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
An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution?

A. ZTNA IP/MAC filtering mode
B. ZTNA access proxy
C. SSL VPN
D. L2TP

Answer: B

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.165): "ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs."
This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials. ZTNA access proxy uses a secure tunnel between the user's device and the FortiGate, and authenticates the user based on device identity and context. The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile. This simplifies remote access and enhances security by reducing the attack surface12

NEW QUESTION 2
A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.
What is the reason for the certificate warning errors?

A. The matching firewall policy is set to proxy inspection mode.
B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
C. The full SSL inspection feature does not have a valid license.
D. The browser does not trust the certificate used by FortiGate for SSL inspection.

Answer: D

Explanation:
FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser."

NEW QUESTION 3
Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srci ntfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dumytracker.org/"
sentbyte=517 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

A. Traffic is blocked because Action is set to DENY in the firewall policy.
B. Traffic belongs to the root VDOM.
C. This is a security log.
D. Log severity is set to error on FortiGate.

Answer: AC

NEW QUESTION 4
Refer to the exhibit.

```
STUDENT # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT       DESTINATION      DESTINATION-NAT
tcp     3598   10.0.1.10:2706  10.200.1.6:2706  10.200.1.254:80  -
tcp     3598   10.0.1.10:2704  10.200.1.6:2704  10.200.1.254:80  -
tcp     3596   10.0.1.10:2702  10.200.1.6:2702  10.200.1.254:80  -
tcp     3599   10.0.1.10:2700  10.200.1.6:2700  10.200.1.254:443 -
tcp     3599   10.0.1.10:2698  10.200.1.6:2698  10.200.1.254:80  -
tcp     3598   10.0.1.10:2696  10.200.1.6:2696  10.200.1.254:443 -
udp     174    10.0.1.10:2694  -                  10.0.1.254:53  -
udp     173    10.0.1.10:2690  -                  10.0.1.254:53  -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

A. Destination NAT is disabled in the firewall policy.
B. One-to-one NAT IP pool is used in the firewall policy.
C. Overload NAT IP pool is used in the firewall policy.
D. Port block allocation IP pool is used in the firewall policy.

Answer: B

Explanation:
FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

NEW QUESTION 5
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent must search security event logs.
D. The NetSession Enum function is used to track user logouts.

Answer: D

Explanation:
FortiGate_Infrastructure_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

NEW QUESTION 6
Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
B. The client FortiGate requires a manually added route to remote subnets.
C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
D. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.9/administration-guide/508779/fortigate-as-ssl-vpn-client
To establish an SSL VPN connection between two FortiGate devices, the following two settings are required:
The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate will use a CA (Certificate Authority) certificate to verify the client FortiGate certificate, ensuring that the client device is trusted and allowed to establish an SSL VPN connection.
