Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

Fortinet

NSE4_FGT-7.0

Fortinet NSE 40 - FortiOS 7.0

Question: 60

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 override for the home page? (Choose two.)
A. www.exaple.com
B. www.example.com/index.html
C. example.com
D. www.example.com:443

Answer: A,C

Explanation:

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names" "no URLs or wildcard characters are allowed".

Question: 61

Which two statements about SSL VPN between two FortiGate devices are true? (Choose two.)
A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
B. The client FortiGate requires a manually added route to remote subnets.
C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VP
E. Server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Answer: C,D

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/266506/ssl-vpn-with-certificateauthentication

Question: 62

Which two statements are true about the Security Fabric rating? (Choose two.)
A. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.
B. Many of the security issues can be fixed immediately by clicking Apply where available.
C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
D. It provides executive summaries of the four largest areas of security focus.

Answer: B,C

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/292634/security-rating
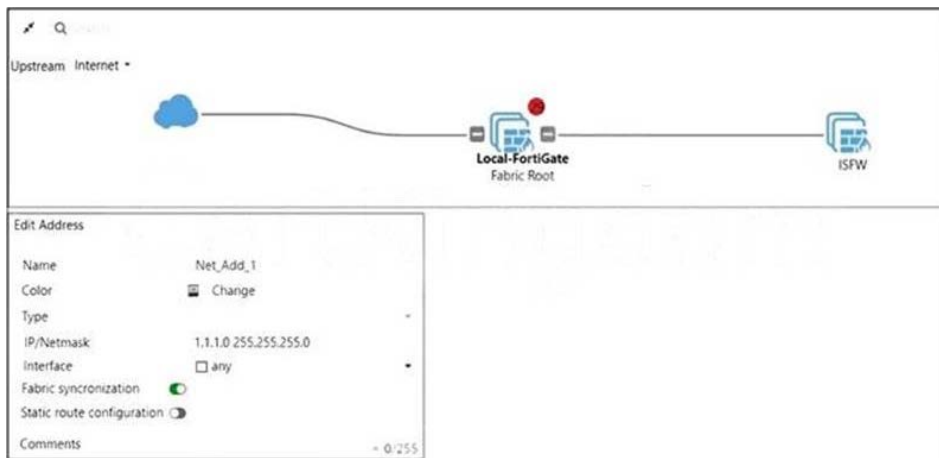
Question: 63

Refer to the exhibits.

Exhibit A.

Exhibit B.

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric.

After synchronization, this object is not available on the downstream FortiGate (ISFW).

What must the administrator do to synchronize the address object?

A. Change the csf setting on Local-FortiGate (root) to set configuration-sync local.

B. Change the csf setting on ISFW (downstream) to set configuration-sync local.

C. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

D. Change the csf setting on ISFW (downstream) to set fabric-object-unification default.

Answer: A

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD43820

Question: 64

Refer to the exhibit.

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. Enable two-factor authentication
B. Change Administrator profile
C. Change password
D. Enable restrict access to trusted hosts.

Answer: B

Explanation:

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

Question: 65

Refer to the exhibit.

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

The override setting is enable for the FortiGate with SN FGVM010000064692.

Which two statements are true? (Choose two.)
A. FortiGate SN FGVM010000065036 HA uptime has been reset.
B. FortiGate devices are not in sync because one device is down.
C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
D. FortiGate SN FGVM010000064692 has the higher HA priority.

Answer: A,D

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-withoverride-disabled-default
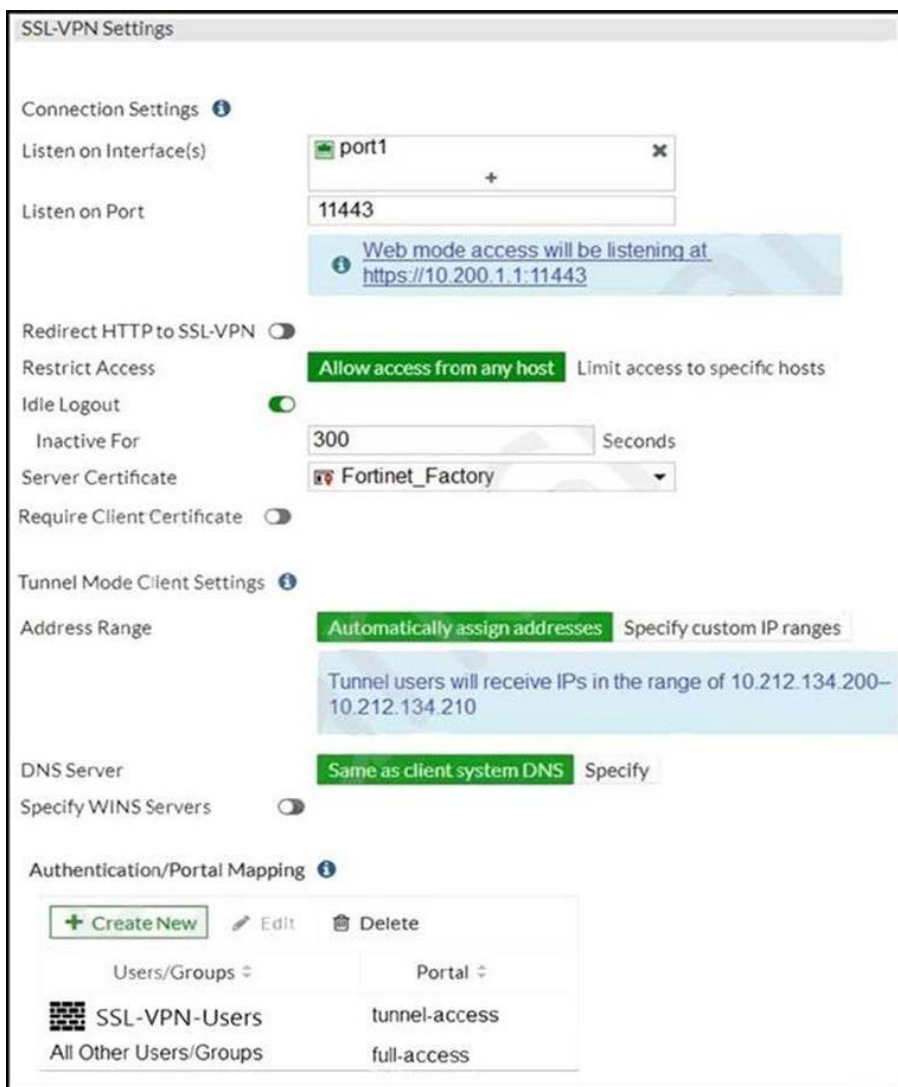
Question: 66

