Question #1 *Topic 1*

Which default Gaia user has full read/write access?

A. superuser

B. monitor

C. altuser

D. admin

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

The_Nart 4 months, 1 week ago

It's D

upvoted 1 times

RabinRam 10 months, 4 weeks ago

Selected Answer: D

it is admin

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: D

It's Admin

upvoted 2 times

Question #2 *Topic 1*

Which icon in the WebUI indicates that read/write access is enabled?

A. Eyeglasses

B. Pencil

C. Padlock

D. Book

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

21beaf1 8 months, 2 weeks ago

Its pencil

upvoted 1 times

RabinRam 10 months, 4 weeks ago

Selected Answer: B

its Pencil

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: B

It's B

upvoted 2 times

YorelPT 1 year, 3 months ago

I thiink the correct is C

upvoted 1 times

YorelPT 1 year, 3 months ago

My answer was wrong, B is the correct one (Pencil)

upvoted 1 times

Question #3 *Topic 1*

Which SmartConsole tab is used to monitor network and security performance?

A. Logs Monitor

B. Manage Settings

C. Security Policies

D. Gateway Servers

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Jennifer_Solomon_Divekar 8 months, 2 weeks ago

A is the Answer

upvoted 1 times

kpapani 10 months, 2 weeks ago

A is correct.

SmartConsole and SmartView Monitor provide a complete picture of network and security performance. Page 751, Kortex for R81.20

SmartView Monitor is opened via Logs and Monitor tab.

upvoted 1 times

RabinRam 10 months, 4 weeks ago

Selected Answer: A

It is A

upvoted 1 times

Maxim_E 1 year ago

I think it's D. Perfomance and traffic counters are in Device & License Information which is on the Gateways Servers tab.

upvoted 3 times

aikaloge 1 year, 2 months ago

Selected Answer: A

It's A

upvoted 2 times

YorelPT 1 year, 3 months ago

The right one is D

upvoted 2 times

Question #4 *Topic 1*

Check Point Update Service Engine (CPUSE), also known as Deployment Agent [DA], is an advanced and intuitive mechanism for software deployment on Gaia OS. What software packages are supported for deployment?

A. It supports deployments of single HotFixes (HF), and of Major Versions. Blink Packages and HotFix Accumulators (Jumbo) are not supported.

B. It supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), and of Major Versions.

C. It supports deployments of Major Versions and Blink packages only.

D. It supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), but not of Major Versions.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

RabinRam 4 months, 3 weeks ago

Selected Answer: B

it is B

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: B

B. It supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), and of Major Versions.

upvoted 1 times

Halbling 5 months, 3 weeks ago

Even BLINK packages are supported by CPUSE. Still B is the best option.

upvoted 1 times

diegofretesc 7 months ago

Selected Answer: B

Es el B

upvoted 1 times

honoriogab 7 months, 2 weeks ago

Actually it's A, tested in Gaia by now

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 3 times

YorelPT 9 months, 3 weeks ago

B is correct: https://supportcenter.us.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92449

upvoted 3 times

Question #5 *Topic 1*

In SmartConsole, on which tab are Permissions and Administrators defined?

A. MANAGE & SETTINGS

B. SECURITY POLICIES

C. GATEWAYS & SERVERS

D. LOGS & MONITOR

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

The_Nart 4 months, 1 week ago

It's A

upvoted 1 times

LEGATTO 5 months ago

Selected Answer: A

correct answer A

upvoted 1 times

Cbscrt 9 months ago

Selected Answer: A

It's A

upvoted 1 times

honoriogab 1 year, 1 month ago

Selected Answer: A

It's A

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: A

It's A

upvoted 1 times

Question #6 *Topic 1*

Which tool allows automatic update of Gaia OS and Check Point products installed on Gaia OS?

A. CPDAS - Check Point Deployment Agent Service

B. CPUSE - Check Point Upgrade Service Engine

C. CPASE - Check Point Automatic Service Engine

D. CPAUE - Check Point Automatic Update Engine

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 2 times

Question #7 *Topic 1*

In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server?

A. Verify and compile Security Policies.

B. Display policies and logs on the administrator's workstation.

C. Store firewall logs to hard drive storage.

D. Manage the object database.

Correct Answer: *B*

Community vote distribution

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: B

B. Display policies and logs on the administrator's workstation.

In the Check Point three-tiered architecture, the Security Management Server does not directly display policies and logs on the administrator's workstation. This function is typically handled by the SmartConsole application, which connects to the Security Management Server to retrieve and display this information.

upvoted 1 times

LEGATT0 5 months ago

Selected Answer: B

Smart console is reponsible for this function

upvoted 1 times

hak01 5 months, 2 weeks ago

The correct answer is B. Display policies and logs on the administrator's workstation.
This task is typically handled by the SmartConsole application, which connects to the Security Management Server to retrieve and display this information.

upvoted 1 times

67578ac 8 months, 2 weeks ago

Selected Answer: B

Display policies and logs on the admin workstation is a Smart Console feature.

upvoted 1 times

mydoglikesboobs 9 months ago

it's B. While the Security Management Server stores and manages policies and logs, it does not directly display them on the administrator's workstation. This task is typically handled by the SmartConsole application, which connects to the Security Management Server to retrieve and display this information.

upvoted 1 times

JimDiGriz 10 months, 2 weeks ago

Selected Answer: C

C. Store firewall logs to hard drive storage.

The Security Management Server primarily handles tasks such as verifying and compiling security policies, managing the object database, and displaying policies and logs on the administrator's workstation. Storing firewall logs to hard drive storage is usually the responsibility of the Security Gateway.

upvoted 1 times

mydoglikesboobs 9 months ago

Policies are shown by smart console not the manager.

upvoted 4 times

aikaloge 1 year, 2 months ago

Selected Answer: B

It's B

upvoted 2 times

tosyeno 1 year, 3 months ago

B

It's only smartconsole that display logs on administrator's workstation

upvoted 4 times

Question #8 *Topic 1*

True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.

A. True, every administrator works on a different database that is independent of the other administrators

B. False, only one administrator can login with write permission

C. True, every administrator works in a session that is independent of the other administrators

D. False, this feature has to be enabled in the Global Properties

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

67578ac 8 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: C

It's C

upvoted 3 times

Question #9 *Topic 1*

What Check Point tool is used to automatically update Check Point products for the Gaia OS?

A. Check Point Update Engine

B. Check Point Upgrade Installation Service

C. Check Point Upgrade Service Engine (CPUSE)

D. Check Point INSPECT Engine

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

aikaloge 8 months, 4 weeks ago

Selected Answer: C

It's C

upvoted 1 times

Question #10 *Topic 1*

If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

A. Delete older versions of database.

B. Publish or discard the session.

C. Revert the session.

D. Save and install the Policy.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: B

It's B

upvoted 1 times

diegofretesc 6 months, 3 weeks ago

Selected Answer: B

yo creo que es B

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Question #11 *Topic 1*

What are the two deployment options available for a security gateway?

A. Bridge and Switch

B. Local and Remote

C. Cloud and Router

D. Standalone and Distributed

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

freefreefree1 1 month ago

Selected Answer: D

D D D D DD !

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: D

D. Standalone and Distributed

upvoted 1 times

diegofretesc 6 months, 3 weeks ago

Selected Answer: D

es D..

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: D

It's D

upvoted 1 times

Question #12 *Topic 1*

One of major features in SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

A. AdminB sees a pencil icon next the rule that AdminB is currently editing.

B. AdminA, AdminB and AdminC are editing three different rules at the same time.

C. AdminA and AdminB are editing the same rule at the same time.

D. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: C

C. AdminA and AdminB are editing the same rule at the same time.

In SmartConsole, concurrent administration allows multiple administrators to work on the same Security Policy simultaneously. However, two administrators cannot edit the same rule at the same time. When one administrator is editing a rule, it is locked for editing by others, and they will see a lock icon indicating that the rule is currently being edited by another administrator.

upvoted 2 times

EssentialD 11 months, 3 weeks ago

Selected Answer: C

C. AdminA and AdminB are editing the same rule at the same time.

upvoted 1 times

aikaloge 1 year, 2 months ago

It's C

upvoted 1 times

tosyeno 1 year, 3 months ago

Selected Answer: C

two Admins cannot edit same policy object at the same time

upvoted 3 times

Question #13 *Topic 1*

Which one of the following is the preferred licensing model? Select the BEST answer.

A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.

B. Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.

C. Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency on the gateway.

D. Central licensing because it ties the package license to the MAC-address of the Security Management Server's Mgmt-interface and has no dependency on the gateway.

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

geekchicadee 2 months, 1 week ago

Selected Answer: C

https://support.checkpoint.com/results/sk/sk62685

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: C

It's C

upvoted 2 times

Question #14 *Topic 1*

A Check Point Software license consists of two components, the Software Blade and the Software Container. There are ____ types of Software Containers: ____.

