Hype vs. Reality in Windows Server 2008 and Vista—Are they More Secure

Beth Quinlan
MCT, MCSE: Security, CISSP
bquinlan@columbus.rr.com
614-348-7869

Agenda – Windows Vista

- Windows Security Center
- Windows Defender
- Windows Firewall
- Internet Explorer 7 Security Features
- User Account Control
- Parental Controls
- Encrypting File System
- Other Security Features

Agenda – Windows Server 2008

- **Server Protection**
  - Windows Server Core Architecture
  - Secure Startup/Code Integrity
  - Windows Service Hardening
  - Windows Firewall and Advanced Security (WFAS)

- **Domain Protection**
  - Active Directory Domain Services Auditing
  - Server and Domain Isolation
  - Read-Only Domain Controller (RODC)

Windows Server 2008, cont.

- **Network Protection**
  - New TCP/IP stack
  - Internet Protocol Security (IPsec)
  - Methods of Security and Policy Enforcement
    - Network Location Awareness
    - Network Access Protection

- **Data Protection**
  - Removable Device Control
  - BitLocker Drive Encryption
  - Rights Management Services

Windows Server 2008, cont.

- **Identity and Access Control**
  - Active Directory Federation Services
  - Authentication Improvements
    - Plug and Play Smart Cards
    - New Logon Architecture
    - Granular Password Control
  - Enterprise PKI
    - Miscellaneous Enhancements
    - Cryptography Next Generation (CNG)

WINDOWS VISTA SECURITY

Windows Security Center

Windows Vista™

- Centralized location for all security needs
  - Alerts if security software is out-of-date
  - Displays firewall settings and reports on automatic updates
  - Verifies existence/status of virus protection software
  - Verifies status of Windows Defender or 3rd party spyware protection
  - Monitors Internet Explorer 7 security settings
  - Monitors and reports on status of account control

Windows Defender

- Introduced in XP SP2; built in to Vista
- Monitors key system locations, watching for changes that signal the presence of spyware
- 3 key technologies
  - Scanning and removal of spyware
  - Real-time protection
  - Ongoing, automatic updates
- Improved user interface
- Integrates with IE7

Windows Firewall

- 1st line of defense against malicious software
- Turned on by default
- More advanced than previous versions
  - Restricts OS resources if they behave in unexpected ways

Internet Explorer 7 Security

- Protected Mode
  - Enabled by default
  - Helps protect against “Elevation of Privilege” attacks
  - Prevents hackers from installing software
  - Protects against malicious downloads
- Phishing Filter
  - Opt-in feature that combines a local system scan for suspicious website characteristics with an online service
- Data Execution Protection (DEP)
  - Set of hardware/software to help protect from malicious software
- Delete Browsing History

Internet Explorer 7 Security, cont.

- Active-X opt-in
  - Automatically disables all but a few well-known, pre-approved controls
- Fix My Settings
  - Alerts you when settings may be unsafe and permits rollback to Medium-Default
- Personal Data Safeguards
  - Security Status Bar
- URL Display Protection
  - Address Bar in every windows
  - IDN display protections

User Account Control

- Prevents potentially dangerous software from making changes to a computer without explicit consent
- Two types of User accounts – Standard and Administrator
  - Both can run applications with roughly the same permissions and change their own settings
  - Standard user is default for everyday use
    - Vista extends the range of common, low-risk tasks available to standard user
- Credential and Consent Prompts
  - Require permissions from another account (administrator) to permit the action and proceed

Parental Controls

- Not just for parents
  - Useful as a control mechanism in small businesses
- Web Restrictions to control what Web sites user can access and what they can download
- Time Limits to control what days and times your child can use the computer
- Control/Block games from systems
- Block access to specific programs
- Display activity reports
  - Web sites visited, how long online, how many emails received, etc.

Encrypting File System

- Available in Business, Enterprise and Ultimate
- Enhanced management enables administrators to store EFS keys on smartcards

Other Security Features

- New Logon Architecture
- USB Device Control
- BitLocker Drive Encryption
- Network Access Protection
- IPv6/Ipsec
- Rights Management

Windows Server® 2008

WINDOWS SERVER 2008 SECURITY

Server Protection: Windows Server Core Arch.

Supported Roles

- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- DHCP Server
- DNS Server
- File Server
- Print
- Windows Media Services
- Windows Virtualization Services

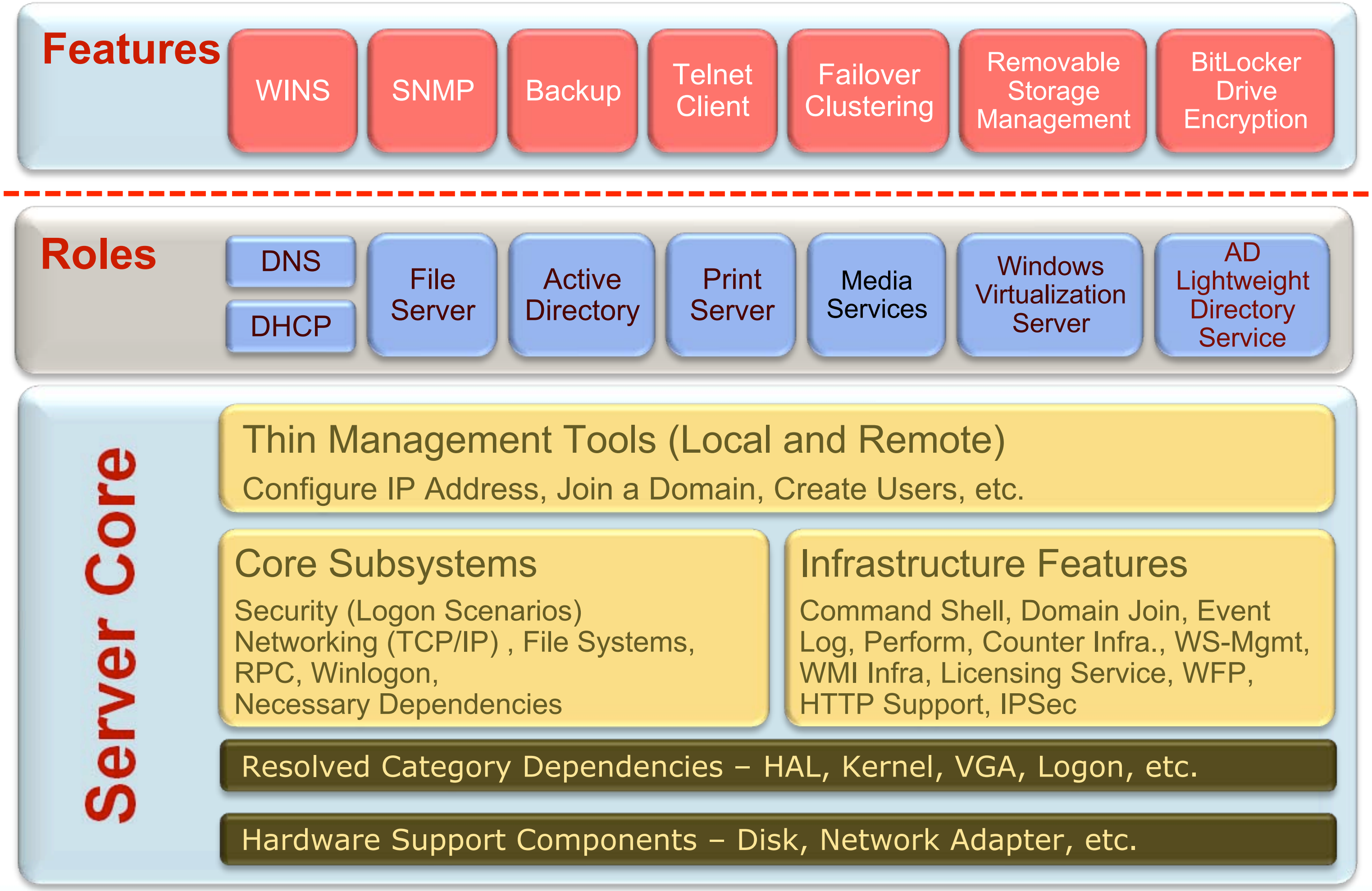
Benefits

- Increased server stability
- Reduced management
- Reduced attack surface
- Reduced software maintenance
- Reduced hardware requirements

