156-585 Q&As

Check Point Certified Troubleshooting Expert

Pass CheckPoint 156-585 Exam with 100% Guarantee

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

https://www.geekcert.com/156-585.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Vanessa is reviewing ike.elg file to troubleshoot failed site-to-site VPN connection After sending Mam Mode Packet 5 the response from the peer is PAYLOAD-MALFORMED" What is the reason for failed VPN connection?

A. The authentication on Phase 1 is causing the problem.Pre-shared key on local gateway encrypted by the hash algorithm created in Packet 3 and Packet 4 doesn\\'t match with the hash on the peer gateway generated by encrypting its preshared key

B. The authentication on Phase 2 is causing the problem Pre-shared key on local gateway encrypted by the hash algorithm created in Packets 1 and 2 doesn\\'t match with the hash on the peer gateway generated by encrypting its pre-shared key

C. The authentication on Quick Mode is causing the problem Pre-shared key on local gateway encrypted by the hash algorithm created in Packets 3 and 4 doesn\\'t match with the hash on the peer gateway generated by encrypting its preshared key

D. The authentication on Phase 1 is causing the problem Pre-shared key on local gateway encrypted by the hash algorithm doesn\\'t match with the hash on the peer gateway generated by encrypting its pre-shared key created in Packet 1 and Packet 2

Correct Answer: B

QUESTION 2

Which command is most useful for debugging the fwaccel module?

A. fw zdebug

B. securexl debug

C. fwaccel dbg

D. fw debug

Correct Answer: C

QUESTION 3

What process is responsible for sending and receiving logs in the management server?

A. FWD

B. CPM

C. FWM

D. CPD

Correct Answer: A

The FWD process is responsible for sending and receiving the logs from the different Check Point entities to the security management\log server (sometimes they are on the same machine).14 de nov. de 2019

QUESTION 4

Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/

B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/

C. $FWDIR/conf/install_firewall_imp/ANTIMALWARE/conf/

D. $FWDIR/log/install_manager_tmp/ANTIMALWARBlog?

Correct Answer: A

QUESTION 5

What is connect about the Resource Advisor (RAD) service on the Security Gateways?

A. RAD has a kernel module that looks up the kernel cache, notifies client about hits and misses and forwards a-sync requests to RAD user space module which is responsible for online categorization

B. RAD is completely loaded as a kernel module that looks up URL in cache and if not found connects online for categorization There is no user space involvement in this process

C. RAD functions completely in user space The Pattern Matter (PM) module of the CMI looks up for URLs in the cache and if not found, contact the RAD process in user space to do online categorization

D. RAD is not a separate module, it is an integrated function of the \\'fw1 kernel module and does all operations in the kernel space

Correct Answer: C