Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT ADMINISTRATOR STUDY GUIDE FOR R80

SUMMARY

The Check Point Certified Security Administrator Course

The *Check Point Security Administrator* course provides a review and practice on a sample of the core troubleshooting and advanced configuration skills the Certified Security Administrator is expected to demonstrate.

The *Check Point Security Administrator Study Guide* supplements knowledge you have gained from the Security Administrator course, and is not a sole means of study.

CCSA OBJECTIVES

Check Point technology is designed to address network exploitation, administrative flexibility and critical accessibility. This Section introduces the basic concepts of network security and management based on Check Point's three-tier structure, and provides the foundation for technologies involved in the Check Point Architecture. These objectives and study questions provide a review of important concepts, but are not all inclusive.

Topic: Introduction to Check Point Architecture

Performance-based	Knowledge-based
• Identify the basic functions of the Web UI. • Create and confirm admin users for the network. • Configure network messages. • Confirm existing network configuration settings. • Install and tour the GUI.	• Describe the key elements of Check Point's unified, 3-tiered architecture. • Interpret the concept of a firewall and understand the mechanisms used for controlling network traffic. • Recognize SmartConsole features, functions and tools. • Understand Check Point deployment options.

Topic: Security Policy Management

Performance-based	Knowledge-based
• Create multiple administrators and apply different roles/permissions for concurrent administration. • Create and configure network, host and gateway objects. • Evaluate and manipulate rules in a unified Access Control security policy. • Apply policy layers and analyze how they affect traffic inspection. • Prepare and schedule backups for the gateway.	• Describe the essential elements of a unified security policy. • Understand how traffic inspection takes place in a unified security policy. • Summarize how administration roles and permissions assist in managing policy. • Recall how to implement Check Point backup techniques.

Topic: Check Point Security Solutions

Performance-based	Knowledge-based
• Evaluate and manage different Check Point security solutions deployed for network access control. • Evaluate and manage Check Point security solutions for threat protection. • Examine how the Compliance blade monitors your Check Point security infrastructure. • Validate existing licenses for products installed on your network.	• Recognize Check Point security solutions & products and the way they protect your network. • Understand licensing and contract requirements for Check Point security solutions.

Topic: Traffic Visibility

Performance-based	Knowledge-based
• Generate network traffic and use traffic visibility tools to monitor the data. • Compare and contrast various tools available for viewing traffic.	• Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements. • Identify tools designed to respond quickly and efficiently to changes in gateways, tunnels, remote users and traffic flow patterns or security activities.

Topic: Basic Concepts of VPN

Performance-based	Knowledge-based
• Configure and deploy a site-to-site VPN. • Test the VPN connection and analyze the tunnel traffic.	• Understand VPN deployments and Check Point Communities. • Understand how to analyze and interpret VPN tunnel traffic.

Topic: Managing User’s Access

Performance-based	Knowledge-based
• Create and define user access for a guest wireless user. • Test Identity Awareness connection.	• Recognize how to define users and user groups for your environment. • Understand how to manage user access for internal users and guests.

Topic: Working with Cluster XL

Performance-based	Knowledge-based
• Install and configure ClusterXL with a High Availability configuration.	• Describe the basic concept of ClusterXL technology and its advantages.

Topic: Administrator Task Implementation

Performance-based	Knowledge-based
• Review rule-base performance for policy control.	• Understand how to perform periodic administrator tasks as specified in Administrator job descriptions.

Topic: SmartEvent Reports

Performance-based	Knowledge-based
• Generate reports that effectively summarize network activity.	• Recognize how to effectively create, customize and generate network activity reports.

