Exam Code: NSE4_FGT-7.2
Exam Name: Fortinet NSE 4 - FortiOS 7.2

Exam A

QUESTION 1
Which two statements are correct about SLA targets? (Choose two.)

A. You can configure only two SLA targets per one Performance SLA.
B. SLA targets are optional.
C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
D. SLA targets are used only when referenced by an SD-WAN rule.

Correct Answer: B, D
Section:

QUESTION 2
Refer to the exhibit.

```
FGT1 # 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
       > - selected route, * - FIB route, p - stale info

S      *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
       *>            [10/0] via 10.0.0.2, port2, [30/0]
S         0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C      *> 10.0.0.0/24 is directly connected, port2
S         172.13.24.0/24 [10.0] is directly connected, port4
C      *> 172.20.121.0/24 is directly connected, port1
S      *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C      *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

A. The port3 default route has the lowest metric.
B. The port1 and port2 default routes are active in the routing table.
C. The ports default route has the highest distance.
D. There will be eight routes active in the routing table.

Correct Answer: B, C
Section:
Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p/197595

QUESTION 3
When configuring a firewall virtual wire pair policy, which following statement is true?

A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.

B. Only a single virtual wire pair can be included in each policy.

C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.

D. Exactly two virtual wire pairs need to be included in each policy.

Correct Answer: A
Section:

QUESTION 4
Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 8001 f020 0a00 0102        E..</...........
0x0010   0808 0808 0800 4d5a 0001 0001 6162 6364        ......MZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 7f01 0106 0a38 f0e4        E..</........8..
0x0010   0808 0808 0800 6159 ec01 0001 6162 6364        ......aY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000   4500 003c 0000 0000 7501 3a95 0808 0808        E..<....u.:.....
0x0010   0a38 f0e4 0000 6959 ec01 0001 6162 6364        .8....iY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000   4500 003c 0000 0000 7401 2bb0 0808 0808        E..<....t.+.....
0x0010   0a00 0102 0000 555a 0001 0001 6162 6364        ......UZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.
Which three pieces of information are included in the sniffer output? (Choose three.)

A. Interface name

B. Ethernet header

C. IP header

D. Application header

E. Packet payload

Correct Answer: A, C, E
Section:
Explanation:
Study Guide -- Routing -- Diagnostics -- Packet Capture Verbosity Level.
diagnose sniffer packet <interface> '<filter>' <verbosity> <count> <timestamp> <frame size>
In the example, verbosity is 5.
The verbosity level specifies how much info you want to display.
1 (default): IP Headers.
2: IP Headers, Packet Payload.
3: IP Headers, Packet Payload, Ethernet Headers.
4: IP Headers, Interface Name.

5: IP Headers, Packet Payload, Interface Name.
6: IP Headers, Packet Payload, Ethernet Headers, Interface Name.

QUESTION 5
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

A. Add the support of NTLM authentication.
B. Add user accounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Correct Answer: D
Section:

QUESTION 6
An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 168. 1.0/24 and the remote quick mode selector is 192. 168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192. 168. 1.0/24
B. 192. 168.0.0/24
C. 192. 168.2.0/24
D. 192. 168.3.0/24

Correct Answer: C
Section:
Explanation:
For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.
To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.
Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

QUESTION 7
Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.
B. FGCP is not used when FortiGate is in transparent mode.
C. FGCP runs only over the heartbeat links.
D. FGCP is used to discover FortiGate devices in different HA groups.

Correct Answer: A, C
Section:
Explanation:
The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:
FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block.
FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.
FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between

the devices. FGCP does not run over other types of links, such as data links.

https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol

FortiGate Infrastructure 7.2 Study Guide (p.292): 'FortiGate HA uses the Fortinet-proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health of members. To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces.'

QUESTION 8
Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

A. The keyUsage extension must be set to keyCertSign.

B. The common name on the subject field must use a wildcard name.

C. The issuer must be a public CA.

D. The CA extension must be set to TRUE.

Correct Answer: A, D
Section:
Explanation:
'In order for FortiGate to act in these roles, its CA certificate must have the basic constraints extension set to cA=True and the value of the keyUsage extension set to keyCertSign.'

QUESTION 9
Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

A. Proxy-based inspection

B. Certificate inspection

C. Flow-based inspection

D. Full Content inspection

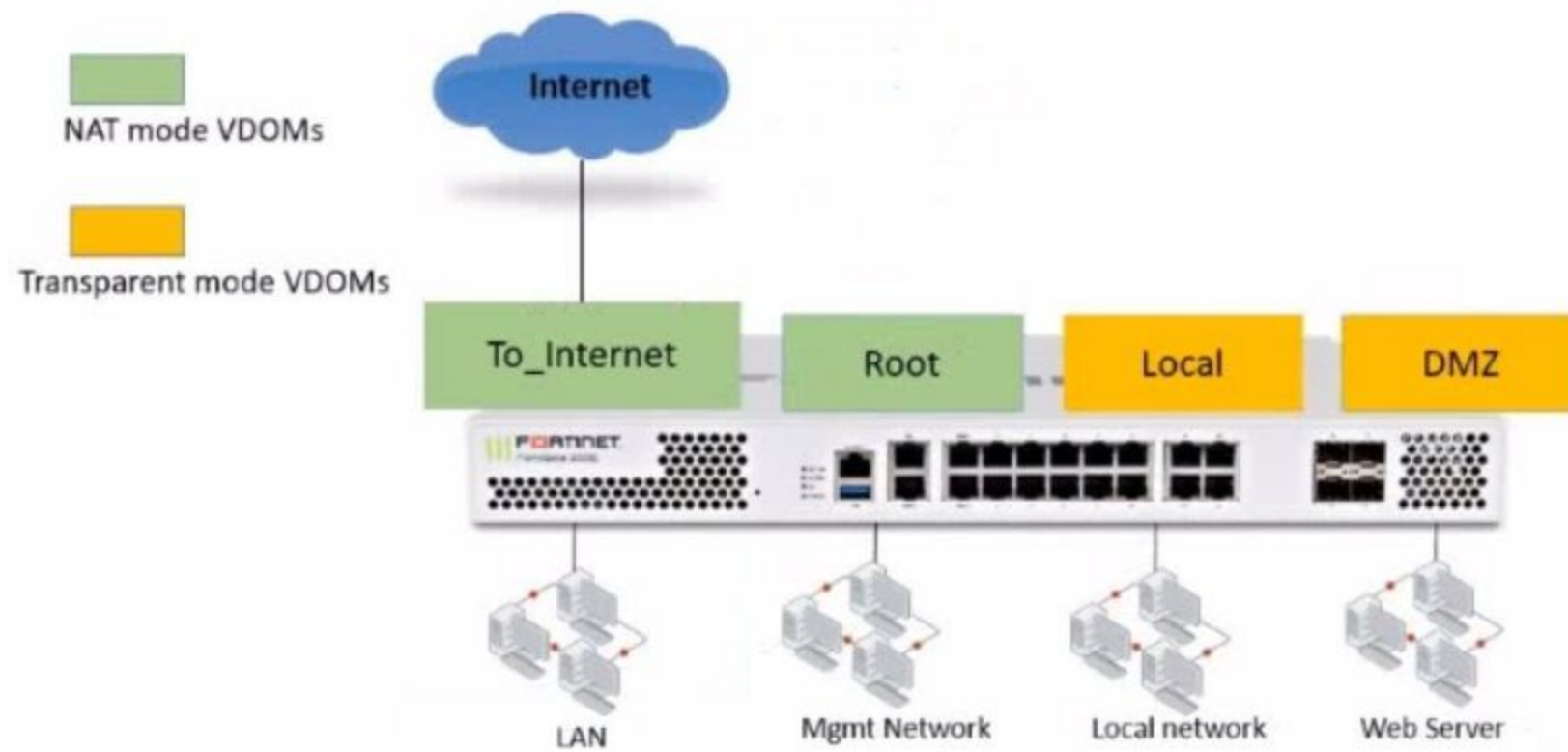**Correct Answer: A, C**
Section:

QUESTION 10
Refer to the exhibit.

The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem .
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.

B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.

C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.

D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Correct Answer: A
Section:

QUESTION 11
Refer to the exhibit.

Edit IPS Sensor

Name: WINDOWS_SERVERS
Comments: Write a comment... 0/255
Block malicious URLs (toggle off)

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging	Status
NTP.Spoofed.KoD.DoS	0	Monitor	✓ Enabled	✓ Enabled
OS Windows		⊘ Block	✗ Disabled	✓ Enabled

The exhibit shows the IPS sensor configuration.
If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Correct Answer: A, B
Section:

QUESTION 12
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status
B. get system performance status
C. diagnose sys top
D. get system arp

Correct Answer: D
Section:
Explanation:
'If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table.'

QUESTION 13
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"
```

