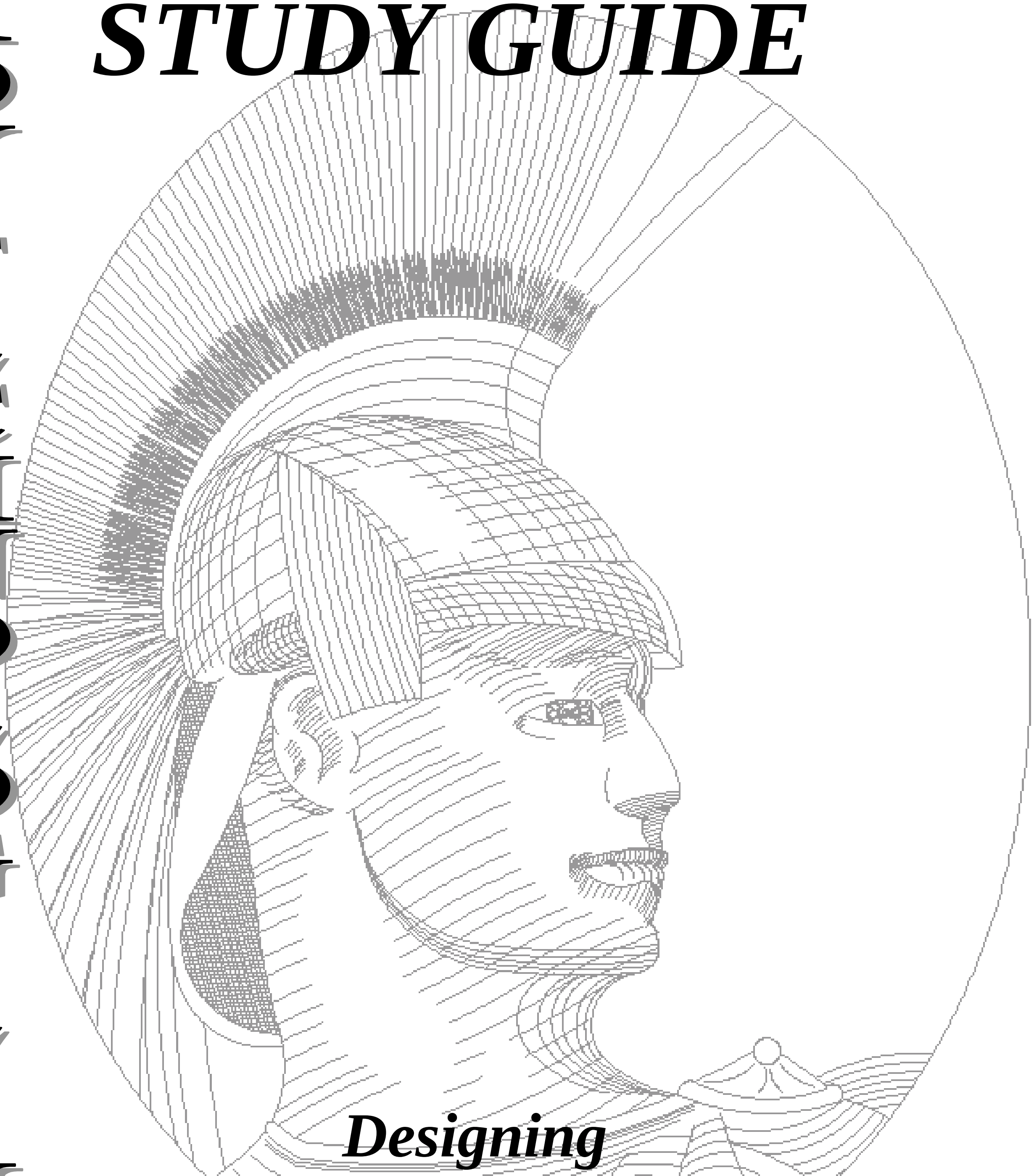
TROY TECHNOLOGIES USA

MCSE STUDY GUIDE



Designing Microsoft Windows 2000 Network Security Exam 70-220

Edition 2

Congratulations!!

You have purchased a ***Troy Technologies USA*** Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official Designing Microsoft Windows 2000 Network Security MCSE exam. Study and memorize the following concepts, questions and answers for approximately 10 to 12 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 10 to 12 hours and then you are ready!!!

GOOD LUCK!

Guarantee

If you use this study guide correctly and still fail the exam, send your official score notice and mailing address to:

Troy Technologies USA
8200 Pat Booker Rd. #368
San Antonio, TX 78233

We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

Table of Contents

Designing Windows 2000 Network Security Concepts

Analyzing Technical Requirements

You must assess how directory services will impact the technical aspects of the network infrastructure. These aspects include performance and stability. You should evaluate the company's existing and planned technical environment. You should attempt to predict the impact of the Active Directory design on the existing and planned technical environment. The following factors are critical:

- Available connectivity between the geographic locations of sites
- Available network bandwidth and latency
- Company size
- Existing and planned network and systems management
- Existing methods for accessing data and systems
- Network roles and responsibilities
- Performance requirements
- Technical support structure
- User and resource distribution

EVALUATING THE EXISTING AND PLANNED TECHNICAL ENVIRONMENT

Areas you will want to consider in assessing the existing technical environment and developing a plan for the transition to Windows 2000 include:

- Proactive training of users before the rollout of the new operating system.
- Training of all technical personnel on the new operating system and how to use the directory services.
- Written documentation to aid in assisting users with common problems, and documenting reported problems.

Analyzing Company Size and User and Resource Distribution

The geographic scope plays an important part of designing your Directory Services. You must take into account the size and geographic location of all parts of the company. Analysis should also include the size and distribution of users, both internal and external. Resource allocation for peripherals and server access must be determined. Connectivity issues across geographic locations and within sites must also be documented. Identify if users are connecting for authentication only or for the entire session as with a Terminal Server.

Assessing Available Connectivity and Bandwidth

You must work closely with the network operations team to assess network connectivity and performance based on reliability, capacity, and latency. Reliability is how dependable the network link is. Capacity is the ability of the connection to transfer data packets. Bandwidth is the theoretical capacity of the network connection. Latency, or delay, is the delay of how long it takes to get data from one point to another.

Performance Requirements

To obtain peak performance, you must assess performance requirements, and create a baseline from which to judge future modifications. You must determine peak utilization, the type of circuits used, application requirements, and resource conflicts. During this analysis, identify any bottlenecks or potential performance hazards.

Analyzing Data and System Access Patterns

In your analysis, you need to determine if all resources are centralized or remotely disbursed. Frequently used resources should be across a highly reliable connection. You must determine if users should go through a firewall, or if they need to use encryption. Authentication can be accomplished through the use of the following:

CHAP	Challenge Handshake Authentication Protocol. Does not use clear-text passwords.
EAP	Extensible Authentication Protocol. The client and the server negotiate the protocol that will be used. Protocols include one-time passwords, username / password combinations, or access tokens.
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol. Requires the client to be using a Microsoft Operating System (Version 2), or other compatible OSs (Version 1).
PAP	Password Authentication Protocol. Uses a plain-text password authentication method and should only be used if clients cannot handle encryption.
SPAP	Shiva Password Authentication Protocol. For backward-compatibility and is not favored for new installations.

Analyzing Network Roles and Responsibilities

Administrative roles are predefined by the operating system with additional responsibilities above the normal user. Administrative type roles include Backup Operator, Server Operator, Print Operator, and Account Operator. Service roles run as services, without user interaction, in the operating system. User roles include the right to logon and use network resources. Other roles include being an application, a group, or owner.

Analyzing Security Considerations

The most effective means of implementing security with Windows 2000 clients is through the use of Group Policies. You must analyze security considerations and provide information about access to data and resources, password policies, security protocols (IPSec), disaster recover, and authentication. You must analyze what are the needs of the organization, and what operating systems does the organization support. In the analysis, ensure that all potential solutions will not conflict with existing third-party tools and applications.

ANALYZING THE IMPACT OF SECURITY DESIGN

Assessing Existing Systems and Applications

To provide high levels of security, Windows 2000 provides the following security features: IPSec, L2TP, Kerberos, an Encrypting Files system (EFS), public key infrastructure, RADIUS, smart card support, and security groups. You need to understand current server applications that may require service packs or patches. You should compile a list of all routers, modems, and remote access servers. This list should include BIOS settings, peripheral device configurations, and driver versions. Determine if current hardware or software is not working due to security reasons. Examine non-Windows NT DNS servers for their implementation of dynamic registration and service (SRV) resource records.

Identifying Upgrades and Rollouts

Identify upgrades and rollouts that are currently in progress. Inquire about and document anything in a planning stage.

Analyze Technical Support Structure

You must determine what kind of support is available, how it's managed, and the level of support staff expertise is.

Analyze Existing and Planned Network and Systems Management

In analyzing the network and systems management, you must document existing policy and guidelines on security. This will help you to determine requirements for appropriate network usage. You must indicate Internet access, all users and their purpose for the Internet access. Document existing policies in place regarding partner access to company networks, whether they are able to access the entire work as recognized users or as anonymous users. Document if encryption and security standards in place or planned, password standards, domain structure, and trust relationships. Identify what security protocols are implemented on the network, (SSL, IPSec or PPTP. Indicate authentication methods for Internet users, dial-up users, and access across WAN links.

Analyzing Security Requirements

DESIGNING A SECURITY BASELINE

DOMAIN CONTROLLERS BASELINE

A domain controller is a Windows 2000 Server that has been configured using the Active Directory Installation Wizard. All Windows 2000 domain controllers store writeable directories. The domain controller manages authentication, user logon processing, directory searches and storage of directory data. You may choose to have several domains to ensure high availability and fault tolerance. The default installation for Windows 2000 Server and Advanced Server is the standalone server model. Servers may be promoted to domain controller status or may be demoted by running the dcpromo wizard.

OPERATIONS MASTERS

Limiting the role of a domain controller may improve performance. The five operations master roles can be assigned to one or more domain controllers. The roles are schema master, domain naming master, relative ID master, primary domain controller (PDC) emulator, and infrastructure master. There can be only one schema master and one domain naming master in the forest at one time. The schema master controls updates and modifications to the schema. To change the forest schema, you must have access to this domain controller and be a member of the Schema Admins group. The domain naming master is in charge of additions and deletions of domains in the forest and of sites. The domain naming master should be located on a system that also contains the Global Catalog. Three roles are domain-wide. There can be only one PDC emulator, one infrastructure master, and one relative ID master in a domain at one time. The relative ID master allocates relative ID sequences to each domain controller. Each new user, group, or computer in a domain gets a unique security ID composed of a unique domain security ID and a relative ID. The relative ID master operations master is required to move objects within domains using the movetree.exe command. The infrastructure master updates the group-to-user references when group members are changed. The infrastructure master compares its data to the Global Catalog data and requests changes. It then replicates this information to other domain controllers in the domain. The PDC emulator acts as a Windows NT PDC if non-Windows 2000 clients are in the domain, or if Windows NT BDCs are present. It can process password changes and replicate updates to the BDCs. The infrastructure master and the Global Catalog host should not be the same domain controller.

APPLICATION SERVERS

The security baseline settings for application servers will depend on the server applications that are running. If the application meets the specification for the Windows 2000 logo, then all users should be members of the Users group. By default, Windows 2000 assigns some non-administration rights and access. This includes making the Authenticated Users group a member of the Power Users group for servers. You can remove this setting to further secure servers on which only logo applications are run. If the applications running on the system do not meet the logo requirements, you may have to make all users Power Users to allow them to run the applications. Another way to do this is to use the compatws template.

FILE AND PRINT SERVERS

Baseline settings for file and print servers should be based on usage considerations of the files stored and the printers that it controls. One method of ensuring a measure of security is to set the Unsigned Driver Installation Behavior option to Do Not Allow Installation. Print servers should enable the security option Prevent Users from Installing Printer Drivers.

RAS SERVERS

Remote access permissions and settings include:

Access by the user	Determined by remote access permission for each user account.
Access by policy (native-mode domain)	Set to Control Access through Remote Access Policy to explicit allow, explicit deny, and implicit deny.
Access by policy in (mixed-mode domain)	Control Access Through Remote Access Policy option is not available on the user account. Access is based on matching a user account to the conditions of a policy.

As part of the baseline, you should specify the authentication service used (Windows, RADIUS, EAP) and the resolution of other security issues (use of reversible encrypted password, smart card remote access, certificate-based EAP).

DESKTOP COMPUTERS

Desktop computers are used based on the abilities and duties of their users. Appropriate polices, and templates should be designed based on the role the desktops play. You should set a security baseline for all desktop computers, whether they are laptops, Windows NT-compatible laptops, or secure desktops located in confidential or sensitive areas of the company. Use standard templates and adapt them to the appropriate security policy. Use the hisecws.inf template to develop a special template for laptop computers. The compatws.inf template can be used to assure compatibility with applications that do not meet the Windows 2000 standards. This template is consistent with most legacy applications.

KIOSKS

Kiosks are generally located in public areas, and security is a major concern. Kiosks can include any system used in an open area to look up items, give directions, or provide information. Security can be enhanced by removing keyboards and allow only touch screens, mouse devices, or other pointing devices; and removing external access from modems or the networks. In most cases, a logon will not be required, and data is not stored locally.

IDENTIFYING REQUIRED LEVELS OF SECURITY

PRINTER

Printer permissions are set on the Security tab of the Printer property pages. Printer permissions control who can print, manage a printer, or manage documents. You must identify the role each printer takes, and determine whether you want to restrict printing access to certain printers. These printers include printers that print sensitive or confidential material, or printers that are costly to operate. The Users group is given Print Permission by default. This allows users to connect and print to a printer, pause, resume, restart, and cancel their own documents. You should create a group or choose a user to manage the printer. The Manage Documents permission allows Control Job Settings for All Documents and Pause, Restart, and Delete All Documents. Manage Printer allows a user to Share a Printer, Change Printer Properties, Delete Printers, and Change Printer Permissions. Administrators, Server Operators, and Print Operators groups are given this permission by default.