A. Two; Security Management and Endpoint Security

B. Three; Security Management, Security Gateway, and Endpoint Security

C. Three; Security Gateway, Endpoint Security, and Gateway Management

D. Two; Endpoint Security and Security Gateway

Correct Answer: *B*

Community vote distribution

Community vote distribution

Bombast Highly Voted 8 months, 3 weeks ago

B it`s correct
https://dl3.checkpoint.com/paid/a8/a81bd8771f3d7bf40a269f64f5b536e7/QuickLicenseGuide.pdf?HashKey=1703189421_16327e393007d8bf8f9de67755d7db72&xtn=.pdf

Software Container
The Software Container is a logical component in the Software Blade Architecture. There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security. The container enables the server functionality, and defines its purpose – e.g, management or gateway. When generated, the license will contain features for the Software Container as well as all Software Blades which are attached to the container.

upvoted 6 times

EssentialD Most Recent 5 months, 2 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Banand 6 months ago

Answer B is correct

upvoted 1 times

juandiegope 7 months, 1 week ago

Selected Answer: B

There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security

upvoted 2 times

BillNosie 7 months, 2 weeks ago

Selected Answer: B

B is correct. There is no Gateway Management.

upvoted 2 times

swindonjogger 8 months, 3 weeks ago

C (see Checkpoint Software Blade quick licensing guide)

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Wrong It's B

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: C

It's C

upvoted 1 times

YorelPT 8 months, 1 week ago

Can't be C cause Gateway Management doesn't exist.

upvoted 1 times

Question #15 *Topic 1*

Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

A. Formal

B. Central

C. Local

D. Corporate

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

geekchicadee 2 months, 1 week ago

Selected Answer: C

https://support.checkpoint.com/results/sk/sk62685

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: C

C. Local

upvoted 1 times

aikaloge 8 months, 4 weeks ago

It's C

upvoted 2 times

Question #16 *Topic 1*

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

A. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.

B. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.

C. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

D. Tom's changes will be lost since he lost connectivity and he will have to start again.

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: C

C. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

upvoted 2 times

aikaloge 8 months, 4 weeks ago

It's C

upvoted 1 times

Question #17 *Topic 1*

In which deployment is the security management server and Security Gateway installed on the same appliance?

A. Switch

B. Standalone

C. Distributed

D. Remote

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

sudya189 3 months, 1 week ago

Selected Answer: B

Standalone

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: B

B. Standalone

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Question #18 *Topic 1*

Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

A. Data Awareness

B. Threat Emulation

C. Application Control

D. Identity Awareness

Correct Answer: *C*

Community vote distribution

Community vote distribution

tosyeno Highly Voted 1 year, 3 months ago

Selected Answer: D

After you activate the Identity Awareness Software Blade, you can create access role objects and use them in the Source and Destination columns of Access Control Policy rules.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Access-Roles.htm?Highlight=identity%20awareness

upvoted 5 times

VadimKaraluba Most Recent 1 week, 1 day ago

Selected Answer: D

As CP employ, D

upvoted 1 times

CountryLance 1 month, 2 weeks ago

Selected Answer: D

Identity awareness blade ENABLES the access control policy to accept/drop/limit. Keyword is enable. The IA blade makes it possible for the App Control blade to block/accept/limit

upvoted 1 times

keikei1228 3 months, 2 weeks ago

Selected Answer: C

C. Application Control

Application Control allows granular control over specific web-enabled applications and can enforce policies based on user, group, and machine.

Identity Awareness is indeed a crucial software blade that helps in identifying users and machines, allowing for more granular access control policies. However, it does not directly control or limit website access. Instead, it works in conjunction with other blades to provide identity-based access control.

upvoted 3 times

r_mcr 3 months, 3 weeks ago

Selected Answer: C

C.The software blade that enables Access Control policies to accept, drop, or limit website access based on user, group, and/or machine is the Application Control Software Blade. This blade allows for granular control over web applications and network protocols, enabling you to create policies based on users or groups to identify, block, or limit usage of web applications.

upvoted 2 times

r_mcr 3 months, 3 weeks ago

C.The software blade that enables Access Control policies to accept, drop, or limit website access based on user, group, and/or machine is the Application Control Software Blade. This blade allows for granular control over web applications and network protocols, enabling you to create policies based on users or groups to identify, block, or limit usage of web applications.

upvoted 2 times

whoamii 3 months, 3 weeks ago

Selected Answer: C

C. Application Control

The Application Control software blade allows Access Control policies to accept, drop, or limit access to websites and applications based on user, group, and/or machine criteria.

upvoted 2 times

EssentialD 11 months, 3 weeks ago

Selected Answer: B

D. Identity Awareness

upvoted 2 times

aikaloge 1 year, 2 months ago

Selected Answer: D

It's D

upvoted 2 times

Question #19 *Topic 1*

DLP and Mobile Access Policy are examples of what type of Policy?

A. Shared Policies

B. Unified Policies

C. Inspection Policies

D. Standard Policies

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: A

A. Shared Policies

Data Loss Prevention and Mobile Access Policy are examples of Shared Policies. These policies are not part of a specific policy package and are shared between all policy packages.

upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: A

A. Shared Policies

upvoted 1 times

Bombast 1 year, 2 months ago

A

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/SmartConsole-Toolbars-Shared-Policies.htm

upvoted 1 times

aikaloge 1 year, 2 months ago

It's A

upvoted 1 times

Question #20 *Topic 1*

What is the default shell of Gaia CLI?

A. Read-only

B. Expert

C. Clish

D. Bash

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

aikaloge 8 months, 4 weeks ago

Selected Answer: C

It's C

upvoted 1 times

Question #21 *Topic 1*

Which of the following is NOT a valid application navigation tab in SmartConsole?

A. WEBUI & COMMAND LINE

B. SECURITY POLICIES

C. GATEWAYS & SERVERS

D. LOGS & MONITOR

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: A

A. WEBUI & COMMAND LINE

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: A

It's A

upvoted 1 times

Question #22 *Topic 1*

What are two basic rules Check Point recommends for building an effective security policy?

A. Accept Rule and Drop Rule

B. Explicit Rule and Implied Rule

C. Cleanup Rule and Stealth Rule

D. NAT Rule and Reject Rule

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: C

C. Cleanup Rule and Stealth Rule

Check Point recommends the following two basic rules for building an effective security policy:

Stealth Rule: This rule prevents direct access to the Security Gateway.
Cleanup Rule: This rule drops all traffic that is not matched by the earlier rules in the policy

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: C

It's C

upvoted 1 times

AlF8812 1 year, 2 months ago

Selected Answer: C

Referred pages 379 & 380
C is Correct

upvoted 1 times

Melhi 7 months, 2 weeks ago

what doc these pages are from, please?

upvoted 1 times

Question #23 *Topic 1*

When dealing with policy layers, what two layer types can be utilized?

A. Inbound Layers and Outbound Layers

B. Ordered Layers and Inline Layers

C. Structured Layers and Overlap Layers

D. R81.X does not support Layers

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: B

B. Ordered Layers and Inline Layers

upvoted 1 times

Bombast 8 months, 3 weeks ago

B

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Ordered-Layers-and-Inline-Layers.htm

upvoted 2 times

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Question #24 *Topic 1*

What are the three main components of Check Point security management architecture?

A. Smart Console, Standalone, Security Management Server

B. Policy-Client, Security Management Server, Security Gateway

C. SmartConsole, Security Policy Server, Logs & Monitoring

D. SmartConsole, Security Management Server, Security Gateway

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: D

D. SmartConsole, Security Management Server, Security Gateway

upvoted 2 times

Bombast 8 months, 3 weeks ago

D

Three Tier Architecture components. The main product of Check Point is the network security solution – Next Generation Firewall (NGFW). When working with it, you will encounter three main components: Security Gateway, Security Management Server and SmartConsole

upvoted 2 times

aikaloge 8 months, 4 weeks ago

Selected Answer: D

It's D

upvoted 1 times

Question #25 *Topic 1*

Which Check Point software blade provides protection from zero-day and undiscovered threats?

A. Threat Extraction

B. Threat Emulation

C. Firewall

D. Application Control

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: B

B. Threat Emulation

upvoted 1 times

Bombast 8 months, 3 weeks ago

B

Check Point SandBlast Threat Emulation prevents infections from zero-day threats, new malware and targeted attacks. As part of the SandBlast™ Zero-Day Protection solution, this innovative sandboxing engine delivers the best possible catch rate for threats and is virtually immune to attackers' evasion techniques

upvoted 3 times

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Question #26 *Topic 1*

What are the three types of UserCheck messages?

A. ask, block, and notify

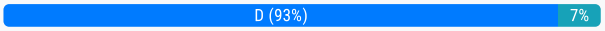
B. block, action, and warn

C. action, inform, and ask

D. inform, ask, and drop

Correct Answer: *D*

Community vote distribution



Community vote distribution

geekchicadee 2 months, 1 week ago

Selected Answer: D

In the UserCheck page, click New, and then select the object type:

Ask
Shows a message to users that asks them if they want to continue with the request or not. To continue with the request, the user is expected to supply a reason.

Inform

Shows an informative message to users. Users can continue to the application or cancel the request.

Block

Shows a message to users and blocks the application request.

upvoted 1 times

r_mcr 3 months, 4 weeks ago

A)
Informative Message: This type of message informs the user about a security event or policy without requiring any action from the user. It is used to raise awareness about security policies and potential risks.

