Fortinet.Pre. NSE6_FWB-6.1.by.VCEplus.30q - DEMO

Exam A

QUESTION 1
Which two statements about running a vulnerability scan are true? (Choose two.)

A. You should run the vulnerability scan during a maintenance window.
B. You should run the vulnerability scan in a test environment.
C. Vulnerability scanning increases the load on FortiWeb, so it should be avoided.
D. You should run the vulnerability scan on a live website to get accurate results.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Should the Vulnerability Scanner allow it, SVMS will set the scan schedule (or schedules) to run in a maintenance window. SVMS will advise Client of the scanner's ability to complete the scan(s) within the maintenance window.

Vulnerabilities on live web sites. Instead, duplicate the web site and its database in a test environment.

Reference: https://www.trustwave.com/media/17427/trustwave_mss_managed-3rd-party-vulnerability-scanning.pdf

https://help.fortinet.com/fweb/552/Content/FortiWeb/fortiweb-admin/vulnerability_scans.htm

QUESTION 2
FortiWeb offers the same load balancing algorithms as FortiGate.

Which two Layer 7 switch methods does FortiWeb also offer? (Choose two.)

A. Round robin
B. HTTP session-based round robin
C. HTTP user-based round robin
D. HTTP content routes

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/399384/defining-your-web-servers

http://fortinet.globalgate.com.ar/pdfs/FortiWeb/FortiWeb_DS.pdf

QUESTION 3
Which would be a reason to implement HTTP rewriting?

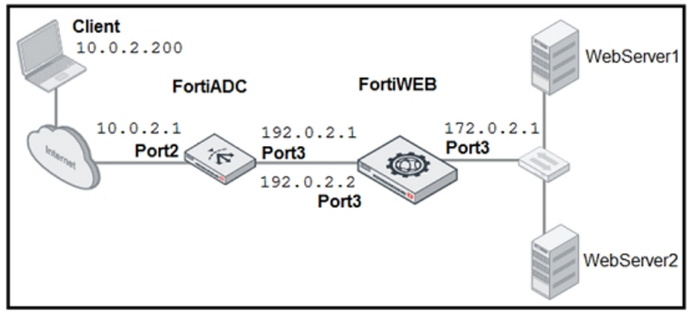
A. The original page has moved to a new URL
B. To replace a vulnerable function in the requested URL
C. To send the request to secure channel
D. The original page has moved to a new IP address

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Create a new URL rewriting rule.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/961303/rewriting-redirecting

QUESTION 4
Refer to the exhibit.



FortiADC is applying SNAT to all inbound traffic going to the servers. When an attack occurs, FortiWeb blocks traffic based on the `192.0.2.1` source IP address, which belongs to FortiADC. The setup is breaking all connectivity and genuine clients are not able to access the servers.

What must the administrator do to avoid this problem? (Choose two.)

A. Enable the Use X-Forwarded-For setting on FortiWeb.
B. No Special configuration is required; connectivity will be re-established after the set timeout.
C. Place FortiWeb in front of FortiADC.
D. Enable the Add X-Forwarded-For setting on FortiWeb.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Configure your load balancer to insert or append to an X-Forwarded-For:, X-Real-IP:, or other HTTP X-header. Also configure FortiWeb to find the original attacker's or client's IP address in that HTTP header

Reference: https://help.fortinet.com/fweb/560/Content/FortiWeb/fortiweb-admin/planning_topology.htm

QUESTION 5
Which statement about local user accounts is true?

A. They are best suited for large environments with many users.
B. They cannot be used for site publishing.
C. They must be assigned, regardless of any other authentication.
D. They can be used for SSO.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can configure the Remedy Single Sign-On server to authenticate TrueSight Capacity Optimization users as local users.

Reference: https://docs.bmc.com/docs/TSCapacity/110/setting-up-local-user-authentication-in-remedy-sso-743238341.html

QUESTION 6
Refer to the exhibit.

Fall-open Setting		
port3-port4	PowerOff-CutOff	PowerOff-Bypass
port5-port6	PowerOff-CutOff	PowerOff-Bypass

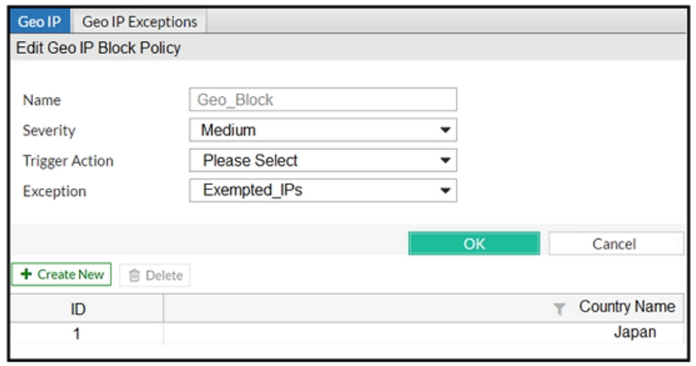
Based on the configuration, what would happen if this FortiWeb were to lose power? (Choose two.)

