FCNSP.V5^{Q&As}

Fortinet Certified Network Security Professional (FCNSP.v5)

Pass Fortinet FCNSP.V5 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/fcnsp-v5.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

* **Instant Download** After Purchase

* **100% Money Back** Guarantee

* **365 Days** Free Update

* **800,000+** Satisfied Customers

QUESTION 1

Which of the following Session TTL values will take precedence?

A. Session TTL specified at the system level for that port number

B. Session TTL specified in the matching firewall policy

C. Session TTL dictated by the application control list associated with the matching firewall policy

D. The default session TTL specified at the system level

Correct Answer: C

QUESTION 2

In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate unit when searching for a suitable gateway?

A. A look-up is done only when the first packet coming from the client (SYN) arrives.

B. A look-up is done when the first packet coming from the client (SYN) arrives, and a second is performed when the first packet coming from the server (SYNC/ACK) arrives.

C. A look-up is done only during the TCP 3-way handshake (SYNC, SYNC/ACK, ACK).

D. A look-up is always done each time a packet arrives, from either the server or the client side.

Correct Answer: B

QUESTION 3

Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of \\'diag sys session stat\\' for the STUDENT device. Exhibit B shows the command output of \\'diag sys session stat\\' for the REMOTE device.

Exhibit A:

```
STUDENT # diagnose sys session stat
Misc info:        session_count=166 setup_rate=68 exp_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
        8 in ESTABLISHED state
        3 in SYN_SENT state
        1 in FIN_WAIT state
        139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

STUDENT # _
```

Exhibit B: Given the information provided in the exhibits, which of the following statements are correct? (Select all that apply.)

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
Misc info:        session_count=11 setup_rate=0 exp_count=0 clash=4
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
        2 in ESTABLISHED state
        1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

A. STUDENT is likely to be the master device.

B. Session-pickup is likely to be enabled.

C. The cluster mode is definitely Active-Passive.

D. There is not enough information to determine the cluster mode.

Correct Answer: AD

QUESTION 4

Which of the following statements correctly describe Transparent Mode operation? (Select all that apply.)

A. The FortiGate unit acts as transparent bridge and routes traffic using Layer-2 forwarding.

B. Ethernet packets are forwarded based on destination MAC addresses NOT IPs.

C. The device is transparent to network hosts.

D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.

E. All interfaces must be on different IP subnets.

Correct Answer: ABCD

QUESTION 5

Which of the following statements are TRUE for Port Pairing and Forwarding Domains? (Select all that apply.)

A. They both create separate broadcast domains.

B. Port Pairing works only for physical interfaces.

C. Forwarding Domains only apply to virtual interfaces.

D. They may contain physical and/or virtual interfaces.

E. They are only available in high-end models.

Correct Answer: AD

QUESTION 6

What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully- meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.

B. Using a hub and spoke topology simplifies configuration because fewer tunnels are required.

C. Using a hub and spoke topology provides stronger encryption.

D. The routing at a spoke is simpler, compared to a meshed node.

Correct Answer: BD

QUESTION 7

An administrator configures a VPN and selects the Enable IPSec Interface Mode option in the phase 1 settings.

Which of the following statements are correct regarding the IPSec VPN configuration?

A. To complete the VPN configuration, the administrator must manually create a virtual IPSec interface in Web Config under System > Network.

B. The virtual IPSec interface is automatically created after the phase1 configuration.

C. The IPSec policies must be placed at the top of the list.

D. This VPN cannot be used as part of a hub and spoke topology.

E. Routes were automatically created based on the address objects in the firewall policies.

Correct Answer: B

QUESTION 8

Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

config router static edit 1 set dst 172.20.168.0 255.255.255.0 set distance 20 set priority 10 set device port1 next edit 2 set dst 172.20.168.0 255.255.255.0 set distance 20 set priority 20 set device port2 next end

Which of the following statements correctly describes the static routing configuration provided above?

A. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 through both routes.

B. The FortiGate unit will share the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.

C. The FortiGate unit will send all the traffic to 172.20.168.0/24 through port1.

D. Only the route that is using port1 will show up in the routing table.

Correct Answer: C

QUESTION 9

In the Tunnel Mode widget of the web portal, the administrator has configured an IP Pool and enabled split tunneling.

Which of the following statements is true about the IP address used by the SSL VPN client?

A. The IP pool specified in the SSL-VPN Tunnel Mode Widget Options will override the IP address range defined in the

SSL-VPN Settings.

B. Because split tunneling is enabled, no IP address needs to be assigned for the SSL VPN tunnel to be established.

C. The IP address range specified in SSL-VPN Settings will override the IP address range in the SSL-VPN Tunnel Mode Widget Options.

Correct Answer: A

QUESTION 10

In HA, the option Reserve Management Port for Cluster Member is selected as shown in the Exhibit below.

Which of the following statements are correct regarding this setting? (Select all that apply.)

A. Interface settings on port7 will not be synchronized with other cluster members.

B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.

