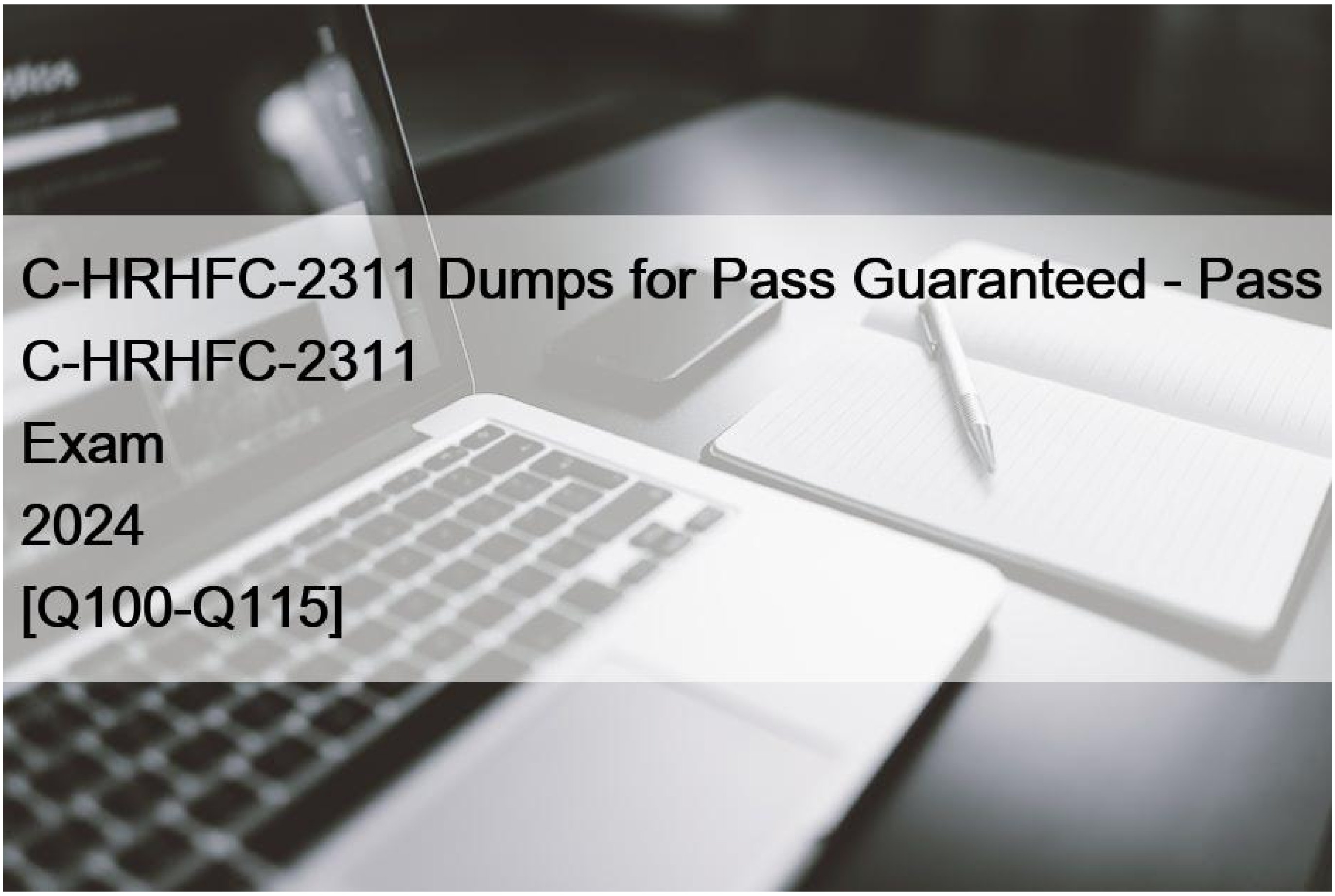
C-HRHFC-2311 Dumps for Pass Guaranteed - Pass C-HRHFC-2311 Exam 2024 [Q100-Q115



