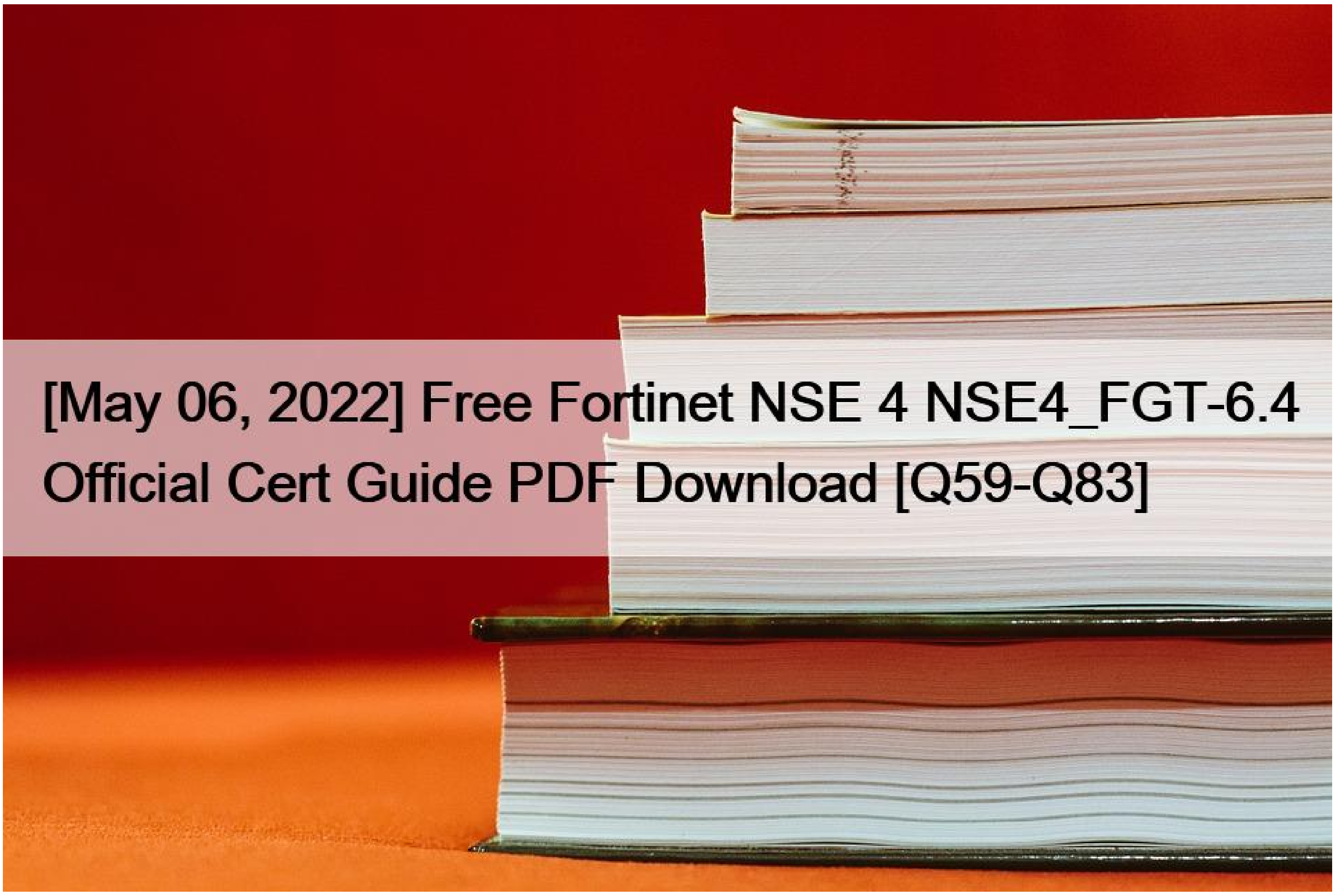
[May 06, 2022 Free Fortinet NSE 4 NSE4_FGT-6.4 Official Cert Guide PDF Download [Q59-Q83



[May 06, 2022] Free Fortinet NSE 4 NSE4_FGT-6.4 Official Cert Guide PDF Download
Fortinet NSE4_FGT-6.4 Official Cert Guide PDF

How to Prepare For Network Security Professional (Fortinet NSE4_FGT-6.4) Professional Exam **Preparation Guide for Network Security Professional (Fortinet NSE4_FGT-6.4) Professional Exam Introduction for Network Security Professional (Fortinet NSE4_FGT-6.4) Professional Exam**

This guide provides a step by step framework of the Network Security Professional (Fortinet NSE4_FGT-6.4) Professional course exam including a broad array of essentials of the test, the exam design, themes, test complexities and readiness techniques, and the intended interest group profile. Thus, we prepare various **FORTINET NSE4_FGT-6.4 exam dumps** as we understand understudy determinations. Our content, helps candidates total assessments.

Fortinet released its initial product, FortiGate, a firewall, in 2002, succeeded by anti-spam and anti-virus software. FortiGate was upgraded to use application-specific integrated circuit (ASIC) architecture.

The Network Security Professional designation recognizes your ability to install and manage the day-to-day configuration, monitoring, and operation of a FortiGate device to support specific corporate network security policies.

