



# NSE4\_FGT-7.0<sup>Q&As</sup>

Fortinet NSE 4 - FortiOS 7.0

## Pass Fortinet NSE4\_FGT-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.pass4itsure.com/nse4\\_fgt-7-0.html](https://www.pass4itsure.com/nse4_fgt-7-0.html)

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Refer to the exhibit to view the firewall policy.

Name	Internet Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all +
Destination	all +
Schedule	always
Service	DNS FTP HTTP HTTPS +
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based
<b>Security Profiles</b>	
AntiVirus	<input checked="" type="checkbox"/> default
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>



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

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

Correct Answer: A

---

### QUESTION 2

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Correct Answer: AC

---

### QUESTION 3

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



### IPS Sensor

Edit IPS Sensor: WINDOWS\_SERVER

Name: EMAIL-SERVER-IPS [View IPS Signatures]

Comments: [text area]

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce		High	Server	TCP_SMT	All	Block	<input checked="" type="checkbox"/>

IPS Filters

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	<input checked="" type="checkbox"/>

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
<input checked="" type="checkbox"/>	IMAPLoginBruteForce	60	10	Source IP	Block	None

Apply

### DoS Policy

Incoming Interface: port1

Source Address: all

Destination Address: all

Services: ALL

#### L3 Anomalies

Name	Status	Logging	Pass	Block	Action
ip_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip\_src\_session
- D. Location: server Protocol: SMTP

Correct Answer: B

#### 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.

Correct Answer: D

---

## QUESTION 5

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.

Correct Answer: D

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

[Latest NSE4\\_FGT-7.0 Dumps](#)

[NSE4\\_FGT-7.0 PDF Dumps](#) [NSE4\\_FGT-7.0 Study Guide](#)