Exam Questions NSE7_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/

NEW QUESTION 1
In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.
B. It provides direct connectivity between spokes by creating shortcuts.
C. It enables spokes to bypass the hub during shortcut negotiation.
D. It enables spokes to establish shortcuts to third-party gateways.

Answer: AB

NEW QUESTION 2
What is the route-tag setting in an SD-WAN rule used for?

A. To indicate the routes for health check probes.
B. To indicate the destination of a rule based on learned BGP prefixes.
C. To indicate the routes that can be used for routing SD-WAN traffic.
D. To indicate the members that can be used to route SD-WAN traffic.

Answer: B

NEW QUESTION 3
What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two)

A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
B. It improves SD-WAN performance on the managed FortiGate devices.
C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
D. It acts as a policy compliance entity to review all managed FortiGate devices.
E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

Answer: AE

NEW QUESTION 4
Which are three key routing principles in SD-WAN? (Choose three.)

A. FortiGate performs route lookups for new sessions only.
B. Regular policy routes have precedence over SD-WAN rules.
C. SD-WAN rules have precedence over ISDB routes.
D. By default, SD-WAN members are skipped if they do not have a valid route to the destination.
E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Answer: BDE

NEW QUESTION 5
Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, packet loss: 2.000%, selected
    2: Seq_num(4 T_MPLS_0), alive, packet loss: 4.000%, selected
    3: Seq_num(5 T_INET_1_0), alive, packet loss: 12.000%, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255

branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "VPN_PING"
        set link-cost-factor packet-loss
        set link-cost-threshold 0
        set priority-members 5 3 4
    next
end
```

The exhibit shows the SD-WAN rule status and configuration.
Based on the exhibit, which change in the measured packet loss will make T_INET_1_0 the new preferred member?

A. When all three members have the same packet loss.
B. When T_INET_0_0 has 4% packet loss.
C. When T_INET_0_0 has 12% packet loss.
D. When T_INET_1_0 has 4% packet loss.

Answer: A

NEW QUESTION 6
Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
    edit "T_INET_0_0"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set comments "[created by FMG VPN Manager]"
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret ENC
6D5rVsaK1MeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc51tCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV21ZUgFjvIpXNxHxpH
LReOFShoH01SPFKz5IYCVA==
    next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD-WAN?

A. You must set ike-version to 1.
B. You must enable net-device.
C. You must enable auto-discovery-sender.
D. You must disable idle-timeout.

Answer: B

NEW QUESTION 7
Which best describes the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

A. Interface-based shaping mode
B. Reverse-policy shaping mode
C. Shared-policy shaping mode
D. Per-IP shaping mode

Answer: A

Explanation:
Interface-based shaping goes further, enabling traffic controls based on percentage of the interface bandwidth.

NEW QUESTION 8
Exhibit A –

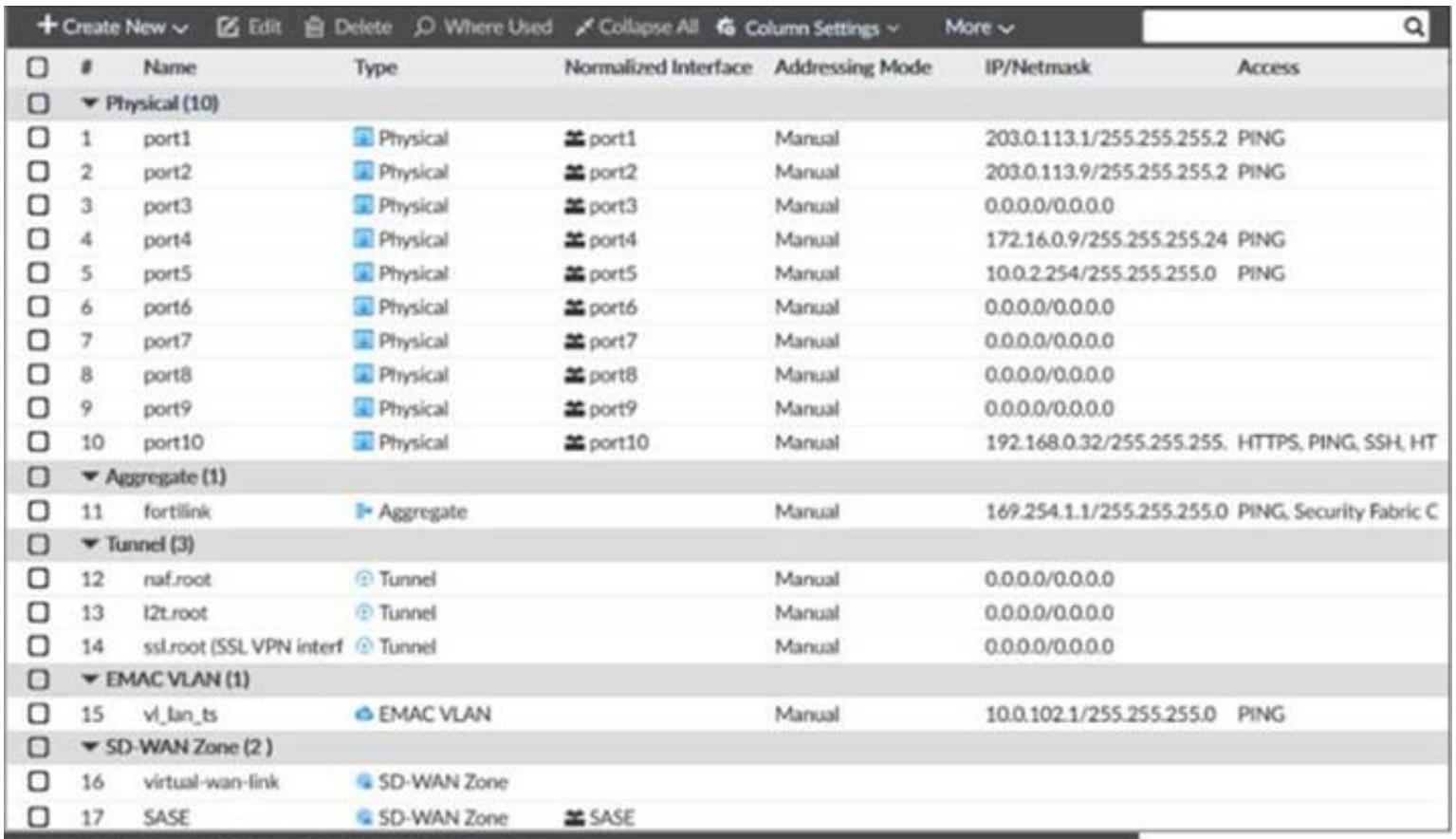


Exhibit B –

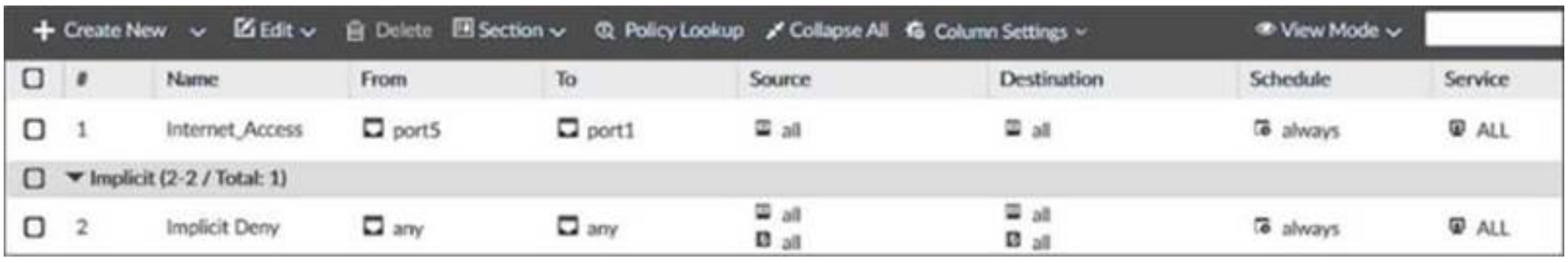


Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate.
Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

A. port1 is assigned a manual IP address.
B. port1 is referenced in a firewall policy.
C. port2 is referenced in a static route.
D. port1 and port2 are not administratively down.

Answer: B

NEW QUESTION 9
Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

A. update-source
B. set-route-tag
C. holdtime-timer
D. link-down-failover

Answer: CD

NEW QUESTION 10
What are two common use cases for remote internet access (RIA)? (Choose two.)

A. Provide direct internet access on spokes
B. Provide internet access through the hub
C. Centralize security inspection on the hub
D. Provide thorough inspection on spokes

Answer: BC

NEW QUESTION 10
Which components make up the secure SD-WAN solution?

A. Application, antivirus, and URL, and SSL inspection
B. Datacenter, branch offices, and public cloud
C. FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy
D. Telephone, ISDN, and telecom network.

Answer: C

NEW QUESTION 12
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: AC

NEW QUESTION 16
Refer to the exhibits.
Exhibit A

Exhibit B