We recommend this exam for network and security professionals who are involved in the day-to-day management, implementation, and administration of a security infrastructure using FortiGate devices

Originally, the FortiGate was a material, rack-mounted product but later on, it became available also as a virtual appliance able to run on virtualization platforms like VMware vSphere. Fortinet also joined its network security offerings, including firewalls, anti-spam and anti-virus software, into a single product.

Fortinet began developing its Security Fabric architecture in April 2016, so many network security products could communicate as one program. The same year, the company supplemented Security Information and Event Management (SIEM) products. In September 2016, the company declared it would combine the SIEM products with the security systems of other merchants.

The Network Security Professional (Fortinet NSE4_FGT-6.4) course identifies a person's capability to establish and maintain the day-to-day configuration, monitoring, and operation of a FortiGate device to carry out particular corporate network security policies.

If you are a customer or a public user, you must first create an account on the NSE Institute. You must use your company email address to register. You must purchase your training though your local distributor.

If you are a partner, you must first create an account on the Partner Portal. You must use your company email address to register.

With 46,000+ active user certifications, the Fortinet Network Security Expert certification program is earning notable critical mass and industry attention. The value of the Fortinet NSE designation is verified every day by security specialists in the field and by trusted sources.

After finishing this course, the candidate will be able to:

> - Examine a FortiGate route table- Propose Fortinet Single Sign-On access to network services, integrated with Microsoft Active Directory- Implement port forwarding, source NAT, and destination NAT- Run packets using policy-based and static routes for multipath and load-balanced deployments- Examine traffic transparently, forwarding as a Layer 2 device- Diagnose declined IKE exchanges- Manage network access to configured networks using firewall policies- Offer an SSL VPN for secure access to a private network- Diagnose and repair common problems- Recognize the features of the Fortinet Security Fabric- Utilize the GUI and CLI for management- Deploy implicit and explicit proxy with firewall policies, authentication, and caching- Verify users using firewall policies- Execute a meshed or partially redundant VPN- Stop hacking and denial of service (DoS) attacks- Partition FortiGate into two or more virtual devices, each operating as an autonomous FortiGate, by configuring virtual domains- Configure security profiles to offset threats and ill-usage, including viruses, torrents, and improper websites- Examine SSL/TLS-secured traffic to stop encryption used to bypass security policies- Implement application control methods to monitor and control network applications that might use standard or non-standard protocols and ports- Deploy FortiGate devices as an HA cluster for fault tolerance and high performance- Authorize an IPsec VPN tunnel connecting two FortiGate devices- Understand encryption uses and certificates

Use **FORTINET NSE4_FGT-6.4 practice exam** and **FORTINET NSE4_FGT-6.4 practice exams** to prepare for the exam.

NEW QUESTION 59

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?

* Log ID
* Universally Unique Identifier
* Policy ID
* Sequence ID

NEW QUESTION 60

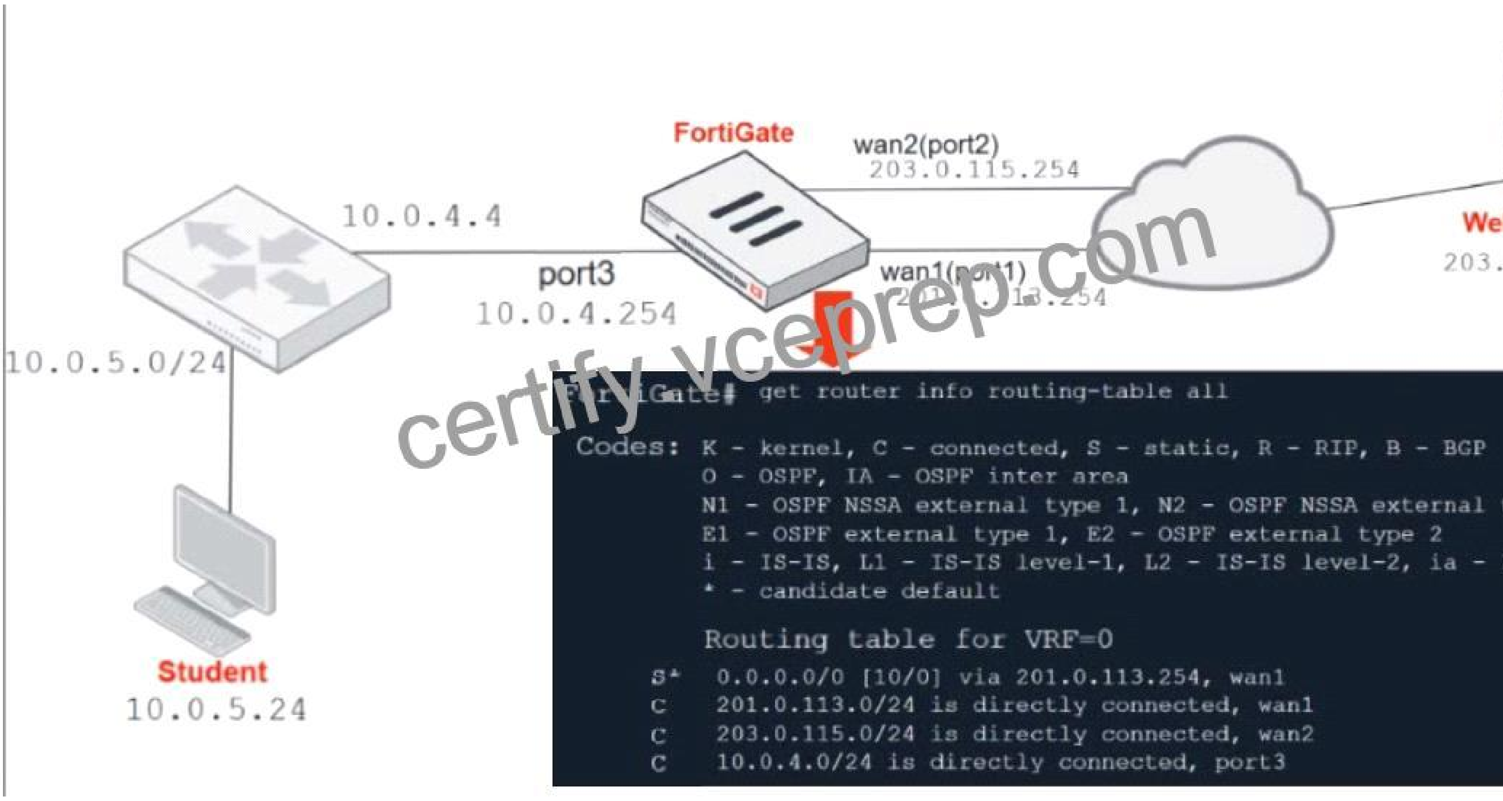
An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

