IBM GLOBAL SERVICES

# Session 024

## Securing Windows Server 2003 and Windows 2000 Server

Andrew Page, Infrastructure Architect

Microsoft Technology Center – Chicago

IBM eserver xSeries
Technical Conference

Aug. 9 - 13, 2004

Chicago, IL



RETURN TO INDEX

# Session Prerequisites

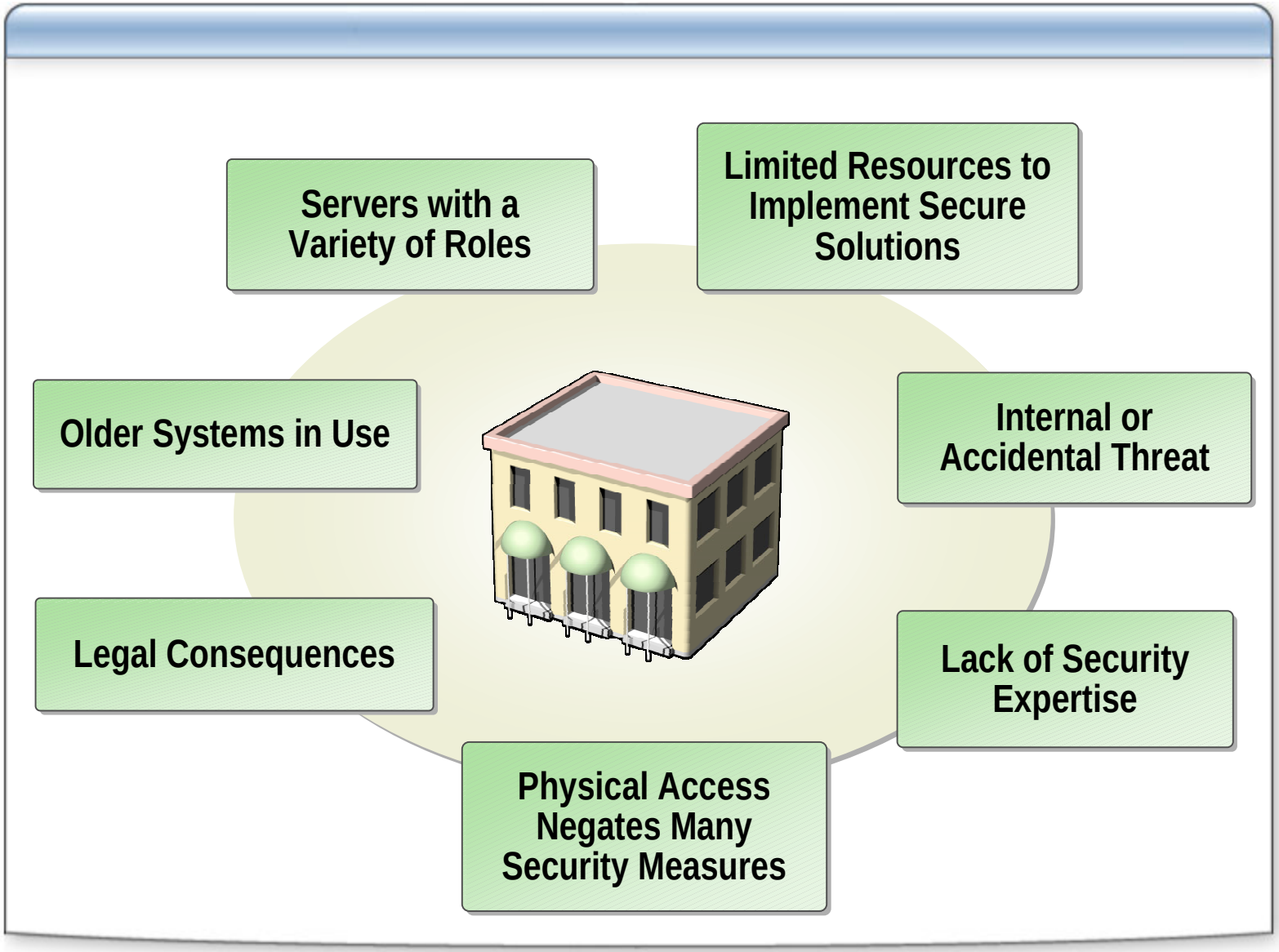
- Hands-on experience with Windows 2000 Server or Windows Server 2003
- Experience with Windows management tools
- Knowledge of Active Directory and Group Policy concepts

