Question #1 *Topic 1*

Which command collects diagnostic data for analyzing customer setup remotely?

A. cpinfo

B. migrate export

C. sysinfo

D. cpview

Suggested Answer: *A*
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 utility for uploading files to Check Point servers).
The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92739

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

Question #2 *Topic 1*

When deploying multiple clustered firewalls on the same subnet, what does the firewall administrator need to configure to prevent CCP broadcasts being sent to the wrong cluster?

A. Set the fwha_mac_magic_forward parameter in the $CPDIR/boot/modules/ha_boot. conf

B. Set the fwha_mac_magic parameter in the $FWDIR/boot/fwkern.conf file

C. Set the cluster global ID using the command "cphaconf cluster_id set <value>"

D. Set the cluster global ID using the command "fw ctt set cluster_id <value>"

Suggested Answer: *C*

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

Question #3 *Topic 1*

Which of these options is an implicit MEP option?

A. Primary-backup

B. Source address based

C. Round robin

D. Load Sharing

Suggested Answer: *A*

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

Question #4 *Topic 1*

John detected high load on sync interface. Which is most recommended solution?

A. For short connections like http service – delay sync for 2 seconds

B. Add a second interface to handle sync traffic

C. For short connections like http service – do not sync

D. For short connections like icmp service – delay sync for 2 seconds

Suggested Answer: *A*

Nikolas 5 years, 5 months ago

from CCSE R80 guide:
For all TCP services whose protocol type is HTTP or None, you can configure the Security Gateway to delay a connection so that it will only be synchronized if it still exists after the connection is initiated for x seconds. This capability is only available if a SecureXL-enabled device is installed on the gateway.

upvoted 3 times

Question #5 *Topic 1*

What is the SOLR database for?

A. Used for full text search and enables powerful matching capabilities

B. Writes data to the database and full text search

C. Serves GUI responsible to transfer request to the DLEserver

D. Enables powerful matching capabilities and writes data to the database

Suggested Answer: *A*

Nikolas 5 years, 5 months ago

from CCSE R80 guide:
CPM saves all data in the Postgres SQL database and stores most of the data in Solr, a standalone search server powered by the Lucene Java search library. The Postgres SQL database contains objects, policies, users, administrators, licenses, and management data.The data is segmented into multiple database domains. Solr generates indexes of the data to be used for full text searching capabilities.

upvoted 3 times

Question #6 *Topic 1*

What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

A. Stateful Mode

B. VPN Routing Mode

C. Wire Mode

D. Stateless Mode

Suggested Answer: *C*
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure
VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30974

Nikolas 5 years, 5 months ago
from CCSE R80 guide:
Wire Mode enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection. Using Wire Mode, the Firewall can be bypassed for VPN connections by defining internal interfaces and communities as “trusted”. This improves the performance of the VPN tunnel and reduces downtime. With Stateful Inspection no longer taking place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed.
upvoted 2 times

Question #7 *Topic 1*

On R80.10 the IPS Blade is managed by:

A. Threat Protection policy

B. Anti-Bot Blade

C. Threat Prevention policy

D. Layers on Firewall policy

Suggested Answer: *A*
Reference:
https://www.checkpoint.com/downloads/product-related/r80.10-mgmt-architecture-overview.pdf very top of last page.

lucky Highly Voted 7 years, 2 months ago
Correct answer should be C. Threat Prevention Policy
upvoted 8 times

chieNchan Most Recent 4 years, 8 months ago
Must be letter C
upvoted 2 times

spaskprost 5 years, 6 months ago
yep, it's threat prevention policy.
upvoted 2 times

sameerbasha 5 years, 6 months ago
correct answer is C
upvoted 2 times

Derbot 5 years, 9 months ago
In R80.10, the IPS Blade is managed by the Threat Prevention policy.
upvoted 2 times

trymo036h 6 years, 4 months ago
Agreed, correct answer should be Threat Prevention Policy
upvoted 4 times

Question #8 *Topic 1*

Which packet info is ignored with Session Rate Acceleration?

A. source port ranges

B. source ip

C. source port

D. same info from Packet Acceleration is used

Suggested Answer: *C*
Reference: http://trlj.blogspot.com/2015/10/check-point-acceleration.html

Nikolas 5 years, 5 months ago
correct, from CCSE R80 guide:
As an example, the source port of a packet flow may be masked off, effectively providing a
global match for source port. Once a flow is validated and established, SecureXL creates and saves a template of that flow with the source port masked off. Any new connection setup packet that matches the other 4 attributes is processed on the accelerated path, thus avoiding Firewall inspection and additional computing overhead. Security is not impacted because the operating system continues to track the state of the new connection using Stateful Inspection
upvoted 2 times

Question #9 *Topic 1*

What is the purpose of Priority Delta in VRRP?

