Question #1 *Topic 1*

Choose the correct syntax to add a new host named “emailserver1” with IP address 10.50.23.90 using GAiA Management CLI?

A. mgmt._cli add host name “emailserver1” ip-address 10.50.23.90

B. mgmt._cli add host “emailserver1” address 10.50.23.90

C. mgmt._cli add host name “myHost12 ip” address 10.50.23.90

D. mgmt._cli add host name ip-address 10.50.23.90

Correct Answer: *A*

Community vote distribution

Community vote distribution

Ziamsu 5 months, 2 weeks ago

A is the closest correct syntex is > mgmt_cli add host name "emailserver1" ip-address "10.50.23.90"

upvoted 2 times

Jallic 8 months, 4 weeks ago

I would pick A, however the commant is 'mgmt_cli' not 'mgmt._cli'

upvoted 1 times

jerj5 9 months ago

Selected Answer: A

Correct answer, there is a similar example in the Student Manual on page 47.

Remember that this command is executed in Expert mode

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

A - mgmt_cli add host name "emailserver1" ip-address 10.50.23.90 - Correct

upvoted 2 times

Question #2 *Topic 1*

Which method below is NOT one of the ways to communicate using the Management API's?

A. Typing API commands using Gaia's secure shell (clish)

B. Typing API commands from a dialog box inside the SmartConsole GUI application

C. Sending API commands over an http connection using web-services

D. Typing API commands using the "mgmt._cli" command

Correct Answer: *C*

Community vote distribution

Community vote distribution

yeru 4 months, 1 week ago

Using the Management APIs

There are four ways to communicate use the management APIs:

Typing API commands from a dialog inside the SmartConsole GUI application.

Typing API commands using the "mgmt_cli" executable (available in both Windows, Linux/Gaia flavors).

Typing API commands using Gaia's secure shell (clish).

Sending API commands over an https connection using web-services

upvoted 1 times

nmelay 5 months, 1 week ago

Oh, you actually can.

upvoted 1 times

nmelay 5 months, 1 week ago

Selected Answer: A

You can't send API commands from clish.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

" C " , https not http for webservices.

upvoted 1 times

winners12 7 months ago

the answer is C

Sending API commands over an https connection using web-services

upvoted 1 times

andymbase 8 months ago

Selected Answer: C

HTTPS not HTTP

upvoted 2 times

8202009 8 months, 3 weeks ago

Selected Answer: C

La opcion correcta es C

Using the Management APIs

There are four ways to communicate use the management APIs:

Typing API commands from a dialog inside the SmartConsole GUI application.

Typing API commands using the "mgmt_cli" executable (available in both Windows, Linux/Gaia flavors).

Typing API commands using Gaia's secure shell (clish).
Sending API commands over an https connection using web-services
upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

Correct answer is C, this is because API commands are sent over HTTPS(443) and not HTTP(80)

There are four ways to communicate use the management APIs:
Typing API commands from a dialog inside the SmartConsole GUI application.
Typing API commands using the "mgmt_cli" executable (available in both Windows, Linux/Gaia flavors).
Typing API commands using Gaia's secure shell (clish).
Sending API commands over an https connection using web-services
upvoted 3 times

Rajeshkashi 9 months, 2 weeks ago

answer is C
upvoted 2 times

Question #3 *Topic 1*

Which of the following is NOT a type of Check Point API available in R80.x?

A. Identity Awareness Web Services

B. OPSEC SDK

C. Management

D. Mobile Access

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: D

The available types of Check Point APIs in R80.x include Identity Awareness Web Services, OPSEC SDK, and Management. Mobile Access is not listed as a type of Check Point API in R80.x.

upvoted 1 times

Jallic 2 months, 1 week ago

Selected Answer: B

https://support.checkpoint.com/results/sk/sk63026

Check Point's OPSEC (Open Platform for Security) integrates and manages all of network security through an open, extensible management framework. Third party security applications can plug into the OPSEC framework via published application programming interfaces (APIs). Once integrated into the OPSEC framework, applications can be configured and managed from a central point, utilizing a single Security Policy editor.

https://sc1.checkpoint.com/documents/latest/api_reference/index.html#
Quantum:
Management API
Identity Awareness API

Harmony:
Harmony Mobile API

I believe the answer here is OPSEC SDK.

upvoted 1 times

mostafa10 2 months, 3 weeks ago

Selected Answer: B

No OPSEC API,
https://sc1.checkpoint.com/documents/latest/api_reference/index.html

upvoted 1 times

chaosisgod 2 months, 3 weeks ago

Selected Answer: D

http://supportcontent.checkpoint.com/solutions?id=sk63026.

upvoted 1 times

Hssilva 2 months, 3 weeks ago

Selected Answer: D

https://support.checkpoint.com/results/sk/sk63026

upvoted 1 times

pabloakd19 3 months ago

Selected Answer: B

OPSEC SDK is the correct answer

upvoted 1 times

JM1 4 months, 2 weeks ago

There is a Harmony Mobile API in R81.20. The correct answer is OPSEC SDK - Answer B.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

B . Starting from R80, OPSEC CPMI commands are considered deprecated and are being replaced by new set of APIs.

upvoted 2 times

cristip 6 months, 1 week ago

Selected Answer: D

For sure it is D

upvoted 2 times

Gme36 7 months ago

The Correct Answer is B. OPSEC SDK is not a type of checkpoint API. Rather, it integrates and manages all of network security through an open, extensible management framework

upvoted 1 times

Question #4 *Topic 1*

What API command below creates a new host object with the name “My Host” and IP address of “192.168.0.10”?

A. set host name “My Host” ip-address “192.168.0.10”

B. create host name “My Host” ip-address “192.168.0.10”

C. new host name “My Host” ip-address “192.168.0.10”

D. mgmt_cli –m <mgmt ip> add host name “My Host” ip-address “192.168.0.10”

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

ias253 4 months ago

D is correct

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Correct Answer is D , https://sc1.checkpoint.com/documents/latest/APIs/index.html#cli/add-host~v1.9.1%20

upvoted 2 times

david_vera 8 months, 1 week ago

Selected Answer: D

according to chatgpt, claude and perplexity is d

upvoted 1 times

8202009 8 months, 2 weeks ago

Selected Answer: D

answer is D

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

D is correct answer

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

answer D

upvoted 1 times

Question #5 *Topic 1*

What command verifies that the API server is responding?

A. api stat

B. show api_status

C. api_get_status

D. api status

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

[Expert@CP-FW03:0]#
[Expert@CP-FW03:0]# api status

API Settings:

Accessibility: Require all granted
Automatic Start: Unknown

Processes:

Name State PID More Information

API Stopped 6564
CPM Starting 6564 Check Point Security Management Server is during initialization
FWM Started 6069
APACHE Started 7348
upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

You don't have to be in export mode to run the command api status.
To verify that the API server is running, run the following command in Expert mode:
api status
To start the API server, run the following command in Expert mode:
api start
To stop the API server, run the following command in Expert mode:
api stop
upvoted 3 times

Question #6 *Topic 1*

What are the different command sources that allow you to communicate with the API server?

A. API_cli Tool, Gaia CLI, Web Services

B. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services

C. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services

D. SmartConsole GUI Console, mgmt._cli Tool, Gaia CLI, Web Services

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

D , https://sc1.checkpoint.com/documents/latest/APIs/#introduction~v1.9.1%20

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

There are four ways to communicate use the management APIs:

Typing API commands from a dialog inside the SmartConsole GUI application.

Typing API commands using the "mgmt_cli" executable (available in both Windows, Linux/Gaia flavors).

Typing API commands using Gaia's secure shell (clish).

Sending API commands over an https connection using web-services

upvoted 1 times

Question #7 *Topic 1*

Alice works for a big security outsourcing provider company and as she receives a lot of change requests per day she wants to use for scripting daily tasks the API services from Check Point for the Management API. Firstly, she needs to be aware if the API services are running for the management. Which of the following Check Point Command is true:

A. status mgmt api

B. api mgmt status.

C. status api

D. api status

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Answer is D

[Expert@CP-FW03:0]# api status

API Settings:

Accessibility: Require all granted
Automatic Start: Enabled

Processes:

Name State PID More Information

API Started 6564
CPM Started 6564 Check Point Security Management Server is running and ready
FWM Started 6069
APACHE Started 7348

upvoted 2 times

david_vera 8 months, 1 week ago

Selected Answer: D

correct d

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

correct

upvoted 1 times

Question #8 *Topic 1*

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

A. Security Gateway failover as well as Security Management Server failover is an automatic procedure.

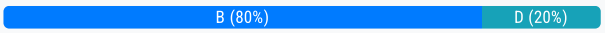
B. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.

C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.

D. Security Gateway failover as well as Security Management Server failover is a manual procedure.

Correct Answer: *B*

Community vote distribution



Community vote distribution

CheckpointMaster 2 months, 2 weeks ago

Selected Answer: B

does anyone know if these dumps are valid for the exam given the amount of question that are on this site and that the R8.20 is new ?

upvoted 1 times

57ad24d 3 months, 1 week ago

Selected Answer: B

In a Check Point environment:

Security Gateway Failover: This is typically an automatic procedure. When a Security Gateway fails or becomes unavailable, the control over traffic is automatically transferred to another active member in the cluster based on internal cluster algorithms. This ensures high availability and minimal disruption in service.

Security Management Server Failover: This process is manual. If the active Security Management Server fails or needs to be changed to standby, an administrator must manually initiate the changeover. The active server synchronizes with the standby server at intervals, but the changeover itself does not happen automatically.

For more detailed information, you can refer to the following sources:

R82 Security Management Administration Guide - Changeover Between Active and Standby

R82 ClusterXL Administration Guide - Initiating Manual Cluster Failover

upvoted 3 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Changeover between the primary (active) and secondary (standby) management server is not automatic. If the Active fails or it is necessary to change the Active to a Standby, you must do this manually. When the management server becomes Standby it becomes Read Only, and gets all changes from the new Active server.

upvoted 2 times

Ziamsu 5 months, 2 weeks ago

Answer is B > If the Active server fails, you can initiate a changeover to make a Standby server become the Active server.

Ref:https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_SecurityManagement_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_SecurityManagement_AdminGuide/161279

upvoted 1 times

paozinho 7 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

LocoDuck 8 months, 1 week ago

B is correct

upvoted 1 times

david_vera 8 months, 1 week ago

Selected Answer: D

According to chatgpt and claude is right.

upvoted 1 times

c0be09e 8 months ago

I think you asked ChatGPT the wrong question 'cause firewall failover is automatic. It wouldn't be logical to have a manual HA solution for them

upvoted 1 times

david_vera 7 months, 4 weeks ago

It's right. It has no sense that gateways is not automatic. IA's are not always trust sources. I just paste the same question and anwers.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

Correct

upvoted 1 times

Question #9 *Topic 1*

What is the most ideal Synchronization Status for Security Management Server High Availability deployment?

A. Never been synchronized

B. Collision

C. Synchronized

D. Lagging

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: C

This status indicates that the peer Security Management Servers are correctly synchronized and have the same database information and installed Security Policy.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Synchronized

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

Correct

upvoted 2 times

Question #10 *Topic 1*

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

A. Lagging

B. Never been synchronized

C. Collision

D. Synchronized

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

57ad24d 3 months, 1 week ago

Selected Answer: C

When both members of a Management High Availability (HA) setup have different policies or databases, the state is referred to as "Collision." In this state, both the Active and Standby Management Servers have different installed Security Policies and databases, which can lead to synchronization issues.

To resolve this, the administrator must perform a manual synchronization and decide which of the Security Management Servers to overwrite.

upvoted 2 times

ias253 4 months ago

Selected Answer: C

correct answer is collision

upvoted 1 times

Kenny4275 4 months, 2 weeks ago

Correct Answer is A.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

Correct

upvoted 1 times

Question #11 *Topic 1*

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

A. cpd

B. fwd

C. cpwd

D. fwm

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: D

The "fwm" process is the main process for the Security Management Server.

upvoted 1 times

Kenny4275 4 months, 2 weeks ago

Selected Answer: D

FWM and CPM are management only processes

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

D - FWM - Legacy Check Point management server main process (R77.x and earlier)

upvoted 1 times

LocoDuck 8 months, 1 week ago

Selected Answer: D

Correct

upvoted 1 times

david_vera 8 months, 1 week ago

Selected Answer: D

is right answer

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

FWM correct

upvoted 1 times

Question #12 *Topic 1*

What is the command used to activate Multi-Version Cluster mode?