* VLAN interface
* Software Switch interface
* Aggregate interface
* Redundant interface

NEW QUESTION 61

Refer to the exhibit.



```
FortiGate # get router info routing-table all
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
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       * - candidate default

       Routing table for VRF=0
S*     0.0.0.0/0 [10/0] via 201.0.113.254, wan1
C      201.0.113.0/24 is directly connected, wan1
C      203.0.115.0/24 is directly connected, wan2
C      10.0.4.0/24 is directly connected, port3
```

Which contains a network diagram and routing table output.

The Student is unable to access Webserver.

What is the cause of the problem and what is the solution for the problem?
* The first packet sent from Student failed the RPF check.

This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
* The first reply packet for Student failed the RPF check.

This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
* The first reply packet for Student failed the RPF check.

This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
* The first packet sent from Student failed the RPF check.

This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

NEW QUESTION 62

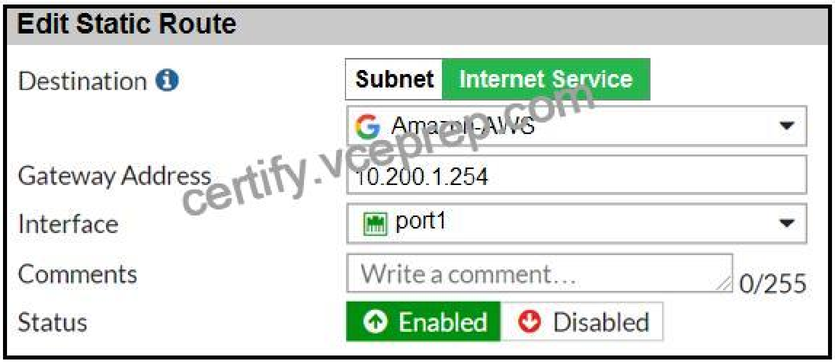
https://www.fast2test.com/NSE4_FGT-6.4-practice-test.html 2

Valid Fast2test NSE4_FGT-6.4 Exam PDF Dumps &#8211; New NSE4_FGT-6.4 Real Exam Questions Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

* Web filter in flow-based inspection
* Antivirus in flow-based inspection
* DNS filter
* Web application firewall
* Application control

NEW QUESTION 63

Refer to the exhibit, which contains a static route configuration.



Edit Static Route

Destination	Subnet / Internet Service Amazon-AWS
Gateway Address	10.200.1.254
Interface	port1
Comments	Write a comment... 0/255
Status	Enabled / Disabled

