



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 1

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check.
- D. FortiGate directs the collector agent to use a remote LDAP server.

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 2

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure web rating override for the home page? (Choose two.)

- A. www.exaple.com
- B. www.example.com/index.html
- C. example.com
- D. www.example.com:443

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 3

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

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

Exhibit A.

### Edit Policy

Name ⓘ	Internet Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

### Firewall/Network Options

NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input checked="" type="checkbox"/> Use Outgoing Interface Address <input type="checkbox"/> Use Dynamic IP Pool
Preserve Source Port	<input type="checkbox"/>
Protocol Options	<input checked="" type="checkbox"/> PROT default

### Security Profiles

AntiVirus	<input checked="" type="checkbox"/> AV default
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>
File Filter	<input type="checkbox"/>
SSL Inspection ⚠	<input checked="" type="checkbox"/> SSL deep-inspection
Decrypted Traffic Mirror	<input type="checkbox"/>

Exhibit B.

### Edit AntiVirus Profile

Name	default
Comments	Scan files and block viruses. 29/255
Detect Viruses	<input checked="" type="checkbox"/> Block <input type="checkbox"/> Monitor
Feature set	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

#### Inspected Protocols

HTTP	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input type="checkbox"/>

#### APT Protection Options

Treat Windows Executables in Email Attachments as Viruses	<input checked="" type="checkbox"/>
Include Mobile Malware Protection	<input checked="" type="checkbox"/>
Quarantine	<input type="checkbox"/>

#### Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database	<input type="checkbox"/>
Use External Malware Block List	<input type="checkbox"/>
Use EMS threat feed	<input type="checkbox"/>

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 4

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiSandbox
- B. FortiCloud
- C. FortiSIEM
- D. FortiCache
- E. FortiAnalyzer

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 5

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 6

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000 4500 003c 2f8f 0000 8001 f020 0a00 0102 E.</.....
0x0010 0808 0808 0800 4d5a 0001 0001 6162 6364 .....MZ...abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000 4500 003c 2f8f 0000 7f01 0106 0a38 f0e4 E.</.....8..
0x0010 0808 0808 0800 6159 ec01 0001 6162 6364 .....aY...abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000 4500 003c 0000 0000 7501 3a95 0808 0808 E.<....u:....
0x0010 0a38 f0e4 0000 6965 ec01 0001 6162 6364 .8....iY...abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000 4500 003c 0000 0000 7401 2bb0 0808 0808 E.<....t.+....
0x0010 0a00 0102 0000 555a 0001 0001 6162 6364 .....UZ...abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)

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

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 7

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibits.

Exhibit A.

### Outgoing Interfaces

Select a strategy for how outgoing interfaces will be chosen.





Manual  
Manually assign outgoing interfaces.

**Best Quality**  
The interface with the best measured performance is selected.

Lowest Cost (SLA)  
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

Maximize Bandwidth (SLA)  
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

 port1	X
 port2	X
 port3	X
 port4	X

Measured SLA: SLA\_1

Quality criteria: Latency

Forward DSCP:

Reverse DSCP:

Status:

Exhibit B.

```
NGFW-1 # diagnose sys sdwan health-check
Health Check(SLA-1):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x1
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x1
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x1
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x1
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check.

Which interface will be selected as an outgoing interface?

- A. port2
- B. port3
- C. port4
- D. port1

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 8

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

An administrator does not want to report the logon events of service accounts to FortiGate.

What setting on the collector agent is required to achieve this?

- A. Add user accounts to the Ignore User List.
- B. Add the support of NTLM authentication.
- C. Add user accounts to the FortiGate group filter.
- D. Add user accounts to Active Directory (AD).

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 9

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibit.

The screenshot shows the configuration page for the Administrator user profile. The 'Username' field is set to 'Administrator' and has a 'Change Password' button next to it. The 'Type' dropdown menu is open, showing 'Local User' as the selected option, with other options including 'Match a user on a remote server group', 'Match all users in a remote server group', and 'Use public key infrastructure (PKI) group'. The 'Comments' field contains the text 'Write a comment...' and has a character count of 0/255. The 'Administrator profile' dropdown is set to 'prof\_admin'. At the bottom, there are three toggle switches, all of which are currently turned off: 'Two-factor Authentication', 'Restrict login to trusted hosts', and 'Restrict admin to guest account provisioning only'.

The global settings on a FortiGate device must be changed to align with company security policies.

What does the Administrator account need to access the FortiGate global settings?

- A. Enable two-factor authentication
- B. Change Administrator profile
- C. Change password
- D. Enable restrict access to trusted hosts.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 10

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 11

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

An administrator has configured outgoing interface any in a firewall policy.

Which statement is true about the policy list view?

- A. Interface Pair view will be disabled.
- B. Search option will be disabled.
- C. Policy lookup will be disabled.
- D. By Sequence view will be disabled.

[Show Suggested Answer](#)



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 12

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibit.

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

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-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.
- D. port1 is a native VLAN.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 13

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

- ⇒ All traffic must be routed through the primary tunnel when both tunnels are up
- ⇒ The secondary tunnel must be used only if the primary tunnel goes down

In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover

▪

Which two key configuration changes are needed in FortiGate to meet the design requirements? (Choose two.)

- A. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
- B. Enable Dead Peer Detection.
- C. Enable Auto-negotiate and Auto Keep Alive on the phase 2 configuration of both tunnels.
- D. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 14

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2021-06-02 10:59:34), state/o/chg_time=2(work)/2(work)/1593701169(2021-06-02 10:46:09)
  pingsvr_flip_timeout/expire=3600s/2781s          2021-06-02
  'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=0x00000000, uptime/reset_cnt=198/0
  'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

The override setting is enable for the FortiGate with SN FGVM010000064692.

Which two statements are true? (Choose two.)

- A. FortiGate SN FGVM010000065036 HA uptime has been reset.
- B. FortiGate devices are not in sync because one device is down.
- C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- D. FortiGate SN FGVM010000064692 has the higher HA priority.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 15

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibits.

Exhibit A shows system performance output.

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```

Exhibit B shows s FortiGate configured with the default configuration of high memory usage thresholds.

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, which two statements are correct? (Choose two.)

- A. FortiGate will start sending all files to FortiSandbox for inspection.
- B. FortiGate has entered conserve mode.
- C. Administrators cannot change the configuration.
- D. Administrators can access FortiGate only through the console port.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 16

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address.

For site A, the local quick mode selector is 192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.

Which subnet must the administrator configure for the local quick mode selector for site B?

- A. 192.168.3.0/24
- B. 192.168.1.0/24
- C. 192.168.0.0/8
- D. 192.168.2.0/24

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 17

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibits.

Exhibit A.

### SSL-VPN Settings

**Connection Settings** ⓘ

Listen on Interface(s)

Listen on Port

*Web mode access will be listening at <https://10.200.1.1:11443>*

Redirect HTTP to SSL-VPN

Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout

Inactive For  Seconds

Server Certificate

Require Client Certificate

**Tunnel Mode Client Settings** ⓘ

Address Range Automatically assign addresses Specify custom IP ranges

*Tunnel users will receive IPs in the range of 10.212.134.200–10.212.134.210*

DNS Server Same as client system DNS Specify

Specify WINS Servers

**Authentication/Portal Mapping** ⓘ

+ Create New Edit Delete

Users/Groups	Portal
SSL-VPN-Users	tunnel-access
All Other Users/Groups	full-access

Exhibit B.

Connection status
✕

Connection: VPN

Server: <https://10.200.1.1:1443/>

Status: Connecting...

Duration: –

Bytes received: 0

Bytes sent: 0

Stop

The SSL VPN connection fails when a user attempts to connect to it.

What should the user do to successfully connect to SSL VPN?

- A. Change the SSL VPN port on the client.
- B. Change the Server IP address.
- C. Change the idle-timeout.
- D. Change the SSL VPN portal to the tunnel.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 18

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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.

Show Suggested Answer



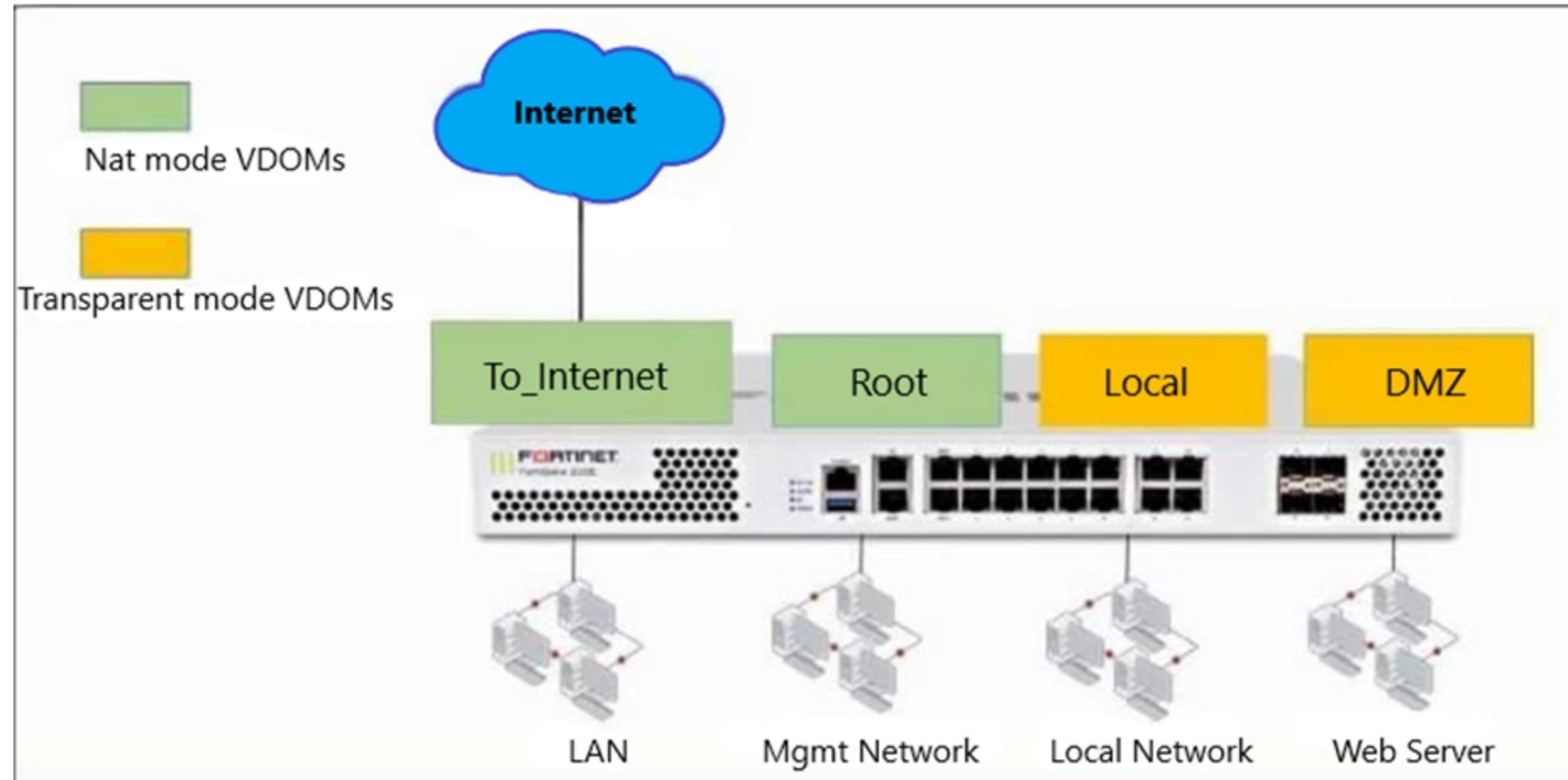
Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 19

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

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 default static route is not 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.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 20

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibits.

Exhibit A.

The screenshot shows the FortiGate GUI. At the top, there is a search bar and a dropdown menu for 'Upstream' set to 'Internet'. Below this is a network diagram showing a cloud icon connected to a 'Local-FortiGate Fabric Root' icon, which is in turn connected to an 'ISFW' icon. A red '29' badge is visible above the Local-FortiGate icon. Below the diagram is the 'Edit Address' configuration window. The 'Name' field is 'Net\_Add\_1', 'Color' is 'Change', 'Type' is 'Subnet', 'IP/Netmask' is '1.1.1.0 255.255.255.0', and 'Interface' is 'any'. The 'Fabric synchronization' toggle is turned on, and 'Static route configuration' is turned off. There is a 'Comments' field with a character count of '0/255'.

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/trtoh2gY Ae5CH8YMAa0GT18aX+/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.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 21

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

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