SECTION 1: INTRODUCTION TO CHECK POINT ARCHITECTURE

Objectives

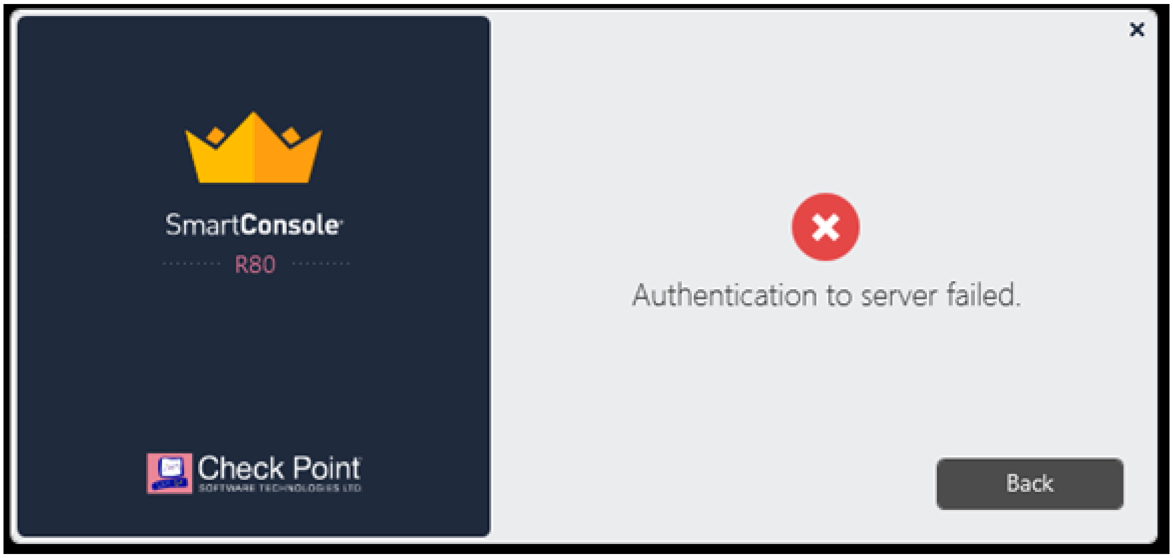
- Identify the basic functions of the Web UI.
- Create and confirm admin users for the network.
- Configure network messages.
- Confirm existing network configuration settings.
- Install and tour the GUI.
- Describe the key elements of Check Point's unified, 3-tiered architecture.
- Interpret the concept of a firewall and understand the mechanisms used for controlling network traffic.
- Recognize SmartConsole features, functions and tools.
- Understand Check Point deployment options.

Do You Know…

1. Which components can store logs on the Check Point Secure Management Architecture?
2. What SIC uses for encryption On R71 Security Gateways and above?
3. The Gaia command that turns the computer off?
4. What Check Point technologies deny or permit network traffic?
5. The advantages of Check Point Security Architectures?
6. Which type of attack can a firewall NOT prevent?
7. Which technology extracts detailed information from packets and stores that information in state tables?
8. The three authentication methods for SIC?
9. At what point the Internal Certificate Authority is created?
10. What Check Point tool is used to automatically update Check Point products for the Gaia OS?
11. Which dynamic routing protocols are supported by the Gaia operating system?
12. The Application Layer Firewalls inspect traffic through the _____ layer(s) of the TCP/IP model and up to and including the _____ layer.
13. Which SmartConsole application correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?
14. The SIC Status "Unknown" means?
15. Which SmartConsole application is used to monitor network and security performance?
16. Which object types can be manipulated in the SmartConsole?
17. What port is used for delivering logs from the gateway to the management server?
18. How many users can have read/write access in Gaia at one time?
19. Which troubleshooting steps could resolve a SIC communication issue?
20. By default, the SIC certificates issued by R80 management server are based on which algorithm
21. Which command is used to obtain the configuration lock in Gaia?
22. Which command is used to add users to or from existing roles?
23. Which CLI command would you use to obtain a configuration lock from anther administrator on a R80 Security Management Server?
24. What the correct address is to access the Gaia platform Web UI via browser to configure NTP on a R80 Security Management Server?