INTERNET ACCESS

Internet access security can be specified by identifying where access occurs and who has what access permissions. You must identify whether computers have dial-up access via modems, if a proxy server, firewall, or routers are utilized on the network. When using a proxy server, you can control access using Windows 2000 users and groups. Firewalls can be used to both block external access to the network, and server to guard access to the Internet. You should identify the specific type of Internet resource (ftp server, telnet), and identify usage intent. Determine if external users access your network from the Internet, and what servers they should have access to.

DIAL-IN ACCESS

To control dial-in access, you need to restrict the right to even connect to the network. For an Windows NT network, after connecting, resource access can be restricted by setting the ability to access resources on just the RAS server, or throughout the network. In a Windows 2000 network where the RAS server is a Windows 2000 Server, you can restrict access through the Routing and Remote Access console. Access is controlled based on dial-in properties of user accounts and policies which are created and maintained through the Remote Access Policies section. Granular access to resources is controlled by native systems, such as by setting NTFS permissions on files and folders, and registry access permissions by using regedt32.exe.

Designing a Windows 2000 Security Solution

DESIGNING AND AUDIT POLICY

In developing an effective audit policy you should determine what can be audited, which objects you need to audit, and on what timed schedule, and what you intend to do with the produced reports. Auditable events include:

- System events
- Account logon events
- Logon events
- Account management
- Privilege use
- Directory service access
- Object access
- Policy change
- Process tracking

DESIGNING A DELEGATION OF AUTHORITY STRATEGY

To limit the scope and power of users in your domain, you can give users administrative rights for a single organizational unit or OU hierarchy within a domain. You can limit rights within the OU, and other OUs nested within the OU hierarchy. To further delegate control, you can adjust the permission to change attributes at the file or folder level.

DESIGNING THE PLACEMENT AND INHERITANCE OF SECURITY POLICIES

Group Policy containers (GPCs) hold collections of computers or users. By creating appropriate Group Policies and linking them to Group Policy containers, you can implement security polices in Windows 2000. Improperly created or applied policy can have serious impact on system operation, performance, and security. You can use Group Policy to set many security settings for implementation across sites, domains, and OUs. Security templates (such as Account Policies, User Rights Assignment, Audit Policy, Public Key Policies, etc.) are available to help develop the appropriate policy. The template is divided into two sections: Computer Configuration and User Configuration.

DESIGNING AN ENCRYPTING FILE SYSTEM STRATEGY

Encrypting File System (EFS) enables users to encrypt files and folders. If folders are encrypted, users need do nothing to encrypt and decrypt any file they place in the folder. You must determine whether you want to disable EFS anywhere, where files should be stored, and who is in charge of recovery keys. You must establish if the EFS should use its own certificates, or should a CA be used. You need to train users to encrypt folders not files, encrypt both the My Documents and Temp folders, and use Active Directory or Certificate services and use Group Policy to implement a central recovery agent.

DESIGNING AND AUTHENTICATION STRATEGY

AUTHENTION METHODS

Certificate-Based Authentication

Accomplished by setting up a public key infrastructure (PKI) via installing Certificate Services, or by using third-party Certificate Authority Services. PKI is used to secure Web communications and Web sites, secure email, digitally sign files, implement smart card authentication and to provide IPSec authentication.

Kerberos

Kerberos defines the rationale behind the framework on which Active Directory lies. It is used by default to authenticate network users using Windows 2000 clients who are logging into a Windows 2000 domain. Kerberos is an IETF standard for authentication. A Kerberos system is made up of several elements:

Component	Description
Authentication Server	Performs authentication of the client against the Kerberos Distribution Center (KDC).
Kerberos Administration Server (KADM)	All modification of the KDC is done from the KADM.
Kerberos Distribution Center (KDC)	The KDC is a service comprised of the Authentication Service and the Ticket-Granting Service.
Kerberos realm	Logical organization of Kerberos servers and clients.,
Key storage	In Kerberos classic, a database called the Kerberos Database (KDB) stores keys. Windows 2000 uses Active Directory for key storage.
Ticket-Granting Server	Grants tickets for resource servers to authenticated clients.

Digest Authentication

Windows NT IIS implementation has been capable of using the Windows NT authentication process to authenticate users without passing passwords in clear text. Windows-integrated authentication is limited in that clients must have a Windows NT account on the IIS Server or in its domain or one it trusts. Digest authentication is not supported by non-Microsoft servers, and cannot pass through a firewall via a proxy unless tunneled. It uses a challenge/response mechanism.

Smart Cards

Smart cards work by having a smart card reader attached to the computer, inserting a valid smart card, and entering a password or PIN. A private key is in a chip on the smart card. Smart cards can be used for SSL authentication and to secure email. Windows 2000 supports smart cards and readers that are compliant with Personal Computer/Smart Card (PC/CS).

NTLM

NTLM is the backward compatible authentication protocol that is used in mixed mode domains. It provides authentication between NT 4.0 BDCs and the Windows 2000 security system. The use of NTLM and NTLMv2 for network authentication is considered much more of a security risk than the use of Kerberos, and its use can be restricted through policy settings in Windows 2000, and registry settings in Windows 9x and Windows NT 4.0. TIP

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is primarily used for two purposes: to authenticate users for access to the Internet, and to authenticate users for remote access to internal networks. It can also be configured to collect information about logon requests, denials, account lockout, and logon and logoff records. Authorization for remote access can be controlled via policy and can include the time (of day or month), the channel used (modem, ISDN, VPN tunnel), the phone number called, the phone number called from, the RADIUS client, and so on.

SSL

SSL provides message integrity, data encryption, server authentication, and optional client authentication. An SSL server and an SSL browser are necessary for operation. SSL is used to encrypt credit card transaction on the Internet. You can set up an SSL-enabled IIS 5.0 server. IIS can also be used to mix basic authentication with SSL.

DESIGNING A SECURITY GROUP STRATEGY

A security group strategy should identify the additional security groups you will create, establish their scope, and identify membership requirements. Not everyone is created equal. No one assignment of rights strategy is possible for the diverse users and information resources in your enterprise. You can match your users to these groups and privileges and, where necessary, extend the model to meet your needs.

If the server is promoted to a domain controller, the Administrator account becomes a member in the following groups:

- Domain Admins
- Domain Users
- Enterprise Admins
- Group Policy Creator Owners
- Schema Admins

The Guest account is also created during installation. It is a member of the Guests group on the local system. Its purpose is to provide an account that can be used by the user who may need occasional access to the computer or to some resource on the computer.

Because this account does not require a password, it can make access convenient and dangerous. The Guest account is dangerous because administrators forget about its existence; they forget that this account can be used by anyone. If the Guest account is enabled, users whose accounts have been disabled can use it.

DESIGNING A PUBLIC KEY INFRASTRUCTURE

A PKI establishes a system of asymmetric key pairs for use in authentication. Users from within and outside of an organization can be vetted and assigned keys. These keys can be linked to access rights, enable closer control over recovery agents in the Encrypting File System (EFS), coupled with smart cards, serve as server authenticators for Web sites, and secure servers of any type. A PKI can go a long way toward implementing tighter security.

A PKI is the technology, hardware, and software that supports the use of public/private key pairs for authentication between servers and clients. In public key technology, a key pair is used. A message, or bit of data, is encrypted with one key and can only be decrypted by using the other key. One key, called the public key, is stored where anyone who knows its location can get it. The other, the private key, is kept secret by its owner. Each participant in the system owns a public and a private key. To join the system, each applicant goes through an enrollment process. This process produces the public/private key pair and returns a certificate and a private key. The certificate contains the public key, identifying information, and is signed by the CA that issued it.

CERTIFICATE AUTHORITY HIERARCHIES

Certificate Authority hierarchies consist of a self-signed root CA and multiple subordinate CAs. The subordinate CAs have a certificate issued by the root, and trust is then inherited from the root. Hierarchies are thought to provide better security and improved scalability.

According to Microsoft, a depth of 3–4 CAs allows the best operations and security compromise. With this level of CAs, you can place the first and second tiers offline for security purposes. A shorter hierarchy decreases security and can provide operational problems because the secured, offline root must frequently be accessed.

CERTIFICATE SERVER ROLES

When you install Certificate Services on a Windows 2000 computer, you create a certificate server. During the installation process, you are asked to choose a role for this CA:

- **Enterprise root CA**—Most trusted CA in enterprise; requires Active Directory.
- **Enterprise subordinate CA—**Issues certificates and obtains certificate from another enterprise CA.
- **Standalone root CA—**Most trusted CA in hierarchy; doesn't require Active Directory.
- **Standalone subordinate CA—**Issues certificates and obtains certificate from another CA.

INTEGRATE WITH THIRD-PARTY CAs

Windows 2000 PKI is based on standards and is interoperable with other PKI products. Interoperability with specific products varies because these products may have chosen to follow proprietary methods or may have implemented the standard in a slightly different way.

Common operations such as CA trust, certificate enrollment, certificate path validation, revocation status checking, and use of public key–enabled applications may be fully supported, supported with workarounds, or not supported in an integrated PKI. You can often anticipate whether Windows 2000 PKI will inter-operate with another PKI by examining the goals of each PKI implementation and the standards that they adhere to.

MAPPING CERTIFICATES

To allow users who are not members of your company access to your resources, you may have decided on a PKI. To allow users who do not have an account in Active Directory to authenticate, the following must be true:

- The user needs a certificate.
- You have created a user account for use by this user or many external users.
- The certificate must be issued by a CA listed in the CTL for the site, domain, or OU in which the user account is created.
- You must map the external user certificate to the Active Directory account (see Step by Step 11.10).

A Certificate Authority Trust can be established by your internal Windows 2000 enterprise root CA. Windows 2000 will then distribute the root certificates. Other root certificates can be distributed using Group Policy. You determine the type of mapping you want based on your desired use of the certificate.

You should choose Use Subject of Alternate Security Identity if multiple types of certificate exist and you want to be specific about which ones are mapped to the user account you have selected.

DESIGN WINDOWS 2000 NETWORK SERVICES SECURITY

DNS SECURITY

DNS in Windows 2000 supports dynamic DNS updates. DNS resource records can be automatically updated by computers and by the Windows 2000 DHCP server. Also new to Microsoft DNS in Windows 2000 is the capability to secure DNS using Active Directory-integrated zone files and the capability to register and use service (SRV) records. SRV records are registered by services with DNS so that clients can locate services by using DNS. When this record is placed in DNS, clients can use it to locate domain controllers nearby. Every domain controller registers services by creating SRV records in DNS. The records are created automatically and are added to DNS database using the
dynamic update protocol. All DNS records are kept in zone files or, if the zone is an Active Directory-integrated zone, in Active Directory. Each zone file represents computers in a contiguous address space.

DNS Server Zone Types and Zone Replication in Windows 2000

Zone files represent contiguous address spaces or DNS domains. Traditional DNS consists of two zone types: primary and secondary. These are called *standard primary* and *standard secondary* in Windows 2000. New in Windows 2000 is the Active Directory-integrated
zone. Windows 2000 zone files are defined as follows:

- **Standard primary—**This is a read/write zone file. Changes to records are recorded in this standard text file.
- **Standard secondary—**This is a read-only zone file. Changes recorded to the primary file are replicated to a secondary file. Secondary zone files are used to distribute the workload across computers and to provide backup.
- **Active Directory-integrated—**This zone file exists only in Active Directory, not in a text file. Updates occur during Active Directory replication, which can simplify planning and configuration of the DNS namespaces because you don’t need to tell DNS servers to specify how and when updates occur. Instead, Active Directory maintains the zone information. No primary and secondary zones exist in an Active Directory-integrated DNS zone. (However, you can create a standard secondary zone and point it to an Active Directory-integrated zone.) If your Active Directory consists of a single domain, there is no need for a secondary or backup file to spread the workload or to be available in case of disaster if you have configured DNS on multiple domain controllers. The workload is spread over multiple computers by virtue of AD replication, and multiple copies of the zone file are always available.

In a multiple-domain Active Directory, you may need to create standard secondary zones that replicate data held in Active Directory-integrated zones. This is because the replication of Active Directory-integrated zone information is limited to the domain in which the zone is created. The standard secondary zone can assure the availability of another domain's zone information. This is especially useful in providing backup and availability of reverse lookup zones and in providing local zone information in remote sites where you do not want to have a domain controller. In traditional DNS and in standard and primary zone files, data is replicated from the primary to the secondary zone. In Windows 2000, it is updated by incremental zone transfer (IXFR), which replicates changes only to the zone file, not the whole file.

Secondary zones are created to provide additional copies of zone file information. When the secondary zone file is created, it receives a copy of the current primary zone file. When new hosts and other records are added to the primary zone file, they are not automatically added to every secondary zone file. Replication must be configured between the primary and secondary zone files.

Active Directory-integrated zone files automatically replicate zone information as part of Active Directory replication. Every domain controller for the domain that is configured to be a DNS server will receive all changes to zone information. There is no need to set up zone replication separately. Each of these domain controllers can be used to make changes to the zone information.

Because replication is managed by the Active Directory replication process, it is multimaster. A second possibility is to use Active Directory-integrated zones instead of the more traditional zones, and configure the zones to accept only secure updates. When Active Directory-integrated zones are used, you can protect the DNS server from unauthorized updating by configuring secure dynamic updates. There are other advantages as well:

- No single point of failure.
- Fault tolerance. All zones are primary zones. Each server that hosts a zone maintains it, but all records are replicated in Active Directory.
- Single replication topology is used. No separate zone transfer takes place. Replication is done in Active Directory replication; you don't configure replication for DNS separately.
- Secure dynamic updates are possible. You can set permissions on zones and records within those zones. Updates that use dynamic update protocol can be updated only by the computer that owns the record.

