DUMPSBOSS.

Fortinet NSE 4 - FortiOS 7.2

Fortinet NSE4_FGT-7.2

Version Demo

Total Demo Questions: 17

Total Premium Questions: 172

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment and System Configuration	28
Topic 2, Firewall Policies and Authentication	50
Topic 3, Content Inspection	36
Topic 4, Routing	19
Topic 5, VPN	23
Topic 6, High Availability	8
Topic 7, Security Fabric	8
Total	172

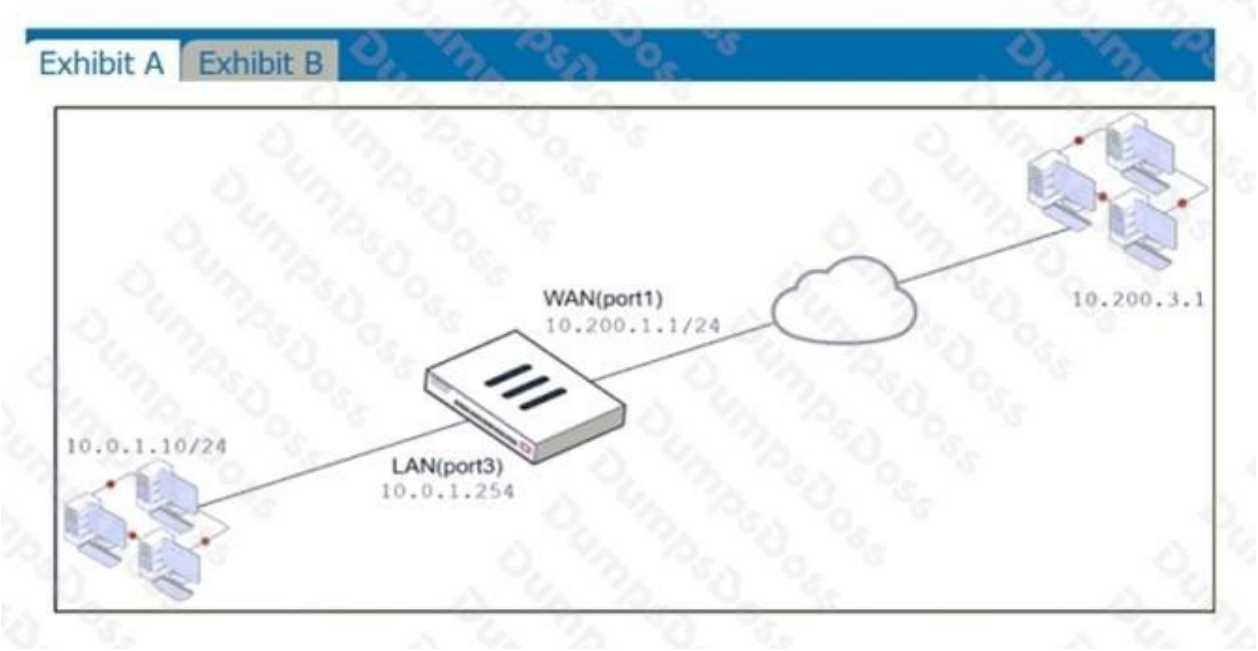
QUESTION NO: 1

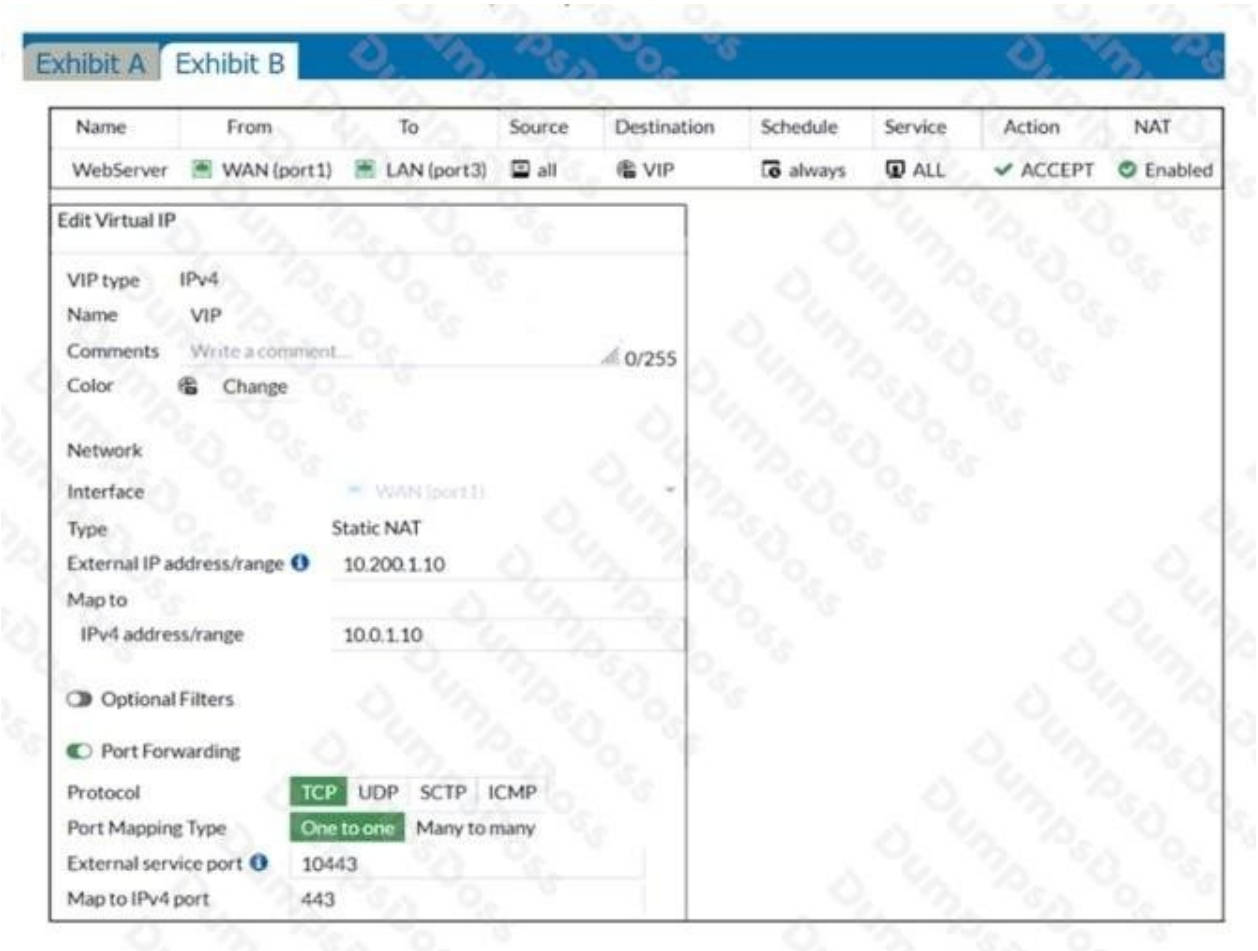
Refer to the exhibits.

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.





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, 10.0.1.10, and 10443, respectively

C. 10.200.3.1, 10.0.1.10, and 443, respectively

ANSWER: C

Explanation:

The packet forwarded to the internal server has source address 10.200.3.1, destination address 10.0.1.10, and destination port 443, respectively. The virtual IP object performs destination NAT for traffic addressed to its external address, 10.200.1.10. Its port-forwarding configuration also translates the received TCP destination port, 10443, to the mapped server port, 443. Therefore, the internal web server receives a connection addressed directly to 10.0.1.10:443.

The original client source address is retained because source NAT is not enabled in the inbound firewall policy shown in the exhibit. VIP processing changes the destination information; it does not inherently replace the initiating client address. Retaining that source address allows the internal server to identify the actual external client, while FortiGate maintains the session state and applies the reverse translation to return traffic. This is the normal behavior for a published