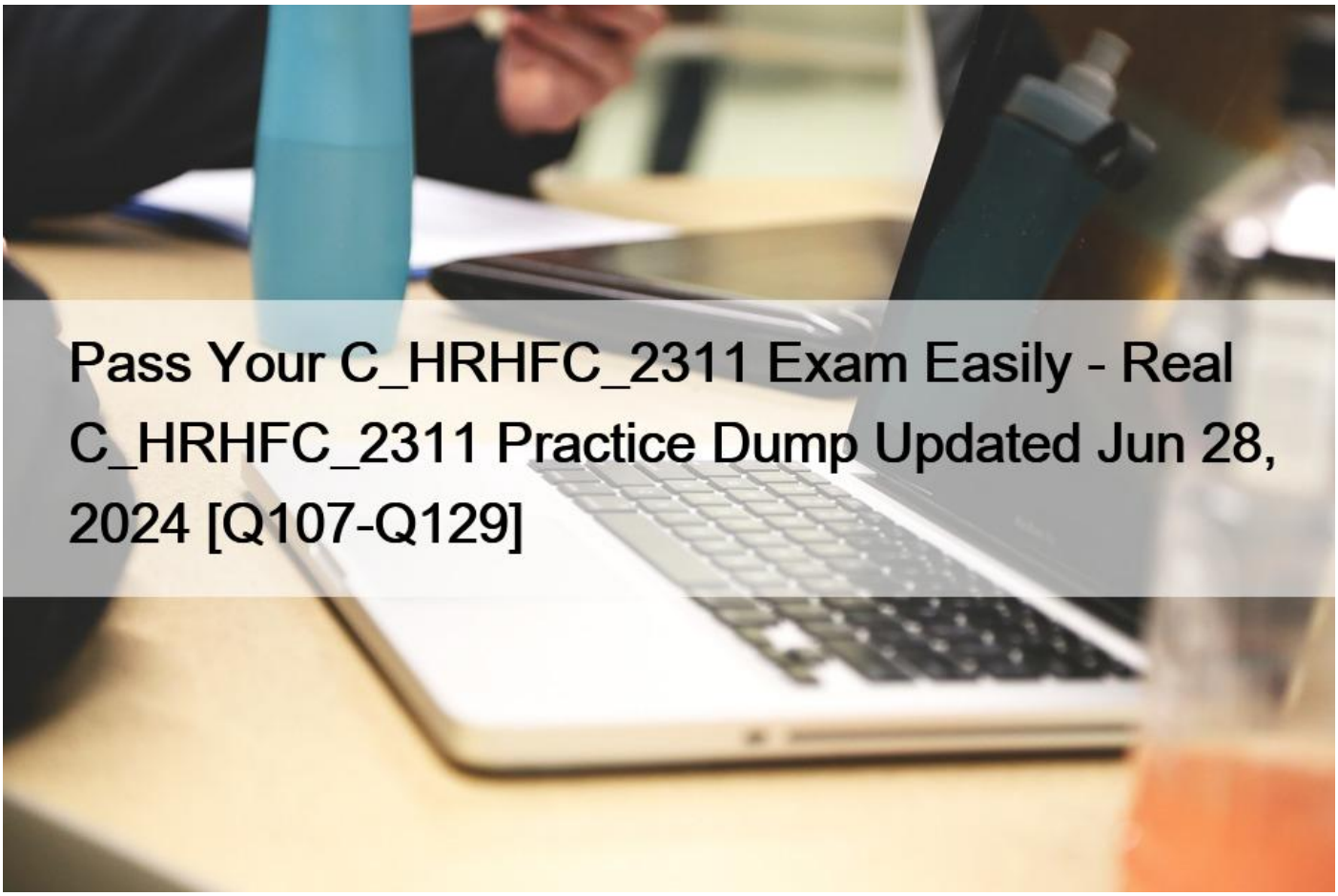
Pass Your C_HRHFC_2311 Exam Easily - Real C_HRHFC_2311 Practice Dump Updated Jun 28, 2024 [Q107-Q129



Pass Your C_HRHFC_2311 Exam Easily - Real C_HRHFC_2311 Practice Dump Updated Jun 28, 2024
2024 Realistic Verified Free SAP C_HRHFC_2311 Exam Questions

Q107. Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?
* Subject Key Identifier value
* SMMIE Capabilities value
* Subject value
* Subject Alternative Name value

Q108. 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.

Q109. The IPS engine is used by which three security features? (Choose three.)
* Antivirus in flow-based inspection

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

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.”

Q110. 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?

* Static IP Address
* Dialup User
* Dynamic DNS
* Pre-shared Key

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

Q111. 51 Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

* The security actions applied on the web applications will also be explicitly applied on the third-party websites.
* The application signature database inspects traffic only from the original web application server.
* FortiGuard maintains only one signature of each web application that is unique.
* FortiGate can inspect sub-application traffic regardless where it was originated.

