642-648 Q&As

Deploying Cisco ASA VPN Solutions (VPN v2.0)

Pass Cisco 642-648 Exam with 100% Guarantee

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

https://www.pass4lead.com/642-648.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The software-based Cisco IPsec VPN Client solution uses bidirectional authentication, in which the client authenticates the Cisco ASA, and the Cisco ASA authenticates the user. Which three methods are software-based Cisco IPsec VPN Client to Cisco ASA authentication methods? (Choose three.)

A. Unified Client Certificate authentication

B. Secure Unit authentication

C. Hybrid authentication

D. Certificate authentication

E. Group authentication

Correct Answer: CDE

ASDM user guide Page 35-69

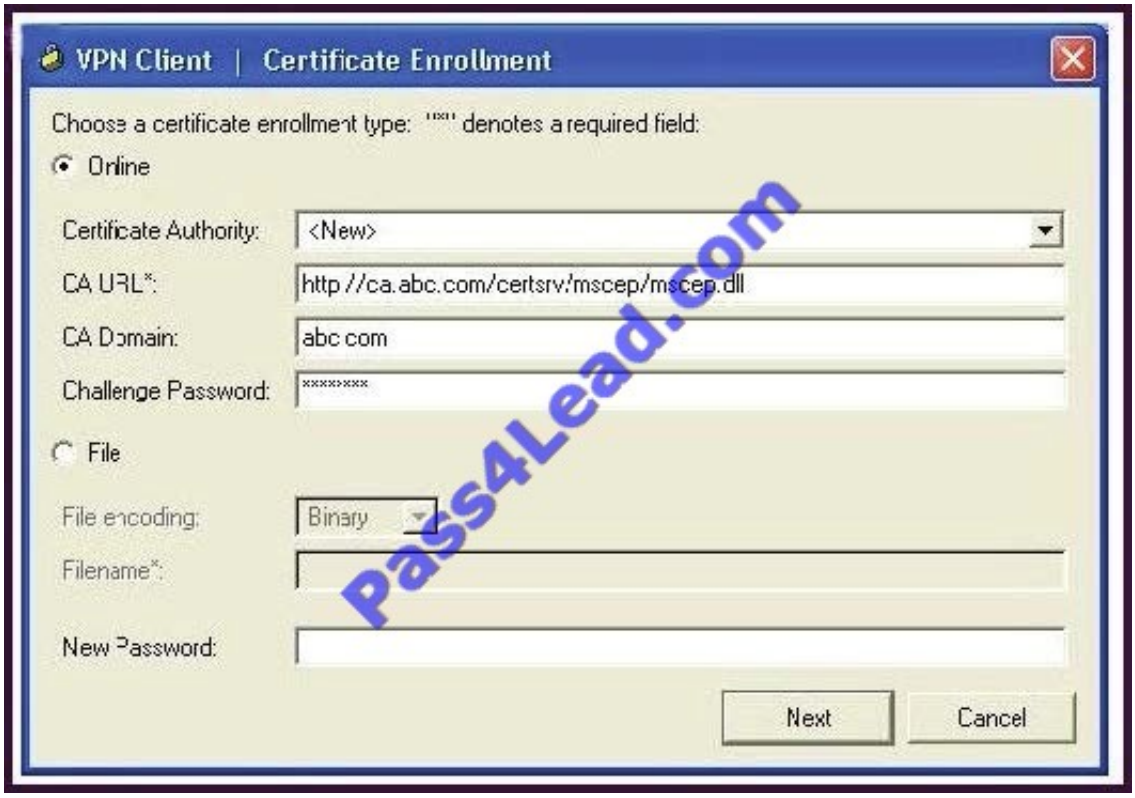
Authentication Mode--Specifies the authentication mode: none, xauth, or hybrid. hybrid--Specifies the use of Hybrid mode, which lets you use digital certificates for security appliance authentication and a different, legacy method--such as

RADIUS, TACACS+ or SecurID--for remote VPN user authentication. This mode breaks phase 1 of the Internet Key Exchange (IKE) into the following steps, together called hybrid authentication:

xauth--Specifies the use of IKE Extended Authentication mode, which provides the capability of authenticating a user within IKE using TACACS+ or RADIUS.

QUESTION 2

Refer to the exhibit.



You are configuring a laptop with the Cisco VPN Client, which uses digital certificates for authentication. Which protocol does the Cisco VPN Client use to retrieve the digital certificate from the CA server?

A. FTP

B. LDAP

C. HTTPS

D. SCEP

E. OCSP

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

About CRLs Certificate Revocation Lists provide the security appliance with one means of determining whether a certificate that is within its valid time range has been revoked by its issuing CA. CRL configuration is a part of the configuration of a trustpoint.

You can configure the security appliance to make CRL checks mandatory when authenticating a certificate (revocation-check crl command). You can also make the CRL check optional by adding the none argument (revocation-check crl none command), which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data. The security appliance can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a length of time configurable for each trustpoint. When the security appliance has cached a CRL for more than the length of time it is configured to cache CRLs, the security appliance considers the CRL too old to be reliable, or "stale". The security appliance attempts to retrieve a newer version of the CRL the next time a certificate authentication requires checking the stale CRL.

QUESTION 3

You have been using pre-shared keys for IKE authentication on your VPN. Your network has grown rapidly, and now you need to create VPNs with numerous IPsec peers. How can you enable scaling to numerous IPsec peers?

A. Migrate to external CA-based digital certificate authentication.

B. Migrate to a load-balancing server.

C. Migrate to a shared license server.

D. Migrate from IPsec to SSL VPN client extended authentication.

Correct Answer: A

QUESTION 4

You have just configured new clientless SSL VPN access parameters.

However, when users connect, they are not getting the expected access that was configured.

What is one possible reason this is occurring?

A. The correct Tunnel Group Lock is not properly set.

B. The corresponding Cisco ASA interface is not enabled for SSL VPN access.

C. The Connection Alias is not enabled.

D. Portal features are disabled.

Correct Answer: A

QUESTION 5

When configuring dead peer detection for remote-access VPN, what does the confidence level parameter represent?

A. It specifies the number of seconds the adaptive security appliance should allow a peer to idle before beginning keepalive monitoring.

B. It specifies the number of seconds to wait between IKE keepalive retries.

C. The higher the number, the more reliable the link is.

D. It is determined dynamically based on reliability, uptime, and load.

Correct Answer: A

```
Chicago(config)# crypto map outside_map 10 set connection-type originate-only
```

ISAKMP Keepalives

The ISAKMP keepalives feature is a way to determine whether the remote VPN peer is still reachable or there are any lingering SAs (SAs that do not get cleared properly). By default, Cisco ASA starts sending Dead Peer Detection (DPD) packets after it stops receiving encrypted traffic over the tunnel from the peer. If it does not hear from its peer for 10 seconds (confidence interval), it sends out a DPD R_U_THERE packet. It keeps sending the R_U_THERE packets every 2 seconds (the retry interval). If it does not receive R_U_THERE_ACK for four consecutive DPDs polling periods, the security appliance deletes the corresponding ISAKMP and IPSec SAs.

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.pass4lead.com/allproducts

Need Help

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