



# Fortinet

## Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

**Answer: B**

### NEW QUESTION 2

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

**Answer: ABD**

#### Explanation:

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

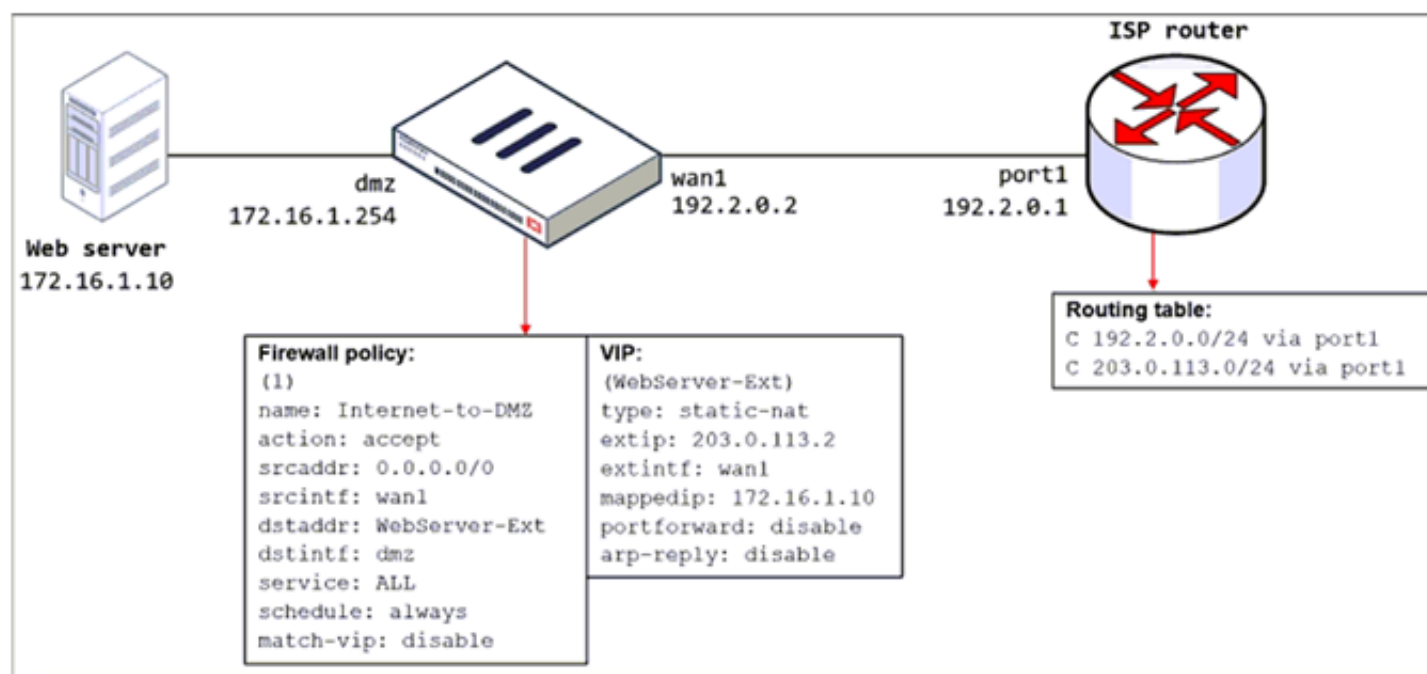
- Incoming Interface
- Outgoing Interface
- Source: IP address, user, internet services
- Destination: IP address or internet services
- Service: IP protocol and port number
- Schedule: Applies during configured times

### NEW QUESTION 3

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

- A. Configure a loopback interface with address 203.0.113.2/32.
- B. In the VIP configuration, enable arp-reply.
- C. Enable port forwarding on the server to map the external service port to the internal service port.
- D. In the firewall policy configuration, enable match-vip.

**Answer: D**

### NEW QUESTION 4

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not. Which configuration option is the most effective way to support this request?

- A. Implement a web filter category override for the specified website
- B. Implement a DNS filter for the specified website.
- C. Implement web filter quotas for the specified website
- D. Implement web filter authentication for the specified website.

