Vendor: Fortinet

Exam Code: NSE4_FGT-7.2

Exam Name: Fortinet NSE 4 - FortiOS 7.2

Version: DEMO

QUESTION 1
Which statement is correct regarding the use of application control for inspecting web applications?

A. Application control can identify child and parent applications, and perform different actions on them.
B. Application control signatures are organized in a nonhierarchical structure.
C. Application control does not require SSL inspection to identify web applications.
D. Application control does not display a replacement message for a blocked web application.

Answer: A
Explanation:
Application control is a feature that allows FortiGate to inspect and control the use of specific web applications on the network. When application control is enabled, FortiGate can identify child and parent applications, and can perform different actions on them based on the configuration.

QUESTION 2
Which timeout setting can be responsible for deleting SSL VPN associated sessions?

A. SSL VPN idle-timeout
B. SSL VPN http-request-body-timeout
C. SSL VPN login-timeout
D. SSL VPN dtls-hello-timeout

Answer: A
Explanation:
The SSL VPN idle-timeout setting determines how long an SSL VPN session can be inactive before it is terminated. When an SSL VPN session becomes inactive (for example, if the user closes the VPN client or disconnects from the network), the session timer begins to count down. If the timer reaches the idle-timeout value before the user reconnects or sends any new traffic, the session will be terminated and the associated resources (such as VPN tunnels and virtual interfaces) will be deleted.

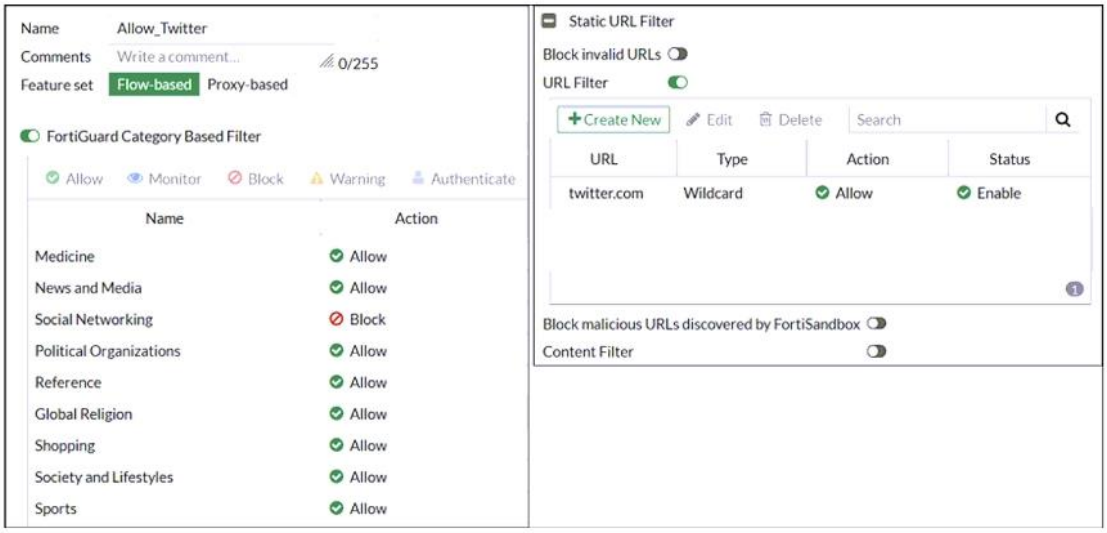
QUESTION 3
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

A. FortiGate uses fewer resources.
B. FortiGate performs a more exhaustive inspection on traffic.
C. FortiGate adds less latency to traffic.
D. FortiGate allocates two sessions per connection.

