NSE4_FGT-6.4$^{Q\&As}$

Fortinet NSE 4 - FortiOS 6.4

QUESTION 1

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.

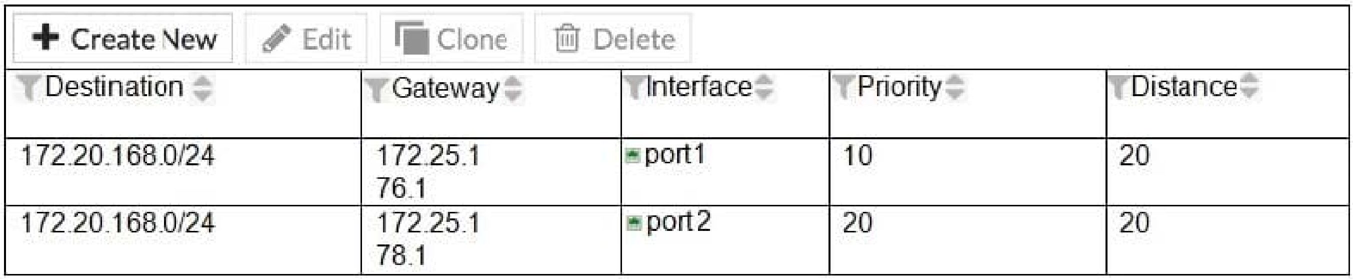
C. To encapsulation ESP packets in UDP packets using port 4500.

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

Correct Answer: AC

QUESTION 2

Examine the two static routes shown in the exhibit, then answer the following question.



Destination	Gateway	Interface	Priority	Distance
172.20.168.0/24	172.25.176.1	🟩 port1	10	20
172.20.168.0/24	172.25.178.1	🟩 port2	20	20

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.

B. FortiGate will use the port1 route as the primary candidate.

C. FortiGate will route twice as much traffic to the port2 route

D. FortiGate will only actuate the port1 route in the routing table

Correct Answer: B

"If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path."

QUESTION 3

Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password

B. FortiGate supports pre-shared key and signature as authentication methods.

C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.

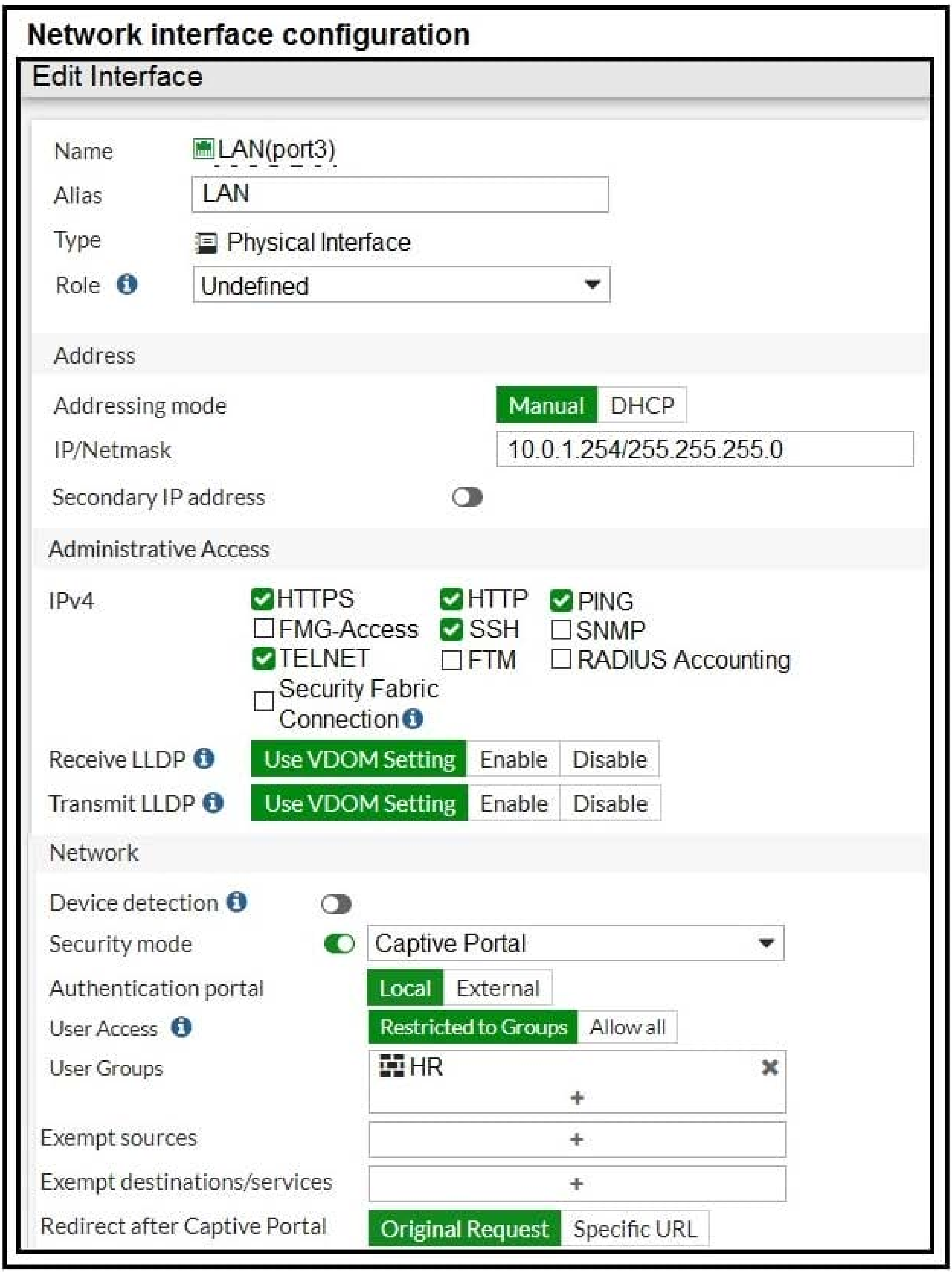
D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticatingaremote-fortigate-peer-with-a-pre-shared-key

QUESTION 4

Refer to the exhibit.