RIS SECURITY

Remote Operating System Installation is a feature of Windows 2000 that is designed to automate installation of Windows 2000 Professional. Remote Installation Services (RIS) is a service that allows installation of Windows 2000 Professional from a RIS server.

The RIS server can deliver unattended system setup, fast recovery, and a network client computer configuration enabled for the remote-boot Preboot Execution Environment (PXE). RIS can support Windows 2000 clients whose operating system needs to be restored, or new clients that have never had an operating system installed. It cannot be used to upgrade existing operating systems to Windows 2000 from downlevel Windows clients. RIS allows the creation of a computer account in Active Directory, if configured to respond to any request for service from an authenticated user. In addition, you can define computer naming policy and the container within which the computer account is created.

Designing Security for RIS

Securing RIS requires knowledge of its operation and the requirements of your organization. Several features of RIS can be configured to make it more secure.

To restrict which computers can update or install the OS, you con-figure the RIS administrative option Do Not Respond to Unknown Client Computers. When this option is checked, only computers that exist in or that have been prestaged (that is, those that have a computer account created in Active Directory) can access the RIS server.

Requirements for RIS

To utilize RIS, you must have the following:

- RIS installed on a Windows 2000 Server.
- A DNS server must be present on the network (any DNS server that supports service records [SRV RR] [RFC 2782] and the dynamic update protocol [RFC 2136]).
- A DHCP server must be present on the network. Remote boot clients will obtain an IP address from the DHCP server.
- Access to Active Directory (membership in an Active Directory domain). RIS uses Active Directory to locate clients and other RIS servers.
- Client machines that meet certain hardware requirements.

SNMP

SNMP is a network management protocol used with TCP/IP networks.

SNMP Security Settings

SNMP agents respond to requests for information, so this information should be restricted. Only rudimentary security configuration is available. Configuring security for SNMP may include any of the following:

- Configure traps to do security checking.
- Join hosts and agents to SNMP communities, and use these to authenticate SNMP messages.
- Secure SNMP messages with IP security.

Traps are configured to generate a message when an event occurs. Such events might be requests for information from an unknown management system or for password violation.

TERMINAL SERVICES

Terminal Services provides access via a Terminal Services client to a Windows 2000 Server. Clients send only keystrokes and mouse clicks. All processing occurs on the server. Terminal Services is available over any TCP/IP connection, including the following:

- Remote access
- Ethernet
- Internet
- Wireless
- WAN
- VPN

Terminal Services clients are available for Windows clients and for other clients via third-party products.

Terminal Services provides Windows 32-bit application emulation. Because only keystrokes and mouse-clicks cross the network from the client and displays from the server, network bandwidth usage is minimized. Centralized security is provided by the data center deployment.

Terminal Server Modes

Windows 2000 Terminal Services runs on standalone member servers or domain controllers. Do *not* install Terminals Services in application sharing mode on a domain controller. If you do you, will give the Domain Users group logon local permission on the domain controller. This, of course, is not a good thing. User profiles can be established for Terminal Services users. If users already have a Windows 2000 profile, the Terminal Services profile can be set up separately. Administrators control access to applications by using mandatory profiles.

Providing Secure Access Between Networks

The following services and processes contribute to secure network communications:

- NAT and Internet Connection Sharing
- Proxy server
- Routing and Remote Access Services
- Internet Authentication Services
- Virtual private networking
- Terminal Services

NAT AND INTERNET CONNECTION SHARING

Network Address Translation (NAT) is an IP router defined in RFC 1631. NAT is used to hide internal IP addresses by inserting new IP addresses and possibly new TCP/UDP port numbers of packets from one network before they are forwarded to another. NAT is also used to connect many computers to the Internet without having a corresponding number of valid Internet addresses. Private network addresses can be mapped to one or to multiple Internet addresses.

Mapping can be dynamic or static. Private IP addressing can be used for the internal, private network. The private IP addressing scheme includes several ranges of IP addresses that are not usable on the Internet. Companies can use these for computers that do not directly connect to the Internet. When these computers need Internet access, they must use a proxy or other address translation scheme. NAT can do this. The computer address (and maybe the port of the source computer) is replaced by the NAT server with a legal Internet address. When the response is returned to the NAT server, NAT replaces the translated address with the private address. NAT is part of the Windows 2000 Routing and Remote Access Protocol. It is also available as part of the Internet Connection Sharing feature of the Dial-up connections folder. Internet Connection Sharing uses a scaled-down version of NAT. Its version of NAT is less configurable than that in the Routing and Remote Access Protocol.
NAT adds no additional authentication or other security configuration or processes.

ROUTING AND REMOTE ACCESS SERVICES

Windows 2000 Routing and Remote Access Services is composed of the following:

- Routing Information Protocol (RIP) version 2, the routing protocol for IP and IPX
- Open Shortest Path First (OSPF) routing protocol for IP
- Demand-dial routing
- ICMP router discovery
- Internet Group Management Protocol (IGMP) and multicast boundary support
- Remote Authentication Dial-In Service (RADIUS) client

- IP and IPX packet filtering
- Point-to-Point Tunneling Protocol (PPTP) support for router-to-router VPN connections
- Routing and Remote Access Console and Netsh (command line) for administration
- Network Address Translation (NAT)
- Integrated AppleTalk routing
- Layer 2 Tunneling Protocol (L2TP) over IP Security (IPSec) support for router-to-router VPN connections
- Support for client-to-router VPN connections Remote Access Server

The remote access server accepts Point-to-Point Protocol (PPP) connections. PPP can be configured to require authentication. The Windows 2000 PPP infrastructure provides support for the following:

- Dial-up remote access
- VPN remote access using either PPTP or L2TP over IPSec
- On-demand or persistent dial-up demand routing
- On-demand or persistent VPN demand-dial routing

INTERNET AUTHENTICATION SERVICES

Internet Authentication Services (IAS) is a Microsoft Windows 2000 implementation of Remote Authentication Dial-In User Service (RADIUS). IAS can be used to perform centralized authentication, authorization, and accounting of dial-up and virtual private network remote access and demand-dial connections. It should be used in connection with Windows 2000 Routing and Remote Access Services.

RADIUS Protocol

RADIUS is an industry standard that provides authorization, authentication, identification, and accounting services. User information is sent to a RADIUS server from a dial-up server. RADIUS servers have been typically located at Internet service providers. The ISPs then established dial-up servers and leased accounts on these servers to the public. The dial-up server is known as the RADIUS client.

VIRTUAL PRIVATE NETWORKING

Virtual private networking is the act of setting up a connection between two parts of a private network across a shared network such as the Internet so that it emulates a private link. Data is encapsulated or given a header that includes routing information. Data may be encrypted for confidentiality. The link is set up between two end-points, either a client and a router, or two routers. This connection is called a virtual private network (VPN). The logical path from endpoint to endpoint is often called a tunnel.

VPN Connections

Two types of connections are possible: the remote access connection and the router-to-router connection. The remote access connection is made between a Windows client and the Routing and Remote Access Server. The router-to-router connection is established between two Routing and Remote Access Servers. In the router-to-router VPN connection, the calling router becomes the VPN client. VPN connections can be established across any IP network. Many VPN connections are designed to be established across the Internet, but there is no reason that a VPN tunnel cannot be created across a private network to establish secure communications. Connections include the following properties:

- Encapsulation
- Data encryption from one tunnel endpoint to the other. The process used depends on the tunneling protocol used and how it is configured.
- Authentication. Both user information and data can be authenticated. Authentication can be configured to authenticate the client only, or both the server and the client. Data can contain a cryptographic checksum based on a shared secret key. This allows either endpoint to ensure that data received originated from the other end.
- Address and name server assignment. The VPN server establishes a virtual interface that consists of an IP address for the client and for itself, and the IP address of the DNS and/or WINS servers in the server environment. This information is delivered to the VPN client if the connection is approved.

Tunneling Protocols

Two options exist for tunneling protocols for Windows 2000 VPN connections:

- PPTP
- L2TP over IPSec

PPTP requires an IP connection between the client and the server. The connection can be made via dial-up. Authentication is via the same mechanisms as PPP. Encryption can be accomplished with Microsoft Point-to-Point Encryption (MPPE) if EAP-TLS or MS-CHAP is used. Encryption is link to link—that is, from the client to the server. Data that travels from the server endpoint across its network to other computers is not encrypted. End-to-end encryption can be accomplished if IPSec is used after the tunnel is established.

SECURE ACCESS TO PUBLIC NETWORKS

Irrespective of company property use, legal issues, and work-avoidance issues, public network access raises many security issues that should be addressed. Although it is impossible to eliminate every risk entirely, you can reduce their probability. To do so, you must focus on the following six areas:

- Protect internal networking address schemes from exposure on the public network.
- Set up server-side configuration to control content access (and level of such access) in the event of a security breach.
- Set up client-side configuration to mitigate the risk.
- Allow only specific protocols to exit and return the organization's boundaries.
- Limit exit and entry points to the network.
- Consider policy, procedure, and politics.

SECURE ACCESS TO PRIVATE NETWORK RESOURCES

To provide secure access from public networks to your private resources, you may want to determine the purpose of the access.

To secure resources, use DACLs and auditing. Reduce user accounts on the exposed machines to the defaults. Protect these accounts with complex passwords. Use the "no access/no time/no where" practice on the Guest account. This practice makes sure that the Guest account is disabled but doesn't rely on it. It does not let one little option stand between a secure network and one that can easily be penetrated.

SECURE ACCESS BETWEEN PRIVATE NETWORKS

Any company that has multiple locations has faced the task of providing connectivity between those locations. This has taken many forms, from private leased lines, to shared Frame Relay, to VPNs constructed across the Internet. Today's enterprise organizations also demand connectivity with their business partners. Suppliers, business customers, and trusted partners in joint projects all want to be able to communicate instantly to trade goods and ideas. Security has never been more paramount.

The security of their connections needs to be designed into the connectivity type chosen. Part of ensuring secure access is to begin with security right within the smallest component of the network, the LAN. Your design should begin there and then expand to cover the following:

- Secure access within a WAN
- Secure access across a public network

Security and the LAN

Secure access within a LAN requires the following:

- Securing administrative access and assigning administrative roles
- Understanding and dealing with IP risks and using IPSec for data encryption and/or signing
- Controlling access to shared resources

- Securing non-Microsoft client access to shared resources

Securing WAN Access

Secure access across a WAN includes access across dedicated links, Frame Relay, and ATM. Although dedicated connections would seem to provide the ultimate in security, you should still maintain your server, file system and user policies. You might consider smart card or certificate deployment to aid in security efforts.

Tunneling across WAN links can also be a good policy. By providing a VPN connection, you are layering security. You can use Internet Authentication Server to authenticate access from branch offices via WAN links as well as dial-up lines. Nothing precludes establishing a firewall or limiting protocol access. Finally, you can use IPSec to secure data transfer as necessary.

DESIGN WINDOWS 2000 SECURITY FOR REMOTE ACCESS USERS

You and your ISP may want to consider placing an IAS server at their location to authenticate access to the tunnel. This is also a good solution when you need to provide remote access for users in other locations. By selecting an ISP with locations that match your needs, you can provide secure remote access. If you have traveling users, choose an ISP with nationwide (or if necessary, worldwide) access points. Some ISPs may also be able to provide you with better quality of service, and possibly more secure arrangements, because they can route your communications across their backbone network instead of relying strictly on links shared with other ISPs.

You may also choose to locate all hardware and software on your network. In either case, be sure to provide adequate backup for the IAS server.

Designing Security for Communication Channels

When dealing with LANs, WANs, and communications that take you to and across public networks, two methods can help you: SMB signing and IPSec. SMB signing refers to the digital signing of each packet in a Server Message Block (SMB) communication between two computers. IPSec, or IP Security, is a protocol that you can use to provide integrity, confidentiality, and authentication of network communications. You can use IPSec to protect communications between Windows 2000 computers. You can use Group Policy to enable and enforce both of these methods.

SMB SIGNING

SMB is the file-sharing protocol used by Windows computers. It is also known as the Common Internet File System (CIFS). A newer version of this protocol has been available for

Windows NT 4.0 since Service Pack 3. This version added two features: the support for mutual authentication and the support for message authentication.

Mutual authentication requires both the client and the server to identify themselves. When authentication is required, the attacker may be able to pretend to be either the client or the server, but he has a hard time proving it.

SMB signing prevents the data in packets from being changed during transit. On Windows NT 4.0 and Windows 98 clients, two registry key entries must be made to implement SMB signing. One key is used to “enable” signing, the other to “require” signing. Both keys must be configured. If servers are configured to enable signing and not configured to require it, unconfigured clients may still communicate in the normal manner. Clients configured to enable SMB signing will communicate in the secure manner. If servers are configured to require signing, communication with nonenabled clients cannot take place.

By default, installing the service pack does not enable or require SMB signing when installed on a server. It is enabled by default when you install it on a Windows NT 4.0 Workstation.

SMB signing does not work with direct host IPX protocol because the direct host IPX protocol modifies SMBs and makes them incompatible with SMB signing. CPU performance is reduced when SMB signing is enabled and required.

IPSEC

The IPSec protocol is used in two ways in Windows 2000: transport mode (used to secure communications between computers within your internal network) and with an L2TP tunnel (to secure, via a VPN and the use of L2TP, communications between net-works).

IPSec also has a tunnel mode, but the current recommendation is to use the tunnel mode of L2TP and use IPSec for encryption. In the first case, the computers involved are each configured to use IPSec when communicating between themselves; in the latter, Routing and Remote Access Service is configured to provide a tunnel endpoint for router-to-router or client-to-router communications.

Both communications are controlled through Group Policy. You can use IPSec to provide the following:

- **Access control—**Connection negotiation and filtering of inbound communications.
- **Integrity—**Checksums and message digest algorithms are used to allow detection of tampered packets.
- **Data origin authentication**—Ensuring source.
- **Outbound protocol filtering—**Management of data before it leaves the system.

