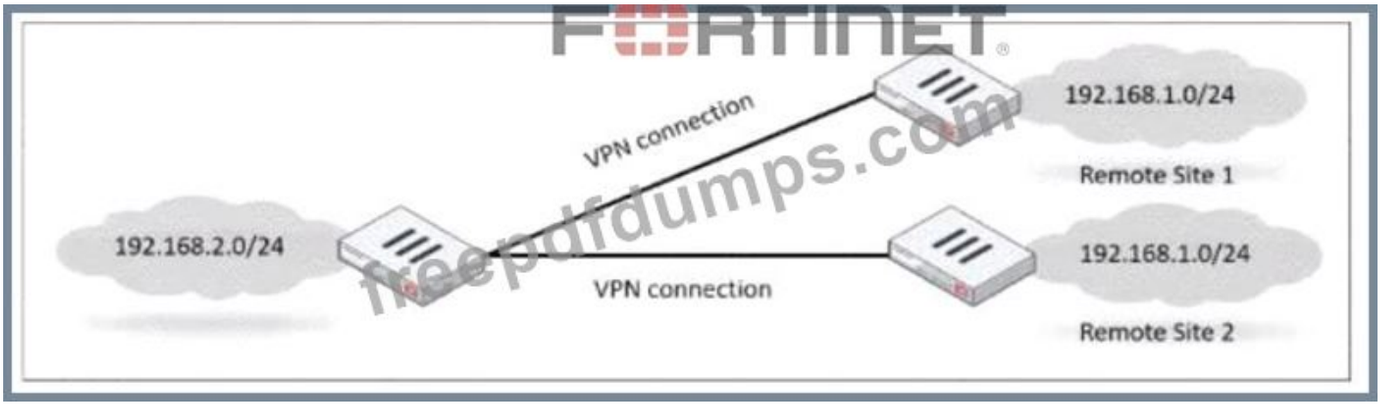
Fortinet.NSE7_EFW-7.2.v2024-05-23.q31

Exam Code:	NSE7_EFW-7.2
Exam Name:	Fortinet NSE 7 - Enterprise Firewall 7.2
Certification Provider:	Fortinet
Free Question Number:	31
Version:	v2024-05-23
# of views:	1398
# of Questions views:	310
https://www.freepdfdumps.com/Fortinet.NSE7_EFW-7.2.v2024-05-23.q31.html	

NEW QUESTION: 1
Which two statements about metadata variables are true? (Choose two.)
A. You create them on FortiGate
B. They apply only to non-firewall objects.
C. The metadata format is $<metadata_variabie_name>.
D. They can be used as variables in scripts
Answer: (SHOW ANSWER)
Metadata variables are custom fields that you can create on FortiManager to store additional information about objects or devices. They can be used as variables in Jinja2 CLI templates or scripts to apply configurations to multiple devices or objects. They do not apply only to non-firewall objects, but also to firewall objects such as addresses, services, policies, etc. The metadata format is not $<metadata_variable_name>, but @<metadata_variable_name>@.
Reference := Using meta field variables, Metadata Variables are supported in Firewall Objects configuration, Technical Tip: New Meta Variables and their usage including Jinja Templates, Technical Tip: Firewall objects use as metadata variable

NEW QUESTION: 2
Refer to the exhibit, which shows a network diagram.



Which IPsec phase 2 configuration should you impalement so that only one remote site is connected at any time?

A. Set route-overlap to allow.

B. Set single-source to enable

C. Set route-overlap to either use-new or use-old

D. Set net-device to enable

Answer: (SHOW ANSWER)

To ensure that only one remote site is connected at any given time in an IPsec VPN scenario, you should use route-overlapwith the option to either use-new or use-old. This setting dictates which routes are preferred and how overlaps in routes are handled, allowing for one connection to take precedence over the other (C).

References:

* FortiOS Handbook - IPsec VPN

NEW QUESTION: 3

You created a VPN community using VPN Manager on FortiManager. You also added gateways to the VPN community. Now you are trying to create firewall policies to permit traffic over the tunnel however, the VPN interfaces do not appear as available options.

A. Create interface mappings for the IPsec VPN interfaces before you use them in a policy.

B. Refresh the device status using the Device Manager so that FortiGate populates the IPSec interfaces

C. Configure the phase 1 settings in the VPN community that you didnt initially configure. FortiGate automatically generates the interfaces after you configure the required settings

D. install the VPN community and gateway configuration on the fortiGate devices so that the VPN interfaces appear on the Policy Objects on fortiManager.