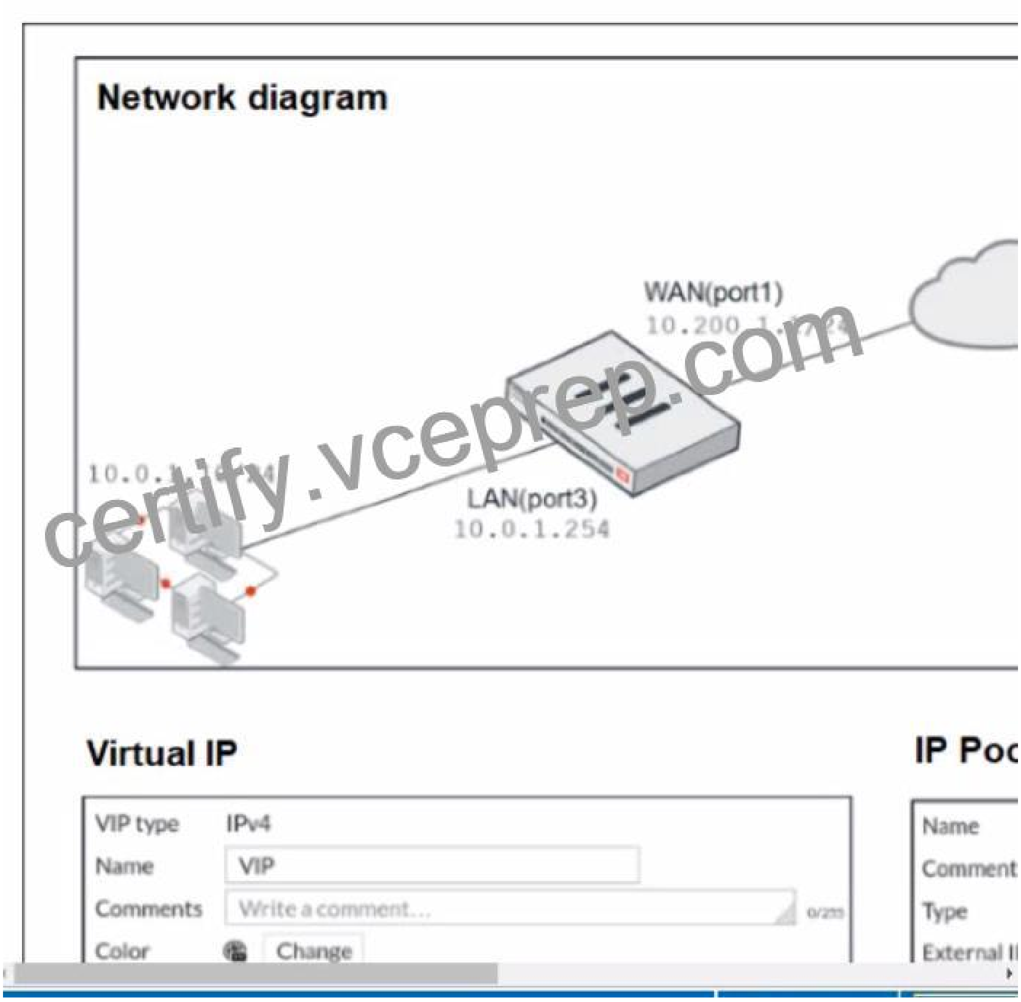
An administrator created a static route for Amazon Web Services.

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

* get router info routing-table all
* get internet service route list
* get router info routing-table database
* diagnose firewall proute list

NEW QUESTION 64

Refer to the exhibit.



Virtual IP

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

IP Poo

Name
Comment
Type
External I

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?
* 10.200.1.1
* 10.200.3.1
* 10.200.1.100
* 10.200.1.10

NEW QUESTION 65

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)
* Shut down/reboot a downstream FortiGate device.

* Disable FortiAnalyzer logging for a downstream FortiGate device.
* Log in to a downstream FortiSwitch device.
* Ban or unban compromised hosts.

NEW QUESTION 66

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?
* VLAN interface
* Software Switch interface
* Aggregate interface
* Redundant interface
Explanation/Reference: https://forum.fortinet.com/tm.aspx?m=120324

NEW QUESTION 67

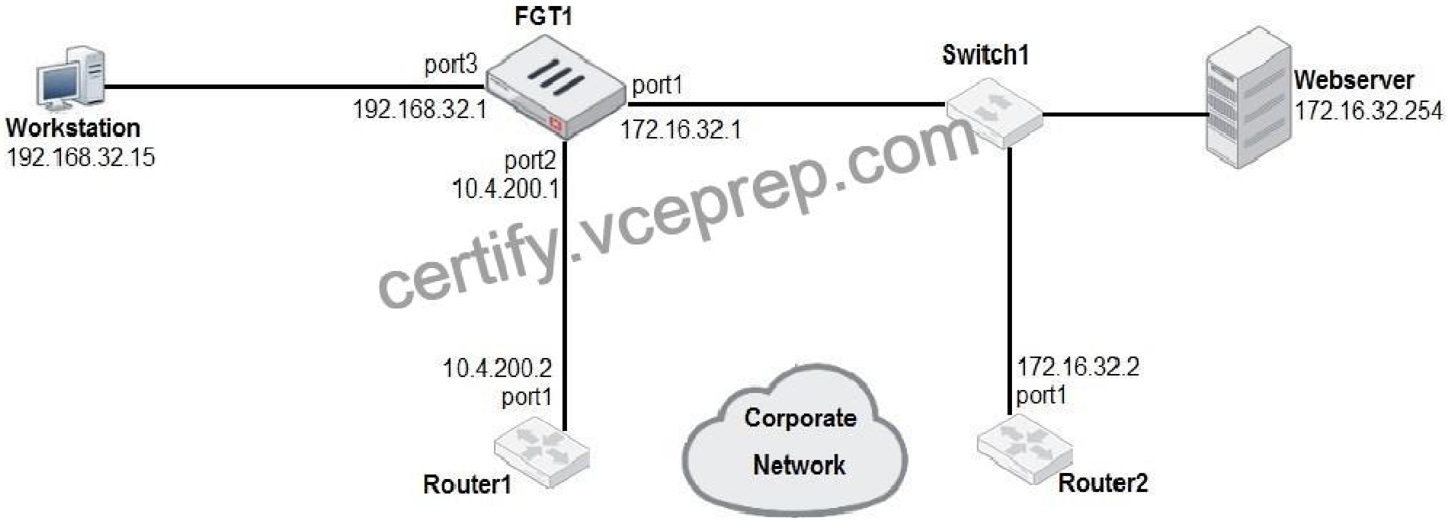
Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)
* The subject field in the server certificate
* The serial number in the server certificate
* The server name indication (SNI) extension in the client hello message
* The subject alternative name (SAN) field in the server certificate
* The host field in the HTTP header
Explanation/Reference: https://checkthefirewall.com/blogs/fortinet/ssl-inspection

