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.lead4pass.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

In which three ways can a Cisco ASA security appliance obtain a certificate revocation list? (Choose three.)

A. FTP

B. SCEP

C. TFTP

D. HTTP

E. LDAP

F. SCP

Correct Answer: BDE

CRLs

CRLs provide the ASA with one way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. CRL configuration is part of configuration of a trustpoint.

You can configure the ASA to make CRL checks mandatory when authenticating a certificate by using the revocation-check crl command. You can also make the CRL check optional by using the revocation-check crl none command, which

allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

The ASA can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a configurable amount of time for each trustpoint.

When the ASA has cached a CRL for longer than the amount of time it is configured to cache CRLs, the ASA considers the CRL too old to be reliable, or "stale." The ASA tries to retrieve a newer version of the CRL the next time that a

certificate authentication requires a check of the stale CRL.

The ASA caches CRLs for an amount of time determined by the following two factors:

?he number of minutes specified with the cache-time command. The default value is 60 minutes. ?he NextUpdate field in the CRLs retrieved, which may be absent from CRLs. You control whether the ASA requires and uses the NextUpdate

field with the enforcenextupdate command. The ASA uses these two factors in the following ways:

?f the NextUpdate field is not required, the ASA marks CRLs as stale after the length of time defined by the cache-time command.?f the NextUpdate field is required, the ASA marks CRLs as stale at the sooner of the two times specified by

the cache-time command and the NextUpdate field. For example, if the cache-time command is set to 100 minutes and the NextUpdate field specifies that the next update is 70 minutes away, the ASA marks CRLs as stale in 70 minutes.

QUESTION 2

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

A. Cisco IPsec VPN SW Client > Client Profile

B. IPsec User Profile

C. Group Policy

D. IKE Policy

E. Crypto Map

Correct Answer: D

QUESTION 3

Your IT department needs to run a custom-built TCP application within the clientless SSL VPN tunnel. The network administrator suggests running the smart tunnel application. Which three statements concerning smart tunnel applications are true? (Choose three.)

A. They support active FTP and other RTSP-based applications.

B. They do not require administrator privileges on the remote system.

C. They require the enabling of port forwarding.

D. They are supported on Windows and MAC OS X platforms.

E. They support native client applications over SSL VPN.

F. They require the modification of the Host file on the end-user PC.

Correct Answer: BDE

Smart Tunnel--Connects a Winsock 2, TCP-based application installed on the end station to a server on the intranet, using a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the security appliance

as a proxy server. Smart Tunnel List--Select the list name from the drop-down menu if you want to provide smart tunnel access.

Assigning a smart tunnel list to a group policy or username enables smart tunnel access for all users whose sessions are associated with the group policy or username, but restricts smart tunnel access to the applications specified in the list.

To view, add, modify, or delete a smart tunnel list, click the adjacent Manage button. Auto Start (Smart Tunnel List)--Check to start smart tunnel access automatically upon user login. Uncheck to enable smart tunnel access upon user login,

but require the user to start it manually, using the Application Access > Start Smart Tunnels button on the Clientless SSL VPN Portal Page. Auto Sign-on Server List--Select the list name from the drop-down menu if you want to reissue the

user credentials when the user establishes a smart tunnel connection to a server. Each smart tunnel auto sign-on list

entry identifies a server with which to automate the submission of user credentials. To view, add, modify, or delete a smart

tunnel auto sign-on list, click the adjacent Manage button.

Domain Name (Optional)--Specify the Windows domain to add it to the username during auto sign-on, if the universal naming convention (domain\username) is required for authentication. For example, enter CISCO to specify CISCO\jsmith

when authenticating for the username jsmith. You must also check the "Use Windows domain name with user name" option when configuring associated entries in the auto sign-on server list.

QUESTION 4

Cisco Secure Desktop seeks to minimize the risks that are posed by the use of remote devices in establishing a Cisco clientless SSL VPN or Cisco AnyConnect VPN Client session. Which two statements concerning the Cisco Secure Desktop Host Scan feature are correct? (Choose two.)

A. It is performed before a user establishes a connection to the Cisco ASA.

B. It is performed after a user establishes a connection to the Cisco ASA but before logging in.

C. It is performed after a user logs in but before a group profile is applied.

D. It is supported on endpoints that run a Windows operating system only.

E. It is supported on endpoints that run Windows and MAC operating systems only.

F. It is supported on endpoints that run Windows, MAC, and Linux operating systems.

Correct Answer: BF

DAP and Anti-Virus, Anti-Spyware, and Personal Firewall Programs The security appliance uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Pre login Assessment and Host Scan modules

of Cisco Secure Desktop return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to select a DAP record that matches the values of those attributes. Most, but not all,

anti-virus, anti-spyware, and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. Host Scan checks to see if an endpoint has a program installed, and if it is

memory resident as follows:

?If the installed program does not support active scan, Host Scan reports the presence of the software. The DAP system selects DAP records that specify the program. ?If the installed program does support active scan, and active scan is

enabled for the program, Host Scan reports the presence of the software. Again the security appliance selects DAP records that specify the program.

?If the installed program does support active scan and active scan is disabled for the program, Host Scan ignores the presence of the software. The security appliance does not select DAP records that specify the program. Further, the output

of the debug trace command, which includes a lot of information about DAP, does not indicate the program presence, even though it is installed.

The following sequence outlines a typical remote access connection establishment.

1.

A remote client attempts a VPN connection.

2.

The security appliance performs posture assessment, using configured NAC and Cisco Secure Desktop Host Scan values.

Operating system support

?Microsoft Windows 2000, Windows XP, or Windows Vista ?Macintosh OS X 10.4.6

?Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)

3.

The security appliance authenticates the user via AAA. The AAA server also returns authorization attributes for the user.

4.

The security appliance applies AAA authorization attributes to the session, and establishes the VPN tunnel.

5.

The security appliance selects DAP records based on the user AAA authorization information and the session posture assessment information. 6. The security appliance aggregates DAP attributes from the selected DAP records, and they

become the DAP policy.

7. The security appliance applies the DAP policy to the session.

QUESTION 5

Which three options are characteristics of WebType ACLs? (Choose three.)

A. They are assigned per-connection profile.

B. They are assigned per-user or per-group policy.

C. They can be defined in the Cisco AnyConnect Profile Editor.

D. They support URL pattern matching.

E. They support implicit deny all at the end of the ACL.

F. They support standard and extended WebType ACLs.

Correct Answer: BDE

You can configure ACLs (Access Control Lists) to apply to user sessions. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers. ?If you do not define any filters, all connections are permitted. ? The security appliance supports only an inbound ACL on an interface. ?At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), the security appliance denies it. ACEs are referred to as rules in this topic. This pane lets you add and edit ACLs to be used for Clientless SSL VPN sessions, and the ACL entries each ACL contains. It also displays summary information about ACLs and ACEs, and lets you enable or disable them, and change their priority order.

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.lead4pass.com/allproducts

Need Help

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