NSE4_FGT-6.4 Q&As

Fortinet NSE 4 - FortiOS 6.4

Pass Fortinet NSE4_FGT-6.4 Exam with 100% Guarantee

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

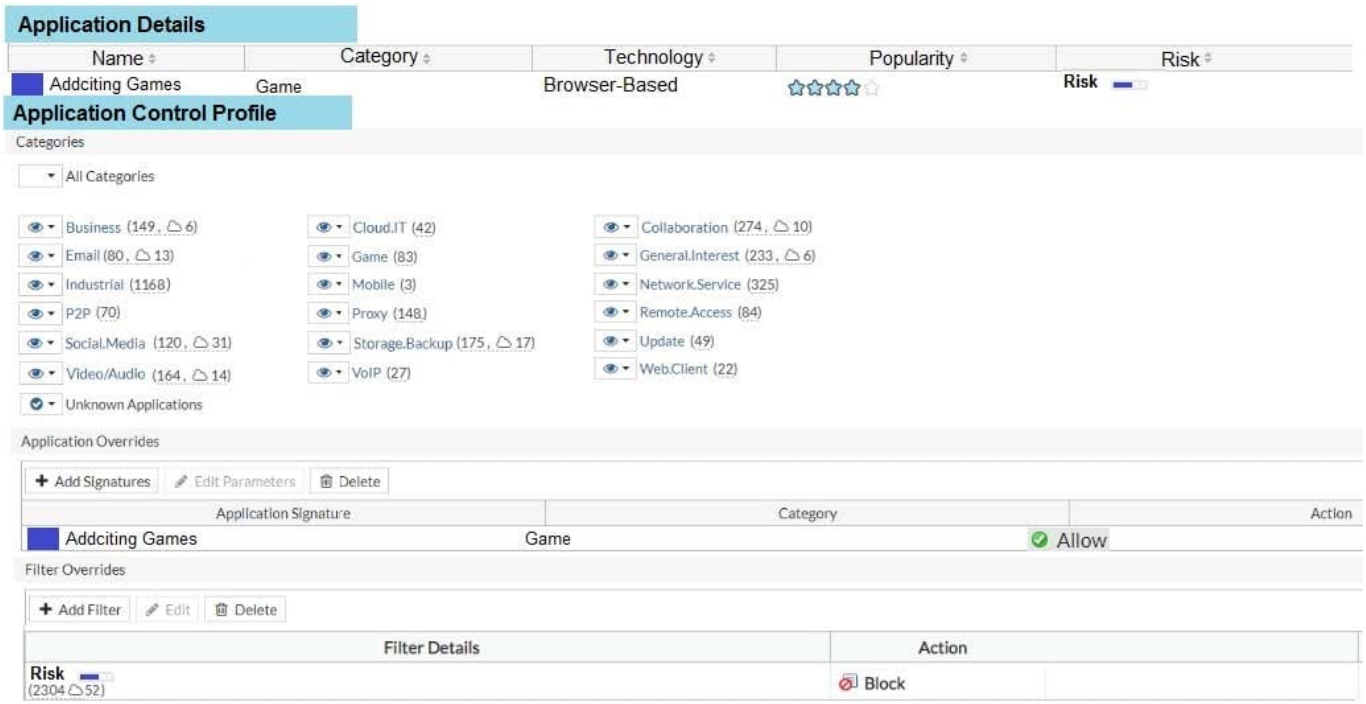
https://www.leads4pass.com/nse4_fgt-6-4.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

View the exhibit.



A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting Games). Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.

B. Addicting.Games is blocked on the Filter Overrides configuration.

C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.

D. Addcting.Games is allowed based on the Categories configuration.

Correct Answer: A

QUESTION 2

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.

Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning

B. File filter

C. DNS filter

D. Intrusion prevention

Correct Answer: AD

QUESTION 3

Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode

B. Can act as a Layer 2 switch as well as a Layer 3 router

C. All interfaces in the software switch share the same IP address

D. It can group only physical interfaces

Correct Answer: AC

QUESTION 4

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, FortiGate buffers the file, but also simultaneously transmits it to the client.

C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.

D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Correct Answer: BC

QUESTION 5

What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Traffic to botnetservers

B. Traffic to inappropriate web sites

C. Server information disclosure attacks

D. Credit card data leaks

E. SQL injection attacks

Correct Answer: CDE

QUESTION 6

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" dstip=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
rcvdbyte=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" dstip=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 rcvdbyte=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. Social networking web filter category is configured with the action set to authenticate.