The IPSec architecture consists of the following:

- Key management via Internet Key Exchange (IKE) formerly referred to as ISAKMP/Oakley
- A Security Policy database that defines the rules for the disposition of all traffic (inbound or outbound)
- The Authentication Header (AH) protocol, which provides integrity and data origin authentication
- The Encapsulating Security Payload (ESP), which provides packet encryption, integrity, and data origin authentication
- Native IP stack implementation

IPSec Encryption Scheme Design

Design an IPSec encryption scheme. Determining the IPSec encryption scheme to be used depends on an evaluation of the available protocols for both negotiation phases against the issues of performance and cost. It also requires a decision about the reuse of keying material.

Designing IPSec Management

IPSec management is accomplished by specifying IPSec policies. Because IPSec policies affect communications between systems, IPSec policies are generally implemented at the site, domain, or OU level, not at the local computer policy level. Computers that store or manage extremely sensitive information can be grouped in an OU. Client systems allowed to communicate with them can also be placed in an OU.

Systems that, although they are joined in a domain, are temporarily out of communication with a domain controller have their policy information cached in their registry. Systems not joined in a domain can have local policies defined.

Management may be delegated to OUs if the OUs represent groups of computers that need to communicate with each other. Domain-level polices can be implemented to cover broad applications such as a requirement to use 3DES as the encryption protocol for all IPSec communications.

IPSec management should be considered when designing OUs and the delegation of administrative responsibilities for those OUs. Three possible OUs might be for computers holding classified, sensitive, or normal information, If computers have been administratively grouped to provide it, policies for these systems can be developed and applied with Group Policy to ensure its usage.

Designing Negotiation Policies and Encryption Schemes

Negotiation of connections is managed by IKE. Two phases are used: one for ensuring a secure communications channel, and the other to negotiate the use of SAs. To design policies that stipulate these negotiations, you must understand their process. Design, then, consists of making the choices in each area negotiated, which will best fulfill the desired level of security for each IPSec connection.

Design security policies.

IPSec policies are composed of rules that determine how and when the policies are used. Rules are triggered by source, destination, and type of IP traffic. The rules consist of a list of filters and filter actions. A match between a filter and packet header information triggers the rule. What happens when the rule is triggered is determined by the filter actions. Each policy can have multiple rules, and the rules can all be active simultaneously or singly.

Designing IPSec policies, then, consists of the following:

- Designing filters
- Designing rules by determining which filters belong in which rule
- Designing policies by determining which rules should be part of the policy

Design IP filters

Filters determine whether a rule is triggered. They determine this by specifying information that can be matched with complementary information in the packets being inspected. IP packet headers contain information on its source and destination address, and the type of traffic. Filters then are designed to indicate acceptance or rejection of each packet based on this information. The process by which they do so is called packet filtering.

Each filter contains the following:

Source and destination address—Can be specific IP addresses, subnets, or networks.
Protocol—The default covers all protocols in the TCP/IP suite. Individual protocols can be specified.
Source and destination ports (TCP and UDP)—The default covers all ports, but can be configured to apply only to packets on a particular port. Both inbound and outbound filters must exist. In both inbound and outbound communications, packets are matched with filters.

Outbound filters trigger a security negotiation

The most common filter to implement is to identify the IP address or range of addresses with which a computer or a group of computers would be allowed to communicate. This is how communications could be secured within a group of computers that consist of sensitive servers of a particular type and the clients that were allowed to communicate with them.

Filters could also be included for specific protocols. If these are implemented, however, care must be taken to include a filter for every protocol that might be used for the allowed communications between the systems.

Filter Lists

Filter lists can include more than one filter. If you are using a filter to cover all computers, use the generic Any IP Address instead of trying to specify all the computers. Filter list order does not matter. All filters are simultaneously retrieved by the IPSec Policy Agent and are processed from most to least specific.

Filter Actions

Filter actions, or what happens if a match is found, is the other part of policy design. Each rule needs to specify what will happen. Filter actions often define the type of policy. They also indicate the connection type and authentication method. The type of policy can be as follows:

- **Passthrough policy**—IPSec ignores the traffic.
- **Blocking policy—**This traffic will not be accepted or allowed to pass. This will help stop communication from a rogue computer; it can also prevent traffic from leaving a system.
- **Permit policy**—No traffic is allowed unless a filter for it is defined.
- **Negotiated policy**—The policy is negotiated with other IPSec-enabled computers, but allows communication with non-IPSec–enabled computers.

Passthrough policy is a good idea when communication is necessary with a computer that cannot be secured, the traffic is not considered sensitive enough, or the traffic provides it own protection (Kerberos, SSL, PPTP). Blocking policy is used to prevent communications with rogue computers. You can also use it to prevent such traffic from leaving a computer.

A permit policy only "permits" traffic to pass that has been specifically identified. Policy negotiations are necessary sometimes—this is a good idea in situations in which you need to control communications from sensitive computers, but allow it from nonsensitive computers. You must control communications with the nonsensitive computer in other ways. This policy is also put into place to ensure some communications if other policies are preventing it incorrectly, or as a default for all communication not specified in the policy.

This type of fallback policy is useful during testing, but can allow unprotected communication if policy negotiations for the more secure policies fail. The connection type defines whether the rule applies to a particular interface such as dial-up adapter or network card. A use of connection type specificity enables you to relegate the use of policy (but only when you are on the road, not when connected to the local LAN).

Authentication methods identify which method can be used for the connection. Because a match must be made with the other side of the connection, some policies specify multiple methods to ensure one can be agreed upon. Greater security can be ensured if smaller ranges are identified. Authentication methods include the following:

- **Kerberos v5—**This is the default authentication protocol in Windows 2000. It can be used for any clients using Kerberos v5 that are members of a trusted domain. (Non-Windows 2000 systems that implement Kerberos v5 and members of a trusted domain can use this method.)
- **Public key certificates—**These are necessary for Internet communications, remote access, external partner access, L2TP communications, and computers that do not use Kerberos v5. To use certificates, at least one trusted Certificate Authority (CA) must be configured.
- **Preshared keys—**These are agreed upon by two users. Both must manually configure IPSec policies. The key is used for authentication, not encryption. The key is stored, unprotected in IPSec policy.

Predefined Policies

Before you develop IPSec policies, you should examine the default policies to see whether they meet some or all of your needs. They are also a good source to examine to understand how GUI interfaces represent rules and filters and their corresponding actions. You can use them as templates in designing your own rules. Predefined default policies, rules, and filter actions are as follows:

- **Client (Respond Only)—**Does not secure communications most of the time. Can respond to requests for secure communications by using default response rule. Only requested port and protocol traffic is secured. This is a good policy to set on clients. When the client needs to access a secured server, it will respond; but otherwise, use normal communications.
- **Server (Request Security)—**Secures communication most of the time. Allows unsecured communication from non-IPSec–enabled computers.
- **Server (Require Security)—**Always requires secured communications. Unsecured communications from any source are rejected.

Levels of computer security identified by Microsoft include the following:

- **Minimal—**No sensitive data, no IPSec.
- **Standard—**Balanced security using a range of policies including minimal policies (including polices such as enabled, but not required).
- **High security—**Highly sensitive data at risk of theft or disruption (that is, remote dial-up, public network communications).

Fashion First Case Study

Background
Fashion First is a clothing retailer that has been in business for eight years. Last year's total sales for all retail stores were $240 million. After tremendous growth during the past eight years the clothing business has slowed in its existing retail stores.

Organization
Headquarters
Our corporate headquarters is located in Tampa, Florida, which employs approximately 80 people. There are twelve employees in the IT department.

Retail Stores
There are approximately 50 employees at each of the retail stores which are located in five major cities in Florida.

Problem Statement
President
Our old business model relied on expansion by building new retail stores. However, expansion takes time, and the area served by a single retail store is limited. The only way to rapidly increase sales is to build a Web site. This site would allow customers from across the United States to buy our clothing.

IT Director
We have three major areas of concern. First, we must ensure that the information on our Web server can be modified only with proper authorization and that the information is distributed only to those authorized. We also want to be informed when someone accesses data on the Web server. Second, information must be secure as it travels from the customer's computer to our server. We must prevent user IDs, passwords, and financial information from being intercepted as this information travels to our server. And lastly, information that customers download must not damage their software or violate licensing agreements.

Our IT department will be expanded to include a Webmaster who will administer the Web site, Web developers who will write code for the Web pages, and Web authors who will create the Web content.

Marketing Director
We have developed an ActiveX control that customers will be able to download from the Web site. Customers can use this control to display different sizes of clothing on a 3-0 model. They can customize the model with their measurements. They can then dress the model with our clothes to show how the clothes will fit and select the correct size.

When people first view our Web site, they will be considered visitors. After visitors enter their name and address and receive an ID we will consider them customers.

For our Web site, we must include a method for the customer to view our clothes and place selected items in a shopping basket. We will need a checkout function that allows the customer to enter shipping and billing information. This should include me customer's name, address, phone number, and credit card number. This information, including the customer's ID and password, will be stored in a database.

When customers revisit our site, we will be able to identify them automatically by their ID and password. They can then view the status of their orders or place additional orders. We should also let customers know that they are connected to Fashion First's Web site.

The entire transaction should be logged. The information will be stored in a transaction-tracking file. This file will contain credit card numbers and other confidential customer information. The transaction-tracking file will allow us to bill the customer and to provide information for our customer service employees if problems arise.

Customer Service Director
All customer service employees must have access to customer information. This includes customers' personal information, such as name, address, phone number, and account number.

Existing IT Environment
Headquarters
Headquarters has four Windows NT Server 4 0 computers. The remote access server is named JTRAS. The primary domain controller is named J1DC1. The other two servers are used to run applications.

Retail Stores
Each retail store has two Windows NT Server 4 0 computers. One server controls all cash register functions. The second server handles inventory and word processing functions and has a dial-up connection to headquarters. All retail stores use TCP/IP. Each office has its own user account for dial-up access. This connection is used to transmit daily sales and merchandise orders to headquarters.

Connectivity
All computers in the headquarters LAN are connected through a 100-Mbps connection. Each retail store is connected to headquarters through a WAN with a 56-Kbps dial-up connection.

Envisioned IT Environment
Headquarters
The existing Windows NT Server domain controller will be upgraded to Windows 2000 native mode, and a single forest will be created.

A DMZ will be set up between the public and private network. In addition, Fashion First plans to add six new Windows 2000 Server computers. A Web server named JTWEB will be multi-homed. A server named JTDEV will be used by programmers to develop the Web content. A server named JTDATA will contain all customer, inventory, and order information. This information will be stored in Microsoft SQL Server databases. A server named JTVPN will be used as the VPN server JTDC2 will be a new domain controller.

The company wants to eliminate its remote access server and allow the retail stores to submit their data over the Internet through a VPN.

Retail Stores
The hardware and software at the retail stores will remain the same.

Connectivity
The Wan and LAN bandwidth will remain the same.

Fashion First Practice Questions

1. **Which type of CA should you use to digitally sign the ActiveX control?**

   A: third-party CA.

2. **Which audit policy should you use on JTWEB?**

   A: success and failure audit for object access.

3. **Which methods should you use to identify and authenticate existing customers on the Web site?**

   A: SSL, anonymous logon and database validation.

4. **Which audit policy should you use to detect possible intrusions into the Fashion First network?**

   A: Success and failure audit for logon events.

5. **Design a solution that allows the retail stores to connect security to headquarters over a VPN and customers to connect securely to headquarters by using SSL (Use all objects and connections.)-**

Resource	
A	Customer
B	Retail Store
C	JTVPN
D	Headquarters
E	JTWEB

	Connection
1	SSL
2	TCP/IP
3	VPN Tunnel

A: B – 3 – C, A – 1 – E, C – 2 – D

6. **Design a network that allows customers to order clothing items on the web site. (Use all computers and connections.)**

Resource	
A	Customer
B	External Firewall
C	JTWEB
D	JTDATA
E	Internal Firewall

	Connection
1	Secure Internet Connection
2	TCP/IP Connection

A: A – 1 – B, B – 2 – C, C - 2 – E, E – 2 – D

7. **How should you authenticate visitors to the Web site?**

A: Authenticate visitors to an anonymous account.

8. **Which technology should you use to securely connect the retail stores to headquarters?-**

A: PPTP

9. **Which authentication protocol should you use to secure the VPN connection from the retail stores to headquarters?**

A: MS-CHAP

10. **Which changes should the retail stores make to support the VPN connection?-**

A: Configure the connection type to dial in to the ISP.
Use PPTP to communicate with the VPN server.

Med Supply Case Study

Background

Med Supply is a medical supply company. The headquarters is located in Jacksonville, Florida. There are more than 1,000 employees at headquarters. Med Supply sells and distributes medical supplies to large hospitals in 23 states. The company has distribution centers in Boston, Massachusetts; Dallas, Texas; Miami, Florida; Minneapolis, Minnesota; New Orleans, Louisiana; Tampa, Florida; Seattle, Washington; and St Louis, Missouri.

Business Process

Sales Representatives

More than 200 of the company's employees are sales representatives. Sales representatives visit their existing customers at least once per week. During the visit, the sales representative receives a weekly supply order from the purchasing manager at the hospital. The sales representative then the hospital warehouse, where the supplies are located. The sales representative checks each supply at the warehouse and fills out a paper order form for the supplies that need to be replenished. The sales representative then faxes the order form to the nearest distribution center.

Distribution Centers

After receiving a faxed order from the sales representative, a clerk at the distribution center enters the order into a mainframe computer. The order is then filled and delivered to the hospital. The entire process from the time the sales representative visits the hospital until the supplies are delivered takes approximately three days.

Employees from each distribution center deliver supplies only within their region. Each distribution center has sales representatives who also check and order supplies within the same region. Sales representatives do not work for multiple distribution centers.