C-HRHFC-2311 Dumps for Pass Guaranteed - Pass C-HRHFC-2311 Exam 2024
C-HRHFC-2311 Exam Dumps - Try Best C-HRHFC-2311 Exam Questions from Training Expert VCEPrep

SAP C-HRHFC-2311 Exam Syllabus Topics:

TopicDetailsTopic 1- Cost Center Replication from SAP ERP to SAP SuccessFactors Employee Central- Organizational Data Replication from SAP SuccessFactors Employee Central to SAP ERPTopic 2- Configure settings you make in Customizing to prepare SAP ERP HCM system- Determine when to use the appropriate APITopic 3- Implement and configure the integration of Cost Centers from SAP SuccessFactors and SAP ERP HCM- Introduce the Employee Central based integration scenariosTopic 4- SAP SuccessFactors Employee Central Integration with SAP ERP Scenarios Overview- SAP ERP Employee Data Migration and Replication with SAP SuccessFactors Employee CentralTopic 5- Implement and configure the extensibility of SAP ERP employee data to SAP SuccessFactors- Implement and configure the replication of Employee Central data from SAP SuccessFactors and SAP ERP HCM

NO.100 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?
* The website is exempted from SSL inspection.
* The EICAR test file exceeds the protocol options oversize limit.
* The selected SSL inspection profile has certificate inspection enabled.
* The browser does not trust the FortiGate self-signed CA certificate.
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.

NO.101 Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?
* To remove the NAT operation.
* To generate logs
* To finish any inspection operations.
* To allow for out-of-order packets that could arrive after the FIN/ACK packets.

NO.102 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.