Reference:

https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300_System/303d_FortiG

Q112. Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

* Proxy-based inspection
* Certificate inspection
* Flow-based inspection
* Full Content inspection

Q113. Refer to the exhibit.

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

https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220

Q114. Refer to the exhibits.

Exhibit A

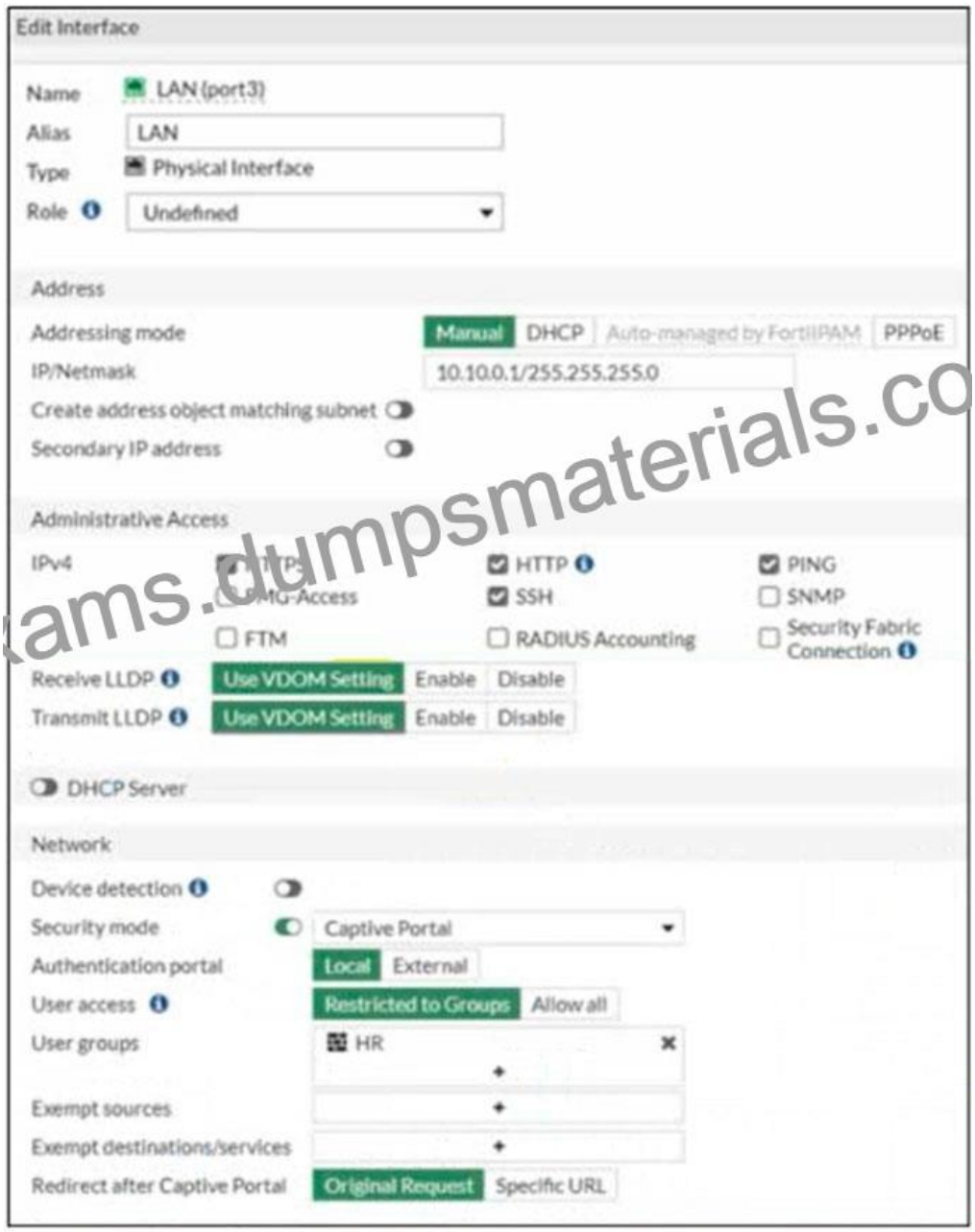
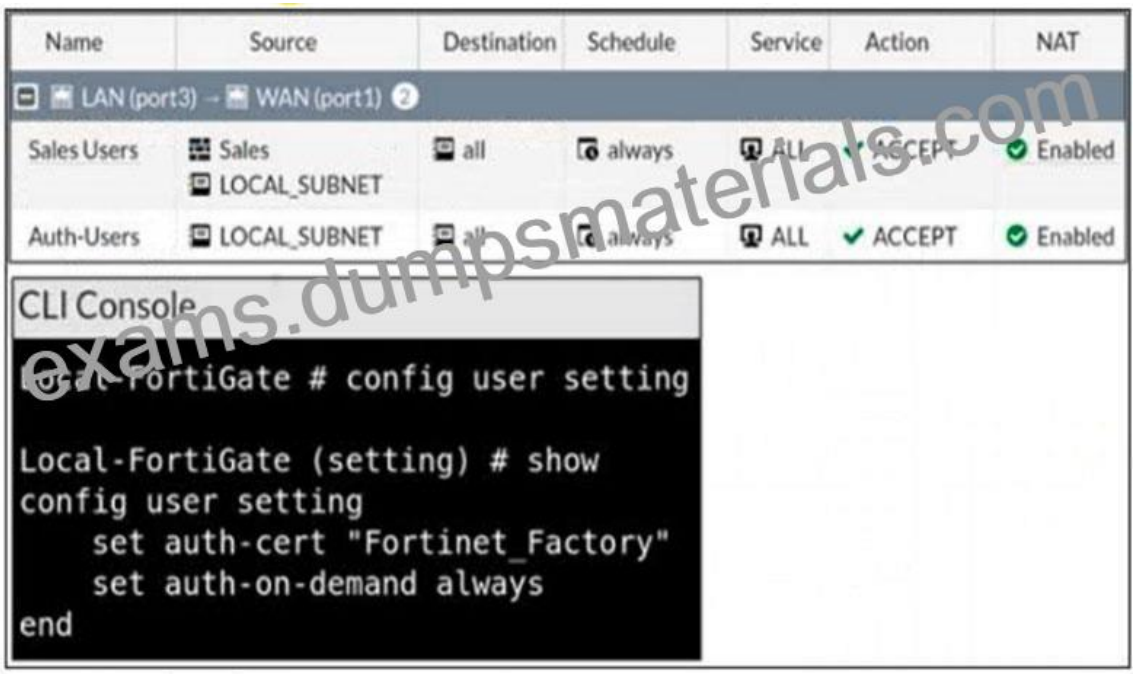

Edit Interface
Name
LAN (port3)
Alias
LAN
Type
Physical Interface
Role
Undefined
Address
Addressing mode
Manual
DHCP
Auto-managed by FortiIPAM
PPPoE
IP/Netmask
10.10.0.1/255.255.255.0
Create address object matching subnet
Secondary IP address
Administrative Access
IPv4
HTTP
PING
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
Receive LLDP
Use VDOM Setting
Enable
Disable
Transmit LLDP
Use VDOM Setting
Enable
Disable
DHCP Server
Network
Device detection
Security mode
Captive Portal
Authentication portal
Local
External
User access
Restricted to Groups
Allow all
User groups
HR
Exempt sources
Exempt destinations/services
Redirect after Captive Portal
Original Request
Specific URL

Exhibit B



The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration.

How will FortiGate handle user authentication for traffic that arrives on the LAN interface?
* If there is a fall-through policy in place, users will not be prompted for authentication.
* Authentication is enforced at a policy level; all users will be prompted for authentication.
* All users will be prompted for authentication, users from the Sales group can authenticate successfully with the correct credentials.
* All users will be prompted for authentication, users from the HR group can authenticate successfully with the correct credentials.

Q115. Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)
* System time
* FortiGuaid update servers
* Operating mode
* NGFW mode

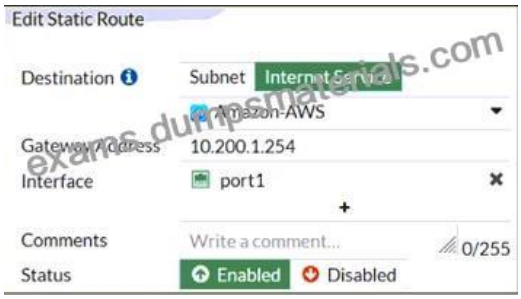
C: “Operating mode is per-VDOM setting. You can combine transparent mode VDOM’s with NAT mode VDOMs on the same physical Fortigate.

D: “Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM”
Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

Q116. Which three statements are true regarding session-based authentication? (Choose three.)
* HTTP sessions are treated as a single user.
* IP sessions from the same source IP address are treated as a single user.
* It can differentiate among multiple clients behind the same source IP address.
* It requires more resources.
* It is not recommended if multiple users are behind the source NAT

Q117. 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?
* get router info routing-table database
* diagnose firewall proute list
* get internet-service route list
* get router info routing-table all
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/198756 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.”

