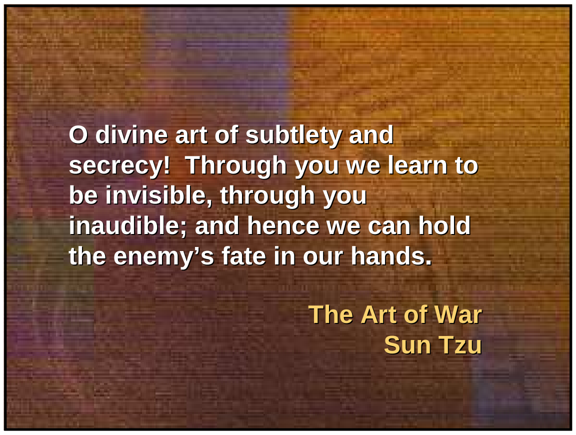
Windows Firewall

Deployment and Use in the Enterprise

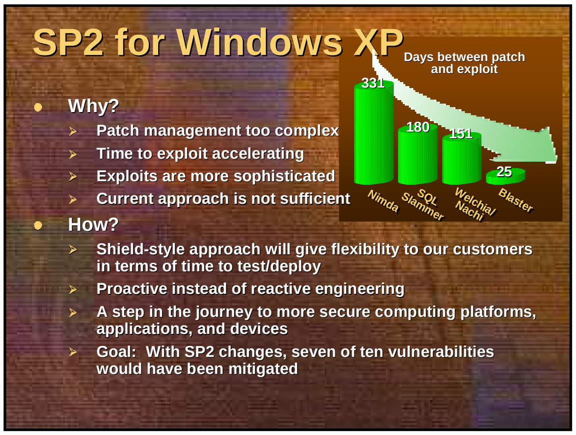
Bob McCoy
Technical Account Manager
Microsoft Premier Support
Microsoft Corporation



> O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence we can hold the enemy's fate in our hands.
>
> The Art of War
> Sun Tzu

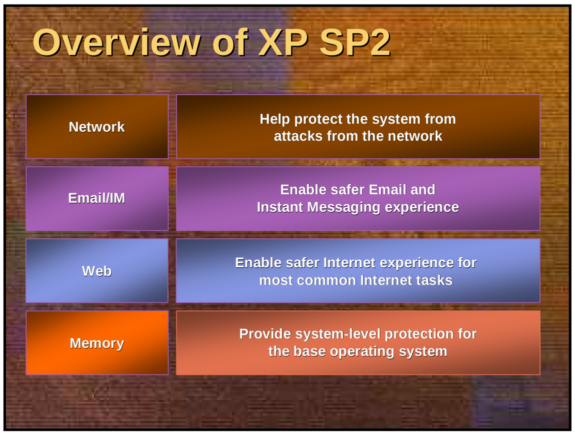
Release Status

- Currently in beta, Release Candidate 2
- Download RC2 from Microsoft
  http://www.microsoft.com/technet/prodtechnol/winxppro/sp2preview.mspx
- Very close to releasing



SP2 for Windows XP

- Why?
  - Patch management too complex
  - Time to exploit accelerating
  - Exploits are more sophisticated
  - Current approach is not sufficient
- How?
  - Shield-style approach will give flexibility to our customers in terms of time to test/deploy
  - Proactive instead of reactive engineering
  - A step in the journey to more secure computing platforms, applications, and devices
  - Goal: With SP2 changes, seven of ten vulnerabilities would have been mitigated

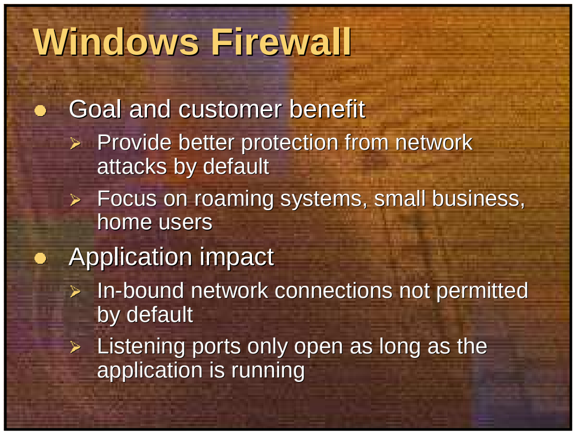


Overview of XP SP2

Network	Help protect the system from attacks from the network
Email/IM	Enable safer Email and Instant Messaging experience
Web	Enable safer Internet experience for most common Internet tasks
Memory	Provide system-level protection for the base operating system