**Level 200**

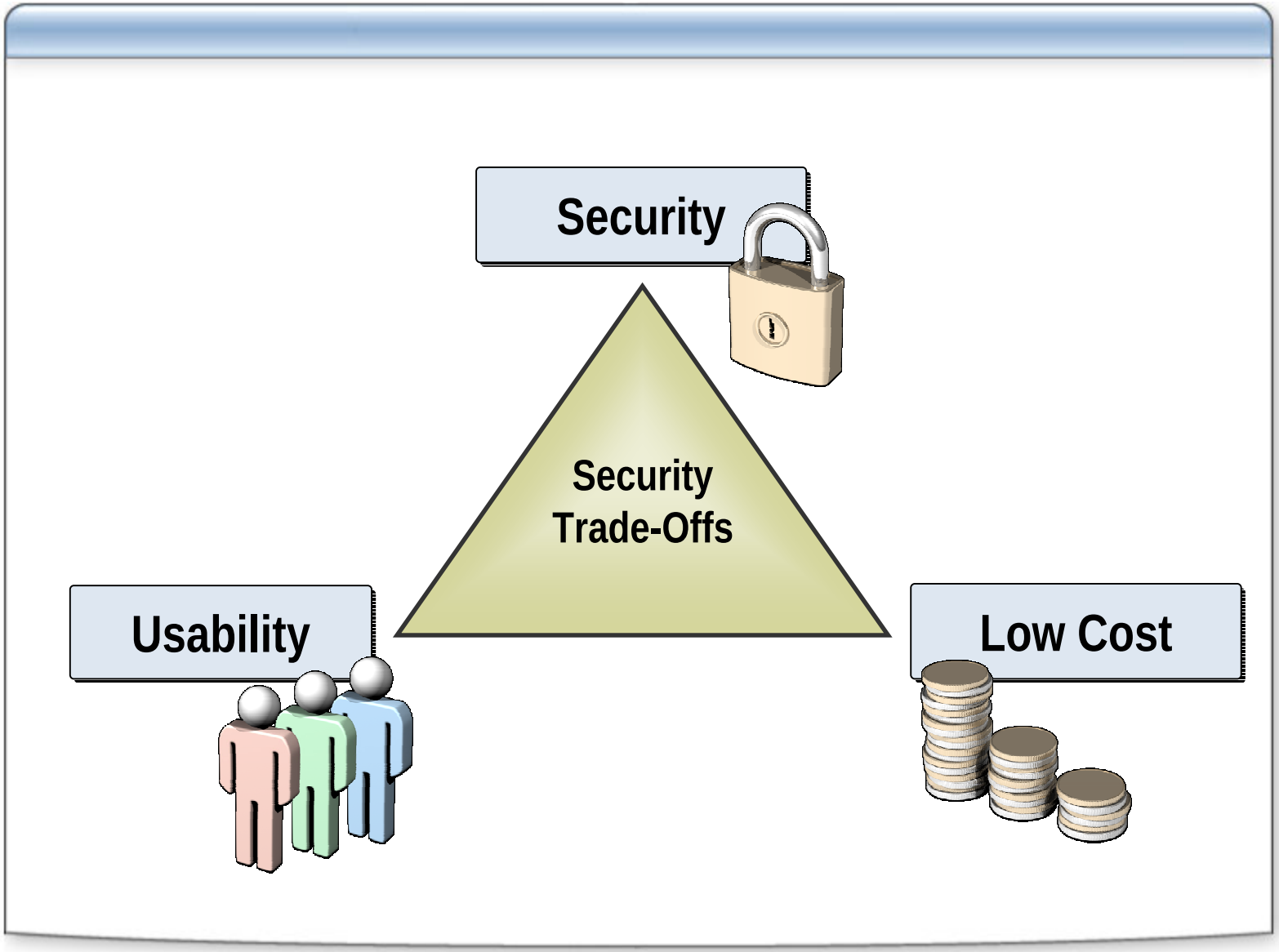
# Introduction to Securing Servers

- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Security Challenges for Small and Medium-Sized Businesses