Answer: (SHOW ANSWER)

To use the VPN interfaces in a policy, you need to install the VPN community and gateway configuration on the FortiGate devices first. This will create the VPN interfaces on the FortiGate and sync them with FortiManager. Reference:

Creating IPsec VPN communities

VPN | FortiGate / FortiOS 7.2.0

NEW QUESTION: 4

You want to block access to the website ww.eicar.org using a custom IPS signature.

Which custom IPS signature should you configure?

A.

```
F-SBID( --name "eicar"; --protocol udp; --flow from_server; --pattern "eicar"; --context host;)
```

B.

```
F-SBID( --name "detect_eicar"; --protocol udp; --service ssl; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

C.

```
F-SBID( --name "detect_eicar"; --protocol tcp; --service dns; --flow from_server; --pattern "eicar"; --no_case;)
```

D.

```
F-SBID( --name "eicar"; --protocol tcp; --service HTTP; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

Answer: D (LEAVE A REPLY)

Option D is the correct answer because it specifically blocks access to the website "www.eicar.org" using TCP protocol and HTTP service, which are commonly used for web browsing. The other options either use the wrong protocol (UDP), the wrong service (DNS or SSL), or the wrong pattern ("eicar" instead of "www.eicar.org"). Reference := Configuring custom signatures | FortiGate / FortiOS 7.4.0 - Fortinet Document Library, section "Signature to block access to example.com".

NEW QUESTION: 5

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.

Answer: C (LEAVE A REPLY)

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. Reference: FortiGate IPSec VPN User Guide - Fortinet Document Library

NEW QUESTION: 6

You contoured an address object on the tool fortiGate in a Security Fabric. This object is not synchronized with a downstream device. Which two reasons could be the cause? (Choose two)

A. The address object on the tool FortiGate has fabric-object set to disable
B. The root FortiGate has configuration-sync set to enable
C. The downstream TortiGate has fabric-object-unification set to local
D. The downstream FortiGate has configuration-sync set to local
Answer: A,C (LEAVE A REPLY)
Option A is correct because the address object on the tool FortiGate will not be synchronized with the downstream devices if it has fabric-object set to disable. This option controls whether the address object is shared with other FortiGate devices in the Security Fabric or not1.
Option C is correct because the downstream FortiGate will not receive the address object from the tool FortiGate if it has fabric-object-unification set to local. This option controls whether the downstream FortiGate uses the address objects from the root FortiGate or its own local address objects2.
Option B is incorrect because the root FortiGate has configuration-sync set to enable by default, which means that it will synchronize the address objects with the downstream devices unless they are disabled by the fabric-object option3.
Option D is incorrect because the downstream FortiGate has configuration-sync set to local by default, which means that it will receive the address objects from the root FortiGate unless they are overridden by the fabric-object-unification option4. Reference: =
1: Group address objects synchronized from FortiManager5
2: Security Fabric address object unification6
3: Configuration synchronization7
4: Configuration synchronization7
5: Security Fabric - Fortinet Documentation

NEW QUESTION: 7
Refer to the exhibit.

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
Answer: A (LEAVE A REPLY)
The configuration does not show any explicit disabling of NPs (Network Processors) or CPs (Content Processors). In Fortinet Enterprise Firewall, unless explicitly disabled, these processors

are enabled by default to handle specific types of traffic efficiently12. Reference := Hardware acceleration | FortiGate / FortiOS 7.2.2 - Fortinet Documentation, NSE 7 Network Security Architect - Fortinet

NEW QUESTION: 8
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
Answer: (SHOW ANSWER)

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.
Reference: =
1: Firewall policies
2: Services
3: Protocol options profiles
4: Application control

NEW QUESTION: 9
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
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 10

Exhibit.

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.com am 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

Answer: B (LEAVE A REPLY)

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.
Reference: =
1: Technical Tip: Verify the webfilter cache content4
2: Hexadecimal to Decimal Converter5
3: FortiGate - Fortinet Community6
4: Web filter | FortiGate / FortiOS 7.2.0 - Fortinet Documentation7

NEW QUESTION: 11
Which configuration can be used to reduce the number of BGP sessions in on IBGP network?
A. Route-reflector-peer enable
B. Route-reflector-client enable
C. Route-reflector enable
D. Route-reflector-server enable
Answer: B (LEAVE A REPLY)
To reduce the number of BGP sessions in an IBGP network, you can use a route reflector, which acts as a focal point for IBGP sessions and readvertises the prefixes to all other peers. To configure a route reflector, you need to enable the route-reflector-client option on the neighbor-group settings of the hub device. This will make the hub device act as a route reflector server and the other devices as route reflector clients. Reference := Route exchange | FortiGate / FortiOS 7.2.0 - Fortinet Documentation

NEW QUESTION: 12
Refer to the exhibit, which shows a routing table.