service using a VIP with port forwarding when the policy does not apply NAT. Fortinet documents VIP objects and their external-to-mapped address translation at FortiGate Administration Guide: Virtual IP addresses. Additional NAT behavior and policy processing are described in the FortiGate Administration Guide: Central SNAT.

QUESTION NO: 2

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

ANSWER: C

Explanation:

Local traffic logs record traffic that is destined for, or originated by, the FortiGate itself rather than traffic merely passing through it. This includes administrative and management-plane communications involving a FortiGate interface IP address, such as an administrator connecting to the FortiGate using HTTPS or SSH, DNS requests sent by the FortiGate, NTP synchronization, routing-protocol communications, and FortiGuard connectivity. Therefore, traffic directly to and from FortiGate management IP addresses is classified and logged as local traffic.

FortiOS distinguishes this traffic from transit traffic because the FortiGate is the endpoint of the session. Local traffic logging is useful when auditing administrative access, troubleshooting services that the FortiGate consumes or provides, and monitoring control- and management-plane activity. In the FortiGate GUI, these records are available under Log & Report in the Local Traffic log view, subject to the applicable local logging settings and the selected log destination. Fortinet's administration guidance describes local traffic logs as records for traffic to and from FortiGate interfaces, while the log-message reference documents the local traffic log category and fields used to identify these sessions.