A. Traffic that passes between port5 and port6 will be inspected.
B. Traffic will be interrupted between port3 and port4.
C. All traffic will be interrupted.
D. Traffic will pass between port5 and port6 uninspected.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortiweb/6.3.10/administration-guide/33485/fail-to-wire-for-power-loss-reboots

QUESTION 7
Refer to the exhibit.



FortiWeb is configured to block traffic from Japan to your web application server. However, in the logs, the administrator is seeing traffic allowed from one particular IP address which is geo-located in Japan.

What can the administrator do to solve this problem? (Choose two.)

A. Manually update the geo-location IP addresses for Japan.
B. If the IP address is configured as a geo reputation exception, remove it.
C. Configure the IP address as a blacklisted IP address.
D. If the IP address is configured as an IP reputation exception, remove it.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IP reputation leverages many techniques for accurate, early, and frequently updated identification of compromised and malicious clients so you can block attackers before they target your servers.
IP blacklisting is a method used to filter out illegitimate or malicious IP addresses from accessing your networks. Blacklists are lists containing ranges of or individual IP addresses that you want to block.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.5/administration-guide/137271/blacklisting-whitelisting-clients

https://www.imperva.com/learn/application-security/ip-blacklist/

QUESTION 8
Which algorithm is used to build mathematical models for bot detection?

A. HCM
B. SVN
C. SVM
D. HMM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiWeb uses SVM (Support Vector Machine) algorithm to build up the bot detection model

Reference: https://docs.fortinet.com/document/fortiweb/6.3.7/administration-guide/193258/machine-learning

QUESTION 9
A client is trying to start a session from a page that would normally be accessible only after the client has logged in.

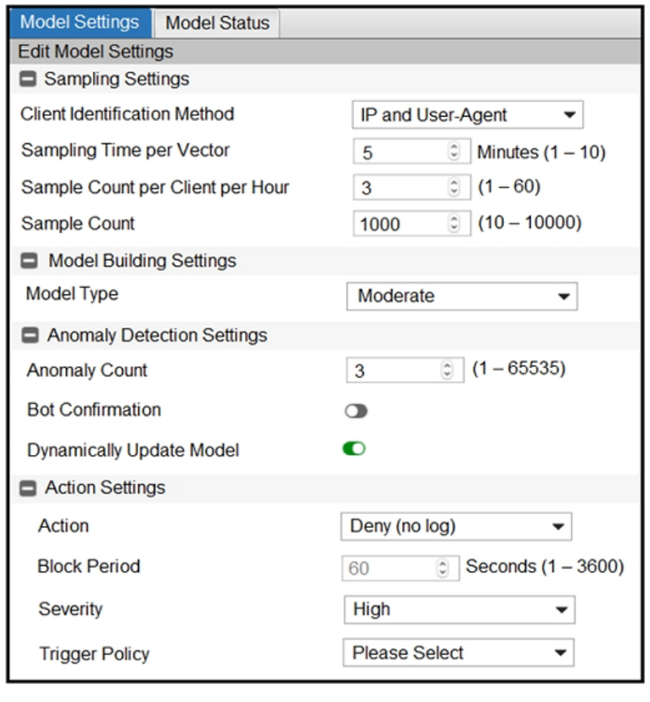
When a start page rule detects the invalid session access, what can FortiWeb do? (Choose three.)

A. Display an access policy message, then allow the client to continue
B. Redirect the client to the login page
C. Allow the page access, but log the violation
D. Prompt the client to authenticate
E. Reply with a 403 Forbidden HTTP error

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://help.fortinet.com/fweb/607/Content/FortiWeb/fortiweb-admin/specify_urls_to_initiate.htm

QUESTION 10
Refer to the exhibit.



Many legitimate users are being identified as bots. FortiWeb bot detection has been configured with the settings shown in the exhibit. The FortiWeb administrator has already verified that the current model is accurate.

What can the administrator do to fix this problem, making sure that real bots are not allowed through FortiWeb?

