KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **156-590**

Title : Check Point Certified Threat Prevention Specialist (CTPS)

Version : DEMO

1.Task: Verify the enabled Software Blades on a Check Point Security Gateway.
A. See the Explanation.
Answer: A
Explanation:
1. SSH into the Security Gateway.
2. Run the command: cplic print to check license details.
3. Use: enabled_blades or cpstat os to verify enabled blades.
4. Confirm Threat Prevention blades like IPS, Anti-Bot, and Anti-Virus are listed.
5. Use SmartConsole > Gateway > General Properties to visually confirm the same.

2.Task: Validate the Threat Prevention policy is applied correctly to a Security Gateway.
A. See the Explanation.
Answer: A
Explanation:
1. Open SmartConsole > Threat Prevention > Policy.
2. Ensure the policy is assigned to the correct Gateway.
3. Publish and Install the policy.
4. SSH into the Gateway and run: fw stat to confirm active policy name.
5. Cross-verify that Threat Prevention blades are enforcing the loaded policy.

3.Task: Use CLI to test the management server connectivity from the Security Gateway.
A. See the Explanation.
Answer: A
Explanation:
1. SSH into the Security Gateway.
2. Ping the management server: ping .
3. Check hostname resolution: nslookup .
4. Confirm SIC is established: cp_conf sic state.
5. Check for outbound connectivity on port 18210 (CPD).

4.Task: Confirm that Security Management Server is operational.
A. See the Explanation.
Answer: A
Explanation:
1. SSH into the Management Server.
2. Check processes: cpwd_admin list.
3. Validate services: cpstat mg.
4. Confirm GUI is accessible via SmartConsole.
5. Run: netstat -an | grep 19009 to ensure GUI port is open.

5.Task: Check Secure Internal Communication (SIC) status between Management Server and Gateway.
A. See the Explanation.
Answer: A
Explanation:

1. On Management, open SmartConsole > Gateways.
2. Right-click the gateway > Test SIC status.
3. CLI: Run cp_conf sic state on the gateway.
4. Check logs in $FWDIR/log/sic.log.
5. Re-initialize SIC if needed via SmartConsole or CLI.