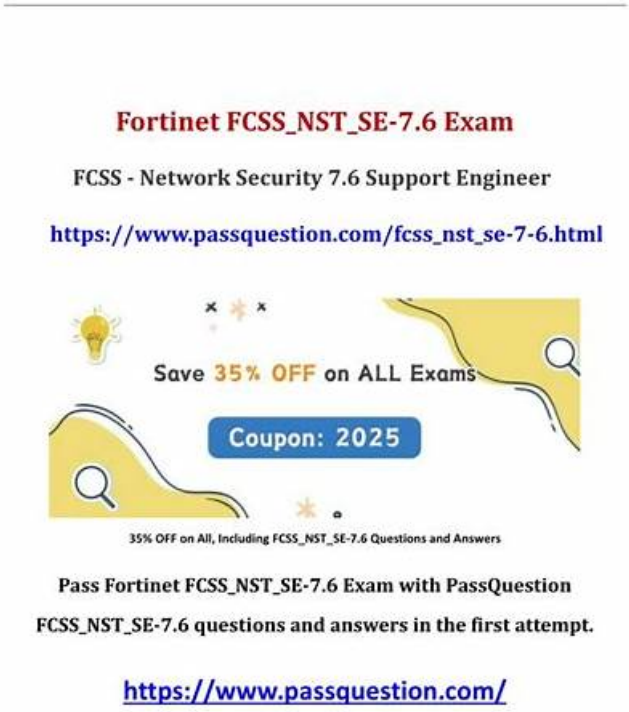
FCSS_NST_SE-7.6 Prüfungsaufgaben & FCSS_NST_SE-7.6 Lernressourcen



Wenn Sie sich sehr müde um die Vorbereitung der FCSS_NST_SE-7.6 Prüfungen bemühen, wissen Sie, was die anderen Kandidaten machen? Warum sind sie sehr Selbstbewusst und sorglos, während Sie sich um die Prüfungen sorgen? Ist Ihre Lernfähigkeit nicht so gut wie sie? Natürlich nicht. Wollen Sie wissen, warum andere sehr leicht Fortinet FCSS_NST_SE-7.6 Prüfung ablegen? Weil Sie Fortinet FCSS_NST_SE-7.6 Dumps von Pass4Test benutzen. Beim Lernen der Prüfungsfragen können Sie sehr einfach diese Prüfung bestehen. Glauben Sie nicht? Probieren Sie bitte mal. Sie können die Demo benutzen, um die Qualität der Zertifizierungsunterlagen selbst kennenzulernen. Bitte klicken Sie Pass4Test Website.

Fortinet FCSS_NST_SE-7.6 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• VPN: This section is aimed at IT Professionals and includes diagnosing and addressing issues with IPsec VPNs, specifically IKE version 1 and 2, to secure remote and site-to-site connections within the network infrastructure.
Thema 2	• Authentication: This section evaluates the abilities of System Administrators and requires troubleshooting both local and remote authentication methods, including resolving Fortinet Single Sign-On (FSSO) problems for secure network access.

Thema 3	• Routing: This section focuses on Network Engineers and involves tackling issues related to packet routing using static routes, as well as OSPF and BGP protocols to support enterprise network traffic flow.
Thema 4	• Security profiles: This part measures skills of Security Operations Specialists and covers identifying and resolving problems linked to FortiGuard services, web filtering configurations, and intrusion prevention systems to maintain protection across network environments.
Thema 5	• System troubleshooting: This section of the exam measures the skills of Network Security Support Engineers and addresses diagnosing and correcting issues within Security Fabric setups, automation stitches, resource utilization, general connectivity, and different operation modes in FortiGate HA clusters. Candidates work with built-in tools to effectively find and resolve faults.

FCSS_NST_SE-7.6 Aktuelle Prüfung - FCSS_NST_SE-7.6 Prüfungsguide & FCSS_NST_SE-7.6 Praxisprüfung

Viele Kandidaten wissen einfach nicht, wie sie sich auf die Prüfung vorbereiten können und hilflos sind. Aber mit den Schulungsunterlagen zur Fortinet FCSS_NST_SE-7.6 Zertifizierungsprüfung von Pass4Test ist alles ganz anders geworden. Mit ihr können Sie sich ganz selbstsicher auf Ihre Prüfung vorbereiten. Sie haben kein Risiko, in der Prüfung durchzufallen, mehr zu tragen. Das ist nicht nur seelische Hilfe. Am wichitgsten ist es, dass Sie die Prüfung bestehen und eine glänzende Zukunft haben können.

