NSE4_FGT-7.2Q&As

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse4_fgt-7-2.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

Correct Answer: BCD

QUESTION 2

Which statement describes a characteristic of automation stitches?

A. They can have one or more triggers.

B. They can be run only on devices in the Security Fabric.

C. They can run multiple actions simultaneously.

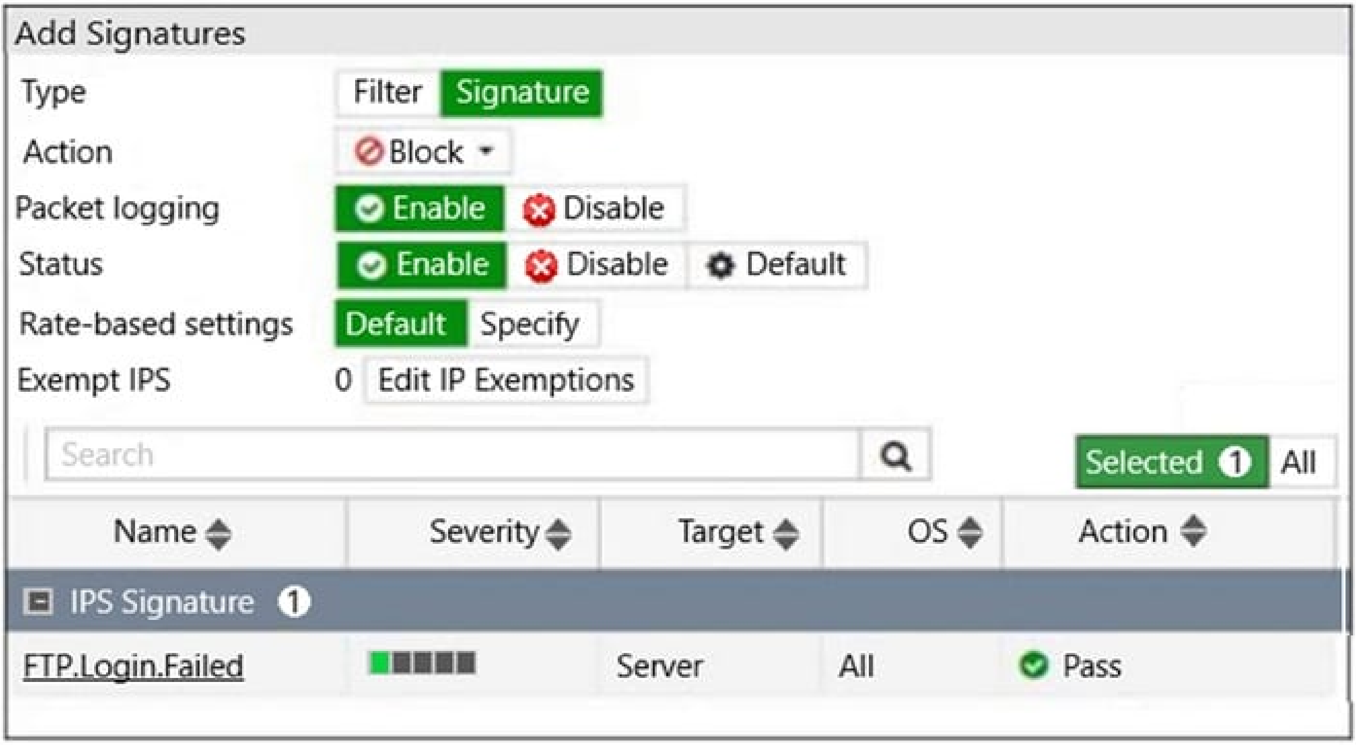
D. They can be created on any device in the fabric.

Correct Answer: C

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/139441/automation-stitches

QUESTION 3

Refer to the exhibit.



Add Signatures

Type: Filter [✓ Signature]

Action: Block

Packet logging: [✓ Enable] Disable

Status: [✓ Enable] Disable Default

Rate-based settings: [✓ Default] Specify

Exempt IPS: 0 Edit IP Exemptions

Name	Severity	Target	OS	Action
IPS Signature 1				
FTP.Login.Failed	■■■■■	Server	All	✓ Pass

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.