Application Problems

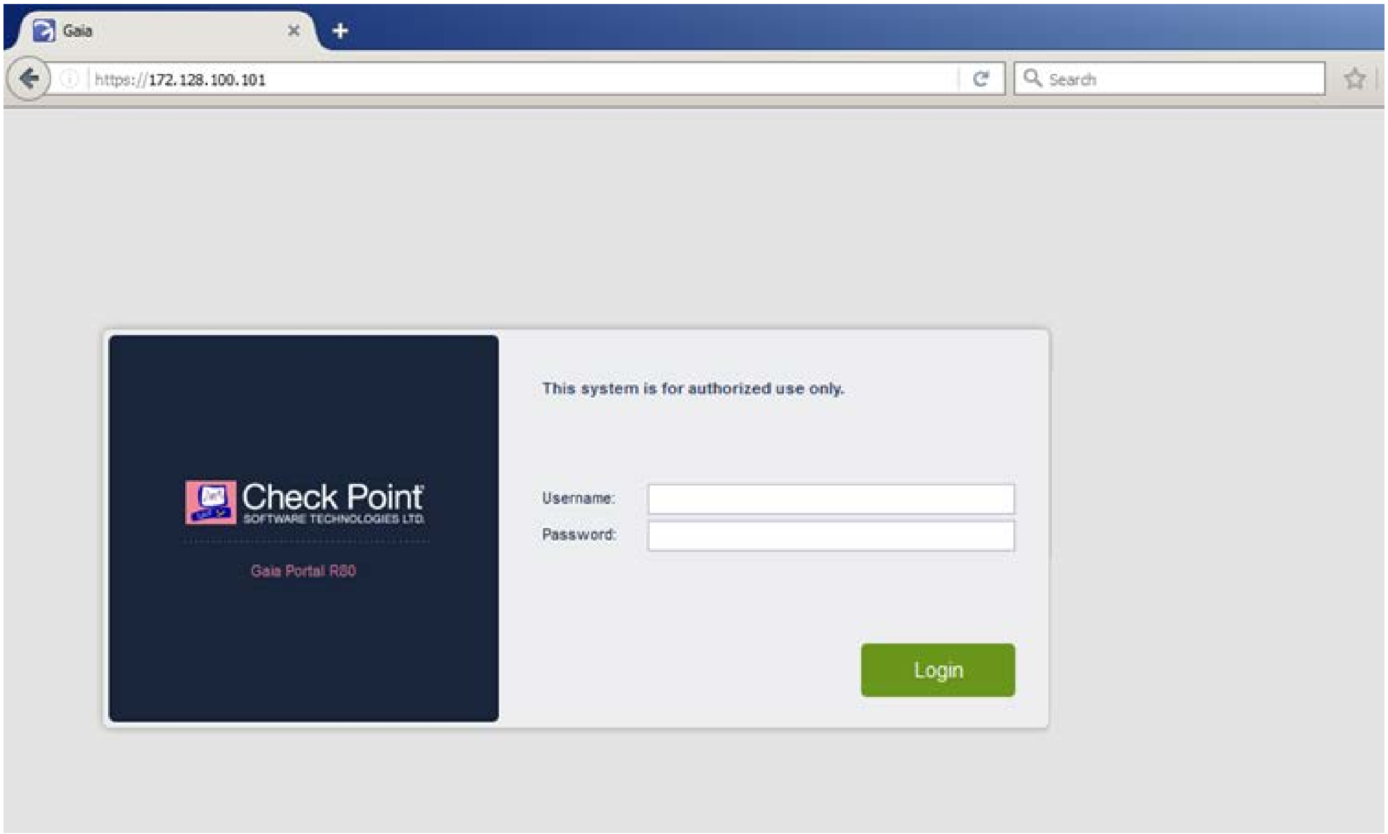
1. Let’s say you log in to the Gaia Web Portal. However, when you use the same username and password for SmartConsole you get the message:



Authentication to server failed.

If the Server IP address is correct and the username and password are correct what is happening?

2. Which CLISH commands are required to change the default Gaia WebUI Portal port number currently set on the default HTTPS port?

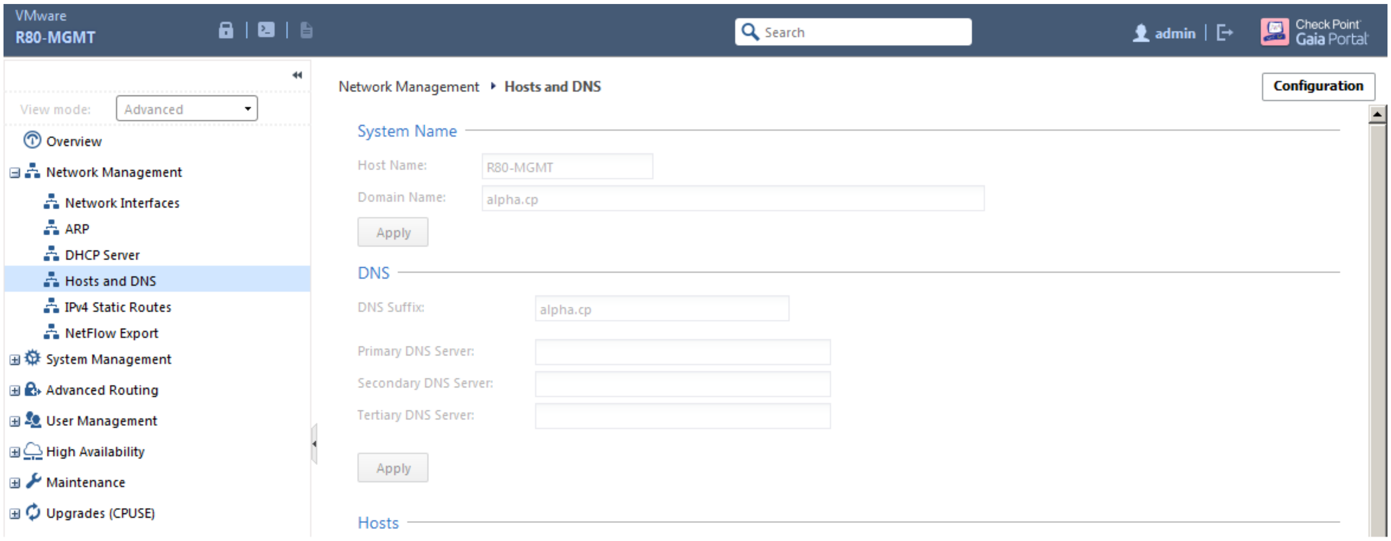


https://172.128.100.101

This system is for authorized use only.

