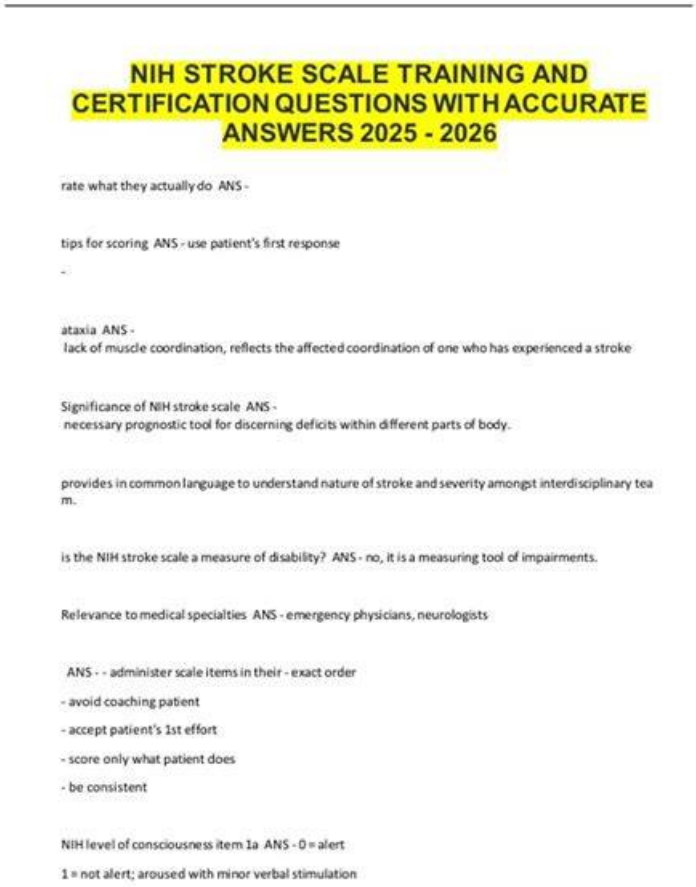
# FCSS_NST_SE-7.6 Certification Test Questions & Free PDF Quiz Fortinet Realistic FCSS - Network Security 7.6 Support Engineer Test Voucher



NIH STROKE SCALE TRAINING AND CERTIFICATION QUESTIONS WITH ACCURATE ANSWERS 2025 - 2026

rate what they actually do ANS -

tips for scoring ANS - use patient's first response

-

ataxia ANS -
lack of muscle coordination, reflects the affected coordination of one who has experienced a stroke

Significance of NIH stroke scale ANS -
necessary prognostic tool for discerning deficits within different parts of body.

provides in common language to understand nature of stroke and severity amongst interdisciplinary tea m.

is the NIH stroke scale a measure of disability? ANS - no, it is a measuring tool of impairments.

Relevance to medical specialties ANS - emergency physicians, neurologists

ANS - - administer scale items in their - exact order
- avoid coaching patient
- accept patient's 1st effort
- score only what patient does
- be consistent

NIH level of consciousness item 1a ANS - 0 = alert
1 = not alert; aroused with minor verbal stimulation

DOWNLOAD the newest VerifiedDumps FCSS_NST_SE-7.6 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=19NyzeALFYUehHlezlSQGJRN9on28w6hg

In order to cater to meet different needs of our customers, three versions of FCSS_NST_SE-7.6 exam bootcamp are available. Each version has its own advantages, and you can choose the most suitable one in accordance with your needs. Furthermore, FCSS_NST_SE-7.6 exam bootcamp is compiled by outstanding experts, therefore the quality and the accuracy can be guaranteed. Besides, we have the professional technicians to examine the website on a regular basis, hence a clean and safe shopping environment will be provided to you. You just need to buy the FCSS_NST_SE-7.6 Exam Dumps with ease.

## Fortinet FCSS_NST_SE-7.6 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • 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. |
| Topic 2 | • 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. |

| | |
|---|---|
| Topic 3 | • 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. |
| Topic 4 | • 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. |
| Topic 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 Test Voucher | Exam FCSS_NST_SE-7.6 Labs

A dedicated team is accessible for VerifiedDumps customers. One can reach our 24/7 customer support team to resolve their queries. Moreover, our team will also assist users if they face any kind of trouble while using above-mentioned formats of FCSS_NST_SE-7.6 practice material. We will offer you a refund guarantee (terms and conditions apply) as saving your money is our priority. Additionally, we offer up to 1 year of free updates and free demo of the FCSS_NST_SE-7.6 product. Order FCSS_NST_SE-7.6 exam questions now and get excellent these offers.

## Fortinet FCSS - Network Security 7.6 Support Engineer Sample Questions (Q24-Q29):

**NEW QUESTION # 24**
Which two statements about Security Fabric communications are true? (Choose two.)

- A. FortiTelemetry must be manually enabled on the FortiGate interface.
- B. FortiTelemetry and Neighbor Discovery both operate using TCP.
- C. By default, the downstream FortiGate establishes a connection with the upstream FortiGate using TCP port 8013.
- D. The default port for Neighbor Discovery can be modified.

