NSE7_EFW-7.2 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.2

Pass Fortinet NSE7_EFW-7.2 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse7_efw-7-2.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Exhibit.

```
# diagnose webfilter fortiguard cache dump

Saving to file [/tmp/urcCache.txt]
Cache Contents:
---------------
Cache Mode:   TTL
Cache DB Ver: 23.6106

Domain   |IP       DB Ver   T URL
34000000|34000000 23.6106   P Bhttp://training.fortinet.com/
25000000|25000000 23.6106   E Bhttps://twitter.com/…

# get webfilter categories
…
g07 General Interest - Business:
     31 Finance and Banking
     …
     51 Government and Legal Organizations
     52 Information Technology
```

Refer to the exhibit, which shows the output from the webfilter fortiguard cache dump and webfilter categories commands.

Using the output, how can an administrator determine the category of the training.fortinet.comam website?

A. The administrator must convert the first three digits of the IP hex value to binary

B. The administrator can look up the hex value of 34 in the second command output.

C. The administrator must add both the Pima in and Iphex values of 34 to get the category number

D. The administrator must convert the first two digits of the Domain hex value to a decimal value

Correct Answer: B

Option B is correct because the administrator can determine the category of the training.fortinet.com website by looking up the hex value of 34 in the second command output. This is because the first command output shows that the domain and the IP of the website are both in category (Hex) 34, which corresponds to Information Technology in the second command output1. Option A is incorrect because the administrator does not need to convert the first three digits of the IP hex value to binary. The IP hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion2. Option C is incorrect because the administrator does not need to add both the Pima in and Iphex values of 34 to get the category number. The Pima in and Iphex values are not related to the category number, but to the cache TTL and the database version respectively3. Option D is incorrect because the administrator does not need to convert the first two digits of the Domain hex value to a decimal value. The Domain hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion2. References: =

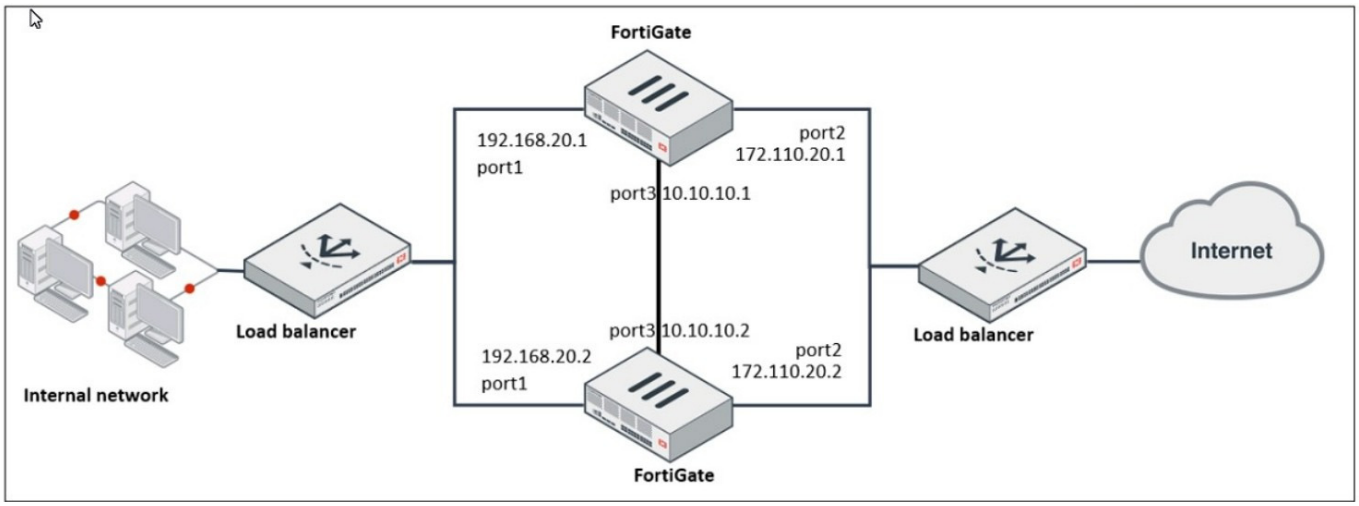
1: Technical Tip: Verify the webfilter cache content4

2: Hexadecimal to Decimal Converter5

3: FortiGate - Fortinet Community6 : Web filter | FortiGate / FortiOS 7.2.0 - Fortinet Documentation7

QUESTION 2

Refer to the exhibit, which shows a network diagram.



Which protocol should you use to configure the FortiGate cluster?

