Windows 2000 Security

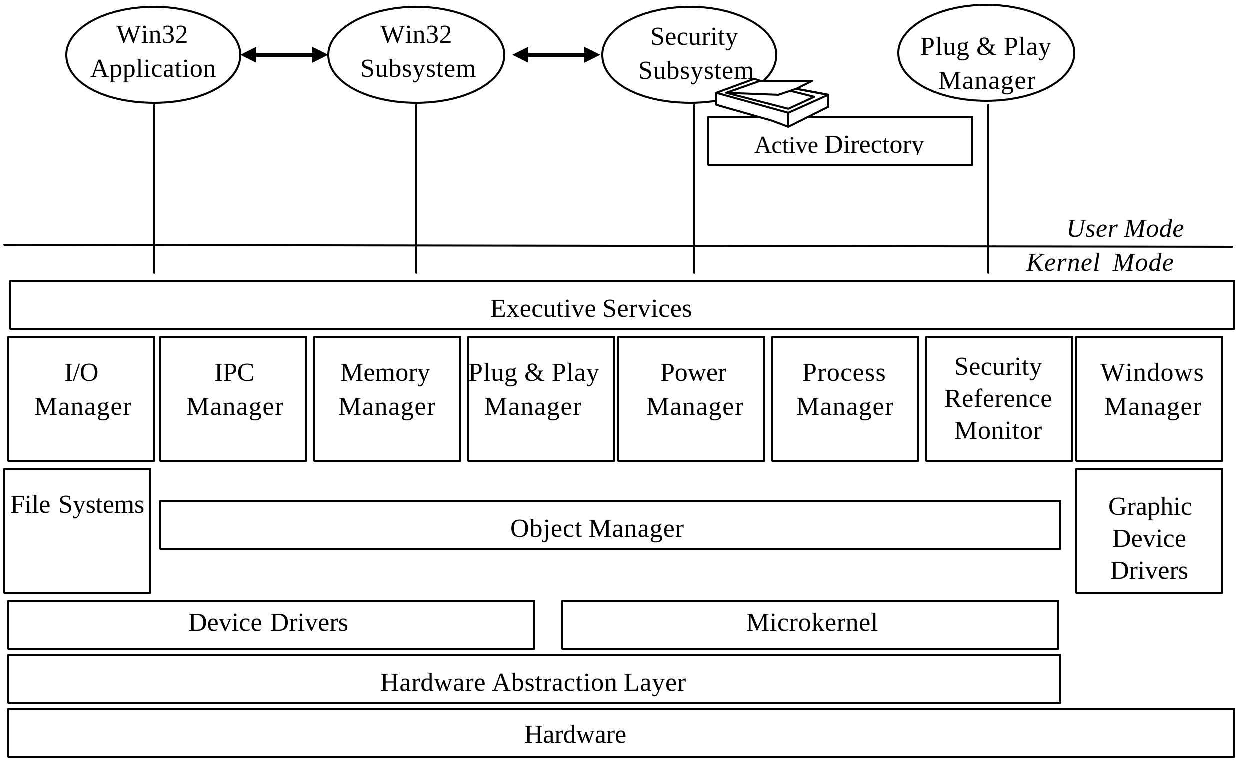
Study Guide
For exam
70-220

Table of Content

Microsoft Windows 2000 Security Services

Windows 2000 operating system provides two processor access modes to ensure that applications are unable to directly access hardware and system code. Applications generally run in what is known as *user mode* and operating system functions run in *kernel mode.*

Security in Windows 2000 is split between user mode and kernel mode. In user mode the security subsystem is the actual subsystem where Active Directory directory service runs. In kernel mode the security reference monitor enforces the security rules of the security subsystem. The actual enforcement of security takes place in kernel mode, where user intervention can't occur



Security within the Windows 200 architecture

The security subsystem runs within the security context of the local security authority (LSA) process. This process is split between user mode and kernel mode. The components within the local security authority process include:

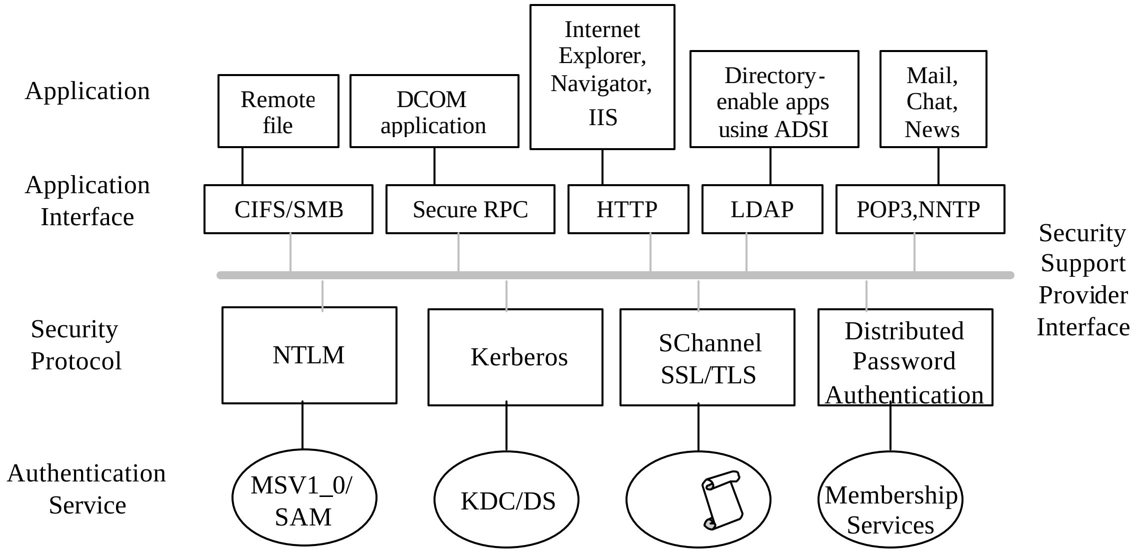
Netlogon service (Netlogon.dll). The Netlogon service maintains a computer's secure channel to a domain controller in its domain

- **NTLM authentication protocol (Msv1_0.dll).** NTLM is used to authenticate clients that are unable to use Kerberos authentication. This includes Windows 95, Windows 98, and Windows NT computers.

    - **Secure Sockets Layer (SSL) authentication protocol (Schannel.dll).** SSL provides encryption services to transported data at the application layer.
    - **Kerberos v5 authentication protocol (Kerberos.dll).** Kerberos v5 is the default authentication protocol used by Windows 2000. Kerberos authentication is based on the use of ticket-granting tickets (TGTs) and service tickets.

- **Kerberos Key Distribution Center (KDC) service (Kdcsvc.dll).** The KDC service is responsible for issuing TGTs to clients when they initially authenticate with the network. A TGT is then used for subsequent requests to acquire service tickets to provide authentication of the requesting client.
- **LSA server service (Lsasrv.dll).** The LSA server service enforces all defined security policies within Active Directory.
- **Security Accounts Manager (SAM) (Samsrv.dll).** The SAM is used on non-domain controllers for the storage of local security accounts. The SAM also enforces all locally stored policies.
- **Directory Service module (ntdsa.dll).** The Directory Service module supports replication between Windows 2000 domain controllers, all Lightweight Directory Access Protocol (LDAP) access to Active Directory and management of naming contexts stored in Active Directory. The naming contexts include the domain naming context, the configuration naming context, and the schema naming context.
- **Multiple Authentication Provider (Secur32.dll).** This Security Support Provider (SSP) supports all security packages available on the system. The security packages include the Kerberos, Windows NT LAN Manager (NTLM), Secure channel, and Distributed Password Authentication (DPA) packages.

Windows 2000 Security Protocols



- **Windows NT LAN Manager (NTLM).** Used by Windows NT, Windows 95, and Windows 98 clients with the Directory Services client installed. NTLM is used for pass-through network authentication, local account authentication for Windows 2000 Professional and Windows 2000 member servers, and access to previous Microsoft operating systems. The NTLM security provider uses the MSV1_0 authentication service and the Netlogon service to provide client authentication and authorization.
- **Kerberos v5**. The default security protocol for Windows 2000–based computers. Kerberos provides mutual authentication of client and server, better performance, and support for delegation. The Kerberos security provider uses the Key Distribution Center (KDC) service on a domain controller and Active Directory for obtaining TGTs and service tickets.
- **Distributed Password Authentication (DPA)**. A shared secret authentication protocol used by Internet membership organizations such as MSN
- **Secure channel (SChannel) services**. Provide the ability to authenticate using public key–based protocols such as SSL and Transport Layer Security (TLS).

Designing Active Directory for Security

Single Forest versus Multiple forest deployment

The most common configuration for deploying an Active Directory in an organization is a single forest. The main reason to deploy a single forest is that it will share common information across each of its component domains. The information that is shared includes

- **Schema.** A schema defines all classes and attributes that can be used within the forest. The write-enabled copy of the schema is maintained on the schema operations master. By default, the first DC installed on the forest is designated as the schema operations master.
- **Configuration.** The configuration naming context maintains a listing of all domains and sites within a forest, thus ensuring that no duplicate names are created.
- **Global catalog.** The global catalog maintains a partial set of attributes for all objects that exist within a forest.

There are limited scenarios in which an organization have to implement multiple forests. These scenarios generally involve decentralized organizations that perform much of their network operations within each individual sector. Another common scenario is an Internet Service Provider (ISP) that doesn't want to have a common directory for all their clients. It's preferable in this case to create separate forests for each client to prevent clients from browsing the directory of another client of the ISP.

These disadvantages range from actual monetary costs to a loss of functionality or flexibility in your network design. Possible problems include:

- A more complicated and expensive domain structure.
- Additional management costs for forest-wide components such as the schema and configuration naming contexts.
- Additional management costs for trust relationships.
- Limited use of universal principal names.
- Limiting smart cards to using default user principal names.

Single Domain versus Multiple Domain implementation

A single-domain forest is commonly implemented in organizations that maintain centralized control of user and computer accounts. By maintaining only a single domain, membership in the Administrators group is easily monitored to ensure that no users are granted excess privileges on the network.

Choosing to implement a single domain will have the following effects on Active Directory:

- It reduces management of the forest.
- It reduces the number of required DCs.
- It reduces the dependency on global catalog servers for authentication.
- It provides an easier migration path to multiple domains.

