Vendor: Cisco

Exam Code: 210-260

Exam Name: Implementing Cisco IOS Network Security (IINS v3.0) Exam

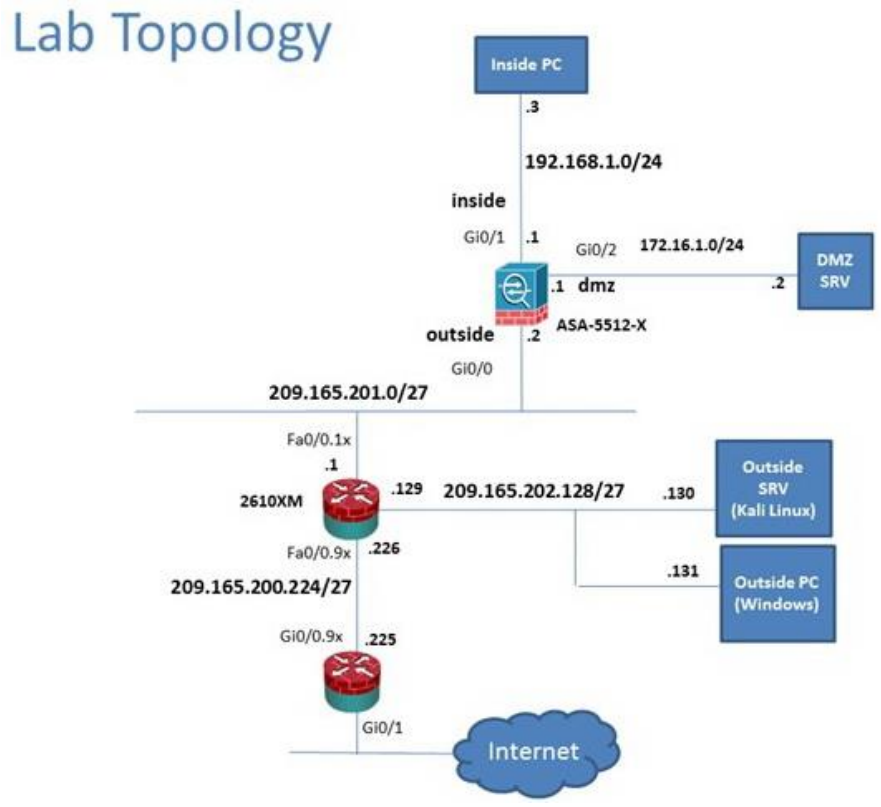
Version: DEMO

QUESTION 1
Which three statements about Cisco host-based IPS solution are true? (Choose three)

A. It work with deployed firewalls.
B. It can be deployed at the perimeter
C. It uses signature-based policies
D. It can have more restrictive policies than network-based IPS
E. It can generate alerts based on behavior at the desktop level
F. It can view encrypted files

Answer: ADF
Explanation:
The key word here is 'Cisco', and Cisco's host-based IPS, CSA, is NOT signature-based and CAN view encrypted files.

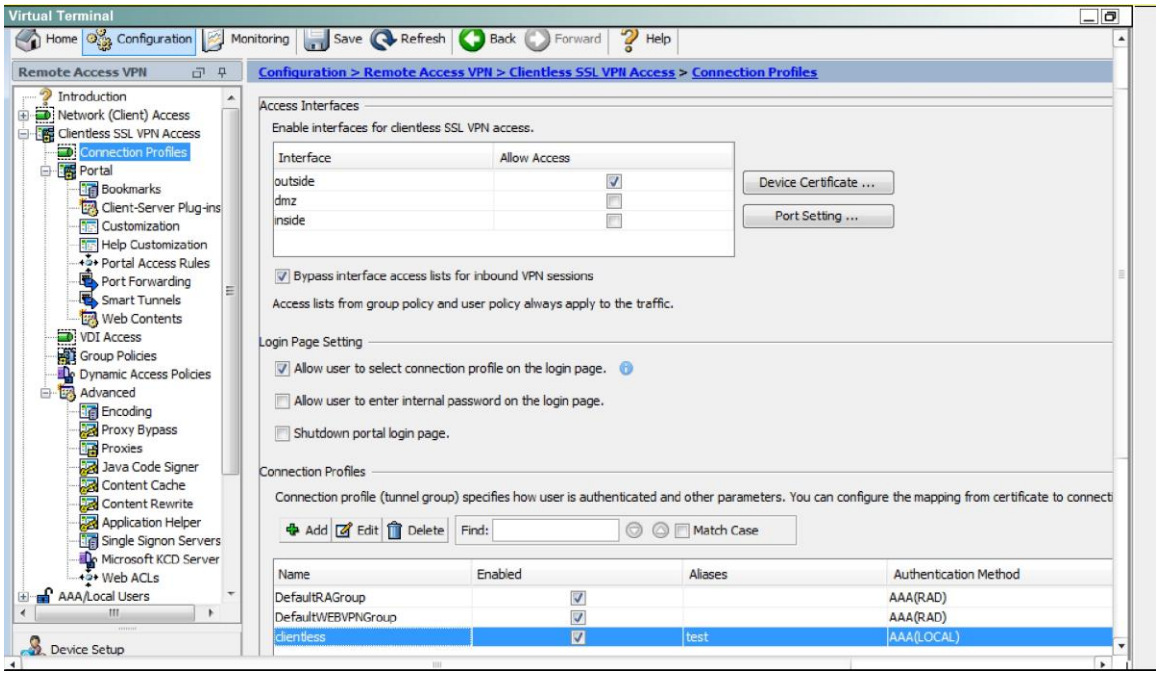
QUESTION 2
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.



