

Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0



NEW QUESTION 1

- (Exam Topic 1)

Refer to the exhibit.

The screenshot shows the 'Add Signatures' configuration window. The settings are as follows:

- Type: Signature
- Action: Block
- Packet logging: Enable
- Status: Enable
- Rate-based settings: Default
- Exempt IPs: 0

Below the settings is a table with the following data:

| Name | Severity | Target | OS | Action | CVE-ID |
|------------------|----------|--------|-----|--------|--------|
| FTP.Login.Failed | High | Server | All | Pass | |

The 'Selected' count is 1.

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

Answer: D

Explanation:

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 2

- (Exam Topic 1)

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

- A. Proxy-based inspection
- B. Certificate inspection
- C. Flow-based inspection
- D. Full Content inspection

Answer: AC

NEW QUESTION 3

- (Exam Topic 1)

Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

- A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
- B. To finish any inspection operations
- C. To remove the NAT operation
- D. To generate logs

Answer: A

Explanation:

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

NEW QUESTION 4

- (Exam Topic 1)

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

Answer: CD

NEW QUESTION 5

- (Exam Topic 1)

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, FortiGate buffers the file, but also simultaneously transmits it to the client.
- C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
- D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: BC

Explanation:

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM—something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

NEW QUESTION 6

- (Exam Topic 1)

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

- A. The keyUsage extension must be set to keyCertSign.
- B. The common name on the subject field must use a wildcard name.
- C. The issuer must be a public CA.
- D. The CA extension must be set to TRUE.

Answer: AD

Explanation:

Reference: https://www.reddit.com/r/fortinet/comments/c7j6jg/recommended_ssl_cert/

NEW QUESTION 7

- (Exam Topic 1)

When configuring a firewall virtual wire pair policy, which following statement is true?

- A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
- B. Only a single virtual wire pair can be included in each policy.
- C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
- D. Exactly two virtual wire pairs need to be included in each policy.

Answer: A

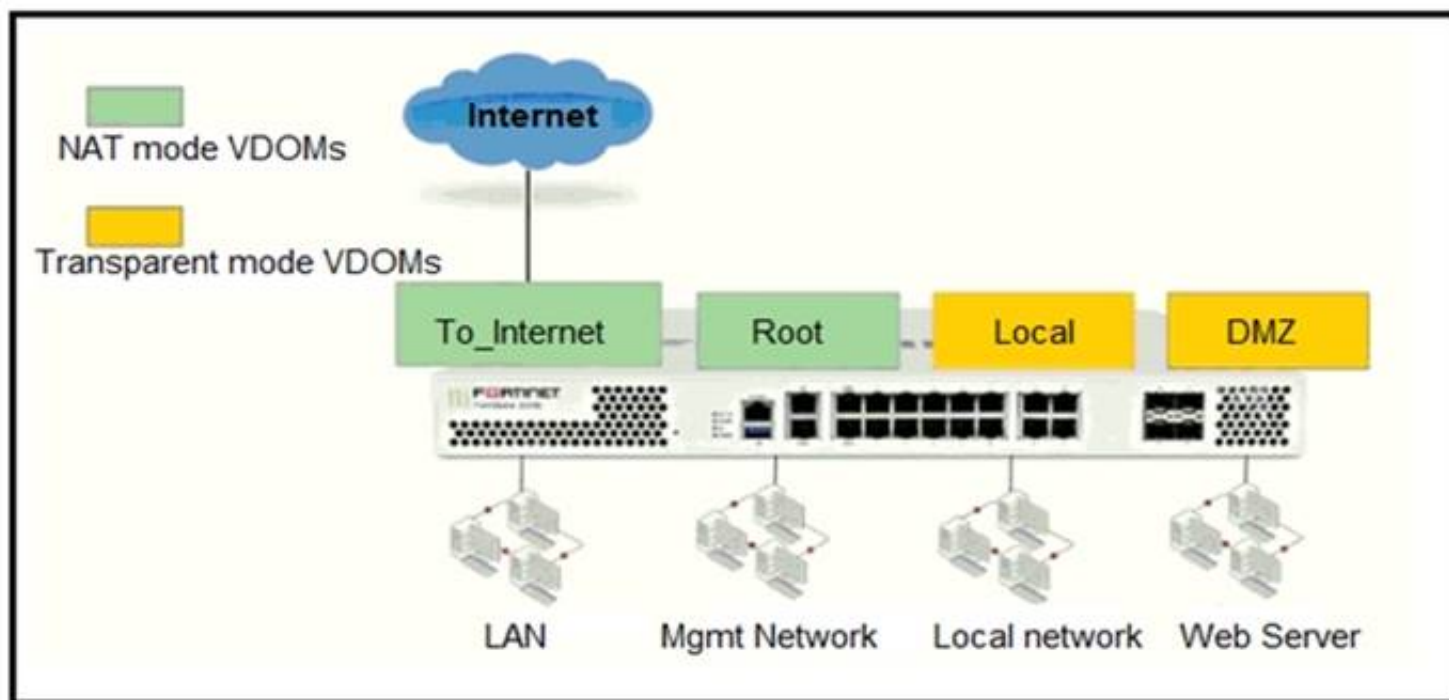
Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48690>