Customer Service

Sales representatives must call the customer service department at the distribution center to request the status of an order. Sales representatives also call to request the availability of an item. Sales representatives use toll-free numbers to place phone calls and send faxes to Med Supply. Eight customer service employees answer order status and availability questions.

Existing IT Environment

Computers

Med Supply has one mainframe computer, which is located at headquarters. There are 250 computer terminals at headquarters connected to the mainframe computer. There are 10 computer terminals at each distribution center.

WAN Connectivity

A T1 line connects the computer terminals at the distribution centers to the mainframe computer.

Envisioned IT Environment

Computers

The mainframe computer at headquarters will be replaced with Windows 2000 Server computers, which will function as domain controllers Headquarters will also set up a VPN server.

All sales representatives will use their own portable computers, and they will be able to load personal programs onto their computers. The portable computers will run Windows 2000 Professional. The portable computers will contain a program named Salesforce, which will be used to order supplies. The portable computers will also contain customer information. This information must be encrypted and recoverable. A Sales Representative group will be created for resource access.

The IT manager must be aware of attempted unauthorized access to the new network.

Distribution Centers

All computer terminals at the distribution centers will be replaced with desktop computers running Windows 2000 Professional. Each distribution center will have a domain controller that runs Routing and Remote Access. Each distribution center will be its own organizational unit (OU). Each distribution center will have an IT administrator. This administrator will be able to add new users, add users to existing groups, modify existing group membership, and create computer accounts.

Each distribution center will have a folder for each hospital. Each hospital's folder will have two subfolders. One subfolder will contain the order status for the hospital, and the other subfolder will contain sales information. The sales information is confidential and will be used only by that hospital's sales representative. The sales representatives can add, delete, and change their hospital folders.

Customer Service

Customer service should have the ability to read and modify orders for all hospitals.

Hospitals

Hospitals should be able to view only their own order status. They will be connected to headquarters by using Routing and Remote Access. Med Supply will supply each hospital with a computer. The hospital will supply the phone line. Each hospital will have a user account.

Problem Statement

Marketing Manager

Sales representatives are spending too much time servicing existing accounts. The sales representatives need a way to place orders quickly, which allow them to increase their number of accounts. The portable computers will allow sales representatives to visit each stockroom in the hospital instead of visiting a warehouse. The sales representatives will use Salesforce to enter the quantities of supplies in each location, and the program will report whether the supply should be ordered. If a supply is needed, an order will be created automatically. After all stockrooms have been checked, the sales representative will connect his or her computer to a phone line in the hospital, connect to the distribution center, and upload the batch of orders. The fulfillment process will not change.

When hospitals call their sales representative to request an order status, it can take up to one day for the sales representative to return the call. The sales representatives should be able to connect to the distribution center at any time to view the status of an order.

Sales representatives should also be able to connect to headquarters either by dialing directly to the remote access server or by dialing a local ISP and connecting through a VPN. Only sales representatives should be able to place an order. A verification process must be in place. Sales representatives should not be able to view other sales representatives' information.

IT Manager
Phone costs are increasing dramatically. An average of 200 faxes are received per day. Fax transmissions can last up to five minutes each. Med Supply receives an average of 300 phone calls per day requesting order status and item availability.

We will add a new distribution center in Pittsburgh, Pennsylvania. The new distribution center will have good Internet connectivity. Because of the high cost of a T1 line, this distribution center will be connected to headquarters through a VPN.

Salesforce program is updated regularly with a disk containing software patches. A copy of the patch is sent on a floppy disk to each center. One person at each distribution center makes a copy of the disk for each sales representative at that distribution center. The copy is distributed to the sales representatives at a monthly sales meeting. We have to make sure that the sales representative receives an unaltered copy of the patch. We have had some problems in the past with employees displaying inappropriate wallpaper on their computers. We need to restrict employees from changing the wallpaper on their computers.

Med Supply Practice Questions

1. **What are the IT administrative models for Med Supply?**

   A: Existing: centralized
   Envisioned: decentralized

2. **To view the status of their orders, how should hospitals connect to headquarters?**

   A: Use Routing and Remote Access with Windows 2000 logon authentication.

3. **Which type of group should you assign sales representatives to?**

A: global

4. **Specify the required level of security for the resources at the Dallas distribution center.**

	Resources
A	Hospital1 folder
B	Hospital1 Orders subfolders
C	Hospital1 Sales Folders

	Permissions
1	All hospitals (read)
2	All hospitals (Modify)
3	All hospitals (Full Control)
4	Dallas Hospital1 hospital (Read)
5	Dallas Hospital1 hospital (Modify)
6	Dallas Hospital1 hospital (Full Control)
7	Dallas Hospital1 sales Rep (Read)
8	Dallas Hospital1 sales Rep (Modify)
9	Dallas Hospital sales Rep (Full Control)

A: A =7, B = 4, C = 8

5. **At each distribution center, how should you grant the necessary permissions to the IT administrator?**

A: Create an administrator group for each distribution center's organizational unit (OU).
Add an existing user designated as an administrator to this account.
Grant the necessary permissions to this group.

6. **To encrypt orders from the sales representatives to the distribution centers, you should do what?**

A: Use 128-bit encryption for Routing and Remote Access
Use PPTP with packet filtering for VPN

7. **What actions should you take to meet the security requirements for the Windows 2000 upgrade? (Choose four)-**

A: Encrypt data transmitted to the distribution centers.
Verify that only unaltered versions of the Salesforce program are loaded onto the portable computers.
Ensure that only the sales representatives can create orders.
Secure data on the portable computers.

8. **Design a RADIUS solution that will allow sales representatives to securely tunnel to HQ. (Use all resources and connections)**

	Resources
A	Portable Computer
B	Radius Server
C	RADIUS Proxy Server
D	RADIUS Client Computer
E	PPTP Server

	Connections
1	PPP
2	RADIUS Access Request
3	Proxied Access Request
4	RADIUS Access Reply
5	Proxied Access Reply

A: A - 1 - D -2 - C - 3 - B - 4 - C - 5 - D - 1 - A - 1 – E

9. What should you do to implement auditing on the Windows 2000 Server computers?

A: Enable failure audit for logon events on the domain controllers.

10. To prevent changes to the wallpaper on all computers, which Group Policy strategy should you use?

A: Create one Group Policy for all distribution centers, and apply the Group Policy at the headquarters domain

11. How should you restrict hospital dial-up connections to only authorized hospitals?

A: Configure Routing and Remote Access on the remote access server to use callback Configure callback to dial a predefined phone number at the hospital.

12. Design a secure connection between headquarters and the Dallas Distribution Center. (Use all resources and connections)

	Resources
A	Headquarters
B	Headquarters Intranet Adapter
C	Headquarters Internet Adapter
D	Headquarters Win2000 Router
E	Dallas Distribution Center
F	Dallas Intranet Adapter
G	Dallas Internet Adapter
H	Dallas Win2000 Router

	Connections
1	Hardware Connection
2	Intranet Connection
3	L2TP Internet Tunnel

A: E – 2 – F, F – 1- H, H – 1 – G, G – 3 – C, C – 1 - D, D – 1 - B, B - 2- A

13. Using all resources and connections, design a secure access solution to allow sales representatives access to the network resources at HQ.

Resources
ISP
Portable Computer
HQ VPN Server
HQ RAS
Med Supply Internal Resources

Connections
ISP Connection
VPN Connection
PPP Connection
HQ Internal Network

A: *Portable Computer – PPP Connection – ISP*
ISP – ISP Connection – HQ VPN Server
Portable Computer – VPN Connection – HQ VPN
Portable Computer – PPP – HQ RAS
HQ VPN Server – HQ Internal Network – Med Supply Internal Resources
HQ RAS – HQ Internal Network – Med Supply Internal Resources

14. What should you do to restrict hospitals' access to the order status information?

A: Set permissions on each hospital's order file to grant that hospital Read permission to its own order file.

15. How should you configure secure communications between the Pittsburgh distribution center and headquarters?

A: Enable L2TP and configure an enterprise subordinate CA on the private Med Supply network.

16. To secure the connection to the Pittsburgh distribution center, how should you implement IP filters at headquarters?

A: Add source filters for the Pittsburgh distribution center for UDP port 1701 and IP protocol 50. Add destination filters for headquarters for UDP port 1701 and IP protocol 50.

Fabricware Case Study

Background

Fabricware

Fabricware is a manufacturer of industrial fabrics. Fabricware has more than 12,000 employees. The headquarters are located in Boston, Massachusetts, and there are manufacturing facilities in Atlanta, Georgia, Baja, Mexico, and Dublin, Ireland. The Chief Information Officer (ClO) has requested a security design proposal for Fabricware.

Facade, Inc.

Facade, Inc. is a manufacturer of specialty blankets. The company has more than 300 employees. Facade, Inc. has only one manufacturing facility in Miami, Florida.

Joint Venture

Fabricware has just completed an agreement with Facade, Inc. to begin a joint venture. Both companies want to expand their product lines to include space blankets. These blankets will protect satellites from collisions with meteorites and other space debris. Engineers from Fabricware and Facade, Inc. will work together to produce the fabric that will be used in the blankets. This joint venture will require the two companies to communicate with each other frequently.

Organization

Fabricware and Facade Inc. both have a similar organizational structure. Each company has an engineering department, a manufacturing department, and a sales department. The engineering department includes engineers who will create the designs for the space blankets. The manufacturing department includes employees who will manufacture the blankets. The sales department includes sales representatives who will sell the blankets.

Existing IT Environment (Fabricware)

Computers

All servers, desktop computers, and portable computers run Windows 2000. Each manufacturing facility and headquarters has a server named MANUFACTURING and a server named ENGINEERING. The MANUFACTURING server contains a schedule that shows the availability of every type of fabric produced by that facility. The ENGINEERING server contains all information needed to produce a new item or improve an existing item.

LAN and WAN Connectivity

The manufacturing facilities are connected to headquarters with T1 lines. The maximum usage for the T1 connection is 40 percent. There is one remote access server at headquarters and one remote access server at each manufacturing facility. The LAN at each manufacturing facility and headquarters runs at 100 Mbps. Fabricware has a single domain named FABWARE. Each manufacturing facility has its own organizational unit (OU). The OUs are named ATLANTA, BAJA, BOSTON, and DUBLIN.

Domain Model
We are committing major resources to the space blanket project. The data related to the project must remain secure. Each manufacturing facility has its own IT employees who administer its OU. This distributed administration will be retained in the new security plan.

Existing IT Environment (Facade, Inc.)
Facade, Inc. has just completed a full upgrade to Windows 2000 on all servers and desktop computers. There is a single domain named FACADE and a domain namespace named facade.com. The company has its own unique Active Directory schema. In addition, Facade, Inc has a VPN server named FABHQVPN and an e-mail server.

All files for the joint venture are stored in a shared folder named FABSPACE. This folder is shared by engineers from Facade, Inc, and Fabricware Facade, Inc. It allows engineers from Fabricware to view and modify all files in the FABSPACE folder.

Envisioned IT Environment (Fabricware)
Computers
All sales representatives will have a folder named Customer on their portable computers. Because this folder will be used to store confidential customer information, the folder must be secure and encrypted. The folder will be updated when the sales representatives dial in to headquarters. The connection must be secure.

Fabricware will have shared folders that will contain information about the joint venture. This folder will be named FACADESPACE. One folder will exist on the ENGINEERING server at each location. The ENGINEERING and MANUFACTURING servers at each location will contain engineering and manufacturing data for that location only.

LAN and WAN Connectivity
The T1 line between headquarters and all manufacturing facilities will remain the same. All remote access servers at the manufacturing facilities will be eliminated. Sales representatives will connect to the network by using a dial-up connection located at headquarters. The remote access server at headquarters will be used as a backup to the VPN. Communication across the VPN connection should be encrypted. Fabricware has a frame relay connection to the Internet through a VPN server.

Domain Model
There will be one DNS namespace named Fabricware.com. The existing domain will be in one forest. The engineering department and the manufacturing department will have their own organizational unit (OU) at each manufacturing facility and headquarters IT employees located at each manufacturing facility will administer the OU for that manufacturing facility. The OU administrators will have full control of all folders on all servers within their OUs.

A trust relationship will be established between BOSTON and FACADE that will allow engineers access to each other’s domains.

Problem Statement (Fabricware)
Chief Executive Officer (CEO)
Engineers from all of our branch offices and engineers from Facade Inc. will be working together. All engineering data that is related to the joint venture must be available to all engineers.

We are committing major resources to the space blanket project. The data related to the project must remain secure.

IT Director
Our employees are encouraged to transfer between branch offices to enhance their job skills. During transfers, it has been difficult to move employees' accounts from one OU to another.

During the joint venture, resources from both companies will be shared. For example, an employee from Fabricware should be able to print to a Facade, Inc, printer and a Facade, Inc employee should be able to print to a Fabricware printer.

Customer information on the sales representatives' portable computers must be secure. I want to know who is modifying or viewing the information in the FACADESPACE folder in any of our branch offices.

Sales Director
The sales representatives are very excited about our new joint venture. The profit on these blankets will be very high, but the number of buyers is limited. We must not let our traditional business suffer. The sales representatives will continue to visit our existing customers and search for new customers within their assigned territory. While visiting our customers, our sales representatives must have access to all manufacturing schedules. Many potential customers want to know about the availability of the product.

Envisioned IT Environment (Facade, Inc.)
The security design for Facade, Inc. will not change.

Fabricware Practice Questions

1. **What are the two primary security risks for Fabricware? (Choose two)**

   A: Facade, Inc, employees viewing confidential information from Fabricware.
   Unauthorized users gaining access to customer information on the portable computers.

2. **Which security group strategy should you use for the Fabricware sales representatives?**

   A: Assign all sales representatives to global groups.
   Put the global groups into domain local groups.

3. **How should you encrypt information over the VPN between the BOSTON organizational unit (OU) and the FACADE domain?-**

   A: Implement L2TP over IPSec at both the Boston OU and the Façade domain.

4. **How should you protect the Internet interface on the Fabricware VPN server from unauthorized users?-**

   A: Use Routing and Remote Access filters on the Internet Interface of the VPN server.

5. **How should you authenticate users from Facade, Inc. who access Fabricware's network over the VPN?**

   A: Use the fully qualified domain name and password.

6. **How should you assign the authority for adding new user accounts at Fabricware after the upgrade?**

   A: Create a new administrative group at each organizational unit (OU) with the authority to create new users at that OU

7. **Which two security components should you use on the portable computers? (Choose two)**

   A: L2TP
   Encrypting File System (EFS)

8. **For the Fabricware sales representatives how should you implement Encrypting File System (EFS) on the portable computers to allow central recovery?**

   A: Create an enterprise root CA at the Boston organizational unit (OU), and create enterprise subordinate CAs at the Atlanta, Baja, and Dublin OUs. Define the recovery agent at the domain level.

9. **Specify the required level of security for each resource. Move the appropriate permissions to the appropriate resource(s). Use only permissions that apply and you might need to reuse permissions.**

	Resources
	Boston Engineering data
	Boston Manufacturing data
	Atlanta Engineering data
	Atlanta Manufacturing data
	Baja Engineering data
	Baja Manufacturing data
	Dublin Engineering data
	Dublin Manufacturing data

	Permissions
1	Baja engineer (Modify)
2	Boston engineer (Modify)
3	Boston Sale Representative (Read)
4	Facade, Inc. engineer (Modify)
5	Facade, Inc. engineer (Read)

A: Boston Engineering Data (4,2)
Boston Manufacturing Data (5,3)
Atlanta Engineering Data (4,2)
Atlanta Manufacturing Data (5,3)
Baja Engineering Data (4,2)
Baja Manufacturing Data (5,3)
Dublin Engineering Data (4,2)
Dublin Manufacturing Data (5,3)

10. Design a secure communication strategy. (use only the locations and connections that apply.)

	Locations
A	Boston
B	Miami
C	Baja
D	Portable Computers
E	Dublin
F	Atlanta

	Connections
1	T1 Line
2	L2TP VPN
3	Routing and remote Access
4	PPTP VPN

A: A – 1 – E, A – 1 – C, A – 1 – F, A – 3 – D, B – 2 – A

Proposal Case Study

Proposal Corp is a temporary staffing agency that provides companies with temp employees. Proposal employs 2,500 people nationwide.

Organization
Headquarters
Headquarters is located in Jacksonville; Florida Headquarters includes the accounting, payroll, human resources, and IT departments. Headquarters employs 150 people.

Branch Offices
Proposal Corporation has branch offices in 200 locations nationwide. Each branch office employs from five to 20 people. Each branch office has a branch manager. One person in each branch office is a representative for the IT department. This person resets routers and helps the IT department troubleshoot technical problems that occur at the branch office.

Regions
Several branch offices that are in the same geographic area make up a region. There are eight regions. One regional manager is assigned to each region. The regional managers submit information about branch offices, regions, and markets for posting on the Web page. Branch managers must approve the content before it is published on the company's Internet Web page.

On-Site Offices
For Proposal Corp largest customers, the company provides one to five employees from the sales department to work full time at the Customer offices. This helps Proposal identify customer needs more efficiently.

Payroll Centers
There are payroll centers in Dallas, Texas, and San Francisco. Florida Payroll centers process paychecks for all employees within their region.

Existing IT Environment
Computers
All headquarters employees, except employees within the IT department, use Windows 98 desktop computers. The IT department uses Windows NT Workstation 4.0 desktop computers.

Proposal Corporation has 28 Windows NT Server 4.0 computers at headquarters. One of these computers is a certificate server that is not being used, two are file servers that store company data, and 25 run Windows NT Server 4.0, Terminal Server Edition.

In addition, Proposal Corporation has one Outlook Web Access (OWA) server named OWA1, two domain controllers named DC1 and DC2, three Microsoft Exchange Server 5.5 computers, four UNIX servers that contain Oracle databases, and one remote access server named RAS1.

On-site employees use OWA1 to connect to headquarters. Anonymous users can connect to OWA1 to post resumes to an Exchange public folder named Recruiting and to fill out online applications. Each branch office has access to this public folder. The IT representative maintains control of this folder.

The company also maintains an Intranet, which includes Web pages for technical support, human resources information, and other company information. Branch offices all have desktop terminals and one computer with a modem. The branch offices connect to a Terminal server at headquarters. There are no servers in the branch offices.

All headquarters employees are granted access to e-mail and the Internet. Users in branch offices and on-site offices are granted access to e-mail and the Internet from the computers. Users of desktop terminals are not granted access to the Internet.

WAN Connectivity
Branch offices are connected to headquarters by fractional T1 lines the committed information rate is 128 Kbps.

Proposal Corporation has a T1 line to the Internet. The company's domain name is proposal.com. Proposal Corporation maintains a web page under this domain.

On-site offices are not connected to the WAN.

Network
All servers have static IP addresses. All client computers use DHCP. Each branch office has its own subnet and a router.

Envisioned IT Environment
Computers
Proposal Corporation wants to upgrade its network to Windows 2000 and use one Active Directory tree. All servers will be upgraded to Windows 2000 Server. All Terminal servers will use the Terminal Services feature. All desktop computers will be upgraded to Windows 2000 Professional.

Proposal Corporation plans to add an additional remote access server, which will be named RAS2. Both remote access servers will run 2000 with Routing and Remote Access. In addition, the company will add an Internet Information Services (IIS) server. OWA1 will not be upgraded to windows 2000.

WAN Connectivity
The WAN bandwidth will remain the same.

Network
Proposal Corporation wants to build a network that can easily accommodate future growth.

Security

Proposal Corporation has implemented digital certificates to communicate securely with customers. The company has implemented one enterprise root CA. Proposal Corporation wants to set up a certificate server for internal use only. The company also wants to implement secure communications to the Human Resources shared folder to prevent theft of confidential data during transmission. The company might consider two-factor authentication methods for portable computers.

Network Roles and Usage

Human Resources

The human resources department maintains a folder that contains confidential employee data. This folder is located on one of the Windows NT 40 file servers.

IT

IT department maintains the network. The Terminal servers provide complete centralized administration for Proposal Corporation. This allows all IT employees to be located at headquarters. The IT department is composed of network administrators and help desk personnel.

Sales

The sales department uses the network to send and receive information from potential temporary employees and to communicate with customers. Sales employees often send confidential information, such as personnel schedules, through e-mail.

Branch Offices

Branch offices store confidential employee data, such as benefits information, in the Human Resources shared folder. The branch manager copies this information to the folder. Only the branch manager has access to this information. The IT representatives in the branch offices report network downtime and are allowed to create global groups on the network for their offices.

Payroll Centers

Payroll centers connect to the Oracle databases at headquarters to obtain payroll data. This data is used to create paychecks.

Proposal Practice Questions

1. **Which business requirement will have the most impact on the Windows 2000 security design?**

   A: Continued use of the OWA1 server in the Windows 2000 environment.

2. **Which two security solutions should you implement for headquarters? (Choose two)**

   A: Digital Certificates

Encrypted Data Transmissions

3. **Design a Windows 2000 authentication strategy for Proposal Corporation.**

	Resources
A	DC1
B	OWA1
C	On-Site Offices
D	Local client computers
E	Anonymous Web Client

	Authentication Methods
1	Basic Auth with SSL
2	NTLM
3	Kerberos

A: E – 1 – B, B – 3 – A, C – 1 – B, D – 2 – A

4. **Which authentication method should Proposal Corporation's employees at on-site offices use after the computers are upgraded to Windows 2000?**

A: basic authentication with SSL.

5. **How can you allow Proposal Corporation's employees at on-site offices to communicate securely with headquarters?**

A: Use basic authentication with SSL.

6. **After all computers are upgraded to Windows 2000, which security component should you reconfigure?**

A: Network access permissions.

7. **What is the primary security risk for Proposal Corp.?**

A: Theft of HR data

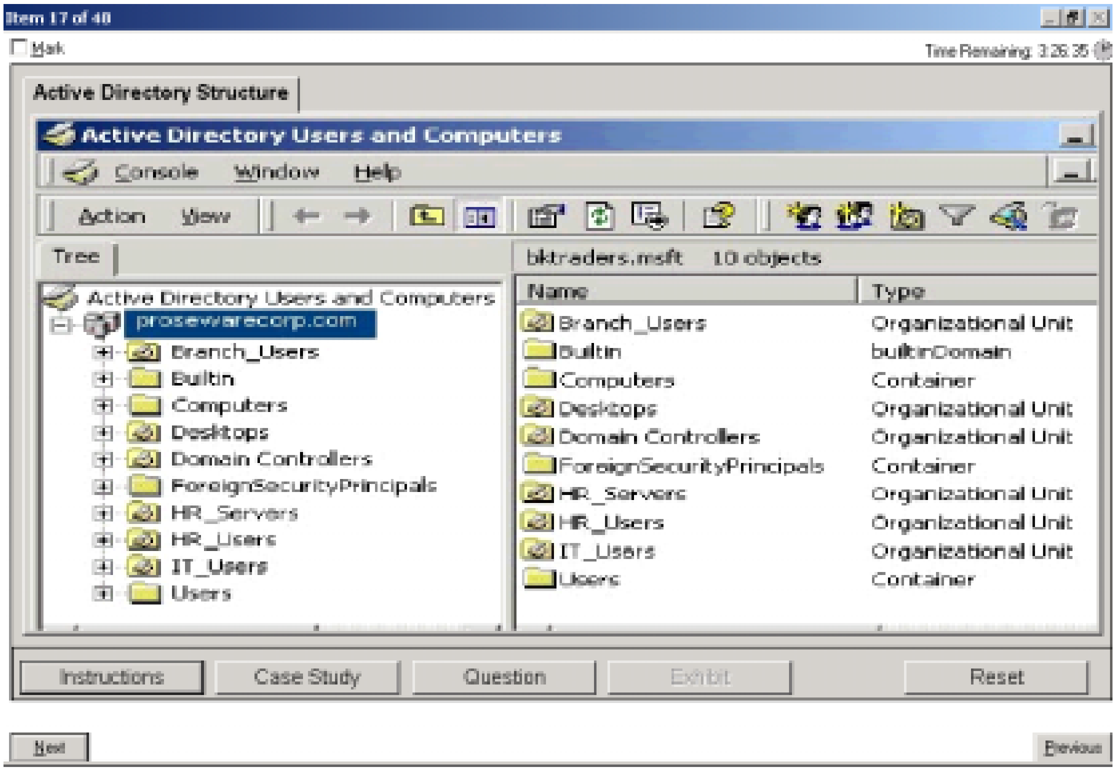
8. **How can you implement secure communications between the IT department and the HR Department? (Choose two)**

A: Use certificate based authentication, 3DES encryption, and ESP
Use pre-shared key authentication, 3DES encryption, and ESP

9. **Which type or types of CA should you implement for internal use? (Choose all that apply)-**

A: Stand Alone root CA
Enterprise root CA

10. How should you implement security for the HR department?



Active Directory Users and Computers
- prosewarecorp.com
  - Branch_Users
  - Builtin
  - Computers
  - Desktops
  - Domain Controllers
  - ForeignSecurityPrincipals
  - HR_Servers
  - HR_Users
  - IT_Users
  - Users

bktraders.msft 10 objects

Name	Type
Branch_Users	Organizational Unit
Builtin	builtinDomain
Computers	Container
Desktops	Organizational Unit
Domain Controllers	Organizational Unit
ForeignSecurityPrincipals	Container
HR_Servers	Organizational Unit
HR_Users	Organizational Unit
IT_Users	Organizational Unit
Users	Container

A: Assign the Secure Server (Require Security) IPSec policy at the HR_Servers OU, and assign the Client (Respond Only) IPSec policy at the Domain level.

11. Design a secure access solution for Proposal Corp. (Use all resources and connections)

	Resources
A	DC1
B	OWA1
C	On-site Offices
D	Terminal Servers
E	Branch Offices

	Connections
1	SSL
2	TCP/IP
3	Remote Desktop Protocol

A: C – 1 – B, E – 3 – D, D – 2 – A

Highabove Toys Case Study

Organization
Headquarters
Headquarters includes the sales and marketing, IT, legal, accounting, HR, and executive departments. It employs 4,500 people, with a growth rate of 20 percent.

Retail Stores
There are 350 retail stores located nationwide. Each store employs 50 – 100 people. Over 50 new stores will be opened each year.

Service Centers
There are 15 service centers nationwide, which employ 100 technicians and five managers.

Existing IT Environment
WAN Connectivity
All stores and service centers are connected to headquarters by 128-Kbps lines. This connection is backed by a 56-Kbps dial-up connection.

LAN Connectivity
All headquarters buildings are connected by T1 lines.

Computers
There are 4,5000 Windows NT Workstation computers, and 150 Windows NT Server computers at headquarters. The Servers are used as application servers and file servers. One server named SALES1 is used as a backup domain controller. It runs Internet Information Services (IIS), and is in the SALES domain. Only domain controllers and applications have shared resources. HR has a server named HR1. All connections to this server must be encrypted.

Each store has 30 Windows 2000 Professional computers and two Windows NT Server computers – one for a primary domain controller for the local domain, and the other is a backup domain controller.

Each service center has 30 Windows 2000 Professional computers and one Windows NT Server which is a backup domain controller.

Network
The company's Internet domain is named highabovetoys.com. On the internal network, the private IP address is 172.16.0.0. All computers use TCP/IP. At headquarters, the Windows NT Servers use static addresses and the Windows NT Workstations use DHCP. Static addresses are used for all retail stores, and service center computers.

Envisioned IT Environment
WAN Connectivity

The WAN bandwidth will remain the same. The proposed overseas retail store will have a LAN with a 64-Kbps connection to headquarters.

