Vendor: Fortinet

Exam Code: NSE4_FGT_AD-7.6

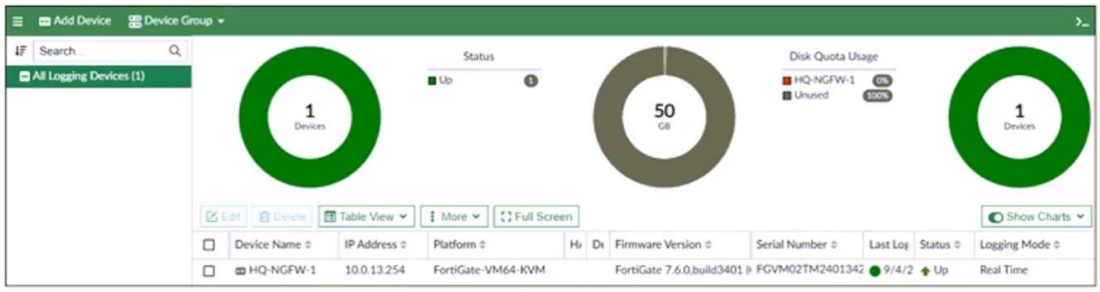
Exam Name: Fortinet NSE 4 - FortiOS 7.6 Administrator

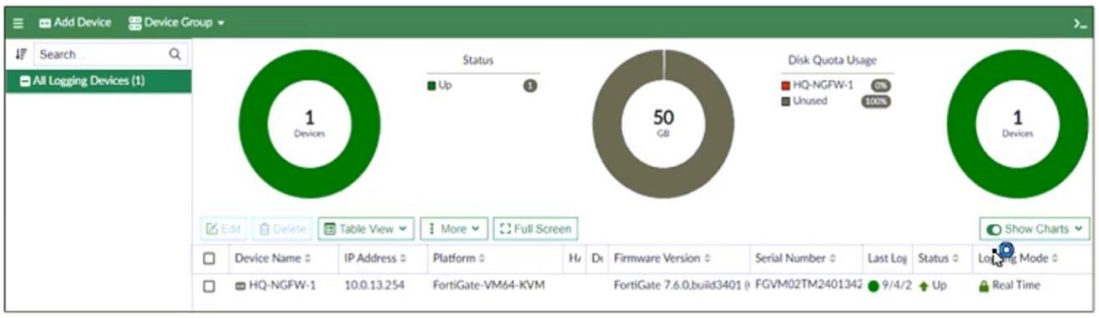
Version: DEMO

QUESTION 1
The FortiGate device HQ-NGFW-1 with the IP address 10.0.13.254 sends logs to the FortiAnalyzer device with the IP address 10.0.13.125. The administrator wants to verify that reliable logging is enabled on HQ-NGFW-1. Which exhibit helps with the verification?

A.
```
HQ-NGFW-1 # diagnose sniffer packet any "host 10.0.13.125" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.13.125]
2.173071 port6 out 10.0.13.254.14974 -> 10.0.13.125.514: udp 347
3.334638 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: psh 4017477514 ack 2638032500
3.335098 port6 in 10.0.13.125.514 -> 10.0.13.254.23054: psh 2638032500 ack 4017477548
3.335129 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: ack 2638032543
```

B.
```
config log fortianalyzer setting
     set status enable
     set server "10.0.13.125"
     set serial "FAZ-VMTM24012176"
     set enc-algorithm high-medium
     set upload-option realtime
end
```

C.


D.


Answer: A
Explanation:
Using the diagnose sniffer packet command with the FortiAnalyzer IP as a filter allows the administrator to see actual log traffic leaving HQ-NGFW-1. This verifies that reliable logging is enabled and logs are being sent to the FortiAnalyzer in real time.

QUESTION 2
Refer to the exhibit. Which two ways can you view the log messages shown in the exhibit? (Choose two.)

