DUMPSARENA

Fortinet NSE 8 Written Exam

Fortinet NSE8_811

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

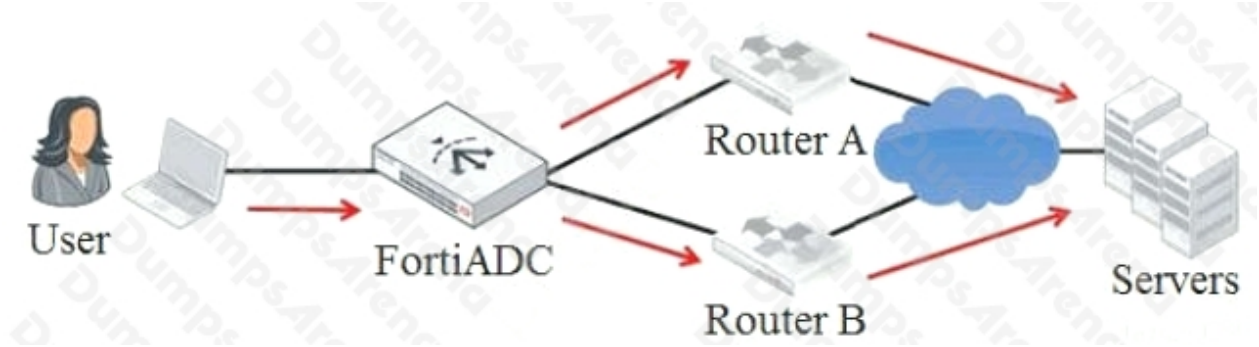
https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Refer to the exhibit.



As shown in the exhibit, a FortiADC is load-balancing IPv4 traffic between two next-hop routers. The FortiADC does not know the IP addresses of the servers. Also, the FortiADC is doing Layer 7 content inspection and modification.

In this scenario, which application delivery control is configured in the FortiADC?

