PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7 - SD-WAN 6.4.5

Fortinet NSE7_SDW-6.4

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, SD-WAN Configuration	11
Topic 2, SD-WAN Rules	16
Topic 3, Performance SLA	9
Topic 4, SD-WAN Diagnostics	12
Topic 5, SD-WAN and IPsec	24
Topic 6, SD-WAN and BGP	6
Topic 7, SD-WAN Deployment	9
Topic 8, Mix Questions	13
Total	100

QUESTION NO: 1

Refer to exhibits.

Exhibit A | Exhibit B

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Google.ICMP	all	Google-ICMP	Latency	port1, port2
2	Vimeo	all	Vimeo		port2
3	All_Access_Rules	all	all		port1
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

Exhibit A | Exhibit B

Add Filter | Details

Date/Time	Source	Destination	Application Name	Result	Policy	Destination Interface
2020/10/15 11:12:27	10.0.1.10	151.101.250.109 (i.vimeocdn.com)	Vimeo	UTM Allowed	Internet Access (1)	port2
2020/10/15 11:12:22	10.0.1.10	34.120.15.67 (fresnel-events.vimeocdn.com)	Vimeo	2.00 kB / 4.33 kB	Internet Access (1)	port1
2020/10/15 11:12:20	10.0.1.10	172.217.13.227 (ocsp.pki.goog)	OCSP	1.28 kB / 1.49 kB	Internet Access (1)	port1
2020/10/15 11:12:07	10.0.1.10	23.47.205.151 (detectportal.firefox.com)	HTTP.BROWSER_Firefox	1.44 kB / 1.55 kB	Internet Access (1)	port1
2020/10/15 11:12:07	10.0.1.10	23.47.205.151 (detectportal.firefox.com)	HTTP.BROWSER_Firefox	1.43 kB / 1.60 kB	Internet Access (1)	port1
2020/10/15 11:12:04	10.0.1.10	99.84.221.62 (snippets.cdn.mozilla.net)	HTTPS.BROWSER	2.08 kB / 13.44 kB	Internet Access (1)	port1

Exhibit A shows the SD-WAN rules and exhibit B shows the traffic logs. The SD-WAN traffic logs reflect how FortiGate processed traffic.

Which two statements about how the configured SD-WAN rules are processing traffic are true? (Choose two.)

A. The implicit rule overrides all other rules because parameters widely cover sources and destinations.

B. SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom.

C. The All_Access_Rules rule load balances Vimeo application traffic among SD-WAN member interfaces.

D. The initial session of an application goes through a learning phase in order to apply the correct rule.

ANSWER: B D

Explanation:

“SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom” is correct because FortiGate processes SD-WAN rules in their configured sequence. For a new session, FortiGate selects the first SD-WAN rule whose match criteria apply, then uses that rule’s configured strategy and eligible members to steer the traffic. Rule ordering is therefore important whenever rules have overlapping source, destination, application, service, or Internet-service criteria. Fortinet documents this ordered rule-processing model and the role of the implicit SD-WAN rule after configured rules in its SD-WAN rules documentation.

“The initial session of an application goes through a learning phase in order to apply the correct rule.” is also correct when application-based matching is configured. Application identification depends on traffic inspection and can require the session’s initial packets to be classified before FortiGate can associate the traffic with the intended application signature. During this learning period, traffic is handled according to the applicable preliminary rule processing; once the application is identified, FortiGate can apply the SD-WAN rule that matches the recognized application. This behavior is central to application-aware SD-WAN steering and is described in Fortinet’s application steering guidance.

QUESTION NO: 2

Which statement about using BGP routes in SD-WAN is true?