The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: The client FortiGate must have an SSL VPN tunnel interface type configured in order to establish an SSL VPN connection. This interface type will be used to connect to the server FortiGate over the SSL VPN.

NEW QUESTION 7
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

A. FortiGate uses fewer resources.
B. FortiGate performs a more exhaustive inspection on traffic.
C. FortiGate adds less latency to traffic.
D. FortiGate allocates two sessions per connection.

Answer: AC

NEW QUESTION 8
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

A. Add the support of NTLM authentication.
B. Add user accounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Answer: D

NEW QUESTION 9
Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

A. VDOMs without ports with connected devices are not displayed in the topology.
B. Downstream devices can connect to the upstream device from any of their VDOMs.
C. Security rating reports can be run individually for each configured VDOM.
D. Each VDOM in the environment can be part of a different Security Fabric.

Answer: A

Explanation:
FortiGate Security 7.2 Study Guide (p.436): "When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and,

because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

NEW QUESTION 10
Refer to the exhibits.
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object 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.

Exhibit A | Exhibit B

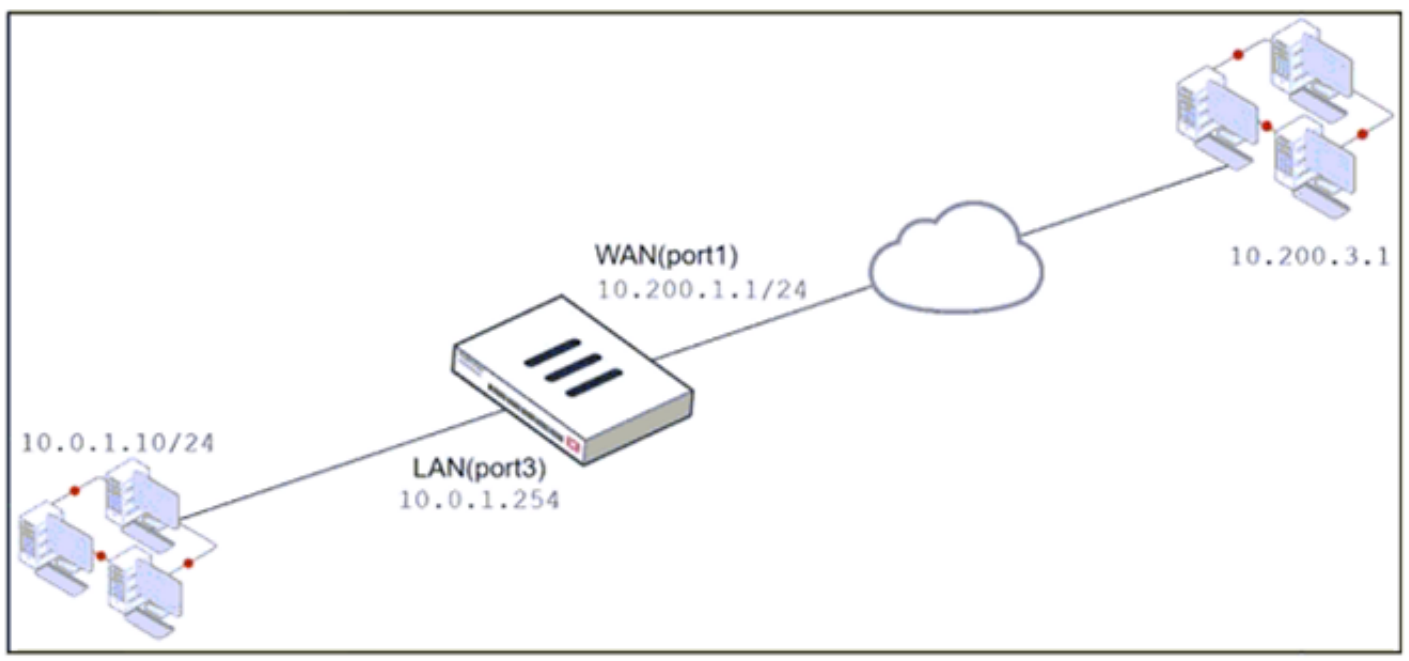


Exhibit A | Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type	IPv4
Name	VIP
Comments	Write a comment... 0/255
Color	Change
Network	
Interface	WAN (port1)
Type	Static NAT
External IP address/range	10.200.1.10
Map to	
IPv4 address/range	10.0.1.10
Optional Filters	
Port Forwarding	
Protocol	TCP UDP SCTP ICMP
Port Mapping Type	One to one Many to many
External service port	10443
Map to IPv4 port	443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

A. 10.0.1.254, 10.0.1.10, and 443, respectively
B. 10.0.1.254, 10.200.1.10, and 443, respectively
C. 10.200.3.1, 10.0.1.10, and 443, respectively
D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Answer: C

Explanation:
The host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, which is the external IP address of the VIP object named VIP in Exhibit B1. The VIP object maps the external IP address and port to the internal IP address and port of the server 10.0.1.10 and 443, respectively1. The VIP object also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.
The firewall policy ID 1 in Exhibit B allows traffic from WAN (port1) to LAN (port3) with the destination address of VIP and the service of HTTPS1. The policy also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.
Therefore, after FortiGate forwards the packet to the destination, the source address, destination address, and destination port of the packet will be 10.200.3.1, 10.0.1.10, and 443, respectively.

You can find more information about VIP objects and firewall policies in the Fortinet Documentation

NEW QUESTION 10
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

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.73): "What about traffic originating from FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate. Traffic coming from FortiGate to those global services originates from the management VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM. It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate."

NEW QUESTION 15
Examine this FortiGate configuration:

```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.
B. It drops the traffic.
C. It authenticates the traffic using the authentication scheme SCHEME2.
D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:
"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

NEW QUESTION 17
What are two characteristics of FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Virtual IP addresses are used to distinguish between cluster members.
B. Heartbeat interfaces have virtual IP addresses that are manually assigned.
C. The primary device in the cluster is always assigned IP address 169.254.0.1.
D. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.

Answer: AD

Explanation:
Fortigate Infrastructure 7.2 Study Guide page 301 FortiGate Infrastructure 7.2 Study Guide (p.301):
"FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number."
"A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster." "The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data." https://networkinterview.com/fortigate-ha-high-availability/

NEW QUESTION 21
Refer to the exhibit.


```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check . Which interface will be selected as an outgoing interface?

A. port2
B. port4
C. port3
D. port1

Answer: D

Explanation:
Port 1 shows the lowest latency.

NEW QUESTION 24
Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.
B. The existing network IP schema must be changed when installing a transparent mode.
C. Static routes are required to allow traffic to the next hop.
D. FortiGate forwards frames without changing the MAC address.

Answer: AD

NEW QUESTION 29
Refer to the web filter raw logs.

```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvdbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"

date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

A. Social networking web filter category is configured with the action set to authenticate.
B. The action on firewall policy ID 1 is set to warning.
C. Access to the social networking web filter category was explicitly blocked to all users.
D. The name of the firewall policy is all_users_web.

Answer: A

NEW QUESTION 34
On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs
B. Forward traffic logs
C. Local traffic logs
D. Security logs

Answer: C

NEW QUESTION 39
Refer to the exhibits.