A. set mvc on in Clish

B. set cluster member mvc on in Clish

C. set cluster mvc on in Expert Mode

D. set cluster MVC on in Expert Mode

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: B

B. set cluster member mvc on in Clish

In Expert Mode, the equivalent command is:
cphaconf mvc on
upvoted 1 times

iulianm 5 months, 1 week ago

B is correct:
upvoted 1 times

Ziamsu 5 months, 2 weeks ago

B

CP-FW03> set cluster member mvc on
Enables (on; default setting) / Disables (off) Multi-Version cluster on this cluster member.

CP-FW03> set cluster member mvc on
upvoted 2 times

jerj5 9 months ago

Selected Answer: B

Correct answer
MVC is disabled by default
Check State of MVC
Gaia Clish: show cluster members mvc
Enable MVC
Gaia Clish: set cluster member mvc on
upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

Correct

Shell Command
Gaia Clish set cluster member mvc {off | on}
Expert mode cphaconf mvc {off | on}
upvoted 1 times

Question #13 *Topic 1*

How many versions, besides the destination version, are supported in a Multi-Version Cluster Upgrade?

A. 4

B. 3

C. 2

D. 1

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: D

In a Multi-Version Cluster, the Cluster Members can run only the destination version and one other version. For example, if the destination version is R81, the other version can be R77.30, R80.10, R80.20, etc.

upvoted 1 times

premoli 3 months, 3 weeks ago

Selected Answer: D

Supported Versions in Multi-Version Cluster

The Multi-Version ClusterClosed (MVC) in an R81 Cluster MemberClosed supports synchronization with peer Cluster Members that run one of these versions:

R80.10 (or higher)*

R77.30

In a Multi-Version Cluster, the Cluster Members can run only these versions:

R81 and R80.10 (or higher)*

R81 and R77.30

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

D is correct

upvoted 1 times

cristip 6 months ago

Selected Answer: D

I think its D

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

correct

1

"Version X" is allowed to be only one of these: R77.30, R80.10, R80.20, and so on.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/MVC-Upgrade-Supported-

Versions.htm
so due to "besides the destination version" 1 other version is correct
upvoted 3 times

Question #14 *Topic 1*

Which upgrade method you should use upgrading from R80.40 to R81.20 to avoid any downtime?

A. Multi-Version Cluster Upgrade (MVC)

B. Zero Downtime Upgrade (ZDU)

C. Connectivity Upgrade (CU)

D. Minimal Effort Upgrade (ME)

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: A

The Multi-Version Cluster (MVC) upgrade method ensures that there is no loss in connectivity and no downtime during the upgrade process.

upvoted 1 times

ias253 4 months ago

Selected Answer: A

correct

upvoted 1 times

ias253 4 months ago

it's A

upvoted 1 times

57ad24d 5 months ago

Selected Answer: A

Multi-Version Cluster Upgrade (MVC)

This method ensures that there is no downtime by upgrading one cluster member at a time while the other continues to handle traffic, avoiding any disruption.

upvoted 3 times

Ziamsu 5 months, 2 weeks ago

A is correct

MVC - Select this method, if connectivity is of utmost concern.

Connection failover is guaranteed - no connections are dropped.

upvoted 1 times

LocoDuck 8 months, 3 weeks ago

A is correct

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

correct

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

Answer is A

upvoted 3 times

Question #15 *Topic 1*

What are the main stages of a policy installation?

A. Initiation, Conversion and Save

B. Initiation, Conversion and FWD REXEC

C. Verification, Commit, Installation

D. Verification, Compilation, Transfer and Commit

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

ias253 4 months ago

Selected Answer: D

correct

upvoted 1 times

57ad24d 5 months ago

Selected Answer: D

D. Verification, Compilation, Transfer and Commit

These are the main stages of a policy installation in Check Point:

Verification: The policy is checked for errors or conflicts.
Compilation: The policy is compiled into a format that can be executed by the security gateways.
Transfer: The compiled policy is transferred to the gateways.
Commit: The policy is committed and enforced on the gateways.

upvoted 3 times

Ziamsu 5 months, 2 weeks ago

https://community.checkpoint.com/t5/Management/Policy-Installation-Stages/td-p/23105

upvoted 2 times

Question #16 *Topic 1*

What are valid Policy Types in R81.X?

A. Access Control, Threat Prevention, QoS, Desktop Security

B. Access Control, IPS, Threat Emulation, NAT

C. Access Control, IPS, QoS, DLP

D. Access Control, RemoteAccess VPN, NAT, IPS

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: A

A. Access Control, Threat Prevention, QoS, Desktop Security

This includes:

Access Control: Manages access to network resources.
Threat Prevention: Protects against various threats such as malware, botnets, and intrusions.
QoS (Quality of Service): Manages bandwidth and prioritizes network traffic.
Desktop Security: Provides security for endpoint devices.

upvoted 1 times

57ad24d 5 months ago

Selected Answer: A

A. Access Control, Threat Prevention, QoS, Desktop Security

These are the valid policy types in Check Point R81.X:

Access Control: Manages the rules governing access to network resources.
Threat Prevention: Includes security features like IPS, Anti-Bot, Anti-Virus, and Threat Emulation.
QoS (Quality of Service): Manages network traffic prioritization.
Desktop Security: Provides security for endpoint devices.

upvoted 4 times

Ziamsu 5 months, 2 weeks ago

Correct A

upvoted 1 times

jerj5 9 months ago

Selected Answer: A

Correct A
Policy packages are logical grouping of one or more of these policy types:
Access Control
QoS
Desktop Security
Threat Prevention

upvoted 3 times

Question #17 *Topic 1*

After some changes in the firewall policy, you run into some issues. You want to test if the policy from two weeks ago has the same issue. You don't want to lose the changes from the last weeks. What is the best way to do it?

A. In SmartConsole under Security Policies go to the Installation History view of the Gateway, select the policy version from two weeks ago and press the 'Install specific version' button

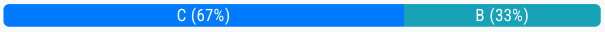
B. Use the Gaia WebUI to take a backup of the Gateway. In SmartConsole under Security Policies go to the Installation History view of the Gateway, select the policy version from two weeks ago and press the 'Install specific version' button

C. In SmartConsole under Manage & Settings go to Sessions –> Revisions and select the revision from two weeks ago. Run the action 'Revert to this revision...'.

D. Use the Gaia WebUI to take a snapshot of management. In the In SmartConsole under Manage & Settings go to Sessions -> Revisions and select the revision from two weeks ago. Run the action 'Revert to this revision...' Restore the management snapshot.

Correct Answer: *A*

Community vote distribution



Community vote distribution

krzaki 3 days, 20 hours ago

Selected Answer: A

Policy Installation History
In the Installation History you can choose a Security Gateway, a date and time when the Policy was installed, and:
See the revisions that were installed on the Security Gateway and who installed the Policy.
See the changes that were installed and who made the changes.
Revert to a specific version, and install the last "good" Policy.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Policy-Installation-History.htm

in oppose to DB revisions
Reverting to a previous revision is an irreversible operation, newer revisions than the target revision are lost.
upvoted 1 times

keikei1228 3 weeks, 6 days ago

Selected Answer: A

This approach allows you to install a specific version of the policy on the gateway without reverting the entire management database, thus preserving the changes made in the last weeks.
upvoted 1 times

bbend 1 month, 3 weeks ago

Selected Answer: A

The best way to test if the policy from two weeks ago have the same issue is to install the specific version of the policy from the installation history view of the gateway. This way, you can keep the changes from the last weeks in the management server and revert back to them later if needed. You do not need to take a backup or a snapshot of the gateway or the management server for this purpose.
upvoted 1 times

Jallic 2 months, 1 week ago

Selected Answer: C

I don't believe the answer here is B, why..What is the point of backing up the gateway when this only holds the complied version of the policy.

I'm leaning towards C here, why...A policy has already been installed and is causing issues (There would be a revision for this), so reverting back to a policy from two weeks ago would still leave a way back to the policy currently installed.
upvoted 1 times

57ad24d 3 months, 1 week ago

Selected Answer: C

C is the correct Answer

upvoted 1 times

babochnik 2 months, 3 weeks ago

C is not correct answer

Reverting to a previous revision is an irreversible operation, newer revisions than the target revision are lost.

Correct answer A or B

upvoted 2 times

vmg83 3 months, 2 weeks ago

Selected Answer: C

C is the exact procedure

upvoted 1 times

premoli 3 months, 3 weeks ago

Selected Answer: C

Correct Answer is C , exact step in Smart console.

upvoted 1 times

premoli 3 months, 3 weeks ago

Correct Answer is C , exact step in Smart console 81.20

upvoted 1 times

Kenny4275 4 months, 2 weeks ago

Selected Answer: C

Correct answer is C

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Correct Answer is C , exact step in Smart console.

upvoted 2 times

cristip 6 months ago

Selected Answer: B

I also think it is B

upvoted 2 times

fc75833 6 months, 1 week ago

I meant C!!!

upvoted 1 times

fc75833 6 months, 1 week ago

I think its B

upvoted 2 times

Question #18 *Topic 1*

Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (ELA) services.

A. DASSERVICE

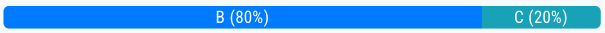
B. FWD

C. CPVIEWD

D. CPD

Correct Answer: *B*

Community vote distribution



Community vote distribution

keikei1228 3 weeks, 6 days ago

Selected Answer: B

The FWD process is responsible for forwarding logs from the Security Gateway to the Log Server, as well as providing Log Export API (LEA) and Event Logging API (ELA) services.

upvoted 1 times

Jallic 2 months, 1 week ago

Selected Answer: B

FWD (port 257) is used to send log information from the GW to SMS.

upvoted 1 times

premoli 3 months, 3 weeks ago

Selected Answer: B

Sorry, B is correct: https://support.checkpoint.com/results/sk/sk97638 fwd: On a Security Gateway - Sending the Security Logs to a Management Server / Log Server and On a Management Server - Handling connections for exporting FireWall logs using OPSEC Log Export API (LEA) products

upvoted 2 times

premoli 3 months, 3 weeks ago

Selected Answer: C

Correct Answer is C , exact step in Smart console 81.20

upvoted 1 times

Kenny4275 4 months, 2 weeks ago

Selected Answer: B

B is Correct Answer

upvoted 1 times

Ziamsu 5 months, 1 week ago

Selected Answer: B

On the SmartCenter side:

FWD listens on port 257, waiting for logs to be sent from various GWs that are connected to it.

On the GW side:
FWD opens a connection to the FWD on the log\SmartCenter server-side on port 257.
Note: In case FWD is down on either SmartCenter or the GW, logging will not work.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

B is correct, The FWD (FireWall Daemon) process main responsibility is sending and receiving the logs from the different Check Point entities to the SmartCenter\log server

upvoted 2 times

jerj5 9 months ago

Selected Answer: B

Correct

Primarily handles passing of logs from the Security Gateways to the Security Management Server, but on the Security Gateway it also acts as a parent process to many security server processes responsible for advanced inspection outside the kernel.

upvoted 1 times

Question #19 *Topic 1*

The back-end database for Check Point Management uses:

A. PostgreSQL

B. MongoDB

C. MySQL

D. DBMS

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Jallic 2 months, 1 week ago

Selected Answer: A

PostgreSQL is where all data is held. Solr is used to index information for fast recovery of data from Postgres.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

PostgreSQL

upvoted 1 times

mfhashmi 6 months, 2 weeks ago

Selected Answer: A

Correct because Solr is the enterprise search platform that handles the state-of-the-art search capabilities in SmartConsole. When a user searches for data in SmartConsole, Solr handles the request and gets the data from the PostgreSQL tables. Solr stores some partial data in a cache for better search performance.

Solr uses port 8983

Solr is deployed at $FWDIR/solr

upvoted 1 times

LocoDuck 8 months, 1 week ago

Selected Answer: A

PostgreSQL

upvoted 1 times

Question #20 *Topic 1*

Where can you see and search records of action done by R80 SmartConsole administrators?

