Up-to-date Questions and
Answers from authentic
resources to improve
knowledge and pass the
exam at very first attempt.
----- Guaranteed.

KILL EXAMS

PASS

killexams.com

CheckPoint

156-585

CheckPoint Certified Troubleshooting Expert

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/156-585

Question: 714

A network administrator is troubleshooting a VPN connection issue and notices that the VPN tunnel is "Down" on the local gateway. The administrator checks the ike.elg file and sees the following error message: "INVALID-COOKIE". What is the most likely cause of this issue?

A. The encryption algorithm configured on the local gateway does not match the encryption algorithm configured on the peer gateway.
B. The authentication method configured on the local gateway does not match the authentication method configured on the peer gateway.
C. The DH group configured on the local gateway does not match the DH group configured on the peer gateway.
D. The pre-shared key configured on the local gateway does not match the pre-shared key configured on the peer gateway.

Answer: B

Explanation:
The "INVALID-COOKIE" error message indicates an issue with the authentication method configured on the local and peer gateways. The most likely cause of this issue is that the authentication method configured on the local gateway does not match the authentication method configured on the peer gateway. This mismatch in the authentication method during the IKE Phase 1 negotiation leads to the VPN tunnel being "Down" because the authentication cookies are invalid.

Question: 715

You need to configure a new security policy rule on a CheckPoint gateway. Which command should you use?

A. fw policy add
B. cpconfig policy add

C. fw ctl rule add
D. cpconfig security add

Answer: C

Explanation: The fw ctl rule add command is used to configure a new security policy rule on a CheckPoint gateway. This command allows you to specify the source, destination, service, and other parameters for the new rule.

Question: 716

Which command is used to view the current state of the firewall's user authentication and authorization mechanisms?

A. fw tab -t auth
B. fw monitor -u
C. fw print -u
D. fw ctl auth -l

Answer: D

Explanation: The fw ctl auth -l command is used to view the current state of the firewall's user authentication and authorization mechanisms, including information about the active user sessions and their associated permissions.

Question: 717

You need to configure a new DHCP server on a CheckPoint gateway. Which command should you use?

A. fw ctl dhcp add
B. cpconfig dhcp create

C. fw dhcp add
D. cpconfig network dhcp

Answer: A

Explanation: The fw ctl dhcp add command is used to configure a new DHCP server on a CheckPoint gateway. This command allows you to specify the DHCP pool, lease duration, and other relevant settings.

Question: 718

What is the purpose of the "Dynamic Routing" feature in Check Point's Security Gateway?

A. To automatically adjust routing tables based on network changes
B. To enable load balancing and failover for traffic traversing the gateway
C. To provide support for advanced routing protocols like OSPF and BGP
D. All of the above

Answer: D

Explanation: The "Dynamic Routing" feature in Check Point's Security Gateway serves to automatically adjust routing tables based on network changes, enable load balancing and failover for traffic traversing the gateway, and provide support for advanced routing protocols like OSPF and BGP.

Question: 719
While troubleshooting a VPN connectivity issue, you notice that the Phase 1 negotiations are failing. Which of the following commands would you use to view the IKE (Internet Key Exchange) logs?

A. cpview ike
B. cpview vpnd

C. cpview vpn
D. cpview phase1

Answer: B

Explanation: The cpview vpnd command is used to view the VPN daemon logs, which include the IKE (Internet Key Exchange) logs. This is the appropriate command to use when troubleshooting VPN connectivity issues, specifically during the Phase 1 negotiation process.

Question: 720

What is the purpose of the "fw ctl syslog" command?

A. To view and manage the system log files on the firewall.
B. To display the current system information for the firewall.
C. To clear the firewall system logs.
D. To update the firewall system software to the latest version.

Answer: A

Explanation: The "fw ctl syslog" command is used to view and manage the system log files on a Check Point security gateway. This includes the ability to view, filter, and manipulate the various log files generated by the firewall and other system components.

Question: 721

What is the purpose of the "cprid" process in CheckPoint?

A. To provide remote access to the management server
B. To manage the firewall acceleration settings
C. To perform intrusion detection and prevention

D. To provide content inspection capabilities

Answer: A

Explanation: The "cprid" process is the CheckPoint Remote Access Daemon, which provides remote access to the management server.

Question: 722

Which command can be used to view the Check Point software version information?

A. cplic
B. cpstat
C. cpview
D. cpver

Answer: D

Explanation: The 'cpver' command can be used to view the Check Point software version information, including the version numbers of the various components and modules installed on the system.

Question: 723

What is the purpose of the "fw ctl monitor" command?

A. To monitor the real-time status of the firewall.
B. To display the current user sessions on the firewall.
C. To clear the firewall event logs.
D. To update the firewall software to the latest version.

Answer: A

Explanation: The "fw ctl monitor" command is used to monitor the real-time status of the firewall on a Check Point security gateway. This includes information about the firewall's performance, resource utilization, and any active connections or events.

Question: 724

What is the purpose of the 'cphactl' command in Check Point?

A. To configure the overall Check Point system settings
B. To manage Check Point user accounts
C. To view and analyze Check Point system logs and statistics
D. To perform high-availability and clustering operations

Answer: D

Explanation: The 'cphactl' command is used to perform high-availability and clustering operations in Check Point, such as starting, stopping, and managing cluster members, as well as initiating failover and switchover processes.

Question: 725

What is the role of the Content Matching Interface (CMI) in the Content Awareness module?