A. Layer 3

B. Layer 4

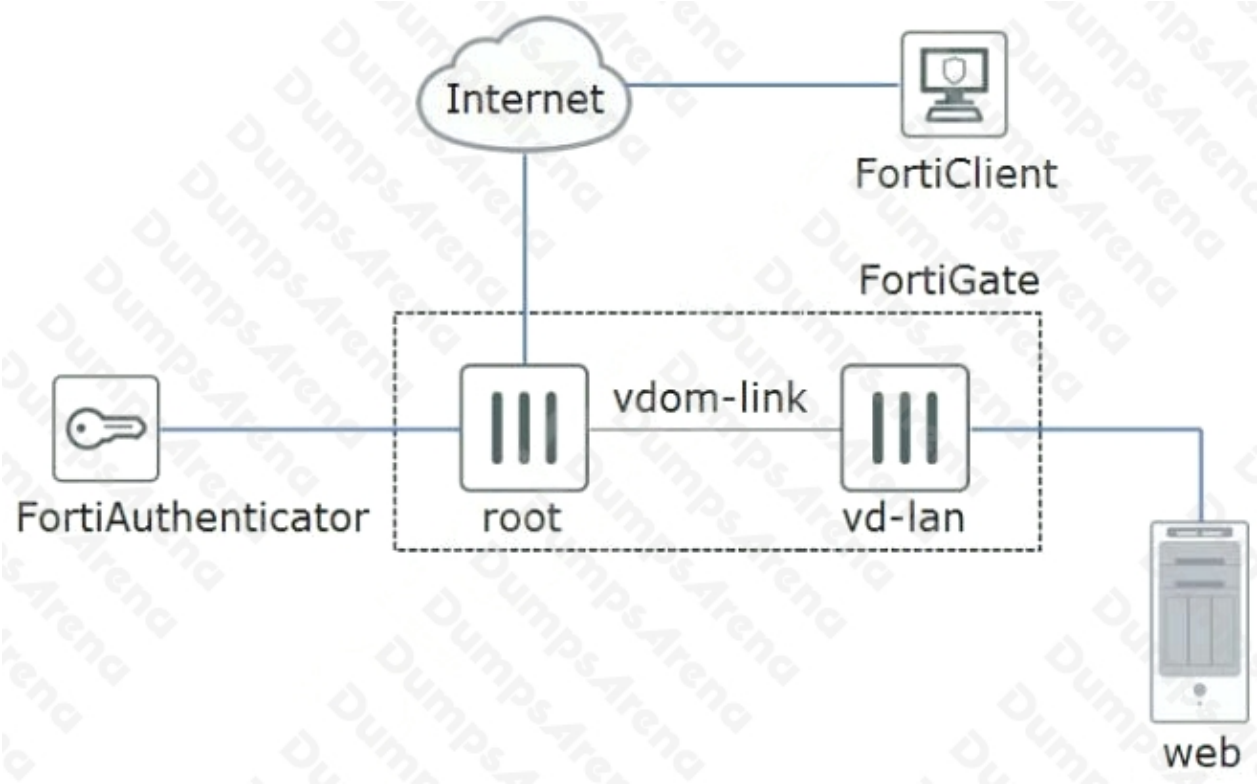
C. Layer 7

D. Layer 2

ANSWER: D

QUESTION NO: 2

Refer to the exhibit.



The exhibit shows a topology where a FortiGate is split into two VDOMs, root and vd-lan. The root VDOM provides external SSL-VPN access, where the users are authenticated by a FortiAuthenticator. The vd-lan VDOM provides internal access to a Web server.

For the remote users to access the internal Web server, there are a few requirements as follows:

• All traffic must come from the SSL-VPN.

• The vd-lan VDOM only allows authenticated traffic to the Web server.

• Users must only authenticate once, using the SSL-VPN portal.

• SSL-VPN uses RADIUS-based authentication.

Given these requirements and the topology shown in the exhibit, which two statements are true? (Choose two.)

A. vd-lan connects to FortiAuthenticator as a regular FSSO client.

B. root is configured for FSSO while vd-lan is configured for RSSO.

C. root sends "RADIUS Accounting Messages" to FortiAuthenticator

D. vd-lan receives authentication messages from root using FSSO.

ANSWER: A C

QUESTION NO: 3

A company has just deployed a new FortiMail in gateway mode. The administrator is asked to strengthen e-mail protection by applying the policies shown below.

• E-mails can only be accepted if a valid e-mail account exists.

• Only authenticated users can send e-mails out.

Which two actions will satisfy the requirements? (Choose two.)

A. Configure recipient address verification.

B. Configure inbound recipient policies.

C. Configure outbound recipient policies.

D. Configure access control rules.

ANSWER: A D

QUESTION NO: 4

A FortiGate is used as a VPN hub for a number of remote spoke VPN units (Group A) spokes using a phase 1 main mode dial-up tunnel and pre-shared keys. You are asked to establish VPN connectivity for a newly acquired organization's sites for which new devices will be provisioned Group B spokes.

Both existing Group A and new Group B spoke units are dynamically addressed through a single public IP Address on the hub. You are asked to ensure that spokes from Group B have different access permissions than the existing VPN spokes units Group A.

Which two solutions meet the requirements for the new spoke group? (Choose two.)

A. Implement a new phase 1 dial-up main mode tunnel with a different pre-shared key than the Group A spokes.

B. Implement a new phase 1 dial-up main mode tunnel with certificate authentication.

C. Implement a new phase 1 dial-up main mode tunnel with pre-shared keys and XAuth.

D. Implement separate phase 1 dial-up aggressive mode tunnels with a distinct peer ID.

ANSWER: C D

QUESTION NO: 5

Refer to the exhibit.

```
BO# config router ospf
      set distribute-list-in incoming
   end
BO# config router access-list
   edit incoming
      config rule
      edit 1
         set action deny
         set prefix 10.0.0.0 255.255.0.0
         set exact-match disable
      next
   end
   next
end
```

```
BO# get router info routing-table all
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
       * - candidate default

S* 0.0.0.0/0 [5/0] via 104.0.168.1, wan1
C 10.0.0.0/8 is directly connected, DMZ
O E2 10.10.10.0/24 [110/10] via 10.0.0.1, HQ-VPN, 00:08:05
C 104.0.168.0/22 is directly connected, wan1
C 172.16.1.0/24 is directly connected, LAN
O 192.168.17.0/24 [110/200] via 10.0.0.1, HQ-VPN, 00:08:05

BO # diag snif pack any 'host 10.10.10.35 and icmp' 4
interfaces=[any]
filters=[host 10.10.10.35 and icmp]
32.079784 DMZ in 172.16.1.70 -> 10.10.10.35: icmp: echo request
33.079792 HQ-VPN out 172.16.1.70 -> 10.10.10.35: icmp: echo request
34.080219 DMZ in 172.16.1.70 -> 10.10.10.35: icmp: echo request
35.080273 HQ-VPN out 10.0.0.2 -> 10.10.10.35: icmp: echo request
```

A VPN IPsec is connecting the headquarters office (HQ) with a branch office (BO). OSPF is used to redistribute routes between the offices. After deployment, a server with IP address 10.10.10.35 located on the DMZ network of the BO FortiGate, was reported unreachable from hosts located on the LAN network of the same FortiGate.

Referring to the exhibit, which statement is true?

A. The ICMP packets are being blocked by an implicit deny policy.

B. A directly connected subnet is being partially superseded by an OSPF redistributed subnet.

C. Enabling NAT on the VPN firewall policy will solve the problem.

D. The incoming access list should have an accept action instead of a deny action to solve the problem.

ANSWER: B

QUESTION NO: 6

Refer to the exhibit.

```
FS448D-A (LAG-1) # show
config switch trunk
   edit "LAG-1"
      set mode lacp-active
      set mclag-icl enable
      set members "port13" "port14"
   next
end

FS448D-B (LAG-2) # show
config switch trunk
   edit "LAG-2"
      set mode lacp-active
      set mclag-icl enable
      set members "port13" "portl4"
   next
end

FortiGate-A # show switch-controller managed-switch
config switch-controller managed-switch
   edit FS448D-A
      config ports
         edit "LAG-3"
            set type trunk
            set mode lacp-active
            set mclag enable
            set members "port15"
         next
      end
   next
   edit FS448D-B
      config ports
         edit "LAG-3"
            set type trunk
            set mode lacp-active
            set mclag enable
            set members "port15"
         next
      end
   next
end
```

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

A. LAG-3 on switches on FS448D-A and FS448D-B may be connected to a single 802.3ad trunk on another device.

B. LAG-1 and LAG-2 should be connected to a 4-port single 802.3ad trunk on another device.

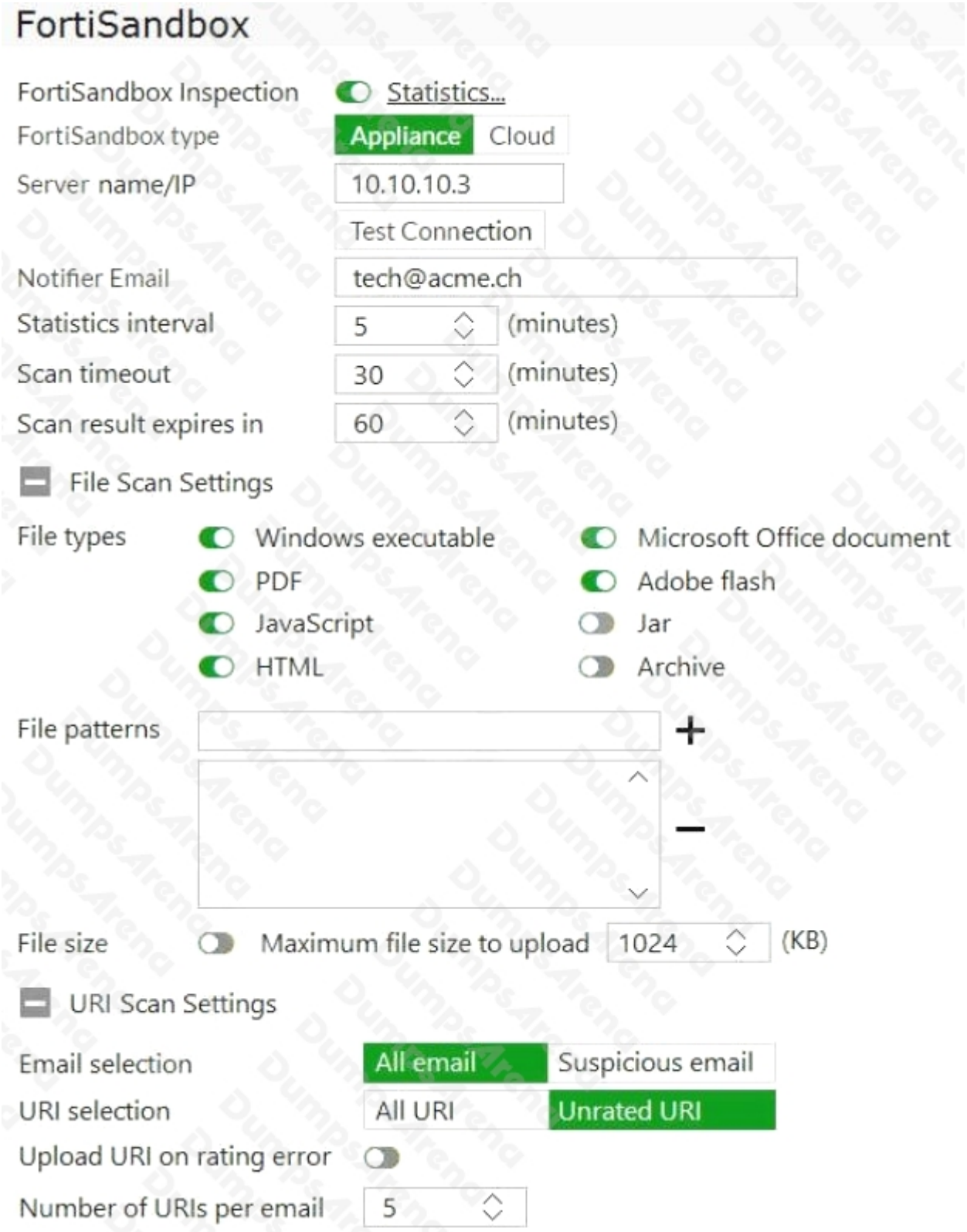
C. port13 and port14 on FS448D-A should be connected to port13 and port14 on FS448D-B.