A. In SmartAudit Log View

B. In Smartlog, all logs

C. In the Logs & Monitor, logs, select “Audit Log View”

D. In SmartView Tracker, open active log

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Correct C

upvoted 1 times

castieltel 8 months, 3 weeks ago

Selected Answer: C

Correct!

Open Audit Logs View - See and search records of actions done by SmartConsole administrators.

https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_LoggingAndMonitoring_AdminGuide/188060

upvoted 1 times

Question #21 *Topic 1*

Identity Awareness allows the Security Administrator to configure network access based on which of the following?

A. Name of the application, identity of the user, and identity of the machine

B. Identity of the machine, username, and certificate

C. Browser-Based Authentication, identity of a user, and network location

D. Network location, identity of a user, and identity of a machine

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

ias253 4 months ago

Selected Answer: D

correct

upvoted 1 times

57ad24d 5 months ago

Selected Answer: D

D. Network location, identity of a user, and identity of a machine

Identity Awareness in Check Point allows the Security Administrator to configure network access based on the user's identity (e.g., username), the machine's identity, and the network location. These factors help enforce granular access control policies based on who the user is, what device they are using, and where they are located.

upvoted 4 times

jerj5 9 months ago

Selected Answer: D

Correct

The Identity Awareness lets you easily configure network access and auditing based on network location, identity of user, and identity of the device.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

correct

upvoted 1 times

Question #22 *Topic 1*

While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

A. Security Gateway is not part of the Domain

B. SmartConsole machine is not part of the domain

C. Identity Awareness is not enabled on Global properties

D. Security Management Server is not part of the domain

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: B

When the SmartConsole machine is not part of the domain, the Identity Awareness wizard may not automatically detect the Windows domain.

upvoted 1 times

57ad24d 5 months ago

Selected Answer: B

B. SmartConsole machine is not part of the domain

The Identity Awareness wizard requires that the SmartConsole machine is part of the domain to automatically detect the Windows domain during the configuration process. If the machine running SmartConsole is not part of the domain, it won't be able to detect the domain information correctly.

upvoted 2 times

cccn714 5 months, 1 week ago

Answer is B

"If the SmartConsole computer is part of the domain, the Wizard fetches all the domain controllers of the domain and all of the domain controllers are configured."

From: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Configuring-Identity-Awareness-Enabling-Identity-Awareness-on-Security-Gateway.htm#:~:text=When%20you%20enable%20Identity%20Awareness%20Software%20Blade%20on%20a%20Security

upvoted 1 times

iulianm 5 months, 1 week ago

I think that the answer is B:

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

The answer is B. SmartConsole machine is not part of the domain.

The Identity Awareness wizard will not automatically detect the Windows domain if the SmartConsole machine is not part of the domain. The SmartConsole machine must be able to communicate with the domain controller in order to detect the domain.

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is B

upvoted 1 times

Question #23 *Topic 1*

Which of the following is NOT a method used by Identity Awareness for acquiring identity?

A. Remote Access

B. Active Directory Query

C. Cloud IdP (Identity Provider)

D. RADIUS

Correct Answer: *C*

Community vote distribution

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: C

The methods used by Identity Awareness for acquiring identity include:
- Remote Access
- Active Directory Query
- RADIUS

Cloud IdP (Identity Provider) is not listed as a method for acquiring identity in the provided documentation.

upvoted 1 times

mostafa10 2 months, 3 weeks ago

Selected Answer: C

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/CP_R81_IdentityAwareness_AdminGuide.pdf

upvoted 1 times

cccn714 5 months, 1 week ago

Selected Answer: C

Answer is C: here is a list of the Identity Provides. Cloud Idp is not listed.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Introduction-Identity-Sources.htm

upvoted 1 times

iulianm 5 months, 1 week ago

It is C: A. Remote Access: Check Point Identity Awareness can acquire user identities through Remote Access VPN connections, where users authenticate and their identities are captured.
B. Active Directory Query (AD Query): This is a common method used by Identity Awareness to query Active Directory and obtain user identities based on login information.
C. Cloud IdP (Identity Provider): While cloud-based identity providers like Azure AD or Google Identity can be integrated into broader security strategies, they are not a native method for acquiring identity directly in the Identity Awareness blade.
D. RADIUS: Identity Awareness can use RADIUS authentication to acquire identity information when users authenticate through RADIUS-based devices like Wi-Fi access points.

upvoted 2 times

Ziamsu 5 months, 2 weeks ago

Tricky one, all are correct based on this Ref:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Identity-Sources.htm?tocpath=Introduction%20to%20Identity%20Awareness%7CIdentity%20Sources%7C____1

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Only not listed is Cloud IDP, however fw can still query from Azure AD. so all are valid.

upvoted 1 times

mfhashmi 5 months, 3 weeks ago

Selected Answer: A

A. Remote Access

Explanation:
B. Active Directory Query: A method used by Identity Awareness to query Active Directory for user identity information.
C. Cloud IdP (Identity Provider): Identity Awareness can integrate with cloud identity providers to acquire identity information.
D. RADIUS: Identity Awareness supports acquiring identities through RADIUS authentication requests.
Remote Access is not a method used by Identity Awareness for acquiring identity; instead, it is a type of VPN connection. Identity Awareness focuses on acquiring user identity through integration with services like Active Directory, RADIUS, and Cloud Identity Providers (IdPs).

upvoted 1 times

Mahant 6 months ago

It should be A - Remote access

upvoted 1 times

Shruikand 9 months, 1 week ago

Selected Answer: C

Identity Provider is not part of it.

You can select remote access, ADQ,RADIUS, Terminal Servers, Browser based auth, Identity agents, web api and remote access in the settings pane of Identity Awareness

upvoted 3 times

KuKuKu83 9 months, 2 weeks ago

A - Remote access

upvoted 1 times

paozinho 6 months, 4 weeks ago

No, is C

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

Answer is C

upvoted 4 times

Question #24 *Topic 1*

Identity Awareness lets an administrator easily configure network access and auditing based on three times. Choose the correct statement.

A. Network location, the identity of a user and the identity of a machine.

B. Geographical location, the identity of a user and the identity of a machine.

C. Network location, the identity of a user and the active directory membership.

D. Network location, the telephone number of a user and the UID of a machine.

Correct Answer: *A*

Community vote distribution

Community vote distribution

57ad24d 2 months, 1 week ago

Selected Answer: A

The correct answer is:

A. Network location, the identity of a user, and the identity of a machine.

Explanation:
Check Point's Identity Awareness enables network access and auditing based on:

Network Location: Determines where the connection is originating from.
Identity of a User: Verifies the user's identity using methods such as Captive Portal, AD Query, or Multi-Factor Authentication.
Identity of a Machine: Identifies the device being used, which can include attributes such as MAC address, hostname, or certificates.
This combination allows administrators to create precise access policies and audit logs for enhanced security and compliance.

upvoted 1 times

jerj5 9 months ago

Selected Answer: A

Correct
The Identity Awareness lets you easily configure network access and auditing based on network location, identity of user, and identity of the device.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

A correct

upvoted 1 times

Question #25 *Topic 1*

Fill in the blanks. Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.

A. 443; 389

B. 636; 8080

C. 290; 3389

D. 389; 636

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: D

Port 389 is used for standard (unencrypted) LDAP connections.

Port 636 is used for LDAP over SSL (LDAPS).

upvoted 1 times

KuKuKu83 3 months, 2 weeks ago

Selected Answer: D

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for

LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS.

upvoted 3 times

Question #26 *Topic 1*

By default, what information is NOT collected from a Security Gateway in a CPINFO?

A. OS and Network Statistics

B. Configuration and database files

C. Firewall logs

D. System message logs

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

jerj5 9 months ago

Selected Answer: C

Correct

CPInfo collects the entire Security Gateway installation directory, including $FWDIR/log/* and other log files. Some other viewable information includes:

System message logs
Module version information
Installed hotfixes information
OS and network statistics
Interfaces and devices information
Various FW1 tables
Configuration and database files
Core dump files

upvoted 4 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

C correct

upvoted 3 times

Question #27 *Topic 1*

What command can you use to have cpinfo display all installed hotfixes?

A. cpinfo-hf

B. cpinfo installed_jumbo

C. cpinfo –get hf

D. cpinfo –y all

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

ias253 4 months ago

D -cpinfo -y all

upvoted 2 times

Ziamsu 5 months, 2 weeks ago

D

[Expert@CP-FW03:0]# cpinfo -y all

This is Check Point CPinfo Build 914000215 for GAIA
[IDA]
No hotfixes..

[MGMT]
No hotfixes..

[CPFC]
No hotfixes..

[FW1]
HOTFIX_GOT_MGMT_AUTOUPDATE
HOTFIX_WEBCONSOLE_AUTOUPDATE
HOTFIX_GOT_TPCONF_AUTOUPDATE
HOTFIX_GOT_TPCONF_MGMT_AUTOUPDATE

FW1 build number:
This is Check Point Security Management Server R81.10 - Build 220
This is Check Point's software version R81.10 - Build 883
kernel: R81.10 - Build 793

upvoted 1 times

jerj5 9 months ago

Selected Answer: D

Correct
Command to view the version and hotfix information for both servers:
cpinfo -y all

upvoted 1 times

Question #28 *Topic 1*

Which command collects diagnostic data for analyzing a customer setup remotely?

A. cpv

B. cpinfo

C. migrate export

D. sysinfo

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

[Expert@CP-FW03:0]# sysinfo
-bash: sysinfo: command not found
[Expert@CP-FW03:0]# migrate export
-bash: migrate: command not found
[Expert@CP-FW03:0]# cpv
-bash: cpv: command not found
[Expert@CP-FW03:0]# cpinfo

This is Check Point CPinfo Build 914000215 for GAIA
Checking for updates...

Updating...

Verifying CK...

Could not verify CK: Could not resolve host
CPinfo update failed, using existing package

Verifying CK...

Could not verify CK: Could not resolve host
Exiting...
[Expert@CP-FW03:0]#

upvoted 1 times

jerj5 9 months ago

Selected Answer: B

Correct
CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers). The CPInfo output file allows analyzing customer setups from a remote location.

upvoted 3 times

Question #29 *Topic 1*

By default, what type of rules in the Access Control rulebase allow the control connections?

A. Implicit Rules

B. Explicitly Implied Rules

C. Implied Rules

D. Explicit Rules

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

ias253 4 months ago

C implied rules

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Answer is C , Implied Rules

Ref : https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Implied_Rules.htm

upvoted 2 times

jerj5 9 months ago

Selected Answer: C

Correct

Implied Rules in the Access Control rulebase allow the control connections. The Security Management Server adds and removes the Implied Rules in the Access Control rulebase when you select or clear Global Properties for Firewalls

upvoted 1 times

Question #30 *Topic 1*

Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called:

A. sysinfo

B. cpsizeme

C. cpinfo

D. cpexport

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: C

The "cpinfo" utility is used to collect diagnostics data on a Check Point system, which is often requested by Check Point Support for analysis.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Correct C : cpinfo

upvoted 1 times

jerj5 9 months ago

Selected Answer: C

Correct

When contacting Check Point Support, collect the CPInfo files from the Security Management server and Security Gateways involved in your case.

upvoted 1 times

Question #31 *Topic 1*

What is the name of the secure application for Mail/Calendar for mobile devices?

A. Secure Workspace

B. Capsule Mail

C. Capsule Workspace

D. Capsule VPN

Correct Answer: *C*

ias253 4 months ago

C capsule workspace

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

C is correct. https://www.checkpoint.com/harmony/mobile-security/mobile-secure-workspace/

upvoted 2 times

Question #32 *Topic 1*

What is the difference between SSL VPN and IPSec VPN?

A. SSL VPN requires installation of a resilient VPN client

B. SSL VPN and IPSec VPN are the same

C. IPSec VPN does not require installation of a resident VPN client

D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: D

- IPSec VPN typically requires a client application to be installed on the endpoint device to establish a secure connection.
- SSL VPN can often be accessed through a web browser without the need for a dedicated client application, making it more convenient for users who need quick and easy access to web-based resources.

upvoted 1 times

exmrrs 7 months ago

Selected Answer: D

correct,
It's worth noting that while browser-based SSL VPN is common, Check Point also offers a client-based SSL VPN option (Capsule VPN) for scenarios requiring more comprehensive access or better performance. However, the key distinction remains that traditional IPSec VPN always requires a dedicated client, while SSL VPN provides options for clientless access.

upvoted 2 times

Question #33 *Topic 1*

Which Remote Access Client does not provide an Office-Mode Address?