A. When a box is up, Effective Priority = Priority + Priority Delta

B. When an Interface is up, Effective Priority = Priority + Priority Delta

C. When an Interface fail, Effective Priority = Priority – Priority Delta

D. When a box fail, Effective Priority = Priority – Priority Delta

Suggested Answer: *C*

Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP.

If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP

HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will beging to send out its own HELLO packet.

Once the master sees this packet with a priority greater than its own, then it releases the VIP.

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk38524

iceoeu 5 years, 3 months ago

sk38524(What is VRRP Monitored Circuits):If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet.

upvoted 1 times

Question #10 *Topic 1*

What is the purpose of a SmartEvent Correlation Unit?

A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server

B. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.

C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.

D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server

Suggested Answer: *C*

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

Question #11 *Topic 1*

The CDT utility supports which of the following?

A. Major version upgrades to R77.30

B. Only Jumbo HFA's and hotfixes

C. Only major version upgrades to R80.10

D. All upgrades

Suggested Answer: *D*
The Central Deployment Tool (CDT) is a utility that runs on an R77 / R77.X / R80 / R80.10 Security Management Server / Multi-Domain Security Management
Server (running Gaia OS).
It allows the administrator to automatically install CPUSE Offline packages (Hotfixes, Jumbo Hotfix Accumulators (Bundles), Upgrade to a Minor Version, Upgrade to a Major Version) on multiple managed Security Gateways and Cluster Members at the same time.
Reference: https://community.checkpoint.com/thread/5319-my-top-3-check-point-cli-commands

iceoeu 5 years, 3 months ago
"B. Only Jumbo HFA's and hotfixes - is not correct". From manual for CDT - Advanced mode - "Best Practice - We recommend this mode to deploy more than one package in the same CDT execution. For example: Major Upgrade and Jumbo Hotfix Accumulator."
upvoted 1 times

Nikolas 5 years, 5 months ago
i think answer is B
from CCSE R80 guide:
Automatic installation on multiple managed gateways and cluster members is supported for the following package types:
• Upgrades to R77.30
• Minor version upgrades
• Hotfixes
• Jumbo Hotfixes (bundles) or HFAs

Do not use CDT for clean installs of a major version. Also, CDT does not support upgrades or installs of ClusterXL in Load Sharing mode.
upvoted 1 times

Question #12 *Topic 1*

The Firewall kernel is replicated multiple times, therefore:

A. The Firewall kernel only touches the packet if the connection is accelerated

B. The Firewall can run different policies per core

C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out

D. The Firewall can run the same policy on all cores

Suggested Answer: *D*
On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core.
These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_PerformanceTuning_WebAdmin/6731.htm

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

Question #13 *Topic 1*

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

A. Symmetric routing

B. Failovers

C. Asymmetric routing

D. Anti-Spoofing

Suggested Answer: *C*

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

Question #14 *Topic 1*

Which is not a blade option when configuring SmartEvent?

A. Correlation Unit

B. SmartEvent Unit

C. SmartEvent Server

D. Log Server

Suggested Answer: *B*
On the Management tab, enable these Software Blades:
⇨ Logging & Status
⇨ SmartEvent Server
⇨ SmartEvent Correlation Unit
Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/120829

redenergizer 3 years, 4 months ago

C:
The SDF is required in cases of Asymmetric Routing. In these cases, the packet is modified by
the cluster member, and since the packet entering the Firewall is not the same as the one
leaving, the regular decision function will not be able to make sure that the packet will go back through the original member. The SDF will try to match each packet to numerous kernel tables in an attempt to decide which member should handle the packet.
upvoted 1 times

Question #15 *Topic 1*

What command would show the API server status?