One of the key reasons to implement multiple domains is a requirement for differing account policies. Account policies can only be applied at a domain level. There's no way to implement varying account policies within a single domain. If varying account policies are defined, this requires that multiple domains exist within the forest.

Account policies include the following three categories of configuration:

- **Password Policy.** Defines the characteristics of passwords that may be used to authenticate to the domain.
- **Account Lockout Policy.** Defines which actions must be taken when a specified amount of failed logon attempts occur in a short period of time.
- **Kerberos Policy.** Defines maximum ticket lifetimes for Kerberos authentication and tolerances for clock synchronization between client computers and servers.

Delegating Control to an Organizational Unit

In Windows 2000, administration can be delegated to a specific OU by using the Delegation of Control Wizard.

Audit Strategy

Within Windows 2000 you can configure several auditing settings. In some cases all you have to do is configure the audit settings within the audit policy

The audit policies that can be defined for a domain include

- **Audit Account Logon Events.** Occurs any time a user logs on to a computer. If the user logs on to the local computer, the event is recorded in the computer's audit log. If the user logs on to a domain, the authenticating domain controller records the account logon event.
- **Audit Account Management.** Occurs whenever a user creates, changes, or deletes a user account or group. It also occurs when a user account is renamed, disabled, or enabled, or a password is set or changed.
- **Audit Directory Service Access.** Occurs whenever a user gains access to an Active Directory object. To log this type of access, you must configure specific Active Directory objects for auditing.

- **Audit Logon Events.** Recorded any time a user authenticates with the local computer or with Active Directory. This includes physically logging on at a computer or establishing a network connection to the computer.
- **Audit Object Access.** Logged any time a user gains access to a file, folder, or printer. The administrator must configure specific files, folders, or printers for auditing.
- **Audit Policy Change.** Occurs any time local policies are changed in Group Policy. This includes user rights, audit policy, or security options.
- **Audit Privilege Use.** Occurs any time a user exercises a user right, such as changing the system time, or any time an administrator takes ownership of a file.
- **Audit Process Tracking.** Occurs any time an application performs an action. This setting is used to determine which files and registry keys an application requires access to when operating.
- **Audit System Events.** Occurs any time a server is restarted or shut down. It also occurs any time the security log is reset on the computer.

Authentication in a Microsoft Windows 2000 Network

Authentication allows network administrators to determine who is accessing the network and to design restrictions so that each authenticated user can access only desired areas of the network.

Kerberos Authentication

The components of the Kerberos v5 protocol include

Key distribution center (KDC). A network service that supplies both ticket-granting tickets (TGTs) and service tickets to users and computers on the network.

TGT. Provided to users the first time they authenticate with the KDC. The TGT is a service ticket for the KDC.

Service ticket. The user provides a service ticket whenever he connects to a service on the network. The user acquires the service ticket by presenting the TGT to the KDC and requesting a service ticket for the target network service.

Referral ticket. Issued anytime a user attempts to connect to a target server that's a member of a different domain.

Kerberos provides the following advantages over the NTLM protocol:

- **Mutual authentication.** For all Kerberos transactions, both the user and the server are authenticated.
- **Single sign-on.** Within a forest, a user who authenticates to the network using Kerberos v5 authentication won't have to provide any other credentials when accessing any resources in the forest.
- **Ticket caching.** After acquiring a service ticket from the KDC, the user then caches the service ticket in the client's personal ticket cache. This reduces the number of times that a user must contact DCs for authentication.
- **Delegation.** Kerberos lets services impersonate connecting users when the service connects to services located on other servers
- **Standards-based protocol.** Kerberos is an industry standard authentication protocol. The Windows 2000 implementation of Kerberos v5 is compliant with Request for Comment (RFC) 1510 and RFC 1964.
- **Interoperability.** Kerberos authentication can be used to provide interoperable authentication between Windows 2000 domains and Kerberos realms in a UNIX environment. This allows ease of access to resources using a secure authentication protocol.

Kerberos Message Exchanges

Authentication Service Exchange. Used by the KDC to provide a user with a logon session key and a TGT for future service ticket requests.

Ticket Granting Service Exchange. Used by the KDC to distribute service session keys and service tickets.

Client/Server Authentication Exchange. A user uses this message exchange when presenting a service ticket to a target service on the network.

Smart Card Authentication

Windows 2000 supports the use of smart card authentication by using PKINIT extensions for Kerberos. This allows public/private keys to be used to authenticate the user when he logs on to the network in place of the standard Kerberos Authentication Service Request and Response.

Private and Public Key Usage for Smart Card Logon

Process	Key Used
Client-side encryption of the preauthentication data	Private key
KDC-side decryption of the preauthentication data	Public key
KDC-side encryption of session key	Public key
Client-side decryption of session key	Private key

NTLM Authentication

Only Windows 2000 clients and UNIX clients can use Kerberos authentication in a Windows 2000 domain. To provide access to Windows NT 4.0 clients and Windows 95 and Windows 98 clients running the Directory Service client, Windows 2000 continues to support the use of the Windows NT LAN Manager (NTLM) authentication protocol.

To counteract security weaknesses in the NTLM protocol, NTLM version 2 was developed for Windows NT 4.0 Service Pack 4. NTLMv2 introduces additional security features, including

- **Unique session keys per connection.** Each time a new connection is established, a unique session key is generated for that session.
- **Session keys protected with a key exchange.** The session key can't be intercepted and used unless the key pair used to protect the session key is obtained.
- **Unique keys generated for the encryption and integrity of session data.** The key that's used for the encryption of data from the client to the server will be different from the one that's used for the encryption of data from the server to the client.

Determining when NTLMv2 Authentication is Used

Client	Use NTLMv2 when
Windows 2000	Authenticating to the local SAM database of a stand-alone Windows 2000–based computer
	Authenticating with a Windows NT 4.0 computer with SP4 or higher installed
Windows NT 4.0	Authenticating with Windows 2000 and Windows NT 4.0 servers and the client has Service Pack 4 or higher applied
	Authenticating with Windows 2000 and Windows NT 4.0 servers and the client has the Directory Services Client installed
Windows 95 / Windows 98	Authenticating with Windows 2000 and Windows NT 4.0 servers and the client has the Directory Services Client installed

Authenticating Down-Level Clients

Without service packs or additional software, Windows NT 4.0, Windows 95, and Windows 98 clients introduce security weaknesses for authentication on a Windows 2000 network.

The Microsoft Directory Service Client (DSClient) has been developed to counteract these weaknesses. The DSClient software allows Windows NT 4.0, Windows 95, and

Windows 98 clients to use NTLMv2 for authentication in the Windows 2000 network. The following section outlines some of the features of the DSClient software.

- **NTLMv2 authentication protocol.** Windows 95, Windows 98, and Windows NT 4.0 clients will use NTLMv2, rather than weaker forms of authentication, when authenticating with Active Directory.
- **Site awareness.** The DSClient software allows the client to query DNS to find a DC in the same site.
- **Search for objects in Active Directory.**The DSClient software allows clients to search Active Directory for printers and users from the Start|Search menu.
- **Reduces dependency on the PDC.** Rather than having to connect to the PDC of the domain for password changes, the DSClient software allows down-level clients to connect to any DC in the domain for password changes.
- **Active Directory Services Interface (ADSI).** The DSClient software provides a common programming API for Active Directory programmers. This allows scripting to take place at the client that writes changes to Active Directory.
- **Distributed Files System (DFS) fault tolerance client.** The DSClient software allows clients to access and find Windows 2000 DFS file shares in Active Directory.
- **Active Directory Windows Address Book (WAB) property pages.** The DSClient software allows users to change attributes of their user object using the Start|Search|For People menu option. This is, of course, subject to the security settings on their user object.

It's also important to note that there are some features that the DSClient software doesn't provide. These features require an upgrade to Windows 2000 as the client operating system:

- **Kerberos support.** The DSClient software doesn't provide Kerberos support to Windows 95, Windows 98, and Windows NT 4.0 clients. They can use only NTLMv2 to strengthen authentication security.
- **Group Policy/Intellimirror support.** Even with the DSClient software loaded, a Windows 95, Windows 98, or Windows NT 4.0 client won't participate in Group Policy or Intellimirror. To deliver similar functionality, system policy must be maintained in the Active Directory environment.
- **IPSec/L2TP support.** Windows 95, Windows 98, and Windows NT 4.0 clients only support PPTP for VPN connections. There's no support for L2TP/IPSec connections.
- **Server Principal Name (SPN)/mutual authentication.** The DSClient doesn't provide SPNs or mutual authentication to Windows 95, Windows 98, and Windows NT clients.
- **Dynamic DNS support.** The DSClient software doesn't allow Windows 95, Windows 98, or Windows NT clients to update their own DNS resource records using dynamic update. For Windows 95, Windows 98, and Windows NT clients, the Dynamic Host Configuration Protocol (DHCP) server must be configured to update the DNS resource records on behalf of the client computers.

- **User Principal Name (UPN) authentication.** The DSClient software doesn't allow users to authenticate using their UPN (user@domain.com). This functionality is only available in Windows 2000 clients.

After distributing DSClient software to clients the protocols can be restricted which can be used to authenticate with a Windows 2000 computer by adjusting registry value HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel at all Windows 2000–based computers in the domain, and setting one of the following six values for the REG-DWORD value:

- **0 (send LM & NTLM responses).** Offers the most interoperability. Any previous down-level clients that use either LM or NTLM for authentication can authenticate with the server.
- **1 (Send LM & NTLM–use NTLMv2 session security if negotiated).** Offers more security when the DSClient software is deployed.
- **2 (Send NTLM response only).** More useful in Windows NT networks where you want to restrict the use of Windows 95 and Windows 98 clients.
- **3 (Send NTLMv2 response only).** Configures the Windows 2000 computer to respond with NTLMv2 authentication for down-level authentication requests.
- **4 (Send NTLMv2 response only\refuse LM).** Configures the Windows 2000 computer to respond with only NTLMv2 authentication for down-level authentication requests
- **5 (Send NTLMv2 response only\refuse LM & NTLM).** Ensures that only NTLMv2 responses are sent and that authentication requests that don't use NTLMv2 will be rejected

Administrative Group Membership

Windows 2000 contains several predefined administrative groups.

The Default Windows 2000 Administrative Groups

Group Name	Group Type	Purpose
Enterprise Admins	Universal	Exists only within the forest root domain. Has forest-wide administrative scope. Members of this group are allowed to modify Enterprise-wide configuration. Membership must be monitored at all times.
Schema Admins	Universal	Exists only within the forest root domain. Members can make changes to the forest schema, including the modification of existing attributes and classes or the addition of new attributes or classes.

Domain Admins	Global	A member of the Administrators group within each domain of the forest. When a member server or workstation joins the domain, the Domain Admins group is added as a member of the local Administrators group. Members can administer the domain in which they are defined. Additionally, members of the Domain Admins group in the forest root domain are permitted to modify membership of the Enterprise Admins or Schema Admins groups as they exist in the forest root domain.
Group Policy Creator Owners	Global	Members are allowed to create new Group Policy objects in Active Directory.
Administrators	Domain Local	Members are allowed to fully manage the domain in which the group exists, including management of services and accounts within Active Directory.
Power Users	Local Group	Exists only on non domain controllers. Members are allowed to manage users and groups in the local SAM database, modify or delete accounts that they created, and manage membership in the Users, Guests, and Power Users groups. Power Users also can install most applications; create, manage, and delete local printers; and create and delete file shares.
Account Operators	Domain Local	Members of this group can create, modify, or delete accounts for users, groups, and computers in any container within the domain where the Account Operators group exists. The only exceptions are the Built in container and the Domain Controllers OU. The only groups that Account Operators are prohibited from managing are the Administrators and Domain Admins groups. In the forest root domain, members can't modify the properties of the Enterprise Admins or Schema Admins groups.
Server Operators	Domain Local	Members are allowed to log on locally at a server, manage network shares, stop and start services, back up and restore data, format hard disk drives, and shut down the computer.
Print Operators	Domain Local	Members can manage printers and printer queues, including managing print jobs that weren't submitted by the member.
Backup Operators	Local	Members are allowed to back up and restore all files on the computer. Members aren't subject to permissions on files when performing the backup. Members also can log on locally and shut down the computer.
Replicators	Domain Local	In Windows NT domains, it's a built-in group used by the File Replication service on DCs.
DHCP Administrators	Domain Local	Members can administer DHCP services within the domain where the group exists. This group is created automatically

		when the DHCP service is installed.
DNS Admins	Domain Local	Members can administer DNS services in the domain where the group is defined. This group has members in any domain where the DNS service is installed.
WINS Admins	Domain Local	Members can administer the Windows Internet Naming Service (WINS) service within the domain where the group is defined. This group is *not* created automatically when the WINS service is installed in a domain.
DNSUpdate Proxy	Global	Members can create DNS resource records without taking ownership of the DNS resource records. Generally, DHCP servers are made members of this group to ensure that a client workstation using Windows 95, Windows 98, or Windows NT can take ownership of the resource record after the computers are upgraded to Windows 2000.
Pre–Windows 2000 Compatible Access	Domain Local	Members can query Active Directory using a NULL session. During the DCPROMO process, which installs and configures Active Directory to promote a server to a DC, if the option to enable pre–Windows 2000 compatible access for remote access is enabled, the Everyone group is added as a member to this group.

Securing Administrative Access to the Network

There are several methods exists to secure how administrators can access the network. These include

- Requiring smart card logon.
- Restricting which workstation administrators can log on to.
- Configuring logon hours.
- Renaming the default administrator account.
- Enforcing strong passwords.

Secondary Access

Windows 2000 allows administrative tasks to be launched at a higher security level than the current user's account. This is done by providing alternate credentials to the RunAs service when launching the administrative tasks.

Holding the Shift key while right-clicking a shortcut. This enables the RunAs option on the pop-up menu. The user can then provide alternative credentials for running the application.

Using the RUNAS command at a command prompt. The RUNAS command allows you to provide both the alternative credentials and the application that you wish to run using the alternative credentials. The syntax of the command is as follows:

- `RUNAS /user:UserName program`

Terminal Services Administration

Securing Terminal Server Access

Task	**Solution**
Limit what utilities can be run by a Terminal Services client	Create a custom desktop and Start menu profile that will be used by the Terminal Service client.
Restrict access to Terminal Services to only administrative personnel	Configure Terminal Services to use Remote Administration mode. This restricts access to only the members of the Administrators group.
Secure transmission of data between the Terminal Services client and the terminal server	Configure the encryption level for the Terminal Services session to be medium or high security. Both medium and high security ensures that data is encrypted in both directions between the client and the server. High security utilizes 128-bit encryption, while medium encryption uses either 40-bit or 56-bit encryption, depending on the client.
Determine Terminal Service access based on individual user permissions	Apply the Notssid.inf security configuration template to the terminal server.
Prevent excess rights to DCs	Don't install Terminal Services on a DC. This requires the Terminal Service users to have the Logon Locally right, which means that they can log on locally at all DCs.
Allow access to Terminal Services from the widest range of platforms	Install the Terminal Services Advanced Client on a Web server to allow all Internet Explorer clients to connect to the terminal server by downloading the ActiveX control that allows access to the terminal server.

Microsoft Windows 2000 Security Groups

In a Windows 2000 network, access to network resources is authorized through the inspection of the user Security Identifier (SID) and any group SIDs for the user account. To allow auditing of security access and to simplify the administration of network resources, use groups when you design security assignments.

You can define two different types of Windows 2000 groups: *security groups* and *distribution groups*. Use security groups for entries in discretionary access control lists (DACLs) and system access control lists (SACLs) to define security and auditing settings for an object.

Group Membership in a Windows 2000 Domain

Group Scope	**Mixed Mode Membership**	**Native Mode Membership**
Domain Local	User accounts from any domain Global groups from any domain	User accounts from any domain Global groups from any domain Universal groups from any domain Domain local groups from the same domain
Global	User accounts from the same domain	User accounts from the same domain Global groups from the same domain
Universal	N/A	User accounts from any domain Global groups from any domain Universal groups from any domain
Computer Local	Local user accounts Domain user accounts from any domain Global groups from any domain	User accounts from any domain Global groups from any domain

User Rights

User rights define who can log on to a computer, the methods that can be used to log on to a computer, and the privileges that have been assigned to a user or group on that computer. Although user rights can be applied locally at a computer, in a Windows 2000 network it's preferable to define user rights by using Group Policy. Within a Group Policy Object, user rights are defined in the following location: Computer Configuration\Windows Settings\Security Settings \Local Policies\User Rights Assignments. As with all Group Policy settings, the Group Policy Object defined closest to the computer object in Active Directory will take precedence in the case of conflicting settings. The only exception is Account Policy settings within Group Policy. Account Policy settings are always applied from the Default Domain Policy.

Securing Access to File Resources

Share Security

Share permissions are used to secure network access to data stored on a server. Share permissions are flexible in that they aren't limited to a specific file system. You can establish shares for folders located on file allocation table (FAT), FAT32, NTFS, and CD-ROM file system (CDFS) volumes.

Note - Although they're flexible, share permissions are limited in that they have no effect on a user who is logged on locally at the computer hosting the shared folder, i.e. user must connect through network.

NTFS Security

While share permissions affect only network users, NTFS permissions affect both network users and users who are at the computer console. In addition to providing local folder security, NTFS allows permissions to be set for individual files within a folder.

Changes in the Windows 2000 NTFS File System

Windows 2000 introduces functionality in the NTFS file system that isn't found in Windows NT. This functionality includes

- **Encryption.** File-level and directory-level encryption is supported in Windows 2000 through the Encrypting Files System (EFS). EFS allows files and folders to be encrypted so that only the user who performed the encryption (or a designated EFS recovery agent) can decrypt the protected files.
- **Quotas.** NTFS allows storage space restrictions to be set on a per volume basis. You can apply these quotas on a per user basis to limit the amount of disk space in which a user can store data on a volume.

- **Permission inheritance.** Permissions configured at a parent folder propagate to subfolders and file objects within the parent folder. This feature reduces the effort required to modify the permissions of multiple files and subfolders.

Securing Access to Print Resources

You assign printer security by defining permissions when a printer is shared. The permissions you can assign for a printer include

- **Print.** A security principal assigned this permission can submit print jobs to a printer and have the printer process the jobs.
- **Manage Documents.** A security principal assigned this permission can change the order of documents and pause or delete documents in the print queue. By default, this permission is assigned to the special group named Creator Owner. This assignment allows all users to manage their own print jobs submitted to a printer.
- **Manage Printers.** A security principal assigned this permission can share a printer and change a printer's properties.

Print Security Design Decisions

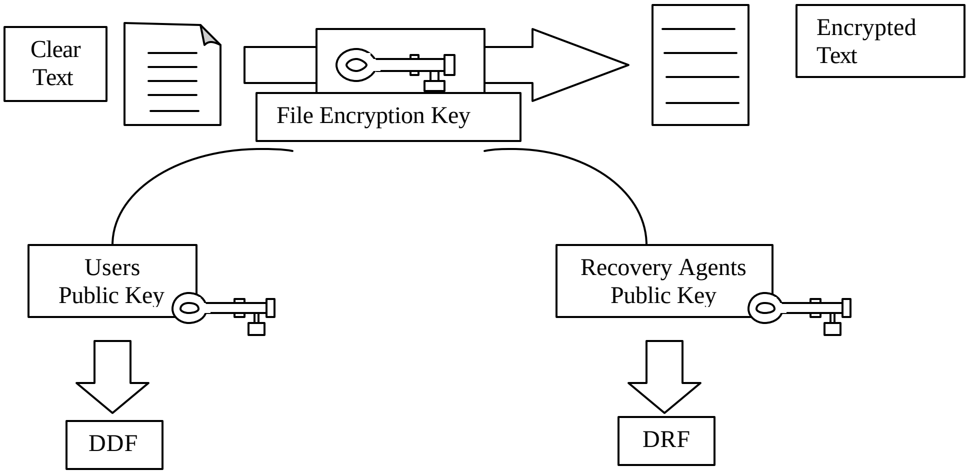
To	**Do the Following**
Restrict access to the printer to specific groups	Change the default permissions to only allow the specific domain local groups Print permissions. You'd of users make the users members of the domain local group by placing the users in a global group that's a member of the domain local group.
Delegate administration of a printer	Make the security principal a member of the Print Operators group. To restrict to a specific printer, assign the Manage Printers permissions to the security principal.
Prevent inspection of print jobs	Use IPSec between the clients and the print server. Locate printers that print confidential data in restricted areas of the office. Attach the printers directly to the print server. Network-attached printers currently are incapable of performing IPSec operations.

