CheckPoint

156-915.80 Exam

Check Point Certified Security Expert Update - R80 Exam

Version: 10.0

Question: 1

What is the port used for SmartConsole to connect to the Security Management Server:

A. CPMI port 18191/TCP
B. CPM port / TCP port 19009
C. SIC port 18191/TCP
D. https port 4434/TCP

Answer: A

Question: 2

Which is the correct order of a log flow processed by SmartEvents components:

A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
B. Firewall > SmartEvent Server Database > Correlation unit > Log Server > SmartEvent Client
C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

Question: 3

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
C. Mail, Block Source, Block Destination, External Script, SNMP Trap
D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

Explanation:
These are the types of Automatic Reactions:
Mail - tell an administrator by email that the event occurred. See Create a Mail Reaction.
Block Source - instruct the Security Gateway to block the source IP address from which this event was detected for a configurable period of time . Select a period of time from one minute to more than three weeks. See Create a Block Source Reaction

Block Event activity - instruct the Security Gateway to block a distributed attack that emanates from multiple sources, or attacks multiple destinations for a configurable period of time. Select a period of time from one minute to more than three weeks). See Create a Block Event Activity Reaction.
External Script - run a script that you provide. See Creating an External Script Automatic Reaction to write a script that can exploit SmartEvent data.
SNMP Trap - generate an SNMP Trap. See Create an SNMP Trap Reaction.

Question: 4

Which components allow you to reset a VPN tunnel?

A. vpn tu command or SmartView monitor
B. delete vpn ike sa or vpn she11 command
C. vpn tunnelutil or delete vpn ike sa command
D. SmartView monitor only

Answer: D

Question: 5

When synchronizing clusters, which of the following statements is FALSE?

A. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
B. Only cluster members running on the same OS platform can be synchronized.
C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.

Answer: D

Question: 6

Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
B. Limits the upload and download throughout for streaming media in the company to 1 Gbps.
C. Time object to a rule to make the rule active only during specified times.
D. Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule

Answer: A

Question: 7

In R80.10, how do you manage your Mobile Access Policy?

A. Through the Unified Policy
B. Through the Mobile Console
C. From SmartDashboard
D. From the Dedicated Mobility Tab

Answer: C

Question: 8

You find one of your cluster gateways showing “Down” when you run the “cphaprob stat” command. You then run the “clusterXL_admin up” on the down member but unfortunately the member continues to show down. What command do you run to determine the case?

A. cphaprob –f register
B. cphaprob –d–s report
C. cpstat–f-all
D. cphaprob –a list

Answer: D

Question: 9

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services

Answer: C

Question: 10

Which of the following is NOT a valid way to view interface’s IP address settings in Gaia?

A. Using the command sthtool in Expert Mode
B. Viewing the file / config/ active
C. Via the Gaia WebUl
D. Via the command show configuration in CLISH

Answer: A

Question: 11

Check Point recommends configuring Disk Space Management parameters to delete old log entities when available disk space is less than or equal to?

A. 50%
B. 75%
C. 80%
D. 15%

Answer: D

Question: 12

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

A. new host name “New Host” ip-address “192.168.0.10”
B. set host name “New Host” ip-address “192.168.0.10”
C. create host name “New Host” ip-address “192.168.0.10”
D. add host name “New Host” ip-address “192.168.0.10”

Answer: D

Sample Command with SmartConsole CLI You can use the add host command to create a new host and then publish the changes. > add host name "Sample_Host" ip-address "192.0.2.3" > publish

Question: 13

What are types of Check Point APIs available currently as part of R80.10 code?

A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API
B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

Question: 14

Which of the following is NOT an internal/native Check Point command?

A. fwaccel on
B. fw ct1 debug

C. tcpdump
D. cphaprob

Answer: C

Question: 15

What is the SandBlast Agent designed to do?

A. Performs OS-level sandboxing for SandBlast Cloud architecture
B. Ensure the Check Point SandBlast services is running on the end user's system
C. If malware enters an end user's system, the SandBlast Agent prevents the malware form spreading with the network
D. Clean up email sent with malicious attachments.

Answer: C

Question: 16

The SmartEvent R80 Web application for real-time event monitoring is called:

A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView

Answer: A

Question: 17

What Shell is required in Gaia to use WinSCP?

A. UNIX
B. CPShell
C. CLISH
D. Bash

Answer: D

Question: 18

Which one of the following is true about Threat Emulation?

A. Takes less than a second to complete
B. Works on MS Office and PDF files only
C. Always delivers a file

D. Takes minutes to complete (less than 3 minutes)

Answer: D

Question: 19

What are the minimum open server hardware requirements for a Security Management Server/Standalone in R80.10?