Only a subset of the executable files and DLLs installed

No GUI interface installed

Windows Server Core Architecture



Features

WINS

SNMP

Backup

Telnet Client

Failover Clustering

Removable Storage Management

BitLocker Drive Encryption

Roles

DNS

DHCP

File Server

Active Directory

Print Server

Media Services

Windows Virtualization Server

AD Lightweight Directory Service

Server Core

Thin Management Tools (Local and Remote)

Configure IP Address, Join a Domain, Create Users, etc.

Core Subsystems

Security (Logon Scenarios)
Networking (TCP/IP) , File Systems,
RPC, Winlogon,
Necessary Dependencies

Infrastructure Features

Command Shell, Domain Join, Event Log, Perform, Counter Infra., WS-Mgmt, WMI Infra, Licensing Service, WFP, HTTP Support, IPSec

Resolved Category Dependencies – HAL, Kernel, VGA, Logon, etc.

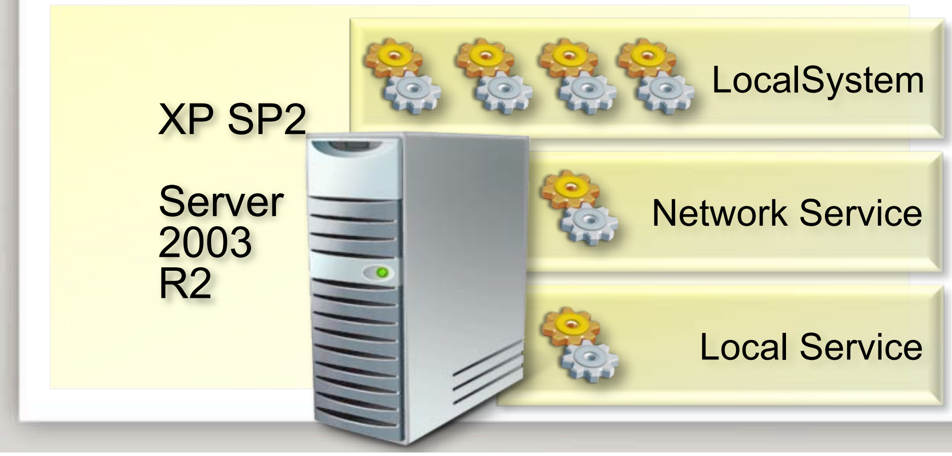
Hardware Support Components – Disk, Network Adapter, etc.

Server Protection Features

- **Secure Startup**
  - Hardware based
  - Protects against data theft when system is offline or while the OS is being installed
- **Code Integrity**
  - Protects OS files when system is running
  - Signs all OS executables and DLLs
  - Signatures are checked for validity when files are loaded into memory

Windows Services Hardening

- Windows Services are profiled for allowed actions
- Reduces size of high-risk layers
- Segments the services
- Increases number of layers



