Microsoft Windows Server
Code Name "Longhorn"

Windows Vista™

Martin Pavlis Microsoft MVP

IT Senior Consultant | KPCS CZ, s.r.o.

martin@pavlis.net | www.pavlis.net | www.kpcs.cz

Agenda

- IE7
- Bitlocker
- UAC
- Windows Defender
- ForeFront Security
- Firewall
- Auditing
- Authentication
- Group Policy
- Network Access Protection

Security and Compliance

Fundamentals

- Security Development Lifecycle
- Threat Modeling and Code Reviews
- Windows Service Hardening

Threat and Vulnerability Mitigation

- IE Protected Mode
- Windows Defender
- Network Access Protection
- IPSec & Bi-Drectional FW
- Address Space Layout Randomization

Security and Compliance

Identity and Access Control

- User Account Control
- Plug and Play Smartcards
- Granular Auditing

Information Protection

- BitLocker™ Drive Encryption
- EFS Smartcards
- RMS Client

Windows Service Hardening

Defense in depth

- Services run with reduced privilege
- Windows services are profiled for allowed actions
- Designed to block attempts by malicious software to exploit a Windows service

Windows Vista

USER ACCOUNT CONTROL

User Account Control

Challenges

Most users run with full administrator privileges all the time

- At risk from malware
- Can't manage desktops or enforce policy
- Expensive to support

Difficult to run a standard user

- User can't perform many tasks
- Many applications don't run

Windows Vista Solution

Easier to Run as Standard User

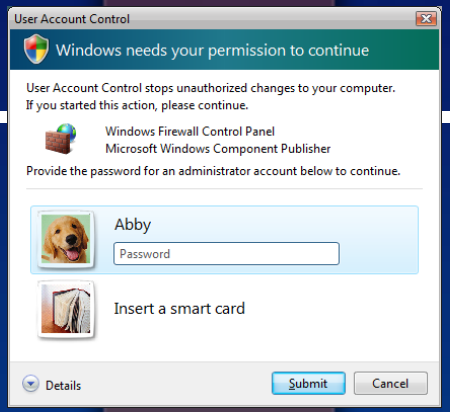
- Users can do more on their own
  - Change time zone, power settings, VPN, and more
  - Install approved devices
  - Admin commands clearly marked
- Higher application compatibility
  - File and registry virtualization

Greater Protection for Admins

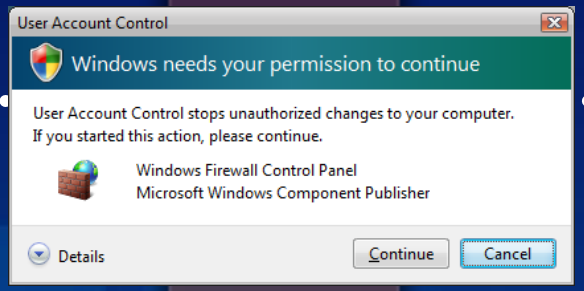
- Software runs with lower privileges by default
- Administrator provides consent before elevation

Elevation Model

Administrator Privileges



Ways to Request Elevation
Application marking
Setup detection
Compatibility fix (shim)
Compatibility assistant
Run as administrator



Standard User Privileges (Default)

Standard User Account

Administrator Account

Standard Users Can Do More

- View system clock and calendar
- Change time zone
- Configure secure wireless (WEP/WPA) connection
- Change power management settings
- Create and configure a Virtual Private Network connection
- Add printers and other devices that have the required drivers installed or allowed by IT policy
- Install approved ActiveX controls
- Disk defragmentation is a scheduled background process

- Shield icon consistently marks what actions a standard user can and cannot do

User Account Control

- Businesses can move to a better-managed desktop and parental controls for consumers
  - Make the system work well for standard users
    - Allow standard users to change relevant settings
    - High application compatibility with file/registry virtualization
    - Make it clear when elevation is required
  - Administrators use full privilege only for admin tasks
  - User provides explicit consent before using elevated privilege

Helping Legacy Applications

Run as Standard User

- Many applications would run fine as standard user, but they needlessly store data in HKLM\Software or %ProgramFiles%
  - They use these locations for per-user data, not global data
  - These locations are system-global and so only writeable by administrators
  - It’s always worked because Windows users have always been administrators
- The solution: help them through virtualization
  - Modifications of most system-global locations go to per-user areas
  - Reads generally go to the per-user location and fall back to the global location

Virtualized Files

- Redirected file system locations:
  - %ProgramFiles% (\Program Files)
  - %AllUsersProfile% (\ProgramData – what was \Documents and Settings\All Users)
  - %SystemRoot% (\Windows)
  - %SystemRoot%\System32 (\Windows\System32)
  - Exceptions:
    - Files that have executable extensions (.exe, .bat, .vbs, .scr, etc)
      - Prevents masking of system executables for servicing and security
    - Exceptions can be added in HKLM\System\CurrentControlSet\Services\Luafv\Parameters \ExcludedExtensionsAdd
- Per-user virtual root:
  - %UserProfile%\AppData\Local\VirtualStore

Note: Virtual files do not roam with Roaming Profiles

Registry Virtualization

- Redirected locations:
  - HKLM\Software
  - Exceptions:
    - HKLM\Software\Microsoft\Windows
    - HMLM\Software\Microsoft\Windows NT
    - Other subkeys under Microsoft
- Per-user virtual root:
  - HKEY_CURRENT_USER\Software\Classes\Virtual Store

Solving Application-Specific Issues

- Some applications have to be helped in other ways to run as Standard User
  - If an application is broken ask the vendor for a fix!!
  - Isolate to standard user compatibility issue
- Common application issues include:
  - *Unnecessary Administrator checks*
  - *Registering a COM object to HKLM*
  - Writing to file or registry locations that are not virtualized

Application Compatibility Toolkit

Customer Target

- Medium/Large Businesses and Large Enterprises

Mission

- A lifecycle management tool that assists in identifying and managing your overall application/device/computer portfolio, reducing the cost and time involved in resolving application compatibility issues, and helping you quickly deploy Windows Vista and Windows Updates.

Strategy

- Help detect, diagnose, and mitigate compatibility issues found in Windows Vista
- Microsoft Compatibility Exchange to facilitate exchange of compatibility data between ISV/IHV, Microsoft, and customers
- Deliver tools that are timely and relevant to Windows releases

Developer and Tester Tools

- Standard User Analyzer
  - Provides a way for testers to further test the LOB applications to determine what will fail as Standard User on Vista
- Internet Explorer Test Tool
  - Provides a way for testers to further test the intranet web applications to understand the exact issue and determine which of their web applications will not work with IE 7
- Setup Analysis Tool
  - Detects issues such as WRP, installing of 32 bit kernel mode drivers, 16 bit components to flag any of your packages which could run into this issue
- Compatibility Administrator
  - Helps IT Admins, Developers, Testers create and test compatibility shim/fixes (no code changes required)

Windows Vista

INTERNET EXPLORER 7

Internet Explorer 7

Social Engineering Protections

- Phishing Filter and Colored Address Bar
- Dangerous Settings Notification
- Secure defaults for IDN

Protection from Exploits

- Unified URL Parsing
- Code quality improvements (SDLC)
- ActiveX Opt-in
- Protected Mode to prevent malicious software

Internet Explorer 7

- Key areas of focus:
  - Makes everyday tasks easier
  - Dynamic security protection
  - Improved platform and manageability
- Enhanced functionality in IE7 in Windows Vista includes:
  - Protected Mode
  - Parental Controls integration

IE7 Security Improvements

New Features – Dynamic Security Protection

Technology to protect against technology attacks

- Limit programmatic access
- Reduce attack surface
- Warn if settings insecure
- Simplified architecture

Technology to protect against social attacks

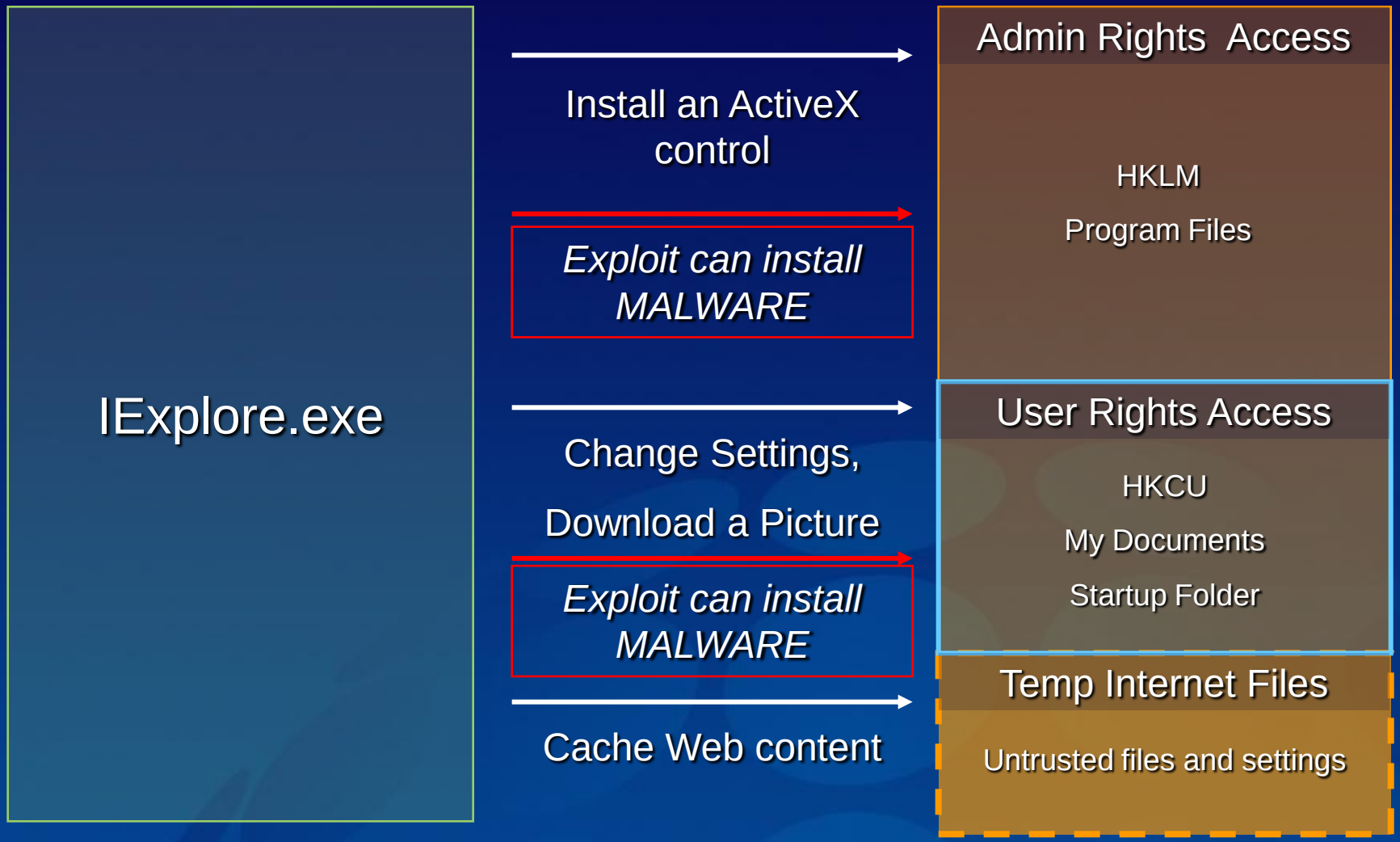
- Anti-phishing service
- Secure site visuals and info
- Address bar anti-spoofing
- “One-click cleanup”
- Extended Validation Certificates

ActiveX Opt-in And Protected Mode

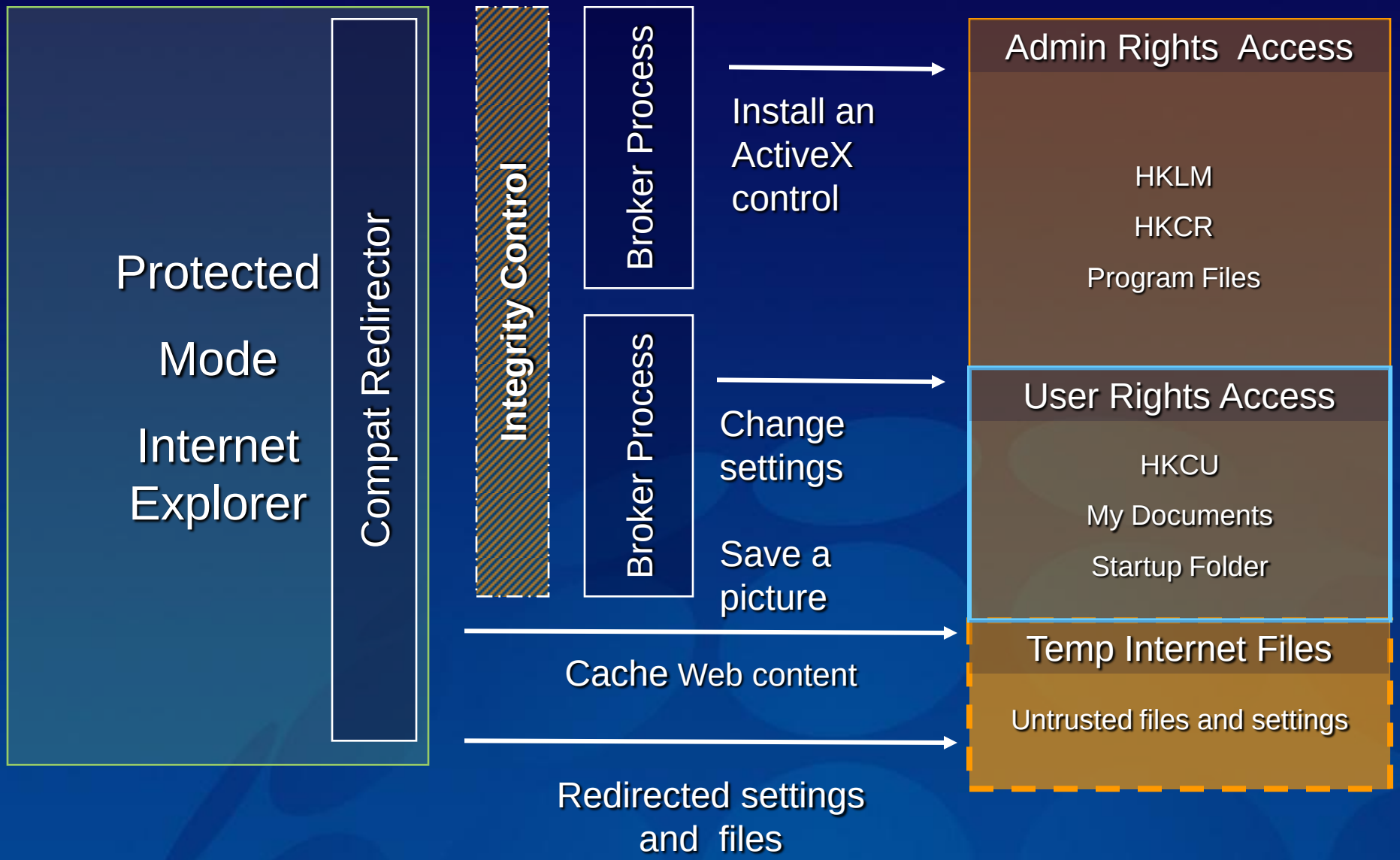
Defending systems from malicious attack

- ActiveX Opt-in puts users in control
  - Reduces attack surface
  - Previously unused controls disabled
  - Retain ActiveX benefits, increase user security
- Protected Mode reduces severity of threats
  - Eliminates silent malware install
  - IE process ‘sandboxed’ to protect OS
  - Designed for security <u>and</u> compatibility

IE Running with Full Privileges



Protected Mode



IE7 Security Improvements

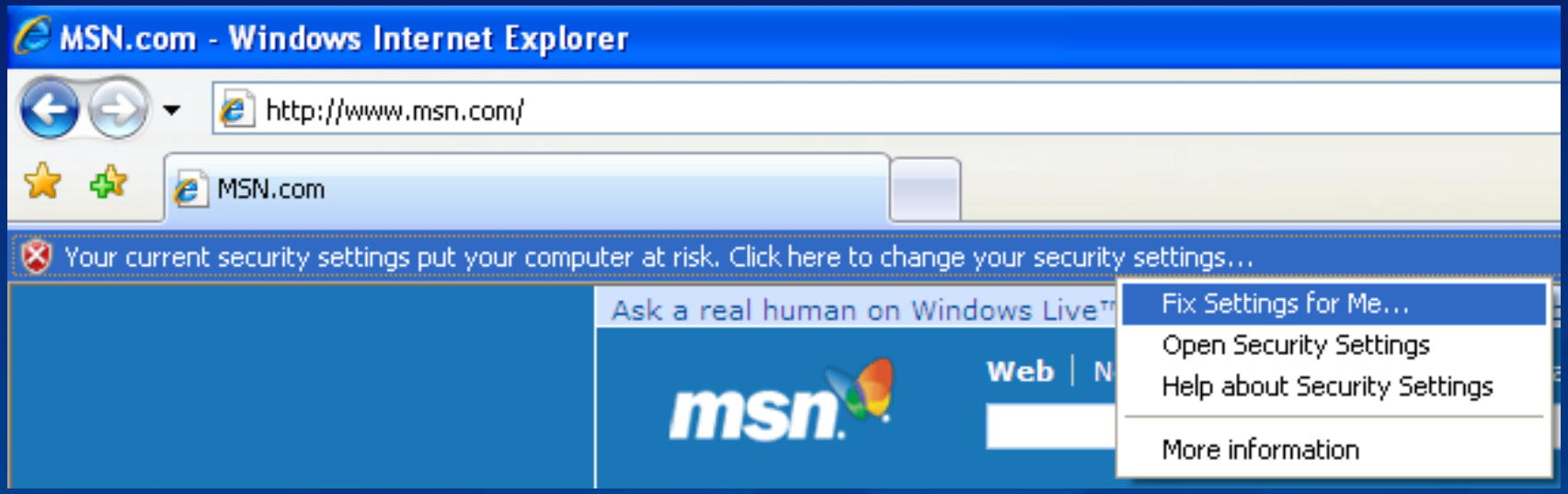
Security Zone Settings

- Only 3 Slider Settings
  - Medium, Medium-High (default), High
  - Use Trusted Sites Instead of ‘Low’ Setting
- “Righting the Wrong”
  - Fix My Settings
  - Reset to Defaults
- Protected Mode

Fix My Settings

Helping Users Avoid Security Exposure

Security Settings warning reminds users when settings may expose their systems to unwanted exposure



Phishing problem

Attacks steal:

- Customer data
  - Keyloggers, redirection, malware
- Customer confidence
  - Good vs Bad sites?
  - Online vs. Traditional Banking

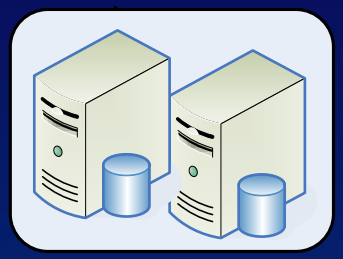
Anti-Phishing Work Group	July 2006
# of unique phishing sites	14191
# brands hijacked	154
Avg time online	4.8 days
Max time online	31 days

IE7 Security Improvements

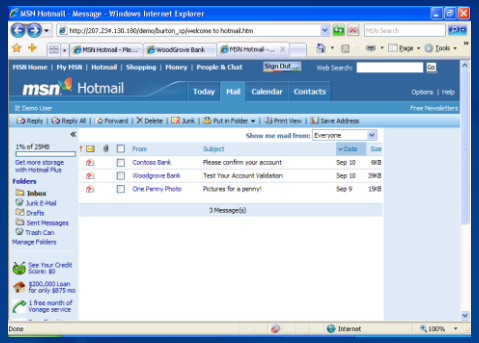
Protecting User Privacy – Phishing Filter

- Client-side heuristics, allow-list, and Web service

URL Reputation Service



https://urs.microsoft.com



Known Good URLs

Controlling Anti-phishing filter

- How do I control this inside my firewall?
  - Controllable through group policy support and IE7 security zone settings
  - Intranet sites are not checked by default
- Can I customize trusted sites for Phishing Filter in IE7?
  - 2 Step Process:
    1. Turn Customization of trusted sites in IE 7 Security Zones settings
    2. Turn off MS Phishing Filter for this zone.
  - Phishing Filter will trust these sites automatically and never check them
- Does this look up every page visited ? What is traffic impact?
  - 4-6k per lookup with about 10% of the pages viewed resulting in lookup.
  - Cache page results so that a page visited often in a day is only looked up once and then cached locally.

SSL Certificates

- Great technology for security:
  - Certificates encrypt data between client and server
  - Protects data in transmission
  - Prevents unwanted disclosure to 3rd parties (man in the middle attacks)
- But no effective protection against social attacks:
  - Lack of industry standard identity validation process
    - Certificates issued within minutes
    - Secure connection to bad people (Bankoamerica.com, Fidellity.com, etc.)
  - After all these years, users are still confused with the Padlock icon

Extended Validation SSL Certificates

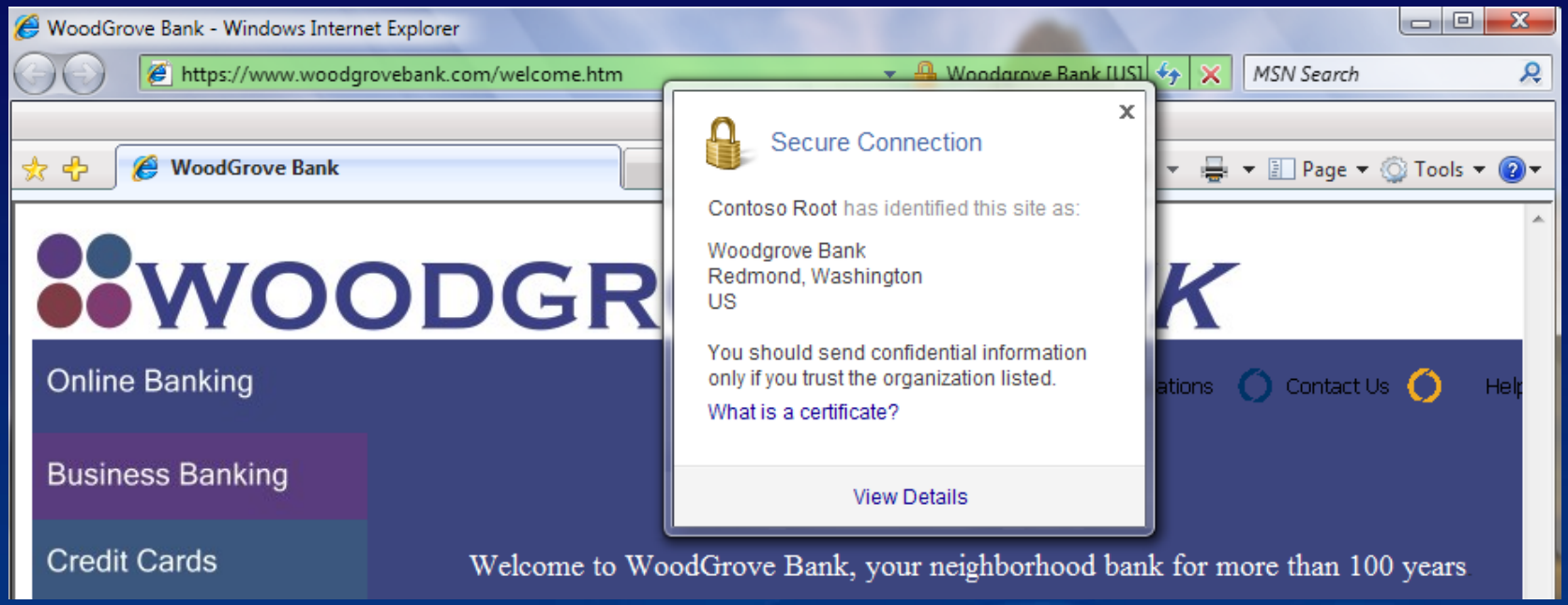
From good to great

- Same great security technology:
  - Uses proven and reliable SSL technology
  - Compatible with existing browsers
- Added protection for social attacks:
  - Improved Entity Validation
    - Comprehensive business review
    - Prevents Phishing copy sites
  - Improved Visual Experience
    - Green Address Bar, with visible Business and CA identities
    - Information is clear and understandable

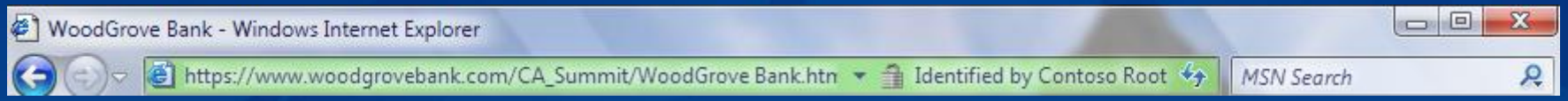
Extended Validation Certs

Enhanced display controls

- Clearer information about trusted sites

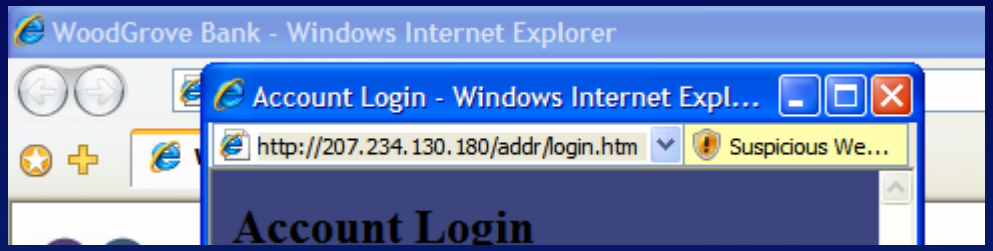


- Trust Badge rotates to show Certificate Authority



Address Bar Everywhere

All windows are clearly labeled



Protects against ‘pop up/under phishing’

Users always see a URL to help them know the actual source of content

Address Bar cannot be modified or deleted

Security Status Bar

Makes users aware of online security and privacy

Extended Validation

Woodgrove Bank [US]

Trusted party has provided extensive verification for the authenticity of certificate holder

Standard Security

Website provided a certificate matching the server and appears trustworthy

Incorrect Data

Certificate Error

There are errors in the certificate provided and the website should not be trusted

Phishing Filter (Warn)

Suspicious Website

The website contains characteristics found in phishing websites … proceed cautiously

Phishing Filter (Block)

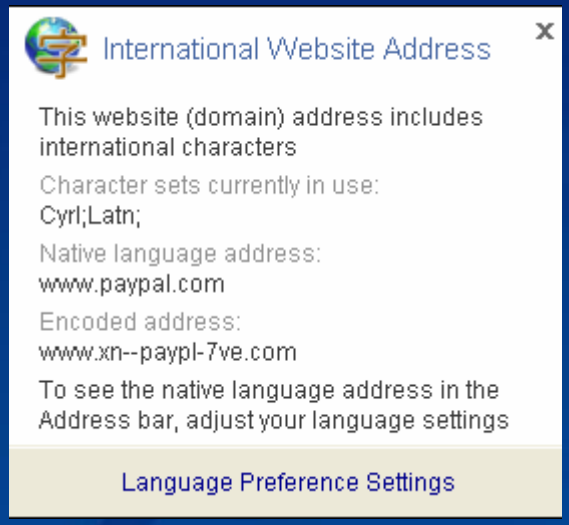
Phishing Website

A warning is displayed and users are navigated away from the website

International Domain Names

Support and security for multiple languages

- IDN security provides:
  - Blocking of multiple languages in a single URL label, protecting users from misleading display addresses
  - Forcing the punycode format display for URLs in languages the user does not have configured



Information window shows URL in both native language and punycode format

Delete Browsing History

Quickly and easily erase user activity

One screen provides ready access to delete any or all categories of browsing history

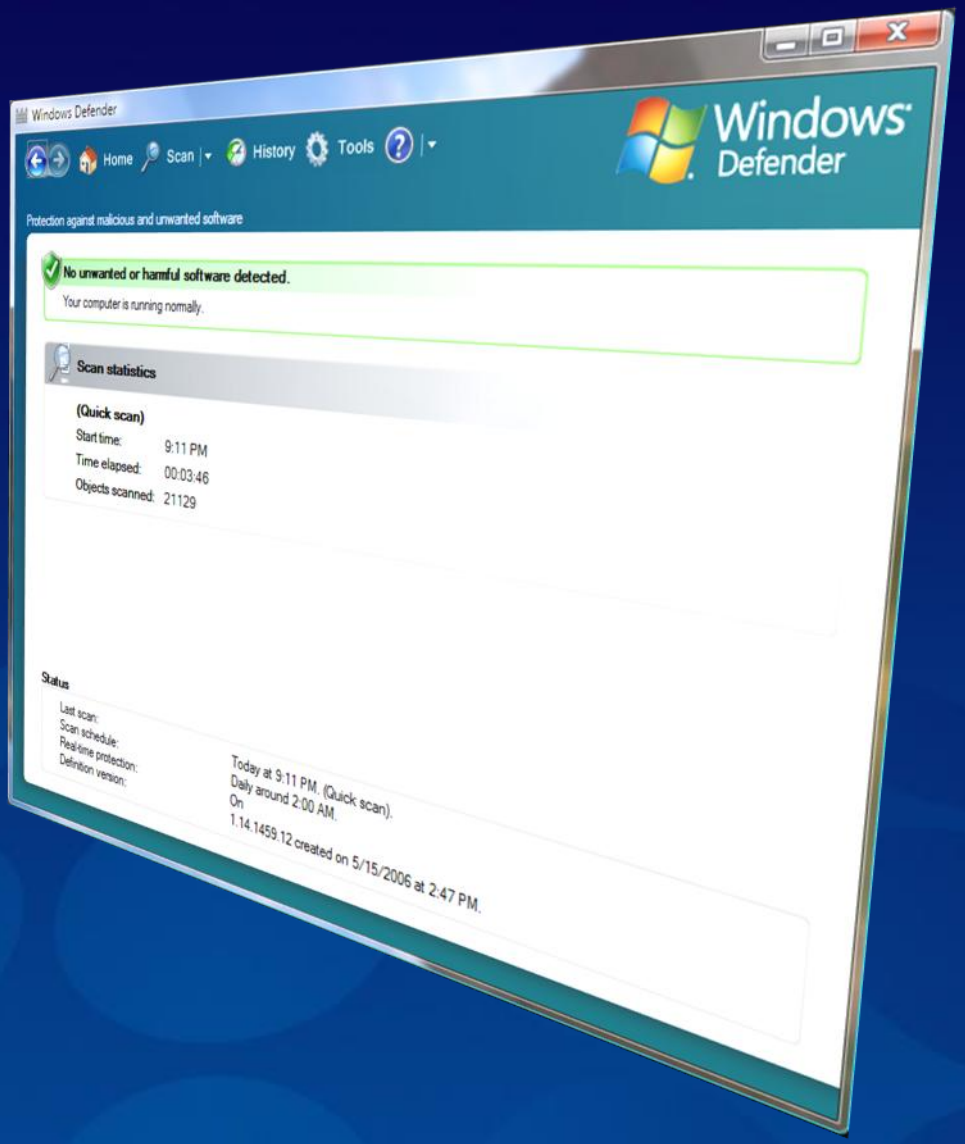
Offers users a simple interface to help fight disclosing personal information in shared computing environments

Windows Vista

WINDOWS DEFENDER

Windows Defender

- Improved Detection and Removal
- Redesigned and Simplified User Interface
- Protection for all user



Windows Vista

FOREFRONT SECURITY

Microsoft®
Forefront™ Client Security

Unified malware protection for business desktops, laptops and server operating systems that is easy to manage and control

Unified Protection

- One solution for spyware and virus protection
- Built on protection technology used by millions worldwide
- Effective threat response