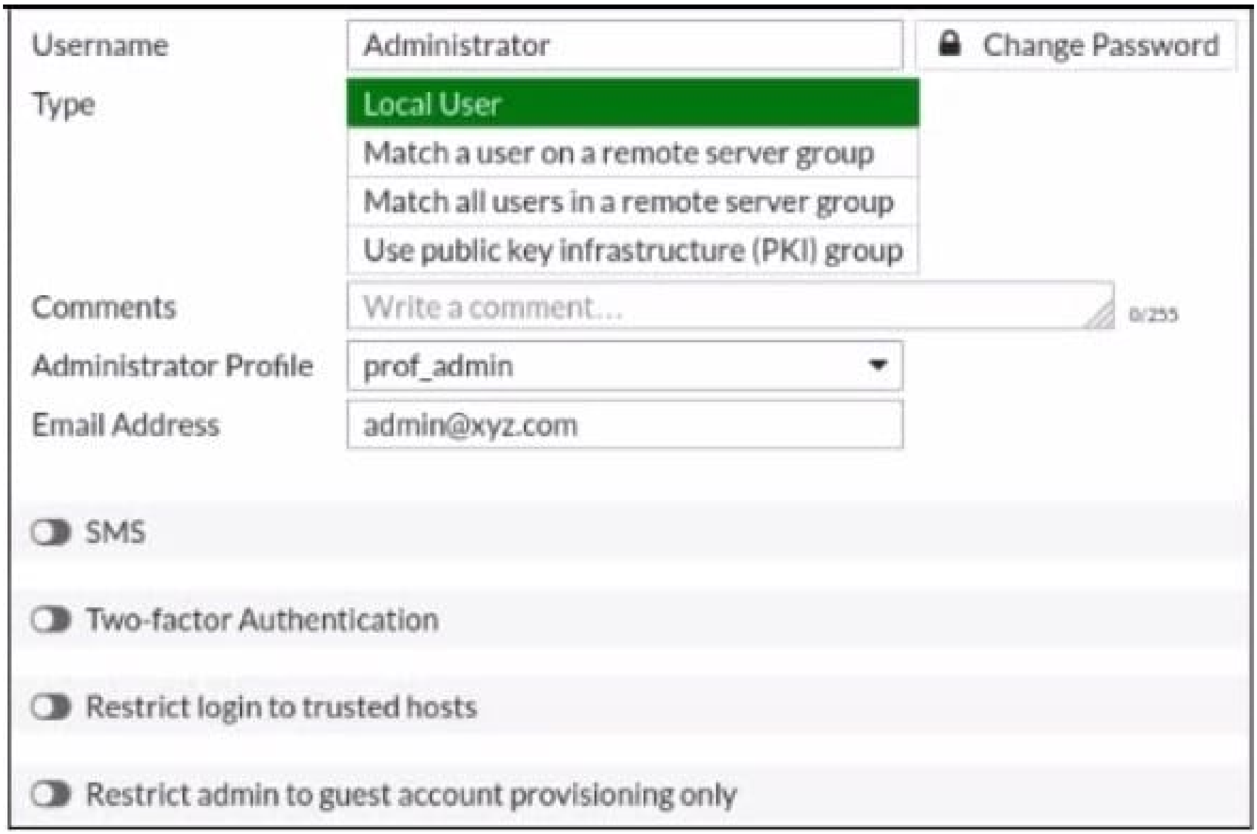
Correct Answer: D

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.

QUESTION 4

Refer to the exhibit.



Username: Administrator
Type: Local User

Change Password
Local User
Match a user on a remote server group
Match all users in a remote server group
Use public key infrastructure (PKI) group

Comments: Write a comment... 0/255
Administrator Profile: prof_admin
Email Address: admin@xyz.com

SMS
Two-factor Authentication
Restrict login to trusted hosts
Restrict admin to guest account provisioning only

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

Correct Answer: C

Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=FD34502

QUESTION 5

What are two functions of the ZTNA rule? (Choose two.)

A. It redirects the client request to the access proxy.

B. It applies security profiles to protect traffic.

C. It defines the access proxy.

D. It enforces access control.

Correct Answer: BD

A ZTNA rule is a policy that enforces access control and applies security profiles to protect traffic between the client and the access proxy1. A ZTNA rule defines the following parameters1:

Incoming interface: The interface that receives the client request.

Source: The address and user group of the client.

ZTNA tag: The tag that identifies the domain that the client belongs to. ZTNA server: The server that hosts the access proxy. Destination: The address of the application that the client wants to access. Action: The action to take for the traffic

that matches the rule. It can be accept, deny, or redirect.

