Fortinet.Premium.NSE4_FGT-7.0.30q - DEMOq

Number: NSE4_FGT-7.0
Passing Score: 800
Time Limit: 120 min

Exam Code: NSE4_FGT-7.0
Exam Name: Fortinet NSE 4 - FortiOS 7.0
Website: https://VCEup.com/
Free Exam: https://vceup.com/NSE4-FGT-7-0/

VCEûp

QUESTION 1
Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

A. FortiGate uses the AD server as the collector agent.
B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
C. FortiGate does not support workstation check.
D. FortiGate directs the collector agent to use a remote LDAP server.

Correct Answer: BD
Section: (none)
Explanation

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

QUESTION 2
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 for the home page? (Choose two.)

A. www.example.com:443
B. www.example.com
C. example.com
D. www.example.com/index.html

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiGate_Security_6.4 page 384
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 3
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

VCEûp

Exhibit A

VCEûp

VCEûp

Exhibit B

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The firewall policy performs the full content inspection on the file.
B. The flow-based inspection is used, which resets the last packet to the user.
C. The volume of traffic being inspected is too high for this model of FortiGate.
D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
• "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
• When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

QUESTION 4
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

VCEUp

A. FortiCache
B. FortiSIEM
C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-andreporting-overview

QUESTION 5
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent must search security event logs.
D. The NetSession Enum function is used to track user logouts.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD34906
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 6
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 6959 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. Ethernet header
C. IP header

VCEûp

D. Application header
E. Packet payload

Correct Answer: ACE
Section: (none)
Explanation

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

QUESTION 7
Refer to the exhibit.


```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check.
Which interface will be selected as an outgoing interface?

A. port2
B. port4
C. port3
D. port1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Port 1 shows the lowest latency.

QUESTION 8
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 the support of NTLM authentication.
B. Add user accounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

VCEup

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 9
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. Change password
B. Enable restrict access to trusted hosts
C. Change Administrator profile
D. Enable two-factor authentication

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 10
An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

A. Policy lookup will be disabled.
B. By Sequence view will be disabled.
C. Search option will be disabled
D. Interface Pair view will be disabled.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821

VCEûp

QUESTION 11
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.)

A. Traffic between port2 and port2-vlan1 is allowed by default.
B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
C. port1 is a native VLAN.
D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interface/ta-p/197640?externalID=FD31639
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

QUESTION 12
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
* All traffic must be routed through the primary tunnel when both tunnels are up * The secondary tunnel must be used only if the primary tunnel goes down * In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover Which two key configuration changes are needed on FortiGate to meet the design requirements?
(Choose two,)

A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
B. Enable Dead Peer Detection.
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B - because the customer requires the tunnels to notify when a tunnel goes down. DPD is designed for that purpose. To send a packet over a firewall to determine a failover for the next tunnel after a specific amount of time of not receiving a response from its peer.
C - remember when it comes to choosing a route with regards to Administrative Distance. The route with the lowest distance for that particular route will be chosen. So, by configuring a lower routing distance on the primary tunnel, means that the primary tunnel will be chosen to route packets towards their destination.

QUESTION 13
Refer to the exhibit.

VCEûp

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
    pingsvr_flip_timeout/expire=3600s/2781s
    'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
    'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
1. Override is disable by default - OK
2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary" The question here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-withoverride-disabled-default

QUESTION 14
Refer to the exhibits.

Exhibit A

