Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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.

Answer: ABD

Explanation:
When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:
• Incoming Interface
• Outgoing Interface
• Source: IP address, user, internet services
• Destination: IP address or internet services
• Service: IP protocol and port number
• Schedule: Applies during configured times

NEW QUESTION 2
Which two statements are correct about SLA targets? (Choose two.)

A. You can configure only two SLA targets per one Performance SLA.
B. SLA targets are optional.
C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
D. SLA targets are used only when referenced by an SD-WAN rule.

Answer: BD

NEW QUESTION 3
Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Antivirus engine
B. Intrusion prevention system engine
C. Flow engine
D. Detection engine

Answer: B

Explanation:
http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control

NEW QUESTION 4
In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.
B. The Incoming Interfac
C. Outgoing Interfac
D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
F. The IP version of the sources and destinations in a policy must match.
G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 5
Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
B. The RPF check is run on the first sent and reply packet of any new session.
C. The RPF check is run on the first sent packet of any new session.
D. The RPF check is run on the first reply packet of any new session.

Answer: AC

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn’t perform any additional RPF checks on that session."
* A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks1
* C. The RPF check is run on the first sent packet of any new session.
This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the

session initiation. This reduces the processing overhead and improves performance2

NEW QUESTION 6
Refer to the exhibit.

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. The signature setting uses a custom rating threshold.
B. The signature setting includes a group of other signatures.
C. Traffic matching the signature will be allowed and logged.
D. Traffic matching the signature will be silently dropped and logged.