A. Endpoint Security Suite

B. Check Point Mobile

C. SecuRemote

D. Endpoint Security VPN

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: C

SecuRemote is a secure, but limited-function IPsec VPN client and does not support Office Mode.

upvoted 1 times

57ad24d 2 months, 1 week ago

Selected Answer: C

Explanation:
SecuRemote is a lightweight VPN client that does not support the use of an Office-Mode Address. Instead, it relies on the local IP address of the user's device for communication. This means it does not assign an internal IP address from the Office-Mode range, unlike other Remote Access clients such as Endpoint Security VPN or Check Point Mobile.

In contrast, other options like:

Endpoint Security Suite
Check Point Mobile
Endpoint Security VPN
support Office-Mode, which provides users with an internal corporate IP address to simplify access to network resources and ensure policy enforcement

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SecuRemote.htm?tocpath=Introduction%20to%20Remote%20Access%20Clients%7C____3

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

3 option:
SecuRemote - secure connectivity;
Endpoint Security VPN - secure connectivity, integrated desktop firewall, security verification, office mode, hub mode;
Check Point Mobile - secure connectivity, security verification, office mode, hub mode.

"SecuRemote is a limited-function IPSec VPN client that only provides secure connectivity. "

upvoted 3 times

Question #34 *Topic 1*

Which feature allows Remote-access VPN users to access resources across a site-to-site VPN tunnel?

A. Mobile Access VPN Domain

B. Community Specific VPN Domain

C. Remote Access VPN Switch

D. Network Access VPN Domain

Correct Answer: *B*

Community vote distribution

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: B

This feature allows remote-access VPN users to access resources across a site-to-site VPN tunnel by configuring a specific VPN domain for the VPN community.

upvoted 1 times

mfhashmi 5 months, 2 weeks ago

Selected Answer: B

B. Community Specific VPN Domain

Explanation:
Community Specific VPN Domain allows remote-access VPN users to access resources across a site-to-site VPN tunnel. This feature ensures that traffic from remote access users is included in the VPN domain for a particular VPN community, enabling them to access resources at different sites connected via the site-to-site VPN.

Mobile Access VPN Domain (Option A) and Network Access VPN Domain (Option D) are not directly related to enabling access across site-to-site tunnels.

Remote Access VPN Switch (Option C) is not a relevant feature.

Thus, Community Specific VPN Domain allows the integration of remote access VPN users into the network paths managed by site-to-site VPNs, facilitating seamless access.

upvoted 2 times

Question #35 *Topic 1*

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?

A. Network and Layers

B. Application and Client Service

C. Network and Application

D. Virtual Adapter and Mobile App

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

57ad24d 2 months, 1 week ago

Selected Answer: C

The two modes of SSL Network Extender (SNX) are:

Network Mode (or Network Extender Mode):

Provides full network connectivity to the corporate network.
The remote client machine is assigned an IP address from the internal network (similar to Office Mode) and can access network resources as if it were inside the office.
This mode supports access to multiple applications, protocols, and services within the internal network.
Application Mode:

Provides access to specific applications via a web interface without assigning the client an IP address.
Only predefined applications (e.g., web-based apps, email) can be accessed through a browser, making it more restrictive and suitable for limited access scenarios.
Uses the Check Point SSL VPN Portal for user interaction.

upvoted 1 times

KuKuKu83 3 months, 1 week ago

Selected Answer: C

SSL Network Extender has two modes:
• Network — Users can access all native IP-based and web-based applications in the internal network. For users to gain access to these applications, System Administrators must first define these as native applications in Mobile Access. The user can access the resources by launching the client either from the desktop or the Mobile Access portal. To work in Network mode, users must have installation privileges.
• Application — Users can access most native IP-based and web-based application types in the internal network, including most TCP applications. Users can only launch the client in the Mobile Access portal. Once installed, users can access internal resources defined as native applications in Mobile Access. Working in Application mode does not require installation privileges.

upvoted 4 times

Question #36 *Topic 1*

Which one of the following is true about Capsule Connect?

A. It is a full layer 3 VPN client

B. It is supported only on iOS phones and Windows PCs

C. It offers full enterprise mobility management

D. It does not support all VPN authentication methods

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

KuKuKu83 Highly Voted 3 months, 1 week ago

Selected Answer: A

Capsule Connect is a full L3 tunnel app that gives users network access to all mobile applications. It supplies secure connectivity and access to all types of corporate resources. It was previously called Mobile VPN.

upvoted 7 times

keikei1228 Most Recent 2 weeks, 6 days ago

Selected Answer: A

Capsule Connect is a full Layer-3 VPN client that provides secure connectivity and access to all types of corporate resources.

upvoted 1 times

Question #37 *Topic 1*

Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

A. Check Point Capsule Workspace

B. Check Point Capsule Remote

C. Check Point Mobile Web Portal

D. Check Point Remote User

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

ias253 4 months ago

A Checkpoint capsule workspace

upvoted 1 times

mfhashmi 5 months, 2 weeks ago

Selected Answer: A

A. Check Point Capsule Workspace

Explanation:
Check Point Capsule Workspace is a mobile access application that creates a secure container on mobile devices, allowing users to access internal resources like websites, file shares, emails, and other corporate applications. The secure container ensures that corporate data is kept separate from personal data on the device, providing enhanced security for mobile users.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

correct

upvoted 1 times

Question #38 *Topic 1*

Which Mobile Access Solution is clientless?

A. Mobile Access Portal

B. Checkpoint Mobile

C. Endpoint Security Suite

D. SecuRemote

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: A

The Mobile Access Portal is a clientless SSL VPN solution that supplies secure access to web-based resources

upvoted 1 times

ias253 4 months ago

A mobile access portal

upvoted 2 times

exmrrs 7 months ago

Selected Answer: A

correct,

Mobile Access Portal

is the clientless mobile access solution offered by Check Point. It allows users to access web-based applications and resources without requiring the installation of a dedicated client on their mobile devices.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

Correct

upvoted 2 times

Question #39 *Topic 1*

The Log server sends what to the Correlation Unit?

A. Authentication requests

B. Event Policy

C. Logs

D. CPMI dbsync

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

57ad24d 2 months, 1 week ago

Selected Answer: C

The correct answer is:

C. Logs

Explanation:
The Log Server sends logs to the Correlation Unit for analysis. The Correlation Unit processes these logs to identify potential threats, generate events, and apply the event correlation policies defined in the system. This is a critical component of Check Point's SmartEvent architecture, which is used for real-time threat detection and security event management.

Other Options:
A. Authentication requests: Not applicable, as authentication is handled by other components like the Security Gateway or RADIUS server.
B. Event Policy: The Event Policy is configured in the SmartEvent GUI and applied to the Correlation Unit, not sent by the Log Server.
D. CPMI dbsync: Refers to synchronization of management data between Check Point components and is unrelated to log processing by the Correlation Unit.

upvoted 1 times

mfhashmi 5 months, 2 weeks ago

Selected Answer: C

C. Logs

Explanation:
The Log Server sends logs to the Correlation Unit. The Correlation Unit analyzes logs in real-time, correlating them to detect security events and incidents, which are then passed to Check Point's SmartEvent for further analysis and response.

upvoted 1 times

Question #40 *Topic 1*

What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

A. Choose different setting for log storage and SmartEvent db

B. It is not possible

C. Install Management and SmartEvent on different machines

D. Use Multi-Domain Management Server

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 2 weeks, 6 days ago

Selected Answer: A

This allows you to configure different retention policies for SmartLog and SmartEvent, meeting the customer's requirements.

upvoted 1 times

mfhashmi 5 months, 1 week ago

Selected Answer: A

SmartEvent to keep events for 180 days is:

A. Choose different setting for log storage and SmartEvent db

This allows you to configure separate retention periods for SmartLog and SmartEvent, meeting the customer's requirements effectively

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

correct A

upvoted 1 times

Question #41 *Topic 1*

What are the two types of tests when using the Compliance blade?

A. Tests conducted based on the IoC XML file and analysis of SOLR documents

B. Access Control policy analysis and Threat Prevention policy analysis

C. Policy-based tests and Global properties

D. Global tests and Object-based tests

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

KuKuKu83 3 months, 1 week ago

Selected Answer: D

There are two types of tests:

• Global tests- Examine configuration settings for the entire organization

• Object- based tests- Examine the configuration settings for particular objects, such as Gateways and profiles

upvoted 3 times

Question #42 *Topic 1*

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

A. 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.

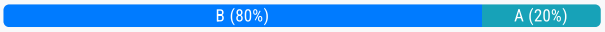
B. NAT Templates are generated to achieve high session rate for NAT. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase lookup. These are enabled by default and work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

C. 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.

D. 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.

Correct Answer: *B*

Community vote distribution



Community vote distribution

Kenny4275 4 months, 2 weeks ago

Selected Answer: B

B is the right answer. Accept and NAT templates are enabled by default. Drop templates needs to be manually enabled under gateway object > optimization then enable the checkbox for drop optimization

upvoted 1 times

laipose 4 months, 2 weeks ago

B

"These are enabled by default and work only if Accept Templates are enabled"

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

[Expert@CP-FW03:0]# fwaccel stat

Accept Templates : enabled
Drop Templates : disabled
NAT Templates : enabled
[Expert@CP-FW03:0]# fw ver
This is Check Point's software version R81.10 - Build 883
[Expert@CP-FW03:0]#

upvoted 1 times

lironzruya7 7 months ago

Selected Answer: B

NAT templates are enabled by default in 81.20

upvoted 1 times

exmrrs 7 months ago

Selected Answer: B

correct,
In R80.20 and above (which includes R81.X), NAT Templates are enabled by default. It's important to note that this answer reflects the behavior in

R81.X and above, as requested. The default state and behavior of NAT Templates have changed from earlier versions (R80.10 and below) where they were disabled by default

upvoted 1 times

c0be09e 8 months ago

Selected Answer: B

NAT templates are enabled by default since at least R80.40

upvoted 2 times

castieltel 8 months, 1 week ago

Selected Answer: B

Enabled by default and only works if Accept Templates are enabled.

upvoted 2 times

WwJim202120 8 months, 3 weeks ago

Selected Answer: A

NAT Templates: These templates are used by SecureXL (Secure Acceleration) to optimize Network Address Translation (NAT) performance. When a connection is processed by SecureXL and matches a rule in the rulebase that requires NAT, SecureXL can create a NAT Template. This template stores the NAT attributes (such as translated IP addresses and ports) so that subsequent similar connections can use this information directly from the template, avoiding the need for a full rulebase lookup during NAT processing.

Enabled/Disabled: NAT Templates are disabled by default in SecureXL. They can be enabled, but they only work if "Accept Templates" are also disabled. This ensures that the templates are used appropriately and do not conflict with other acceleration mechanisms.

upvoted 2 times

c0be09e 8 months ago

NAT templates are enabled by default since at least R80.40, so A is incorrect

upvoted 1 times

Question #43 *Topic 1*

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

A. SND is used to distribute packets among Firewall instances

B. SND is a feature to accelerate multiple SSL VPN connections

C. SND is a feature of fw monitor to capture accelerated packets

D. SND is an alternative to IPSec Main Mode, using only 3 packets.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: A

The Secure Network Distributor (SND) is responsible for processing incoming traffic from the network interfaces, securely accelerating authorized packets (if SecureXL is enabled), and distributing non-accelerated packets among Firewall kernel instances.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: A

SND (secure Network Dispatcher) forward packets require to inspect to FWK. for slow and medium path.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

The CoreXL software architecture includes the Secure Network Distributor. The SND is responsible for processing incoming traffic from the network interfaces, securely accelerating authorized packets (if SecureXL is running), and distributing non-accelerated packets among kernel instances. In other words, the SND is essentially a CPU core running both SecureXL and CoreXL.

upvoted 1 times

Question #44 *Topic 1*

Which statement is most correct regarding about “CoreXL Dynamic Dispatcher’?