Refer to the exhibits.

Exhibit A.

SSL-VPN Settings

Connection Settings ℹ️

Listen on Interface(s)   📇 port1   ✕
                                           +

Listen on Port   11443

                                ℹ️ Web mode access will be listening at
                                   https://10.200.1.1:11443

Redirect HTTP to SSL-VPN ◯

Restrict Access   [Allow access from any host] Limit access to specific hosts

Idle Logout   ◉

   Inactive For   300   Seconds

Server Certificate   🔐 Fortinet_Factory   ▼

Require Client Certificate ◯

Tunnel Mode Client Settings ℹ️

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   ◯

Authentication/Portal Mapping ℹ️

  [+ Create New]   ✏️ Edit   🗑️ Delete

   Users/Groups ⇅   Portal ⇅

   ▦ SSL-VPN-Users   tunnel-access
   All Other Users/Groups   full-access

Exhibit B.

Connection status   ⊗

Connection: VPN

Server: https://10.200.1.1:1443/

Status: Connecting...

Duration: —

Bytes received: 0

Bytes sent: 0

              [Stop]

The SSL VPN connection fails when a user attempts to connect to it.

What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.

B. Change the Server IP address.

C. Change the idle-timeout.

D. Change the Server IP address.

Answer: A

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494

Question: 67

Refer to the exhibits.

Exhibit A shows system performance output.

Exhibit B shows s FortiGate configured with the default configuration of high memory usage thresholds.

Based on the system performance output, which two statements are correct? (Choose two.)
A. FortiGate will start sending all files to FortiSandbox for inspection.
B. FortiGate has entered conserve mode.
C. Administrators cannot change the configuration.
D. Administrators can access FortiGate only through the condole port.

Answer: B,C

Explanation:

Reference: https://www.skillfulist.com/fortigate/fortigate-conserve-mode-how-to-stop-it-and-what-it-means/

Question: 68

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?
A. NetAPI polling can increase bandwidth usage in large networks.
B. The NetSessionEnum function is used to track user logouts.
C. The collector agent must search security event logs.
D. The collector agent uses a Windows API to query DCs for user logins.

Answer: B

Explanation:

Reference: https://kb.fortinet.com/kb/microsites/search.do?
cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=210966035&stateId=1%200%20210968009%27)

Question: 69

Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000    4500 003c 2f8f 0000 8001 f020 0a00 0102        E..</..........
0x0010    0808 0808 0800 4d5a 0001 0001 6162 6364        ......MZ....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000    4500 003c 2f8f 0000 7f01 0106 0a38 f0e4        E..</........8..
0x0010    0808 0808 0800 6159 ec01 0001 6162 6364        ......aY....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000    4500 003c 0000 0000 7501 3a95 0808 0808        E..<....u.:.....
0x0010    0a38 f0e4 0000 6965 ec01 0001 6162 6364        .8....iY....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000    4500 003c 0000 0000 7401 2bb0 0808 0808        E..<....t.+.....
0x0010    0a00 0102 0000 555a 0001 0001 6162 6364        ......UZ....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)
A. Interface name
B. IP header
C. Application header
D. Packet payload
E. Ethernet header

Answer: A,B,D

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=11186

Question: 70

An administrator does not want to report the logon events of service accounts to FortiGate.

What setting on the collector agent is required to achieve this?
A. Add user accounts to the Ignore User List.
B. Add the support of NTLM authentication.
C. Add user accounts to the FortiGate group filter.
D. Add user accounts to Active Directory (AD).

Answer: A

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.