared secret and PKI Certificate

B. Kerberos and LDAP

C. OCSP and Certificate Revocation List

D. RSA SecurID and Dynamic ID

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

When a solution is configured with Route-based VPN method what interfaces are used?

A. The Gaia Portal Web User Interface (WebUI)

B. Only the internal interfaces, which are included in a special Route-based Domain (Network Group object).

C. Virtual Tunnel Interfaces (VTI)

D. External interface with a secondary IP address

Suggested Answer: *C*

Community vote distribution

C (100%)

greeklover84 3 weeks ago

Selected Answer: C

Yes C. no doubt.

upvoted 1 times

Question #40 *Topic 1*

When creating a VPN tunnel with a third party product which object should you create in Smart Console to represent the remote side?

A. Externally Managed VPN Gateway

B. Gateway

C. Host

D. Interoperable Object

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

How many packets are used in Aggressive Mode for negotiation?

A. 3

B. 4

C. 8

D. 6

Suggested Answer: *A*

Community vote distribution

A (100%)

Armrest9955 1 month, 1 week ago

Selected Answer: A

Main Mode uses 6 packets Aggressive mode uses 3 packets

upvoted 1 times

Question #42 *Topic 1*

Any VPN Gateway that can establish a direct VPN Tunnel with any Peer Gateway is member of which VPN Community

A. Direct Community

B. Any Community

C. Star Community

D. Mesh Community

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Where can Firewall administrator configure VPN routes between Security Gateways?

A. vpn_route.conf (on Security Management)

B. via Gaia Portal or CLI (on Security Gateway)

C. VTI_route.conf (on Security Management)

D. vpn_route.conf (on Security Gateway)

Suggested Answer: *D*

Community vote distribution

A (100%)

Armrest9955 1 month, 1 week ago

Selected Answer: A

You can also configure VPN routing between Security Gateways in the correspondingvpn_route.conf file that is configured on the Management Server.

upvoted 1 times

dustinsach 2 months, 3 weeks ago

Selected Answer: A

You can also configure VPN routing between Security Ga teways in the corresponding vpn_route.conf file that is configured on the Management Server.

upvoted 3 times

Question #44 *Topic 1*

Choose the correct object name for a third-Party (Non-Check Point) IPSec VPN device.

A. External Device

B. External Gateway

C. Interoperable Device

D. 3rd-Party Device

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

How many packets are used in IKEv1 Phase1 Main Mode exchange?

A. 6

B. 5

C. 8

D. 3

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

Which of the following is a trigger for synchronization between Active and Standby Management Servers?

A. Publishing a session in SmartConsole

B. Making a change in a network object and clicking on OK

C. Running the Save operation from the SmartConsole toolbar or Menu

D. After 10 seconds of inactivity in SmartConsole

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

The IPSec VPN solution lets the Security Gateway encrypt and decrypt traffic to and from other Security Gateways and client. The VPN tunnel guarantees:

A. Confidentiality, Identity and Authenticity

B. Confidentiality, Identity and Availability

C. Confidentiality, Integrity and Authenticity

D. Confidentiality, Integrity and Availability

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

Under which circumstances are automatic scans performed for Continuous Compliance Monitoring?

A. Every time the CPM and CPD process was restarted.

B. Every time the FWD or CPM service on the gateway was restarted.

C. Daily and SmartConsole changes with the Publish action.

D. Daily and weekly.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

How does SmartEvent determine whether events originated internally or externally?

A. By defining the Internal Network under the Initial Settings in SmartEvent GUI Client

B. Events with a non-routable private source IPs are considered to be originating from internal networks

C. SmartEvent queries Security Gateway topology to determining the direction of events

D. SmartEvent uses AI / ML to determine the direction of events

Suggested Answer: *C*

Community vote distribution

A (100%)

dustinsach 2 months, 3 weeks ago

Selected Answer: A

See page 242

Internal Network - Define the Internal Netw ork to help SmartEvent determine whether events have originated inte rnally or externally.

upvoted 3 times

Question #50 *Topic 1*

Select the most appropriate statement regarding the Management HA Solution.

A. After installing the Primary Management Server, one or more Secondary Management Servers may be installed for redundancy and database backup

B. After installing the Primary Management Server, only one Secondary Management Server can be deployed in the same environment

C. The Management Server which is nearest to a Security Gateway becomes its Primary Management Server

D. A Management Server running in the Active mode is called the Primary Management Server

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!