156-587 Zertifizierungsantworten, 156-587 Fragen Und Antworten

Fast2test bietet verschiedene Schulungsunterlagen und Ressourcen zur Vorbereitung der CheckPoint 156-587 Prüfung. Es umfasst Kurse, Praxis-Test, Online Test Engine und einen Teil kostenloser PDF-Download.

CheckPoint 156-587 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Advanced Firewall Kernel Debugging: This section of the exam measures the skills of Check Point Network Security Administrators and focuses on kernel-level debugging for firewalls. Candidates will learn how to analyze kernel logs and troubleshoot firewall-related issues at a deeper level.
Thema 2	• Advanced Management Server Troubleshooting: This section of the exam measures the skills of Check Point System Administrators and focuses on troubleshooting management servers. It emphasizes understanding server architecture and diagnosing problems related to server performance and connectivity.
Thema 3	• Advanced Access Control Troubleshooting: This section of the exam measures the skills of Check Point System Administrators in demonstrating expertise in troubleshooting access control mechanisms. It involves understanding user permissions and resolving authentication issues.
Thema 4	• Advanced Identity Awareness Troubleshooting: This section of the exam measures the skills of heck Point Security Consultants and focuses on troubleshooting identity awareness systems.

>> 156-587 Zertifizierungsantworten <<

156-587 Fragen Und Antworten, 156-587 Prüfungsinformationen

Im Informationszeitalter kümmern sich viele Leute um die IT-Branche. Aber es fehlen trozt den vielen Exzellenten doch IT-

Fachleute. Viele Firmen stellen ihre Angestellte nach ihren Fragenkataloge Zertifikaten ein. Deshalb sind die Zertifikate bei den Firmen sehr beliebt. Aber es ist nicht so leicht, diese Zertifikate zu erhalten. Die CheckPoint 156-587 Zertifizierungsprüfung ist eine schwierige Zertifizierungsprüfung. Obwohl viele Menschen beteiligen sich an der CheckPoint 156-587 Zertifizierungsprüfung, ist jedoch die Pass-Quote eher niedrig.

CheckPoint Check Point Certified Troubleshooting Expert - R81.20 156-587 Prüfungsfragen mit Lösungen (Q93-Q98):

93. Frage
You need to monitor traffic pre-inbound and before the VPN module in a Security Gateway. How would you achieve this using fw monitor?

- A. fw monitor -pi -vpn
- B. fw monitor -p all
- C. fw monitor -pi +vpn
- D. fw monitor -pi +vpn

Antwort: A

Begründung:
The fw monitor command is a powerful troubleshooting tool in Check Point Gateways that captures packets at various points in the processing chain. The question asks how to capture traffic pre-inbound (before inbound processing, i.e., at the "i" inspection point) and before the VPN module (before VPN decryption or processing).
The fw monitor syntax allows specifying inspection points using options like -pi (pre-inbound) and module names (e.g., -vpn for the VPN module). The correct syntax to capture traffic before a specific module is -pi -<module>, where the module name is prefixed with a minus sign to indicate "before" the module.
Option A: Incorrect. fw monitor -p all captures packets at all inspection points in the chain, which includes pre-inbound, post-inbound, pre-outbound, and post-outbound points, as well as points around all modules. This is too broad and does not specifically target pre-inbound and before the VPN module.
Option B: Correct. fw monitor -pi -vpn captures packets at the pre-inbound inspection point ("i") and before the VPN module (-vpn). The -pi specifies the pre-inbound point, and -vpn ensures the capture occurs before VPN processing (e.g., decryption).
Option C: Incorrect. fw monitor -pi +vpn would capture packets at the pre-inbound point but after the VPN module (+vpn indicates after the module), which contradicts the requirement to capture before the VPN module.
Option D: Incorrect. This option is a duplicate of Option C in the provided question, likely a typographical error. Even if corrected, +vpn is incorrect for the same reason as Option C.
Reference:
The Check Point R81.20 Gaia Administration Guide explains the fw monitor command and its options, including how to specify inspection points and module positions. The CCTE R81.20 course includes hands-on labs for using fw monitor to troubleshoot packet flow, emphasizing precise inspection point selection.
For precise details, refer to:
Check Point R81.20 Gaia Administration Guide, section on "fw monitor" (available via Check Point Support Center).
CCTE R81.20 Courseware, which covers advanced packet capture techniques with fw monitor (available through authorized training partners).

94. Frage
Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application & Control URL Filtering?

- A. cprad
- B. pdpd
- C. rad
- D. pepd

Antwort: C

95. Frage
Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

- A. cpstat
- B. CPstat
- C. CPstat is not a valid command. The correct command is cpstat, which is case-sensitive.
- D. CPview
- E. fwstat

Antwort: A

Begründung:
The correct Check Point command to display status and statistics information for various Check Point products and applications is cpstat. This command provides a dynamic real-time view of the system, showing the information such as the number of connections, packets, drops, CPU usage, memory usage, disk space, license status, and blade status. The cpstat command can be customized by using various options and flags to specify the product, the interval, the fields, and the format of the output. For example, to display the status and statistics of the firewall module every 5 seconds, the command would be:
cpstat fw -f all -i 5
The other commands are incorrect because:
A: CPview is a Check Point tool that displays information about the system performance, such as the CPU, memory, disk, network, and firewall. It does not show information about other products and applications, such as VPN, Identity Awareness, Anti-Virus, etc.
C: fwstat is not a valid command. The correct command is fw ctl pstat, which displays information about the firewall kernel, such as the number of connections, packets, drops, memory, and synchronization. It does not show information about other products and applications, such as VPN, Identity Awareness, Anti-Virus, etc.
Reference:
cpstat - Check Point Software
CPView Utility
fw ctl pstat - Check Point Software
(CCTE) - Check Point Software

96. Frage
Which command is used to write a kernel debug to a file?

- A. fw ctl debut -T -f > debug.txt
- B. fw ctl debug -S -t > debug.txt
- C. fw ctl kdebug -T -I > debug.txt
- D. fw ctl kdebug -T -f > debug.txt

Antwort: D

97. Frage
What are the three main component of Identity Awareness?

- A. Client, SMS and Secure Gateway
- B. User, Active Directory and Access Role
- C. Identity Source Identity Server (POP) and Identity Enforcement (PEP)
- D. Identity Awareness Blade on Security Gateway, User Database on Security Management Server and Active Directory

Antwort: C

98. Frage
......