Fortinet

NSE4_FGT-6.2 Exam

Fortinet NSE 4 - FortiOS 6.2 Exam

Questions & Answers
Demo

Version: 8.0

Question: 1

Examine the FortiGate configuration:

```
config user settings
      set auth-on-demand implicitly
end
```

What will happen to unauthenticated users when an active authentication policy is followed by a fall through
policy without authentication?

A. The user must log in again to authenticate.
B. The user will be denied access to resources without authentication.
C. The user will not be prompted for authentication.
D. User authentication happens at an interface level.

Answer: A

Explanation
Explanation/Reference:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46875

Question: 2

Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled
on all FortiGate devices?

A. FG-traffic VDOM
B. Root VDOM
C. Customer VDOM
D. Global VDOM

Answer: B

Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/new-features/287377/split-task-vdom-support

Question: 3

In a high availability (HA) cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?

A. Client > primary FortiGate> secondary FortiGate> primary FortiGate> web server.
B. Client > secondary FortiGate> web server.
C. Clinet >secondary FortiGate> primary FortiGate> web server.
D. Client> primary FortiGate> secondary FortiGate> web server.

Answer: D

Question: 4

Which statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode antivirus buffers the whole file for scarring before sending it to the client.
B. In flow-based inspection mode, you can use the CLI to configure antivirus profiles to use protocol option profiles.
C. In proxy-based inspection mode, if a virus is detected, a replacement message may not be displayed immediately.
D. In quick scan mode, you can configure antivirus profiles to use any of the available signature data bases.

Answer: A, B

A: Buffers the whole file, packets sent to the client after scan finishes-
B: When the antivirus profile is operating in flow-based inspection mode, two scanning mode options are available: full scan mode and quick scan mode.(Normal extended, or extreme-depending on what is configured in the CLI).

Question: 5

The FSSO Collector Agent set to advanced access mode for the Windows Active Directory uses which of the following?

A. LDAP convention
B. NTLM convention
C. Windows convention – NetBios\Username
D. RSSO convention

Answer: A

Question: 6

Which Statements about virtual domains (VDOMs) arc true? (Choose two.)

A. Transparent mode and NAT/Route mode VDOMs cannot be combined on the same FortiGate.
B. Each VDOM can be configured with different system hostnames.
C. Different VLAN sub-interface of the same physical interface can be assigned to different VDOMs.
D. Each VDOM has its own routing table.

Answer: C,D

Question: 7

What FortiGate components are tested during the hardware test? (Choose three.)

A. Administrative access
B. HA heartbeat
C. CPU
D. Hard disk
E. Network interfaces

Answer: C,D,E

Question: 8

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

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

Answer: A

Question: 9

Examine the exhibit, which shows the output of a web filtering real time debug.

```
Local-FortiGate # diagnose  debug enable

Local-FortiGate # diagnose debug application urlfilter -1

Local-FortiGate # msg="received a request /tmp/.wad_192_0_0.url.socket, addr_len
=31: d=www.bing.com:80, id=29, vfname='root', vfid=0, profile='default', type=0,
 client=10.0.1.10, url_source=1, url="/"
Url matches local rating
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=63683 dst=2
04.79.197.200 dport=80 service="http" cat=26 cat_desc="Malicious Websites" hostn
ame="www.bing.com" url="/"
```

Why is the site www.bing.com being blocked?

A. The web site www.bing.com is categorized by FortiGuard as Malicious Websites.
B. The user has not authenticated with the FortiGate yet.
C. The web server IP address 204.79.197.200 is categorized by FortiGuard as Malicious Websites.
D. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked.

Answer: D

Question: 10

When using WPAD DNS method, which FQDN format do browsers use to query the DNS server?

A. srv_proxy.<local-domain>/wpad.dat
B. srv_tcp.wpad.<local-domain>
C. wpad.<local-domain>
D. proxy.<local-domain>.wpad

Answer: C

https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/600_Objects/607_Web-proxy-global.htm

Question: 11

You have tasked to design a new IPsec deployment with the following criteria:
* All satellite offices must connect to the two HQ sites.
* The satellite offices do not need to communicate directly with other satellite offices.
* Backup VPN is not required.
* The design should minimize the number of tunnels being configured.
Which topology should be used to satisfy all of the requirements?

A. Partial mesh
B. Hub-and-spoke
C. Fully meshed
D. Redundant

Answer: B

Question: 12

What criteria does FortiGate use to look for a matching firewall policy to process traffic? (Choose two.)

A. Services defined in the firewall policy.
B. Incoming and outgoing interfaces
C. Highest to lowest priority defined in the firewall policy.
D. Lowest to highest policy ID number.

Answer: A,B

Question: 13

You are configuring the root FortiGate to implement the security fabric. You are configuring port10 to communicate with a downstream FortiGate. View the default Edit Interface in the exhibit below:

Edit Interface

Interface Name	port10(00:0C:29:53:DE:D7)
Alias	
Link Status	Up ⬆
Type	Physical Interface

Tags

Role ⓘ   Undefined ▾

➕ Add Tag Category

Address

Addressing mode   **Manual** DHCP One-Arm-Sniffer Dedicated to FortiSwitch

IP/Network Mask

Administrative Access

IPv4   ☐ HTTPS   ☐ HTTP ⓘ   ☐ PING   ☐ FMG-Access
         ☐ CAPWAP   ☐ SSH   ☐ SNMP   ☐ FTM
         ☐ RADIUS Accounting   ☐ FortiTelemetry

⬤ DHCP Server

Networked Devices

Device Detection ⬤

                        OK   Cancel

When configuring the root FortiGate to communicate with a downstream FortiGate, which settings are required to be configured? (Choose two.)

A. Device detection enabled.
B. B. Administrative Access: FortiTelemetry.
C. IP/Network Mask.
D. Role: Security Fabric.

Answer: B,C