Exhibit A Exhibit B

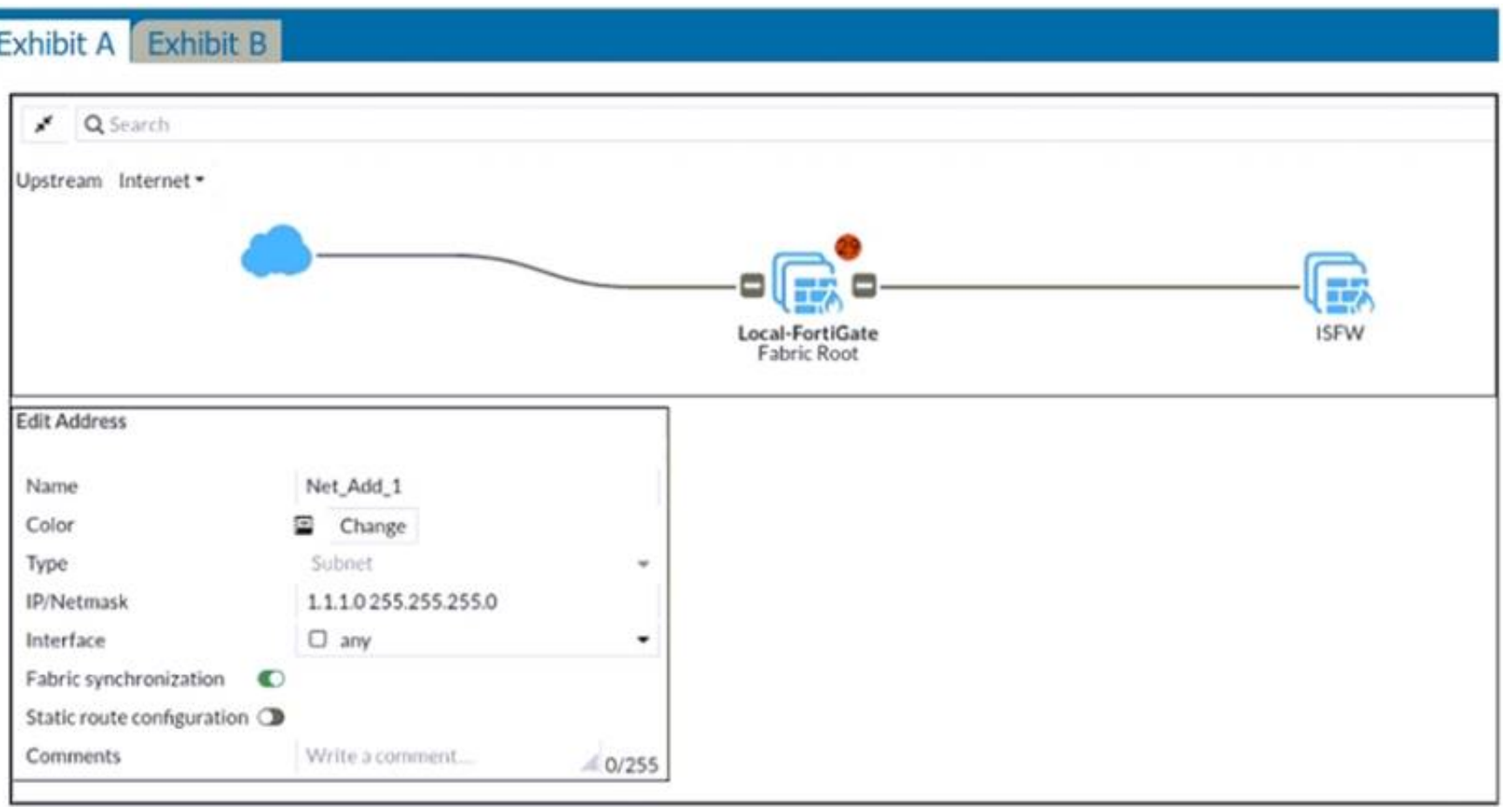


Exhibit A | Exhibit B

```
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
```

