KillTest

質量更高　服務更好

學習資料

http://www.killtest.net

一年免費更新服務

Exam : **FCSS_NST_SE-7.6**

Title : Fortinet NSE 6 - Network Security 7.6 Support Engineer

Version : DEMO

1.Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.
Which action will FortiGate take when using the default settings for SSL certificate inspection?
A. FortiGate uses the SNI from the user's web browser.
B. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.
C. FortiGate uses the first entry listed in the SAN field in the server certificate.
D. FortiGate uses the CN information from the Subject field in the server certificate.
Answer: D
Explanation:
When FortiGate performs SSL certificate inspection with default settings, it checks if the Server Name Indication (SNI) matches either the Common Name (CN) or any Subject Alternative Name (SAN) in the server certificate. If there is no match, FortiGate does not block the connection; instead, it uses the CN value from the certificate's subject field to continue web filtering and categorization.
This behavior is described in the official Fortinet 7.6.4 Administration Guide:
“Check the SNI in the hello message with the CN or SAN field in the returned server certificate: Enable: If it is mismatched, use the CN in the server certificate.” This is the default (Enable) mode, which differs from the Strict mode that would block the mismatched connection.
By default, this policy ensures service continuity and prevents disruptions due to certificate mismatches, allowing FortiGate to log and inspect based on the CN even when the requested SNI does not match. It provides a balance between connection reliability and the accuracy of filtering by certificate identity, allowing security policies to remain functional without unnecessary blocks. This approach is recommended by Fortinet to maintain usability for end-users while still supporting granular inspection.
References: FortiGate 7.6.4 Administration Guide: Certificate Inspection SSL/SSH Inspection Profile Configuration

2.Exhibit.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response.
ike 0: Remotesite:3: VID DD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated                FC77570100
ike 0: Remotesite:3: VID FORTIGATE 8299031757A3608
ike 0: Remotesite:3: peer is Fortifate/Fartios, (v2C6A621DE00000000
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EB0 bo)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: received peer identifier FQDNCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: negotiation result            'remote"
ike 0: Remotesite:3: proposal id =1:
ike 0: Remotesite:3:       protocol id = ISAKMP:
ike 0: Remotesite:3:           trans id = KEY IKE.
ike 0: Remotesite:3:           encapsulation = IKE/
ike 0: Remotesite:3:               type=OAKLEY _ENCRnone
ike 0: Remotesite:3:               type=OAKLEY HASH?YPT _ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3:           type=AUTH METHOD, va ALG, val=SHA.
ike 0: Remotesite:3:           type=OAKLEY _GROUP, l=PRESHARED KEY.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400      val=MODP1024.
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CCZA
ike 0: Remotesite:3: sent IKE msg (agg i2send): 10.0.0.1:500->10.0.0.2:500, len=140, id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06689c022d4df682
```

Refer to the exhibit, which contains partial output from an IKE real-time debug.

Which two statements about this debug output are correct? (Choose two.)
A. Perfect Forward Secrecy (PFS) is enabled in the configuration.
B. The local gateway IP address is 10.0.0.1.
C. It shows a phase 2 negotiation.
D. The initiator provided remote as its IPsec peer ID.
Answer: C,D
Explanation:
From the exhibit, you can observe that the debug output captures an IKEv1 negotiation in aggressive mode. Let's break down the supporting details in line with official Fortinet IPsec VPN troubleshooting resources and debug guides:
For Option B:
The very first line of the debug output shows:
comes 10.0.0.2:500->10.0.0.1:500, ifindex=7.
This indicates the traffic direction—from the remote IP (10.0.0.2) with port 500 to the local IP (10.0.0.1) with port 500. According to Fortinet's documentation, the right side of the arrow always represents the local FortiGate gateway. Thus, 10.0.0.1 is the local gateway IP address.
For Option D:
You see the statement:
negotiation result "remote"
and
received peer identifier FQDNCE88525E7DE7F00D6C2D3C00000000
Official debug documentation describes that the "peer identifier" or peer ID sent by the initiator is displayed here. In the context of IKE/IPsec negotiation, this value is used as the IPsec peer ID for authentication and identification purposes. The initiator is providing "remote" as the peer ID for its connection.
Why Not A or C:
Perfect Forward Secrecy (PFS): The debug does not show any DH group negotiation in phase 2 (no reference to group2, group5, etc., for phase 2), so you cannot deduce the presence of PFS solely from this output.
Phase 2 negotiation: The log focuses on IKE (phase 1) negotiation and establishment; there’s no reference to ESP protocol, Quick Mode, or other identifiers that would show phase 2 SA negotiation and establishment.
This interpretation aligns with the explanation in the FortiOS 7.6.4 Administration Guide's VPN section and the official debug command output samples published in Fortinet’s documentation. It demonstrates how to distinguish between local and remote addresses and how to identify the use of peer IDs.
Reference: FortiOS 7.6.4 Administration Guide: IPsec VPN and Debugging VPNs
Technical Support Resources on interpreting IKE debug output and peer ID roles

3.Exhibit.