C. Port7 appears in the routing table.

D. A gateway address may be configured for port7.

E. When connecting to port7 you always connect to the master device.

Correct Answer: AD

QUESTION 11

A FortiClient fails to establish a VPN tunnel with a FortiGate unit.

The following information is displayed in the FortiGate unit logs:

msg="Initiator: sent 192.168.11.101 main mode message #1 (OK)" msg="Initiator: sent 192.168.11.101 main mode message #2 (OK)" msg="Initiator: sent 192.168.11.101 main mode message #3 (OK)" msg="Initiator: parsed 192.168.11.101 main mode message #3 (DONE)" msg="Initiator: sent

192.168.11.101 quick mode message #1 (OK)" msg="Initiator: tunnel 192.168.1.1/192.168.11.101 install ipsec sa" msg="Initiator: sent 192.168.11.101 quick mode message #2 (DONE)" msg="Initiator: tunnel 192.168.11.101, transform=ESP_3DES, HMAC_MD5" msg="Failed to acquire an IP address

Which of the following statements is a possible cause for the failure to establish the VPN tunnel?
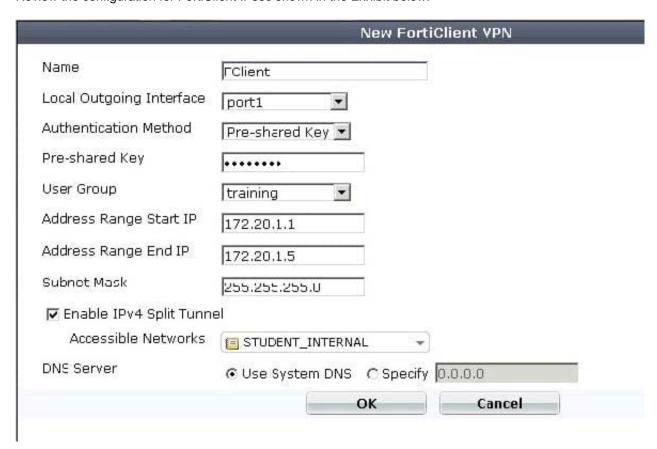
A. An IPSec DHCP server is not enabled on the external interface of the FortiGate unit.

B. There is no IPSec firewall policy configured for the policy-based VPN.

C. There is a mismatch between the FortiGate unit and the FortiClient IP addresses in the phase 2 settings.

D. The phase 1 configuration on the FortiGate unit uses Aggressive mode while FortiClient uses Main mode.

Correct Answer: A

QUESTION 12

Review the configuration for FortiClient IPsec shown in the Exhibit below.

Which of the following statements is correct regarding this configuration?

A. The connecting VPN client will install a route to a destination corresponding to the STUDENT_INTERNAL address object

B. The connecting VPN client will install a default route

C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range

D. The connecting VPN client will connect in web portal mode and no route will be installed

Correct Answer: A

QUESTION 13

A portion of the device listing for a FortiAnalyzer unit is displayed in the exhibit.

	Name ▲	Model	IP Address	Logs	DLP	Quar	IPS	Secure	Quota Usage
☐	🖥 User3	FG50BH		●	●	●	●	🔓	
☐	👤 FMG03K0000000000	FMG03K		●				🔓	
☐	📁 FGT60B3907503043		192.168.203.1	✕				🔓	

Which of the following statements best describes the reason why the FortiGate 60B unit is unable to archive data to the FortiAnalyzer unit?

A. The FortiGate unit is considered an unregistered device.

B. The FortiGate unit has been blocked from sending archive data to the FortiAnalyzer device by the administrator.

C. The FortiGate unit has insufficient privileges. The administrator should edit the device entry in the FortiAnalyzer and modify the privileges.

D. The FortiGate unit is being treated as a syslog device and is only permitted to send log data.

Correct Answer: A

QUESTION 14

An administrator has formed a High Availability cluster involving two FortiGate 310B units.

[Multiple upstream Layer 2 switches] -- [FortiGate HA Cluster] -- [Multiple downstream Layer 2 switches]

The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.

Which of the following options describes the best step the administrator can take?

The administrator should...

A. set up a full-mesh design which uses redundant interfaces.

B. increase the number of FortiGate units in the cluster and configure HA in Active-Active mode.

C. enable monitoring of all active interfaces.

D. configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

Correct Answer: A

QUESTION 15

Shown below is a section of output from the debug command diag ip arp list.

index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e state=00000004 use=4589 confirm=4589 update=2422 ref=1

In the output provided, which of the following best describes the IP address 172.20.187.150?

A. It is the primary IP address of the port1 interface.

B. It is one of the secondary IP addresses of the port1 interface.

C. It is the IP address of another network device located in the same LAN segment as the FortiGate unit\\'s port1 interface.

Correct Answer: C

Latest FCNSP.V5 Dumps   FCNSP.V5 Study Guide   FCNSP.V5 Exam Questions