A. FGCP in active-passive mode

B. OFGSP

C. VRRP

D. FGCP in active-active mode

Correct Answer: A

Given the network diagram and the presence of two FortiGate devices, the Fortinet Gate Clustering Protocol (FGCP) in active-passive mode is the most appropriate for setting up a FortiGate cluster. FGCP supports high availability configurations and is designed to allow one FortiGate to seamlessly take over if the other fails, providing continuous network availability. This is supported by Fortinet documentation for high availability configurations using FGCP.

QUESTION 3

In which two ways does fortiManager function when it is deployed as a local FDS? (Choose two)

A. It can be configured as an update server a rating server or both

B. It provides VM license validation services

C. It supports rating requests from non-FortiGate devices.

D. It caches available firmware updates for unmanaged devices

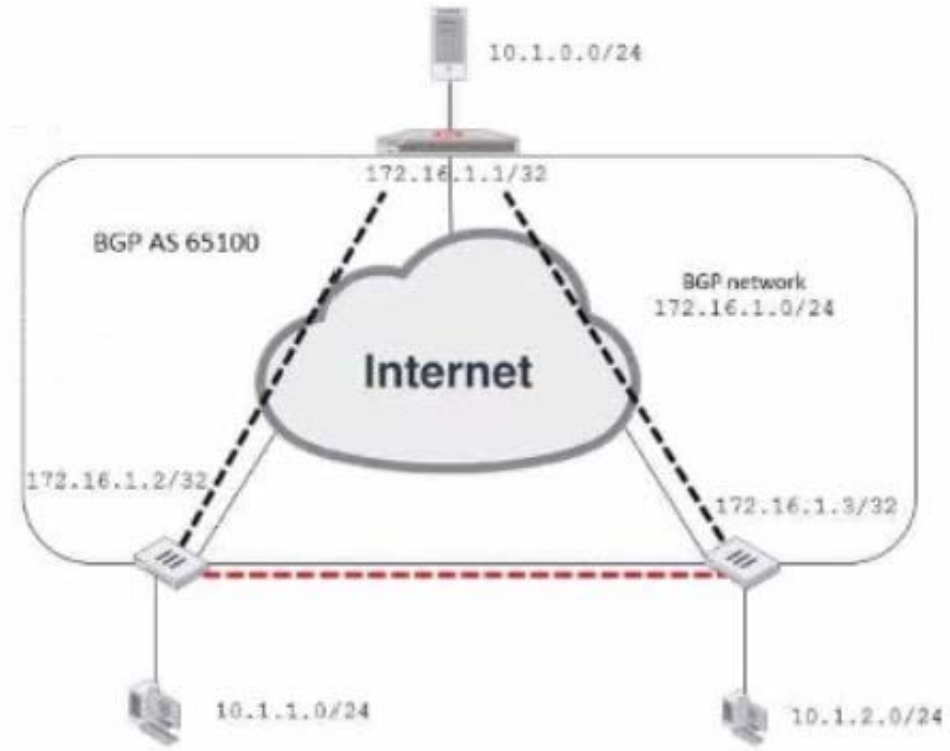
Correct Answer: AB

When deployed as a local FortiGuard Distribution Server (FDS), FortiManager functions in several capacities. It can act as an update server, a rating server, or both, providing firmware updates and FortiGuard database updates. Additionally, it plays a crucial role in VM license validation services, ensuring that the connected FortiGate devices are operating with valid licenses. However, it does not support rating requests from non-FortiGate devices nor cache firmware updates for unmanaged devices. Fortinet FortiOS Handbook: FortiManager as a Local FDS Configuration

QUESTION 4

Exhibit.

Network diagram



Partial BGP configuration

```
Hub # show router bgp
config router bgp
    set as 65100
    set router-id 172.16.1.1
    config neighbor-group
        edit "advpn"
            set remote-as 65100
            ...
        next
    end
....
end
```

Refer to the exhibit, which contains an ADVPN network diagram and a partial BGP con figuration Which two parameters Should you configure in config neighbor range? (Choose two.)

A. set prefix 172.16.1.0 255.255.255.0

B. set route reflector-client enable

C. set neighbor-group advpn

D. set prefix 10.1.0 255.255.255.0

Correct Answer: AC

In the ADVPN configuration for BGP, you should specify the prefix that the neighbors can advertise. Option A is correct as you would configure the BGP network prefix that should be advertised to the neighbors, which matches the BGP network in the diagram. Option C is also correct since you should reference the neighbor group configured for the ADVPN setup within the BGP configuration.

QUESTION 5

After enabling IPS you receive feedback about traffic being dropped.