```
FGT # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Mon May  1 03:47:52 2023) -=-

IP                                          Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost           Updated Time
64.26.151.37                                    10     45          -5              262432         0        846 Mon May  1 03:47:43 2023
64.26.151.35                                    10     46          -5              329072         0       6806 Mon May  1 03:47:43 2023
66.117.56.37                                    10     75          -5               71638         0        275 Mon May  1 03:47:43 2023
65.210.95.240                                   20     71          -8               36875         0         92 Mon May  1 03:47:43 2023
209.22.147.36                                   20     103 DI      -8               34784         0       1070 Mon May  1 03:47:43 2023
208.91.112.194                                  20     107 D       -8               35170         0       1533 Mon May  1 03:47:43 2023
                                                                    0                33728         0        120 Mon May  1 03:47:43 2023
                                                                    1                33797         0        192 Mon May  1 03:47:43 2023
                                                                    9                33754         0        145 Mon May  1 03:47:43 2023
                                                                   -5                26410     26226      26227 Mon May  1 03:47:43 2023
```

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

What can you conclude about the debug output in this scenario?

A. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

B. There is a natural correlation between the value in the FortiGuard-requests field and the value in the Weight field.

C. FortiGate used 64.26.151.37 as the initial server to validate its contract.

D. Servers with a negative TZ value are less preferred for rating requests.

Answer: C

Explanation:

The exhibit displays the output from the diagnose debug rating command on a FortiGate device. This command is used to display information about FortiGuard Web Filtering or other security-related queries performed by FortiGate to FortiGuard servers. Official Fortinet documentation outlines the meaning of each field in the server list. The FortiGate maintains a list of available FortiGuard servers, selecting the optimal server based on factors such as weight, round-trip time (RTT), and regional settings.

The very first entry in the server list after "Server List" is the server FortiGate initially uses, prioritized by factors such as proximity and RTT. Here, 64.26.151.37 is listed first, and the FortiGuard-requests value confirms that this server handled the highest number of requests.

The IPs, weights, and lost/failed counters are monitored for server performance and selection over time. FortiGate's default operational logic is to try the first entry for contract validation and use the next in the list if the first is unavailable or has high latency or packet loss.

There is no direct correlation between the Weight and the number of FortiGuard-requests. The servers with higher or lower weights may still handle different request volumes based on availability and performance.

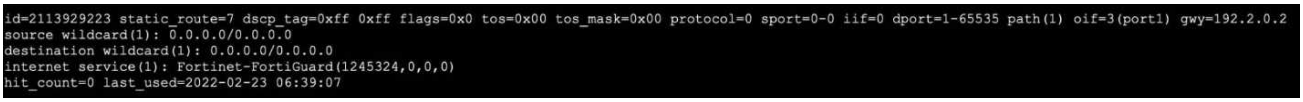
The TZ (time zone) value's sign (positive or negative) does not affect server preference; it is informational, showing the server's location relative to UTC, not a rating metric.

DNS query results for FortiGuard servers are not shown here, and the provided servers are not returned in DNS query order.

This command and interpretation are detailed in the FortiOS Administration Guide’s section describing FortiGuard server selection and contract validation processes.

References: FortiOS Administration Guide: FortiGuard Service Connectivity and Debugging Official Technical Notes on diagnose debug rating output structure

4.Refer to the exhibit, which shows the output of a policy route table entry.



Which type of policy route does the output show?
A. An ISDB route
B. A regular policy route
C. A regular policy route, which is associated with an active static route in the FIB
D. An SD-WAN rule
Answer: A
Explanation:
The exhibit for question 4 shows a policy route table entry, and key fields are as follows:
internet service (1): Fortinet-FortiGuard (1245324,0.0.0.0,0.0.0.0)
According to the Fortinet official documentation, when a policy route is based on Internet Service Database (ISDB) entries, the route entry will specifically mention “internet service,” showing the service being referenced (in this example, Fortinet-FortiGuard). This is fundamentally different from a regular policy route, which is defined by source, destination, and service wildcards without referencing an ISDB signature. A regular policy route's output would not contain the line “internet service.”
Policy routes that use ISDB allow FortiGate to steer traffic for specific well-known services (like FortiGuard, Google, Microsoft) based on traffic pattern recognition, even if the destination IP is dynamic. The matching and route selection follow the ISDB tag and can coexist with static or regular policy routes. Thus, this entry is correctly and uniquely an ISDB route, as explained in the FortiOS policy routing documentation and ISDB configuration references.
References: FortiOS Administration Guide: Policy Routing, ISDB integration and interpretation of route table entries ISDB-based Routing and Official CLI Outputs in Fortinet’s documentation

5.Exhibit.

Refer to the exhibit, which shows a FortiGate configuration.

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator do to fix the issue?

A. Disable webfilter-force-off.

B. Increase webfilter-timeout.

C. Enable fortiguard-anycast.

D. Change protocol to TCP.

Answer: A

Explanation:

The exhibit shows a FortiGate configuration under config system fortiguard related to web filtering and FortiGuard options.

There is a line:

set webfilter-force-off enable

According to official Fortinet documentation, the "webfilter-force-off" option, when enabled, causes the FortiGate to bypass web filtering for all traffic—even if a web filter profile is applied to a policy. This override is typically used for troubleshooting or performance reasons and is documented as an explicit bypass feature.

If an administrator wants to enforce web filtering inspection, this setting must be disabled. The correct

way to restore web filtering functionality is to run:
set webfilter-force-off disable
Once done, traffic passing through policies with web filter profiles will be inspected and filtered as per configuration. Other settings such as timeout or cache TTL do not bypass web filtering; they only affect operational nuances.
Reference: FortiOS Administration Guide: Web Filtering, FortiGuard Options, “webfilter-force-off” CLI