Answer: D

Explanation:
Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be 'Pass' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be 'Default'.
Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 7
An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.12" 5
```

Which three pieces of Information will be Included in me sniffer output? {Choose three.)

A. Interface name
B. Packet payload
C. Ethernet header
D. IP header
E. Application header

Answer: ABD

NEW QUESTION 8
If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

A. The Services field prevents SNAT and DNAT from being combined in the same policy.
B. The Services field is used when you need to bundle several VIPs into VIP groups.
C. The Services field removes the requirement to create multiple VIPs for different services.
D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

Answer: C

NEW QUESTION 9
If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source filed of a firewall policy?

A. IP address
B. Once Internet Service is selected, no other object can be added
C. User or User Group
D. FQDN address

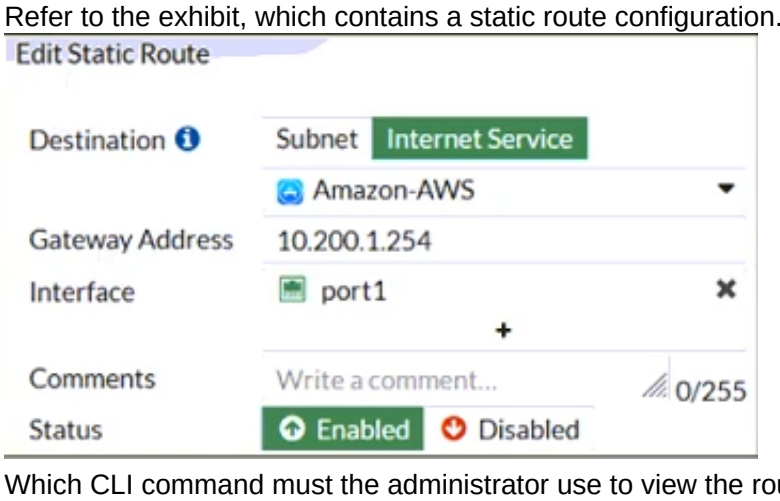
Answer: B

NEW QUESTION 10
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

A. diagnose sys top
B. execute ping
C. execute traceroute
D. diagnose sniffer packet any
E. get system arp

Answer: BCD

NEW QUESTION 10
Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.



Which CLI command must the administrator use to view the route?

A. get router info routing-table database
B. diagnose firewall route list
C. get internet-service route list
D. get router info routing-table all

Answer: B

Explanation:
ISDB static route will not create entry directly in routing-table. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1
and here
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640
FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

NEW QUESTION 13
Refer to the exhibits.

Exhibit A Exhibit B

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Exhibit A Exhibit B

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

A. Administrators can access FortiGate only through the console port.
B. FortiGate has entered conserve mode.
C. FortiGate will start sending all files to FortiSandbox for inspection.
D. Administrators cannot change the configuration.

Answer: BD

NEW QUESTION 16
The IPS engine is used by which three security features? (Choose three.)

A. Antivirus in flow-based inspection
B. Web filter in flow-based inspection
C. Application control

D. DNS filter
E. Web application firewall

Answer: ABC

Explanation:
FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

NEW QUESTION 18
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

Answer: AC

NEW QUESTION 22
Refer to the exhibits.
The exhibits show a network diagram and firewall configurations.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver.
Remote-User2 must not be able to access the Webserver.

Exhibit A Exhibit B

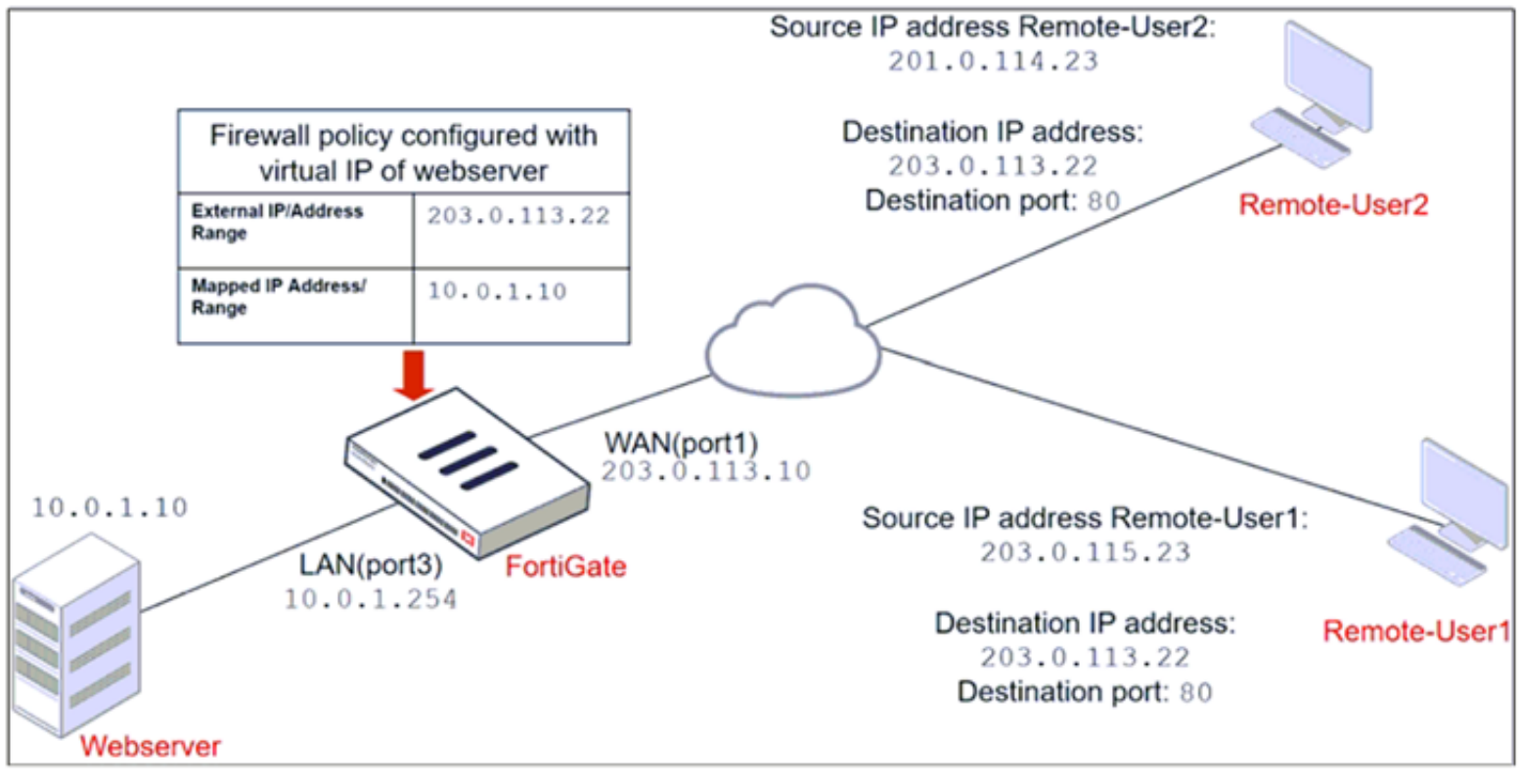
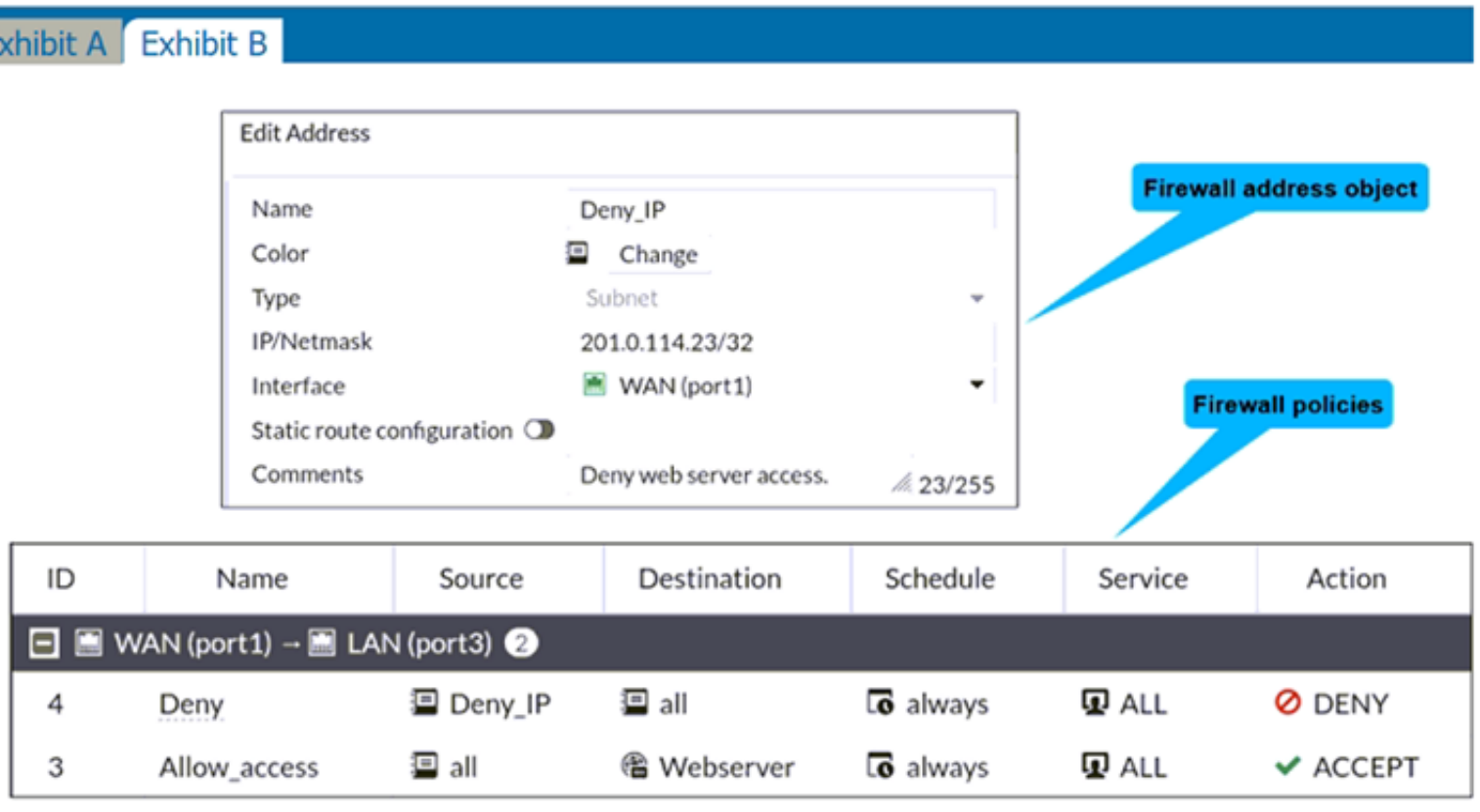


Exhibit A Exhibit B



In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.
B. Set the Destination address as Deny_IP in the Allow-access policy.

C. Enable match vip in the Deny policy.
D. Set the Destination address as Web_server in the Deny policy.

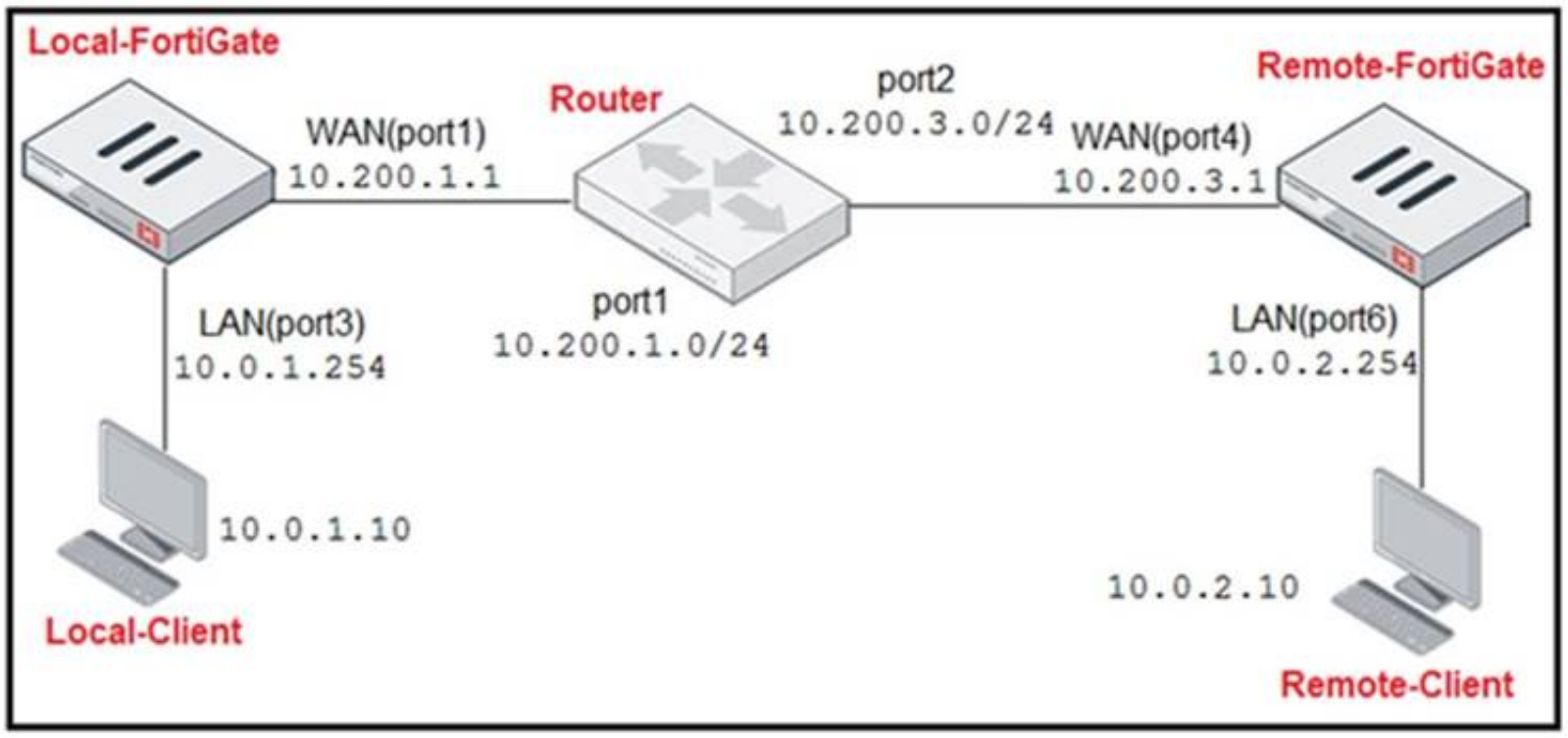
Answer: BC

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta The exhibits show a network diagram and firewall configurations for a FortiGate unit that has two policies:
Allow_access and Deny. The Allow_access policy allows traffic from the WAN (port1) interface to the LAN (port3) interface with the destination address of VIP and the service of HTTPS. The VIP object maps the external IP address 10.200.1.10 and port 10443 to the internal IP address 10.0.1.10 and port 443 of the Webserver. The Deny policy denies traffic from the WAN (port1) interface to the LAN (port3) interface with the source address of Deny_IP and the destination address of All.
In this scenario, the administrator wants to deny Webserver access for Remote-User2, who has the IP address 10.200.3.2 , which is included in the Deny_IP address object. Remote-User1, who has the IP address 10.200.3.1, must be able to access the Webserver.
To achieve this goal, the administrator can make two changes to deny Webserver access for Remote-User2:

- Set the Destination address as Webserver in the Deny policy. This will make the Deny policy more specific and match only the traffic that is destined for the Webserver's internal IP address, instead of any destination address.
- Enable match-vip in the Deny policy. This will make the Deny policy apply to traffic that matches a VIP object, instead of ignoring it1. This way, the Deny policy will block Remote-User2's traffic that uses the VIP object's external IP address and port.

NEW QUESTION 27
Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

+ Create New | Edit | Delete | Search

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

+ Create New | Edit | Clone | Delete | Search

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200. 1. 1/24.
The LAN (port3) interface has the IP address 10.0. 1.254/24.
A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.
Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0. 1. 10) pings the IP address of Remote-FortiGate (10.200.3. 1)?

A. 10.200. 1. 149
B. 10.200. 1. 1
C. 10.200. 1.49
D. 10.200. 1.99

Answer: D

NEW QUESTION 30
Refer to the exhibits.