Answer: AC
Explanation:
Flow-based inspection is a type of traffic inspection that is used by some firewall devices, including FortiGate, to analyze network traffic. It is designed to be more efficient and less resource-intensive than proxy-based inspection, and it offers several benefits over this approach.
Two benefits of flow-based inspection compared to proxy-based inspection are:
- FortiGate uses fewer resources: Flow-based inspection uses fewer resources than proxy-based inspection, which can help to improve the performance of the firewall device and reduce the impact on overall system performance.
- FortiGate adds less latency to traffic: Flow-based inspection adds less latency to traffic than proxy-based inspection, which can be important for real-time applications or other types of traffic

that require low latency.

QUESTION 4
Refer to exhibit. An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.



Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking.
B. On the Static URL Filter configuration, set Type to Simple.
C. On the Static URL Filter configuration, set Action to Exempt.
D. On the Static URL Filter configuration, set Action to Monitor.

Answer: C
Explanation:
Based on the exhibit, the administrator has configured the FortiGuard Category Based Filter to block access to all social networking sites, and has also configured a Static URL Filter to block access to twitter.com. As a result, users are being redirected to a block page when they try to access twitter.com.
To allow users to access twitter.com while blocking all other social networking sites, the administrator can make the following configuration change:
On the Static URL Filter configuration, set Action to Exempt: By setting the Action to Exempt, the administrator can override the block on twitter.com that was specified in the FortiGuard Category Based Filter. This will allow users to access twitter.com, while all other social networking sites will still be blocked.

QUESTION 5
What are two functions of ZTNA? (Choose two.)

A. ZTNA manages access through the client only.
B. ZTNA manages access for remote users only.
C. ZTNA provides a security posture check.
D. ZTNA provides role-based access.

Answer: CD
Explanation:
ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.
Two functions of ZTNA are:
- ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the device's software and hardware configurations, security settings, and the presence of malware.
- ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

QUESTION 6
Which statement correctly describes the use of reliable logging on FortiGate?

A. Reliable logging is enabled by default in all configuration scenarios.
B. Reliable logging is required to encrypt the transmission of logs.
C. Reliable logging can be configured only using the CLI.
D. Reliable logging prevents the loss of logs when the local disk is full.

Answer: D
Explanation:
On a FortiGate device, reliable logging is a feature that helps to prevent the loss of log messages when the local disk is full. When reliable logging is enabled, the FortiGate will store log messages in a buffer until they can be written to the local disk. This helps to ensure that log messages are not lost due to a full disk, allowing administrators to maintain an accurate record of activity on the network.
Reliable logging is not enabled by default in all configuration scenarios, and it does not encrypt the transmission of logs or require the use of the CLI to be configured. However, it is a useful feature to enable in order to maintain a comprehensive record of activity on the network and help with troubleshooting and security analysis.

QUESTION 7
Refer to the exhibits. The exhibits show the firewall policies and the objects used in the firewall policies.
The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Exhibit A | Exhibit B

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0/0
FQDN 6	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,025		
Facebook-Web	Destination	26,578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80 443 8443	TCP	Enabled
1.9.91.17 - 1.9.91.18	443	UDP	Enabled
1.9.91.30	443	UDP	Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	ACCEPT	Enabled

Exhibit A | Exhibit B

Policy Lookup

Incoming Interface	port3
IP Version	IPv4
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	facebook.com
Destination Port	443

