



Vendor: Cisco

Exam Code: 642-648

Exam Name: Deploying Cisco ASA VPN Solutions (VPN v2.0)

Version: DEMO

QUESTION 1

Authorization of a clientless SSL VPN defines the actions that a user may perform within a clientless SSL VPN session. Which statement is correct concerning the SSL VPN authorization process?

- A. Remote clients can be authorized by applying a dynamic access policy, which is configured on an external AAA server.
- B. Remote clients can be authorized externally by applying group parameters from an external database.
- C. Remote client authorization is supported by RADIUS and TACACS+ protocols.
- D. To configure external authorization, you must configure the Cisco ASA for cut-through proxy.

Answer: B

QUESTION 2

After adding a remote-access IPsec tunnel via the VPN wizard, an administrator needs to tune the IPsec policy parameters. Where is the correct place to tune the IPsec policy parameters in Cisco ASDM?

- A. IPsec user profile
- B. Crypto Map
- C. Group Policy
- D. IPsec Policy
- E. IKE Policy

Answer: B

QUESTION 3

Refer to the exhibit. While troubleshooting a remote-access application, a new NOC engineer received the logging message that is shown in the exhibit. Which configuration is most likely to be mismatched?

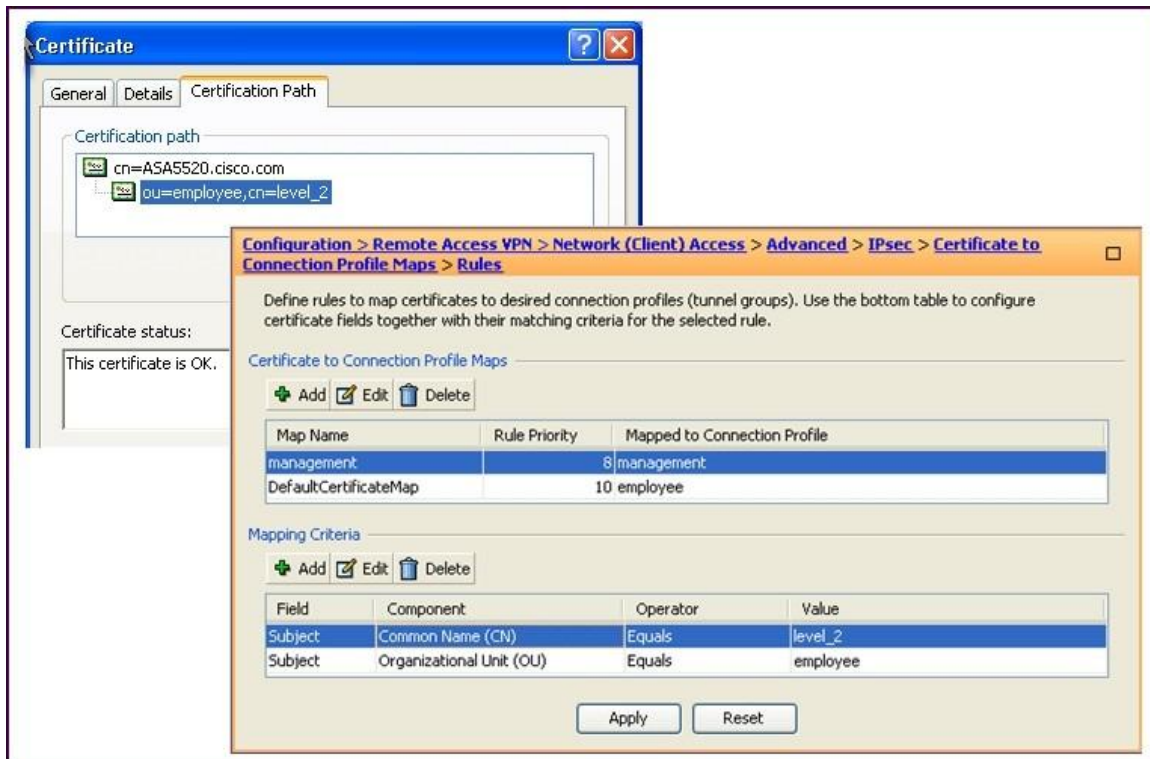
%ASA-5-713259: Group = contractor, Username = vpnuser, IP = 172.16.1.20, Session is being torn down. Reason: Phase 2 Mismatch