Which two statements about the debug flow output are correct? (Choose two.)

A. The debug flow is of ICMP traffic.
B. A firewall policy allowed the connection.
C. A new traffic session is created.
D. The default route is required to receive a reply.

Correct Answer: A, C
Section:

QUESTION 14
Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
B. The client FortiGate requires a manually added route to remote subnets.
C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
D. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Correct Answer: C, D
Section:
Explanation:
https://docs.fortinet.com/document/fortigate/7.0.9/administration-guide/508779/fortigate-as-ssl-vpn-client
To establish an SSL VPN connection between two FortiGate devices, the following two settings are required:
The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate will use a CA (Certificate Authority) certificate to verify the client FortiGate certificate, ensuring that the client device is trusted and allowed to establish an SSL VPN connection.
The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: The client FortiGate must have an SSL VPN tunnel interface type configured in order to establish an SSL VPN connection. This interface type will be used to connect to the server FortiGate over the SSL VPN.

QUESTION 15
On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs
B. Forward traffic logs
C. Local traffic logs
D. Security logs

Correct Answer: C
Section:
Explanation:
Traffic logs record the traffic flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through FortiGate, this type of logging is also called firewall policy logging. Firewall policies control all

traffic attempting to pass through the FortiGate unit, between FortiGate interfaces, zones, and VLAN sub-interfaces.
FortiGate Security 7.2 Study Guide (p.176): 'Local traffic logs contain information about traffic directly to and from the FortiGate management IP addresses. They also include connections to the GUI and FortiGuard queries.'

QUESTION 16
Which statement about the policy ID number of a firewall policy is true?

A. It is required to modify a firewall policy using the CLI.
B. It represents the number of objects used in the firewall policy.
C. It changes when firewall policies are reordered.
D. It defines the order in which rules are processed.

Correct Answer: A
Section:

QUESTION 17
Refer to the exhibits.

SSL-VPN Settings

Connection Settings ℹ

Listen on Interface(s)	🖥 port1 ✕ ＋
Listen on Port	10443
	ℹ Web mode access will be listening at https://10.200.1.1:10443
Redirect HTTP to SSL-VPN	⬤
Restrict Access	**Allow access from any host** | Limit access to specific hosts
Idle Logout	🟢
Inactive For	300 Seconds
Server Certificate	🔒 Fortinet_Factory ▼
Require Client Certificate	⬤

Tunnel Mode Client Settings ℹ

Address Range	**Automatically assign addresses** | Specify custom IP ranges
	Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210
DNS Server	**Same as client system DNS** | Specify
Specify WINS Servers	⬤

Authentication/Portal Mapping ℹ

＋ Create New ✎ Edit 🗑 Delete

Users/Groups ⇅	Portal ⇅
👤 sslvpn	tunnel-access
All Other Users/Groups	full-access

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.
B. Change the Server IP address.
C. Change the idle-timeout.
D. Change the SSL VPN portal to the tunnel.

Correct Answer: A
Section:

QUESTION 18
An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

A. The strict RPF check is run on the first sent and reply packet of any new session.
B. Strict RPF checks the best route back to the source using the incoming interface.
C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
D. Strict RPF allows packets back to sources with all active routes.

Correct Answer: B
Section:
Explanation:
Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.

QUESTION 19
Refer to the exhibits.

Exhibit A

Edit Policy

Name ℹ️	Facebook SSL Inspection
Incoming Interface	🖧 port2 ▾
Outgoing Interface	🖧 port1 ▾
Source	🖥 all ✖
Destination	🖥 all ✖
Service	🔘 ALL ✖

Firewall / Network Options

ℹ️ Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

Security Profiles

SSL Inspection	SSL certificate-inspection ▾ ✏️

Exhibit B

Edit Policy

Name ℹ️	Facebook Access
Incoming Interface	🖧 port2 ▾
Outgoing Interface	🖧 port1 ▾
Source	🖥 all ✖
Destination	🖥 all ✖
Schedule	🕒 always ▾
Service	**App Default** Specify
Application	Facebook ✖
	Facebook_Like.Button 🔒 ✖
	Facebook_Video.Play ✖
URL Category	+
Action	✔ ACCEPT ⊘ DENY

Firewall / Network Options

Protocol Options	PRX default ▾ ✏️

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
Section:
Explanation:
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.

QUESTION 20
Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

A. FortiGate uses the AD server as the collector agent.

B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

C. FortiGate does not support workstation check .

D. FortiGate directs the collector agent to use a remote LDAP server.

Correct Answer: B, C
Section:
Explanation:
You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent.
Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs.
FG acts as a collector. It 's responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349

QUESTION 21
Refer to the exhibit.

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check . Which interface will be selected as an outgoing interface?

A. port2

B. port4

C. port3

D. port1

Correct Answer: D
Section:
Explanation:
Port 1 shows the lowest latency.

QUESTION 22
Refer to the exhibit.

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. The signature setting uses a custom rating threshold.

B. The signature setting includes a group of other signatures.

C. Traffic matching the signature will be allowed and logged.

D. Traffic matching the signature will be silently dropped and logged.

Correct Answer: D
Section:
Explanation:
Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be 'Pass' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be 'Default'.
Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

QUESTION 23
Refer to the exhibit.

Network diagram

WAN(port1)
10.200.1.1/24

10.0.1.10/24

LAN(port3)
10.0.1.254

Virtual IP

VIP type	IPv4
Name	VIP
Comments	Write a comment... 0/255
Color	🎨 Change

IP Poo

Name
Comment
Type
External I

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration.

The WAN (port1) interface has the IP address 10.200. 1. 1/24.

The LAN (port3) interface has the IP address 10 .0.1.254. /24.

The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0. 1. 10?

A. 10.200. 1. 1

B. 10.200.3. 1

C. 10.200. 1. 100

D. 10.200. 1. 10

Correct Answer: C
Section:
Explanation:

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

QUESTION 24
Refer to the exhibit.