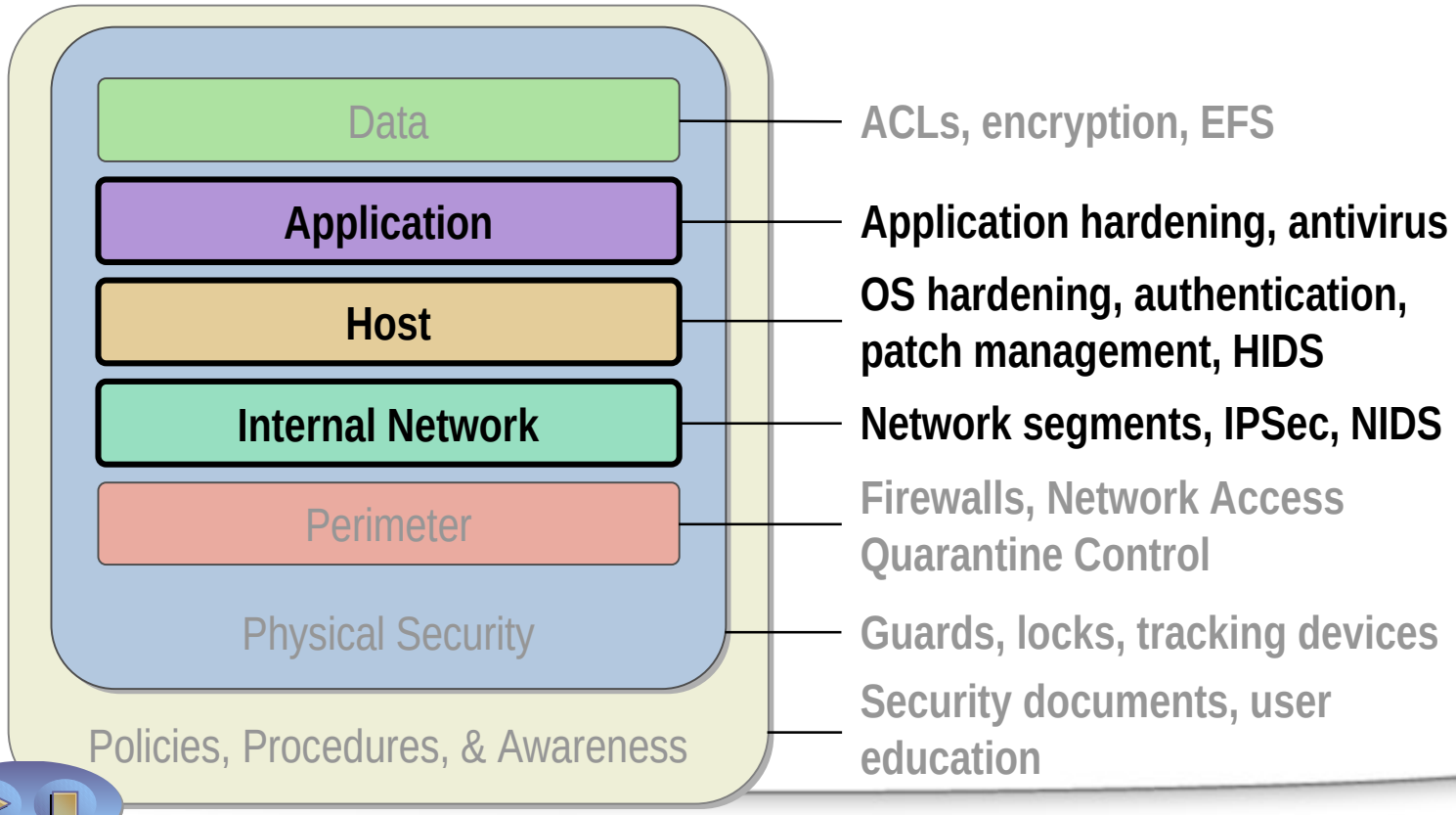
# Fundamental Security Trade-Offs



# Defense in Depth

## Using a layered approach

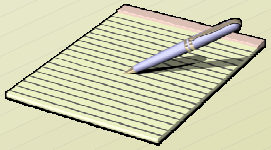
- Increases an attacker's risk of detection
- Reduces an attacker's chance of success

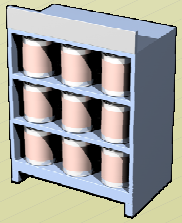


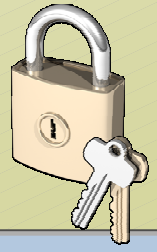
# Threat Modeling

Threat modeling is a risk assessment and mitigation practice that includes:

- Documenting the environment and configurations
- Compartmentalizing systems by application and security requirements
- Restricting the environment and granting privileges only to those that require them





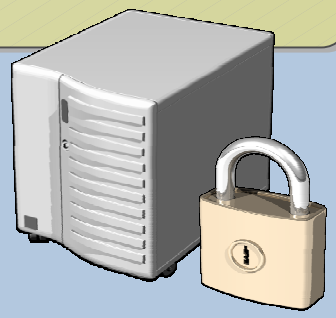


# Core Server Security

- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Core Server Security Practices

- Apply the latest service pack and all available security patches
- Use Group Policy to harden servers
- Restrict physical and network access to servers



# Managing Software Updates

**Implement an appropriate patch management solution to manage software updates**

| Customer type | Scenario | Customer chooses |
|---|---|---|
| **Small business** | Has one to three Windows 2000 or newer servers and one IT administrator | **Windows Update Services** |
| **Medium or large enterprise** | Wants a patch management solution with basic level of control that updates Windows 2000 and newer versions of Windows | **Windows Update Services** |
| | Wants a single flexible patch management solution with extended level of control to patch, update, and distribute all software | **SMS** |

# Recommendations for Hardening Servers

- Rename the built-in Administrator and Guest accounts
- Restrict access for built-in and non-operating-system service accounts
- Do not configure a service to log on using a domain account
- Use NTFS permissions to secure files and folders

# Active Directory Security

- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Active Directory Components