```
STUDENT # get system session list
PROTO    EXPIRE  SOURCE          SOURCE-NAT      DESTINATION     DESTINATION-NAT
tcp      3598    10.0.1.10:2706  10.200.1.6:2706 10.200.1.254:80 -
tcp      3598    10.0.1.10:2704  10.200.1.6:2704 10.200.1.254:80 -
tcp      3596    10.0.1.10:2702  10.200.1.6:2702 10.200.1.254:80 -
tcp      3599    10.0.1.10:2700  10.200.1.6:2700 10.200.1.254:443 -
tcp      3599    10.0.1.10:2698  10.200.1.6:2698 10.200.1.254:80 -
tcp      3598    10.0.1.10:2696  10.200.1.6:2696 10.200.1.254:443 -
udp      174     10.0.1.10:2694  -                10.0.1.254:53  -
udp      173     10.0.1.10:2690  -                10.0.1.254:53  -
```

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 22

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which two statements are correct about SLA targets? (Choose two.)

- A. You can configure only two SLA targets per one Performance SLA.
- B. SLA targets are optional.
- C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
- D. SLA targets are used only when referenced by an SD-WAN rule.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 23

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

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

```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
origin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80 (10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024 (10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is in SYN\_SENT state.
- B. The session is in FIN\_WAIT state.
- C. The session is in ESTABLISHED state.
- D. The session is in FIN\_ACK state.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 24

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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.

Show Suggested Answer







Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 25

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

- A. Intrusion prevention system engine
- B. Detection engine
- C. Flow engine
- D. Antivirus engine

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 26

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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 generate logs
- D. To remove the NAT operation

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 27

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibit.



**Phase 2 Selectors**

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

**Edit Phase 2**

Name: ToRemote

Comments: Comments

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

**Advanced**

**Phase 2 Proposal** Add

Encryption: AES128 Authentication: SHA1

Enable Replay Detection

Enable Perfect Forward secrecy(PFS)

Diffie-Hellman Group:
  32  31  30  29  28  27  
 21  20  19  18  17  16  
 15  14  5  2  1

Local Port: All

Remote Port: All

Protocol: All

Auto-negative:

Autokey Keep Alive:

Key Lifetime: Seconds

Seconds: 43200

**Phase 2 Selectors**

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

**Edit Phase 2**

Name: ToRemote

Comments: Comments

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

**Advanced**

**Phase 2 Proposal** Add

Encryption: AES256 Authentication: SHA1

Enable Replay Detection

Enable Perfect Forward secrecy(PFS)

Diffie-Hellman Group:
  32  31  30  29  28  27  
 21  20  19  18  17  16  
 15  14  5  2  1

Local Port: All

Remote Port: All

Protocol: All

Auto-negative:

Autokey Keep Alive:

Key Lifetime: Seconds

Seconds: 43200

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

- A. On HQ-FortiGate, enable Auto-negotiate.
- B. On HQ-FortiGate, enable Diffie-Hellman Group 2.
- C. On HQ-FortiGate, set Encryption to AES256.
- D. On Remote-FortiGate, set Seconds to 43200.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 28

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

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

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 29

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 30

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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

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

Show Suggested Answer



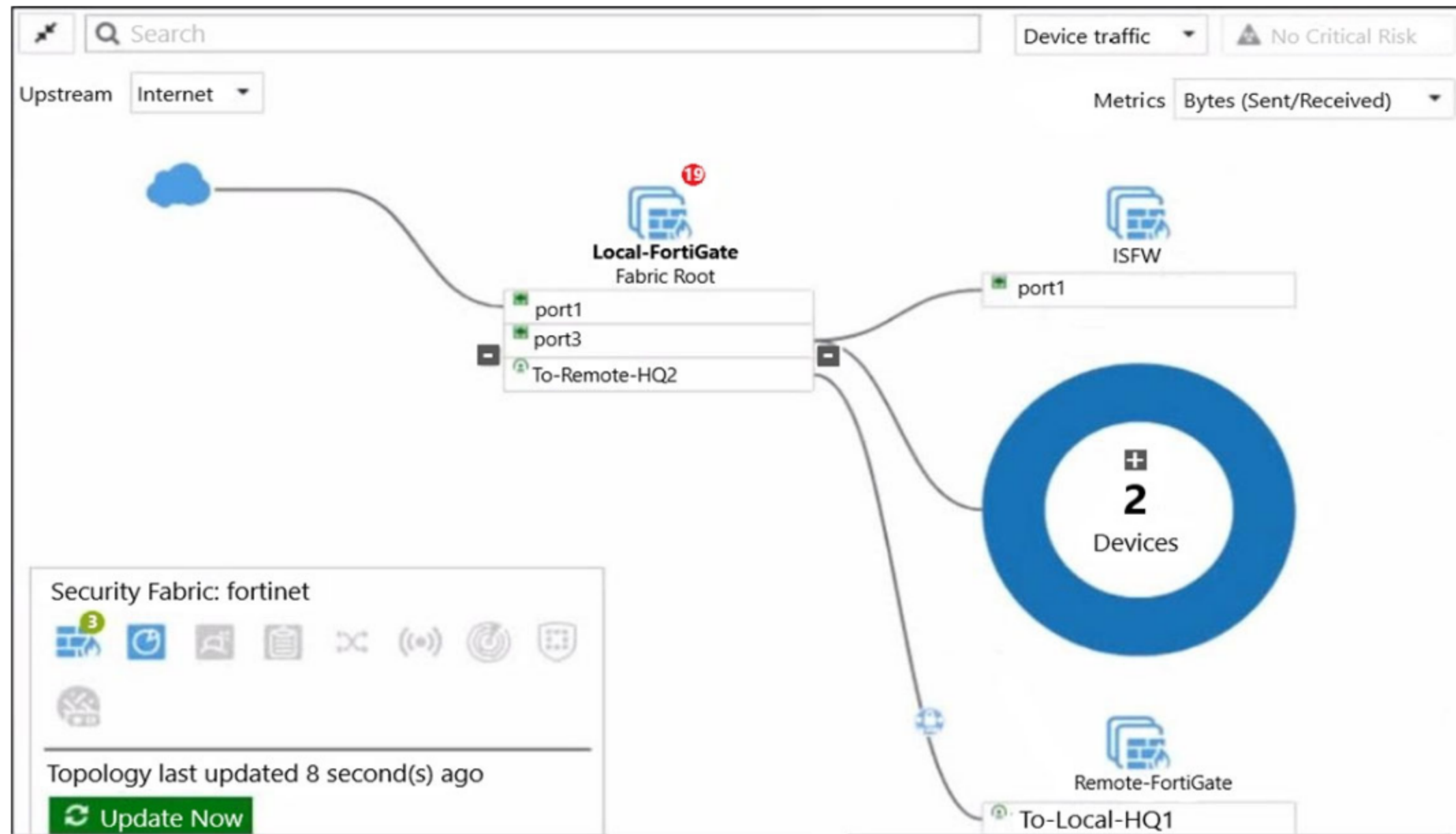
Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 31

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

- A. There are five devices that are part of the security fabric.
- B. There are 19 security recommendations for the security fabric.
- C. Device detection is disabled on all FortiGate devices.
- D. This security fabric topology is a logical topology view.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 32

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.

What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Dialup User
- B. Static IP Address
- C. Pre-shared Key
- D. Dynamic DNS

Show Suggested Answer







Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 33

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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. On Demand
- B. Disabled
- C. On Idle
- D. Enabled

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 34

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

Which three statements about a flow-based antivirus profile are correct? (Choose three.)

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 35

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 36

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibit.

**Add Signatures**

Type: Filter **Signature**

Action:  Block

Packet logging:  Enable  Disable

Status:  Enable  Disable  Default

Rate-based settings: **Default** Specify

Exempt IPS: 0

Search

Selected **1** All

Name	Severity	Target	OS	Action
<input checked="" type="checkbox"/> <b>IPS Signature 1</b>				
<u>FTP.Login.Failed</u>	█ █ █ █ █	Server	All	<input checked="" type="radio"/> Pass

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

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 37

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibit.

### Edit IPS Sensor

Name:

Comments:  0/255

Block malicious URLs:

#### IPS Signatures and Filters

[+Create New](#) [Edit](#) [Delete](#)

Details	Exempt IPs	Action	Packet Logging
NTP.Spoofed.KoD.Dos	0	Monitor	Enabled
Windows		Block	Disabled

The exhibit shows the IPS sensor configuration.

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

- A. The sensor will block all attacks aimed at Windows servers.
- B. The sensor will gather a packet log for all matched traffic.
- C. The sensor will allow attackers matching the NTP.Spoofed.KoD.DoS signature.
- D. The sensor will reset all connections that match these signatures.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 38

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 39

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

- A. Antivirus definitions are not up to date.
- B. SSL/SSH Inspection profile is incorrect.
- C. Antivirus profile configuration is incorrect.
- D. Application control is not enabled.

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 40

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 41

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibit.

```
FGT1 # get router info routing-table database
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
       > - selected route, * - FIB route, p - stale info

S    *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
     *>           [10/0] via 10.0.0.2, port2, [30/0]
S    0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C    *> 10.0.0.0/24 is directly connected, port2
S    172.13.24.0/24 [10/0] is directly connected, port4
C    *> 172.20.121.0/24 is directly connected, port1
S    *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C    *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

- A. The port3 default route has the lowest metric.
- B. There will be eight routes active in the routing table.
- C. The port1 and port2 default routes are active in the routing table.
- D. The port3 default route has the highest distance.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 42

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which statement about the policy ID number of a firewall policy is true?

- A. It changes when firewall policies are reordered.
- B. It defines the order in which rules are processed.
- C. It represents the number of objects used in the firewall policy.
- D. It is required to modify a firewall policy using the CLI.

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 43

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. Operating mode
- B. NGFW mode
- C. System time
- D. FortiGuard update servers

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 44

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibits.

Exhibit A.

### Edit Policy

Name	Facebook SSL Inspection
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Service	ALL

### Firewall/Network Options

**i** Central NAT is enabled so NAT settings from matching [Central SNAT policies](#) will be applied.

### Security Profiles

SSL Inspection: **SSL** certificate-inspection

Exhibit B.

### Edit Policy

Name	Facebook Access									
Incoming Interface	port2									
Outgoing interface	port1									
Source	all									
Destination	all									
Schedule	always									
Service	App Deafult Specify									
Application	<table border="1"> <tr> <td>Facebook</td> <td></td> <td>X</td> </tr> <tr> <td>Facebook_Like.Button</td> <td>🔒</td> <td>X</td> </tr> <tr> <td>Facebook_Video.Play</td> <td></td> <td>X</td> </tr> </table>	Facebook		X	Facebook_Like.Button	🔒	X	Facebook_Video.Play		X
Facebook		X								
Facebook_Like.Button	🔒	X								
Facebook_Video.Play		X								
URL Category										
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY									

### Firewall/Network Options

Protocol Options: **PRX** 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?

- Add Facebook in the URL category in the security policy.
- Additional application signatures are required to add to the security policy.
- Force access to Facebook using the HTTP service.
- The SSL inspection needs to be a deep content inspection.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 45

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 46

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibit, which contains a radius server configuration.

**New RADIUS Server**

Name: FortiAuthenticator-RADIUS

Authentication method: Default Specify

NAS IP:

Include in every user group

**Primary Server**

IP/Name: 10.0.1.149

Secret: \*\*\*\*\*

Test Connectivity

Test User Credentials

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option. What will be the impact of using Include in every user group option in a RADIUS configuration?

- A. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- B. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
- C. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 47

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 48

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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

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

Show Suggested Answer







Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 49

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

An administrator wants to configure timeouts for users. Regardless of the user's behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

- A. soft-timeout
- B. new-session
- C. idle-timeout
- D. hard-timeout
- E. auth-on-demand

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 50

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) form port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) form local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)

- A. The default route is required to receive a reply.
- B. A new traffic session is created.
- C. A firewall policy allowed the connection.
- D. The debug flow is of ICMP traffic.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 51

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 52

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 53

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which type of logs on FortiGate record information about traffic directly to and from the FortiGate management IP addresses?

- A. System event logs
- B. Security logs
- C. Forward traffic logs
- D. Local traffic logs

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 54

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an HTTP reverse proxy.
- B. FortiGate acts as router.
- C. FortiGate acts as DNS server.
- D. FortiGate acts as an FDS server.

[Show Suggested Answer](#)





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 55

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- A. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy.
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs.
- C. NGFW policy-based mode does not require the use of central source NAT policy.
- D. NGFW policy-based mode policies support only flow inspection.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 56

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibits.

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

Exhibit A.

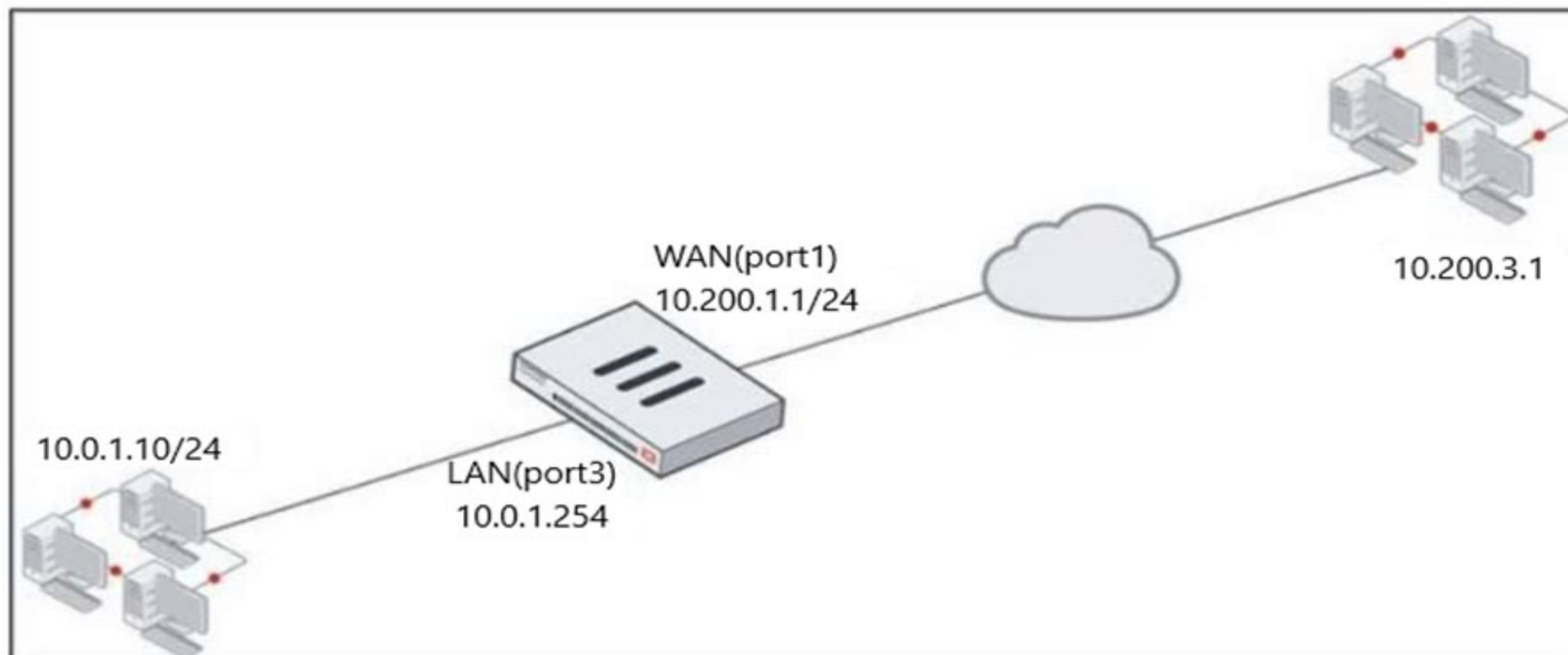


Exhibit B.

+ Create New
Edit
Delete
Policy Lookup

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. 10.200.1.100
- B. 10.200.1.10
- C. 10.200.1.1
- D. 10.200.3.1

Show Suggested Answer







Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 57

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 58

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which two statements are true about the FGCP protocol? (Choose two.)

- A. Is used to discover FortiGate devices in different HA groups
- B. Runs only over the heartbeat links
- C. Elects the primary FortiGate device
- D. Not used when FortiGate is in Transparent mode

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 59

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the web filter raw logs.