Simplified Administration

- One console for simplified security administration
- Define one policy to manage client protection agent settings
- Integrates with your existing infrastructure

Visibility & Control

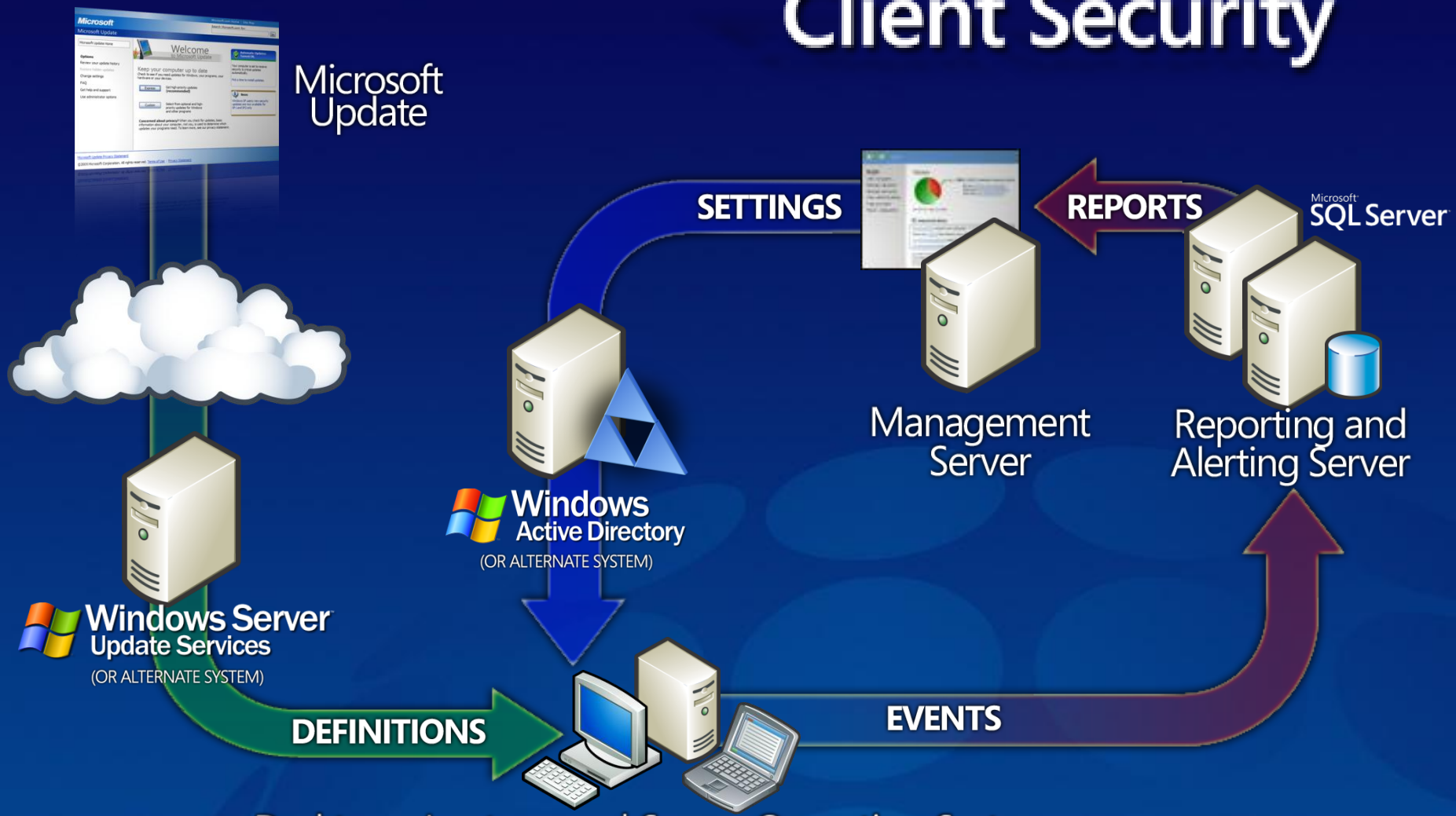
- One dashboard for visibility into threats and vulnerabilities
- View insightful reports
- Stay informed with state assessment scans and security alerts

Client Anti-Malware Offerings

	FOR INDIVIDUAL USERS				FOR BUSINESSES
	MSRT	Windows Defender	Windows Live OneCare Safety Scanner	Windows Live OneCare	Forefront Client Security
Remove most prevalent viruses	✓		✓	✓	✓
Remove all known viruses			✓	✓	✓
Real-time antivirus				✓	✓
Remove all known spyware		✓	✓	✓	✓
Real-time antispyware		✓		✓	✓
Central reporting and alerting					✓
Customization					✓
IT Infrastructure Integration					✓

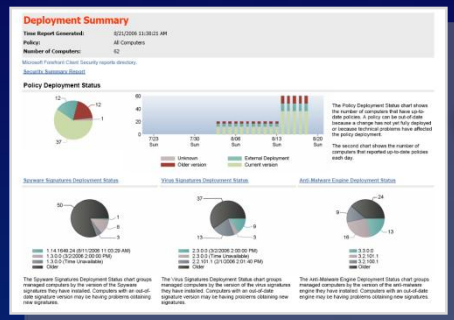
How It Works

Microsoft® Forefront™ Client Security



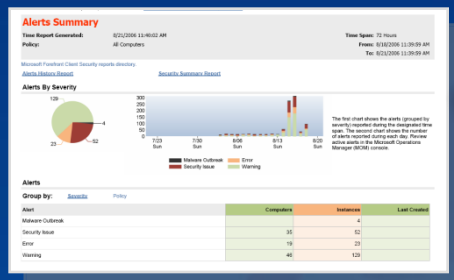
Critical Visibility & Control

Summary Report

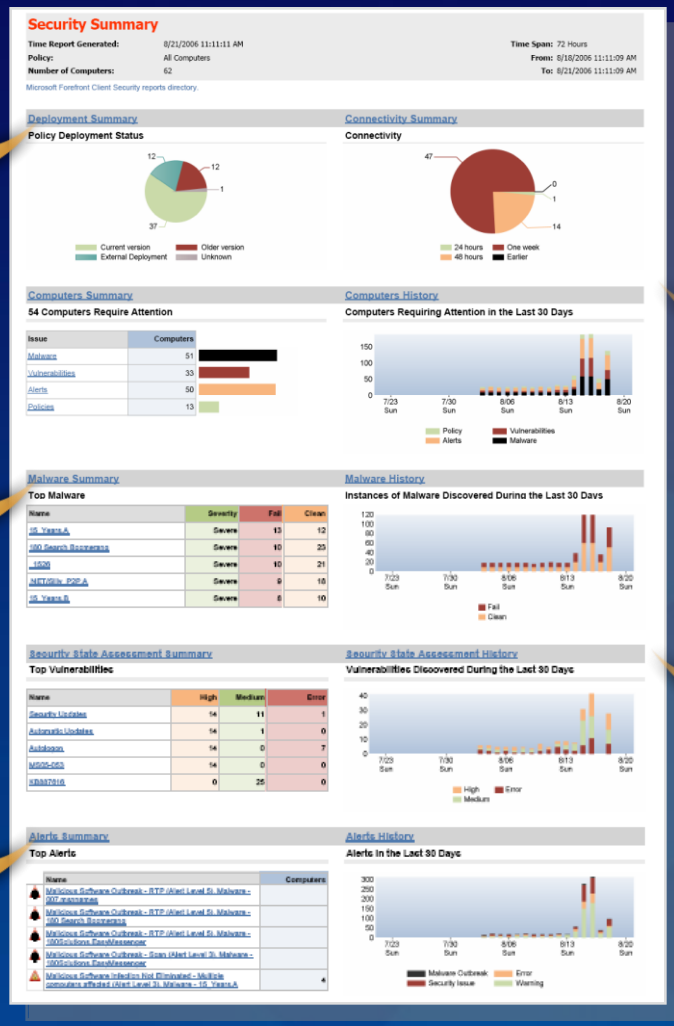


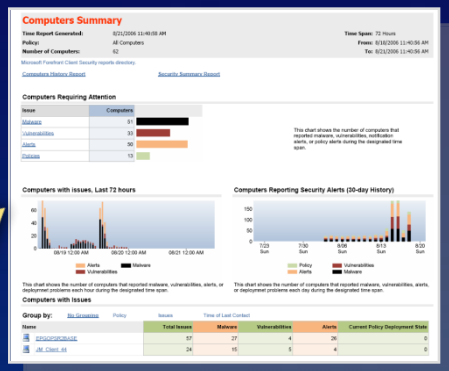
Deployment Summary

Malware Summary

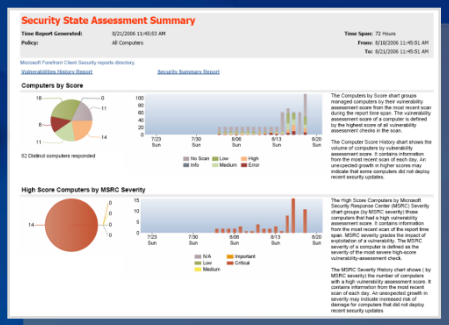


Alerts Summary





Computer Summary

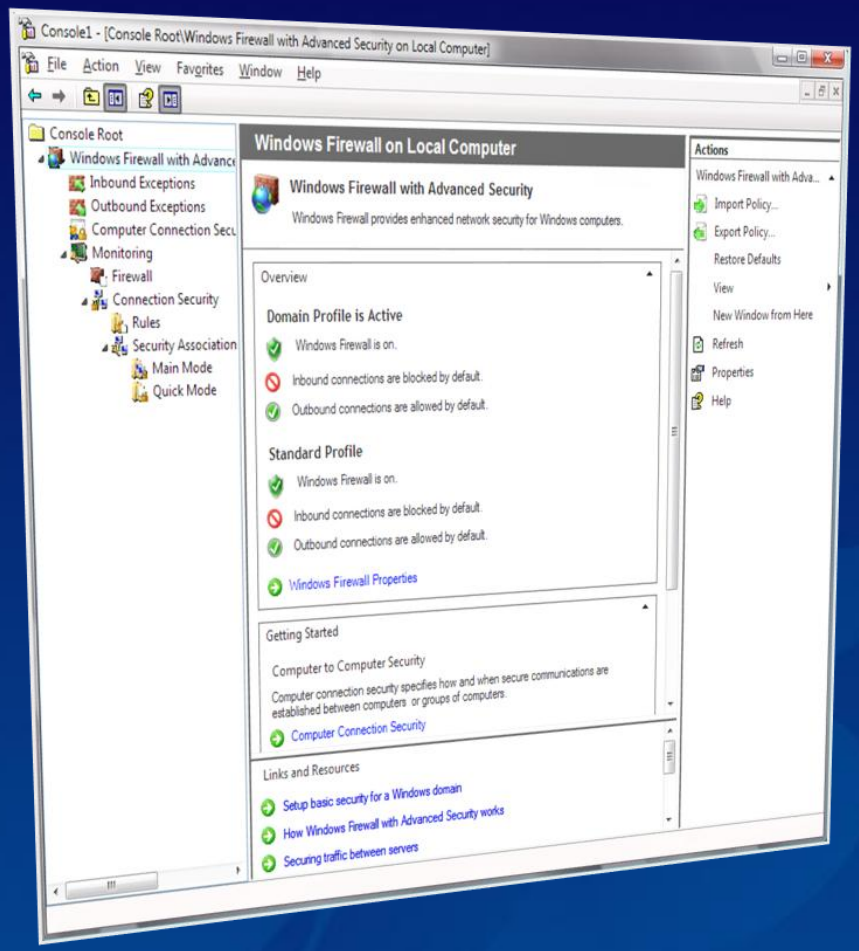


Security State Assessment Summary

Windows Vista

VISTA FIREWALL

Windows Vista Firewall



- Combined firewall and IPsec management
- Firewall rules become more intelligent
- Outbound filtering
- Simplified protection policy reduces management overhead

Filtering directions

Inbound

Default:

Block most

Few core exceptions

Allow rules:

Programs, services

Users, computers

Protocols, ports

Outbound

Default:

Allow all interactive

Restrict services

Block rules:

Programs, services

Users, computers

Protocols, ports

Comparing features

	Windows XP SP2	Windows Vista
Direction	Inbound	Inbound, outbound
Default action	Block	Configurable for direction
Packet types	TCP, UDP, some ICMP	All
Rule types	Application, global ports, ICMP types	Multiple conditions from basic five-tuple to IPsec metadata
Rule actions	Block	Block, allow, bypass; with rule merge logic
UI and tools	Control Panel, netsh	C-Panel, more netsh, MMC
APIs	Public COM, private C	More COM to expose rules, more C to expose features
Remote management	none	Via hardened RPC interface
Group policy	ADM file	MMC, netsh
Terminology	Exceptions; profiles	Rules; categories=profiles

Configuration

- Control panel: similar to Windows XP
  - A few changes to presentation
- New MMC user interface for all the extra goodies
  - “Windows Firewall with Advanced Security” snap-in
  - Predefined console in Administrative Tools
  - Can assign settings to remote computers
  - Integrates *and simplifies* IPsec settings here, too
- Also new **`netsh advfirewall`** command line

Rule types

Program	Allows traffic for a particular program
Port	Allows traffic on a particular TCP or UDP port or list of ports
Predefined	Groups of rules that allow Windows functionality on the network (for instance: file and printer sharing, network discovery, remote assistance, remote service administration, Windows collaboration, others)
Custom	All the knobs and dials, switches and buttons

The firewall rule

```
DO Action = {By-pass | Allow | Block} IF:
   Protocol = X AND
   Direction = {In | Out} AND
   Local TCP/UDP port is in {Port list} AND
   Remote TCP/UDP port is in {Port list} AND
   ICMP type code is in {ICMP type-code list} AND
   Interface NIC is in {Interface ID list} AND
   Interface type is in {Interface types list} AND
   Local address is found in {Address list} AND
   Remote address is found in {Address list} AND
   Application = <Path> AND
   Service SID = <Service Short Name> AND
   Require authentication = {TRUE | FALSE} AND
   Require encryption = {TRUE | FALSE} AND
   Remote user has access in {SDDL} AND
   Remote computer has access in {SDDL} AND
   OS version is in {Platform List}
```

Example rules

Allow Internet Explorer to connect outbound to destination port 80/tcp

Allow svchost.exe hosting RPCSS to listen for inbound traffic on port 135/tcp from remote addresses

Allow UPnP service to listen for inbound traffic on <*Interface-ID*> from USB devices, on ports 2869 and 1900

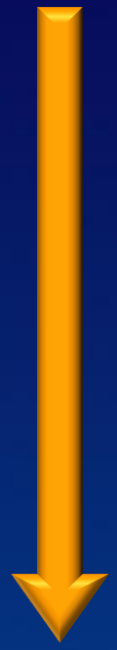
(must use API for rules with <interface-ID>s

Block svchost.exe hosting MPSSVC from connecting outbound or listening inbound

Allow svchost.exe hosting PolicyAgent to listen on dynamic RPC ports from remote computer <*hostname*> and user <*username*>

Rule merging and evaluation order

Highest



Lowest

Service restrictions	Restricts connections that services can establish; OS services already configured appropriately
Connection rules	Restricts connections from particular computers; uses IPsec to require authentication and authorization
Authenticated bypass	Allows specified authenticated computers to bypass other rules
Block rules	Explicitly blocks specified incoming or outgoing traffic
Allow rules	Explicitly allows specified incoming or outgoing traffic
Default rules	Default behavior for a connection

More flexible exceptions

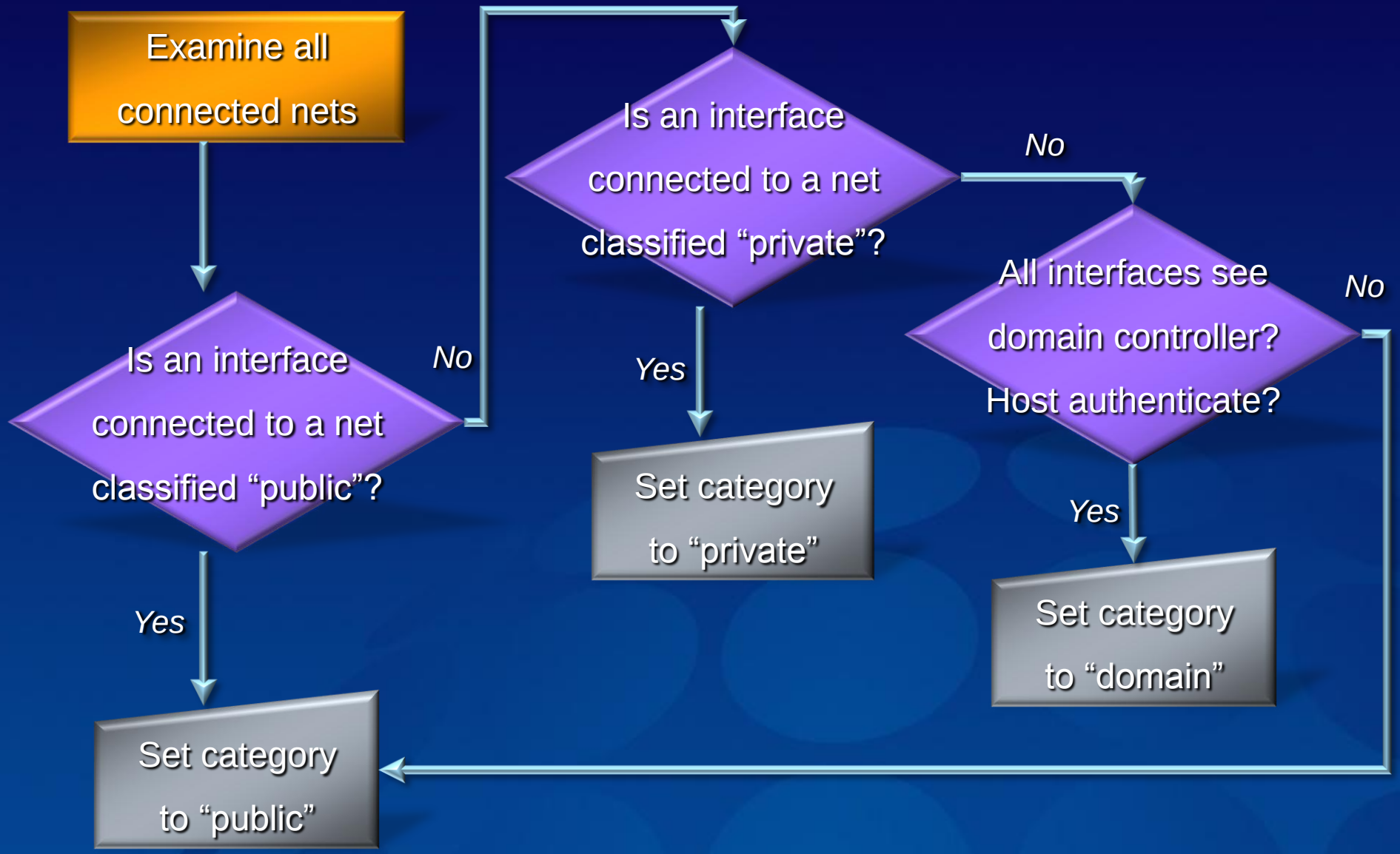
Active Directory user/computer accounts and groups
Source and destination IP addresses (individual or range)
Source and destination TCP/UDP ports
Comma-delimited list of ports (but not low-high range)
IP protocol number
Types of interfaces (wired, wireless, VPN/RAS)
ICMP type and code
Services (used by service profiling to limit access)

Network profile

Domain	When the computer is domain-joined and connected to the domain; automatically selected
Private	When the computer is connected to a defined private network
Public	All other networks

- NLA detects network changes
  - Identifies characteristics, assigns a GUID
- Network profile service creates profile upon connection
  - Interfaces, DC, authenticated machine, gateway MAC, …
- NPS notifies firewall whenever NLA detects change
  - Firewall changes category within 200ms
- If not domain, user is queried for public or private
  - Must be local administrator to define a private network

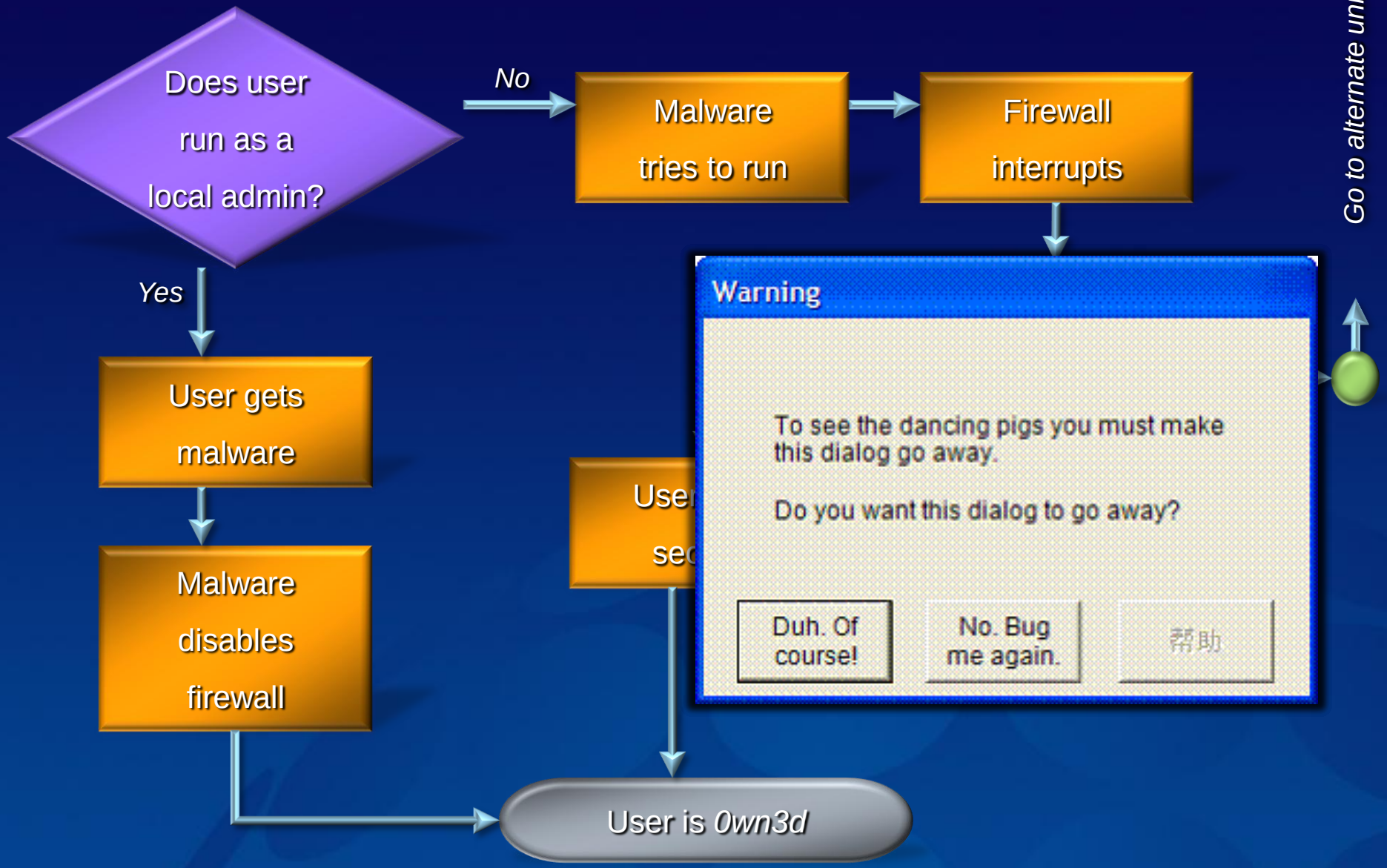
What if multiple interfaces?



Group policy processing

- Previously, this is what you got
  - Computer polices: when OS boots
  - User policies: when user logs on
  - Periodic refresh
- Now you also get
  - Computer and user: upon establishing VPN connection
  - Computer and user: when computer resumes from hibernation or standby
- FW/IPsec policy is, of course, per-computer only

Why other host firewalls still suck



Therefore

- Outbound control works only on machines that aren’t compromised and operated by people who care about security
- Outbound control won’t work where you want it to: on compromised machines or those operated by people who don’t care about security

- Outbound control is useful for administratively restricting known software from communicating
- Switch off the prompting

Windows Firewall

Turn Windows Firewall on or off

Allow a program through Windows Firewall

Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

How does a firewall help protect my computer?

For your security, some settings are controlled by Group Policy

Windows Firewall is helping to protect your computer

Windows Firewall is on. Change settings

Inbound connections that do not have an exception are blocked.

Display a notification when a program is blocked: Yes

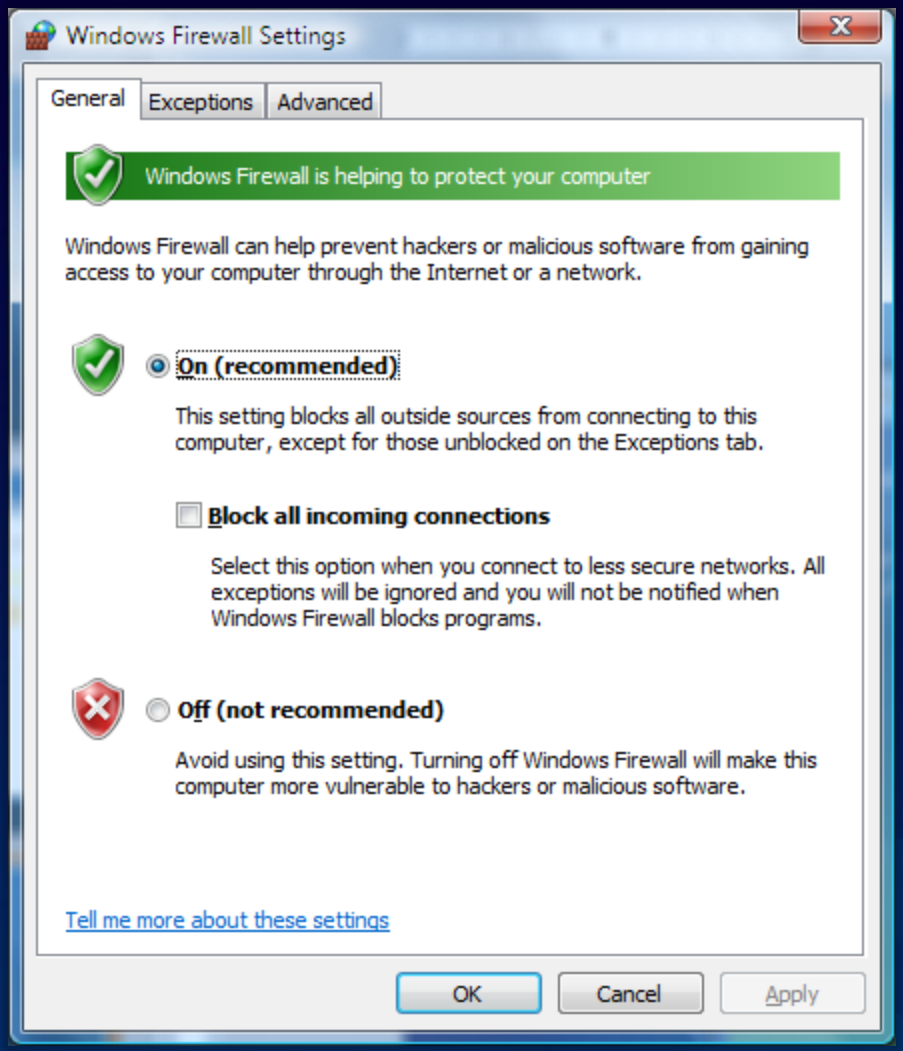
Network location: Public network

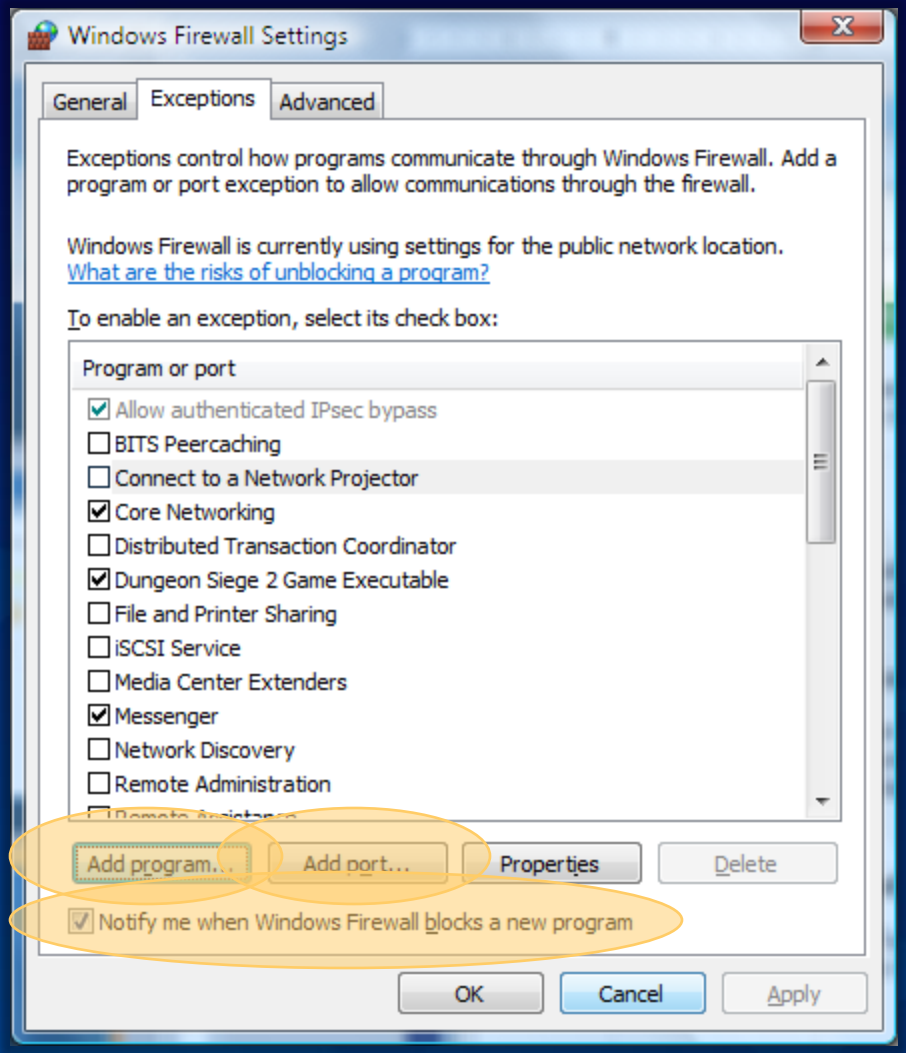
What are network locations?

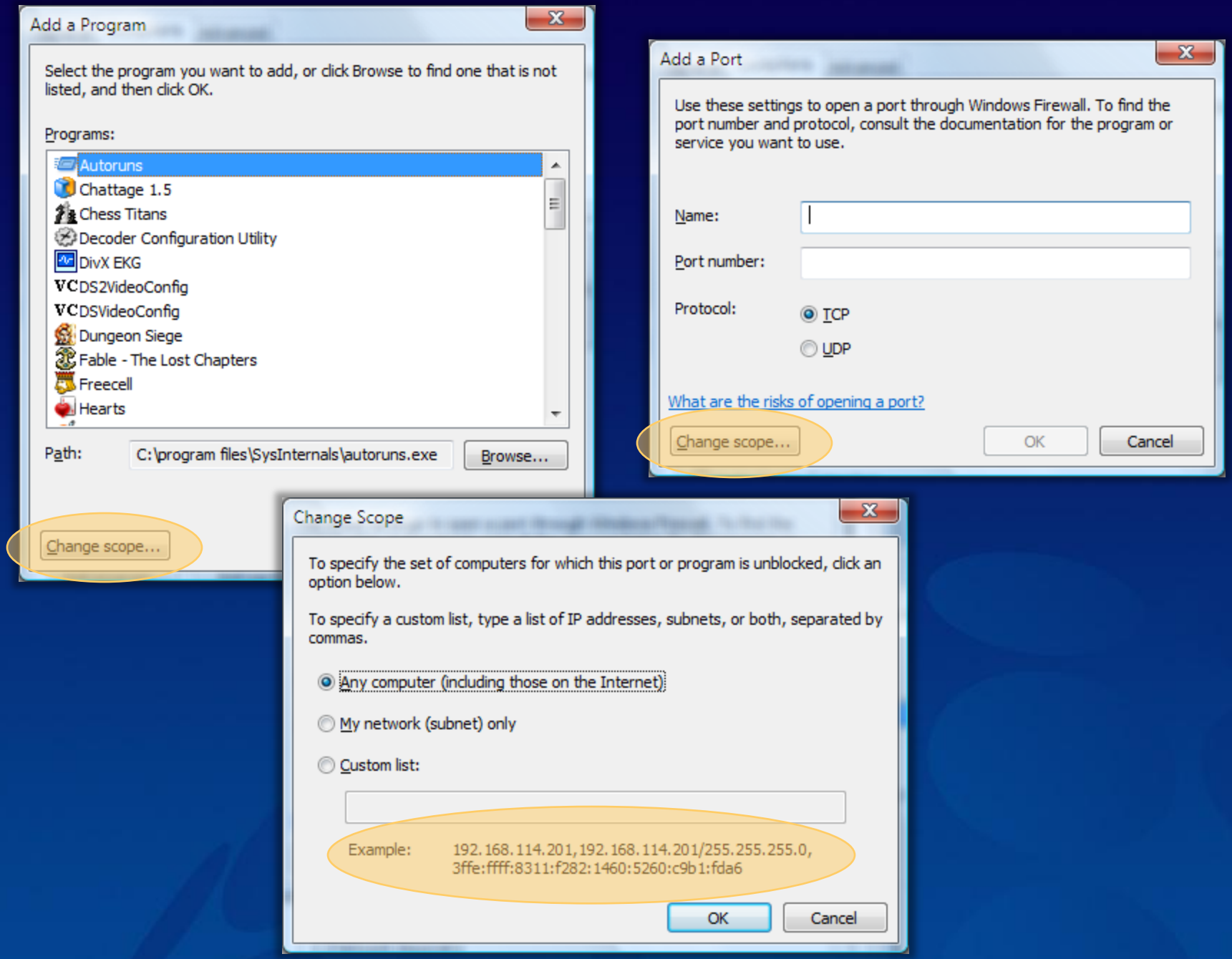
See also

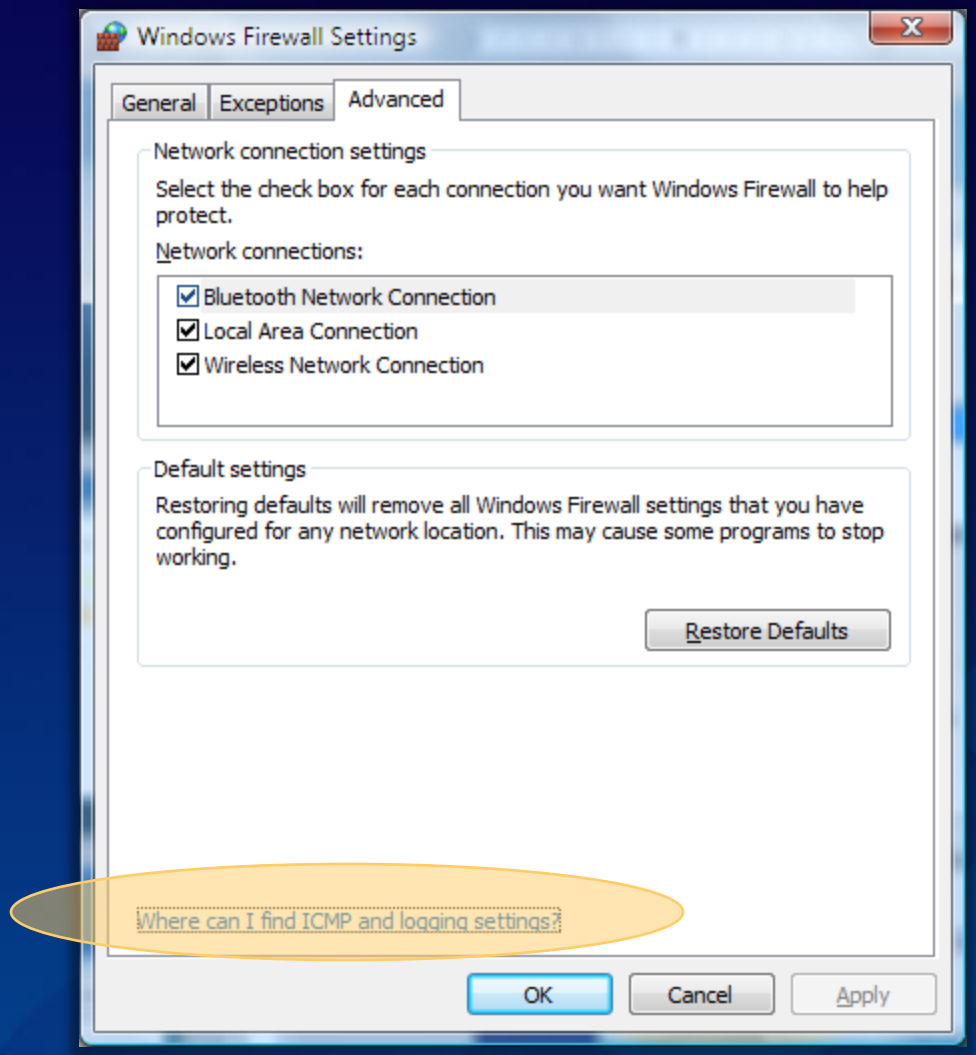
Security Center

Network Center


Windows Firewall Settings
General
Exceptions
Advanced
Windows Firewall is helping to protect your computer
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.
Block all incoming connections
Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.
Tell me more about these settings
OK
Cancel
Apply


Windows Firewall Settings
General
Exceptions
Advanced
Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.
Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?
To enable an exception, select its check box:
Program or port
Allow authenticated IPsec bypass
BITS Peercaching
Connect to a Network Projector
Core Networking
Distributed Transaction Coordinator
Dungeon Siege 2 Game Executable
File and Printer Sharing
iSCSI Service
Media Center Extenders
Messenger
Network Discovery
Remote Administration
Add program...
Add port...
Properties
Delete
Notify me when Windows Firewall blocks a new program
OK
Cancel
Apply


Add a Program
Select the program you want to add, or click Browse to find one that is not listed, and then click OK.
Programs:
Autoruns
Chattage 1.5
Chess Titans
Decoder Configuration Utility
DivX EKG
VCDS2VideoConfig
VCDSVideoConfig
Dungeon Siege
Fable - The Lost Chapters
Freecell
Hearts
Path:
C:\program files\SysInternals\autoruns.exe
Browse...
Change scope...
Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
Port number:
Protocol:
TCP
UDP
What are the risks of opening a port?
Change scope...
OK
Cancel
Change Scope
To specify the set of computers for which this port or program is unblocked, click an option below.
To specify a custom list, type a list of IP addresses, subnets, or both, separated by commas.
Any computer (including those on the Internet)
My network (subnet) only
Custom list:
Example:
192.168.114.201,192.168.114.201/255.255.255.0,
3ffe:ffff:8311:f282:1460:5260:c9b1:fda6
OK
Cancel


Windows Firewall Settings
General
Exceptions
Advanced
Network connection settings
Select the check box for each connection you want Windows Firewall to help protect.
Network connections:
Bluetooth Network Connection
Local Area Connection
Wireless Network Connection
Default settings
Restoring defaults will remove all Windows Firewall settings that you have configured for any network location. This may cause some programs to stop working.
Restore Defaults
Where can I find ICMP and logging settings?
OK
Cancel
Apply

Windows Firewall with Advanced Security

File Action View Help

- Windows Firewall with Advanced Sec
  - Inbound Rules
  - Outbound Rules
  - Connection Security Rules
  - Monitoring

Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides enhanced network security for Windows computers.

Overview

For your security, some settings are controlled by Group Policy

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

Anthenticate communications between computers

Specify how and when connections between computers are authenticated and protected using Internet Protocol security (IPsec). After specifying how to protect connections using connection security rules, create firewall rules for connections you wish to allow.

Connection Security Rules

View and create firewall rules

Create rules to allow or block connections to specific programs or ports. You can further restrict connections based on criteria such as whether the connection is authenticated or the users or groups who are initiating the connection. If a connection does not match a specified rule, the default behavior applies.

Inbound Rules

Outbound Rules

View current policy and activity

View information about currently applied policy settings and security associations for active connections.

Monitoring

Resources

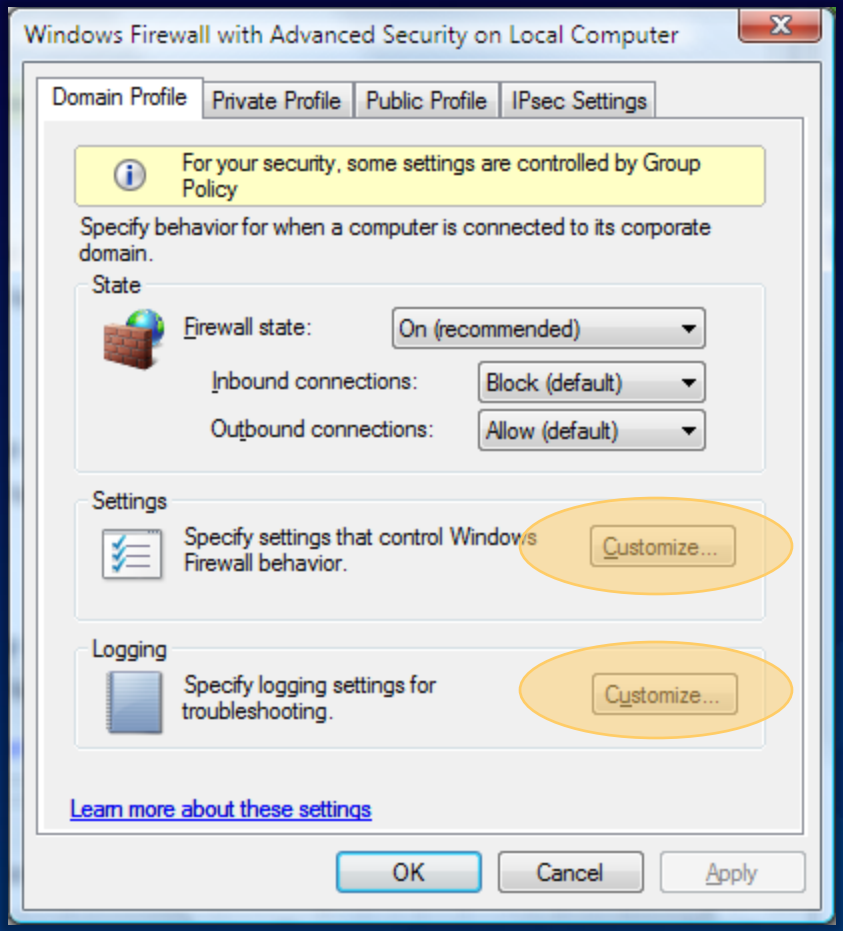
- Getting started
- Diagnostics and troubleshooting
- Documentation overview

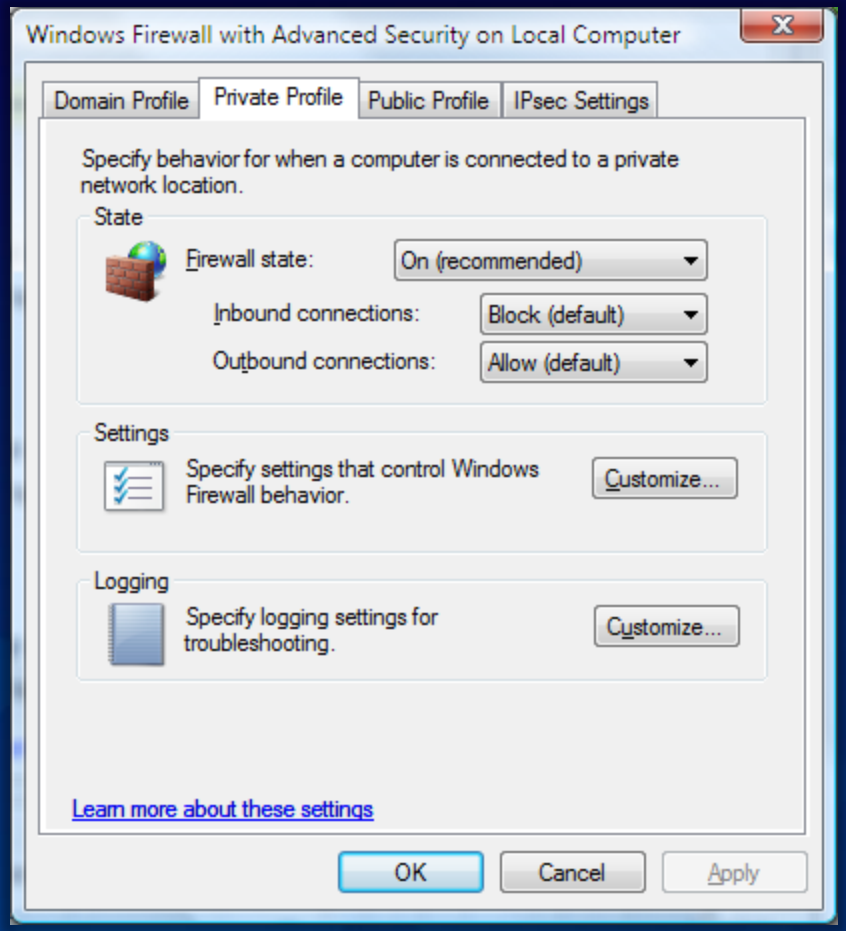
Actions

Windows Firewall with Advanced Se...

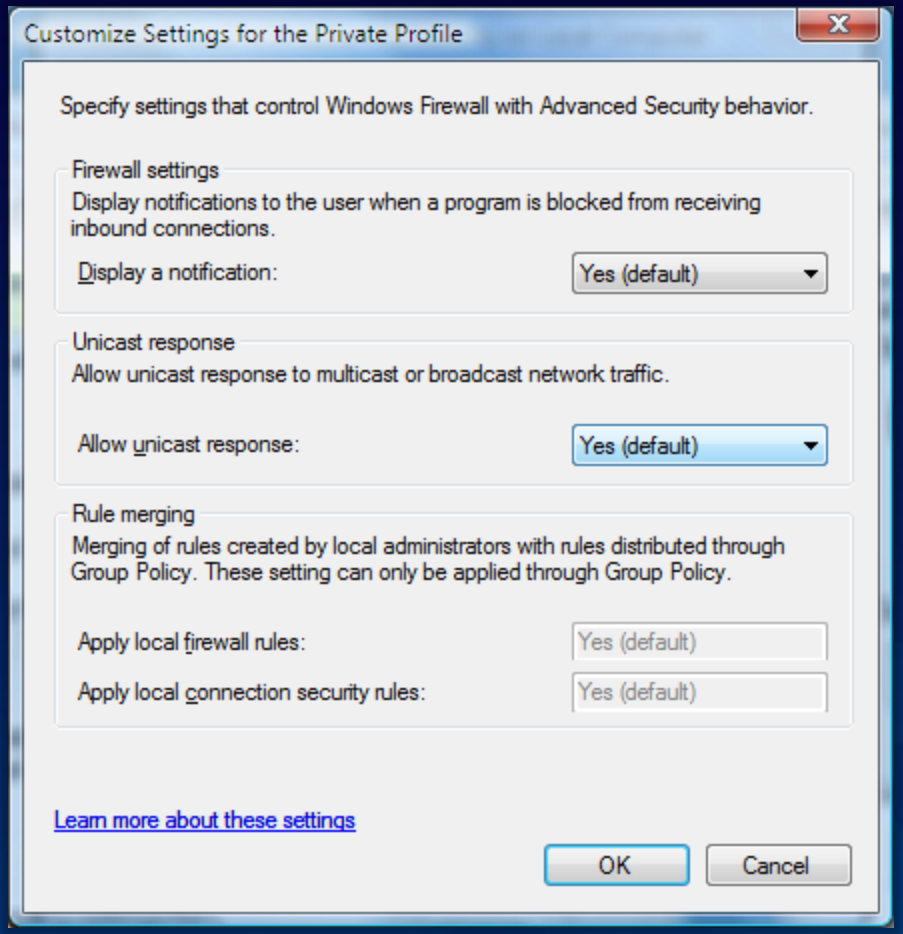
- Import Policy...
- Export Policy...
- Restore Defaults
- View
- Refresh
- Properties
- Help

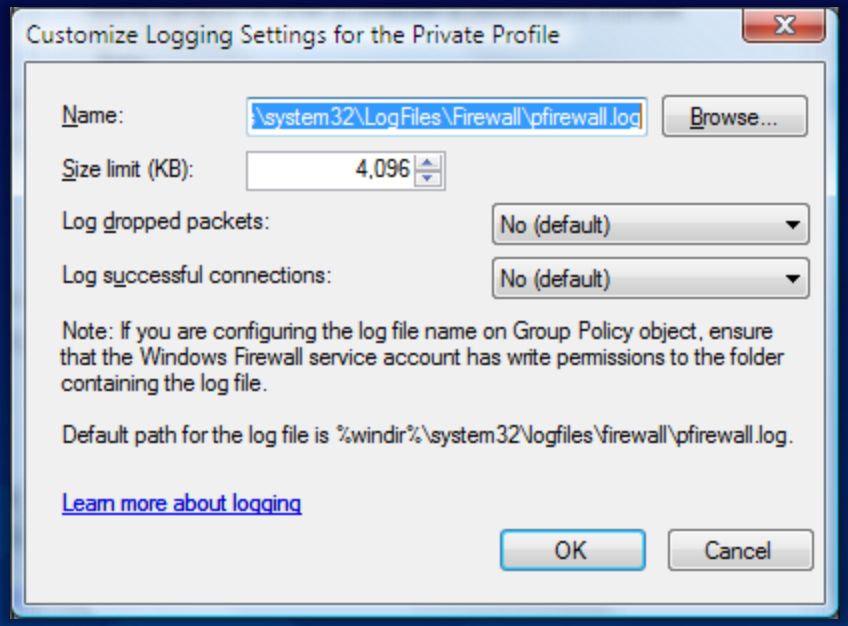
Global settings





Global settings





Creating a rule

Windows Firewall with Advanced Security

File Action View Help

- Windows Firewall with Advance
  - Inbound Rules
  - Outbound Rules
  - Connection Security Rules
  - Monitoring

Inbound Rules

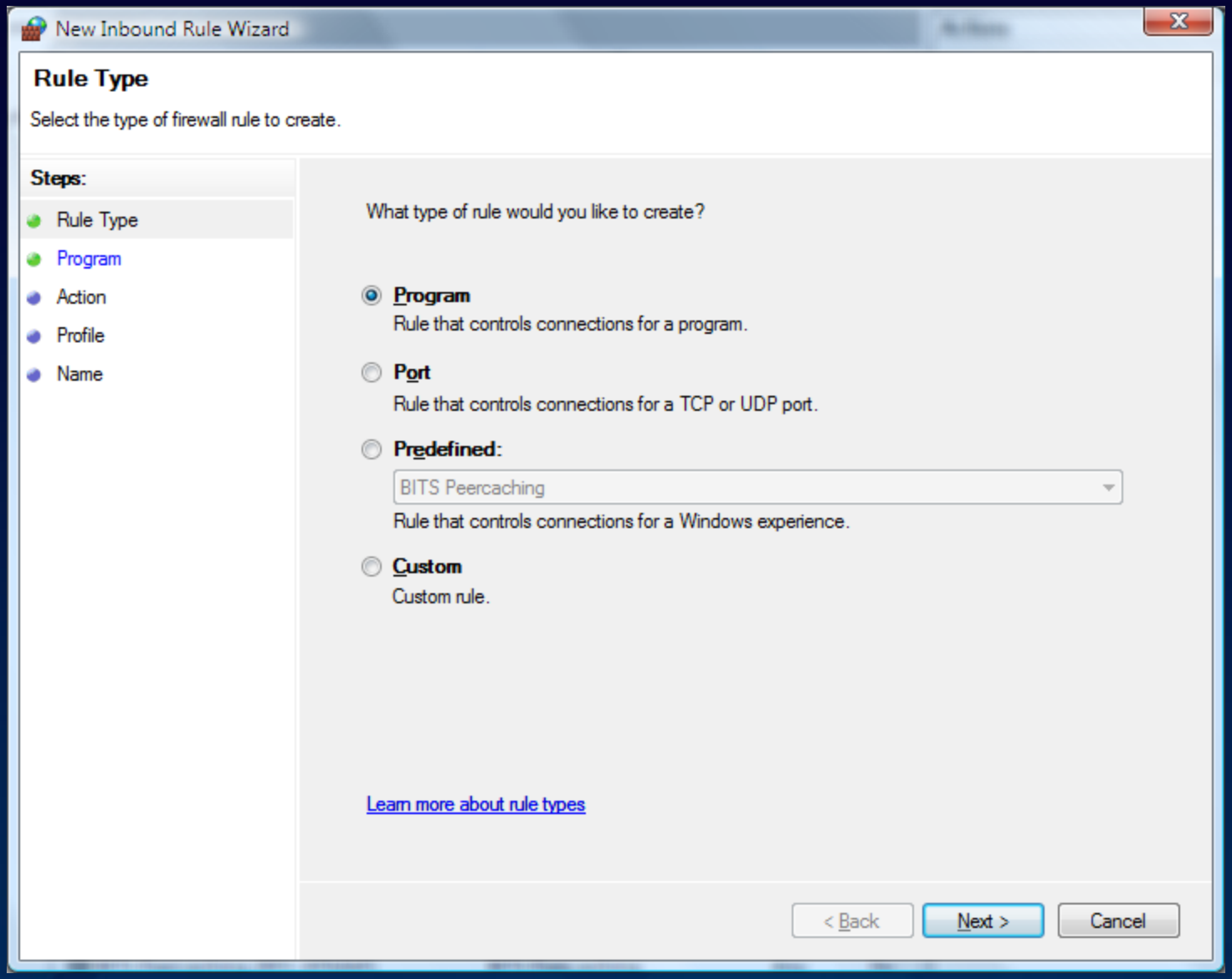
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Allowed Users	Allowed Computers
Communicator		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Communicator		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Dungeon Siege 2 Game Executable		Public	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Dungeon Siege 2 Game Executable		Public	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
File Transfer Program		Domain	Yes	Allow	No	C:\windo...	Any	Any	TCP	Any	Any	Any	Any
File Transfer Program		Domain	Yes	Allow	No	C:\windo...	Any	Any	UDP	Any	Any	Any	Any
Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any	Any
Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any	Any	Any
Microsoft Office Outlook		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	6004	Any	Any	Any
Rise of Nations		Private	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Rise of Nations		Private	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Windows Live Messenger 8.0		Private	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Windows Live Messenger 8.0		Private	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Private	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Windows Live Messenger 8.0 (Phone)		Private	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Yahoo! FT Server		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Yahoo! FT Server		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Yahoo! Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any	Any
Yahoo! Messenger		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any	Any	Any
Yahoo! Messenger		Domain	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Yahoo! Messenger		Domain	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
BITS Peercaching (Content-In)	BITS Peercaching	Any	No	Allow	No	System	Any	Local subnet	TCP	2178	Any	Any	Any
BITS Peercaching (RPC)	BITS Peercaching	Any	No	Allow	No	%System...	Any	Local subnet	TCP	Dynamic...	Any	Any	Any
BITS Peercaching (RPC-EPMAP)	BITS Peercaching	Any	No	Allow	No	%System...	Any	Local subnet	TCP	RPC End...	Any	Any	Any
BITS Peercaching (WSD-In)	BITS Peercaching	Any	No	Allow	No	%System...	Any	Local subnet	UDP	3702	Any	Any	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private, Public	No	Allow	No	%System...	Any	Local subnet	TCP	Any	Any	Any	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow	No	System	Any	Any	TCP	5357	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private, Public	No	Allow	No	System	Any	Local subnet	TCP	5357	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow	No	System	Any	Any	TCP	5358	Any	Any	Any
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private, Public	No	Allow	No	System	Any	Local subnet	TCP	5358	Any	Any	Any
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	Any	No	Allow	No	%System...	Any	Local subnet	UDP	3702	Any	Any	Any
Core Networking - Destination Unreacha...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Destination Unreacha...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any	Any
Core Networking - Dynamic Host Config...	Core Networking	Any	Yes	Allow	No	%System...	Any	Any	UDP	68	Any	Any	Any
Core Networking - Internet Group Mana...	Core Networking	Any	Yes	Allow	No	System	Any	Any	IGMP	Any	Any	Any	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	Any	Yes	Allow	No	System	Any	Any	IPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Do...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Qu...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Neighbor Discovery A...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Neighbor Discovery S...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Packet Too Big (ICMP...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Parameter Problem (I...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Router Advertisement...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Teredo (UDP-In)	Core Networking	Any	Yes	Allow	No	%System...	Any	Any	UDP	Edge Tra...	Any	Any	Any
Core Networking - Time Exceeded (ICMP...	Core Networking	Any	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	Domain	No	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	Private, Public	No	Allow	No	%System...	Any	Local subnet	TCP	Any	Any	Any	Any

Actions

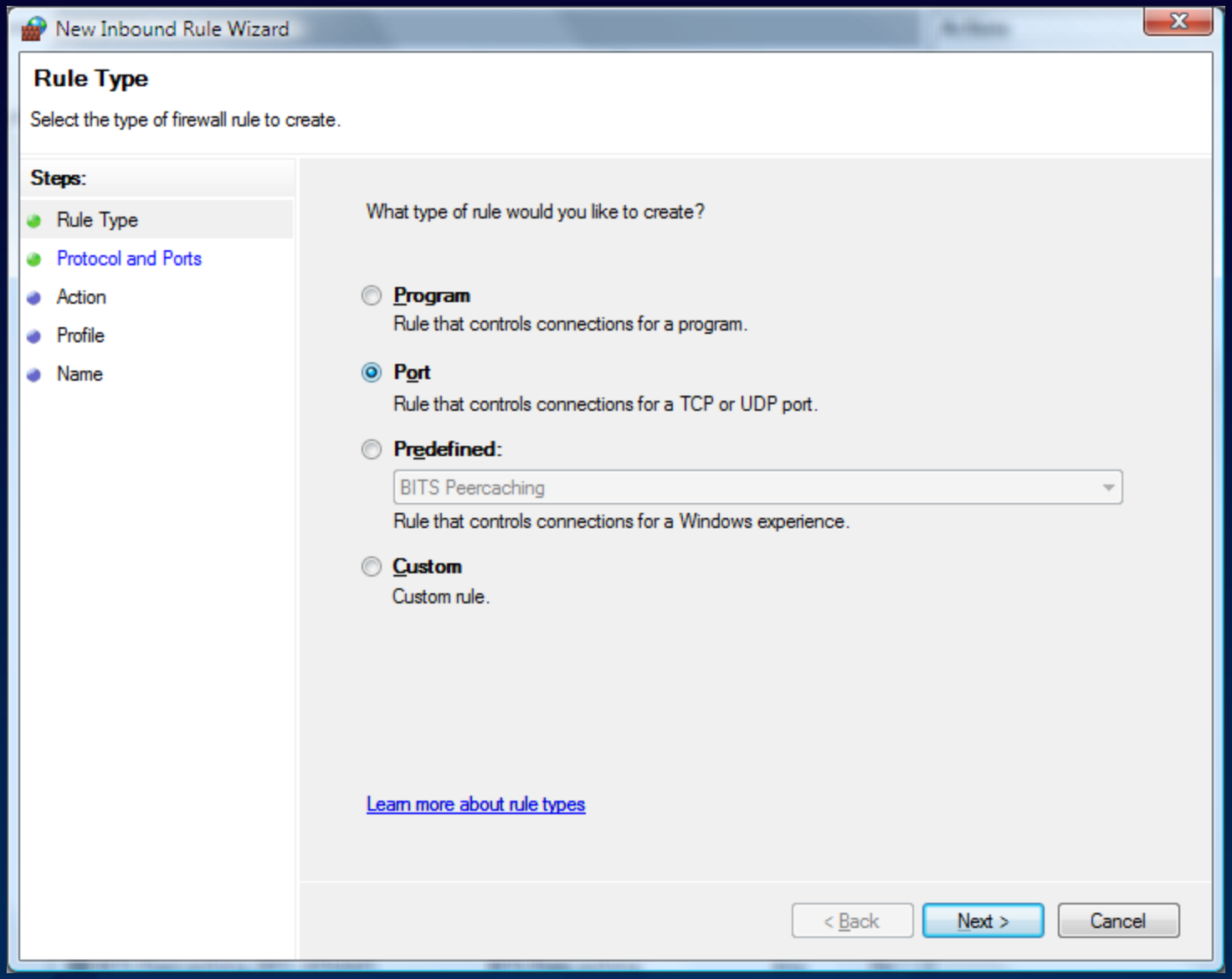
Inbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Communicator
- Disable Rule
- Delete
- Properties
- Help

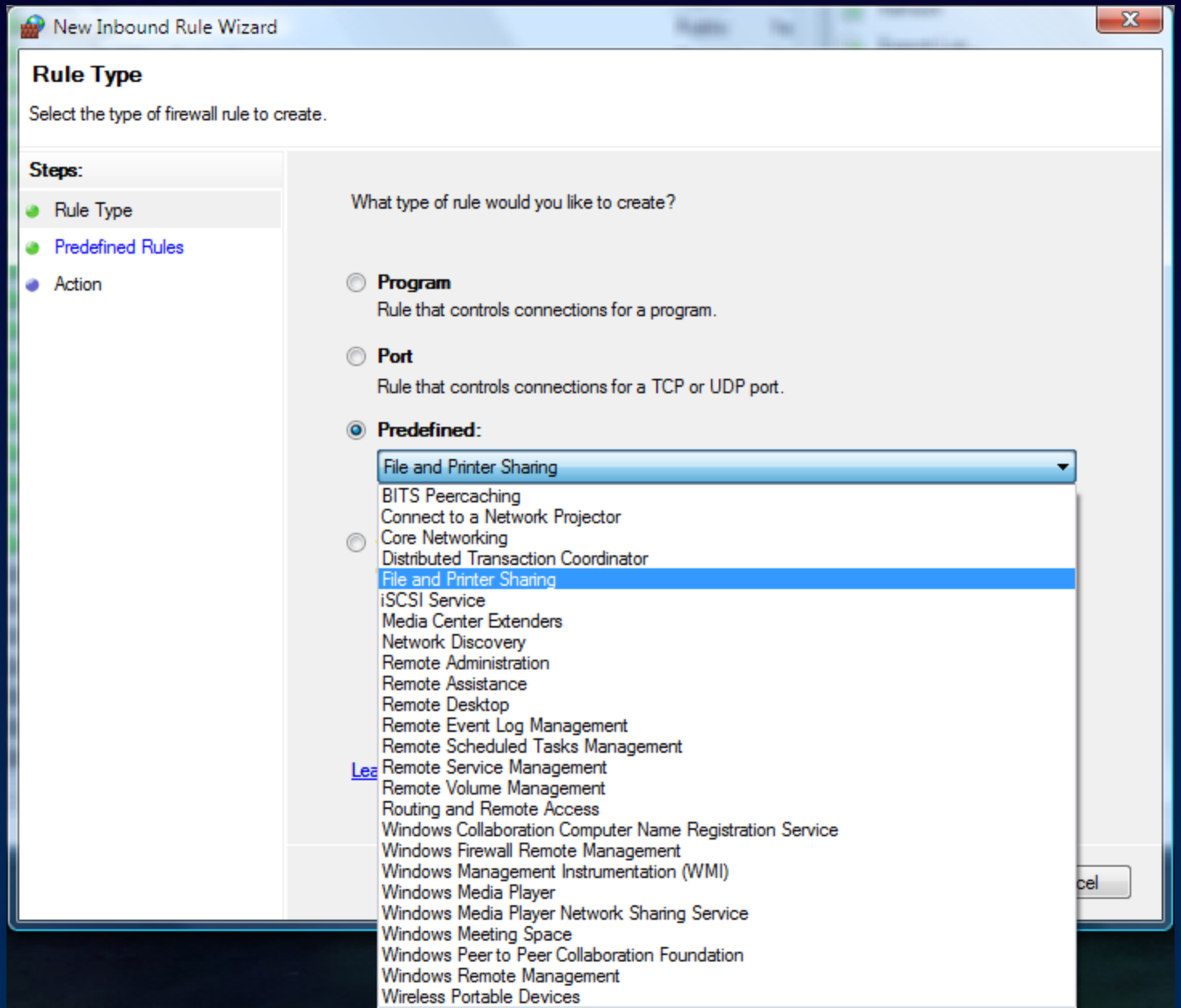
Rule types


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
BITS Peercaching
Rule that controls connections for a Windows experience.
Custom
Custom rule.
Learn more about rule types
< Back
Next >
Cancel

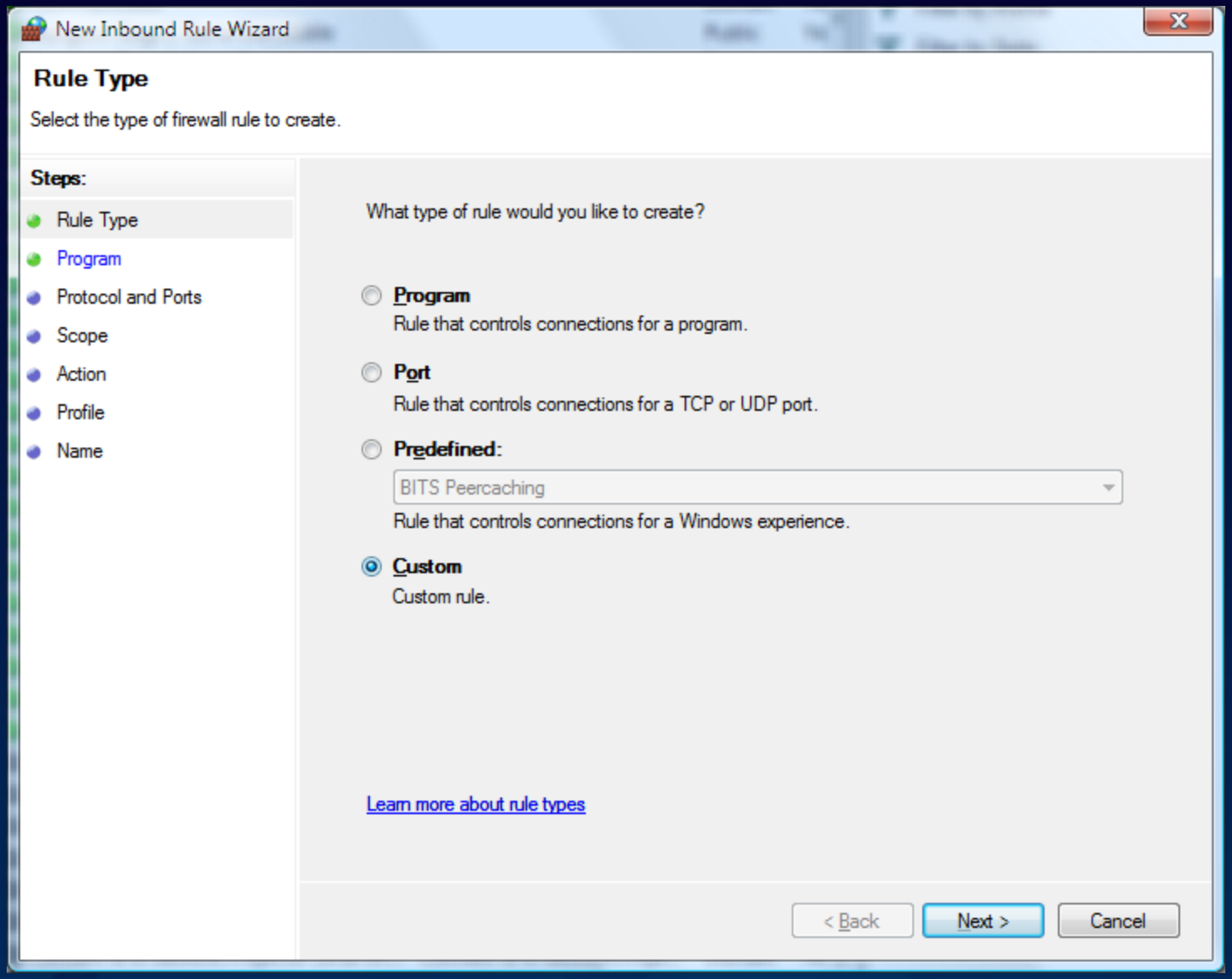
Rule types


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
BITS Peercaching
Rule that controls connections for a Windows experience.
Custom
Custom rule.
Learn more about rule types
< Back
Next >
Cancel

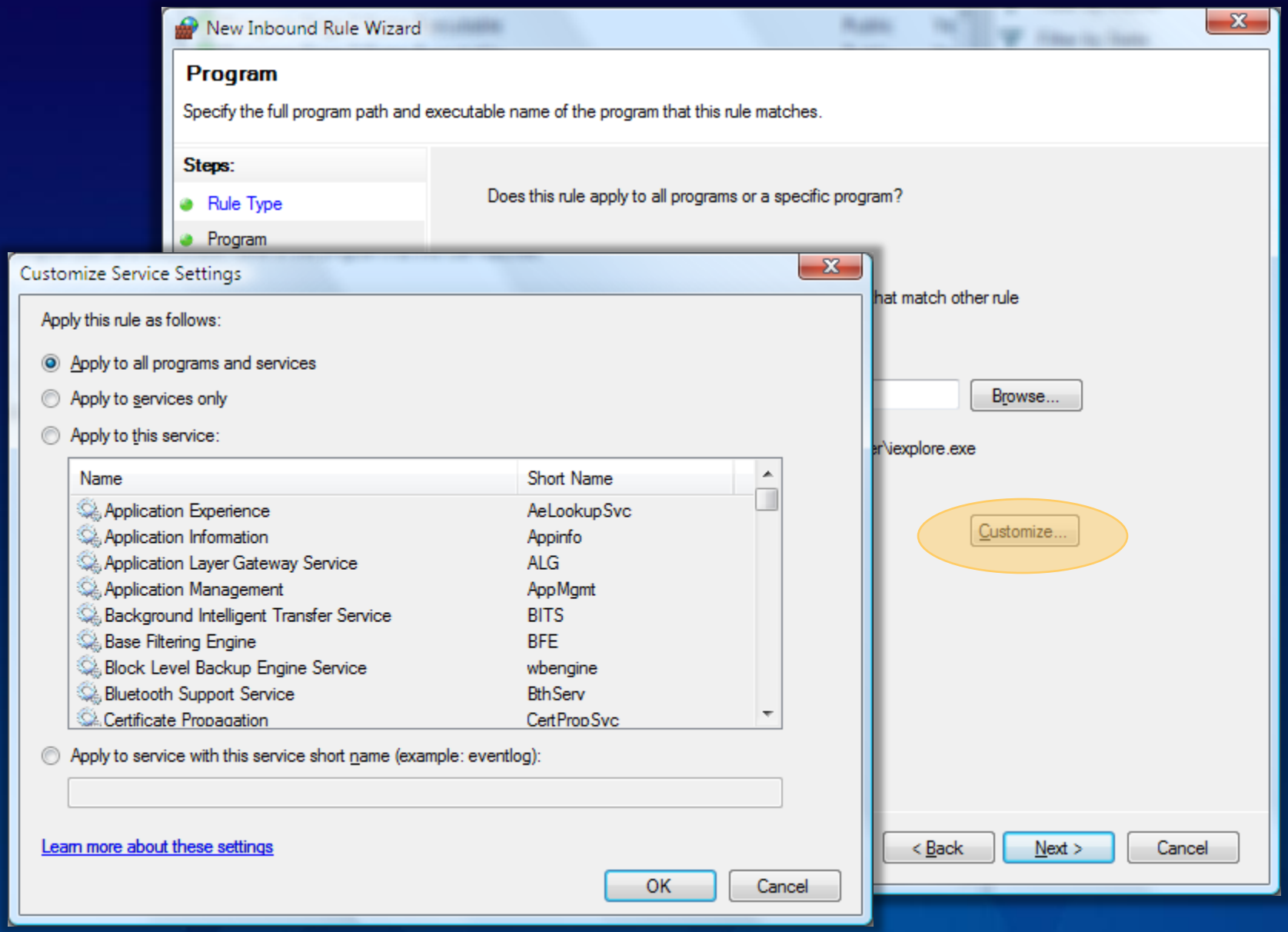
Rule types


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Predefined Rules
Action
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
File and Printer Sharing
BITS Peercaching
Connect to a Network Projector
Core Networking
Distributed Transaction Coordinator
File and Printer Sharing
iSCSI Service
Media Center Extenders
Network Discovery
Remote Administration
Remote Assistance
Remote Desktop
Remote Event Log Management
Remote Scheduled Tasks Management
Remote Service Management
Remote Volume Management
Routing and Remote Access
Windows Collaboration Computer Name Registration Service
Windows Firewall Remote Management
Windows Management Instrumentation (WMI)
Windows Media Player
Windows Media Player Network Sharing Service
Windows Meeting Space
Windows Peer to Peer Collaboration Foundation
Windows Remote Management
Wireless Portable Devices

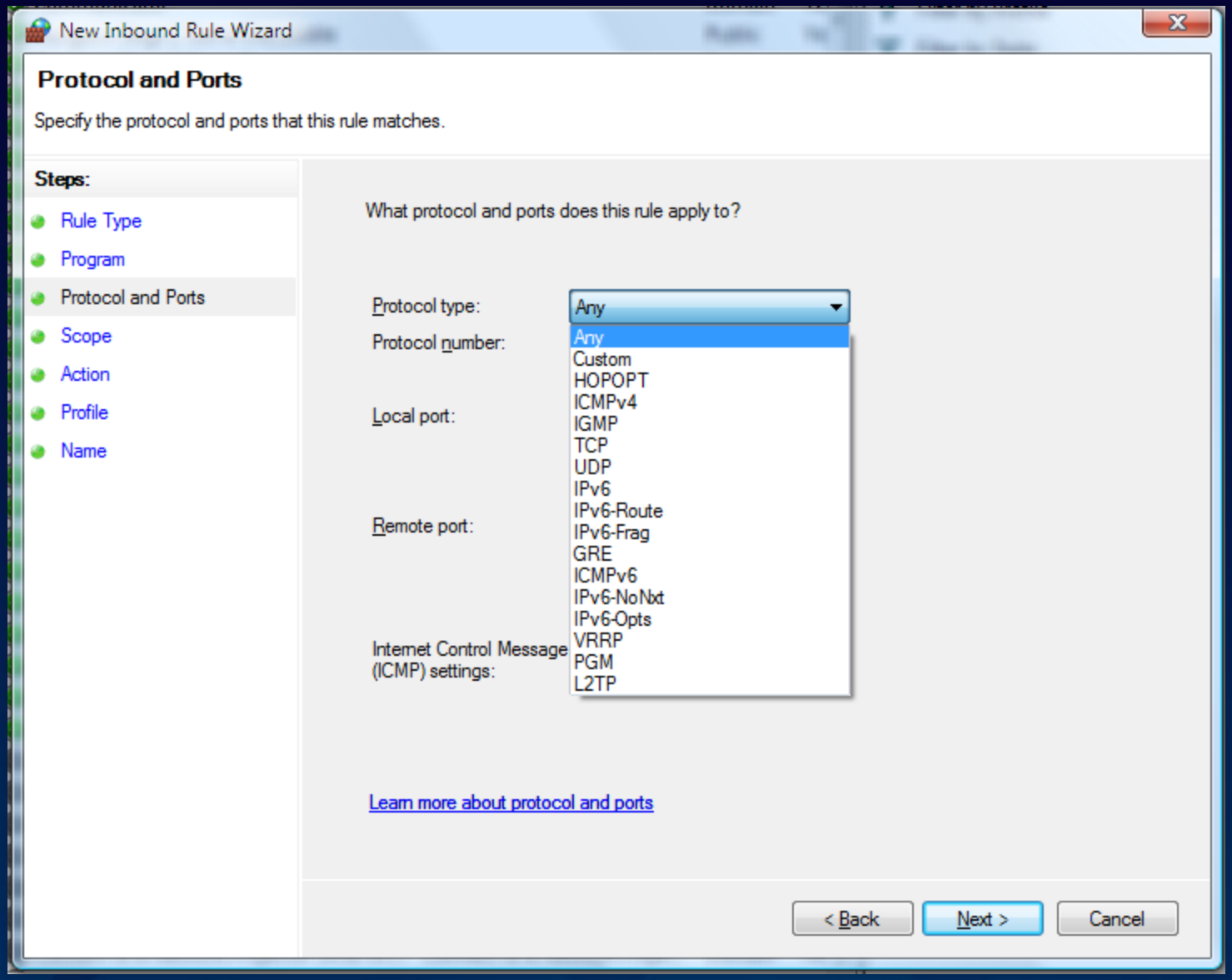
Rule types


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
BITS Peercaching
Rule that controls connections for a Windows experience.
Custom
Custom rule.
Learn more about rule types
< Back
Next >
Cancel

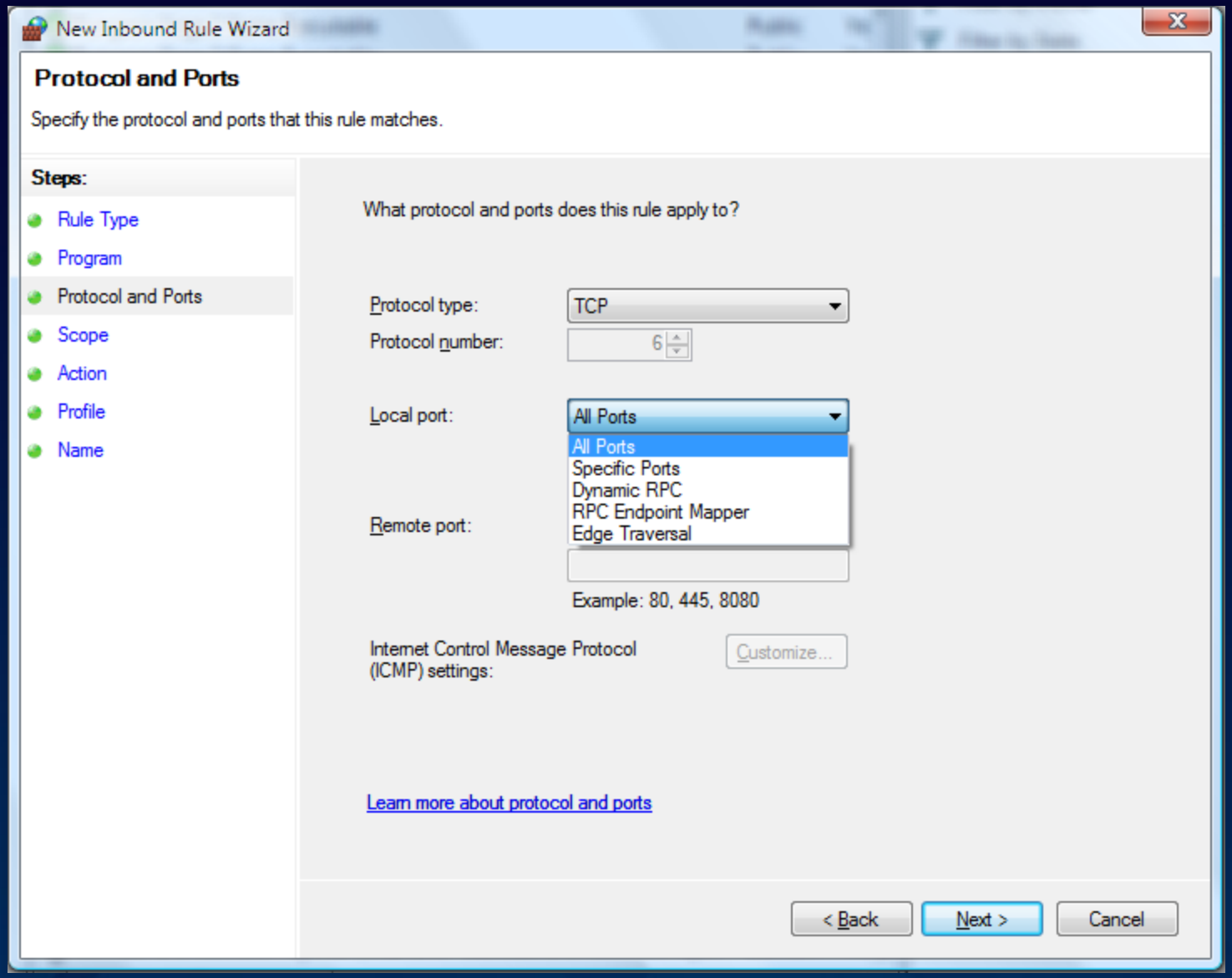
Program rule



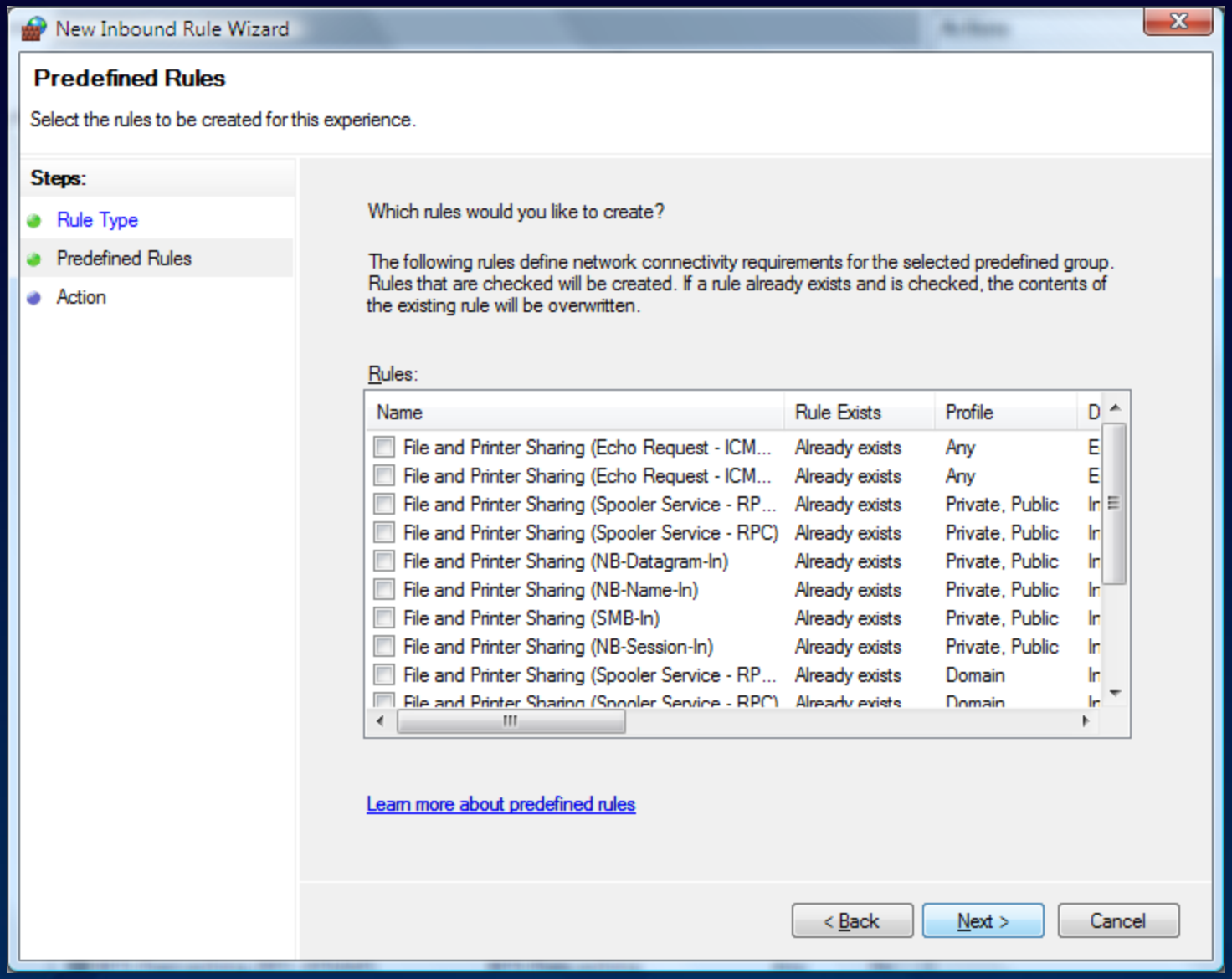
Port rule


New Inbound Rule Wizard
Protocol and Ports
Specify the protocol and ports that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What protocol and ports does this rule apply to?
Protocol type:
Any
Protocol number:
Any
Custom
HOPOPT
ICMPv4
IGMP
TCP
UDP
IPv6
IPv6-Route
IPv6-Frag
GRE
ICMPv6
IPv6-NoNxt
IPv6-Opts
VRRP
PGM
L2TP
Local port:
Remote port:
Internet Control Message (ICMP) settings:
Learn more about protocol and ports
< Back
Next >
Cancel

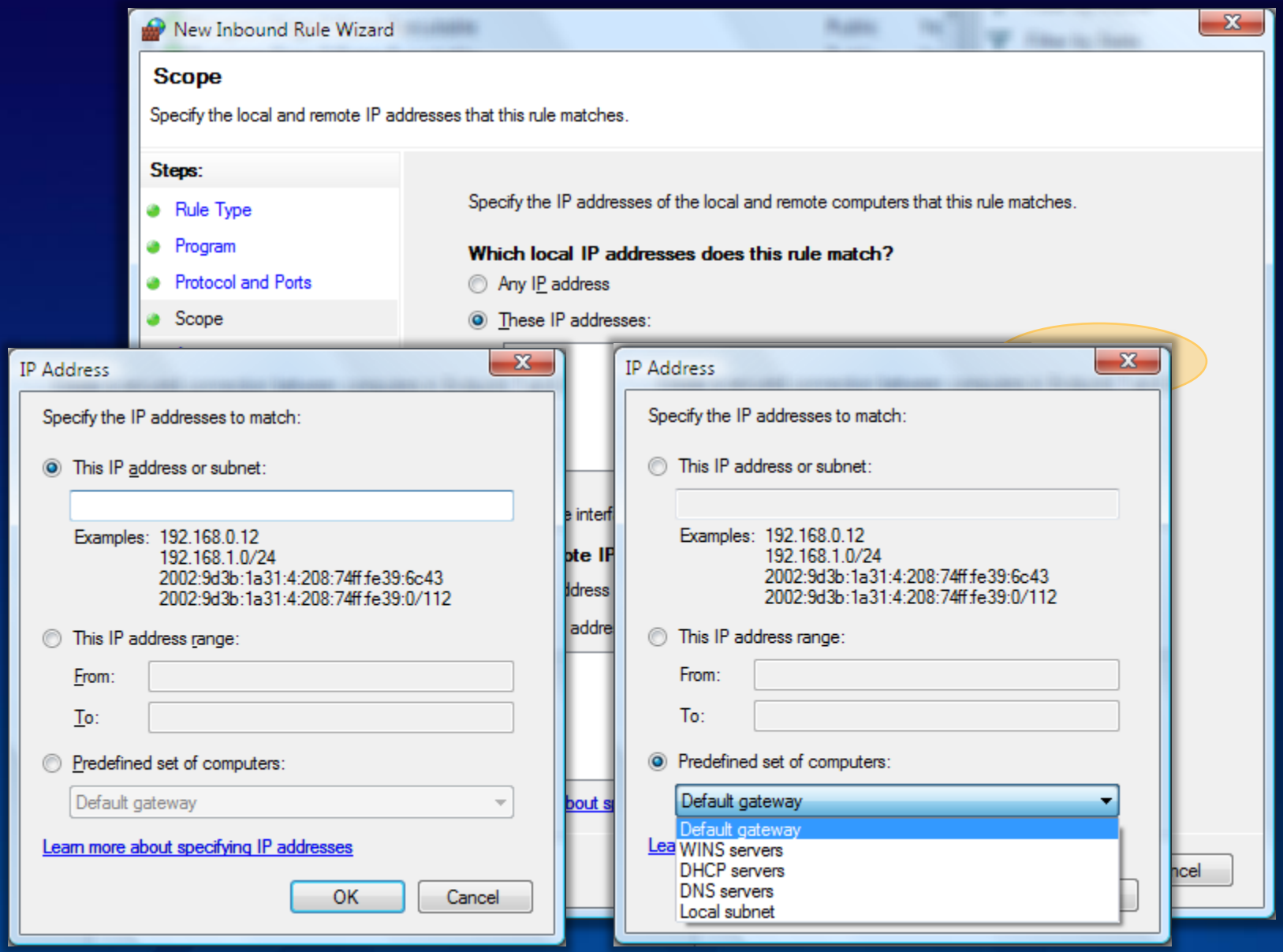
Port rule


New Inbound Rule Wizard
Protocol and Ports
Specify the protocol and ports that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What protocol and ports does this rule apply to?
Protocol type:
TCP
Protocol number:
6
Local port:
All Ports
All Ports
Specific Ports
Dynamic RPC
RPC Endpoint Mapper
Edge Traversal
Remote port:
Example: 80, 445, 8080
Internet Control Message Protocol (ICMP) settings:
Customize...
Learn more about protocol and ports
< Back
Next >
Cancel

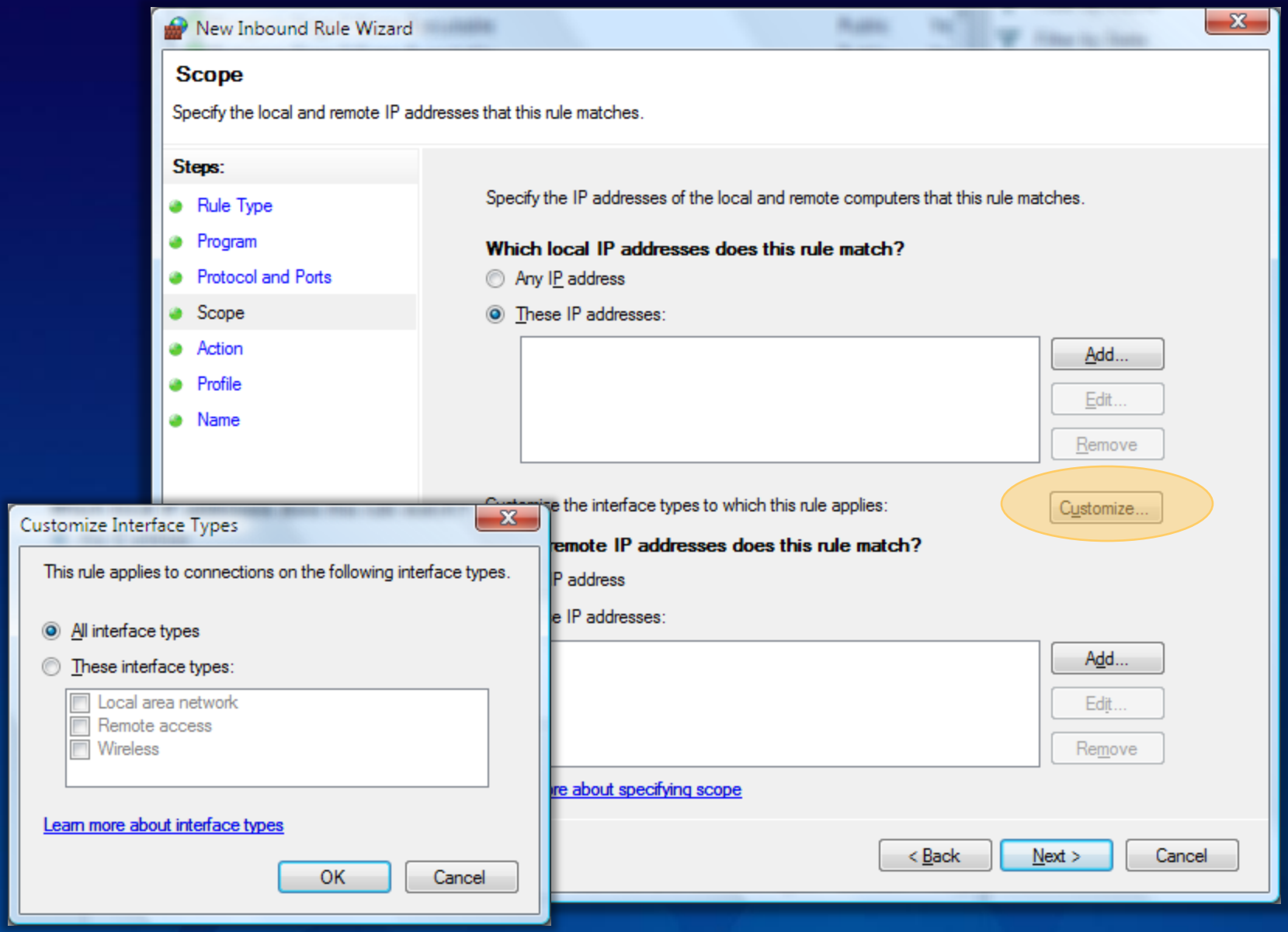
Predefined rules



Scope


New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Specify the IP addresses of the local and remote computers that this rule matches.
Which local IP addresses does this rule match?
Any IP address
These IP addresses:
IP Address
Specify the IP addresses to match:
This IP address or subnet:
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112
This IP address range:
From:
To:
Predefined set of computers:
Default gateway
Learn more about specifying IP addresses
OK
Cancel
IP Address
Specify the IP addresses to match:
This IP address or subnet:
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112
This IP address range:
From:
To:
Predefined set of computers:
Default gateway
Default gateway
WINS servers
DHCP servers
DNS servers
Local subnet

Scope


New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Specify the IP addresses of the local and remote computers that this rule matches.
Which local IP addresses does this rule match?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize...
Customize Interface Types
This rule applies to connections on the following interface types.
All interface types
These interface types:
Local area network
Remote access
Wireless
Learn more about interface types
OK
Cancel
< Back
Next >
Cancel

Action

New Inbound Rule Wizard

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

Allow the connection

Allow connections that have been protected with IPsec as well as those that have not.

Allow the connection if it is secure

Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Require the connections to be encypted

Require privacy in addition to integrity and authentication.

Override block rules

Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

Block the connection

Learn more about actions

< Back | Next > | Cancel

Action - secured with IPsec

New Inbound Rule Wizard

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Users and Computers
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

Allow the connection

Allow connections that have been protected with IPsec as well as those that have not.

Allow the connection if it is secure

Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Require the connections to be encypted

Require privacy in addition to integrity and authentication.

Override block rules

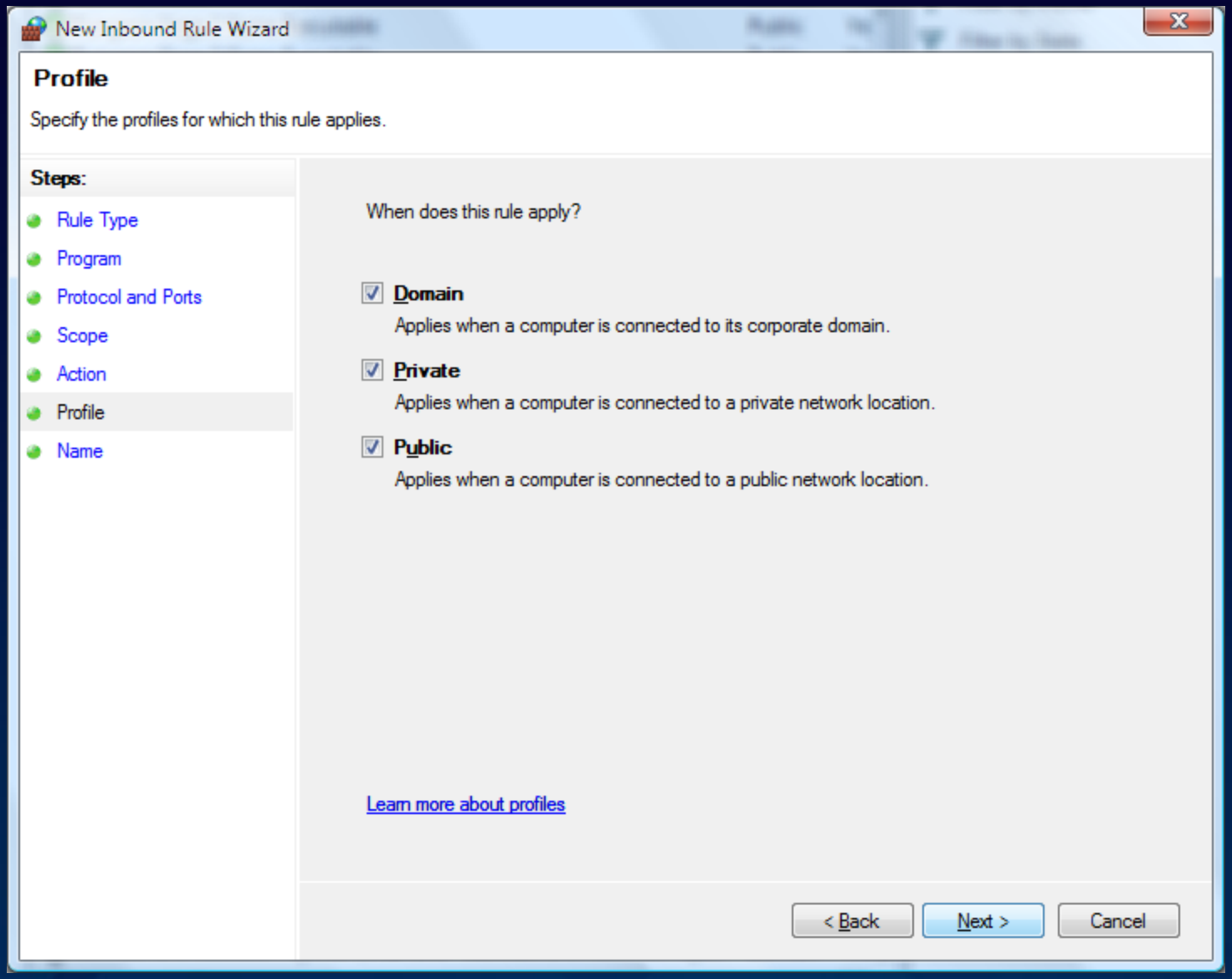
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

Block the connection

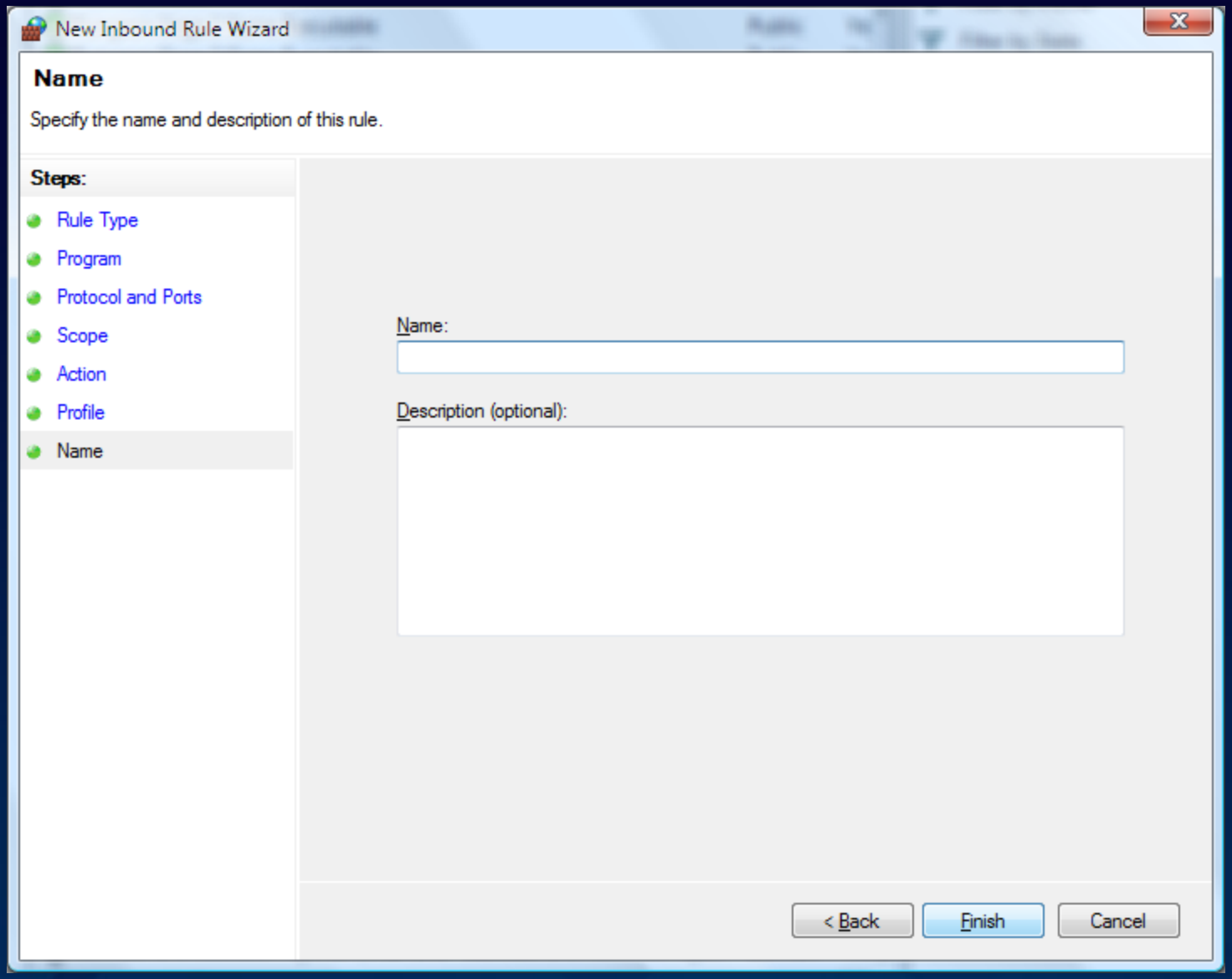
Learn more about actions

< Back | Next > | Cancel

Profile


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location.
Public
Applies when a computer is connected to a public network location.
Learn more about profiles
< Back
Next >
Cancel

Name


New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
Description (optional):
< Back
Finish
Cancel

Programmatic interfaces

- INetFwPolicy2
  - Provides access to the policy
- INetFwRule
  - Provides access to rule properties
- INetFwRules
  - Provides access to a collection of firewall or Windows Service Hardening rules
- INetFwServceRestriction
  - Provides access to the Windows Service Policy

Is the firewall enabled?

```
option explicit
Dim CurrentProfile
' Create the FwPolicy2 object.
Dim fwPolicy2
Set fwPolicy2 = CreateObject("HNetCfg.FwPolicy2")
CurrentProfile = fwPolicy2.CurrentProfileTypes
if fwPolicy2.FirewallEnabled(CurrentProfile) <> TRUE then
    WScript.Echo("Firewall is disabled.")
else
    WScript.Echo("Firewall is enabled.")
end if
```

netsh advfirewall

- Full configuration interface
- Scriptable
  - Dump rules
  - Export rules
  - Import rules
  - Create rules
- Contexts for firewall rules and IPsec (connection security) rules
- Set and show global and per-profile properties
- Display active state (firewall rules, IPsec rules and security associations)

IPSec

- Simplified policy configuration
- Client-to-DC protection
- Improved support for load balancing and clustering
- Improved authentication
- More cryptographic suites
- New configuration options
- More events and counters

Integrated with the firewall

- Eliminates confusion and rule overlap
- All firewall rules can be IPsec aware

"Allow application *foo* to receive traffic on port *bar* only if it's authenticated (and optionally encrypted) by IPsec"

"Allow service *foo* to receive traffic from a remote computer or a remote user only if it's identified by IKE"

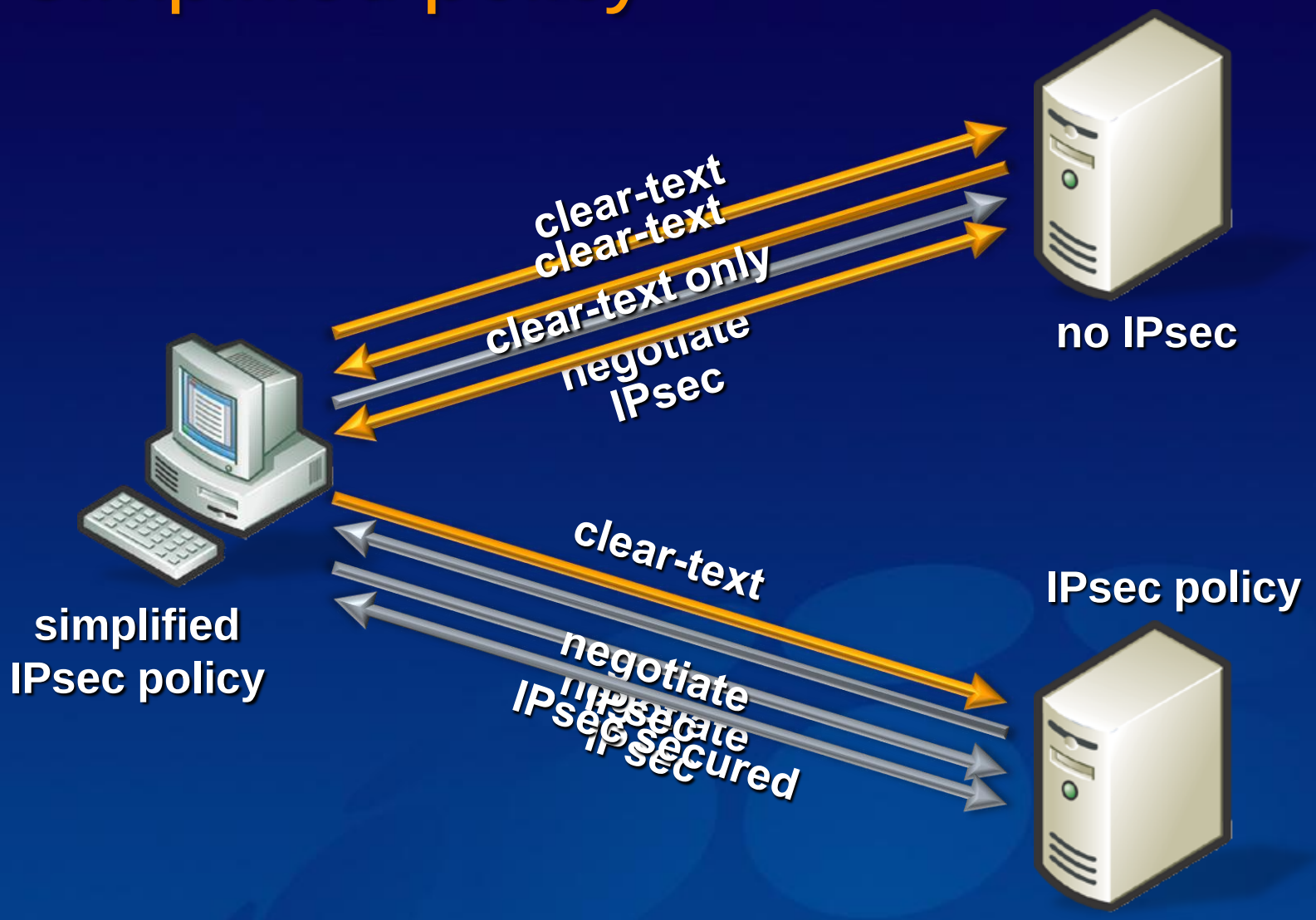
Isolation: authentication

- Here’s your wizard for server and domain isolation
  - Request authN for inbound and outbound
  - Require authN for inbound, request for outbound
  - Require authN for inbound and outbound
- Authentication types
  - Computer and user (with Kerberos)
  - Computer (with Kerberos)
  - Computer certificate
  - Health certificate (NAP)
  - Combinations

Simplified policy

- Initiator communicates to responder simultaneously in clear-text and with IPsec
  - Switch to IPsec if responder can support
  - Remain clear-text if not
- Eliminates delay issues with current “fall back to clear” implementation
- Eliminates need to create policies filled with exceptions for non-IPsec devices

Simplified policy



Working with domain controllers

Configuring IPsec on DCs…	*…will result in this*
Request	• Domain joins and logons in clear text • Subsequent communications protected
Require	• Domain joins will require entering user ID and password of a domain account • Works only on Windows Vista clients

New cryptographic algorithms

Encryption	• AES-128 • AES-192 • AES-256
Key exchange	• P-256 (DH group 19 elliptic curve) • P-384 (DH group 20 elliptic curve)

Improved authentication

- Require a health certificate
- New “extended mode”
  - IKE extension known as AuthIP
  - User authentication: Kerberos, NTLMv2, certificate
  - Health certificates use extended mode
- Multiple methods tried
  - Doesn’t give up after first fails
  - Tried in the specified order
  - Allows for differing authentication and crypto sets on individual SAs between a pair of peers

Rule actions

Inbound		*Outbound*
Reject if IPsec fails	Secure	Reject if IPsec fails
Reject if IPsec fails	Secure server	Negotiate
Negotiate	DMZ	Negotiate
Proceed in clear	Do not secure	Proceed in clear

More flexible exceptions

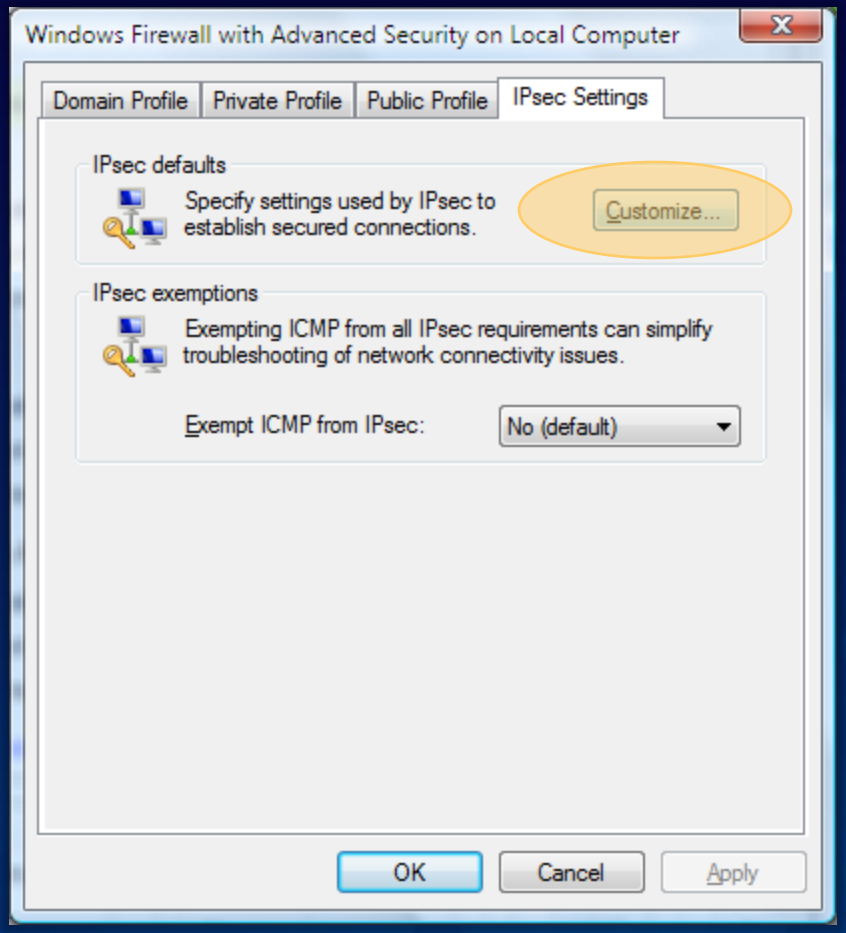
Active Directory user/computer accounts and groups
Source and destination IP addresses (individual or range)
Source and destination TCP/UDP ports
Comma-delimited list of ports (but not low-high range)
IP protocol number
Types of interfaces (wired, wireless, VPN)
ICMP type and code
Services (used by service profiling to limit access)

- Most require IPsec-aware firewall rules to configure (can't be configured through connection security rules)

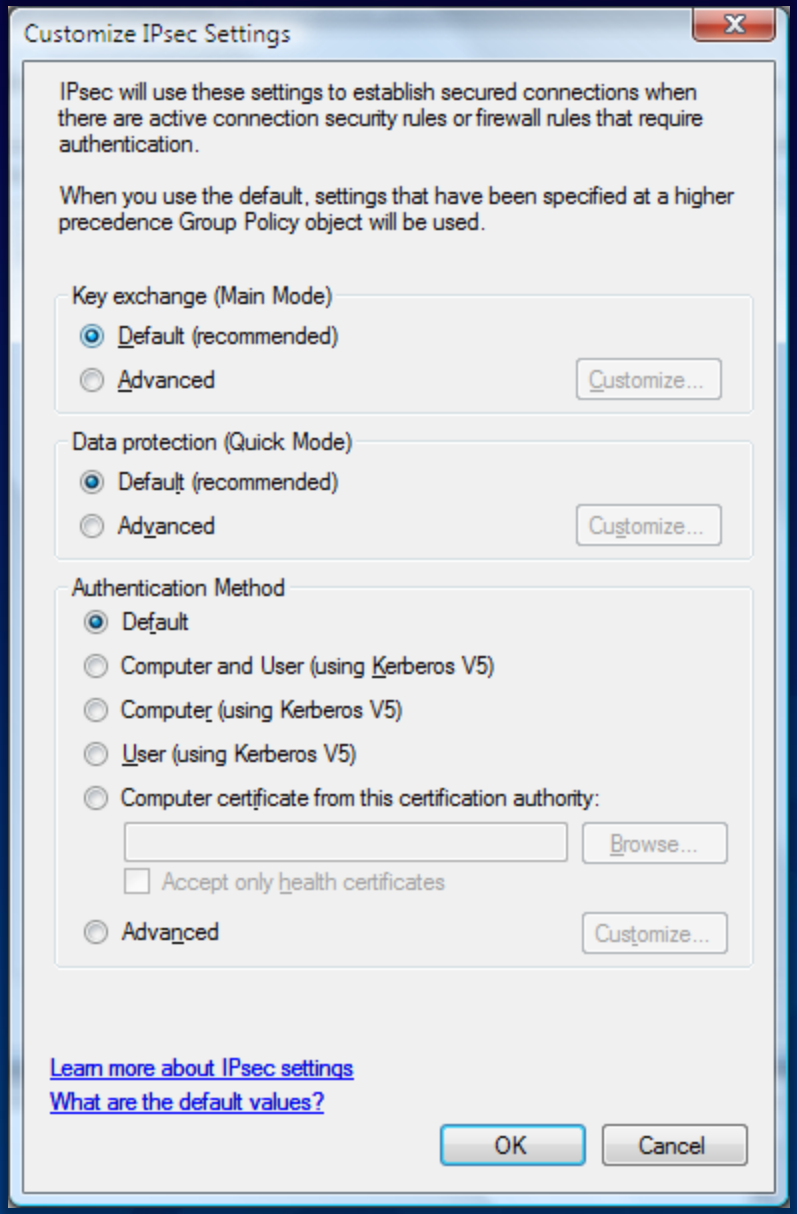
More about rules

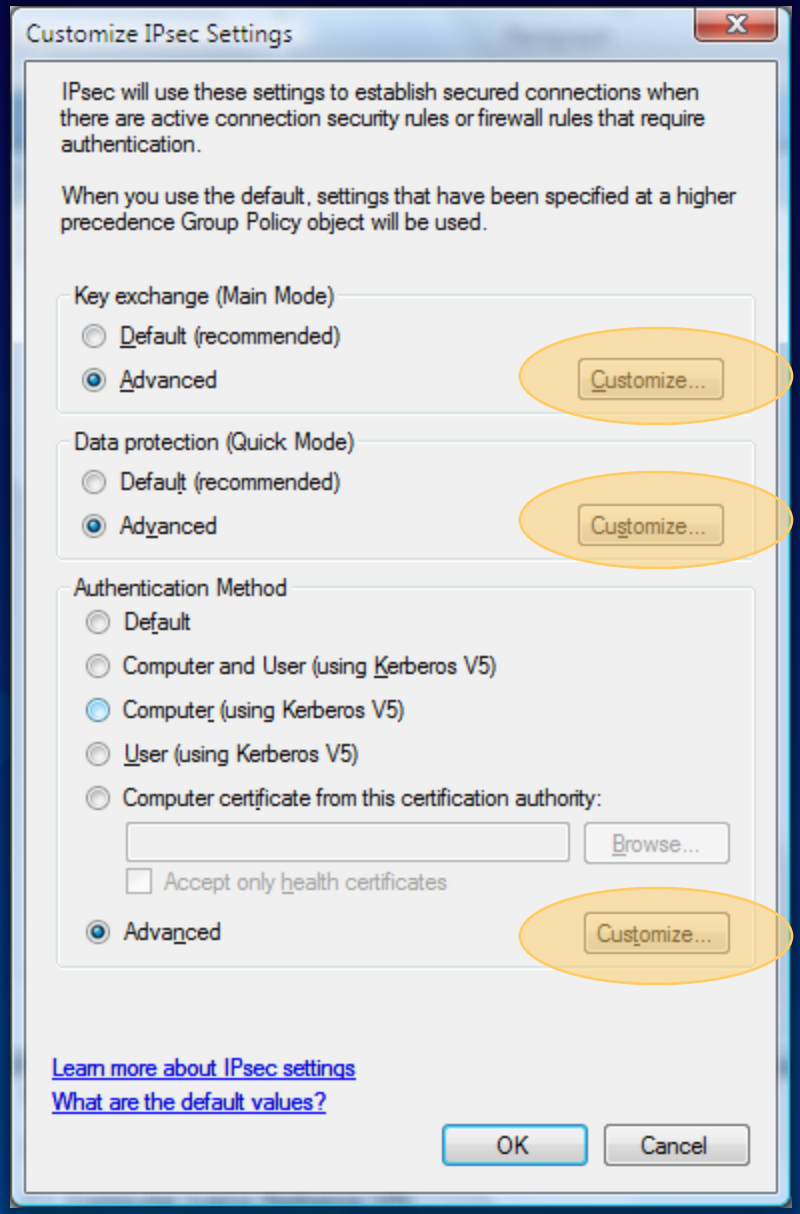
- Ordering: same as current Windows
  - Ordered by specificity
  - ❶ AuthN bypass ❷ Block ❸ Allow
- Authenticated rules: firewall rules that are aware of IPsec protection
  - Make filtering decisions based on SAs
  - Do *not* control creating SAs: you must still write the IPsec rules to create the SA

Global settings

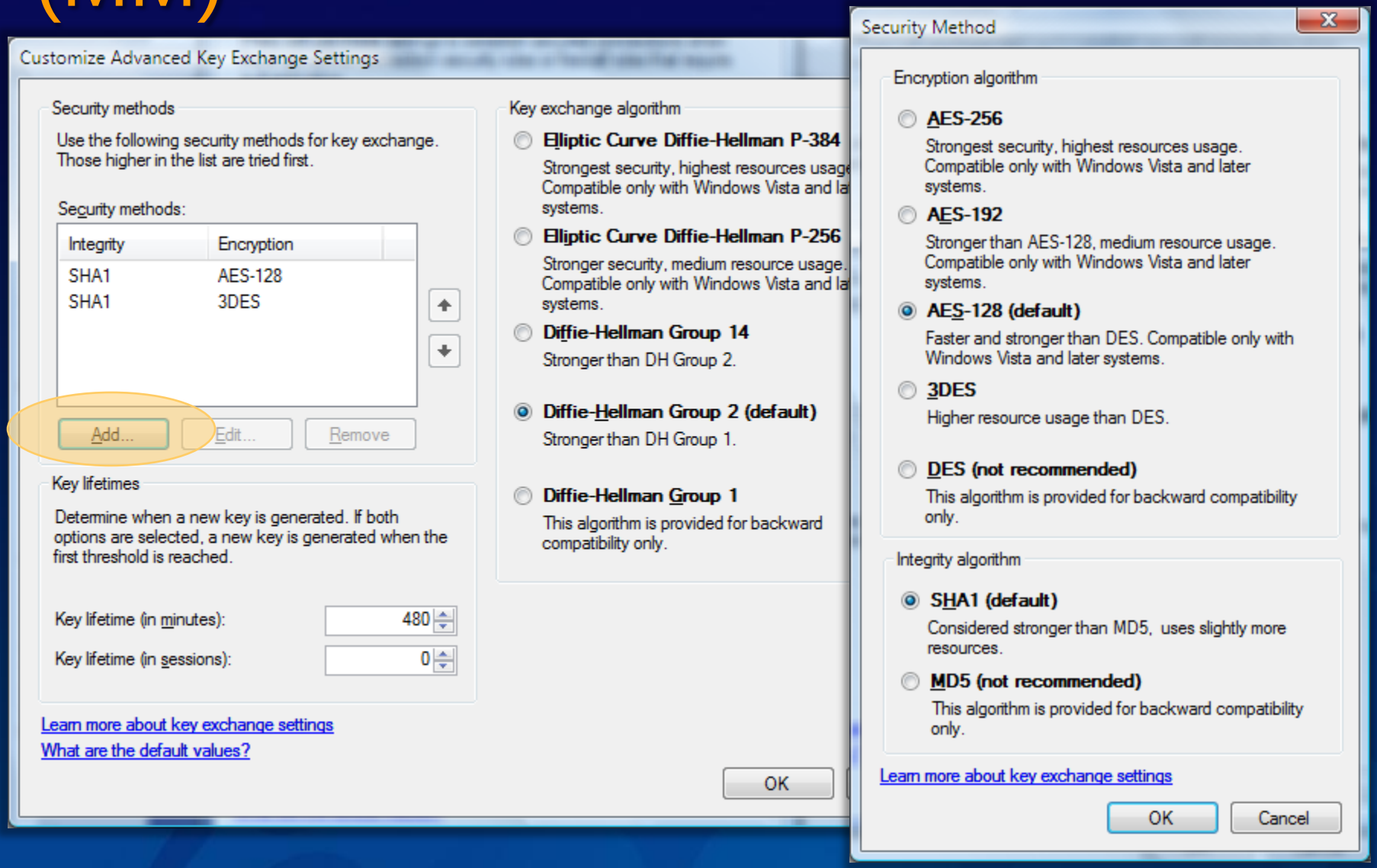


Global settings

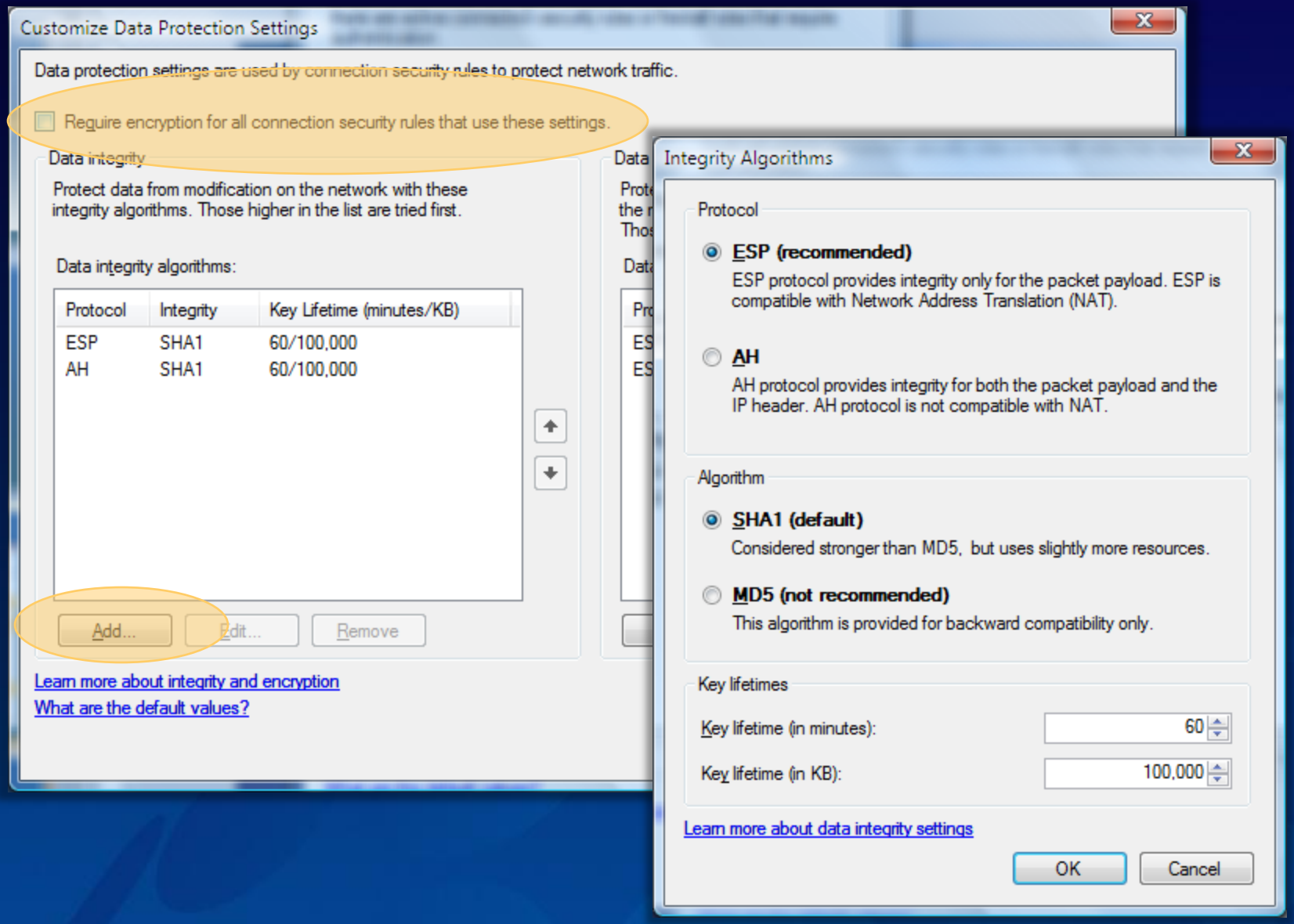




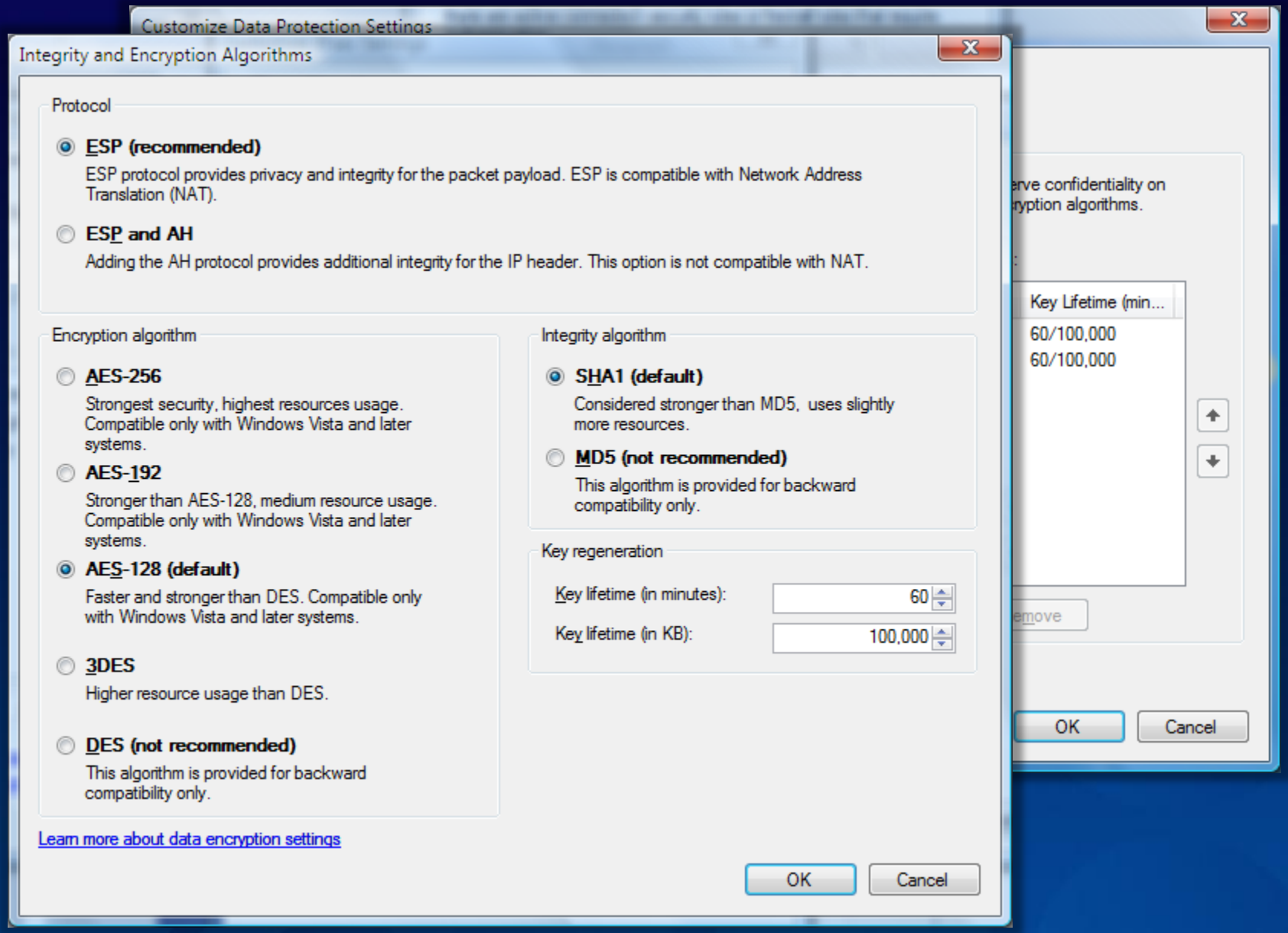
Global settings - key exchange (MM)



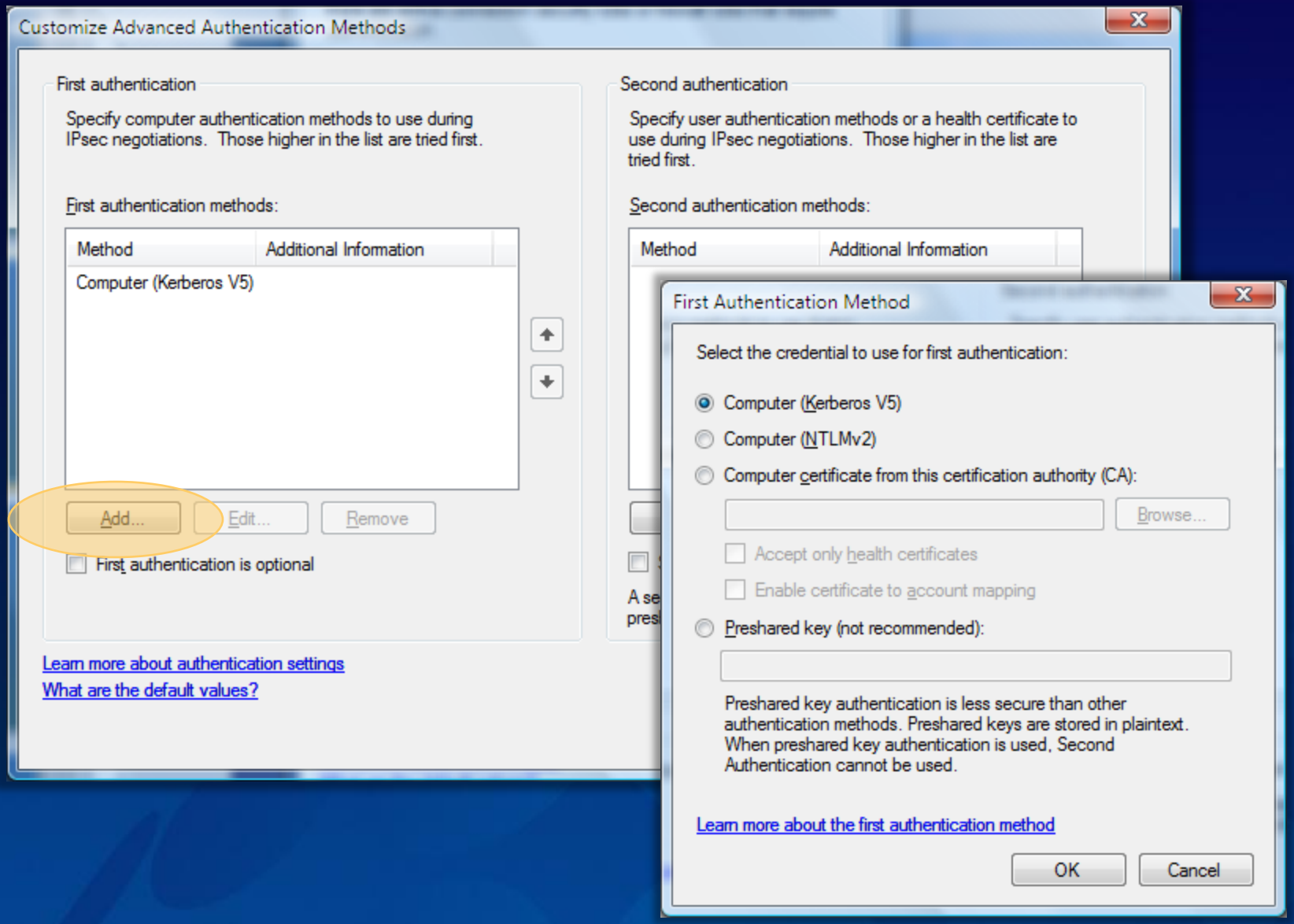
Global settings - data protection (QM)



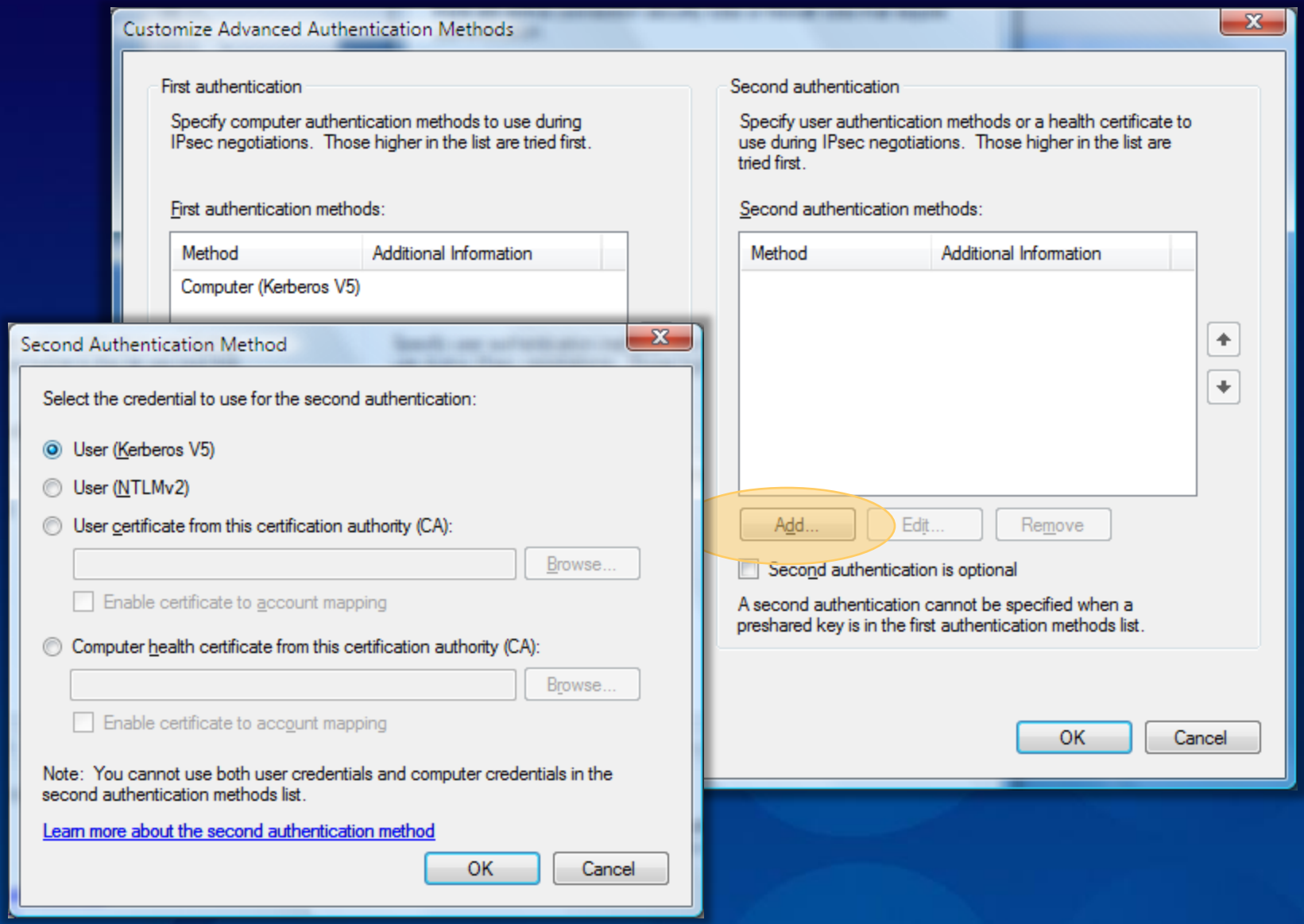
Global settings - data protection (QM)



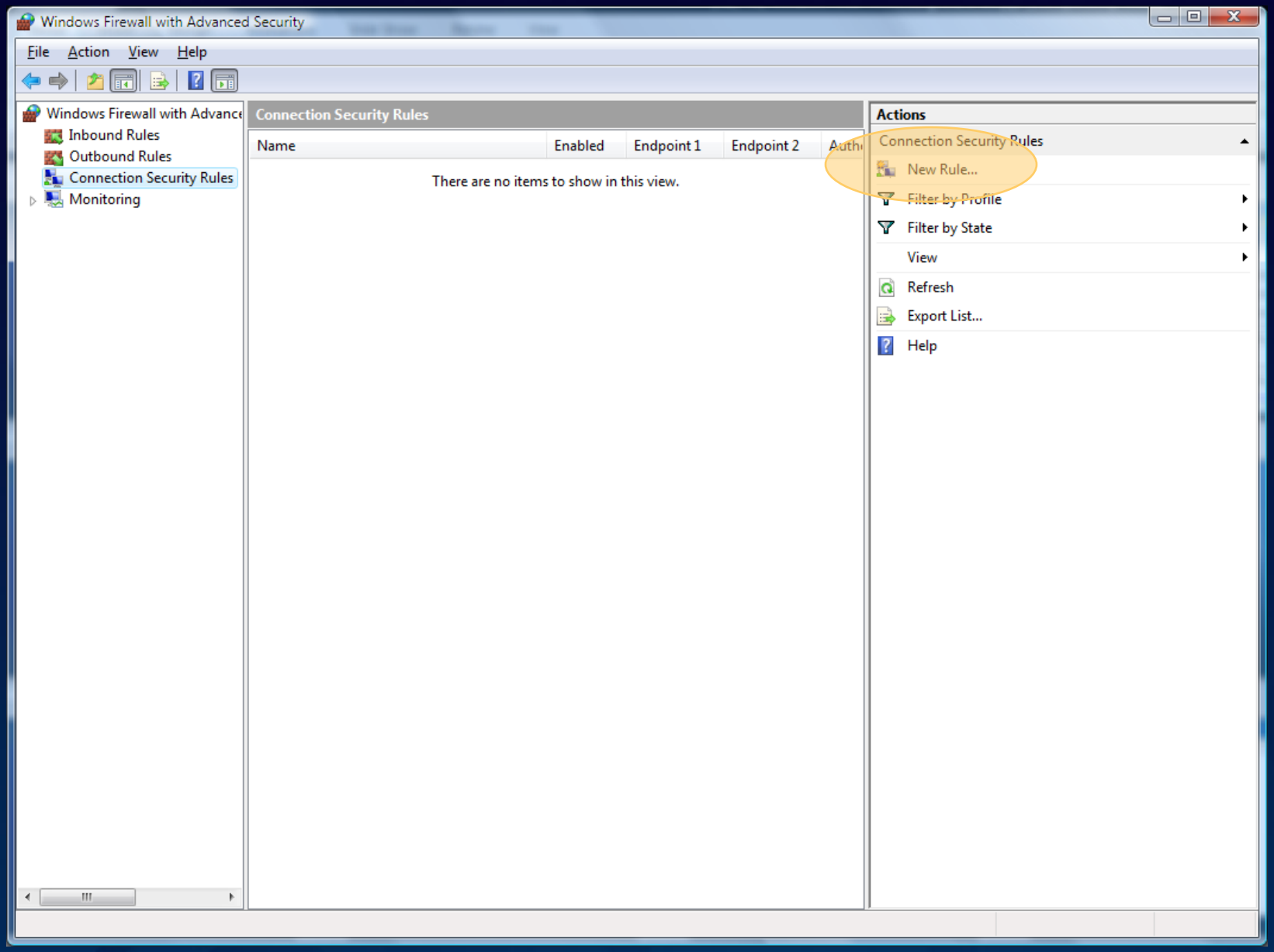
Global settings - authentication



Global settings - authentication



Connection security rules



New rule

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

- (selected) **Isolation**
  Restrict connections based on authentication criteria, such as domain membership or health status.
- **Authentication exemption**
  Do not authenticate connections from the specified computers.
- **Server-to-server**
  Authenticate connection between the specified computers.
- **Tunnel**
  Authenticate connections between gateway computers.
- **Custom**
  Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

Learn more about rule types

< Back | Next > | Cancel

New rule

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Exempt Computers
- Profile
- Name

What type of connection security rule would you like to create?

Isolation
Restrict connections based on authentication criteria, such as domain membership or health status.

Authentication exemption
Do not authenticate connections from the specified computers.

Server-to-server
Authenticate connection between the specified computers.

Tunnel
Authenticate connections between gateway computers.

Custom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

Learn more about rule types

< Back | Next > | Cancel

New rule

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

Isolation
Restrict connections based on authentication criteria, such as domain membership or health status.

Authentication exemption
Do not authenticate connections from the specified computers.

Server-to-server
Authenticate connection between the specified computers.

Tunnel
Authenticate connections between gateway computers.

Custom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

Learn more about rule types

< Back | Next > | Cancel

New rule

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Tunnel Endpoints
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

Isolation
Restrict connections based on authentication criteria, such as domain membership or health status.

Authentication exemption
Do not authenticate connections from the specified computers.

Server-to-server
Authenticate connection between the specified computers.

Tunnel
Authenticate connections between gateway computers.

Custom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

Learn more about rule types

< Back | Next > | Cancel

New rule

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

Isolation
Restrict connections based on authentication criteria, such as domain membership or health status.

Authentication exemption
Do not authenticate connections from the specified computers.

Server-to-server
Authenticate connection between the specified computers.

Tunnel
Authenticate connections between gateway computers.

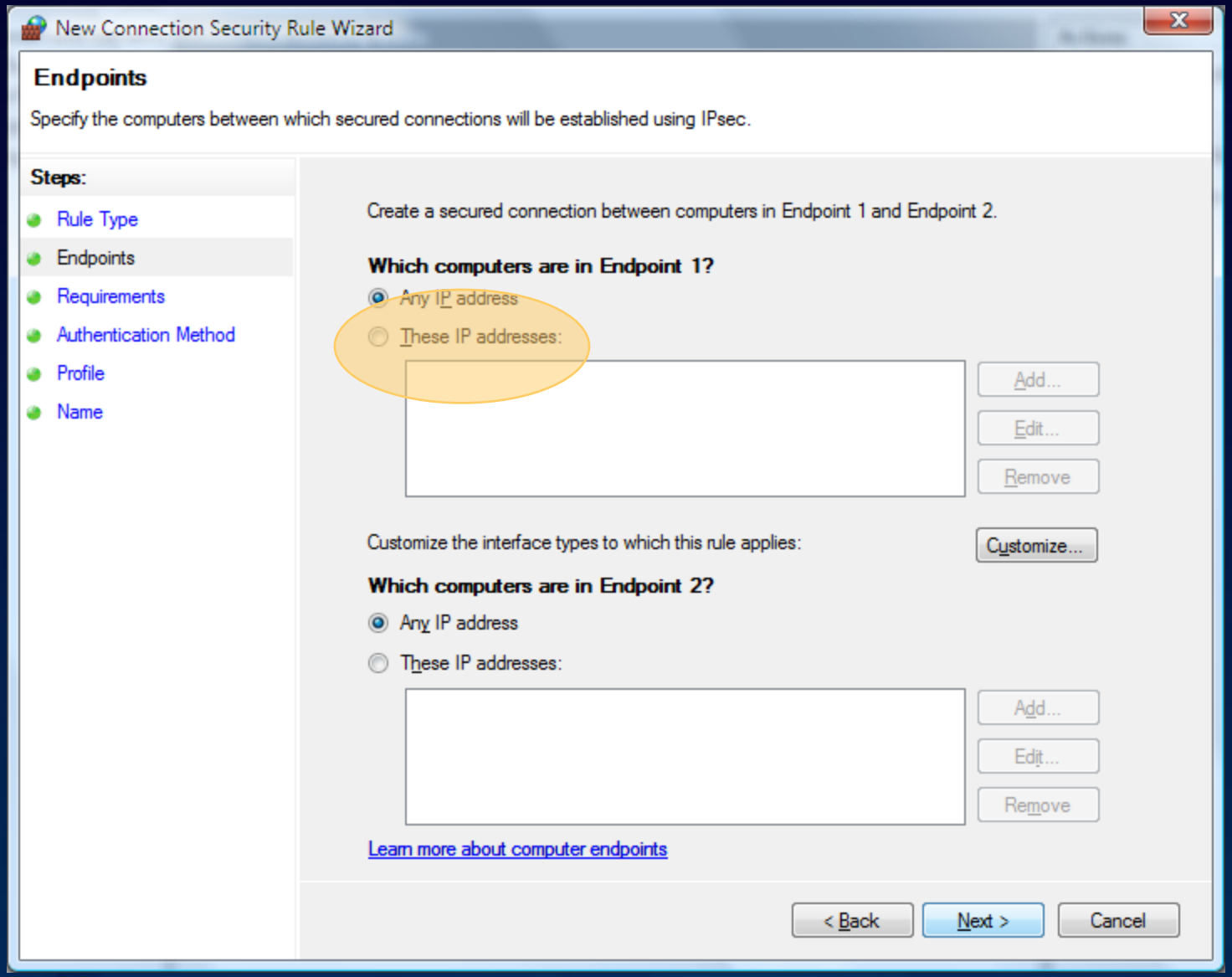
Custom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

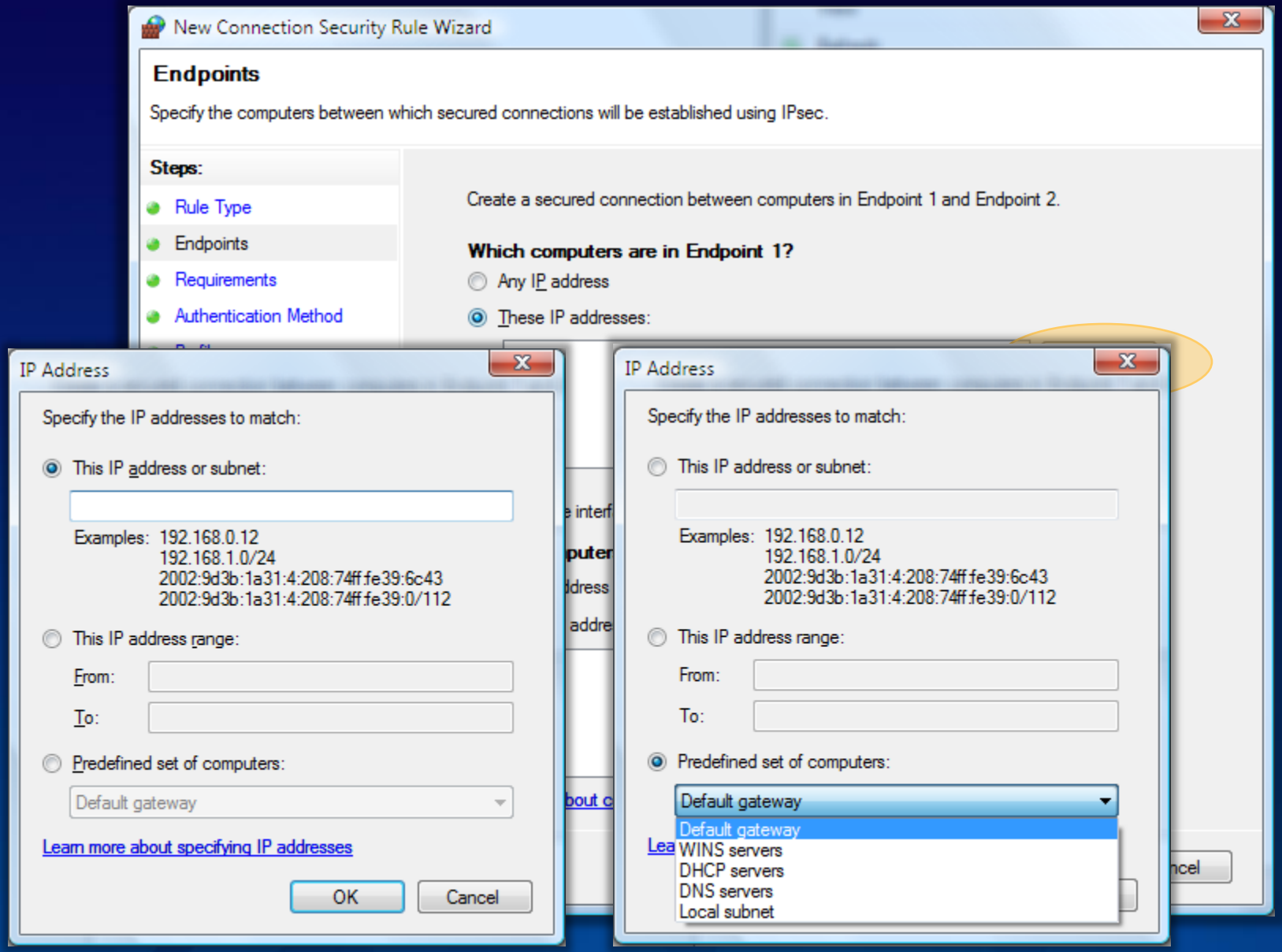
Learn more about rule types

< Back | Next > | Cancel

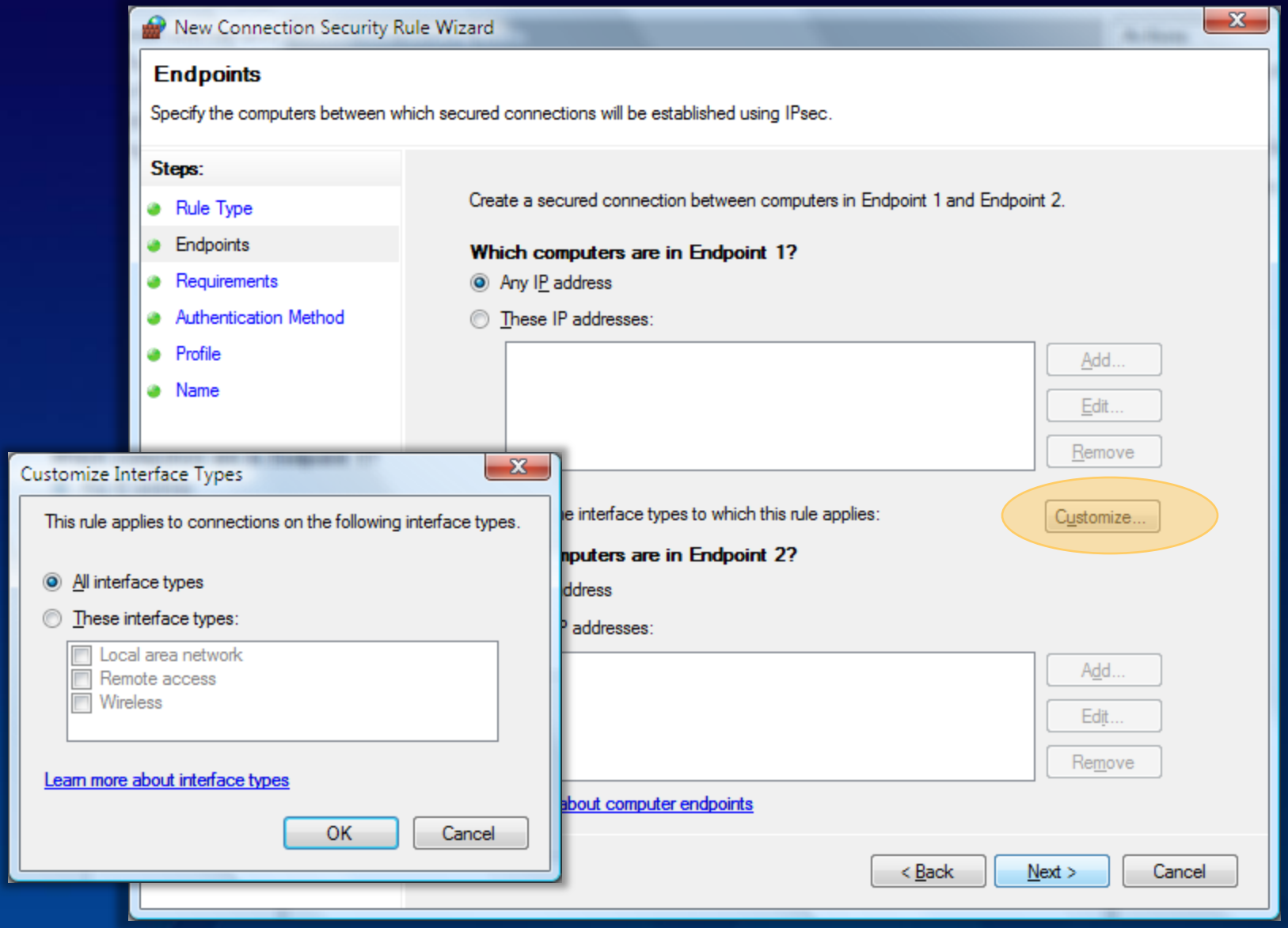
New rule - endpoints



New rule - endpoints



New rule - endpoints



New rule - tunnel endpoints

New Connection Security Rule Wizard

Tunnel Endpoints

Specify the endpoints for the IPsec tunnel defined by this rule.

Steps:

- Rule Type
- Tunnel Endpoints
- Authentication Method
- Profile
- Name

Connections from Endpoint 1 to Endpoint 2 will pass through the specified tunnel endpoints. Tunnel endpoints are generally gateway servers.

Which computers are in Endpoint 1?

Add...
Edit...
Remove

What is the local tunnel computer (closest to computers in Endpoint 1)?

IPv4 address:

IPv6 address:

What is the remote tunnel computer (closest to computers in Endpoint 2)?

IPv4 address:

IPv6 address:

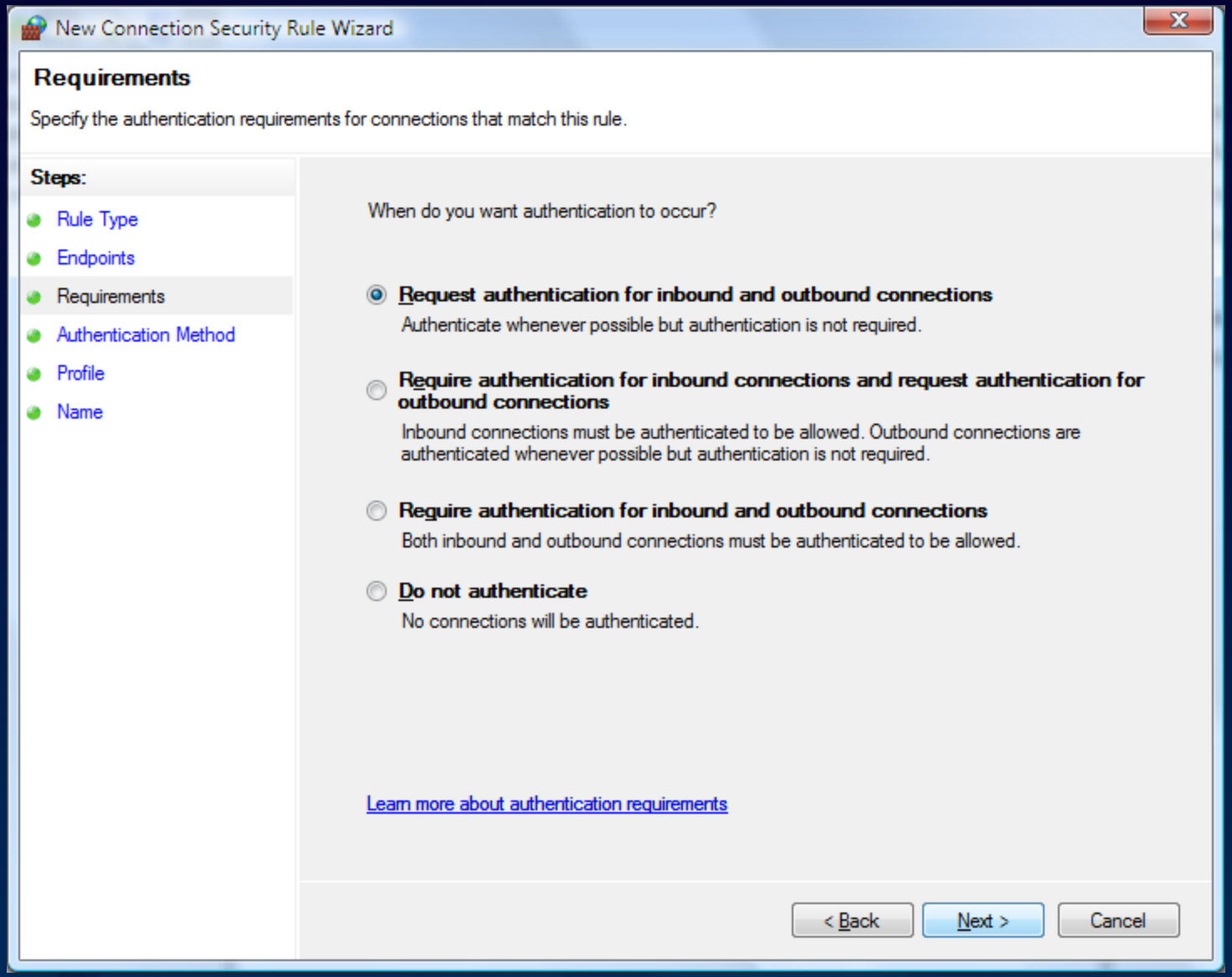
Which computers are in Endpoint 2?

Add...
Edit...
Remove

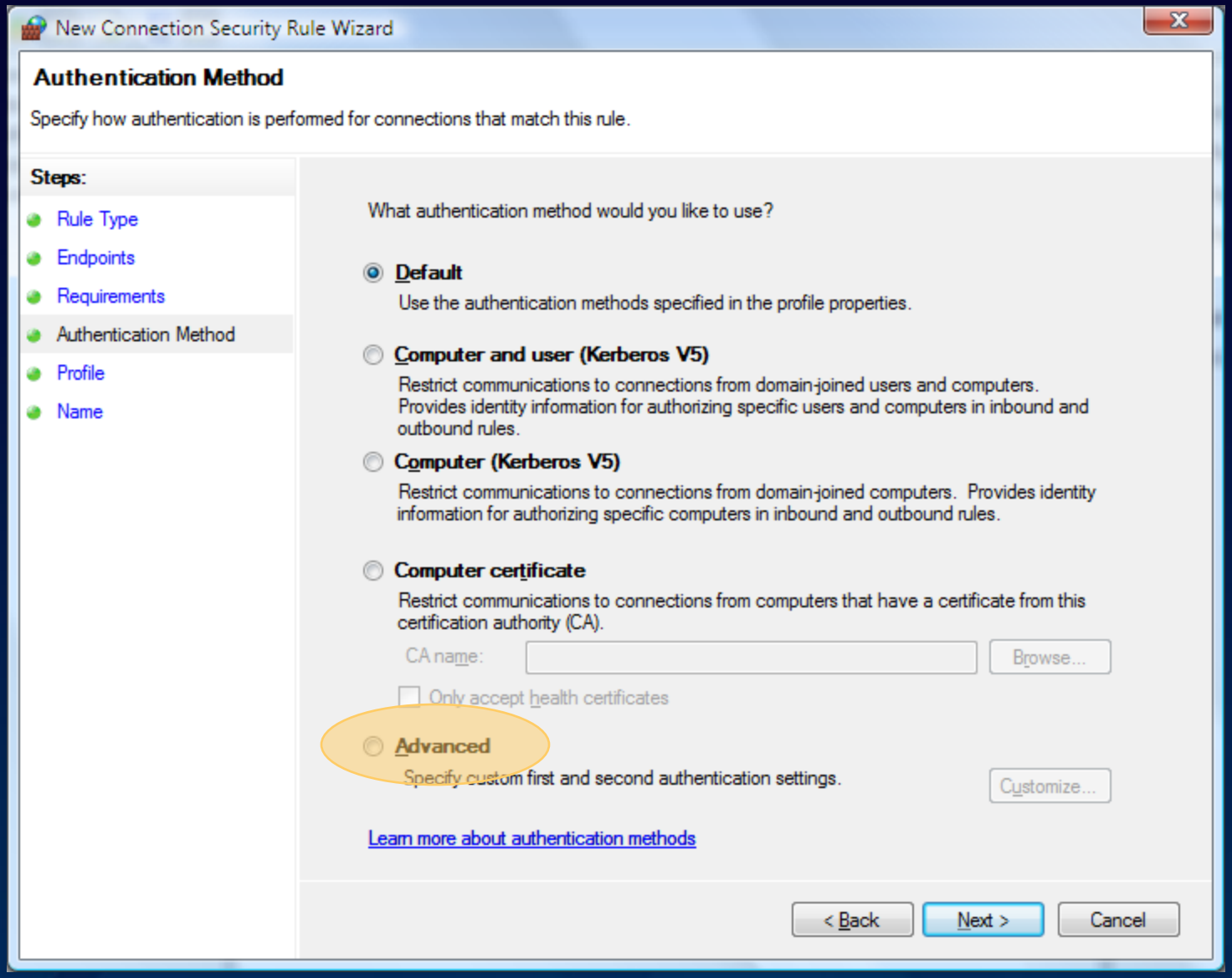
Learn more about tunnel endpoints

< Back | Next > | Cancel

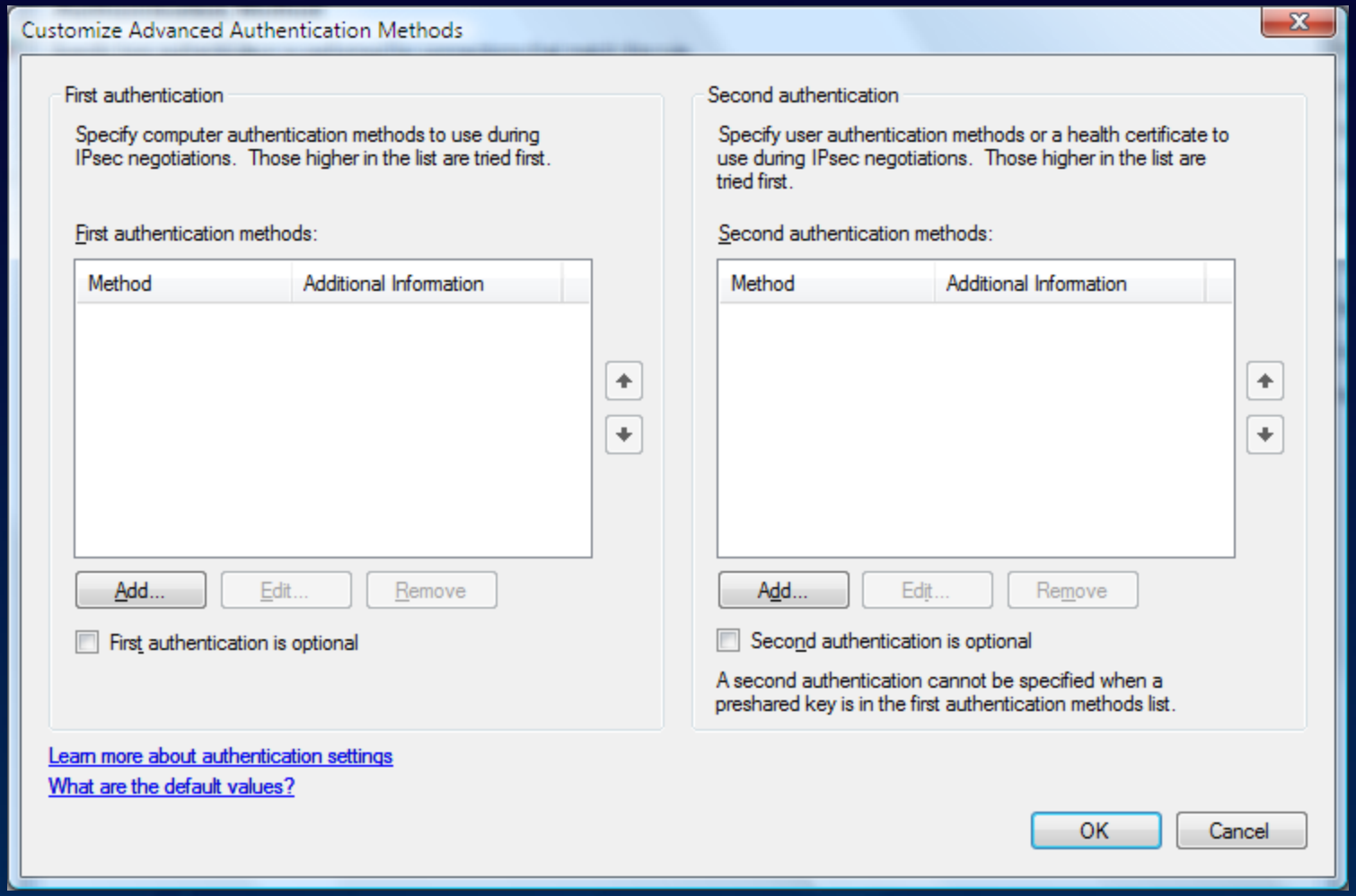
New rule - requirements



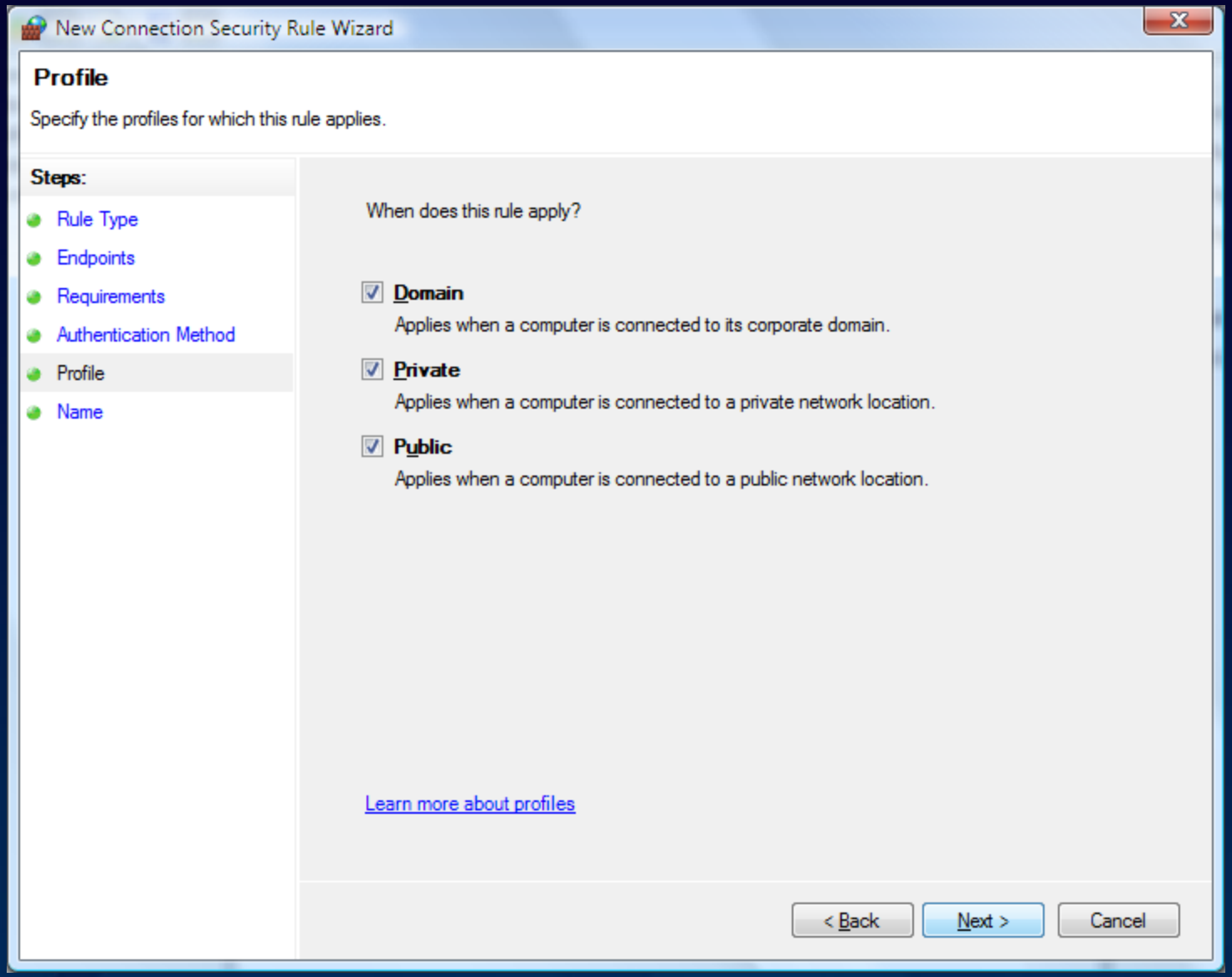
New rule - authentication



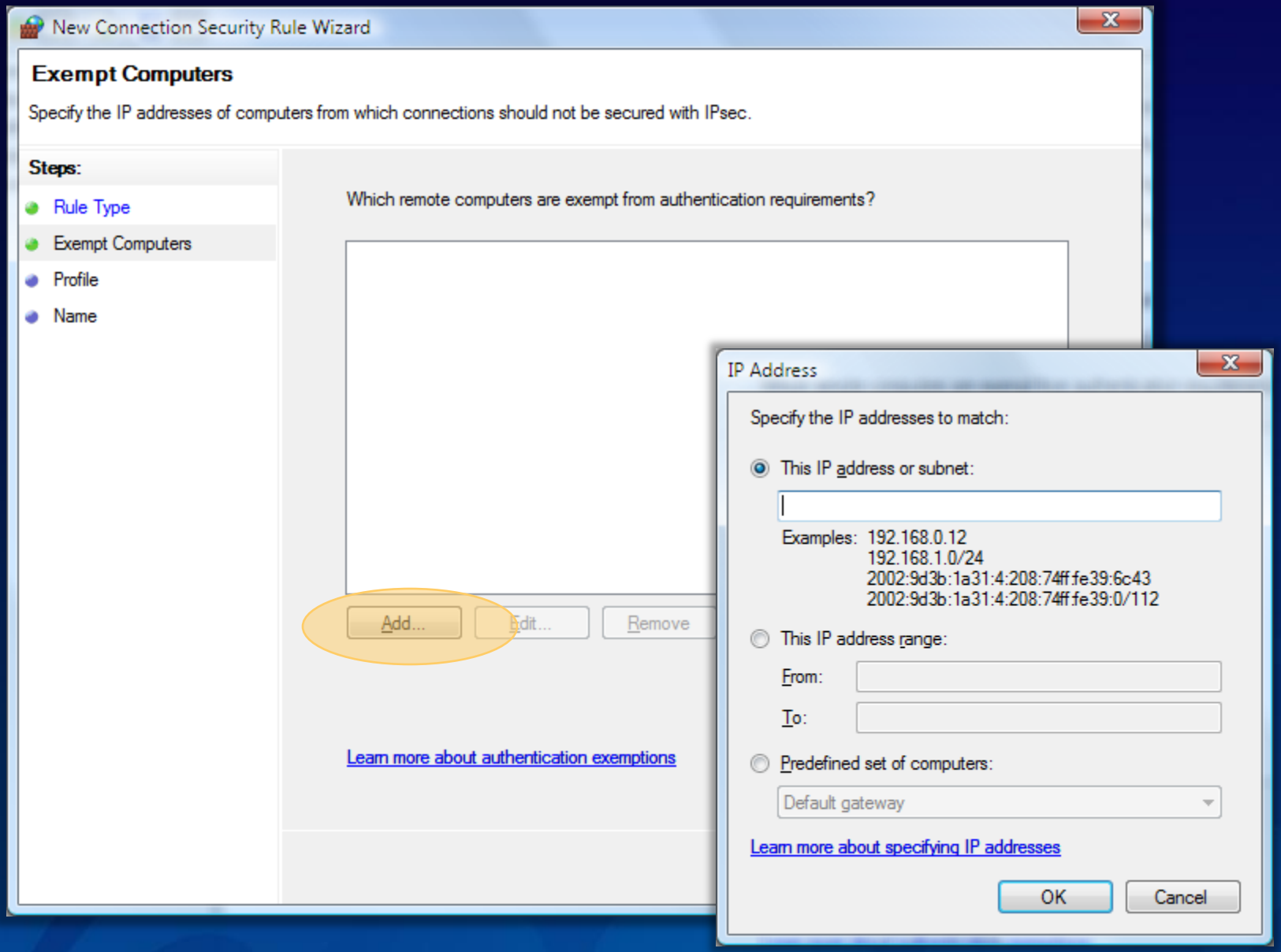
New rule - authentication



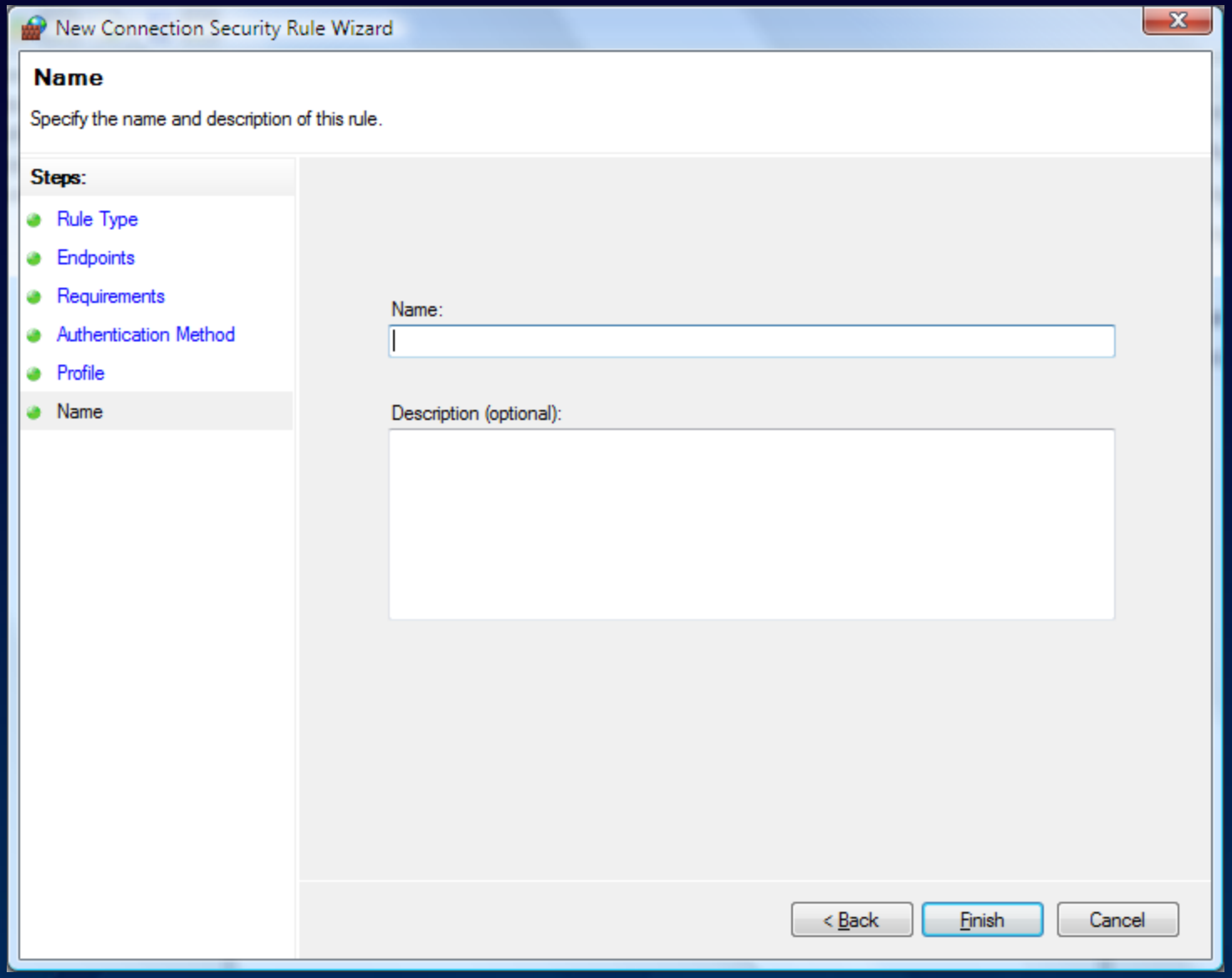
New rule - profile



New rule - exemptions



New rule - name



IPsec auditing and diagnostics

- Added 15 new IPsec audit-specific events and 20 new firewall events
- 25 legacy event texts rewritten to reflect a more accurate state
- No more generic events

- Implemented granular control of the IPsec audit policy (3 main categories with 8 sub categories)

- Events include all the information needed for troubleshooting; no tracing required
- Oakley log replaced with WPP tracing (intended for Microsoft internal use only)

- Defined different logical Perfmon counters sets (IKE4, IKEv6, AUTHIPv4, AuthIPv6, …)
- Overall added 150 new Perfmon counters between IPsec and firewall

- Improved IPsecmon—event texts include troubleshooting hints

- Integrated with NetXP, an end-user tool for diagnosing and resolving connection problems

Monitoring

Windows Firewall with Advanced Security

File Action View Help

- Windows Firewall with Advanced Se
  - Inbound Rules
  - Outbound Rules
  - Connection Security Rules
  - Monitoring
    - Firewall
    - Connection Security Rules
    - Security Associations
      - Main Mode
      - Quick Mode

Connection Security Rules

Name	Endpoint 1	Endpoint 2	Authentication mode	1st Auth

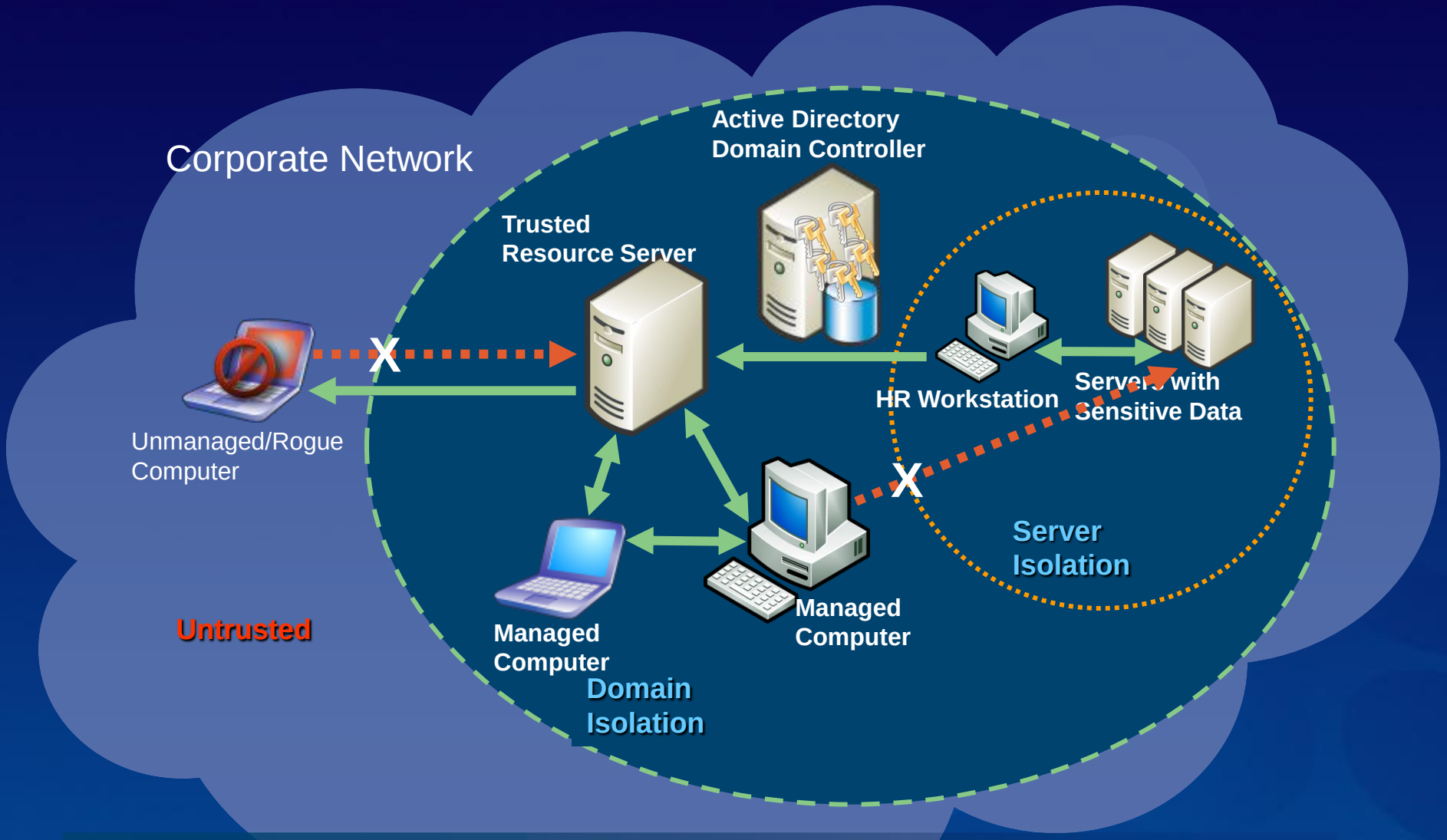
There are no items to show in this view.

Actions

Connection Security Rules

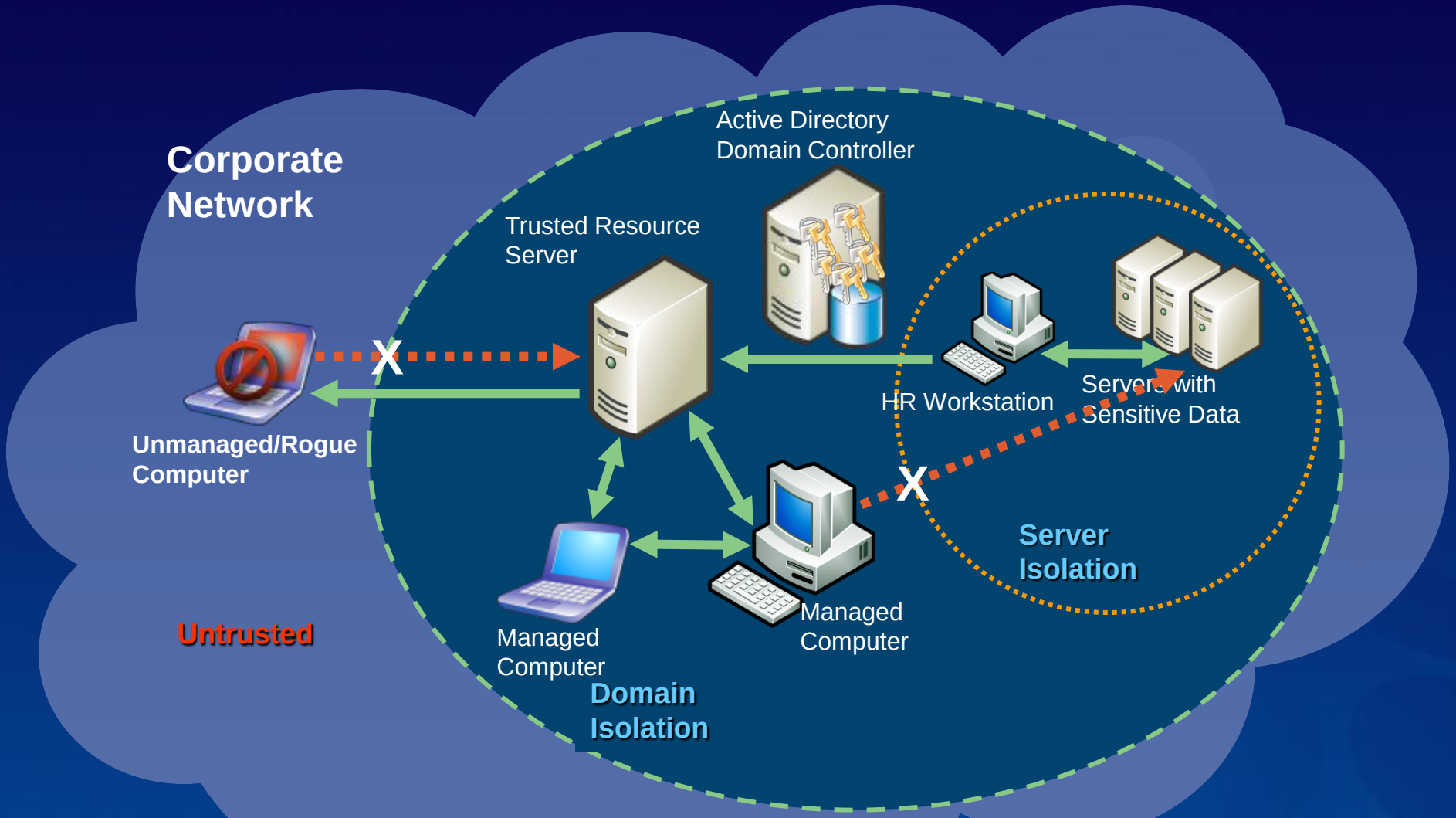
- View
- Refresh
- Export List...
- Help

Server and Domain Isolation



Enable tiered-access to sensitive resources

Server and Domain Isolation



Enable tiered-access to sensitive resources

Windows Vista

BITLOCKER

The Threats

- Computer is lost or stolen
  - Theft or compromise of data
  - Attack against corporate network
- Damage to OS if attacker installs alternate OS
- Difficult and time-consuming to truly erase decommissioned disks
- Existing ways to mitigate these threats are too easy for user to circumvent

Won’t EFS protect me?

- Yes, for those who know what they’re doing!
- Users often store data on the desktop - is it EFSed?
- EFS doesn’t protect the operating system
- EFS is very strong against attacks
  - Four levels of key protection
  - Properly configured, EFS is computationally infeasible to crack

Vista Information Protection

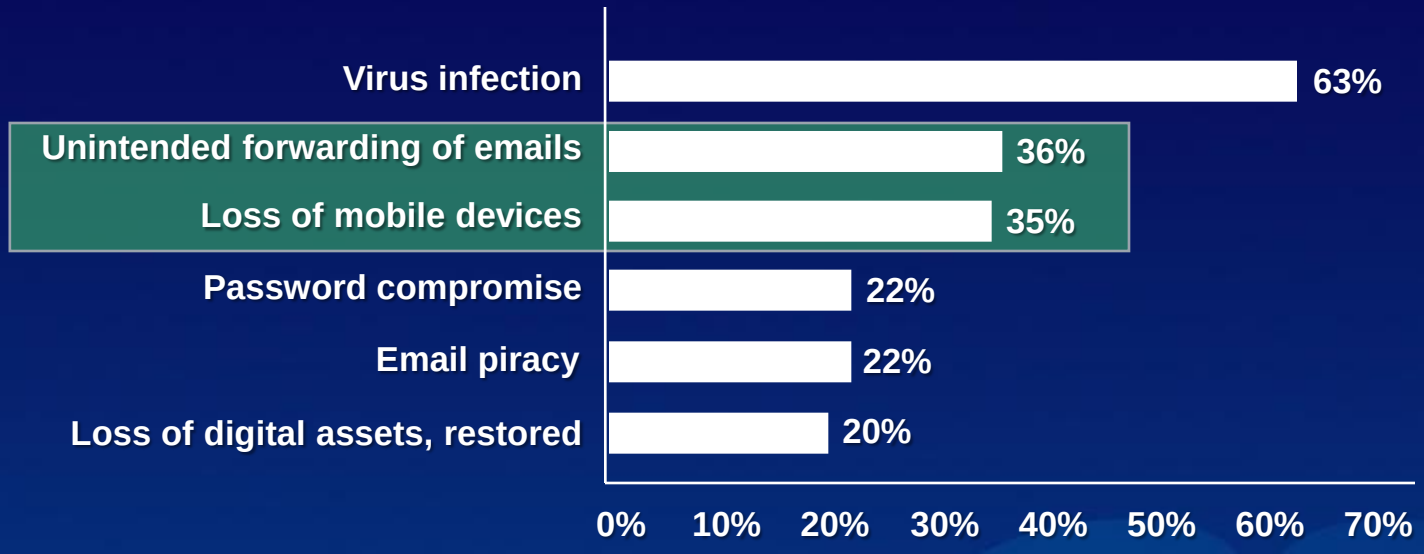
Who are you protecting against?