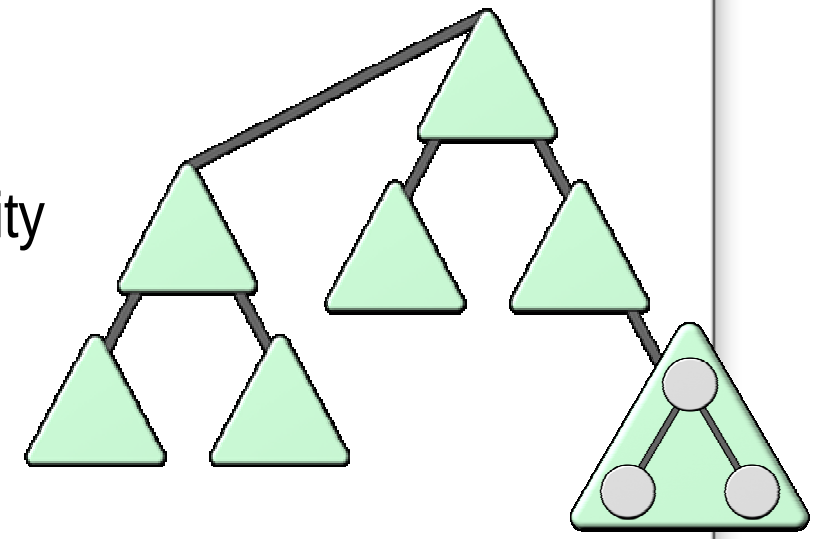
- **Group Policy**

  Group Policy is a key tool for implementing and managing network security

- **Forest**

  A forest functions as a security boundary in Active Directory

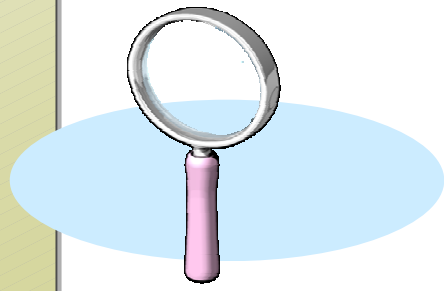
- **Domain**
- **Organizational Unit (OU)**

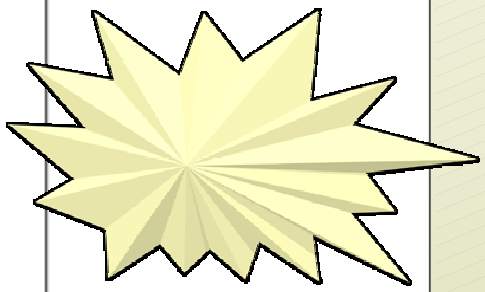


# Planning Active Directory Security

**Analyze the environment:**

- Intranet data center
- Branch office
- Extranet data center





**Perform threat analysis:**

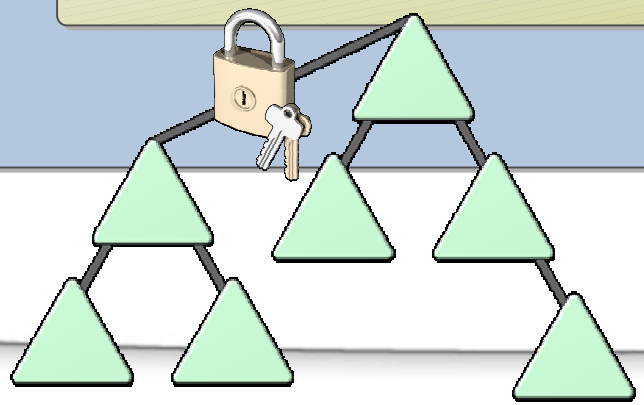
- Identify threats to Active Directory
- Determine security measures for identified threats
- Establish contingency plans

# Establishing Active Directory Security Boundaries

Specify security and administrative boundaries based on need for delegation of administration

Design an Active Directory structure based on delegation requirements

Implement security boundaries based on the *Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations*



# How to Create a Forest Trust with Selective Authentication

1. Start Active Directory Domains and Trusts
2. Create a one-way or a two-way forest trust
3. Open the Properties box for the trust relationship
4. On the Authentication tab, enable Selective authentication for the trust

# How to Configure Selective Authentication for a Server

1. Start Active Directory Users and Computers
2. Open the Properties box for the server you want to configure
3. On the Security tab, add users or groups and assign them the Allowed to Authenticate permission to the server