```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstrip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"
```

```
date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstrip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

- A. The name of the firewall policy is all\_users\_web.
- B. Social networking web filter category is configured with the action set to authenticate.
- C. The action on firewall policy ID 1 is set to warning.
- D. Access to the social networking web filter category was explicitly blocked to all users.

Show Suggested Answer

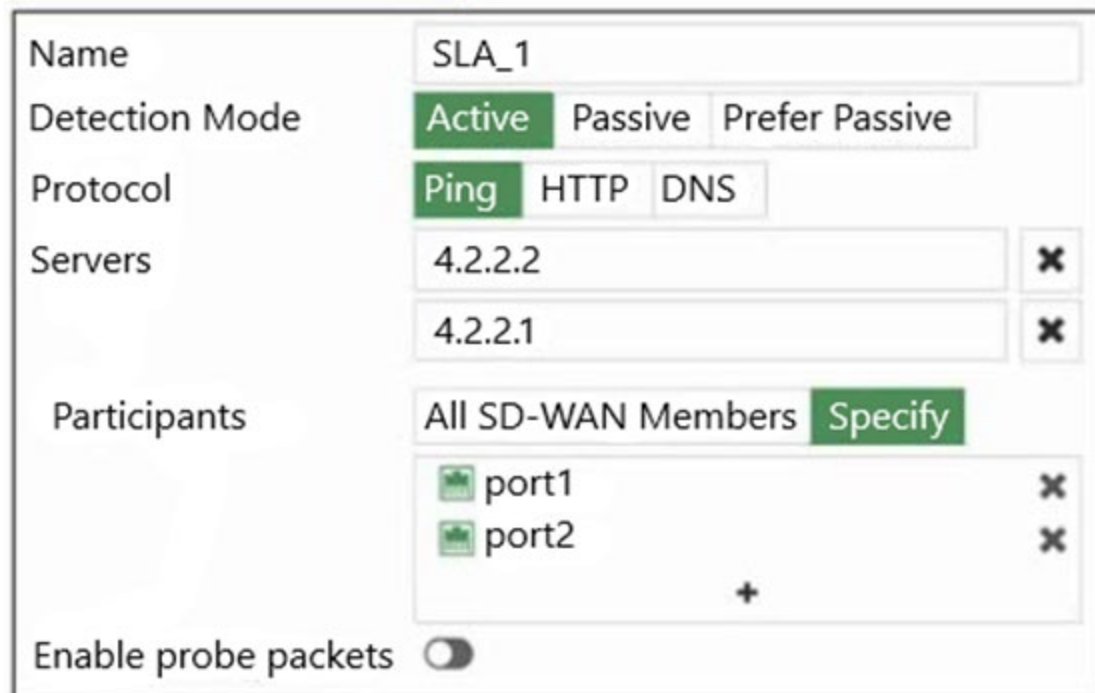
Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 60