References: FortiGate 7.2 Administration Guide: Logging and reporting; FortiOS 7.2 Log Message Reference: Local traffic logs.

QUESTION NO: 3

16

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning

B. File filter

C. DNS filter

D. Intrusion prevention

E. WinSecLog

ANSWER: A D

Explanation:

Antivirus scanning and intrusion prevention are the additional security-profile capabilities that can be applied to a policy when FortiGate operates in policy-based NGFW mode. In this mode, the policy itself is built around application and web-category matching, so application control and web filtering are configured directly within the policy rather than being attached through the conventional profile-based policy workflow. Antivirus inspection remains available to detect and block malicious content in supported traffic, while an IPS sensor can be applied to inspect traffic for known exploit signatures, protocol anomalies, and attack techniques. Together, these controls extend the policy beyond application and URL/category enforcement by providing payload-malware detection and network-exploit prevention. The relevant policy must use an inspection configuration compatible with the selected features, and SSL/TLS traffic generally requires an appropriate SSL inspection profile for FortiGate to inspect encrypted application content effectively. Fortinet documents policy-based NGFW behavior and the security controls available in this operating mode in the FortiOS 7.2 Administration Guide. Additional configuration guidance for antivirus and IPS is available in Fortinet's FortiGate Administration documentation.

QUESTION NO: 4

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.

ANSWER: D

Explanation:

Interface Pair view will be disabled. The Interface Pair policy-list view organizes firewall policies into rows based on a specific incoming-interface and outgoing-interface combination. This display depends on each policy having an explicitly defined destination interface so that the policy can be placed in the appropriate interface-pair grouping. When a firewall policy uses *any* as its outgoing interface, it does not represent one fixed interface pair. Consequently, FortiOS cannot reliably include that policy in the interface-pair organization, and the policy-list interface-pair view is unavailable. The policy remains valid and can still be evaluated normally by the firewall; this behavior concerns only how policies can be displayed and organized in the graphical policy list. Administrators can use the sequence-based policy view to review policies when broad interface matching is configured. Fortinet documents the available firewall-policy display arrangements and the conditions associated with interface-pair organization in its administration guidance. See the FortiGate 7.2 Administration Guide: Firewall policy and Fortinet's technical tip on unavailable interface-pair policy view.

QUESTION NO: 5

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.

ANSWER: B

Explanation:

It uses UDP 53. When FortiGate is configured to use FortiGuard DNS servers with the default DNS settings, it sends ordinary, clear-text DNS queries to the configured resolver on the standard DNS service port, UDP port 53. This is the conventional transport for DNS lookups and is the default protocol behavior for FortiGate system DNS resolution. FortiGuard DNS server addresses can be selected through the GUI or configured in the CLI as the primary and secondary system DNS servers; selecting those addresses does not, by itself, enable an encrypted DNS transport.

FortiOS supports DNS transport-related configuration in applicable releases and configurations, but such behavior must be explicitly configured where available. Therefore, the default FortiGuard DNS resolver connection remains a standard UDP DNS query on port 53. This DNS resolution is used by the FortiGate itself when it needs to resolve names for services and features that rely on system DNS, subject to normal DNS behavior such as retry or fallback handling when needed. Fortinet's documentation describes configuring FortiGuard servers as system DNS servers and the FortiOS DNS CLI settings at FortiGate 7.2 Administration Guide: DNS and FortiGate 7.2 CLI Reference: config system dns.

QUESTION NO: 6

Refer to the exhibits.

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

A. Administrators can access FortiGate only through the console port.

B. FortiGate has entered conserve mode.

C. FortiGate will start sending all files to FortiSandbox for inspection.

D. Administrators cannot change the configuration.

ANSWER: B D

Explanation:

The system performance output indicates that used memory has reached the configured red memory threshold. With the default FortiGate thresholds, the green threshold is 82%, the red threshold is 88%, and the extreme threshold is 95% of total memory. Reaching the red threshold causes the FortiGate to enter conserve mode. This is a protective operating state intended to preserve sufficient memory for critical system processes when memory pressure is high.

While conserve mode is active, FortiGate restricts operations that could require additional memory. In particular, administrators cannot make configuration changes until memory usage falls below the relevant recovery threshold and the device can leave conserve mode. This protects the appliance from further memory exhaustion and helps it maintain essential traffic-processing and system functions.