A. The CoreXL FW instances assignment mechanism is based on IP Protocol type.

B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores

C. The CoreXL FW instances assignment mechanism is based on Source MAC addresses, Destination MAC addresses

D. The CoreXL FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP ‘Protocol’ type.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: B

This is because the CoreXL Dynamic Dispatcher assigns traffic to CoreXL Firewall instances based on the CPU utilization of each instance, aiming to balance the load across the available CPU cores.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

https://support.checkpoint.com/results/sk/sk105261

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Rather than statically assigning new connections to a CoreXL FW instance based on packet's IP addresses and IP protocol (static hash function), the new dynamic assignment mechanism is based on the utilization of CPU cores, on which the CoreXL FW instances are running.

upvoted 1 times

Brilliantel 9 months ago

Correct answer is B

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

Answer is B

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

Answer is B

upvoted 2 times

Question #45 *Topic 1*

What kind of information would you expect to see when using the “sim affinity –l” command?

A. Overview over SecureXL templated connections

B. The VMACs used in a Security Gateway cluster

C. Affinity Distribution

D. The involved firewall kernel modules in inbound and outbound packet chain

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: C

The "sim affinity -l" command is used to display the current affinity settings, which show how network interfaces are distributed among CPU cores. This command provides an overview of the affinity distribution, helping to understand how the load is balanced across the available CPU cores.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

sim affinity has been deprecated. See sk170012 for replacement commands.

fw ctl affinity is the replacement command

[Expert@CP-FW03:0]# fw ctl affinity -l
Kernel fw_0: CPU 3
Kernel fw_1: CPU 2
Kernel fw_2: CPU 1
Daemon cprid: CPU 1 2 3
Daemon cpca: CPU 1 2 3
Daemon mpdaemon: CPU 1 2 3
Daemon status_proxy: CPU 1 2 3
Daemon fwd: CPU 1 2 3
Daemon in.asessiond: CPU 1 2 3
Daemon cprid: CPU 1 2 3
Daemon cpd: CPU 1 2 3
[Expert@CP-FW03:0]#

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

Sim affinity -l" command is a command that displays the affinity distribution of the Security Gateway's interfaces. Affinity distribution is the assignment of CPU cores to handle the traffic from different interfaces

upvoted 3 times

Question #46 *Topic 1*

CoreXL is NOT supported when one of the following features is enabled:

A. Overlapping NAT

B. Route-based VPN

C. IPv6

D. IPS

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

wack0 1 month, 2 weeks ago

Selected Answer: A

CoreXL is not supported when one of the following features is enabled:
VPN Traditional mode
Overlapping NAT
CCSE R81.20 Manual Page 720
upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: A

R81 CoreXLClosed does not support:

Overlapping NAT

VPN Traditional Mode

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/Topics-PTG/CoreXL-Limitations.htm
upvoted 1 times

lironzruya7 7 months ago

Selected Answer: A

A is correct
upvoted 1 times

exmrrs 7 months ago

Selected Answer: A

IPv6: does not support in R75.40 and below.
Route-based VPN: does not support in R80.10 and below except R77.20 with T169.
so only Overlapping NAT is not supported for this question (scope R81.x)

answer: A
upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

CoreXL Limitations
R81 CoreXLClosed does not support:

Overlapping NAT
VPN Traditional Mode

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

Answer is A

upvoted 1 times

Question #47 *Topic 1*

What are the three SecureXL Templates available in R81.10?

A. Accept Templates, Drop Templates, NAT Templates

B. PEP Templates, QoS Templates, VPN Templates

C. Accept Templates, PDP Templates, PEP Templates

D. Accept Templates, Drop Templates, Reject Templates

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: A

fwaccel stat

Accept Templates : enabled
Drop Templates : disabled
NAT Templates : enabled
[Expert@CP-FW03:0]#

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

correct A

upvoted 1 times

Question #48 *Topic 1*

What is the correct description for the Dynamic Balancing / Spit feature?

A. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)

B. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)

C. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)

D. Dynamic Balancing / Spit dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)

Correct Answer: *A*

Community vote distribution

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: A

cpview > sysinfo > dynamic balancing status. I guess only supported in checkpoint appliance.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

CP-FW03> set dynamic-balancing state enable

Dynamic Balancing is not supported on open server appliances

upvoted 1 times

8202009 8 months, 2 weeks ago

Selected Answer: A

Answer is A. Check Point appliances only.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

Security Gateway R80.40 and higher contains the CoreXL Dynamic Balancing (formerly, Dynamic Split) feature - a performance-enhancing daemon that balances the load between CoreXL SND instances and CoreXL Firewall instances. It dynamically changes the split between CoreXL SND instances and CoreXL Firewall instances

The distribution of jobs across a Security Gateway's CPUs is referred to as the Security Gateway's split. As the distribution of work across these groups depends on your security policy and traffic

Supported Platforms

Check Point Appliances only

(Virtual Machines and Open Servers are not supported)

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

Answer is A

upvoted 1 times

Question #49 *Topic 1*

Which statement is WRONG regarding the usage of the Central Deployment in SmartConsole?

A. Only Hotfixes can be installed with the Central Deployment in SmartConsole

B. You can install Hotfixes with the Central Deployment in SmartConsole

C. You can upgrade your cluster without user intervention with the Central Deployment in SmartConsole from R80.40 to R81.20.

D. You can install Jumbo Hotfix accumulators with the Central Deployment in SmartConsole.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: A

This statement is incorrect because, in addition to Hotfixes, you can also install Jumbo Hotfix Accumulators using the Central Deployment in SmartConsole.

upvoted 1 times

mfhashmi 5 months, 1 week ago

Selected Answer: A

A. Only Hotfixes can be installed with the Central Deployment in SmartConsole

Central Deployment in SmartConsole allows you to install not only Hotfixes but also Jumbo Hotfix Accumulators and perform upgrades on Security Gateways and Cluster Members

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

correct

upvoted 1 times

Question #50 *Topic 1*

What is false regarding prerequisites for the Central Deployment usage?

A. The Security Gateway must have a policy installed

B. The administrator must have write permission on SmartUpdate

C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically

D. Security Gateway must have the latest CPUSE Deployment Agent

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: C

Explanation: SIC (Secure Internal Communication) must already be established between the Management Server and the target Security Gateways and Cluster Members. The CDT tool does not automatically establish SIC.

upvoted 1 times

mfhashmi 5 months, 1 week ago

Selected Answer: C

The CDT tool does not automatically handle SIC establishment

upvoted 1 times

jerj5 8 months, 3 weeks ago

Selected Answer: C

Correct

To use the SmartConsole Central Deployment function:

• The administrator must have SmartUpdate write permission on the Management Server.

• The latest build of the CPUSE Deployment Agent must be installed on the target Security Gateways and Cluster Members.

• SIC must already be established between the Management Server and the target Security Gateways and Cluster Members.

• A policy must be installed on the target Security Gateways and Cluster Members.

• Only full clusters can be deployed. You cannot select and deploy one Cluster Member.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

correct

upvoted 1 times

Question #51 *Topic 1*

The installation of a package via SmartConsole CANNOT be applied on

A. A single Security Gateway

B. A full Security Cluster (All Cluster Members included)

C. Multiple Security Gateways and/or Clusters

D. R81.20 Security Management Server

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: D

SmartConsole is used to manage and deploy packages to Security Gateways and Clusters, but not directly on the Security Management Server itself.

upvoted 1 times

mfhashmi 5 months, 1 week ago

Selected Answer: D

SmartConsole is used to manage and deploy policies and updates to Security Gateways and Clusters, but not directly to the Security Management Server itself

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

Correct

upvoted 1 times

Question #52 *Topic 1*

What is the purpose of the command “ps aux | grep fwd”?

A. You can check whether the IPS default setting is set to Detect or Prevent mode

B. You can check the Process ID and the processing time of the fwd process.

C. You can convert the log file into Post Script format.

D. You can list all Process IDs for all running services.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: B

This command lists the details of the "fwd" process, including its Process ID (PID) and other information such as the processing time.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

[Expert@CP-FW03:0]# ps aux | grep fwd

admin 6055 0.1 0.4 636692 75404 ? Ssl 19:57 0:07 fwd

[Expert@CP-FW03:0]#

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

correct

upvoted 1 times

Question #53 *Topic 1*

Which of these statements describes the Check Point ThreatCloud?

A. Blocks or limits usage of web applications

B. Prevents or controls access to web sites based on category

C. A worldwide collaborative security network

D. Prevents Cloud vulnerability exploits

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: C

Check Point ThreatCloud is a dynamically updated service based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

Correct answer C

upvoted 1 times

jerj5 8 months, 3 weeks ago

Selected Answer: C

Correct

The Check Point Anti-Bot Software Blade detects bot-infected machines, prevents bot damages by blocking bot Command and Control (C&C) communications, and is continually updated from ThreatCloud™, which is the first collaborative network to fight cybercrime

upvoted 1 times

Question #54 *Topic 1*

Using Web Services to access the API, which Header Name/Value had to be in the HTTP Post request after the login?

A. uuid Universally Unique Identifier

B. API-Key

C. user-uid

D. X-chkp-sid Session Unique Identifier

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 1 week, 6 days ago

Selected Answer: D

After logging in, you need to include the "X-chkp-sid" header with the session unique identifier in each HTTP Post request to access the API.

upvoted 1 times

5a7f608 3 months, 2 weeks ago

Selected Answer: D

HTTP headers:

content-Type: application/json

x-chkp-sid: <session ID token as returned by the login command>

Font: Checkpoint Certified Security Expert manual page 48

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: D

x-chkp-sid is the key return after login, to use the same key for subsequence command without logging in again and again.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

HTTP Headers

content-Type: application/json

x-chkp-sid: <session ID token as returned by the login command>

The x-chkp-sid header is mandatory in all API calls except the login API.

upvoted 1 times

Question #55 *Topic 1*

What command would show the API server status?

A. api status

B. show api status

C. cpm status

D. api restart

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

5a7f608 3 months, 2 weeks ago

Selected Answer: A

Check Point Certified Security Expert manual page: 64

"1A-1.4:

Run the following command to check the status of the Security Management Server:

api status"

upvoted 1 times

mfhashmi 5 months, 1 week ago

Selected Answer: A

correct

upvoted 1 times

Question #56 *Topic 1*

What could NOT be a reason for synchronization issues in a Management HA environment?

A. Hardware clocks do not match even with adjustments for different time zones

B. Accidentally, you have configured unique IP addresses per Management Server which invalidates the CA Certificate

C. There is a network connectivity failure between the servers

D. The products installed on the servers do not match: one device is a Standalone Server while the other is only a Security Management server.

Correct Answer: *A*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 1 week, 5 days ago

Selected Answer: B

B. Accidentally, you have configured unique IP addresses per Management Server which invalidates the CA Certificate

This is not a valid reason for synchronization issues in a Management HA environment. Each Management Server should indeed have a unique IP address, and this does not invalidate the CA Certificate. The other options listed (A, C, and D) are valid reasons that could cause synchronization issues.

upvoted 1 times

yeru 2 weeks, 6 days ago

Based on CCSE 82.10 manual course, page 87
Synchronization Failure
Possible causes of management synchronization failure include:
1. Installed Hotfixes do not match between servers. Different Hotfixes are installed on each server.
2.Hardware clocks do not match, even with adjustments for different time
zones.
3.The products installed on the servers do not match: one device is a Standalone Security Management Server / Security Gateway Combination and the other is only a Security Management Server.

Based on this the answer should be B for What could NOT be a reason for synchronization issues in a Management HA environment?

upvoted 1 times

Bruce730 3 weeks ago

Selected Answer: B

Bi s correct according to the book for CCSE

upvoted 1 times

wack0 1 month, 2 weeks ago

Selected Answer: A

Hardware clocks do not match, even with adjustments for different time zones
CCSE R81.20 manual page 87

upvoted 1 times

yeru 2 weeks, 6 days ago

I checked pager 87,
Synchronization Failure
Possible causes of management synchronization failure include:
1. Installed Hotfixes do not match between servers. Different Hotfixes are installed on each server.
2.Hardware clocks do not match, even with adjustments for different time

zones.
3.The products installed on the servers do not match: one device is a Standalone Security Management Server / Security Gateway Combination and the other is only a Security Management Server.