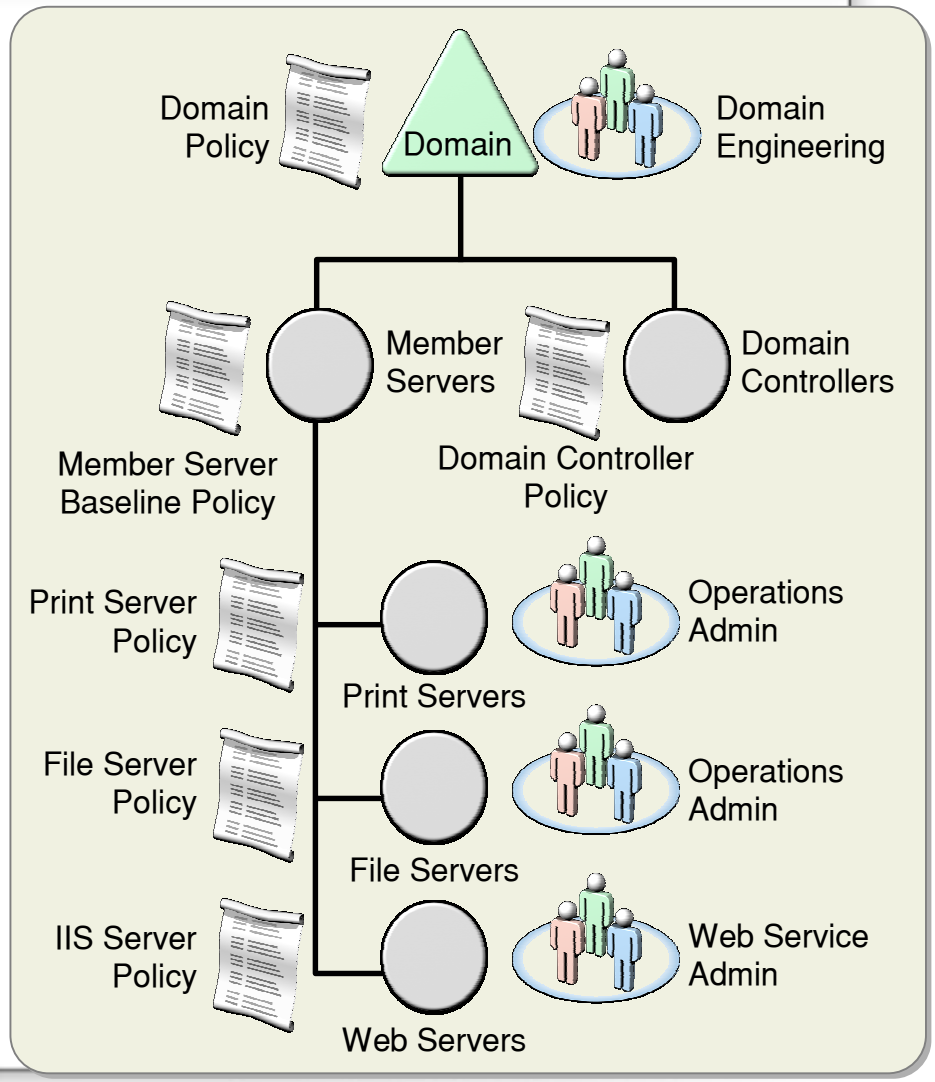
# Strengthening Domain Policy Settings

- Strengthen the settings for the Domain by creating and linking a new GPO at the domain level
- Ensure that password and account policies meet your organization's security requirements
- Analyze threats and update security policy to reflect and counter those threats

# Establishing a Role-Based OU Hierarchy

**An OU hierarchy based on server roles:**

- Simplifies security management issues
- Applies security policy settings to servers and other objects in each OU

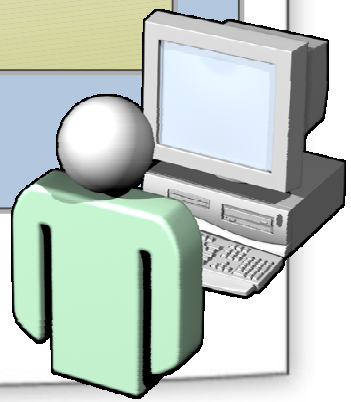


# How to Create an OU Hierarchy for Managing and Securing Servers

1. Create an OU named Member Servers
2. Create OUs within the Member Servers OU for each server role
3. Move each server object into the appropriate OU according to role
4. Delegate control of each role-based OU to the appropriate security group

# Administrative Best Practices

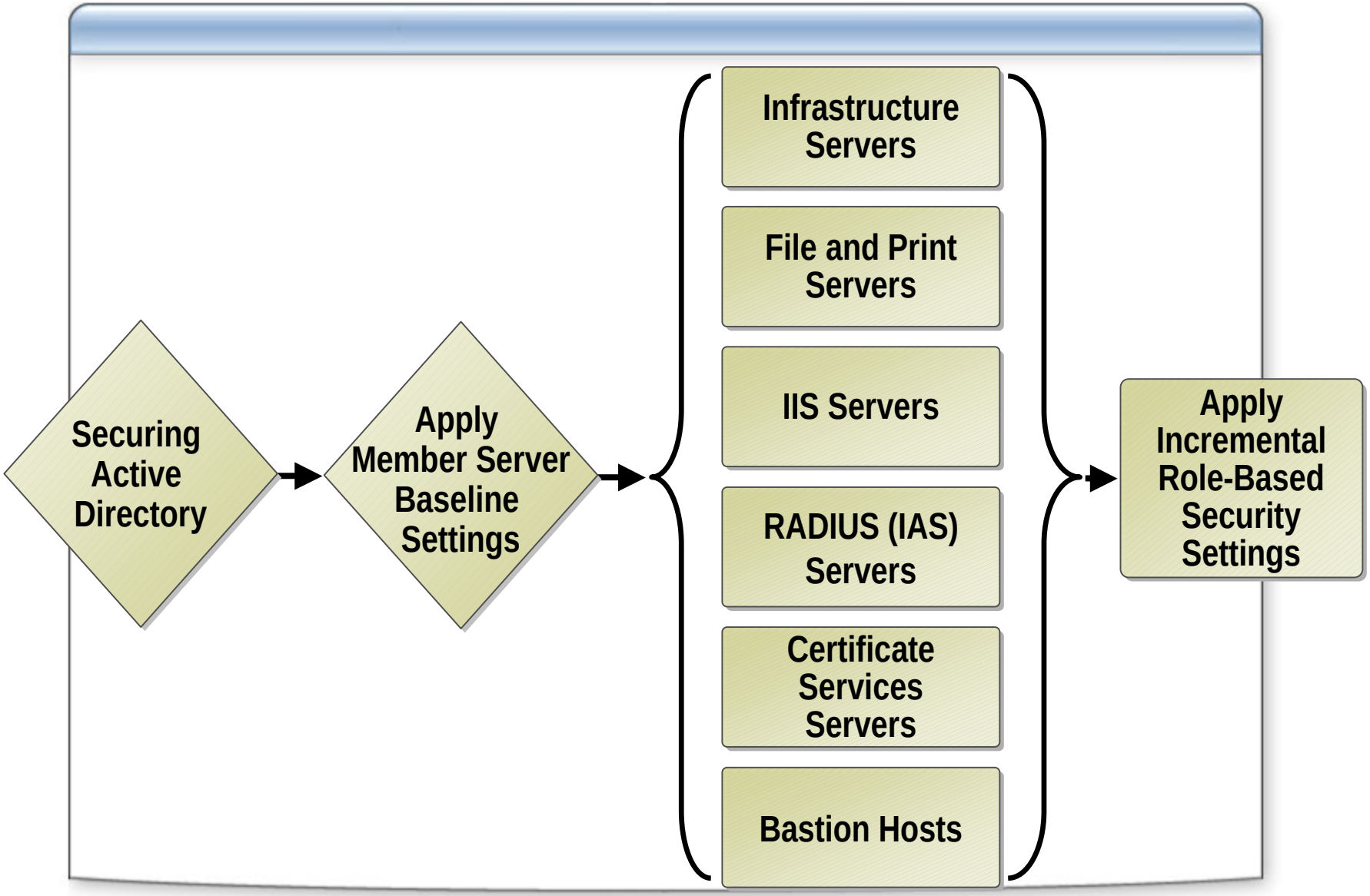
- Distinguish between service and data administrative roles
- Take steps to secure administrative accounts
- Delegate the minimum permissions required