**Answer: D**

#### NEW QUESTION 5

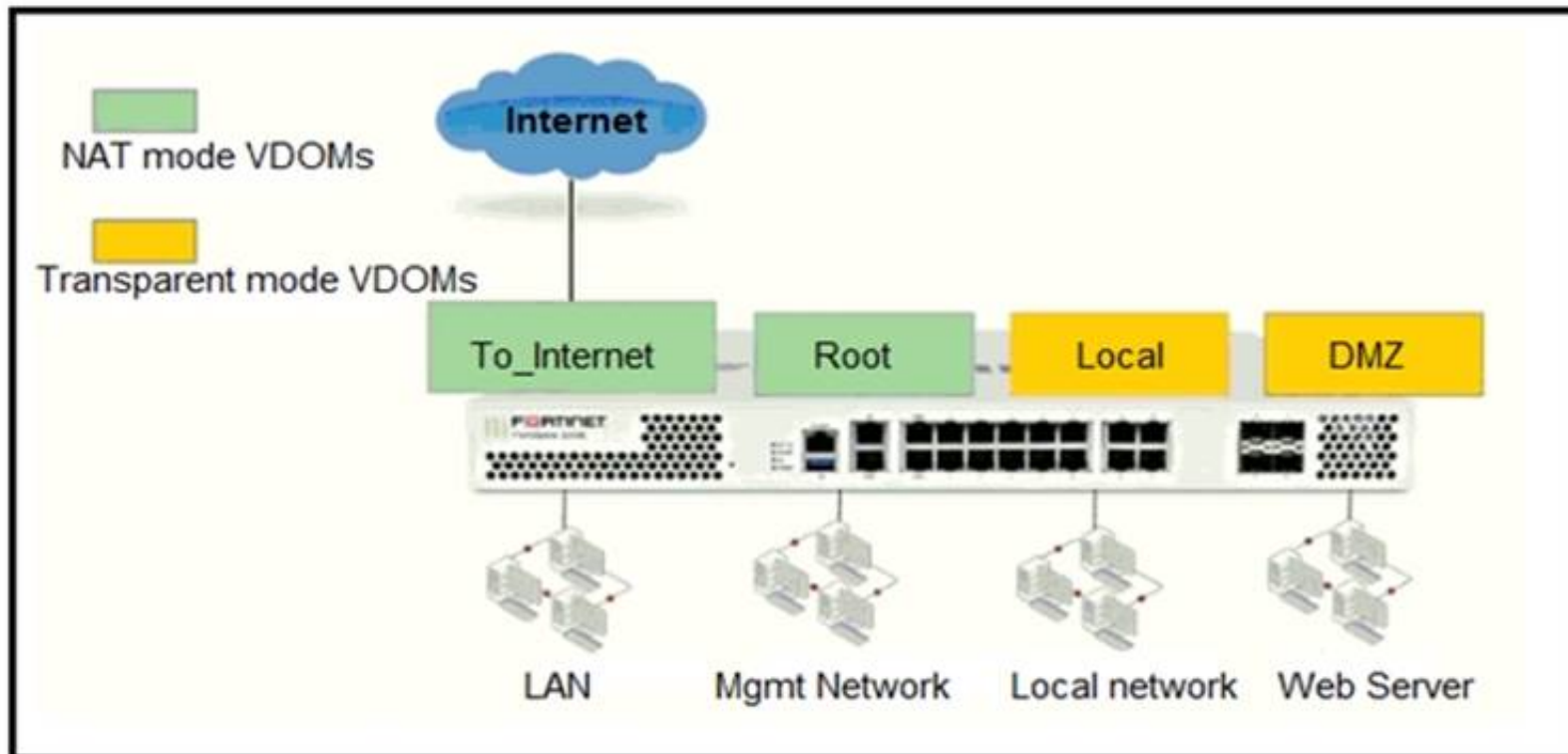
You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk . What is the default behavior when the local disk is full?

- A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.
- B. No new log is recorded until you manually clear logs from the local disk .
- C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.
- D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

**Answer: C**

#### NEW QUESTION 6

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**

#### NEW QUESTION 7

An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

- A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
- B. Create a new service object for HTTP service and set the session TTL to never
- C. Set the TTL value to never under config system-ttl
- D. Set the session TTL on the HTTP policy to maximum

**Answer: BC**

#### NEW QUESTION 8

Which two statements explain antivirus scanning modes? (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 9

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:**

y default, "fortiguard-anycast" is enabled, and this setting only works with "set protocol https". To use udp (ie. "set protocol udp"), "fortiguard-anycast" must be disabled.

**NEW QUESTION 10**

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 10**

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

- A. The administrator can register the same FortiToken on more than one FortiGate.
- B. The administrator must use a FortiAuthenticator device
- C. The administrator can use a third-party radius OTP server.
- D. The administrator must use the user self-registration server.

**Answer:** B

**NEW QUESTION 13**

Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

- A. Security policy
- B. SSL inspection and authentication policy CD

**Answer:** AB

**NEW QUESTION 17**

Which timeout setting can be responsible for deleting SSL VPN associated sessions?

