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

PASS



BES

NSE4_FGT-7.0 Dumps NSE4_FGT-7.0 Braindumps NSE4_FGT-7.0 Real Questions NSE4_FGT-7.0 Practice Test NSE4_FGT-7.0 Actual Questions

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.

dit Address Name Net_Add_1 Color I Change Type - IP/Netmask 1.1.10.255.255.255.0 Interface I any Fabric syncronization ♥	International and the second secon	Image: State of the state	1 Q				
Fabric Root ISFW Gdt Address	Fabric Root ISHW Fabric Root Fabric Root	Fabric Root ISHW Git Address Name Name Net, Add, 1 Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface any Fabric syncronization C Static route configuration -	lpstream Internet •				
IbitW Fabric Root IbitW Idit Address	Fabric Root ISHW Idit Address Name Name Net_Add_1 Color Change Type - IP/Netmask 1.1.10 255.255.255.0 Interface any Fabric syncronization © Static route configuration >	Fabric Root ISHW Idit Address Name Name Net, Add, 1 Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface I any Fabric syncronization • Static route configuration •		-			
Fabric Root ISFW Gdt Address	Fabric Root ISHW Fabric Root Fabric Root	Fabric Root ISHW Git Address Name Name Net, Add, 1 Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface any Fabric syncronization C Static route configuration -		0		— •	0
Edit Address Fabric Root ISFW Edit Address Name Net_Add_1 Color Interface Interface IP/Netmask 1.1.1.0 255.255.255.0 Interface Interface Fabric syncronization Image: Top Construction	Edit Address Fabric Root Name Net_Add_1 Color Change Type - IP/Netmask 1.1.1.0.255.255.255.0 Interface any Static route configuration	Edit Address Name Net_Add_1 Color Change Type IP/Netmask 1.1.1.0.255.255.255.0 Interface Any Static route configuration			6		
Edit Address Name Net_Add_1 Color I Change Type - IP/Netmask 1.1.1.0.255.255.0 Interface I any - Fabric syncronization	Edit Address Name Net_Add_1 Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface any - Fabric syncronization Static route configuration	Edit Address Name Net_Add_1 Color Change Type P/Netmask 1.1.10.255.255.255.0 Interface any Fabric syncronization Static route configuration					ISFW
Name Net_Add_1 Color I Change Type - IP/Netmask 1.1.1.0.255.255.0 Interface I any - Fabric syncronization	Name Net_Add_1 Color Change Type - IP/Netmask 1.1.1.0.255.255.255.0 Interface any - Fabric syncronization C	Name Net_Add_1 Color Change Type - IP/Netmask 1.1.1.0.255.255.255.0 Interface any - Fabric syncronization C				Fabric Root	
Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface any Fabric syncronization	Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface any - Fabric syncronization Static ronization	Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface any - Fabric syncronization C	dit Address				
Color Change Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface any - Fabric syncronization	Color Color Change Type - IP/Netmask 1.1.1.0.255.255.255.0 Interface any - Fabric syncronization Static round configuration	Color Change Type - IP/Netmask 1.1.1.0.255.255.0 Interface any - Fabric syncronization C					
Type - IP/Netmask 1.1.1.0 255.255.255.0 Interface □ any • Fabric syncronization ●	Type - IP/Netmask 1.1.1.0.255.255.255.0 Interface any - Fabric syncronization Static route configuration	Type - IP/Netmask 1.1.10.255.255.255.0 Interface any - Fabric syncronization • Static ronfiguration •	Name	Net_Add_1			
P/Netmask 1.1.1.0.255.255.0 Interface any • Fabric syncronization	IP/Netmask 1.1.1.0.255.255.255.0 Interface □ any • Fabric syncronization © Static ronfiguration ●	IP/Netmask 1.1.1.0.255.255.0 Interface □ any • Fabric syncronization ● Static routic configuration ●	Color	Change			
Interface any • Fabric syncronization	Interface any • Fabric syncronization • Static route configuration •	Interface any - Fabric syncronization Static route configuration	Туре				
Fabric syncronization	Fabric syncronization Static route configuration	Fabric syncronization O Static route configuration O	IP/Netmask	1,1.1.0 255.255.255.0			
	Static route configuration 🔿	Static route configuration 🗇	Interface	🗆 any	-		
			Fabric syncronization	0			
Static route configuration ()		Comments - 0/255	Static route configura	ition 🔿			
Comments		« 0.255	Commante				
comments = 0/255	comments « 0/255		Comments		= 0/255		
Exhibit B.	Exhibit B.						
Exhibit B.	Exhibit B.				ion system caf		
Local-FortiGate # show full-configuration system caf ISFW # show full-configuration system csf	Local-FortiGate # show full-configuration system csf ISFW # show full-configuration system csf						
Local-FortiGate # show full-configuration system caf config system csf	Local-FortiGate # show full-configuration system caf config system csf	config system csf					
Local-FortiGate # show full-configuration system csf config system csf 	Local-ForLiGate & show full-configuration system csf config system csf set status enable :	config system csf set status enable set status enable					
Local-FortiGate # show full-configuration system caf config system caf set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254	Local-FortiGate (show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254	config system csf config system csf set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254				set group-name ''	