B. The action on firewall policy ID 1 is set to warning.

C. Access to the social networking web filter category was explicitly blocked to all users.

D. The name of the firewall policy is all_users_web.

Correct Answer: A

QUESTION 7

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view

B. Log backups from the CLI cannot be restored to another FortiGate.

C. Log backups from the CLI can be configured to upload to FTP as a scheduled time

D. Log downloads from the GUI are stored as LZ4 compressed files.

Correct Answer: AB

QUESTION 8

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.

B. By default, the SSL VPN portal requires the installation of a client\\'s certificate.

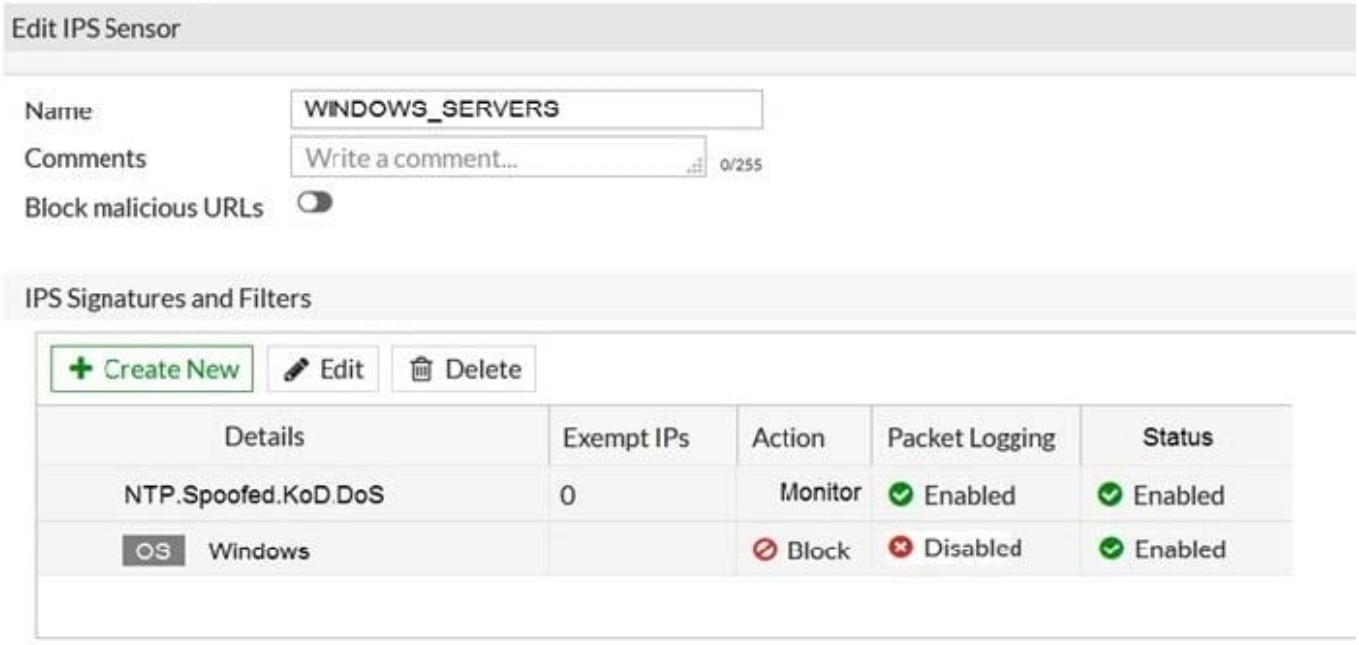
C. By default, split tunneling is enabled.

D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Correct Answer: D

QUESTION 9

Refer to the exhibit.



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 allow attackers matching the NTP.Spoofed.KoD.DoS signature.

