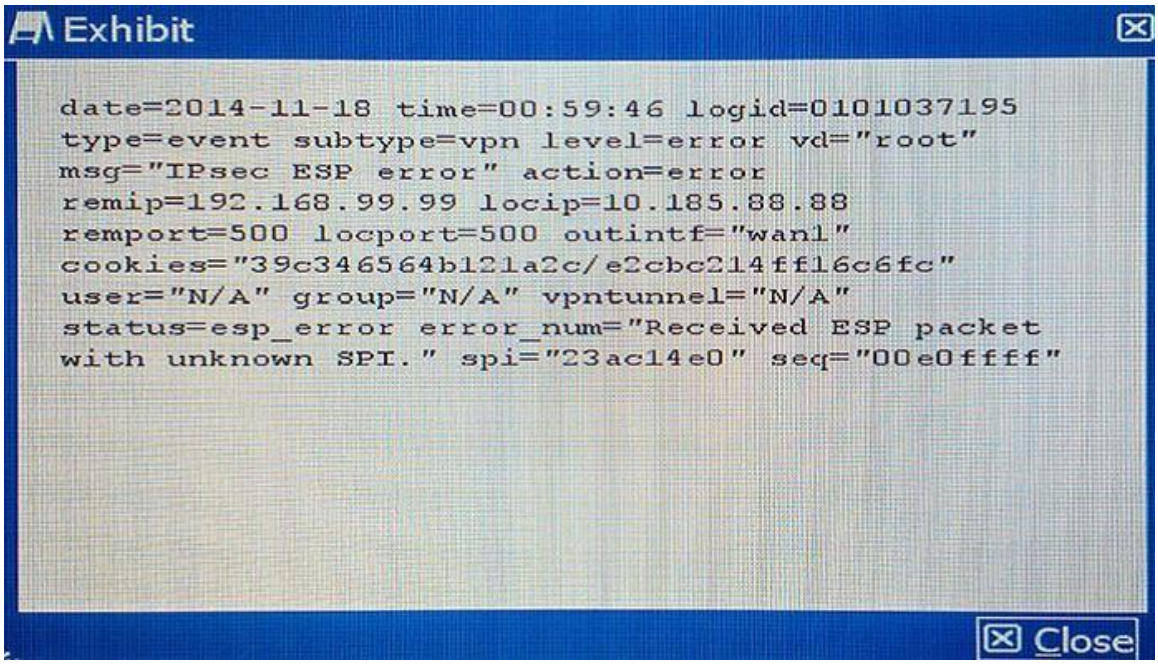
Vendor: Fortinet

Exam Code: NSE8

Exam Name: Fortinet Network Security Expert 8 Written Exam (800)

Version: DEMO

QUESTION 1
Referring to the exhibit, which statement is true?



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.

Answer: A

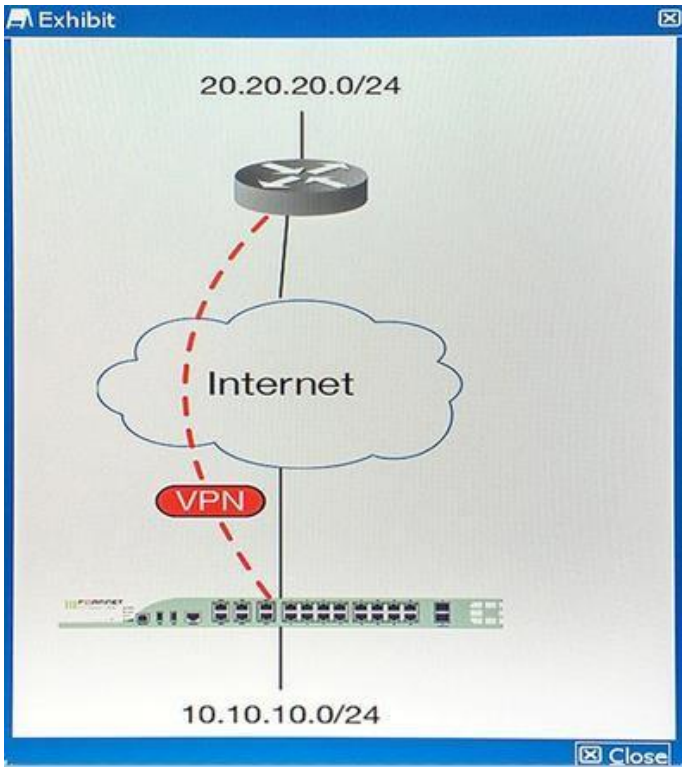
QUESTION 2
A cafe offers free Wi-Fi. Customers' portable electronic devices often do not have antivirus software installed and may be hosting worms without their knowledge.
You must protect all customers from any other customers' infected devices that join the same SSID.
Which step meets the requirement?

A. Enable deep SSH inspection with antivirus and IPS.
B. Use a captive portal to redirect unsecured connections such as HTTP and SMTP to their secured equivalents, preventing worms on infected clients from tampering with other customer traffic.
C. Use WPA2 encryption and configure a policy on FortiGate to block all traffic between clients.
D. Use WPA2 encryption, and enable "Block Intra-SSID Traffic".

Answer: B

QUESTION 3
You are asked to establish a VPN tunnel with a service provider using a third-party VPN device. The service provider has assigned subnet 30.30.30.0/24 for your outgoing traffic going towards the services hosted by the provider on network 20.20.20.0/24.
You have multiple computers which will be accessing the remote services hosted by the service

provider.
Which three configuration components meet these requirements? (Choose three.)