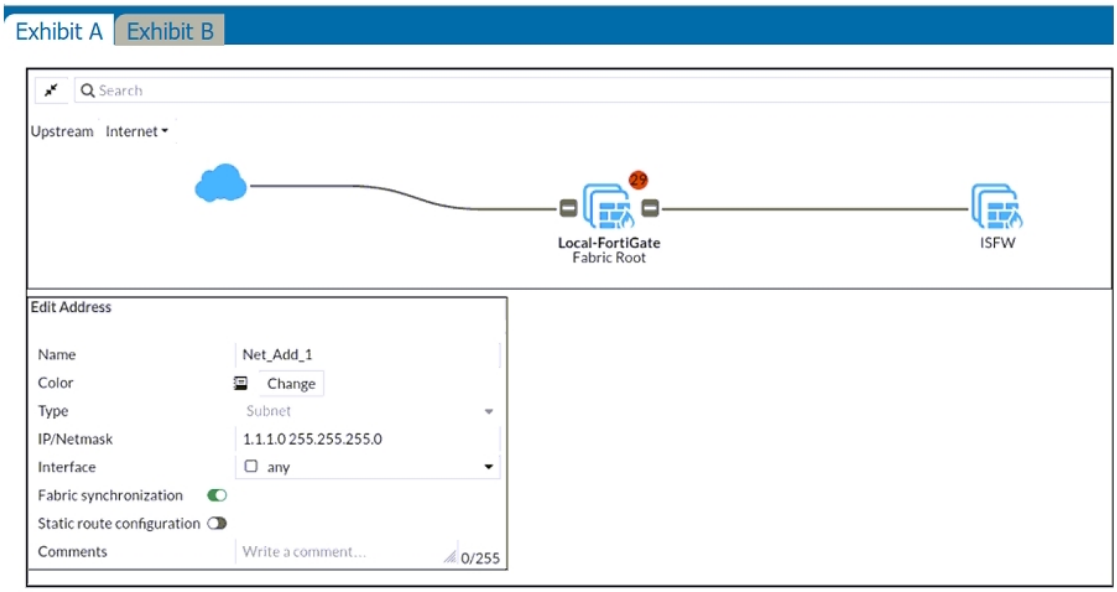
Search | Close

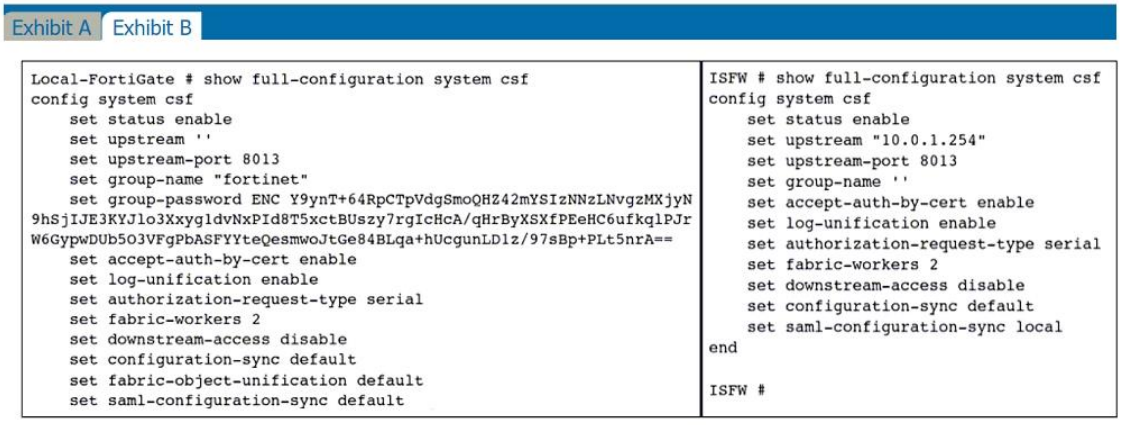
Which policy will be highlighted, based on the input criteria?

A. Policy with ID 4.
B. Policy with ID 5.
C. Policies with ID 2 and 3.
D. Policy with ID 4.

Answer: B
Explanation:
It's coming from port 3 - hits Facebook-Web (Application) from the screenshot it show that it allows http and https traffic (80, 443).

QUESTION 8
Refer to the exhibits. 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 ISFW (downstream) to set configuration-sync local.
B. Change the csf setting on ISFW (downstream) to set authorization-request-type certificate.
C. Change the csf setting on both devices to set downstream-access enable.
D. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

Answer: D
Explanation:
On the config output set fabric-object-unification is se to local, which means the device does not synchronize objects from the root but will send the synchronized objects downstream. So it must be changed back to default (which is the default setting) and Global CMDB objects will be synchronized in the Security Fabric.
https://docs.fortinet.com/document/fortigate/6.4.5/administration-guide/880913/synchronizing-objects-across-the-security-fabric

QUESTION 9
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.