- A. IKE configuration
- B. extended authentication configuration
- C. IPsec configuration
- D. digital certificate configuration

Answer: C

QUESTION 4

Refer to the exhibit. The ABC Corporation is changing remote-user authentication from pre-shared keys to certificate-based authentication. For most employee authentication, its group membership (the employees) governs corporate access. Certain management personnel need access to more confidential servers. Access is based on the group and name, such as finance and level_2. When it is time to pilot the new authentication policy, a finance manager is able to access the department-assigned servers but cannot access the restricted servers. As the network engineer, where would you look for the problem?



- A. Check the validity of the identity and root certificate on the PC of the finance manager.
- B. Change the Management Certificate to Connection Profile Maps > Rule Priority to a number that is greater than 10.
- C. Check if the Management Certificate to Connection Profile Maps > Rules is configured correctly.
- D. Check if the Certificate to Connection Profile Maps > Policy is set correctly.

Answer: D

QUESTION 5

Refer to the exhibit. The user "contractor" inherits which VPN group policy?



- A. employee
- B. management
- C. DefaultWEBVPNGroup

- D. DfltGrpPolicy
- E. new_hire

Answer: D

QUESTION 6

Refer to the exhibit. In the CLI snippet that is shown, what is the function of the deny option in the access list?

```
access-list outside_cryptomap_1 line 1 extended deny tcp any host 10.0.4.4 eq https
access-list outside_cryptomap_1 line 1 extended permit tcp any host 10.0.4.0 255.255.255.0 eq https
crypto map outside_map 1 match address outside_cryptomap_1
```

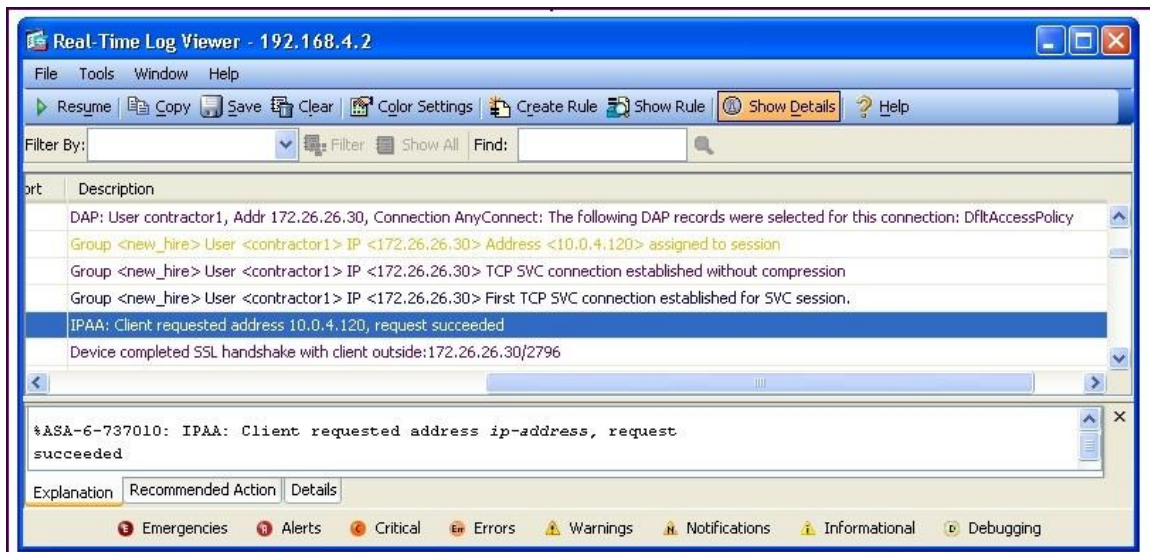
- A. When set in conjunction with outbound connection-type bidirectional, its function is to prevent the specified traffic from being protected by the crypto map entry.
- B. When set in conjunction with connection-type originate-only, its function is to instruct the Cisco ASA to deny specific inbound traffic if it is not encrypted.
- C. When set in conjunction with outbound connection-type answer-only, its function is to instruct the Cisco ASA to deny specific outbound traffic if it is not encrypted.
- D. When set in conjunction with connection-type originate-only, its function is to cause all IP traffic that matches the specified conditions to be protected by the crypto map.