**Answer: A,C**

**NEW QUESTION # 25**
Refer to the exhibit.

**Debug output**

```
FGT # diagnose debug application ike -1

FGT # diagnose debug enable

FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b0b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B708100501[illegible]9E253B0B0000006CE306FFBD5AD97F5AD027B12CAE19C5EFA091209F6D184E10DF2548B9B1FF60F6A13167A172
26398E                851BE86CDACD29234B58E5F48024711F4FA1F216E791CB1B13650F1E469BCEA5AE53CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB0000002000000001010108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000010110 8D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B8204D090A367DBDDDB20E5E12CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:1b1dd9b5f len=108 vrf=0
ike 0: in 82A79C36BC7F9ECDE1062B00FEBC8E239F55E1F3E3819655C641FDAAF20304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 0CC06CBD0000002000000001010108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B0000002000000001010108D2930DB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A69398EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB56B354FE46B84E6A79622FC1D44BC7F964986AD95D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 03A44559000000020000000010110 8D283DDB9994E7E8547D50F9D18113B6CA9900000002C0D9E6CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A63380C0000020000000010110 8D293CDB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BDDB812D02AE1672BD0E893431344D7BC31E9323A2C56E27DB43B747870885D7954558993B25BC43110695BEA47
ike 0:VPN_0:24266: recv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255.255 tunnel 73.25.189.174 oif VPN_0(12922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: delete
```

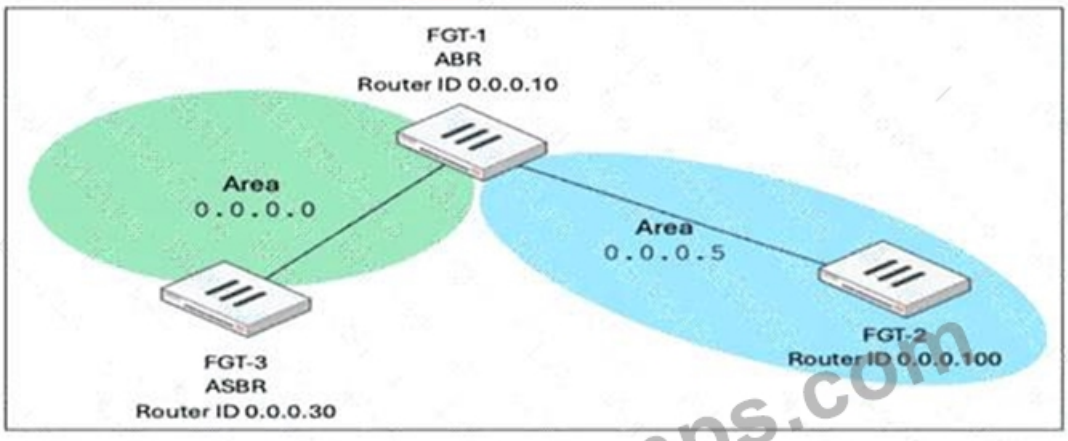
An IPsec VPN tunnel is dropping, as shown by the debug output.
Analyzing the debug output, what could be causing the tunnel to go down?

- A. Phase 2 drops but Phase 1 is up.
- B. The tunnel drops after the timer expires.
- C. Dead Peer Detection is not receiving its acknowledge packet.
- D. The tunnel drops during rekey negotiation.

**Answer: C**

**NEW QUESTION # 26**
While troubleshooting a FortiGate web filter issue, users report that they cannot access any websites, even though those sites are not explicitly blocked by any web filter profiles that are applied to firewall policies.

Network topology




OSPF database

```
FGT-2 # get router info ospf database brief

            OSPF Router with ID (0.0.0.100) (Process ID 0, VRF 0)

                Router Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag Link count
0.0.0.10        0.0.0.10        302  80000008 13ea  0002 1
0.0.0.100       0.0.0.100       295  8000000b 8761  0021 1

                Net Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag
100.64.1.1      0.0.0.10        302  80000001 feaa  0002

                Summary Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag Route
0.0.0.0         0.0.0.10        320  80000005 df70  0002 0.0.0.0/0
10.1.0.0        0.0.0.10        315  80000002 fc54  0002 10.1.0.0/24
10.1.10.0       0.0.0.10        311  80000001 9aac  0002 10.1.10.0/24
```



What are the three most likely reasons for this behavior? (Choose three answers)

- A. The SSL/TLS deep inspection was configured but the browsers do not have the FortiGate certificate installed.
- B. The FortiGuard Web Filtering license has expired, causing FortiGate to apply the default block action.
- C. The webfilter-force-off setting has been enabled under config system fortiguard.
- D. The web filter cache has been cleared causing all websites to take longer to be rated.
- E. The DNS server is unreachable, preventing URL resolution.