Exhibit A shows the application sensor configuration. Exhibit B shows the Excessive-Bandwidth and Apple filter details.

Exhibit A | Exhibit B

Edit Application Sensor

Categories

All Categories

Business (179, 6)	Cloud.IT (31)
Collaboration (293, 6)	Email (87, 12)
Game (124)	General.Interest (241, 9)
Mobile (3)	Network.Service (332)
P2P (85)	Proxy (106)
Remote.Access (91)	Social.Media (150, 31)
Storage.Backup (296, 16)	Update (48)
Video/Audio (206, 13)	VoIP (31)
Web.Client (18)	Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	Block
2	VEND Apple	Filter	Monitor

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

A. Apple FaceTime will be allowed, based on the Categories configuration.
B. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.
C. Apple FaceTime will be allowed, based on the Apple filter configuration.
D. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.310): "Then, FortiGate scans packets for matches, in this order, for the application control profile: 1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies. 2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories."

NEW QUESTION 34
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scanning of application traffic to the DNS protocol only.
B. It limits the scanning of application traffic to use parent signatures only.
C. It limits the scanning of application traffic to the browser-based technology category only.
D. It limits the scanning of application traffic to the application category only.

Answer: C

Explanation:
FortiGate Security 7.2 Study Guide (p.317): "You can configure the URL Category within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website."

NEW QUESTION 35
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 .

Answer: D

NEW QUESTION 38
A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.
What is the reason for the failed virus detection by FortiGate?