- A. SSL VPN idle-timeout
- B. SSL VPN http-request-body-timeout
- C. SSL VPN login-timeout
- D. SSL VPN dtls-hello-timeout

**Answer:** A

**NEW QUESTION 22**

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

**Answer:** D

**NEW QUESTION 26**

Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

- A. Subject Key Identifier value
- B. SMMIE Capabilities value
- C. Subject value
- D. Subject Alternative Name value

**Answer:** A

**NEW QUESTION 27**

Refer to the exhibit.



```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

**Answer:** A

### NEW QUESTION 32

Refer to the exhibit.



Access Control	Permissions	Set All
Security Fabric	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
FortiView	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
User & Device	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Firewall	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
VPN	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
WAN Opt & Cache	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
WiFi & Switch	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	

Permit usage of CLI diagnostic commands ☐

☐ Override Idle Timeout

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

- A. Custom permission for Network
- B. Read/Write permission for Log & Report
- C. CLI diagnostics commands permission
- D. Read/Write permission for Firewall

**Answer:** C

### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220>

### NEW QUESTION 33

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

NEW QUESTION 36

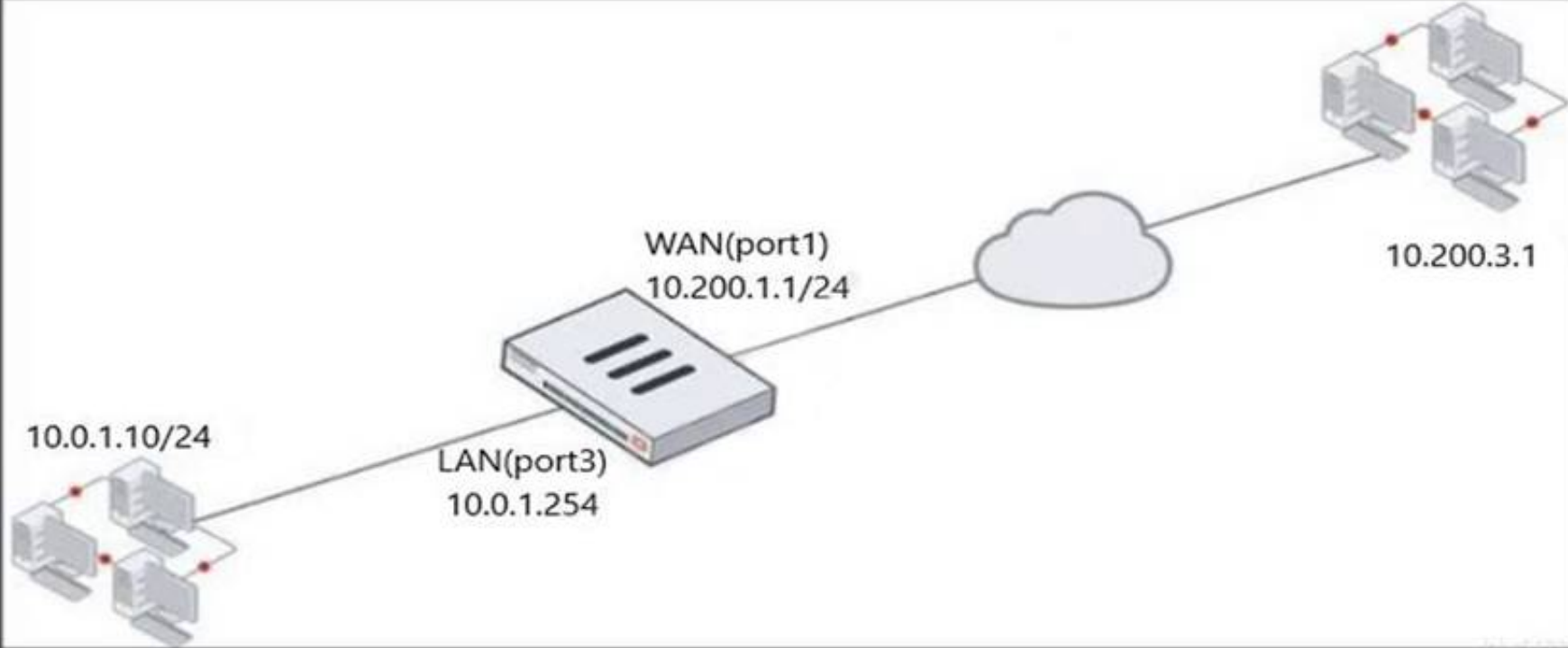
In an explicit proxy setup, where is the authentication method and database configured?

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

Answer: D

NEW QUESTION 41

Refer to the exhibit.



ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT
1	Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT	IP Pool
2	WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Disabled

VIP type: IPv4

Name: VIP

Comments: Write a comment... 0/255

Color: Change

Network

Interface: port1

Type: Static NAT

External IP addresses/range: 10.200.1.10

Mapped IP addresses/range: 10.0.1.10

Optional Filters

Source Address: 10.200.3.1

Services: ALL\_ICMP, HTTP, HTTPS

Name: IP Pool

Comments: Write a comment... 0/255

Type: Overload, One-to-One, Fixed Port Range, Port Block Allocation

External IP address/range: 10.200.1.100-10.200.1.100