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibit.



The screenshot shows the configuration for a performance SLA named 'SLA\_1'. The 'Detection Mode' is set to 'Active'. The 'Protocol' is set to 'Ping'. The 'Servers' list contains two entries: '4.2.2.2' and '4.2.2.1'. The 'Participants' are set to 'All SD-WAN Members' with a 'Specify' button. Below this, two participants are listed: 'port1' and 'port2'. The 'Enable probe packets' toggle is currently turned off.

Name	SLA_1		
Detection Mode	Active	Passive	Prefer Passive
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"/>		

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

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 61

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

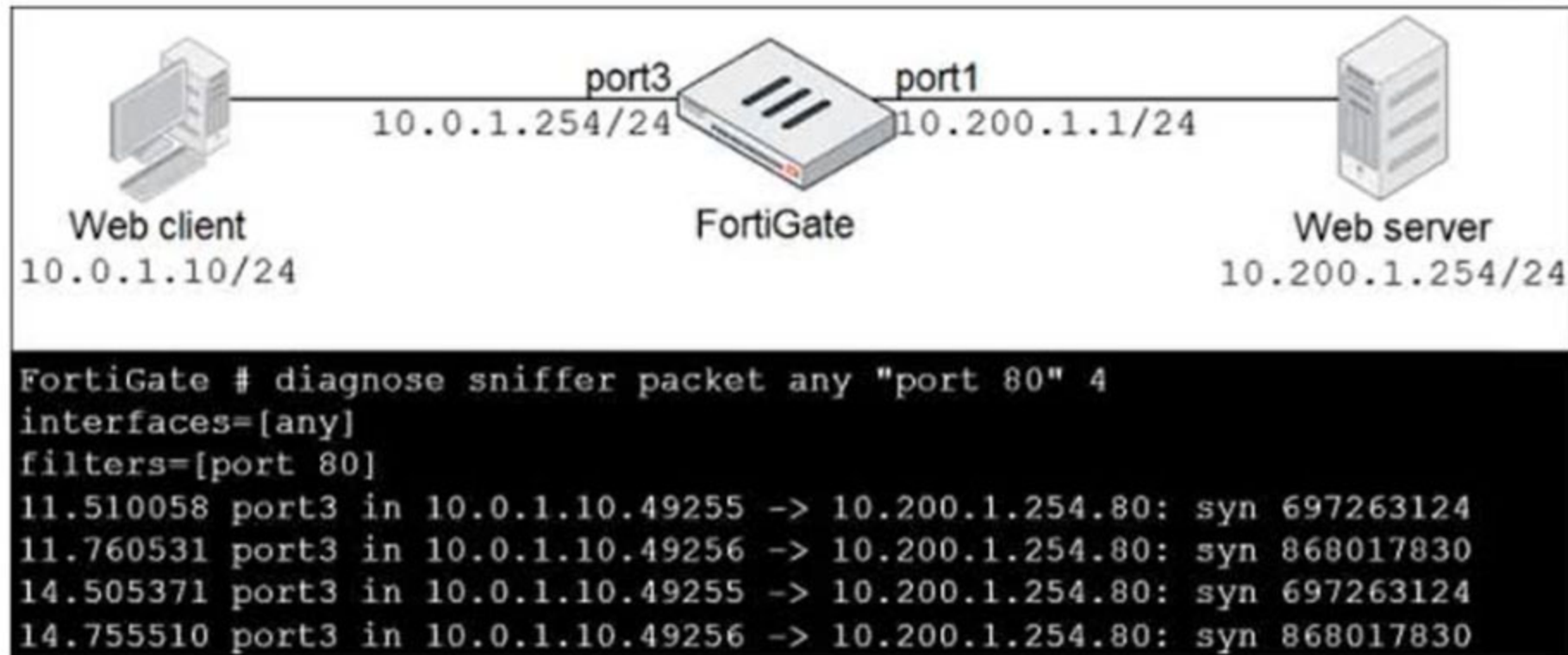
Question #: 62

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 63

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

- A. execute ping
- B. diagnose sys top
- C. get system arp
- D. execute traceroute
- E. diagnose sniffer packet any

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 64

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

Refer to the exhibits.

Exhibit A.