Based on this the answer should be B for What could NOT be a reason for synchronization issues in a Management HA environment?
upvoted 1 times

lironzruya7 7 months ago

Selected Answer: B

B is correct
upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

General restrictions for Primary and Secondary Security Management servers:
- The SmartEvent Software Blade can only be enabled on the active server in Management High Availability environment
- Must have identical Check Point versions and identical hotfixes installed.
To see the build number, run cpinfo -y FW1
- Must have identical products installed (i.e, Management HA is not supported between a Standalone machine and machine that runs only Security Management server)
upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is B
upvoted 1 times

Question #57 *Topic 1*

What order should be used when upgrading a Management High Availability Cluster?

A. Secondary Management, then Primary Management

B. Active Management, then Standby Management

C. Standby Management, then Active Management

D. Primary Management, then Secondary Management

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 1 week, 5 days ago

Selected Answer: C

This ensures that the active management server remains operational while the standby server is upgraded first. Once the standby server is successfully upgraded and verified, the active server can then be upgraded, minimizing downtime and maintaining high availability.

upvoted 1 times

yeru 4 days, 13 hours ago

In Management High Availability, make sure the Primary Security Management Server is upgraded and runs, before you start the upgrade on other servers.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/Upgrading-SecMmgt-Servers-in-Mmgt-HA-from-R80_20-and-higher.htm

Step Instructions 7

It should be D,

upvoted 1 times

lironzruya7 7 months ago

Selected Answer: D

d is correct

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

"In Management High Availability, make sure the Primary Security Management Server is upgraded and runs, before you start the upgrade on other servers."

upvoted 4 times

Rajeshkashi 9 months, 2 weeks ago

Answer is D

upvoted 1 times

Question #58 *Topic 1*

You need to see which hotfixes are installed on your Check Point server, which command would you use?

A. cpinfo –h all

B. cpinfo –o hotfix

C. cpinfo –y all

D. cpinfo –I hotfix

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

mfhashmi 5 months, 1 week ago

Selected Answer: C

correct

upvoted 1 times

WSCOSTA 8 months, 2 weeks ago

Answer is C

upvoted 1 times

Question #59 *Topic 1*

What mechanism can ensure that the Security Gateway can communicate with the Management Server with ease in situations with overwhelmed network resources?

A. There is a feature for ensuring stable connectivity to the management server and is done via Priority Queuing.

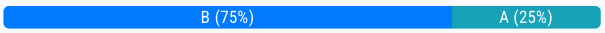
B. The corresponding feature is new to R81.10 and is called “Management Data Plane Separation”

C. The corresponding feature is called “Dynamic Split”

D. The corresponding feature is called “Dynamic Dispatching”

Correct Answer: *B*

Community vote distribution



Community vote distribution

keikei1228 1 week, 4 days ago

Selected Answer: B

Management Data Plane Separation (MDPS) allows a Security Gateway to have isolated Management and Data networks, ensuring stable connectivity to the management server even when network resources are overwhelmed.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

Vote for B, I have done MDPS and this is more relevant answer

upvoted 1 times

david_vera 7 months, 3 weeks ago

Selected Answer: B

According to Check Point Cybersecurity Bootcamp CCSE course that I took 1 month ago the same text that jerj5 posted:
With heavy network traffic, the Security Gateway might become overwhelmed and be unable to communicate with some systems, losing some functionality or management connectivity.
To prevent such situations, Management Data Plane Separation (MDPS) lets a Security Gateway to have isolated Management and Data networks.

upvoted 1 times

jerj5 8 months ago

Selected Answer: B

Although MDPS was introduced in version R80.20, the CCSE guide mentions the following:
With heavy network traffic, the Security Gateway might become overwhelmed and be unable to communicate with some systems, losing some functionality or management connectivity.
To prevent such situations, Management Data Plane Separation (MDPS) lets a Security Gateway to have isolated Management and Data networks.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

Priority queue pyritizes traffic to mgmt server on Control queue, second highest level. Level 0, highest is used for Routing whch guarantees the communication from GW to mgmt server will be in place

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is A

upvoted 1 times

Question #60 *Topic 1*

Which process is used mainly for backward compatibility of gateways in R80.x and newer? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.

A. cpm

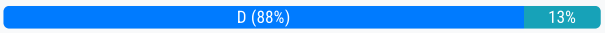
B. fwd

C. cpd

D. fwm

Correct Answer: *D*

Community vote distribution



Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: D

FWM is the correct answer

upvoted 1 times

jerj5 8 months ago

Selected Answer: D

FWM - Firewall Management. Responsible for most SmartConsole connections, policy verification and compilation, and Management High Availability (HA) synchronization.

upvoted 3 times

sivaN9 8 months, 2 weeks ago

Selected Answer: D

The fwm process is used mainly for backward compatibility of gateways.
It provides GUI client communication, database manipulation, policy compilation, and
Management High Availability synchronization.

upvoted 3 times

WwJim202120 8 months, 2 weeks ago

Selected Answer: C

cpd is correct

upvoted 1 times

WwJim202120 8 months, 2 weeks ago

Not C, sorry

upvoted 2 times

Question #61 *Topic 1*

What component of Management is used for indexing?

A. fwm

B. SOLR

C. API Server

D. DBSync

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

SOLR is correct

upvoted 1 times

jerj5 8 months ago

Selected Answer: B

Correct

SOLR - Used for indexing and parsing logs. If the logs are not indexed, then they need to be viewed by selecting an individual log file.

upvoted 1 times

Question #62 *Topic 1*

What is the responsibility of SOLR process on the management server?

A. Validating all data before it's written into the database

B. It generates indexes of data written to the database

C. Communication between SmartConsole applications and the Security Management Server

D. Writing all information into the database

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

jerj5 8 months ago

Selected Answer: B

SOLR - Used for indexing and parsing logs. If the logs are not indexed, then they need to be viewed by selecting an individual log file.

upvoted 1 times

Question #63 *Topic 1*

What is the difference between Updatable Objects and Dynamic Objects

A. Updatable Objects is a Threat Cloud Service. The provided Objects are updated automatically. Dynamic Objects are created and maintained locally. In both cases there is no need to install policy for the changes to take effect.

B. Dynamic Objects are maintained automatically by the Threat Cloud. For Dynamic Objects there is no need to install policy for the changes to take effect. Updatable Objects are created and maintained locally.

C. Updatable Objects is a Threat Cloud Service. The provided Objects are updated automatically. Dynamic Objects are created and maintained locally. For Dynamic Objects there is no need to install policy for the changes to take effect.

D. Dynamic Objects are maintained automatically by the Threat Cloud. Updatable Objects are created and maintained locally. In both cases there is no need to install policy for the changes to take effect.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

WwJim202120 8 months, 3 weeks ago

Selected Answer: A

Updatable Objects

An updatable object is a network object which represents an external service, such as Office 365, AWS, GEO locations and more. External services providers publish lists of IP addresses or Domains or both to allow access to their services. These lists are dynamically updated. Updatable objects derive their contents from these published lists of the providers, which Check Point uploads to the Check Point cloud. The updatable objects are updated automatically on the Security Gateway each time the provider changes a list. There is no need to install policy for the updates to take effect. You can use an updatable object in the Access Control policy as a source or a destination.

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

The Updatable Objects are updated automatically on the Security Gateway each time the provider changes a list. There is no need to install policy for the updates to take effect.

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

A or C

upvoted 1 times

Question #64 *Topic 1*

Which process handles connections from SmartConsole R80?

A. cpm

B. cpd

C. cpmd

D. fwd

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 1 week, 4 days ago

Selected Answer: A

The CPM (Check Point Management) process is responsible for serving requests from SmartConsole and writing all information to the PostgreSQL and SOLR databases.

upvoted 1 times

jerj5 8 months ago

Selected Answer: A

Correct

CPM - Accepts connections and commands from SmartConsole and stores information to the database. Actually a JAVA application

upvoted 2 times

Question #65 *Topic 1*

Identity Awareness allows easy configuration for network access and auditing based on what three items?

A. Client machine IP address.

B. Network location, the identity of a user and the identity of a machine

C. Log server IP address.

D. Gateway proxy IP address.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

jerj5 8 months ago

Selected Answer: B

Correct

Identity Awareness lets you configure network access and auditing based on one or more of the following items:

• Network location

• The identity of a user

• The identity of a machine

upvoted 1 times

Question #66 *Topic 1*

Which of the following cannot be configured in an Access Role Object?

A. Networks

B. Machines

C. Users

D. Time

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 1 week, 4 days ago

Selected Answer: D

Access Role objects can include Networks, Machines, and Users, but they do not include Time as a configurable parameter.

upvoted 1 times

wack0 1 month, 2 weeks ago

Selected Answer: D

CCSE R81.20 manual page 410

upvoted 1 times

jerj5 8 months ago

Selected Answer: D

Correct

Access Role objects include one or more of these objects:

• Networks

• Users and user groups

• Computers and computer groups

• Remote Access Clients

upvoted 1 times

Question #67 *Topic 1*

Fill in the blank: RADIUS protocol uses _____ to communicate with the gateway.

A. TDP

B. CCP

C. HTTP

D. UDP

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

premoli 3 months, 3 weeks ago

Selected Answer: D

UDP Port

UDP port used on RADIUS server.

The default port is 1812 as specified by the RADIUS standard.

The range of valid port numbers is from 1 to 65535.

Port 1645 is non-standard, but is commonly used as alternative to port 1812.

upvoted 1 times

Question #68 *Topic 1*

Which of the following is NOT a component of a Distinguished Name?

A. Common Name

B. Country

C. User container

D. Organizational Unit

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

Canferno 3 months, 2 weeks ago

Selected Answer: C

i believe this question is poorly asked. When referring to DN, someone with AD experience normally thinks about the Distinguished name of an account. (Not the DN within a certificate.) i can understand why the answer is C, however the question itsself should be enhanced so that whoever reads should think about the attribute fields of certificate.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

If you generate a user certificate with a non-Check Point Certificate Authority, enter the Common Name (CN) component of the Distinguished Name (DN).

For example, if the DN is [CN = James, O = My Organization, C = My Country], then enter James as the username. If you use Common Names as user names, they must contain exactly one string with no spaces.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Configuring_User_Access_Using_Radius_Server_Groups.htm?Highlight=Distinguished%20Name%20Components

upvoted 2 times

Question #69 *Topic 1*

Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

A. Enable .exe bat protection in IPS Policy

B. tecli advanced attributes set prohibited_file_types exe, bat

C. create FW rule for particular protocol

D. enable DLP and select .exe and .bat file type

Correct Answer: *B*

Community vote distribution

Community vote distribution

keikei1228 1 week, 4 days ago

Selected Answer: B

This option directly configures the Threat Emulation blade to block these specific file types.

upvoted 1 times

5a7f608 3 months, 1 week ago

Selected Answer: B

As user kambata correctly said in https://www.examtopics.com/discussions/checkpoint/view/7481-exam-156-31580-topic-1-question-197-discussion/ : "DLP, IPS and FW blades have nothing to do with Threat Emulation Blade"

upvoted 1 times

premoli 3 months, 3 weeks ago

Selected Answer: D

There a similiar command in https://support.checkpoint.com/results/sk/sk123140 to B option, but the sintax is wrong

upvoted 1 times

lironzruya7 7 months ago

Selected Answer: B

Answer is B

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

https://community.checkpoint.com/fyrhh23835/attachments/fyrhh23835/taiwan/422/1/Check%20Point%20Sandblast%20PoC%20Guide%20v91.pdf page 101

To block certain filetypes inside archives (which is currently not possible with AV filetype blocking) use the following TECLI command: Enabling prohibited file types in archives On the gateway, run the command: tecli advanced attribute set prohibited_file_types , For example to block every archive that contains an exe file run: tecli advanced attribute set prohibited_file_types exe

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is B

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

Answer is D

upvoted 2 times

Question #70 *Topic 1*

A user complains that some Internet resources are not available. The Administrator is having issues seeing if packets are being dropped at the firewall (not seeing drops in logs). What is the solution to troubleshoot the issue?

A. run “fw ctl zdebug drop” on the relevant gateway

B. run “cpstop” on the relevant gateway and check the ping again

C. run “fw unloadlocal” on the relevant gateway and check the ping again

D. run “fw log” on the relevant gateway

Correct Answer: *A*

keikei1228 1 week, 4 days ago

Selected Answer: A

This command will help the administrator see if packets are being dropped at the firewall in real-time and provide an explanation as to why the packets are being dropped.

upvoted 1 times

Question #71 *Topic 1*

Which command will reset the kernel debug options to default settings?