Fortinet FCSS - Network Security 7.6 Support Engineer FCSS_NST_SE-7.6 Prüfungsfragen mit Lösungen (Q90-Q95):

90. Frage
Refer to the exhibit, which shows the output o! the BGP database.

Which two statements are correct? (Choose two.)

- A. The output shows all prefixes advertised by all neighbors as well as the local router.
- B. The first four prefixes are being advertised using a legacy route advertisement.
- C. The advertised prefix of 10.20.30.0/24 was configured using the network command.
- D. The advertised prefix of 10.20.30.0/24 is being advertised through the redistribution of another routing protocol.

Antwort: A,C

Begründung:
* For Option A:In Fortinet BGP (and standard BGP), when a prefix is displayed with an "i" (lowercase i) in the Path column, it represents an internal prefix that originated from the local router, typically configured via the BGP "network" command. In the exhibit, the prefix 10.20.30.0/24 is listed with a Path value of i, indicating it was injected into BGP by the local router using the

network statement, not via redistribution from another routing protocol. The same logic applies to i as documented: "Origin code 'i' means the route was injected via the network command."
* For Option D:The get router info bgp network output is a summary table displaying both local and received BGP routes. It lists all known routes to the BGP process, whether received from peers or originated locally. The exhibit shows all BGP prefixes known to the local router, matching the official admin guide's description of this command's output.
* Explanation for B and C:
* The phrase "legacy route advertisement" is not formalized in BGP documentation or Fortinet's admin guide; the output uses standard BGP mechanics.
* If a route was redistributed into BGP from another routing protocol, the Path field would display a "?" (question mark) for incomplete (redistributed) origin. Here the /24 route has "i" so it is NOT a redistribution.
References:
FortiOS Administration Guide: BGP Configuration and Route Table Interpretation Official BGP Command Reference: Show BGP Network, Path Codes, Route Origination Indicators

91. Frage
Refer to the exhibit, which shows the modified output of the routing kernel.

Routing information

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S        0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S        8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O        10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C     *> 10.0.2.0/24 is directly connected, port4
B     *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B        10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```


Which statement is true?

- A. The BGP route to 10.0.4.0/24 is not in the forwarding information base.
- B. The default static route through port2 is in the forwarding information base.
- C. The default static route through 10.200.1.254 is not in the forwarding information base.
- D. The egress interface associated with static route 8.8.8.8/32 is administratively up.

Antwort: A

92. Frage
Which three common FortiGate-to-collector-agent connectivity issues can you identify using the FSSO real- time debug? (Choose three.)

- A. The connection was refused. There may be a mismatch of the TCP port.
- B. The pro-shared key does not match
- C. The SSL certificate used for FSSO over SSL has expired.
- D. The group filters do not match.
- E. FortiGate cannot reach the IP address of the collector agent.

Antwort: A,B,E

Begründung:
The diagnose debug authd fsso server command is the primary tool for troubleshooting communication between the FortiGate and the FSSO Collector Agent. This debug output reveals the status of the connection and the reasons for failure. The three most

common connectivity issues identified by this debug are:
* FortiGate cannot reach the IP address of the collector agent (Option C): The debug will show connection timeouts or "host unreachable" errors if the Layer 3 connectivity is missing.
* The connection was refused / Port mismatch (Option B): If the FortiGate can reach the IP but the Collector Agent is not listening on the specified port (default 8000), the debug will display "Connection refused." This often happens if the port configured on the FortiGate does not match the listening port on the agent.
* The pre-shared key does not match (Option D): If the IP and Port are correct, the next step is authentication. If the password configured on the FortiGate does not match the one on the Collector Agent, the debug will explicitly show an "Authentication failed" or "password mismatch" error during the handshake.
Note on other options: Option A (SSL) is less common than basic connectivity/auth mismatches. Option E (Group filters) relates to user processing logic, which occurs after connectivity is established.
Reference:
FortiGate Security 7.6 Study Guide (FSSO Troubleshooting): "Troubleshooting FSSO... Check connectivity (IP/Port) and authentication (Password)."

93. Frage
Refer to the exhibit.

FortiGate is showing continuous high CPU usage During a maintenance window, the CLI command diagnose sys top displays the output shown in the exhibit. The CLI command diagnose twat application ipsmonitor 5 was run. but the CPU usage by daemon ipsengine did not drop Which immediate action can you take to reduce the CPU usage effectively?

- A. Reduce the number of IPS signatures enabled on the active IPS profiles
- B. Bypass all IPS engines
- C. Disable IPS on all firewall policies.
- D. Execute diagnose test application ipsMonitor 2inatead.

