DUMPSARENA

Fortinet NSE 4 - FortiOS 7.0

Fortinet NSE4_FGT-7.0

Version Demo

Total Demo Questions: 10

Total Premium Questions: 190

Buy Premium PDF

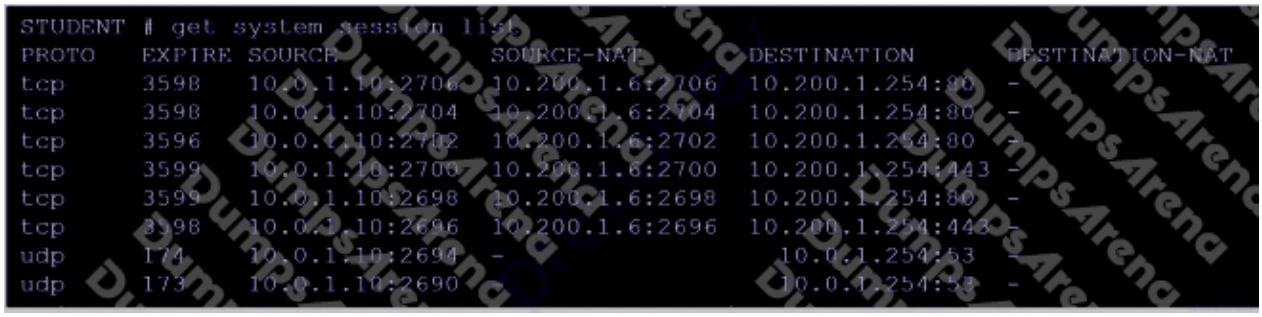
https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Refer to the exhibit, which contains a session list output.



Based on the information shown in the exhibit, which statement is true?

A. One-to-one NAT IP pool is used in the firewall policy.

B. Destination NAT is disabled in the firewall policy.

C. Port block allocation IP pool is used in the firewall policy.

D. Overload NAT IP pool is used in the firewall policy.

ANSWER: A

QUESTION NO: 2

Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.

B. In flow-based inspection mode, files bigger than the buffer size are scanned.

C. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

D. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.

ANSWER: C D

QUESTION NO: 3

Refer to the exhibit.

Which contains a network diagram and routing table output.

The Student is unable to access Webserver.

What is the cause of the problem and what is the solution for the problem?

A. The first packet sent from Student failed the RPF check.
This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.

B. The first reply packet for Student failed the RPF check.
This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.

C. The first reply packet for Student failed the RPF check.
This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

D. The first packet sent from Student failed the RPF check.
This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

ANSWER: D

QUESTION NO: 4

Examine the following web filtering log.

```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

Which statement about the log message is true?

A. The action for the category Games is set to block.

B. The usage quota for the IP address 10.0.1.10 has expired

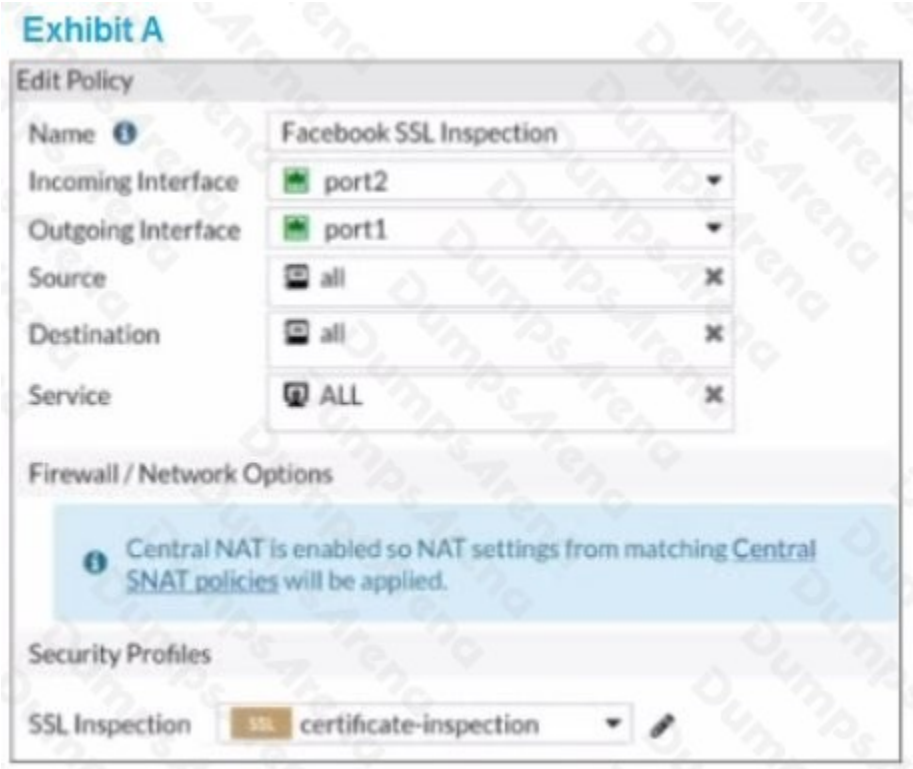
C. The name of the applied web filter profile is default.

D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

ANSWER: C

QUESTION NO: 5

Refer to the exhibits.



The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) tor Facebook.

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

A. The SSL inspection needs to be a deep content inspection.

B. Force access to Facebook using the HTTP service.

C. Additional application signatures are required to add to the security policy.

D. Add Facebook in the URL category in the security policy.

ANSWER: A

Explanation:

The lock logo behind Facebook_like.Button indicates that SSL Deep Inspection is Required.

QUESTION NO: 6

Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
 if (shExpMatch (url, "*.fortinet.com/*")) {
    return "DIRECT";}
 if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
    return "PROXY" altproxy.corp.com: 8060";}
 return "PROXY proxy.corp.com: 8090";
}
```

Which of the following statements are true? (Choose two.)

A. Browsers can be configured to retrieve this PAC file from the FortiGate.

B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.

C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.

D. Any web request fortinet.com is allowed to bypass the proxy.

ANSWER: A D

QUESTION NO: 7

Which two statements are true about the Security Fabric rating? (Choose two.)

A. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.

B. Many of the security issues can be fixed immediately by clicking Apply where available.

C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.

D. It provides executive summaries of the four largest areas of security focus.

ANSWER: B C

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/292634/security-rating

QUESTION NO: 8

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.

ANSWER: A C

Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD48755

QUESTION NO: 9

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on

which device?

A. FortiManager

B. Root FortiGate

C. FortiAnalyzer

D. Downstream FortiGate

ANSWER: B

QUESTION NO: 10

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.

ANSWER: A B

Explanation:

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