# Hardening Member Servers

- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Server Hardening Overview

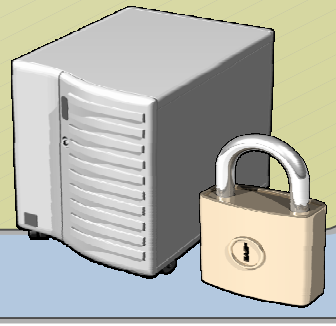


# Member Server Baseline Security Template

Modify and apply the Member Server Baseline security template to all member servers

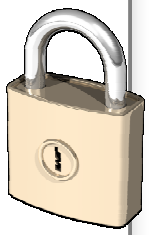
Settings in the Member Server Baseline security template:

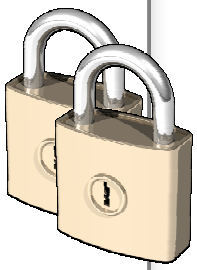
- Audit Policy
- User Rights Assignment
- Security Options
- Event Log
- System Services

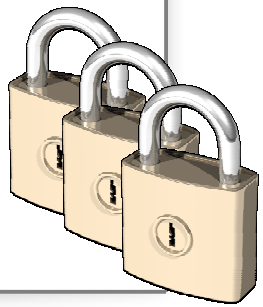


# Security Template Types

| Template type | Security level/Environment |
|---|---|
| **Legacy Client** | • Provides adequate security<br>• Used where Active Directory is used with Windows 98 clients or with Windows NT 4.0 clients and member servers |
| **Enterprise Client** | • Provides solid security<br>• Used where Active Directory is used with Windows 2000 or higher clients and servers |
| **High Security** | • Provides very strong security<br>• Used only where security is the preeminent concern, and Active Directory is used with Windows 2000 or higher clients and servers |







# How to Apply a Security Template

1. Open Group Policy Management, and then navigate to the OU to which you want to apply the security template
2. Create a new GPO and link it to the OU
3. Navigate to Computer Configuration\Windows Settings\Security Settings
4. Right-click Security Settings, and then click Import Policy
5. Select the security template, and then click OK

# Best Practices for Using Security Templates

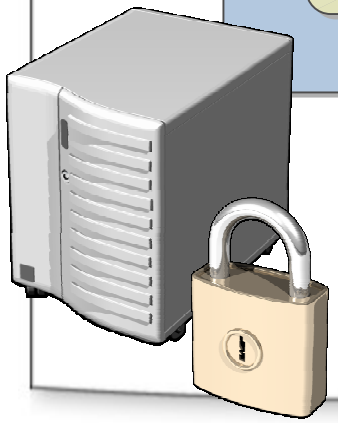
- Review and modify security templates before using them
- Use Security Configuration and Analysis tool to review template settings before applying them
- Test templates thoroughly before deploying them
- Store security templates in a secure location

# Hardening Domain Controllers

- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Configuring Security for Domain Controllers

- Secure the domain controller build environment
- Establish domain controller build practices that provide security
- Maintain physical security



# How to Prevent the Storage of LM Hashes in Active Directory

1. Open Group Policy Management, and then navigate to the Domain Controllers OU
2. Create a GPO, link it to the Domain Controllers OU, and then open the GPO for editing
3. Navigate to Computer Configuration\Windows Settings\Security Settings\Local Policies, and then click Security Options
4. In the list of available policies, double-click Network security: Do not store LAN Manager hash value on next password change
5. Click Enabled, and then click OK

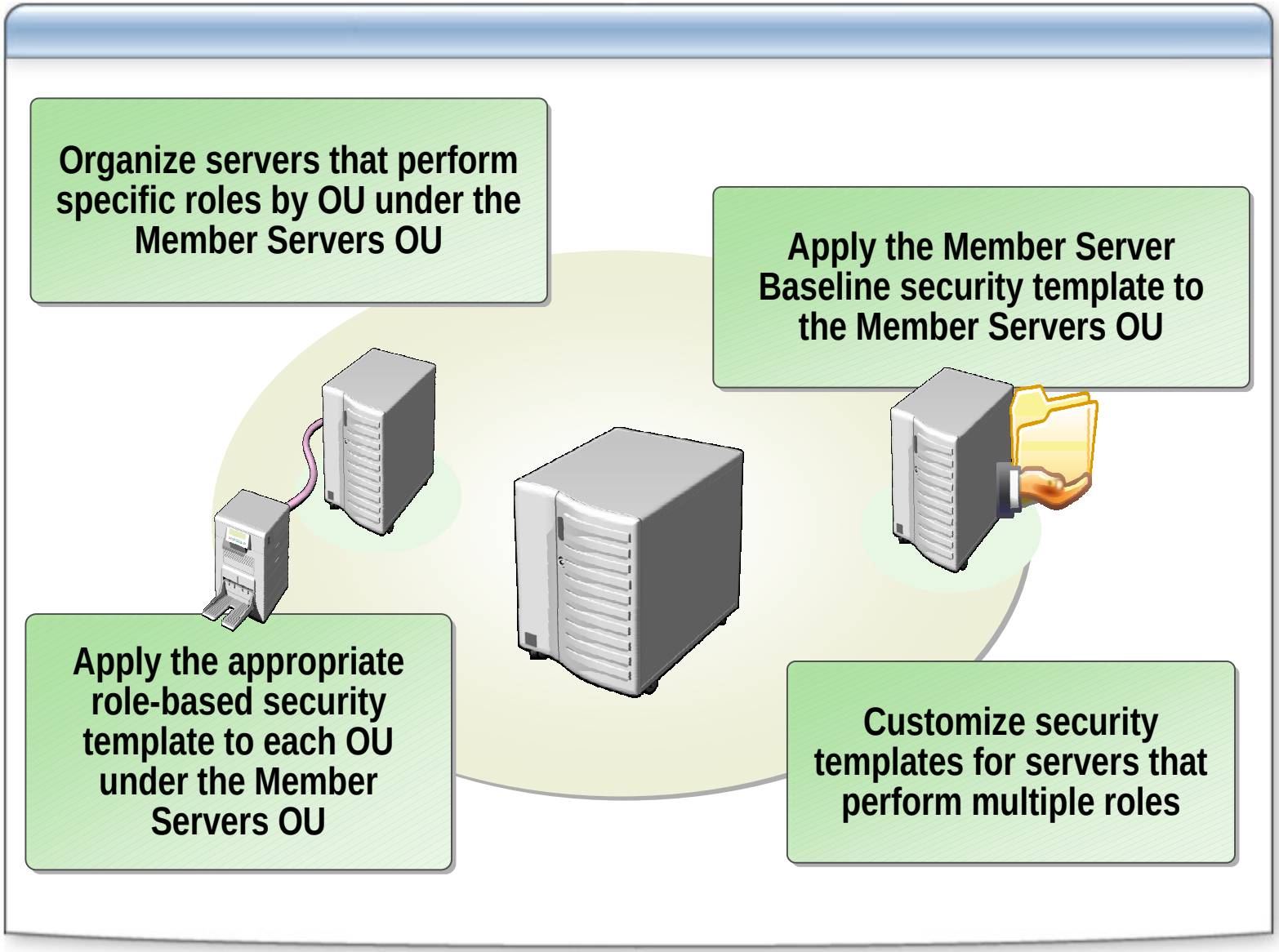
# Best Practices for Hardening Domain Controllers

- Use Group Policy to apply the Domain Controller security template to all domain controllers
- Disable services that are not required
- Do not run services on domain controllers using the same accounts used to run services on other computers
- Implement appropriate auditing and event log settings

# Hardening Servers for Specific Roles

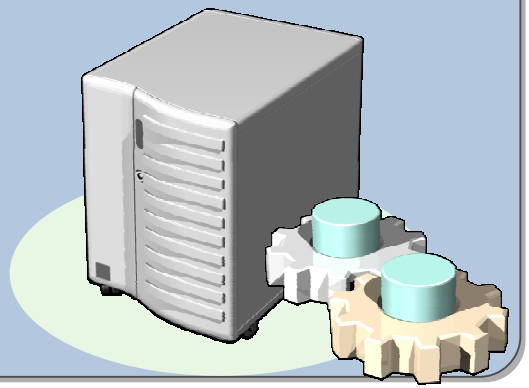
- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Using Security Templates for Specific Server Roles