A. To manage the content filtering policies and configurations
B. To intercept the network traffic and apply the content filtering rules
C. To provide an interface for other security components to interact with the content filtering capabilities
D. To collect data from the contexts and decide if the file is matched by a data type

Answer: C

Explanation: The Content Matching Interface (CMI) in the Content Awareness module provides an interface for other security components to interact with the content filtering capabilities. It allows these components to leverage the content matching and data type detection features of the Content Awareness module.

Question: 726

What is the purpose of the FWKERN process in a CheckPoint deployment?

A. To handle user authentication and authorization
B. To manage the firewall and VPN connections
C. To provide a web-based management interface
D. To implement the core firewall and VPN functionality

Answer: D

Explanation: The FWKERN process is responsible for implementing the core firewall and VPN functionality in a CheckPoint deployment. It handles the processing and enforcement of firewall rules, VPN tunnels, and other security-related operations.

Question: 727

You are troubleshooting an issue where a user is unable to access a specific internal resource. Which of the following commands would you use to check the firewall rule logs for the specific resource?

A. cpview rule
B. cpview connections
C. cpstat -r
D. cpinfo -f

Answer: A

Explanation: The cpview rule command is used to view the logs related to the firewall rules on a Check Point Security Gateway, including the logs for specific resources. This command provides access to the relevant logs that can be analyzed to troubleshoot issues with firewall rule configuration or behavior.

Question: 728

A Checkpoint security administrator needs to investigate a potential security breach on a security gateway. Which of the following tools or commands should be used to collect the most comprehensive set of forensic data from the system?

A. fw ctl zdebug all
B. CPINFO
C. fw ctl monitor -c
D. fw ctl fwm_dump

Answer: B

Explanation: The CPINFO tool is the most comprehensive option for collecting forensic data from a Checkpoint security gateway. CPINFO gathers a wide range of system information, including log files, configuration data, and system state, which can be crucial for investigating a potential security breach. The other options, while useful for specific troubleshooting tasks, do not provide the same level of comprehensive data collection for forensic purposes.

Question: 729

Which command is used to view the firewall's NAT table?

A. "fw tab -t nat"

B. "fw tab -t connections"
C. "fw tab -t accels"
D. "fw tab -t interfaces"

Answer: A

Explanation: The "fw tab -t nat" command is used to view the firewall's NAT table, which contains information about the network address translations performed by the firewall.

Question: 730

A network administrator is troubleshooting a VPN connection issue and notices that the VPN tunnel is "Down" on the local gateway. The administrator checks the ike.elg file and sees the following error message: "INVALID-TRANSFORM-ATTRIBUTE". What is the most likely cause of this issue?

A. The encryption algorithm configured on the local gateway does not match the encryption algorithm configured on the peer gateway.
B. The authentication method configured on the local gateway does not match the authentication method configured on the peer gateway.
C. The DH group configured on the local gateway does not match the DH group configured on the peer gateway.
D. The transform attribute in the IKE proposal is not supported by the peer gateway.

Answer: D

Explanation:
The "INVALID-TRANSFORM-ATTRIBUTE" error message indicates an issue with the transform attribute in the IKE proposal. The most likely cause of this issue is that the transform attribute in the IKE proposal is not supported by the peer gateway. This mismatch in the supported transform attributes during

the IKE negotiation leads to the VPN tunnel being "Down" because the gateways cannot agree on a compatible transform attribute.

Question: 731

A Checkpoint security administrator needs to troubleshoot an issue where the firewall is experiencing high network utilization. Which of the following commands should be used to get the most detailed information about the network traffic on the system?

A. fw ctl zdebug network
B. fw ctl monitor -c net
C. fw ctl fwm_dump
D. CPINFO

Answer: B

Explanation: The 'fw ctl monitor -c net' command provides the most detailed information about the network traffic on a Checkpoint security gateway. This command allows the administrator to monitor real-time network utilization metrics, including bandwidth consumption, packet rates, and connection counts, which can be crucial for troubleshooting high network utilization issues. The other options, while potentially useful for other troubleshooting tasks, are not as focused on collecting network-specific data.

Question: 732

A customer reports that their Check Point gateway is experiencing issues with URL filtering functionality. Which of the following commands would be the most effective for troubleshooting this problem?

A. fw ctl zdebug urlf
B. fw monitor

C. fw tab -t connections
D. cpinfo

Answer: A

Explanation: The fw ctl zdebug urlf command provides detailed information about the URL filtering-related activities and connections on the Check Point gateway, which is exactly what you need to troubleshoot URL filtering functionality issues. This command can help you identify any errors, problems, or anomalies related to the URL filtering configuration or operation. The fw monitor command can provide a broader view of the gateway's network activity, but may not be as specific to URL filtering-related issues. The fw tab -t connections and cpinfo commands are more focused on overall system information and may not be as helpful for this specific problem.

Question: 733

What is the purpose of the "fw ctl pstat" command?

A. To display information about the firewall process status
B. To start or stop the firewall process
C. To view the firewall policy installation status
D. To generate a firewall performance report

Answer: A

Explanation: The "fw ctl pstat" command is used to display information about the current status of the firewall process, including the process ID, CPU and memory usage, and other relevant metrics.

Question: 734

Which of the following is the recommended approach for troubleshooting issues with the Mobile Access client application on the user's device?

A. Uninstall and reinstall the client application
B. Analyze the client-side logs and debug information
C. Perform a factory reset on the user's device
D. All of the above

Answer: D

Explanation: The recommended approach for troubleshooting issues with the Mobile Access client application on the user's device includes:

Uninstall and reinstall the client application
Analyze the client-side logs and debug information
Perform a factory reset on the user's device
This comprehensive approach allows you to identify and resolve any issues related to the client application, its configuration, or the device itself, which can all contribute to problems with the Mobile Access functionality.