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 upstream-port 8013 Set upstream-port 8013	Local-FortiGate / show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set upstream-port 8013	config system csf config system csf set status enable set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set upstream-port 8013 set upstream-port 8013	set group-p	sassword ENC X18CLzrc0B	lq9yz9nryP+YfM16	set accept-auth-by-cert enable	
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"	Local-FortiGate (show full-configuration system caf config system caf set status enable set upstream-ip 0.0.0.0 set upstream-port 8013 set group-name "fortinet" Local-FortiGate (show full-configuration system caf config system caf set status enable set upstream-ip 10.0.1.254 set group-name "fortinet"	config system csf config system csf set status enable set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set upstream-port.8013 set upstream-port 8013 set group-name "fortiset" set group-name "fortiset"	BJkv/S/trtoh2q1	Ae5CH8YMAa0GT18aX)/dKH	oSizw1ZEoN1QN2N	set log-unification enable	
<pre>tocal-ForLiGate # show full-configuration system csf config system csf set status enable set upstream-port 8013 set group-name "fortinet" set group-passeord ENC X18Ctzrc0BUg%yz%nryP*YfM16 set accept-auth-by-cert enable</pre>	<pre>tocal-FortiGate # show full-configuration system csf config system csf set status enable set upstream-pol.8013 set group-name "fortinet" set group-name "KN 1818CtzrcUBUq%yz%nryPYYN16 set accept-auth-by-cert enable</pre>	config system csf set status enable set upstream-ip 0.0.0.0 set upstream-ip 0.0.1.254 set upstream-ip 10.1.254 set upstream-ip 10.1.254 set group-name "fortinet" set group-name "fortinet" set accept-auth-by-cert enable	FGLT4r5zZAyYI81	i1Pxut,iLcsCp1AdZadv1CxD	661dLX716o22J9P		rial
Local-FortiGate # show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set group-name "fortinet" set group-name "fortinet" set group-name of KNTELZzroUBUG%yz%nryPsYfM16 BJKv/S/trtoh2gYAeSCH8YMAaOGT18aXi/dKH/oSizw1ZEONION2N	Local-FortiGate / show full-configuration system csf config system csf set status enable set upstream-jp 0,0,0,0 set upstream-jp 0,0,0,0 set upstream-port 8013 set group-password ENC X18CtzrcUBBUq%yz%nryPfYfN16 BJKV/S/trtch2qYAsCUBFYMAGCT18AX/dKU/obixV12KON10N2N set log-initication enable	config system csf config system csf set status enable set status enable set upstream-jp 0.0,0,0 set upstream-jp 10.0,1,254 set group-name "fortinel" set upstream-port 8013 set group-name "fortinel" set accept-auth-by-cert enable BJKv/S/ttoh_2qVAsCHEYMA40CTHEAx/dKU/obizx12E0N1QN2N set log-inification enable				set fabric-workers 2	
<pre>Local-ForLiGate (show full-configuration system csf config system csf set status enable set upstream-port 8013 set group-name "fortinet" set aroup-password ENC X16CtzrcUBUg9yz9nryP*YfM16 BR/kV15/tit0h2g/ke5CH8YMAB00T18Axi/4KH/r05izk1280M10M2N set accept-auth-by-cert enable set authorization-request-type serial set fabric-workers 2</pre>	<pre>Local-ForLiGate (show full-configuration system csf config system csf set status enable set upstream-pot.8013 set group-name "fortinet" set aroup-passerd ENC X18CtzrcUBUq9yz9nryP+YfN16 B3kV/3/trtoh2g/AeSCH8YMA00T18AX/AKH/AbizW1ZE0N10N2N FGLT4r5z2AyYT811PxutiLcnCp1AdZady1CxDe661dLX7160223P set accept-auth-by-cert enable set fabric=workers 2</pre>	config system csf config system csf set status enable set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set upstream-ip 10.0.1.254 set upstream-ip 10.0.1.254 set group-name "fortinet" set group-name "fortinet" set group-name "fortinet" set accept-auth-by-cert enable set/s2/trtoh2qYAeSCH8YMAA00TBAXF/4KH/ASizxHZKONTQN2N set accept-auth-by-cert enable set accept-auth-by-cert enable set autorization enable set accept-auth-by-cert enable set fabric-workers 2				set downstream-access disable	
Local-FortiGate # show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set group-name "fortinet" set group-name of KINCLINE BJKV/S/trtoh2gYAe5CH8YMAa0GT18aXi/dKH/o5izw1ZE0N10N2N set accept-auth-by-cert enable set accept-auth-by-cert enable	Local-ForLiGate I show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set group-name "fortinet" set group-name of KOTLinet" SUMTS/trtoh2gYAe5CH8YMAa0GT18ax1/dKH/o5izw12E0N10N2N set accept-auth-by-cert enable set accept-auth-by-cert enable	config system csf config system csf set status enable set status enable set upstream-jp 0.0.0.0 set upstream-jp 10.0.1.254 set upstream-port 8013 set upstream-port 8013 set groip-name "fortinel" set upstream-port 8013 set groip-name "fortinel" set upstream-port 8013 set groip-name "fortinel" set upstream-port 8013 set group-name "fortinel" set upstream-port 8013 set group-name "fortinel" set upstream-port 8013 set upstream-port 8012 set accept-auth-by-cert enable set accept-auth-by-cert enable set authorization-request-type serial set log-unification enable set downstream-access disable			rial		