Username:
Password:

3. What is the likely cause when a new administrator logs into the Gaia Portal to make some changes and he is unable to make any changes because all configuration options are greyed out?



System Name

Host Name: R80-MGMT

Domain Name: alpha.cp

DNS

DNS Suffix: alpha.cp

Primary DNS Server:

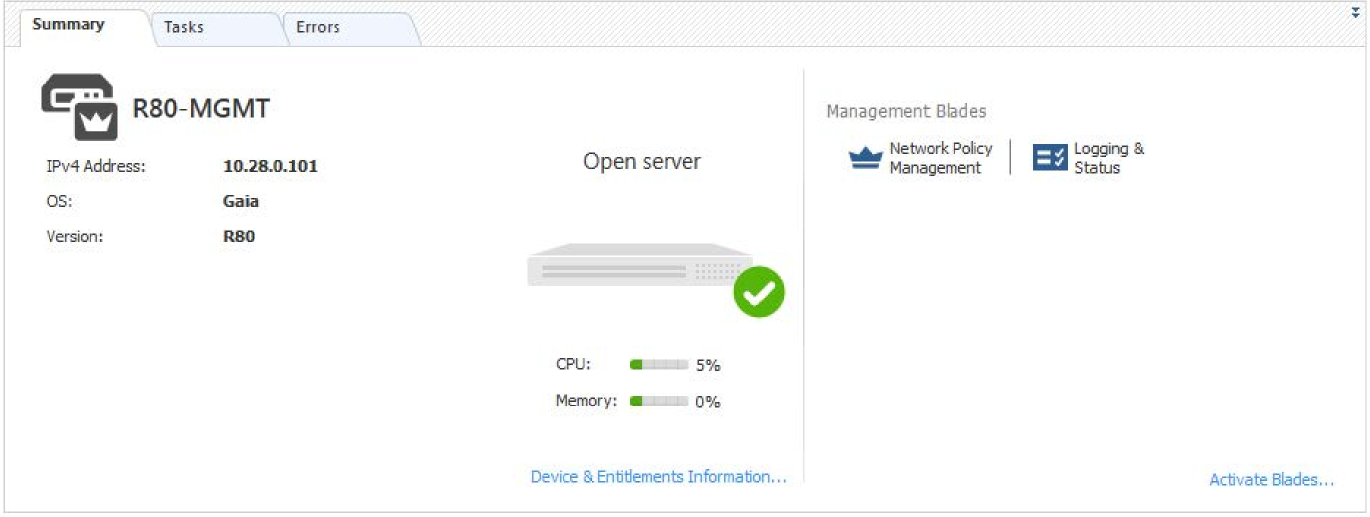
Secondary DNS Server:

Tertiary DNS Server:

Hosts

4. Which encryption is used in Secure Internal Communication between central management and firewall on each location assuming: 1) the Check Point firewalls on central and remote locations are centrally managed by an R80 Security Management Server; 2) the central location is a R77.30 Gateway on Open server; and 3) the Remote location is using Check Point UTM-1 570 series appliance with R71?

5. Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the Summary screen, the screenshot below. What is an “Open Server?”



