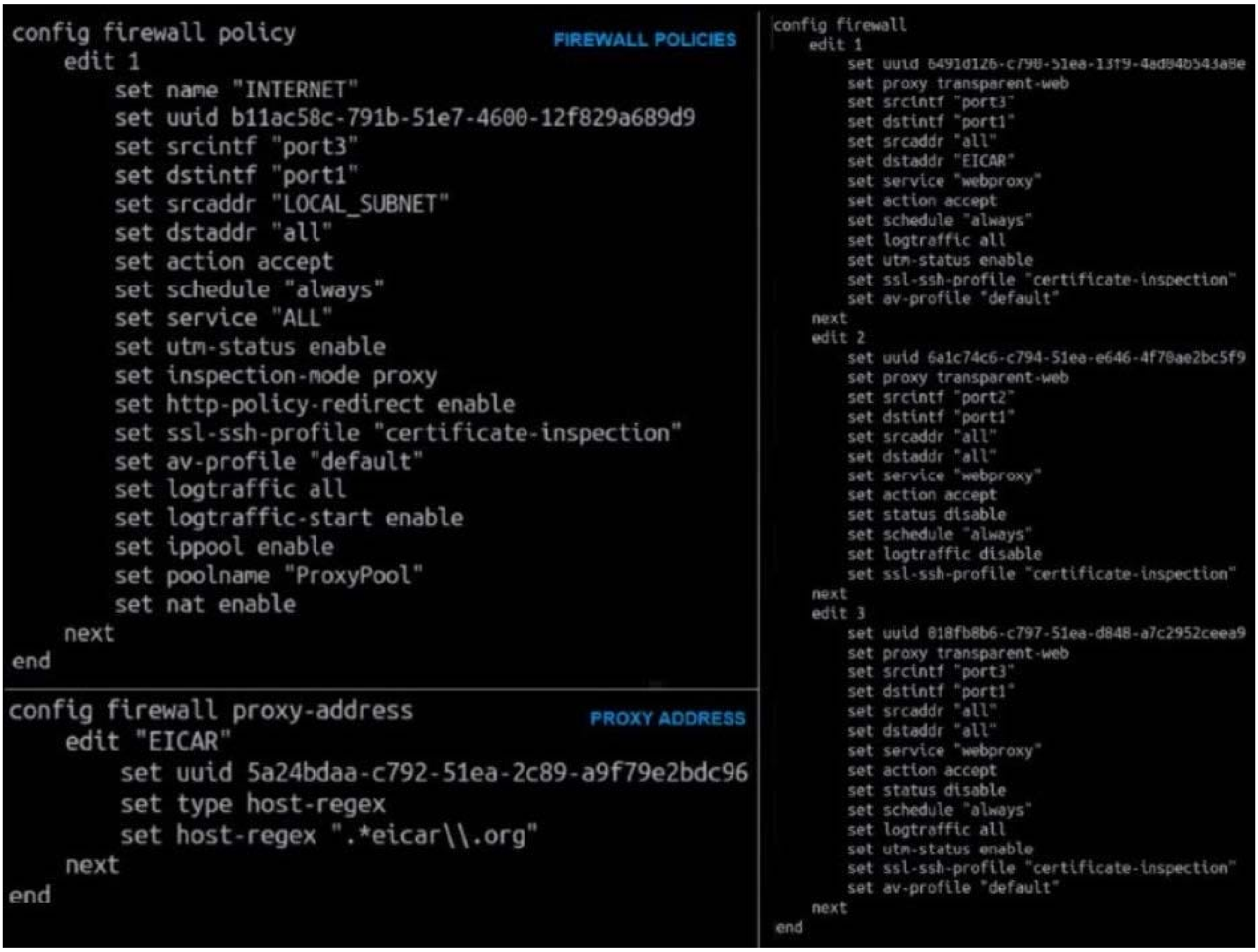
NSE4_FGT-6.4$^{\text{Q\&As}}$

Fortinet NSE 4 - FortiOS 6.4

Pass Fortinet NSE4_FGT-6.4 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit.



```
config firewall policy
    edit 1
        set name "INTERNET"
        set uuid b11ac58c-791b-51e7-4600-12f829a689d9
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "LOCAL_SUBNET"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set http-policy-redirect enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set logtraffic all
        set logtraffic-start enable
        set ippool enable
        set poolname "ProxyPool"
        set nat enable
    next
end
```

```
config firewall proxy-address
    edit "EICAR"
        set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96
        set type host-regex
        set host-regex ".*eicar\\.org"
    next
end
```

```
config firewall
    edit 1
        set uuid 6491d126-c798-51ea-13f9-4ad94b543a8e
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "EICAR"
        set service "webproxy"
        set action accept
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
    next
    edit 2
        set uuid 6a1c74c6-c794-51ea-e646-4f70ae2bc5f9
        set proxy transparent-web
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set status disable
        set schedule "always"
        set logtraffic disable
        set ssl-ssh-profile "certificate-inspection"
    next
    edit 3
        set uuid 818fb8b6-c797-51ea-d848-a7c2952ceea9
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set status disable
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
    next
end
```

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.

How does FortiGate process the traffic sent to http://www.fortinet.com?

A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.

B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.

C. Traffic will be redirected to the transparent proxy and It will be allowed by proxy policy ID 1.

D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Correct Answer: D

QUESTION 2

Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.

B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.

D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Correct Answer: BC

QUESTION 3

Which two statements are true about collector agent standard access mode? (Choose two.)

A. Standard mode uses Windows convention-NetBios: Domain\Username.

B. Standard mode security profiles apply to organizational units (OU).

C. Standard mode security profiles apply to user groups.

D. Standard access mode supports nested groups.

Correct Answer: AC

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso

QUESTION 4

Consider the topology:

Application on a Windows machine FGT--> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.

The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

A. Set the maximum session TTL value for the TELNET service object.

B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.

C. Create a new service object for TELNET and set the maximum session TTL.

D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Correct Answer: CD

QUESTION 5

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 browser requires a software update.

B. FortiGate does not support full SSL inspection when web filtering is enabled.

C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.

D. There are network connectivity issues.

Correct Answer: C

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394