The screenshot shows three configuration panels for an SD-WAN member:

- virtual-wan-link:** A table listing four interfaces: port1 (Gateway: 10.200.1.254, Cost: 15), port2 (Gateway: 10.200.2.254, Cost: 5), port3 (Gateway: 10.200.3.254, Cost: 5), and port4 (Gateway: 10.200.4.254, Cost: 1).
- SLA\_1:** Configuration for an SLA target. Detection Mode is Active, Protocol is Ping. Servers are 4.2.2.2 and 4.2.2.1. Participants include port1, port2, port3, and port4. Enable probe packets is checked. SLA Target is checked. Latency threshold is 50 ms, Jitter threshold is 5 ms, and Packet Loss threshold is 0%.
- Outgoing Interfaces:** Strategy is set to Lowest Cost (SLA). Interface preference list includes port1, port2, port3, and port4. Required SLA target is SLA\_1. Forward DSCP and Reverse DSCP are disabled. Status is Enable.

Exhibit B.

```

NGFW-1 # diagnose sys sdwan health-check
Health Check(SLA_1):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x1
Seq(2 port2): state(alive), packet-loss(0.000%) latency(34.349), jitter(3.887) sla_map=0x1
Seq(3 port3): state(alive), packet-loss(0.100%) latency(31.476), jitter(3.254) sla_map=0x1
Seq(4 port4): state(alive), packet-loss(2.130%) latency(46.229), jitter(4.287) sla_map=0x1

```

The exhibit shows the configuration for the SD-WAN member, Performance SLA, and SD-WAN Rule, as well as the output of diagnose sys virtual-wan-link health-check.

Which interface will be selected as an outgoing interface?

- A. port2
- B. port3
- C. port4
- D. port1

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 65

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 66

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 67

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

---

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface. In this scenario, which statement about the VLAN IDs is true?

- A. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
- B. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.
- C. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.
- D. The two VLAN subinterfaces must have different VLAN IDs.

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 68

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

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

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is in TCP ESTABLISHED state.
- B. The session is a bidirectional UDP connection.
- C. The session is a UDP unidirectional state.
- D. The session is a bidirectional TCP connection.

Show Suggested Answer

Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 69

Topic #: 1

[\[All NSE4\\_FGT7.0 Questions\]](#)

Refer to the exhibits.

The exhibits contain a network diagram, central SNAT policy, and IP pool configuration.

Exhibit A.

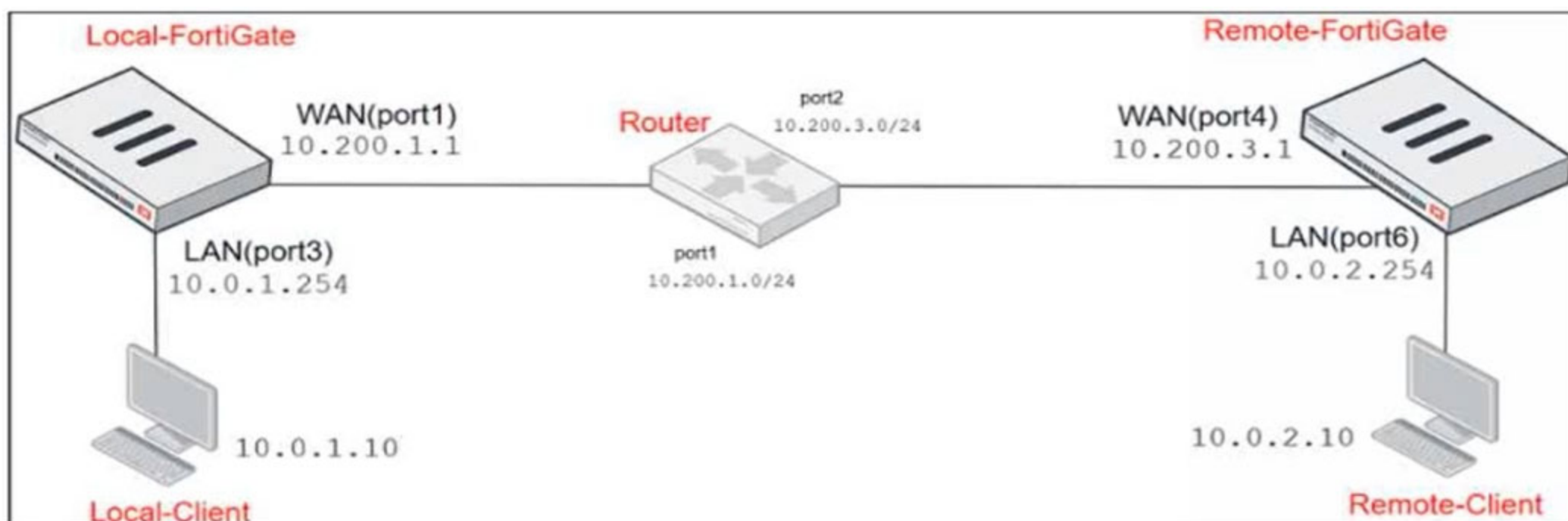


Exhibit B.

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
IPv4 3						
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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4\_FGT-7.0

Question #: 70

Topic #: 1

[\[All NSE4\\_FGT-7.0 Questions\]](#)

---

Which scanning technique on FortiGate can be enabled only on the CLI?

- A. Antivirus scan
- B. Machine learning scan
- C. Trojan scan
- D. Ransomware scan

Show Suggested Answer