Encrypting File System (EFS) Security

Encrypting File System (EFS) allows you to secure files that are stored locally. In addition to encrypting files, you must develop a plan for recovering data in the event recovery keys are lost.

Encrypting EFS Data

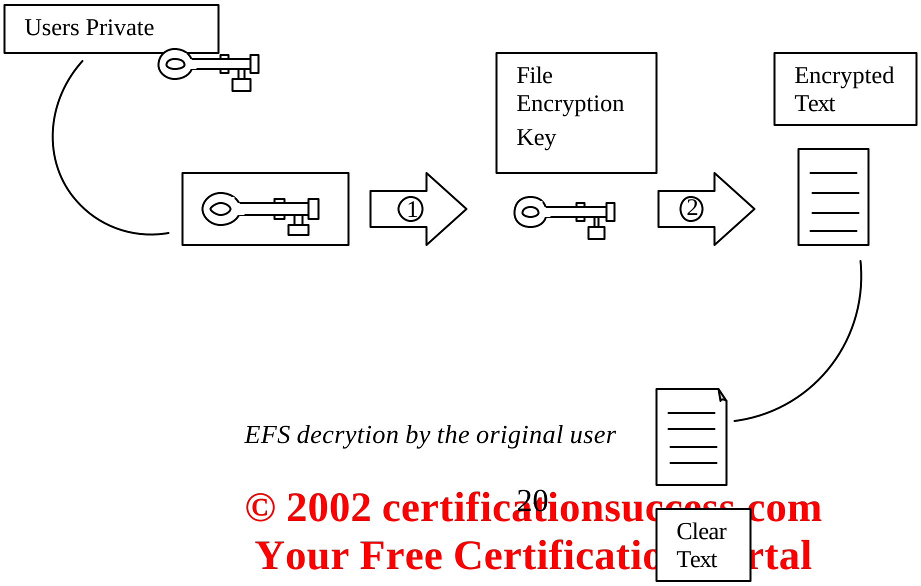
The data encryption process takes place any time a user sets the encryption attribute on a file or folder or when the user saves a file that has the encryption attribute enabled.



The EFS encryption process

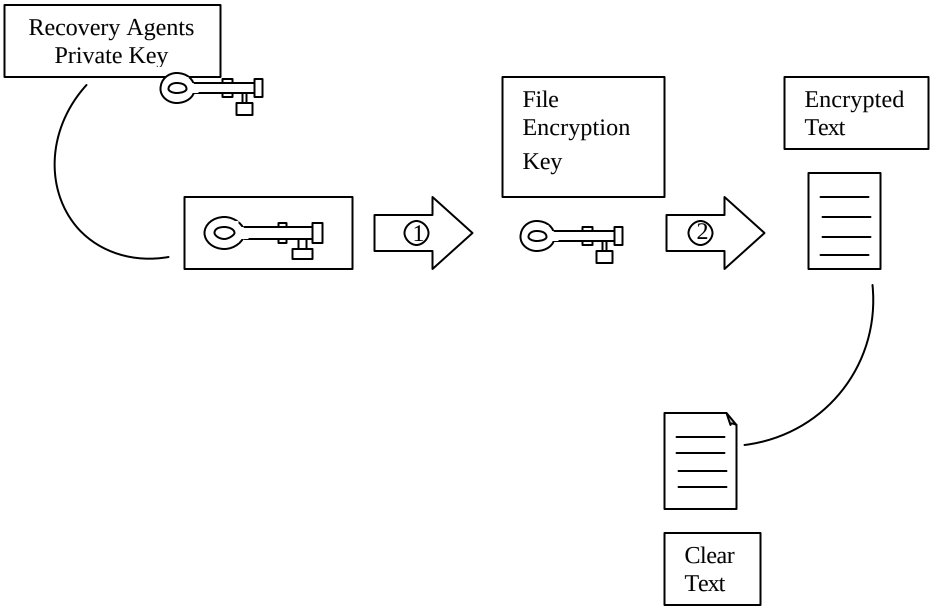
Decrypting EFS Data

Once a file is encrypted, only the user who encrypted the file or a designated EFS recovery agent can open the file and view its contents. The process of decrypting the file differs based on whether it's done by the user or the EFS recovery agent.



EFS decrytion by the original user

Decryption by an EFS Recovery Agent



EFS decrytion by the EFS recovery agent

Decision Factors for EFS Recovery Agents

To	**Do the Following**
Ensure the recoverability of all EFS-encrypted files in a domain	Define an encrypted data recovery agent in the default domain policy.
Prevent EFS encryption from being used	Delete all existing recovery agent certificates in the Encrypted Data Recovery Agent policy.
Prevent specific computers from using EFS encryption	Place all computers that can't use EFS encryption in a separate OU or OU structure. At the OU or the parent OU, define a Group Policy object that has an empty policy. This is accomplished by initializing an empty policy from encrypted data recovery agents in the Group Policy object.
Restrict EFS encryption to specific users	You can't do this unless all users have only one computer where they log on to the network. EFS recovery agents are a property of the computer, not the user.

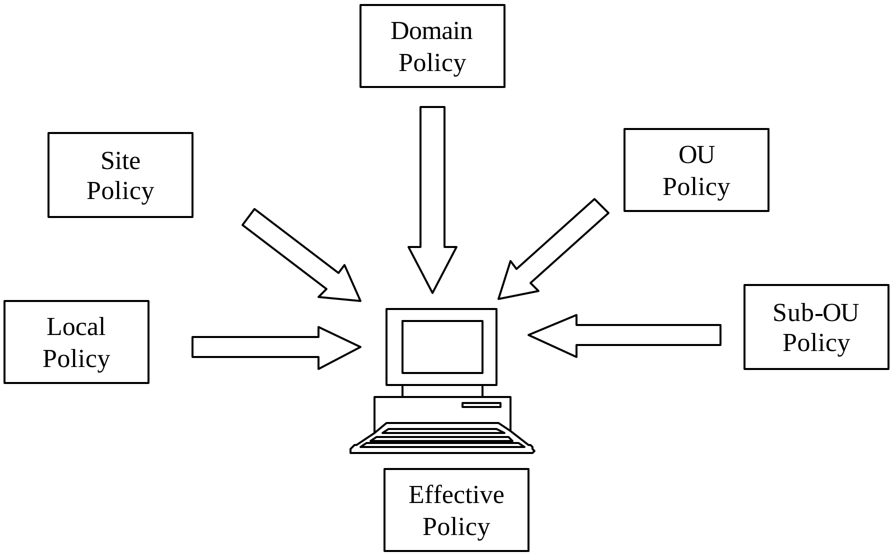
Planning EFS Recovery

To	Do the Following
Restrict the ability to recover encrypted files	Export the private key of the defined recovery agent to a PKCS#12 file. Import the file only when it's necessary to recover an encrypted file.
Restrict recovery to a specific workstation	Create a new account to perform the recovery and restrict the account to the desired workstation. Import the PKCS#12 file to restore the private key for recovery.
Allow more than one private key to perform EFS recovery	Designate more than one certificate in the encrypted data recovery agent policy.
Determine which users can decrypt a file	Use Efsinfo /U /C to determine which private key is required to decrypt the DDF and decrypt the File Encryption Key.
Determine which recovery agents can decrypt a file	Use Efsinfo /R /C to determine which private key is required to decrypt the DRF and decrypt the File Encryption Key.

Deployment of Group Policy

Group Policy allows centralized control of user and computer configuration settings. Rather than applying security settings at each computer in an organization, Group Policy uses Active Directory to centralize management and standardize security settings.

Inheritance simplifies Group Policy administration by allowing administrators to apply widespread policy settings only to higher-level OUs.



Group Policy application Order

Designing Group Policy Application

To	Do the Following
Simplify the troubleshooting of Group Policy	Allow only default inheritance to take place, rather than implementing Block Policy Inheritance or No Override settings. This action might require extensive reworking of your OU design.
Minimize the time spent processing Group Policy during logon	Minimize the number of levels where Group is applied in the OU structure. Avoid cross-linking Group Policy objects between domains.
Prevent blocking of key Group Policy settings	Break the key settings into a separate Group Policy object and apply the No Override attribute to the Group Policy object.
Prevent users from changing configuration by applying Local Group Policies	Ensure that important settings are defined in Group Policy. Group Policy settings always take precedence over local Group Policy settings.
Apply central Group Policy that will affect all users	Apply the Group Policy object higher in the Active Directory hierarchy. These Group Policy objects are commonly applied at the domain or at a top-level OU.
Apply specific Group Policy to a limited number of computers or users	Apply the Group Policy object at the OU where the user or computer objects are located in Active Directory.

Designing Group Policy Filtering

To	Incorporate the Following into Your Design Plan
Ensure that a Group Policy is applied to a security group	Assign both the Read and Apply Group Policy permissions to the security group.
Prevent an OU administrator from blocking inheritance	Don't assign the OU administrator the Write permission for the Group Policy object. Apply the Group Policy object at the parent OU and filter the Group Policy object so that it's applied to only the computers or users in the child OU.
Prevent application of a Group Policy object to a specific group of users or computers	Create a security group with those users or computers as members. Assign the security group the Deny permission for Apply Group Policy. This security assignment prevents the Group Policy object from being applied to the security group.

Troubleshooting Group Policy

One common reason that Group Policy application doesn't always work as expected is that there's been a misapplication of the Block Policy Inheritance or No Override attributes to Group Policy. Take the following steps to troubleshoot Group Policy application:

- Inspect the Active Directory hierarchy.

Inspect applied Group Policies by using Gpresult. The Gpresult utility from the *Microsoft Windows 2000 Server Resource Kit* shows which Group Policies were applied to the computer or user.

The Gpresult utility uses the following parameters:

```
gpresult [/V] [/S] [/C | /U] [/?]
```

where:

/V runs Gpresult in verbose mode

/S runs Gpresult in super verbose mode

/C displays only the Group Policy objects applied to the computer

/U displays only the Group Policy objects applied to the user

In addition to showing which Group Policy objects were applied, the Gpresult utility also lists all group memberships of the user or computer being analyzed.