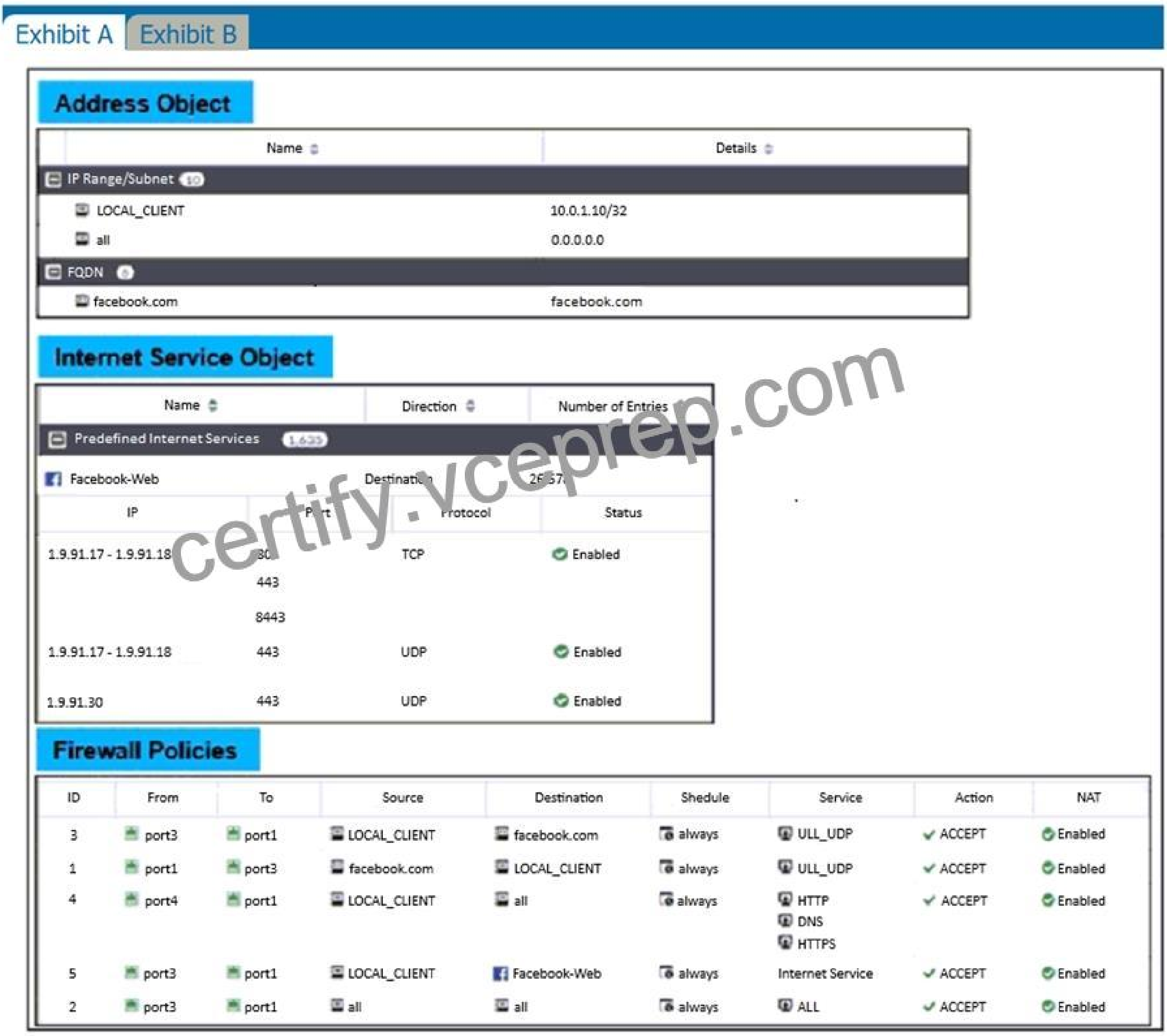


Exhibit A | Exhibit B

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0.0
FQDN 6	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,635		
Facebook-Web	Destination	2657

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

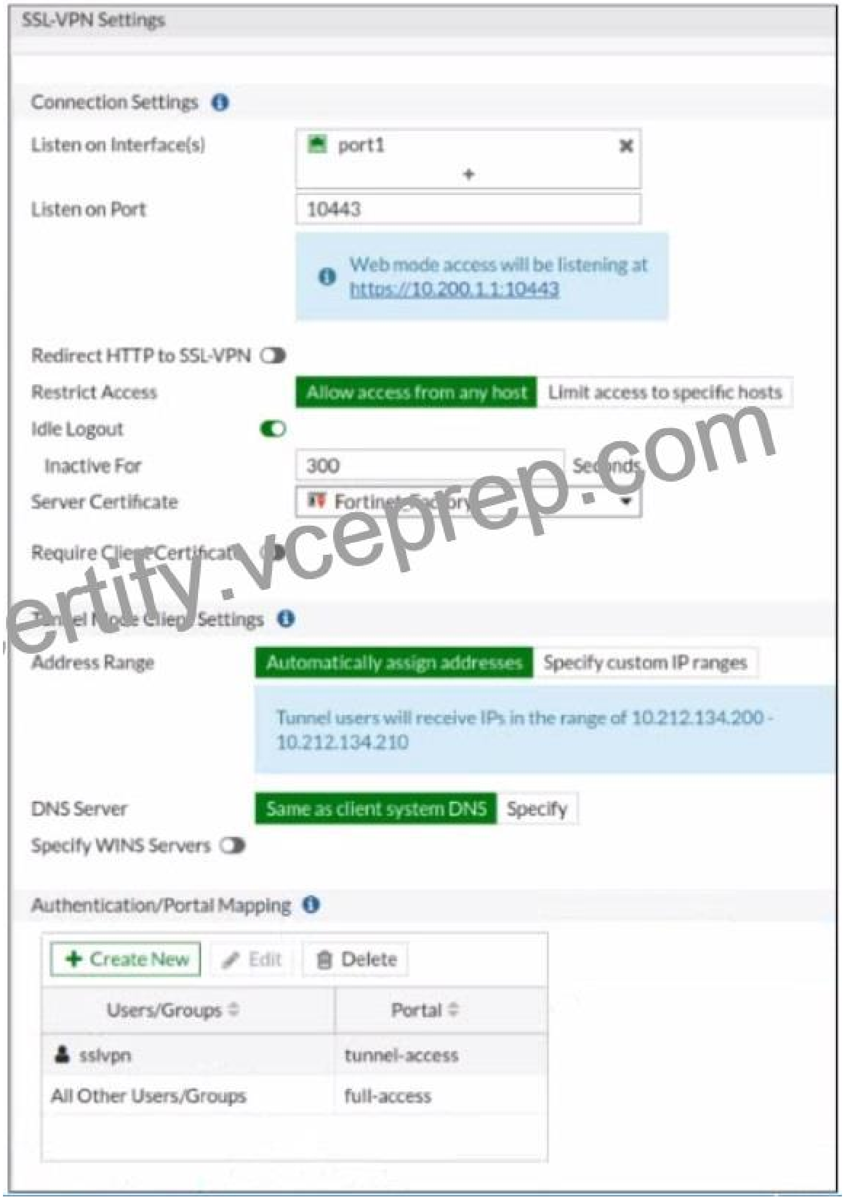
Which policy will be highlighted, based on the input criteria?
* Policy with ID 4.
* Policy with ID 5.
* Policies with ID 2 and 3.
* Policy with ID 4.
Reference:

We are looking for a policy that will allow or deny traffic from the source interface Port3 and source IP address 10.1.1.10 (LOCAL_CLIENT) to facebook.com TCP port 443 (HTTPS). There are only two policies that will match this traffic, policy ID 2 and 5. In FortiGate, firewall policies are evaluated from top to bottom. This means that the first policy that matches the traffic is applied, and subsequent policies are not evaluated. Based on the Policy Lookup criteria, Policy ID 5 will be highlighted

NO.103 Which feature in the Security Fabric takes one or more actions based on event triggers?
* Fabric Connectors

* Automation Stitches
* Security Rating
* Logical Topology

NO.104 Refer to the exhibits.



SSL-VPN Settings

Connection Settings

Listen on Interface(s): port1

Listen on Port: 10443

Web mode access will be listening at https://10.200.1.1:10443

Redirect HTTP to SSL-VPN: off

Restrict Access: Allow access from any host | Limit access to specific hosts

Idle Logout: on

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

Require Client Certificate: off

Tunnel Mode Client Settings

Address Range: Automatically assign addresses | Specify custom IP ranges

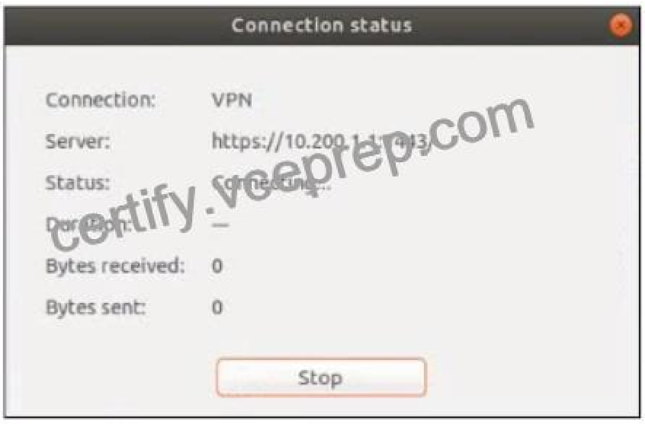
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: Same as client system DNS | Specify

Specify WINS Servers: off

Authentication/Portal Mapping

Users/Groups	Portal
sslvpn	tunnel-access
All Other Users/Groups	full-access



Connection status

Connection: VPN
Server: https://10.200.1.1:443/
Status: Connecting...
Duration: --
Bytes received: 0
Bytes sent: 0

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?
* Change the SSL VPN port on the client.
* Change the Server IP address.
* Change the idle-timeout.
* Change the SSL VPN portal to the tunnel.

NO.105 Which two statements are true about the FGCP protocol? (Choose two.)
* FGCP elects the primary FortiGate device.
* FGCP is not used when FortiGate is in transparent mode.
* FGCP runs only over the heartbeat links.
* FGCP is used to discover FortiGate devices in different HA groups.
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&#8217;s priority, to determine which device should be the primary.