NEW QUESTION 68

Which two statements are true about the RPF check? (Choose two.)
* The RPF check is run on the first sent packet of any new session.
* The RPF check is run on the first reply packet of any new session.
* The RPF check is run on the first sent and reply packet of any new session.
* RPF is a mechanism that protects FortiGuard and your network from IP spoofing attacks.
Explanation/Reference: https://www.programmersought.com/article/16383871634/

NEW QUESTION 69

Examine the network diagram shown in the exhibit, then answer the following question:

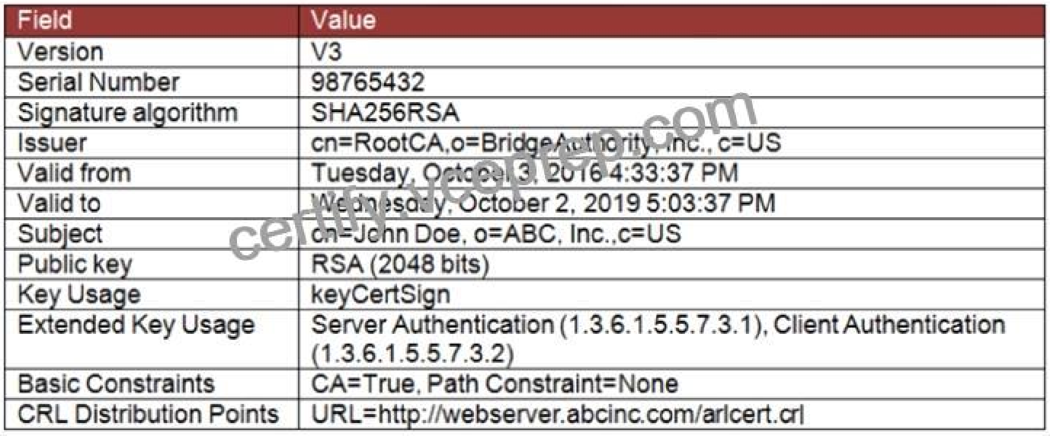


Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

* 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
* 0.0.0.0/0 [20/0] via 10.4.200.2, port2
* 10.4.200.0/30 is directly connected, port2
* 172.16.32.0/24 is directly connected, port1

NEW QUESTION 70

Refer to the exhibit.



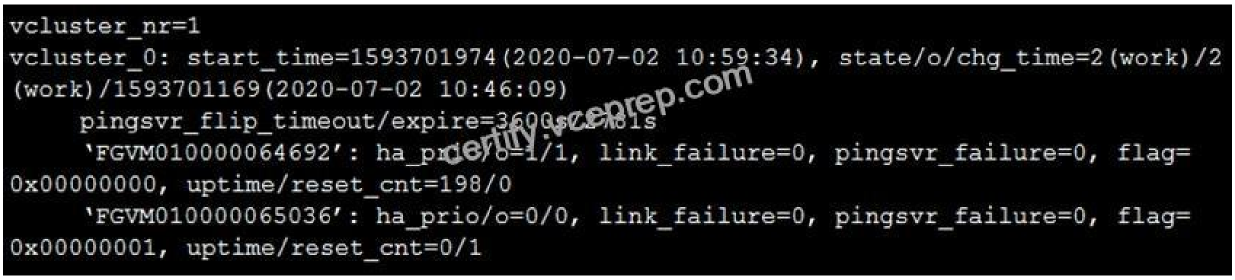
Field	Value
Version	V3
Serial Number	98765432
Signature algorithm	SHA256RSA
Issuer	cn=RootCA,o=BridgeAuthority, Inc., c=US
Valid from	Tuesday, October 3, 2016 4:33:37 PM
Valid to	Wednesday, October 2, 2019 5:03:37 PM
Subject	cn=John Doe, o=ABC, Inc.,c=US
Public key	RSA (2048 bits)
Key Usage	keyCertSign
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	CA=True, Path Constraint=None
CRL Distribution Points	URL=http://webserver.abcinc.com/arlcert.crl

According to the certificate values shown in the exhibit, which type of entity was the certificate issued to?

* A user
* A root CA
* A bridge CA
* A subordinate

NEW QUESTION 71

Refer to the exhibit.



```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
     pingsvr_flip_timeout/expire=3600s/[illegible]81s
     'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
     'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

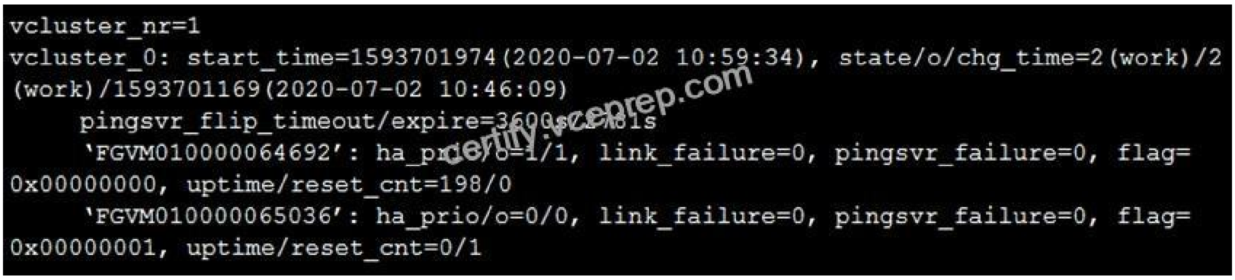
The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

Which two statements are true? (Choose two.)

- FortiGate SN FGVM010000065036 HA uptime has been reset.
- FortiGate devices are not in sync because one device is down.
- FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- FortiGate SN FGVM010000064692 has the higher HA priority.

NEW QUESTION 72

Refer to the exhibit.



```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
     pingsvr_flip_timeout/expire=3600s/[illegible]81s
     'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
     'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

Which two statements are true? (Choose two.)

- FortiGate SN FGVM010000065036 HA uptime has been reset.
- FortiGate devices are not in sync because one device is down.
- FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- FortiGate SN FGVM010000064692 has the higher HA priority.

NEW QUESTION 73

Which of the following statements about central NAT are true? (Choose two.)

- IP tool references must be removed from existing firewall policies before enabling central NAT.
- Central NAT can be enabled or disabled from the CLI only.
- Source NAT, using central NAT, requires at least one central SNAT policy.

* Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

NEW QUESTION 74

What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)
* Traffic to botnetservers
* Traffic to inappropriate web sites
* Server information disclosure attacks
* Credit card data leaks
* SQL injection attacks
https://help.fortinet.com/fweb/570/Content/FortiWeb/fortiweb-admin/web_protection.htm

NEW QUESTION 75

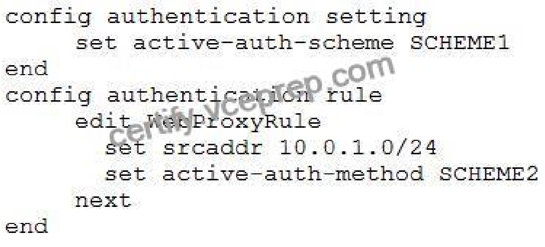
To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?
* FortiManager
* Root FortiGate
* FortiAnalyzer
* Downstream FortiGate

NEW QUESTION 76

Which two statements are true about collector agent advanced mode? (Choose two.)
* Advanced mode uses Windows convention-NetBios: DomainUsername.
* FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate
* Advanced mode supports nested or inherited groups
* Security profiles can be applied only to user groups, not individual users.

NEW QUESTION 77

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?
* It always authorizes the traffic without requiring authentication.
* It drops the traffic.
* It authenticates the traffic using the authentication scheme SCHEME2.
* It authenticates the traffic using the authentication scheme SCHEME1.
Explanation

&#8220;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&#8221;

NEW QUESTION 78

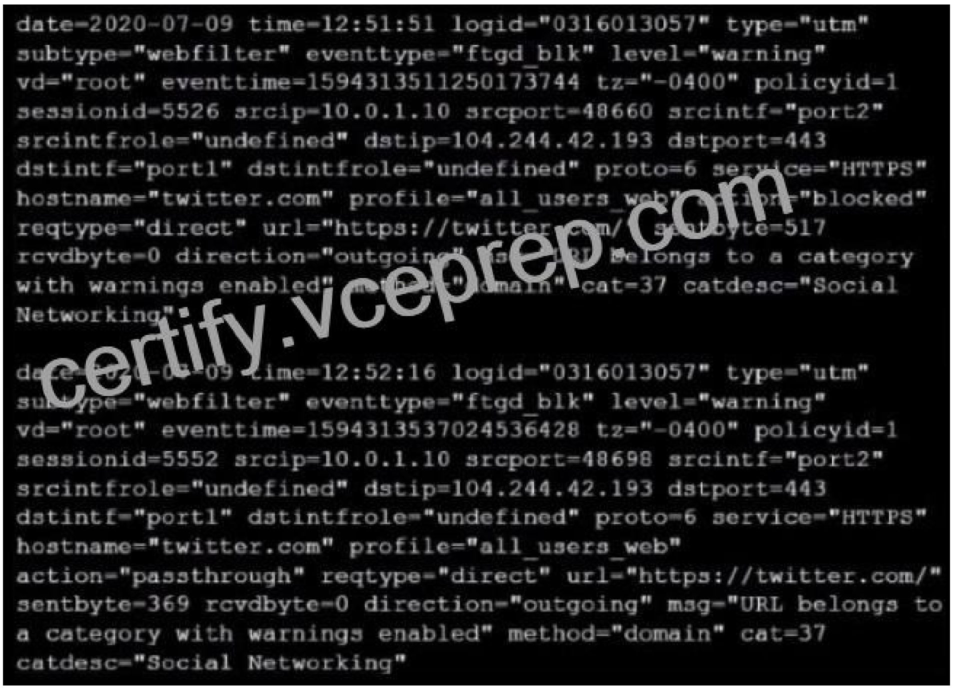
FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure web rating for the home page? (Choose two.)
* www.example.com:443
* www.example.com
* example.com
* www.example.com/index.html
Explanation

FortiGate_Security_6.4 page 384

NEW QUESTION 79

Refer to the web filter raw logs.