A. cpm status

B. api restart

C. api status

D. show api status

Suggested Answer: *C*

Reference: https://www.hurricanelabs.com/blog/check-point-api-merging-management-servers-with-r80-10

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

Question #16 *Topic 1*

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You dont have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw cti multik dynamic_dispatching on

B. fw cti multik dynamic_dispatching set_mode 9

C. fw cti multik set_mode 9

D. fw cti multik pq enable

Suggested Answer: *C*
To fully enable the CoreXL Dynamic Dispatcher on Security Gateway:
1. Run in Expert mode:
[Expert@HostName]# fw ctl multik set_mode 9
:
[Expert@R77.30:0]# fw ctl multik set_mode 9

Please reboot the system -
[Expert@R77.30:0]#
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk105261

Community vote distribution
A (50%) B (50%)

FMorales 1 year, 2 months ago

Selected Answer: A
Configuration on Security Gateway R80.10 and higher.
[Expert@R80.10:0]# fw ctl multik dynamic_dispatching on
New mode is: On
Please reboot the system
[Expert@R80.10:0]#
https://support.checkpoint.com/results/sk/sk105261
upvoted 1 times

FMorales 1 year, 2 months ago

Selected Answer: B
Configuration on Security Gateway R80.10 and higher.
[Expert@R80.10:0]# fw ctl multik dynamic_dispatching on
New mode is: On
Please reboot the system
[Expert@R80.10:0]#
https://support.checkpoint.com/results/sk/sk105261
upvoted 1 times

mmenen 4 years, 5 months ago

A (from my poin of view):

[Expert@mmenen-GW-1:0]# fw ctl multik set_mode 9
Usage:
fw ctl multik stat
fw ctl multik start
fw ctl multik stop
fw ctl multik utilize
fw ctl multik print_heavy_conn
fw ctl multik heavy_conn_analyzer
fw ctl multik get_instance [command args...]

fw ctl multik dynamic_dispatching [command args...]
fw ctl multik prioq [command args...]
fw ctl multik print_bl [command args...]
fw ctl multik gconn [command args...]
[Expert@mmenen-GW-1:0]# fw ctl multik dynamic_dispatching on
New mode is: On
Please reboot the system
upvoted 1 times

Checky_McPoint 5 years, 3 months ago
All questions are wrong, since it's "ctl" and not "cti".

Jokes aside. Without the typo A is the closest answer, since C would be for R77.30 only.

In R80.10 and above Priority Queue is set to 'deactivated' by default and is no longer related to Dynamic Dispatcher as it was in R77.x. The Heavy Connections mechanism (Evaluator only mode) is enabled by default ("#fw ctl multik prioq" -> 1). See sk105762, VIII. for details.

Thus to my understanding the command "#fw ctl multik prioq" -> 2 has to be executed as well to fully enable Priority Queue.
upvoted 2 times

Synchronized 5 years, 3 months ago
According to SK105261 Answer C is the right one.

To fully enable the CoreXL Dynamic Dispatcher on Security Gateway:

Note: In cluster environment, this procedure must be performed on all members of the cluster. Since a reboot is required, it is recommended to follow the Gaia Installation and Upgrade Guide - either "Minimal Effort" procedure, or "Zero Downtime" procedure.

Run in Expert mode:

[Expert@HostName]# fw ctl multik set_mode 9

Example output:

[Expert@R77.30:0]# fw ctl multik set_mode 9
Please reboot the system
[Expert@R77.30:0]#
Reboot (in cluster, this might cause fail-over).
upvoted 1 times

Nikolas 5 years, 5 months ago
agree, answer is A
upvoted 1 times

bulerias 5 years, 6 months ago
According to CCSE Manual, page 418: "To fully enable Dynamic Dispatcher on a Security Gateway, run the following command in expert mode and tgen reboot : fw ctl multik dynamic_dispatching on".
upvoted 2 times

ToadRobertson2 5 years, 7 months ago
According to Check Point, the correct answer in R80.10 is none of those options:

"Set the mode of the Firewall Priority Queues on Security Gateway to enabled:

R80.10: [Expert@HostName]# fw ctl multik prioq
Select mode 2 "On".

R77.30: [Expert@HostName]# fw ctl multik set_mode 9
upvoted 1 times

Snir 5 years, 9 months ago

Correct answer A for R80 and above

upvoted 2 times

Question #17 *Topic 1*

You have existing dbedit scripts from R77. Can you use them with R80.10?