NEW QUESTION 8

- (Exam Topic 1)

Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode. The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem. With this configuration, which statement is true?

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542>

NEW QUESTION 9

- (Exam Topic 1)

Refer to the exhibits.
 Exhibit A.

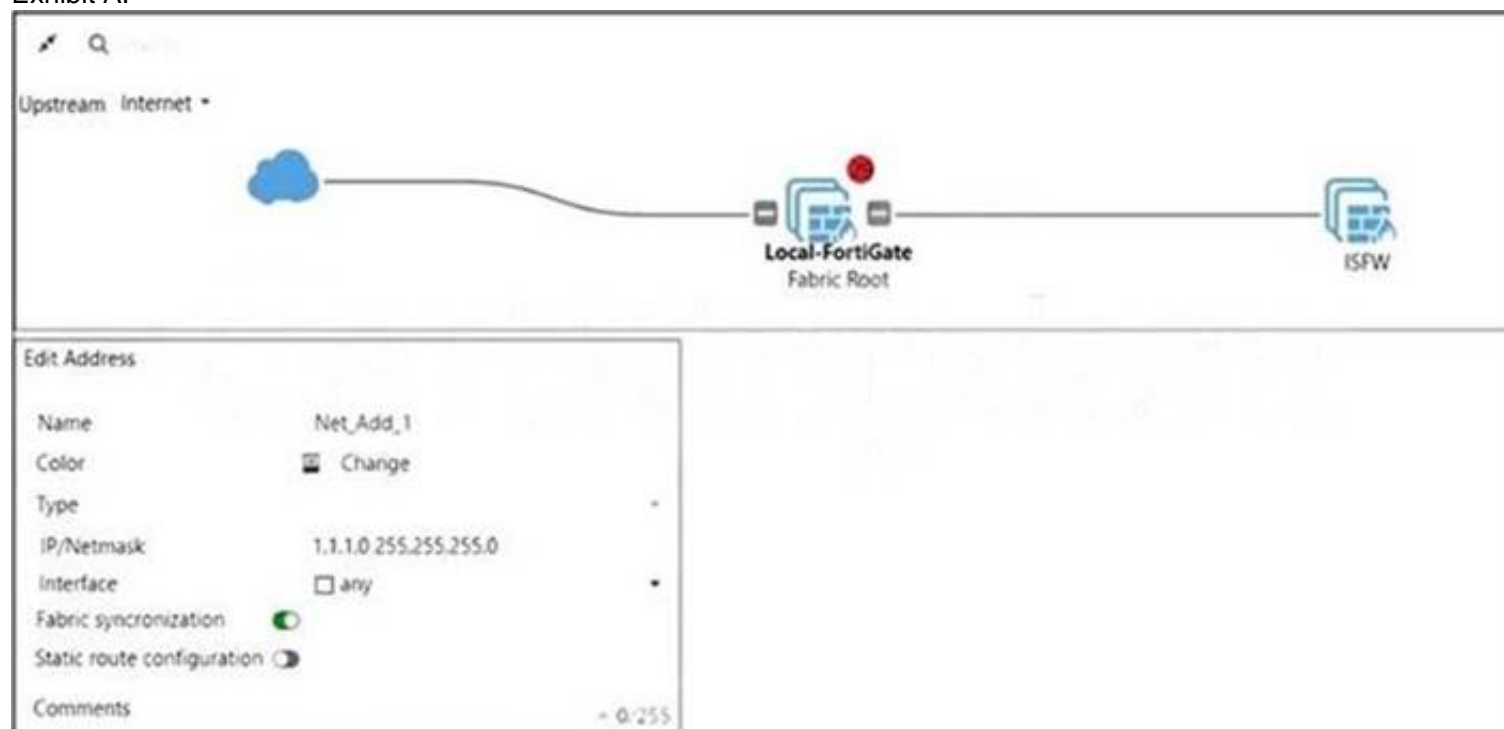


Exhibit B.

```

Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 0.0.0.0
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC X18CtzrcUBUq9yz9nryP+YfM16
    BJKv7S/trtoh2gYAe5CH8YMAa0GT18aX+/dKH/o5izw1ZEoN1QN2N
    PGLT4r5z2AyYI8i1PxutiLcsCplAdZadv1Cx0e66IdLX7I6o22J9P
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml-configuration-sync default
    
```

```

ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 10.0.1.254
    set upstream-port 8013
    set group-name ""
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync default
end
ISFW #
ISFW #
    
```

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).
 What must the administrator do to synchronize the address object?

- A. Change the csf setting on Local-FortiGate (root) to sec configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
- C. Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion defaultc.
- D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaultc.

Answer: A

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD43820>

NEW QUESTION 10

- (Exam Topic 1)

Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

- A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
- B. The application signature database inspects traffic only from the original web application server.
- C. FortiGuard maintains only one signature of each web application that is unique.
- D. FortiGate can inspect sub-application traffic regardless where it was originated.

Answer: D

Explanation:

Reference:

https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300_System/303d_FortiG

NEW QUESTION 10

- (Exam Topic 1)

By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

- A. set fortiguard-anycast disable
- B. set webfilter-force-off disable
- C. set webfilter-cache disable
- D. set protocol tcp

Answer: A

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48294>

NEW QUESTION 12

- (Exam Topic 1)

Refer to the exhibit.

| | Name | Type | IP/Netmask | VLAN ID |
|-----------------------|--------------|--------------------|--------------------------|---------|
| Physical Interface 14 | | | | |
| | port1 | Physical Interface | 10.200.1.1/255.255.255.0 | |
| | port1-vlan10 | VLAN | 10.1.10.1/255.255.255.0 | 10 |