 Local-FortiGate I show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set group-name "fortinet" set group-password ENC X18CtzruBB1q9yz9nryPsYfM16 BJKV/S/trtoh2qYAe5CH8YMA0CT18X:/dKU/o5iz4ZE0N10N2N set accept-auth-by-cert enable set accept-auth-by-cert enable set group-name in the system csf set accept-auth-by-cert enable set accept-auth-by-cert enable set group-name in the system csf set group-name in the system csf set accept-auth-by-cert enable set authorization-request-type serial set configuration system csf set authorization-request-type serial 	<pre>Local-FortiGate # show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set group-name "fortinet" set group-password ENC X18CE2rcUBUq9y29nryPiYIM16 BJKV/S/trioh2qTAe5CH8YMA0CT18AXi/dKH/o5izM12KONIQN2N set accept-auth-by-cert enable set accept-auth-by-cert enable set authorization-request-type serial set configuration system csf config system csf config system csf set status enable set substream-ip 0.0.1.254 set group-name " set accept-auth-by-cert enable set authorization-request-type serial set configuration system csf set status enable set accept-auth-by-cert enable set authorization-request-type serial set configuration-system default</pre>	config system csf config system csf set status enable set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set upstream-port 8013 set upstream-ip 10.0.1.254 set group-password ENC X18Ctrrc018Uq9y29nryPiYIM16 set group-name * set group-password ENC X18Ctrrc018Uq9y29nryPiYIM16 set accept-auth-by-cert enable set accept-auth-by-cert enable set log-inification enable set log-inification enable set downstream-access disable set log-inification enable set downstream-access disable set log-inification-request-type serial set configuration-sync default					114
 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-password ENC X16CtrcUBUq9y29nryP4YIN16 Bckv75/trtoh2qVAe5C187MAa0CT18ax/4KKI/o5izx1226NIQN2N set log-unification-request-type serial set authorization-request-type serial set authorization-request-type serial set fabric-workers 2 set same csf set same csf set config system csf set group-password ENC X16CtrcUBUq9y29nryP4YIN16 set authorization-sync default set fabric-workers 2 set downstream-access disable set saml-configuration-sync default 	Local-FortiGate (show full-configuration system csf config system csf set upstream-ip 0.0,0,0 set upstream-ip 0.0,0,0 set upstream-port 8013 set group-name "fortinet" set group-name "fortinet" set accept-auth-by-cert enable set fabric-workers 2 set configuration-sync default	config system csf config system csf set status enable set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set group-name "fortinet" set upstream-ip 10.0.1.254 set group-name "fortinet" set upstream-port 8013 set group-name "fortinet" set accept-auth-by-cert enable set coept-auth-by-cert enable set indo-unification enable set coept-auth-by-cert enable set forume request-type serial set indo-unification enable set forum-request-type serial set indo-unification enable set downstream-access disable set indo-unification enable set configuration-sync default set indo-unification enable set forum-request default set indo-unification enable set forum-request default				end	
 Local-FortiGate I show full-configuration system csf config system csf set status enable set upstream-ip 0.0.0.0 set group-name "fortinet" set group-name "fortinet" set group-name "fortinet" set group-name "fortinet" set group-name "fortinet" set accept-auth-by-cert enable set accept-auth-by-cert enable set authorization-request-type serial set fabric-workers 2 set downstream-access disable ISEW I 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 "fortinet" set accept-auth-by-cert enable set authorization-request-type serial set fabric-workers 2 set downstream-access disable 	<pre>Local-FortiGate # show full-configuration system csf config system csf act status enable set upstream-ip 0.0.0.0 set upstream-ip 0.0.0.0 set upstream-port 8013 set group-name "fortinet" set group-namesord ENC X18CtzrcU8849yz9nryPiYIN16 BJkv/S/trtoh2qXAebCH8YMAa0GT18axi/dK8/o5izx12KoN10N2N rel arcopt-auth-by-cert enable set accept-auth-by-cert enable set accept-auth-by-cert enable set authorization-request-type serial set fabric-workers 2 set downstream-access disable </pre>	config system csf config system csf set talus enable set stalus enable set upstream-port.8013 set upstream-port.8013 set group-name "fortinel" set accept-auth-by-cert enable set log-unification enable set fabric-workers 2 set fabric-workers 2 set saml-configuration-sync default set fabric-workers 2 set saml-configuration-sync default set fabric-workers 2 set saml-configuration-sync default			1	ISFW	
config system csf config system csf set status enable set status enable set upstream-port.8013 set upstream-port.8013 set group-password ENC X18CtzrcUBUg%y2%nryP*Y(M16 set upstream-port.8013 B&kv/3/trtoh20YAe5CH%YMA0CT18Ax+/dKH/dbizx12E0M10M2N set accept-auth-by-cert enable Set log-unification enable set ind=unification enable set accept-auth-by-cert enable set fabric-workers 2 set fabric-workers 2 set ionin-request-type serial set downstream-access disable set saml-configuration-sync default set configuration-sync default end	Local-FortiGate & show full-configuration system caf config system caf set upstream-ip 0.0.0.0 set upstream-ip 0.0.0.0 set upstream-ip 0.0.1.254 set group-name '' set group-name '' set accept-auth-by-cert enable set configuration-sync default end	config system csf config system csf set status enable set status enable set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set upstream-ip 0.0.0.0 set upstream-ip 10.0.1.254 set group-passed ENC X18CtrcUBUq4y24nryPiYfM16 set group-name *fortinet* set group-passed ENC X18CtrcUBUq4y24nryPiYfM16 set accept-auth-by-cert enable set log-unification enable set log-unification enable set log-unification enable set fabric-workers 2 set fabric-workers 2 set downstream-access disable set downstream-access disable set sam1-configuration-sync default		antiquiration-synd defaul		ISEW I	