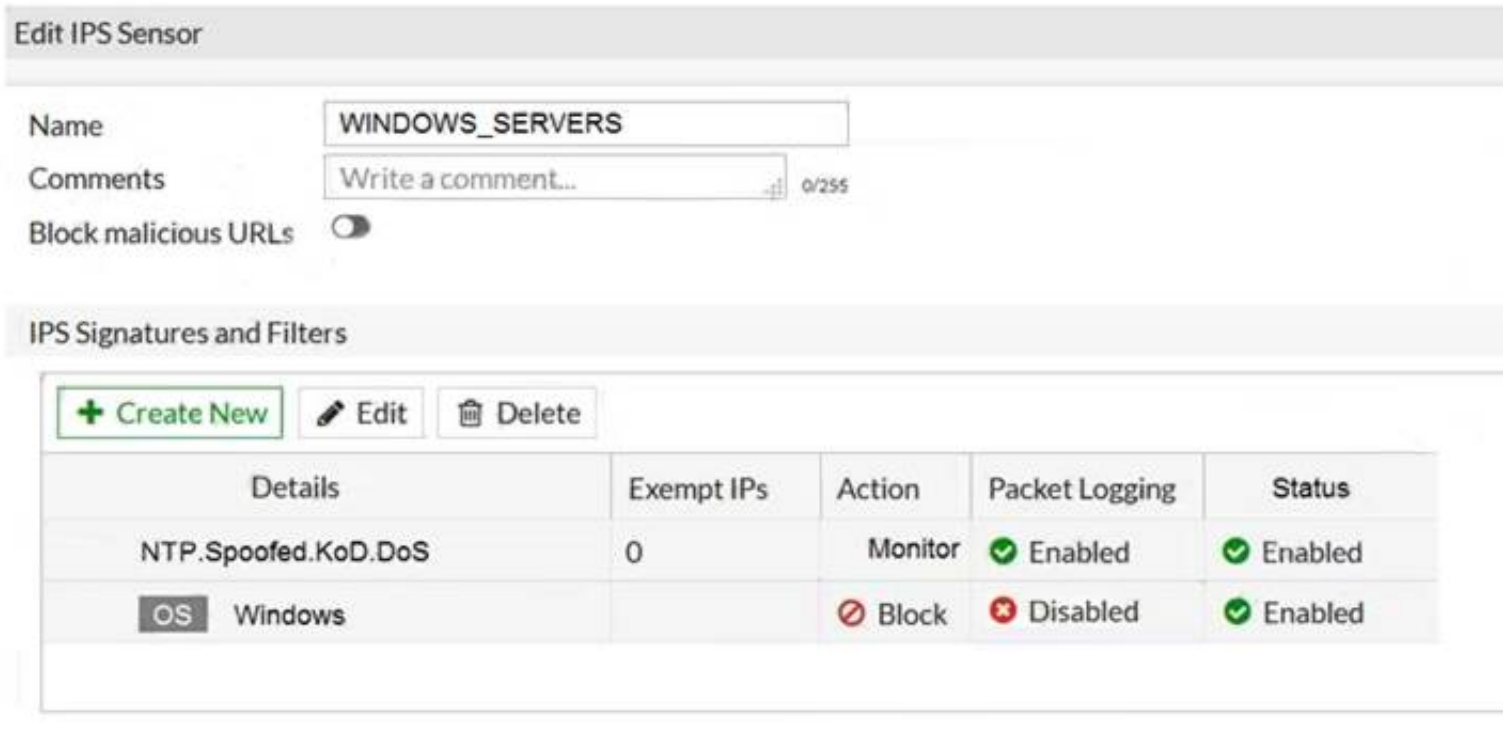
```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream "10.0.1.254"
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    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 43
Refer to the exhibit.



The exhibit shows the IPS sensor configuration.
If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 48
Which feature in the Security Fabric takes one or more actions based on event triggers?

A. Fabric Connectors
B. Automation Stitches