A. The website is exempted from SSL inspection.
B. The EICAR test file exceeds the protocol options oversize limit.

C. The selected SSL inspection profile has certificate inspection enabled.
D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: AC

Explanation:
SSL Inspection Profile, on the Inspection method there are 2 options to choose from, SSL Certificate Inspection or Full SSL Inspection. FG SEC 7.2 Studi Guide: Full SSL Inspection level is the only choice that allows antivirus to be effective.

NEW QUESTION 41
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache
B. FortiSIEM
C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Answer: BCE

NEW QUESTION 46
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries
B. PKI
C. Traffic shaping
D. DNS

Answer: AD

NEW QUESTION 48
A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.
What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

A. Static IP Address
B. Dialup User
C. Dynamic DNS
D. Pre-shared Key

Answer: B

Explanation:
Dialup user is used when the remote peer's IP address is unknown. The remote peer whose IP address is unknown acts as the dialup clien and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

NEW QUESTION 52
Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.
B. FGCP is not used when FortiGate is in transparent mode.
C. FGCP runs only over the heartbeat links.
D. FGCP is used to discover FortiGate devices in different HA groups.

Answer: AC

Explanation:
The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:
FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.
FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices. FGCP does not run over other types of links, such as data links.

NEW QUESTION 55
Refer to the exhibits.

Exhibit A | Exhibit B

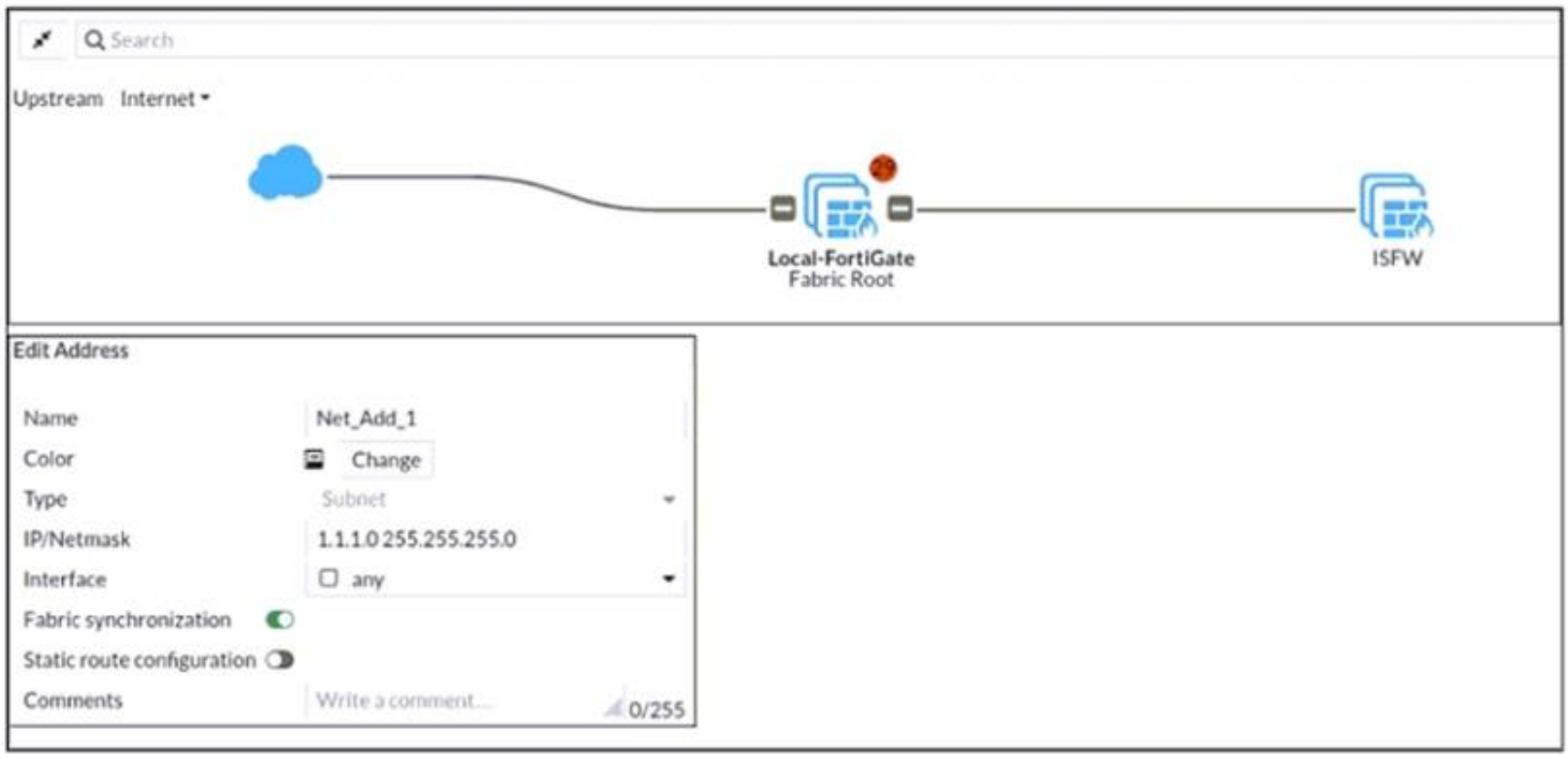


Exhibit A | Exhibit B