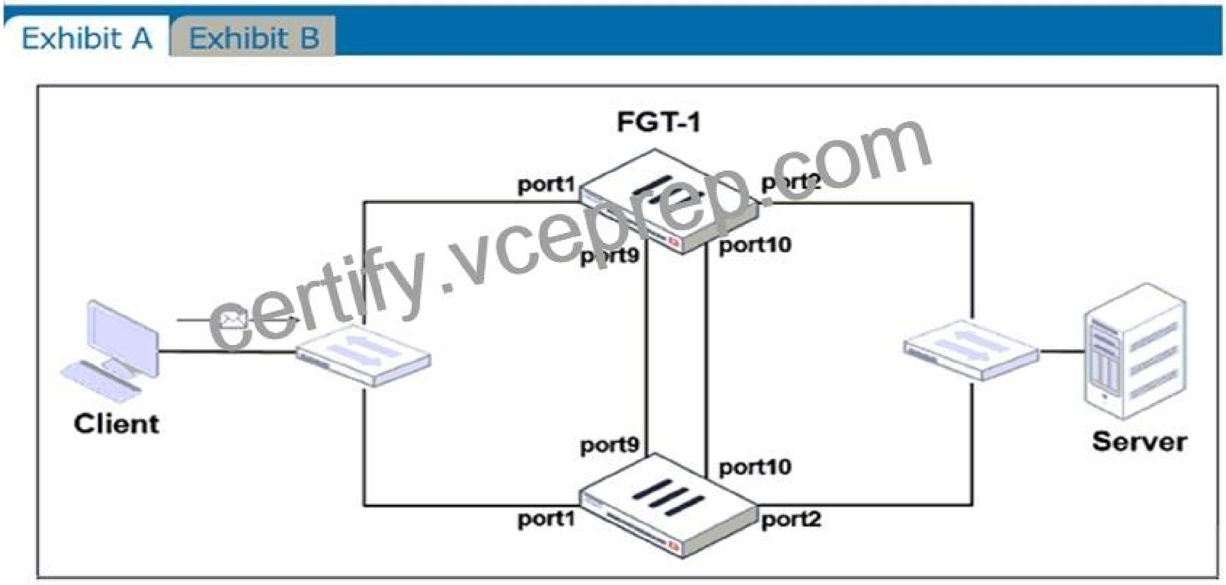
FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices. FGCP does not run over other types of links, such as data links.

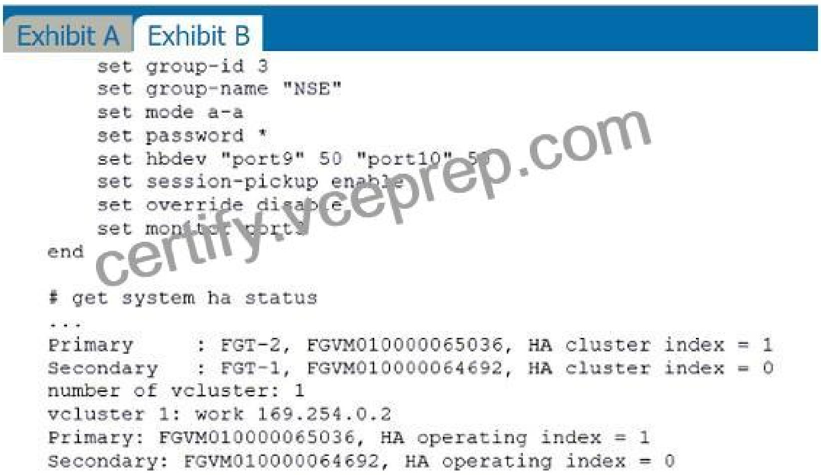
Reference:

https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol FortiGate Infrastructure 7.2 Study Guide (p.292): &#8220;FortiGate HA uses the Fortinet-proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health of members. To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces.&#8221;

NO.106 Refer to the exhibits.

Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.





```
      set group-id 3
      set group-name "NSE"
      set mode a-a
      set password *
      set hbdev "port9" 50 "port10" 50
      set session-pickup enable
      set override disable
      set monitor port3
end

# get system ha status
...
Primary     : FGT-2, FGVM010000065036, HA cluster index = 1
Secondary   : FGT-1, FGVM010000064692, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000065036, HA operating index = 1
Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

* For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.

* The traffic sourced from the client and destined to the server is sent to FGT-1.

* The cluster can load balance ICMP connections to the secondary.

* For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

FortiGate Infrastructure 7.2 Study Guide (p.317 & p.320): &#8220;To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses.&#8221; &#8220;The primary forwards the SYN packet to the selected secondary. (&#8230;) This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic.&#8221;

NO.107 Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true?

(Choose two.)
* Log downloads from the GUI are limited to the current filter view
* Log backups from the CLI cannot be restored to another FortiGate.
* Log backups from the CLI can be configured to upload to FTP as a scheduled time
* Log downloads from the GUI are stored as LZ4 compressed files.

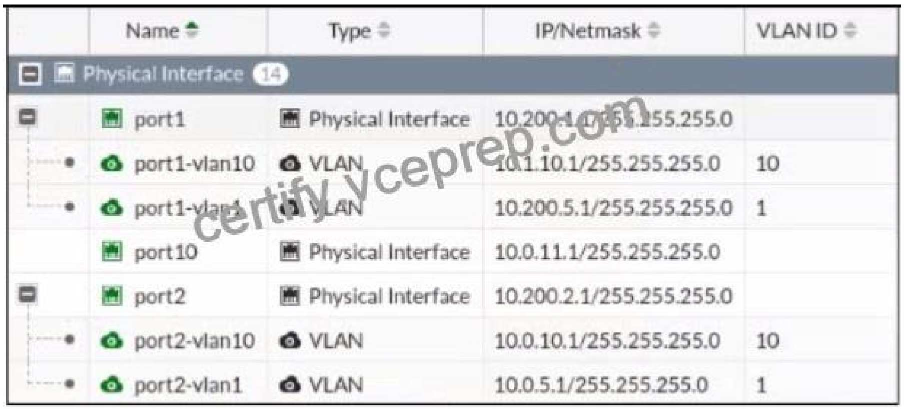
NO.108 Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?
* get system status
* get system performance status
* diagnose sys top
* get system arp

&#8220;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.&#8221;

NO.109 Which statement correctly describes the use of reliable logging on FortiGate?
* Reliable logging is enabled by default in all configuration scenarios.
* Reliable logging is required to encrypt the transmission of logs.
* Reliable logging can be configured only using the CLI.
* Reliable logging prevents the loss of logs when the local disk is full.

FortiGate Security 7.2 Study Guide (p.192): &#8220;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.&#8221;

NO.110 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.)
* Traffic between port2 and port2-vlan1 is allowed by default.
* port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
* port1 is a native VLAN.
* port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf

https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

NO.111 Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)
* FortiGate points the collector agent to use a remote LDAP server.

* FortiGate uses the AD server as the collector agent.
* FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
* FortiGate queries AD by using the LDAP to retrieve user group information.
Fortigate Infrastructure 7.0 Study Guide P.272-273

https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

NO.112 An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?
* The administrator can register the same FortiToken on more than one FortiGate.
* The administrator must use a FortiAuthenticator device
* The administrator can use a third-party radius OTP server.
* The administrator must use the user self-registration server.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-FortiToken-for-multiple-units/ta-p/194435

NO.113 How can you disable RPF checking?
* Disable strict-src-check under system settings.
* Disable src-check on the interface level settings
* Unset fail-alert-interfaces on the interface level settings.
* Disable fail-detect on the interface level settings.

NO.114 An employee needs to connect to the office through a high-latency internet connection.

Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?
* idle-timeout
* login-timeout
* udp-idle-timer
* session-ttl
FortiGate Infrastructure 7.2 Study Guide (p.222):

&#8220;When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under config vpn ssl settings have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections.&#8221;

NO.115 Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?
* VDOMs without ports with connected devices are not displayed in the topology.
* Downstream devices can connect to the upstream device from any of their VDOMs.
* Security rating reports can be run individually for each configured VDOM.
* Each VDOM in the environment can be part of a different Security Fabric.
FortiGate Security 7.2 Study Guide (p.436): &#8220;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.&#8221;

Latest 100% Passing Guarantee - Brilliant C-HRHFC-2311 Exam Questions PDF:
https://www.vceprep.com/C-HRHFC-2311-latest-vce-prep.html]