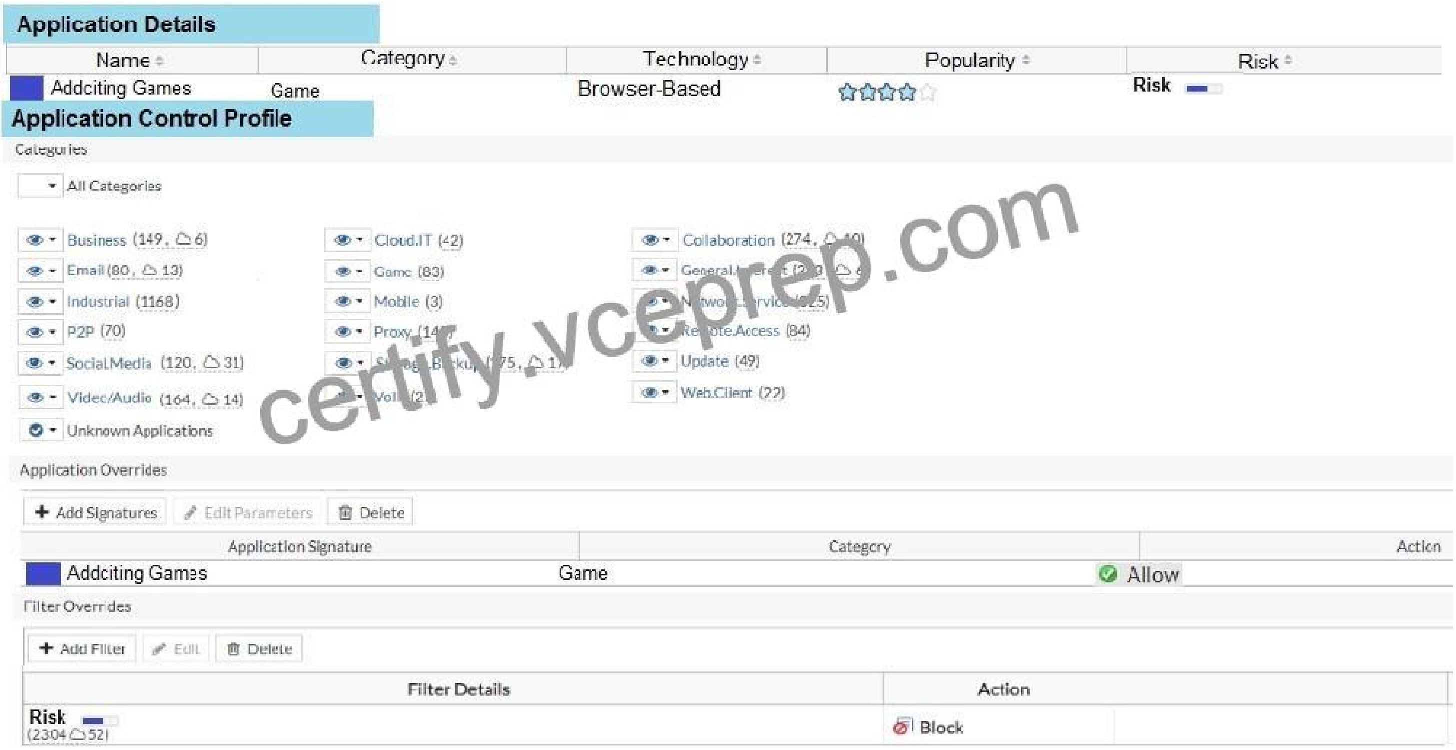
```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
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?
* Social networking web filter category is configured with the action set to authenticate.
* The action on firewall policy ID 1 is set to warning.
* Access to the social networking web filter category was explicitly blocked to all users.
* The name of the firewall policy is all_users_web.

NEW QUESTION 80

View the exhibit. A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting Games). Based on this configuration, which statement is true?



Application Details

Name	Category	Technology	Popularity	Risk
Addciting Games	Game	Browser-Based	★★★★☆	Risk

Application Control Profile

Categories

All Categories

Business (149, 6)	Cloud.IT (42)	Collaboration (274, 10)
Email (80, 13)	Game (83)	General.Interest (2...
Industrial (1168)	Mobile (3)	Network.Service (325)
P2P (70)	Proxy (14...	Remote.Access (84)
SocialMedia (120, 31)	Storage.Backup (175, 1...	Update (49)
Video/Audio (164, 14)	VoIP (2...	Web.Client (22)
Unknown Applications		

Application Overrides

Application Signature	Category	Action
Addciting Games	Game	Allow

Filter Overrides

Filter Details	Action
Risk (2304 52)	Block

- * Addicting.Games is allowed based on the Application Overrides configuration.
- * Addicting.Games is blocked on the Filter Overrides configuration.
- * Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
- * Addcting.Games is allowed based on the Categories configuration.

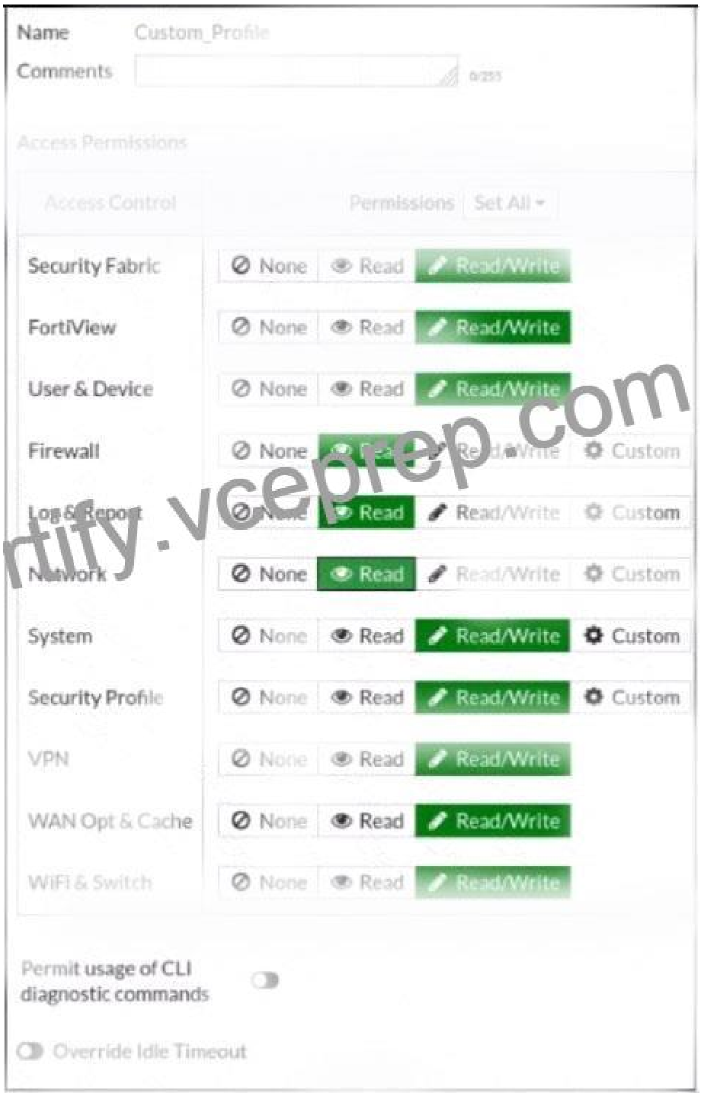
NEW QUESTION 81

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

- * FortiGuard web filter queries
- * PKI
- * Traffic shaping
- * DNS

NEW QUESTION 82

Refer to the exhibit.



Name Custom_Profile
Comments 0/255

Access Permissions

Access Control	Permissions
Security Fabric	None Read [✓ Read/Write]
FortiView	None Read [✓ Read/Write]
User & Device	None Read [✓ Read/Write]
Firewall	None [✓ Read] Read/Write Custom