Blocking Message: This message is displayed when a user's action is blocked by a security policy. It informs the user that their action is not allowed and provides details about the policy that caused the block.

Ask User Message: This type of message prompts the user to make a decision regarding their action. It provides options for the user to either proceed with their action or cancel it, based on the security policy in place. This allows users to have some control over their actions while still adhering to security policies

upvoted 1 times

hak01 5 months, 2 weeks ago

UserCheck Interactions
Message windows: Ask, Cancel, Certificate Template, Inform, and Drop

upvoted 1 times

Didesouzads 10 months, 3 weeks ago

There are not a full complete answer.The correct is Inform, ask and block.

I believe in the exam the answers are corrects, the mistake is in this dumb

upvoted 3 times

91ca199 10 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

Blurock 11 months, 2 weeks ago

Selected Answer: A

Sorry but D is for UserCheck Actions. A is for UserCheck messages. Ignore my earlier vote for "D".
https://sc1.checkpoint.com/documents/R81.20/SmartConsole_OLH/EN/Topics-OLH/yVFfYIsC-kghEFffDaZFOQ2.htm?Highlight=messages

upvoted 1 times

Didesouzads 10 months, 3 weeks ago

Correct is inform not notify

upvoted 1 times

Blurock 11 months, 2 weeks ago

Selected Answer: D

Same source as @Kuro1984 mentioned

upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: D

D. inform, ask, and drop. Tested in the LAB

upvoted 2 times

Kuro1984 11 months, 3 weeks ago

Selected Answer: D

https://sc1.checkpoint.com/documents/R81.20/SmartConsole_OLH/EN/Topics-OLH/AVpngGVpF7G1O0O8nM1RSQ2.htm?Highlight=usercheck

upvoted 2 times

juandiegope 1 year, 1 month ago

Selected Answer: D

The correct answer should be: Inform, Ask and Block.
Due to the lack of the correct option, the closest one is D)

upvoted 1 times

BillNosie 1 year, 1 month ago

Selected Answer: D

D is correct.

upvoted 1 times

metalmuff 1 year, 1 month ago

Selected Answer: D

The correct answer is D. inform, ask, and drop.

upvoted 1 times

immp 1 year, 1 month ago

Inform ask drop based from official study guide

upvoted 1 times

Darkflame 1 year, 2 months ago

Ask Block inform. is the correct answer.

upvoted 2 times

Darkflame 1 year, 2 months ago

There is no drop mesage. its a block message. notify or inform are the same.

upvoted 2 times

Bombast 1 year, 2 months ago

no current answer
current is:
inform

block

ask

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: D

It's D

upvoted 2 times

Question #27 *Topic 1*

By default, which port is used to connect to the GAiA Portal?

A. 4434

B. 80

C. 8080

D. 443

Correct Answer: *D*

Community vote distribution

Community vote distribution

Mrnemesis 6 months, 1 week ago

It's Dii

upvoted 1 times

Normanby 9 months, 3 weeks ago

Selected Answer: D

443 IS correct as the 'default', however, CP recommend later on to move it to 4434, this is the confusion.

upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: D

it's D !!

upvoted 1 times

kmdls 1 year, 1 month ago

Selected Answer: D

D is tecnically correct, the request goes on 443 by default then if needed for different services (example Endpoint Security SSL) or functions that are not the Gaia Portal it redirects to 4434

upvoted 1 times

metalmuff 1 year, 1 month ago

Selected Answer: D

The correct answer is D. 443.

upvoted 1 times

Bombast 1 year, 2 months ago

D

Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

listens to SSL traffic for all services on the TCP port 443 in these cases: If you performed a clean installation of a Security Management Server.

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: D

It's D

upvoted 1 times

YorelPT 1 year, 3 months ago

Selected Answer: D

According to R81.20 Admin Guide, To log in to the Gaia Portal: Enter this URL in your browser:

https://<IP Address of Gaia Management Interface>

https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Gaia_AdminGuide/Content/Topics-GAG/Gaia-Portal-Introduction.htm?tocpath=____5

So D is the correct one
upvoted 4 times

tosyeno 1 year, 3 months ago

Selected Answer: A

Gaia portal listen on port 4434 on all services

Reference: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/Gaia-Portal-Introduction.htm#:~:text=When%20you%20disable%20the%20Endpoint,the%20default%20TCP%20port%20443.
upvoted 2 times

juandiegope 1 year, 1 month ago

Wrong! The correct answer is 443.

Please read this: If you upgraded a Security Management Server with enabled Endpoint Policy Management Software Blade to R81, then the SSL port configuration remains as it was in the previous version, from which you upgraded:

A Security Management Server listens to Endpoint Security SSL traffic on the TCP port 443

A Security Management Server listens to SSL traffic for all other services on the TCP port 4434
upvoted 1 times

Question #28 *Topic 1*

Choose what BEST describes a Session.

A. Sessions ends when policy is pushed to the Security Gateway.

B. Sessions locks the policy package for editing.

C. Starts when an Administrator logs in through SmartConsole and ends when the Administrator logs out.

D. Starts when an Administrator publishes all the changes made on SmartConsole.

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

geekchicadee 2 months, 1 week ago

Selected Answer: C

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Session-flow-for-Administrators.htm

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: C

It's C

upvoted 1 times

Question #29 *Topic 1*

Which command shows detailed information about VPN tunnels?

A. cat $FWDIR/conf/vpn.conf

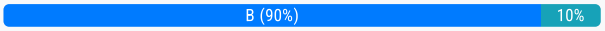
B. vpn tu tlist

C. vpn tu

D. cpview

Correct Answer: *B*

Community vote distribution



Community vote distribution

geekchicadee 1 month, 3 weeks ago

Selected Answer: B

There are two solutions: vpn tu list tunnels OR vpn tu tlist

B. vpn tu tlist is the only option listed so its B. (C. vpn tu - Launches the TunnelUtil tool)

upvoted 1 times

ad69781 4 months, 2 weeks ago

Selected Answer: B

vpn tu tlist

upvoted 1 times

hak01 5 months, 2 weeks ago

B

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/CLI/vpn-tu-tlist.htm

upvoted 1 times

RemmyT 1 year ago

Selected Answer: D

CPVIEW. Software-blades . VPN.Detailed

Shows detailed information about VPN tunnels

vpn tu tlist

Shows information about VPN tunnels.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/CLI/vpn-tu-tlist.htm

upvoted 1 times

oaraujo 1 year ago

Selected Answer: B

Shows information about VPN tunnels.

upvoted 2 times

metalmuff 1 year, 1 month ago

Selected Answer: B

vpn tu tlist: This command adds the "tlist" option, which provides detailed information about each VPN tunnel, including its name, local and remote gateways, status, encryption level, and other parameters.

upvoted 2 times

Darkflame 1 year, 2 months ago

check the answers. it is vpn tu list not vpn tu tlist

upvoted 1 times

Didesouzads 10 months, 3 weeks ago

No, the correct is vpn tu tlist

upvoted 1 times

Bombast 1 year, 2 months ago

B

https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SitetoSiteVPN_AdminGuide/Content/Topics-VPNSG/CLI/vpn-tu-list.htm?tocpath=Command%20Line%20Reference%7Cvpn%7Cvpn%20tu%7C____2

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: B

It's B

upvoted 1 times

AlF8812 1 year, 2 months ago

Selected Answer: B

B is Correct

upvoted 1 times

tosyeno 1 year, 3 months ago

Selected Answer: B

According to the reference below, the correct answer is B.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/CLI/vpn-tu-tlist.htm

upvoted 2 times

YorelPT 1 year, 3 months ago

According to CLI R81.20 Reference Guide, page 1532, the correct one is B (vpn tu tlist).

https://dl3.checkpoint.com/paid/19/196f93c20f9bbade688c9480b1f30ceb/CP_R81.20_CLI_ReferenceGuide.pdf?HashKey=1700406746_b5e12724a597db025a483e179560e2c6&xtn=.pdf

upvoted 4 times

Question #30 *Topic 1*

After a new Log Server is added to the environment and the SIC trust has been established with the SMS what will the gateways do?

A. Gateways will send new firewall logs to the new Log Server as soon as the SIC trust is set up between the SMS and the new Log Server.

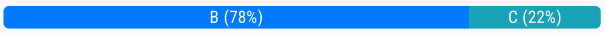
B. Logs are not automatically forwarded to a new Log Server. SmartConsole must be used to manually configure each gateway to send its logs to the server.

C. The firewalls will detect the new Log Server after the next policy install and redirect the new logs to the new Log Server.

D. The gateways can only send logs to an SMS and cannot send logs to a Log Server. Log Servers are proprietary log archive servers.

Correct Answer: *B*

Community vote distribution



Community vote distribution

keikei1228 3 months, 2 weeks ago

Selected Answer: B

After a new Log Server is added to the environment and the Secure Internal Communication (SIC) trust has been established with the Security Management Server (SMS), the gateways will need to be manually configured to send their logs to the new Log Server. This is not an automatic process.

upvoted 2 times

r_mcr 3 months, 3 weeks ago

Selected Answer: C

Once the Secure Internal Communication (SIC) trust is established between the Security Gateways and the new Log Server, the log forwarding process is automatic. The gateways will begin to send their log data to the new Log Server without requiring additional manual configuration, provided that the policy is installed to recognize the new Log Server.

upvoted 1 times

itcom 5 months, 2 weeks ago

I literally just spun up an R81.20 Management server and gateway and without changing anything the gateway has the option "Send gateway logs and alerts to server" so it definitely isnt B

upvoted 1 times

Pochex 5 months, 2 weeks ago

Logs are not automatically forwarded to a Log Server. You must manually configure each relevant Security Gateway to send its logs to the new Domain Log Server. Refer to https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Multi-DomainSecurityManagement_AdminGuide/Topics-MDSG/Configuring-Logging-in-Logging-and-Monitoring.htm?TocPath=Logging%20and%20Monitoring%7CConfiguring%20Logging%7C____0#Configuring_Logging

upvoted 1 times

Slicklinton 10 months, 1 week ago

Selected Answer: B

https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_Multi-DomainSecurityManagement_AdminGuide/Topics-MDSG/Configuring-Logging-in-Logging-and-Monitoring.htm

upvoted 3 times

WwJim202120 10 months, 1 week ago

Selected Answer: C

Once the new Log Server is added and the SIC trust is established, the gateways will be aware of the new Log Server during the next policy installation, and they will begin sending their logs to it accordingly.

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: B

It's B

upvoted 2 times

Question #31 *Topic 1*

Which of the following is a valid deployment option?

A. CloudSec deployment

B. Disliked deployment

C. Router only deployment

D. Standalone deployment

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

aikaloge 8 months, 4 weeks ago

Selected Answer: D

It's D

upvoted 1 times

Question #32 *Topic 1*

Using the SmartConsole, which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

A. Read Only All

B. Full Access

C. Editor

D. Super User

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

84507ab 4 days ago

Selected Answer: A

to audit = A

upvoted 1 times

keikei1228 3 months, 4 weeks ago

Selected Answer: A

A. Read Only All

This profile provides full read permissions but no write permissions, allowing the administrator to audit all configurations without making any changes.

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: A

It's A

upvoted 1 times

Question #33 *Topic 1*

Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?

A. Logging and Status

B. Monitoring

C. Threat Emulation

D. Application Control

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

Chopaka 5 months ago

It's b!

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: B

it's B

upvoted 1 times

Bombast 8 months, 3 weeks ago

B

The Check Point Monitoring Software Blade presents a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events. The Software Blade centrally monitors Check Point devices and alerts security administrators to changes to gateways, endpoints, tunnels, remote users and security activities.

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Question #34 *Topic 1*

Which type of Check Point license ties the package license to the IP address of the Security Management Server?

A. Formal

B. Corporate

C. Central

D. Local

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

davidjow Highly Voted 10 months ago

Selected Answer: C

from:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/Licenses-Stored-in-Licenses-and-Contracts-Repository.htm

Central:

The Central license is the preferred method of licensing.
A Central license is tied to the IP address of the Management Server.
There is one IP address for all licenses.
The license remains valid if you change the IP address of the Security Gateway.
A license can be moved from one Check Point Security Gateway to another easily.
Maximum flexibility.

Local:

The Local license is an older method of licensing that is still supported.
A Local license is tied to the IP address of the specific Security Gateway.
Cannot be transferred to a Security Gateway with a different IP address.

upvoted 5 times

Blurock Most Recent 5 months, 2 weeks ago

Selected Answer: C

C is correct. It would be "Local" if the question was talking about Security Gateway

upvoted 1 times

Kuro1984 5 months, 3 weeks ago

Selected Answer: C

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/Licenses-Stored-in-Licenses-and-Contracts-Repository.htm

upvoted 1 times

juandiegope 7 months, 1 week ago

Selected Answer: C

The Central license is the preferred and recommended method of licensing. This license ties the package license to the IP address of the management server and has no dependency on the gateway IP.

upvoted 1 times

BillNosie 7 months, 2 weeks ago

Selected Answer: C

Central ties to the Management Server IP address, Local ties to the Security Gateway.

upvoted 2 times

Eroman 7 months, 3 weeks ago

it is C

upvoted 1 times

Wyp 7 months, 3 weeks ago

Selected Answer: C

A Central license is tied to the IP address of the Management Server, not security gateway

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: C

It's C

upvoted 1 times

pigtail 9 months, 1 week ago

Selected Answer: C

C is the correct answer

upvoted 1 times

kismet99 9 months, 2 weeks ago

Selected Answer: C

C is the correct answer

upvoted 1 times

DannyYo 9 months, 2 weeks ago

Selected Answer: C

C is the right answer.

upvoted 1 times

tosyeno 9 months, 2 weeks ago

Selected Answer: C

The central license is tied to the IP address of the security management server.

Correct answer is C

upvoted 1 times

Question #35 *Topic 1*

Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? Choose the BEST answer.

A. Anti-Malware

B. Content Awareness

C. Anti-Virus

D. IPS

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

EssentialD 6 months, 3 weeks ago

Selected Answer: C

The terms malware and virus are often used interchangeably because they have significant overlap. A virus is a specific type of malware, but malware is a general term that also includes many types of malicious software that lack viruses' ability to self-replicate.

upvoted 1 times

Bombast 8 months, 3 weeks ago

C

Anti-Virus - Pre-infection detection and blocking of malware at the gateway. The Anti-Virus Software Blade is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: C

It's C

upvoted 1 times

Question #36 *Topic 1*

URL Filtering cannot be used to:

A. Control Data Security

B. Decrease legal liability

C. Improve organizational security

D. Control Bandwidth issues

Correct Answer: *A*

Community vote distribution

Community vote distribution

n00bcyborg 4 weeks, 1 day ago

Selected Answer: A

Page 600 of R81.20 training book. URL filtering CAN be used to control bandwidth issues

upvoted 1 times

whoamii 3 months, 3 weeks ago

Selected Answer: D

D. Control Bandwidth issues

URL Filtering is primarily used to block or allow access to specific websites or categories of websites to improve organizational security, control data security, and decrease legal liability. However, it is not designed to directly manage or control bandwidth issues, which would typically require Quality of Service (QoS) or traffic shaping tools.

upvoted 1 times

keikei1228 3 months, 4 weeks ago

Selected Answer: A

A. Control Data Security

URL Filtering is primarily used to control access to websites, improve organizational security by blocking malicious sites, decrease legal liability by preventing access to inappropriate content, and control bandwidth issues by restricting access to high-bandwidth sites. However, it is not specifically designed to control data security, which involves protecting data from unauthorized access and ensuring data integrity and confidentiality.

upvoted 1 times

Pochex 5 months, 2 weeks ago

I did not take the bootcamp but I cannot see how URLF controls bandwidth, that is usually handled by QoS feature. QoS leverages the industry's most advanced traffic inspection and bandwidth control technologies.

Refer to https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_QoS_AdminGuide/Topics-QoSG/Introduction-to-QoS.htm

D is the correct one

upvoted 2 times

david_vera 8 months, 1 week ago

Selected Answer: A

According to "Check Point Cybersecurity Bootcamp R81.20: CCSA & CCSE" (official book) that I made last week, literally says:

URL filtering can be used to:

- Control employee Internet access to inappropiate and illicit websites

- Control Bandwidth issues
- Decrease legal liability
- Improve organizational security

So, I think is A the right answer
upvoted 3 times

1ca883b 10 months, 3 weeks ago
Answer is D

URL Filtering is a blade that enables administrators to control access to millions of websites by category, users, groups, and machines.

URL Filtering can be used to improve organizational security, decrease legal liability, and control data security by preventing users from accessing malicious or inappropriate websites.

However, URL Filtering cannot be used to control bandwidth issues, such as limiting the amount of traffic or prioritizing certain applications over others. For that purpose, other blades such as QoS (Quality of Service) or SecureXL are more suitable.
Reference: Check Point R81 URL Filtering Administration Guide
upvoted 1 times

kazooka 3 months, 4 weeks ago
URL Filtering can control bandwidth issues by blocking high bandwidth sites. Other tools can priorities or shape the bandwidth. But URL filtering can be used to block YouTube, Netflix etc.. .completely to control bandwidth.
upvoted 1 times

EssentialD 11 months, 2 weeks ago
Selected Answer: A
I think It's A
upvoted 1 times

aikaloge 1 year, 2 months ago
Selected Answer: A
It's A
upvoted 1 times

Gabsf 1 year, 3 months ago
CCSA R81.20 Page 600
A is the correct
upvoted 2 times

reinhardtvdw 1 year, 3 months ago
Correct answer is A
https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/Content/Topics-SECMG/Creating-Application-Control-and-URL-Filtering-Rules.htm?tocpath=Creating%20an%20Access%20Control%20Policy%7C____6
upvoted 1 times

pigtail 1 year, 3 months ago
A is the correct answer.

URL Filtering can be used to:
- Control employee Internet access to inappropriate and illicit websites.
- Control bandwidth issues.
- Decrease legal liability.
- Improve organizational security.
upvoted 2 times

tosyeno 1 year, 3 months ago
Correct answer is D.
URL filtering is not a feature that control anything that has to do with bandwidth control/issue, that is the work of QoS.
upvoted 4 times

Question #37 *Topic 1*

Which one of the following is TRUE?

A. One policy can be either inline or ordered, but not both.

B. Inline layer can be defined as a rule action.

C. Ordered policy is a sub-policy within another policy.

D. Pre-R80 Gateways do not support ordered layers.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: B

B. Inline layer can be defined as a rule action.

An Inline Layer can be defined as a rule action within an Ordered Layer, allowing for more granular control and organization of the security policy.

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: B

It's B

upvoted 1 times

Question #38 *Topic 1*

Fill in the blanks: A Check Point software license consists of a ____ and ____.

A. Software container; software package

B. Software package; signature

C. Signature; software blade

D. Software blade; software container

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: D

D. Software blade; software container

A Check Point software license consists of a software blade and a software container. The software blade provides specific security functionalities, while the software container is the base license required to use any of the software blades.

upvoted 1 times

1ca883b 10 months, 3 weeks ago

D

A Check Point software license consists of a Software blade and a Software container.

A Software blade is a modular security feature that delivers security functionality to the gateway or management server.

A Software container is a set of Software blades that can be purchased as a bundle.

Reference: Check Point R81 Security Management Administration Guide, page 14.

upvoted 1 times

oaraujo 1 year ago

A Check Point software license consists of two components: Software Blade y Software Container

Link: https://support.checkpoint.com/results/sk/sk11054

upvoted 1 times

BillNosie 1 year, 1 month ago

Selected Answer: D

Software Blade and Software Container

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: D

It's D

upvoted 1 times

pigtail 1 year, 3 months ago

Selected Answer: D

A Check Point software license consists of two primary components:

- Software Blade
- Software Container

upvoted 1 times

tosyeno 1 year, 3 months ago

Selected Answer: D

Software container & Blade

upvoted 1 times

davidjow 1 year, 3 months ago

Selected Answer: D

from: CCSA R81.20 page 316

A CP software license consists of two primary components:

Software Blade

Software Container

upvoted 3 times

Question #39 *Topic 1*

Which of the following is used to initially create trust between a Gateway and Security Management Server?

A. One-time Password

B. Token

C. Certificate

D. Internal Certificate Authority

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: A

A. One-time Password

A one-time password (also known as an activation key) is used to initially create trust between a Gateway and the Security Management Server. Once the initial trust is established using the one-time password, further communication is based on security certificates issued by the Internal Certificate Authority (ICA).

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: A

It's A

upvoted 2 times

Haliteh 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 3 times

Question #40 *Topic 1*

What are the two elements of address translation rules?

A. Original packet and translated packet

B. Manipulated packet and original packet

C. Untranslated packet and manipulated packet

D. Translated packet and untranslated packet

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 3 months, 4 weeks ago

Selected Answer: A

A. Original packet and translated packet

Address translation rules consist of two main elements: the original packet (which includes the original source, destination, and services) and the translated packet (which includes the translated source, destination, and services). These elements define how the Security Gateway should modify the packet's addressing information.

upvoted 1 times

EssentialD 1 year ago

Selected Answer: A

It's A

upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: A

It's A

upvoted 1 times

Question #41 *Topic 1*

Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

A. 192.168.1.1 AND 172.26.1.1 AND drop

B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop

C. 192.168.1.1 OR 172.26.1.1 AND action:Drop

D. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Question #42 *Topic 1*

Fill in the blanks: The ____ collects logs and sends them to the ____.

A. Log server; Security Gateway

B. Security Gateways; log server

C. Log server; security management server

D. Security management server; Security Gateway

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

84507ab 3 weeks, 4 days ago

Selected Answer: B

In Smart Console, you can configure a Security GatewayClosed, that when it fails to send its logs to one Log Server it will send its logs to a secondary Log Server.

upvoted 1 times

Slicklinton 4 months ago

Selected Answer: B

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Log-Server-High-Availability.htm?tocpath=Logging%7C____6

upvoted 2 times

aikaloge 8 months, 4 weeks ago

Selected Answer: B

It's B

upvoted 1 times

Question #43 *Topic 1*

Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

A. RADIUS

B. SecurID

C. Check Point password

D. Security questions

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: D

It's D

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: D

It's D

upvoted 1 times

Question #44 *Topic 1*

Which of the following statements about Site-to-Site VPN Domain-based is NOT true?

A. Route-based- The Security Gateways will have a Virtual Tunnel Interface (VTI) for each VPN Tunnel with a peer VPN Gateway. The Routing Table can have routes to forward traffic to these VTIs. Any traffic routed through a VTI is automatically identified as VPN Traffic and is passed through the VPN Tunnel associated with the VTI.

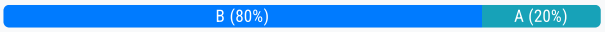
B. Domain-based- VPN domains are pre-defined for all VPN Gateways.
A VPN domain is a service or user that can send or receive VPN traffic through a VPN Gateway.

C. Domain-based- VPN domains are pre-defined for all VPN Gateways. A VPN domain is a host or network that can send or receive VPN traffic through a VPN Gateway.

D. Domain-based- VPN domains are pre-defined for all VPN Gateways.
When the Security Gateway encounters traffic originating from one VPN Domain with the destination to a VPN Domain of another VPN Gateway, that traffic is identified as VPN traffic and is sent through the VPN Tunnel between the two Gateways.

Correct Answer: *B*

Community vote distribution



Community vote distribution

n00bcyborg 4 weeks, 1 day ago

Selected Answer: A

The question is asking about Domain-based yet A is talking about route-based

upvoted 1 times

keikei1228 3 months, 3 weeks ago

Selected Answer: B

The correct definition is that a VPN domain is a host or network that can send or receive VPN traffic through a VPN Gateway, not a service or user.

upvoted 1 times

thakickback 8 months ago

Selected Answer: A

its A, cuz its explanation for route-based

upvoted 1 times

EssentialD 11 months, 2 weeks ago

Selected Answer: B

It's B the one

upvoted 1 times

kmdls 1 year, 1 month ago

Selected Answer: B

a vpn domain or enc-domain can't have services or users inside of it
it is the networks/hosts decided for the phase 2

also a VTI is indeed an interface created for the vpn and it allows implied routes to send packets in the vpn tunnel

upvoted 1 times

FDZ83 1 year, 2 months ago

Selected Answer: B

a vpn domain is a "host or network" not a "service". Answer: B

upvoted 1 times

Bombast 1 year, 2 months ago

It`s A

upvoted 1 times

Question #45 *Topic 1*

What is the main objective when using Application Control?

A. To see what users are doing.

B. Ensure security and privacy of information.

C. To filter out specific content.

D. To assist the firewall blade with handling traffic.

Correct Answer: *B*

Community vote distribution

Community vote distribution

whoamii 3 months, 3 weeks ago

Selected Answer: C

C. To filter out specific content.

The main objective of using Application Control is to filter and control access to specific applications and content within an organization's network. This helps manage which applications and services users can access, ensuring that only approved or safe content is allowed.

upvoted 1 times

keikei1228 3 months, 3 weeks ago

Selected Answer: B

B. Ensure security and privacy of information.

Application Control helps in identifying, allowing, or blocking specific applications to protect against threats and ensure that only authorized applications are used within the network, thereby maintaining security and privacy.

upvoted 1 times

ad69781 4 months, 3 weeks ago

Selected Answer: B

Correct is B.

upvoted 1 times

Normanby 4 months, 4 weeks ago

Selected Answer: B

I am just doing the 'official' practice exam , it has this exact questions - the Answer is 'Ensure security and privacy of information'.

The explanation is:
Enabling application control allows us to block applications that forms a security risk like anonymizers.

upvoted 1 times

Melhi 6 months, 3 weeks ago

Selected Answer: C

I would say it's definitely "C". It is used to create granular policies to allow or deny access to Internet Applications based on business requirements.

From the CCSA course material on Kortex - App Control main use cases : 1) Learn about applications; 2) Create a granular policy; 3) Track Employees Online Usage; 4) Keep Policies updated, 5) Customize Applications, Sites, categories and groups.

upvoted 1 times

david_vera 8 months, 1 week ago

Selected Answer: C

I thing the key point of the question is "the main objective".
Answers are too generics.

A, is right that see what users are doing, but is not the main objective.
B, is right that ensure security but the thing is ensure the privacy of information? Why? Privacy information is done by encryption for example, among others, and Application control does this kind of function? I don't think so.
C, Application Control filters out specific content, yes. It seems to be the main objective, at least more than the others answers.
D, is like A.

So for me is C
upvoted 1 times

Uruguay 11 months, 1 week ago

Selected Answer: B

it is B
upvoted 2 times

Blurock 11 months, 2 weeks ago

Selected Answer: C

https://www.checkpoint.com/cyber-hub/network-security/what-is-application-control/

The whole idea is to control what applications or what part of the applications are allowed. Like you can view post on FB but you cannot post.
upvoted 2 times

Didesouzads 10 months, 3 weeks ago

Answer C is Content Awareness
upvoted 1 times

EssentialD 11 months, 2 weeks ago

Selected Answer: B

I think it's B

B. Ensure security and privacy of information.
upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: B

I think we should focus on the "main objective" which is "Ensure security and privacy of information." . Sure you can filter out specific content however this is not the primary objective.
upvoted 1 times

aikaloge 1 year, 2 months ago

Selected Answer: B

It's B
upvoted 1 times

Question #46 *Topic 1*

Fill in the blank: Backup and restores can be accomplished through ____.

A. CLI, SmartUpdate, or SmartBackup

B. SmartUpdate, SmartBackup, or SmartConsole

C. SmartConsole, WebUI, or CLI

D. WebUI, CLI, or SmartUpdate

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: C

C. SmartConsole, WebUI, or CLI

upvoted 1 times

Bombast 8 months, 3 weeks ago

C

Backup and Restore -

These options let you:

➪ Back up the Gaia OS configuration and the firewall database to a compressed file

➪ Restore the Gaia OS configuration and the firewall database from a compressed file

To back up a configuration:

1. Right-click the Security Gateway.

2. Select Backup and Restore > Backup.

The Backup window opens.

3. Select the backup location.

Reference:

https://community.checkpoint.com/thread/5375-checkpoint-gateway-firewall-backup-through-smart-console

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: C

IT's C

upvoted 1 times

Question #47 *Topic 1*

What kind of NAT enables Source Port Address Translation by default?

A. Automatic Hide NAT

B. Automatic Static NAT

C. Manual Static NAT

D. Manual Hide NAT

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: A

A. Automatic Hide NAT

upvoted 1 times

Bombast 8 months, 3 weeks ago

A

The two major kinds of NAT are Automatic NAT and Manual NAT. Automatic NAT is configured through the Network Object, the Host Object, and the Address Range Object. It can also be configured from the Gateway Object to HIDE NAT all internal networks behind the Gateway IP address.

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: A

It's A

upvoted 1 times

Question #48 *Topic 1*

Fill in the blanks: In ____ NAT, Only the ____ is translated.

A. Hide; source

B. Simple; source

C. Static; source

D. Hide; destination

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: A

A. Hide; source

upvoted 1 times

Bombast 8 months, 3 weeks ago

A

https://sc1.checkpoint.com/documents/R80.20/SmartConsole_OLH/EN/html_frameset.htm?topic=documents/R80.20/SmartConsole_OLH/EN/VVea8IK8WGKYQDx2xIMHpA2

upvoted 1 times

aikaloge 8 months, 4 weeks ago

Selected Answer: A

It's A

upvoted 1 times

Question #49 *Topic 1*

Application Control/URL filtering database library is known as:

A. AppWiki

B. Application-Forensic Database

C. Application Library

D. Application database

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: A

A. AppWiki

upvoted 1 times

kmdls 7 months, 3 weeks ago

Selected Answer: A

Product Specifications:

AppWiki Application Classification Library

To support the dynamic nature of Internet applications, the Application Control database is continuously and automatically updated- AppWiki enables application scanning and detection of nearly 8,000 distinct applications and over 250,000 Web widgets.

upvoted 1 times

Question #50 *Topic 1*

Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

A. Security Management Server

B. Security Gateway

C. SmartConsole

D. SmartManager

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

huba 1 month, 3 weeks ago

Selected Answer: A

sms must backup frequently

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: A

A. Security Management Server

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: A

it's A

upvoted 1 times

Question #51 *Topic 1*

Which of the following technologies extracts detailed information from packets and stores that information in different tables?

A. Application Layer Firewall

B. Packet Filtering

C. Next-Generation Firewall

D. Stateful Inspection

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: D

D. Stateful Inspection - It's Correct

upvoted 1 times

Question #52 *Topic 1*

You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

A. Open SmartEvent to see why they are being blocked.

B. From SmartConsole, go to the Log & Monitor tab and filter for the IP address of the tablet.

C. Open SmartMonitor and connect remotely to the wireless controller.

D. Open SmartUpdate and review the logs tab.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

Didesouzads 5 months ago

Selected Answer: B

Answer B

upvoted 1 times

Question #53 *Topic 1*

Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

A. Gaia iOS

B. Red Hat Enterprise Linux version 4

C. Centos Unix

D. Gaia embedded

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

b73f343 3 months, 1 week ago

Selected Answer: D

.....

upvoted 1 times

EssentialD 5 months, 2 weeks ago

Selected Answer: D

It's D

upvoted 1 times

BillNosie 7 months, 2 weeks ago

Selected Answer: D

Gaia Embedded.

upvoted 1 times

YorelPT 8 months, 2 weeks ago

Selected Answer: D

D is the right one.

upvoted 1 times

Gabsf 9 months, 1 week ago

Quantum Spark is Gaia Embedded, D is Correct

upvoted 2 times

agolarait 9 months, 1 week ago

Correct answer is D

upvoted 3 times

reinhardtvdw 9 months, 1 week ago

D is the correct answer.

upvoted 1 times

Question #54 *Topic 1*

What command from the CLI would be used to view current licensing?

A. cplic print

B. show license -s

C. fw ctl tab -t license -s

D. license view

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

Slicklinton 4 months ago

Selected Answer: A

https://www.tech-wiki.net/index.php/Useful_Check_Point_CLI_commands

upvoted 1 times

Didesouzads 5 months ago

Selected Answer: A

Answer A

upvoted 1 times

Question #55 *Topic 1*

A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?

A. Security Zones are not supported by Check Point firewalls.

B. The firewall rule can be configured to include one or more subnets in a zone.

C. The zone is based on the network topology and determined according to where the interface leads to.

D. The local directly connected subnet defined by the subnet IP and subnet mask.

Correct Answer: *C*

Community vote distribution

Community vote distribution

kalbeckscs 3 months, 2 weeks ago

Selected Answer: C

C is the answer

upvoted 1 times

b73f343 9 months, 1 week ago

Selected Answer: C

.....

upvoted 1 times

Chopaka 11 months ago

Selected Answer: D

I think that D is correct. Does Someone has A theorie why C is correct?

upvoted 1 times

EssentialD 11 months, 2 weeks ago

Selected Answer: C

It's C for sure

upvoted 2 times

BillNosie 1 year, 1 month ago

Selected Answer: C

C is correct.

upvoted 1 times

justinljw 1 year, 2 months ago

Selected Answer: C

It's C

upvoted 2 times

Gabsf 1 year, 3 months ago

C is the correct

upvoted 1 times

tosyeno 1 year, 3 months ago

Correct answer is C

upvoted 2 times

Question #56 *Topic 1*

Which of the completed statements is NOT true? The GAiA Portal (WebUI) can be used to manage Operating System user accounts and:

A. assign privileges to users.

B. assign user rights to the directory structure on the Security Management Server.

C. add more users to the Gaia operating system.

D. change the home directory of the user.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: B

B. assign user rights to the directory structure on the Security Management Server.

The GAiA Portal (WebUI) can be used to manage Operating System user accounts and perform tasks such as assigning privileges to users, adding more users to the Gaia operating system, and changing the home directory of the user, but it does not manage user rights to the directory structure on the Security Management Server.

upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: B

it's B

upvoted 1 times

Question #57 *Topic 1*

Which encryption algorithm is the least secured?

A. 3DES

B. AES-128

C. DES

D. AES-256

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: C

C. DES

DES (Data Encryption Standard) is considered the least secure due to its shorter key length (56 bits), which makes it more vulnerable to brute-force attacks compared to the other algorithms listed.

upvoted 1 times

Didesouzads 11 months ago

Selected Answer: C

The order the least for the most secure encryptions

DES
3DES
AES-128
AES-256

upvoted 3 times

Question #58 *Topic 1*

Fill in the blank: SmartConsole, SmartEvent GUI client, and ____ allow viewing of billions of consolidated logs and shows them as prioritized security events.

A. SmartMonitor

B. SmartReporter

C. SmartTracker

D. SmartView Web Application

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Didesouzads 5 months ago

Selected Answer: D

SmartView Web Application is one alternative to see logs in CheckPoint

SmartMonitor you can see counters, traffic and etc

SmartReporter and SmartTracker dont exist

upvoted 1 times

Question #59 *Topic 1*

What is the default tracking option of a rule?

A. None

B. Alert

C. Log

D. Tracking

Correct Answer: *C*

Community vote distribution

Community vote distribution

n00bcyborg 1 month ago

Selected Answer: A

Default is None according to the R81.20 training material (page 378). Confirmed using lab environment.

upvoted 3 times

dude87 1 month ago

Selected Answer: A

Page 378 of the Check Point Certified Security Administrator R81.20

Track: The default None

upvoted 2 times

Derelicto 3 months ago

Selected Answer: C

Tracking Options

Select these options in the Track column of a ruleClosed:

None - Do not generate a log.

Log -This is the default Track option. It shows all the information that the Security GatewayClosed used to match the connection. At a minimum, this is the Source, Destination, Source Port, and Destination Port. If there is a match on a rule that specifies an application, a session log shows the application name (for example, Dropbox). If there is a match on a rule that specifies a Data TypeClosed, the session log shows information about the files, and the contents of the files.

Accounting - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

upvoted 1 times

Mrnemesis79 3 months ago

Selected Answer: A

A es la correcta.

upvoted 1 times

kalbeckscs 3 months, 2 weeks ago

Selected Answer: C

Trick question... The default tracking "option" is Log, it is the default option on log field

upvoted 1 times

keikei1228 3 months, 2 weeks ago

Selected Answer: C

The default tracking option of a firewall rule in Check Point is:

C. Log

This option shows all the information that the Security Gateway used to match the connection, including the Source, Destination, Source Port, and Destination Port.

upvoted 1 times

r_mcr 3 months, 2 weeks ago

Selected Answer: C

From version 80 onwards, it became log.Of course, when coming from an upgrade, this option is suppressed, which can lead to misunderstanding.Therefore, the option is C.

https://support.checkpoint.com/results/sk/sk116580

upvoted 1 times

sx89andjey 3 months, 3 weeks ago

Selected Answer: C

81.20 now have default role log. So C is correct

upvoted 1 times

694a477 3 months, 3 weeks ago

Selected Answer: C

It is a bit of a trick question...the default tracking "option" is Log.

upvoted 1 times

ad69781 4 months, 3 weeks ago

i did a new rule at smart console and correct is none. A

upvoted 2 times

ad69781 4 months, 3 weeks ago

81.20 now have default role log. So C is correct

upvoted 1 times

ad69781 4 months, 3 weeks ago

Sorry, i did a new rule at smart console and correct is none. A.

upvoted 1 times

cd947f5 5 months, 1 week ago

Selected Answer: C

Answer: C Log is the correct answer. Also checked with the checkpoint Practice exam

upvoted 1 times

Pochex 5 months, 1 week ago

Answer A - Tested in a lab

upvoted 1 times

Shonnie_ 6 months ago

Selected Answer: A

None - This option is the default and it does not generate a log

upvoted 1 times

caf7705 7 months ago

copy a statement from document "CP_R81.20_Quantum_SecurityManagement_AdminGuide, page 266"

Log -This is the default Track option. It shows all the information that the Security

Gateway used to match the connection

Answer: A

upvoted 1 times

caf7705 7 months ago

Sorry, type mistake,

Correct Answer is C

upvoted 1 times

b73f343 9 months, 1 week ago

Selected Answer: A

A.....

upvoted 1 times

Didesouzads 10 months ago

Selected Answer: A

Answer A

upvoted 1 times

Question #60 *Topic 1*

Fill in the blank: Once a license is activated, a ____ should be installed.

A. License Management file

B. License Contract file

C. Security Gateway Contract file

D. Service Contract file

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

keikei1228 3 months, 2 weeks ago

Selected Answer: D

Once a license is activated, a Service Contract file should be installed to ensure that the purchased services are properly enabled and maintained. This file contains information about the service contracts associated with the licenses and is necessary for the proper functioning of the licensed features.

upvoted 1 times

EssentialD 11 months, 2 weeks ago

Selected Answer: D

D. Service Contract file

upvoted 1 times

Question #61 *Topic 1*

When should you generate new licenses?

A. Only when the license is upgraded.

B. After a device upgrade.

C. When the existing license expires, the license is upgraded, or the IP address associated with the license changes.

D. Before installing contract files.

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

ad69781 4 months, 3 weeks ago

Answer C

upvoted 1 times

Didesouzads 11 months ago

Selected Answer: C

Answer C

upvoted 1 times

Question #62 *Topic 1*

Fill in the blank: The position of an Implied rule is manipulated in the ____ window.

A. Firewall

B. Object Explorer

C. Global Properties

D. NAT

Correct Answer: *A*

Community vote distribution

Community vote distribution

n00bcyborg 1 month ago

Selected Answer: C

Keyword is window. The changes are made in the Fireall section, but that section is within the Global Properties window. Confirmed using a lab.

upvoted 1 times

dude87 1 month ago

Selected Answer: C

Global Properties window (Firewall section)

upvoted 1 times

pedropedropedro 1 month, 2 weeks ago

Selected Answer: C

C

Global properties "To configure the implied rules", Firewall "To view the implied rules"

CP_R81.20_Quantum_SecurityManagement_AdminGuid Page 430 o 301

upvoted 1 times

Dash 3 months, 1 week ago

Selected Answer: C

C=Global Propertys

upvoted 1 times

kalbeckscs 3 months, 2 weeks ago

Selected Answer: A

To configure the implied rules in SmartConsole:

In the top left corner, click Menu > Global properties.

In the Firewall page, select the applicable options and configure the order of the implied rules.

Click OK

upvoted 2 times

r_mcr 3 months, 4 weeks ago

A,

he position of an Implied Rule in Check Point can be manipulated in the Global Properties settings of the Security Management Server. Here's how you can do it:

Open SmartConsole: Launch the SmartConsole application and connect to your Security Management Server.

Navigate to Global Properties: Go to the "Security Policies" tab and click on "Global Properties" in the toolbar.

Select Implied Rules: In the Global Properties window, navigate to the "Firewall" section and then to the "Implied Rules" tab.

Adjust Rule Position: Here, you can see the list of implied rules and their current positions. You can adjust the position of these rules by selecting options such as "First", "Before Last", or "Last". This determines where the implied rules will be placed in relation to the manually defined rules in the rulebase.

Apply and Save: After making the necessary adjustments, click "OK" to apply the changes and save the configuration.

upvoted 1 times

ad69781 4 months, 2 weeks ago

Selected Answer: C

c , global

upvoted 1 times

Mrnemesis79 4 months, 2 weeks ago

Firewall window inside the Global Properties, what is the correct answer? A or c?

upvoted 1 times

ad69781 4 months, 3 weeks ago

Global Proprieties is correct. C.

upvoted 1 times

hector255 5 months ago

Selected Answer: C

Global Properties is right!

upvoted 1 times

Slicklinton 10 months ago

Selected Answer: A

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

upvoted 1 times

Didesouzads 11 months ago

Firewall window inside the Global Properties

upvoted 1 times

Didesouzads 11 months ago

Selected Answer: A

Answer A

upvoted 1 times

Question #63 *Topic 1*

Which of the following situations would not require a new license to be generated and installed?

A. The existing license expires.

B. The Security Gateway is upgraded.

C. The license is upgraded.

D. The IP address of the Security Management or Security Gateway has changed.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

84507ab 2 weeks, 5 days ago

Selected Answer: B

If a Gateway has been upgraded the licenses remain the same

upvoted 1 times

Didesouzads 5 months ago

Selected Answer: B

If a Gateway has been upgraded the licenses remain the same

upvoted 1 times

Question #64 *Topic 1*

You have enabled “Extended Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Log Trimming is enabled.

B. Content Awareness is not enabled.

C. Logging has disk space issues.

D. Identity Awareness is not enabled.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

EssentialD 6 months ago

Selected Answer: B

B it's correct as per : https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Working-with-logs.htm

Detailed Log and Extended Log are only available if one or more of these Blades are enabled on the Layer: Application & URL Filtering, Content Awareness, or Mobile Access.

upvoted 2 times

Question #65 *Topic 1*

Fill in the blank: In order to install a license, it must first be added to the ____.

A. Package repository

B. Download Center Web site

C. License and Contract repository

D. User Center

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

Didesouzads 5 months ago

Selected Answer: C

Answer C

upvoted 2 times

Question #66 *Topic 1*

What is required for a certificate-based VPN tunnel between two gateways with separate management systems?

A. Shared Secret Passwords

B. Unique Passwords

C. Shared User Certificates

D. Mutually Trusted Certificate Authorities

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

U2D2A2R2A 2 months, 2 weeks ago

Selected Answer: D

The correct answer is D

Mutually Trusted Certificate Authorities

upvoted 1 times

keikei1228 3 months, 3 weeks ago

Selected Answer: D

D. Mutually Trusted Certificate Authorities

For a certificate-based VPN tunnel between two gateways with separate management systems, it is required that both gateways have certificates issued by Certificate Authorities (CAs) that are mutually trusted. This means that each gateway must trust the CA that issued the certificate for the other gateway.

upvoted 2 times

Didesouzads 11 months ago

Selected Answer: D

Answer D

upvoted 1 times

Question #67 *Topic 1*

Main Mode in iKEv1 uses how many packages for negotiation?

A. 3

B. depends on the make of the peer gateway

C. 6

D. 4

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

84507ab 2 weeks, 5 days ago

Selected Answer: C

iKEv1 Phase I page 654: main mode

upvoted 1 times

Slicklinton 4 months ago

Selected Answer: C

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/IPsec-and-IKE.htm

upvoted 1 times

Didesouzads 5 months ago

Selected Answer: C

Main Mode 6 packages

Agressive Mode 3 packages

upvoted 3 times

Didesouzads 5 months ago

Selected Answer: C

Main Mode 6 messages

Agressive Mode 3 messages

upvoted 1 times

Question #68 *Topic 1*

Which is a main component of the Check Point security management architecture?