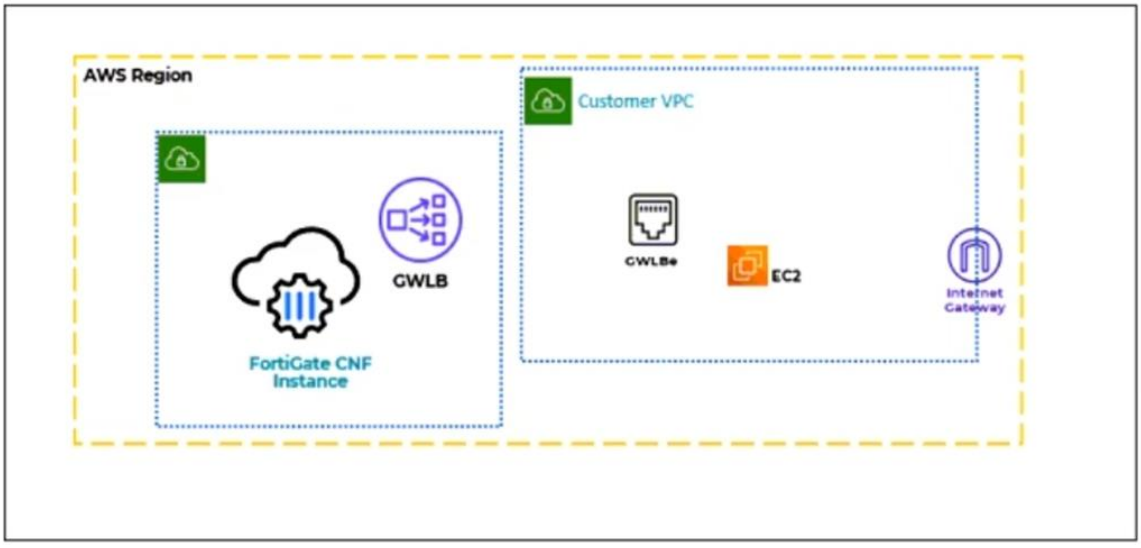
```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

A. By right clicking the implicit deny policy
B. By filtering the policy universally unique identifier (UUID) and application name in the log entry
C. Using the FortiGate CLI command `diagnose log test`
D. In the Forward Traffic section

Answer: BD
Explanation:
You can view log messages by filtering based on the policy UUID and application name in the log entry, and also in the Forward Traffic section, which displays logs related to allowed and denied traffic.

QUESTION 3
Refer to the exhibit.

A partial cloud topology is shown.



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.

During the deployment, which components must be FortiGate CNF create to handle traffic from the EC2 instance?

A. The GWLB, GWLBe, and the internet gateway (IGW) in the customer VPC
B. The CNF VPC, customer VPC, and GWLB
C. The customer VPC and GWLBe
D. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)

Answer: D
Explanation:
The FortiGate CNF must create the gateway load balancer endpoint (GWLBe) in the customer VPC to handle traffic redirection from EC2 instances to the FortiGate CNF via the gateway load balancer (GWLB).

QUESTION 4
Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Choose two.)

A. FortiExtender
B. VPN policies
C. The proxy auto-configuration (PAC) file
D. FortiSASE Firewall-as-a-Service (FWaaS)

Answer: BD
Explanation:
In agent-based mode, FortiSASE Secure Internet Access uses VPN policies for secure connectivity, and the FortiSASE Firewall-as-a-Service (FWaaS) component for enforcing security policies and filtering user traffic.

QUESTION 5
How does FortiExtender connect to FortiSASE in a site-based, remote internet access method?

A. FortiExtender establishes a secure SSL connection using FortiClient.
B. FortiExtender uses the proxy auto-configuration (PAC) file and an explicit web proxy to connect.
C. FortiExtender first connects to a FortiGate LAN extension through a secure web gateway (SWG).
D. FortiExtender uses a Virtual Extensible LAN (VXLAN)-over-IPsec connection.