A. Adding static routes must be enabled on all ADVPN interfaces.

B. VPN topologies must be form using only BGP dynamic routing with SD-WAN

C. Learned routes can be used as dynamic destinations in SD-WAN rules

D. Dynamic routing protocols can be used only with non-encrypted traffic

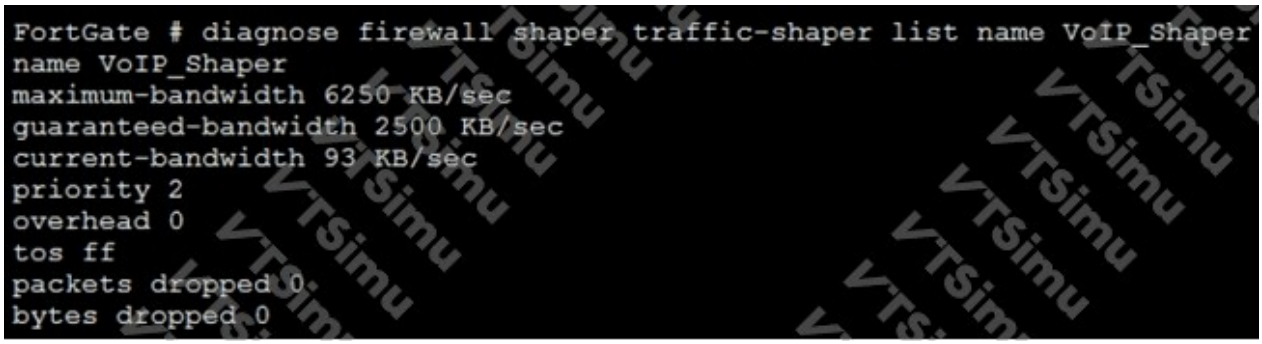
ANSWER: C

Explanation:

Learned routes can be used as dynamic destinations in SD-WAN rules. FortiGate can receive prefixes through BGP and install the selected paths in its routing table. SD-WAN uses this routing information when evaluating traffic, allowing policies to match destinations that are dynamically learned rather than requiring every remote network to be maintained manually as a static address object or static route. This is especially useful in large hub-and-spoke or ADVPN deployments, where new branch prefixes, cloud prefixes, or remote-site networks can be advertised and withdrawn through BGP. When a learned prefix is present, traffic for that prefix can be steered according to the applicable SD-WAN service rule and the health or SLA status of eligible SD-WAN members. If the BGP route is withdrawn or a better route is selected, FortiGate updates its forwarding decision accordingly. This combines BGP's scalable route distribution with SD-WAN's application-aware path selection and performance-based steering. Fortinet documents BGP as a supported dynamic-routing mechanism for overlay VPN and SD-WAN designs; see the FortiOS 6.4.5 Administration Guide and Fortinet's SD-WAN deployment documentation.

QUESTION NO: 3

Refer to the exhibit.



Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

A. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.

B. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

C. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.

D. The measured bandwidth is less than 100 KBps.

ANSWER: A D

Explanation:

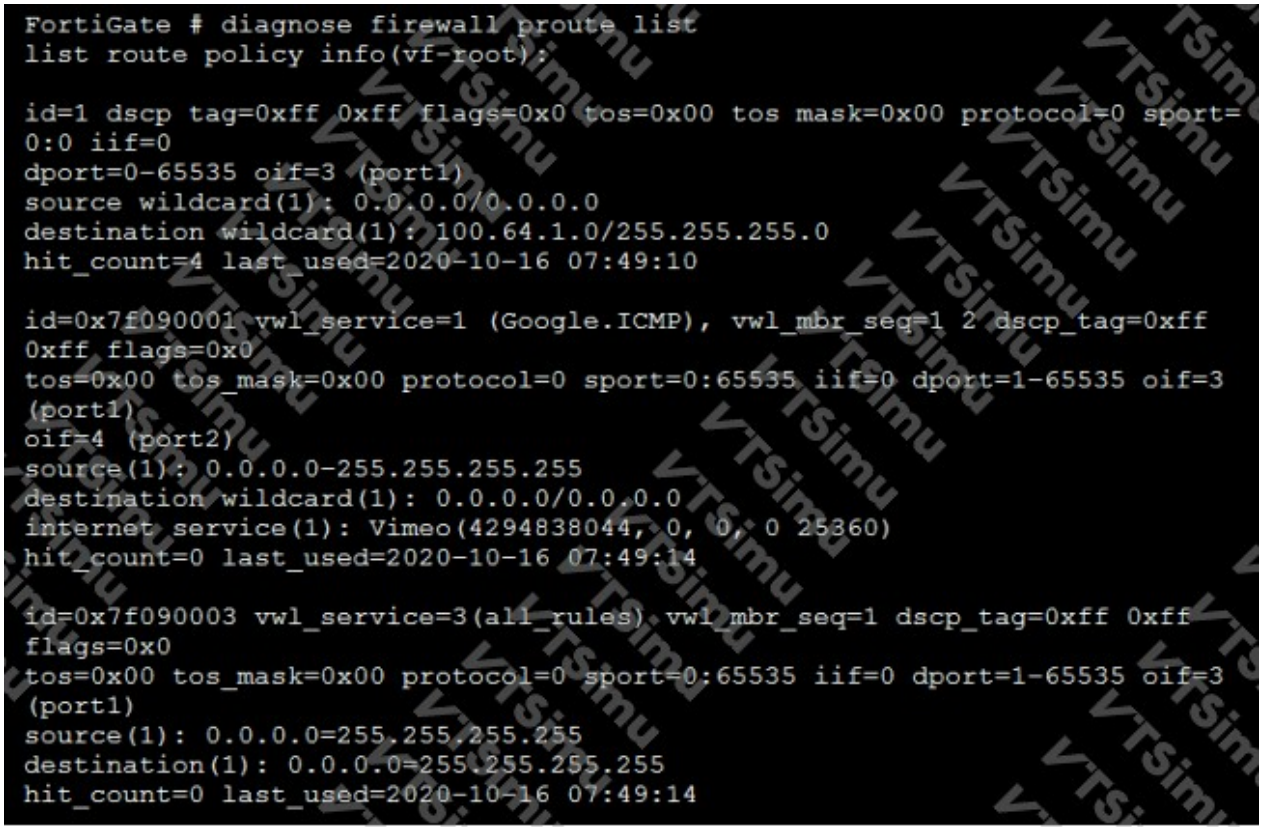
The traffic shaper drops packets if the bandwidth exceeds 6250 KBps. A traffic shaper's maximum-bandwidth setting is the upper throughput limit applied to traffic matching the related shaping policy. When matching traffic reaches that configured ceiling, FortiGate enforces the limit; traffic beyond the available shaped rate is not forwarded immediately and may be dropped when it cannot be queued. The exhibit's configured maximum of 6250 KBps therefore establishes the relevant maximum bandwidth threshold for the matched traffic.

The measured bandwidth is less than 100 KBps. The traffic-shaper monitoring information in the exhibit shows the current measured rate below the 100 KBps mark. This is a measurement of the actual traffic presently matching the shaper, not a replacement for its configured guaranteed or maximum bandwidth parameters. FortiGate exposes both configured shaping values and real-time traffic measurements so administrators can verify whether a shaper is actively approaching its configured limit.

Fortinet documents traffic-shaping concepts, including the use of maximum and guaranteed bandwidth values, in the FortiOS 6.4 Administration Guide. Additional configuration and operational guidance is available through the FortiGate 6.4 documentation portal.

QUESTION NO: 4

Refer to the exhibit.



Based on the output, which two conclusions are true? (Choose two.)

A. The all_rules rule represents the implicit SD-WAN rule.

B. There is more than one SD-WAN rule configured.

C. Entry 1 (id=1) is a regular policy route.

D. The SD-WAN rules takes precedence over regular policy routes.

ANSWER: B C

Explanation:

The output indicates that more than one SD-WAN rule is configured because it contains separate SD-WAN rule entries, including the catch-all rule entry and another explicitly defined rule. FortiGate evaluates SD-WAN rules to select an appropriate member according to the configured traffic-matching and service criteria. The presence of distinct rule records in this diagnostic output is therefore evidence of multiple configured SD-WAN rules, rather than a single rule with multiple members.