ARP Reply: On

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies 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.

The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0. 1. 10?

- A. 10.200. 1. 1
- B. 10.200.3. 1

C. 10.200. 1. 100  
D. 10.200. 1. 10

**Answer:** C

**Explanation:**

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

**NEW QUESTION 42**

Refer to the exhibits.



Exhibit A shows the configuration for a policy named "Facebook SSL Inspection". The configuration is as follows:

Field	Value
Name	Facebook SSL Inspection
Incoming interface	port2
Outgoing interface	port1
Source	all
Destination	all
Service	ALL

Below the configuration, there is a section for "Firewall/Network Options" with a message: "CentralNAT is enabled so NAT settings from matching Central SNAT policies will be applied".

At the bottom, there is a section for "Security Profiles" with "SSL Inspection" set to "certificate-inspection".

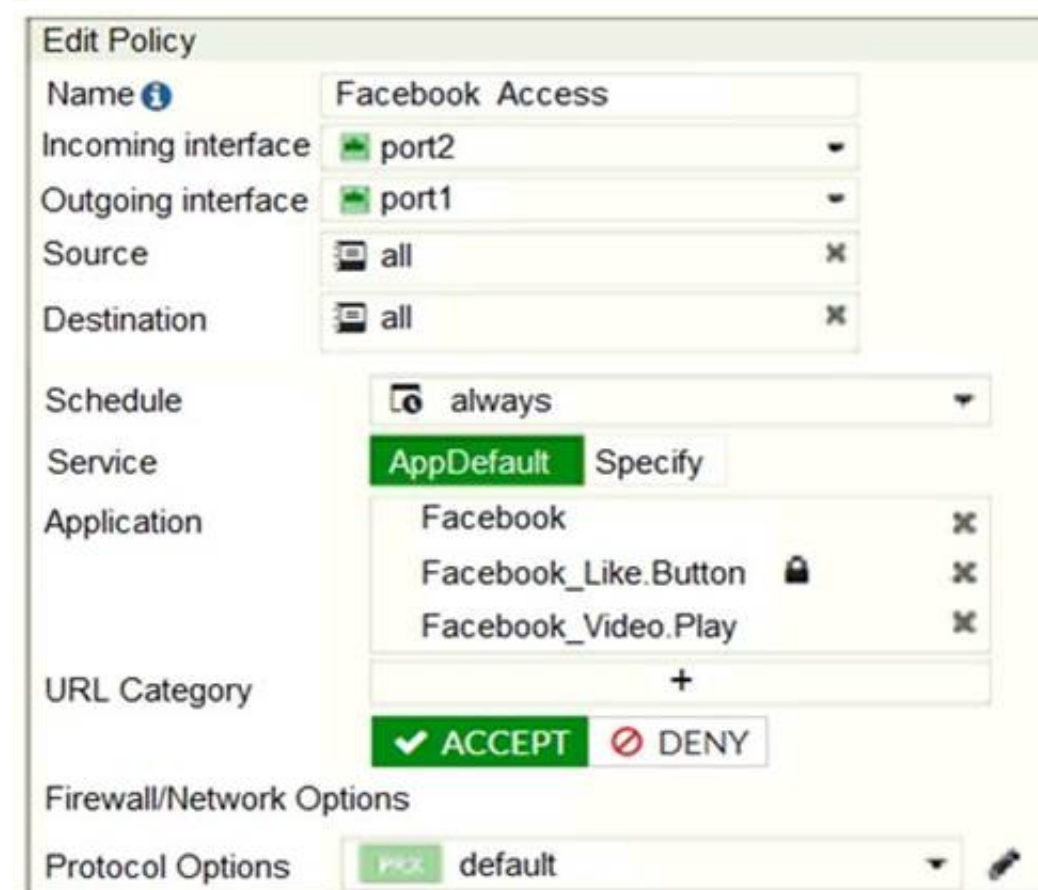


Exhibit B shows the configuration for a policy named "Facebook Access". The configuration is as follows:

Field	Value
Name	Facebook Access
Incoming interface	port2
Outgoing interface	port1
Source	all
Destination	all
Schedule	always
Service	AppDefault
Application	Facebook, Facebook_Like.Button, Facebook_Video.Play
URL Category	+
Action	ACCEPT

Below the configuration, there is a section for "Firewall/Network Options" with "Protocol Options" set to "default".

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for 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. Make SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Get the 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:**

They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather then adding an app rule.

**NEW QUESTION 44**

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



- A. IP tool references must be removed from existing firewall policies before enabling central NAT .
- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

**Answer:** AB

#### NEW QUESTION 48

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

- A. It provides executive summaries of the four largest areas of security focus.
- 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. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.

**Answer:** BC

#### NEW QUESTION 51

Refer to the exhibits.  
 Exhibit A.

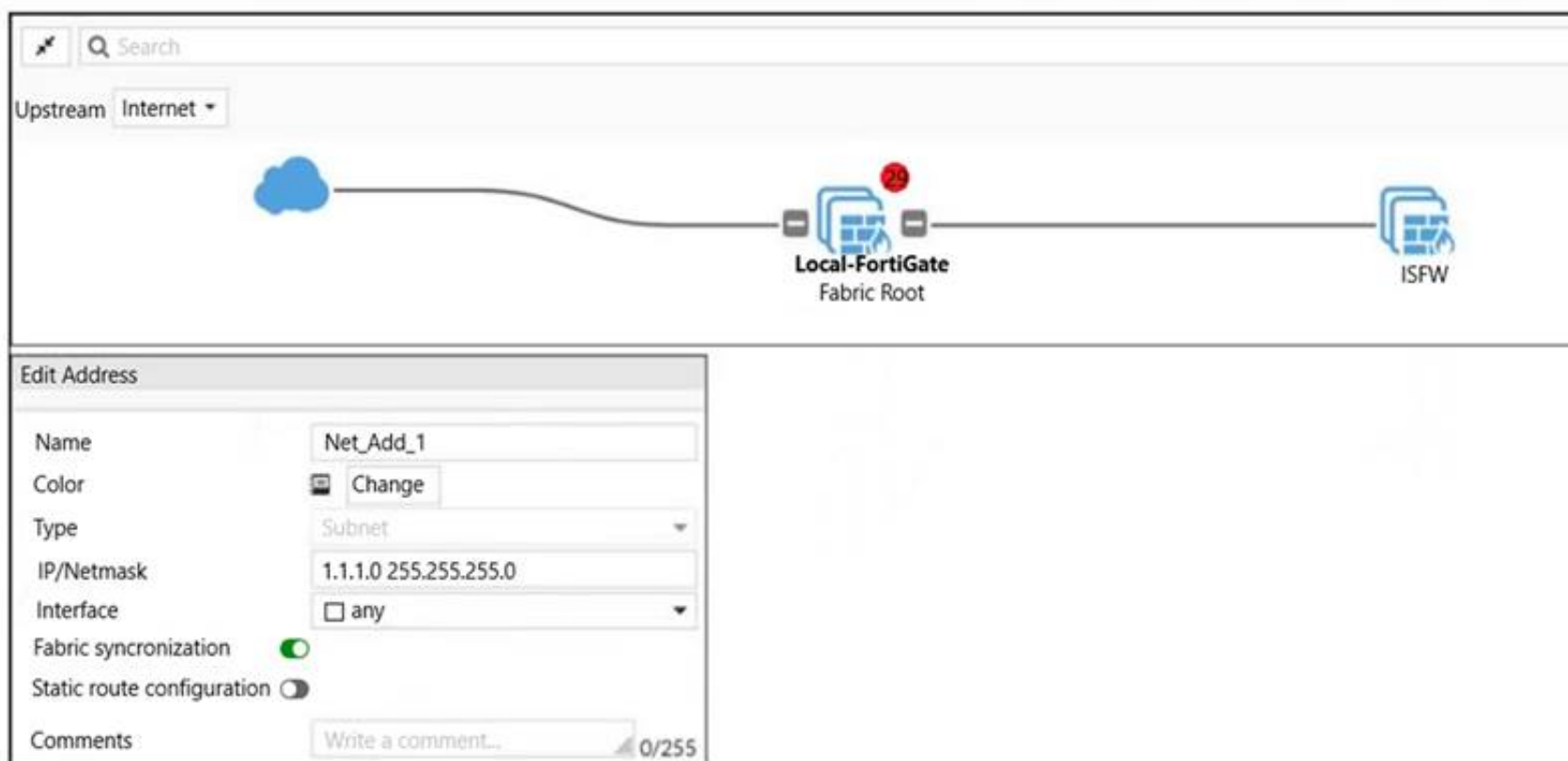


Exhibit B.

