# NSE4_FGT-7.2 Q&As

Fortinet NSE 4 - FortiOS 7.2

## Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

**https://www.passapply.com/nse4_fgt-7-2.html**

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

Which three methods are used by the collector agent for AD polling? (Choose three.)

A. FortiGate polling

B. NetAPI

C. Novell API

D. WMI

E. WinSecLog

Correct Answer: BDE

FortiGate Infrastructure 7.2 Study Guide (p.127-128): "As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to

least recommended:

(WMI, WinSecLog, and NetAPI)"

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

**QUESTION 2**

An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSL/TLS connection.

Which FortiGate configuration can achieve this goal?

A. SSL VPN bookmark

B. SSL VPN tunnel

C. Zero trust network access

D. SSL VPN quick connection

Correct Answer: B

FortiGate Infrastructure 7.2 Study Guide (p.198): "Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as fortissl to the user\\'s PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated. The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel."

An SSL VPN tunnel allows remote users to establish a secure and encrypted Virtual Private Network (VPN) connection to the private network using the SSL/TLS protocol1. An SSL VPN tunnel can provide access to network resources such as FTP servers, as well as external applications running on the user\\'s PC1. An SSL VPN bookmark is a web link that provides access to network resources through the SSL VPN web portal1. It does not support external applications

running on the user\\'s PC. Zero trust network access (ZTNA) is a security model that provides role-based application access to remote users without exposing the private network to the internet2. It does not use SSL/TLS protocol, but rather a proprietary ZTNA protocol. SSL VPN quick connection is a feature that allows users to connect to an SSL VPN tunnel without installing FortiClient or any other software on their PC3. It requires a web browser that supports Java or ActiveX. It does not support external applications running on the user\\'s PC.

**QUESTION 3**

Which three statements explain a flow-based antivirus profile? (Choose three.)

A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.

B. If a virus is detected, the last packet is delivered to the client.

C. The IPS engine handles the process as a standalone.

D. FortiGate buffers the whole file but transmits to the client at the same time.

E. Flow-based inspection optimizes performance compared to proxy-based inspection.

Correct Answer: ADE

Reference: https://forum.fortinet.com/tm .aspx?m=192309

**QUESTION 4**

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

What two conclusions can you make from the debug flow output? (Choose two.)

A. The debug flow is for ICMP traffic.

B. The default route is required to receive a reply.

C. Anew traffic session was created.

D. A firewall policy allowed the connection.

Correct Answer: AC

The debug flow output shows the result of a diagnose command that captures the traffic flow between the source and destination IP addresses1. The debug flow output reveals the following information about the traffic flow1:

The protocol is 1, which means that the traffic uses ICMP protocol2. ICMP is a protocol that is used to send error messages and test connectivity between devices2.

The session state is 0, which means that a new traffic session was created3. A session is a data structure that stores information about a connection between two devices3.

The policy ID is 1, which means that the traffic matched the firewall policy with ID

14. A firewall policy is a rule that defines how FortiGate processes traffic based on the source, destination, service, and action parameters4. The action is 0, which means that the traffic was allowed by the firewall policy. An action is a

parameter that specifies what FortiGate does with the traffic that matches a firewall policy.

Therefore, two conclusions that can be made from the debug flow output are:

The debug flow is for ICMP traffic.

A new traffic session was created.

**QUESTION 5**

Refer to the exhibits.

Exhibit A

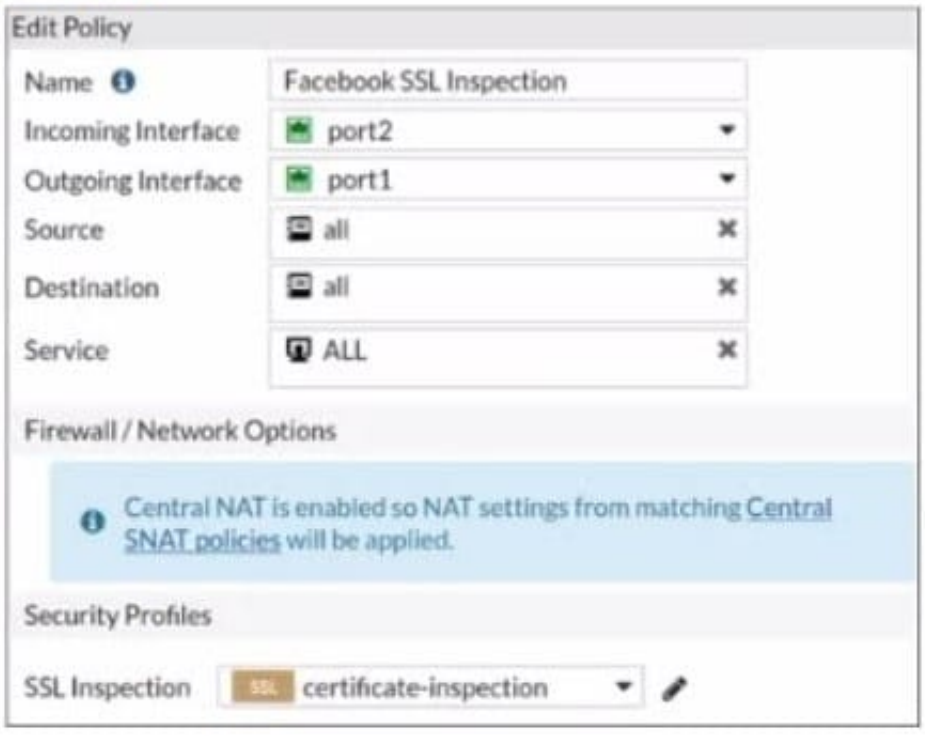

Exhibit B


The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook .

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

A. Make SSL inspection needs to be a deep content inspection.

B. Force access to Facebook using the HTTP service.

C. Get the additional application signatures are required to add to the security policy.

D. Add Facebook in the URL category in the security policy.

Correct Answer: A

They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather then adding an app rule.