Entry 1, identified as `id=1`, is a regular policy route. In FortiGate diagnostic policy-route output, regular policy routes and SD-WAN-related generated routing entries can be displayed together. The entry's identification and displayed route characteristics distinguish it as a conventional policy-route record. This is useful when troubleshooting forwarding decisions, because policy routes can influence the lookup process alongside routes associated with SD-WAN configuration. Fortinet's SD-WAN documentation describes how SD-WAN rules steer matching traffic through selected members, while the policy-route documentation describes policy-based forwarding and its diagnostic visibility. See the FortiGate SD-WAN rules documentation and the FortiGate policy routes documentation.

QUESTION NO: 5

Which statement about using BGP routes in SD-WAN is true?

A. Learned routes can be used as dynamic destinations in SD-WAN rules.

B. You must use BGP to route traffic for both overlay and underlay links.

C. You must configure AS path prepending.

D. You must use external BGP.

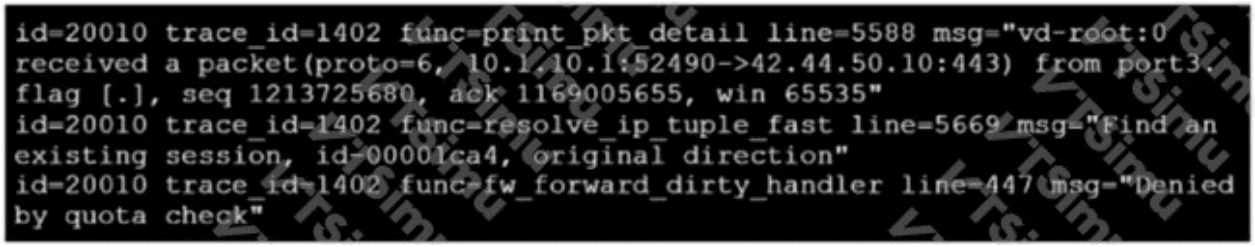
ANSWER: A

Explanation:

Learned routes can be used as dynamic destinations in SD-WAN rules. FortiGate can learn reachable prefixes through BGP and use that routing information to populate dynamic destinations for SD-WAN services. This lets an SD-WAN rule match traffic destined for networks advertised by BGP without requiring an administrator to manually maintain every individual destination prefix in the rule. As BGP advertisements change, the learned route set can change accordingly, allowing SD-WAN policy matching to follow the dynamically learned network topology. This is particularly useful in large hub-and-spoke, cloud, or multi-site deployments, where remote networks and their preferred paths are distributed through BGP. BGP therefore complements SD-WAN: BGP supplies dynamic reachability information, while SD-WAN rules apply service-based steering and link-selection logic to traffic matching those destinations. FortiGate supports BGP as a dynamic routing protocol and documents SD-WAN configuration and behavior in its FortiOS administration resources. See the FortiOS 6.4 Administration Guide and Fortinet's FortiOS 6.4 New Features documentation for the relevant routing and SD-WAN feature documentation.

QUESTION NO: 6

Refer to the exhibit.



Which conclusion about the packet debug flow output is correct?

A. The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.

B. The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the firewall policy, and the packet was dropped.

C. The packet size exceeded the outgoing interface MTU.

D. The total number of daily sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.

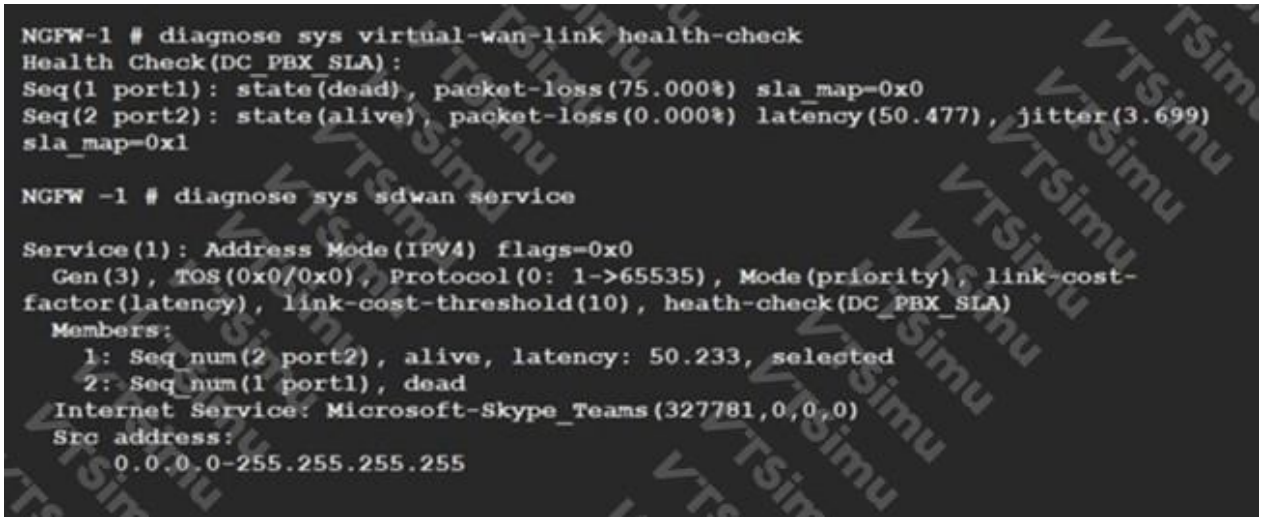
ANSWER: A

Explanation:

The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped. The debug flow message identifies traffic-shaper processing as the point at which FortiGate rejects the packet and indicates that the concurrent-session threshold has been reached for the relevant IP address. A traffic shaper can impose a maximum concurrent-session limit in addition to bandwidth controls. When a new session would cause the configured limit to be exceeded, FortiGate drops the packet rather than creating the additional session. The address shown in the flow output, 10.1.10.1, is therefore the address whose session count is being evaluated against that shaper limit. This is a concurrent count: it represents active sessions at that time, not a cumulative count of sessions opened during a day. FortiGate debug flow is particularly useful here because it reports the feature and decision responsible for the disposition of a packet, allowing an administrator to associate the drop directly with the configured traffic-shaper session limit. Fortinet documents traffic-shaper configuration and session controls in the FortiOS 6.4.5 Administration Guide; related command syntax is available in the FortiOS 6.4.5 CLI Reference.

QUESTION NO: 7

Refer to the exhibit.



Based on the exhibit, which status description is correct?

A. Port1 is dead because it does not meet the SLA target.

B. Port2 is alive because its packet loss is lower than 10%.

C. The SD-WAN members are monitored by different performance SLAs.

D. Traffic matching the SD-WAN rule is steered through port2.

ANSWER: D

Explanation:

Traffic matching the SD-WAN rule is steered through port2. FortiGate evaluates SD-WAN health-check measurements against the configured performance-SLA thresholds and uses that resulting health status when it selects an egress member for an SD-WAN rule. In the displayed status, port2 is the usable member selected for traffic that matches the rule's configured criteria. Therefore, sessions matching that rule are forwarded through port2 rather than remaining on a member that is not eligible under the rule's SLA-driven path-selection logic.

This behavior is central to FortiGate SD-WAN: performance SLAs continuously probe links for latency, jitter, and packet loss, and SD-WAN rules can use those SLA results to make dynamic forwarding decisions. When the preferred path does not satisfy the rule's required health condition, FortiGate selects an eligible alternative according to the rule's strategy and member order. The monitor and rule status shown in the exhibit consequently indicate port2 as the forwarding path for

matching traffic. Fortinet documents performance-SLA health checking and its use by SD-WAN rules in the FortiGate Administration Guide: Performance SLA and the FortiGate Administration Guide: SD-WAN rules.

QUESTION NO: 8

Refer to the exhibit.