What two options can you configure in OSPF to block the advertisement of the 10.1.10.0 prefix? (Choose two.)
A. Remove the 16.1.10.C prefix from the OSPF network
B. Configure a distribute-list-out
C. Configure a route-map out
D. Disable Redistribute Connected
Answer: B,C (LEAVE A REPLY)
To block the advertisement of the 10.1.10.0 prefix in OSPF, you can configure a distribute-list-out or a route-map out. A distribute-list-out is used to filter outgoing routing updates from being advertised to OSPF neighbors1. A route-map out can also be used for filtering and is applied to

outbound routing updates2. References := Technical Tip: Inbound route filtering in OSPF usi ... - Fortinet Community, OSPF | FortiGate / FortiOS 7.2.2 - Fortinet Documentation

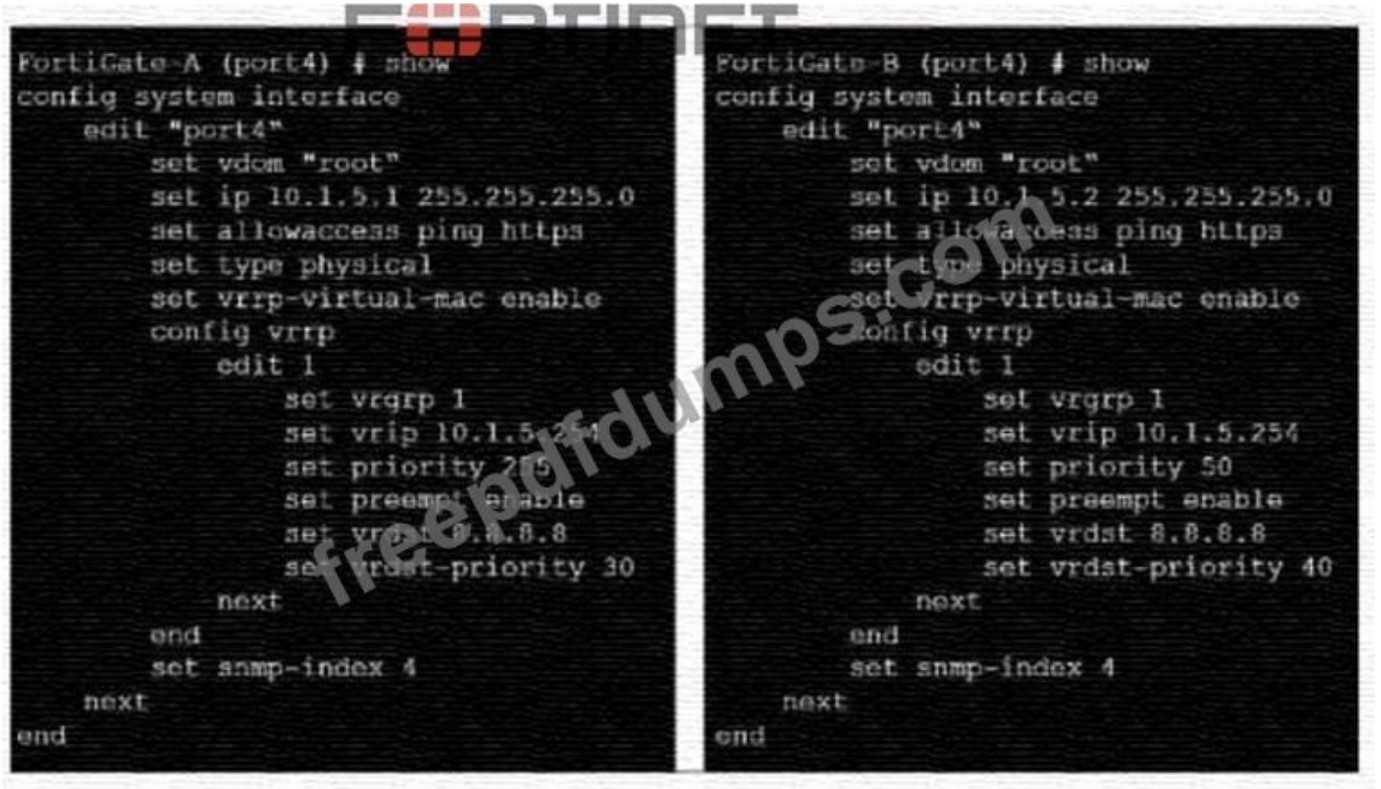
NEW QUESTION: 13
You want to configure faster failure detection for BGP
Which parameter should you enable on both connected FortiGate devices?
A. Ebgp-enforce-multihop
B. bfd
C. Distribute-list-in
D. Graceful-restart
Answer: (SHOW ANSWER)
BFD (Bidirectional Forwarding Detection) is a protocol that provides fast failure detection for BGP by sending periodic messages to verify the connectivity between two peers1. BFD can be enabled on both connected FortiGate devices by using the command set bfd enable under the BGP configuration2. Reference: = Technical Tip : FortiGate BFD implementation and examples ..., Configure BGP | FortiGate / FortiOS 7.0.2 - Fortinet Documentation

NEW QUESTION: 14
Exhibit.

Refer to the exhibit, which contains a CLI script configuration on fortiManager. An administrator configured the CLI script on FortiManager rut the script tailed to apply any changes to the managed device after being executed.
What are two reasons why the script did not make any changes to the managed device? (Choose two)
A. The commands that start with the # sign did not run.

B. Incomplete commands can cause CLI scripts to fail.
C. Static routes can be added using only TCI scripts.
D. CLI scripts must start with #!.
Answer: A,B (LEAVE A REPLY)
The commands that start with the # sign did not run because they are treated as comments in the CLI script.
Incomplete commands can cause CLI scripts to fail because they are not recognized by the FortiGate device.
The other options are incorrect because static routes can be added using CLI or GUI, and CLI scripts do not need to start with #!. References := Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section "CLI script syntax".

NEW QUESTION: 15
Exhibit.



Refer to the exhibit, which contains the partial interface configuration of two FortiGate devices. Which two conclusions can you draw from this con figuration? (Choose two)
A. 10.1.5.254 is the default gateway of the internal network
B. On failover new primary device uses the same MAC address as the old primary
C. The VRRP domain uses the physical MAC address of the primary FortiGate
D. By default FortiGate B is the primary virtual router
Answer: A,B (LEAVE A REPLY)
The Virtual Router Redundancy Protocol (VRRP) configuration in the exhibit indicates that 10.1.5.254 is set as the virtual IP (VRIP), commonly serving as the default gateway for the internal network (A). With vrrp-virtual-macenabled, both FortiGates would use the same virtual

MAC address, ensuring a seamless transition during failover (B). The VRRP domain does not use the physical MAC address (C), and the priority settings indicate that FortiGate-A would be the primary router by default due to its higher priority (D).

NEW QUESTION: 16
Which configuration can be used to reduce the number of BGP sessions in on IBGP network?
A. Route-reflector-peer enable
B. Route-reflector-client enable
C. Route-reflector enable
D. Route-reflector-server enable
Answer: (SHOW ANSWER)
To reduce the number of BGP sessions in an IBGP network, you can use a route reflector, which acts as a focal point for IBGP sessions and readvertises the prefixes to all other peers. To configure a route reflector, you need to enable the route-reflector-client option on the neighbor-group settings of the hub device. This will make the hub device act as a route reflector server and the other devices as route reflector clients. References := Route exchange | FortiGate / FortiOS 7.2.0 - Fortinet Documentation

NEW QUESTION: 17
Which two statements about ADVPN are true? (Choose two.)
A. You must disable add-route in the hub.
B. AllFortiGate devices must be in the same autonomous system (AS).
C. The hub adds routes based on IKE negotiations.
D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0.
Answer: C,D (LEAVE A REPLY)
C). The hub adds routes based on IKE negotiations: This is part of the ADVPN functionality where the hub learns about the networks behind the spokes and can add routes dynamically based on the IKE negotiations with the spokes.
D). You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0: This wildcard setting in the phase 2 selectors allows any-to-any tunnel establishment, which is necessary for the dynamic creation of spoke-to-spoke tunnels.

These configurations are outlined in Fortinet's documentation for setting up ADVPN, where the hub's role in route control and the use of wildcard selectors for phase 2 are emphasized to enable dynamic tunneling between spokes.

NEW QUESTION: 18

Exhibit.

Refer to the exhibit, which shows information about an OSPF interlace

What two conclusions can you draw from this command output? (Choose two.)

A. The port3 network has more man one OSPF router

B. The OSPF routers are in the area ID of 0.0.0.1.

C. The interfaces of the OSPF routers match the MTU value that is configured as 1500.

D. NGFW-1 is the designated router

Answer: A,C (LEAVE A REPLY)

From the OSPF interface command output, we can conclude that the port3 network has more than one OSPF router because the Neighbor Count is 2, indicating the presence of another OSPF router besides NGFW-1.

Additionally, we can deduce that the interfaces of the OSPF routers match the MTU value configured as 1500, which is necessary for OSPF neighbors to form adjacencies. The MTU mismatch would prevent OSPF from forming a neighbor relationship.

References:

* Fortinet FortiOS Handbook: OSPF Configuration

NEW QUESTION: 19

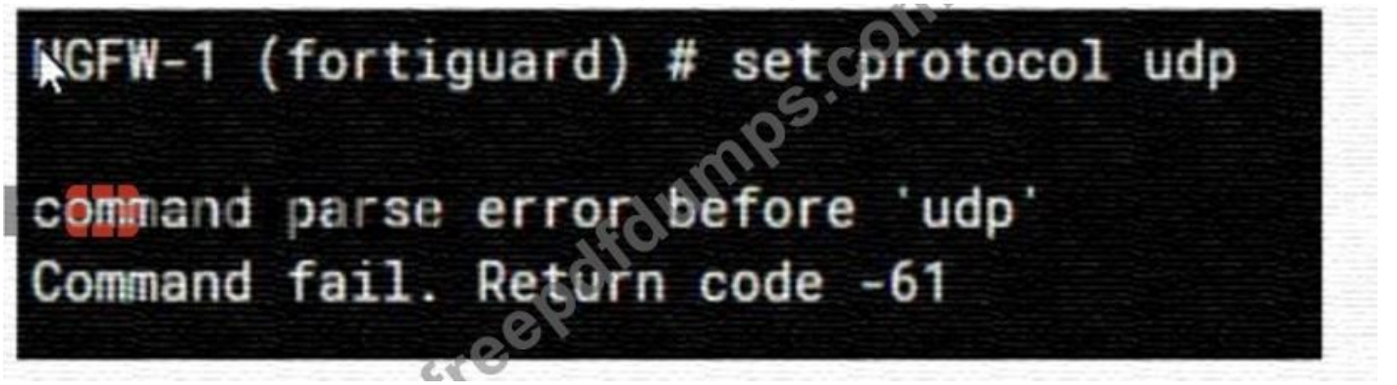
You created a VPN community using VPN Manager on FortiManager. You also added gateways to the VPN community. Now you are trying to create firewall policies to permit traffic over the tunnel however, the VPN interfaces do not appear as available options.

A. Create interface mappings for the IPsec VPN interfaces before you use them in a policy.

B. Refresh the device status using the Device Manager so that FortiGate populates the IPSec interfaces
C. Configure the phase 1 settings in the VPN community that you didnt initially configure. FortiGate automatically generates the interfaces after you configure the required settings
D. install the VPN community and gateway configuration on the fortiGate devices so that the VPN interfaces appear on the Policy Objects on fortiManager.
Answer: (SHOW ANSWER)
To use the VPN interfaces in a policy, you need to install the VPN community and gateway configuration on the FortiGate devices first. This will create the VPN interfaces on the FortiGate and sync them with FortiManager. References:
* Creating IPsec VPN communities
* VPN | FortiGate / FortiOS 7.2.0

NEW QUESTION: 20
You want to configure faster failure detection for BGP.
Which parameter should you enable on both connected FortiGate devices?
A. Ebgp-enforce-multihop
B. bfd
C. Distribute-list-in
D. Graceful-restart
Answer: B (LEAVE A REPLY)
BFD (Bidirectional Forwarding Detection) is a protocol that provides fast failure detection for BGP by sending periodic messages to verify the connectivity between two peers1. BFD can be enabled on both connected FortiGate devices by using the command set bfd enable under the BGP configuration2. References:
= Technical Tip : FortiGate BFD implementation and examples ..., Configure BGP | FortiGate / FortiOS 7.0.2
- Fortinet Documentation

NEW QUESTION: 21
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.
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 22
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
Answer: B (LEAVE A REPLY)
* 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

NEW QUESTION: 23

An administrator has configured two fortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device What can the administrator do to fix this problem?

A. Verity Mai the speed and duplex settings match between me FortiGate interfaces and the connected switch ports

B. Configure set link -failed signal enable under-config system ha on both Cluster members

C. Configure remote link monitoring to detect an issue in the forwarding path

D. Configure set send-garp-on-failover enables under config system ha on both cluster members

Answer: (SHOW ANSWER)

Virtual MAC Address and Failover

- The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port.

- Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces):

#Config system ha

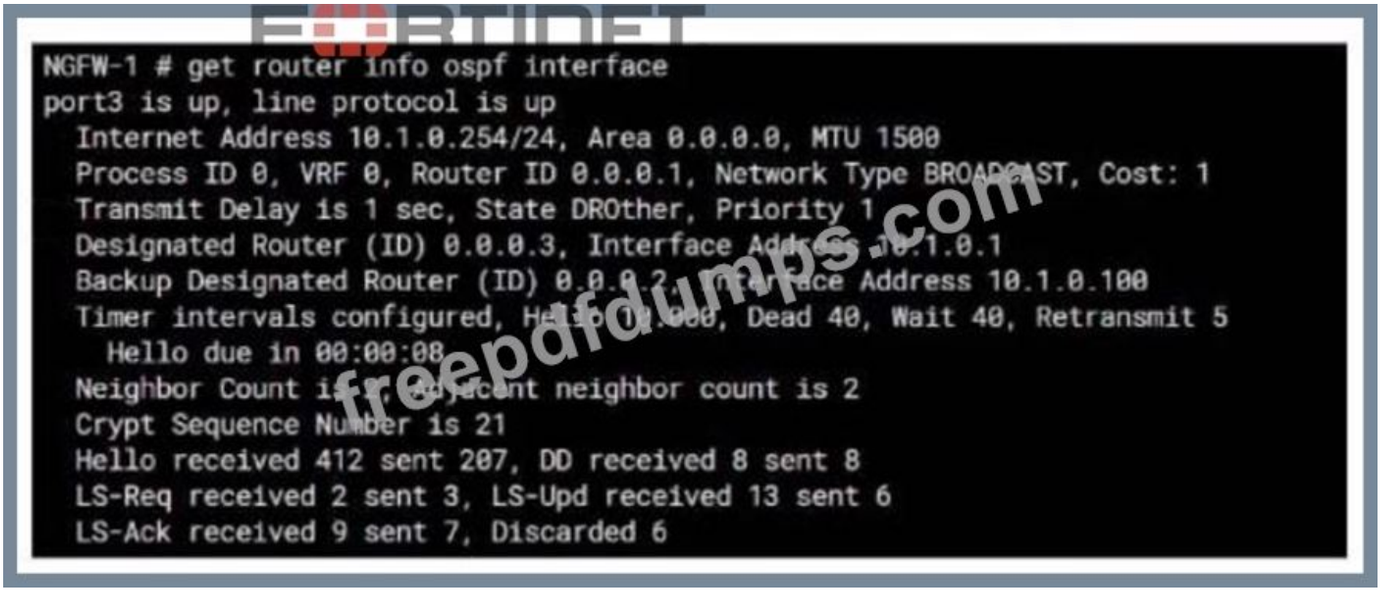
set link-failed-signal enable

end

- This simulates a link failure that clears the related entries from MAC table of the switches.

NEW QUESTION: 24

Exhibit.



Refer to the exhibit, which shows information about an OSPF interlace

What two conclusions can you draw from this command output? (Choose two.)

A. The port3 network has more man one OSPF router

B. NGFW-1 is the designated router

C. The interfaces of the OSPF routers match the MTU value that is configured as 1500.

D. The OSPF routers are in the area ID of 0.0.0.1.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 25
Which ADVPN configuration must be configured using a script on fortiManager, when using VPN Manager to manage fortiGate VPN tunnels?
A. Enable AD-VPN in IPsec phase 1
B. Disable add-route on hub
C. Configure IP addresses on IPsec virtual interlaces
D. Set protected network to all
Answer: A (LEAVE A REPLY)
To enable AD-VPN, you need to edit an SD-WAN overlay template and enable the Auto-Discovery VPN toggle. This will automatically add the required settings to the IPsec template and the BGP template. You cannot enable AD-VPN directly in the IPsec phase 1 settings using VPN Manager. References := ADVPN | FortiManager 7.2.0 - Fortinet Documentation

NEW QUESTION: 26
Refer to the exhibit, which shows config system central-management information.

```
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set fmg "10.1.0.241"
    config server-list
        edit 1
            set server-type update
            set server-address 10.1.0.241
        next
    end
    set include-default-servers disable
end
```


Which setting must you configure for the web filtering feature to function?
A. Add server. fortiguard. net to the server list.
B. Configure securewf.fortiguard. net on the default servers.
C. Set update-server-location to automatic.
D. Configure server-type with the rating option.
Answer: D (LEAVE A REPLY)
For the web filtering feature to function effectively, the FortiGate device needs to have a server configured for rating services. The rating option in the server-type setting specifies that the server

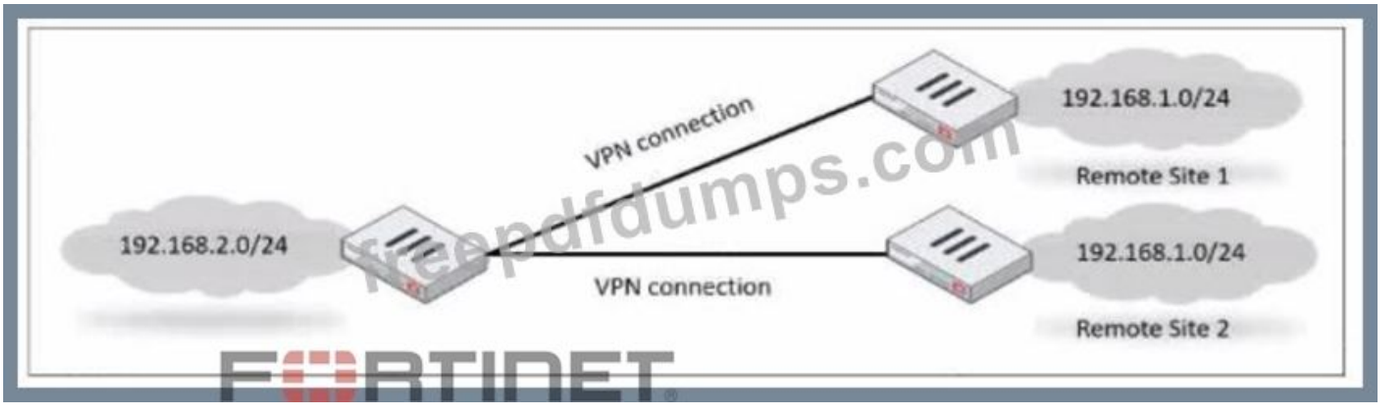
is used for URL rating lookup, which is essential for web filtering. The displayed configuration does not list any FortiGuard web filtering servers, which would be necessary for web filtering. The setting set include-default-servers disable indicates that the default FortiGuard servers are not being used, and hence, a specific server for web filtering (like securewf.fortiguard.net) needs to be configured.

NEW QUESTION: 27
Which statement about network processor (NP) offloading is true?
A. For TCP traffic FortiGate CPU offloads the first packets of SYN/ACK and ACK of the three-way handshake to NP
B. The NP provides IPS signature matching
C. You can disable the NP for each firewall policy using the command np-acceleration st to loose.
D. The NP checks the session key or IPSec SA
Answer: B (LEAVE A REPLY)
Network processors (NPs) are specialized hardware within FortiGate devices that accelerate certain security functions. One of the primary functions of NPs is to provide IPS signature matching (B), allowing for high-speed inspection of traffic against a database of known threat signatures.

NEW QUESTION: 28
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
Answer: A,B,E (LEAVE A REPLY)
* 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.

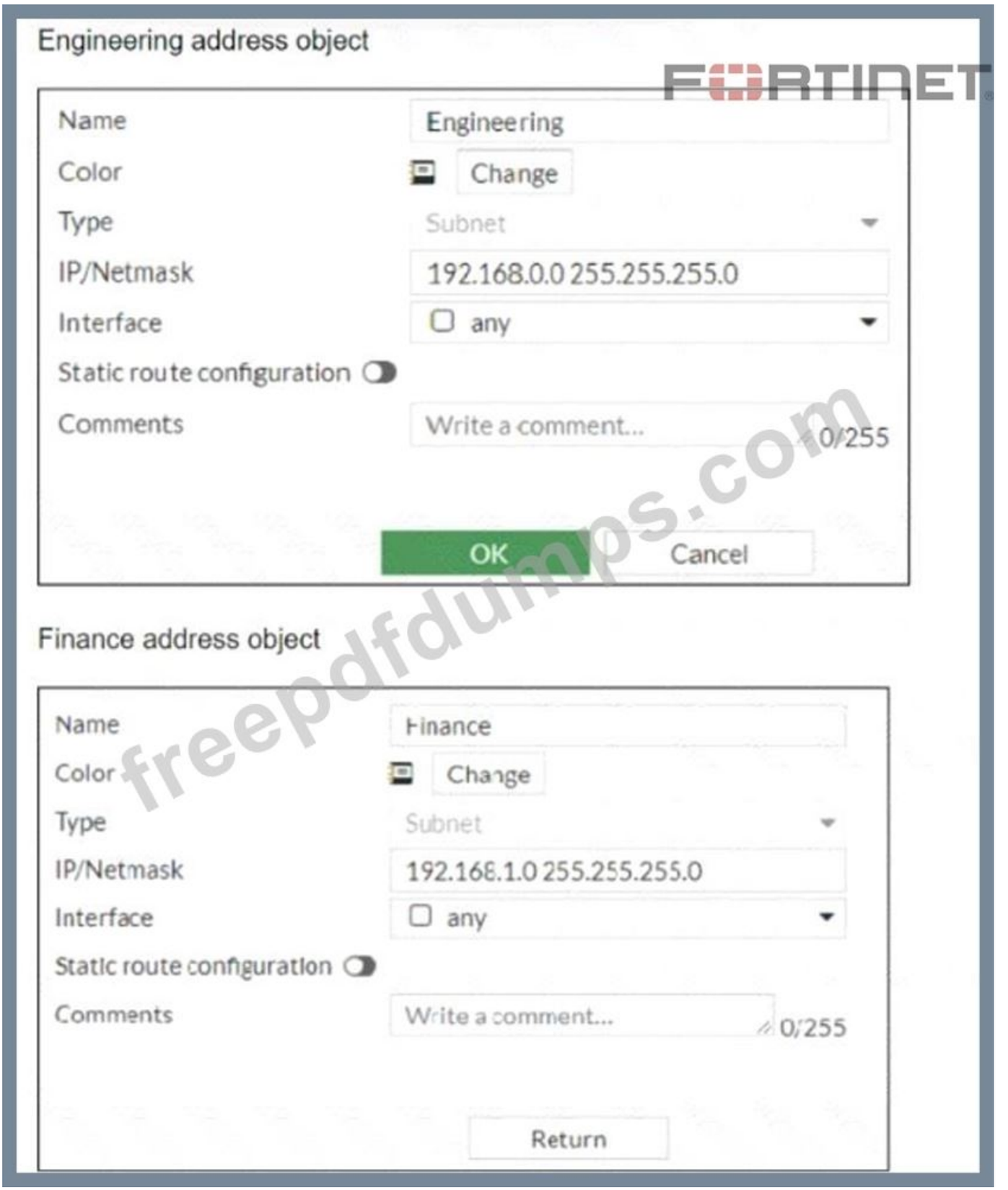
* Option D is incorrect because the OSPF link costs are used to calculate the shortest path to a destination network based on the bandwidth of the links. The link costs do not have to match for the routers to become neighbors, but they affect the routing decisions5. References: =
* 1: OSPF network types
* 2: OSPF router ID
* 3: OSPF authentication
* 4: OSPF interface priority
* 5: OSPF link cost

NEW QUESTION: 29
Refer to the exhibit, which shows a network diagram.



Which IPsec phase 2 configuration should you impalement so that only one remote site is connected at any time?
A. Set route-overlap to allow.
B. Set single-source to enable
C. Set route-overlap to either use-new or use-old
D. Set net-device to enable
Answer: B (LEAVE A REPLY)
The "single-source" option ensures that only one remote site is connected at any time, which aligns with the requirement in the question. This option prevents multiple VPN tunnels from being established between the same source and destination networks, and allows only the most recent tunnel to be active. This can be useful for scenarios where multiple remote sites have the same IP address range, as shown in the exhibit. Reference := Fortinet Enterprise Firewall Study Guide for FortiOS 7.2, page 142.

NEW QUESTION: 30
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.

Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 31
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
Answer: B (LEAVE A REPLY)
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. Reference: =
1: Security Fabric - Fortinet Documentation1
2: FortiAnalyzer Demo6
3: Security Fabric topology
4: Security Fabric UTM features
5: Security Fabric session handling

been corrected get the **newest** Actual4test.com NSE7_EFW-7.2 dumps with Test Engine here: https://www.actual4test.com/NSE7_EFW-7.2_examcollection.html (**82** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

Valid NSE7_EFW-7.2 Dumps shared by Actual4test.com for Helping Passing NSE7_EFW-7.2 Exam! Actual4test.com now offer the **newest NSE7_EFW-7.2 exam dumps**, the Actual4test.com NSE7_EFW-7.2 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NSE7_EFW-7.2 dumps with Test Engine here: https://www.actual4test.com/NSE7_EFW-7.2_examcollection.html (**82** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)