- Other users or administrators on the machine? EFS
- Unauthorized users with physical access? BitLocker™

Scenarios	BitLocker	EFS	RMS
Laptops	●		
Branch office server	●		
Local *single-user* file & folder protection	●		
Local *multi-user* file & folder protection		●	
Remote file & folder protection		●	
Untrusted network admin		●	
Remote document policy enforcement			●

Some cases can result in overlap. (e.g. Multi-user roaming laptops with untrusted network admins)

Information Leakage Is Top-of-mind With Business Decision Makers



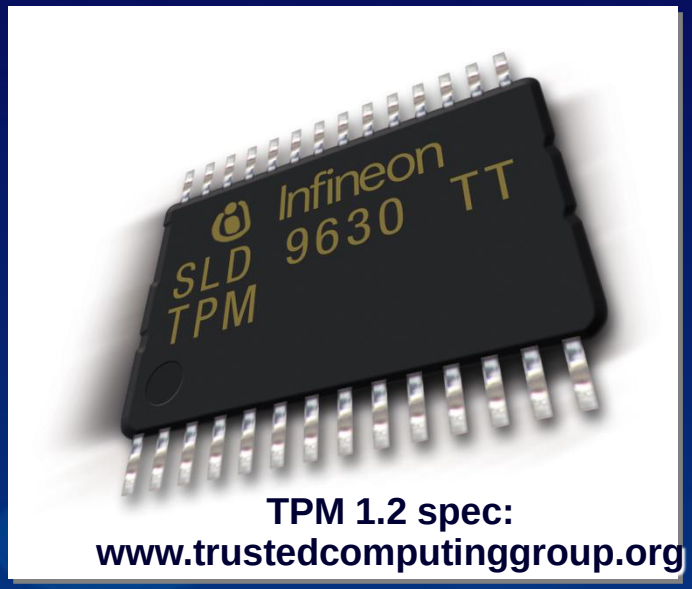
"After virus infections, businesses report unintended forwarding of e-mails and loss of mobile devices more frequently than they do any other security breach"

Jupiter Research Report, 2004

What Is A Trusted Platform Module?

Smartcard-like module on the motherboard that:

- Performs cryptographic functions
  - RSA, SHA-1, RNG
  - Meets encryption export requirements
- Can create, store and manage keys
- Holds Platform Measurements
- Anchors chain of trust for keys and credentials
- Protects itself against attacks



TPM 1.2 spec: www.trustedcomputinggroup.org

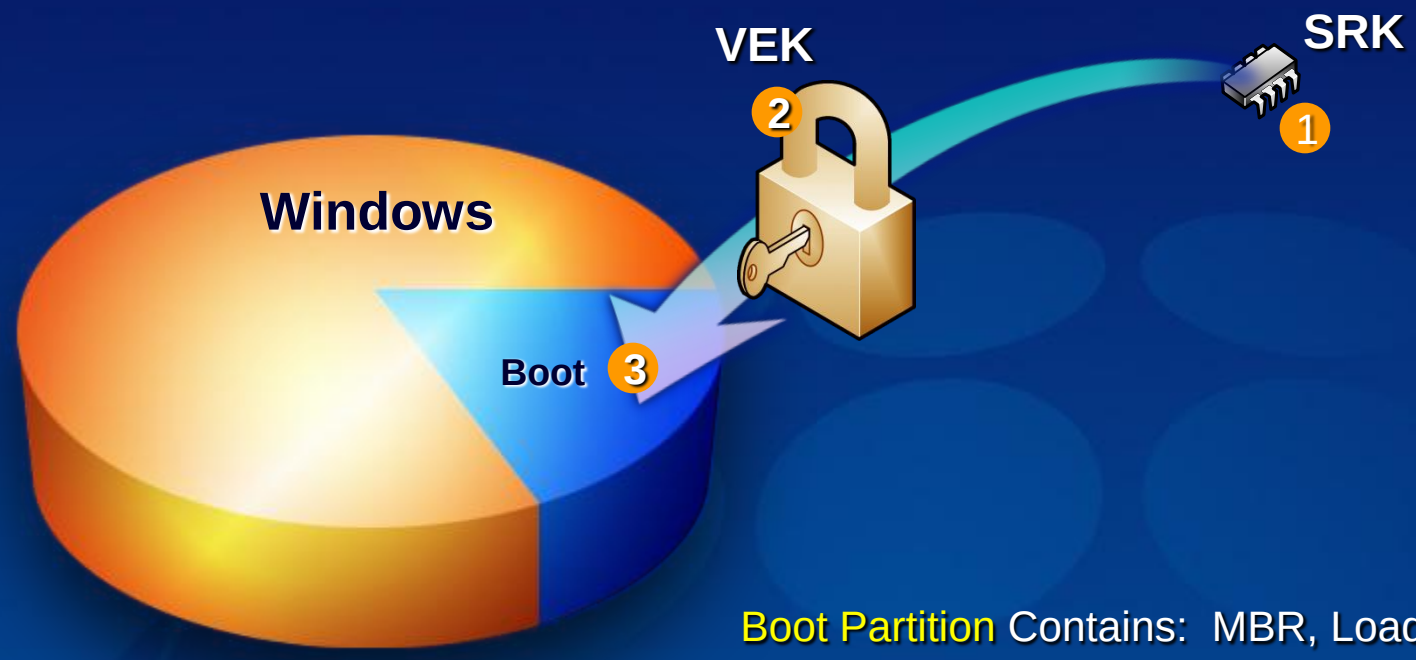
Disk Layout & Key Storage

Windows Partition Contains

- Encrypted OS
- Encrypted Page File
- Encrypted Temp Files
- Encrypted Data
- Encrypted Hibernation File

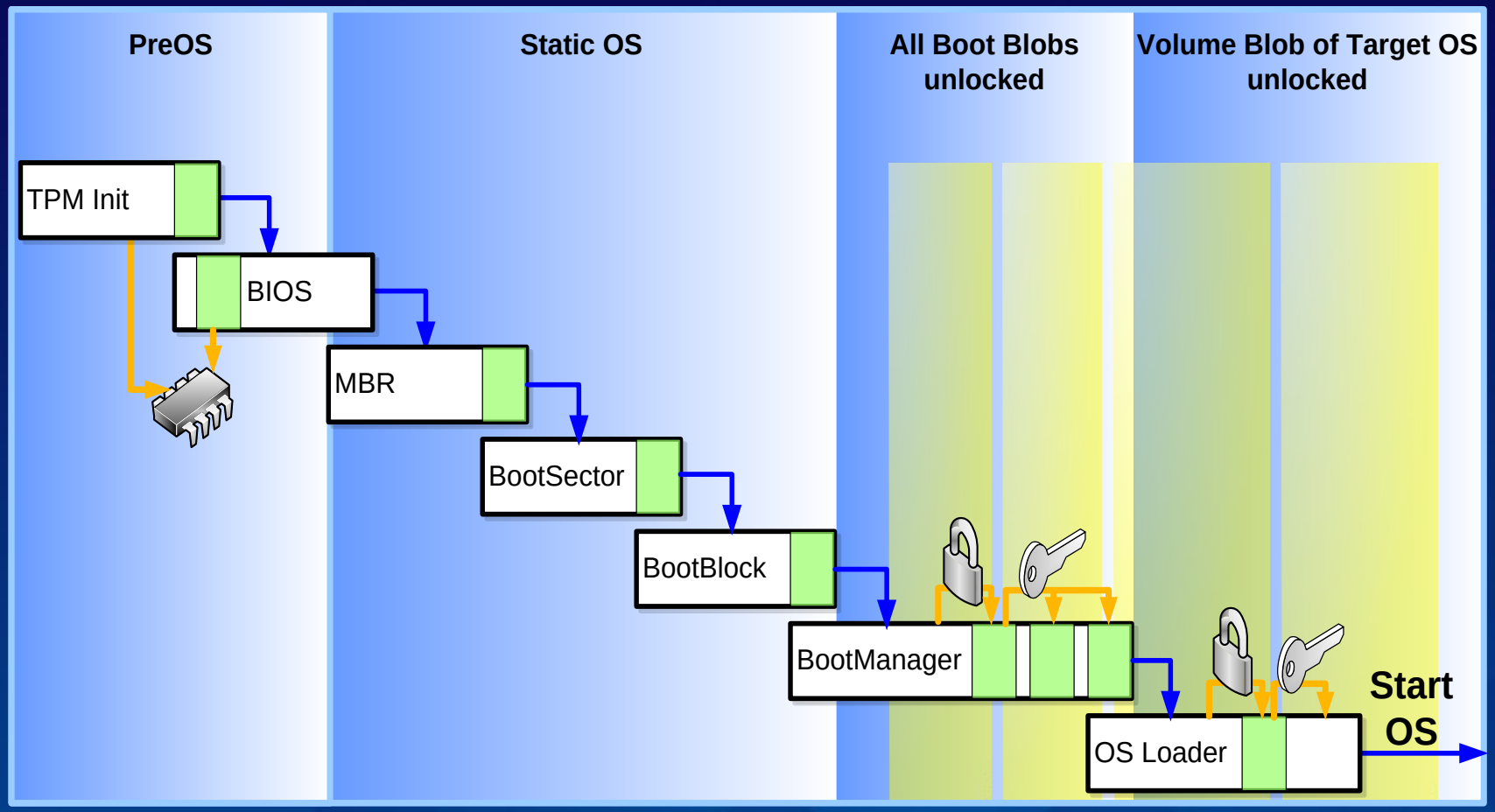
Where's the Encryption Key?

1. *SRK* (Storage Root Key) contained in TPM
2. *SRK* encrypts *VEK* (Volume Encryption Key) protected by TPM/PIN/Dongle
3. *VEK* stored (encrypted by *SRK*) on hard drive in Boot Partition



Boot Partition Contains: MBR, Loader, Boot Utilities (Unencrypted, small)

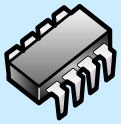
Static Root of Trust Measurement



Spectrum Of Protection

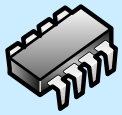
BitLocker offers a spectrum of protection allowing customers to balance ease-of-use against the threats they are most concerned with.

Ease of Use



TPM Only
"What it is."
Protects against: SW-only attacks
Vulnerable to: HW attacks (including potentially "*easy*" HW attacks)

Dongle Only
"What you have."
Protects against: All HW attacks
Vulnerable to: Losing dongle Pre-OS attacks



*****

TPM + PIN
"What you know."
Protects against: Many HW attacks
Vulnerable to: TPM breaking attacks

TPM + Dongle
"Two what I have's."
Protects against: Many HW attacks
Vulnerable to: HW attacks

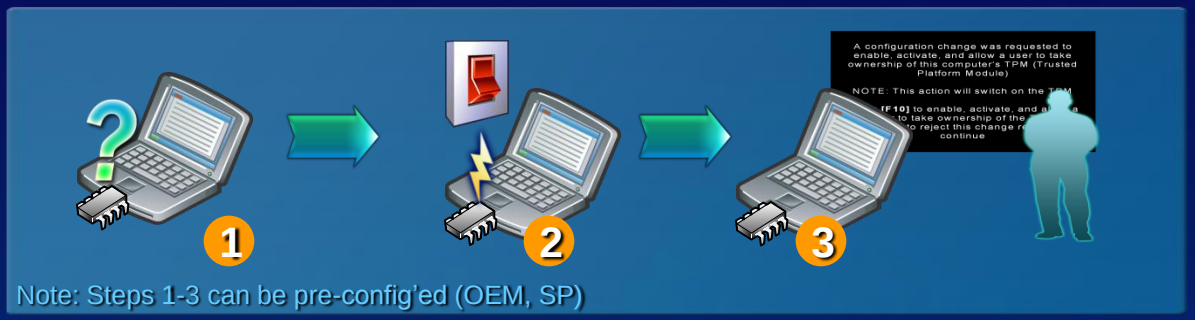
Security

Enabling BitLocker

- Create a 1.5GB active partition
  - This becomes your “system” partition - where OS boots
  - The TPM boot manager uses only 50MB
  - Windows runs from on your “boot” partition - where the system lives
- Initialize TPM chip if you’re using it
  - In management console or BIOS
- Enable BitLocker in Security Center
  - Update hard disk MBR
  - Encrypt Windows “boot” partition

BitLocker™

TPM Administration Storyboard – New Machine



Basic TPM Administration/Deployment

1.Machine arrives at enterprise in un-initialized state.

2.Turn TPM On

3.Check for physical presence by rebooting the machine and prompting user at BIOS screen for key press.

4.Log back into Windows Vista

5.Take Ownership of TPM

6.Check for existence of Endorsement Key (Provided by OEM)

7.Create TPM Administration Password.

8.Commit changes to TPM and initialize.

9.Publish TPM Administration Password to AD/File

10.TPM Initialization Complete

BitLocker™

Single Machine Deployment with TPM

Windows Vista Install

Windows Vista Install

- BDE requires a partition separate from the Windows Vista OS partition with a min free space of 350Mb
- During installation the system is checked for correct version of TPM (v 1.2) and BIOS via Plug and Play
- TPM & BDE drivers are installed

BDE Installation

1. Start installation through the BDE control panel applet
2. Installation checks for required disk partition layout. This partition needs to be formatted NTFS and contain a Windows Vista installation
3. Installation enables BDE for Windows Volume
4. Installation verifies that the TPM has initialized
5. User selects Recovery Key Backup method, and installation continues with volume encryption
6. Installation displays background encryption progress bar and tray icon, then notifies user when BDE is complete

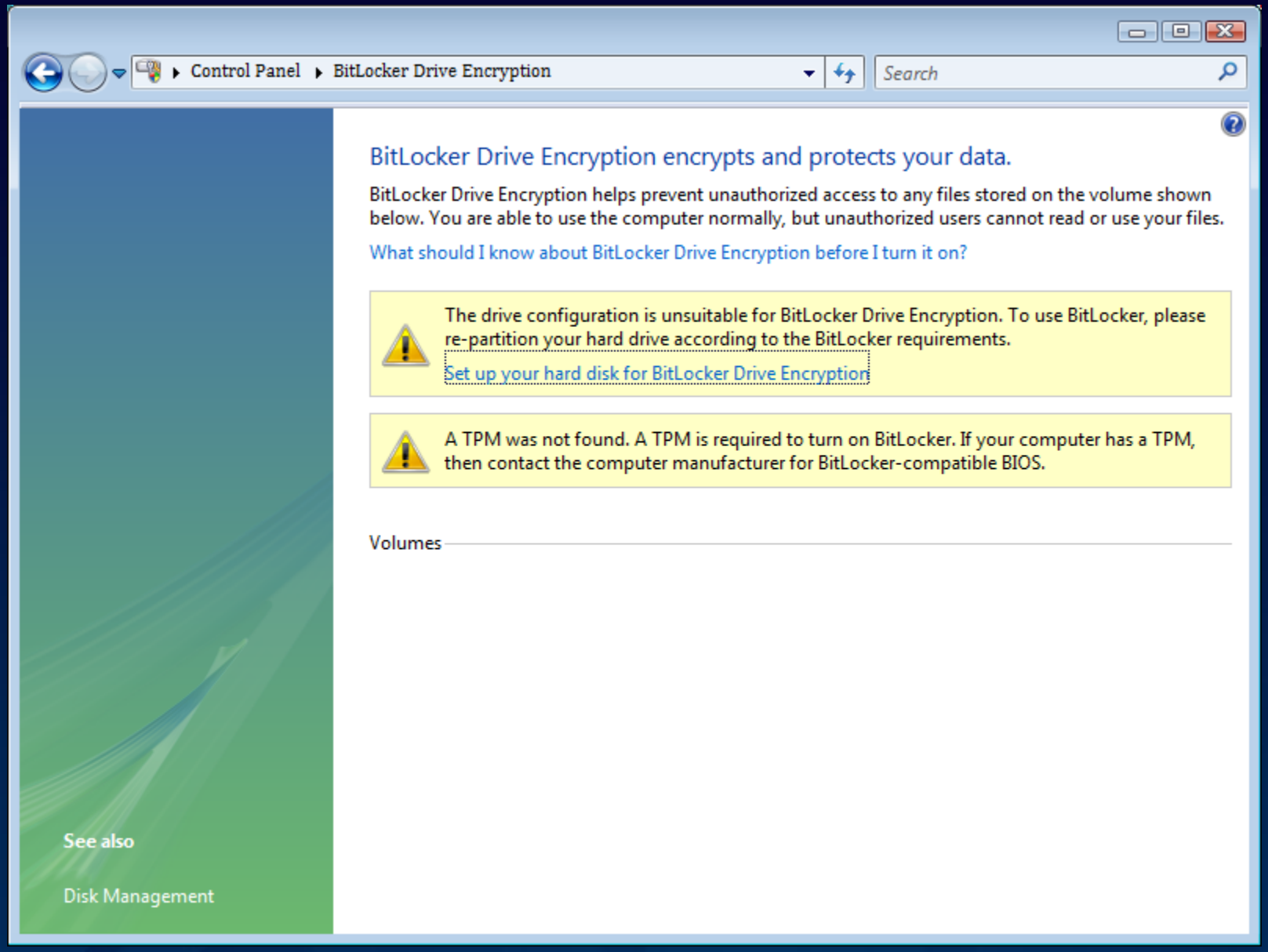
BitLocker™

Enterprise Machine Deployment with TPM

BDE installation

1. Active Directory prepared for BDE keys
2. Windows Vista Install
   - a. BDE requires a partition separate from the Windows Vista OS partition with a min free space of 350Mb
   - b. During installation the system is checked for correct version of TPM (v 1.2) and BIOS via Plug and Play
   - c. TPM & BDE drivers are installed
3. BDE Initialization
   - a. Scripted initialization of TPM
   - b. TPM Ownership password saved to Active Directory
4. Remote executed Script BDE
   - a. Policy saves recovery key to AD
   - b. System encrypted
5. Inspect audit logs for successful end to encryption

Control panel



Group policy

Group Policy Object Editor

File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - System
      - Windows Components
        - ActiveX Installer Service
        - Application Compatibility
        - AutoPlay Policies
        - Backup
        - BitLocker Drive Encryption
        - Credential User Interface
        - Desktop Window Manager
        - Digital Locker
        - Event Log Service
        - Event Viewer
        - Game Explorer
        - Import Video
        - Internet Explorer
        - Internet Information Service

Setting	State
Turn on BitLocker backup to Active Directory Domain Services	Not configured
Control Panel Setup: Co	
Control Panel Setup: Co	
Control Panel Setup: En	
Configure encryption m	
Prevent memory overw	
Configure TPM platform	

Extended | Standard

Control Panel Setup: Enable advanced startup options Properti...

Setting | Explain

Control Panel Setup: Enable advanced startup options

- Not Configured
- Enabled
- Disabled

☑ Allow BitLocker without a compatible TPM (requires a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup key option:

Allow user to create or skip

Configure TPM startup PIN option:

Allow user to create or skip

IMPORTANT: If you require the startup key,

Supported on: At least Windows Vista

Previous Setting | Next Setting

OK | Cancel | Apply

Command line

Select Administrator: C:\Windows\system32\cmd.exe

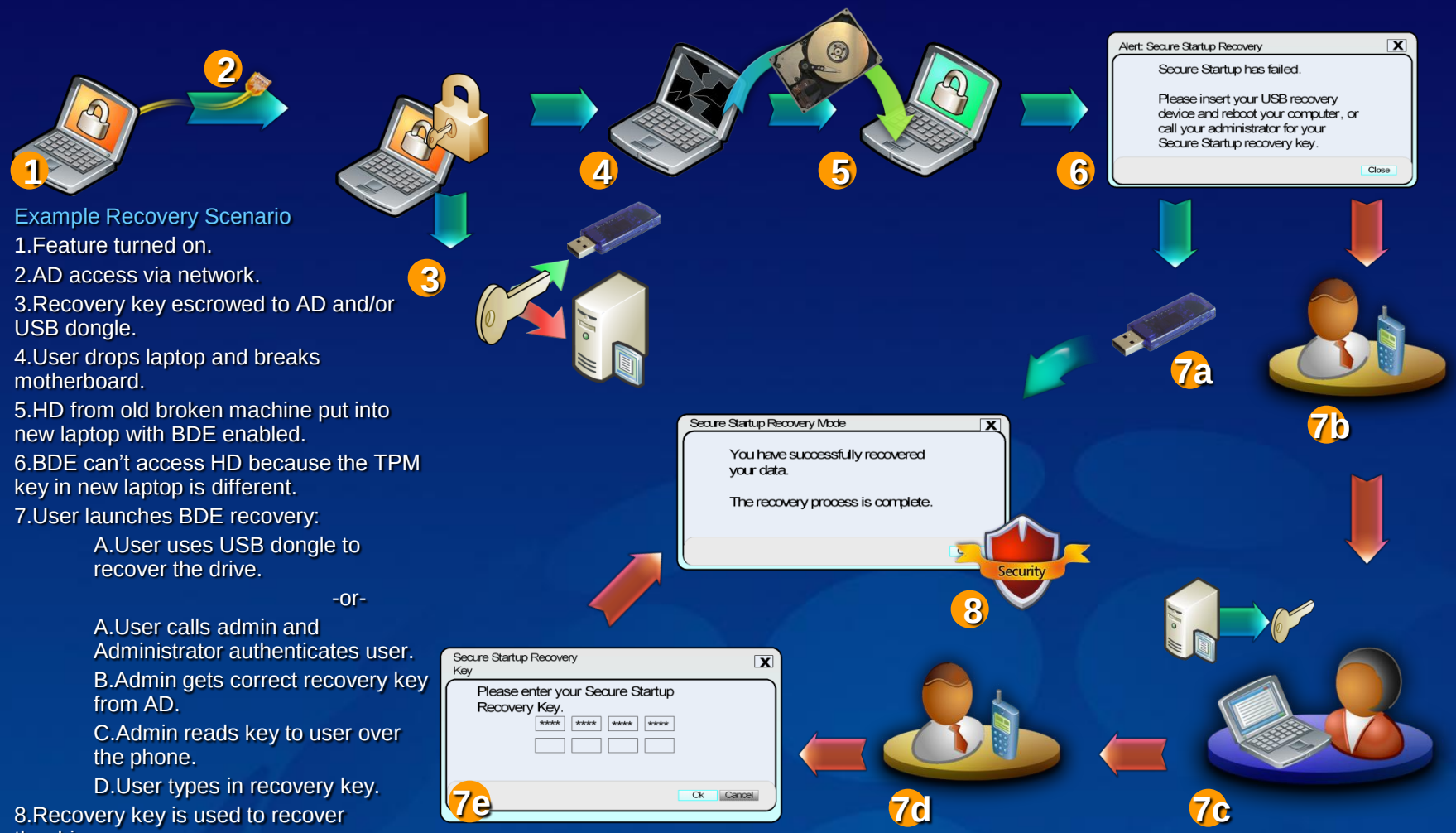
```
C:\Windows\System32>cscript manage-bde.wsf
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

manage-bde[.wsf] -parameter [arguments]

Description:
    Configures BitLocker Drive Encryption on disk volumes.

Parameter List:
    -status     Provides information about BitLocker-capable volumes.
    -on         Encrypts the volume and turns BitLocker protection on.
    -off        Decrypts the volume and turns BitLocker protection off.
    -pause      Pauses encryption or decryption.
    -resume     Resumes encryption or decryption.
    -lock       Prevents access to BitLocker-encrypted data.
    -unlock     Allows access to BitLocker-encrypted data.
    -autounlock Manages automatic unlocking of data volumes.
    -protectors Manages protection methods for the encryption key.
    -tpm        Configures the computer's Trusted Platform Module (TPM).
    -ForceRecovery or -fr
                Forces a BitLocker-protected OS to recover on restarts.
    -ComputerName or -cn
                Runs on another computer. Examples: "ComputerX", "127.0.0.1"
    -? or /?    Displays brief help. Example: "-ParameterSet -?"
    -Help or -h Displays complete help. Example: "-ParameterSet -h"

Examples:
    manage-bde -status
    manage-bde -on C: -RecoveryPassword -RecoveryKey F:\
    manage-bde -unlock E: -RecoveryKey F:\84E151C1...7A62067A512.bek
```

Recovery Options

- BitLocker™ setup will automatically escrow keys and passwords into AD
  - Centralized storage/management keys (EA SKU)
- Setup may also try (based on policy) to backup keys and passwords onto a USB dongle or to a file location
  - Default for non-domain-joined users
  - Exploring options for web service-based key escrow
- Recovery password known by the user/administrator
  - Recovery can occur “in the field”
  - Windows operation can continue as normal

BitLocker™

Recovery Storyboard – Broken Hardware



Example Recovery Scenario

1. Feature turned on.
2. AD access via network.
3. Recovery key escrowed to AD and/or USB dongle.
4. User drops laptop and breaks motherboard.
5. HD from old broken machine put into new laptop with BDE enabled.
6. BDE can't access HD because the TPM key in new laptop is different.
7. User launches BDE recovery:
   - A. User uses USB dongle to recover the drive.

     -or-

   - A. User calls admin and Administrator authenticates user.
   - B. Admin gets correct recovery key from AD.
   - C. Admin reads key to user over the phone.
   - D. User types in recovery key.
8. Recovery key is used to recover the drive

BitLocker can’t stop everything

- Hardware debuggers
- Online attacks - BitLocker is concerned only with the system’s startup process
- Post logon attacks
- Sabotage by administrators
- Poor security maintenance

Windows Vista

GROUP POLICY

Group Policy Control of Devices

- Control whether or not device drivers can install
- Control what types of devices are allowed (or not)
- Control what specific devices are allowed (or not)
- Block CD/DVD Burning

Managing Device Driver Installation

Problem: In enterprises, Standard Users cannot install device drivers but need network printers.

- Device Management Infrastructure introduced in Windows Vista
  - Configurable by Group Policy
  - Allows Standard Users to install drivers
- Hardware-first install initiates automatic search for drivers

Device Driver Installation Policy

- Device Management Infrastructure policy is based on the driver location, signature, and device class guid.
- The Driver Store is a trusted cache of drivers on client machines
  - Dynamic and updatable
  - Windows Vista installs these trusted drivers as needed
- Device Drivers must be signed by a certificate in the Enterprise Trusted Publishers store.
- Device class must be enabled for Standard User installation using Group Policy in Driver Installation ADM.

ActiveX Installer Service: Policy

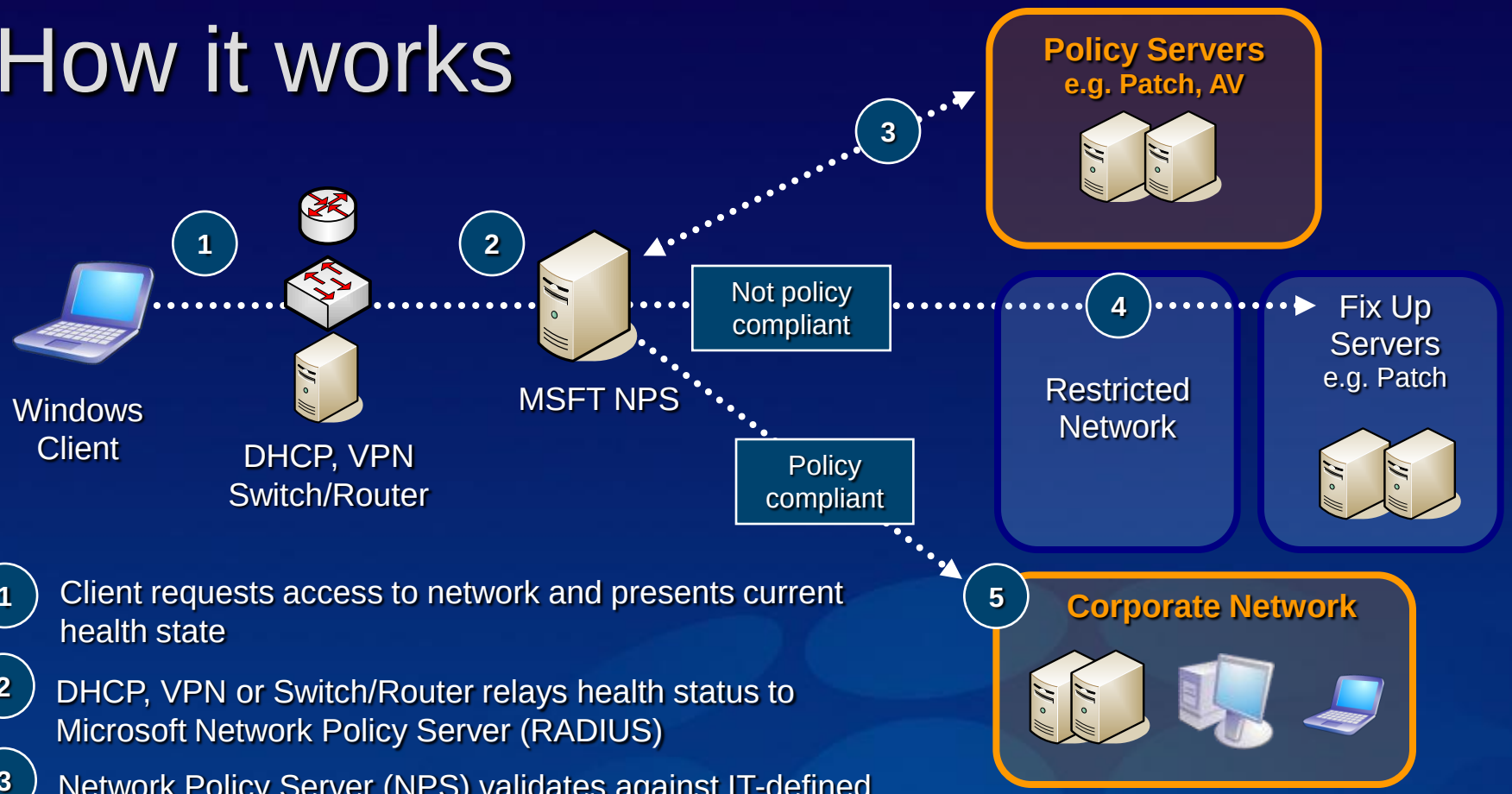
- Installation Policy based on Host URL and signature of content
  - Host defined by URL http or https (recommended)
  - Cab file signature can be checked against enterprise Trusted Publishers store.
- ActiveX Controls can be deployed from a central server using CodeBaseSearch path.
- Attempt to install ActiveX control is audited.

Windows Vista

NETWORK ACCESS PROTECTION (NAP)

Network Access Protection

How it works



1. Client requests access to network and presents current health state
2. DHCP, VPN or Switch/Router relays health status to Microsoft Network Policy Server (RADIUS)
3. Network Policy Server (NPS) validates against IT-defined health policy
4. If not policy compliant, client is put in a restricted VLAN and given access to fix up resources to download patches, configurations, signatures (Repeat 1 - 4)
5. If policy compliant, client is granted full access to corporate network

NAP Benefits with Windows Vista

NAP will work with Windows XP, but…

- Windows Vista will have NAP built in where as the XP client will be an add on.
- The local configuration MMC will only be available on Vista
- The Vista NAP client will take advantage of the Windows Defender support in Security Center to provide integrated current state of health
- In Vista, the underlying enforcement technologies will have more advanced features like Auth IP for IPsec and Single Sign-On support for 802.1x.

Windows Vista

AUDITING

Improved Auditing

- More Granularity
  - Support for many auditing subcategories
- New Logging Infrastructure
  - Filter out the “noise”
    - Search and filtering with new XML format
  - Tasks tied to events
    - Send an email on an event

Windows Vista

AUTHENTICATION

Authentication Improvements

- Plug and Play Smart Cards
  - Drivers and Certificate Service Provider (CSP) included in Windows Vista
  - Login and credential prompts for User Account Control all support Smart Cards
- New logon architecture
  - GINA (the old Windows logon model) is gone.
  - Third parties can add biometrics, one-time password tokens, and other authentication methods to Windows with much less coding

Otázky?

Martin Pavlis Microsoft MVP

IT Senior Consultant | KPCS CZ, s.r.o.

martin@pavlis.net | www.pavlis.net | www.kpcs.cz