Antwort: D

Begründung:
To solve this high CPU usage scenario involving the ipsengine, we must understand the specific functions of the diagnose test application ipsmonitor commands shown in the troubleshooting steps.
* Analyze the Situation:
* Exhibit: The diagnose sys top output shows the ipsengine process is in a run state (R) consuming 99% CPU.
* Previous Action: The administrator already ran diagnose test application ipsmonitor 5.
* Result: The CPU usage did not drop.
* Understand the Commands:
* diagnose test application ipsmonitor 5: This command toggles IPS Bypass Mode. When enabled, the IPS engine lets traffic pass through without inspection.
* Implication: If the CPU was high due to traffic volume, enabling bypass would drop the CPU load immediately.
* Failure: Since the CPU remained at 99% after bypass, the ipsengine process is likely frozen, stuck, or in an internal infinite loop unrelated to the current traffic flow. The process itself is the problem, not the traffic volume.
* Evaluate the Solution (Option B):
* diagnose test application ipsmonitor 2: This command toggles the IPS engine's Enable /Disable status.
* Because the engine is stuck (bypass failed to relieve pressure), the "Immediate action" required is to stop or restart the process entirely.
* Running option 2 effectively disables/kills the stuck IPS engine instance, which will immediately drop the CPU usage to near zero. (It can then be toggled again to restart it).
* Why other options are incorrect:
* A (Reduce signatures): This is a tuning measure for normal operation, not an immediate fix for a stuck process at 99% CPU.

* C (Disable IPS on policies): This is a configuration change that takes time and requires a commit; it is not the most immediate diagnostic tool available.
* D (Bypass all IPS engines): This describes the action of command 5 (Bypass), which the prompt explicitly states was already performed and failed.
Reference:
FortiGate Security 7.6 Study Guide (IPS & Diagnostics): "Troubleshooting IPS high CPU: 1. Check top. 2. Try bypass (ipsmonitor 5). 3. If CPU persists, restart the engine (ipsmonitor 99 or 2)."

94. Frage
Refer to the exhibits.

An OSPF peer is advertising route 172.16.52.0/24. The local FortiGate is configured with an inbound distribution list that allows the 172.16.0.0/16 network to be injected into its routing table. However, the
1'2.16.52.0/24 subnet cannot be seen in the FIB.
Which two stops can the administrator of the local FortiGate take to ensure that the advertised 172.16. 52.0/24 subnet will be injected into the routing table? (Choose two.)

- A. Modify the default prefix-list behavior from implicit deny to implicit allow.
- B. Change the R- value lo 16.
- C. Change the ge value to 17.
- D. Add another entry to the prefix list to specifically allow the 172.16.52.0/24 network.

Antwort: C,D

Begründung:
The issue is caused by the strict matching logic of the configured Prefix List.
* Current State: The rule is edit 1 with set prefix 172.16.0.0 255.255.0.0 and both ge (greater than or equal) and le (less than or equal) are unset.
* Behavior: When ge and le are unset, FortiOS requires an exact match of the subnet mask. The current rule only matches the exact network 172.16.0.0/16. It denies 172.16.52.0/24 because the mask (/24) does not match the rule's mask (/16).
To fix this and inject 172.16.52.0/24, you must modify the list to match the /24 mask:
* A. Add another entry to the prefix list to specifically allow the 172.16.52.0/24 network:
* Creating a new rule (e.g., edit 2) with set prefix 172.16.52.0 255.255.255.0 will provide an exact match for the incoming route, allowing it to pass the distribute-list.
* B. Change the ge value to 17:
* By configuring set ge 17 on the existing rule (conceptually 172.16.0.0/16 ge 17), you change the logic from "exact match" to "range match".
* This configuration tells the router to match any prefix starting with 172.16.x.x that has a subnet mask length of 17 or greater.
* Since the incoming route is a /24, and 24 is greater than 17, the route will match the prefix list and be accepted.
Why other options are incorrect:
* C: The option text appears to read "Change the ... value to 16". If this refers to le 16, it would enforce the mask to be exactly /16 or less, which still excludes /24.

* D: Changing the default behavior to implicit allow defeats the purpose of a filter (security control) and is not a standard configuration step for fixing a single missing route.
Reference:
FortiGate Security 7.6 Study Guide (Routing): "In prefix-lists, if ge and le are not used, the subnet mask must match exactly. To match subnets within a range, you must define the prefix length boundaries using ge or le."

95. Frage
.....