```
# 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: 83 / 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
```

VCEûp

Exhibit A Exhibit B

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

Exhibit A shows system performance output. Exhibit B shows a 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. Administrators can access FortiGate only through the console port.
B. FortiGate has entered conserve mode.
C. FortiGate will start sending all files to FortiSandbox for inspection.
D. Administrators cannot change the configuration.

Correct Answer: BD
Section: (none)
Explanation

VCEûp

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

QUESTION 15
An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192.168.1.0/24
B. 192.168.0.0/24
C. 192.168.2.0/24
D. 192.168.3.0/24

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Refer to the exhibits.

VCEûp

VCEûp

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 SSL VPN portal to the tunnel.

VCEûp

VCEûp

Correct Answer: A
Section: (none)
Explanation

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

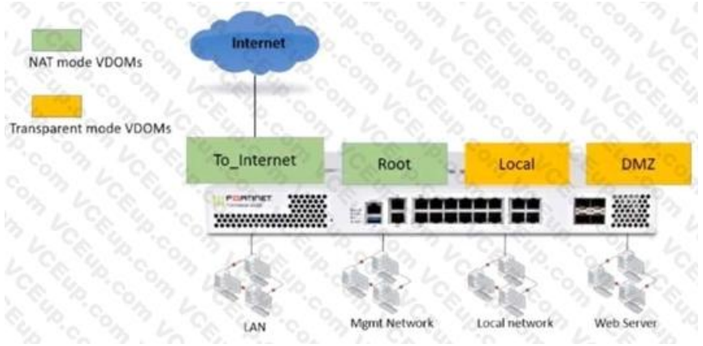
QUESTION 17
Which two statements about SSL VPN between two FortiGate devices are true? (Choose two.)

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 VPN.
D. Server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Correct Answer: CD
Section: (none)
Explanation

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

QUESTION 18
Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542

QUESTION 19
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 X18CtzrcUBUq9yz9nryP+YfM16
BJkv7S/trtoh2gYAe5CH8YMAa0GT10aX+/dKH/o5izw1ZEoN1QN2N
FGLT4r5z2AyYI8i1PxutlLcaCp1AdZadv1CxDe66IdLX7I6o22J9P
    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
```

```
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?

A. Change the csf setting on Local-FortiGate (root) to sec configuration-sync local.
B. Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
C. Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion defaulc.
D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaulc.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 20
Refer to the exhibit.

```
STUDENT # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT       DESTINATION      DESTINATION-NAT
tcp     3598   10.0.1.10:2706  10.200.1.6:2706  10.200.1.254:80  -
tcp     3598   10.0.1.10:2704  10.200.1.6:2704  10.200.1.254:80  -
tcp     3596   10.0.1.10:2702  10.200.1.6:2702  10.200.1.254:80  -
tcp     3599   10.0.1.10:2700  10.200.1.6:2700  10.200.1.254:443 -
tcp     3599   10.0.1.10:2698  10.200.1.6:2698  10.200.1.254:80  -
tcp     3598   10.0.1.10:2696  10.200.1.6:2696  10.200.1.254:443 -
udp     174    10.0.1.10:2694  -                  10.0.1.254:53  -
udp     173    10.0.1.10:2690  -                  10.0.1.254:53  -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

VCEUp

A. Destination NAT is disabled in the firewall policy.
B. One-to-one NAT IP pool is used in the firewall policy.
C. Overload NAT IP pool is used in the firewall policy.
D. Port block allocation IP pool is used in the firewall policy.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

QUESTION 21
Which two statements are correct about SLA targets? (Choose two.)

A. You can configure only two SLA targets per one Performance SLA.
B. SLA targets are optional.
C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
D. SLA targets are used only when referenced by an SD-WAN rule.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-slasla-targets