R80-MGMT

IPv4 Address: 10.28.0.101

OS: Gaia

Version: R80

CPU: 5%

Memory: 0%

SECTION 2: SECURITY POLICY MANAGEMENT

Objectives

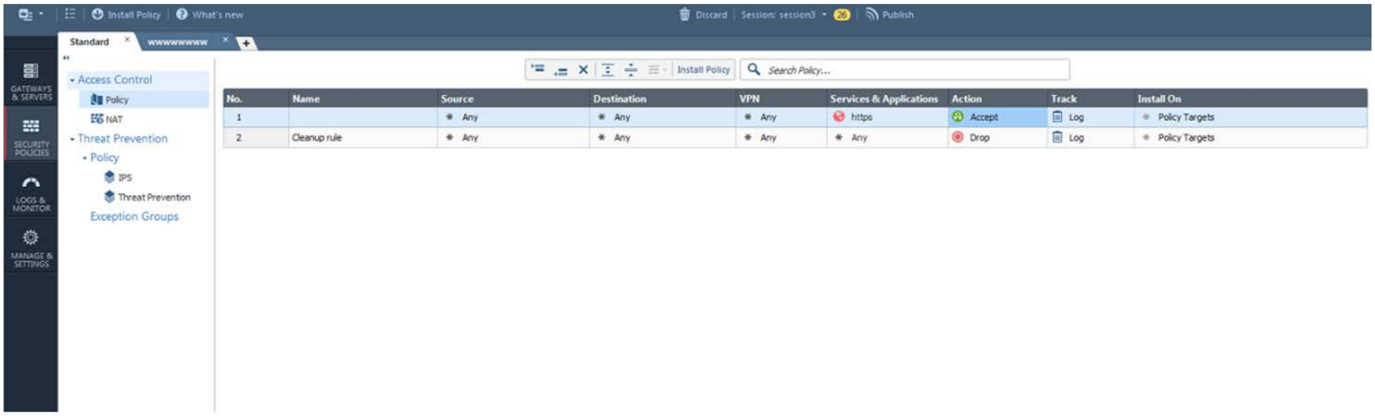
- Describe the essential elements of a unified security policy.
- Understand how traffic inspection takes place in a unified security policy.
- Summarize how administration roles and permissions assist in managing policy.
- Recall how to implement Check Point backup techniques.
- Create multiple administrators and apply different roles/permissions for concurrent administration.
- Create and configure network, host and gateway objects
- Evaluate and manipulate rules in a unified Access Control security policy.
- Apply policy layers and analyze how they affect traffic inspection.
- Prepare and schedule backups for the gateway.

Do You Know…

1. What a Security Gateway needs to correctly enforce the Security Policy?
2. The SmartConsole categories established for objects representing physical and virtual network components, and logical components?
3. How many policy layers the Access Control Policy supports?
4. The purpose of the Stealth Rule?
5. The purpose of the Cleanup Rule?
6. The Implicit Clean Rule?
7. How to determine the software version from the CLI?
8. How to create a draft of an edited policy on the Security Management Server?
9. Which policy type has its own Exceptions section?
10. Which feature allows administrators to share a policy with other policy packages?
11. What is used to enforce changes made to a Rule Base?
12. What is distributed to the target installation Security Gateways when a policy package is installed?
13. How to describe the Policy Layer Traffic Inspection?
14. Which rule is created by an administrator and located before the first and before last rules in the Rule Base.
15. What type of NAT is a one-to-one relationship where each host is translated to a unique address?
16. Which tracking actions can an administrator select to be done when spoofed packets are detected?
17. The two types of address translation rules?
18. Administrator wishes to update IPS from SmartConsole by clicking on the option “update now” under the IPS tab. Which device requires internet access for the update to work?
19. The three conflict resolution rules in the Threat Prevention Policy Layers?
20. How many sessions can be opened on the Management Server at the same time?
21. What are the three types of permission profiles?
22. How can a superuser administrator see the changes made by an administrator before publishing the session?
23. What two ordered layers make up the Access Control Policy Layer?
24. Which data saving tool captures the most information and create the largest archives?
25. Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?
26. How backups are stored in Check Point appliances?
27. Which backup method uses the command line to create an image of the OS?
28. Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?
29. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries
30. Which tool an administrator would use to view the policy installation history for each gateway?
31. What the best way is to create multiple new policies for new customers with R80 security management?

Application Problems

1. What needs to be configured if the NAT property ‘Translate destination on client side’ is not enabled in Global Properties?
2. AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a Rule Base?
3. On the following graphic you will find layers of policies.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Any	Any	Any	https	Accept	Log	Policy Targets
2	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

What is a precedence of traffic inspection for defined policies?

4. Administrator Dave, logs into R80 Management Server to review and make some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base. Insert Graphic: DNS Rule Lock What is the possible explanation for this?
5. You are the senior Firewall administrator for Alpha Corp and have returned from a training course on Check Point’s new advanced R80 management platform. You are presenting an in-house overview of the new features of Check Point R80 Management to the other admins in Alpha Corp. Insert Graphic: Publish Button How will you describe the new “Publish” button in R80 Management Console?
6. John is the administrator of a R80 Security Management server managing a R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John’s changes available to other administrators, and to save the database before installing a policy, what must John do
7. The best location of a Security Management Server backup file named backup_fw, on a Checkpoint Appliance?
8. Which backup solution you should use to ensure your database can be restored after a major upgrade?
9. If there two administrators are logged in to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators.
10. Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes. He suddenly loses connectivity but connectivity is restored shortly after. What will happen to the changes already made:
11. Network operation center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You don’t want to give her access to the expert-mode, but still she should be able to run tcpdump. How can you achieve this requirement?
12. After the initial installation on Check Point appliance you notice that the Management-interface and default gateway are incorrect. Which commands do you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1
13. Do you know what it means when you are making changes in the Rule Base and notice that rule 6 has a pencil icon next to it?