```
branch1_fgt # diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0
```

```
config service
    edit 1
        set name "Critical-DIA"
        set mode priority
        set src "LAN-net"
        set internet-service enable
        set internet-service-app-ctrl 16354 41468 16920
        set health-check "Level3_DNS"
        set priority-members 1 2
    next
end
```

Exhibit A shows an SD-WAN event log and exhibit B shows the member status and the SD-WAN rule configuration.
Based on the exhibits, which two statements are correct? (Choose two.)

A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
B. Port2 has the highest member priority.
C. Port2 has a lower latency than port1.
D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

Answer: AC

NEW QUESTION 19
Which diagnostic command can you use to show the configured SD-WAN zones and their assigned members?

A. diagnose sys sdwan zone
B. diagnose sys sdwan service
C. diagnose sys sdwan member
D. diagnose sys sdwan interface

Answer: A

NEW QUESTION 23
Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port1), alive, selected
    2: Seq_num(2 port2), alive, selected
  Internet Service(3): GoToMeeting(4294836966,0,0,0 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0 41468) Salesforce(4294837976,0,0,0 16920)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2), alive, selected
  Internet Service(2): Facebook(4294836806,0,0,0 15832) Twitter(4294838278,0,0,0 16001)
  Src address(1):
        10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836806): 157.240.229.35 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.205.106.86 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.212.249.144 6 443 Tue Mar  8 12:24:39 2022
Salesforce(16920 4294837976): 23.212.249.11 6 443 Tue Mar  8 12:24:04 2022

branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
                  [1/0] via 192.2.0.10, port2
...
```

Exhibit B

Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	APP 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP 2		port1
23.212.249.144	HTTPS	GoToMeeting	APP 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP 2		port2

Security	
APP Count	2
Level	notice
General	
Log ID	0000000013
Session ID	769
Tran Display	snat
Virtual Domain	root
Source	
Country	Reserved
Device ID	FGVM01TM22000077
Device Name	branch1_fgt
IP	10.0.1.101
Interface	port5
Interface Role	undefined
NAT IP	192.2.0.9
NAT Port	51042
Port	51042
Source	10.0.1.101
UEBA Endpoint ID	1025
UEBA User ID	3
Destination	
Country	United States
End User ID	3
Endpoint ID	101
Host Name	www.gotomeeting.com
IP	23.212.248.205
Interface	port2

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A.
After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1.
Which two reasons explain why the traffic matched the implicit SD-WAN rule? (Choose two.)

A. FortiGate did not refresh the routing information on the session after the application was detected.
B. Port1 and port2 do not have a valid route to the destination.
C. Full SSL inspection is not enabled on the matching firewall policy.
D. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

Answer: AC

NEW QUESTION 27
Refer to the exhibit.

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=17 sport=0-65535 iif=7
dport=53 path(1) oif=3(port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 4.2.2.1/255.255.255.255
hit_count=0 last_used=2022-03-25 10:53:26

id=2131165185(0x7f070001) 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=2022-03-24 12:18:16

id=2131165186(0x7f070002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xff
0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535
path(1) 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(2): Facebook(4294836806,0,0,0, 15832) Twitter(4294838278,0,0,0, 16001)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165187(0x7f070003) vwl_service=3(all_rules) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(1)
oif=3(port1)
source(1): 0.0.0.0-255.255.255.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=0 last_used=2022-03-25 10:58:12
```

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

A. There is more than one SD-WAN rule configured.
B. The SD-WAN rules take precedence over regular policy routes.
C. The all_rules rule represents the implicit SD-WAN rule.
D. Entry 1(id=1) is a regular policy route.

Answer: AD

NEW QUESTION 30
Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
    2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
    3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "VPN_PING"
        set priority-members 3 4 5
    next
end
```

The exhibit shows the SD-WAN rule status and configuration.
Based on the exhibit, which change in the measured latency will make T_MPLS_0 the new preferred member?

A. When T_INET_0_0 and T_MPLS_0 have the same latency.
B. When T_MPLS_0 has a latency of 100 ms.

C. When T_INET_0_0 has a latency of 250 ms.
D. When T_N1PLS_0 has a latency of 80 ms.

Answer: D

NEW QUESTION 34
Refer to the exhibit.

```
config system sdwan
    set status enable
    set load-balance source-dest-ip-based
    config zone
        edit "virtual-wan-link"
        next
        edit "SASE"
        next
        edit "underlay"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
            set gateway 192.2.0.2
        next
        edit 2
            set interface "port2"
            set zone "underlay"
            set gateway 192.2.0.10
        next
    end
...
end
```

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.
B. All traffic from a source IP is sent to the same interface.
C. All traffic from a source IP is sent to the most used interface.
D. All traffic from a source IP to a destination IP is sent to the least used interface.

Answer: A

NEW QUESTION 39
Refer to the exhibits. Exhibit A

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end

config system sdwan
    config service
        edit 1
            set name "Facebook-YouTube"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

Exhibit B

```
config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
        members(2): 3(port1) 4(port2)
```

Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.
Based on the exhibits, which two statements are correct about the health and performance of port1 and port2? (Choose two.)

A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
B. FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.
C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
D. Non-TCP Facebook and YouTube traffic are not used for performance measurement.

Answer: AD

Explanation:
Study Guide 7.0, pages 88 - 89.
Study Guide 7.2, pages 103 - 104.
Another comment said "because without using application Control on the firewall policy, SDWAN can't work" but there is a app control "default" defined on config.

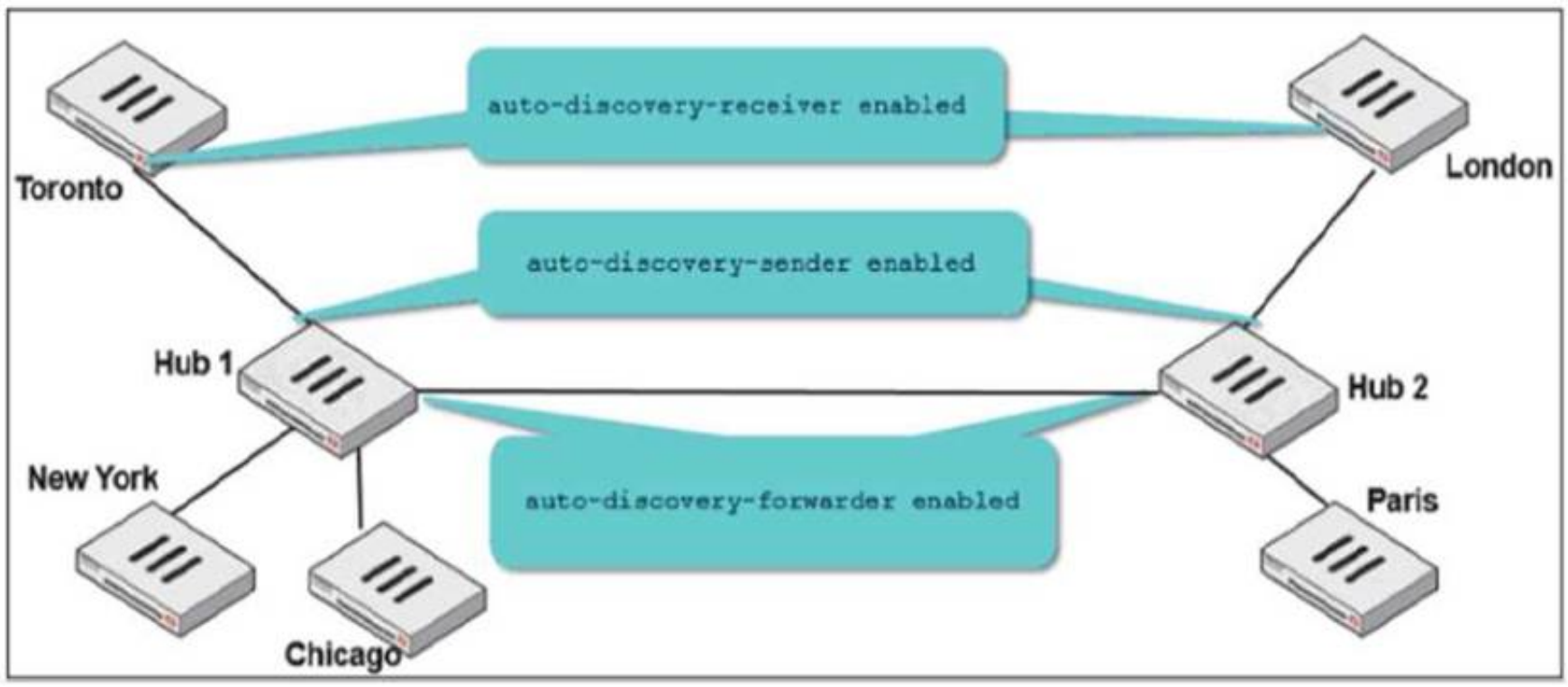
NEW QUESTION 44
Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

```
# diagnose firewall shaper traffic-shaper list name VoIP_Shaper
name VoIP_Shaper
maximum-bandwidth 6250 KB/sec
guaranteed-bandwidth 2500 KB/sec
current-bandwidth 93 KB/sec
priority 2
overhead 0
tos ff
packets dropped 0
bytes dropped 0
```

A. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
B. The measured bandwidth is less than 100 KBps.
C. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.
D. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

Answer: BC

NEW QUESTION 46
Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. The administrator configured ADVPN on both hub-and-spoke groups.



Which two outcomes are expected if a user in Toronto sends traffic to London? (Choose two.)

A. London generates an IKE information message that contains the Toronto public IP address.
B. Traffic from Toronto to London triggers the dynamic negotiation of a direct site-to-site VPN.
C. Toronto needs to establish a site-to-site tunnel with Hub 2 to bypass Hub 1.
D. The first packets from Toronto to London are routed through Hub 1 then to Hub 2.

Answer: BD

NEW QUESTION 51
Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

A. Encapsulating Security Payload (ESP)
B. Secure Shell (SSH)
C. Internet Key Exchange (IKE)
D. Security Association (SA)

Answer: AC

NEW QUESTION 55
Refer to the exhibit.

```
config firewall policy
    edit 1
        set anti-replay disable
    next
end
```

In a dual-hub hub-and-spoke SD-WAN deployment, which is a benefit of disabling the anti-replay setting on the hubs?

A. It instructs the hub to disable the reordering of TCP packets on behalf of the receiver, to improve performance.
B. It instructs the hub to disable TCP sequence number check, which is required for TCP sessions originated from spokes to fail over back and forth between the hubs.
C. It instructs the hub to not check the ESP sequence numbers on IPsec traffic, to improve performance.
D. It instructs the hub to skip content inspection on TCP traffic, to improve performance.

Answer: B

NEW QUESTION 59
Which statement is correct about SD-WAN and ADVPN?

A. Routes for ADVPN shortcuts must be manually configured.
B. SD-WAN can steer traffic to ADVPN shortcuts, established over IPsec overlays, configured as SD-WAN members.
C. SD-WAN does not monitor the health and performance of ADVPN shortcuts.
D. You must use IKEv2 on IPsec tunnels.

Answer: B

NEW QUESTION 60
Which SD-WAN setting enables FortiGate to delay the recovery of ADVPN shortcuts?

A. hold-down-time
B. link-down-failover
C. auto-discovery-shortcuts
D. idle-timeout

Answer: A

NEW QUESTION 65
Which three matching traffic criteria are available in SD-WAN rules? (Choose three.)

A. Type of physical link connection
B. Internet service database (ISDB) address object
C. Source and destination IP address
D. URL categories
E. Application signatures

Answer: BCE

NEW QUESTION 66
Refer to the exhibit.

```
config router bgp
    set as 65000
    set router-id 10.1.0.1
    set ibgp-multipath enable
    set additional-path enable
    set additional-path-select 3
    config neighbor-group
        edit "Branches_INET_0"
            set interface "T_INET_0_0"
            set remote-as 65000
            set update-source "T_INET_0_0"
        next
        edit "Branches_INET_1"
            set interface "T_INET_1_0"
            set remote-as 65000
            set update-source "T_INET_1_0"
        next
        edit "Branches_MPLS"
            set interface "T_MPLS_0"
            set remote-as 65000
            set update-source "T_MPLS_0"
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.201.1.0 255.255.255.0
            set neighbor-group "Branches_INET_0"
        next
        edit 2
            set prefix 10.202.1.0 255.255.255.0
            set neighbor-group "Branches_INET_1"
        next
        edit 3
            set prefix 10.203.1.0 255.255.255.0
            set neighbor-group "Branches_MPLS"
        next
    end
...
end
```

The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths.
Based on the exhibit, which three settings must the administrator configure inside each BGP neighbor group so spokes can learn other spokes prefixes and their additional paths? (Choose three.)