```
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
    FGLT4r5z2AyYI8i1PxutiLcsCp1AdZadv1CxDe66IdLX7I6o22J9P
    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 set configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to set configuration-sync local.
- C. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.
- D. Change the csf setting on ISFW (downstream) to set fabric-object-unification default.

**Answer:** C

#### NEW QUESTION 56

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. The collector agent uses a Windows API to query DCs for user logins.
- B. NetAPI polling can increase bandwidth usage in large networks.
- C. The collector agent must search security event logs.

D. The NetSession Enum function is used to track user logouts.

**Answer:** D

**Explanation:**

FortiGate\_Infrastructure\_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

**NEW QUESTION 60**

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

- A. The next-hop IP address is unreachable.
- B. It failed the RPF check .
- C. It matched an explicitly configured firewall policy with the action DENY.
- D. It matched the default implicit firewall policy.

**Answer:** D

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=13900>

**NEW QUESTION 65**

View the exhibit.

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Interface	TunnelB		
Administrative Distance	5		
Comments			
Status	Enabled Disabled		
Advanced Options			
Priority	30		

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Interface	TunnelA		
Administrative Distance	10		
Comments			
Status	Enabled Disabled		
Advanced Options			
Priority	0		

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

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote sit
- D. The TunnelA route is used only if the TunnelB VPN is down.
- E. This is a redundant IPsec setup.