Answer: D
Explanation:
In a site-based, remote internet access deployment, FortiExtender connects to FortiSASE using a Virtual Extensible LAN (VXLAN)-over-IPsec connection, providing secure and scalable connectivity for branch locations.

QUESTION 6
There are multiple dialup IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels. Which phase 1 setting you can configure to match the user to the tunnel?

A. Dead Peer Detection
B. Peer ID
C. Local Gateway
D. IKE Mode Config

Answer: B
Explanation:
Peer ID is used in aggressive mode dialup IPsec VPNs to identify and match incoming VPN connections to their correct phase 1 configuration/tunnel. This allows each department or user to have a unique identifier, ensuring users are connected to the correct VPN tunnel. This is the

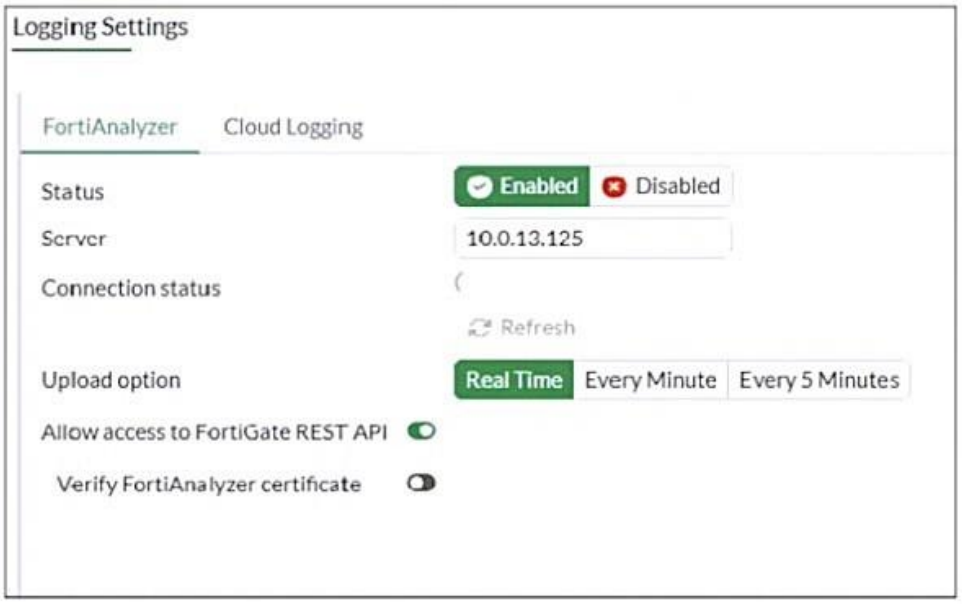
recommended approach for environments with multiple dial-up users or tunnels.

QUESTION 7
An administrator wants to address shadow IT visibility challenges and prevent users from sending sensitive files outside the organization without proper approval. Which FortiSASE method should the administrator implement to achieve these goals?

A. Secure internet access (SIA)
B. Secure private access (SPA)
C. Secure SaaS access (SSA)
D. Secure SD-WAN access (SSD-WAN)

Answer: C
Explanation:
Secure SaaS Access (SSA) provides visibility into shadow IT and allows control over SaaS applications, including enforcing policies to prevent sensitive files from being uploaded or shared without proper approval.

QUESTION 8
Refer to the exhibit. You are configuring FortiAnalyzer on FortiGate.



Which step must you take to connect FortiAnalyzer to FortiGate?

A. Verify the FortiAnalyzer serial number.
B. Enable disk logging on FortiGate.
C. Authorize FortiGate on FortiAnalyzer.
D. Configure UDP port 514 on FortiGate.

Answer: C
Explanation:
Before FortiGate can send logs to FortiAnalyzer, the FortiGate device must be authorized on the FortiAnalyzer. This establishes trust and allows log forwarding from FortiGate to FortiAnalyzer.

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**