



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.pass4itsure.com/642-648.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Refer to the exhibit.

```
tunnel-group BASIC-ANYCONNECT-PROFILE general-attributes
 authentication-server-group MY-RADIUS-SVRS
 secondary-authentication-server-group MY-LDAP-SVRS
!
tunnel-group BASIC-ANYCONNECT-PROFILE webvpn-attributes
 authentication aaa
```



Given the example that is shown, what can you determine?

- A. Users are required to perform RADIUS or LDAP authentication when connecting with the Cisco AnyConnect client.
- B. Users are required to perform AAA authentication when connecting via WebVPN.
- C. Users are required to perform double AAA authentication.
- D. The user access identity is prefilled at login, requiring users to enter only their password.

Correct Answer: C

QUESTION 2

Which four parameters must be defined in an ISAKMP policy when you are creating an IPsec site-to-site VPN using the Cisco ASDM? (Choose four.)

- A. encryption algorithm
- B. hash algorithm
- C. authentication method
- D. IP address of remote IPsec peer
- E. D-H group
- F. perfect forward secrecy

Correct Answer: ABCE

ASDM User guide Page 34-5 Should this not be IKE policy?



Fields

Priority #—Type a number to set a priority for the IKE policy. The range is 1 to 65,543, with 1 the highest priority.

Encryption—Select an encryption method. This is a symmetric encryption method that protects data transmitted between two IPsec peers. The choices follow:

des	56-bit DES-CBC. Less secure but faster than the alternatives. The default.
3des	168-bit Triple DES.
aes	128-bit AES.
aes-192	192-bit AES.
aes-256	256-bit AES.

Hash—Select the hash algorithm that ensures data integrity. It ensures that a packet comes from whom you think it comes from, and that it has not been modified in transit.

sha	SHA-1	The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	

Authentication—Select the authentication method the security appliance uses to establish the identity of each IPsec peer. Pre-shared keys do not scale well with a growing network but are easier to set up in a small network. The choices follow:

pre-share	Pre-shared keys.
-----------	------------------





rsa-sig	A digital certificate with keys generated by the RSA signatures algorithm.
crack	IKE Challenge/Response for Authenticated Cryptographic Keys protocol for mobile IPsec-enabled clients which use authentication techniques other than certificates.

D-H Group—Select the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other.

1	Group 1 (768-bit)	The default, Group 2 (1024-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 2 or 5.
2	Group 2 (1024-bit)	
5	Group 5 (1536-bit)	
7	Group 7 (Elliptical curve field size is 163 bits.)	Group 7 is for use with the Movian VPN client, but with any peer that supports Group 7 (ECC).

Lifetime (secs)—Either select Unlimited or type an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the security appliance sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Time Measure—Select a time measure. The security appliance accepts the following values:

- 120 - 86,400 seconds
- 2 - 1440 minutes
- 1 - 24 hours
- 1 day



QUESTION 3

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 4

You are configuring bookmarks for the clientless SSL VPN portal without the use of plug-ins.

Which three bookmark types are supported? (Choose three.)


- A. RDP
- B. HTTP
- C. FTP
- D. CIFS
- E. SSH
- F. Telnet

Correct Answer: BCD

http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html#w p1227212

QUESTION 5

Refer to the exhibit.

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

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?

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

Correct Answer: C

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtmland %ASA-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down. Reason: reason The termination



reason for the ISAKMP session appears, which occurs when the session is torn down through session management. ?roupname--The tunnel group of the session being terminated ?ername--The username of the session being terminated ?eerIP--The peer address of the session being terminated ?eason--The RADIUS termination reason of the session being terminated. Reasons include the following:

- Port Preempted (simultaneous logins)
- Idle Timeout
- Max Time Exceeded
- Administrator Reset

[Latest 642-648 Dumps](#)

[642-648 VCE Dumps](#)

[642-648 Study Guide](#)



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.pass4itsure.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4itsure, All Rights Reserved.