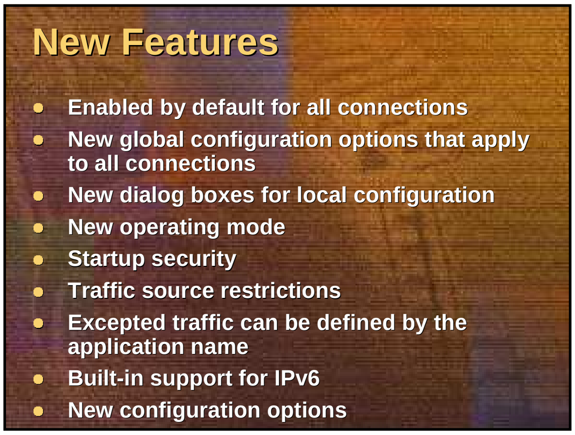
© 2001 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



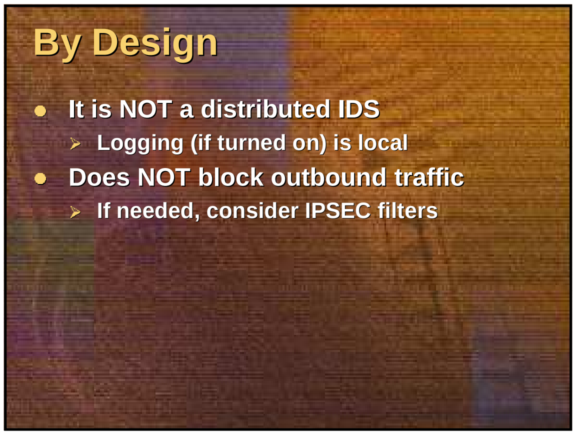
Windows Firewall

- Goal and customer benefit
  - Provide better protection from network attacks by default
  - Focus on roaming systems, small business, home users
- Application impact
  - In-bound network connections not permitted by default
  - Listening ports only open as long as the application is running



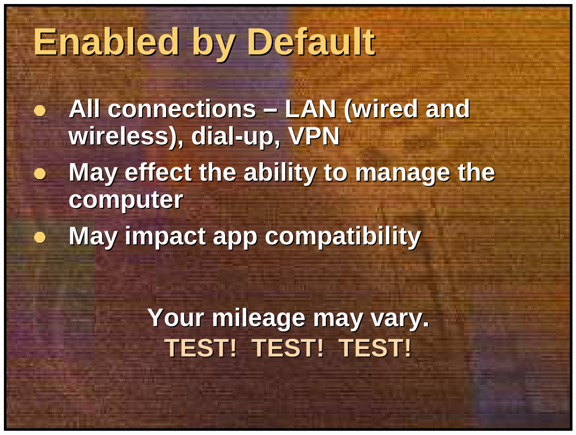
New Features

- Enabled by default for all connections
- New global configuration options that apply to all connections
- New dialog boxes for local configuration
- New operating mode
- Startup security
- Traffic source restrictions
- Excepted traffic can be defined by the application name
- Built-in support for IPv6
- New configuration options



