[Dec 11, 2024 FCP_FGT_AD-7.4 Practice Exam Dumps - 99% Marks In Fortinet Exam [Q26-Q45

[Dec 11, 2024] FCP_FGT_AD-7.4 Practice Exam Dumps - 99% Marks In Fortinet Exam
Updated Verified FCP_FGT_AD-7.4 Q&As - Pass Guarantee or Full Refund

NO.26 What are two features of collector agent advanced mode? (Choose two.)
* In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
* Advanced mode supports nested or inherited groups.
* In advanced mode, security profiles can be applied only to user groups, not individual users.
* Advanced mode uses the Windows convention -NetBios: DomainUsername.

Advanced mode allows for configuration as an LDAP client and supports group filtering directly on the FortiGate, as well as nested or inherited groups.

NO.27 Refer to the exhibit.

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.

What is the most likely reason for this situation?
* The Service DNS is required in the firewall policy.
* The user is using an incorrect user name.
* The Remote-users group is not added to the Destination.
* No matching user account exists for this user.

Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not be presented with the login prompt when attempting to access an external website.

References:

* FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

NO.28 An administrator has configured central DNAT and virtual IPs.

Which item can be selected in the firewall policy Destination field?
* An IP pool
* A VIP object
* A VIP group
* The mapped IP address object of the VIP object

– when central NAT is enabled => put the mapped IP address of the VIP object.

– when central NAT is disabled => put the VIP object.

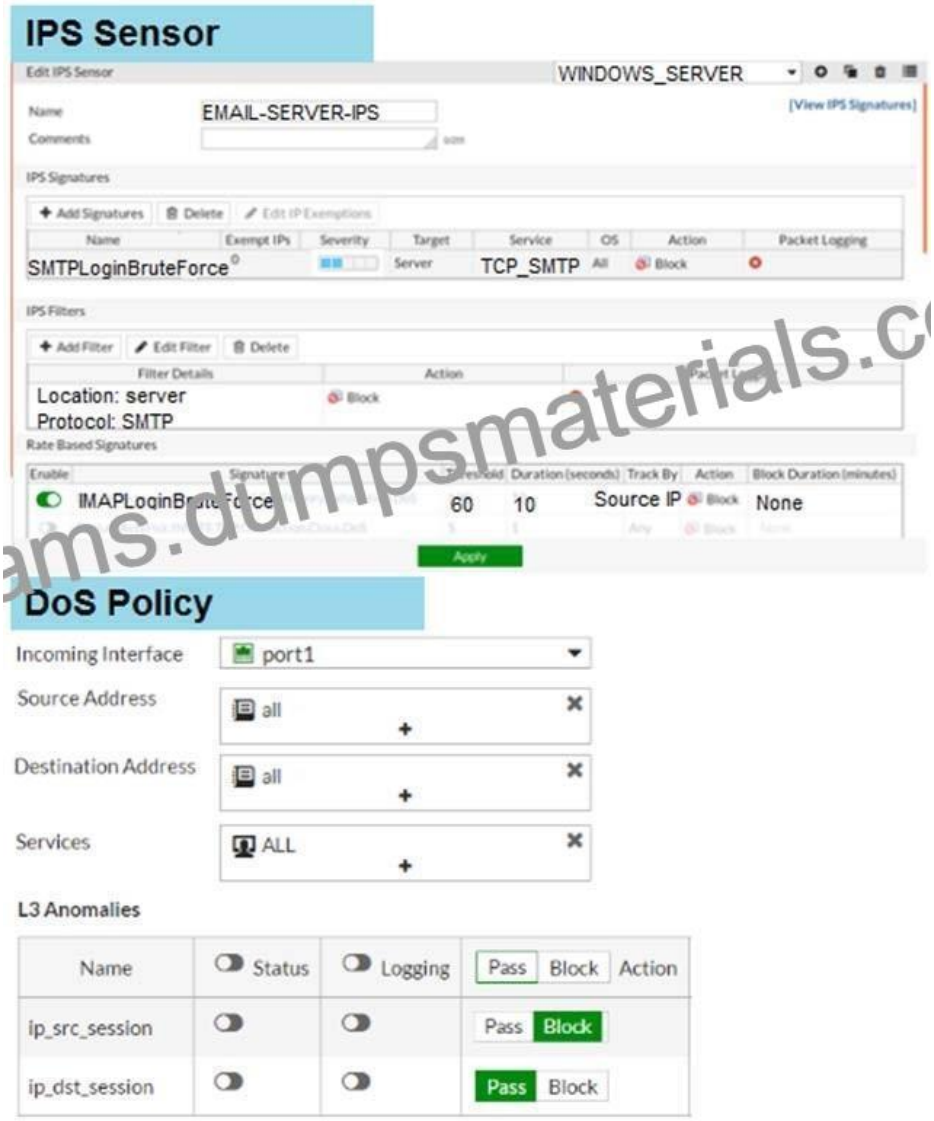
In the context of central DNAT and virtual IPs in FortiGate, the correct option for the firewall policy Destination field is:

D. The mapped IP address object of the VIP object

When configuring central DNAT, you typically select the mapped IP address object associated with the VIP object in the firewall policy Destination field. This mapped IP address represents the internal destination to which traffic will be redirected.

So, the correct choice is D.

NO.29 Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

* SMTP.Login.Brute.Force
* IMAP.Login.brute.Force
* ip_src_session
* Location: server Protocol: SMTP

IMAP.Login.brute.Force

Anomalies can be zero-day or denial of service attack

Are Detected by behaivoral analysis:

Rate Based IPS Signatures.

DoS Policies.

Protocol Constraint Inspections.

DoS policy disabled in this scenario.

NO.30 Which statement is a characteristic of automation stitches?
* They can be run only on devices in the Security Fabric.
* They can be created only on downstream devices in the fabric.
* They can have one or more triggers.
* They can run multiple actions at the same time.

NO.31 Refer to the exhibit.

Which contains a network diagram and routing table output. The Student is unable to access Webserver.

What is the cause of the problem and what is the solution for the problem?
* The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
* The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
* The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
* The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

Option C is the correct answer based on the provided information, let’s analyze it:

Option C states: “The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.” The issue is related to the first reply packet from the Student failing the Reverse Path Forwarding (RPF) check and that adding a static route to 203.0.114.24/32 through “port3” will resolve the problem, then you can go ahead with this solution.

In a typical RPF check scenario, it ensures that the incoming packet is arriving on the expected interface based on the routing table. Adding a static route to 203.0.114.24/32 through “port3” may indeed resolve the RPF issue if the routing is misconfigured.

Option C is the correct solution based on your network setup and further analysis, you can proceed with implementing that static route to see if it resolves the issue. Additionally, it’s a good practice to monitor the network to ensure that the problem is indeed resolved after making the change.

NO.32 Which two statements about the application control profile mode are true? (Choose two.)
* It uses flow-based scanning techniques, regardless of the inspection mode used.
* It cannot be used in conjunction with IPS scanning.
* It can be selected in either flow-based or proxy-based firewall policy.
* It can scan only unsecure protocols.

The two statements about the application control profile mode that are true are:

A. It uses flow-based scanning techniques, regardless of the inspection mode used.

The application control profile can be applied in both flow-based and proxy-based inspection modes, and it utilizes flow-based scanning techniques for application identification.

C. It can be selected in either flow-based or proxy-based firewall policy.

You can choose the application control profile in either flow-based or proxy-based firewall policies, providing flexibility in the application of application control.

The other options are not accurate:

B is incorrect because the application control profile can be used in conjunction with IPS (Intrusion Prevention System) scanning.

D is incorrect because the application control profile can scan both secure and unsecure protocols.

So, the correct choices are A and C.

NO.33 Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)
* The host field in the HTTP header.
* The server name indication (SNI) extension in the client hello message.
* The subject alternative name (SAN) field in the server certificate.
* The subject field in the server certificate.
* The serial number in the server certificate.

When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:

* Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows FortiGate to identify the server’s hostname during the SSL handshake.

* Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.

* Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server’s identity during SSL certificate inspection.

The other options are not used in SSL certificate inspection for hostname identification:

* Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.

* Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.

References

* FortiOS 7.4.1 Administration Guide – SSL/SSH Inspection, page 1802.

* FortiOS 7.4.1 Administration Guide – Configuring SSL/SSH Inspection Profile, page 1799.