A. fw ctl dbg –a 0

B. fw ctl debug set 0

C. fw ctl debug 0

D. fw ctl dbg resetall

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

premoli 3 months, 3 weeks ago

Selected Answer: C

Reset the kernel debug options.

On the Security Gateway / each Cluster Member, run:

fw ctl debug 0

On the Scalable Platform Security Group, run:

g_fw ctl debug 0

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

[Expert@CP-FW03:0]# fw ctl debug 0
Defaulting all kernel debugging options
Debug state was reset to default.
PPAK 0: Get before set operation succeeded of simple_debug_filter_off
[Expert@CP-FW03:0]#

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

Reset the kernel debug options.
On the Security Gateway / each Cluster Member, run: fw ctl debug 0.

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is C

upvoted 1 times

Question #72 *Topic 1*

Which Operating Systems are supported for the Endpoint Security VPN?

A. Windows and Red Hat Linux

B. Windows and SPARC Solaris

C. Windows and x86 Solaris

D. Windows and macOS computers

Correct Answer: *D*

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

Question #73 *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 capable of issuing and managing certificate. Alice uses the Check Point command “cpconfig” to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances “Primary & Secondary”. Which configuration option does she need to look for?

A. Certificate's Fingerprint

B. Random Pool

C. Certificate Authority

D. CA Authority

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 1 week, 4 days ago

Selected Answer: C

Alice needs to look for the Certificate Authority configuration option in the "cpconfig" tool. This option initializes the Internal Certificate Authority (ICA) and configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN), which is responsible for issuing and managing certificates.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

Configuration Options:

---

(1) Licenses and contracts
(2) Administrator
(3) GUI Clients
(4) SNMP Extension
(5) PKCS#11 Token
(6) Random Pool
(7) Certificate Authority
(8) Certificate's Fingerprint
(9) Check Point CoreXL
(10) Automatic start of Check Point Products

(11) Exit

Enter your choice (1-11) :7

Configuring Certificate Authority...

==========

The Internal CA is initialized with the following name: CP-FW03

Do you want to change it (y/n) [n] ?

upvoted 2 times

Question #74 *Topic 1*

Is it possible to establish a VPN before the user login to the Endpoint Client.

A. Yes, you had to set neo_remember_user_password to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_remember_user_password attribute in the trac_client_1.ttm file located in the $FWDIR/conf directory on the Security Gateway

B. Yes, you had to set neo_always_connected to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_always_connected attribute in the trac_client_1.ttm file located in the $FWDIR/conf directory on the Security Gateway

C. No, the user must login first.

D. Yes, you have to enable Machine Authentication in the Gateway object of the Smart Console

Correct Answer: *B*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 1 week, 4 days ago

Selected Answer: D

To establish a VPN before the user logs in to the Endpoint Client, you need to enable Machine Authentication. This can be configured in the Gateway object of the Smart Console. Additionally, you can set the "machine_tunnel_before_logon" attribute to "true" in the "trac.defaults" configuration file on the client computer.

upvoted 1 times

premoli 3 months, 3 weeks ago

Selected Answer: D

https://community.checkpoint.com/t5/Security-Gateways/Machine-certificate-auth/td-p/210437

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

D.

Machine-only authentication - Authenticate with a machine certificate only. This mode is available before and after the user logs in to Windows.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RemoteAccessVPN_AdminGuide/Topics-VPNRG/Machine-Certificate.htm?tocpath=____12

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is D

upvoted 1 times

Question #75 *Topic 1*

Mobile Access Gateway can be configured as a reverse proxy for Internal Web Applications. Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Which of the following Check Point command is true for enabling the Reverse Proxy:

A. ReverseProxy

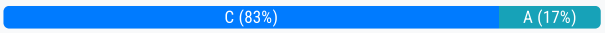
B. ReverseCLIProxy

C. ReverseProxyCLI

D. ProxyReverseCLI

Correct Answer: *C*

Community vote distribution



Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

[Expert@CP-FW03:0]# ReverseProxyCLI on
Enabling ...
This operation may take a few seconds ...

Applying your configuration ...

Finished applying configuration with WARNING/s:

- Mobile Access is NOT Running on your Gateway, Please Make sure Mobile Access Blade is enabled and running in order for the Reverse Proxy to work.
- The Platform Portal on your Gateway is NOT accessible, Please change 'Platform Portal' in your Gateway object in the Security Management to a different port than (443) OR a different path than (/)

Reverse Proxy Clear is ENABLED.
Reverse Proxy SSL is ENABLED.
[Expert@CP-FW03:0]#
[Expert@CP-FW03:0]# ReverseProxyCLI off
Disabling ...
This operation may take a few seconds ...
Reverse Proxy Clear is DISABLED.
Reverse Proxy SSL is DISABLED.
[Expert@CP-FW03:0]#
upvoted 2 times

paozinho 6 months, 2 weeks ago

Selected Answer: C

Answer is C
upvoted 1 times

lironzruya7 7 months ago

Selected Answer: A

Answer is A
upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

Reverse Proxy is disabled by default and can be enabled through the CLI command: ReverseProxyCLI

upvoted 3 times

Rajeshkashi 9 months, 2 weeks ago

Answer is C

upvoted 1 times

Question #76 *Topic 1*

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?

A. For compliance/host checking, Workspace offers the MDM cooperative enforcement, whereas Connect offers both jailbreak/root detection and MDM cooperative enforcement.

B. Workspace can support any application, whereas Connect has a limited number of application types which it will support

C. Workspace supports iOS, Android, and WP8, whereas Connect supports iOS and Android only

D. For credential protection, Connect uses One-time Password login support, but has no SSO support, whereas Workspace offers both One-Time Password login support as well as SSO for specific applications.

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

KuKuKu83 3 months, 1 week ago

Selected Answer: D

Connect:
• One-Time Password
(OTP) login support
• No SSO support
Workspase:
• OTP login support
• SSO for Workspace apps
upvoted 1 times

Question #77 *Topic 1*

What are the two modes for SNX (SSL Network Extender)?

A. Network Mode and Hub Mode

B. Network Mode and Application Mode

C. Visitor Mode and Office Mode

D. Office Mode and Hub Moe

Correct Answer: *C*

Community vote distribution

Community vote distribution

57ad24d 2 months, 1 week ago

Selected Answer: B

The two modes for SNX are Network Mode and Application Mode, providing flexibility for full network access or limited application-level access, depending on user needs.

upvoted 1 times

lironzruya7 7 months ago

Selected Answer: B

Answer is B

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

SSL Network Extender can operate in two modes: Network Mode and Applications Mode.

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is B

upvoted 1 times

Question #78 *Topic 1*

Native Applications require a thin client under which circumstances?

A. If you want to have assigned a particular Office Mode IP address

B. If you are about to use a client (FTP, RDP, ...) that is installed on the endpoint.

C. If you want to use a VPN Client that is not officially supported by the underlying operating system

D. If you want to use a legacy 32-Bit Windows OS

Correct Answer: *C*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 1 week, 4 days ago

Selected Answer: B

Native applications require a thin client when you need to use a client that is installed on the endpoint, such as FTP, RDP, etc. This thin client ensures that all traffic between the endpoint and the Mobile Access gateway is encrypted.

upvoted 1 times

lironzruya7 7 months ago

Selected Answer: B

Answer is B

upvoted 2 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: B

FTP, RDP, SSH

upvoted 2 times

Rajeshkashi 9 months, 2 weeks ago

Answer is B

upvoted 1 times

Question #79 *Topic 1*

In SmartConsole, where do you manage your Mobile Access Policy?

A. Through the Mobile Console

B. Shared Gateways Policy

C. From the Dedicated Mobility Tab

D. Smart Dashboard

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

yeru 1 week, 1 day ago

Selected Answer: D

Policy type:
1. Mobile Access Policy--->
Uses the Legacy Policy, configured in SmartConsole > Security Policies view > Shared Policies section > Mobile Access section > Policy page. This is the default.
2. Unified Access Policy--->
Includes Mobile Access rules in the Unified Access Policy, configured in SmartConsole > Security Policies view > Access Control section > Policy page.

The question is policy type of Mobile Access Policy.
Creating Mobile Access Rules in the Legacy Policy In SmartConsole, select Security Policies > Shared Policies > Mobile Access and click Open Mobile Access Policy in SmartDashboard.
SmartDashboard opens and shows the Mobile Access tab.

upvoted 1 times

Jallic 1 month, 1 week ago

Selected Answer: D

So if you are using legacy (which is default), in the mobile access section under shared policy you can only launch Smart dashboard.

upvoted 1 times

Jallic 1 month, 2 weeks ago

Selected Answer: C

Select the policy type:
The default is to use the Legacy Policy, configured in the Mobile Access tab in SmartConsole.
To include Mobile Access in the Unified Access Policy, select this in Gateway Properties > Mobile Access.

Unified Access Policy - Configure all rules for the Security Gateway in the Unified Access Policy. See Mobile Access and the Unified Access Policy.

Legacy Policy - Configure all rules for the Security Gateway in the shared Mobile Access Policy in the SmartDashboard. This option is available for Security Gateways of all versions and is the default for all Security Gateways.
Above is from the link I posted.
So we can see in the first line "SmartConsole" and "Mobile Access tab", as the question is not telling us the default settings have been updated, I think this adds further weight to 'C' being the correct answer in this case.

upvoted 1 times

Jallic 1 month, 2 weeks ago

Selected Answer: C

https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_MobileAccess_AdminGuide/Content/Topics-MABG/Getting-Started.htm

upvoted 1 times

KuKuKu83 3 months, 1 week ago

Selected Answer: D

correct

upvoted 1 times

Question #80 *Topic 1*

You have used the SmartEvent GUI to create a custom Event policy. What is the best way to display the correlated Events generated by SmartEvent Policies?

A. In the SmartConsole / Logs & Monitor –> open the Logs View and use type:Correlated as query filter.

B. Select the Events tab in the SmartEvent GUI or use the Events tab in the SmartView web interface.

C. Open SmartView Monitor and select the SmartEvent Window from the main menu.

D. In the SmartConsole / Logs & Monitor –> open a new Tab and select External Apps / SmartEvent.

Correct Answer: *B*

Community vote distribution

A (100%)

Community vote distribution

chaosisgod 2 months, 3 weeks ago

Selected Answer: A

https://community.checkpoint.com/t5/Management/Question-about-Log-type-Correlated/m-p/86709

upvoted 1 times

iulianm 5 months, 1 week ago

Correct is B

upvoted 2 times

lironzruya7 7 months ago

Selected Answer: A

Correct is A

upvoted 1 times

castieltel 8 months, 1 week ago

Selected Answer: A

Correct is A

upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

Answer is A

upvoted 2 times

Question #81 *Topic 1*

When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

A. Syslog

B. SNMP Trap

C. Mail

D. Block Source

Correct Answer: *D*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 1 week, 3 days ago

Selected Answer: A

The possible automatic reactions include:
SNMP Trap
Mail
Block Source
upvoted 1 times

57ad24d 2 months, 1 week ago

Selected Answer: A

While Syslog is commonly used for forwarding log information to an external system, it is not a configurable Automatic Reaction in Check Point SmartEvent. Automatic Reactions are specific actions that can be triggered in response to detected events, and Syslog is not listed as one of these actions
upvoted 1 times

darwin_2024 5 months, 3 weeks ago

The answer is A
upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

These are the types of Automatic Reactions:
Mail - Tell an administrator by email that the event occurred. See Creating a Mail Reaction.
Block Source - Instruct the Security GatewayClosed to block the source IP address from which this event was detected for a configurable timeframe . Select a timeframe from one minute to more than three weeks. See Creating a Block Source Reaction.
Block Event activity - Instruct the Security Gateway to block a distributed attack that emanates from multiple sources, or attacks multiple destinations for a configurable timeframe. Select a timeframe from one minute to more than three weeks). See Creating a Block Event Activity Reaction.
External Script - Run a script that you provide. See Creating an External Script Automatic Reaction to write a script that can exploit SmartEvent data.
SNMP Trap - Generate an SNMP Trap. See Creating an SNMP Trap Reaction.
upvoted 1 times

Rajeshkashi 9 months, 2 weeks ago

answer is A
upvoted 1 times

Question #82 *Topic 1*

What are possible Automatic Reactions in SmartEvent?

A. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script

B. Web Mail, Block Service, SNMP Trap, SmartTask, Geo Protection

C. Web Mail, Block Destination, SNMP Trap, SmartTask

D. Mail, SNMP Trap, Block Source, Block Event Activity, External Script

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

yeru 2 weeks, 5 days ago

Selected Answer: D

Another Q When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

A. Syslog

B. SNMPTrap

C. Block Source

D. Mail

upvoted 1 times

KuKuKu83 3 months, 1 week ago

Selected Answer: D

correct

types of Automatic Reactions:

Mail - Tell an administrator by email that the event occurred. See Creating a Mail Reaction.

Block Source - Instruct the Security GatewayClosed to block the source IP address from which this event was detected for a configurable timeframe . Select a timeframe from one minute to more than three weeks. See Creating a Block Source Reaction.

Block Event activity - Instruct the Security Gateway to block a distributed attack that emanates from multiple sources, or attacks multiple destinations for a configurable timeframe. Select a timeframe from one minute to more than three weeks). See Creating a Block Event Activity Reaction.

External Script - Run a script that you provide. See Creating an External Script Automatic Reaction to write a script that can exploit SmartEvent data.

SNMP Trap - Generate an SNMP Trap. See Creating an SNMP Trap Reaction.

upvoted 2 times

Question #83 *Topic 1*

Which command can you use to enable or disable multi-queue per interface?

A. Cpmqueue set

B. Set cpmq enable

C. Cpmq config

D. cpmq set

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

[Expert@CP-FW03:0]# cpmq set
Note: 'cpmq' is deprecated and no longer supported. For multiqueue management, please use 'mq_mng'
Current multiqueue status:
No multiqueue supported interfaces available
[Expert@CP-FW03:0]# mq_mng
error: Missing arguments
[Expert@CP-FW03:0]#

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

correct

upvoted 1 times

Question #84 *Topic 1*

What is Dynamic Balancing?

A. It is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load

B. It is a ClusterXL feature that switches an HA cluster into an LS cluster if required to maximize throughput.

C. It is a CoreXL feature that assigns the SND to network interfaces to balance the RX Cache of the interfaces

D. It is a new feature that is capable of dynamically reserve the amount of Hash kernel memory to reflect the resource usage necessary for maximizing the session rate.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: A

A is correct, when there are many fast path packet, it overload SND, and more core can assign SND from FWK in dynamic actions. Previously before dynamic balancing feature allocation need to assign manually.

upvoted 1 times

jerj5 8 months ago

Selected Answer: A

Correct

Dynamic Balancing (Dynamic Split) balances the load between Firewall instances and Secure Network Distributors (SNDs) by dynamically changing the number of instances and SNDs based on the current load.

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

Correct

upvoted 1 times

Question #85 *Topic 1*

Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

A. ip show int eth0

B. show interface eth0 mq

C. ifconfig –i eth0 verbose

D. ethtool –i eth0

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: D

[Expert@CP-FW03:0]# ethtool -i eth0
driver: e1000
version: 7.3.21-k8-NAPI
firmware-version:
expansion-rom-version:
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: no
[Expert@CP-FW03:0]

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: D

correct

upvoted 1 times

Question #86 *Topic 1*

What is the minimum number of CPU cores required to enable CoreXL?

A. 2

B. 1

C. 4

D. 6

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: A

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/Topics-PTG/CoreXL-Default-Configuration.htm

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

2 is correct

upvoted 1 times

Question #87 *Topic 1*

What does Backward Compatibility mean upgrading the Management Server and how can you check it?

A. The Management Server is able to manage older Gateways. The lowest supported version in the Installation and Upgrade Guide

B. The Management Server is able to manage older Gateways. The lowest supported version is documented in the Release Notes

C. You will be able to connect to older Management Server with the SmartConsole. The lowest supported version is documented in the Release Notes

D. You will be able to connect to older Management Server with the SmartConsole. The lowest supported version is documented in the Installation and Upgrade Guide

Correct Answer: *A*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 1 week, 3 days ago

Selected Answer: B

Backward Compatibility means that the Management Server can manage older versions of Security Gateways. The lowest supported version for this compatibility is documented in the Release Notes.

upvoted 1 times

57ad24d 2 months, 1 week ago

Selected Answer: B

Backward Compatibility in the context of upgrading a Check Point Management Server refers to its ability to manage older Security Gateways that are running a previous version of the software. This ensures a smooth transition during upgrades, as it allows the Management Server to maintain control over gateways that have not yet been upgraded to the same version.

upvoted 1 times

KuKuKu83 3 months, 1 week ago

Selected Answer: B

https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RN/Topics-RN/Backward-Compatibility.htm?tocpath=____7#Supported_Backward_Compatibility_Gateways

upvoted 1 times

Rajeshkashi 3 months, 2 weeks ago

Answer is B

upvoted 1 times

Question #88 *Topic 1*

How can you switch the active log file?

A. Run fw logswitch on the Management Server

B. Run fwm logswitch on the Management Server

C. Run fw logswitch on the gateway

D. Run fwm logswitch on the gateway

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: A

[Expert@MDM01:0]# fw logswitch
Log file has been switched to: 2024-09-27_223824.log
[Expert@MDM01:0]#

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: A

correct

upvoted 1 times

Question #89 *Topic 1*

What destination versions are supported for a Multi-Version Cluster Upgrade?

A. R77.30 and later

B. R80.10 and Later

C. R70 and Later

D. R76 and later

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

krzaki 3 weeks, 3 days ago

Selected Answer: A

The Multi-Version ClusterClosed (MVC) in an R81 Cluster MemberClosed supports synchronization with peer Cluster Members that run one of these versions:

R80.10 (or higher)*

R77.30

In a Multi-Version Cluster, the Cluster Members can run only these versions:

R81 and R80.10 (or higher)*

R81 and R77.30

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/MVC-Upgrade-Supported-Versions.htm

upvoted 1 times

premoli 3 months, 3 weeks ago

Selected Answer: B

Multi-Version Cluster (MVC) Upgrade

The Multi-Version Cluster (MVC) mechanism synchronizes connections between Cluster Members that run different versions.

You can upgrade to a newer version without a loss in connectivity and test the new version on some of the Cluster Members before you decide to upgrade the rest of the Cluster Members.

Important - The Multi-Version Cluster Upgrade replaced the Connectivity Upgrade.

upvoted 1 times

Question #90 *Topic 1*

Which command can you use to verify the number of active concurrent connections?

A. fw conn all

B. show all connections

C. fw ctl pstat

D. show connections

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

[Expert@CP-FW03:0]# fw ctl pstat

deleted some...

Connections
719 total, 562 TCP, 157 UDP, 0 ICMP,
0 other, 0 anticipated, 11 recovered, 9 concurrent,
515 peak concurrent

Fragments:
2 fragments, 1 packets, 0 expired, 0 short,
0 large, 0 duplicates, 0 failures

NAT:
0/0 forw, 0/0 bckw, 0 tcpudp,
0 icmp, 0-0 alloc

Sync: Run "cphaprob syncstat" for cluster sync statistics.

[Expert@CP-FW03:0]#

upvoted 1 times

jerj5 8 months ago

Selected Answer: C

Correct
fw ctl pstat - Shows Security Gateway various internal statistics:
System Capacity Summary
Hash kernel memory (hmem) statistics
System kernel memory (smem) statistics
Kernel memory (kmem) statistics
Cookies
Connections
Fragments
NAT
Handles

upvoted 1 times

Question #91 *Topic 1*

Under which file is the proxy arp configuration stored?

A. $FWDIR/state/_tmp/proxy.arp on the security gateway

B. $FWDIR/conf/local.arp on the management server

C. $FWDIR/conf/local.arp on the gateway

D. $FWDIR/state/proxy_arp.conf on the management server

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

https://www.wiresandwi.fi/blog/check-point-configuring-proxy-arp-non-vsx-gateway

upvoted 1 times

Question #92 *Topic 1*

What are the correct steps upgrading a HA cluster (M1 is active, M2 is passive) using Multi-Version Cluster(MVC)Upgrade?

A. 1) In SmartConsole, change the version of the cluster object
2) Upgrade the passive node M2 to R81.20
3) Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 in CLISH: set cluster member mvc on
4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy SmartConsole, change the version of the cluster object,

B. 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on
2) Upgrade the passive node M2 to R81.20
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy

C. 1) Enable the MVC mechanism on both cluster members in CLISH: set cluster member mvc on
2) Upgrade the passive node M2 to R81.20
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism

D. 1) Upgrade the passive node M2 to R81.20
2) Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 #cphaconf mvc on
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.20

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Jallic 1 month, 4 weeks ago

Selected Answer: A

Looking at this again, C is missing a second policy push for M1.
So this is not totally correct either.
Out of the two A would seem to have all the steps required (with the exception setting the cluster object version in step 6 which is not required as this was set in Step1).

upvoted 1 times

Jallic 2 months ago

Selected Answer: C

I would have sad A, however step 6 makes no sense ie. change the "version of the cluster object". This was done in step1.

So I believe C is the correct answer here. Please feel free to correct me with the explanation as to why you would need to change the version to R81.20 'twice'.

upvoted 1 times

premoli 3 months, 3 weeks ago

Selected Answer: A

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/MVC-Upgrade-of-ClusterXL-GW-mtocpath=Upgrade%20of%20Security%20Gateways%20and%20Clusters%7CUpgrading%20ClusterXL%252C%20VSX%20Cluster%252C%20or%20VRRP%20CluVersion%20Cluster%20(MVC)%20Upgrade%7C____4

upvoted 1 times

coolbacha 7 months, 3 weeks ago

A is correct

upvoted 2 times

Question #93 *Topic 1*

You pushed a policy to your gateway, and you cannot access the gateway remotely anymore. What command should you use to remove the policy from the gateway by logging in through console access?

A. “fw unloadpolicy”

B. “fw unloadlocal”

C. “fw cpstop”

D. “fw undo”

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 1 week, 3 days ago

Selected Answer: B

This command uninstalls all policies from the Security Gateway or Cluster Member, allowing you to regain access. However, please note that this command will prevent all traffic from passing through the Security Gateway because it disables IP Forwarding in the Linux kernel and removes all policies, leaving the gateway unprotected.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

fw unloadlocal

[Expert@CP-FW01:0]# fw unloadlocal

Uninstalling Security Policy from all.all@CP-FW01
Done.
[Expert@CP-FW01:0]#

this command safe a lot of trouble.

upvoted 1 times

Question #94 *Topic 1*

Which command would disable a Cluster Member permanently?

A. clusterXL_admin_down

B. cphaprob_admin down

C. clusterXL_admin down –p

D. set clusterXL down –p

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 1 week, 3 days ago

Selected Answer: C

This command sets the Cluster Member to an administratively down state and makes the change persistent across reboots.

upvoted 1 times

Ziamsu 5 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

KuKuKu83 9 months, 2 weeks ago

Selected Answer: C

clusterXL_admin down-p

upvoted 2 times

Question #95 *Topic 1*

While using the Gaia CLI, what is the correct command to publish changes to the management server?

A. json publish

B. mgmt publish

C. mgmt._cli commit

D. commit

Correct Answer: *B*

Community vote distribution

Community vote distribution

Ziamsu 5 months, 2 weeks ago

Selected Answer: B

CP-FW01> mgmt publish
MGMT9205 You are not logged in to management server, in order to log-in you will need to run "mgmt login user [user name]"
CP-FW01> mgmt login user admin
Enter password:
CP-FW01> mgmt publish

Time: [11:14:56] 28/9/2024

"Publish operation" succeeded (100%)
tasks:
- task-id: "01234567-89ab-cdef-a084-44209a48af35"
task-name: "Publish operation"
status: "succeeded"
progress-percentage: 100
suppressed: false
task-details:
- publishResponse:
numberOfPublishedChanges: 0
mode: "async"
revision: "d0889331-67e5-4698-a541-4816325e74be"

CP-FW01>

upvoted 1 times

lironzruya7 7 months ago

Selected Answer: B

mgmt publish

upvoted 1 times

jerj5 8 months ago

Selected Answer: B

Correct
Example
> mgmt add host name myHost12 ip-address 3.3.3.3
> mgmt publish