156-215.81 Q&As

Check Point Certified Security Administrator R81

Pass CheckPoint 156-215.81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/156-215-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

A. External-user group

B. LDAP group

C. A group with a genetic user

D. All Users

Correct Answer: B

QUESTION 2

Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAiA, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

A. She needs to edit /etc/SSHd/SSHd_config and add the Standard Mode account.

B. She needs to run sysconfig and restart the SSH process.

C. She needs to edit /etc/scpusers and add the Standard Mode account.

D. She needs to run cpconfig to enable the ability to SCP files.

Correct Answer: C

QUESTION 3

To enforce the Security Policy correctly, a Security Gateway requires: A. a routing table

B. awareness of the network topology

C. a Demilitarized Zone

D. a Security Policy install

Correct Answer: B

The network topology represents the internal network (both the LAN and the DMZ) protected by the

gateway. The gateway must be aware of the layout of the network topology to:

Correctly enforce the Security Policy.

Ensure the validity of IP addresses for inbound and outbound traffic.

Configure a special domain for Virtual Private Networks.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?

topic=documents/R76/CP_R76_SecMan_WebAdmin/118037

QUESTION 4

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. Central

B. Corporate

C. Formal

D. Local

Correct Answer: D

QUESTION 5

You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After a while, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

A. Run fwm dbexport -1 filename. Restore the database. Then, run fwm dbimport -1 filename to import the users.

B. Run fwm_dbexport to export the user database. Select restore the entire database in the Database Revision screen. Then, run fwm_dbimport.

C. Restore the entire database, except the user database, and then create the new user and user group.

D. Restore the entire database, except the user database.

Correct Answer: D

QUESTION 6

How many packets does the IKE exchange use for Phase 1 Main Mode?

A. 12

B. 1

C. 3

D. 6

Correct Answer: D

QUESTION 7

What is the purpose of a Clean-up Rule?

A. Clean-up Rules do not server any purpose.

B. Provide a metric for determining unnecessary rules.

C. To drop any traffic that is not explicitly allowed.

D. Used to better optimize a policy.

Correct Answer: C

These are basic access control rules we recommend for all Rule Bases:

1.

Stealth rule that prevents direct access to the Security Gateway.

2.

Cleanup rule that drops all traffic that is not allowed by the earlier rules.

There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

QUESTION 8

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

A. INSPECT Engine

B. Next-Generation Firewall

C. Packet Filtering

D. Application Layer Firewall

Correct Answer: B

QUESTION 9

The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

A. There is a virus found. Traffic is still allowed but not accelerated

B. The connection required a Security server

C. Acceleration is not enabled

D. The traffic is originating from the gateway itself

Correct Answer: D

QUESTION 10

To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

A. Protections

B. IPS Protections

C. Profiles

D. ThreatWiki

Correct Answer: B

QUESTION 11

Look at the following screenshot and select the BEST answer.

A. Clients external to the Security Gateway can download archive files from FTP_Ext server using FTP.

B. Internal clients can upload and download any-files to FTP_Ext-server using FTP.

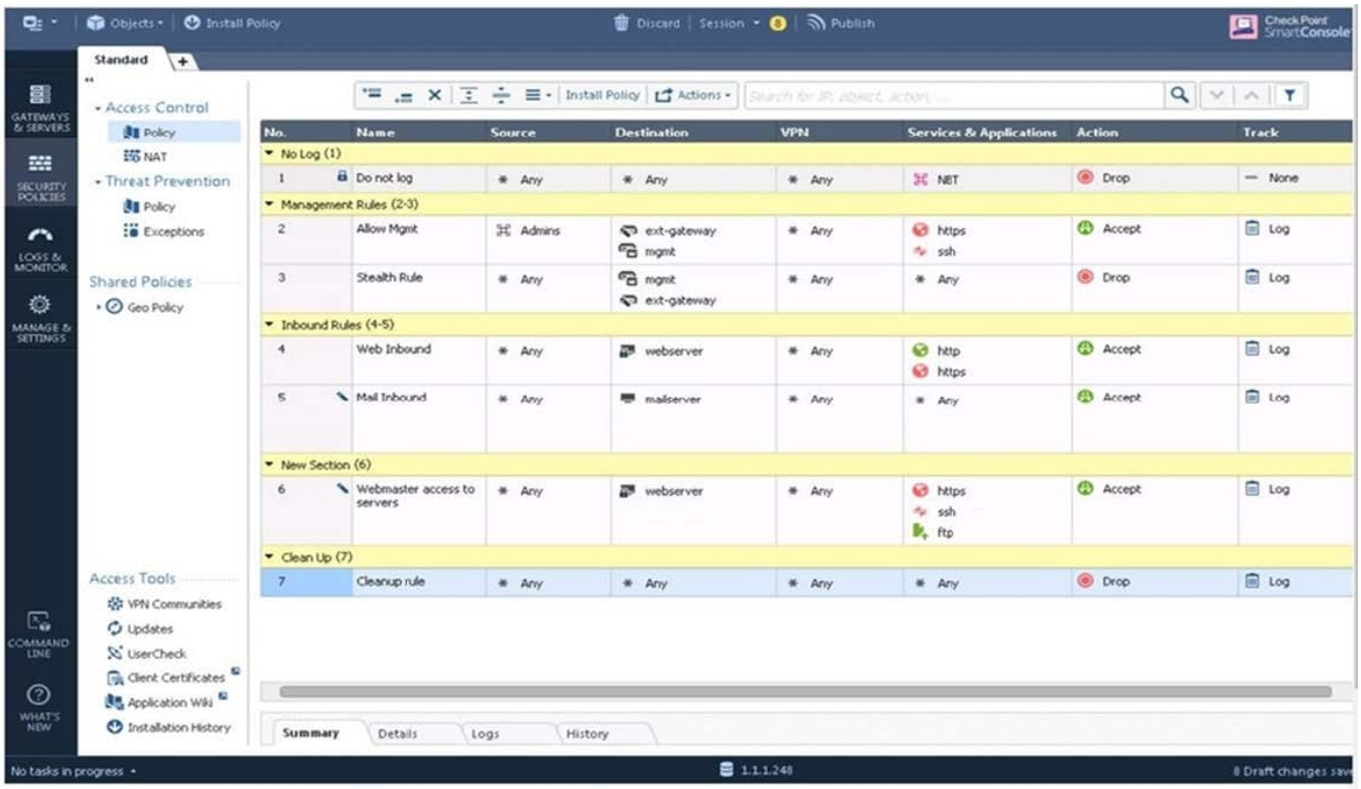
C. Internal clients can upload and download archive-files to FTP_Ext server using FTP.

D. Clients external to the Security Gateway can upload any files to the FTP_Ext-server using FTP.

Correct Answer: A

QUESTION 12

Examine the sample Rule Base.



What will be the result of a verification of the policy from SmartConsole?

A. No errors or Warnings

B. Verification Error. Empty Source-List in Rule 5 (Mail Inbound)

C. Verification Error. Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)

D. Verification Error. Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule

Correct Answer: C

QUESTION 13

In Unified SmartConsole Gateways and Servers tab you can perform the following functions EXCEPT

A. Upgrade the software version

B. Open WebUI

C. Open SSH

D. Open service request with Check Point Technical Support

Correct Answer: C

QUESTION 14

Fill in the blank: A _____ is used by a VPN gateway to send traffic as if it were a physical interface.

A. VPN Tunnel Interface

B. VPN community

C. VPN router

D. VPN interface

Correct Answer: A

Route Based VPN VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it were a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols. Reference: http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

QUESTION 15

You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

A. The POP3 rule is disabled.

B. POP3 is accepted in Global Properties.

C. The POP3 rule is hidden.

D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.

Correct Answer: C