Answer: A

QUESTION 7

Refer to the exhibit. A new NOC engineer, while viewing a real-time log from an SSL VPN tunnel, has a question about a line in the log.

The IP address 172.26.26.30 is attached to which interface in the network?



- A. the Cisco ASA physical interface
- B. the physical interface of the end user
- C. the Cisco ASA SSL VPN tunnel interface
- D. the SSL VPN tunnel interface of the end user

Answer: B

QUESTION 8

Refer to the exhibit. When the user "contractor" Cisco AnyConnect tunnel is established, what type of Cisco ASA user restrictions are applied to the tunnel?

Configuration > Remote Access VPN > AAA/Local Users > Local Users					
Create entries in the ASA local user database.					
Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization .					
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication .					
Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
employee1	15	Full	employee	-- Inherit Group Polic...	Add
manager1	2	No ASDM/CLI	management	-- Inherit Group Polic...	Edit
contractor	15	Full	-- Inherit Group Policy --	-- Inherit Group Polic...	Delete
contractor1	2	No ASDM/CLI	new_hire	-- Inherit Group Polic...	

- A. full restrictions (no Cisco ASDM, no CLI, no console access)
- B. full restrictions (no read, no write, no execute permissions)
- C. full restrictions (CLI show commands and Cisco ASDM monitoring permissions only)
- D. full access with no restrictions

Answer: D

QUESTION 9

Which statement regarding hashing is correct?

- A. MD5 produces a 64-bit message digest.
- B. SHA-1 produces a 160-bit message digest.
- C. MD5 takes more CPU cycles to compute than SHA-1.
- D. Changing 1 bit of the input to SHA-1 can change up to 5 bits in the output.

Answer: B

QUESTION 10

When initiating a new SSL or TLS session, the client receives the server SSL certificate and validates it. After validating the server certificate, what does the client use the certificate for?

- A. The client and server use the server public key to encrypt the SSL session data.
- B. The server creates a separate session key and sends it to the client. The client decrypts the session key by using the server public key.
- C. The client and server switch to a DH key exchange to establish a session key.
- D. The client generates a random session key, encrypts it with the server public key, and then sends it to the server.

Answer: D

QUESTION 11

When attempting to tunnel FTP traffic through a stateful firewall that might be performing NAT or PAT, which type of VPN tunneling should you use to allow the VPN traffic through the stateful firewall?

- A. clientless SSL VPN
- B. IPsec over TCP
- C. smart tunnel
- D. SSL VPN plug-ins

Answer: B

QUESTION 12

Refer to the exhibit. While troubleshooting on a remote-access VPN application, a new NOC engineer received the message that is shown. What is the most likely cause of the problem?

"ASA-5-722006: Group (contractor) User (vpnuser) IP (172.16.1.20) Invalid address (0.0.0.0)" assigned to SVC connection.

- A. The IP address that is assigned to the PC of the VPN user is not within the range of addresses that are assigned to the SVC connection.
- B. The IP address that is assigned to the PC of the VPN user is in use. The remote user needs to select a different host address within the range.
- C. The IP address that is assigned to the PC of the VPN user is in the wrong subnet. The remote user needs to select a different host number within the correct subnet.
- D. The IP address pool for contractors was not applied to their connection profile.

Answer: D

QUESTION 13

Which two statements about the Cisco ASA load balancing feature are correct? (Choose two.)

- A. The Cisco ASA load balances both site-to-site and remote-access VPN tunnels.
- B. The Cisco ASA load balances remote-access VPN tunnels only.
- C. The Cisco ASA load balances IPsec VPN tunnels only.
- D. The Cisco ASA load balances IPsec VPN and Cisco AnyConnect SSL VPN tunnels only.
- E. The Cisco ASA load balances IPsec VPN, clientless, and Cisco AnyConnect SSL VPN tunnels

Answer: BE

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>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives®

10% Discount Coupon Code: ASTR14