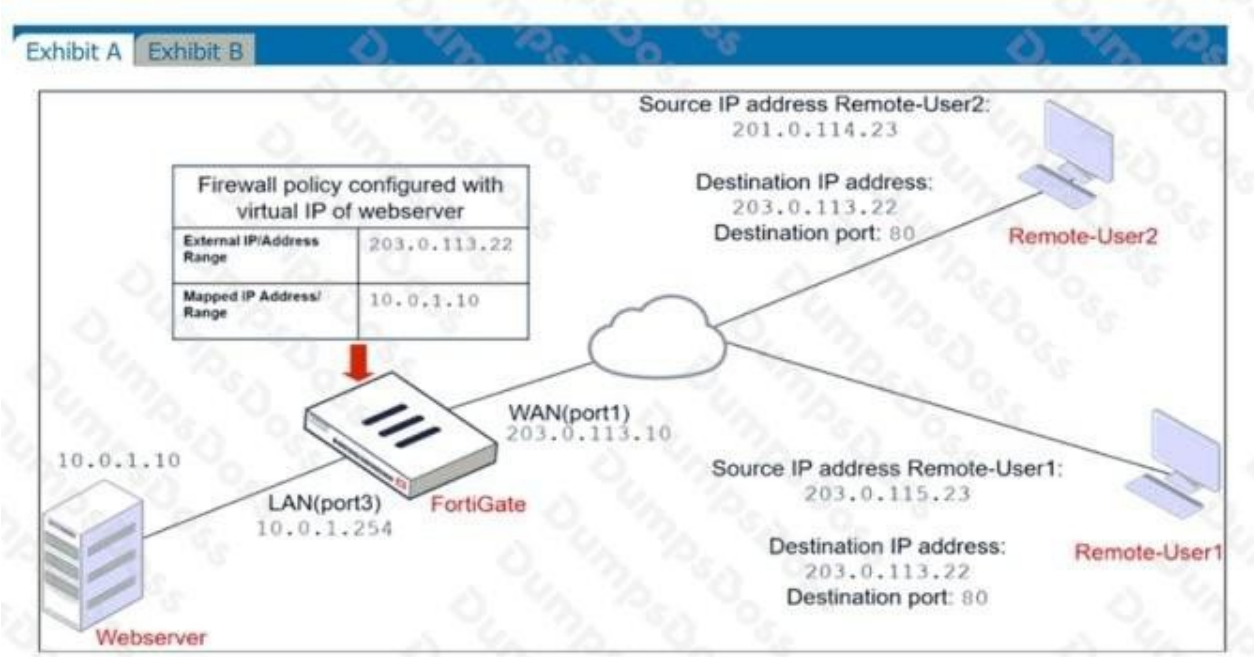
Fortinet documents the default thresholds and conserve-mode behavior in its Technical Tip: Conserve mode changes. Additional operational guidance is available in the FortiOS 7.2 Administration Guide.

QUESTION NO: 7

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.



In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.

B. Set the Destination address as Deny_IP in the Allow-access policy.

C. Enable match vip in the Deny policy.

D. Set the Destination address as Web_server in the Deny policy.

ANSWER: C D

Explanation:

Enabling `match-vip` in the Deny policy makes the policy evaluate traffic addressed to a virtual IP. This is needed when the deny rule uses a broad destination, such as `all`, but the actual incoming connection is addressed to the Webserver VIP's external address. With VIP matching enabled and Remote-User2 defined as the source, the Deny policy can match that user's connection before the permit rule is selected. FortiGate evaluates firewall policies from top to bottom, so the specific deny policy must be positioned above the policy that permits access.

Setting the Deny policy destination to `Web_server` is also valid because it explicitly identifies the VIP associated with the published web service. A policy that directly references the VIP can match traffic sent to that VIP, allowing the administrator to deny only Remote-User2 while retaining the separate allow policy for Remote-User1. This approach is especially clear operationally because the policy destination documents the protected published service rather than relying on a generic destination match. Fortinet describes the VIP and firewall-policy matching behavior in its VIP firewall policy matching technical tip and in the FortiOS 7.2 Administration Guide.

QUESTION NO: 8

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.