Log & Report	None [✓ Read] Read/Write Custom
Network	None [✓ Read] Read/Write Custom
System	None Read [✓ Read/Write] Custom
Security Profile	None Read [✓ Read/Write] Custom
VPN	None Read [✓ Read/Write]
WAN Opt & Cache	None Read [✓ Read/Write]
WiFi & Switch	None Read [✓ Read/Write]

Permit usage of CLI diagnostic commands ○

○ Override Idle Timeout

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

- Custom permission for Network
- Read/Write permission for Log & Report
- CLI diagnostics commands permission
- Read/Write permission for Firewall

NEW QUESTION 83

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?
* It always authorizes the traffic without requiring authentication.
* It drops the traffic.
* It authenticates the traffic using the authentication scheme SCHEME2.
* It authenticates the traffic using the authentication scheme SCHEME1.
&#8220;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&#8221;

Fortinet NSE4_FGT-6.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Configure application control to monitor and control network applications- Identify and Configure how firewall policy NAT and central NAT worksTopic 2- Configure FortiGate to act as an implicit and explicit web proxy- Identify FortiGate inspection modes and configure web and DNS filteringTopic 3- Configure IPS,DoS,and WAF to protect the network from hacking and DDoS attacks- Explain and configure antivirus scanning modes to neutralize malware threats
Topic 4- Identify and configure different methods of firewall authentication- Explain FSSO deployment and configurationTopic 5- Configure and route packets using static and policy-based routes- Configure log settings and diagnose problems using the logsTopic 6- Describe and configure VDOMs to split a FortiGate device into multiple virtual devices- Describe and inspect encrypted traffic using certificates

Free NSE4_FGT-6.4 Exam Dumps to Improve Exam Score: https://www.vceprep.com/NSE4_FGT-6.4-latest-vce-prep.html]