C. Security Rating
D. Logical Topology

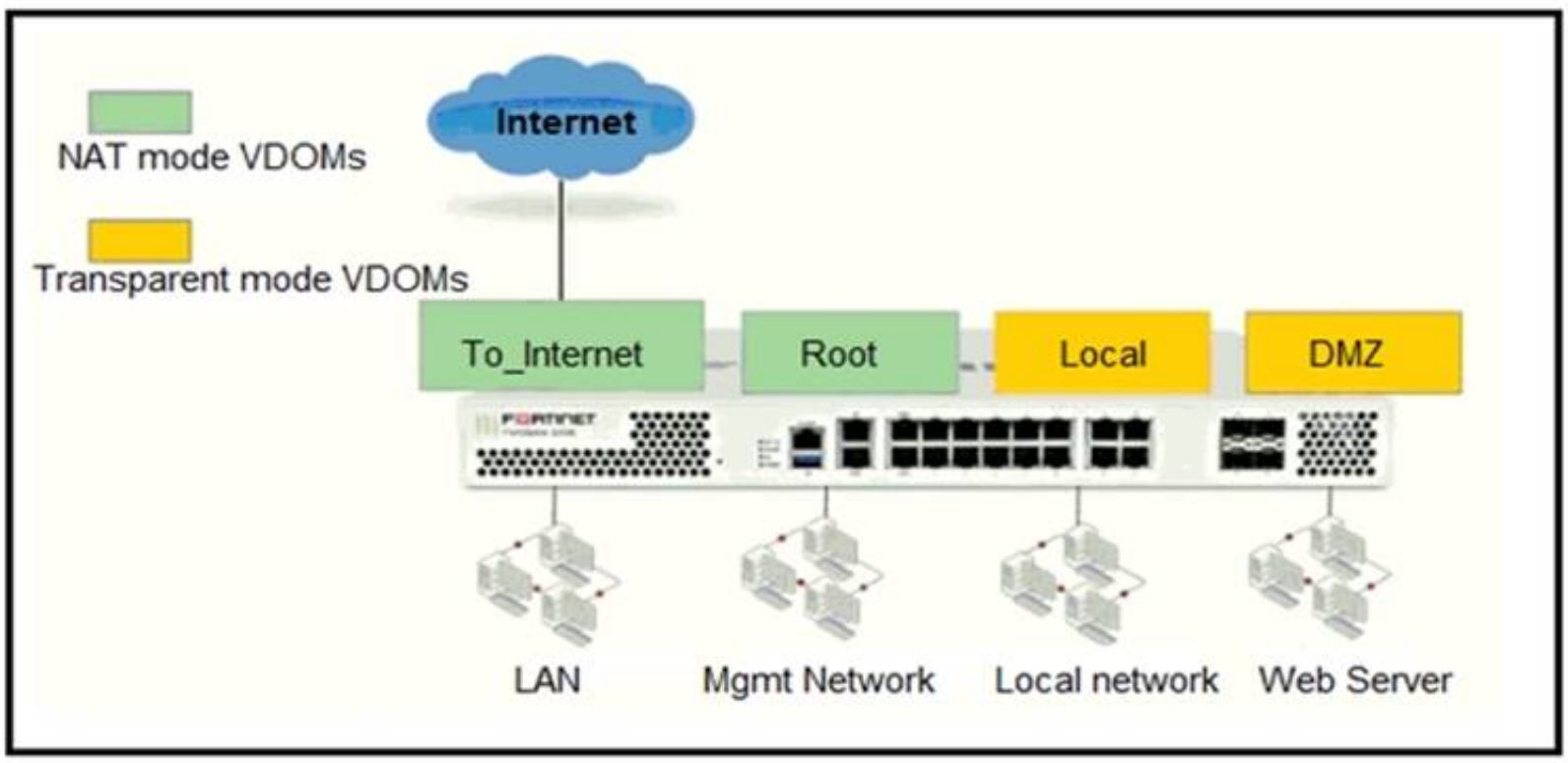
Answer: B

NEW QUESTION 51
How does FortiGate act when using SSL VPN in web mode?

A. FortiGate acts as an FDS server.
B. FortiGate acts as an HTTP reverse proxy.
C. FortiGate acts as DNS server.
D. FortiGate acts as router.

Answer: B

NEW QUESTION 54
Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem .
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

NEW QUESTION 58
Refer to the exhibit.