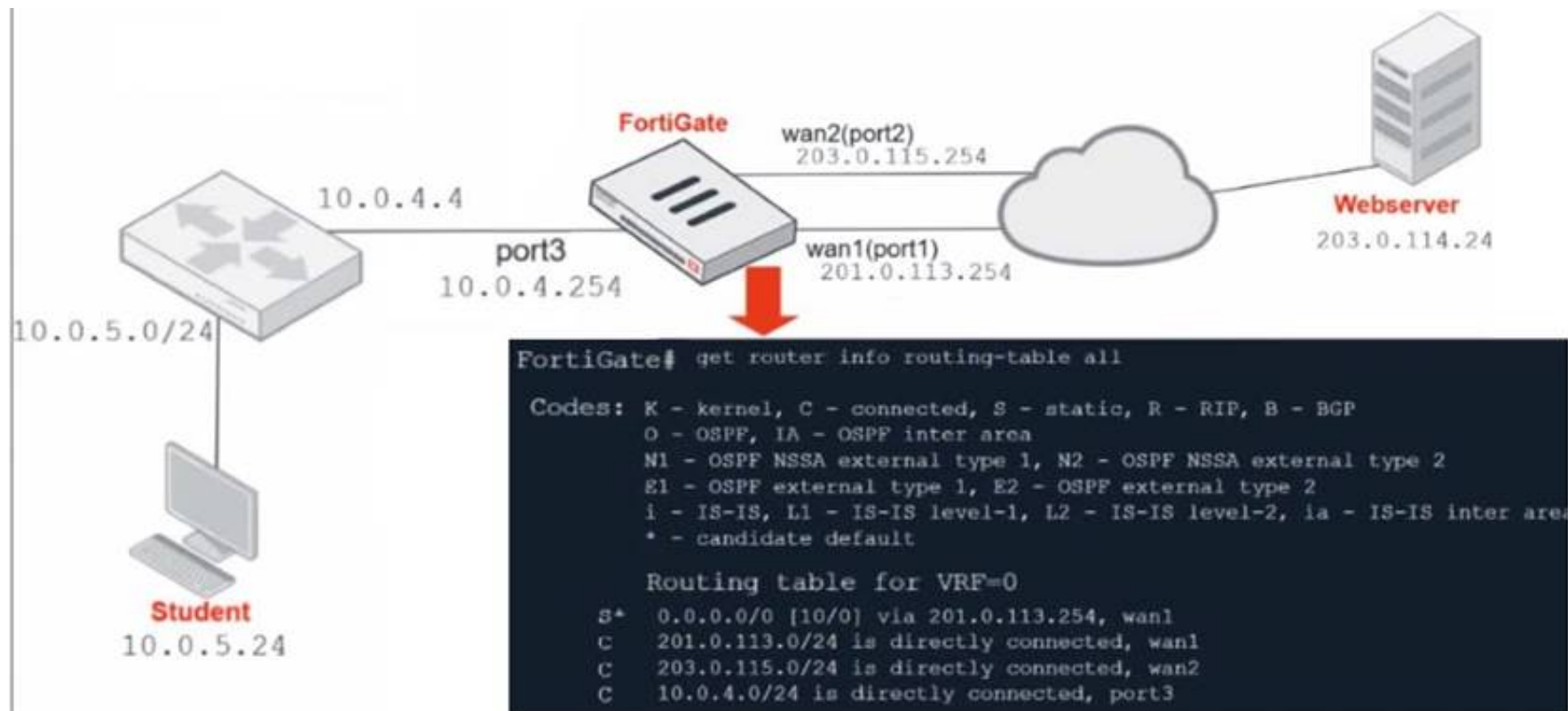
**Answer:** CD

**Explanation:**

<https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundan>

**NEW QUESTION 67**

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**

#### NEW QUESTION 71

Which three statements explain a flow-based antivirus profile? (Choose three.)

