Check Point Certified Security Expert Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. The default port for the Web User interface on a Security Gateway installed on GAIA R80 is?

A. TCP 18211

B. TCP 257

C. TCP 4433

D. TCP 443

2. How many images are included with Check Point TE appliance in Recommended Mode?

A. 2 (OS) images

B. Images are chosen by the administrator during installation

C. As many as licensed for

D. The most new image

3. Which is NOT a component of Check Point SandBlast?

A. Threat Emulation

B. Threat Simulator

C. Threat Extraction

D. Threat Cloud

4. Which command is used to view cluster interface status?

A. cphaprob status

B. cphaprob interfaces

C. cphaprob show

D. cphaprob cluster

5. In which file is the proxy ARP configuration stored?

A. $FWDIR/state/proxy_arp.conf on the management server

B. $FWDIR/conf/local.arp on the management server

C. $FWDIR/state/_tmp/proxy.arp on the security gateway

D. $FWDIR/conf/local.arp on the gateway

6. What action does the firewall take for packets that are matched but not explicitly allowed by a rule?

A. Drop them and log the event

B. Drop them silently

C. Allow them through

D. Return the packets to sender

7. Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs

B. Capsule Cloud

C. Capsule Enterprise

D. Capsule Workspace

8. As an Administrator, to add a logo to reports, where should you copy the image on the SmartEvent Server?

A. $FWDIR/smartevent/conf

B. $RTDIR/smartevent/conf

C. $RTDIR/smartview/conf

D. $FWDIR/smartview/conf

9. Which command is used to check the status of the Check Point kernel?

A. fw status

B. cpsamp status

C. cpwd_admin list

D. fw ctl pstat

10. What is the primary function of the Threat Emulation service in Check Point?

A. Prevent intrusion attempts.

B. Emulate and analyze files in a secure environment to detect malware.

C. Monitor network traffic for anomalies.

D. Control access to sensitive data.

Answers

1. D
2. A
3. B
4. A
5. D
6. A
7. C
8. C
9. C
10. B

Explanations

1. The default port for the Web User interface on a Security Gateway installed on GAIA R80 is?

A. TCP 18211

B. TCP 257

C. TCP 4433

D. TCP 443

The default port for the Web User Interface (WebUI) on a Security Gateway installed on GAIA R80 is TCP 443. This port is commonly used for HTTPS traffic, which provides a secure channel over the network. Since web interfaces require a secure connection to protect sensitive configurations and data from being intercepted, TCP 443, which is dedicated to HTTPS, is the logical default choice. In the context of network security and management tools, utilizing TCP 443 ensures that communications between administrators and the Security Gateway are encrypted, enhancing the overall security posture of the environment. By default, most systems that provide web-based management functionalities tend to target this port because of its widespread use and compatibility with standard security practices across various platforms. In contrast, the other options represent non-standard ports for this function within the context of GAIA R80. While there may be other services running on those ports, they are not used for the Web User Interface by default, which reinforces the significance of recognizing TCP 443 as the standard port for this purpose.

2. How many images are included with Check Point TE appliance in Recommended Mode?

A. 2 (OS) images

B. Images are chosen by the administrator during installation

C. As many as licensed for

D. The most new image

In Recommended Mode, Check Point TE (Threat Emulation) appliances typically include two operating system images. This setup is designed to enhance redundancy and provide failover capabilities. By having two OS images, the appliance can ensure high availability and allow for one image to be in use while the other can be updated or configured without downtime. This approach allows administrators to maintain a stable and reliable environment, facilitating seamless updates and reducing the risk of service interruptions. In contexts where continuous security monitoring and threat emulation are crucial, having multiple OS images serves to bolster system resilience. The other possibilities do not accurately reflect the standard configuration; while images might be chosen during a personalized installation process, the default in Recommended Mode specifically includes two images. Therefore, the answer aligns with established practices for ensuring redundancy and reliability in security appliances.