```
FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > -  selected route, * - FIB route, p - stale info

S      *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
       *>           [10/0] via 10.0.0.2, port2, [30/0]
S         0.0.0.0/0  [20/0] via 192.168.15.2, port3, [10/0]
C      *> 10.0.0.0/24 is directly connected, port2
S         172.13.24.0/24  [10.0] is directly connected, port4
C      *> 172.20.121.0/24 is directly connected, port1
S      *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C      *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

A. The port3 default route has the lowest metric.
B. The port1 and port2 default routes are active in the routing table.
C. The ports default route has the highest distance.
D. There will be eight routes active in the routing table.

Answer: BC

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p

NEW QUESTION 60
Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeou
B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
C. It is a hard timeou

D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
E. It is an idle timeou
F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
G. It is a hard timeou
H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Answer: A

NEW QUESTION 61
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

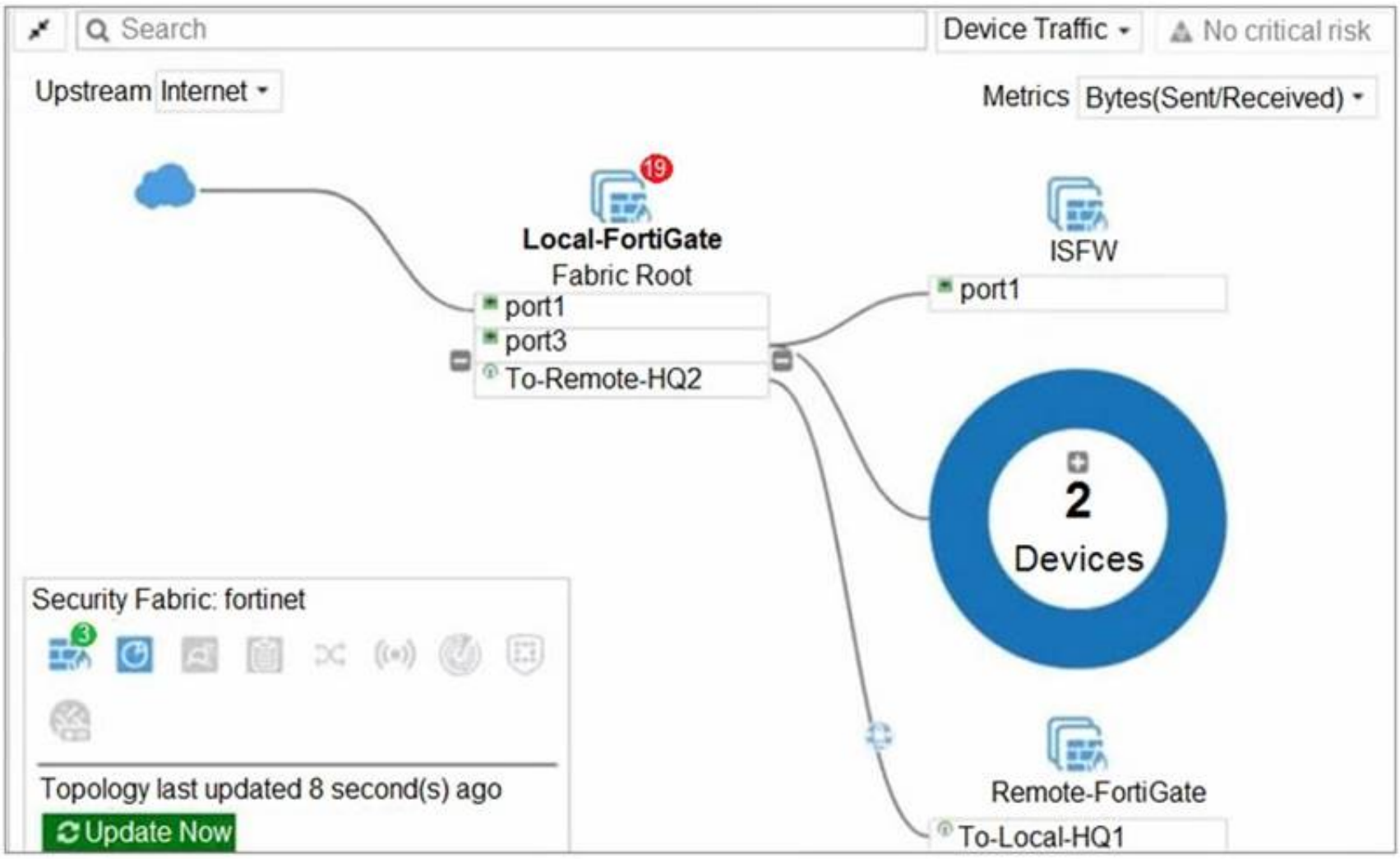
NEW QUESTION 62
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

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 63
Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. There are five devices that are part of the security fabric.
B. Device detection is disabled on all FortiGate devices.
C. This security fabric topology is a logical topology view.
D. There are 19 security recommendations for the security fabric.

Answer: CD

Explanation:
References: https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology

NEW QUESTION 66
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 67
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 70
Refer to the exhibit.