B. The sensor will block all attacks aimed at Windows servers.

C. The sensor will reset all connections that match these signatures.

D. The sensor will gather a packet log for all matched traffic.

Correct Answer: AB

QUESTION 10

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 11

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

A. Configure Source IP Pools.

B. Configure split tunneling in tunnel mode.

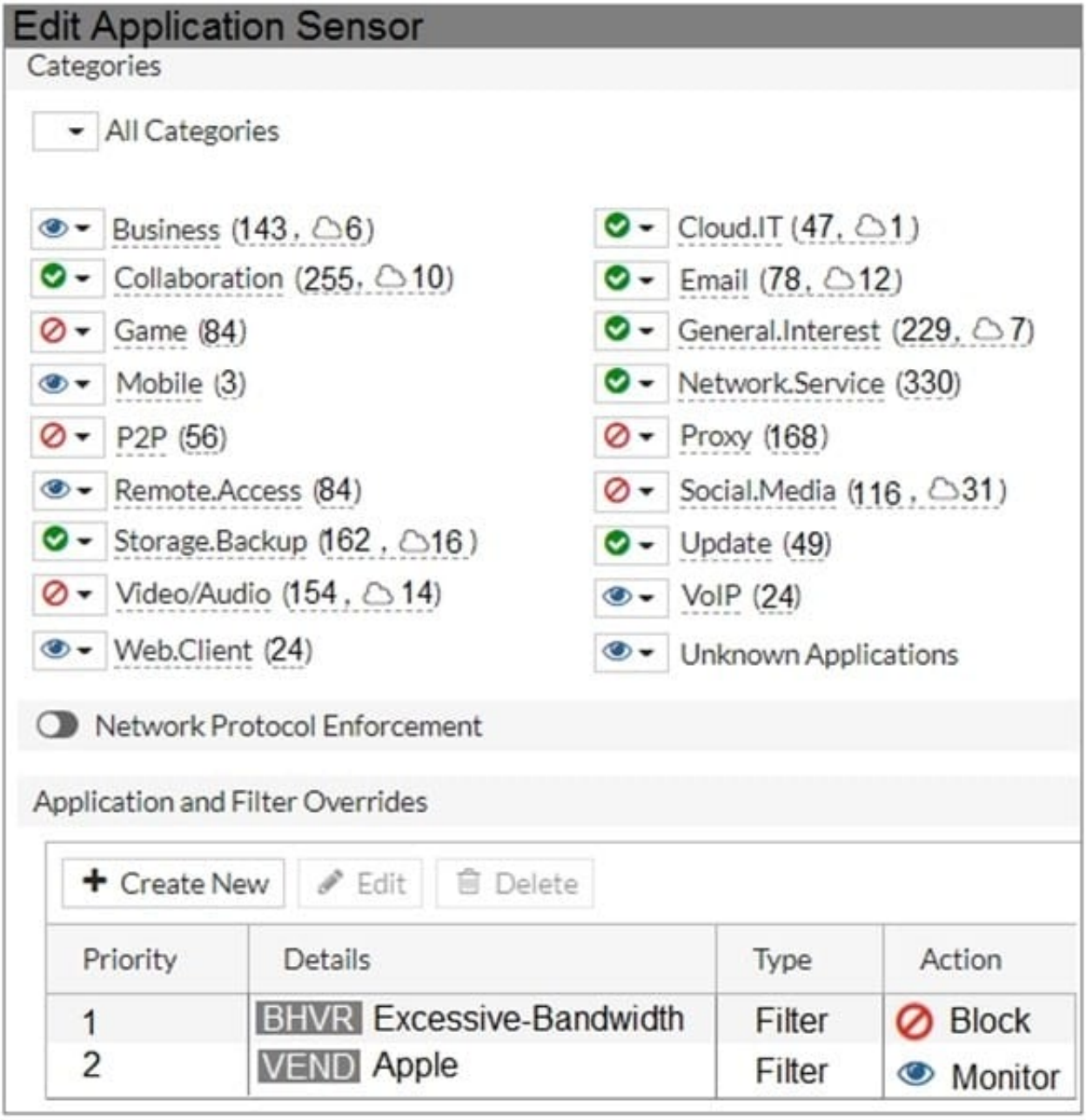
C. Configure different SSL VPN realms.

D. Configure host check.

Correct Answer: D

QUESTION 12

Refer to the exhibit to view the application control profile.



Users who use Apple FaceTime video conferences are unable to set up meetings. In this scenario, which statement is true?