Answer: CD
Explanation:
To establish an SSL VPN connection between two FortiGate devices, the following two settings are required:
- The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate will use a CA (Certificate Authority) certificate to verify the client FortiGate certificate, ensuring that the client device is trusted and allowed to establish an SSL VPN connection.
- The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: The client FortiGate must have an SSL VPN tunnel interface type configured in order to establish an SSL VPN connection. This interface type will be used to connect to the server FortiGate over the SSL VPN.

QUESTION 10
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

Answer: BC
Explanation:
To create a web rating override for the home page of the example.com domain, the administrator must use one of the following syntaxes:
www.example.com: This syntax specifies the fully qualified domain name (FQDN) of the website, including the www subdomain. This syntax will apply the web rating override to all pages on the website, including the home page.

example.com: This syntax specifies the root domain of the website, without the www subdomain. This syntax will also apply the web rating override to all pages on the website, including the home page.

QUESTION 11
What are two features of FortiGate FSSO agentless polling mode? (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.

Answer: BC
Explanation:
You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent.
Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs.
FG acts as a collector. It 's responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

QUESTION 12
Based on the routing database shown in the exhibit, which two conclusions can you make about the routes? (Choose two.)

```
FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S    *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
S    *>           [10/0] via 10.0.0.2, port2, [30/0]
S       0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C    *> 10.0.0.0/24 is directly connected, port2
S       172.13.24.0/24 [10/0] is directly connected, port4, [1/0]
C    *> 172.20.121.0/24 is directly connected, port1
S    *> 192.168.1.0/24 [10/0] via 10.0.0.2, port2, [1/0]
```

A. The port3 default route has the highest distance.
B. The port3 default route has the lowest metric.
C. There will be eight routes active in the routing table.
D. The port1 and port2 default routes are active in the routing table.

Answer: AD
Explanation:
*> mean active routes

first square bracked mean administrative distance
second bracket square mean priority (valid only on static routes)
metric applies only in multiroutes with same administrative distance

QUESTION 13
Refer to the exhibit. 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.)

```
Local-FortiGate # diagnose sniffer packet any "icmp" 5
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
10.207548 port3 in 10.0.1.10 -> 8.8.8.8: icmp: echo request
0x0000   4500 0054 8707 4000 4001 9888 0a00 010a        E..T..@.@.......
0x0010   0808 0808 0800 88d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        ............ !"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567

10.207655 port1 out 10.200.1.1 -> 8.8.8.8: icmp: echo request
0x0000   4500 0054 8707 4000 3f01 98c9 0ac8 0101        E..T..@.?.......
0x0010   0808 0808 0800 88d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        ............ !"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567

10.215940 port1 in 8.8.8.8 -> 10.200.1.1: icmp: echo reply
0x0000   4500 0054 0000 0000 7101 2dd1 0808 0808        E..T....q.-.....
0x0010   0ac8 0101 0000 90d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        ............ !"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567

10.215976 port3 out 8.8.8.8 -> 10.0.1.10: icmp: echo reply
0x0000   4500 0054 0000 0000 7001 2f90 0808 0808        E..T....p./.....
0x0010   0a00 010a 0000 90d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        ............ !"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567
```

A. Interface name
B. Ethernet header
C. IP header
D. Application header
E. Packet payload

Answer: ACE
Explanation:
Study Guide – Routing – Diagnostics – Packet Capture Verbosity Level.
diagnose sniffer packet <interface> '<filter>' <verbosity> <count> <timestamp> <frame size>