A. Configure an IP Pool of type Overload for range 30.30.30.10-30.30.30.10. Enable NAT on a policy from your LAN forwards the VPN tunnel and select that pool.
B. Configure IPsec phase 2 proxy IDs for a source of 10.10.10.0/24 and destination of 20.20.20.0/24.
C. Configure an IP Pool of Type One-to-One for range 30.30.30.10-30.30.30.10. Enable NAT on a policy from your LAN towards the VPN tunnel and select that pool.
D. Configure a static route towards the VPN tunnel for 20.20.20.0/24.
E. Configure IPsec phase 2 proxy IDs for a source of 30.30.30.0/24 and destination of 20.20.20.0/24.

Answer: C

QUESTION 4
You verified that application control is working from previous configured categories.
You just added Skype on blocked signatures. However, after applying the profile to your firewall policy, clients running Skype can still connect and use the application.
What are two causes of this problem? (Choose two.)

A. The application control database is not updated.
B. SSL inspection is not enabled.
C. A client on the network was already connected to the Skype network and serves as relay prior to configuration changes to block Skype
D. The FakeSkype.botnet signature is included on your application control sensor.

Answer: AB

QUESTION 5
Given the following FortiOS 5.2 commands:

```
config system global
     set strong-crypto enable
end
```

Which vulnerability is being addresses when managing FortiGate through an encrypted management protocol?

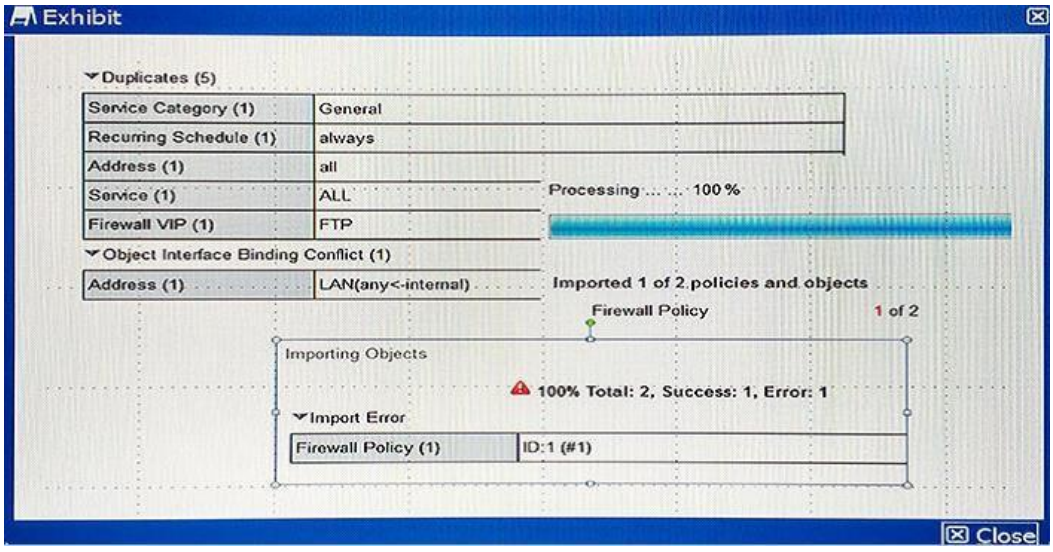
A. Remote Exploit Vulnerability in Bash (ShellShock)
B. Information Disclosure Vulnerability in OpenSSL (Heartbleed)
C. SSL v3 POODLE Vulnerability
D. SSL/TLS MITM vulnerability (CVE-2014-0224)

Answer: C

QUESTION 6
Given the following error message:

```
Start to import config from device(STUDENT-2) vdom(root) to adom(root), package(STUDENT-2)
"firewall service category",SUCCESS,"(name=General, oid=377, DUPLICATE)"
"firewall schedule recurring",SUCCESS,"(name=always, oid=473, DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=364, DUPLICATE)"
"firewall service custom",SUCCESS,"(name=ALL, oid=426, DUPLICATE)"
"firewall vip",SUCCESS,"(name=FTP, iod=475, DUPLICATE)"
"firewall policy",FAIL"(name=ID:1 (#1), oid=513, reason=interface binding contradiction)"
"firewall policy", SUCCESS,"(name=3, oid=514, new object)"
```

FortiManager fails to import policy ID 1.
What is the problem?



A. FortiManager already has Address LAN which has interface mapping set to "internal" in its database, it is contradicting with the STUDENT-2 FortiGate device which has address LAN mapped to "any".

B. FortiManager already has address LAN which has interface mapping set to "any" in its database; this conflicts with the STUDENT-2 FortiGate device which has address "LAN" mapped to "internal".
C. Policy ID 1 for this managed FortiGate device already exists on the FortiManager policy package named STUDENT-2.
D. Policy ID 1 does not have interface mapping on FortiManager.

Answer: D

QUESTION 7
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.

Answer: D

QUESTION 8
You are asked to design a secure solution using Fortinet products for a company. The company recently has Web servers that were exploited and defaced. The customer has also experienced Denial or Service due to SYN Flood attacks. Taking this into consideration, the customer's solution should have the following requirements:

```
- management requires network-based content filtering with man-in-the-
middle inspection
- the customer has no existing public key infrastructure but requires
centralized certificate management
- users are tracked by their active directory username without
installing any software on their hosts
- Web servers that have been exploited need to be protected from the OW
ASP Top 10
- notification of high volume SYN Flood attacks when a threshold has
been triggered.
```

Which three solutions satisfy these requirements? (Choose three.)

A. FortiGate
B. FortiCiient
C. FortiWeb
D. FortiAuthenticator
E. FortiDDOS

Answer: ACE

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: **STNAR2014**