A. Apple FaceTime belongs to the custom monitored filter.

B. The category of Apple FaceTime is being monitored.

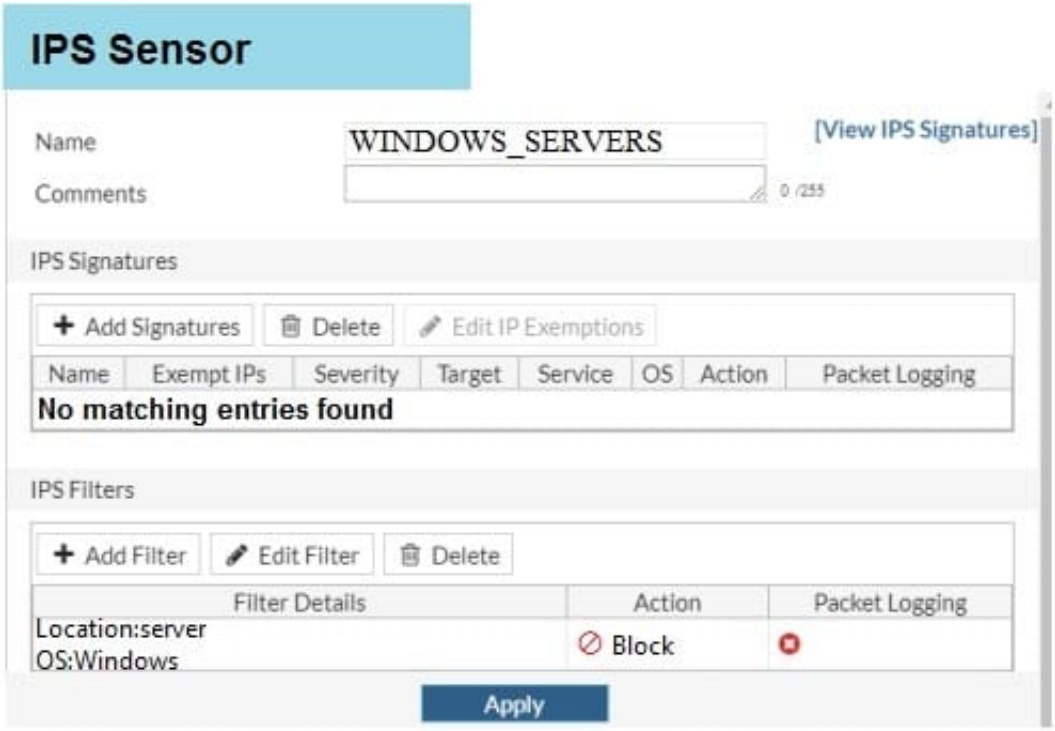
C. Apple FaceTime belongs to the custom blocked filter.

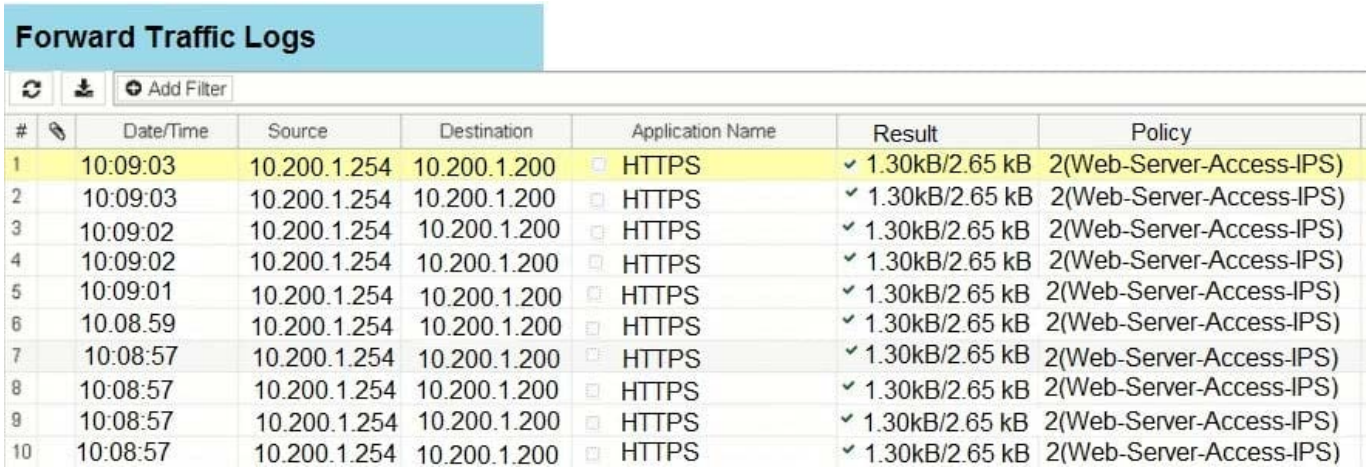
D. The category of Apple FaceTime is being blocked.

Correct Answer: C

QUESTION 13

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





An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.

What is a possible reason for this?

A. The IPS filter is missing the Protocol: HTTPS option.

B. The HTTPS signatures have not been added to the sensor.

C. A DoS policy should be used, instead of an IPS sensor.

D. A DoS policy should be used, instead of an IPS sensor.

E. The firewall policy is not using a full SSL inspection profile.

Correct Answer: E

QUESTION 14

Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.

B. Source IP is translated to the outgoing interface IP.

C. Connections are tracked using source port and source MAC address.

D. Port address translation is not used.

Correct Answer: BD

QUESTION 15

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

A. Source defined as Internet Services in the firewall policy.

B. Destination defined as Internet Services in the firewall policy.

C. Highest to lowest priority defined in the firewall policy.

D. Services defined in the firewall policy.

E. Lowest to highest policy ID number.

Correct Answer: ABD

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435