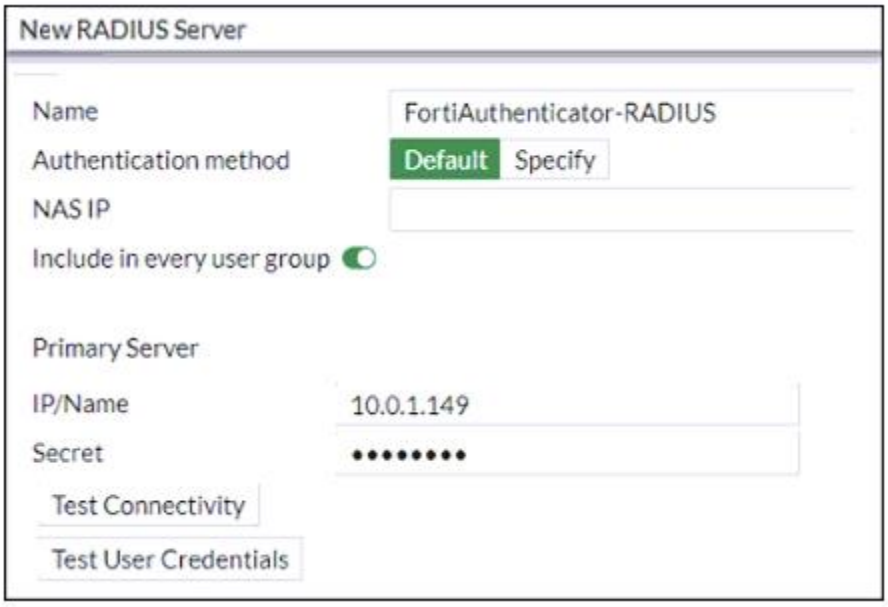
In the example, verbosity is 5.
The verbosity level specifies how much info you want to display.
1 (default): IP Headers.
2: IP Headers, Packet Payload.
3. IP Headers, Packet Payload, Ethernet Headers.
4: IP Headers, Interface Name.
5: IP Headers, Packet Payload, Interface Name.
6: IP Headers, Packet Payload, Ethernet Headers, Interface Name.

QUESTION 14
An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
Which DPD mode on FortiGate will meet the above requirement?

A. Disabled
B. On Demand
C. Enabled
D. On Idle

Answer: D
Explanation:
On Idle: FortiGate sends DPD probes when no traffic is observed in the tunnel. An idle tunnel does not necessarily mean the tunnel is dead. Avoid this mode if you have many tunnels, because the overhead introduced by DPD can be very resource intensive.

QUESTION 15
Refer to the exhibit. An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.



What is the impact of using the Include in every user group option in a RADIUS configuration?

A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.

B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Answer: A
Explanation:
The INCLUDE IN EVERY USER GROUP option adds the Radius server and all user that can authenticate against it, to every user group created on the FortiGate.

QUESTION 16
Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.
C. Highest to lowest priority defined in the firewall policy.
D. Services defined in the firewall policy.
E. Lowest to highest policy ID number.

Answer: ABD
Explanation:
When a packet arrives, how does FortiGate find a matching policy?
Each policy has match criteria, which you can define using the following objects:
• Incoming Interface
• Outgoing Interface
• Source: IP address, user, internet services
• Destination: IP address or internet services
• Service: IP protocol and port number
• Schedule: Applies during configured times

QUESTION 17
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The NetSessionEnum function is used to track user logouts.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent uses a Windows API to query DCs for user logins.
D. The collector agent do not need to search any security event logs.

Answer: A
Explanation:
Study Guide – FSSO – FSSO with Windows Active Directory – Collector Agent-Based Polling Mode Options.
Collector agent-based polling mode has three methods (or options) for collecting logon info: NetAPI, WinSecLog and WMI.
NetAPI: Polls temporary sessions created on the DC when a user logs on or logs off and calls the NetSessionEnum function on Windows. It's faster than the WinSec and WMI methods; however, it can miss some logon events if a DC is under heavy system load. This is because sessions can be quickly created and purged form RAM, before the agent has a chance to poll and notify FG.

LEAD2PASS
First Test, First Pass!

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: ASTR14