Question #1 *Topic 1*

What are the key components that make up the Check Point Three-Tier Architecture?

A. Gaia WebUI Portal, Security Management and Security Gateway installed together on same server

B. Security Dashboard, Management Database Server, Firewall

C. Web Security Console, Log Server, Firewall

D. SmartConsole, Security Management Server, Security Gateway

Suggested Answer: *D*

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

Question #2 *Topic 1*

What provides the trusted client option in SmartConsole?

A. IP address(es) allowed to connect to the Gaia Portal

B. IP address(es) allowed to connect to the Security Management Server using SmartConsole

C. IP address(es) allowed to connect to the Security Management Server using ssh

D. IP address(es) allowed to connect to the Security Gateway(s)

Suggested Answer: *B*

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

Question #3 *Topic 1*

Identify the default username and password for a newly installed Check Point appliance.

A. admin/password

B. admin/Chkp1234

C. cpadmin/cpadmin

D. admin/admin

Suggested Answer: *B*

f3eb371 1 month, 3 weeks ago

Selected Answer: D

Check Point Certified Security Administrator (CCSA) R82

upvoted 1 times

vpkings 2 months ago

Selected Answer: D

The default user/password is admin/admin.

upvoted 2 times

DarthFrank 2 months ago

Selected Answer: D

This is D admin/admin. Not sure why they put in B. You can even do a basic google search of this question and it shoots out it's admin/admin

upvoted 2 times

Question #4 *Topic 1*

What is the main purpose of objects in SmartConsole?

A. They are essential for defining security policies, network topologies, and other network configurations.

B. The objects represent potential targets of a DoS attack.

C. The objects serve as a target of an Access Control Policy.

D. The objects are items which has to be placed in the Track column of a security policy.

Suggested Answer: *A*

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

Question #5 *Topic 1*

How could you benefit from exporting a SmartConsole object to a CSV file?

A. To integrate object into Third Party Security Systems such as FortiManager.

B. You can use it in a script. For example, batch import to a different Quantum Security environment.

C. To get RADIUS Accounting information based on the utilization of those objects.

D. For saving the information as inventory information.

Suggested Answer: *B*

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

Question #6 *Topic 1*

What is the primary purpose of SmartConsole Objects?

A. To provide out-of-the-box threat prevention

B. To monitor user activity

C. To manage network traffic

D. To simplify and enhance cybersecurity management

Suggested Answer: *D*

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

Question #7 *Topic 1*

What is a Security Policy?

A. A collection of rules and settings that control network traffic and enforce the organization guidelines for data protection.

B. This is stored on the Security Gateway and enforced by the Security Management Server.

C. This is a written policy which has to conform with the Regulatory Compliance standards.

D. This is stored on the Security Management Server and enforced by the log server.

Suggested Answer: *A*

Community vote distribution

A (100%)

f3eb371 1 month ago

Selected Answer: A

A is the answer correct. confirmed with guide 82

upvoted 1 times

Question #8 *Topic 1*

Select the most correct statement about policy types.

A. IPS Threat Cloud Protections are included in Access Control Policy. Anti-Virus, Anti-Bot and SandBlast are included in the Threat Prevention Policy

B. Access Control Policy includes features like Firewall, Application Control and URL Filtering, IPS Threat Cloud Protections

C. NAT policy is a subset of Access Control Policy

D. Application Control is included in Access Control Policy. URL Filtering is included in the Threat Prevention Policy

Suggested Answer: *B*

Community vote distribution

C (100%)

kakashi74 1 week, 2 days ago

Selected Answer: C

C is correct, due to IPS is not included in access control, it is include in Threat Prevention Policy, NAT policy is included in access control

upvoted 1 times

f3eb371 1 month, 3 weeks ago

Selected Answer: C

IPS Threat Cloud Protections is not included in Access Control

upvoted 2 times

Question #9 *Topic 1*

What happens to packets if Explicit Default Rule is missing?

A. The Implicit Cleanup Rule is applied.

B. It depends on the Post NAT Rule.

C. It depends on the matching feature located after the Access Control policy.

D. Nothing happens as there is no matching rule.

Suggested Answer: *A*

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

Question #10 *Topic 1*

What is the effect of enabling “Shared Layer” in an Inline Layer?

A. It enables NAT translation

B. It disables the layer in other policies

C. It restricts access to the layer

D. It allows the layer to be used in multiple rules and policies

Suggested Answer: *D*

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

Question #11 *Topic 1*

When Accounting is enabled what is the time interval the logs are being updated?

A. The log is updated in 10-minute intervals.

B. The log update interval has to be specified as a firewall kernel parameter.

C. The log is updated in 10-minute intervals or if 20 MB of log data is collected.

D. The log update interval varies upon the queued user mode processes on the Management Servers, such as FWD, CPD, CPM.

Suggested Answer: *C*

Community vote distribution

A (100%)

f3eb371 1 month, 3 weeks ago

Selected Answer: A

CCSA Guide R82: Accounting

When Accounting is enabled, the system shows how much data has passed in the connection, including upload bytes, download bytes, and browse time. The log is updated in 10-minute intervals.

upvoted 1 times

Zxuen 2 months ago

Selected Answer: A

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.
Browse time is the total duration of a user session, including both active usage and idle
time. The session times out after the defined idle time.Idle time is the period within a
session when there is no user activity, but the connection remains open. <- From R82 admin guide

upvoted 1 times

Question #12 *Topic 1*

Select the correct option available in Tops in SmartConsole Logs view.

A. Top Users

B. Top Hosts

C. Top Gateways

D. Top Locations

Suggested Answer: *A*

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

Question #13 *Topic 1*

An administrator wants to identify which users are generating the most security events.
Which SmartConsole feature provides this insight?

A. Track Options

B. Log Indexing

C. Alerts

D. Tops

Suggested Answer: *D*

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

Question #14 *Topic 1*

What are the two main processes of the Identity Awareness blade?

A. Identity Decision Process (IDP)
Identity Direction and Accounting Process (IDAP)

B. Pre-Deployment Process (PDP)
Pre-Enforcement Process (PEP)

C. Policy Decision Point (PDP)
Policy Enforcement Point (PEP)

D. Inter-Process Communication (IPC)
Remote-Process Communication (RPC)

Suggested Answer: *C*

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

Question #15 *Topic 1*

Which of the following best describes how Access Role objects enhance identity-based policies in SmartConsole?

A. They store logs of user activity for auditing

B. They replace the need for traditional firewall rules

C. They allow grouping of users, computers, and networks into a single rule condition

D. They authenticate users before granting access

Suggested Answer: *C*

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

Question #16 *Topic 1*

Which of these is one of the Identity Sources used by the Identity Awareness Blade?

A. Identity Proxy API

B. LDAP Authentication

C. RADIUS Accounting

D. Certificate Enrolment Service (CES)

Suggested Answer: *B*

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

Question #17 *Topic 1*

Which component is essential for enabling HTTPS Inspection on a Security Gateway?

A. URL Filtering blade

B. DNS Resolver

C. Certificate Authority (CA) certificate

D. Static NAT rule

Suggested Answer: *C*

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

Question #18 *Topic 1*

What is the purpose of the "Fail Mode" setting in HTTPS Inspection?

A. To enforce strict NAT policies

B. To define how the gateway handles inspection failures

C. To disable inspection for internal traffic

D. To allow only HTTP traffic

Suggested Answer: *B*

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

Question #19 *Topic 1*

Some use cases for Application Control and URL Filtering rules are:

A. Monitor Applications, Allow Applications and Inform Users, Block malicious files

B. limit Applications traffic, Allow Applications and Inform Users, Block malicious files

C. limit Applications traffic, Block Applications and Inform Users, Block malicious files

D. Monitor Applications, Block Applications and Inform Users, Block Sites

Suggested Answer: *D*

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

Question #20 *Topic 1*

What are the predefined Autonomous Threat Prevention Profiles?

A. Perimeter, Strict, DMZ, guest

B. Perimeter, Strict, Internal, Guest

C. Perimeter, Strict, External, Guest

D. Perimeter, Strict, Internet, Guest

Suggested Answer: *B*

Community vote distribution

B (100%)

f3eb371 1 month, 3 weeks ago

Selected Answer: B

Perimeter, Strict, Internal, Guest, and "Monitor"... confirmed from the Smartconsole..

upvoted 1 times

Question #21 *Topic 1*

With Autonomous Threat-Prevention, you can choose a profile that best fits your needs.
What are the available options?

A. Perimeter, Cloud North-West, East-West, Lateral Movement, External Network.

B. Perimeter, Cloud/Data Center, Internal Network, Guest Network

C. Perimeter, Cloud/Data Center, East-West-Traffic, Guest Network

D. Perimeter, Fully Overlapping Encryption Domain, Partially Overlapping Encryption Domain, Proper Subset.

Suggested Answer: *B*

Community vote distribution

B (100%)

a36a80a 1 month, 1 week ago

Selected Answer: B

Strict Security for Perimeter Profile: Provides maximum security for perimeter gateways, offering a more aggressive posture to stop threats.
Cloud/Data Center Profile: Optimized to prevent cyberattacks targeting data centers, with extensive protection tailored for server traffic and east-west movement.
Internal Network Profile: Provides maximum security for traffic between internal users and internal servers, focusing on preventing lateral movement.
Recommended for Guest Network Profile: A "Detect-mode" profile designed to monitor cyberattack attempts via Guest Wi-Fi/networks in a non-intrusive way.

upvoted 2 times

Question #22 *Topic 1*

What is a recommended best practice after deploying Autonomous Threat Prevention?

A. Regularly monitor logs and reports for unusual activity

B. Use the same profile for all network segments

C. Disable logging to improve performance

D. Avoid customizing any profiles

Suggested Answer: *A*

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

Question #23 *Topic 1*

There are 2 ordered layers in a policy with 20 rules each. A connection matches rule number 5 in the first layer and the action for that rule is Drop. What will the firewall do now?

A. Both layers are checked simultaneously and the strictest action is taken, hence the Firewall will wait for the matching results of the second layer before taking an action

B. The Firewall will check if any rules in the second layer match with the connection and take action accordingly

C. The Firewall will drop the connection and stop further inspection for it

D. The Firewall will check if there is an Inline Layer attached to the rule 5 and will continue inspection if found

Suggested Answer: *C*

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

Question #24 *Topic 1*

Choose what best describes how Outbound HTTPS Inspection works.

A. The user's browser and the web server perform the HTTPS negotiation, which is monitored by the Security Gateway to collect the encryption keys. Once the encrypted communication between the user and the web server begins, the Security Gateway intercepts and decrypts it with the acquired encryption key.

B. The Security Gateway impersonates the requested Web Site and completes the HTTPS negotiation. A separate HTTPS-encrypted connection is automatically created between Security Gateway and the web server.

C. The user must insert a static encryption key provided by the filewall, into their browser. All HTTPS communication by the user's browser is always encrypted with this key. As the key is provided by the Security Gateway, it can decrypt the communication between the user and the web server

D. When HTTPS Inspection is enabled on the Security Gateway, a JavaScript payload is sent to the user's browser when a request to connect to HTTPS websites is made. The JavaScript code inserts a Browser Helper Module (BHO) that helps detects and shares the encryption key with the Security Gateway.

Suggested Answer: *B*

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

Question #25 *Topic 1*

In HTTPS Inspection, what is the role of Categorization Mode?

A. It disables inspection for trusted sites

B. It decrypts all HTTPS traffic by default

C. It blocks all encrypted traffic

D. It categorizes traffic based on domain and certificate without decryption

Suggested Answer: *D*

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

Question #26 *Topic 1*

By default, alerts about specific security events are sent by which method?

A. pop-ups

B. log

C. SNMP

D. mail

Suggested Answer: *B*

Community vote distribution

A (100%)

a36a80a 1 month, 1 week ago

Selected Answer: A

Alert Workflow and Methods

Default Behavior: The Security Management Server forwards alerts to SmartView Monitor, which then triggers the pop-up notification by default.

upvoted 1 times

Question #27 *Topic 1*

What is the purpose of the Explicit Default Cleanup Rule?

A. To forward unmatched traffic

B. To accept unmatched traffic

C. To drop unmatched traffic

D. To encrypt unmatched traffic

Suggested Answer: *C*

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

Question #28 *Topic 1*

What is the main purpose of SecureXL?

A. Provides software-based solution Security Management Performance.

B. The gateway accesses the central ThreatCloud information to get the verdict of specific files prior to sending it to the intended destination.

C. This is a solution to offer SSL Offloading to minimize the performance impact of the servers located in the Web Server farm.

D. Provides software-based solution for Security Gateway Performance.

Suggested Answer: *D*

Community vote distribution

D (100%)

f3eb371 1 month, 2 weeks ago

Selected Answer: D

Provides software-based solution for Security Gateway Performance, confirmed from Guide R82

upvoted 1 times

Question #29 *Topic 1*

What management solution does Check Point offer as a service to deliver unified management for self-hosted Security Gateways, and ensures secure multifactor authentication access?

A. CloudGuard SaaS

B. CloudGuard Network Security

C. Smart-1 Cloud

D. SMS Cloud Extension Hotfix (SCEH)

Suggested Answer: *C*

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

Question #30 *Topic 1*

Which of the following is the default role-based shell on Gaia?

A. Expert

B. AdvancedCLI

C. Supermode

D. Clish

Suggested Answer: *D*

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

Question #31 *Topic 1*

Which tool provides a graphical interface for centralized management of the Check Point Security environment?

A. Gaia Portal

B. Security Management Server

C. SmartConsole

D. SmartEvent

Suggested Answer: *C*

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

Question #32 *Topic 1*

One of the key component of the Three-Tier Architecture of Check Point R82 is:

A. SmartDashboard

B. SmartProvisioning

C. SmartUpdate

D. SmartConsole

Suggested Answer: *D*

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

Question #33 *Topic 1*

What is the primary purpose of SecureXL?

A. Provides software-based solution for Security Gateway performance

B. Encrypts and decrypts traffic to and from Security Gateways

C. Protect sensitive data from being lost, stolen, or accessed by unauthorized users

D. Identifies and controls sensitive data within network

Suggested Answer: *A*

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

Question #34 *Topic 1*

What is the access available to connect to cli?

A. SCP

B. SSH

C. SNMP

D. FTP

Suggested Answer: *B*

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

Question #35 *Topic 1*

What are some of the common tasks that the SmartConsole is used for?

A. Create and manage policies, Monitor logs, Maintain licenses and contracts

B. Create and manage licenses. Monitor policies, Maintain performance

C. Manage all devices on the corporate network, including firewalls, security gateway, switches, routers and load balancers.

D. Redeploy the management server and gateways during troubleshooting

Suggested Answer: *A*

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

Question #36 *Topic 1*

What is the purpose of the Security Policies menu in SmartConsole?

A. To create and manage security policies

B. To monitor security logs

C. To install policies

D. To configure system settings

Suggested Answer: *A*

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

Question #37 *Topic 1*

What is the role of the Security Gateway in the Check Point environment?

A. To act as a centralized management server

B. To provide a web-based interface

C. To inspect inbound and outbound traffic

D. To manage objects and policies

Suggested Answer: *C*

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

Question #38 *Topic 1*

What control is available in SmartConsole GUI Main Window?

A. Objects Manager

B. Objects Explorer

C. Objects Selector

D. Objects Menu

Suggested Answer: *D*

Community vote distribution

B (100%)

a36a80a 1 month, 1 week ago

Selected Answer: B

he main SmartConsoleClosed Menu. When SmartConsole is connected to a Security Management ServerClosed, this includes:

Manage policies and layers

Open Object Explorer

New object (opens menu to create a new object)

Publish session

Discard session

Session details

Install policy

Verify Access Control Policy

Install Database

Uninstall Threat Prevention policy

Management High AvailabilityClosed

Manage Licenses and Packages

Global Properties

View (opens menu to select a View to open)

upvoted 2 times

Question #39 *Topic 1*

What is the correct default permission profile?

A. Super Admin

B. Super Profile

C. Super Permission

D. Super User

Suggested Answer: *D*

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

Question #40 *Topic 1*

Which authentication method is the simplest for SmartConsole admin accounts?

A. Check Point Password

B. SecurID

C. RADIUS

D. OS Password

Suggested Answer: *A*

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

Question #41 *Topic 1*

What is the primary function of the 'Trusted Clients' feature in SmartConsole?

A. To restrict access to the management server

B. To manage user accounts

C. To configure network settings

D. To install security policies

Suggested Answer: *A*

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

Question #42 *Topic 1*

Which type of administrator account is used to log in to the Gaia Portal or Gaia Clish command line?

A. Primary Security Management Server admin account

B. Gaia admin account

C. API admin account

D. SmartConsole admin account

Suggested Answer: *B*

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

Question #43 *Topic 1*

What is the purpose of the 'Advanced' window in SmartConsole session management?

A. To define session requirements

B. To compare selected revisions

C. To manage security policies

D. To view connected administrator sessions

Suggested Answer: *A*

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

Question #44 *Topic 1*

Which feature enhances security by restricting access to the Management Server to only those SmartConsole clients that are explicitly permitted?

A. Gaia Admin Roles

B. Permission Profiles

C. allowed-gui-ips.conf file in $CPDIR/conf

D. Trusted Clients

Suggested Answer: *D*

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

Question #45 *Topic 1*

Which of the following groups represents valid administrator types in the Quantum Security environment?

A. Quantum global admin, Quantum local admin, Quantum cloud admin

B. CloudGuard admin, Harmony admin, Infinity admin

C. Firewall admin, Management admin, OS admin

D. Gaia admin, Primary SMS admin, SmartConsole admin

Suggested Answer: *D*

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

Question #46 *Topic 1*

Where is it possible to view SmartConsole locked account?

A. Administrators list under Permissions & administrators

B. View Sessions in Gaia portal

C. View Sessions in SmartConsole

D. cpview in ssh

Suggested Answer: *C*

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

Question #47 *Topic 1*

The Objects menu provides more management capabilities than the GATEWAYS & SERVERS New menu. It lets you add all types of custom objects. What other object management tool can the administrator use to manage objects in a separate window?

A. The Objects Pane

B. The Categories Explorer

C. The Object Explorer

D. The More object types menu

Suggested Answer: *C*

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

Question #48 *Topic 1*

Which type of object represents Office365?

A. Updatable object

B. server

C. host

D. logical object

Suggested Answer: *A*

Community vote distribution

A (100%)

f3eb371 4 weeks ago

Selected Answer: A

R82 Guide: updatable objext arespecial types Network Object that represent external services, such as Office365, AWS, and GEO locations....

upvoted 1 times

Question #49 *Topic 1*

What is the most appropriate statement about methods of managing objects in SmartConsole?

A. Objects can be managed by various methods like New Menu in Gateways & Servers, Objects Menu, Object Explorer, or, Rules in the Security Policy

B. Only Gateway and Management Objects are managed from the New Menu in Gateways and Servers. All other objects can be managed from Objects Menu or Object Explorer. Objects can only be selected in the Rules in Security Policy

C. Objects can only be managed from the Object Explorer, however they can be viewed in the Rules in Security Policy

D. Objects can be management either from Objects Menu or from Object Explorer. All other methods including the Rules in Security Policy are for view only

Suggested Answer: *A*

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

Question #50 *Topic 1*

Which menu in SmartConsole provides the most comprehensive object management capabilities?

A. Rule menu

B. Object Explorer

C. Objects menu

D. New menu

Suggested Answer: *B*

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

Question #51 *Topic 1*

What are the default zone objects?

A. InternalZone, ExternalZone, DMZZone

B. InternalZone, PublicZone, DMZZone

C. InternalZone, WanZone, DMZZone

D. InternalZone, Internetzone, DMZZone

Suggested Answer: *A*

Community vote distribution

A (100%)

DarthFrank 2 months ago

Selected Answer: A

Yeah, I confirmed on Checkpoint site. Confirmed they are InternalZone, ExternalZone, DMZZone. Glad this is why we double check our work

upvoted 2 times

herroyip 2 months ago

Selected Answer: A

The answer should be InternalZone, ExternalZone and DMZZone.

upvoted 3 times

TaiwanCanHelp 2 months ago

Selected Answer: A

According to the Object menu in Smartconsole, they are InternalZone, ExternalZone and DMZZone. Arem't they ?

upvoted 3 times

Question #52 *Topic 1*

How are objects organized in the SmartConsole?

A. These objects are organized by type in SmartConsole.

B. These objects are organized by priority in SmartConsole.

C. These objects are organized by category in SmartConsole.

D. These objects are organized alphabetically in SmartConsole.

Suggested Answer: *C*

Community vote distribution

C (100%)

a36a80a 1 month, 1 week ago

Selected Answer: C

Object Categories

Objects in SmartConsoleClosed represent networks, devices, protocols and resources. SmartConsole divides objects into these categories:

upvoted 2 times

f3eb371 1 month, 2 weeks ago

Selected Answer: C

These objects are organized by category in SmartConsole. Confirmed from the Smartconsole.

upvoted 1 times

Question #53 *Topic 1*

What is the purpose of Dynamic Objects in SmartConsole?

A. To change IP addresses dynamically

B. To provide default security settings

C. To represent external services

D. To manage user accounts

Suggested Answer: *C*

Community vote distribution

A (100%)

f3eb371 1 month, 3 weeks ago

Selected Answer: A

Common use cases: * Interfaces with IP addresses obtained via DHCP.

Environments where IP addresses change frequently and immediate updates are required without centralized management.

Automation scripts that update local blocklists.

upvoted 1 times

DarthFrank 2 months ago

Selected Answer: A

Yeah it's A. I mean the answer is in the wording "Dynamic" so it changes. I googled the question and confirmed this is correct. Double checked on Checkpoint site as well.

upvoted 3 times

1e0adb2 2 months, 1 week ago

Selected Answer: A

Dynamic objects are special types of logical objects that can change their IP address dynamically. A Is the correct answer

upvoted 1 times

Question #54 *Topic 1*

What is the primary purpose of the Security Policy Management solution?

A. To provide out-of-the-box threat prevention

B. To manage network traffic

C. To simplify and enhance cybersecurity management

D. To monitor user activity

Suggested Answer: *C*

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

Question #55 *Topic 1*

How many predefined Security Zones as a starting point are available in a newly installed Security Management Server?

A. 5

B. 4

C. 3

D. 6

Suggested Answer: *C*

Community vote distribution

B (100%)

kakashi74 1 week, 2 days ago

Selected Answer: B

B is correct,

WirelessZone - Networks that can be accessed by users and applications with a wireless connection.

ExternalZone - Networks that are not secure, such as the Internet and other external networks.

DMZZone - A DMZ (demilitarized zone) is sometimes referred to as a perimeter network. It contains company servers that can be accessed from external sources

InternalZone - Company networks with sensitive data that must be protected and used only by authenticated users.

upvoted 1 times

DarthFrank 2 months ago

Selected Answer: B

Yeah, I have to go with B. When I google search and search on Checkpoint, I see it states 4.

upvoted 1 times

TaiwanCanHelp 2 months ago

Selected Answer: B

According to page 308 of R82 management guide, there are four Predefined Zone objects： WirelessZone, InternalZone, DMZZone and ExternalZone. So I think the answer is B.

upvoted 2 times

Question #56 *Topic 1*

Automatic NAT rules can be enabled inside the _____.

A. Domain Object

B. Network Group Object

C. Service Object

D. Host Object

Suggested Answer: *D*

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

Question #57 *Topic 1*

What are the capabilities integrated into a Threat Prevention Policy?

A. IPS Anti-Bot, Anti-Virus, Content Awareness, URL Filtering

B. IPS, Anti-Bot, Anti-Virus, SandBlast

C. IPS, Anti-Bot, Application Control, URL Filtering

D. Application Control, URL Filtering, Content Awareness, IPS

Suggested Answer: *B*

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

Question #58 *Topic 1*

What is the difference between the Positive Control Model and the Negative Control Model?

A. The Positive Control Model allows is what routers use and simply route traffic with no security rules. The Negative Control Model is what firewalls use and they require explicit rules to allow and route traffic.

B. The Positive Control Model allows specific, approved actions or traffic and blocks everything else. The Negative Control Model begins by blocking specific, known threats, or unwanted actions and allows everything else.

C. The Positive Control Model begins by blocking specific, known threats, or unwanted actions and allows everything else. The Negative Control Model allows specific, approved actions or traffic and blocks everything else.

D. The Positive Control Model aims to keep administrators in a positive mind set. The Negative Control Model results in administrators having a negative mind set.

Suggested Answer: *B*

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

Question #59 *Topic 1*

Which type of Control Model is used in Application Control & URL Filtering and Content Awareness Policy?

A. Permissive Control Model (also known as Whitelist Model)

B. Restrictive Control Model (also known as Blacklist Model)

C. Positive Control Model (also known as Whitelist Model)

D. Negative Control Model (also known as Blacklist Model)

Suggested Answer: *D*

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

Question #60 *Topic 1*

What is the purpose of the Cleanup Rule in a security policy?

A. To accept all unmatched traffic

B. To log all security events

C. To block all known malicious traffic

D. To drop or reject all traffic that does not match any rule in the rulebase

Suggested Answer: *D*

Community vote distribution

D (100%)

DarthFrank 2 months ago

Selected Answer: D

Yeah, it's sort of D. Checkpoint drops all traffic that isn't explicitly accepted no matter what. Technically the "drop" rule is to really "log" everything so you can track everything that drops for record keeping and auditing purposes. This also allows you to check out everything in case someone needs access and it's not working. You can review the log and see "ok you're hitting the drop rule so I need to put in something to allow it". If you didn't have that rule, it gets dropped anything, but just doesn't get logged. Majority of companies require you to log all of this for compliance issues. This also helps you look out for potential attacks as well. So it's silly when they ask this type of questions and they put this type of answer.

upvoted 2 times

Question #61 *Topic 1*

Select the correct description of the Explicit Rules.

A. Explicit rules are created by the administrator

B. Explicit rules are created in Security Policies by the Security Management Server

C. Explicit rules are created by the Security Gateway

D. Explicit rules are created in the Global Properties on the Security Management Server

Suggested Answer: *A*

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

Question #62 *Topic 1*

The Access Control Policy includes which of these features?

A. Firewall, Application & URL Filtering, Content Awareness, IPsec VPN and Mobile Access, Identity Awareness

B. Firewall, Application &U RL Filtering, Data Loss Prevention, IPsec VPN and Mobile Access, Identity Awareness

C. Firewall, Application &U RL Filtering, antivirus, IPsec VPN and Mobile Access, Identity Awareness

D. Firewall, Application &U RL Filtering, file content analysis, IPsec VPN and Mobile Access, Identity Awareness

Suggested Answer: *A*

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

Question #63 *Topic 1*

What is the difference between the Access Control policy and NAT policy?

A. The Access Control policy is a collection of rules that control network access. The NAT rules can be used to make the gateway change IP addresses and port numbers in packets.

B. The Access Control policy is an enforced on the Security Gateway. The NAT rules are enforced on a separate NAT Gateway.

C. The Access Control policy is a collection of rules that control application and web site access. The NAT rules allow or deny connections on the gateway and can also change IP addresses and port numbers in packets.

D. The Access Control policy is a collection of rules that mostly blocks network access. The NAT rules are used to allow access through the gateway. A NAT rule causes the gateway to allow access to or from the IP addresses and translates the packet according to the rule.

Suggested Answer: *A*

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

Question #64 *Topic 1*

Inline Layers are evaluated against the rules; if none of the rules match _____ is applied.

A. the Accept action

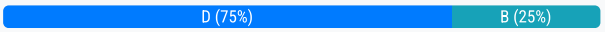
B. the Implicit Cleanup Rule

C. the Drop action

D. the Explicit Cleanup Rule if exists

Suggested Answer: *D*

Community vote distribution



f3eb371 1 month, 2 weeks ago

Selected Answer: D

Check Point Certified Security Administrator (CCSA) R82 /pg 252: -

- If none of the rules match, the Explicit Default Cleanup Rule is applied.
- if Explicit Default Cleanup Rule is missing , the Implicit Cleanup Rule is applied.

upvoted 1 times

DarthFrank 2 months ago

Selected Answer: B

B is Correct. Inline Layers are evaluated against the rules; if none of the rules match the Implicit Cleanup Rule is applied. This ensures that traffic not matching any specific rule within the sub-policy is handled according to the default behavior, often resulting in a drop, similar to how an explicit cleanup rule behaves when no rules match

upvoted 1 times

1e0adb2 2 months, 2 weeks ago

Selected Answer: D

If there is an explicit cleanup rule it goes first so this is the correct answer

upvoted 2 times

DarthFrank 2 months ago

It's B. See my other comment

upvoted 1 times

Question #65 *Topic 1*

What happens when a rule in an Ordered Layer matches a packet and the action is Drop?

A. The packet is encrypted

B. The packet is dropped and no further rules are checked

C. The packet is logged and forwarded

D. The packet is sent to the next layer

Suggested Answer: *B*

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

Question #66 *Topic 1*

Which Identity Awareness Client can collect identities from not only Active Directory Domain Controllers, but also from Cisco Identity Services Engine Servers or NetIQ eDirectory Servers?

A. Identity Agent for a User Endpoint Computer

B. Identity Agent for a Terminal Server v2

C. Identity Agent for a Terminal Server

D. Identity Collector

Suggested Answer: *D*

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

Question #67 *Topic 1*

When looking at the Ordered Access Control Layers in the SmartConsole they are organized sequentially. How does the security gateway enforce the rules?

A. All ordered layers are analyzed in parallel. If there is a matched drop rule in any layer then the traffic is allowed.

B. After checking each layer the firewall engages the relevant blades and starts to evaluate again one at a time while working with the other access control blades.

C. Each layer is evaluated independently.

D. All ordered layers are analyzed in parallel. If there is a matched accept rule in any layer then the traffic is allowed.

Suggested Answer: *C*

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

Question #68 *Topic 1*

Which of the following is a best practice for policy layers?

A. Avoid sharing layers across policies

B. Use only one layer per policy

C. Disable implicit cleanup rules

D. Share layers with other policy packages

Suggested Answer: *D*

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

Question #69 *Topic 1*

What is the purpose of Audit logs?

A. Audit Logs record administrative actions, such as configuration of static routes in CLISH or adding an OS administrator password.

B. Audit Logs record administrative actions, such as policy modifications, user logins, and configuration changes.

C. Audit Logs is to check the validity of the IPS, Anti-Bot, Anti-Virus, URL Filtering, Application Control subscription license from the Check Point ThreatCloud repository.

D. Audit Log is to comply with the Regulations, such as FIPS, HIPAA or PCI-DSS.

Suggested Answer: *B*

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

Question #70 *Topic 1*

In which deployment type is the log indexing disabled by default?