Q118. An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)
* Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
* Create a new service object for HTTP service and set the session TTL to never
* Set the TTL value to never under config system-ttl
* Set the session TTL on the HTTP policy to maximum

Q119. Which two statements are true when FortiGate is in transparent mode? (Choose two.)
* By default, all interfaces are part of the same broadcast domain.
* The existing network IP schema must be changed when installing a transparent mode.
* Static routes are required to allow traffic to the next hop.
* FortiGate forwards frames without changing the MAC address.
Reference:

attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

Q120. An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?
* Configure Source IP Pools.
* Configure split tunneling in tunnel mode.
* Configure different SSL VPN realms.
* Configure host check .

Q121. 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?
* The matching firewall policy is set to proxy inspection mode.
* The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
* The full SSL inspection feature does not have a valid license.
* The browser does not trust the certificate used by FortiGate for SSL inspection.

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.”

Q122. What is a reason for triggering IPS fail open?
* The IPS socket buffer is full and the IPS engine cannot process additional packets.
* The IPS engine cannot decode a packet.
* The IPS engine is upgraded.
* The administrator enabled NTurbo acceleration.

Q123. Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)
* SSH
* HTTPS
* FTM
* FortiTelemetry

Reference:

https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios

Q124. 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.)
* diagnose sys top
* execute ping
* execute traceroute
* diagnose sniffer packet any
* get system arp

Q125. FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.

In this scenario, what are two requirements for the VLAN ID? (Choose two.)
* The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
* The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.
* The two VLAN subinterfaces must have different VLAN IDs.
* The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-emac-vlan-to-share-the-same-VLAN/ta-p/192843?externalID=FD43883 When FortiGate is operating in NAT mode, it means that it uses network address translation (NAT) to modify the source or destination IP addresses of the traffic passing through it1. NAT mode allows FortiGate to hide the IP addresses of the internal network from the external network, and to conserve IP addresses by using a single public IP address for multiple private IP addresses1.

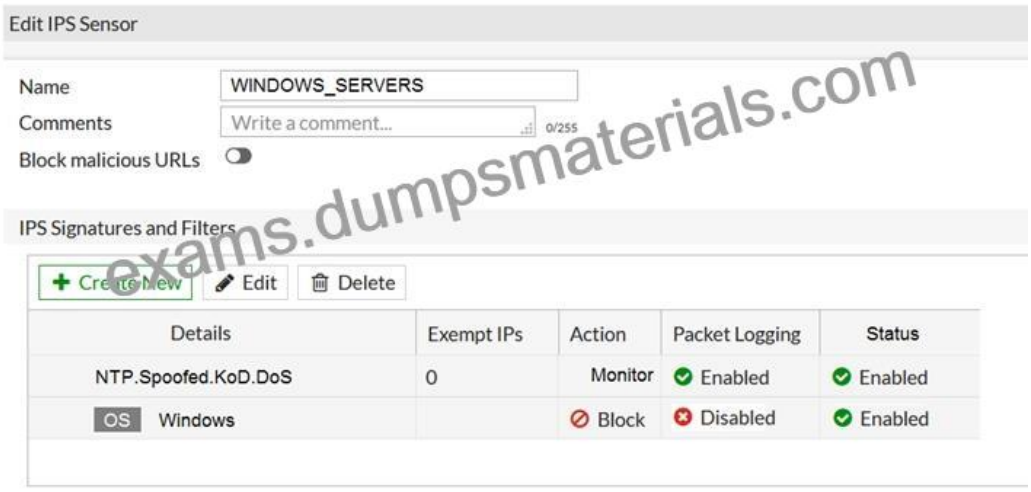
A virtual LAN (VLAN) subinterface is a logical interface that allows traffic from different VLANs to enter and exit the FortiGate unit2. A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface2. A VLAN ID is a numerical identifier that distinguishes one VLAN from another2.

In this scenario, there are two requirements for the VLAN ID of the VLAN subinterfaces added to the same physical interface:

The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs2. If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish the traffic from each other, and they will not be able to forward the traffic to the correct destination.

The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs. This is because VDOMs are virtual instances of FortiGate that can have their own interfaces, policies, and routing tables3. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs3. However, this requires inter-VDOM links to allow traffic between different VDOMs3.

Q126. 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.)
* The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
* The sensor will block all attacks aimed at Windows servers.
* The sensor will reset all connections that match these signatures.
* The sensor will gather a packet log for all matched traffic.

Q127. What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?
* It limits the scope of application control to the browser-based technology category only.
* It limits the scope of application control to scan application traffic based on application category only.
* It limits the scope of application control to scan application traffic using parent signatures only
* It limits the scope of application control to scan application traffic on DNS protocol only.

Q128. 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.)
* Antivirus scanning
* File filter
* DNS filter
* Intrusion prevention

Q129. Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)
* Warning
* Exempt
* Allow
* Learn

C_HRHFC_2311 Real Exam Questions and Answers FREE:
https://www.dumpsmaterials.com/C_HRHFC_2311-real-torrent.html]