SECTION 3: CHECK POINT SECURITY SOLUTIONS

Objectives

- Recognize Check Point security solutions & products and the way they protect your network.
- Understand licensing and contract requirements for Check Point security solutions.
- Evaluate and manage different Check Point security solutions deployed for network access control.
- Evaluate and manage Check Point security solutions for threat protection.
- Examine how the Compliance blade monitors your Check Point security infrastructure.
- Validate existing licenses for products installed on your network.

Do You Know…

1. Which Threat Prevention Software Blade provides comprehensive protection against malicious and unwanted network traffic, focusing on application and server vulnerabilities?
2. Which Threat Prevention Software Blade provides protection from malicious software trying to infect your network computers?
3. Which of five Check Point Software Blade Package Solutions is NOT a part of Next Generation Data Protection (NGTP).
4. Which Check Point software blade provides application security and identity control?
5. Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?
6. Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?
7. Which Check Point software blade provides protection from zero-day and undiscovered threats?
8. Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?
9. Which software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware?
10. If, on a Distributed Environment, a Central License can be install via CLI on a Security Gateway?
11. Which blade is NOT subscription-based and therefore doesn't have to be renewed on a regular basis?
12. Which command shows the installed licenses?
13. where a package or license stored When you upload a package or license to the appropriate repository in SmartUpdate?
14. What is the best immediate action to take when You have discovered suspicious activity in your network?
15. Which licenses are considered temporary?
16. Which type of Check Point license ties the package license to the IP address of the Security Management Server?
17. 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?
18. What licensing feature is used to verify licenses and activate new licenses added to the License & Contracts repository?
19. Which repositories are installed on the Security Management Server by SmartUpdate?
20. Which command is used to verify license installation?
21. Which Automatically Generated Rules NAT rules have the lowest implementation priority?
22. What does the “unknown” SIC status shown on SmartConsole mean
23. Which GUI tool can be used to view and apply Check Point licenses?
24. When should you generate new licenses?
25. Which application should you use to install a contract file?

Application Problems

1. Which blade to enable to protect sensitive information from intentional loss when users browse to a specific URL: https://personal.mymail.com,?
2. You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point product protects best against malware and zero-day attacks while ensuring quick delivery of safe content to your users?
3. Administrator Kofi, has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets an error message. Where can the administrator check for more information on such errors?
4. Your Security Gateway CPU-level is peaking to 100%, causing problems with traffic. You suspect that the problem might be with the Threat Prevention settings. How could you tune a profile in order to lower the CPU load while still maintaining the level of security required by corporate policy?

SECTION 4: TRAFFIC VISIBILITY

Objectives

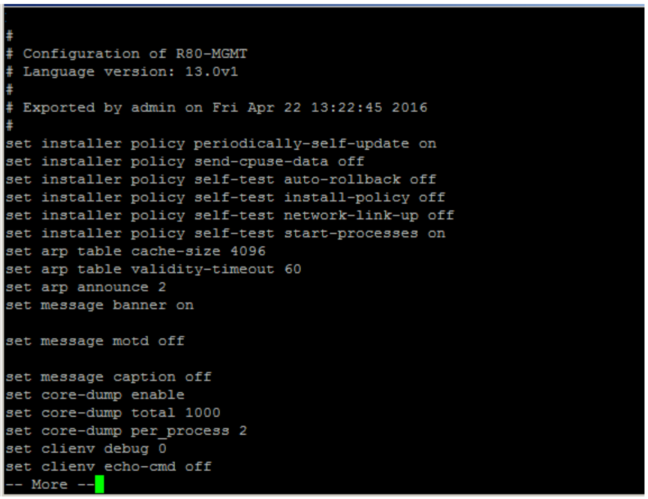
- Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements.
- Identify tools designed to respond quickly and efficiently to changes in gateways, tunnels, remote users and traffic flow patterns or security activities.
- Generate network traffic and use traffic visibility tools to monitor the data.
- Compare and contrast various tools available for viewing traffic.

Do You Know…

1. Which feature is integrated with SmartView Monitor and used to block suspicious activities?
2. Which SmartView Monitor view is used to show the status of gateway-to-gateway VPN tunnels?
3. Which information is included in Full Log tracking option, but not included in Log tracking option?
4. Which SmartView Monitor statuses indicates a host cannot access the Internet?