NO.34 Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

System Performance output

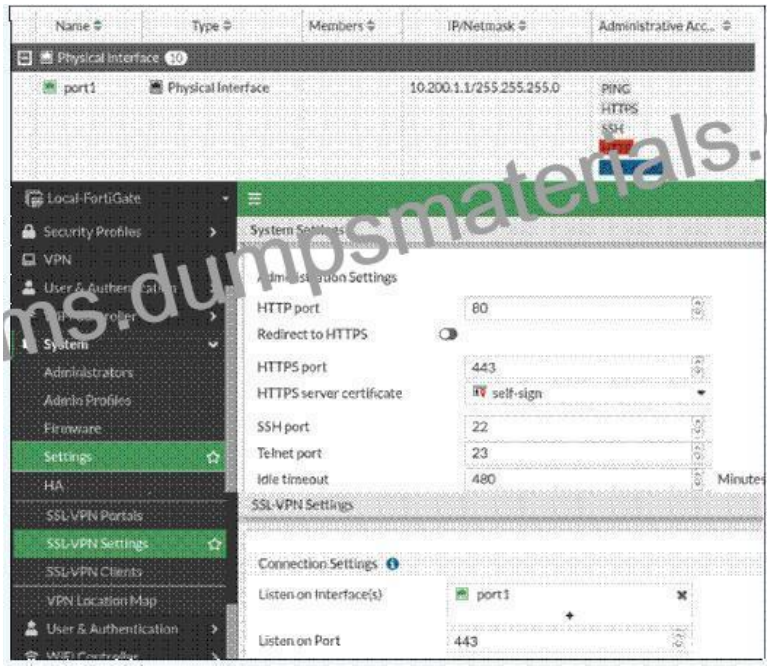
```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% so
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% s
Memory: 2061108k total, 1854997k used (90%), 206111k free (5.1%), 100
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minu
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3
Average session setup rate: 0 sessions per second in last 1 minute, 0
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)
* FortiGate will start sendingall files to FortiSandbox for inspection.
* FortiGate has entered conserve mode.
* Administrators cannot change the configuration.
* Administrators can access FortiGate onlythrough the console port.

NO.35 Refer to the exhibit.



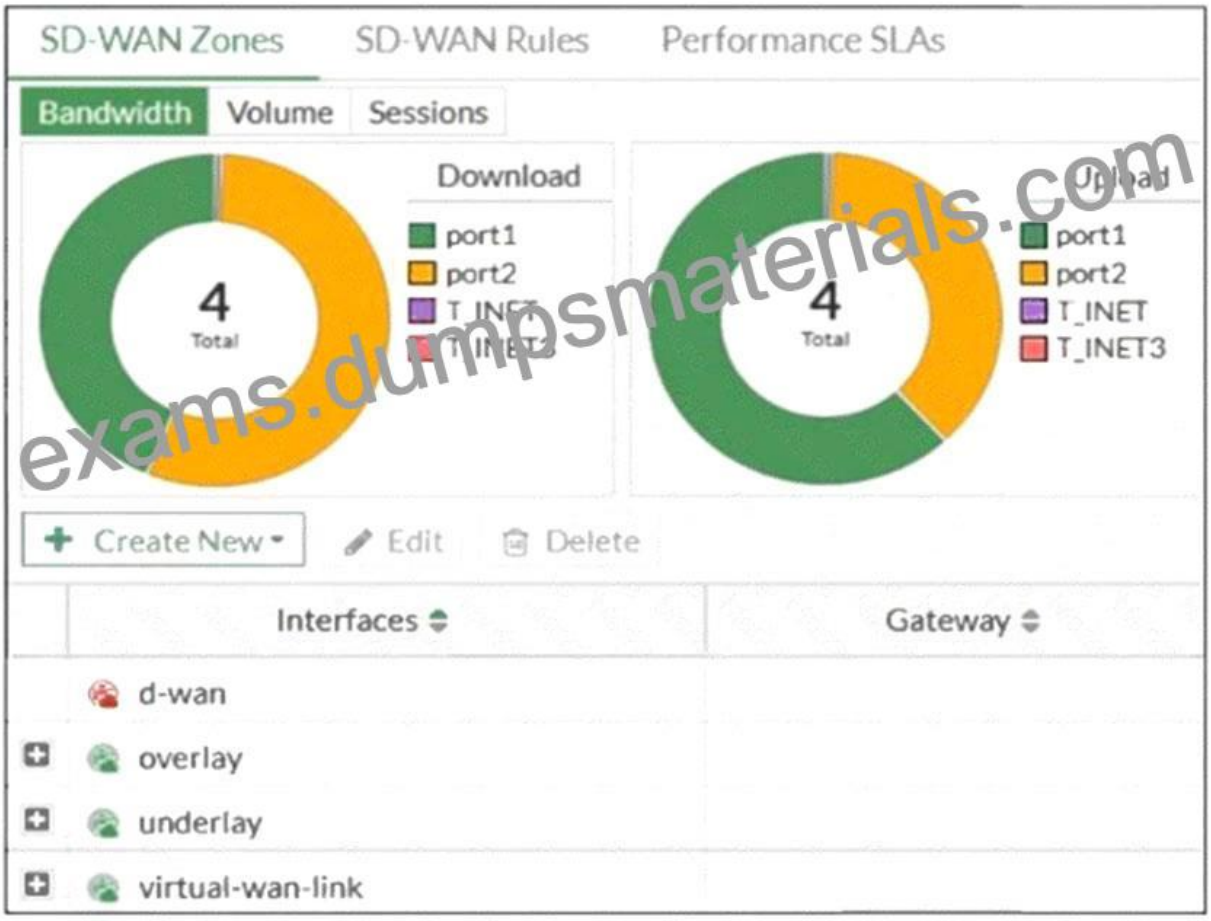
Which statement about the configuration settings is true?
* When a remote user accesses http://10.200.1.1:443, the SSL-VPN login page opens.
* When a remote user accesses https://10.200.1.1:443, the SSL-VPN login page opens.
* When a remote user accesses https://10.200.1.1:443, the FortiGate login page opens.
* The settings are invalid. The administrator settings and the SSL-VPN settings cannot use the same port.

B. When a remote user accesses https://10.200.1.1:443, the SSL-VPN login page opens.

In this scenario, the remote user is accessing the FortiGate device using HTTPS (port 443), which is typically used for SSL-VPN access. Therefore, when accessing the device at that address and port, the SSL-VPN login page should open for the user to authenticate and establish a VPN connection.

NO.36 Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration



Based on the exhibit, which statement is true?

* The underlay zone contains port1and
* The d-wan zone contains no member.
* The d-wan zone cannot be deleted.
* The virtual-wan-link zone contains no member.

NO.37 Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

* Checksums of devices are compared against each other to ensure configurations are the same.
* Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.
* Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster
* Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

NO.38 Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
	Physical Interface 14			
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10

Given the interfaces shown in the exhibit, which two statements are true? (Choose two.)
* Traffic between port2 and port2-vlan1 is allowed by default.
* port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
* port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.
* port1 is a native VLAN.

C: port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

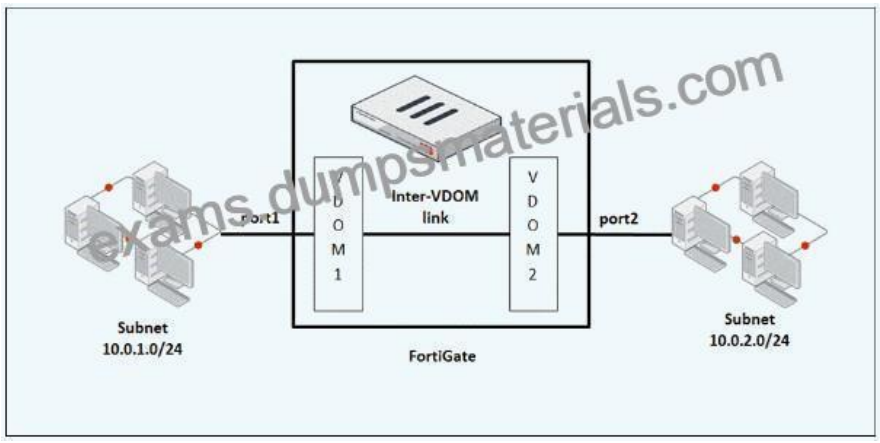