A. 2 CPU cores, 4GB of RAM and 15GB of disk space
B. 8 CPU cores, 16GB of RAM and 500 GB of disk space
C. 4 CPU cores, 8GB of RAM and 500GB of disk space
D. 8 CPU cores, 32GB of RAM and 1 TB of disk space

Answer: C

Question: 20

The “MAC magic” value must be modified under the following condition:

A. There is more than one cluster connected to the same VLAN
B. A firewall cluster is configured to use Multicast for CCP traffic
C. There are more than two members in a firewall cluster
D. A firewall cluster is configured to use Broadcast for CCP traffic

Answer: D

Question: 21

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

A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode

Answer: C

Explanation:
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any

other connections along a dedicated wire, thus the meaning of "Wire Mode".

Question: 22

On R80.10 the IPS Blade is managed by:

A. Threat Protection policy
B. Anti-Bot Blade
C. Threat Prevention policy
D. Layers on Firewall policy

Answer: C

Question: 23

Which packet info is ignored with Session Rate Acceleration?

A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used

Answer: C

Question: 24

What is the purpose of Priority Delta in VRRP?

A. When a box is up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fail, Effective Priority = Priority – Priority Delta
D. When a box fail, Effective Priority = Priority – Priority Delta

Answer: C

Explanation:
Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will beging to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP.

Question: 25

What is the purpose of a SmartEvent Correlation Unit?

A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server
B. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.
C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server

Answer: C

Question: 26

The CDT utility supports which of the following?

A. Major version upgrades to R77.30
B. Only Jumbo HFA's and hotfixes
C. Only major version upgrades to R80.10
D. All upgrades

Answer: D

Explanation:
The Central Deployment Tool (CDT) is a utility that runs on an R77 / R77.X / R80 / R80.10 Security Management Server / Multi-Domain Security Management Server (running Gaia OS).
It allows the administrator to automatically install CPUSE Offline packages (Hotfixes, Jumbo Hotfix Accumulators (Bundles), Upgrade to a Minor Version, Upgrade to a Major Version) on multiple managed Security Gateways and Cluster Members at the same time.

Question: 27

You have created a Rule Base for firewall, websydney. Now you are going to create a new policy package with security and address translation rules for a second Gateway.

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	websydney	Any	Any	websydney (Hid	Original	Original	fwsydney
2	net_singapore	net_singapore	Any	Original	Original	Original	All
3	net_singapore	Any	Any	net_singapore (H	Original	Original	All
4	Any	websydney	Any	Original	websydney	Original	Policy Targets
5	Any	websignapore	HTTP_and_HTTPS	Original	Original	http	Policy Targets

What is TRUE about the new package's NAT rules?

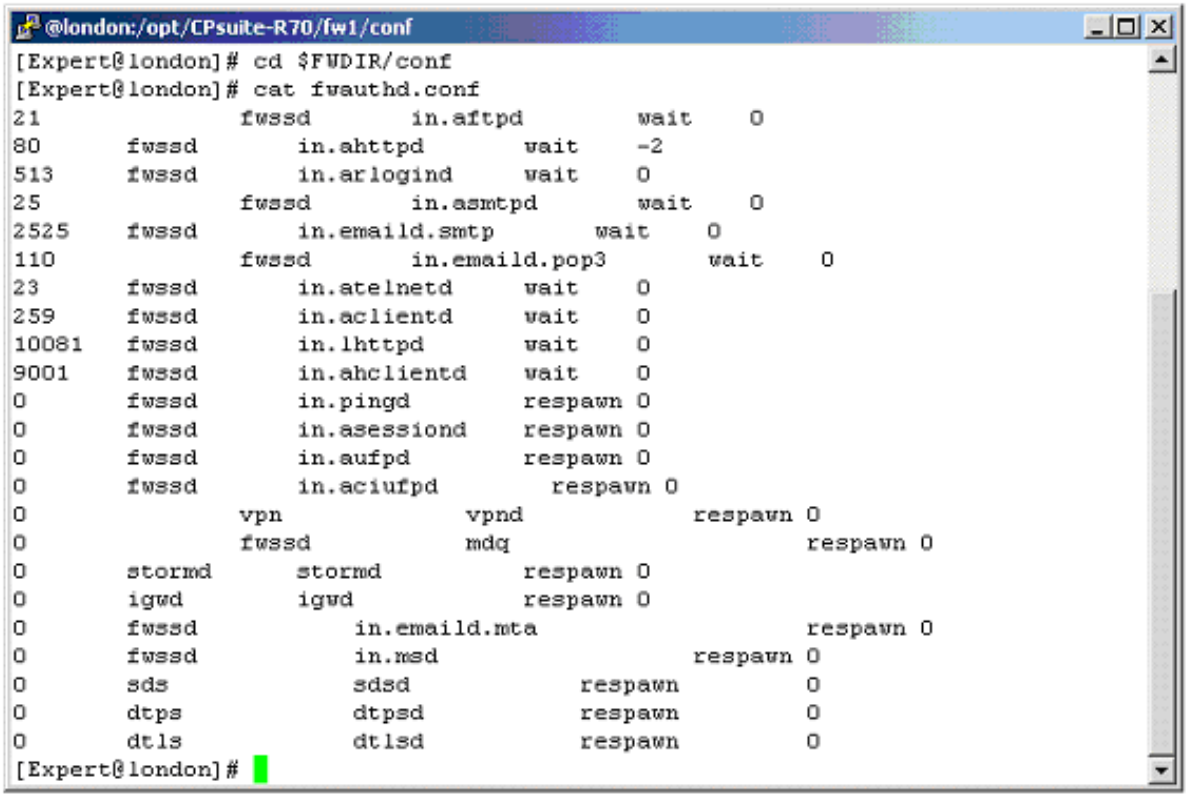
A. Rules 1, 2, 3 will appear in the new package.
B. Only rule 1 will appear in the new package.