Application Problems

1. The “Hit count” feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits even if the Track option is set to None?
2. What CLISH command provides this output?



```
#
# Configuration of R80-MGMT
# Language version: 13.0v1
#
# Exported by admin on Fri Apr 22 13:22:45 2016
#
set installer policy periodically-self-update on
set installer policy send-cpuse-data off
set installer policy self-test auto-rollback off
set installer policy self-test install-policy off
set installer policy self-test network-link-up off
set installer policy self-test start-processes on
set arp table cache-size 4096
set arp table validity-timeout 60
set arp announce 2
set message banner on

set message motd off

set message caption off
set core-dump enable
set core-dump total 1000
set core-dump per_process 2
set clienv debug 0
set clienv echo-cmd off
-- More --
```

3. You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be.
4. You have enabled “Full 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?

SECTION 5: BASIC CONCEPTS OF VPN

Objectives

- Understand VPN deployments and Check Point Communities.
- Understand how to analyze and interpret VPN tunnel traffic.
- Configure and deploy a site-to-site VPN.
- Test the VPN connection and analyze the tunnel traffic.

Do You Know…

1. Which commands can be used to remove site-to-site IPSEC Security Associations (SA)?
2. Which utility shows the security gateway general system information statistics like operating system information and resource usage, and individual software blade statistics of VPN, Identity awareness and DLP?
3. The most important part of a site-to-site VPN deployment?
4. What VPN gateways use to authenticate?
5. Which is the most secure means of authentication?
6. What is used by a VPN gateway to send traffic as if it were a physical interface?
7. Which VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.
8. In which VPN community a satellite VPN gateway is not allowed to create a VPN tunnel with another satellite VPN gateway?
9. Which VPN routing option uses VPN routing for every connection a satellite gateway handles?
10. Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?
11. Which message indicates IKE Phase 2 has completed successfully?
12. Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?
13. Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

Application Problems

1. An administrator is creating an IPSec site to site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret is shaded and cannot be enabled. Why does it not allow to specify the pre-shared secret.
2. When attempting to start a VPN tunnel, in the logs the error “no proposal chosen” is seen numerous times. No other VPN-related log entries are present. Which phase of the VPN negotiations has failed?

SECTION 6: MANAGING USER'S ACCESS

Objectives

- Recognize how to define users and user groups for your environment.
- Understand how to manage user access for internal users and guests.
- Create and define user access for a guest wireless user.
- Test Identity Awareness connection.

Do You Know…

1. The BEST object type to represent an LDAP group in a Security Policy when defining group-based access in an LDAP environment with Identity Awareness?
2. What is used to obtain identification and security information about network users?
3. The identity acquisition methods that allow a Security Gateway to identify Active Directory users and computers?
4. What an endpoint identity agent uses for user authentication?
5. Which authentication scheme requires a user to possess a token?
6. The purpose of Captive Portal?
7. The ports to which the Client Authentication daemon listens on by default?
8. Which Identity Source should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?
9. When Identity Awareness is enabled, which identity source is used for Application Control?
10. Which two Identity Awareness commands are used to support identity sharing?
11. What is Identity Sharing?
12. Where does RADIUS Accounting acquire data from requests generated by the accounting client?
13. How does a RADIUS protocol communicate with the gateway?
14. Which type of Endpoint Identity Agent includes packet tagging and computer authentication?
15. When configuring LDAP User Directory integration, what happens to changes applied to a User Directory template?
16. The authentication method used for Identity Awareness?
17. Which Windows Security Event will NOT map a username to an IP address in Identity Awareness?
18. The BEST method to deploy identity awareness for roaming users?

Application Problems

1. How can you fix this? You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet.
2. The best method for an administrator to enable Identity Awareness on MegaCorp's Check Point firewalls? Currently they allow users to use company issued laptops and their personal laptops. Which of suit this company
3. Why does the Identity Awareness wizard not automatically detect the windows domain while enabling the Identity Awareness blade?

SECTION 7: WORKING WITH CLUSTERXL

Objectives

- Describe the basic concept of ClusterXL technology and its advantages.
- Install and configure ClusterXL with a High Availability configuration.

Do You Know…

1. Which of of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?
2. When Check Point ClusterXL Active/Active deployment is used?
3. What protocol is used for clustered environments?
4. The two high availability modes?
5. Which of the following commands is used to monitor cluster members?
6. Which tool is used to enable ClusterXL?
7. Where can you trigger a failover of the cluster members?

Application Problems

1. Whether FW_A will become active automatically when it re-joins the cluster under the following conditions? There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High avalabiltiy) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic today morning. FW_B was standby. Around 1100 am, FW_A's interfaces went down and this caused a failover. FW_B became active. After an hour FW_A's interface issues were resolved and it became operational.