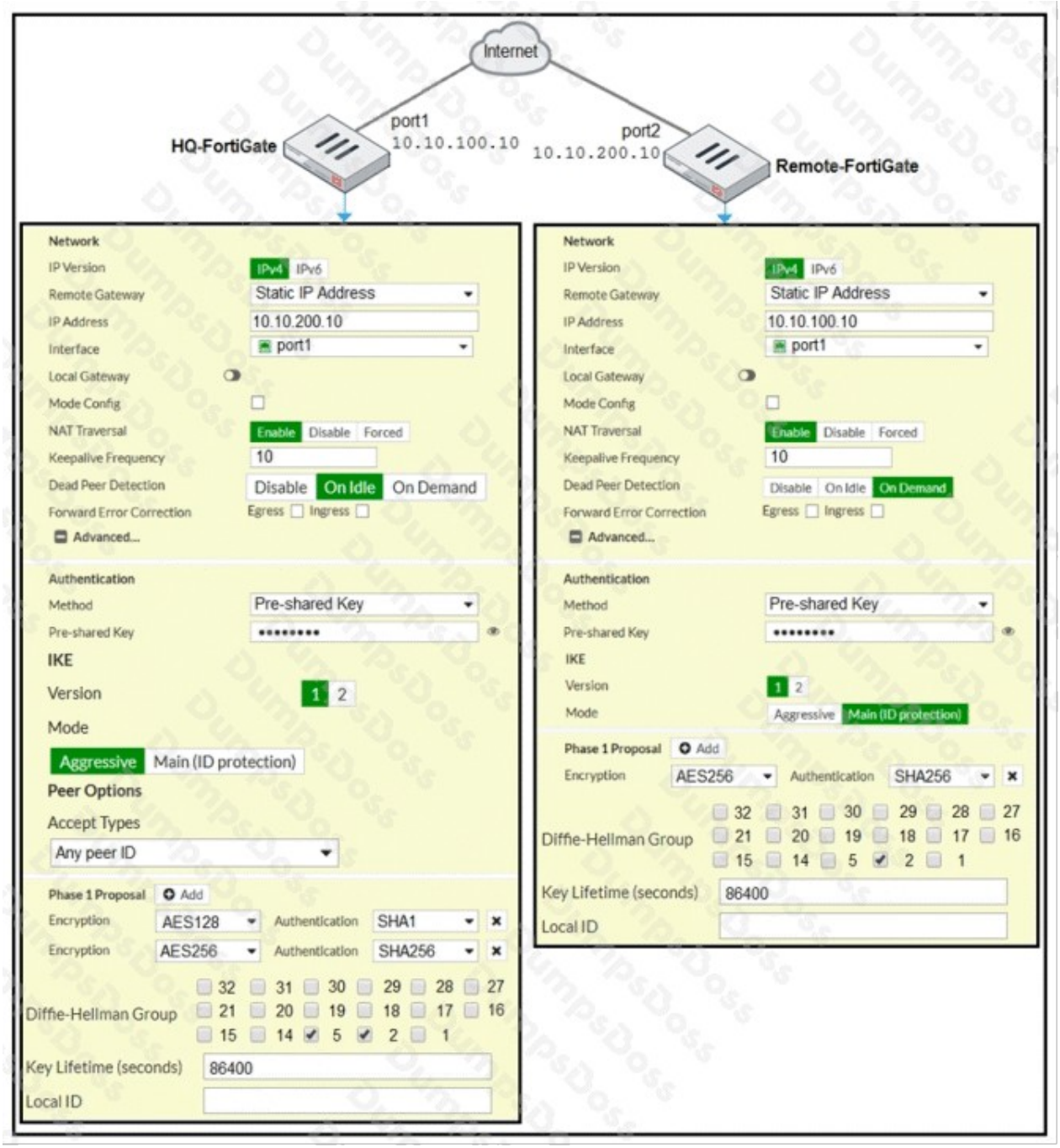
ANSWER: C

Explanation:

It is an ISDB policy route with an SDWAN rule. The diagnostic output identifies a policy route that uses an Internet Service Database (ISDB) entry as its matching destination and associates the route with SD-WAN handling. ISDB objects represent FortiGuard-maintained Internet services rather than conventional IP-prefix destinations. When such an object is used for routing decisions, FortiGate can classify traffic for the identified Internet service and then pass the matching traffic to the applicable SD-WAN rule. The SD-WAN rule determines the preferred member or service path according to its configured strategy and health-check status, while the policy route provides the ISDB-based traffic match. This combination is useful when traffic steering must be based on a recognized cloud or Internet application/service instead of only source and destination addresses. Fortinet documents that ISDB and application matching can be used in SD-WAN rule selection, and that the related route information can be inspected with diagnostic commands. See Fortinet's technical tip on SD-WAN rule matching for ISDB and application IDs and the FortiOS 7.2 SD-WAN administration documentation.