# Hardening Infrastructure Servers

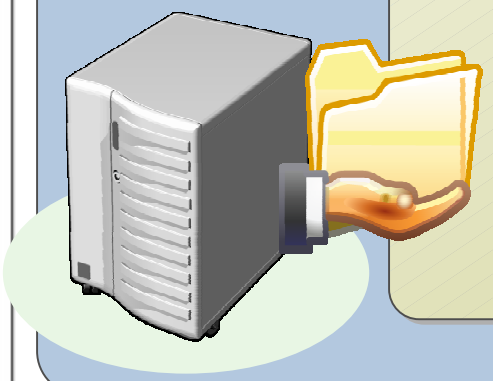
- **Apply the Infrastructure Server security template**
- **Manually configure additional settings as appropriate:**
  - Configure DHCP logging
  - Protect against DHCP DoS attacks
  - Use Active Directory integrated DNS zones
  - Use IPSec filters to restrict ports



# Hardening File Servers

- **Apply the security settings in the File Server security template**

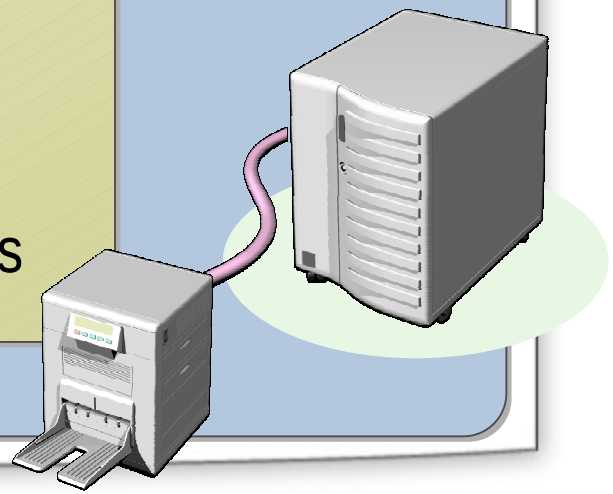
- **Manually configure additional settings on each file server:**
  - Disable DFS and FRS if not required
  - Secure all shared files and folders by using NTFS and share permissions
  - Enable auditing of critical files
  - Restrict ports by using IPSec filters



# Hardening Print Servers

- **Apply the security settings in the Print Server security template**

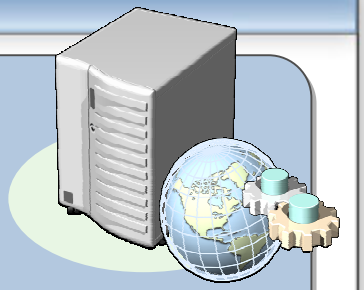
- **Manually configure additional settings on each print server:**
  - Ensure that the Print Spooler service is enabled
  - Ensure that SMB signing is not required by the print server
  - Restrict ports by using IPSec filters



# Hardening IIS Servers (Part 1)

- Apply the security settings in the IIS Server security template
- If possible, upgrade Web servers to Windows Server 2003 and IIS 6.0
- Install and run the IIS Lockdown Wizard and configure URLScan to help secure IIS 4.*x* and 5.*x* installations

# Hardening IIS Servers (Part 2)



**Manually configure each IIS server:**

- Enable only essential IIS components
- Install IIS and store Web content on a dedicated disk volume
- Configure NTFS permissions for all folders that contain Web content
- Do not enable both the Execute and Write permissions on the same Web site
- On IIS 5.0 servers, run applications using Medium or High Application Protection
- Use IPSec filters to allow only TCP Port 80 and Port 443

# Best Practices for Hardening Servers for Specific Roles

- Modify security templates as needed for servers with multiple roles
- Enable only services required by role
- Enable service logging to capture relevant information
- Use IPSec filtering to block all ports except the specific ports needed, based on server role
- Secure service accounts and well-known user accounts

# Hardening Stand-Alone Servers

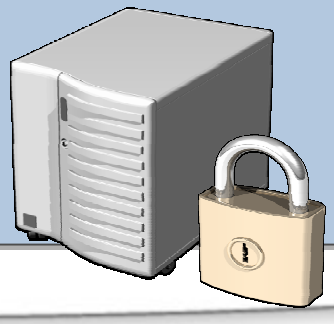
- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Applying Security Templates on Stand-Alone Servers

You must manually apply security settings to each stand-alone server

You may need to create a customized security template for each stand-alone server

Use the Security Configuration and Analysis tool, Secedit, or GPEdit.msc to apply security template settings on stand-alone servers



# Best Practices for Hardening Stand-Alone Servers

- Create a customized security template for each type of stand-alone server
- Enable only services required by role
- Enable service logging to capture relevant information
- Use IPSec filters to restrict ports based on server role

# Session Summary

- Introduction to Securing Servers
- Core Server Security
- Active Directory Security
- Hardening Member Servers
- Hardening Domain Controllers
- Hardening Servers for Specific Roles
- Hardening Stand-Alone Servers

# Next Steps

- **Find additional security training events:**

  http://www.microsoft.com/seminar/events/security.mspx

- **Sign up for security communications:**

  http://www.microsoft.com/technet/security/signup/default.mspx

- **Order the Security Guidance Kit:**

  http://www.microsoft.com/security/guidance/order/default.mspx

- **Get additional security tools and content:**

  http://www.microsoft.com/security/guidance

Microsoft®

*Your potential. Our passion.™*



RETURN TO INDEX