Security profiles: The security features to apply to the traffic, such as antivirus, web filter, application control, and so on.

A ZTNA rule does not redirect the client request to the access proxy. That is the function of a policy route that matches the ZTNA tag and sends the traffic to the ZTNA server2. A ZTNA rule does not define the access proxy. That is done by

creating a ZTNA server object that specifies the IP address, port, and certificate of the access proxy3.

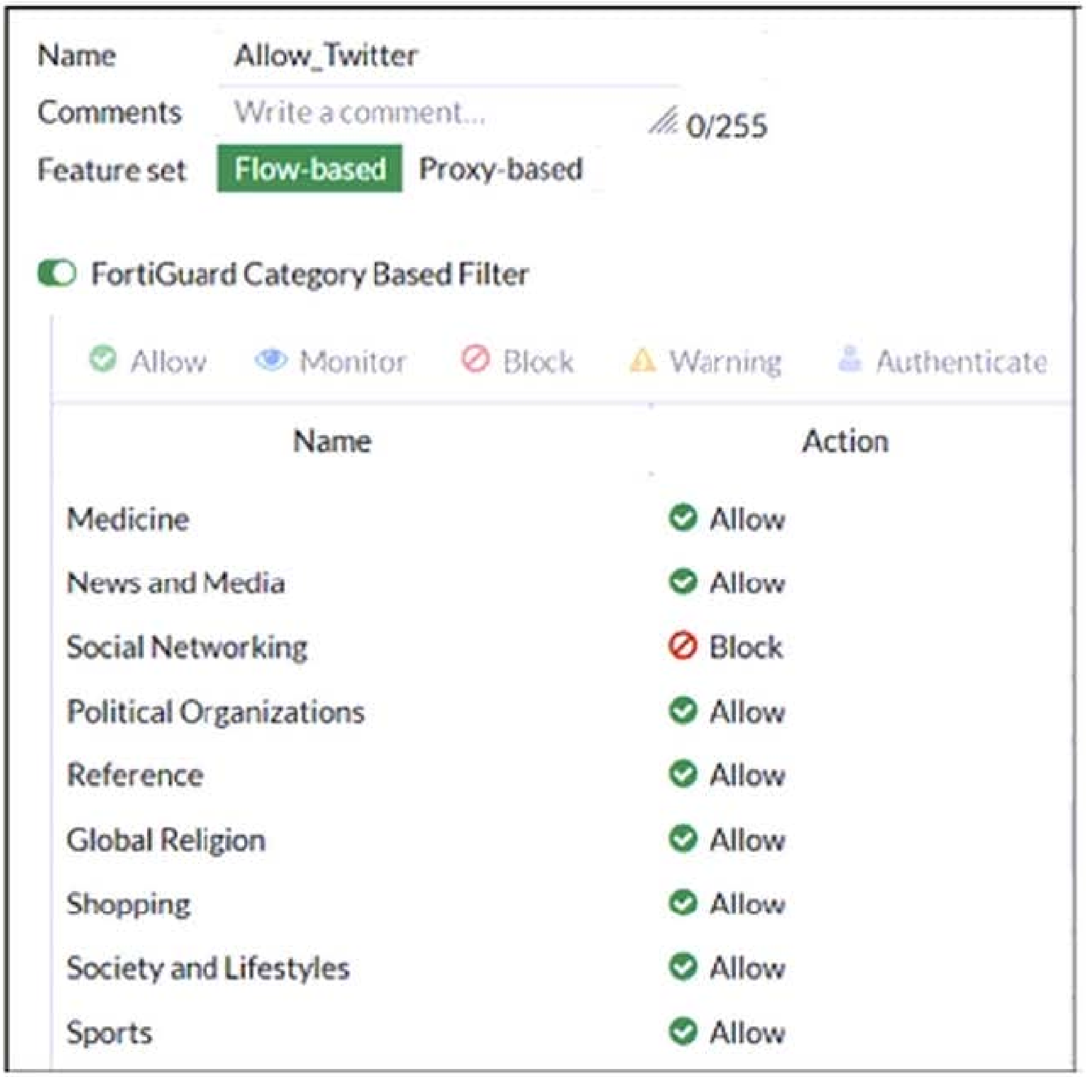
FortiGate Infrastructure 7.2 Study Guide (p.177): "A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role- based access. To create a rule, type a rule name, and add IP

addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic."

QUESTION 6

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.



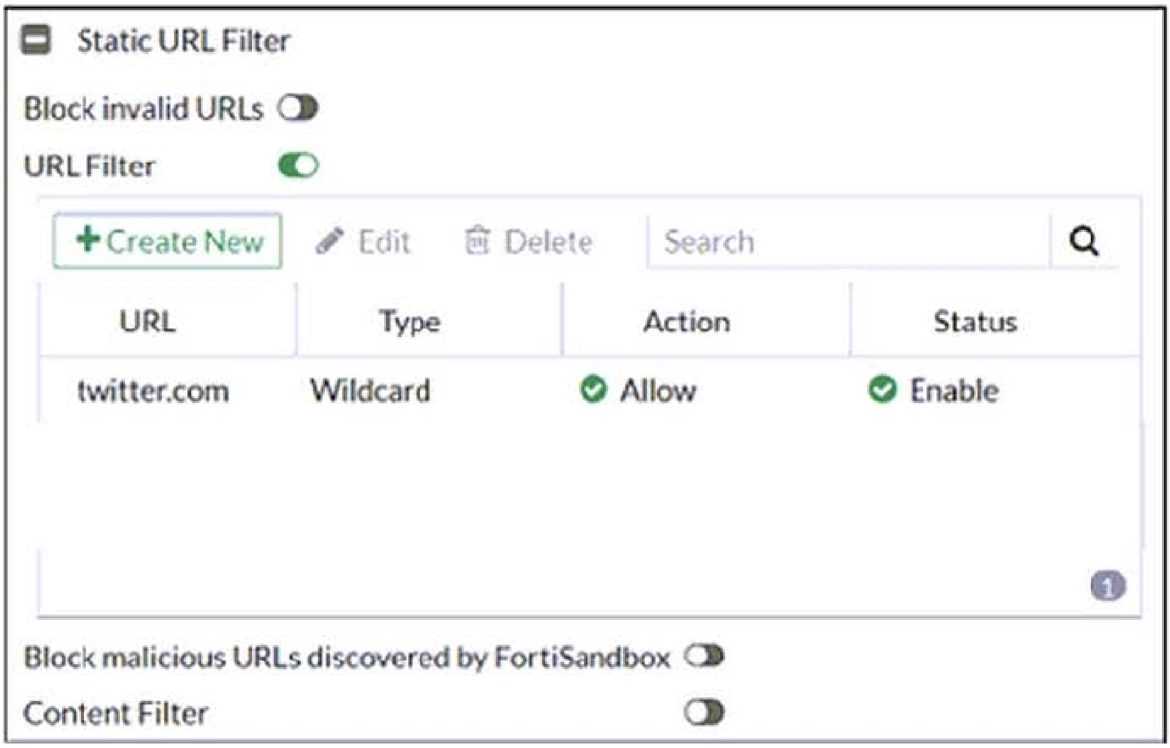
Name Allow_Twitter

Comments Write a comment... 0/255

Feature set [✓ Flow-based] Proxy-based

● FortiGuard Category Based Filter

Name	Action
Medicine	✓ Allow
News and Media	✓ Allow
Social Networking	⊘ Block
Political Organizations	✓ Allow
Reference	✓ Allow
Global Religion	✓ Allow
Shopping	✓ Allow
Society and Lifestyles	✓ Allow
Sports	✓ Allow



Static URL Filter

Block invalid URLs ○

URL Filter ●

URL	Type	Action	Status
twitter.com	Wildcard	✓ Allow	✓ Enable

Block malicious URLs discovered by FortiSandbox ○

Content Filter ○

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking

B. On the Static URL Filter configuration, set Type to Simple

C. On the Static URL Filter configuration, set Action to Exempt.

D. On the Static URL Filter configuration, set Action to Monitor.

Correct Answer: C

Reference: https://fortinet77.rssing.com/chan-56127603/article113.html Based on the exhibit, the administrator has configured the FortiGuard Category Based Filter to block access to all social networking sites, and has also configured a Static URL Filter to block access to twitter.com. As a result, users are being redirected to a block page when they try to access twitter.com. To allow users to access twitter.com while blocking all other social networking sites, the administrator can make the following configuration change: On the Static URL Filter configuration, set Action to Exempt: By setting the Action to Exempt, the administrator can override the block on twitter.com that was specified in the FortiGuard Category Based Filter. This will allow users to access twitter.com, while all other social networking sites will still be blocked.