Troubleshooting Group Policy Application

To	Do the Following
Determine all possible locations where Group Policy objects may be defined	Inspect the Active Directory structure to determine the site, domain, and OUs that could have Group Policy applied to the user or computer.
Determine whether the Group Policy that was applied is a user or computer configuration setting	Use the Gpresult utility from the *Microsoft Windows 2000 Server Resource Kit* to determine which Group Policies were applied to the computer or user.
Determine why a higher-level Group Policy isn't applied	Look for Block Policy Inheritance settings or conflicting settings at an OU closer to the user or computer object than where the higher-level Group Policy is defined. Alternatively, determine if any Group Policy filtering has

	been configured. If the affected computer or user isn't a member of a security group that has the Read and Apply Group Policy permissions assigned, the Group Policy object won't be applied. Look for a Group Policy object with the No Override attribute set at an OU, domain, or site higher in the hierarchy.
Determine why a lower-level Group Policy isn't applied	As an alternative, determine if any Group Policy filtering has been configured. If the affected computer or user isn't a member of a security group that has the Read and Apply Group Policy permissions assigned, the Group Policy object won't be applied.
Determine why a Group Policy doesn't apply to all computers or users within a site, domain, or OU	Inspect the Group Policy object's Security tab to determine which security groups have been assigned the Read Group Policy and Apply Group Policy permissions. To apply Group Policy, you must assign both permissions.

Microsoft Windows 2000 Security Templates

Windows 2000 has made it easier to apply consistent security by introducing security templates. Security templates define security based on seven categories of configuration.

- **Account Policy.** Defines account authentication configuration settings.
  - **Password Policy.** Defines password restrictions. These restrictions include minimum password length, password history maintenance, minimum and maximum password age, password complexity, and the use of reversible encryption for storing passwords.
  - **Account Lockout Policy.** Defines what action is to be taken when a user enters incorrect passwords.
  - **Kerberos Policy.** Defines Kerberos v5 protocol settings. These settings include lifetimes for Ticket Granting Tickets (TGTs), Service Tickets (STs), maximum clock deviance, and the verification of group memberships and account lockout status.
  - **Local Policy.** Defines security settings only for the computer on which the security template is applied. Local computer policies are applied to the local computer account database and are composed of the following three categories:
    - **Audit Policy.** Defines the events that will be audited. The audited events will be stored in the local computer's security log.

- **User Rights Assignment.** Defines which security principals will be assigned user rights on the local computer.
- **Security Options.** Define a wide variety of settings that are configured in the Windows 2000 registry.

- **Event Log.** Defines the properties of the application, security, and system logs.
- **Restricted Groups.** Used to define memberships of security groups. The creator of the security template selects the security groups. Common groups that are included in this policy are Power Users, Enterprise Admins, and Schema Admins. Memberships include which security principals can be members of the restricted group. The policy also defines what other groups the restricted group can be a member of.
- **Systems Services.** Allows you to define restrictions for services installed on a computer. These restrictions include defining whether a service is enabled or disabled and which security principals can start or stop the selected service.
- **Registry.** Allows you to define security for registry keys and their subtrees.
- **File System.** Defines discretionary access control list (DACL) and system access control list (SACL) settings for any folders included within this policy. This policy requires NTFS to be used as the file system where the folders exist.

Applying Windows 2000 Default Security Configuration

If the Computer Is	**Do the Following**
Upgraded from Windows 95 or Windows 98 to Windows 2000 Professional	Ensure that during the upgrade you choose to convert the file system to NTFS. Do nothing else. The Defltwk.inf security template will be applied automatically.
Upgraded from Windows NT 4.0 Workstation to Windows 2000 Professional	Ensure that the file system is converted to NTFS. Apply the Basicwk.inf security template to ensure that default security is applied.
A member server upgraded from Windows NT 4.0 to Windows 2000	Ensure that the file system is converted to NTFS. Apply the Basicsv.inf security template to ensure that default security is applied.
A DC upgraded from Windows NT 4.0 to Windows 2000	Ensure that the file system is converted to NTFS. Apply the Basicdc.inf security template to ensure that default security is applied.
A new install of Windows 2000	Ensure that the system and boot partitions are configured to use NTFS. Do nothing else. The default security templates will be applied automatically and stored in the Setup Security.inf file.

Incremental Security Templates

the default Windows 2000 security configurations provide adequate security for many situations, sometimes additional security configuration is required. To help you define additional security, Microsoft has included several incremental security templates. These incremental templates provide security settings that are best applied in specific scenarios, such as when Terminal Services is deployed on a Windows 2000 Server.

NOTE
The incremental templates are effective only if the default or basic templates have already been applied.

Designing Incremental Security Template Usage

Use This Template	When You Have the Following Security Requirements
No Terminal Services ID	You've deployed Windows 2000 servers with Terminal Services configured to use Application Mode.
	You wish to secure access to Terminal Services and the resources on the terminal server on a per user basis.
	You are deploying Terminal Services as a desktop replacement and want to provide maximum security for all users.
Compatible Workstation	Your budget doesn't allow for an immediate upgrade to a Windows 2000–certified version of the application.
	You don't want to make all users members of the Power Users group.
	You can't identify which individual NTFS files or registry keys require modified permissions.
Optional Components	You've installed additional components to Windows 2000 and want to maintain the highest level of security.
DC Security	You want to ensure that initial DC security is still applied to a DC.
Secure	You're in a mixed environment of Windows 2000 and down-level clients.
	You wish to have the strongest security without excluding down-level clients.
High Security	No down-level clients remain on the network.
	You want to provide the strongest form of security for all data usage.

Extending the Security Configuration Tool Set

Although you can create custom security templates from existing settings, sometimes the settings you require might not be included in the Security Configuration Tool Set (SCTS). For example, you may want to use Group Policy to prevent Windows 2000 client computers from attempting to register the Host (A) and Pointer (PTR) resource records with Domain Name System (DNS) by using dynamic updates. You can extend the SCTS to include the registry entry to prevent dynamic updates for all network adapters.

Task	Solution
Determine what registry values need to be added	Identify registry values that are commonly modified at Windows 2000–based computers for security configuration as part of the installation process. The registry values may be defined in documentation or knowledge base articles.
Identify the properties of the registry value that must be added to the Sceregvl.inf file.	Identify the properties for a specific registry value by reviewing the Regentry.chm compressed help file included with the *Microsoft Windows 2000 Resource Kit*, or by reading knowledge base articles or the software documentation.
Protect the original Sceregvl.inf file	Save a copy of the original Sceregvl.inf file in a secure location before making any modifications.
Register the changes in the Security Templates console	Run **REGSVR32 SCECLI.DLL** at the command prompt. Ensure that the modified Sceregvl.inf file is located in the *systemroot*\inf folder.
Verify the configuration changes	Open the Security Templates console and verify that the new entry appears in the Security Options settings. Also attempt to apply the setting by using the Security Configuration And Analysis console.
Ensure that all required stations see the modified entries	Register the modified Sceregvl.inf file at all Windows 2000–based computers where the security template will be modified.

Analyzing Security Settings with Security Configuration and Analysis

The Security Configuration And Analysis console to analyze a computer's current security settings against a security template. The console indicates whether a Windows 2000–based computer's current security configuration matches the defined configuration in the security template.

To perform the analysis, following steps must be completed:

1. Load the Security Configuration And Analysis console into an MMC console.
2. Create a new database locally for storing the imported security template and the analysis data.
3. Import the desired security template into the security database.
4. Analyze the current security against the security configuration now stored in the security database.
5. Review the analysis information. The Security Configuration And Analysis console displays whether individual security options match (indicated by a green check mark) or don't match (indicated by a red x) the configured settings in the security template.
6. Choose either to rework the security template or to apply the security template to the local security configuration.

Deploying Security Templates in a Workgroup

A workgroup or non-Microsoft network is unable to use Group Policy to provide continued deployment of the security template. The only way to ensure continued application of the security template is to import the security template into local computer policy.

the security template can be applied automatically by saving the security template locally to the computer and using the Secedit command within a batch file to apply the security template. This can be done by using Secedit with the /CONFIGURE parameter:

```
SECEDIT /CONFIGURE [/DB filename] [/CFG filename ] [/OVERWRITE]
     [/LOG logpath] [/VERBOSE] [/QUIET]
```

where

- **/DB *filename*** provides the path to the database file that contains the stored configuration from the desired security template indicated in the /CFG option.
- **/CFG *filename*** provides the path to the security template that's imported into the database for analysis. If this option isn't provided, it's assumed that a security template has already been imported in the indicated database.
- **/OVERWRITE** ensures that any previous security template imported into the security database is overwritten with the information in the indicated security template rather than having the security template information appended to the stored template.
- **/LOG *logpath*** provides the path that's used to log the reports of the analysis.
- **/VERBOSE** indicates that the log file contains more detailed progress information than is regularly recorded.
- **/QUIET** suppresses all log and screen output. This option is useful to prevent the user from realizing the continued application of the security template.

Microsoft Windows 2000 Services Security

DNS Security

DNS provides the ability to resolve host names to IP addresses on a Transmission Control Protocol/Internet Protocol (TCP/IP) network. DNS is the standard resolution service that the Internet uses for addressing and resolving Internet-based resources. Within a Windows 2000 network, DNS provides the locator service for Windows 2000 service through the implementation of Service (SRV) resource records as defined in RFC 2782, as well as standard DNS resource records such as Host (A), Canonical Name (CNAME), Mail Exchanger (MX), and Pointer (PTR) records.

Securing the DNS Service

To	Do the Following
Protect the internal address space	Deploy separate DNS services for the internal and the external network. The external DNS server should never have internal resource records in the zone.
Prevent the failure of a single server from stopping dynamic DNS updates	Design the DNS zones as Active Directory–integrated DNS zones.
Prevent unauthorized DNS servers from hosting your DNS zone data	Configure zone transfers to take place only to authorized servers.
Prevent registration of unauthorized resource records	Use Active Directory–integrated zones. When using a BIND DNS server, restrict by IP address.
Prevent unauthorized membership in the DNS Admins group	Define the membership in the Restricted Groups Group Policy setting to include only authorized members.

DHCP Security

The DHCP Service provides IP address configuration to DHCP clients on the network. These clients depend on the DHCP Service to provide them with correct IP addressing information. If the client were to receive an incorrect IP address from the DHCP Service, the result could be a loss of connectivity on the network—and, in the worst case, provide connectivity to unauthorized servers on the network.