3. Which is NOT a component of Check Point SandBlast?

A. Threat Emulation

B. Threat Simulator

C. Threat Extraction

D. Threat Cloud

The correct response identifies that the "Threat Simulator" is not a component of Check Point SandBlast. Check Point SandBlast is designed to protect networks from advanced threats and comprises several key components that focus on proactive threat defense. Threat Emulation is a critical feature that allows the system to analyze files in a secure environment before they reach the endpoint, identifying potential threats through sandboxing techniques. This means that suspicious files are executed in a controlled virtual environment to understand their behavior and determine if they are malicious. Threat Extraction is another significant feature where potentially harmful content is removed from files to clean them before they are delivered to the end-users. This process focuses on ensuring that any detected threats are eliminated and that the files remain functional for the users. Threat Cloud is a part of Check Point's broader security ecosystem that utilizes cloud-based intelligence to provide real-time insights and updates about emerging threats, enhancing the overall effectiveness of SandBlast. In contrast, "Threat Simulator" does not exist as a standalone component within the SandBlast suite, making it the correct choice for the question.

4. Which command is used to view cluster interface status?

A. cphaprob status

B. cphaprob interfaces

C. cphaprob show

D. cphaprob cluster

The command used to view cluster interface status is "cphaprob interfaces." This command provides detailed information specific to the status of the interfaces in a cluster setup within Check Point's security architecture. While "cphaprob status" is useful in providing an overall status of the cluster, including its health and synchronization status, it does not specifically focus on the interfaces themselves. The other options, while related to cluster operations, do not directly give the interface status like "cphaprob interfaces" does. Therefore, this command is the precise tool for checking the condition and functionality of the individual interfaces within the cluster environment, ensuring that network connectivity and redundancy are maintained as expected. Understanding this command's output can be critical for maintaining a resilient network infrastructure, allowing for quick diagnostics and validation of the cluster's operational integrity.

5. In which file is the proxy ARP configuration stored?

A. $FWDIR/state/proxy_arp.conf on the management server

B. $FWDIR/conf/local.arp on the management server

C. $FWDIR/state/_tmp/proxy.arp on the security gateway

D. $FWDIR/conf/local.arp on the gateway

The configuration for proxy ARP is primarily stored in the local.arp file located in the configuration directory of the security gateway. This file plays a critical role in defining how the gateway responds to ARP requests for IP addresses that are not directly assigned to local interfaces. By managing this configuration in local.arp, administrators can effectively control how the security gateway interacts with ARP requests, allowing for proper network communications in scenarios where proxy ARP is necessary. The local.arp file ensures that the rules for proxy ARP can be customized per gateway, which is essential for maintaining network integrity and security. This file contains mappings that the gateway uses to forward requests to correct interfaces, a vital function in environments where IP addresses are shared or stretched across multiple networks. Understanding the significance of the local.arp file highlights the importance of proper ARP configuration in network security practices, as it directly influences the effectiveness of the security gateway in managing traffic and maintaining communication with devices across network boundaries.

6. What action does the firewall take for packets that are matched but not explicitly allowed by a rule?

A. Drop them and log the event

B. Drop them silently

C. Allow them through

D. Return the packets to sender

When a packet matches a rule in the firewall but is not explicitly allowed, the firewall typically takes the action to drop the packet while also logging the event. This behavior is designed to enhance security by ensuring that only recognized and permitted traffic can pass through the firewall. By logging this dropped traffic, administrators are provided with valuable insights into potential security threats or misconfigurations that may need to be addressed. Logging the event serves as a critical function because it notifies the network administrators about suspicious activities or unauthorized access attempts that could compromise the security posture of the network. This allows for proactive monitoring and response to potential security issues in real-time. The other options do not align with standard firewall behaviors. Silently dropping packets would mean there is no log for the event, making it difficult for administrators to be aware of potentially malicious activity. Allowing the packets through contradicts the principle of restrictive security, where only explicitly permitted traffic is allowed. Returning packets to the sender is not a common firewall behavior, as it could reveal information about the network's structure and potentially open avenues for attacks.

7. Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs

B. Capsule Cloud

C. Capsule Enterprise

D. Capsule Workspace

The correct answer is Capsule Enterprise because it is not a recognized component of Check Point Capsule. Check Point Capsule is a suite of security solutions designed to protect sensitive information on mobile devices and endpoints. The components that are part of Capsule include Capsule Docs, which enables secure document collaboration and sharing; Capsule Cloud, which provides cloud-based security features; and Capsule Workspace, which offers a secure environment for accessing corporate applications and data. Capsule Enterprise does not exist within the Check Point Capsule offerings, indicating that this answer is correct. Understanding the proper components of Check Point Capsule helps clarify the functionalities related to data protection and secure access, which are vital for organizations in maintaining data integrity and security across devices.

8. As an Administrator, to add a logo to reports, where should you copy the image on the SmartEvent Server?

A. $FWDIR/smartevent/conf

B. $RTDIR/smartevent/conf

C. $RTDIR/smartview/conf

D. $FWDIR/smartview/conf

To add a logo to reports generated by SmartEvent, the correct location is in the directory that specifically handles SmartView configurations. The $RTDIR/smartview/conf directory is designated for settings and configurations relevant to SmartView utilities, including report customization features such as adding logos. This ensures that the logo you include will be properly recognized and utilized during the report generation process in SmartEvent. Choosing the right directory is essential because placing the image in other directories, such as those associated with SmartEvent's core functionality or other components, would not affect the SmartView reporting tools. Configurations are organized by functionality, so understanding the purpose of each directory is vital for effective management and customization within the Check Point environment.

9. Which command is used to check the status of the Check Point kernel?

A. fw status

B. cpsamp status

C. cpwd_admin list

D. fw ctl pstat

The command that is used to check the status of the Check Point kernel is "cpwd_admin list." This command provides detailed information regarding the status of the various Check Point processes running on the device, which includes kernel processes that are crucial for system functionality. It shows whether these processes are alive, their uptime, and other operational details, allowing administrators to monitor the health and performance of the Check Point environment. The other commands serve different purposes. "fw status" is typically used to check the status of the firewall and its configuration but does not specifically focus on the kernel's operational state. The "cpsamp status" command is related to the sampling process in the Check Point system, and while it provides useful information about network performance, it is not meant for kernel status. The "fw ctl pstat" command provides statistics related to the state of the Check Point firewall, including connections and memory usage, but again, it does not focus specifically on the kernel status itself. Thus, "cpwd_admin list" is the most relevant command for checking the status of the Check Point kernel.

10. What is the primary function of the Threat Emulation service in Check Point?

A. Prevent intrusion attempts.

B. Emulate and analyze files in a secure environment to detect malware.

C. Monitor network traffic for anomalies.

D. Control access to sensitive data.

The primary function of the Threat Emulation service in Check Point is to emulate and analyze files in a secure environment to detect malware. This process involves executing files in a controlled, virtual environment to observe their behavior without risking the integrity of the organization's systems. By doing this, the service can identify sophisticated threats that traditional security measures might miss, such as zero-day exploits and advanced persistent threats (APTs). In the context of modern cybersecurity, where threats are constantly evolving, identifying and neutralizing malware before it can execute and cause damage is crucial. The capability to safely analyze unknown files allows organizations to proactively defend against potential attacks by isolating and understanding the nature of suspicious files. While the other options pertain to overall security functions, they do not specifically capture the unique offering of Threat Emulation. For instance, preventing intrusion attempts focuses on blocking unauthorized access, monitoring network traffic aims at identifying irregular patterns, and controlling access to sensitive data is concerned with information security and rights management. Each of these functions is important in a comprehensive cybersecurity strategy, but they do not specifically address the need to analyze potentially malicious files through emulation.