```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream ''
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC Y9ynT+64RpCTpVdgSmoQHZ42mYSIzNNzLNvgzMXjyN
9hSjIJE3KYJlo3Xxyg1dvNxPId8T5xctBUszy7rgIcHcA/qHrByXSXfPEeHC6ufkqlPJr
W6GypwDUb5O3VFgPbASFYYteQesmwoJtGe84BLqa+hUcgunLD1z/97sBp+PLt5nrA==
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification default
    set saml-configuration-sync default
```

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream "10.0.1.254"
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync local
end

ISFW #
```

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).
What must the administrator do to synchronize the address object?

A. Change the csf setting on ISFW (downstream) to set configuration-sync local.
B. Change the csf setting on ISFW (downstream) to set authorization-request-type certificate.
C. Change the csf setting on both devices to set downstream-access enable.
D. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

Answer: C

NEW QUESTION 59
Refer to the exhibits.
The exhibits show the firewall policies and the objects used in the firewall policies.
The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Exhibit A | Exhibit B

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 1	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,635		
Facebook-Web	Destination	26,578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80 443 8443	TCP	Enabled
1.9.91.17 - 1.9.91.18	443	UDP	Enabled
1.9.91.30	443	UDP	Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	ACCEPT	Enabled

Exhibit A | Exhibit B

Policy Lookup

Incoming Interface	port3
IP Version	IPv4
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	facebook.com
Destination Port	443

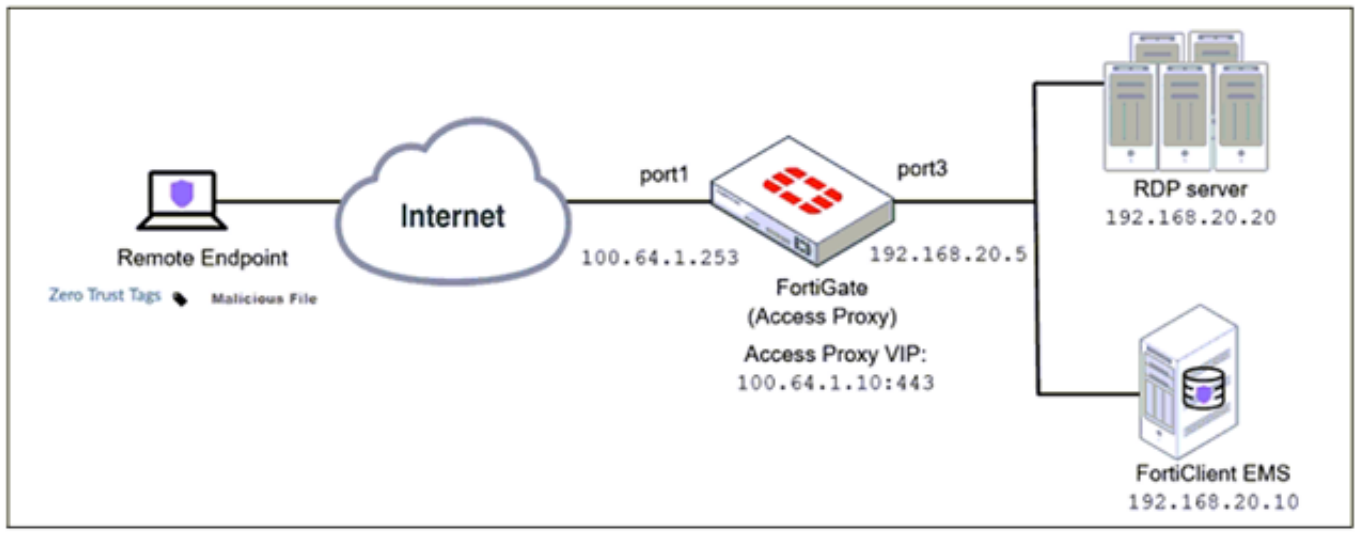
Search | Close

Which policy will be highlighted, based on the input criteria?

A. Policy with ID 4.
B. Policy with ID 5.
C. Policies with ID 2 and 3.
D. Policy with ID 4.

Answer: B

NEW QUESTION 63
Refer to the exhibit.



Based on the ZTNA tag, the security posture of the remote endpoint has changed. What will happen to endpoint active ZTNA sessions?

A. They will be re-evaluated to match the endpoint policy.
B. They will be re-evaluated to match the firewall policy.
C. They will be re-evaluated to match the ZTNA policy.
D. They will be re-evaluated to match the security policy.

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-zt FortiGate Infrastructure 7.2 Study Guide (p.182):
"Endpoint posture changes trigger active ZTNA proxy
sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy."

NEW QUESTION 66
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

A. diagnose wad session list
B. diagnose wad session list | grep hook-pre&&hook-out
C. diagnose wad session list | grep hook=pre&&hook=out
D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 71
View the exhibit.

Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.
B. Dead peer detection must be disabled to support this type of IPsec setup.
C. The TunnelB route is the primary route for reaching the remote sit
D. The TunnelA route is used only if the TunnelB VPN is down.
E. This is a redundant IPsec setup.

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundan

NEW QUESTION 75
An administrator must disable RPF check to investigate an issue.
Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

A. Enable asymmetric routing, so the RPF check will be bypassed.
B. Disable the RPF check at the FortiGate interface level for the source check.
C. Disable the RPF check at the FortiGate interface level for the reply check .
D. Enable asymmetric routing at the interface level.

Answer: B

NEW QUESTION 80
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

Answer: AC

NEW QUESTION 84
Refer to the exhibit.

```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

A. The session is in SYN_SENT state.
B. The session is in FIN_ACK state.
C. The session is in FTN_WAIT state.
D. The session is in ESTABLISHED state.

Answer: A

Explanation:
Indicates TCP (proto=6) session in SYN_SENT state (proto=state=2) https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NEW QUESTION 89
Refer to the exhibits.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook .
Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.
Which part of the policy configuration must you change to resolve the issue?

A. Make SSL inspection needs to be a deep content inspection.
B. Force access to Facebook using the HTTP service.
C. Get the additional application signatures are required to add to the security policy.
D. Add Facebook in the URL category in the security policy.

Answer: A

Explanation:
They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather then adding an app rule.

NEW QUESTION 93
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

Answer: AD

NEW QUESTION 96
In an explicit proxy setup, where is the authentication method and database configured?

A. Proxy Policy
B. Authentication Rule
C. Firewall Policy
D. Authentication scheme

Answer: D

NEW QUESTION 98
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status
B. get system performance status
C. diagnose sys top
D. get system arp

Answer: D

Explanation:
"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

NEW QUESTION 100
Refer to the exhibit.

The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

A. Change password
B. Enable restrict access to trusted hosts
C. Change Administrator profile
D. Enable two-factor authentication

Answer: C

NEW QUESTION 104
Refer to the exhibit.

Name	Type	IP/Netmask	VLAN ID
Physical Interface 14			
port1	Physical Interface	10.200.1.1/255.255.255.0	
port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
port10	Physical Interface	10.0.11.1/255.255.255.0	
port2	Physical Interface	10.200.2.1/255.255.255.0	
port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

A. Traffic between port2 and port2-vlan1 is allowed by default.
B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
C. port1 is a native VLAN.
D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Answer: CD

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

NEW QUESTION 107
If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL
B. A person
C. A subordinate CA
D. A root CA

Answer: D

NEW QUESTION 109
Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

What two conclusions can you make from the debug flow output? (Choose two.)

A. The debug flow is for ICMP traffic.
B. The default route is required to receive a reply.
C. Anew traffic session was created.
D. A firewall policy allowed the connection.

Answer: AC

Explanation:
The debug flow output shows the result of a diagnose command that captures the traffic flow between the source and destination IP addresses1. The debug flow output reveals the following information about the traffic flow1:

- The protocol is 1, which means that the traffic uses ICMP protocol2. ICMP is a protocol that is used to send error messages and test connectivity between devices2.
- The session state is 0, which means that a new traffic session was created3. A session is a data structure that stores information about a connection between two devices3.
- The policy ID is 1, which means that the traffic matched the firewall policy with ID 14. A firewall policy is a rule that defines how FortiGate processes traffic based on the source, destination, service, and action parameters4.
- The action is 0, which means that the traffic was allowed by the firewall policy. An action is a parameter that specifies what FortiGate does with the traffic that matches a firewall policy.

Therefore, two conclusions that can be made from the debug flow output are:

- The debug flow is for ICMP traffic.
- A new traffic session was created.

NEW QUESTION 114
.....

Relate Links

100% Pass Your NSE4_FGT-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/