The DHCP Service's security risks can be broken down into three categories:

- The risk of an unauthorized DHCP server assigning incorrect IP addressing information.
- The ability of the DHCP server to overwrite static IP address information in DNS.
- Unauthorized DHCP clients leasing IP addresses on the netwo rk.

Securing the DHCP Service

To	**Include the Following in Your Design**
Prevent unauthorized DHCP servers on the network	Upgrade all computers running DHCP services to Windows 2000. Only authorize the required DHCP servers in Active Directory.
Protect DC-related DNS resource records	Don't install DHCP services on a Windows 2000 DC *and* make the DHCP server a member of the DNSUpdateProxy group.
Ensure that only authorized clients receive DHCP addresses from the DHCP server	Create reservations for all DHCP clients. Ensure that all addresses in the DHCP scope are associated with a MAC address to prevent unauthorized clients from receiving DHCP-assigned IP addresses.
Detect unauthorized non-Windows 2000 DHCP servers	Watch for pockets of misconfigured IP addresses. Use IPCONFIG /ALL at the DHCP client to determine the IP address of the DHCP server that assigned the address.

RIS Security

RIS is a collection of services that work together to allow remote installations of preconfigured Windows 2000 Professiona l desktop computers. The services that comprise RIS include the following,

- **Boot Information Negotiation Layer (BINL).** The BINL service answers DHCP requests from Preboot Execution Environment (PXE) network adapters or clients using a remote installation floppy
- **Trivial File Transfer Protocol Daemon (TFTPD).** The files that initiate the RIS installation are transferred from the RIS server to the client by using Trivial File Transfer Protocol (TFTP).
- **Single Instance Store (SIS).** The SIS allows multiple RIS images to be stored at a RIS server but reduces the duplication of files stored at the RIS server. If a file is duplicated between multiple images, the SIS keeps only a single instance of the file.

Securing RIS Deployments

Task	Solution
Prevent deployment of unauthorized RIS servers	Restrict membership in the Enterprise Admins group because only members of this group can authorize RIS servers.
	Authorize only approved RIS servers.
	Restrict installation of RIS services on existing DHCP servers since they are already authorized in Active Directory.
Restrict RIS-installed computer accounts to a specific OU	Allow only prestaged computer accounts to install RIS images.
	Create the prestaged computer accounts in the desired OU.
	Alternatively, configure a specific location in Active Directory where computer accounts will be created for remote installations.
Restrict who can perform remote installations	Assign only approved users the permission to create computer accounts in the OU where remote installation computer accounts will be created.
	If using prestaged computer accounts, assign only approved users the permissions to modify the attributes of the prestaged computer accounts.
Restrict which images a user can load using remote installation	Change the DACLs on the RIS image's Templates subfolder to only allow authorized security groups READ permissions.
Maintain default security for RIS images	Preconfigure all security settings at the source computer before running the RIPrep utility to create the remote installation image.
Protect administrative permissions during RIS installations	Delegate the permissions to create computer accounts in Active Directory and never use an Administrator account for the remote installation because the TFTP protocol doesn't encrypt network data transmissions.

SNMP Security

SNMP allows a network administrator to proactively manage a network by providing early detection of network faults or incorrect network configuration. Network administrators use SNMP to do the following:

- **Monitor network performance.** SNMP can determine network throughput and determine if data is being transmitted successfully on the network.
- **Detect network faults or unauthorized access.** You can configure SNMP alerts to inform the SNMP management station when specified events take place.
- **Configure network devices.** Use SNMP to configure SNMP agents remotely.
- **Audit network usage.** Use SNMP to determine network usage.

Securing the SNMP Service

Task	**Solution**
Prevent SNMP management stations from modifying configuration by using SNMP SET commands	Configure the communities in which the SNMP agent participates to be Read-Only communities. This configuration prevents the SNMP agent from processing SNMP SET messages.
Prevent unauthorized SNMP management stations from managing SNMP agents	Change the community name from the default name of "Public." Be sure to choose a community name that's difficult to guess.
Track unauthorized management attempts	Configure the SNMP agent to send trap messages for authentication traps and to have the SNMP traps sent to a specific SNMP management station.
Protect SNMP messages from interception	Encrypt SNMP messages by using IPSec. This requires that all SNMP management stations and SNMP agents support IPSec encryption.

Terminal Services Security

Terminal Services allows clients to run Windows 2000 compatible applications on a terminal server without loading Windows 2000 at the client computer. The terminal server hosts all client data processing, application execution, and data storage. The Terminal Services client sends only keyboard input and mouse movement to the terminal server. The terminal server performs all processing and returns only display information to the Terminal Services client.

Securing Terminal Services Access

Task	**Solution**
Limit access to administrators of the network	Configure Terminal Services to run in Remote Administration Mode. You must be a member of the Administrators group to connect with a Terminal Services client.
Restrict access to the local file system	Ensure that all volumes are formatted with NTFS and that permissions have been set to restrict access to the file system.
Prevent users from being	Don't install Terminal Services in Application Server

assigned excess user rights	Mode on a DC, because the user must be granted Log On Locally permissions to use the terminal server.
Determine if a user is connected to the network using Terminal Services	Inspect the user's environment variables for the %clientname% or %sessionname% environment variables. These environment variables only exist within a Terminal Services session.
Restrict access to a single application	Configure Terminal Services to use an alternate shell program. Configure the shell program to be the single application.
Protect data transmissions between the Terminal Services client and the terminal server	Implement either medium or high security for the Terminal Services session.
Restrict access to Terminal Services	Assign only the permission to use Terminal Services to the individual user accounts that require Terminal Services access.

Public Key Infrastructure

A Public Key Infrastructure (PKI) is a combination of technologies, protocols, standards, and services that allows an organization to provide strong authentication and encryption services on the network.

A PKI is comprised of several services and components working together. A PKI's primary components include

- **Certificates.**
- **Certificate templates.**
- **Certificate Revocation List (CRL).**
- **Certification authority (CA).**
- **Certificate management tools.**

Certificate distribution point. Public key–enabled applications and services.
Certificates are fundamental elements of the Microsoft public key infrastructure (PKI).
Certificate enable users to use smart card, logon, send encrypted e-mail, & sign electronic documents.
Certificates are issued managed, renamed, & revoked by certificate authorities.
Certificate is a digital document that attests to the binding of a public key to an entity.
A certificate may consist of a public key signed by a trusted entity.
Most widely used structure and syntax for digital certificate is defined by the International Telecommunication Union (ITU) in ITU-T recommendation X.509.

Creation of a certificate

- Generating a Key pair
- Collecting Required Information
- Requesting the Certificate
- Verifying the information
- Creating the Certificate
- Sending or Posting the Certificate

Certificate Authorities

1) Enterprise Root CA – is the root of an organizations CA hierarchy.
   It requires the followings:
   1) Windows 2000 DNS Service
   2) Windows 2000 Active Directory Service
   3) Administrative Privileges on all servers.
2) Enterprise Subordinate CA - is the subordinate to another CA in the organization hierarchy. Requirement of this type of CA
   1) It must be associated with a CA that will process the subordinate CA's certificate requests.
   2) Windows 2000 DNS service.
   3) Windows 2000 ADS
   4) Administrative Privileges on all servers.
3) Stand alone root CA – is the root of a CA trust hierarchy, it requires administrative privileges on the local server.
4) Stand alone subordinate CA- is a CA that operates as a solitary certificate server or exists in a CA trust hierarchy.
   Requirements are
   1) It must be associated with a CA that will process the subordinate CA's certificate requests.
   2) Administrative privileges on the local server.
   3) Certificate enrollment is the process of obtaining a digital certificate.

Deploying a CA

The certificate services Installation wizard takes the administrator through the installation process.

4) Establishing windows 2000 domains.
5) Active Directory integration
6) Selecting the host server
7) Naming
8) Key generation
9) CA certificate

10) Issuing policy.

Certificate Enrollment

The process of obtaining a digital certificate is called certificate enrollment. There are various enrollment methods like.

1) Web-Based enrollment.
2) Client certificate enrollment.
3) Automated enrollment.

- Within the Microsoft PKI, cryptographic keys & associated certificates are stored and managed by the crypto API subsystem.

Store	Description
MY	This store is used to hold a user's or computer's certificates, for which the associated private key is available
CA	This store is used to hold issuing or intermediate CA certificates to use in building certificate verification chains.
TRUST	This store is used to hold certificate trust lists. This is an alternate mechanism for allowing an administrator to specify a collection of trusted CA's. An advantage is that they are digitally signed and may be transmitted over no secure links.
ROOT	This store holds only self-signed CA certificates for trusted root CA's
UserDS	This store provides a logical view of a certificate repository stored in the Active Directory(for example, in the user Certificate property of the user object) .Its purpose is to simplify access to these external repositories

Authenticity and Integrity of Transmitted Data

Windows 2000 network has two distinct methods for providing authenticity and integrity of transmitted data at the application layer.

Server message block (SMB)

SMB signing can help ensure that file transmissions between a client and a server aren't modified in transit.

The key used to create the digests is created using the Message Digest v5 (MD5) algorithm. The MD5 message digest algorithm breaks the data into 512-bit blocks and produces a 128-bit message digest for each 512-bit block of the data. The key is computed from the session key established between the client and the server and the initial response sent by the client to the server's challenge.

SMB signing is commonly implemented in high-security networks to prevent impersonation of clients and servers. SMB signing authenticates the user and the server hosting the data. If either side fails the authentication, data transmission won't take place.

Digital Signing

Digital signatures differ from SMB signing in that a Public Key Infrastructure (PKI) is required to deploy the necessary public/private key pairs to participating clients. Once a participating client has acquired a private/public key pair, the client can implement digital signatures to protect e-mail messages.

Digital signatures function by applying a digest function to the contents of the message. The digest function creates a message digest as output. The message digest is a representation of the message. If the contents of the message are modified, the message digest output will also change. Both the sender and receiver of the message will run the same digest function against the e-mail message. The recipient's e-mail application will compare the two digests to determine if the contents have been modified. If the digests match, the contents haven't been modified.

Two protocols currently provide digital signatures for e-mail applications:

- **Secure Multipurpose Internet Mail Extensions (S/MIME).** An S/MIME extension provides the ability to encrypt and digitally sign e-mail messages by using public and private key pairs. The biggest benefit of implementing S/MIME is that S/MIME is an Internet Engineering Task Force (IETF) standard designed to extend the MIME standard to provide secure e-mail functions.

- **Pretty Good Privacy (PGP).** PGP is also a protocol that provides the ability to encrypt and digitally sign e-mail messages. As with S/MIME, PGP provides this ability by using private/public key pairs. The main difference with PGP is that PGP isn't controlled by a centralized standard organization.

Encryption of Transmitted Data

Although digital signing protects e-mail messages from modification, it doesn't prevent someone from inspecting them during transmission across the network. The default protocol used for sending e-mail messages is Simple Mail Transfer Protocol (SMTP). SMTP doesn't include any extensions for the encryption of email.

E-mail messages can be encrypted by using different algorithms. Supported algorithms in Microsoft Outlook 2000 include

- **Rivest's Cipher v2 (RC2).** RC2 is a secret-key block encryption algorithm developed by Ron Rivest at RSA Security that uses 64-bit input and output blocks. The key size can be varied up to 128 bits in length with most implementations using 40-bit or 128-bit length keys. RC2 is optimized for speed and encrypts messages faster than DES or 3DES on slower computers.
- **Data Encryption Standard (DES).** DES is the most widely used encryption algorithm in the world. DES takes 64-bit blocks of plaintext and applies a 56-bit key to each block of plaintext. This key is the recipient's public key. The encrypted package is decrypted using the recipient's private key.
- **Triple DES (3DES).** 3DES increases the strength of DES by using an encrypt-decrypt-encrypt process that uses three keys. The 64-bit plaintext message block is first encrypted with the first key. Then the encrypted result is decrypted using a second key. Finally, the result of the decryption process is encrypted using a third key. The formula to arrive at the encrypted packet is $E_{k3}[D_{k2}[E_{k1}[\text{Plaintext}]]]$ where E_{k3}, E_{k2}, and E_{k1} are the three separate encryption keys. The resulting encryption strength is 168 bits (3 × 56-bits).

Application-Level Encryption with SSL/TLS

Applications other than e-mail, such as Web pages containing sensitive data, also require encryption of data when it's transmitted. For example, Windows 2000 supports two forms of application-level encryption: SSL and Transport Layer Security (TLS).

SSL. Provides encryption services to several applications by using public and private keys to encrypt data transmitted between a server and a client. While most commonly associated with Web browsers, SSL is also used to provide encryption services to Lightweight Directory Access Protocol (LDAP) queries, Network News Transfer

Protocol (NNTP) authentication and news group transfers, Post Office Protocol v3 (POP3) authentication and e-mail retrieval encryption, and Internet Message Access Protocol v4 (IMAP4) authentication and e-mail retrieval encryption. As with secured Web browsing, the applications must support the use of SSL encryption.

TLS. TLS is very similar to SSL in that it provides communications privacy, authentication, and message integrity by using a combination of public key and symmetric encryption. TLS uses different encryption algorithms than SSL. TLS is an IETF draft standard. Windows 2000 uses TLS to encrypt smart card authentication information transmitted when using Extended Authentication Protocol (EAP).

Standard and SSL Ports

Protocol	Standard Port	SSL Port
Hypertext Transfer Protocol (HTTP)	80	443
Internet Message Access Protocol v4 (IMAP4)	143	993
Lightweight Directory Access Protocol (LDAP)	389	636
Network News Transfer Protocol (NNTP)	119	563
Post Office Protocol v3 (POP3)	110	995
Simple Mail Transfer Protocol (SMTP)	25	465

Securing Data with Internet Protocol Security (IPSec)

IPSec Policies

IPSec implements encryption and authenticity at a lower level in the Transmission Control Protocol/Internet Protocol (TCP/IP) stack than application-layer protocols such as Secure Socket Layer (SSL) and Transport Layer Security (TLS). Because the protection process takes place lower in the TCP/IP stack, IPSec protection is transparent to applications. The applications require only a recognized port to be protected by IPSec.

IPSec provides two protocols for protection of transmitted data,

Authentication Headers (AH) - AH provides authentication and integrity services to transmitted data

Encapsulating Security Payloads (ESP) - ESP provides encryption services.

Preconfigured IPSec Policies

Windows 2000 includes three default IPSec policies

- **Secure Server (Require Security).** This policy secures all network traffic to or from the computer that the IPSec policy is applied to, with the exception of

Internet Control Message Protocol (ICMP), better known as Packet InterNet Groper (PING) traffic. This policy rejects any connection attempts by non-IPSec aware clients.

- **Server (Request Security).** This policy differs from the Secure Server IPSec policy in that it only requests that IPSec security be applied. If the connecting client is non-IPSec aware, the Server (Request Security) policy allows unsecured communications to take place.
- **Client (Respond Only).** This policy doesn't enable IPSec for specific protocols, but it allows the affected computer to negotiate an IPSec SA with any servers that request or require IPSec protection. When you apply this IPSec policy, the client computer will never initiate IPSec protection but will participate in IPSec SAs when requested to do so by another computer.

Troubleshooting IPSec Problems

Sometimes an IPSec design doesn't work as expected. When this occurs, several tools can be used to determine why an IPSec SA isn't being established. These tools include

- **Ping.** Use Ping to ensure that the SA is being correctly established between two computers. Ping uses the Internet Control Message Protocol (ICMP),
- **IPSec Monitor.** The IPSec Monitor (Ipsecmon.exe) shows any currently active IPSec SAs that are established with your computer and the current IPSec statistics for your computer,
- **Netdiag.** The Netdiag utility, included in the Windows 2000 Support Tools, allows you to verify the current SAs active on your computer. By using the /debug option, you can verify the actual IPSec policy applied, the filter that was applied, and the authentication protocol used. The command used to show the information is NETDIAG /TEST:IPSEC /DEBUG.
- **System Management Server (SMS) Network Monitor.** The SMS Network Monitor allows you to inspect data packets as they're transmitted across the network. You can use the Network Monitor to determine if the IKE negotiation takes place (look for ISAKMP packets) and whether the negotiation succeeded (look for AH or ESP packets). You can't use the Network Monitor to inspect the contents of an ESP packet because the contents are encrypted.
- **Oakley logs.** As a last resort, you can enable Oakley logs to look at detailed debugging of an IPSec connection. Oakley logs provide detailed reporting on the ISAKMP negotiation process, and a security technician can use them to identify incorrect configuration information.

Remote Access Security

Windows 2000 offers two methods for remote users to connect to the local network:

Dial-up remote access, where the user connects to the network by using a modem.

VPN, where the user connects through a tunnel that's running over an existing network connection.

Remote Access Authentication

Windows 2000 RRAS supports the following authentication methods:

- **Password Authentication Protocol (PAP).** PAP offers the most flexibility among the authentication protocols because it's supported by almost all dial-up network services. The danger is that PAP sends the user password as a plaintext string
- **Shiva Password Authentication Protocol (SPAP).** SPAP uses a reversible encryption method supported by Shiva remote access servers and Windows 2000 remote access servers. The encryption algorithms are stronger than those used in PAP, but SPAP doesn't provide protection against server impersonation.
- **Challenge Handshake Authentication Protocol (CHAP).** CHAP sends the password and a challenge from the server through a hashing algorithm. The recipient identifies the user, obtains the password from the directory, and performs the same hashing algorithm against the challenge and password. If the results match, the user is authenticated.

- **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).** MS-CHAP increases security by dropping the requirement to store the user's password in a plaintext format at the domain controller. MS-CHAP creates the challenge response by passing the challenge and the user's password through the Message Digest v4 (MD4) hashing algorithm rather than the MD5 algorithm. Because the algorithm is well known, MS-CHAP is also vulnerable to dictionary attacks if short passwords or passwords that are found in a dictionary are used. MS-CHAP uses Microsoft Point-to-Point Encryption (MPPE) Protocol to encrypt all data transmitted between the remote access client and the Network Access Server (NAS).
- **Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2).** MS-CHAPv2 improves security by supporting mutual authentication, stronger data encryption keys, and separate encryption keys for sending and receiving data.
- **Extensible Authentication Protocol (EAP).** EAP provides extensions to dial-up and VPN connections. These extensions provide two-factor authentication by using devices such as smart cards to provide network credentials. EAP uses Transport Layer Security (TLS) to secure the authentication process. EAP

requires that both the remote access client and the NAS run Windows 2000 and that a Public Key Infrastructure (PKI) is deployed to provide certificates for both the NAS and the remote access clients.

Securing an Extranet

A firewall is placed between the private and public networks to secure the private network from the public network.

A firewall acts as a barrier against attacks launched from the public network. A firewall can be a physical hardware device or a software application that executes on a computer.

To protect the private network, firewalls can offer a suite of services, including

- **Network Address Translation (NAT).** Translation of the source address of all outbound packets from a private network address to a public network address.
- **Packet filtering.** Configuration of rules at a firewall that define which protocols are allowed to pass through the firewall.
- **Static address mapping.** Configuration of how incoming packets are rerouted to servers using private network addressing.
- **Stateful inspection of network traffic.** Verification that protocols are following basic rules of communications. Stateful inspection ensures that sessions aren't hijacked by an attacker.
- **Advanced features that detect common attacks against the private network.** These include setting time-outs for incomplete session establishment and inspecting the content of incoming packets.

Securing a Web Server

1. Track all access to the Web server - Implement auditing at the Web server and ensure that the logs are stored in a format that facilitates inspection of the log files.

2. Provide the strongest security to Web-accessible data - Separate the data by content type and apply the most restrictive permissions that still allow functionality.

3. Prevent an attacker from accessing unauthorized areas of the disk subsystem - Disable the use of parent paths in the Web site's property pages.

4. Prevent port scans against common attacked ports - Apply an IPSec block policy to commonly attacked ports that shouldn't be available on the Web server. This prevents a port scanner from detecting the status of the port. Remove all unnecessary services from the Web server to eliminate ports from inspection.

5. Detect hacking attempts - Deploy intrusion detection software to detect hacking attempts. Be aware that some normal traffic patterns may appear as hacking attempts.

6. Prevent a successful attack against the Web server from compromising other data stored on the network - Don't make the Web server a member of the private network forest. Don't store confidential documents on the disk subsystem of the Web server.

7. Ensure that the latest security fixes are applied to the Web server - Ensure that the latest service packs and hot fixes are applied to the Web server. Periodically connect to the Windows Update Web site *(windowsupdate.microsoft.com/.*

8. Limit the effect of a successful hacking attempt - Configure the Web server to participate in an NLBS cluster. If one node is brought down, all incoming traffic will be redirected to the remaining servers in the cluster.

