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.pass2lead.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

A FortiGate administrator configures a Virtual Domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in Web Config in the management VDOM.

What would be a possible cause for this problem?

A. The dmz interface is referenced in the configuration of another VDOM.

B. The administrator does not have the proper permissions to reassign the dmz interface.

C. Non-management VDOMs can not reference physical interfaces.

D. The dmz interface is in PPPoE or DHCP mode.

E. Reassigning an interface to a different VDOM can only be done through the CLI.

Correct Answer: A

QUESTION 2

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

QUESTION 3

The following diagnostic output is displayed in the CLI:

diag firewall auth list

policy iD. 9, srC. 192.168.3.168, action: accept, timeout: 13427 user: forticlient_chk_only, group: flag (80020): auth timeout_ext, flag2 (40): exact group iD. 0, av group: 0 ----- 1 listed, 0 filtered -----

Based on this output, which of the following statements is correct?

A. Firewall policy 9 has endpoint compliance enabled but not firewall authentication.

B. The client check that is part of an SSL VPN connection attempt failed.

C. This user has been associated with a guest profile as evidenced by the group id of 0.

D. An auth-keepalive value has been enabled.

Correct Answer: A

QUESTION 4

You are the administrator in charge of a FortiGate unit which acts as a VPN gateway. You have chosen to use Interface Mode when configuring the VPN tunnel and you want users from either side to be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate unit already has a default route.

Which of the following configuration steps are required to achieve these objectives? (Select all that apply.)

A. Create one firewall policy.

B. Create two firewall policies.

C. Add a route for the remote subnet.

D. Add a route for incoming traffic.

E. Create a phase 1 definition.

F. Create a phase 2 definition.

Correct Answer: BCEF

QUESTION 5

Bob wants to send Alice a file that is encrypted using public key cryptography.

Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.

B. Bob will use his public key to encrypt the file and Alice will use Bob\\'s private key to decrypt the file.

C. Bob will use Alice\\'s public key to encrypt the file and Alice will use her private key to decrypt the file.

D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

E. Bob will use Alice\\'s public key to encrypt the file and Alice will use Bob\\'s public key to decrypt the file.

Correct Answer: C

QUESTION 6

Which of the following statements are correct regarding Application Control?

A. Application Control is based on the IPS engine.

B. Application Control is based on the AV engine.

C. Application Control can be applied to SSL encrypted traffic.

D. Application Control cannot be applied to SSL encrypted traffic.

Correct Answer: AC

QUESTION 7

Which of the following report templates must be used when scheduling report generation?

A. Layout Template

B. Data Filter Template

C. Output Template

D. Chart Template

Correct Answer: A

QUESTION 8

Which of the following statements is correct about configuring web filtering overrides?

A. The Override option for FortiGuard Web Filtering is available for any user group type.

B. Admin overrides require an administrator to manually allow pending override requests which are listed in the Override Monitor.

C. The Override Scopes of User and User Group are only for use when Firewall Policy Authentication is also being used.

D. Using Web Filtering Overrides requires the use of Firewall Policy Authentication.

Correct Answer: C

QUESTION 9

An administrator wishes to generate a report showing Top Traffic by service type, but wants to exclude SMTP traffic from the report.

Which of the following statements best describes how to do this?

A. In the Service field of the Data Filter, type 25/smtp and select the NOT checkbox.

B. Add the following entry to the Generic Field section of the Data Filter: service="!smtp".

C. When editing the chart, uncheck mlog to indicate that Mail Filtering data is being excluded when generating the chart.

D. When editing the chart, enter \\'dns\\' in the Exclude Service field.

Correct Answer: A

QUESTION 10

An administrator sets up a new FTP server on TCP port 2121. A FortiGate unit is located between the FTP clients and the server. The administrator has created a policy for TCP port 2121.

Users have been complaining that when downloading data they receive a 200 Port command successful message followed by a 425 Cannot build data connection message.

Which of the following statements represents the best solution to this problem?

A. Create a new session helper for the FTP service monitoring port 2121.

B. Enable the ANY service in the firewall policies for both incoming and outgoing traffic.

C. Place the client and server interface in the same zone and enable intra-zone traffic.

D. Disable any protection profiles being applied to FTP traffic.

Correct Answer: A

QUESTION 11

A network administrator connects his PC to the INTERNAL interface on a FortiGate unit. The administrator

attempts to make an HTTPS connection to the FortiGate unit on the VLAN1 interface at the IP address of

10.0.1.1, but gets no connectivity.

The following troubleshooting commands are executed from the CLI:

user1 # get system interface

== [internal]

namE. internal modE. static ip: 10.0.1.254 255.255.255.128 status: up netbios-forwarD. disable typE.

physical mtu-overridE. disable == [vlan1]

namE. vlan1 modE. static ip: 10.0.1.1 255.255.255.128 status: up netb ios-forwarD. disable typE. vlan mtuoverridE. disable

user1 # get router info routing-table all

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF

external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default

S 10.0.0.0/8 [10/0] is a summary, Null

C 10.0.1.0/25 is directly connected, vlan1

C 10.0.1.128/25 is directly connected, internal

user1 # diagnose debug flow trace start 100

user1 # diagnose debug ena

user1 # diagnose debug flow filter daddr 10.0.1.1 10.0.1.1

id=20085 trace_id=277 msg="vd-root received a packet(proto=6, 10.0.1.130 :47922->10.0.1.1:443) from

internal."

id=20085 trace_id=277 msg="allocate a new session-00000b21" id=20085 trace_id=277

msg="iprope_in_check() check failed, drop" Based on the output from these commands, which of the

following is a possible cause of the problem?

A. The FortiGate unit has no route back to the PC.

B. The PC has an IP address in the wrong subnet.

C. The PC is using an incorrect default gateway IP address.

D. There is no firewall policy allowing traffic from INTERNAL -> VLAN1.

Correct Answer: D

QUESTION 12

The eicar test virus is put into a zip archive, which is given the password of "Fortinet" in order to open the archive. Review the configuration in the exhibits shown below; then answer the question that follows.

Exhibit A Antivirus Profile:

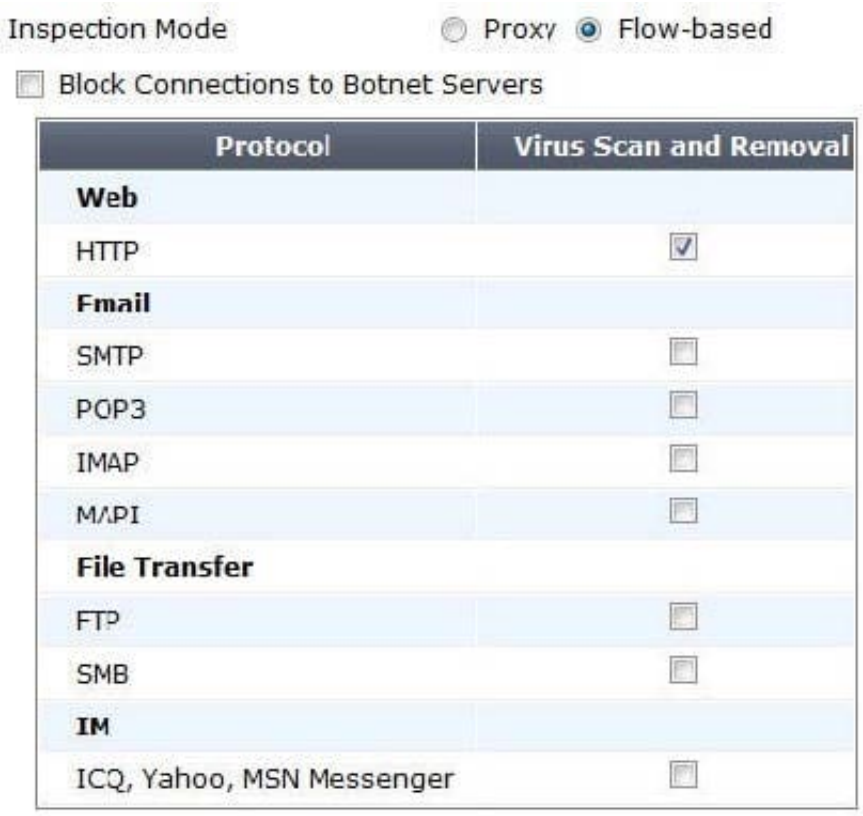
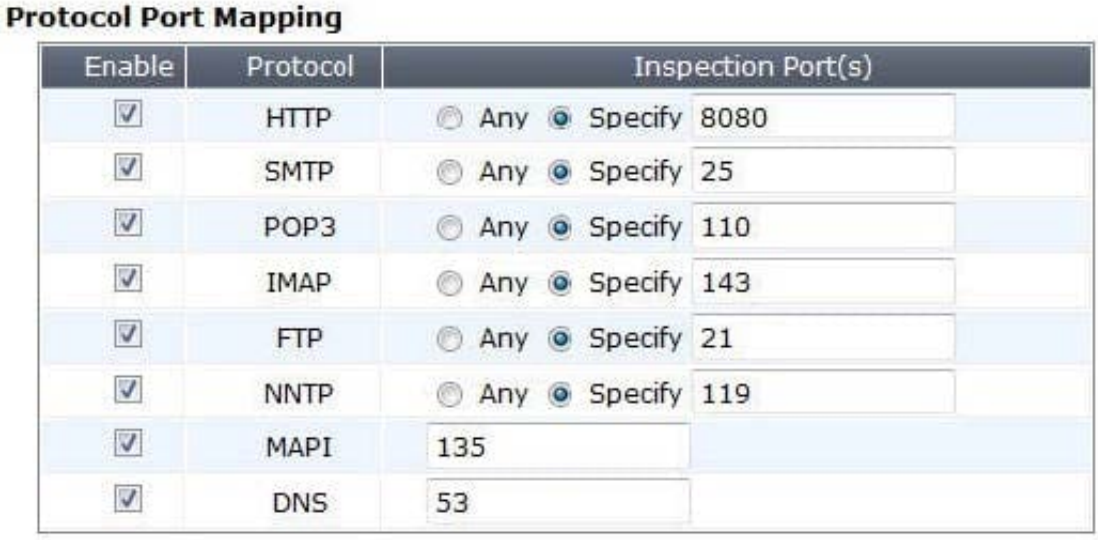


Exhibit B Non-default UTM Proxy Options Profile: Exhibit C DLP Profile:



Which of one the following profiles could be enabled in order to prevent the file from passing through the FortiGate device over HTTP on the standard port for that protocol?

A. Only Exhibit A

B. Only Exhibit B

C. Only Exhibit C with default UTM Proxy settings.

D. All of the Exhibits (A, B and C)

E. Only Exhibit C with non-default UTM Proxy settings (Exhibit B).

Correct Answer: C

QUESTION 13

WAN optimization is configured in Active/Passive mode. When will the remote peer accept an attempt to initiate a tunnel?

A. The attempt will be accepted when the request comes from a known peer and there is a matching WAN optimization passive rule.

B. The attempt will be accepted when there is a matching WAN optimization passive rule.

C. The attempt will be accepted when the request comes from a known peer.

D. The attempt will be accepted when a user on the remote peer accepts the connection request.

Correct Answer: A

QUESTION 14

How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

A. File TypE. Microsoft Office(msoffice)

B. File TypE. Archive(zip)

C. File TypE. Unknown Filetype(unknown)

D. File NamE. "*.ppt", "*.doc", "*.xls"

E. File NamE. "*.pptx", "*.docx", "*.xlsx"

Correct Answer: BE

QUESTION 15

Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. ICMP type and code

B. TCP/UDP source and destination ports

C. IP protocol number

D. TCP sequence number

Correct Answer: D