QUESTION 7

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.

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets

QUESTION 8

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

Correct Answer: AC

QUESTION 9

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

Correct Answer: B

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

QUESTION 10

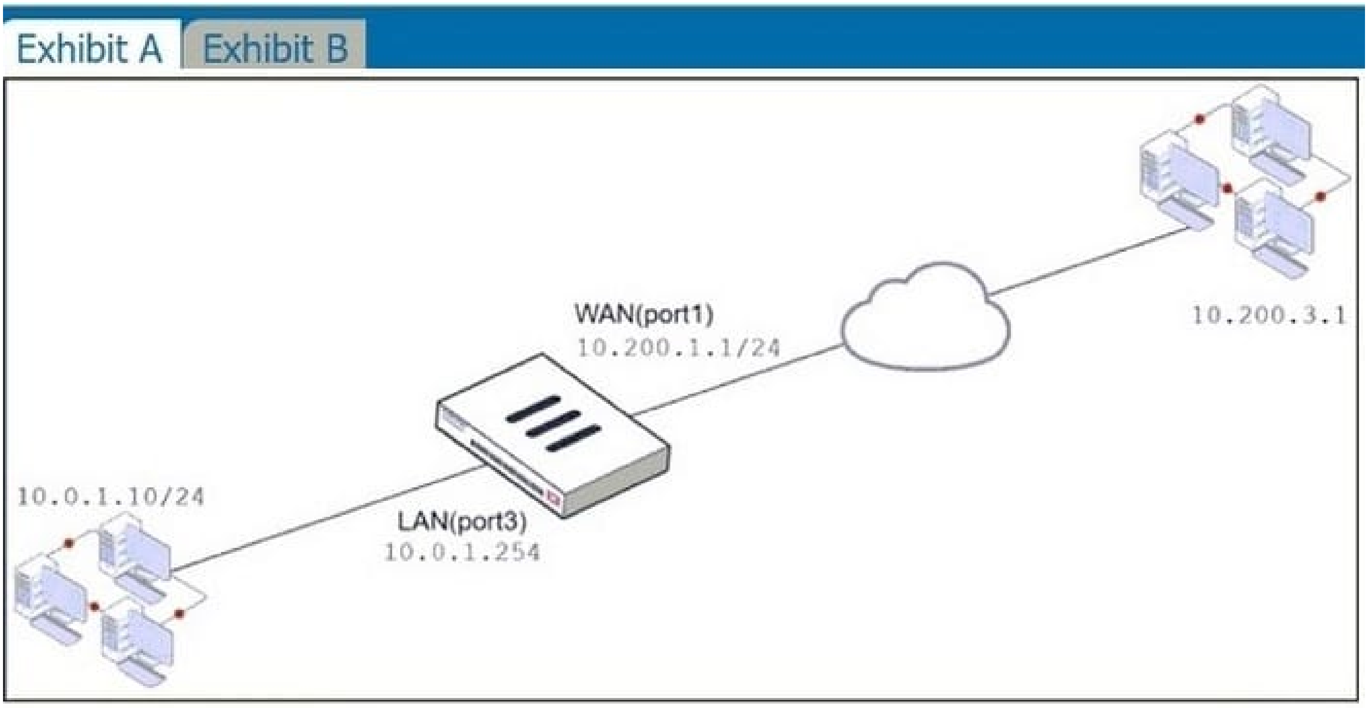
Refer to the exhibits.