A. Change Model Type to Strict
B. Change Action under Action Settings to Alert
C. Disable Dynamically Update Model
D. Enable Bot Confirmation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bot Confirmation
If the number of anomalies from a user has reached the Anomaly Count, the system executes Bot Confirmation before taking actions.
The Bot Confirmation is to confirm if the user is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check if it's a real bot.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.1/administration-guide/600188/configuring-bot-detection-profiles

QUESTION 11
What can an administrator do if a client has been incorrectly period blocked?

A. Nothing, it is not possible to override a period block.
B. Manually release the ID address from the temporary blacklist.
C. Force a new IP address to the client.
D. Disconnect the client from the network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Block Period
Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds. The default value is 60 seconds.
This option only takes effect when you choose Period Block in Action.
Note: That's a temporary blacklist so you can manually release them from the blacklist.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.1/administration-guide/600188/configuring-bot-detection-profiles

QUESTION 12
Which regex expression is the correct format for redirecting the URL http://www.example.com?

A. www\.example\.com
B. www.example.com
C. www\example\com
D. www/.example/.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
\1://www.company.com/\2/\3

Reference: https://learn.akamai.com/en-us/webhelp/edge-redirector/edge-redirector-guide/GUID-0C22DFC2-DCC4-42AF-BDB2-9537FBEE03FD.html

QUESTION 13
When FortiWeb triggers a redirect action, which two HTTP codes does it send to the client to inform the browser of the new URL? (Choose two.)

A. 403
B. 302
C. 301
D. 404

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/302

QUESTION 14
True transparent proxy mode is best suited for use in which type of environment?

A. New networks where infrastructure is not yet defined
B. Flexible environments where you can easily change the IP addressing scheme
C. Small office to home office environments
D. Environments where you cannot change the IP addressing scheme

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Does not require changes to the IP address scheme of the network. Requests are destined for a web server and not the FortiWeb appliance. This operation mode supports the same feature set as True Transparent Proxy mode.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/211763/planning-the-network-topology

QUESTION 15
Review the following configuration:

```
config waf machine-learning-policy
edit 1
set sample-limit-by-ip 0
next
end
```

What is the expected result of this configuration setting?

A. When machine learning (ML) is in its collecting phase, FortiWeb will accept an unlimited number of samples from the same source IP address.
B. When machine learning (ML) is in its running phase, FortiWeb will accept an unlimited number of samples from the same source IP address.
C. When machine learning (ML) is in its collecting phase, FortiWeb will not accept any samples from any source IP addresses.
D. When machine learning (ML) is in its running phase, FortiWeb will accept a set number of samples from the same source IP address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which two statements about the anti-defacement feature on FortiWeb are true? (Choose two.)

A. Anti-defacement can redirect users to a backup web server, if it detects a change.
B. Anti-defacement downloads a copy of your website to RAM, in order to restore a clean image, if it detects defacement.
C. FortiWeb will only check to see if there are changes on the web server; it will not download the whole file each time.
D. Anti-defacement does not make a backup copy of your databases.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Anti-defacement backs up web pages only, **not** databases.
If it detects any file changes, the FortiWeb appliance will download a new backup revision.

Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

QUESTION 17
What must you do with your FortiWeb logs to ensure PCI DSS compliance?

A. Store in an off-site location
B. Erase them every two weeks
C. Enable masking of sensitive data
D. Compress them into a .zip file format

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docplayer.net/8466775-Fortiweb-web-application-firewall-ensuring-compliance-for-pci-dss-requirement-6-6-solution-guide.html

QUESTION 18
What role does FortiWeb play in ensuring PCI DSS compliance?

