



Vendor: Fortinet

Exam Code: NSE4_FGT-7.0

Exam Name: Fortinet NSE 4 - FortiOS 7.0

Version: DEMO

QUESTION 1

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

Exhibit A

The screenshot shows the 'Edit Policy' configuration window. It is divided into several sections: 'Inspection Mode' with 'Flow-based' selected; 'Firewall / Network Options' containing 'NAT' (enabled), 'IP Pool Configuration' (set to 'Use Outgoing Interface Address'), 'Preserve Source Port' (disabled), and 'Protocol Options' (set to 'PRX'); and 'Security Profiles' containing 'AntiVirus' (enabled, set to 'AV'), 'Web Filter' (disabled), 'DNS Filter' (disabled), 'Application Control' (disabled), 'IPS' (disabled), 'SSL Inspection' (set to 'deep-inspection' with a warning icon), and 'Decrypted Traffic Mirror' (disabled). Each profile has a toggle switch and a dropdown menu for selection, with edit icons on the right.

Section	Option	Value / Status
Inspection Mode	Flow-based	Selected
	Proxy-based	Available
Firewall / Network Options	NAT	Enabled
	IP Pool Configuration	Use Outgoing Interface Address
	Preserve Source Port	Disabled
	Protocol Options	PRX
Security Profiles	AntiVirus	Enabled, AV
	Web Filter	Disabled
	DNS Filter	Disabled
	Application Control	Disabled
	IPS	Disabled
	SSL Inspection	Warning, deep-inspection
	Decrypted Traffic Mirror	Disabled

Exhibit B

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:

As we can see in the last slide, in flow-based inspection if a virus is detected after a few packets the block page is not displayed.

QUESTION 2

Which two statements about SSL VPN between two FortiGate devices are true? (Choose two.)

- A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
- B. The client FortiGate requires a manually added route to remote subnets.
- C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
- D. Server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Answer: CD

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/266506/ssl-vpn-with-certificate-authentication>

QUESTION 3

Refer to the exhibits. 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).

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 X18CtzrcUB0q9ya9nryP+YfM1E
BJkv7S/Lrtch2qY Ae5C8i0YMAa0GT18aX+/dKH/o5izw1ZEon1QN2M
PGLT4r5z2AyY18ilP xutilCsCplAdZadv1Cx0e66IdLX7I6o22J9P
  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
end

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 #
```

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>

QUESTION 4

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_FortiGuard.htm

QUESTION 5

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

Answer: D

Explanation:

"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

QUESTION 6

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>

QUESTION 7

Which statement about video filtering on FortiGate is true?

- A. Full SSL Inspection is not required.
- B. It is available only on a proxy-based firewall policy.
- C. It inspects video files hosted on file sharing services.
- D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer: B

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering>

QUESTION 8

Refer to the exhibits. The exhibits contain a network diagram, virtual IP, IP pool, and firewall policies configuration.

Exhibit A.

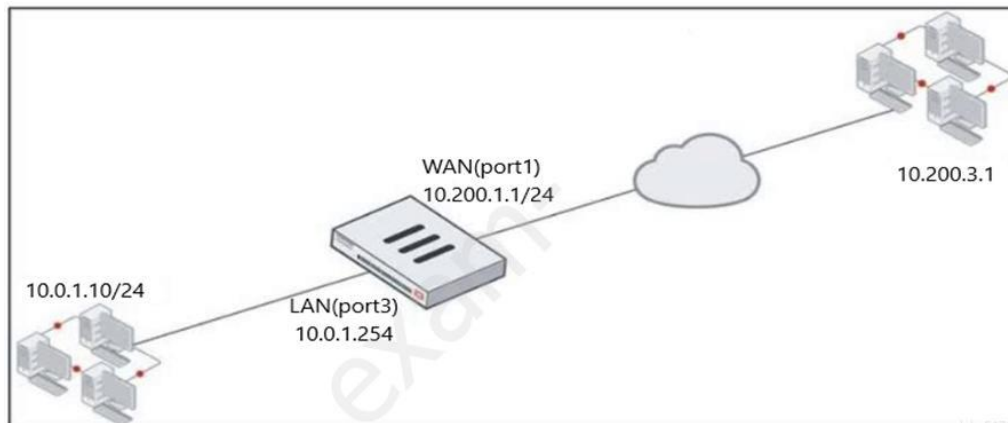


Exhibit B.

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

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: A

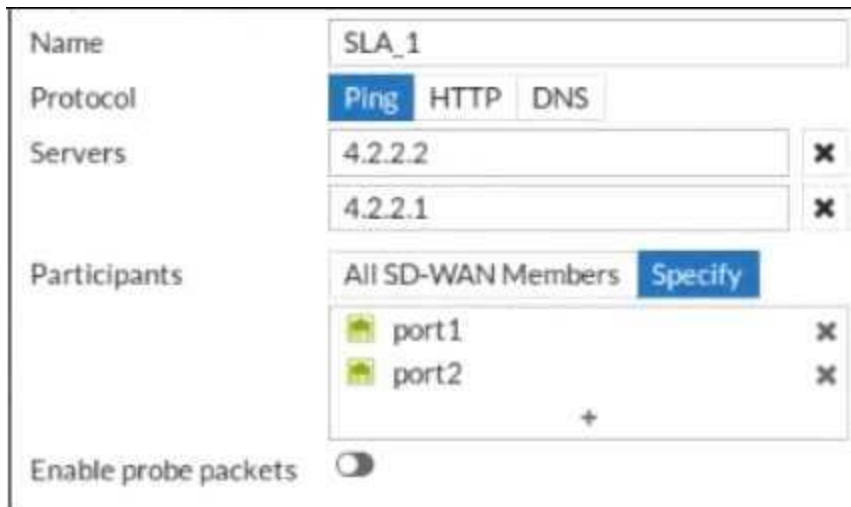
Explanation:

Reference: <https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/Concepts%20-%20Firewall/Static%20NAT.htm>

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD44529>

QUESTION 9

Refer to the exhibit. An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.



The screenshot shows the FortiGate SLA configuration window. The 'Name' field is set to 'SLA_1'. The 'Protocol' is set to 'Ping'. The 'Servers' list contains two entries: '4.2.2.2' and '4.2.2.1'. The 'Participants' list is set to 'All SD-WAN Members'. The 'Enable probe packets' checkbox is unchecked.

Name	SLA_1		
Protocol	Ping	HTTP	DNS
Servers	4.2.2.2	X	
	4.2.2.1	X	
Participants	All SD-WAN Members Specify		
	port1	X	
	port2	X	
	+		
Enable probe packets	<input type="checkbox"/>		

Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

- A. The Detection Mode setting is not set to Passive.
- B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
- C. The configured participants are not SD-WAN members.
- D. The Enable probe packets setting is not enabled.

Answer: BD

Thank You for Trying Our Product

Passleader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



10% Discount Coupon Code: ASTR14