A. Set additional-path to send
B. Enable route-reflector-client
C. Set advertisement-interval to the number of additional paths to advertise
D. Set adv-additional-path to the number of additional paths to advertise
E. Enable soft-reconfiguration

Answer: ABD

NEW QUESTION 70
What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

A. FEC supports hardware offloading.
B. FEC improves reliability of noisy links.
C. FEC transmits parity packets that can be used to reconstruct packet loss.
D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

Answer: BC

NEW QUESTION 71
Refer to the exhibits. Exhibit A

```
branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode sla
        set dst "Corp-net"
        set src "LAN-net"
        config sla
            edit "VPN_PING"
                set id 1
            next
            edit "VPN_HTTP"
                set id 1
            next
        end
        set priority-members 3 4 5
        set gateway enable
    next
end
```

Exhibit B

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
    2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
    3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt # get router info routing-table all | grep T_
S       10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
                   [1/0] via T_INET_1_0 tunnel 100.64.1.9
S       10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S       10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S       10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5


branch1_fgt # diagnose sys sdwan member | grep T_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1,  peer: 10.201.1.254,
priority: 0 1024, weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9,  peer: 10.202.1.254,
priority: 0 1024, weight: 0
Member(5): interface: T_MPLS_0, flags=0x4 , gateway: 172.16.1.5,  peer: 10.203.1.254,
priority: 0 1024, weight: 0
```

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status.
The administrator wants to understand the expected behavior for traffic matching the SD-WAN rule. Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

A. The traffic will be load balanced across all three overlays.
B. The traffic will be routed over T_INET_0_0.
C. The traffic will be routed over T_MPLS_0.
D. The traffic will be routed over T_INET_1_0.

Answer: D

NEW QUESTION 75
Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(3 T_INET_0_0), alive, selected
    2: Seq_num(4 T_INET_1_0), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, priority: 0 1024,
weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S       10.0.0.0/8 [1/0] via T_INET_1_0 tunnel 100.64.1.9
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over T_INET_0_0. However, the traffic is routed over T_INET_1_0.
Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

A. The traffic matches a regular policy route configured with T_INET_1_0 as the outgoing device.
B. T_INET_1_0 has a lower route priority value (higher priority) than T_INET_0_0.
C. T_INET_0_0 does not have a valid route to the destination.
D. T_INET_1_0 has a higher member configuration priority than T_INET_0_0.

Answer: AC

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Assigning-Priority-to-SD-WAN-Members-for-Defau

NEW QUESTION 78
Exhibit.