Name	SLA_1
Protocol	Ping HTTP DNS
Servers	4.2.2.2 ✖
	4.2.2.1 ✖
Participants	All SD-WAN Members Specify
	🖼 port1 ✖
	🖼 port2 ✖
	+
Enable probe packets	⬤

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.
Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

A. The Detection Mode setting is not set to Passive.
B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
C. The configured participants are not SD-WAN members.
D. The Enable probe packets setting is not enabled.

Correct Answer: B, D
Section:

QUESTION 25
Refer to the exhibit.

```
STUDENT # get system session list
PROTO    EXPIRE  SOURCE           SOURCE-NAT        DESTINATION        DESTINATION-NAT
tcp      3598    10.0.1.10:2706   10.200.1.6:2706   10.200.1.254:80    -
tcp      3598    10.0.1.10:2704   10.200.1.6:2704   10.200.1.254:80    -
tcp      3596    10.0.1.10:2702   10.200.1.6:2702   10.200.1.254:80    -
tcp      3599    10.0.1.10:2700   10.200.1.6:2700   10.200.1.254:443   -
tcp      3599    10.0.1.10:2698   10.200.1.6:2698   10.200.1.254:80    -
tcp      3598    10.0.1.10:2696   10.200.1.6:2696   10.200.1.254:443   -
udp      174     10.0.1.10:2694   -                 10.0.1.254:53      -
udp      173     10.0.1.10:2690   -                 10.0.1.254:53      -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

A. Destination NAT is disabled in the firewall policy.
B. One-to-one NAT IP pool is used in the firewall policy.

C. Overload NAT IP pool is used in the firewall policy.

D. Port block allocation IP pool is used in the firewall policy.

Correct Answer: B
Section:
Explanation:
FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

QUESTION 26
FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.
Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

A. www.example.com:443

B. www.example.com

C. example.com

D. www.example.com/index.html

Correct Answer: B, C
Section:
Explanation:
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names - no URLs or wildcard characters are allowed.
OK: google.com or www.google.com
NO OK: www.google.com/index.html or google.*
FortiGate_Security_6.4 page 384
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names-- 'no URLs or wildcard characters are allowed'.

QUESTION 27
Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
      pingsvr_flip_timeout/expire=3600s/2781s
       'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
       'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.
Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.

B. FortiGate devices are not in sync because one device is down.

C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.

D. FortiGate SN FGVM010000064692 has the higher HA priority.

Correct Answer: A, D

Explanation:
1. Override is disable by default - OK
2. 'If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the
primary' The QUESTION NO : here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab

QUESTION 28
Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
    pingsvr_flip_timeout/expire=3600s/2781s
    'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
    'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.
Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.

B. FortiGate devices are not in sync because one device is down.

C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.

D. FortiGate SN FGVM010000064692 has the higher HA priority.

Correct Answer: A, D
Explanation:
1. Override is disable by default - OK
2. 'If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the
primary' The QUESTION NO : here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab

QUESTION 29
Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up. but phase 2 fails to come up.
Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

A. On HQ-FortiGate, enable Auto-negotiate.

B. On Remote-FortiGate, set Seconds to 43200.

C. On HQ-FortiGate, enable Diffie-Hellman Group 2.

D. On HQ-FortiGate, set Encryption to AES256.

Correct Answer: D
Section:
Explanation:
Encryption and authentication algorithm needs to match in order for IPSEC be successfully established.

QUESTION 30
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache

B. FortiSIEM

C. FortiAnalyzer

D. FortiSandbox

E. FortiCloud

Correct Answer: B, C, E
Section:
Explanation:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview

QUESTION 31
A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.
What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

A. Static IP Address
B. Dialup User
C. Dynamic DNS
D. Pre-shared Key

Correct Answer: B
Section:
Explanation:
Dialup user is used when the remote peer's IP address is unknown. The remote peer whose IP address is unknown acts as the dialup clien and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

QUESTION 32
An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

A. Policy lookup will be disabled.
B. By Sequence view will be disabled.
C. Search option will be disabled
D. Interface Pair view will be disabled.

Correct Answer: D
Section:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821

QUESTION 33
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent must search security event logs.
D. The NetSession Enum function is used to track user logouts.

Correct Answer: D
Section:
Explanation:
FortiGate_Infrastructure_7.0 page 270: 'NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows.'
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1

QUESTION 34

An administrator has configured the following settings:

```
config system settings
  set ses-denied-traffic enable
end
config system global
  set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

A. Device detection on all interfaces is enforced for 30 minutes.

B. Denied users are blocked for 30 minutes.

C. A session for denied traffic is created.

D. The number of logs generated by denied traffic is reduced.

Correct Answer: C, D
Section:
Explanation:
ses-denied-traffic
Enable/disable including denied session in the session table.
https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/20620/config-system-settings
block-session-timer
Duration in seconds for blocked sessions .
integer
Minimum value: 1 Maximum value: 300
30
https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/1620/config-system-global

QUESTION 35
In an explicit proxy setup, where is the authentication method and database configured?

A. Proxy Policy

B. Authentication Rule

C. Firewall Policy

D. Authentication scheme

Correct Answer: D
Section:

QUESTION 36
In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.

B. The Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.

C. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.

D. The IP version of the sources and destinations in a policy must match.

E. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Correct Answer: B, D, E
Section:

QUESTION 37
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning

B. Exempt

C. Allow

D. Learn

Correct Answer: A, C
Section:

QUESTION 38
Examine this FortiGate configuration:

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
      set srcaddr 10.0.1.0/24
      set active-auth-method SCHEME2
    next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic.

C. It authenticates the traffic using the authentication scheme SCHEME2.

D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D
Section:
Explanation:
'What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting'

QUESTION 39
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries

B. PKI

C. Traffic shaping

D. DNS

Correct Answer: A, D
**Section:**
Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.73): 'What about traffic originating from FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate. Traffic coming from FortiGate to those global services originates from the management VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM. It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate.'