What could be the reason?

A. Np-accel-mode is set to enable

B. Traffic-submit is set to disable

C. IPS is configured to monitor

D. Fail-open is set to disable

Correct Answer: D

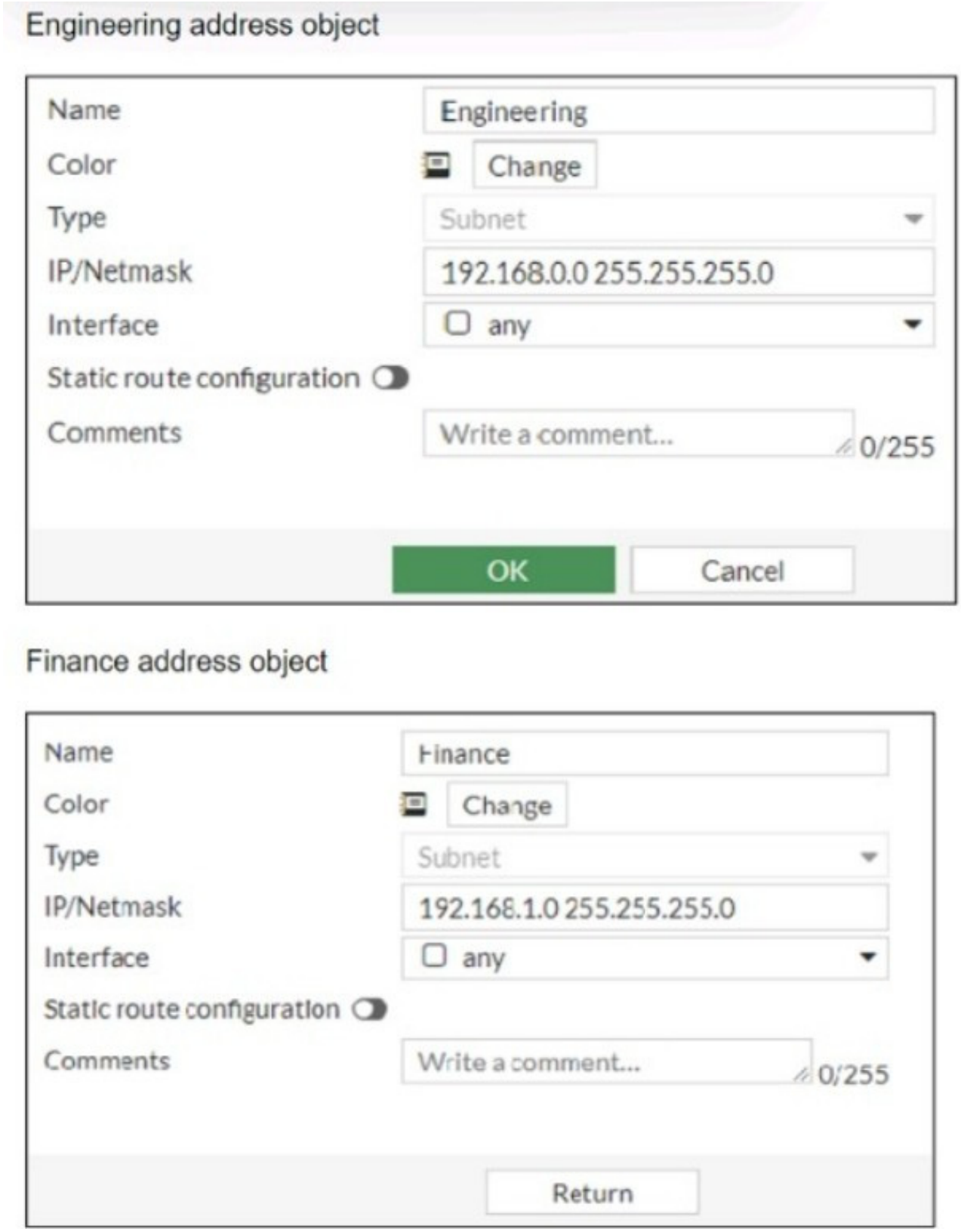
Fail-open is a feature that allows traffic to pass through the IPS sensor without inspection when the sensor fails or is overloaded. If fail-open is set to disable, traffic will be dropped in such scenarios1. References: = IPS | FortiGate / FortiOS

7.2.3 - Fortinet Documentation

When IPS (Intrusion Prevention System) is configured, iffail-openis set to disable, it means that if the IPS engine fails, traffic will not be allowed to pass through, which can result in traffic being dropped (D). This is in contrast to a fail-open setting, which would allow traffic to bypass the IPS engine if it is not operational.