```
id=20010 trace_id=1402 func=print_pkt_detail line=5588 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:52490->42.44.50.10:443) from port3. flag [.], seq 1213725680,
ack 1169005655, win 65535"
id=20010 trace_id=1402 func=resolve_ip_tuple_fast line=5669 msg="Find an existing
session, id-00001ca4, original direction"
id=20010 trace_id=1402 func=fw_forward_dirty_handler line=447 msg="Denied by quota
check"
```

Which conclusion about the packet debug flow output is correct?

A. 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.
B. The packet size exceeded the outgoing interface MTU.
C. 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.
D. 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.

Answer: C

Explanation:
In a Per-IP shaper configuration, if an IP address exceeds the configured concurrent session limit, the message "Denied by quota check" appears. SD-WAN 7.0 Study Guide page 287

NEW QUESTION 80
Refer to the exhibits.
Exhibit A

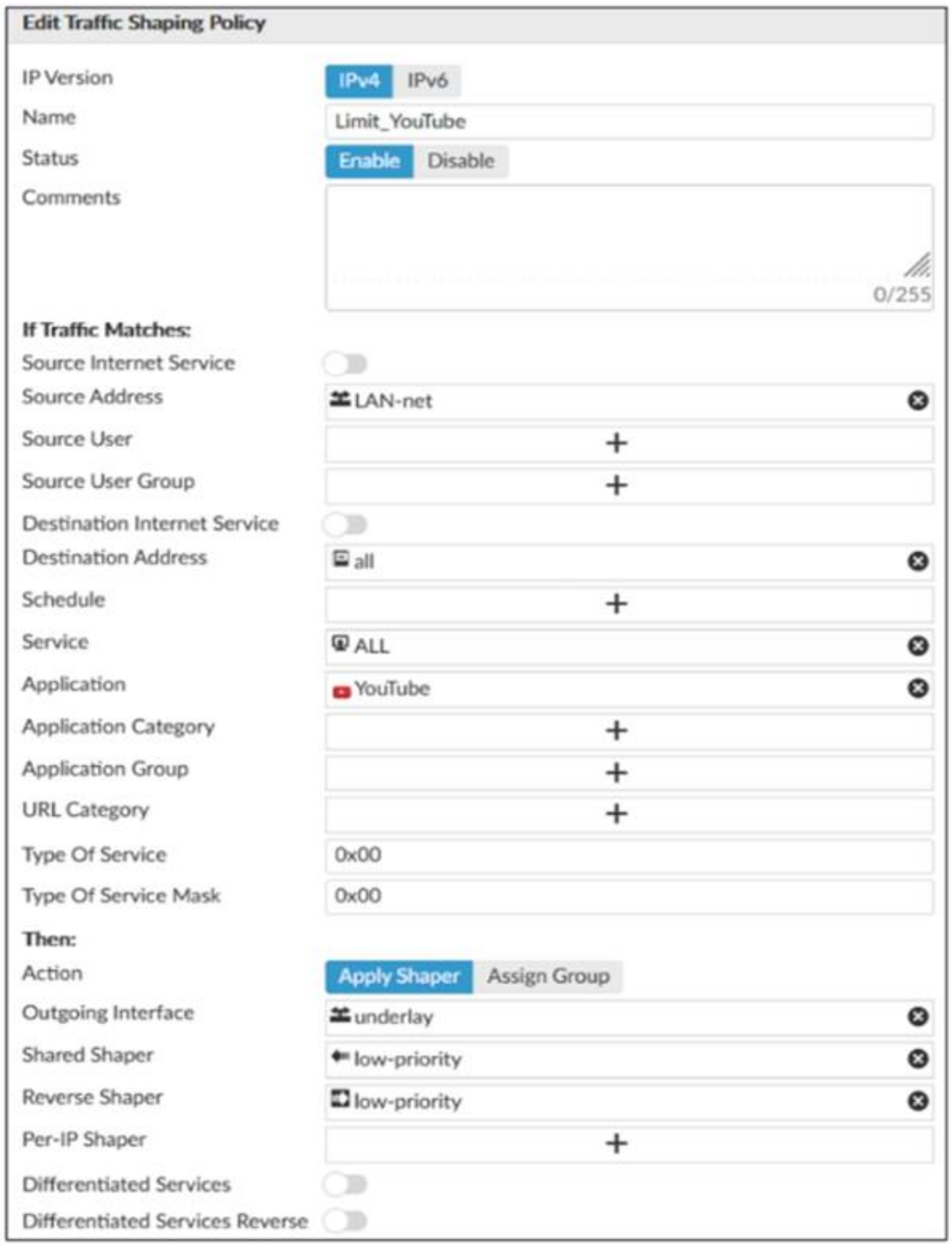

Edit Traffic Shaping Policy
IP Version
IPv4
IPv6
Name
Limit_YouTube
Status
Enable
Disable
Comments
0/255
If Traffic Matches:
Source Internet Service
Source Address
LAN-net
Source User
Source User Group
Destination Internet Service
Destination Address
all
Schedule
Service
ALL
Application
YouTube
Application Category
Application Group
URL Category
Type Of Service
0x00
Type Of Service Mask
0x00
Then:
Action
Apply Shaper
Assign Group
Outgoing Interface
underlay
Shared Shaper
low-priority
Reverse Shaper
low-priority
Per-IP Shaper
Differentiated Services
Differentiated Services Reverse

Exhibit B

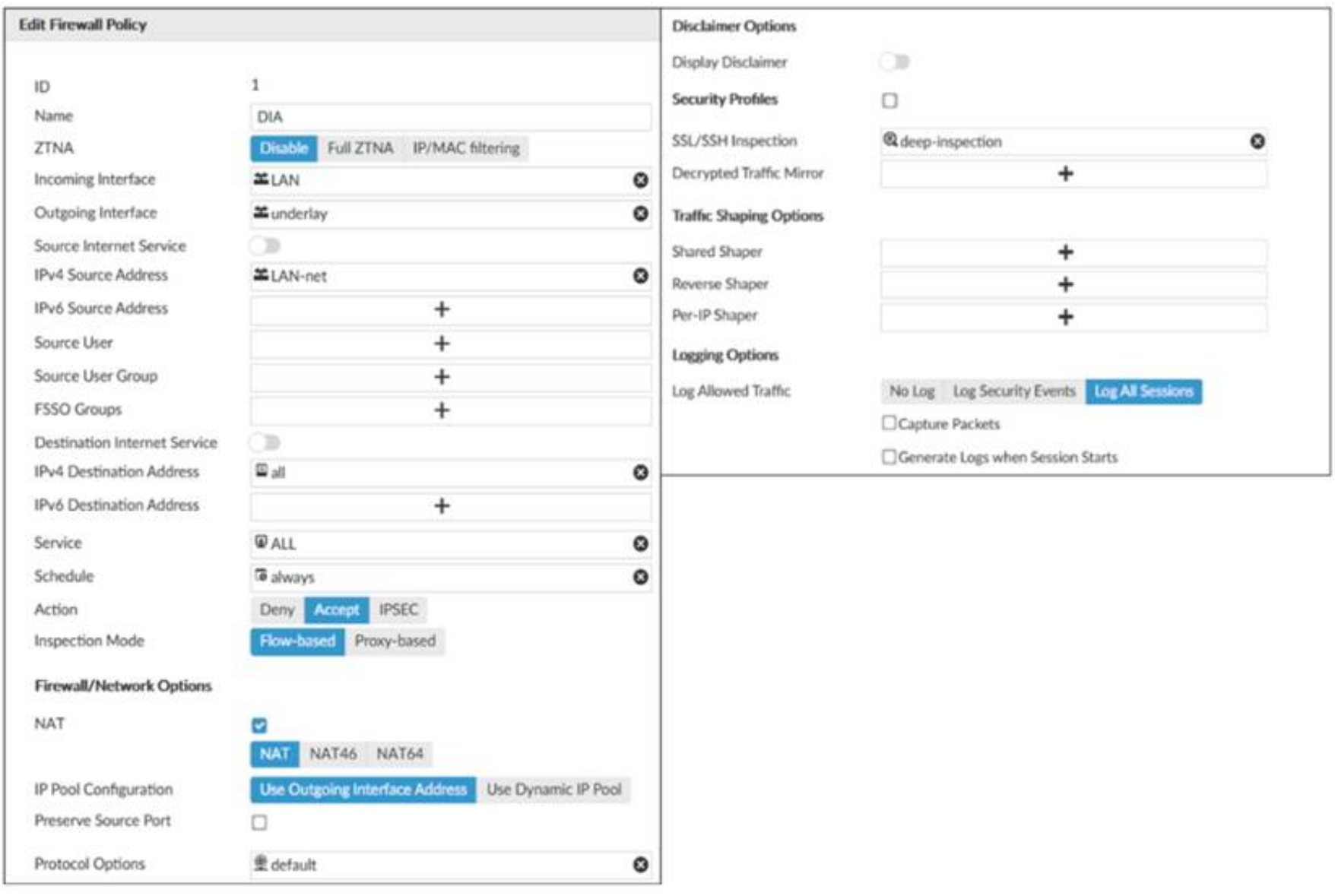

Edit Firewall Policy
ID
1
Name
DIA
ZTNA
Disable
Full ZTNA
IP/MAC filtering
Incoming Interface
LAN
Outgoing Interface
underlay
Source Internet Service
IPv4 Source Address
LAN-net
IPv6 Source Address
Source User