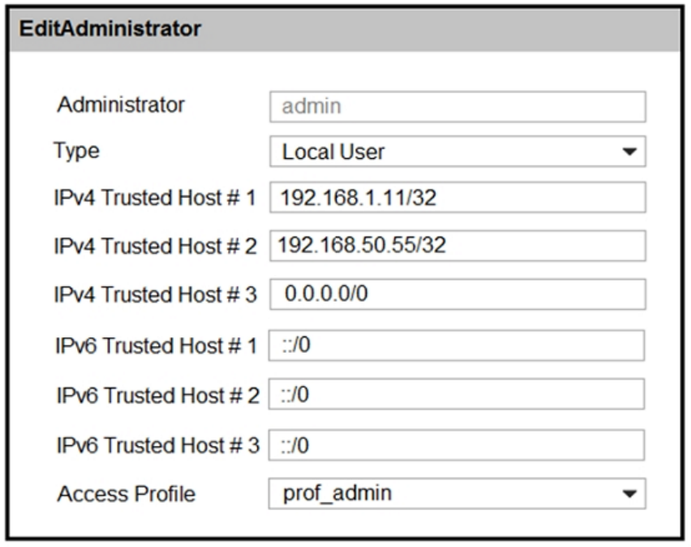
A. It provides the ability to securely process cash transactions.
B. It provides the required SQL server protection.
C. It provides the WAF required by PCI.
D. It provides credit card processing capabilities.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiWeb protects against attacks that lead to sensitive data exposure such as SQL Injection and other injection types. Additionally, FortiWeb inspects all web server outgoing traffic for sensitive data such as Social Security numbers, credit card numbers and other predefined or custom based sensitive data.

Reference: https://www.gordion.de/fileadmin/user_upload/SG-PCI-Compliance.pdf

QUESTION 19
Refer to the exhibit.



There is only one administrator account configured on FortiWeb. What must an administrator do to restrict any brute force attacks that attempt to gain access to the FortiWeb management GUI?

A. Delete the built-in administrator user and create a new one.
B. Configure IPv4 Trusted Host # 3 with a specific IP address.
C. The configuration changes must be made on the upstream device.
D. Change the Access Profile to Read_Only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortiweb/6.1.1/administration-guide/397469/preventing-brute-force-logins

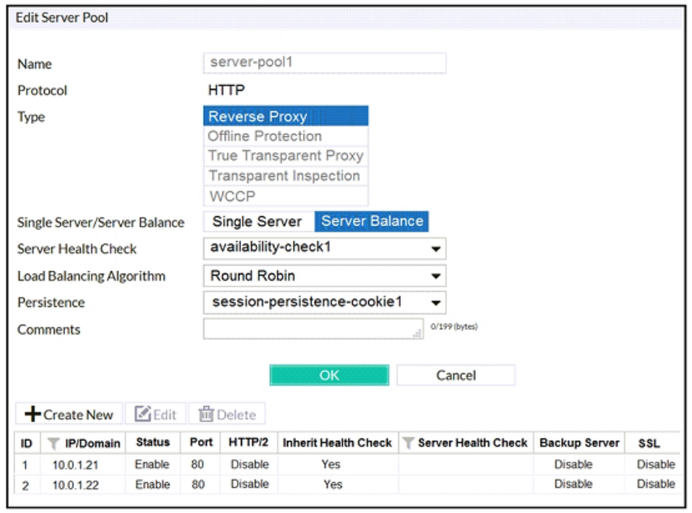
QUESTION 20
What key factor must be considered when setting brute force rate limiting and blocking?

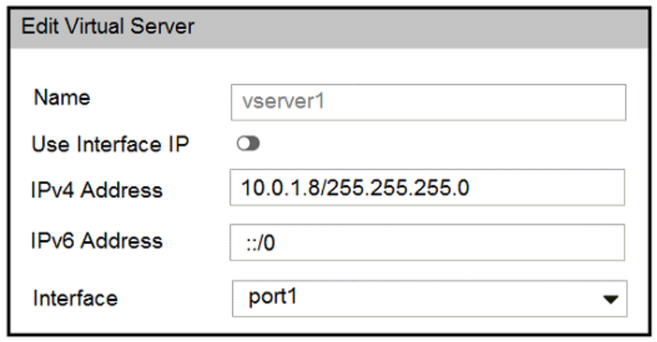
A. A single client contacting multiple resources
B. Multiple clients sharing a single Internet connection
C. Multiple clients from geographically diverse locations
D. Multiple clients connecting to multiple resources

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Refer to the exhibits.





FortiWeb is configured in reverse proxy mode and it is deployed downstream to FortiGate. Based on the configuration shown in the exhibits, which of the following statements is true?

A. FortiGate should forward web traffic to the server pool IP addresses.
B. The configuration is incorrect. FortiWeb should always be located upstream to FortiGate.
C. You must disable the Preserve Client IP setting on FotriGate for this configuration to work.
D. FortiGate should forward web traffic to virtual server IP address.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ebe2ce28-5c66-11eb-b9ad-00505692583a/FortiWeb_6.3.10_Administration_Guide.pdf

QUESTION 22
When is it possible to use a self-signed certificate, rather than one purchased from a commercial certificate authority?