QUESTION 6

Refer to the exhibits, which show the configurations of two address objects from the same FortiGate.



Why can you modify the Engineering address object, but not the Finance address object?

A. You have read-only access.

B. FortiGate joined the Security Fabric and the Finance address object was configured on the root FortiGate.

C. FortiGate is registered on FortiManager.

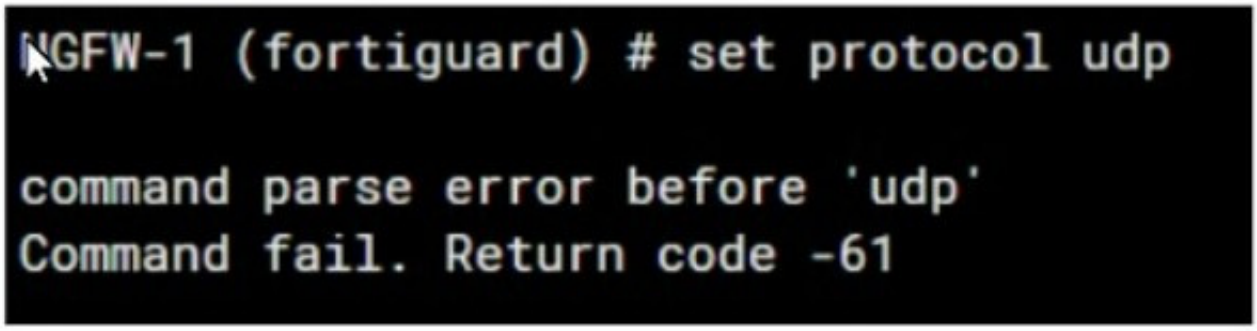
D. Another user is editing the Finance address object in workspace mode.

Correct Answer: B

The inability to modify the Finance address object while being able to modify the Engineering address object suggests that the Finance object is being managed by a higher authority in the Security Fabric, likely the root FortiGate. When a FortiGate is part of a Security Fabric, address objects and other configurations may be managed centrally. This aligns with the Fortinet FortiGate documentation on Security Fabric and central management of address objects.

QUESTION 7

Refer to the exhibit, which shows an error in system fortiguard configuration.



What is the reason you cannot set the protocol to udp in config system fortiguard?

A. FortiManager provides FortiGuard.

B. fortiguard-anycast is set to enable.

C. You do not have the corresponding write access.

D. udp is not a protocol option.

Correct Answer: D

The reason for the command failure when trying to set the protocol to UDP in theconfig system fortiguardis likely that UDP is not a protocol option in this context. The command syntax might be incorrect or the option to set a protocol for FortiGuard updates might not exist in this manner. So the correct answer is D. udp is not a protocol option.

QUESTION 8

Refer to the exhibit, which contains a partial BGP combination.

```
config router bgp
    set as 65200
    set router-id 172.16.1.254
    config neighbor
        edit 100.64.1.254
            set remote-as 65100
        next
    end
end
```

You want to configure a loopback as the OGP source.

Which two parameters must you set in the BGP configuration? (Choose two)

A. ebgp-enforce-multihop

B. recursive-next-hop

C. ibgp-enfoce-multihop

D. update-source

Correct Answer: AD

To configure a loopback as the BGP source, you need to set the "ebgp- enforce-multihop" and "update-source" parameters in the BGP configuration. The "ebgp- enforce-multihop" allows EBGP connections to neighbor routers that are not directly connected, while "update-source" specifies the IP address that should be used for the BGP session1. References := BGP on loopback, Loopback interface, Technical Tip: Configuring EBGP Multihop Load-Balancing, Technical Tip: BGP routes are not installed in routing table with loopback as update source

QUESTION 9

Exhibit.

```
config vpn ipsec phase1-interface
    edit tunnel
        set type dynamic
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set add-route enable
        set psksecret fortinet
    next
end
```

Refer to the exhibit, which contains a partial VPN configuration. What can you conclude from this configuration1?

A. FortiGate creates separate virtual interfaces for each dial up client.

B. The VPN should use the dynamic routing protocol to exchange routing information Through the tunnels.

C. Dead peer detection s disabled.

D. The routing table shows a single IPSec virtual interface.

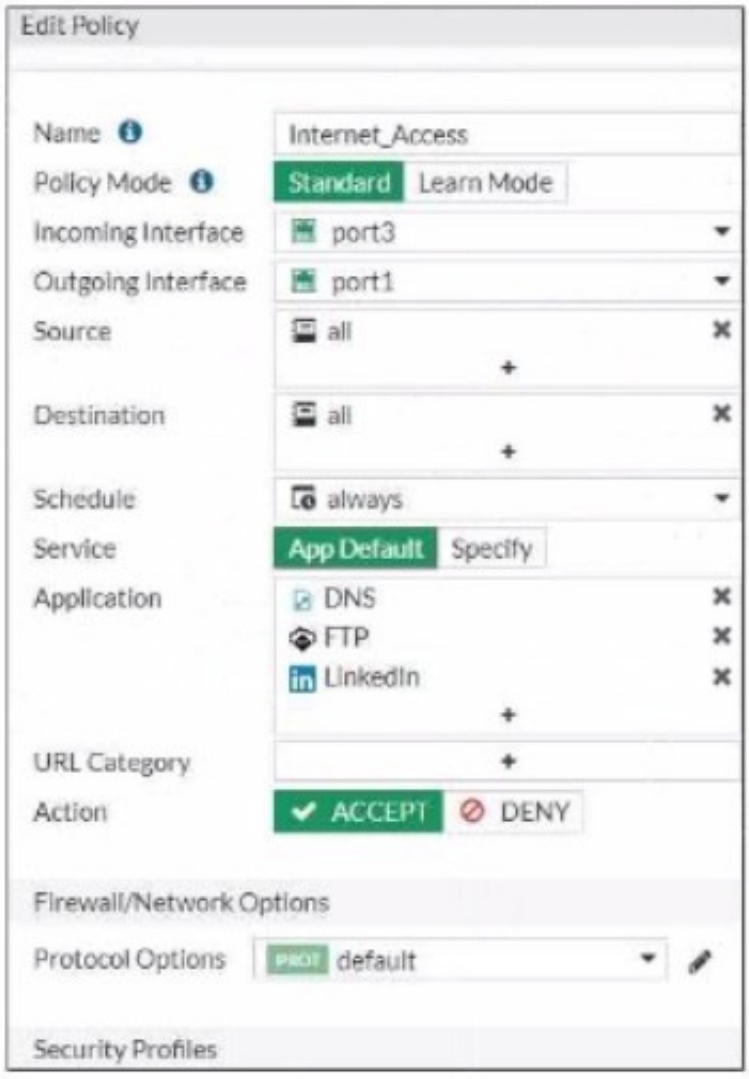
Correct Answer: C

The configuration line "set dpd on-idle" indicates that dead peer detection (DPD) is set to trigger only when the tunnel is idle, not actively disabled1. References: FortiGate IPSec VPN User Guide - Fortinet Document Library

From the given VPN configuration, dead peer detection (DPD) is set to \\'on-idle\\', indicating that DPD is enabled and will be used to detect if the other end of the VPN tunnel is still alive when no traffic is detected. Hence, option C is incorrect. The configuration shows the tunnel set to type \\'dynamic\\', which does not create separate virtual interfaces for each dial- up client (A), and it is not specified that dynamic routing will be used (B). Since this is a phase 1 configuration snippet, the routing table aspect (D) cannot be concluded from this alone.

QUESTION 10

Exhibit.



Refer to the exhibit, which contains a partial policy configuration.

Which setting must you configure to allow SSH?

A. Specify SSH in the Service field

B. Configure pot 22 in the Protocol Options field.

C. Include SSH in the Application field

D. Select an application control profile corresponding to SSH in the Security Profiles section

Correct Answer: A

Option A is correct because to allow SSH, you need to specify SSH in the Service field of the policy configuration. This is because the Service field determines which types of traffic are allowed by the policy1. By default, the Service field is set to App Default, which means that the policy will use the default ports defined by the applications. However, SSH is not one of the default applications, so you need to specify it manually or create a custom service for it2. Option B is incorrect because configuring port 22 in the Protocol Options field is not enough to allow SSH. The Protocol Options field allows you to customize the protocol inspection and anomaly protection settings for the policy3. However, this field does not override the Service field, which still needs to match the traffic type. Option C is incorrect because including

SSH in the Application field is not enough to allow SSH. The Application field allows you to filter the traffic based on the application signatures and categories4. However, this field does not override the Service field, which still needs to match the traffic type. Option D is incorrect because selecting an application control profile corresponding to SSH in the Security Profiles section is not enough to allow SSH. The Security Profiles section allows you to apply various security features to the traffic, such as antivirus, web filtering, IPS, etc. However, this section does not override the Service field, which still needs to match the traffic type. References: =

1: Firewall policies

2: Services

3: Protocol options profiles

4: Application control