Which user authentication method is used when users login to the Clientless SSL VPN portal using https://209165.201.2/test?

A. Both Certificate and AAA with LOCAL database
B. AAA with RADIUS server
C. Both Certificate and AAA with RADIUS server
D. AAA with LOCAL database
E. Certificate

Answer: D
Explanation:
This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration, where the alias of test is being used.



QUESTION 3
What are two users of SIEM software? (Choose two)

A. performing automatic network audits
B. configuring firewall and IDS devices
C. alerting administrators to security events in real time
D. scanning emails for suspicious attachments
E. collecting and archiving syslog data

Answer: CE
Explanation:
The other choices are not functions of SIEM software.

QUESTION 4
Which Sourfire secure action should you choose if you want to block only malicious traffic from a particular end-user?

A. Trust

B. Block
C. Allow without inspection
D. Monitor
E. Allow with inspection

Answer: E
Explanation:
Allow with Inspection allows all traffic except for malicious traffic from a particular end-user. The other options are too restrictive, too permissive, or don't exist.

QUESTION 5
Which two next-generation encryption algorithms does Cisco recommends? (Choose two)

A. SHA-384
B. MD5
C. DH-1024
D. DES
E. AES
F. 3DES

Answer: AE
Explanation:
From Cisco documentation:
A. SHA-384 - YES
B. MD5 - NO
C. DH-1024 - NO
D. DES - NO
E. AES - YES (CBC, or GCM modes)
F. 3DES - Legacy

QUESTION 6
How does a device on a network using ISE receive its digital certificate during the new-device registration process?

A. ISE acts as a SCEP proxy to enable the device to receive a certificate from a central CA server
B. The device request a new certificate directly from a central CA
C. ISE issues a pre-defined certificate from a local database
D. ISE issues a certificate from its internal CA server.

Answer: A
Explanation:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.pdf

QUESTION 7
Which three ESP fields can be encrypted during transmission? (Choose three)

A. Next Header
B. MAC Address
C. Padding

D. Pad Length
E. Sequence Number
F. Security Parameter Index

Answer: ACD
Explanation:
The last encrypted part is the Payload Data. The unencrypted parts are the Security Parameter Index and the Sequence Number.

QUESTION 8
You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP address Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

A. Create a custom blacklist to allow traffic
B. Create a whitelist and add the appropriate IP address to allow traffic.
C. Create a user based access control rule to allo the traffic.
D. Create a network based access control rule to allow the traffic.
E. Create a rule to bypass inspection to allow the traffic

Answer: C
Explanation:
Custom whitelists override blacklists and mitigate false positives.

QUESTION 9
Which EAP method uses protected Access Credentials?

A. EAP-TLS
B. EAP-PEAP
C. EAP-FAST
D. EAP-GTC

Answer: C

QUESTION 10
In which two situations should you use out-of-band management? (Choose two)

A. when a network device fails to forward packets
B. when management applications need concurrent access to the device
C. when you require ROMMON access
D. when you require adminstrator access from multiple locations
E. when the control plane fails to respond

Answer: AC

QUESTION 11
Refer to the exhibit while troubleshooting site-to-site VPN, you issued the show crypto isakamp sa command. What does the given output shows?

```
dst          src         state          conn-id     slot
10.10.10.2   10.1.1.5    MM_NO_STATE    1           0
```

A. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2
B. IKE Phase 1 main mode has successfully negotiate between 10.1.1.5 and10.10.10.2
C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2
D. IKE Phase 1 aggressive mode was create on 10.1.1.5, but it failed to negotiate with 10.10.10.2

Answer: A
Explanation:
The MM_NO_STATE state indicates that the phase 1 policy does not match on both sides, therefore main mode failed to negotiate. Aggressive mode is indicated by AG instead of MM.

QUESTION 12
What type of packet creates and performs network operations on a network device?

A. data plane packets
B. management plane packets
C. services plane packets
D. control plane packets

Answer: D

QUESTION 13
What is a valid implicit permit rule for traffic that is traversing the ASA firewall?

A. Unicast IPv6 traffic from a higher security interface to a lower security interface is permitted in transparent mode only
B. Only BPDUs from a higher security interface to a lower security interface are permitted in routed mode.
C. ARPs in both directions are permitted in transparent mode only
D. Unicast IPv4 traffic from a higher security interface to a lower security interface is permitted in routed mode only
E. Only BPDUs from a higher security interface to a lower security interface are permitted in transparent mode.

Answer: C
Explanation:
IPv4 and IPv6 traffic is permitted in both routed and transparent mode from higher to lower security interfaces.

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**