| | port1-vlan1 | VLAN | 10.200.5.1/255.255.255.0 | 1 |
| | port10 | Physical Interface | 10.0.11.1/255.255.255.0 | |
| | port2 | Physical Interface | 10.200.2.1/255.255.255.0 | |
| | port2-vlan10 | VLAN | 10.0.10.1/255.255.255.0 | 10 |
| | port2-vlan1 | VLAN | 10.0.5.1/255.255.255.0 | 1 |

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

- A. Traffic between port2 and port2-vlan1 is allowed by default.
- B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- C. port1 is a native VLAN.
- D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Answer: CD

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf>

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883>

NEW QUESTION 13

- (Exam Topic 2)

View the exhibit:

| ⌵ Status | ⌵ Name | ⌵ VLAN ID | ⌵ Type | ⌵ IP/Netmask |
|--------------|--------------|-----------|--------------------|---------------------------|
| Physical(12) | | | | |
| | port1 | | Physical Interface | 10.200.1.1 255.255.255.0 |
| | port1-VLAN1 | 1 | VLAN | 10.200.5.1 255.255.255.0 |
| | port1-VLAN10 | 10 | VLAN | 10.0.10.1 255.255.255.0 |
| | port2 | | Physical Interface | 10.200.2.1 255.255.255.0 |
| | port2-VLAN1 | 1 | VLAN | 10.0.5.1 255.255.255.0 |
| | port2-VLAN10 | 10 | VLAN | 10.0.20.254 255.255.255.0 |
| | port3 | | Physical Interface | 10.0.1.254 255.255.255.0 |

Which the FortiGate handle web proxy traffic rue? (Choose two.)

- A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
- B. port-VLAN1 is the native VLAN for the port1 physical interface.
- C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
- D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: AC

NEW QUESTION 14

- (Exam Topic 2)

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.

What should the administrator do next to troubleshoot the problem?

- A. Run a sniffer on the web server.
- B. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10"
- D. Execute a debug flow.

Answer: D

NEW QUESTION 18

- (Exam Topic 2)

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

Answer: AD

NEW QUESTION 23

- (Exam Topic 2)

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The subject field in the server certificate
- B. The serial number in the server certificate
- C. The server name indication (SNI) extension in the client hello message
- D. The subject alternative name (SAN) field in the server certificate
- E. The host field in the HTTP header

Answer: ACD

Explanation:

Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>

NEW QUESTION 26

- (Exam Topic 2)

Which two statements are true about the RPF check? (Choose two.)