D: port1 is a native VLAN.

Incorrect:

A: Traffic between port2 and port2-vlan1 is allowed by default.

B: port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

NO.39 View the exhibit.



Both VDOMs are operating in NAT/route mode. The subnet 10.0.1.0/24 is connected to VDOM1. The subnet 10.0.2.0/24 is connected to VDOM2. There is an inter-VDOM link between VDOM1 and VDOM2.

Also, necessary firewall policies are configured in VDOM1 and VDOM2.

Which two static routes are required in the FortiGate configuration, to route traffic between both subnets through an inter-VDOM link? (Choose two.)
* A static route in VDOM1 with the destination subnet matching the subnet assigned to the inter-VDOM link
* A static route in VDOM2 for the destination subnet 10.0.1.0/24
* A static route in VDOM1 for the destination subnet 10.0.2.0/24
* A static route in VDOM2 with the destination subnet matching the subnet assigned to the inter- VDOM link
The two static routes required in the FortiGate configuration to route traffic between both subnets through an inter-VDOM link are:

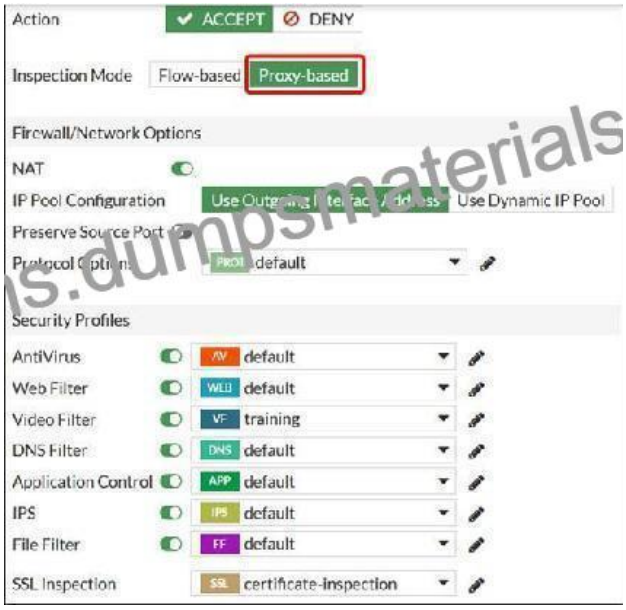
B. A static route in VDOM2 for the destination subnet 10.0.1.0/24

C. A static route in VDOM1 for the destination subnet 10.0.2.0/24

In VDOM1, a static route for the destination subnet 10.0.2.0/24 is needed to route traffic destined for VDOM2’s subnet through the inter-VDOM link.

In VDOM2, a static route for the destination subnet 10.0.1.0/24 is needed to route traffic destined for VDOM1’s subnet through the inter-VDOM link.

NO.40 Examine the exhibit, which shows a firewall policy configured with multiple security profiles.



Which two security profiles are handled by the IPS engine? (Choose two.)
* Web Filter
* IPS
* AntiVirus

* Application Control

When the FortiGate is set for proxy inspection mode, the IPS engine will handle the Application Control and IPS security profiles.

The security profiles that will be handled by the IPS engine when the FortiGate is set for proxy inspection mode are Application Control and IPS. In this mode, the FortiGate acts as an intermediary between the client and the server, intercepting and inspecting traffic to enforce security policies. The IPS engine is responsible for analyzing network traffic and identifying any malicious or suspicious activity based on predefined rules and signatures.

NO.41 Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

* Pre-shared key and certificate signature as authentication methods
* Extended authentication (XAuth)to request the remote peer to provide a username and password
* Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
* No certificate is required on the remote peer when you set the certificate signature as the authentication method

FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.

References:

* FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

NO.42 Refer to the exhibit.

In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.

What should the administrator do next to troubleshoot the problem?

* Run a sniffer on the web server.
* Capture the traffic using an external sniffer connected to port1.
* Execute another sniffer in the FortiGate, this time with the filter “host 10.0.1.10”
* Execute a debug flow.

Execute a debug flow.

Because sniffer shows the ingressing and egressing packets, but we cannot see dropped packets by fortigate in a sniffer. Debugging

can show the packets are not entering for any reasons caused by fortigate. So, if a packed is reached to fortigate and dropped , debug will show us.

NO.43 An employee needs to connect to the office through a high-latency internet connection.

Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?
* SSL VPN idle-timeout
* SSL VPN login-timeout
* SSL VPN dtls-hello-timeout
* SSL VPN session-ttl

NO.44 Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)
* If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
* If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
* If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP
* If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.

When SD-WAN is enabled on FortiGate, the load balancing algorithm for Equal-Cost Multi-Path (ECMP) is configured using the load-balance-mode parameter under SD-WAN settings. However, if SD-WAN is disabled, the ECMP load balancing algorithm can be configured under config system settings. This flexibility allows FortiGate to control traffic routing behavior based on the network configuration and requirements.

References:

* FortiOS 7.4.1 Administration Guide: ECMP Configuration

NO.45 Refer to the exhibit, which shows a partial configuration from the remote authentication server.

Why does the FortiGate administrator need this configuration?
* To authenticate only the Training user group.
* To set up a RADIUS server Secret
* To authenticate and match the Training OU on the RADIUS server.
* To authenticate Any FortiGate user groups.

The configuration shown in the exhibit indicates that the FortiGate is using a Fortinet-specific RADIUS attribute (Fortinet-Group-Name) with the value “Training.” This setup allows the FortiGate to authenticate users against the RADIUS server and match them to the “Training” Organizational Unit (OU). By doing so, only users within this specific group or OU can be authenticated and allowed access through the FortiGate.

References:

* FortiOS 7.4.1 Administration Guide: RADIUS Server Configuration

FCP_FGT_AD-7.4 Real Valid Brain Dumps With 50 Questions:
https://www.dumpsmaterials.com/FCP_FGT_AD-7.4-real-torrent.html]