**Answer: A,B,E**

Explanation:
The reported symptom-users unable to access any websites despite no explicit blocks in the profile-points to systemic connectivity or configuration issues rather than specific URL filtering rules.
* Option B (SSL/TLS Inspection): When Deep Inspection is enabled, the FortiGate acts as a Man-in- the-Middle (MitM) and re-signs server certificates using its own CA. If the clients (browsers) do not trust this CA (i.e., the certificate is not installed in their Trusted Root store), they will reject the connection with certificate errors, effectively preventing access to all HTTPS websites.
* Option D (DNS): Web browsing relies on DNS resolution. If the configured DNS server is unreachable or failing, the FortiGate (or the client) cannot resolve FQDNs to IP addresses.
Consequently, browsers will fail to load any page, resulting in a total loss of web access.
* Option E (License): If the FortiGuard Web Filtering license expires, the FortiGate can no longer query the FortiGuard Distribution Network (FDN) for ratings. By default, or if the allow-when-rating- error setting is disabled (a common security practice), the FortiGate will block all web traffic that it cannot rate, often displaying a "Web Filter Service Error" or invalid license page.
Option A is incorrect because clearing the cache only increases latency, it does not block traffic. Option C is incorrect because webfilter-force-off is typically used to disable the service (often allowing traffic to bypass checks if the service is down), rather than blocking it.

**NEW QUESTION # 27**

Refer to the exhibit, which shows the output of a BGP debug command.

```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.125.0.60     4      65060    1698    1756      103    0    0 03:02:49        1
10.127.0.75     4      65075    2206    2250      102    0    0 02:45:55        1
100.64.3.1      4      65501     101     115        0    0    0 never       Active

Total number of neighbors 3
```

What can you conclude about the router in this scenario?

- A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the 8GP session with the local router.
- B. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
- C. An inbound route-map on local router is blocking the prefixes from neighbor 100.64.3.1.
- D. The BGP session with peer 10.127.0.75 is up.

**Answer: D**

Explanation:
The BGP debug output shows session information for peers, including state details. According to official Fortinet BGP documentation, if the session state with a peer does not show " Idle, " " Active, " or " Connect, " but instead shows " Established, " " Up, " or related counters (e.g., messages sent/received or uptime), it indicates the session is operational. In this scenario, the peer 10.127.0.75 is the only one showing a positive indication of a live, established session. Other options like neighbor-range configuration, AS mismatch, or route-maps blocking prefixes are not supported by evidence provided in a simple BGP session state debug, nor does the output show errors relating to local or remote AS issues.
The correct interpretation comes from Fortinet ' s BGP troubleshooting guide, which outlines how to read session status and neighbor states in debug and summary outputs.
References:
FortiOS BGP Debugging Guide: Session State Interpretation
BGP CLI Reference: Neighbor Status Fields

**NEW QUESTION # 28**
Refer to the exhibit, which shows the output of a real-time debug. Which statement about this output is true?
(Choose one answer)

```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training. fortinet.com:443, id=68[illegible]cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9 (ftgd-allow) wf-act=5 (ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

- A. FortiGate found the requested URL in its local cache.
- B. The server hostname was extracted from the SNI in the client request, or from the CN in the server certificate.
- C. This web request was inspected using the ftgd-allow web filter profile.
- D. The requested URL belongs to category ID 255.

**Answer: B**

Explanation:
The correct answer is A .
The debug output is for an HTTPS request and shows a hostname value. The study guide explains that with SSL certificate inspection, FortiGate extracts the FQDN from either:
* "TLS extension server name indication (SNI)"

* "SSL certificate common name (CN)"
So the hostname shown in the real-time web-filter debug can be derived from the SNI in the client request or, if needed, from the CN in the server certificate. That makes A correct.
Why the other options are wrong:
* B is wrong because the study-guide example for web-filter real-time debug explicitly says: "This slide shows an example of real-time debug output when the URL to categorize isn ' t in the FortiGuard cache." In these debugs, cat=255 appears before the final lookup result, so this does not indicate a local- cache hit.
* C is wrong because ftgd-allow is the action , not the profile name. The debug line shows the action as action=9 (ftgd-allow) while the profile shown is profile= ' default ' . FortiOS web-filter logs also use the profile field separately from the action field
* D is wrong because the final category shown is url_cat=52 , not 255. The study guide's example shows the same pattern: an initial cat=255 in the request line, followed by the resolved result cat=52 url_cat=52 So the verified answer is: A .

**NEW QUESTION # 29**
.....

www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2026 Fortinet FCSS_NST_SE-7.6 dumps are available on Google Drive shared by VerifiedDumps: https://drive.google.com/open?id=19NyzeALFYUehHlezlSQGJRN9on28w6hg