A. dbedit is not supported in R80.10

B. dbedit is fully supported in R80.10

C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers

D. dbedit scripts are being replaced by mgmt._cli in R80.10

Suggested Answer: *D*
dbedit (or GuiDbEdit) uses the cpmi protocol which is gradually being replaced by the new R80.10 automation architecture. cpmi clients are still supported in
R80.10, but there are some functionalities that cannot be managed by cpmi anymore. For example, the Access and Threat policies do not have a cpmi representation. They can be managed only by the new mgmt_cli and not by cpmi clients. There are still many tables that have an inner cpmi representation (for example, network objects, services, servers, and global properties) and can still be managed using cpmi.
Reference:
https://www.checkpoint.com/downloads/product-related/r80.10-mgmt-architecture-overview.pdf

TienTM 4 years, 8 months ago
I test with R80.10 dbedit still using normally. So for me B is correct answer
upvoted 1 times

Question #18 *Topic 1*

SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

A. This statement is true because SecureXL does improve all traffic

B. This statement is false because SecureXL does not improve this traffic but CoreXL does

C. This statement is true because SecureXL does improve this traffic

D. This statement is false because encrypted traffic cannot be inspected

Suggested Answer: *C*
SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.
Reference:
https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/10001/FILE/SecureXL_and_Nokia_IPSO_White_Paper_20080401.pdf

Nikolas 5 years, 5 months ago
correct, from CCSE R80 guide:
SecureXL improves non-encrypted Firewall traffic throughput and encrypted (VPN) traffic throughput by a significant amount, particularly for small packets flowing in long duration connections.
upvoted 1 times

Question #19 *Topic 1*

What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect

B. Capsule Workspace, Capsule Cloud, Capsule Connect

C. Capsule Workspace, Capsule Docs, Capsule Connect

D. Capsule Workspace, Capsule Docs, Capsule Cloud

Suggested Answer: *D*

Reference: https://www.checkpoint.com/solutions/mobile-security/check-point-capsule/

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

Question #20 *Topic 1*

Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

A. mgmt_cli add-host "Server_1" ip_ address "10.15.123.10" – format txt

B. mgmt_ cli add host name "Server_ 1" ip-address "10.15.123.10" – format json

C. mgmt_ cli add object-host "Server_ 1" ip-address "10.15.123.10" – format json

D. mgmt_cli add object "Server_ 1" ip-address "10.15.123.10" – format json

Suggested Answer: *B*
Example:
mgmt_cli add host name "New Host 1" ip-address "192.0.2.1" --format json
"--format json" is optional. By default the output is presented in plain text.
Reference: https://sc1.checkpoint.com/documents/latest/APIs/index.html#cli/add-host~v1.1%20

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

Question #21 *Topic 1*

When defining QoS global properties, which option below is not valid?

A. Weight

B. Authenticated timeout

C. Schedule

D. Rate

Suggested Answer: *C*
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_QoS_AdminGuide/14871.htm

Checky_McPoint 5 years, 3 months ago
C is correct, but document is outdated. R80.10 Admin Guide:
https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_QoS_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_QoS_AdminGuide/128687
upvoted 1 times

Question #22 *Topic 1*

Check Point APIs allow system engineers and developers to make changes to their organizations security policy with CLI tools and Web Services for all of the following except? rd

A. Create new dashboards to manage 3 party task

B. Create products that use and enhance 3 rd party solutions.

C. Execute automated scripts to perform common tasks.

D. Create products that use and enhance the Check Point Solution.

Suggested Answer: *A*
Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:
☞ Use an automated script to perform common tasks
☞ Integrate Check Point products with 3rd party solutions
☞ Create products that use and enhance the Check Point solution
Reference:
http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf?HashKey=1522190468_125d63ea5296b7dadd3e4fd81c708cc5&xtn=.pdf

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

Question #23 *Topic 1*

What happen when IPS profile is set in Detect-Only Mode for troubleshooting?

A. It will generate Geo-Protection traffic

B. Automatically uploads debugging logs to Check Point Support Center

C. It will not block malicious traffic

D. Bypass licenses requirement for Geo-Protection control

Suggested Answer: *C*
It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic. During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IPS_AdminGuide/12750.htm

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

Question #24 *Topic 1*

When simulating a problem on CLusterXL cluster with cphaprob d STOP s problem t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

A. cphaprob –d STOP unregister

B. cphaprob STOP unregister

C. cphaprob unregister STOP

D. cphaprob –d unregister STOP

Suggested Answer: *A*
esting a failover in a controlled manner using following command;
cphaprob -d STOP -s problem -t 0 register
This will register a problem state on the cluster member this was entered on;
If you then run;
cphaprob list
this will show an entry named STOP.
to remove this problematic register run following;
cphaprob -d STOP unregister
Reference: https://fwknowledge.wordpress.com/2013/04/04/manual-failover-of-the-fw-cluster/

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