- A. The RPF check is run on the first sent packet of any new session.
- B. The RPF check is run on the first reply packet of any new session.
- C. The RPF check is run on the first sent and reply packet of any new session.
- D. RPF is a mechanism that protects FortiGate and your network from IP spoofing attacks.

Answer: AD

Explanation:

Reference: <https://www.programmersought.com/article/16383871634/>

NEW QUESTION 30

- (Exam Topic 2)

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID

D. Sequence ID

Answer: B

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies>

NEW QUESTION 35

- (Exam Topic 2)

An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.2" 5
```

Which three pieces of Information will be Included in the sniffer output? {Choose three.}

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

Answer: ABD

NEW QUESTION 38

- (Exam Topic 2)

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

NEW QUESTION 43

- (Exam Topic 2)

Which feature in the Security Fabric takes one or more actions based on event triggers?

- A. Fabric Connectors
- B. Automation Stitches
- C. Security Rating
- D. Logical Topology

Answer: B

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/286973/fortinet-security-fabric>

NEW QUESTION 44

- (Exam Topic 2)

NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

- A. Web filtering
- B. Antivirus
- C. Web proxy
- D. Application control

Answer: B

NEW QUESTION 46

- (Exam Topic 2)

Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match. Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to Main (ID protection).
- B. On both FortiGate devices, set Dead Peer Detection to On Demand.
- C. On HQ-FortiGate, disable Diffie-Helman group 2.
- D. On Remote-FortiGate, set port2 as Interface.

Answer: AD

NEW QUESTION 48

- (Exam Topic 2)

Which of statement is true about SSL VPN web mode?

- A. The tunnel is up while the client is connected.
- B. It supports a limited number of protocols.
- C. The external network application sends data through the VPN.
- D. It assigns a virtual IP address to the client.

Answer: B

Explanation:

FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 49

- (Exam Topic 2)

Refer to the exhibit to view the firewall policy.

| | | |
|---------------------|-----------------------------|--|
| Name | Internet Access | |
| Incoming Interface | port2 | |
| Outgoing Interface | port1 | |
| Source | all | |
| Destination | all | |
| Schedule | always | |