QUESTION 40
Refer to the exhibit.
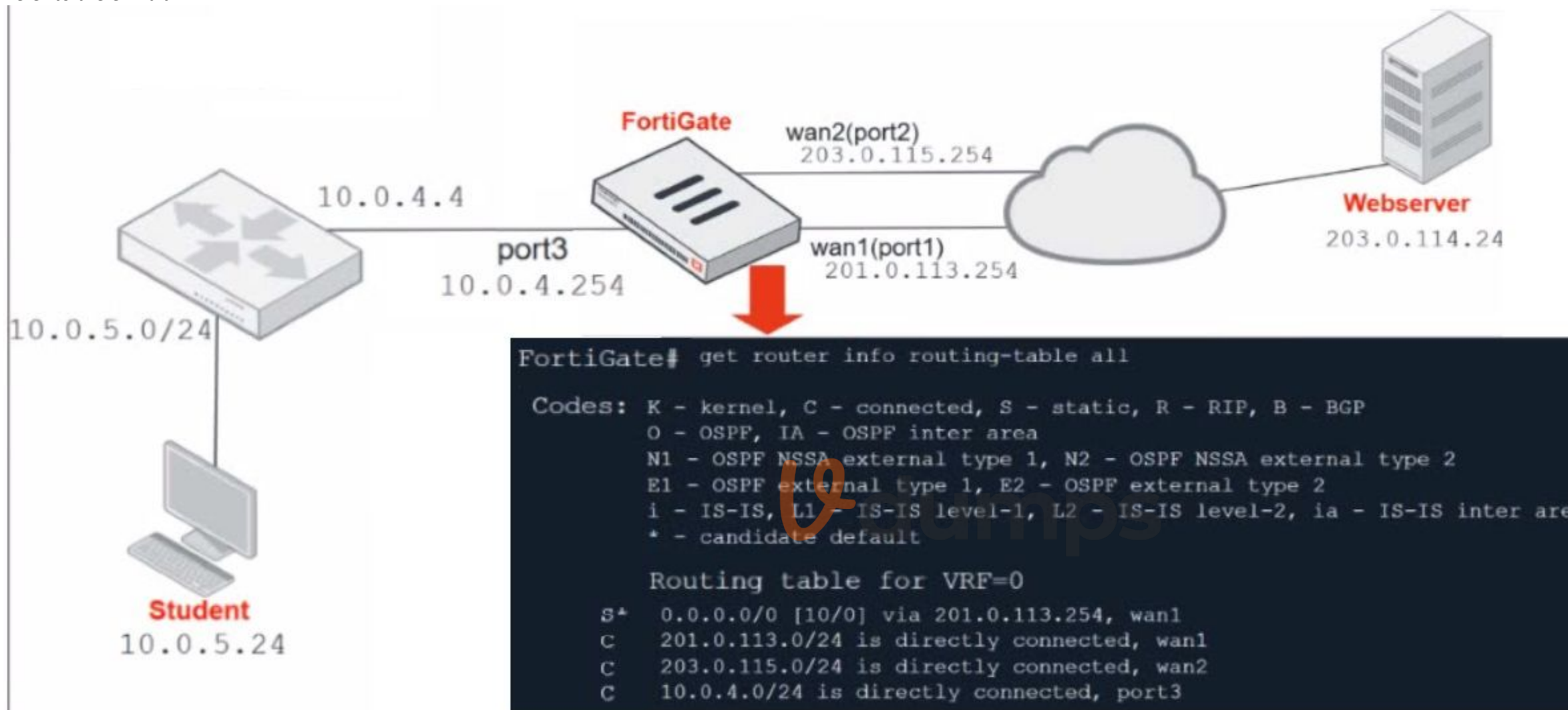
Which contains a network diagram and routing table output.
The Student is unable to access Webserver.
What is the cause of the problem and what is the solution for the problem?

A. 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.
B. 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.
C. 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.
D. 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.

Correct Answer: D
Section:

QUESTION 41
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

A. diagnose wad session list

B. diagnose wad session list | grep hook-pre&&hook-out
C. diagnose wad session list | grep hook=pre&&hook=out
D. diagnose wad session list | grep 'hook=pre'&'hook=out'

Correct Answer: A
Section:

QUESTION 42
Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.
C. Highest to lowest priority defined in the firewall policy.
D. Services defined in the firewall policy.
E. Lowest to highest policy ID number.

Correct Answer: A, B, D
Section:
Explanation:
When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which
you can define using the following objects:
* Incoming Interface
* Outgoing Interface
* Source: IP address, user, internet services
* Destination: IP address or internet services
* Service: IP protocol and port number
* Schedule: Applies during configured times

QUESTION 43
Which scanning technique on FortiGate can be enabled only on the CLI?

A. Heuristics scan
B. Trojan scan
C. Antivirus scan
D. Ransomware scan

Correct Answer: A
Section:

QUESTION 44
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.
D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Correct Answer: A, C
Section:

QUESTION 45
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scanning of application traffic to the DNS protocol only.
B. It limits the scanning of application traffic to use parent signatures only.
C. It limits the scanning of application traffic to the browser-based technology category only.
D. It limits the scanning of application traffic to the application category only.

Correct Answer: C
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.317): 'You can configure the URL Category within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website.'

QUESTION 46
Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides
(client and server) have terminated the session?

A. To remove the NAT operation.
B. To generate logs
C. To finish any inspection operations.
D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

Correct Answer: D
Section:

QUESTION 47
Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin ->sink: org pre->post, reply pre->post dev=5->3/3 ->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53 -> 10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```
Which statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.
B. The session is in TCP ESTABLISHED state.
C. The session is a bidirectional UDP connection.
D. The session is a bidirectional TCP connection.

Correct Answer: C
Section:
Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

QUESTION 48
A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.

Network (HQ-FortiGate)

Field	Value
IP Version	**IPv4** IPv6
Remote Gateway	Static IP Address
IP Address	10.10.200.10
Interface	port1
Local Gateway	
Mode Config	☐
NAT Traversal	**Enable** Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable **On Idle** On Demand
Forward Error Correction	Egress ☐ Ingress ☐
Advanced...	

Authentication

Field	Value
Method	Pre-shared Key
Pre-shared Key	••••••••

IKE

Version **1** 2

Mode

Aggressive Main (ID protection)

Peer Options

Accept Types

Any peer ID

Phase 1 Proposal ⊕ Add

Encryption	AES128	Authentication	SHA1	✕
Encryption	AES256	Authentication	SHA256	✕

Diffie-Hellman Group: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 ☑5 ☑2 1

Key Lifetime (seconds) 86400

Local ID

Network (Remote-FortiGate)

Field	Value
IP Version	**IPv4** IPv6
Remote Gateway	Static IP Address
IP Address	10.10.100.10
Interface	port1
Local Gateway	
Mode Config	☐
NAT Traversal	**Enable** Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable On Idle **On Demand**
Forward Error Correction	Egress ☐ Ingress ☐
Advanced...	

Authentication

Field	Value
Method	Pre-shared Key
Pre-shared Key	••••••••

IKE

Version **1** 2

Mode Aggressive **Main (ID protection)**

Phase 1 Proposal ⊕ Add

Encryption	AES256	Authentication	SHA256	✕

Diffie-Hellman Group: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 ☑2 1

Key Lifetime (seconds) 86400

Local ID

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

A. On HQ-FortiGate, set IKE mode to Main (ID protection).

B. On both FortiGate devices, set Dead Peer Detection to On Demand.

C. On HQ-FortiGate, disable Diffie-Helman group 2.

D. On Remote-FortiGate, set port2 as Interface.

Correct Answer: A, D
Section:
Explanation:
'In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel.'

QUESTION 49
Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

A. To detect intermediary NAT devices in the tunnel path.

B. To dynamically change phase 1 negotiation mode aggressive mode.

C. To encapsulation ESP packets in UDP packets using port 4500.

D. To force a new DH exchange with each phase 2 rekey.

Correct Answer: A, C
Section:

QUESTION 50
An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.

B. Create a new service object for HTTP service and set the session TTL to never

C. Set the TTL value to never under config system-ttl

D. Set the session TTL on the HTTP policy to maximum

Correct Answer: B, C
Section:

QUESTION 51
A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not Which configuration option is the most effective way to support this request?

A. Implement a web filter category override for the specified website

B. Implement a DNS filter for the specified website.

C. Implement web filter quotas for the specified website

D. Implement web filter authentication for the specified website.

Correct Answer: D
Section:

QUESTION 52

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

A. The matching firewall policy is set to proxy inspection mode.

B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

C. The full SSL inspection feature does not have a valid license.

D. The browser does not trust the certificate used by FortiGate for SSL inspection.

Correct Answer: D
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.235): 'If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser.'

QUESTION 53
Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

A. Subject Key Identifier value

B. SMMIE Capabilities value

C. Subject value

D. Subject Alternative Name value

Correct Answer: A
Section:

QUESTION 54
Which two statements are true about the RPF check? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.