SECTION 8: ADMINISTRATOR TASK IMPLEMENTATION

Objectives

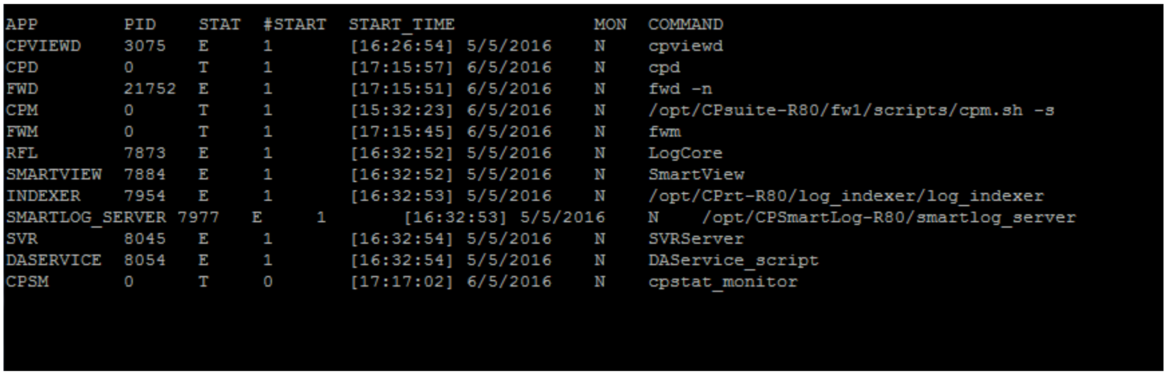
1. Understand how to perform periodic administrator tasks as specified in Administrator job descriptions.
2. Review rule-base performance for policy control.

Do You Know…

1. What happens when Bob and Joe are both logged in on a Gaia Platform? Bob and Joe both have Admin Role. Bob logs in on the WEBui and then Joe logs in through CLI.
2. Which utility allows you to configure the DHCP service on GAIA from the command line?
3. The effect of running the fw unloadlocal on the Management Server?
4. The default time length that Hit Count Data is kept?
5. What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?
6. Where to place the most hit rules to optimize Rule Base efficiency?

Application Problems

1. The reason why you are unable to connect to SmartDashboard? You log into the management server and run #cpwd_admin list with the following output.



```
APP         PID    STAT  #START  START_TIME             MON  COMMAND
CPVIEWD     3075   E     1       [16:26:54] 5/5/2016    N    cpviewd
CPD         0      T     1       [17:15:57] 6/5/2016    N    cpd
FWD         21752  E     1       [17:15:51] 6/5/2016    N    fwd -n
CPM         0      T     1       [15:32:23] 6/5/2016    N    /opt/CPsuite-R80/fw1/scripts/cpm.sh -s
FWM         0      T     1       [17:15:45] 6/5/2016    N    fwm
RFL         7873   E     1       [16:32:52] 5/5/2016    N    LogCore
SMARTVIEW   7884   E     1       [16:32:52] 5/5/2016    N    SmartView
INDEXER     7954   E     1       [16:32:53] 5/5/2016    N    /opt/CPrt-R80/log_indexer/log_indexer
SMARTLOG_SERVER 7977   E     1       [16:32:53] 5/5/2016    N    /opt/CPSmartLog-R80/smartlog_server
SVR         8045   E     1       [16:32:54] 5/5/2016    N    SVRServer
DASERVICE   8054   E     1       [16:32:54] 5/5/2016    N    DAService_script
CPSM        0      T     0       [17:17:02] 6/5/2016    N    cpstat_monitor
```

CONCLUSION

You knew all that?

Does your Pearson VUE profile email address match your User Center profile email address?

Then you are ready. Go to Pearson VUE and request exam 156-215.80.

Good testing!

Restricted Rights Legend:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

Trademarks:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http:// www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

International Headquarters:	5 Ha'Solelim Street Tel Aviv 67897, Israel Tel: +972-3-753 4555
U.S. Headquarters:	959 Skyway Road, Suite 300 San Carlos, CA 94070 Tel: 650-628-2000 Fax: 650-654-4233
Technical Support, Education and Professional Services:	6330 Commerce Drive, Suite 120 Irving, TX 75063 Tel: 972-444-6612 Fax: 972-506-7913 E-mail any comments or questions about our courseware to courseware@checkpoint.com. E-mail any comments or questions about our certifications to certification@checkpoint.com. For questions or comments about other Check Point documentation, e-mail CP_TechPub_Feedback@checkpoint.com.
Document #:	CPTS-DOC-CCSA-SG-R77