LAN Connectivity
The LAN bandwidth will remain the same.

Computers
The company will upgrade to a Windows 2000 network with one Active Directory tree and two domains sharing the same namespace. Highabove Toys wants to design a directory service that allows for some autonomy, and wants to ensure that business units can be added, removed, or changed without undue overhead. The SALES1 server will not be upgraded. It will be replaced with a Windows 2000 Server after all other computers are upgraded to Windows 2000. After this server is replaced, the network will run in native mode. The legal department will have its own Windows 2000 Server named LEGAL1. The department will implement a secure private network between LEGAL1 and HR1.

Network
The envisioned physical network will not change. The company wants to create one account domain for headquarters, and one account domain for retail stores. The overseas retail store will have a help desk employee located on-site to perform end-user application support and to resolve hardware issues.

Security
Authorized remote users should be able to access shared resources at headquarters through secure tunneling. Confidential documents should be sent internally in a secure manner. Highabove needs to accept transmission of confidential information form manufacturers in a fast, easy, and reliable manner. No training should be required. The company wants to implement a Public Key Infrastructure (PKI).

Network Roles and Usage
IT
The IT department administers user and computer accounts for the company. Strong passwords are not implemented. Users at headquarters have access to e-mail and the Internet. The IT department is divided into three groups: the WAN group, the LAN group, and the Internet group. The LAN group manages user accounts, oversees the LAN, the Windows 2000 Servers and domains, and the retail store servers. The WAN group oversees the WAN. The Internet group oversees Internet security and connectivity. Each group has a different manager. Communication and agreement among the groups is poor. The Internet group wants autonomy within the Active Directory.

Sales and Marketing
The sales and marketing department uses the network to exchange e-mail and download information from manufacturer and competitor Web sites. It works with more than 1,000 manufacturers. The department needs to receive information from new manufacturers and to verify their

authenticity securely. The sales and marketing department needs to access the retail stores for sales history information. They require color printing, and depend on portable computers to access information regardless of their location.

Legal
The legal department needs to copy confidential documents to shard folders for the HR department, the executive department, and the company's law firm.

Retail Stores
The cash registers run Windows NT Workstation. Cash registers boot with a generic logon for cashier access. The cash registers do not contain any data. Store managers have Windows 2000 Professional desktop computers, with e-mail and unlimited Internet access. Each store also has five secured Windows NT Workstation computers for employees to browse pre-approved Internet Web sites. Each store has three public kiosks. Customers can use kiosks to register for gifts or place orders. The kiosks automatically boot with and authenticate to a secured generic account.

Service Centers
Each center uses unique logon names for access to the network. Each center technician has access to e-mail and the Internet.

Highabove Practice Questions

1. **Which security requirement will affect design of windows 2000 forest?**

   A: Organization of user accounts

2. **Which server or servers provide the least security for user access?-**

   A: SALES1

3. **How should you secure the new servers at the overseas store?**

   A: Install the servers into a new OU and implement Group Policies at the OU Level.

.

4. **Which strategy should you use to accommodate the new overseas store?**

   A: Delegate authority to the Help Desk employee to modify accounts and groups

5. **Which security method should you implement to provide data security between LEGAL1 and HR1?**

   A: IPSec with ESP (encrypts data)

6. **Which security solution should you implement to allow the service centers to communicate with manufactures?**

   A: Secure Email

7. **How should you design windows 2000 domain and OU structure for Highabove?**

   A: Two accounts domains, and migrate existing retail stores resource domains into OUs under the retail stores domain.

8. **Specify the required level of security for each resource.**

Resources
Domain Controller
Application Server
Cash register
Public Kiosk

	Security Options
1	Additional restrictions for anonymous connections
2	Disable CTRL+ALT+DEL requirements for logon
3	Do not display last user name in logon screen
4	Message text for user attempting to log on
5	Rename administrator account

   A: Domain controllers: 1, 4, 5. Application servers: 1, 4, 5. Cash registers: 2, 3, 4, 5. Public kiosks: 2, 3, 4, 5.

Facade Case Study

Background

Facade, Inc. is a manufacturer of beverage and food products. The company employs more than 20,000 people worldwide, with more than 10,000 employees located outside the United States. The headquarters is located in Santa Fe, New Mexico. The company is divided into three groups Corporate, Engineering, and Operations.

Organization

Corporate

Most of the Corporate group is located at headquarters. The Corporate group includes the human resources, legal, executive, accounting, and sales and marketing departments. The Corporate group has its own IT employees.

Engineering

Engineering group is responsible for designing and building the operations facilities for Facade, Inc. The Engineering group also designs and installs the network in new facilities. After the facilities are constructed and tested, they are turned over to the Operations group for ongoing management. The Engineering group is located in Santa Fe in a building on the headquarters campus, but it is run in a highly autonomous manner. In particular, this group has its own IT employees who manage its network. The Engineering group does not want IT employees from the Corporate group to manage its computer resources or accounts.

Operations

Operations group is responsible for maintaining the operations facilities. Although the executives in the Operations group are located at headquarters, most of the employees in this group work at the operations facilities. The Operations group has its own IT employees who manage the network for the operations facilities headquarters; most of the employees in this group work at the operations facilities. The Operations group has its own IT employees who manage the network for the operations facilities.

Problem Statement

Chief Technology Officer (CTO)

Having done a good job providing the basic tools people need to communicate with one another and to manage their own work, however, we have not been as vigilant as we should have been about securing confidential information. The recipes for some of our products are trade secrets with a … that is impossible to measure. In addition, our competitors eagerly seek our plans for creating new products and opening new markets. We need to improve our overall data security and enhance the privacy of our corporate communications. I have been pushing for tighter security for about a year, ever since what we refer to as the incident. One of our competitors somehow accessed our network and viewed our plans for launching a new product. We didn't learn about this until months later. We thought it was a coincidence when they launched a similar product just before we did, but our worst fears were later confirmed when we received reliable information that they had accessed our plans.

Chief Information Officer (CIO)
Although I agree with our CIO's position on enhancing security, the situation is not that simple with thousands of people worldwide and dozens of operational IT systems in place, it will be a challenge to evolve our existing IT infrastructure. We have run most of our networks on Windows NT for many years. We now run Windows NT 4.0, and we are vigilant about applying service packs and keeping systems up-to-date. After a joint evaluation involving employees from the Corporate group, the Engineering group, and the Operations group, we have decided to deploy 2000 over the next one and a half years. We have already begun aggressively upgrading the network at headquarters, and we are nearly complete with that work. Primary goal of our migration to Windows 2000 is to replace our multi-master domain model with a new model based on Active Directory. We want to be able to delegate authority at the organizational unit (OU) level Members from each group have formed an enterprise architecture committee to resolve issues that affect all groups. Members from this committee will be assigned to the Enterprise Admins group.

Vice President of Operations
Security initiative is somewhat overblown. A sales employee leaves some plans in a bar on a napkin, and now all my employees have to learn new procedures. We'll go along with corporate directives, but we haven't seen a need for dramatically new approaches. I think this whole thing is politically motivated. I don't intend to fight it directly, but I don't want to add any unnecessary workload for my employees. We have enough work to do already.

Vice President of Engineering
Engineers, we have always taken network security seriously. We have been telling employees at headquarters that too much information has been vulnerable. Finally, someone is listening.

IT Security Director
Some of the newer security technologies in Windows 2000 seem like a natural fit, while others might cause problems of a political nature. The Engineering group is interested in using everything from smart cards to data encryption on their portable computers. Because they have already upgraded to Windows 2000 Professional, this will help them incorporate new technologies. The operations group thinks that everything is fine the way it is today. Ironically, the facilities that are run by the Operations group might be the most susceptible. The information on their file servers is as confidential as the information at headquarters, but the Operations group does not effectively limit physical access to their facilities and network. It is too easy for someone to walk into one of the facilities with a portable computer and log on to network. I intend to ensure that the Operations group complies with this security initiative.

Existing IT Environment
Domain Structure
Facade, Inc, uses a Windows NT 4.0 multi-master domain model. Each of the three primary groups has its own master domain that contains the user accounts for its employees. The domains are CORP, ENGR, and OPER. Resource domains are added as needed for each major

geographic location. These domains establish a one-way trust to master domains only when necessary.

A resource domain named ENGRFLD includes all temporary resources located at construction sites worldwide, typically connected over demand-dial lines. ENGRFLD also includes numerous centrally managed remote access servers. These servers support individual engineers who travel to existing sites for repairs, improvements, and other modifications. Routing and Remote Access is used for dial-up access only.

Resource domains for the Operations group have one-way trust relationships with all three master domains to enable visiting employees to access local resources with their single user accounts.

WAN
All computers use TCP/IP exclusively. Remote locations are connected to headquarters in a variety of ways, depending on size and bandwidth requirements. Large sites have private, high-speed leased-line connections, smaller sites have slower connections.

Facade Practice Questions

1. What is Facade, Inc.'s business model?

A: decentralized management and centralized operations.

2. What is the Engineering group's tolerance for risk?

A: The Engineering group is willing to try some new approaches.

3. What is Facade, Inc.'s IT model for management and operations?

A: decentralized management and decentralized operations.

4. Which two security risks facing the Operations group can you reduce or eliminate by using smart cards? (Choose two)

A: Remote hackers connected via modem.
Unauthorized visitors physically entering a facility and connecting via the LAN.

5. Which Windows 2000 domain structure should you use for Facade, Inc.?

A: Create three domains trees one domain tree for Corporate, one domain tree for Engineering, and one domain tree for Operations. Create the trees in the same forest. Replace existing resource domains with organizational units (OUs).

6. **Which four technologies should you include in the security strategy for the Engineering group? (Choose four)**

   A: Kerberos authentication
   EAP
   L2TP over IPSec
   Certificate Services

7. **Which technology or technologies should you include in your security strategy for the Operations group? (Choose all that apply)**

   A: Encrypting File System (EFS)
   L2TP over IPSec
   Kerberos authentication

8. **What should you include in an audit policy for the CORP domain?**

   A: success and failure audit for object access
   success and failure audit for policy change
   success and failure audit for account logon events
   success and failure audit for directory service access

9. **Which administrative task or tasks should you complete to maintain the network at the operations facilities? (Choose all that apply)**

   A: Group Policy administration
   Digital certificate administration
   Remote access administration

10. **Which two technologies should engineers use for secure dial-up access when traveling? (Choose two)**

    A: Smart cards
    PPTP

11. **Which technology should you use for engineers working at existing operations' facilities?**

    A: basic authentication with SSL

12. **Which three policies should you include in a security strategy for the CORP domain? (Choose three)**

    A: Enable account lockout

Prevent the installation of unsigned drivers
Enforce strong passwords and password aging

13. **How should you prevent unauthorized users from accessing the Engineering group's file servers?**

    A: Block access to TCP and UDP ports 135-139 at the server, enforce strong passwords, implement password aging, and use Encrypting File System (EFS) to control access to folders containing confidential files.

Photosup Case Study

Background

Photosup sells digital cameras, printers and supplies to photography studios throughout NA. The Company's Headquarters is located in Cleveland Ohio.

Photography studios use digital cameras to take pictures of their customers and then allow customers to immediately view the proofs at the studio. When customers decide which pictures they want to purchase, the pictures are either printed at the studio, if the studio has a digital printer, or sent to a film-processing laboratory on a Zip disk or CD. Customers can choose to pick up the pictures at the studio or have the pictures mailed directly to them.

Existing Environment

President

We have supplied photography studios with camera equipment and supplies for the past 20 years. For the past year, we have sold digital cameras. Even though we sell the latest digital equipment, many studios still view us as a traditional photographic supplier. Nearly 2, 000 studios buy our products. The number of studios is increasing.

We recently merged with a French photographic supply company that has three offices in France. We now have eight offices and employ 1, 200 people.

IT Director

All of our company's offices are connected through a WAN. I have a staff of five IT employees to maintain the computers in each regional office. Headquarters has four network engineers, one Webmaster, three Web developers for the intranet, and 10 programmer/analysts. The programmer/analysts maintain the inventory, purchasing, billing, and payroll applications.

Customer Service Representative

Each office has its own customer service employees. Studios call us when they are having problems with their equipment. Studios also call us to order supplies. We keep records of each call. If a studio or customer calls to report a problem with our Web site, we will either try to make changes the photo folders to resolve it or notify the Webmaster.

Envisioned Environment

President

We want to offer more services to the studios. I would like to develop a Web site that studios can use to post proofs of their customers' photos. The 11 studios would give IDs and passwords to customers so that they can access their photos over the Internet. Customers could then view their proofs on our company's Web site and place orders for photos. Customers could share their IDs and passwords with relatives or friends, who could also view proofs and order photos from the Web site.

IT Director

The Web site will be hosted at headquarters. We will use Windows 2000 and Internet Information Services (IIS) on the servers. When a customer, visits the Web site to view photos, programs developed in Microsoft Visual Basic will be loaded on their computers. These programs will format the pictures for viewing on the customer's computer. The programs will be stored in a folder named Program on the Web server.

I will hire five Web developers to develop the Web site and a Webmaster to administer the Web site. The Webmaster will have total control of the Web servers. Each studio will have its own folder on the Web server. Each studio's folder will contain a folder for the studio's purchase history and a customer folder for each of the studio's customers. The customer folder will contain confidential information that should not be available to the customer. The photos will be placed in a separate photo folder inside the customer folder. Each customer will have only one folder for photos. An office manager at each studio will be responsible for creating customer folders and placing photos in the folders. We will also train office managers to add customers to the Active Directory tree for their studio.

Problem Statement

IT Director

I'm not sure how to secure files from customers that don't have IDs and passwords. To take it easier for customers to order from the Web site, we should allow studios to give each customer a plastic card with the customer's ID and password printed on it.

Customer Service Representative

When a studio calls with a problem, we have to look through paper files to find out if the studio is under warranty or uses a maintenance contract. If the studio calls to order supplies, we have to look through paper files to find the studio's credit terms.