A. Proxy Server

B. Endpoint VPN client

C. Identity Collector

D. SmartConsole

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

Didesouzads 5 months ago

Selected Answer: D

3 tier architecture components in CheckPoint

Security Gateway, Security Management Server and SmartConsole

upvoted 4 times

Question #69 *Topic 1*

What are the two types of NAT supported by the Security Gateway?

A. Destination and Hide

B. Source and Destination

C. Static and Source

D. Hide and Static

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: D

D. Hide and Static

upvoted 1 times

Question #70 *Topic 1*

Fill in the blank: A(n) ____ rule is created by an administrator and configured to allow or block traffic based on specified criteria.

A. Explicit

B. Implicit drop

C. Implicit accept

D. Inline

Correct Answer: *A*

Community vote distribution

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: A

Explicit , it's A

upvoted 1 times

Question #71 *Topic 1*

Where is the "Hit Count" feature enabled or disabled in SmartConsole?

A. In Global Properties.

B. On each Security Gateway.

C. On the Policy layer.

D. On the Policy Package.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: A

A. In Global Properties.

The "Hit Count" feature is enabled or disabled in SmartConsole under Global Properties. Additionally, it can also be enabled or disabled on each Security Gateway individually.

upvoted 1 times

67578ac 10 months ago

Selected Answer: A

Global Properties

upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: A

In Global Properties

upvoted 1 times

BillNosie 1 year, 1 month ago

Selected Answer: A

It is enabled in Global Properties, on the Hit Count page.

upvoted 2 times

pigtail 1 year, 3 months ago

Selected Answer: A

"By default, Hit Count is globally enabled for all supported Security Gateways. The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable Hit Count for one or more Security Gateways."

upvoted 1 times

agolarait 1 year, 3 months ago

Selected Answer: A

Global

upvoted 2 times

Question #72 *Topic 1*

Log query results can be exported to what file format?

A. Comma Separated Value (csv).

B. Word Document (docx).

C. Text (txt).

D. Portable Document Format (pdf).

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: A

It's A -. Comma Separated Value (csv).

upvoted 2 times

Question #73 *Topic 1*

In order to modify Security Policies the administrator can use which of the following tools? Select the BEST answer.

A. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.

B. SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.

C. mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.

D. SmartConsole and WebUI on the Security Management Server.

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: B

It's B

upvoted 2 times

Question #74 *Topic 1*

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

A. Anti-spam and Email Security

B. Anti-Virus

C. Firewall

D. Application Control

Correct Answer: *B*

Community vote distribution

B (100%)

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: B

B. Anti-Virus

The Anti-Virus Check Point Software Blade prevents malicious files from entering a network using real-time virus signatures and anomaly-based protections from ThreatCloud.

upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: B

It's B for sure

upvoted 1 times

Question #75 *Topic 1*

When a Security Gateway communicates about its status to an IP address other than its own, which deployment option was chosen?

A. Targeted

B. Bridge Mode

C. Distributed

D. Standalone

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: C

C. Distributed

In a distributed deployment, the Security Gateway communicates about its status to an IP address other than its own, typically the IP address of the Security Management Server.

upvoted 1 times

EssentialD 11 months, 3 weeks ago

Selected Answer: C

C. Distributed

upvoted 1 times

Question #76 *Topic 1*

In HTTPS Inspection policy, what actions are available in the "Actions" column of a rule?

A. "Inspect", "Bypass", "Block"

B. "Inspect", "Bypass", "Categorize"

C. "Inspect", "Bypass"

D. "Detect", "Bypass"

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

GeorgySid 3 months, 1 week ago

HTTPS Inspection is not covered in the 156-215.81.20 exam

upvoted 2 times

darwin_2024 6 months, 3 weeks ago

Hi Everyone. I think we forgot that checkpoint has the https inspection profile.
by default there are two profile which is Default and Recommended and we can also clone those profiles and with that we can block specific protocol and services. so the answer is A

upvoted 2 times

1ca883b 10 months, 3 weeks ago

C

The actions available in the “Actions” column of a rule in HTTPS Inspection policy are “Inspect” and “Bypass”.

“Inspect” means that the HTTPS traffic will be decrypted and inspected according to the
Access Control policy.

“Bypass” means that the HTTPS traffic will not be decrypted and will be allowed
without inspection.

The other options are not valid actions for HTTPS Inspection policy

upvoted 2 times

EssentialD 11 months, 3 weeks ago

Selected Answer: C

C. "Inspect", "Bypass"

upvoted 1 times

BillNosie 1 year, 1 month ago

Selected Answer: C

Options are Bypass and Inspect.

upvoted 2 times

kmdls 1 year, 1 month ago

Selected Answer: C

Https inspection, as the name suggests, it allows to inspect and bypass actions
Does not have the power to block.

upvoted 2 times

Gabsf 1 year, 3 months ago

Selected Answer: C

C is the correct

upvoted 2 times

tosyeno 1 year, 3 months ago

Selected Answer: C

Inspect and Bypass are the only options under the action part of Https inspection. The appropriate answer is C

upvoted 1 times

Question #77 *Topic 1*

Why is a Central License the preferred and recommended method of licensing?

A. Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.

B. Central Licensing actually not supported with Gaia.

C. Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.

D. Central Licensing is the only option when deploying Gaia.

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: A

A. Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.

This provides flexibility and ease of management, as the license remains valid even if the IP address of the Security Gateway changes.

upvoted 1 times

Didesouzads 11 months ago

Selected Answer: A

Central Licensing ties with the Management

Local Licensing ties with the Gateway

upvoted 1 times

Question #78 *Topic 1*

In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

A. Install policy

B. Publish changes

C. Install database

D. Save changes

Correct Answer: *A*

Community vote distribution

A (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: A

A. Install policy

upvoted 1 times

Question #79 *Topic 1*

Which of the following is NOT an alert option?

A. SNMP

B. User defined alert

C. High alert

D. Mail

Correct Answer: *C*

Community vote distribution

C (100%)

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: C

C. High alert

"High alert" is not an alert option. The available alert options are:

SNMP
User defined alert
Mail
Alert (which can include various actions like showing a popup, sending an email, or running a script)

upvoted 1 times

Didesouzads 11 months ago

Selected Answer: C

Answer C

upvoted 1 times

Question #80 *Topic 1*

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

A. The Firewall will send out the packet on all interfaces

B. The Firewall will inform the client that the tunnel is down

C. The Firewall can update the Link Selection entries to start using a different link for the same tunnel

D. The Firewall will drop the packets

Correct Answer: *C*

Community vote distribution

Community vote distribution

keikei1228 3 months, 3 weeks ago

Selected Answer: C

C. The Firewall can update the Link Selection entries to start using a different link for the same tunnel

If the primary VPN link goes down, the Firewall can update the Link Selection entries to start using a different link for the same tunnel, ensuring continuity of the VPN connection.

upvoted 1 times

Normanby 5 months ago

Selected Answer: C

Key Word in Question = Primary, implying that there is a secondary, the Link Selector will select the secondary if the primary fails.

upvoted 1 times

67578ac 8 months, 2 weeks ago

Selected Answer: C

IT's C

upvoted 1 times

Slicklinton 10 months ago

Selected Answer: C

It's a vague question. it's C becuase the question says "primary vpn link" it means there is a secondary link. if there is no other link it's D..

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/Link-Selection.htm

upvoted 3 times

Didesouzads 11 months ago

Selected Answer: D

If you want link redundancy, you need to configure the option Use probing, in gateway's object

upvoted 2 times

Question #81 *Topic 1*

A layer can support different combinations of blades. What are the supported blades:

A. Firewall, NAT, Content Awareness and Mobile Access

B. Firewall, URLF, Content Awareness and Mobile Access

C. Firewall (Network Access Control), Application & URL Filtering and Content Awareness

D. Firewall (Network Access Control), Application & URL Filtering, Content Awareness and Mobile Access

Correct Answer: *D*

Community vote distribution

D (100%)

Community vote distribution

EssentialD 5 months, 2 weeks ago

Selected Answer: D

D. Firewall (Network Access Control), Application & URL Filtering, Content Awareness and Mobile Access

upvoted 1 times

EssentialD 6 months, 3 weeks ago

Selected Answer: D

I think it's D:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Ordered-Layers-and-Inline-Layers.htm

Ordered Layers and Inline Layers of the Policy. Here you can enable:

Firewall. This includes VPN (see VPN Column).
Application & URL Filtering (see Services & Applications Column).
Content Awareness (see Content Column).
Mobile Access (see Mobile Access to the Network).

upvoted 1 times

BillNosie 7 months, 2 weeks ago

Selected Answer: D

D is correct. Firewall, Applications & URL Filtering, Content Awareness, and Mobile Access are the available Blades when creating a new layer.

upvoted 1 times

pigtail 9 months ago

Selected Answer: D

Mobel Access is also an available blade.

upvoted 1 times

agolarait 9 months, 1 week ago

Selected Answer: D

the correct answer,
Firewall (Network Access Control): This blade is responsible for access control and inspection of network traffic based on defined rules and policies.

Application & URL Filtering: This blade allows administrators to control and manage applications and websites that users can access.

Content Awareness: This blade enables deep inspection of application data, including identification and control of sensitive data in protocols such as HTTP, SMTP, and FTP.