B. The RPF check is run on the first reply packet of any new session.

C. The RPF check is run on the first sent and reply packet of any new session.

D. RPF is a mechanism that protects FortiGate and your network from IP spoofing attacks.

Correct Answer: A, D
Section:

QUESTION 55
Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

A. DNS

B. ping

C. udp-echo

D. TWAMP

Correct Answer: C, D

QUESTION 56
An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

A. The administrator can register the same FortiToken on more than one FortiGate.
B. The administrator must use a FortiAuthenticator device
C. The administrator can use a third-party radius OTP server.
D. The administrator must use the user self-registration server.

Correct Answer: B
Section:

QUESTION 57
Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.
B. The existing network IP schema must be changed when installing a transparent mode.
C. Static routes are required to allow traffic to the next hop.
D. FortiGate forwards frames without changing the MAC address.

Correct Answer: A, D
Section:
Explanation:
attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

QUESTION 58
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

A. diagnose sys top
B. execute ping
C. execute traceroute
D. diagnose sniffer packet any
E. get system arp

Correct Answer: B, C, D
Section:

QUESTION 59
Examine this PAC file configuration.
Which of the following statements are true? (Choose two.)

A. Browsers can be configured to retrieve this PAC file from the FortiGate.
B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
D. Any web request fortinet.com is allowed to bypass the proxy.

Correct Answer: A, D
Section:

QUESTION 60
If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL
B. A person
C. A subordinate CA
D. A root CA

Correct Answer: D
Section:

QUESTION 61
Which three statements are true regarding session-based authentication? (Choose three.)

A. HTTP sessions are treated as a single user.
B. IP sessions from the same source IP address are treated as a single user.
C. It can differentiate among multiple clients behind the same source IP address.
D. It requires more resources.
E. It is not recommended if multiple users are behind the source NAT

Correct Answer: A, C, D
Section:

QUESTION 62
Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeout. The FortiGate considers a user to be 'idle' if it does not see any packets coming from the user's source IP.
B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
C. It is an idle timeout. The FortiGate considers a user to be 'idle' if it does not see any packets coming from the user's source MAC.
D. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Correct Answer: A
Section:

QUESTION 63
Which of statement is true about SSL VPN web mode?

A. The tunnel is up while the client is connected.
B. It supports a limited number of protocols.
C. The external network application sends data through the VPN.
D. It assigns a virtual IP address to the client.

Correct Answer: B
Section:

Explanation:
FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

QUESTION 64
What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

A. Full Content inspection
B. Proxy-based inspection
C. Certificate inspection
D. Flow-based inspection

Correct Answer: D
Section:

QUESTION 65
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

Correct Answer: A, C
Section:

QUESTION 66
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries
B. PKI
C. Traffic shaping
D. DNS

Correct Answer: A, D
Section:

QUESTION 67
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries
B. PKI
C. Traffic shaping
D. DNS

Correct Answer: A, D
Section:

QUESTION 68
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

A. diagnose wad session list
B. diagnose wad session list | grep hook-pre&&hook-out
C. diagnose wad session list | grep hook=pre&&hook=out
D. diagnose wad session list | grep 'hook=pre'&'hook=out'

Correct Answer: A
Section:

QUESTION 69
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.
D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Correct Answer: A, C
Section:

QUESTION 70
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.
B. By default, the SSL VPN portal requires the installation of a client's certificate.
C. By default, split tunneling is enabled.
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Correct Answer: D
Section:

QUESTION 71
Refer to the exhibits.
The exhibits show the firewall policies and the objects used in the firewall policies.
The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 0	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1.635		
Facebook-Web	Destination	26.578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80	TCP	Enabled
	443		
	8443		
1.9.91.17 - 1.9.91.18	443	UDP	Enabled
1.9.91.30	443	UDP	Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP / DNS / HTTPS	ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	ACCEPT	Enabled

Which policy will be highlighted, based on the input criteria?

A. Policy with ID 4.
B. Policy with ID 5.
C. Policies with ID 2 and 3.
D. Policy with ID 4.

Correct Answer: B
Section:
Explanation:
We are looking for a policy that will allow or deny traffic from the source interface Port3 and source IP address 10.1.1.10 (LOCAL_CLIENT) to facebook.com TCP port 443 (HTTPS). There are only two policies that will match this traffic, policy ID 2 and 5. In FortiGate, firewall policies are evaluated from top to bottom. This means that the first policy that matches the traffic is applied, and subsequent policies are not evaluated. Based on the Policy Lookup criteria, Policy ID 5 will be highlighted

QUESTION 72
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, which statement about VLAN IDs is true?

A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.

B. The two VLAN subinterfaces must have different VLAN IDs.

C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.

D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

Correct Answer: C, D
Section:

QUESTION 73
Which statement correctly describes the use of reliable logging on FortiGate?

A. Reliable logging is enabled by default in all configuration scenarios.

B. Reliable logging is required to encrypt the transmission of logs.

C. Reliable logging can be configured only using the CLI.

D. Reliable logging prevents the loss of logs when the local disk is full.

Correct Answer: B
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.192): 'if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI.'

QUESTION 74
Refer to the exhibit.
The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.
When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.
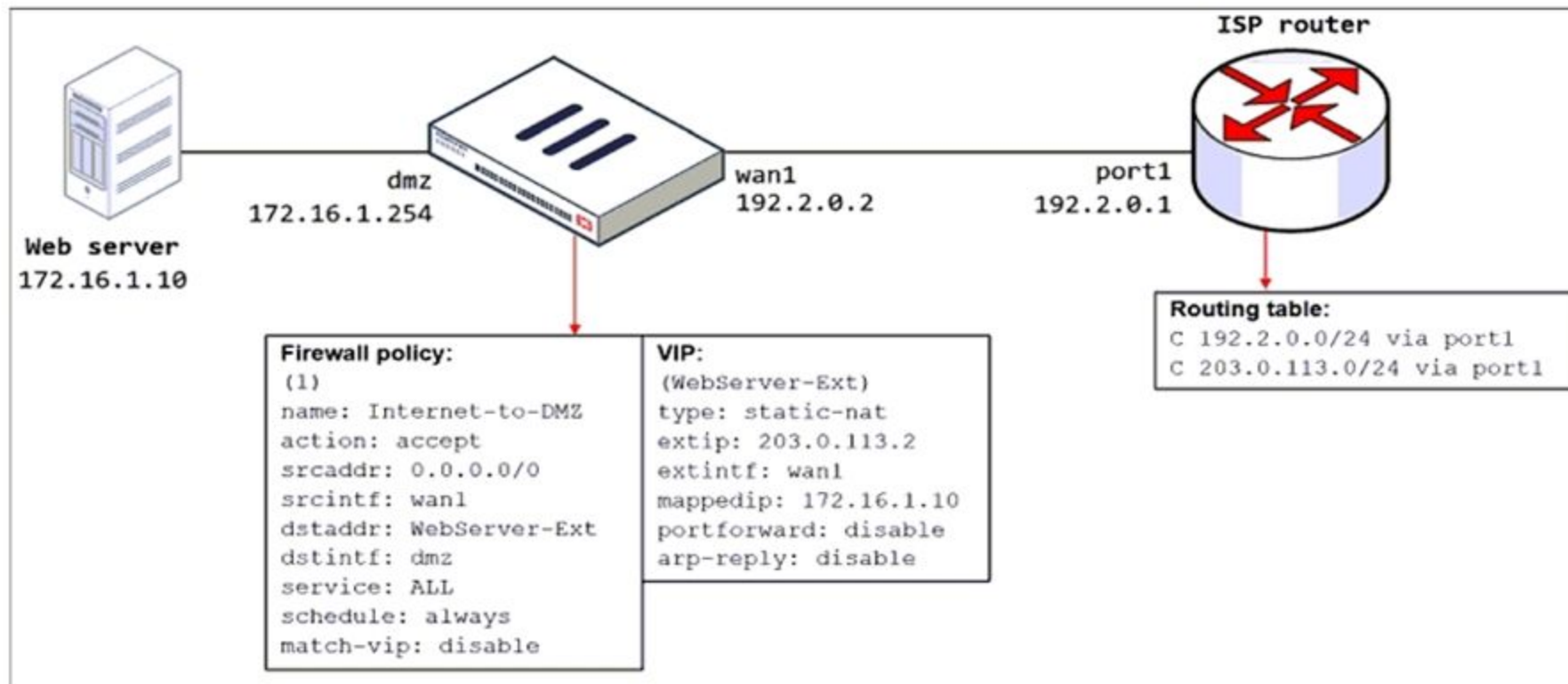
Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

A. Configure a loopback interface with address 203.0.113.2/32.

B. In the VIP configuration, enable arp-reply.

C. Enable port forwarding on the server to map the external service port to the internal service port.

D. In the firewall policy configuration, enable match-vip.

Correct Answer: B
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.115): 'Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled.'

QUESTION 75
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

A. FortiGate uses fewer resources.

B. FortiGate performs a more exhaustive inspection on traffic.

C. FortiGate adds less latency to traffic.

D. FortiGate allocates two sessions per connection.

Correct Answer: A, C
Section:
Explanation:
Flow-based inspection is a type of traffic inspection that is used by some firewall devices, including FortiGate, to analyze network traffic. It is designed to be more efficient and less resource-intensive than proxy-based inspection, and it offers several benefits over this approach.
Two benefits of flow-based inspection compared to proxy-based inspection are:

FortiGate uses fewer resources: Flow-based inspection uses fewer resources than proxy-based inspection, which can help to improve the performance of the firewall device and reduce the impact on overall system performance.

FortiGate adds less latency to traffic: Flow-based inspection adds less latency to traffic than proxy-based inspection, which can be important for real-time applications or other types of traffic that require low latency.

QUESTION 76

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking

B. On the Static URL Filter configuration, set Type to Simple

C. On the Static URL Filter configuration, set Action to Exempt.

D. On the Static URL Filter configuration, set Action to Monitor.

Correct Answer: C
Section:
Explanation:
Based on the exhibit, the administrator has configured the FortiGuard Category Based Filter to block access to all social networking sites, and has also configured a Static URL Filter to block access to twitter.com. As a result, users are being redirected to a block page when they try to access twitter.com. To allow users to access twitter.com while blocking all other social networking sites, the administrator can make the following configuration change: On the Static URL Filter configuration, set Action to Exempt: By setting the Action to Exempt, the administrator can override the block on twitter.com that was specified in the FortiGuard Category Based Filter. This will allow users to access twitter.com, while all other social networking sites will still be blocked.

QUESTION 77
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. hard-timeout

B. auth-on-demand
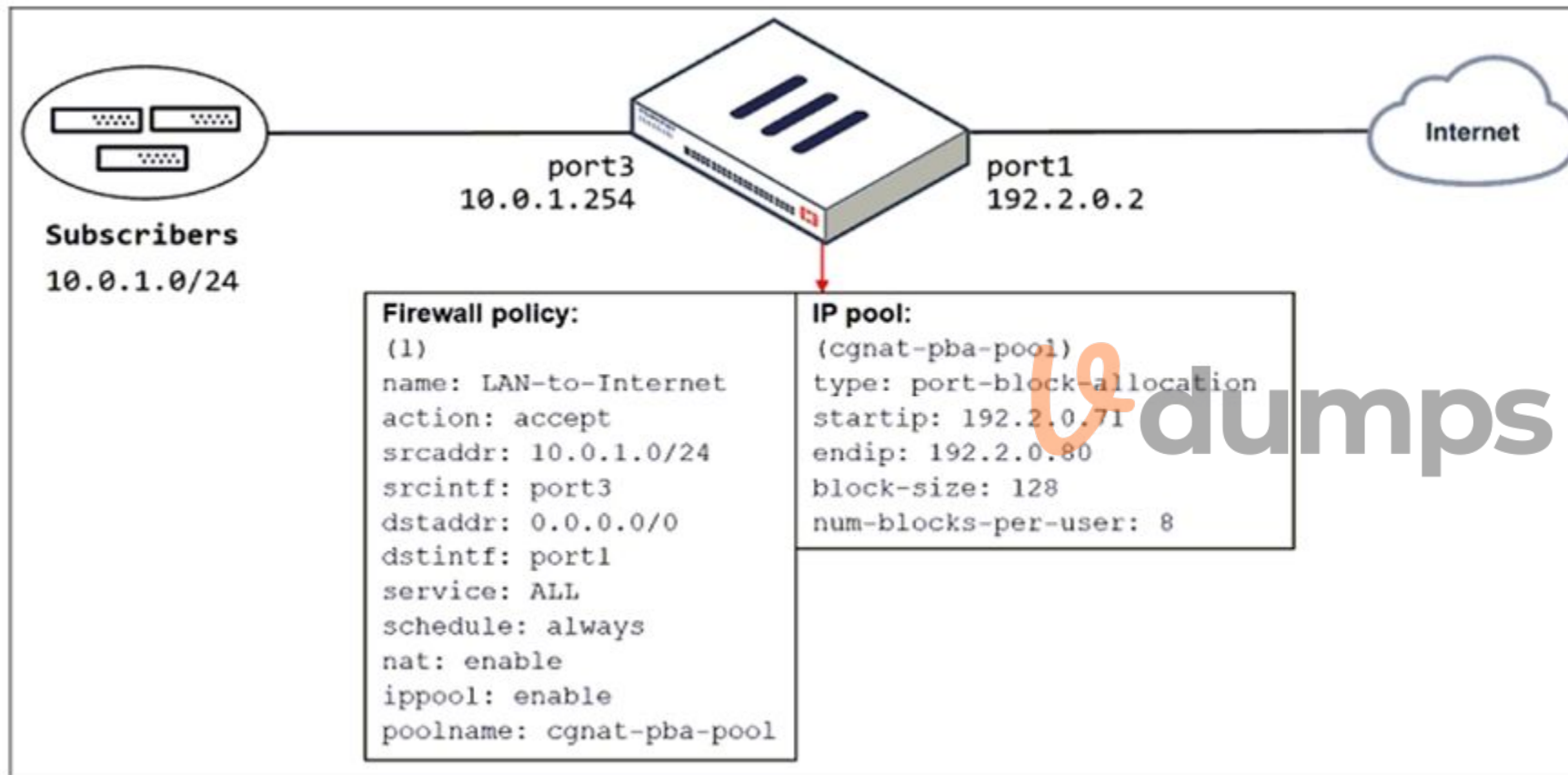
C. soft-timeout

D. new-session

E. Idle-timeout

Correct Answer: A, D, E
Section:

QUESTION 78
Refer to the exhibit.
The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.


```
Subscribers                port3              port1
10.0.1.0/24                10.0.1.254         192.2.0.2
```

```
Firewall policy:                    IP pool:
(1)                                 (cgnat-pba-pool)
name: LAN-to-Internet               type: port-block-allocation
action: accept                      startip: 192.2.0.71
srcaddr: 10.0.1.0/24                endip: 192.2.0.80
srcintf: port3                      block-size: 128
dstaddr: 0.0.0.0/0                  num-blocks-per-user: 8
dstintf: port1
service: ALL
schedule: always
nat: enable
ippool: enable
poolname: cgnat-pba-pool
```

Which two actions does FortiGate take on internet traffic sourced from the subscribers? (Choose two.)

A. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.

B. FortiGate allocates port blocks on a first-come, first-served basis.

C. FortiGate generates a system event log for every port block allocation made per user.

D. FortiGate allocates 128 port blocks per user.

Correct Answer: B, C
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.109): 'FortiGate allocates port blocks on a first-come, first-served basis.' 'For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator.'

QUESTION 79
Which statement about video filtering on FortiGate is true?

A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

B. It does not require a separate FortiGuard license.

C. Full SSL inspection is not required.

D. its available only on a proxy-based firewall policy.

Correct Answer: D
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.279): 'To apply the video filter profile, proxy-based firewall polices currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy.'
https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-categories

QUESTION 80
Which statement describes a characteristic of automation stitches?

A. They can have one or more triggers.

B. They can be run only on devices in the Security Fabric.

C. They can run multiple actions simultaneously.

D. They can be created on any device in the fabric.

Correct Answer: C
Section:
Explanation:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches

QUESTION 81
Refer to the exhibits.
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.
The WAN (port1) interface has the IP address 10.200.1.1/24.
The LAN (port3) interface has the IP address 10.0.1.254/24.

WAN(port1)
10.200.1.1/24

10.200.3.1

10.0.1.10/24
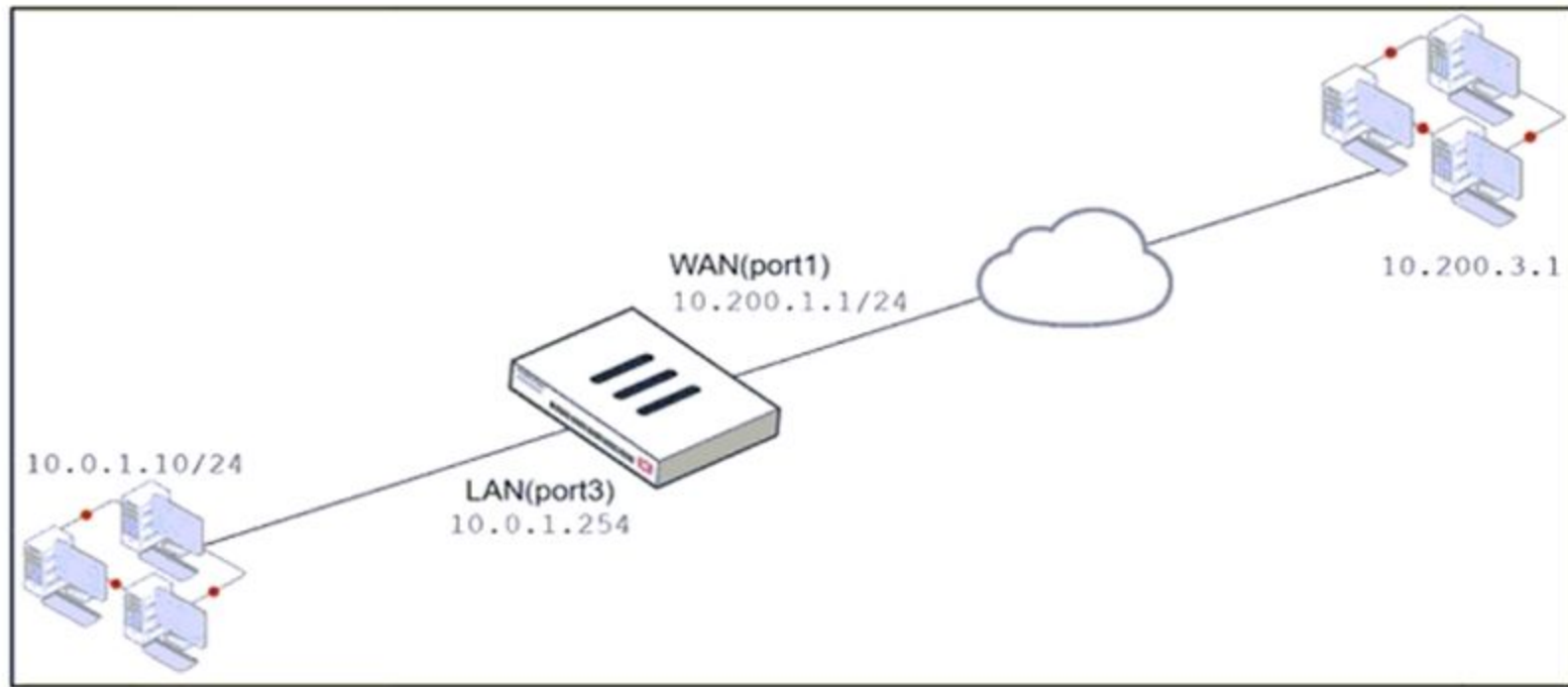
LAN(port3)
10.0.1.254

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type   IPv4

Name   VIP

Comments   Write a comment...   0/255

Color   Change

Network

Interface   WAN (port1)

Type   Static NAT

External IP address/range ❶   10.200.1.10

Map to

IPv4 address/range   10.0.1.10

Optional Filters

Port Forwarding

Protocol   TCP UDP SCTP ICMP

Port Mapping Type   One to one Many to many

External service port ❶   10443

Map to IPv4 port   443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

A. 10.0.1.254, 10.0.1.10, and 443, respectively

B. 10.0.1.254, 10.200.1.10, and 443, respectively

C. 10.200.3.1, 10.0.1.10, and 443, respectively

D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Correct Answer: C
Section:
Explanation:
The host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, which is the external IP address of the VIP object named VIP in Exhibit B1. The VIP object maps the external IP address and port to the internal IP address and port of the server 10.0.1.10 and 443, respectively1. The VIP object also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.
The firewall policy ID 1 in Exhibit B allows traffic from WAN (port1) to LAN (port3) with the destination address of VIP and the service of HTTPS1. The policy also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.
Therefore, after FortiGate forwards the packet to the destination, the source address, destination address, and destination port of the packet will be 10.200.3.1, 10.0.1.10, and 443, respectively.
You can find more information about VIP objects and firewall policies in the Fortinet Documentation