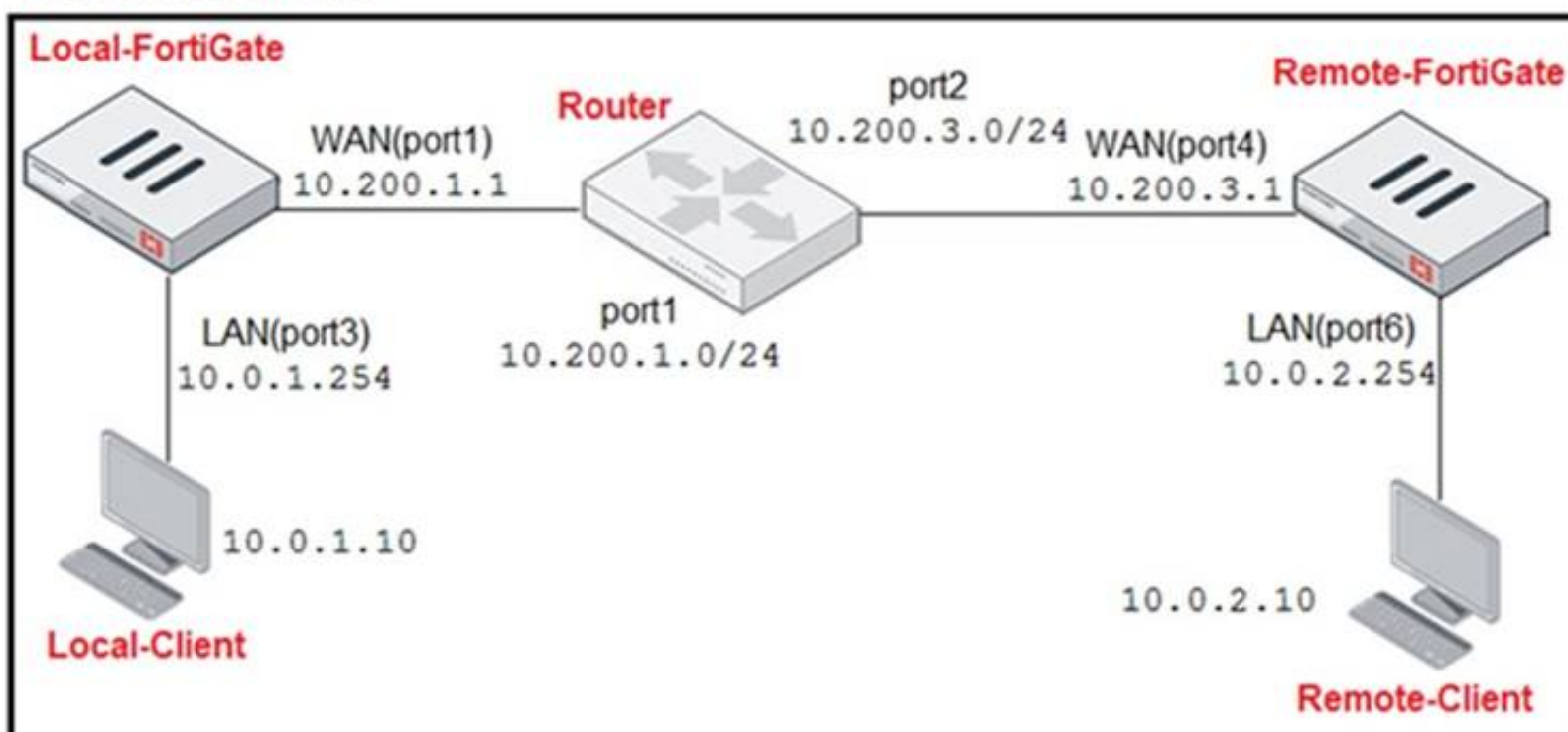
- A. IPS engine handles the process as a standalone.
- B. FortiGate buffers the whole file but transmits to the client simultaneously.
- C. If the virus is detected, the last packet is delivered to the client.
- D. Optimized performance compared to proxy-based inspection.
- E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

**Answer: BDE**

#### NEW QUESTION 73

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 75

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. What order must FortiGate use when the web filter profile has features enabled, such as safe search?

- A. DNS-based web filter and proxy-based web filter
- B. Static URL filter, FortiGuard category filter, and advanced filters
- C. Static domain filter, SSL inspection filter, and external connectors filters
- D. FortiGuard category filter and rating filter

**Answer: B**

#### NEW QUESTION 77

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

**Answer: AB**

#### NEW QUESTION 79

What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

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

**Answer: D**



### NEW QUESTION 81

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. A session for denied traffic is created.
- D. The number of logs generated by denied traffic is reduced.

**Answer:** CD

#### Explanation:

ses-denied-traffic

Enable/disable including denied session in the session table. <https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/20620/config-system-settings-block-session-timer>

Duration in seconds for blocked sessions . integer

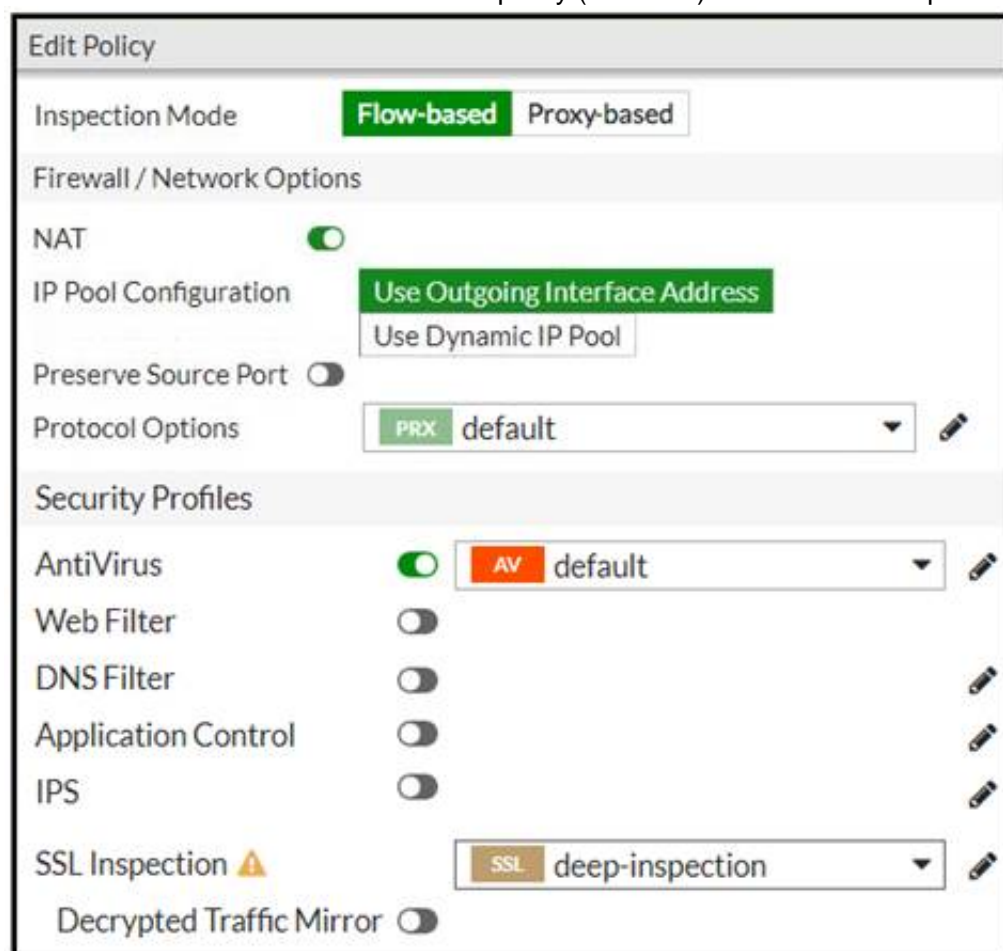
Minimum value: 1 Maximum value: 300

30

<https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/1620/config-system-global>

### NEW QUESTION 83

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).



**Edit Policy**

Inspection Mode: **Flow-based** Proxy-based

**Firewall / Network Options**

NAT: ☒

IP Pool Configuration: **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port: ☐

Protocol Options: **PRX** default

**Security Profiles**

AntiVirus: ☒ **AV** default

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

SSL Inspection: **SSL** deep-inspection

Decrypted Traffic Mirror: ☐

Edit AntiVirus Profile

Name

default

Comments

Scan files and block viruses. 29/255

Detect Viruses

Block Monitor

Feature set

Flow-based Proxy-based

Inspected Protocols

HTTP

SMTP

POP3

IMAP

FTP

CIFS

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses

Include Mobile Malware Protection

Virus Outbreak Prevention

Use FortiGuard Outbreak Prevention Database

Use External Malware Block List

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

**Answer:** B

**Explanation:**

· "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately

· When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

**NEW QUESTION 85**

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

**Answer:** B

**Explanation:**

Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.

**NEW QUESTION 90**

An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.

Which DPD mode on FortiGate will meet the above requirement?

- A. Disabled
- B. On Demand

- C. Enabled
- D. On Idle

**Answer:** D

#### NEW QUESTION 95

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

#### NEW QUESTION 96

Which statement describes a characteristic of automation stitches?

- A. They can have one or more triggers.
- B. They can be run only on devices in the Security Fabric.
- C. They can run multiple actions simultaneously.
- D. They can be created on any device in the fabric.

**Answer:** C

#### NEW QUESTION 99

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract

Num. of servers : 3
Protocol    : https
Port        : 443
Anycast     : Disable
Default servers : Included
== Server List (Mon July 5 12:00:25 2021) ==
```

IP	Weight	RTT	Flags	TZ	FortiGuard-requests	Curr	Lost	Total	Lost	Updated Time
173.243.138.210	10	350	DI	-8	29	0		0		Mon Jul 5 09:23:33 2021
12.34.97.18	20	30		-5	25	0		0		Mon Jul 5 09:23:33 2021
210.7.96.18	160	605		9	25	0		0		Mon Jul 5 09:23:33 2021

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

- A. A local FortiManager is one of the servers FortiGate communicates with.
- B. One server was contacted to retrieve the contract information.
- C. There is at least one server that lost packets consecutively.
- D. FortiGate is using default FortiGuard communication settings.

**Answer:** BD

#### NEW QUESTION 101

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

**Answer:** ADE

#### Explanation:

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

#### NEW QUESTION 106

.....

## Relate Links

**100% Pass Your NSE4 Exam with Exambible Prep Materials**

<https://www.exambible.com/NSE4-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>