QUESTION NO: 9

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.



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.

ANSWER: A D

Explanation:

Phase 1 requires both peers to negotiate compatible IKE settings and to use the correct local interface for the configured peer relationship. Setting IKE mode to Main (ID protection) on HQ-FortiGate aligns the IKE negotiation mode with the remote peer. Main mode performs the IKE phase 1 exchange using identity protection and must match the peer's configured

negotiation mode for the exchange to proceed successfully. Once both peers use Main mode, they can continue negotiating the configured authentication, encryption, integrity, and Diffie-Hellman parameters.

Setting port2 as Interface on Remote-FortiGate ensures that the phase 1 configuration is bound to the interface that is actually connected toward HQ-FortiGate. The interface selected in a route-based IPsec phase 1 definition identifies the local network interface through which IKE packets are sourced and received. Selecting the interface shown as the remote device's path to the peer allows the IKE security association negotiation to reach the correct endpoint and establish phase 1. FortiGate documents the phase 1 interface setting and IKE mode as core parameters of an IPsec phase 1 configuration in the FortiOS 7.2 CLI Reference and the FortiOS 7.2 IPsec VPN administration guidance.

QUESTION NO: 10

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.

E. Reliable logging preserves pending logs and retransmits them to FortiAnalyzer when delivery resumes.

ANSWER: E

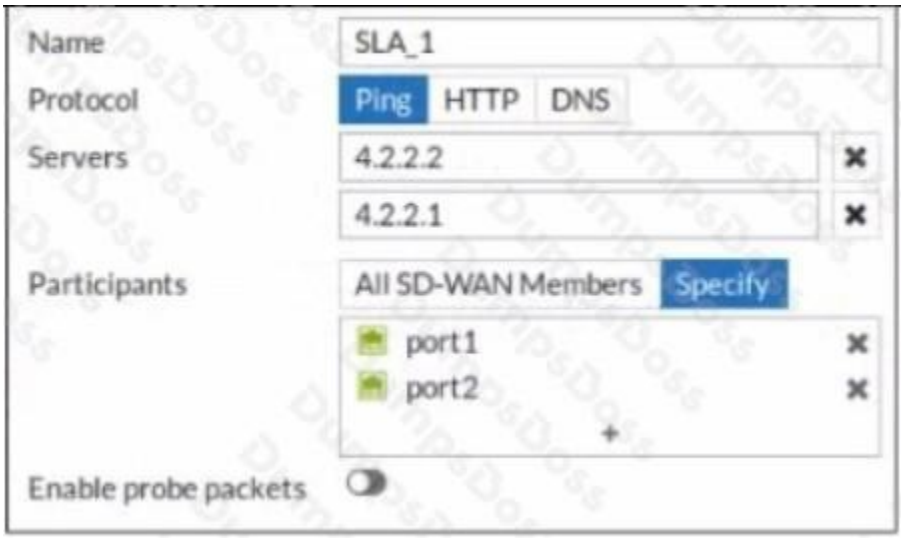
Explanation:

Reliable logging ensures more dependable delivery of logs to FortiAnalyzer. When this feature is enabled for the FortiAnalyzer logging destination, FortiGate retains log data that has not been successfully delivered and retransmits it when communication is restored or delivery can continue. This protects the continuity of the remote logging stream during temporary connectivity or FortiAnalyzer availability issues, rather than treating logging as a best-effort transmission. The feature is configured in the FortiAnalyzer logging settings, where the `reliable` setting enables reliable log delivery behavior. It is particularly useful when FortiAnalyzer is the central system of record for operational monitoring, incident investigation, reporting, and compliance, because gaps caused by transient transport failures can materially reduce the value of collected logs. Reliable logging is therefore about preserving and delivering pending remote logs to FortiAnalyzer; it is not a disk-capacity feature. Administrators should also ensure that the FortiGate has appropriate local storage and logging capacity, because retention and buffering requirements depend on log volume and the duration of any outage. See the FortiOS 7.2 Administration Guide and the FortiOS 7.2 CLI Reference for FortiAnalyzer logging configuration and the reliable logging setting.

QUESTION NO: 11

17

Refer to the exhibit.



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.

ANSWER: B D

Explanation:

FortiGate can send active health-check probes for a performance SLA only when probe packets are enabled. Enabling this setting instructs the SLA to originate synthetic traffic, such as ICMP echo requests or the selected protocol probes, toward the configured health-check servers. Therefore, if *Enable probe packets* is not enabled, the SLA will not generate probe traffic to 4.2.2.2 or 4.2.2.1.