C. NAT rules will be empty in the new package.
D. Rules 4 and 5 will appear in the new package.

Answer: A

Question: 28

Your customer, Mr. Smith needs access to other networks and should be able to use all services. Session authentication is not suitable. You select Client Authentication with HTTP. The standard authentication port for client HTTP authentication (Port 900) is already in use. You want to use Port 9001 but are having connectivity problems. Why are you having problems?



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http, ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets

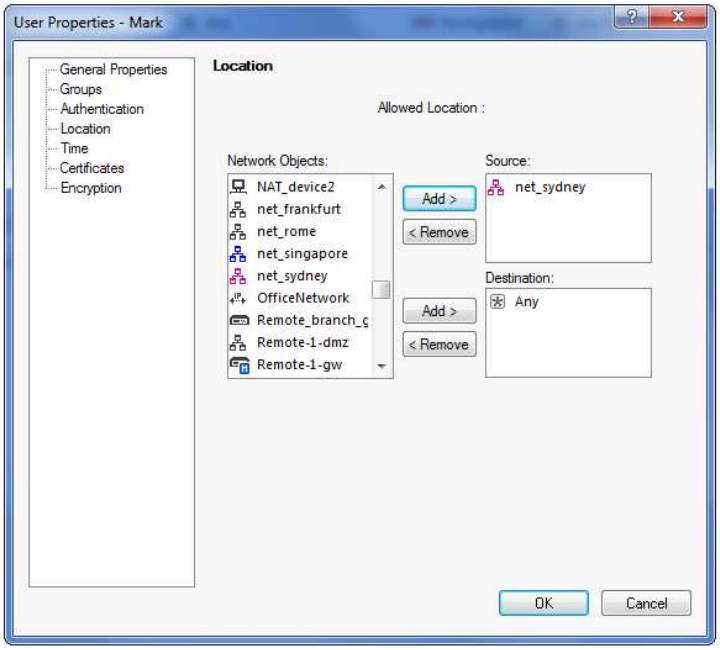
A. The configuration file $FWDIR/conf/fwauthd.conf is incorrect.
B. The Security Policy is not correct.
C. You can't use any port other than the standard port 900 for Client Authentication via HTTP.
D. The service FW_clntauth_http configuration is incorrect.

Answer: A

Question: 29

Charles requests a Website while using a computer not in the net_singapore network.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None	Policy Targets
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	Log	Policy Targets
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
4	0	Authentication	All Users@net_singapore	Any	Any Traffic	http	User Auth	Log	Policy Targets
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	Any	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	ftp	accept	Log	Policy Targets
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets



What is TRUE about his location restriction?

A. Source setting in Source column always takes precedence.
B. Source setting in User Properties always takes precedence.
C. As location restrictions add up, he would be allowed from net_singapore and net_sydney.
D. It depends on how the User Auth object is configured; whether User Properties or Source Restriction takes precedence.

Answer: D

Question: 30

In the Rule Base displayed, user authentication in Rule 4 is configured as fully automatic. Eric is a member of the LDAP group, MSD_Group.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	Log	Policy Targets
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None	Policy Targets
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log	Policy Targets
4	0	Authentication	MSAD_Group@net_singapore	Any	Any Traffic	http	User Auth	Log	Policy Targets
5	0	Partner City	net_singapore net_frankfurt	net_frankfurt net_singapore	frankfurt_singapore	Any	accept	Log	Policy Targets
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	ftp icmp-proto https http dns	accept	Log	Policy Targets
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

What happens when Eric tries to connect to a server on the Internet?

A. None of these things will happen.
B. Eric will be authenticated and get access to the requested server.
C. Eric will be blocked because LDAP is not allowed in the Rule Base.
D. Eric will be dropped by the Stealth Rule.

Answer: D

Thank You for trying 156-915.80 PDF Demo

To Buy Latest 156-915.80 Full Version Download visit link below

https://www.certkillers.net/Exam/156-915.80

Start Your 156-915.80 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further 10% discount on your purchase. Test your 156-915.80 preparation with actual exam questions.