| Service | DNS FTP HTTP HTTPS | |
| Action | ACCEPT DENY | |
| Inspection Mode | Flow-based Proxy-based | |
| Security Profiles | | |
| AntiVirus | AV default | |
| Web Filter | | |
| DNS Filter | | |
| Application Control | | |
| IPS | | |

Which statement is correct if well-known viruses are not being blocked?

- A. The firewall policy does not apply deep content inspection.
- B. The firewall policy must be configured in proxy-based inspection mode.
- C. The action on the firewall policy must be set to deny.
- D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

Answer: A

NEW QUESTION 53

- (Exam Topic 2)
Which two statements are true about collector agent standard access mode? (Choose two.)

- A. Standard mode uses Windows convention-NetBios: Domain\Username.
- B. Standard mode security profiles apply to organizational units (OU).
- C. Standard mode security profiles apply to user groups.
- D. Standard access mode supports nested groups.

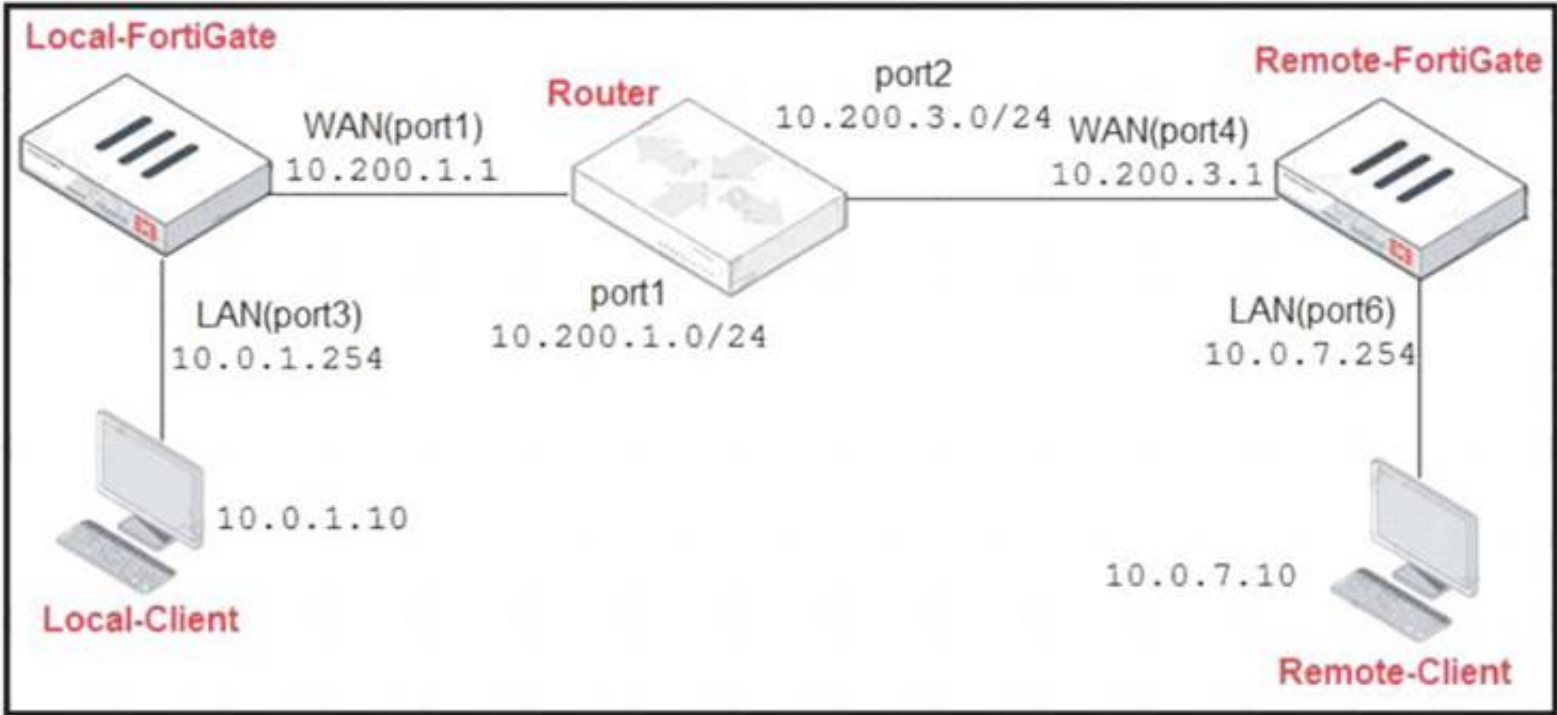
Answer: AC

Explanation:
Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>

NEW QUESTION 58

- (Exam Topic 2)
Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

| ID | From | To | Source Address | Protocol Number | Destination Address | Translated Address |
|----|------------|------------|----------------|-----------------|---------------------|--------------------|
| 2 | LAN(port3) | WAN(port1) | all | 6 | REMOTE_FORTIGATE | SNAT-Pool |
| 1 | LAN(port3) | WAN(port1) | all | 1 | all | SNAT-Remote1 |
| 3 | LAN(port3) | WAN(port1) | all | 2 | all | SNAT-Remote |

IP Pool Local-FortiGate

| Name | External IP Range | Type | ARP Reply |
|--------------|---------------------------|----------|-----------|
| SNAT-Pool | 10.200.1.49-10.200.1.49 | Overload | Enabled |
| SNAT-Remote | 10.200.1.149-10.200.1.149 | Overload | Enabled |
| SNAT-Remote1 | 10.200.1.99-10.200.1.99 | Overload | Enabled |

Protocol Number Table

| Protocol | Protocol Number |
|----------|-----------------|
| TCP | 6 |
| ICMP | 1 |
| IGMP | 2 |

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24. A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied. Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

- A. 10.200.1.149
- B. 10.200.1.1
- C. 10.200.1.49
- D. 10.200.1.99

Answer: D

NEW QUESTION 60

- (Exam Topic 2)
 Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 62

- (Exam Topic 2)

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

Answer: AD

NEW QUESTION 66

- (Exam Topic 2)

Exhibit:



```
Fortigate # show authentication rule
config authentication rule
    edit "NTLM_rule"
        set srcaddr "all"
        set ip-based disable
        set web-auth-cookie enable
    next
end
```

Refer to the exhibit to view the authentication rule configuration. In this scenario, which statement is true?

- A. IP-based authentication is enabled
- B. Route-based authentication is enabled
- C. Session-based authentication is enabled.
- D. Policy-based authentication is enabled

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD45387>

NEW QUESTION 67

- (Exam Topic 2)

Examine this FortiGate configuration:

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:

“What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting”

NEW QUESTION 69

- (Exam Topic 2)

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

Answer: D

NEW QUESTION 71

- (Exam Topic 2)

What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

- A. Traffic to botnetservers
- B. Traffic to inappropriate web sites
- C. Server information disclosure attacks
- D. Credit card data leaks
- E. SQL injection attacks

Answer: CDE

NEW QUESTION 73

- (Exam Topic 2)

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The Services field prevents SNAT and DNAT from being combined in the same policy.
- B. The Services field is used when you need to bundle several VIPs into VIP groups.
- C. The Services field removes the requirement to create multiple VIPs for different services.
- D. The Services field prevents multiple sources of traffic from using multiple services to connect to a singlecomputer.

Answer: C

NEW QUESTION 76

- (Exam Topic 2)

Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

- A. Fabric Coverage
- B. Automated Response
- C. Security Posture
- D. Optimization

Answer: C

Explanation:

Reference:

<https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-bestpractices.pdf>

NEW QUESTION 78

- (Exam Topic 2)

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
- B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
- C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
- D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Answer: B

Explanation:

Reference: <http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html>

NEW QUESTION 79

- (Exam Topic 2)

Consider the topology:

Application on a Windows machine <--(SSL VPN) -->FGT--> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.

The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

- A. Set the maximum session TTL value for the TELNET service object.
- B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
- C. Create a new service object for TELNET and set the maximum session TTL.
- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer: CD

NEW QUESTION 82

- (Exam Topic 2)

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only
- D. It limits the scope of application control to scan application traffic on DNS protocol only.

Answer: A

NEW QUESTION 86

- (Exam Topic 2)

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

Answer: ABC

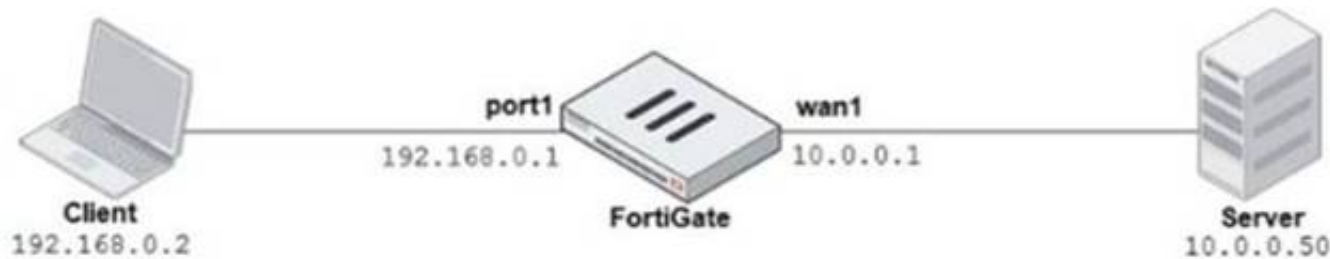
Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

NEW QUESTION 87

- (Exam Topic 2)

Refer to the exhibit.



Explicit Proxy

Explicit Web Proxy

Listen on Interfaces

port1

+

x

HTTP Port

8080 - 8080

HTTPS Port

Use HTTP Port Specify

FTP over HTTP

Proxy auto-config (PAC)

Proxy FQDN

default.fqdn

Max HTTP request length

8 KB

Max HTTP message length

32 KB

Unknown HTTP version

Best Effort Reject

Realm

default

Default Firewall Policy Action

Accept Deny

The exhibits show a network diagram and the explicit web proxy configuration.

In the command diagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

- A. 'host 192.168.0.2 and port 8080'
- B. 'host 10.0.0.50 and port 80'
- C. 'host 192.168.0.1 and port 80'
- D. 'host 10.0.0.50 and port 8080'

Answer: A

NEW QUESTION 91

- (Exam Topic 2)

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 94

- (Exam Topic 2)

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

- A. remote user’s public IP address
- B. The public IP address of the FortiGate device.
- C. The remote user’s virtual IP address.
- D. The internal IP address of the FortiGate device.

Answer: D

Explanation:

Source IP seen by the remote resources is FortiGate’s internal IP address and not the user’s IP address

NEW QUESTION 95

- (Exam Topic 2)

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

| + Create New Edit Clone Delete | | | | |
|--------------------------------------|------------------|-----------|----------|----------|
| Destination | Gateway | Interface | Priority | Distance |
| 172.20.168.0/24 | 172.25.1 76.1 | port1 | 10 | 20 |
| 172.20.168.0/24 | 172.25.1 78.1 | 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

Answer: B

Explanation:

“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.”

NEW QUESTION 97

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE4_FGT-7.0 Practice Exam Features:

- * NSE4_FGT-7.0 Questions and Answers Updated Frequently
- * NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT-7.0 Practice Test Here](#)