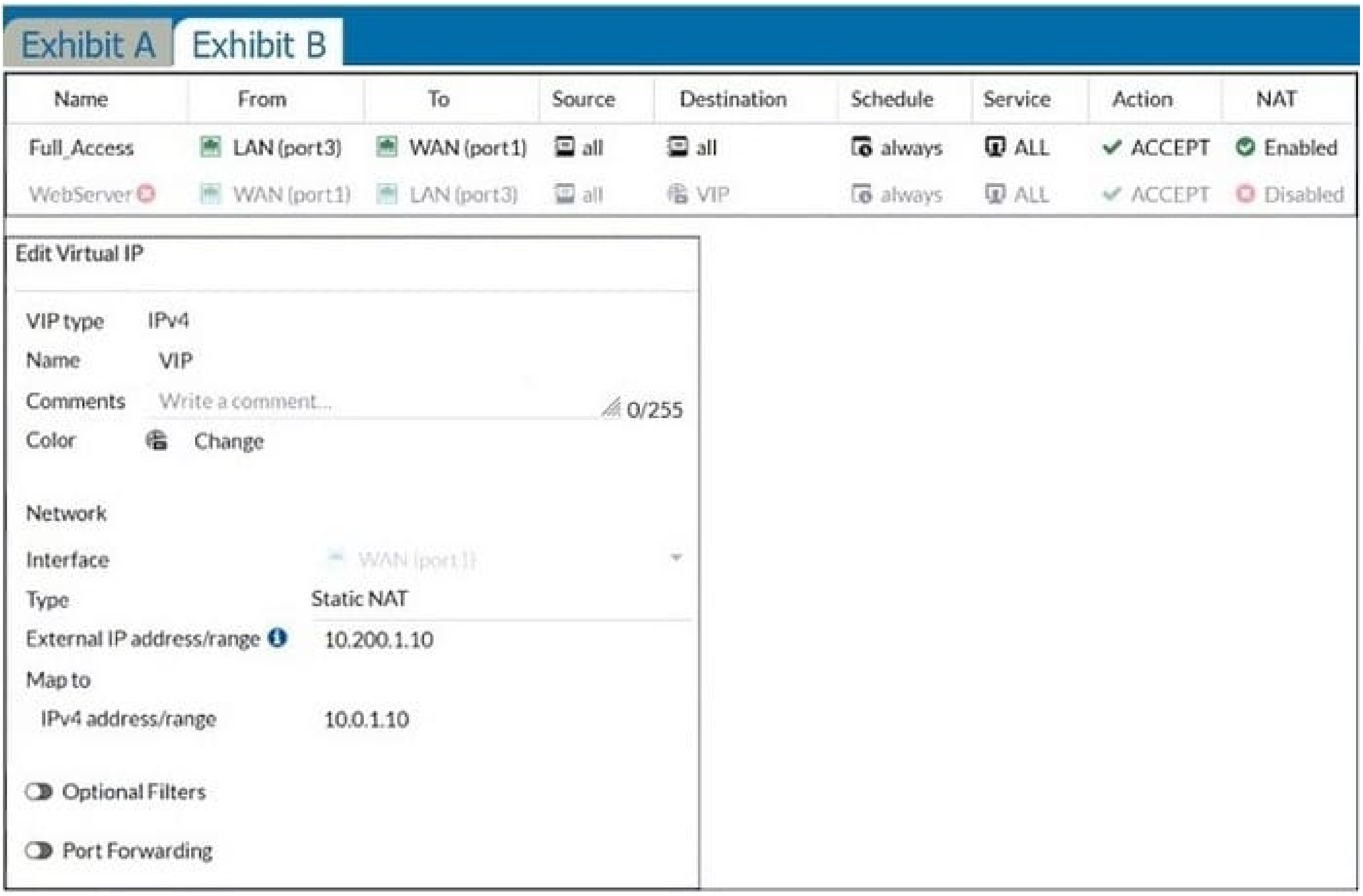
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.

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.

The administrator disabled the WebServer firewall policy.





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

Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

A. 10.200.1.10

B. 10.0.1.254

C. 10.200.1.1

D. 10.200.3.1

Correct Answer: C

Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

QUESTION 11

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

Correct Answer: D

QUESTION 12

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

A. Log ID

B. Universally Unique Identifier

C. Policy ID

D. Sequence ID

Correct Answer: B

FortiGate Security 7.2 Study Guide (p.67): "When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer."

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies

QUESTION 13

In which two ways can RPF checking be disabled? (Choose two)

A. Enable anti-replay in firewall policy.

B. Disable the RPF check at the FortiGate interface level for the source check

C. Enable asymmetric routing.

D. Disable strict-arc-check under system settings.

Correct Answer: CD

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

QUESTION 14

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not Which configuration option is the most effective way to support this request?

A. Implement a web filter category override for the specified website

B. Implement a DNS filter for the specified website.

C. Implement web filter quotas for the specified website

D. Implement web filter authentication for the specified website.

Correct Answer: D

QUESTION 15

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.

Correct Answer: C