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.

Username	Administrator	Change Password
Туре	Local User	
	Match a user on a remote server group Match all users in a remote server group	
	Use public key infrastructure (PKI) group	
Comments	Write a contrient	2 0/255
Administrator profile	prof_admin •	
 Two-factor Auth Restrict login to 		
C Destrict admin t		
D Restrict admin to	o guest account provisioning only	

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 ()	
Listen on Interface(s)	🖻 port1 🛛 🗙
Listen on Port	11443
	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	3
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 Mappir	ng 🟮
+ Create New / Edi	1 Delete
Users/Groups ©	Portal 🗘
SSL-VPN-Users	tunnel-access
All Other Users/Groups	full-access

Exhibit B.

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

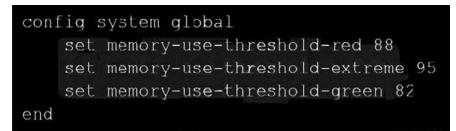
Question: 67

Refer to the exhibits.

Exhibit A shows system performance output.



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

<u>Actual Exam Questions</u>: 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.

<u>Exam Dumps</u>: 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.

<u>Practice Tests</u>: 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.

<u>Guaranteed Success</u>: 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.

<u>Updated Content:</u> 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.

<u>Technical Support</u>: 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.

For More exams visit https://killexams.com/vendors-exam-list Kill your exam at First Attempt....Guaranteed!