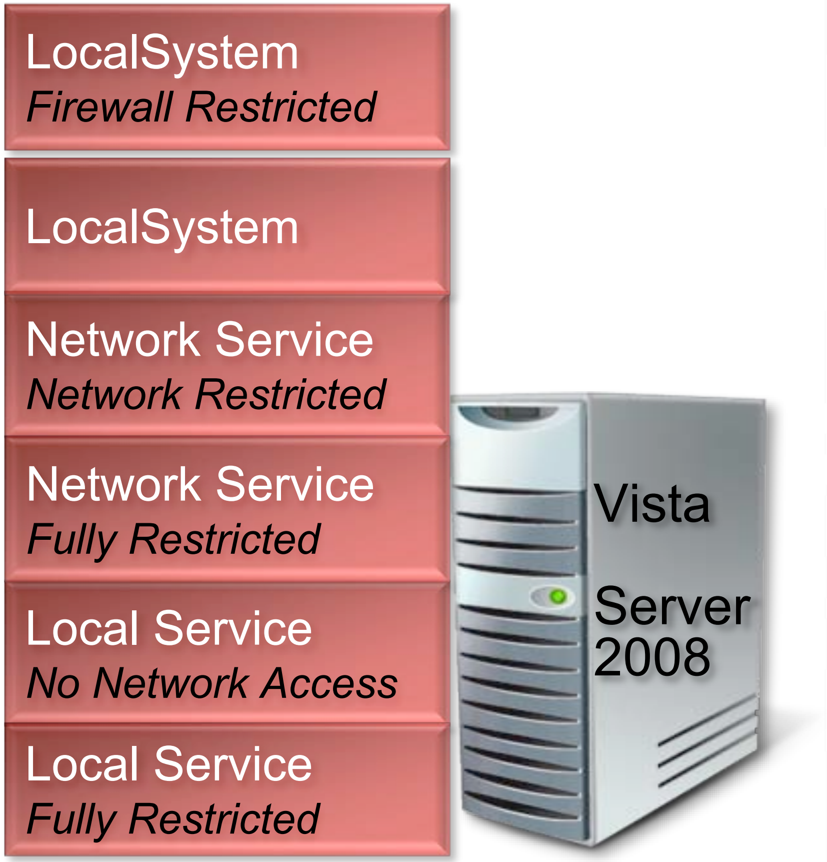
XP SP2

Server 2003 R2

LocalSystem

Network Service

Local Service



LocalSystem
Firewall Restricted

LocalSystem

Network Service
Network Restricted

Network Service
Fully Restricted

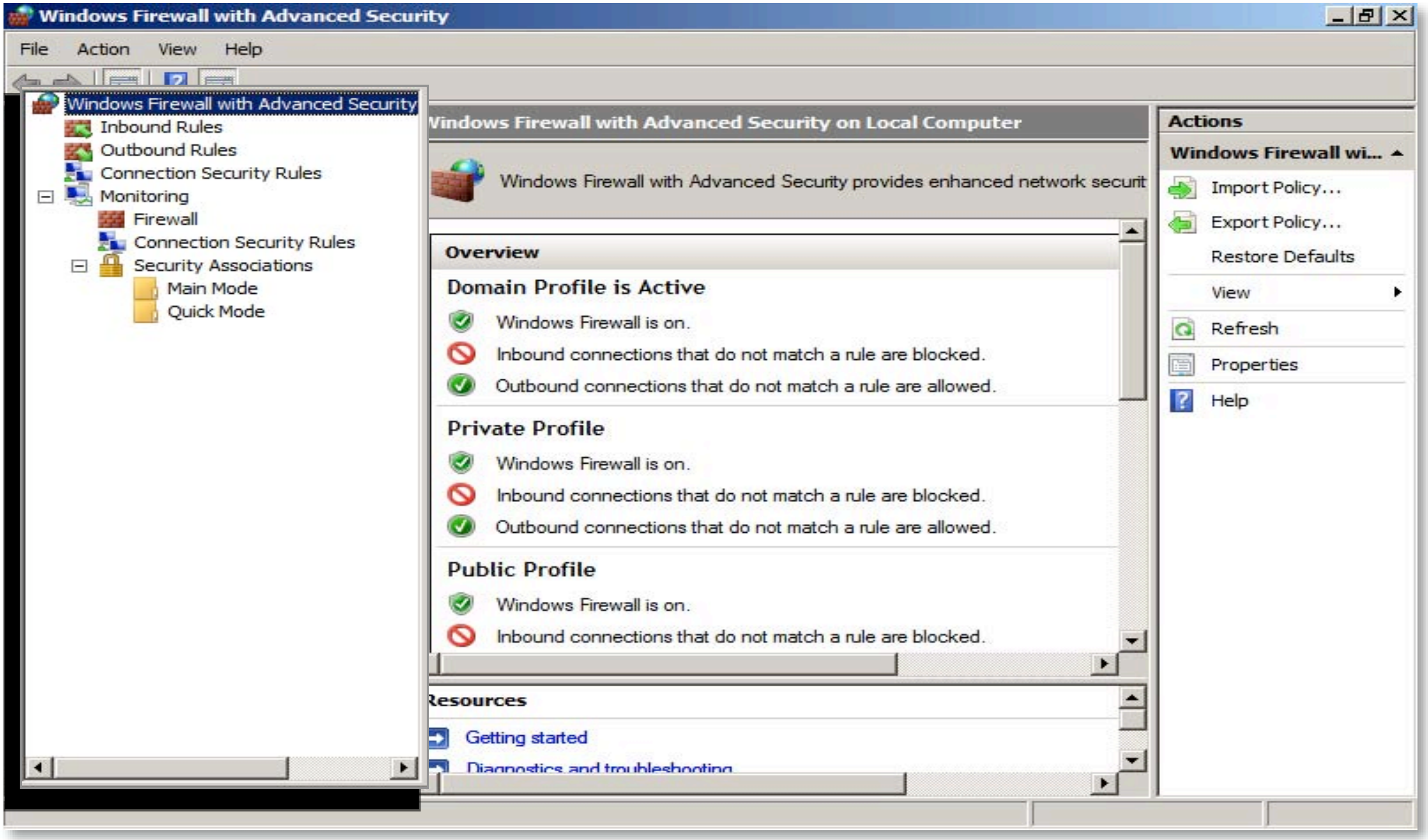
Local Service
No Network Access

Local Service
Fully Restricted

Vista

Server 2008

Combined Firewall and IPSec Management



Vindows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides enhanced network securit

Overview

Domain 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.

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.

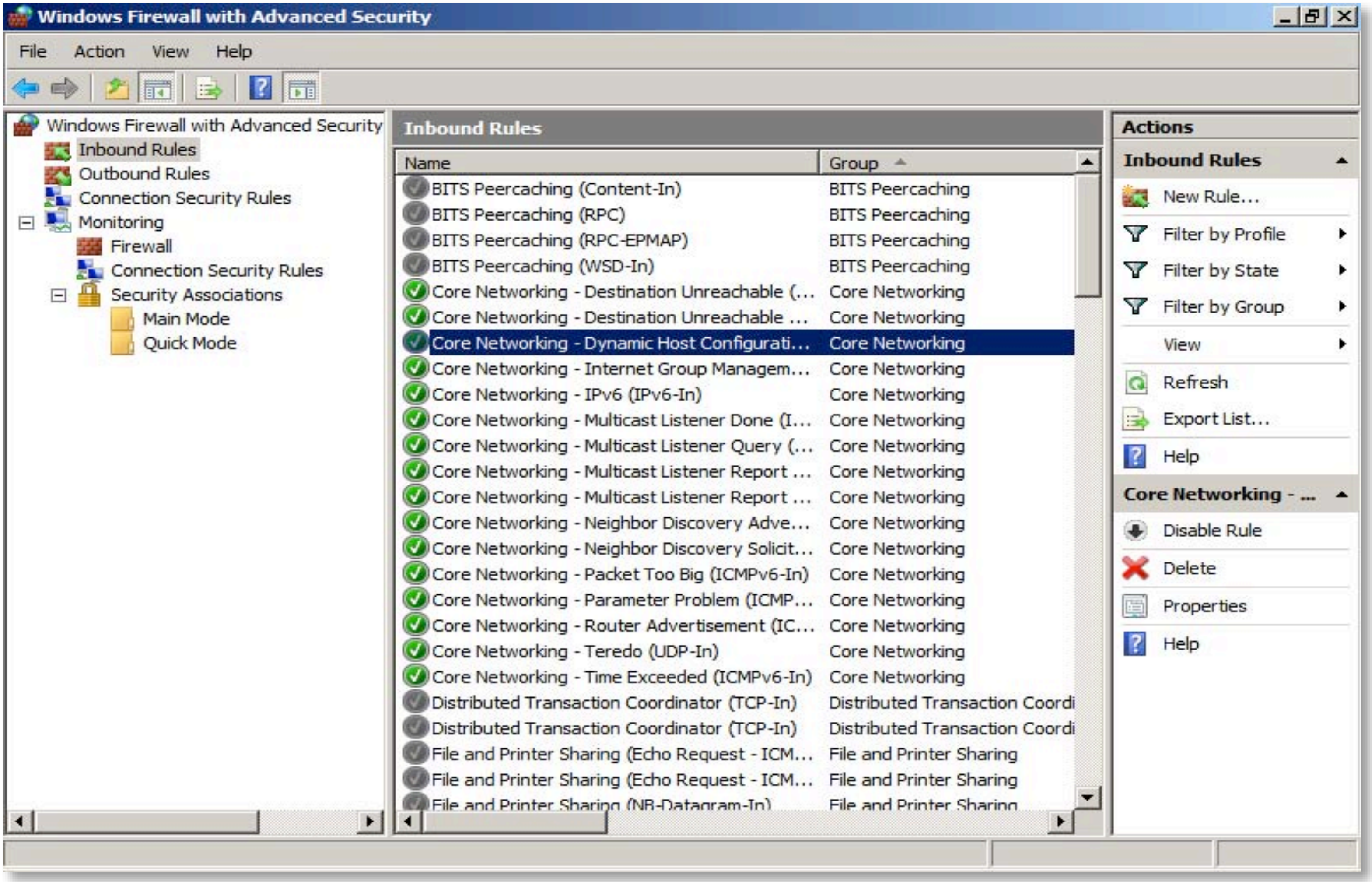
Public Profile

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

Resources

- Getting started
- Diagnostics and troubleshooting

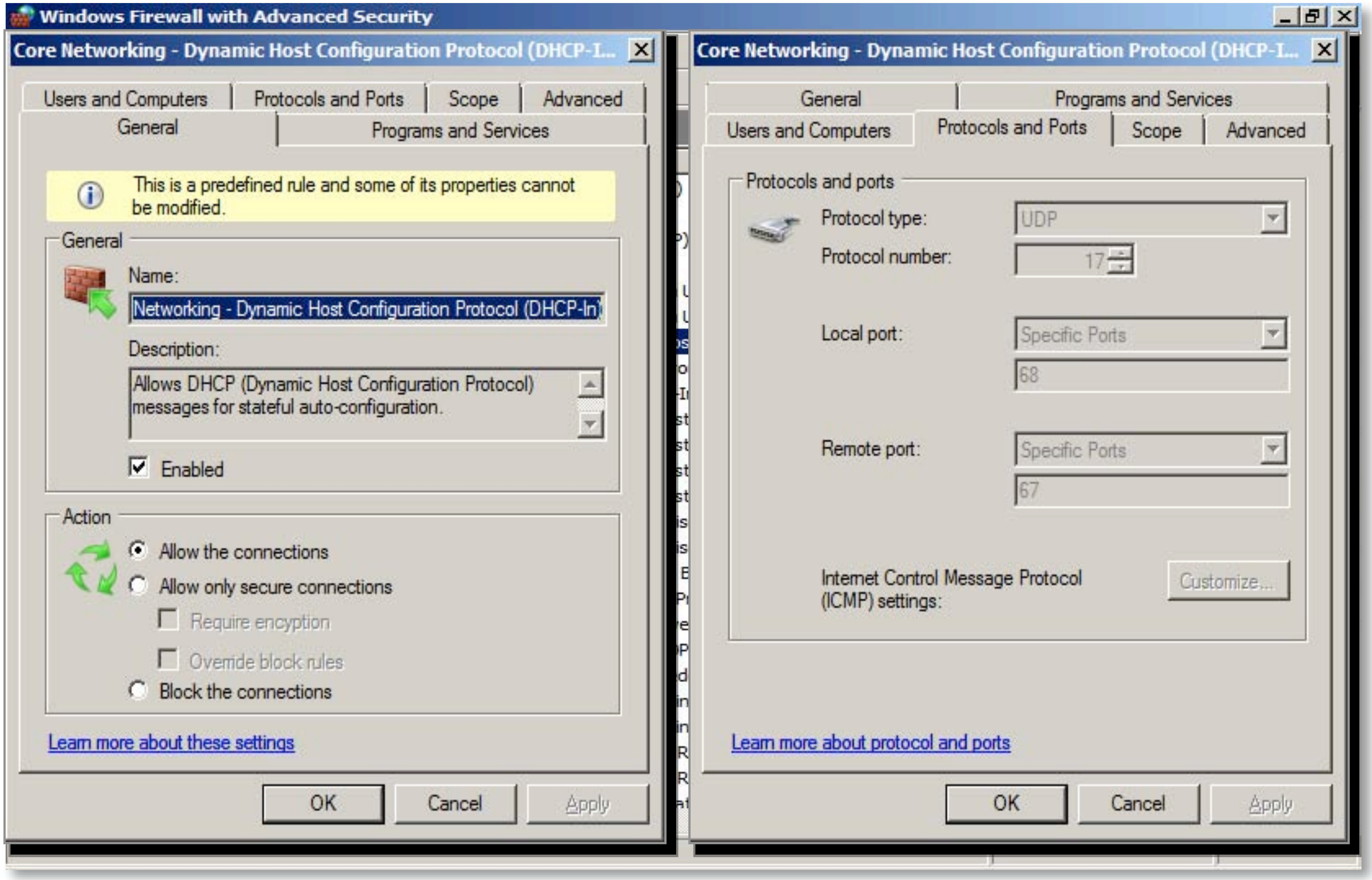
Firewall Rules are More Intelligent



Inbound Rules

Name	Group
BITS Peercaching (Content-In)	BITS Peercaching
BITS Peercaching (RPC)	BITS Peercaching
BITS Peercaching (RPC-EPMAP)	BITS Peercaching
BITS Peercaching (WSD-In)	BITS Peercaching
Core Networking - Destination Unreachable (...	Core Networking
Core Networking - Destination Unreachable ...	Core Networking
Core Networking - Dynamic Host Configurati...	Core Networking
Core Networking - Internet Group Managem...	Core Networking
Core Networking - IPv6 (IPv6-In)	Core Networking
Core Networking - Multicast Listener Done (I...	Core Networking
Core Networking - Multicast Listener Query (...	Core Networking
Core Networking - Multicast Listener Report ...	Core Networking
Core Networking - Multicast Listener Report ...	Core Networking
Core Networking - Neighbor Discovery Adve...	Core Networking
Core Networking - Neighbor Discovery Solicit...	Core Networking
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking
Core Networking - Parameter Problem (ICMP...	Core Networking
Core Networking - Router Advertisement (IC...	Core Networking
Core Networking - Teredo (UDP-In)	Core Networking
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coordi
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coordi
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing

Firewall Rules are More Intelligent


Windows Firewall with Advanced Security
Core Networking - Dynamic Host Configuration Protocol (DHCP-I...
Users and Computers
Protocols and Ports
Scope
Advanced
General
Programs and Services
OK
Cancel
Apply

This is a predefined rule and some of its properties cannot be modified.

General

Name: Networking - Dynamic Host Configuration Protocol (DHCP-In)

Description: Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.

☑ Enabled

Action

● Allow the connections

○ Allow only secure connections

□ Require encryption

□ Override block rules

○ Block the connections

Learn more about these settings

Protocols and ports

Protocol type: UDP

Protocol number: 17

Local port: Specific Ports

68

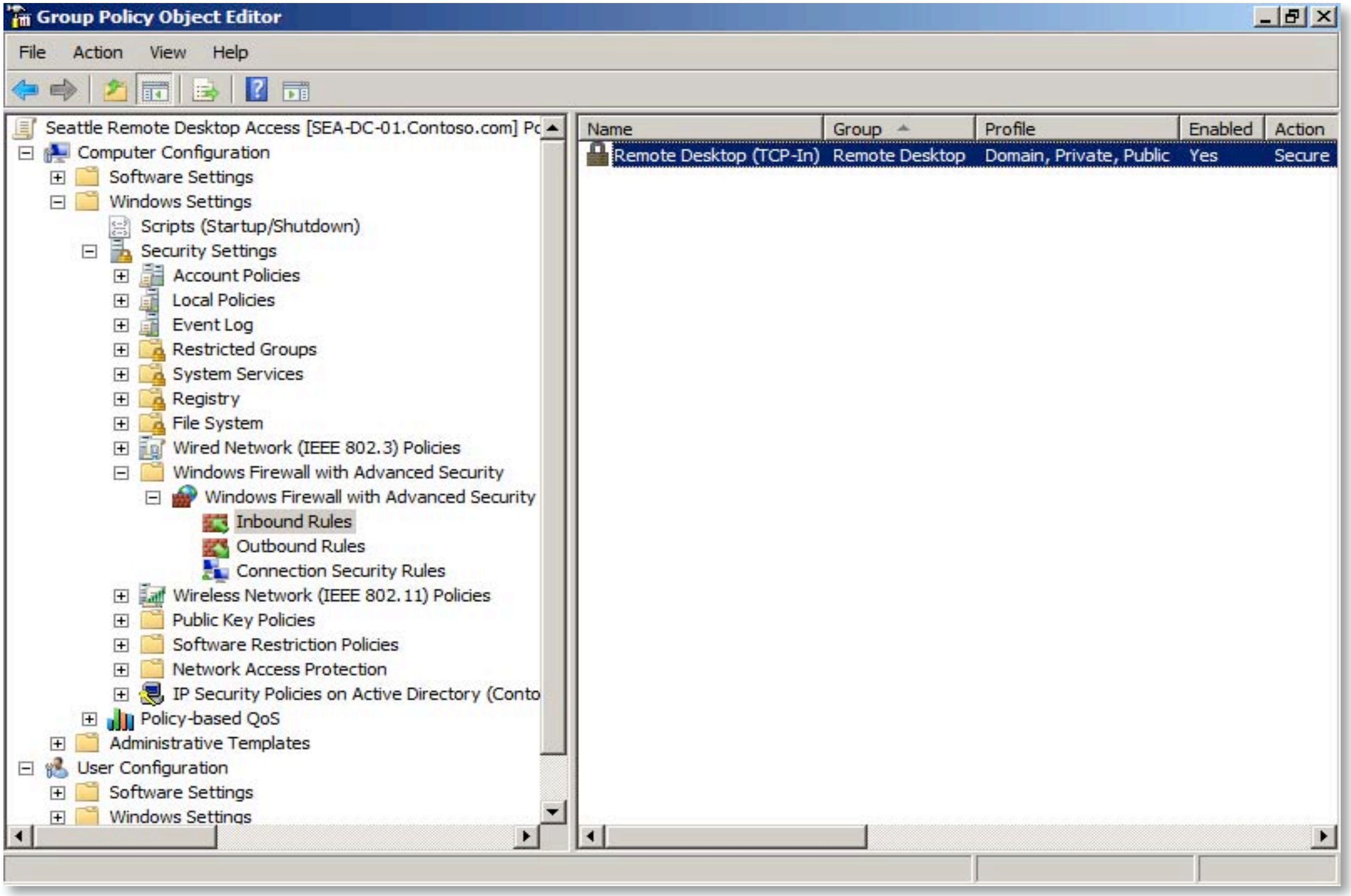
Remote port: Specific Ports

67

Internet Control Message Protocol (ICMP) settings: Customize...

Learn more about protocol and ports

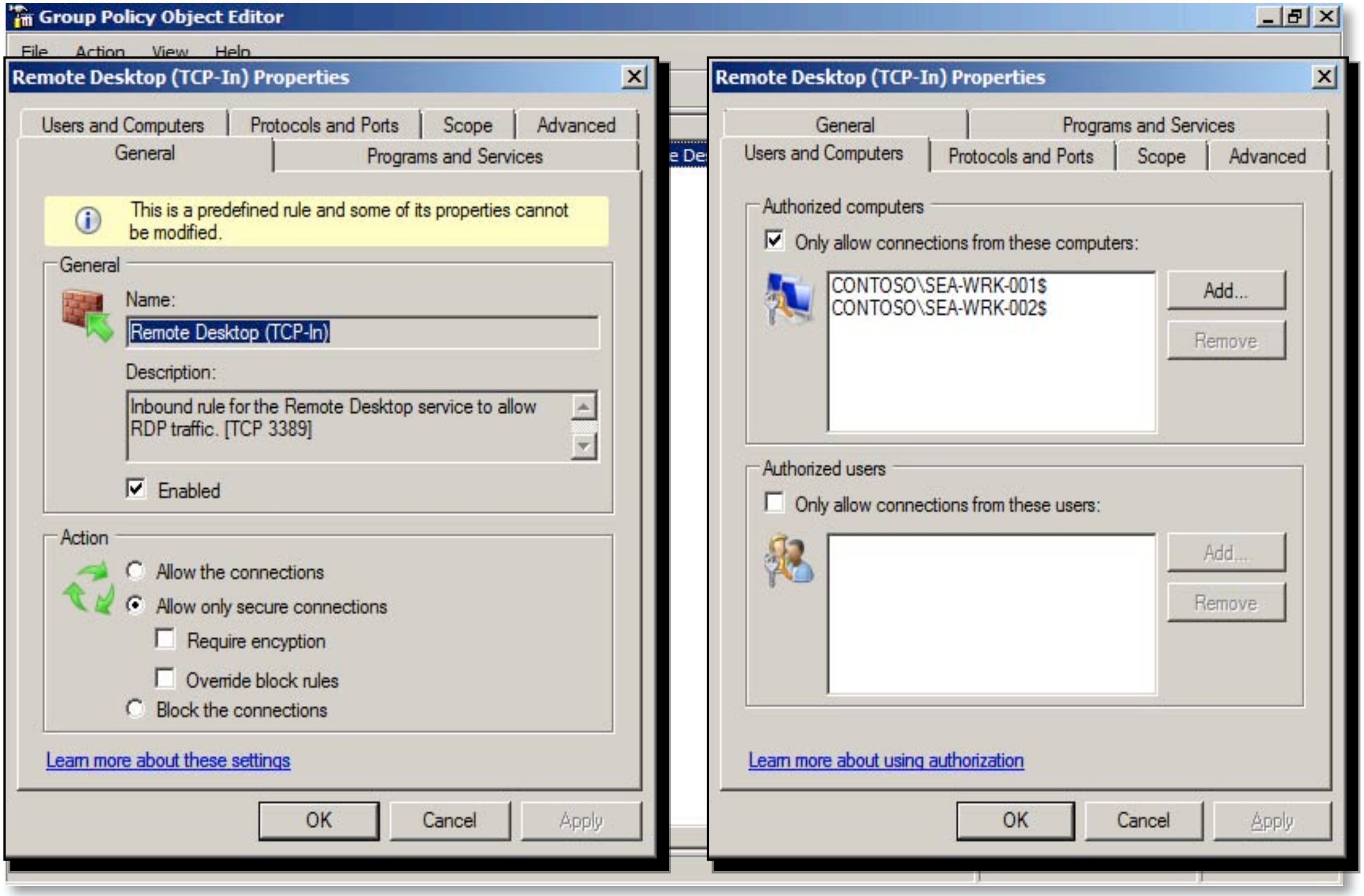
Policy-Based Networking



- Seattle Remote Desktop Access [SEA-DC-01.Contoso.com] Pc
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Security
          - Windows Firewall with Advanced Security
            - Inbound Rules
            - Outbound Rules
            - Connection Security Rules
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection
        - IP Security Policies on Active Directory (Conto
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings

Name	Group	Profile	Enabled	Action
Remote Desktop (TCP-In)	Remote Desktop	Domain, Private, Public	Yes	Secure

Policy-Based Networking



Group Policy Object Editor
File Action View Help

Remote Desktop (TCP-In) Properties

Users and Computers | Protocols and Ports | Scope | Advanced
General | Programs and Services

This is a predefined rule and some of its properties cannot be modified.

General

Name: Remote Desktop (TCP-In)

Description: Inbound rule for the Remote Desktop service to allow RDP traffic. [TCP 3389]

☑ Enabled

Action

○ Allow the connections

● Allow only secure connections

□ Require encryption

□ Override block rules

○ Block the connections

Learn more about these settings

Remote Desktop (TCP-In) Properties

General | Programs and Services
Users and Computers | Protocols and Ports | Scope | Advanced

Authorized computers

☑ Only allow connections from these computers:

CONTOSO\SEA-WRK-001$
CONTOSO\SEA-WRK-002$

Authorized users

□ Only allow connections from these users:

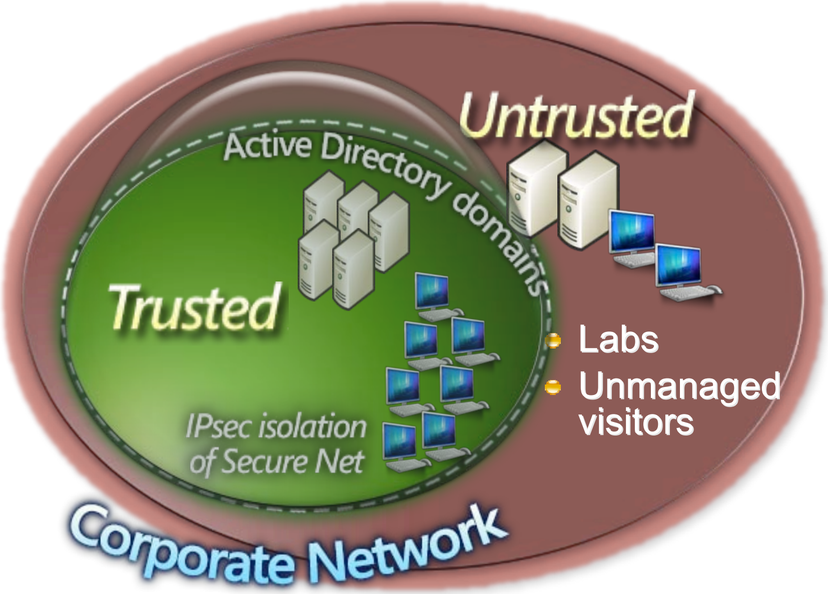
Learn more about using authorization

Active Directory Domain Services (AD DS) Auditing

- **More Granularity**
  - Support for many auditing subcategories: Logon, logoff, file system access, registry access, use of administrative privilege, Active Directory
  - Captures the who, the what & the when
  - From and To values for objects or attributes
  - Logs All: Creates, modifies, moves, deletes
- **New Logging Infrastructure**
  - Easier to filter out “noise” in logs
  - Tasks tied to events: When an event occurs, tasks such as sending an email to an auditor can run automatically

Domain Protection: Server and Domain Isolation

Dynamically segment Windows environments into more secure and isolated logical networks based on policy



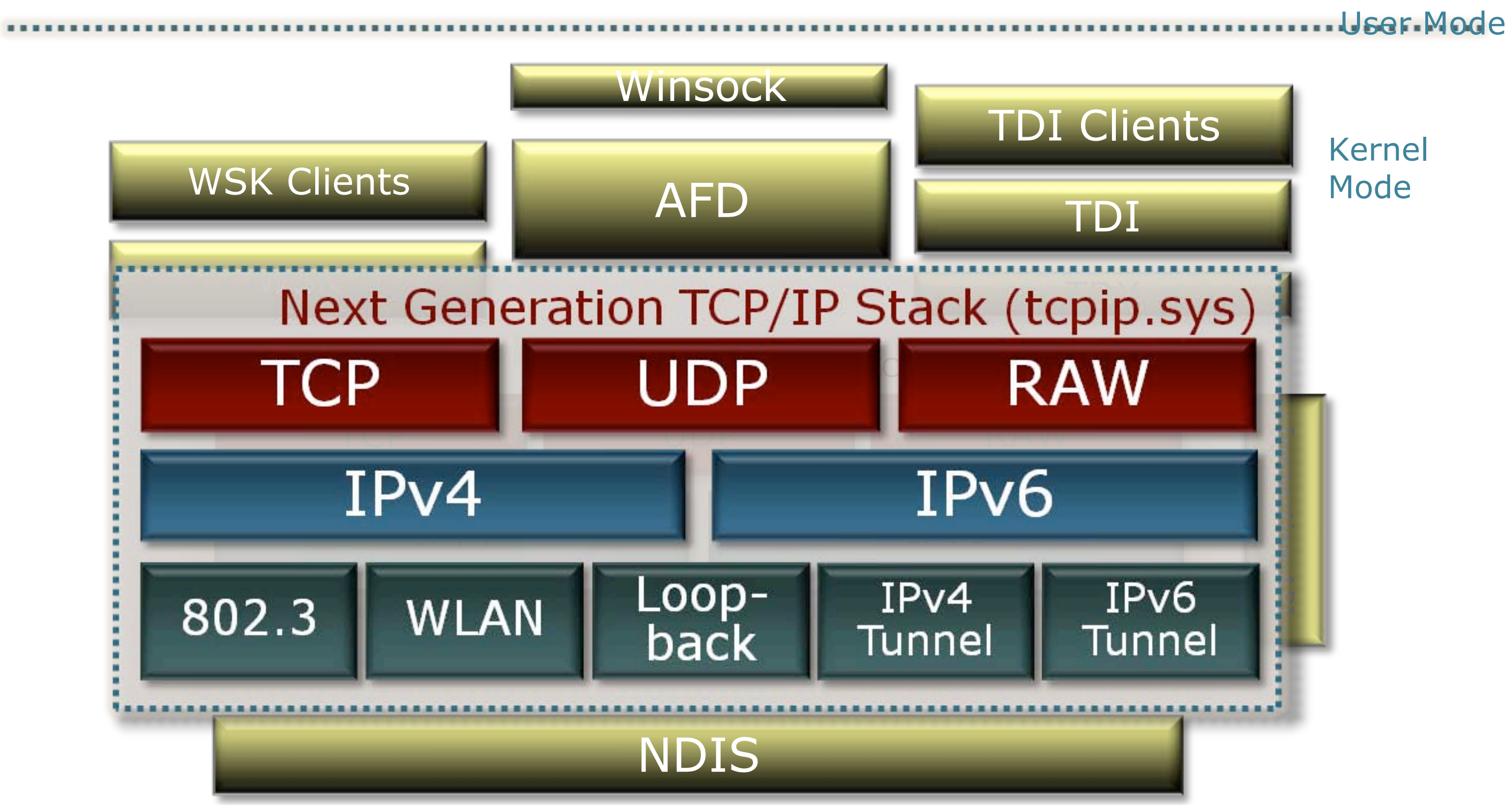
Server Isolation — Protect specific high-value servers and data

Domain Isolation — Protect managed computers from unmanaged or rogue computers and users

Read-Only Domain Controller

- **Features**
  - Read-only Active Directory database
  - Only allowed user passwords stored on RODC
  - Unidirectional replication for AD and FRS/DFSR
  - Role separation
- **Benefit**
  - Increases security for remote domain Controllers where physical security cannot be guaranteed

Network Protection: Next Generation TCP/IP



- Dual-IP layer architecture for native IPv4 and IPv6 support
- Greater extensibility and reliability through rich APIs

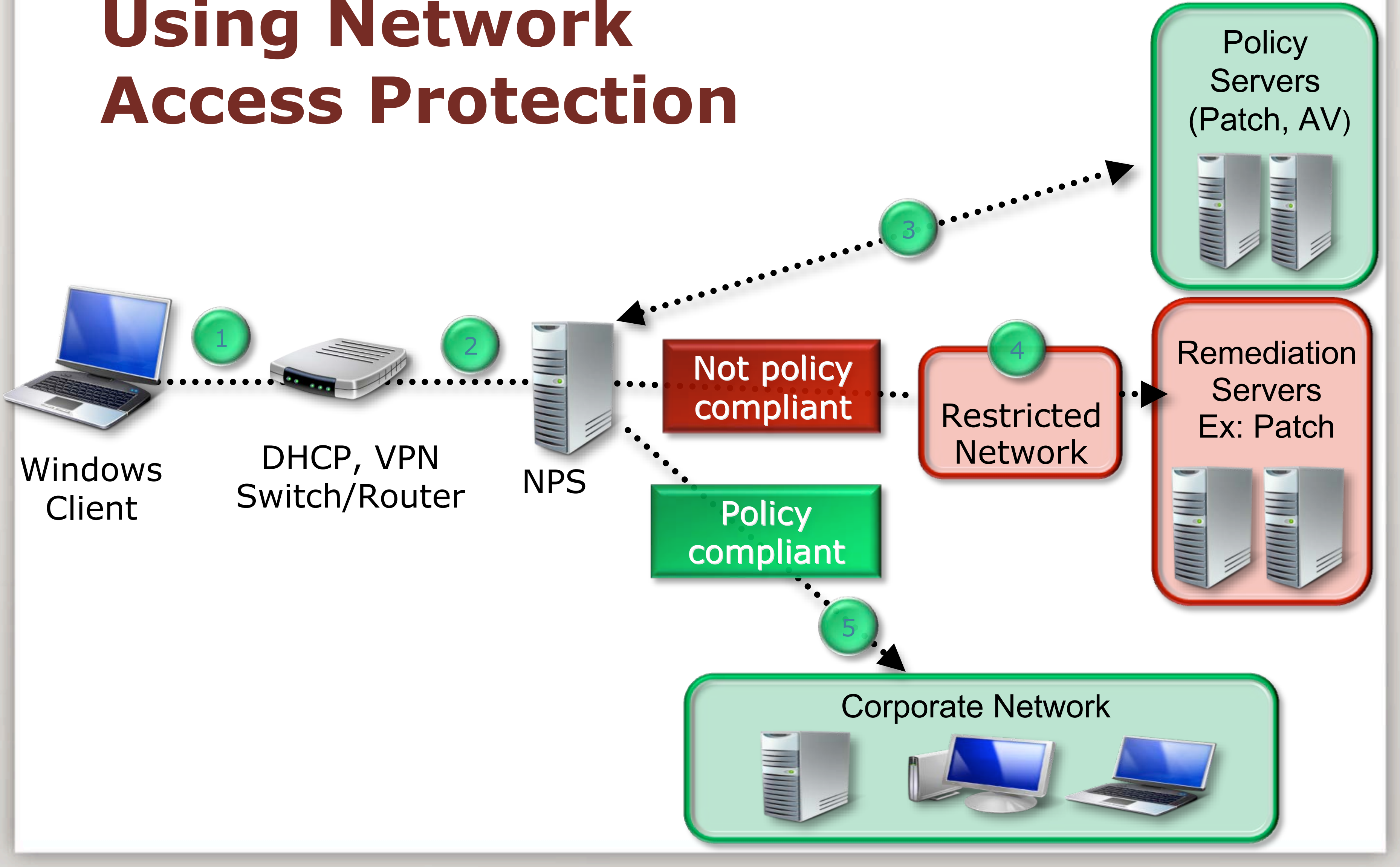
Internet Protocol Security (IPsec)

- **Enhancements**
  - Simplified IPsec Policy Configuration
  - Client-to-DC IPsec Protection
  - Improved Load Balancing and Clustering Server Support
  - Improved IPsec Authentication
  - Integration with NAP
  - Multiple Authentication Methods
  - New Cryptographic Support
  - Integrated IPv4 and IPv6 Support
  - Extended Events and Performance Monitor Counters
  - Network Diagnostics Framework Support
- **Integrated with WFAS**

Methods of Policy Enforcement

- Network Location Awareness (NLA)
  - Monitors network for any changes
  - Constant awareness – no longer dependent on ICMP
  - Network border devices won’t inhibit processing
- Network Access Protection (NAP)
  - Checks system health & restricts access of systems that are not in compliance
    - Roaming laptops
    - Desktop computers
    - Visiting laptops
    - Unmanaged home computers

Using Network Access Protection



NAP - Better Security and Business Value

Health and Policy Validation

Defense at Multiple Layers

Risk Level

Enhanced Security

- All communications are authenticated, authorized & healthy
- Defense-in-depth on your terms with DHCP, VPN, IPSec, 802.1X
- Policy-based access that can be set and controlled

Increased Business Value

- Preserves user productivity
- Extends existing investments in Microsoft and 3rd party infrastructure
- Broad industry partnership

ROI

Healthy Endpoints Connect

Leverage Existing Investments

Data Protection: Removable Device Control

- Group Policy settings
- Control how devices may/may not be used
  - Prevent users from installing any device
  - Allow installation of devices on an “approved list”
  - Prevent installation of devices on a “prohibited list”
  - Deny read or write access to users for devices that are themselves removable or that use removable media

BitLocker Drive Encryption

- **Drive Protection and Integrity Checking**
  - Simple and comprehensive volume encryption solution - TPM provides non-intrusive layer of physical security
  - Integrated disaster recovery features
  - Decommission old hard drives w/o requiring physical destruction
  - Government regulations
- **BDE Hardware and Software Requirements**
  - Windows Server 2008 or Vista
  - TPM microchip, version 1.2; a TCG-compliant BIOS
  - 2 NTFS drive partitions (system volume and OS volume)
  - BIOS set to start up first from hard drive, not USB or CD

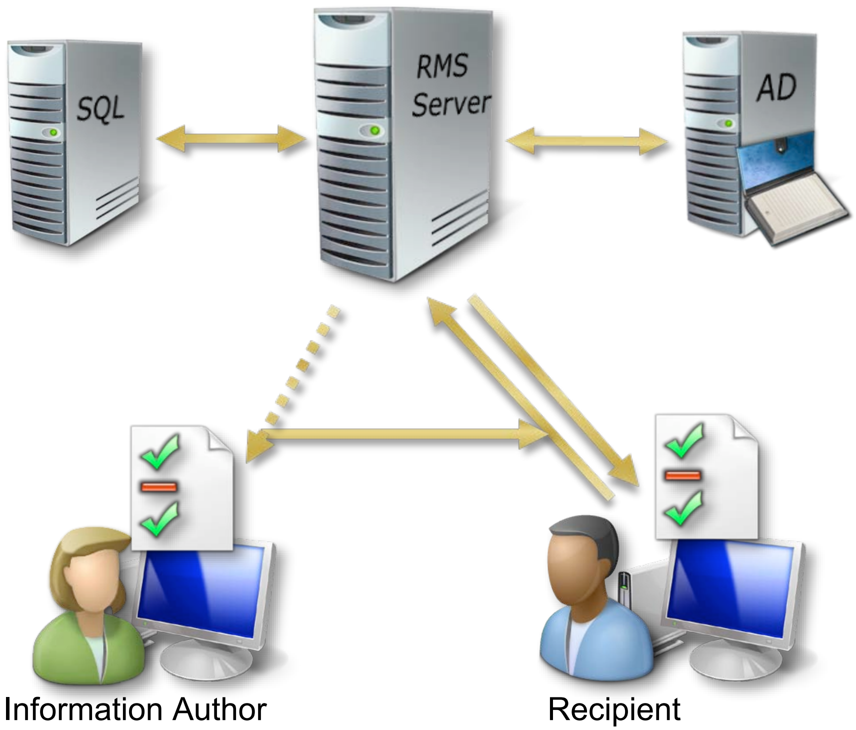
Who are you protecting against?

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

Scenarios	BitLocker	EFS	RMS
Laptops	●		
Remote 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)

AD Rights Management Services



- Protects access to an organization’s digital files
- Protects access to an organization’s digital files
- Includes several new features
- Improved installation and administration experience
- Self-enrollment of the AD RMS cluster
- Integration with AD Federation Services
- New AD RMS administrative roles

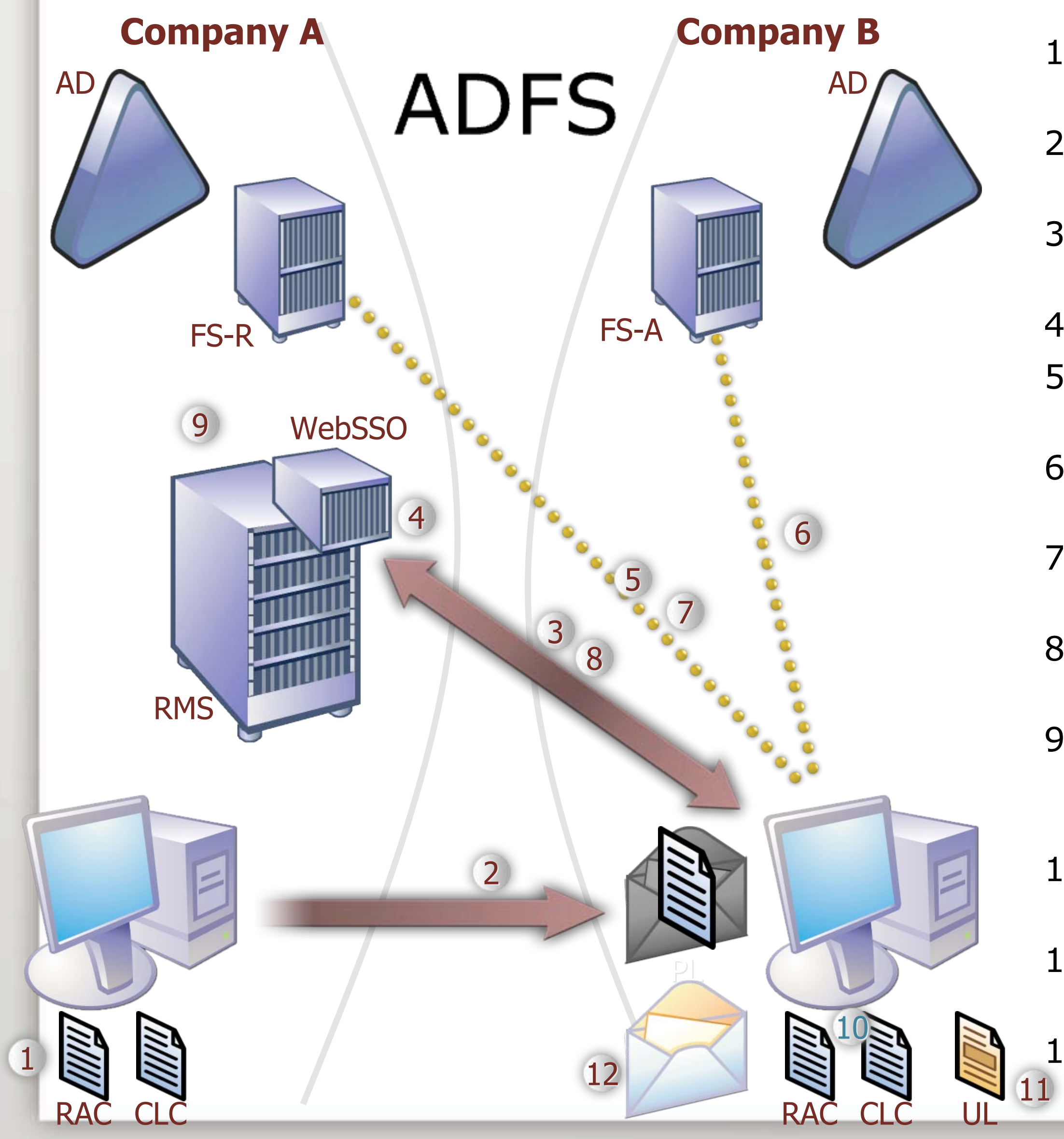
Combine with *ADFS*

Federated Collaboration

- Collaborate with external entities
  - RMS is a supported claims-aware app
  - SharePoint becomes claims-aware

Easing Management

- Simplified Deployments - Native Platform Integration
- Stronger Administrative Controls
- Better Informed Administrators



1. Assume author is already bootstrapped
2. Author sends protected email to recipient at Company A
3. Recipient contacts Company ARMS server to get bootstrapped
4. WebSSO agent intercepts request
5. RMS client is redirected to FS-R for home realm discovery
6. RMS client is redirected to FS-A for authentication
7. RMS client is redirected back to FS-R for authentication
8. RMS client makes request to RMS server for bootstrapping
9. WebSSO agent intercepts request, checks authentication, and sends request to RMS server
10. RMS server returns bootstrapping certificates to recipient
11. RMS server returns use license to recipient
12. Recipient accesses protected content

Authentication Improvements

- **Plug and Play Smart Cards**
  - Drivers and Certificate Service Provider (CSP) included
  - 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 with much less coding

Granular Password Control

- Password policies can be set on users and/or groups (different from the domain‘s password policies)
- Requirements for different password policies no longer result in deploying multiple domains
- New in Active Directory - Password Settings Object
- Password settings are configured using those objects in the Password Settings Container

PKI Enhancements

Enterprise PKI (PKIView)

- Now a Microsoft Management Console snap-in
- Support for Unicode characters

Online Certificate Status Protocol (OSCP)

- Online responders
- Responder arrays

Network Device Enrollment Service

- Simple Certificate Enrollment Protocol (SCEP)
- Enhances communications security by using IPsec

Web Enrollment

- Removed previous ActiveX® enrollment control - XEnroll.dll
- Enhanced new COM enrollment control - CertEnroll.dll

Cryptography Next Generation (CNG)

- Includes algorithms for encryption, digital signatures, key exchange, and hashing
- Supports cryptography in kernel mode
- Supports the current set of CryptoAPI 1.0 algorithms
- Support for elliptic curve cryptography (ECC) algorithms
- Perform basic cryptographic operations, such as creating hashes and encrypting and decrypting data

Windows Server 2008 in brief:

- Improved server protection through server core, Windows service hardening, and improvements to Windows firewall and advanced security
- Improved domain protection through AD Domain Services Auditing, Server and Domain Isolation, and read-only domain controllers
- Improved network protection in the TCP/IP stack, IPSec, network location awareness, and network access protection
- Improved data protection with removable device control, BitLocker drive encryption, and rights management services
- Improved identity and access control through AD federation services, authentication, and enterprise PKI

The Question:

Are Windows Server 2008 and Windows Vista really more secure?

The Answer:

Absolutely!