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.geekcert.com/nse7_efw-7-2.html

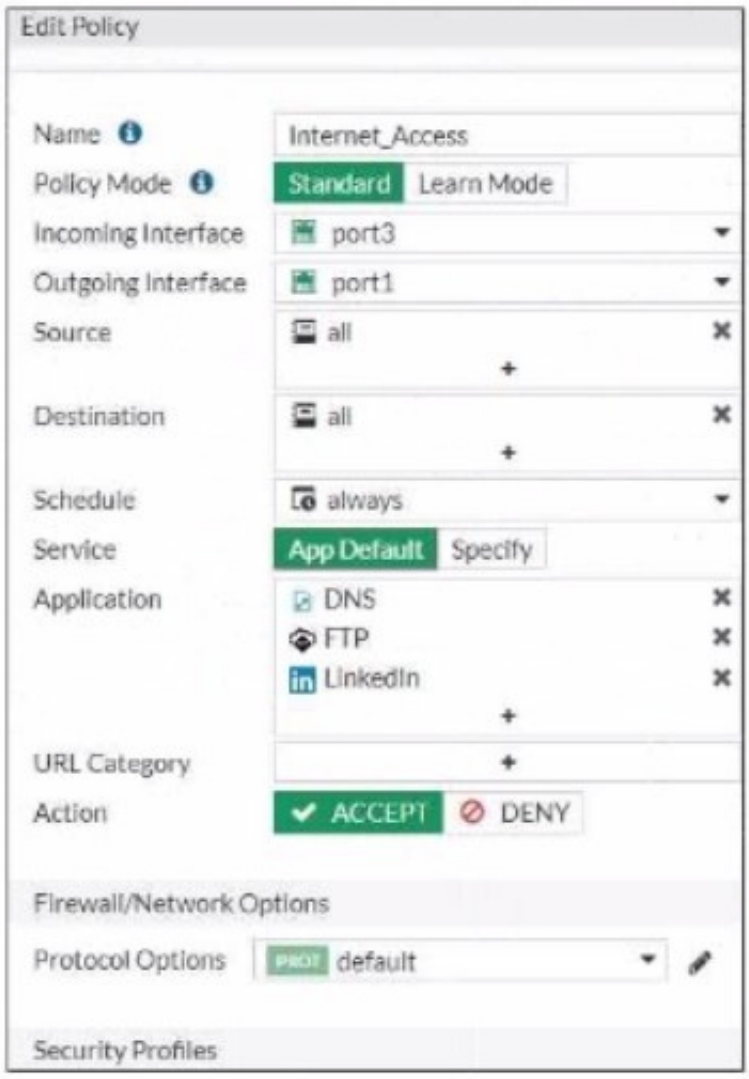
100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

QUESTION 2

Exhibit.

```
config vpn ipsec phase1-interface
    edit "tunnel"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device enable
        set proposal aes128gcm-prfsha256 aes256gcm-prfsha384
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret fortinet
    next
```

Refer to the exhibit, which contains the partial ADVPN configuration of a spoke.

Which two parameters must you configure on the corresponding single hub? (Choose two.)

A. Set auto-discovery-sender enable

B. Set ike-version 2

C. Set auto-discovery-forwarder enable

D. Set auto-discovery-receiver enable

Correct Answer: AC

For an ADVPN spoke configuration shown, the corresponding hub must have auto-discovery-senderenabled to send shortcut advertisement messages to the spokes. Also, the hub would need to haveauto-discovery-forwarderenabled if it is to forward on those shortcut advertisements to other spokes. This allows the hub to inform all spokes about the best path to reach each other. Theike-versiondoes not need to be reconfigured on the hub if it\\'s already set to version 2 andautodiscovery-receiveris not necessary on the hub because it\\'s the one sending the advertisements, not receiving. References: FortiOS Handbook - ADVPN

QUESTION 3

Which, three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. OSPF interface network types match

B. OSPF router IDs are unique

C. OSPF interface priority settings are unique

D. OSPF link costs match

E. Authentication settings match

Correct Answer: ABE

Option A is correct because the OSPF interface network types determine how the routers form adjacencies and exchange LSAs on a network segment. The network types must match for the routers to become neighbors1. Option B is correct because the OSPF router IDs are used to identify each router in the OSPF domain and to establish adjacencies. The router IDs must be unique for the routers to become neighbors2. Option E is correct because the authentication settings control how the routers authenticate each other before exchanging OSPF packets. The authentication settings must match for the routers to become neighbors3. Option C is incorrect because the OSPF interface priority settings are used to elect the designated router (DR) and the backup designated router (BDR) on a broadcast or non-broadcast multi-access network. The priority settings do not have to be unique for the routers to become neighbors, but they affect the DR/BDR election process4. Option D is incorrect because the OSPF link costs are used to calculate the shortest path to a destination network based on the bandwidth of the links. The link costs do not have to match for the routers to become neighbors, but they affect the routing decisions5. References: =

1: OSPF network types

2: OSPF router ID

3: OSPF authentication

4: OSPF interface priority

5: OSPF link cost

QUESTION 4

Refer to the exhibit.

```
config system global
    set admin-https-pki-required disable
    set av-failopen pass
    set check-protocol-header loose
    set memory-use-threshold-extreme 95
    set strict-dirty-session-check enable
    ...
end
```

which contains a partial configuration of the global system. What can you conclude from this output?

A. NPs and CPs are enabled

B. Only CPs arc disabled

C. Only NPs are disabled

D. NPs and CPs arc disabled

Correct Answer: D

The configuration output shows various global settings for a FortiGate device. The terms NP (Network Processor) and CP (Content Processor) relate to FortiGate\\'s hardware acceleration features. However, the provided configuration output does not directly mention the status (enabled or disabled) of NPs and CPs. Typically, the command to disable or enable hardware acceleration features would specifically mention NP or CP in the command syntax. Therefore, based on the output provided, we cannot conclusively determine the status of NPs and CPs, hence option D is the closest answer since the output does not confirm that they are enabled. References: FortiOS Handbook - CLI Reference for FortiOS 5.2

QUESTION 5

Which FortiGate in a Security I auric sends togs to FortiAnalyzer?

A. Only the root FortiGate.

B. Each FortiGate in the Security fabric.

C. The FortiGate devices performing network address translation (NAT) or unified threat management (UTM). if configured.

D. Only the last FortiGate that handled a session in the Security Fabric

Correct Answer: B

Option B is correct because each FortiGate in the Security Fabric can send logs to FortiAnalyzer for centralized logging and analysis12. This allows you to monitor and manage the entire Security Fabric from a single console and view

aggregated reports and dashboards.

Option A is incorrect because the root FortiGate is not the only device that can send logs to FortiAnalyzer. The root FortiGate is the device that initiates the Security Fabric and acts as the central point of contact for other FortiGate devices3.

However, it does not have to be the only log source for FortiAnalyzer. Option C is incorrect because the FortiGate devices performing NAT or UTM are not the only devices that can send logs to FortiAnalyzer. These devices can perform

additional security functions on the traffic that passes through them, such as firewall, antivirus, web filtering, etc4. However, they are not the only devices that generate logs in the Security Fabric.

Option D is incorrect because the last FortiGate that handled a session in the Security Fabric is not the only device that can send logs to FortiAnalyzer. The last FortiGate is the device that terminates the session and applies the final security

policy5. However, it does not have to be the only device that reports the session information to FortiAnalyzer. References: =

1: Security Fabric - Fortinet Documentation1

2: FortiAnalyzer Demo6

3: Security Fabric topology

4: Security Fabric UTM features

5: Security Fabric session handling