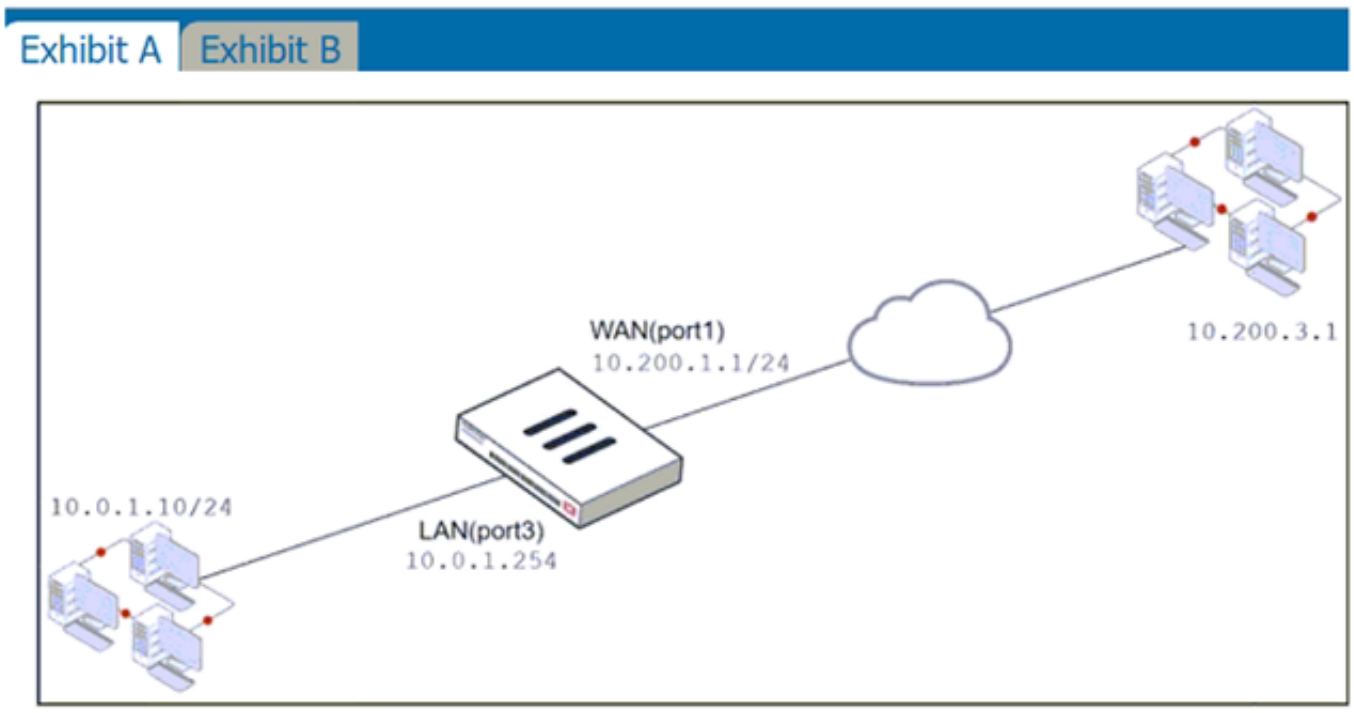


Exhibit A | Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT	IP Pool
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Disabled

Edit Virtual IP

VIP type IPv4
Name VIP
Comments Write a comment... 0/255
Color Change

Network
Interface port1
Type Static NAT
External IP address/range 10.200.1.10
Map to
IPv4 address/range 10.0.1.10

Optional Filters

Port Forwarding
Protocol TCP UDP SCTP ICMP
Port Mapping Type One to one Many to many
External service port 443
Map to IPv4 port 443

Edit Dynamic IP Pool

Name IP Pool
Comments Write a comment... 0/255
Type Overload One-to-One Fixed Port Range Port Block Allocation
External IP address/range 10.200.1.100-10.200.1.100
NAT64
ARP Reply

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies 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. The first firewall policy has NAT enabled using IP Pool.
The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0. 1. 10?

A. 10.200. 1. 1
B. 10.200.3. 1
C. 10.200. 1. 100
D. 10.200. 1. 10

Answer: C

Explanation:
Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

NEW QUESTION 73
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 75
Which statement correctly describes the use of reliable logging on FortiGate?

A. Reliable logging is enabled by default in all configuration scenarios.
B. Reliable logging is required to encrypt the transmission of logs.
C. Reliable logging can be configured only using the CLI.
D. Reliable logging prevents the loss of logs when the local disk is full.

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.192): "if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI."

NEW QUESTION 79
Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.
B. AH does not support perfect forward secrecy.
C. AH provides data integrity bur no encryption.
D. AH provides strong data integrity but weak encryption.

Answer: C

NEW QUESTION 84
Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 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=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e 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 statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.
B. The session is in TCP ESTABLISHED state.
C. The session is a bidirectional UDP connection.
D. The session is a bidirectional TCP connection.

Answer: C

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NEW QUESTION 86
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. hard-timeout
B. auth-on-demand
C. soft-timeout
D. new-session
E. Idle-timeout

Answer: ADE

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

NEW QUESTION 87
.....

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/