A. If you are a small business or home office
B. If you are an enterprise whose employees use only mobile devices
C. If you are an enterprise whose resources do not need security
D. If you are an enterprise whose computers all trust your active directory or other CA server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This can include SSL/TLS certificates, code signing certificates, and S/MIME certificates. The reason why they're considered different from traditional certificate-authority signed certificates is that they're created, issued, and signed by the company or developer who is responsible for the website or software being signed. This is why self-signed certificates are considered unsafe for public-facing websites and applications.

Reference: https://sectigostore.com/page/what-is-a-self-signed-certificate/

QUESTION 23
In which scenario might you want to use the compression feature on FortiWeb?

A. When you are serving many corporate road warriors using 4G tablets and phones
B. When you are offering a music streaming service
C. When you want to reduce buffering of video streams
D. Never, since most traffic today is already highly compressed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiWeb might expend resources compressing responses that have already been compressed by the server.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.7/administration-guide/650285/compression

QUESTION 24
The FortiWeb machine learning (ML) feature is a two-phase analysis mechanism.

Which two functions does the first layer perform? (Choose two.)

A. Determines whether an anomaly is a real attack or just a benign anomaly that should be ignored
B. Builds a threat model behind every parameter and HTTP method
C. Determines if a detected threat is a false-positive or not
D. Determines whether traffic is an anomaly, based on observed application traffic over time

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The first layer uses the Hidden Markov Model (HMM) and monitors access to the application and collects data to build a mathematical model behind every parameter and HTTP method.

Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/193258/machine-learning

QUESTION 25
In which two operating modes can FortiWeb modify HTTP packets? (Choose two.)

A. Offline protection
B. Transparent inspection
C. True transparent proxy
D. Reverse proxy

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiWeb appliances operating in offline protection mode or either of the transparent modes

Reference: https://help.fortinet.com/fweb/541/Content/FortiWeb/fortiweb-admin/planning_topology.htm

QUESTION 26

When viewing the attack logs on FortiWeb, which client IP address is shown when you are using XFF header rules?

A. FortiGate public IP
B. FortiWeb IP
C. FortiGate local IP
D. Client real IP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When an XFF header reaches Alteon from a client, Alteon removes all the content from the header and injects the client IP address. Alteon then forwards the header to the server.

Reference: https://support.radware.com/app/answers/answer_view/a_id/20925/~/modifying-the-client-ip-address-in-the-xff-header-using-httpmod

QUESTION 27
Which three statements about HTTPS on FortiWeb are true? (Choose three.)

A. In true transparent mode, the TLS session terminator is a protected web server.
B. After enabling HSTS, redirects to HTTPS are never needed.
C. For SNI, you select the certificate that FortiWeb presents in the server pool, not in the server policy.
D. Enabling RC4 protects against the BEAST attack, but is not recommended if you configure FortiWeb to offer only TLS 1.2.
E. In transparent inspection mode, you select the certificate that FortiWeb presents in the server pool, not in the server policy.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortiweb/6.3.0/administration-guide/742465/supported-cipher-suites-protocol-versions

QUESTION 28
What is one of the key benefits of the FortiGuard IP reputation feature?

A. It maintains a list of private IP addresses.
B. It provides a document of IP addresses that are suspect, so that administrators can manually update their blacklists.
C. It is updated once per year.
D. It maintains a list of public IPs with a bad reputation for participating in attacks.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiGuard IP Reputation service assigns a poor reputation, including virus-infected clients and malicious spiders/crawlers.

Reference: https://docs.fortinet.com/document/fortiweb/6.1.1/administration-guide/137271/blacklisting-whitelisting-clients

QUESTION 29
How does FortiWeb protect against defacement attacks?

A. It keeps a complete backup of all files and the database.
B. It keeps hashes of files and periodically compares them to the server.
C. It keeps full copies of all files and directories.
D. It keeps a live duplicate of the database.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The anti-defacement feature examines a web site's files for changes at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb appliance can notify you and quickly react by automatically restoring the web site contents to the previous backup.

Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

QUESTION 30
You are using HTTP content routing on FortiWeb. You want requests for web application A to be forwarded to a cluster of web servers, which all host the same web application. You want requests for web application B to be forwarded to a different, single web server.

Which statement about this solution is true?

A. The server policy applies the same protection profile to all of its protected web applications.
B. You must put the single web server in to a server pool, in order to use it with HTTP content routing.
C. You must chain policies so that requests for web application A go to the virtual server for policy A, and requests for web application B go to the virtual server for policy B.
D. Static or policy-based routes are not required.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: