NSE8$^{Q\&As}$

Fortinet Network Security Expert 8 Written (800)

Pass Fortinet NSE8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/nse8.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Referring to the exhibit, which statement is true?


```
date=2014-11-18 time=00:59:46 logid=0101037195
type=event subtype=vpn level=error vd="root"
msg="IPsec ESP error" action=error
remip=192.168.99.99 locip=10.185.88.88
remport=500 locport=500 outintf="wan1"
cookies="39c346564b121a2c/e2cbc214ff16c6fc"
user="N/A" group="N/A" vpntunnel="N/A"
status=esp_error error_num="Received ESP packet
with unknown SPI." spi="23ac14e0" seq="00e0ffff"
```

A. The packet failed the HMAC validation.

B. The packet did not match any of the local IPsec SAs.

C. The packet was protected with an unsupported encryption algorithm.

D. The IPsec negotiation failed because the SPI was unknown.

Correct Answer: A

Explanation: http://kb.fortinet.com/kb/viewContent.do?externalId=FD33101

QUESTION 2

You are an administrator of FortiGate devices that use FortiManager for central management. You need to add a policy on an ADOM, but upon selecting the ADOM drop-down list, you notice that the ADOM is in locked state. Workflow mode

is enabled on your FortiManager to define approval or notification workflow when creating and installing policy changes.

What caused this problem?

A. Another administrator has locked the ADOM and is currently working on it.

B. There is pending approval waiting from a previous modification.

C. You need to use set workspace-mode workflow on the CLI.

D. You have read-only permission on Workflow Approve in the administrator profile.

Correct Answer: D

http://docs.fortinet.com/uploaded/files/2250/FortiManager-5.2.1-Administration-Guide.pdf

QUESTION 3

Your marketing department uncompressed and executed a file that the whole department received using Skype.
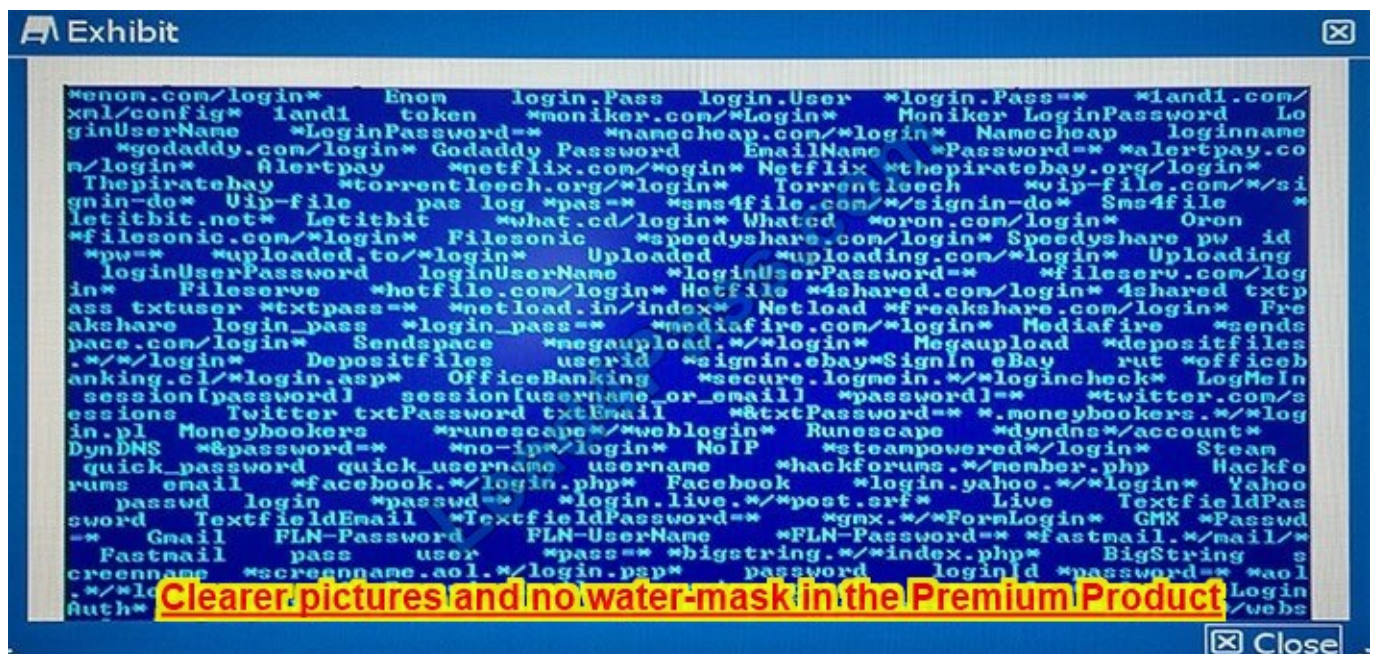
Reviewing the exhibit, which two details do you determine from your initial analysis of the payload?

A. The payload contains strings that the malware is monitoring to harvest credentials.

B. This is a type of Trojan that will download and pirate movies using your Netflix credentials.

C. This type of threat of a DDoS attack using instant messaging to send e-mails to further spread the infection.

D. This threat payload is uploading private user videos which are then used to extort Bitcoin payments.

Correct Answer: B

QUESTION 4

Exhibit

Peering IP:	5.5.5.5
Peering AS:	5555
Customer AS:	54321
Customer IP:	1.1.1.1

Current FortiGate BGP configuration:

```
config router bgp
    set as 54321
        config neighbor
            edit "5.5.5.5"
                set remote-as 5555
            next
        end
end
```

AS 5555
lo0: 5.5.5.5
.1
20.20.20.0/24
.2
.2
10.10.10.0/24
.1 (wan1)
lo0: 1.1.1.1
AS 54321

Close

You must establish a BGP peering with a service provider. The provider has supplied you with BGP peering parameters and you performed the basic configuration shown in the exhibit on your FortiGate unit. You notice that your peering session is not coming up. Which three missing configuration statements are needed to make this configuration functional? (Choose three.)

A.
```
config router static
    edit 0
        set device wan1
        set dst 5.5.5.5
        set gateway 20.20.20.1
    next
end
```

B.
```
config router static
    edit 0
        set device wan1
        set dst 5.5.5.5
        set gateway 10.10.10.2
    next
end
```

C.
```
config router bgp
    config neighbor
        edit "5.5.5.5"
            set ebgp-enforce-multihop enable
        next
    end
end
```

D.
```
config router bgp
    config neighbor
        edit "5.5.5.5"
            set update-source lo0
        next
    end
end
```

E.
```
config router bgp
    config neighbor
        edit "5.5.5.5"
            set next-hop-self enable
        next
    end
end
```

A. B. C. D. E.

Correct Answer: CDE

QUESTION 5

The SECOPS team in your company has started a new project to store all logging data in a disaster recovery center. All FortiGates will log to a secondary FortiAnalyzer and establish a TCP session to send logs to the syslog server. Which two configurations will achieve this goal? (Choose two.)

A.
```
config log syslogd setting
    set port 514
    set reliable enable
    set server 172.20.120.24
    set status enable
```

B.
```
config log fortianalyzer setting
    edit 2
    set status enable
    set server 172.20.120.23
    set conn-timeout 100
```

C.
```
config log syslogd setting
    set csv enable
    set facility local 5
    set port TCP 514
    set server 172.20.120.24
    set status enable
```

D.
```
config log fortianalyzer2 setting
    set status enable
```

A. B. C. D.

Correct Answer: AC

https://forum.fortinet.com/tm.aspx?m=122848

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
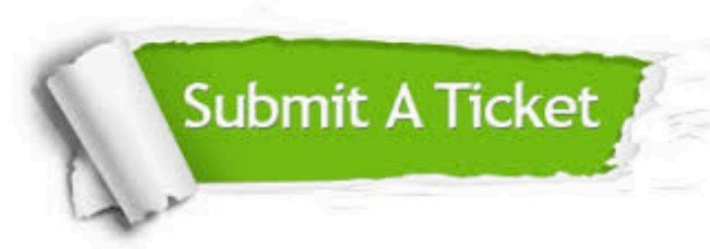Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: