



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



NSE4_FGT-7.0 MCQs
NSE4_FGT-7.0 TestPrep
NSE4_FGT-7.0 Study Guide
NSE4_FGT-7.0 Practice Test
NSE4_FGT-7.0 Exam Questions



Fortinet

NSE4_FGT-7.0

Fortinet NSE 40 - FortiOS 7.0



https://killexams.com/pass4sure/exam-detail/NSE4_FGT-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.

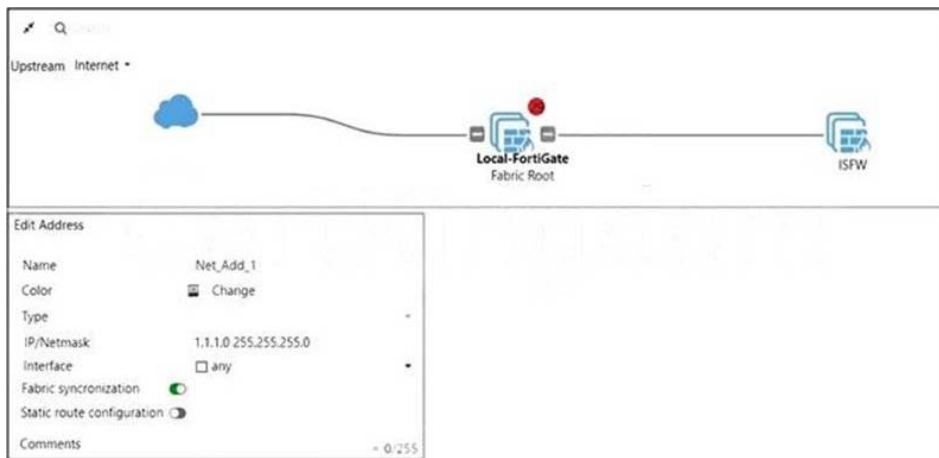


Exhibit B.

```
Local-FortiGate # show full-configuration system csf
config system csf
  set status enable
  set upstream-ip 0.0.0.0
  set upstream-port 8013
  set group-name "fortinet"
  set group-password ENC X18CLzrcUBUq9yz9nryP+YfM16
  set accept-auth-by-cert enable
  set log-unification enable
  set authorization-request-type serial
  set fabric-workers 2
  set downstream-access disable
  set configuration-sync default
  set fabric-object-unification local
  set saml-configuration-sync default
end

ISFW # show full-configuration system csf
config system csf
  set status enable
  set upstream-ip 10.0.1.254
  set upstream-port 8013
  set group-name ""
  set accept-auth-by-cert enable
  set log-unification enable
  set authorization-request-type serial
  set fabric-workers 2
  set downstream-access disable
  set configuration-sync default
  set saml-configuration-sync default
end

ISFW #
ISFW #
```

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?

- Change the csf setting on Local-FortiGate (root) to set configuration-sync local.
- Change the csf setting on ISFW (downstream) to set configuration-sync local.
- Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.
- 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 screenshot shows the 'Administrator' user configuration page. The 'Username' is 'Administrator' and the 'Type' is 'Local User'. A dropdown menu for 'Type' is open, showing options: 'Local User' (selected), 'Match a user on a remote server group', 'Match all users in a remote server group', and 'Use public key infrastructure (PKI) group'. Below this, there is a 'Comments' field with the text 'Write a comment' and a character count '0/255'. The 'Administrator profile' is set to 'prof_admin'. At the bottom, there are three toggle switches: 'Two-factor Authentication' (disabled), 'Restrict login to trusted hosts' (disabled), and 'Restrict admin to guest account provisioning only' (disabled).

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.

```
vcluster nr-1
vcluster 0: start_time-1593701574(2021-06-02 10:59:34), state/o/chg_time-2(work)/2(work)/1593701169(2021-06-02 10:46:09)
pingsvr flip timeout/expire-3600s/2781s 2021-06-02
'FGVM010000064692': ha prio/o-1/1, link failure-0, p.ngsvr failure-0, flag-0x00000000, uptime/reset crt-198/0
'FGVM010000065036': ha prio/o-0/0, link failure-0, p.ngsvr failure-0, flag-0x00000001, uptime/reset crt-0/1
```

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 ⓘ

Listen on Interface(s)

Listen on Port

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 Seconds

Server Certificate

Require Client Certificate ☐

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 ☐

Authentication/Portal Mapping ⓘ

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

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.

```
! get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 81 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```

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

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

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 console 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?](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))

[cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=210966035&stateId=1%200%20210968009%27\)](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>

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Exam Questions:

Killexams.com provides 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 questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

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

Practice Test:

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

Guaranteed Success:

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

Updated Contents:

Killexams.com regularly updates its question bank of MCQs 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.