QUESTION 82
Refer to the exhibit.
The exhibit shows the output of a diagnose command.

```
# diagnose firewall proute list

list route policy info(vf=root):

id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff

flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)

oif=3(port1) oif=4(port2)

source(1): 10.0.1.0-10.0.1.255

destination wildcard(1): 0.0.0.0/0.0.0.0

internet service(3): GoToMeeting(4294836966,0,0,0, 16354)

Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)

hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

A. It is an ISDB route in policy route.
B. It is a regular policy route.
C. It is an ISDB policy route with an SDWAN rule.
D. It is an SDWAN rule in policy route.

Correct Answer: D
Section:
Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.59): 'ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the vwl_service field, and ISDB route entries don't.'

QUESTION 83
Refer to the exhibit.
A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, which configuration change will bring phase 2 up?

A. On Remote-FortiGate, set Seconds to 43200.
B. On HQ-FortiGate, set Encryption to AES256.
C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
D. On HQ-FortiGate, enable Auto-negotiate.

Correct Answer: B
Section:

QUESTION 84
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.
What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.
B. It uses UDP 53.

C. It uses DNS over HTTPS.

D. It uses DNS overTLS.

Correct Answer: D
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.15): 'When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic.'
When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic1. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol2. This prevents eavesdropping, tampering, and spoofing of DNS data by third parties.
The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net1. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration1.

QUESTION 85
Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

B. The RPF check is run on the first sent and reply packet of any new session.

C. The RPF check is run on the first sent packet of any new session.

D. The RPF check is run on the first reply packet of any new session.

Correct Answer: A, C
Section:
Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.41): 'The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table.' 'FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session.'
A) The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks1
C) The RPF check is run on the first sent packet of any new session.
This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance2

QUESTION 86
What is a reason for triggering IPS fail open?

A. The IPS socket buffer is full and the IPS engine cannot process additional packets.

B. The IPS engine cannot decode a packet.

C. The IPS engine is upgraded.

D. The administrator enabled NTurbo acceleration.

Correct Answer: A
Section:

QUESTION 87
How can you disable RPF checking?

A. Disable strict-src-check under system settings.

B. Disable src-check on the interface level settings

C. Unset fail-alert-interfaces on the interface level settings.

D. Disable fail-detect on the interface level settings.

Correct Answer: B
Section:

QUESTION 88
What are two features of the NGFW policy-based mode? (Choose two.)

A. NGFW policy-based mode does not require the use of central source NAT policy.

B. NGFW policy-based mode can only be applied globally and not on individual VDOMs_

C. NGFW policy-based mode policies support only flow inspection.

D. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy

Correct Answer: C, D
Section:
Explanation:
C) NGFW policy-based mode policies support only flow inspection. This is correct.This is a feature of the NGFW policy-based mode, according to the Fortinet documentation 'Profile-based NGFW vs policy-based NGFW'1. The documentation states that ''In policy-based NGFW mode, you can only select flow inspection. Proxy inspection is not supported.''
D) NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy. This is correct.This is a feature of the NGFW policy-based mode, according to the Fortinet documentation 'Profile-based NGFW vs policy-based NGFW'1. The documentation states that ''In policy-based NGFW mode, you allow applications and URL categories to be used directly in security policies, without requiring web filter or application control profiles.''

QUESTION 89
Refer to the exhibit.
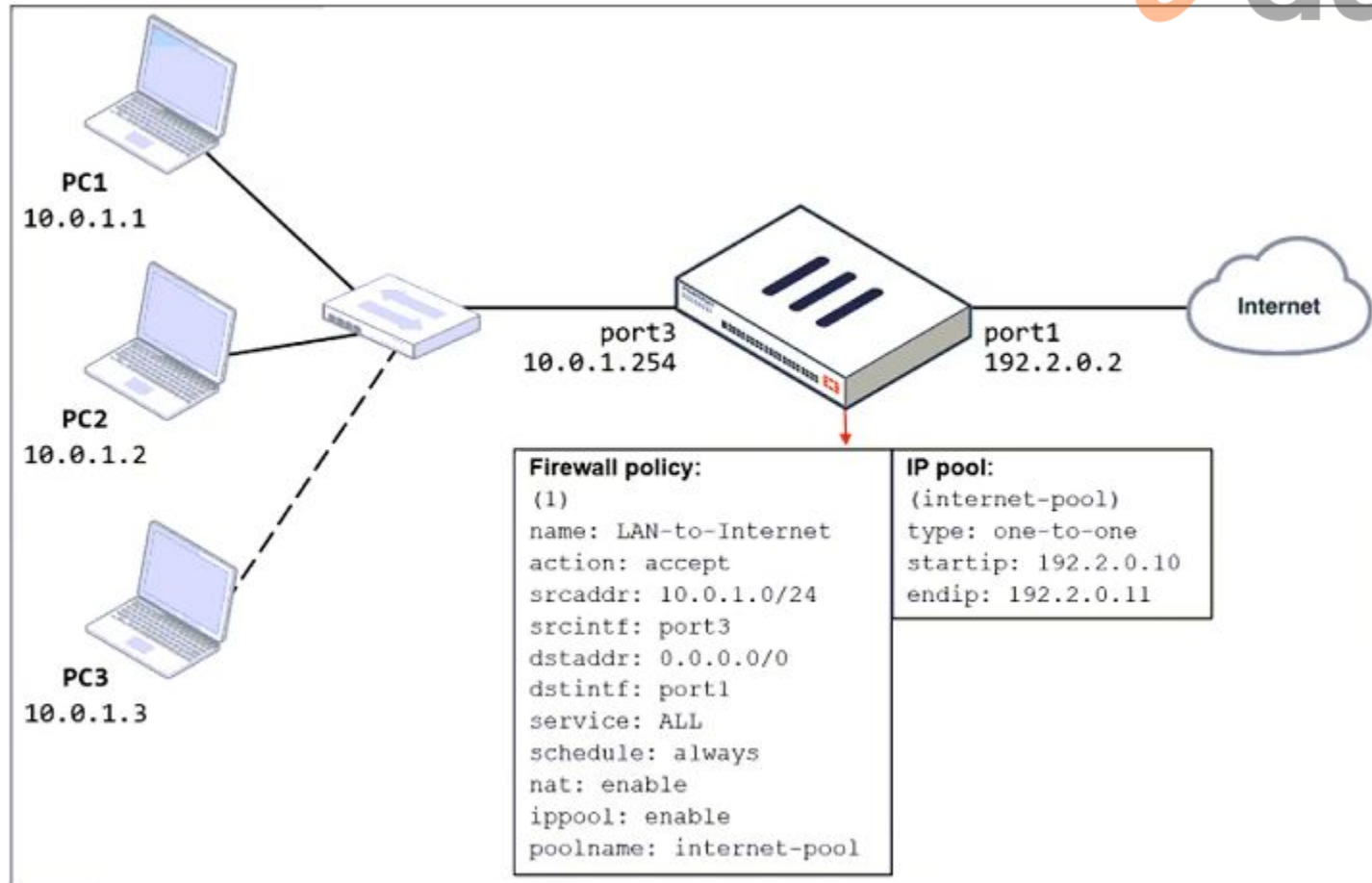
The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.

Two PCS, PCI and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the Intarnet_

Based on the information shown in the exhibit, which three configuration changes should the administrator make to fix the connectivity issue for PC3? (Choose three.)

A. In the IP pool configuration, set type to overload.

B. Configure 192.2. O. 12/24 as the secondary IP address on port1

C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.

D. In the IP pool configuration, set endip to 192.2. O .12

E. In the firewall policy configuration, disable ippool.

Correct Answer: A, D, E
Section:

QUESTION 90
What are two scanning techniques supported by FortiGate? (Choose two.)

A. Machine learning scan

B. Antivirus scan

C. Ransomware scan

D. Trojan scan

Correct Answer: A, B
Section:
Explanation:
FortiGate Security 7.2 Study Guide (p.341):
'Like viruses, which use many methods to avoid detection, FortiGate uses many techniques to detect viruses. These detection techniques include:
* Antivirus scan
* Grayware scan
* Machine learning (AI) scan
If all antivirus features are enabled, FortiGate applies the following scanning order: antivirus scan, followed by grayware scan, followed by AI scan.'