9. Apply the recommended security configuration for your Web server - Use the IIS 5.0 security checklist tool.

Protecting Internet-Accessible Resources

1. FTP services - Change NTFS permissions to match the allowed transactions. For example, if only FTP downloads are allowed, configure permissions to allow only the anonymous FTP account Read permissions.
2. To prevent password interception - allow only anonymous connections.
3. Telnet services - Create a local security group named TelnetClients to restrict Telnet access to authorized users.

4. DNS services - If using the same namespace internally and externally, ensure that the external DNS server doesn't contain private network IP addressing. Restrict zone transfers at the external DNS server to only approved DNS servers to prevent an attacker from retrieving the entire zone data file.

5. All services - If allowing only specific protocol connections, block all other protocols with an IPSec block action. This will prevent any other ports from responding to port scans or access attempts. If you require private network access to the restricted ports on a server in the DMZ, change the IPSec action to negotiate so that private network client computers can establish an IPSec SA with the server in the DMZ.

6. Interaction between servers - Configure servers in the DMZ to use IPSec transport mode for data transmitted between the servers. IPSec transport mode encrypts all data exchanged between the servers and prevents unauthorized connections to the server. IPSec transport mode can pass through a firewall as long as NAT isn't performed against the data.

Securing Access to the Internet by Private Network Users

Reduce the risk of viruses - Deploy virus scanning software at each client computer to detect locally introduced viruses. Ensure that virus signatures are regularly updated at all deployed locations.

Prevent the installation of unauthorized software - Restrict installation to signed software when installing from the Internet. Configure Internet Explorer security settings to restrict what content can be installed. Don't include users in Power Users or local Administrators group. This will restrict user access to specific areas of the local disk system where they can install software.

Prevent Internet users from revealing the private network addressing scheme - Deploy a NAT service at a firewall between the private network and the public network so that all source IP address information is replaced with a common browsing IP address configured at the firewall. Have all internal client computers access the Internet by connecting to the Proxy Server. All requests will appear as if they were requested by the Proxy Server.

Prevent users from bypassing network security when accessing the Internet - Don't deploy modems to the desktop unless required for another application. Use Group Policy to disable the Remote Access Connection Manager and thereby prevent dial-up sessions. Configure the firewall to allow only authorized computers to connect directly to the Internet.

Providing Interoperability Between Windows 2000 and Heterogeneous Networks

AppleTalk Network Integration Services

You can use AppleTalk Network Integration Services to allow Macintosh client computers to securely access resources in a Windows 2000 network. The services that provide this functionality are included with Windows 2000 and are named File Services for Macintosh and Print Services for Macintosh.

Microsoft Services for NetWare 5.0

Microsoft Services for NetWare 5.0 is an add-on product that allows integration of Windows 2000 and Novell NetWare networks through the following utilities:

- **Microsoft Directory Synchronization Services (MSDSS).** Allows two-way synchronization between Active Directory and Novell Directory Services (NDS). This synchronization allows users to maintain the same password in the two directory services.
- **Microsoft File Migration Utility.** Allows the migration of files from NetWare file resources to a Windows 2000 server. The File Migration Utility translates the NetWare trustee rights to NTFS permissions during the migration process.
- **File and Print Services for NetWare (FPNW).** Enables computers running Windows 2000 to emulate a NetWare 3.*x* server and provide file and print services to NetWare clients.

Microsoft Services for UNIX 2.0

Microsoft Services for UNIX version 2.0 is an add-on product that allows the integration of Windows 2000 and UNIX clients in a single network. Services for UNIX 2.0 includes the following components.

- **NFS software.** Includes an NFS client, NFS server, and NFS gateway.The NFS client allows Microsoft clients to connect to UNIX NFS servers. The NFS server allows UNIX NFS clients to connect to a Windows 2000 server for file access using the NFS protocol. The NFS gateway allows a Windows 2000 server to publish UNIX NFS data as a Windows 2000 share so that Microsoft clients can connect to NFS resources without installing NFS client software.
- **Telnet services.** Includes a Telnet server that allows up to 64 connections and a Telnet client for connecting to Telnet services on a UNIX computer.
- **Management tools.** Includes the Services for UNIX MMC console for managing various services for UNIX utilities and the ActivePerl script engine. ActivePerl allows UNIX scripts to take advantage of the Windows Management Instrumentation (WMI) and automate routine network administration tasks.
- **Network Information Services (NIS).** Includes the NIS to Active Directory Migration Wizard and the Server for NIS. The migration wizard allows the import of UNIX NIS source files into Active Directory to provide a single directory service. Server for NIS allows a Windows 2000 domain controller (DC) to act as a primary server for NIS.
- **Two-Way Password Synchronization.** Provides the ability to synchronize passwords between Active Directory and UNIX systems.
- **User Name Mapping.** Allows Windows 2000 account names to be mapped to UNIX User Identifiers (UIDs) so that a user connecting to an NFS resource doesn't have to provide alternate credentials for the UNIX system.

Securing Macintosh User Authentication

Allow unauthenticated access to Macintosh users - Enable the Guest account at the server hosting File Services for Macintosh. Enable Guest access for the Macintosh-accessible volume. Have Macintosh users connect to the volume as a guest.

Allow all Macintosh clients to connect to the Windows 2000 server - Enable File Server for Macintosh to access Apple Clear Text authentication or enable Apple Clear Text or Microsoft authentication.

Require encrypted authentication - Configure all user accounts for Macintosh users to store passwords in reversible encrypted format. Configure File Server for Macintosh properties to require Apple Encrypted authentication or Microsoft authentication.

Restrict supported authentication methods - Configure File Server for Macintosh properties to accept only authentication requests using authorized methods.

Limit access to a volume - Create a volume password that must be provided in addition to user credentials to gain access to a volume.

Securing NetWare User Authentication

Allow NetWare clients to authenticate with a Windows 2000 Server - Install FPNW on a Windows 2000 server. Enable each required user account to maintain NetWare compatible login Install the IPX/SPX Compatible transport on the Windows 2000 server running FPNW.

Limit the number of simultaneous connections by a single user account - Limit the number of concurrent connections in the NW Compatible tab of the Properties dialog box of a user account.

Allow authentication by Windows for Workgroups 3.11, Windows 95, Windows 98, or Windows NT client computers - Windows for Workgroups 3.11, Windows 95, Windows 98, and Windows NT clients allow the installation of multiple network clients. Rather than install FPNW, consider deploying the Microsoft and NetWare clients to all client computers.

Securely Synchronizing Multiple Directories

Microsoft Metadirectory Services (MMS) 2.2 allows integration of identity information from multiple directory services. By using MMS, you ensure that the organization has a single authoritative directory store that collects all of its information from multiple existing directories.

MMS establishes a single directory by deploying a *metadirectory*. A metadirectory is a service that collects directory information from multiple directories.

Securing Windows 2000 Resource Access for Macintosh Clients

Allow Macintosh clients to access NTFS volumes - Install File Services for Macintosh on any servers to which Macintosh clients require access. Ensure that all Macintosh clients are running System 6.0.7 or later as their operating system. Define Mac-accessible volumes in the Computer Management console.

Ensure the highest level of security for Macintosh users - Deploy the MS-UAM to all Macintosh clients to enable 14-character encrypted passwords.

Restrict access to Mac-accessible volumes to authorized users - Disable guest access to the Mac-accessible volume. Configure a volume password and distribute the password only to authorized users. Define NTFS permissions on files and folders in the Mac-accessible volume to restrict access for Macintosh users.

Securing Windows 2000 Resource Access for NetWare Clients

Allow NetWare clients to access NTFS volumes - Install File and Print Services for NetWare on any servers to which NetWare clients require access Ensure that all NetWare clients have the FPNW server configured as their preferred server. Define NetWare volumes in the Computer Management console.

Restrict which user accounts can access NetWare volumes stored on a Windows 2000–based server - Define authorized accounts to be only NetWare-enabled user accounts. Configure volume and NTFS permissions to restrict access to authorized user accounts.

Restrict access to printer resources - Assign Windows 2000 print permissions to groups consisting of NetWare-enabled accounts.

Securing UNIX Client Access to Windows 2000 Resources

Provide NFS access to file resources by UNIX clients - Install Services for UNIX 2.0 on the Windows 2000 Server providing UNIX client access. Configure Server for NFS to provide access to UNIX NFS clients. Configure User Name Mappings to associate UNIX UIDs and GIDs to Active Directory user and group accounts.

Provide SMB access to file resources by UNIX clients - Install Samba client software on all UNIX clients requiring SMB access to a Windows 2000–based server.

Secure WinSock application access to Windows 2000 resources - Enable SSL or IPSec encryption of all data transmitted between the client and the server.

Secure all file resources access by UNIX clients - Store all data accessible by UNIX clients on NTFS partitions. Configure NTFS permissions to restrict access to only authorized users. Ensure that the user accounts assigned to UNIX users are included in groups assigned access to the resources.

Allow UNIX clients to print to Windows 2000 printers - Install Microsoft Print Services for UNIX to allow LPR connections to Windows 2000 printers. Configure the LPD service to start automatically.

Designing Access to NetWare Resources

Client Services for NetWare - User-level security is required in the NetWare environment. CSNW requires that each user has an account in the NetWare environment your network allows protocols other than TCP/IP to be installed at client computers.

Novell Client v4.8 for Windows NT/2000 - All connectivity with the NetWare environment requires TCP/IP protocols. Administration of the Novell environment must take place from the Windows 2000 Professional based computer Synchronization of passwords between Active Directory and NDS using MSDSS is required

Gateway Services for NetWare - Users must have only a single account in the enterprise network. Instead of the user having two accounts, one in Active Directory and one in NDS, the gateway account will be used to access NetWare resources. Both Windows 2000 and NetWare administrators will manage security for NetWare resources. Limit deployment of the IPX/SPX protocol in the Microsoft network

Designing Access to UNIX NFS Resources

Client for NFS-User-level security in the UNIX environment preventing the gateway from becoming a bottleneck and limiting access to the NFS server all security management of the NFS data to be performed at the UNIX server.

Gateway for NFS - No need to differentiate between user accounts when accessing the NFS share. The security for NFS resources has to be managed by both Windows 2000 and UNIX administrators.