In addition, each SD-WAN member participating in the health check needs a usable next-hop gateway. FortiGate uses that gateway to resolve the forwarding path and transmit probes through the applicable member interface. If no gateway is configured for a member, or if its configured gateway is invalid or unreachable, FortiGate cannot establish a valid egress path for the SLA probes on that member. Configuring valid member gateways and enabling probe packets allows FortiGate to actively measure latency, jitter, and packet loss against the specified servers. Fortinet documents SD-WAN health checks and performance SLAs in the FortiOS 7.2 Administration Guide and the associated configuration commands in the FortiOS 7.2 CLI Reference.

QUESTION NO: 12

Which two statements are correct about firewall schedules on FortiGate? (Choose two.)

A. A recurring schedule can specify days of the week and a time period.

B. A one-time schedule can specify a defined start and end date.

C. A schedule can be applied only to an IPsec VPN interface.

D. A policy with an inactive schedule continues to match new sessions.

ANSWER: A B

Explanation:

A recurring schedule can define selected days of the week and a time period during which a firewall policy is active. This is appropriate for access rules that must repeat on a regular timetable, such as allowing a contractor group access during business hours.

A one-time schedule defines a specific start and end date and time. After its configured end time, a policy using that schedule no longer matches traffic. Schedules are evaluated as part of firewall-policy matching, along with interfaces, addresses, services, and other policy criteria. Fortinet documents schedule types and their use in policies in the FortiOS 7.2 Administration Guide: Firewall schedules.

QUESTION NO: 13

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.

ANSWER: A D

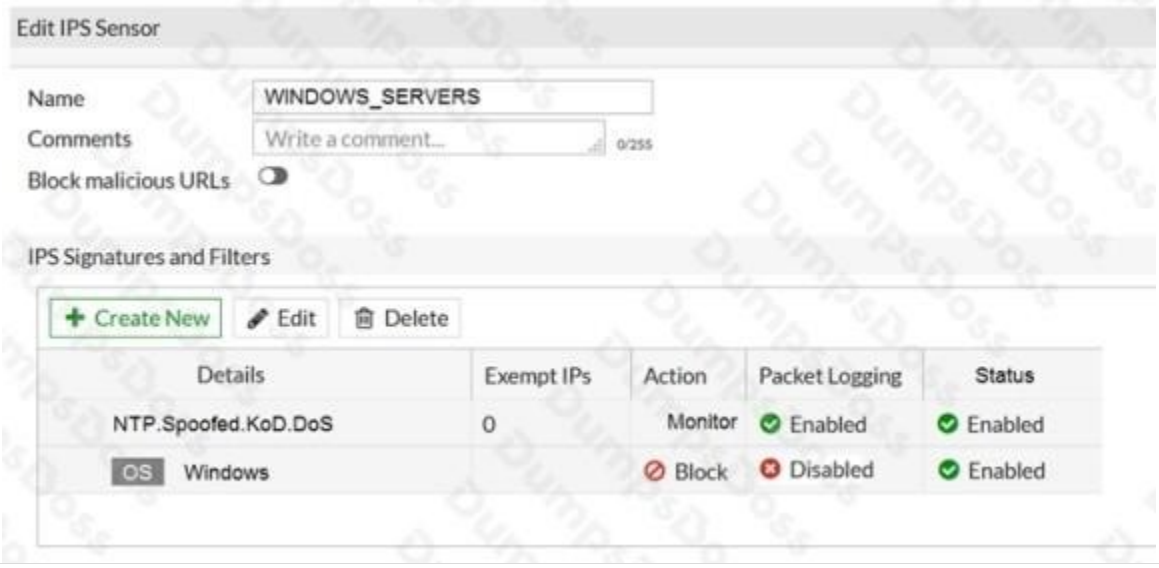
Explanation:

For SSL deep inspection, FortiGate dynamically generates substitute server certificates for inspected TLS sessions and signs those certificates with the configured inspection certificate. Therefore, that certificate must be authorized to operate as a certificate authority. The **CA extension must be set to TRUE**, formally the Basic Constraints extension with `cA=TRUE`, identifies the certificate as eligible to issue and sign other certificates. This establishes the certificate's certificate-authority role in the validation chain.