Network interface configuration

Edit Interface

Name: LAN(port3)
Alias: LAN
Type: Physical Interface
Role: Undefined

Address

Addressing mode: [✓ Manual] DHCP
IP/Netmask: 10.0.1.254/255.255.255.0
Secondary IP address: ○

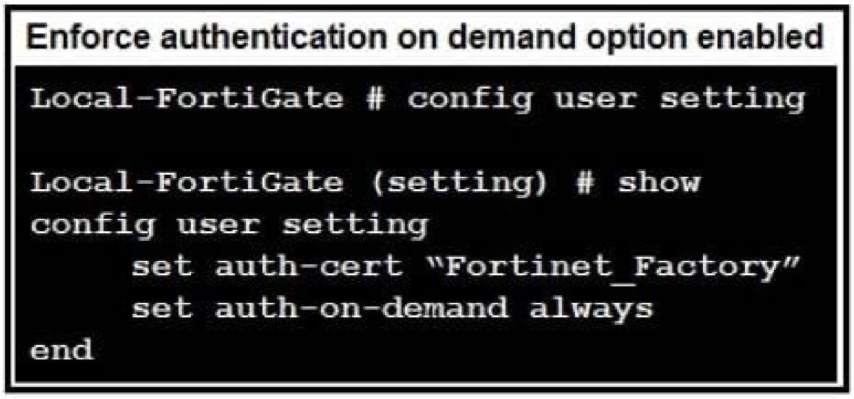
Administrative Access

IPv4: ☑ HTTPS ☑ HTTP ☑ PING
□ FMG-Access ☑ SSH □ SNMP
☑ TELNET □ FTM □ RADIUS Accounting
□ Security Fabric Connection

Receive LLDP: [✓ Use VDOM Setting] Enable Disable
Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

Network

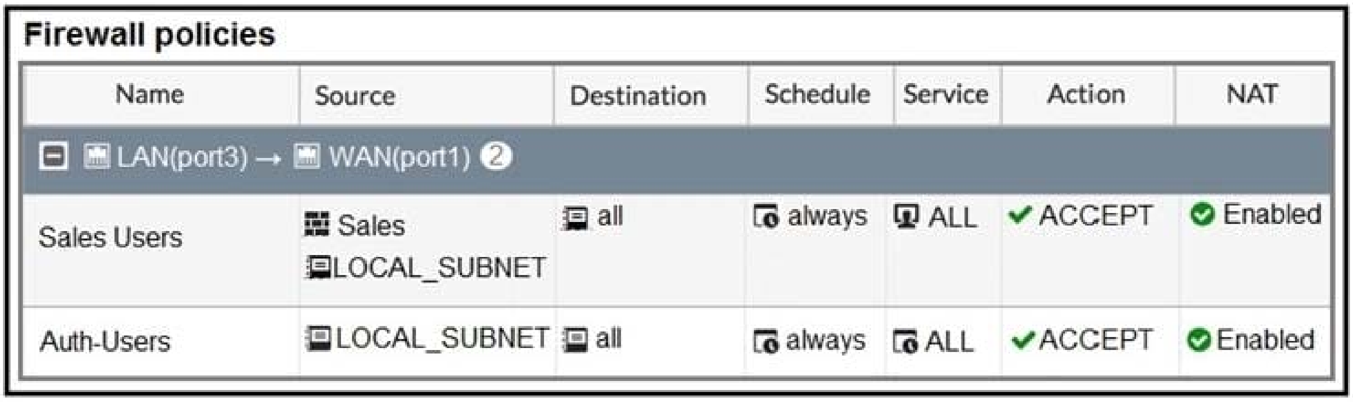
Device detection: ○
Security mode: ● Captive Portal
Authentication portal: [✓ Local] External
User Access: [✓ Restricted to Groups] Allow all
User Groups: HR
Exempt sources: +
Exempt destinations/services: +
Redirect after Captive Portal: [✓ Original Request] Specific URL



Enforce authentication on demand option enabled

```
Local-FortiGate # config user setting

Local-FortiGate (setting) # show
config user setting
     set auth-cert "Fortinet_Factory"
     set auth-on-demand always
end
```



Firewall policies

Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port3) → WAN(port1) 2						
Sales Users	Sales LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled
Auth-Users	LOCAL_SUBNET	all	always	ALL	✓ACCEPT	✓Enabled

The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration.

How will FortiGate handle user authentication for traffic that arrives on the LAN interface?

A. If there is a full-through policy in place, users will not be prompted for authentication.

B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.

C. Authentication is enforced at a policy level; all users will be prompted for authentication.

D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Correct Answer: C

QUESTION 5

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: ADE

https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221