Sales Representative

Currently, customer information is stored in several places. Customer service representatives sometimes take an order when the studio is on the phone and then do not inform the sales representatives about the order. We have to look through the paper files to find any history of problems or purchases.

Photography Studio

I want to ensure that no one can change the photos on the Web site. When customers place an order, I want to ensure that their credit cards will be secure and that their information will not be accessed by one of my competitors.

Requirements

President

We need a Web site that will allow our studios to display their customers' photos. The customers should be able to securely access their photos, and order prints. The customers should also be able to specify whether they want to pick up their pictures at the studio or have the pictures mailed to them. The Web site should be able to handle 5,000 active customer accounts I also need to see how many orders are placed on our Web site.

IT Director

The new Web site will have two servers. The first server, named PHOWEB, will be the Web server that will display all of the photos. All hard disks on the Web server will be formatted with NTFS. All offices will use the same Web server. The second server, named PHODATA, will contain customer information, such as name, address, and order history. In addition, we will have a proxy server named PHOPROX and a domain controller named PHODC. Web developers should be limited to a development environment; they should not have any access to the Web server. Only the Webmaster should be able to move new programs to PHOWEB. Studios should be able to post pictures to the Web site over the Internet. Studios should also be able to maintain their own customer accounts. The company will have a single domain named PHOSUP. Each studio and customer will have a user account in this domain. Each studio will be an organizational unit (OU).

Photography Studio

We need an easy way to load our photos onto the Web site and set up the customer data, including IDs and passwords. We want the customer photos to be displayed on the Web for only 30 days. We will disable the customer account and remove the photos after 30 days.

Customer

I want to be sure that my credit card information is not made available to anyone other than the studio and the film-processing laboratory.

Web Developer

Changes to the Web software are requested, we need to be able to upgrade the Web server.

Customer Service Representative

We need access to customer information to resolve questions.

Sales Representative

Need access to the customer order history so that we can see what customers have bought and whether they have had any problems with our equipment and service.

Webmaster

My main goal is a secure and stable Web site. I need to move programs from a test computer to the Web server and to upgrade the Web software as needed. I will also be responsible for identifying and fixing problems in each studio's folder on the Web site.

Conclusion

The new Web site should enable customers to securely view and order photos. It should allow photography studios to load photos only to their folders. Customer information should be available for reports, support, and marketing. The Web site should be stable.

Photosup Practice Questions

1. **What is the primary security requirement for the studios?**

   A: *Ensure that photos on the Web site cannot be altered.*
   Ensure that customers' credit card numbers are secure.

2. **To which type of group should you assign all Web developers?**

   A: *global*

3. **How should you ensure that each customer's account is disabled after 30 days?**

   A: *Set an expiration date on each customer's user account.*

4. **Which task should you delegate to the office managers?**

   A: *Create, delete, and manage customer accounts.*

5. **Which type of CA should you use to digitally sign the Microsoft Visual Basic programs?**

   A: *third-party CA.*

6. **Which two authentication methods should you use to allow customers access to their photos on the Web site? (Choose two)**

   A: *basic authentication with SSL.*
   digest authentication with SSL.

7. **How should you allow studios to create their own customer accounts?**

   A: *Delegate authority to the office manager in each studio's organizational unit (OU).*

8. **Which authentication method or methods can you use to allow studios to securely post pictures to PHOWEB? (Choose all that apply)**

   A: *digest authentication with SSL.*
   basic authentication with SSL.

9. **How should you allow programming changes to the Web site?**

   A: *Grant the Webmaster Full Control permission.*

10. Which audit policy should you use on PHOWEB to detect unauthorized access to the credit card files?

A: success and failure audit for object access.

11. How should you secure the customer photos on PHOWEB?

A: Grant customers Read permission to their own photo folder.

Cybernetic Software Case Study

Background
Cybernetic Software is a software consulting company. The annual growth rate of income, and office resources is 200 and 50 percent respectively.

Organization
Headquarters
Headquarters, which employs approximately 300 people, includes marketing, sales, IT, HR, accounting, and the executive departments. Only 50 of the headquarters employees are permanent employees.

WAN Connectivity
Headquarters has a T1 connection to the Internet. Two of the branch offices connect to headquarters via frame relay. The overseas branch is not connected to headquarters.

LAN Connectivity
The headquarters LAN runs on a 100-Mbps network.

Branch Offices
Each branch has approximately 15 Windows 2000 portable computers, and at least one Windows 2000 desktop computer. Each branch is connected to the Internet via a T1 connection. The overseas office has an Exchange Server, domain controller, and a RAS server named RAS2. The overseas branch administers and maintains its own network.

Security
Headquarters
Security is of utmost importance. Password policies are established, and resources are secure. Customer data has been compromised through the theft of portable computers. Historically, Cybernetic Software has incorrectly granted permissions to shared files for internal employees. This has led to accidental unauthorized access to confidential data. Cybernetic Software wants to encrypt data for transmission to vendors and customers by implementing a Public Key Infrastructure (PKI).

Branch Offices
The overseas office will implement PKI to issue certificates to its employees. Cybernetic Software wants to use secure tunneling for the overseas office. The WAN connection to the stateside branch office will remain the same.

Network Roles and Usage
Human Resources
The HR department uses a network file server to store confidential employee information. The HR manager can manage HR resources throughout the company.

IT
The IT department maintains the network, and controls hardware and software purchases. IT implements physical and network security for the company. The Server Operators group designs networks, resolves tier-two support problems, and resolves network problems. The help desk administers the network, resolves tier-one support problems and resolves problems with employees' computers.

Sales
The Sales employees want their personal and shared sales documents to be more secure. They save personal sales documents on their portable computers, and save shared sales to the SALES\Documents folder. Sales leads, submitted by employees, are stored in the LEADS folder which resides on the Intranet. Employees receive a bonus if their tip is utilized. The Sales department needs to run reports on the sales leads information, and the Executive department needs to review the leads and the reports. The IT department publishes the Web page that lists the leads.

Consultants
Consultants enter their work hours into the TimeClock program. It requires the consultants to enter the date ad number of hours billed, the customer to bill, expenses incurred and the nature of the work accomplished. The TimeClock program is accessed through a secure Web browser.

Branch Offices
Employees must be able to connect to headquarters to access customer and billing information. Stateside branches can access this information through the WAN. The overseas office cannot access the information in the current environment.

Cybernetic Software Practice Questions

1. **What permission should be granted for the LEADS folder?**

   A: IT Department (Full Control)
   Sales Department (Full Control)
   Everyone (Modify)

2. **How should you configure OWA1 and TIME1 to allow secure access for remote employees? (Choose all that apply)**

   A: Place TIME1 in a DMZ.
   Place OWA1 in a DMZ.
   Allow only TCP port 443 connection from the external network.

3. **Which two technologies should you implement to provide additional security for the portable computers? (Choose two)**

A: Digital certificates
Encrypting File System (EFS)

4. **How should you implement Certificate Services for the Omaha offices?**

   A: Use the Certificate Services from the Minneapolis office.

5. **Which type of CA should you implement for the overseas office after it is connected to the WAN?**

   A: Enterprise subordinate CA

6. **Which data from the overseas office should you encrypt?**

   A: L2TP data

7. **Which type of CA should you implement at headquarters?**

   A: An offline enterprise root CA with an online enterprise subordinate CA.

8. **What are the two primary security risks for Cybernetic Software? (Choose two)**

   A: Unauthorized network access by employees.
   Data stolen from portable computers.

   What are the four most important security priorities for Cybernetic Software?

   A: Preventing unauthorized network access.
   Ensuring secure authentication.
   Protecting employee data on portable computers.
   Providing secure communications between the overseas and headquarters offices.

9. **How should you encrypt the Sales departments files?**

   A: Encrypt only personal Sale document individual.

Life Insurance Company Case Study

Background
Life Insurance Company is a subsidiary of Data Corporation, a large financial services company dealing in mainly life insurance. Life Insurance Co. is creating a web site that will allow brokers to configure, price quote, and purchase life insurance policies. The actual delivery of the policy will be made by third party providers.

This web site will be designed to be used by brokers, who do not work for Life Insurance Co., and policy holders. All of the independent brokers must register with Life Insurance Co. before they can use the web site.

Some of the policies sold allow policy holders to allocate the value into various investments. The policy holder can view current allocations and make changes within certain guidelines. Policy holders cannot buy or terminate policies with out the aid of a broker.

Problem

Vice President of Sales of Data Corp.
The company is starting to lose some of its customers to web based insurance concerns. The new web site should help us maintain customers and attract new ones.

The brokers are concerned about other brokers being able to access their information. Nor do they want to hire a computer expert just to use the site. These brokers will cease seeking personal assistance if we can only provide them the on-line resources to guide them.

The success or failure of this project will allow us to attempt similar projects, or we might just sell the whole company.

CIO of Life Insurance Co.
Although the web site is considered separate from Data Corp., we still have to report our results to them at frequent intervals during the first year. They must also be able to check the status of the web site at anytime. The VP of Sales, myself, and the IS Director are required to keep up-to-date with developments at Data Corp. We have user accounts at Data Corp. for that purpose.

IS Director of Life Insurance Co.
We have chosen Windows 2000 as our platform for developing this web site that will act as a virtual insurance company. We are developing a multi-tier Windows DNA insurance application along with the capability that the site will also include content describing the products.

We need to create this environment using only 6 servers. The primary goal will be to ensure that the site is secure and that we can monitor who is accessing it. There will be 3 distinct types of users: brokers, policy holders, and Data Corp/Life Insurance Co. employees. There will also be some subdivision of these primary users.

Lead Developer at Life Insurance Co.
In the past we have used a SQL database to store userIDs and passwords. However, this time we want to take advantage of the Public Key Infrastructure (PKI) features in Windows 2000 to provide increased security.

Logistics Manager at Life Insurance Co.
During the initial enrollment period of operation, we will be signing up in access of 5000 new brokers for this site. After this, we expect only a few brokers to join or leave the site on a daily basis. We can hire temps to handle the initial enrollment period.

Certificate registration and delivery will be handled off-line and brokers must register either by phone or in person. After brokers are registered, the client certificate will be delivered on a floppy or CD by a secure courier.

Envisioned Environment

Servers
All 6 servers will exist within a single domain. WEB1 will be the name of the Web Server. This server will run IIS and mid-tier COM components designed for the insurance application. DATA1 will be used as the database server and it will run Microsoft SQL 7.0. DC1 will be the name of the domain controller and certificate server. This server will also run DNS, WINS and DHCP. A multi-homed server called VPN1 will be used to create a VPN to Data Corp. WEB2 will be used as an Intranet web serve, a file and print server, and a domain controller. FIRE1 will be used as a firewall server running third-part firewall software.

Local Client Computers
There will be fewer than 20 employees required to manage this site once it is on-line. Only about 5 of these should ever need to access the site remotely via portable computers.

Internet Client Computers
Brokers will connect to the site over the Internet and they will have a limited technical background. Any setup process for this site must be easy to follow. Most of this site will not be available to the general public. Therefore, the site will be designed specifically for IE 4.0 or later. The public section of the site will be designed for IE or Netscape browsers.

Administration
Only a small group of users will be able to administer the site and they will perform these tasks either at the servers or from locally connected desktops.

LAN
A new LAN will be created to host the site and all necessary services, such as DNS, will be handled by that LAN's computers. There are 2 Class C address spaces. One will be used by the publicly available servers, and the other will be used for internal computers that should not be access from the Internet. NAT will not be used and all desktops will run Windows 2000 Professional.

WAN
Life Insurance Co. will host the site at its location and is not directly connected to the Data Corp. WAN. Instead, Data Corp will be able to access the site through a VPN connection trough the Internet.

Internet Connectivity
Life Insurance Co. has secured the domain name lifeinsuranceco.com and has leased a single T3 line for connectivity to the Internet.

Life Insurance Company Practice Questions

1. **What is Life Insurance Co.'s tolerance for risk?**

A: They are willing to try some new approaches.

2. **What is the primary risk for desktop computers at Life Insurance Co.?**

A: Another Life Insurance Co. employee connected to a desktop via the LAN.

3. **What should be included in an audit policy for DC1?**

A: Success and failure audit for account logon events.
Success and failure audit for object access.

4. **What technology should you include in your security strategy to secure broker access?**

A: SSL, digital certificates, and Directory Service mapping.

5. **How should you design the Active Directory structure for Life Insurance Co.?**

A: Create a single domain in its own forest.
Establish a one-way trust relationship with Data Corp.'s domain.

6. **Design an authentication strategy for the web site after certificates have been issued to the brokers. (Use only what applies)**

	Computers
A	Broker
B	Life Insurance Co. employee
C	DATA1
D	DC1
E	VPN1
F	WEB1

	Authentication Methods
1	Kerberos
2	Basic Authentication with SSL
3	SSL and Directory Service Mapping
4	HTTP and Directory Service Mapping

A: B – 2 – E, A – 3 – F, F – 1 – D, C – 4 - F

7. **Which technology should you implement to provide the highest level of security for communications between employees of Data Corp. and Life Insurance Co.?**

A: L2TP over IPSec

8. **How should you separate intranet resources from publicly visible Internet Servers?**

A: Use corp.lifeinsuranceco.com as a suffix for all internal sites.
Configure the internal DNS to resolve internal names, but do not include these names in the internal DNS.

9. **How would you implement a Public Key Infrastructure at Life Insurance Co?**

A: Install off-line enterprise root CA
Install on-line enterprise subordinate CA
Issue client certificates on the subordinate CA

10. **Which 3 options should you include in a security template for WEB1?**

A: Set the NTLM authentication level to LM and NTLM.
Limit CD-ROM access to users who are logged on locally.
Rename the Administrator account.

11. **Which technologies should you include in your security strategy to secure broker access \to the web?**

A: SSL. Digital certificates, and Directory Service Mapping

INDEX