Source User Group
FSSO Groups
Destination Internet Service
IPv4 Destination Address
all
IPv6 Destination Address
Service
ALL
Schedule
always
Action
Deny
Accept
IPSEC
Inspection Mode
Flow-based
Proxy-based
Firewall/Network Options
NAT
NAT
NAT46
NAT64
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
default
Disclaimer Options
Display Disclaimer
Security Profiles
SSL/SSH Inspection
deep-inspection
Decrypted Traffic Mirror
Traffic Shaping Options
Shared Shaper
Reverse Shaper
Per-IP Shaper
Logging Options
Log Allowed Traffic
No Log
Log Security Events
Log All Sessions
Capture Packets
Generate Logs when Session Starts

Exhibit A shows the traffic shaping policy and exhibit B shows the firewall policy.
The administrator wants FortiGate to limit the bandwidth used by YouTube. When testing, the administrator determines that FortiGate does not apply traffic shaping on YouTube traffic.
Based on the policies shown in the exhibits, what configuration change must be made so FortiGate performs traffic shaping on YouTube traffic?

A. Destination internet service must be enabled on the traffic shaping policy.
B. Application control must be enabled on the firewall policy.
C. Web filtering must be enabled on the firewall policy.
D. Individual SD-WAN members must be selected as the outgoing interface on the traffic shaping policy.

Answer: B

NEW QUESTION 83
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_SDW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_SDW-7.0 Product From:

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/

Money Back Guarantee

NSE7_SDW-7.0 Practice Exam Features:

* NSE7_SDW-7.0 Questions and Answers Updated Frequently

* NSE7_SDW-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_SDW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_SDW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year