D. LAG-1 and LAG-2 should be connected to a single 4-port 802.3ad interface on the FortiGate-A.

ANSWER: A C

QUESTION NO: 7

Refer to the exhibit.



You have installed a FortiSandbox and configured it in your FortiMail.

Referring to the exhibit, which two statements are correct? (Choose two.)

A. If FortiMail is not able to obtain the results from the FortiGuard queries, URIs will not be checked by the FortiSandbox.

B. FortiMail will cache the results for 30 minutes

C. If the FortiSandbox with IP 10.10.10.3 is not available, the e-mail will be checked by the FortiCloud Sandbox.

D. FortiMail will wait up to 30 minutes to obtain the scan results.

ANSWER: A D

QUESTION NO: 8

An organization has one central site and three remote sites. A FortiSIEM has been installed on the central site and now all devices across the remote sites must be centrally monitored by the FortiSIEM at the central site.

Which action will reduce the WAN usage by the monitoring system?

A. Enable SD-WAN FEC (Forward Error Correction) on the FortiGate at the remote site.

B. Install both Supervisor and Collector on each remote site.

C. Install local Collectors on each remote site.

D. Disable real-time log upload on the remote sites.

ANSWER: C

QUESTION NO: 9

Refer to the exhibit.

```
config waf url-rewrite url-rewrite-rule
    edit "NSE8-rule"
        set action redirect
        set location "https://$0/$1"
        set host-status disable
        set host-use-pserver disable
        set referer-status disable
        set referer-use-pserver disable
        set url-status disable
config match-condition
    edit 1
        set reg-exp "(.*)"
        set protocol-filter enable
    next
    edit 2
        set object http-url
        set reg-exp "^/(.*)$"
    next
end
    next
end
config waf url-rewrite url-rewrite-policy
    edit "nse8-rewrite"
config rule
    edit 1
        set url-rewrite-rule-name "NSE8-rule"
    next
    end
    next
end
```

The exhibit shows the steps for creating a URL rewrite policy on a FortiWeb.

Which statement represents the purpose of this policy?

A. The policy redirects all HTTPS URLs to HTTP.

B. The policy redirects all HTTP URLs to HTTPS.

C. The policy redirects only HTTP URLs containing the ^/(.*)$ string to HTTPS.

D. The policy redirects only HTTPS URLs containing the ^/(.*)$ string to HTTP.

ANSWER: B

QUESTION NO: 10

You configured a firewall policy with only a Web filter profile for accessing the Internet. Access to websites belonging to the "Information Technology" category are blocked and to the "Business" category are allowed. SSL deep inspection is not enabled on this policy.

A user wants to access the website https://www.it-acme.com which presents a certificate with CN=www.acme.com. The it-acme.com domain is categorized as "Information Technology" and the acme.com domain is categorized as "Business".

Which statement regarding this scenario is correct?

A. The FortiGate is able to read the URL within HTTPS sessions when using SSL certificate inspection so the website will be blocked by the "Information Technology".

B. The website will be blocked by category "Information Technology" as the SNI takes precedence over the certificate name.

C. The website will be allowed by category "Business" as the certificate name takes precedence over the URL.

D. Only with SSL deep inspection enabled will the FortiGate be able to categorized this website.

ANSWER: B