QUESTION 22
Refer to the exhibit.

```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

A. The session is in SYN_SENT state.
B. The session is in FIN_ACK state.
C. The session is in FTN_WAIT state.
D. The session is in ESTABLISHED state.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Indicates TCP (proto=6) session in SYN_SENT state (proto=state=2)

VCEUp

https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

QUESTION 23
Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPXAdminGuide/300_System/303d_FortiGuard.htm

QUESTION 24
Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Antivirus engine
B. Intrusion prevention system engine
C. Flow engine
D. Detection engine

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/applicationcontrol

QUESTION 25
Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

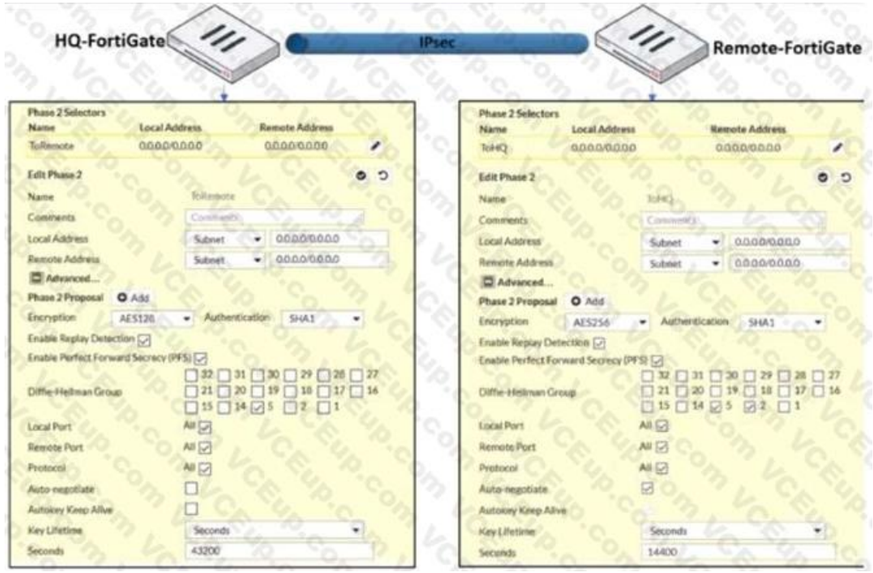
A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
B. To finish any inspection operations
C. To remove the NAT operation
D. To generate logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

QUESTION 26
Refer to the exhibit.

VCEûp



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up. but phase 2 fails to come up.
Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

A. On HQ-FortiGate, enable Auto-negotiate.
B. On Remote-FortiGate, set Seconds to 43200.
C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
D. On HQ-FortiGate, set Encryption to AES256.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495Encryption and authentication algorithm needs to match in order for IPSEC be successfullyestablished.

QUESTION 27
Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.
Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.
B. The IPS engine was unable to prevent an intrusion attack.
C. The IPS engine was blocking all traffic.
D. The IPS engine will continue to run in a normal state.

Correct Answer: A

VCEûp

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshootinghigh-cpu-usage

QUESTION 28
An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

A. Device detection on all interfaces is enforced for 30 minutes.
B. Denied users are blocked for 30 minutes.
C. A session for denied traffic is created.
D. The number of logs generated by denied traffic is reduced.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328

QUESTION 29
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

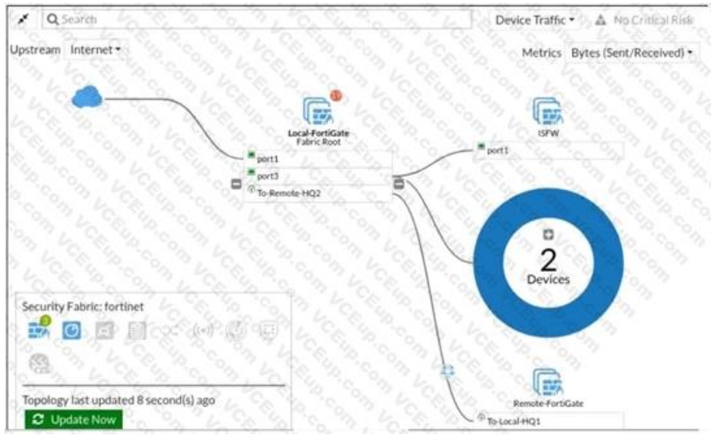
A. get system status
B. get system performance status
C. diagnose sys top
D. get system arp

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"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."

QUESTION 30
Refer to the exhibit.

VCEup



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. There are five devices that are part of the security fabric.
B. Device detection is disabled on all FortiGate devices.
C. This security fabric topology is a logical topology view.
D. There are 19 security recommendations for the security fabric.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
References:
https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabrictopology

VCEup