Based on the output, which two statements are true? (Choose two)

A. The diagnostic output presents only of the policy routes

B. The all_rules rule is the implicit SD-WAN rule in place

C. There is more than one SD-WAN rule configured

D. At least one policy route is implemented and in effect

ANSWER: A C

Explanation:

The diagnostic output presents only of the policy routes is correct because the displayed diagnostic information is limited to the policy-route entry or entries that are shown in the command output; it is not a complete configuration listing of every routing or SD-WAN-related object on the FortiGate. Policy routes are evaluated independently of the regular routing table and can be inspected with FortiGate diagnostic commands to confirm their active parameters and matching behavior. Therefore, the presence of the displayed policy-route information establishes what is presented by this particular diagnostic view.

There is more than one SD-WAN rule configured is also correct because the output identifies multiple SD-WAN service-rule entries. In FortiOS SD-WAN, a service rule defines traffic matching criteria and the SD-WAN members or performance-SLA behavior used when that traffic matches. Diagnostic SD-WAN service output lists these rules individually, allowing an administrator to distinguish multiple configured rule definitions and review their state. This is consistent with Fortinet's SD-WAN rule model, where several ordered rules can coexist to steer different traffic classes according to application, source, destination, health checks, and selected members. See Fortinet's SD-WAN rules documentation and policy routes documentation.

QUESTION NO: 9

Refer to Exhibit:



Which statement is correct it the responder FortiGate is using a dynamic routing protocol over the IPsec VPN interface?

A. The phase 1 type must be changed to static for dynamic routing.

B. Only dial-up connections without XAuth can be used for the dynamic routing

C. add-route must be disabled to prevent FortiGate from installing VPN static routes

D. peertype must be set to accept only one peer ID for a unique VPN interface

ANSWER: C

Explanation:

add-route must be disabled to prevent FortiGate from installing VPN static routes is correct. When a route-based IPsec tunnel is used as the transport for a dynamic routing protocol, such as BGP or OSPF, the routing protocol should determine and install reachability information through the tunnel. The IPsec Phase 1 interface setting `add-route` controls whether FortiGate automatically adds a static route for the remote protected network when the tunnel comes up. On a responder using a dialup IPsec configuration, the peer and/or protected subnets can be learned dynamically, so automatically created VPN routes can be unsuitable or can interfere with the routing design. Disabling `add-route` prevents FortiGate from injecting those automatic static routes, leaving route selection to the configured dynamic routing protocol and its learned routes. The IPsec tunnel interface can then be enabled within the routing process, and routing adjacencies can form across it as intended. Fortinet documents the `add-route` setting under the Phase 1 interface IPsec CLI configuration and describes dynamic-routing deployment concepts in the FortiGate administration documentation. See the FortiOS 6.4 CLI Reference and the FortiOS 6.4 Administration Guide.

QUESTION NO: 10

What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process? (Choose two.)

A. The FortiGate cloud key has not been added to the FortiGate cloud portal.

B. FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager

C. The zero-touch provisioning process has completed internally, behind FortiGate.

D. FortiGate has obtained a configuration from the platform template in FortiGate cloud.

E. A factory reset performed on FortiGate.

ANSWER: A C

Explanation:

Zero-touch provisioning depends on FortiDeploy being able to associate the connecting device with the correct customer account and deployment record. The FortiGate cloud key has not been added to the FortiGate cloud portal prevents that association from being established. The cloud key is the registration credential used to authorize the FortiGate for the organization's FortiDeploy workflow; without it, the service cannot deliver the intended initial provisioning details to the device.

The zero-touch provisioning process has completed internally, behind FortiGate is also a valid reason that a new provisioning attempt cannot complete. FortiDeploy provisioning is a stateful, initial-deployment workflow. After the service has recorded the provisioning transaction as completed, it does not treat the unit as an unprovisioned device awaiting the same initial workflow again. Administrators must therefore ensure that the device's FortiDeploy registration and provisioning state match the intended deployment before expecting a new automated provisioning run.

Fortinet documents FortiDeploy as the cloud service used to provide initial configuration and bootstrap a FortiGate for centralized management. See the FortiOS 6.4 Administration Guide and Fortinet's FortiDeploy product documentation for deployment and registration guidance.