

GlobalTcert

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

© Copy Right 1998-2005 GlobalTcert LLC. All Rights Reserved.

particular city to a single administrator. This administrator will be responsible for all user, group, and resource management for only the branch offices in his or her city.

Help desk personnel require the ability to perform limited administrative tasks in the la.corp.woodgrovebank.com domain and the den.corp.woodgrovebank.com domain. These tasks include resetting users' passwords and creating new user accounts for branch office users. Help desk personnel must not be able to perform any other administrative tasks.

Network Infrastructure

The following network infrastructure requirements must be considered:

All connections made over the frame-relay WAN connections must be encrypted and authenticated. Certificate Services must be installed on at least one server in each domain. The configuration of CAs must be based on the needs of each domain.

A Software Update Services (SUS) server must be installed in each regional office domain. The Microsoft Baseline Security Analyzer (MBSA) must be deployed to all computers in each domain.

Case Study #5, Woodgrove Bank (8 Questions)

QUESTION 1

You need to design a remote access strategy for the customer support users when they work from home. Your solution must meet security requirements.

What should you do?

- A. Deploy an L2TP/IPsec VPN server in each call center. Configure the portable computers as L2TP VPN clients.
- B. Create IPSec tunnel mode connections between the customer support users home and the company's Internet-facing routers.
- C. Create IP packet filters on the company's Internet-facing routers to allow the Remote Desktop Protocol (RDP). Create IPSec filters on the terminal servers to allow only connections that use RDP.
- D. Create IP packet filters on the company's Internet-facing routers to allow the IPSec protocols. Assign the Secure Server (Require Security) IPSec policy to the terminal servers. Assign the Client (Respond only) IPSec policy to the portable computers.

Answer: A

Explanation: L2TP can encapsulate PPP frames just as PPTP can, but in contrast can then be sent over IP, ATM, or Frame Relay. It is rather more complicated than PPTP, and it is more secure.

Here's how the L2TP/IPSec combination works:

1. The client and server establish an IPSec security association using the ISAKMP and Oakley protocols. At this point, the two machines have an encrypted channel between them.
2. The client builds a new L2TP tunnel to the server. Because this happens after the channel has been encrypted, there's no security risk.
3. The server sends an authentication challenge to the client.
4. The client encrypts its answer to the challenge and returns it to the server.
5. The server checks the challenge response to see whether or not it's valid; if so, the server can determine which account is connecting. Subject to whatever access policies you've put in place, at this point the server can accept the inbound connection.

Steps 3 through 5 mirror the steps for PPTP tunneling. This is because the authorization process is a function of

the remote access server, not the VPN stack. All the VPN does is provide a secure communications channel, and something else has to decide who gets to use it.

Bottom line: L2TP with IPsec to provide for higher layer encapsulation and encryption features necessary for VPN connectivity. This combination is known as L2TP/IPsec.

Requirements for an L2TP implementation of a LAN-to-LAN VPN: First, a user certificate needs to be installed on the calling router, and a computer certificate needs to be installed on the answering router.

Now consider the following:

Woodgrove Bank operates a 24-hour call center to support customers and partners.

The Los Angeles and Denver offices each maintain a customer support call center.

IT personnel must be able to connect to the network from home. All connections made by IT personnel from outside the network must use the strongest available encryption and authentication methods.

You would thus need to deploy a L2TP/IPsec VPN server in each call centre and configure the portable computers as L2TP VPN clients so as to comply with security requirements.

Incorrect answers:

B: Creating IPsec tunnel mode connections between customer support users home and the company's Internetfacing

routers is not going to comply with all the security requirements. A L2TP/IPsec VPN connection will be more suitable and secure.

C: This option does not comply with security requirements as stated in the case study.

D: Deploying a L2TP/IPsec VPN server in each call centre and configure the portable computers as L2TP VPN client would be the best option and not just simply assigning IPsec policy.

Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, p. 335

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 7, pp. 433-438

QUESTION 2

You need to design an access control strategy for resources that are located in the extranet for partners and for internal users. Your solution must meet business and security requirements.

What should you do?

A. Create a new child domain named extranet.corp.woodgrovebank.com in the existing forest.

Create user accounts for users from partner companies in the new child domain.

Create shortcut trusts in which the child domain trusts every domain in the forest.

B. Create a new forest and domain named extranet.woodgrovebank.com.

Create user accounts for users from partner companies in the new domain.

Create a one-way forest trust relationship in which the extranet forest trusts the company forest.

C. Create a new forest and domain named extranet.woodgrovebank.com.

Create user accounts for users from partner companies in the new domain.

Create an external trust relationship in which the extranet domain trusts the den.corp.woodgrovebank.com domain.

D. Create a child domain of the den.corp.woodgrovebank.com domain for the extranet.

Create user accounts for users from partner companies in the new child domain.

Create an external trust relationship in which the forest root domain trusts the extranet domain.

Answer: B

Explanation: Windows Server 2003 allows trust relationships between separate Active Directory forests. Forest trusts act much like domain trusts, except that they extend to every domain in two forests. Domains are connected to one another through logical structure relationships. The relationships are implemented through domain trees and domain forests.

A domain tree is a hierarchical organization of domains in a single, contiguous namespace. In the Active Directory, a tree is a hierarchy of domains that are connected to each other through a series of trust relationships (logical links that combine two or more domains into a single administrative unit). The advantage of using trust relationships between domains is that they allow users in one domain to access resources in another domain, assuming the users have the proper access rights.

A forest is a set of trees that does not form a contiguous namespace. For example, you might have a forest if your company merged with another company. With a forest, you could each maintain a separate corporate identity through your namespace, but share information across Active Directory.

Woodgrove Bank operates a 24-hour call center to support customers and partners.

Woodgrove Bank partners with an external auditing company to provide audit services for customers.

The user from the audit company have access to the extranet in the Denver office. These users need to be able to access file resources that are located on a server on the Denver internal network named Server1.

Users from Partner companies require access to information stored on a Microsoft SQL Server 2000 computer that is located on the Denver internal network. Users on the internal network must also be able to access the information on the SQL Server by using Microsoft Access 2000.

Thus you would design your access control strategy by creating extranet.woodgrovebank.com, a new forest and domain. After which you create user accounts for the users from the partner companies in the new domain and then create a one-way forest trust relationship in which the extranet forest trusts the company forest.

Incorrect answers:

A: Child domains are not necessary. Furthermore shortcut trusts will not meet business and security requirements. What is necessary is a new forest and domain and a one-way trust in which the extranet forest trusts the company forest.

C: An external trust relationship is unnecessarily risky and will not comply with security requirements.

D: This will not work for the reasons stated in A and C above.

Reference:

Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows (r) Server 2003 Environment Management and Maintenance Study Guide, p. 20

QUESTION 3

You need to design a remote access authentication strategy that will allow users in the IT department to remotely connect to the network. Your solution must meet security requirements.

What should you do?

A. Install Internet Authentication Services (IAS) on a server in the den.corp.woodgrovebank.com domain. Configure the VPN servers as RADIUS clients.

B. Install Internet Authentication Services (IAS) on a stand-alone server in the Denver extranet. Create local user accounts for the IT personnel on the IAS server. Configure the VPN servers as RADIUS clients.

C. Create a remote access policy on each of the VPN servers.