A. Bridge mode

B. Distributed

C. Maestro Orchestrator

D. Standalone

Suggested Answer: *D*

Community vote distribution

D (100%)

a36a80a 1 month, 1 week ago

Selected Answer: D

Enabling Log Indexing

Log indexing on the Security Management Server or Log Server reduces the time it takes to run a query on the logs. Log indexing is enabled by default.

In a standaloneClosed deployment, log indexing is disabled by default. Enable log indexing only if the standalone server CPU has 4 or more cores.

upvoted 1 times

DarthFrank 2 months ago

Selected Answer: D

Incorrect. It's Standalone. Confirmed on checkpoint site. From checkpoint "In a standalone deployment, log indexing is disabled by default"

upvoted 2 times

Question #71 *Topic 1*

What happens when disk space on the Log Server drops below 5000 MBytes by default?

A. A popup alert is triggered

B. Files begin to be deleted

C. Logging stops immediately

D. A script is executed

Suggested Answer: *B*

Community vote distribution

B (100%)

f3eb371 1 month, 2 weeks ago

Selected Answer: B

Confirmed in R82 Guide, file begin to delete.

upvoted 1 times

DarthFrank 2 months ago

Selected Answer: B

Can confirm with Checkpoint that they will begin to delete. It's B

upvoted 1 times

Toma1998 2 months, 1 week ago

Selected Answer: B

Files begin to delete

upvoted 3 times

Question #72 *Topic 1*

Which component is the source of the Logs sent to the Log Server?

A. The SmartReporter along with the Eventia Reporter.

B. The SmartEvent Correlation Unit

C. The SmartEvent Server

D. Security Gateway

Suggested Answer: *D*

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

Question #73 *Topic 1*

When should you enable log indexing on a Standalone Deployment?

A. Log indexing is enabled by default on all deployments

B. only when the standalone computer CPU has 8 or more cores

C. Log indexing is disabled by default only on Bridge mode deployments

D. only when the standalone computer CPU has 4 or more cores

Suggested Answer: *D*

Community vote distribution

D (100%)

DarthFrank 2 months ago

Selected Answer: D

What is funny is the other question that says Log indexing is disabled for distributed, but it's actually standalone. Here it shows the right answer for Standalone and you want to do it when its for the 4 CPU. This is the right answer.

upvoted 2 times

Question #74 *Topic 1*

Select the correct description of the SmartView Monitor.

A. Used to view collected logs, monitor health, performance, and regulatory compliance of Check Point components

B. Used to view collected logs and query for information

C. Used to monitor health, performance, and regulatory compliance of Check Point components using web browser

D. Used to monitor health, performance, and regulatory compliance of Check Point components

Suggested Answer: *D*

Community vote distribution

D (100%)

f3eb371 1 month, 2 weeks ago

Selected Answer: D

Used to monitor health, performance, and regulatory compliance of Check Point components. From R82 Guide.D is the correct.

upvoted 1 times

Question #75 *Topic 1*

What type of logs capture security-related events such as firewall activity and VPN connections?

A. Audit Logs

B. Security Logs

C. Compliance Logs

D. Traffic Logs

Suggested Answer: *B*

Community vote distribution

B (100%)

f3eb371 1 month, 2 weeks ago

Selected Answer: B

B. Security Logs

upvoted 1 times

Question #76 *Topic 1*

What is the difference between generating logs per connection or per session?

A. Per Session is only available for URL Filtering, whereas the Connection could be applied to URL Filtering as well as Application Control.

B. Per connection means that a log is generated for each connection in the session while per session means that only one log per session is generated.

C. Per Session means that you will get the name of application in Application Control, although the applications were not specified in the rule base. Per Connections means that you will get the whole list of content in the Content Awareness blade.

D. Per session means that a log is collected for each session in a connection while per connection means that only one log is collected per session.

Suggested Answer: *B*

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

Question #77 *Topic 1*

Which Identity Awareness client is used in high-volume environments that use Microsoft Active Directory, Cisco Identity Services, NetIQ eDirectory, or Syslog?

A. Identity Agent for a Terminal Server

B. Identity Collector

C. RADIUS Accounting

D. Identity Agent for a User Endpoint Computer

Suggested Answer: *B*

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

Question #78 *Topic 1*

How do you match a user or a computer identity in the security policy?

A. Use identity awareness objects in source or destination columns.

B. Use the AD Query Object in source or destination column.

C. Use a user or a user group object in source or destination column.

D. Use Access Role Objects in source or destination columns.

Suggested Answer: *D*

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

Question #79 *Topic 1*

What is the first step in deploying Identity Awareness?

A. Publish Session Changes

B. Configure Identity Sources

C. Enable Identity Awareness

D. Install Security Policy

Suggested Answer: *C*

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

Question #80 *Topic 1*

What is the role of Policy Decision Point (PDP) in Identity Awareness?

A. The PDP receives identity data from identity sources

B. The PDP receives identity data from the identity sources and enforces network access restrictions on traffic based on the identity of a user

C. The PDP is an object to configure specifies users, computers, and network locations as one object

D. The PDP enforces network access restrictions on traffic based on the identity of a user

Suggested Answer: *A*

Community vote distribution

A (100%)

a36a80a 1 month, 1 week ago

Selected Answer: A

Identity Acquisition: The PDP acts as a central repository that learns which user is associated with which IP address by querying or receiving updates from identity sources.

Policy Calculation: Once identities are known, the PDP calculates the appropriate Access Roles for those identities and communicates the decisions to the Policy Enforcement Point (PEP).

Separation of Roles: In the Check Point architecture, the PDP is the "brain" that knows who the users are, while the PEP is the "bouncer" that actually enforces the rules on the traffic.

upvoted 1 times

f3eb371 1 month, 2 weeks ago

Selected Answer: A

Guide R82: "The PDP receives identity data from the identity sources. It organizes the data into tables before forwarding the data to the PEP.

The PEP enforces network access restrictions on traffic based on the identity and negotiates with PDP about shared identities."

upvoted 1 times

TaiwanCanHelp 1 month, 3 weeks ago

Selected Answer: A

I think the answer is A. Enforcing network access restrictions is exclusively the PEP's responsibility, not the PDP

upvoted 1 times

Question #81 *Topic 1*

What of the following is NOT an Identity Source supported by the Check Point Identity Awareness Blade?

A. Remote Access and Terminal Servers.

B. Identity Connector and TACACS

C. Browser-Based Authentication and AD Query.

D. RADIUS Accounting, Identity Collector.

Suggested Answer: *B*

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

Question #82 *Topic 1*

Which Identity Source provides identity information through Captive Portal login or Transparent Kerberos Authentication?

A. Browser-Based Authentication

B. Identity Agents

C. RADIUS Accounting

D. AD Query

Suggested Answer: *A*

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

Question #83 *Topic 1*

What is the purpose of the Policy Enforcement Point (PEP) in Identity Awareness?

A. To receive identity data from identity sources

B. To organize identity data

C. To store logs of user activity

D. To enforce network access restrictions based on identity

Suggested Answer: *D*

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

Question #84 *Topic 1*

Which HTTPS Inspection setting allows bypassing connections to software update services?

A. Fail Mode

B. Categorization Mode

C. Bypass Allow List

D. Certificate Blocking

Suggested Answer: *C*

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

Question #85 *Topic 1*

After enabling and configuring Outbound HTTPS inspection on Security Gateway, you need to prevent users from getting warnings about the generated CA certificates that HTTPS Inspection uses.
In which certificate store do you need to add exported HTTPS Inspection certificate to client computer?

A. Third-party Root Certification Authorities certificate store - (Local Computer)

B. Trusted Root Certification Authorities certificate store - (Local computer)

C. Third-party Root Certification Authorities certificate store - (Current User)

D. Trusted Root Certification Authorities certificate store - (Current user)

Suggested Answer: *B*

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

Question #86 *Topic 1*

You have been tasked with determining how much resources will be consumed by a potential HTTPS inspection deployment.
Which of the following tools can you use?

A. listening mode

B. Learning mode

C. inbound HTTPS inspection only

D. Full Deployment

Suggested Answer: *A*

Community vote distribution

B (100%)

a36a80a 1 month, 1 week ago

Selected Answer: B

In Check Point R82, Learning Mode is a feature specifically designed to help administrators determine the potential impact of an HTTPS inspection deployment. It allows the Security Gateway to inspect a small, representative percentage of traffic to collect data on CPU utilization, memory usage, and connection success rates. By analyzing this data over a learning period (typically two weeks), the gateway can provide a reliable estimation of resource consumption and identify potential connectivity issues before a full-scale rollout is implemented.

upvoted 2 times

f3eb371 1 month, 2 weeks ago

Selected Answer: B

Guide R82: BESTPRACTICE When enabling HTTPS Inspection for the first time in an environment, it is considered best practice to start in Learning Mode to minimize the risk of traffic disruption.

upvoted 1 times

Question #87 *Topic 1*

Which of the following is a best practice for URL Filtering?

A. Disable HTTPS Inspection to reduce complexity

B. Use outdated URL databases for stability

C. Combine both in a single rule for simplicity

D. Create custom URL categories for specific needs

Suggested Answer: *D*

Community vote distribution

D (100%)

f3eb371 1 month, 2 weeks ago

Selected Answer: D

R82 Guide confirmed.

upvoted 1 times

Question #88 *Topic 1*

What is true of the URL Filtering Software Blade?

A. It's part of HTTPS Inspection Policy

B. It's part of URL Filtering policy

C. It's part of the Access Control Policy

D. It's part of Threat Prevention Policy

Suggested Answer: *C*

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

Question #89 *Topic 1*

How does Application Control blade identify and control the usage of applications?

A. By using signatures to determine applications from the traffic flow

B. by using port and protocol, to determine the application from the traffic flow

C. by using protocol and encryption, to determine the application from the traffic flow

D. by using port, protocol and encryption, to determine the application from the traffic flow

Suggested Answer: *A*

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

Question #90 *Topic 1*

What is one main purpose of URL Filtering?

A. Automatic translation of foreign web sites into your preferred language.

B. Specify the application which should be blocked during business hours, such as Facebook-Game, Indeed-Chat, among others.

C. Synchronizing verdicts on URL Categories for better hit rates.

D. Use URL Categories to block access to malicious or non-work-related websites.

Suggested Answer: *D*

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