By Design

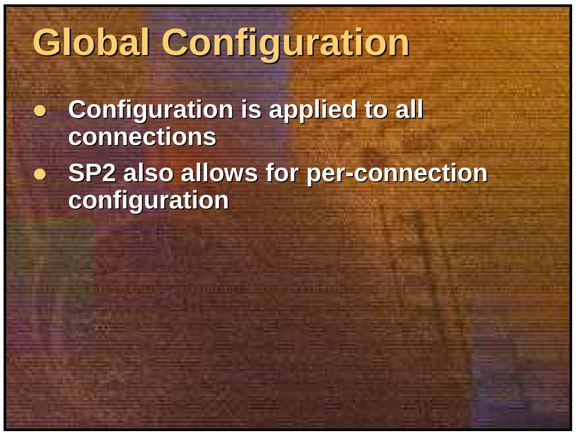
- It is NOT a distributed IDS
  - Logging (if turned on) is local
- Does NOT block outbound traffic
  - If needed, consider IPSEC filters



Enabled by Default

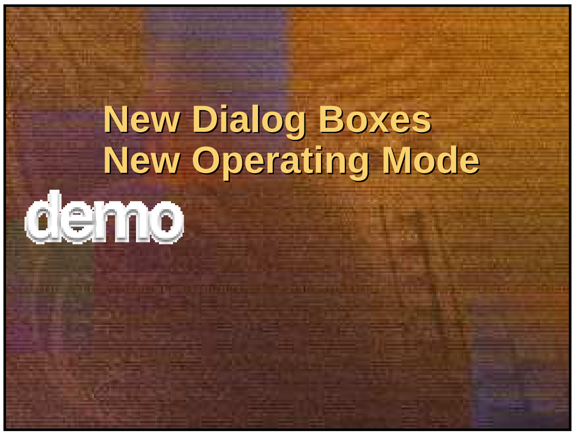
- All connections – LAN (wired and wireless), dial-up, VPN
- May effect the ability to manage the computer
- May impact app compatibility

Your mileage may vary.
TEST! TEST! TEST!



Global Configuration

- Configuration is applied to all connections
- SP2 also allows for per-connection configuration



New Dialog Boxes
New Operating Mode

demo

© 2001 Microsoft Corporation. All rights reserved.

Startup Security

- ICF dependencies in the network stack
- Brief period of exposure
- WF Startup Policy
  - Allows for initial connections to the net
  - Not configurable
  - Uses its configuration once WF is fully started

Source Restrictions

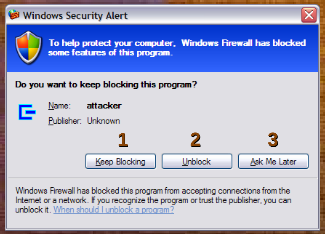
Excepted traffic can originate from:

- Any IP address
- Local subnet
- Custom list of specific addresses and/or network
  - No AD site awareness
  - Does not have to include the entire Enterprise address space – just those resources authorized to initiate traffic to the desktop

Application-Defined Traffic

- ICF only allowed exceptions based upon TCP and UDP ports
- WF exceptions can also be defined by ports
- NEW: Exceptions allowed defined by the executable's name

Prompted User Control



Windows Security Alert

To help protect your computer. Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: attacker

Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

1. Make an exception entry, unchecked
2. Make an exception entry, checked
3. Don't make an exception entry, keep blocking

IPv6 Support

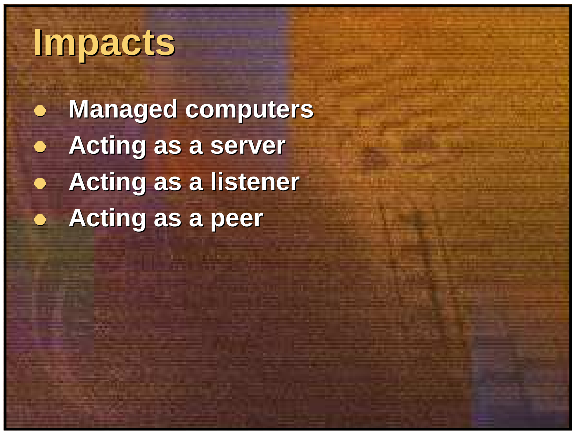
- Automatically enabled on all IPv6 connections
- Configured using the commands in the netsh firewall context

New Configuration Options

- Netsh commands extended
  - Deployment Guide is a great reference
- New configuration APIs
- Group Policy extended
- Two different protection profiles
  - Domain
  - Standard

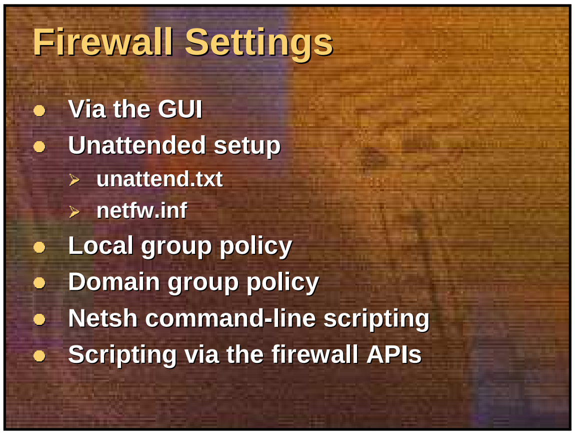
© 2001 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



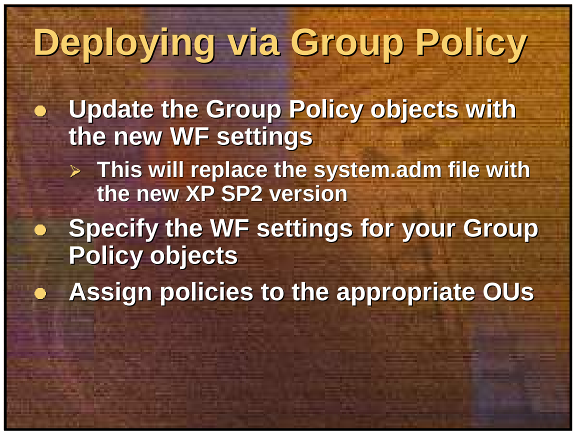
Impacts

- Managed computers
- Acting as a server
- Acting as a listener
- Acting as a peer



Firewall Settings

- Via the GUI
- Unattended setup
  - unattend.txt
  - netfw.inf
- Local group policy
- Domain group policy
- Netsh command-line scripting
- Scripting via the firewall APIs

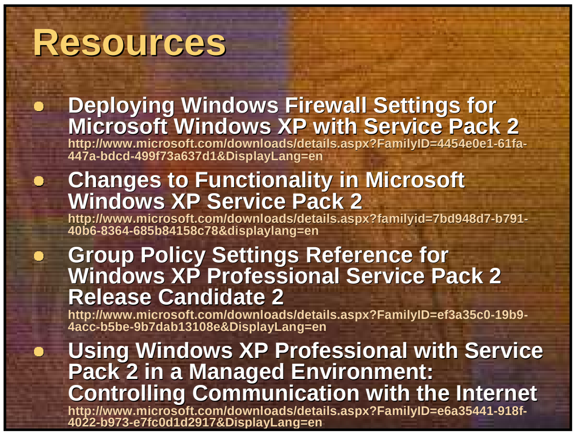


Deploying via Group Policy

- Update the Group Policy objects with the new WF settings
  - This will replace the system.adm file with the new XP SP2 version
- Specify the WF settings for your Group Policy objects
- Assign policies to the appropriate OUs

Windows Firewall

demo



Resources

- Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2
  http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en
- Changes to Functionality in Microsoft Windows XP Service Pack 2
  http://www.microsoft.com/downloads/details.aspx?familyid=7bd948d7-b791-40b6-8364-685b84158c78&displaylang=en
- Group Policy Settings Reference for Windows XP Professional Service Pack 2 Release Candidate 2
  http://www.microsoft.com/downloads/details.aspx?FamilyID=ef3a35c0-19b9-4acc-b5be-9b7dab13108e&DisplayLang=en
- Using Windows XP Professional with Service Pack 2 in a Managed Environment: Controlling Communication with the Internet
  http://www.microsoft.com/downloads/details.aspx?FamilyID=e6a35441-918f-4022-b973-e7fc0d1d2917&DisplayLang=en

Microsoft®

© 2002 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

© 2001 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.