The **keyUsage extension must be set to keyCertSign** because Key Usage defines the cryptographic operations for which a certificate's public key is permitted. The `keyCertSign` usage specifically authorizes signing certificates. Together, Basic Constraints and Key Usage ensure that the certificate FortiGate uses for SSL inspection is structurally and cryptographically valid for signing the generated replacement certificates presented to clients. Clients must also trust the corresponding FortiGate inspection CA certificate for browsers and applications to accept those re-signed connections without certificate warnings. Fortinet documents SSL inspection certificate configuration in the FortiOS Administration Guide; the X.509 extension requirements are defined in RFC 5280.

QUESTION NO: 14

Refer to the exhibit.



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.

ANSWER: A B

Explanation:

The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature because that signature has an explicit *pass* action in the IPS sensor. A directly configured signature entry takes precedence over a broader IPS filter that could also select the same signature. Therefore, traffic identified by that specific signature is permitted rather than receiving the filter's blocking action.

The sensor will block all attacks aimed at Windows servers because the configured IPS filter selects signatures whose target operating system is Windows and assigns them the *block* action. FortiGate IPS filters use signature attributes, including the target OS, to select a set of IPS signatures and apply the configured action to matching detected traffic. The specific iSCSI signature remains governed by its explicit pass entry, while the Windows-targeted signatures selected by the filter are handled using block. This configuration lets an administrator broadly prevent detected attacks against Windows systems while retaining a deliberate exception for a particular signature. Fortinet documents IPS sensor signature overrides and filters in the FortiGate 7.2 IPS administration guide and the available IPS actions in the FortiOS IPS sensor CLI reference.

QUESTION NO: 15

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.

ANSWER: C

Explanation:

By default, split tunneling is enabled for the standard `full-access` SSL VPN portal configuration. Split tunneling determines which client traffic is sent through the SSL VPN tunnel after a user connects. When it is enabled, FortiGate uses the configured split-tunneling routing destinations to decide what traffic enters the tunnel; traffic not matching those destinations continues to use the client's local network connection. This allows administrators to limit VPN-tunneled traffic to corporate networks and services that actually require access through FortiGate, rather than automatically forwarding every destination through the VPN.

The portal's split-tunneling behavior can be adjusted in the GUI or with the portal CLI configuration, including selecting the routing addresses and choosing the applicable routing-address source. Administrators should review these destinations carefully because they define the traffic scope protected and inspected through the remote-access VPN. Fortinet documents split tunneling as a portal-level SSL VPN setting and describes the default portal profiles, including `full-access`, in its SSL VPN administration guidance. See the FortiGate 7.2 SSL VPN documentation and the SSL VPN portals documentation.

QUESTION NO: 16

74

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface

B. Software Switch interface

C. Aggregate interface

D. Redundant interface

ANSWER: C

Explanation:

Aggregate interface is correct because it combines multiple physical FortiGate interfaces into one logical link by using link aggregation. This is commonly implemented with the IEEE 802.3ad Link Aggregation Control Protocol (LACP), although static aggregation modes are also available when appropriate. The logical aggregate interface can then be used in firewall policies, routing, and other FortiGate configuration areas as a single interface.

An aggregate provides both requested outcomes. It can increase available bandwidth by distributing eligible traffic flows across the member links according to the configured load-balancing algorithm. It also provides link resiliency: if an individual member link fails while other member links remain operational, the aggregate interface stays available and traffic can continue over the remaining links. For end-to-end operation, the connected switch must be configured with a matching link-aggregation group and compatible LACP or static settings.

FortiOS exposes aggregation settings under interface configuration, including the aggregation type, member interfaces, LACP mode, and load-balancing behavior. See the Fortinet FortiGate 7.2 Administration Guide and the FortiOS interface CLI reference for interface and aggregate configuration details.

QUESTION NO: 17

An administrator creates multiple SD-WAN rules that can match the same traffic.

How does FortiGate select an SD-WAN rule?

A. FortiGate uses the first matching SD-WAN rule in the configured sequence.

B. FortiGate uses the matching rule with the lowest rule ID.

C. FortiGate evaluates all matching rules and combines their members.

D. FortiGate always selects the rule with the lowest measured latency.

ANSWER: A

Explanation:

FortiGate evaluates SD-WAN rules in their configured sequence and uses the first rule whose matching criteria apply to the traffic. After a rule is selected, FortiGate uses that rule's configured strategy, members, and any associated Performance SLA requirements to select an eligible path.

Rule order is therefore important. A broad rule positioned before a more specific rule can match the traffic first and prevent the later rule from being evaluated. Fortinet describes SD-WAN rule matching and rule ordering in the FortiOS 7.2 Administration Guide: SD-WAN.