# Усовершенствования системы безопасности Windows Server 2008

**Семинары TechNet. Осень 2007**

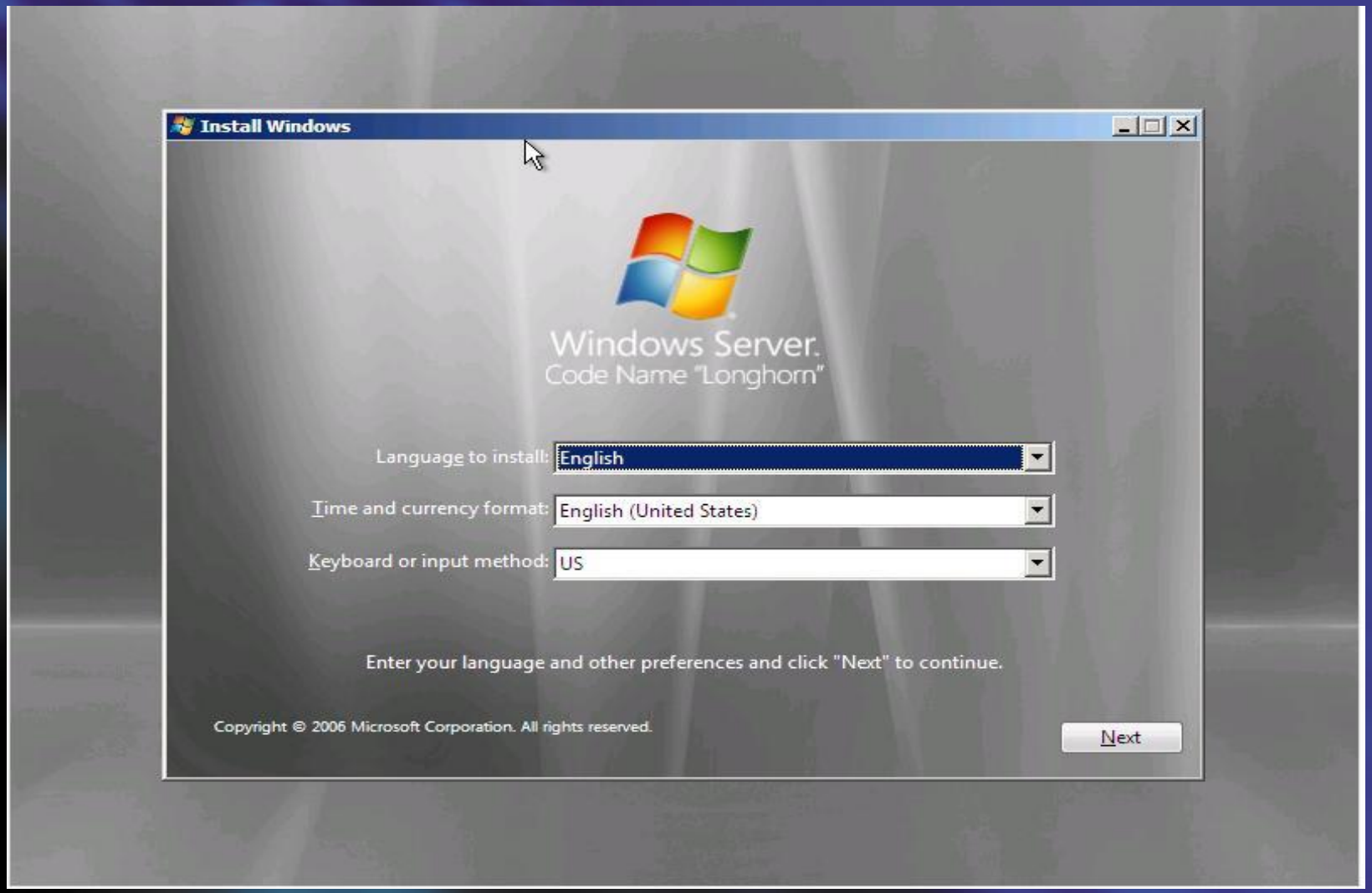
Краснодар, Казань, Новосибирск, Санкт-Петербург, Самара, Екатеринбург, Ростов-на-Дону, Н. Новгород, Владивосток, Хабаровск

Microsoft TechNet

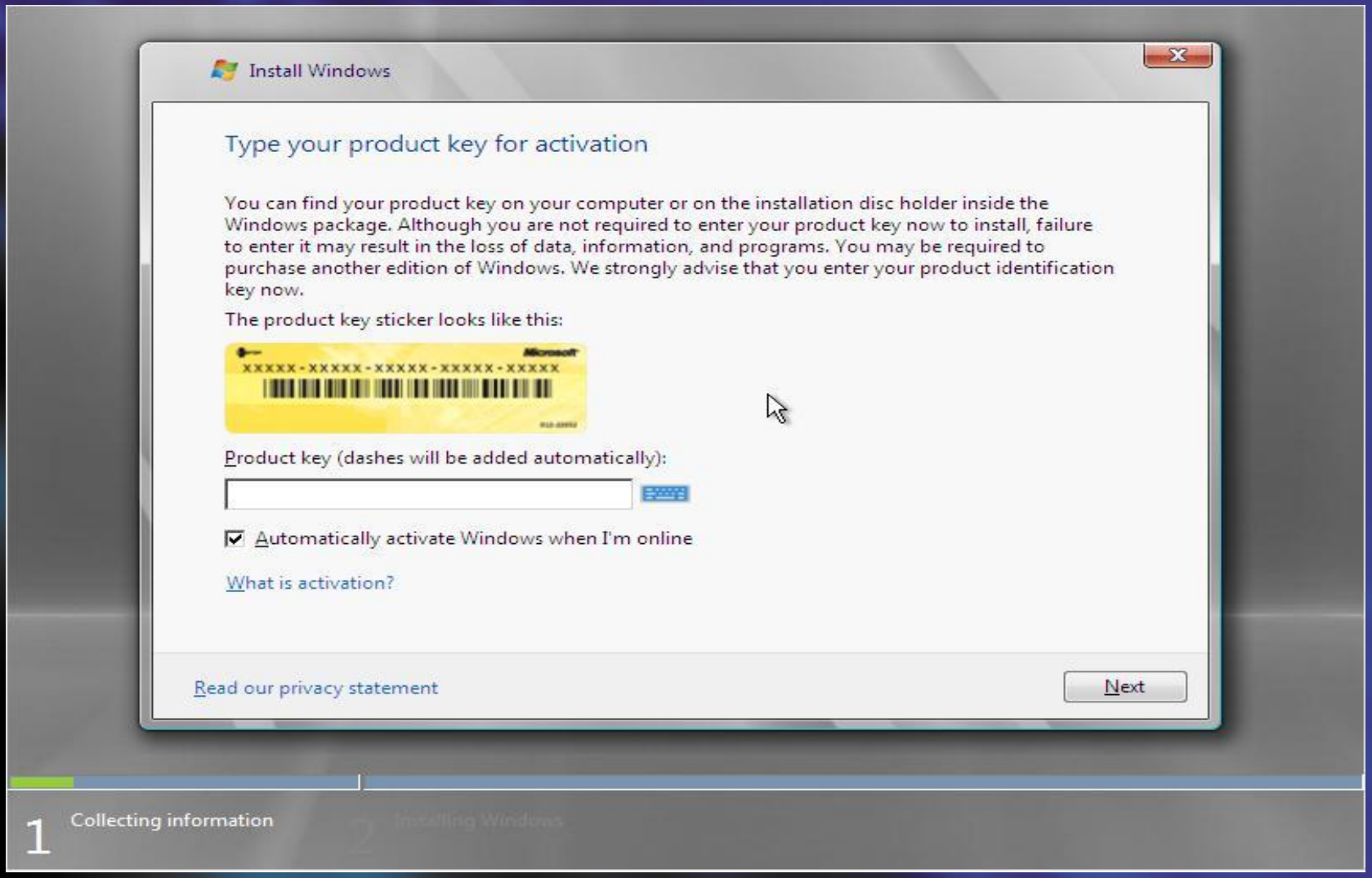
# Больше нет необходимости сидеть и пристально наблюдать за установкой системы.

- Отвечаем на 4 простых вопроса и идем пить кофе.

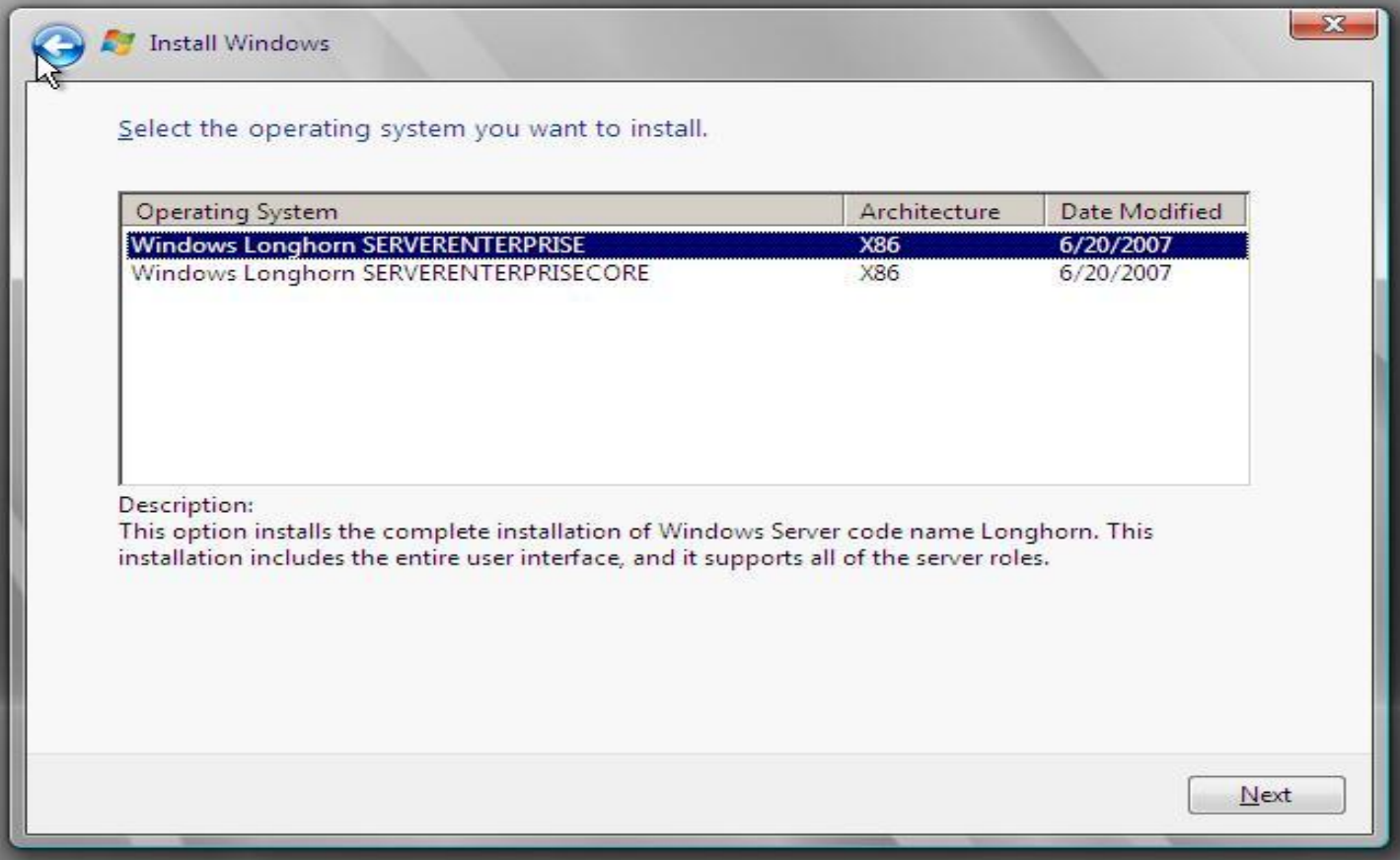
# Простота инсталляции



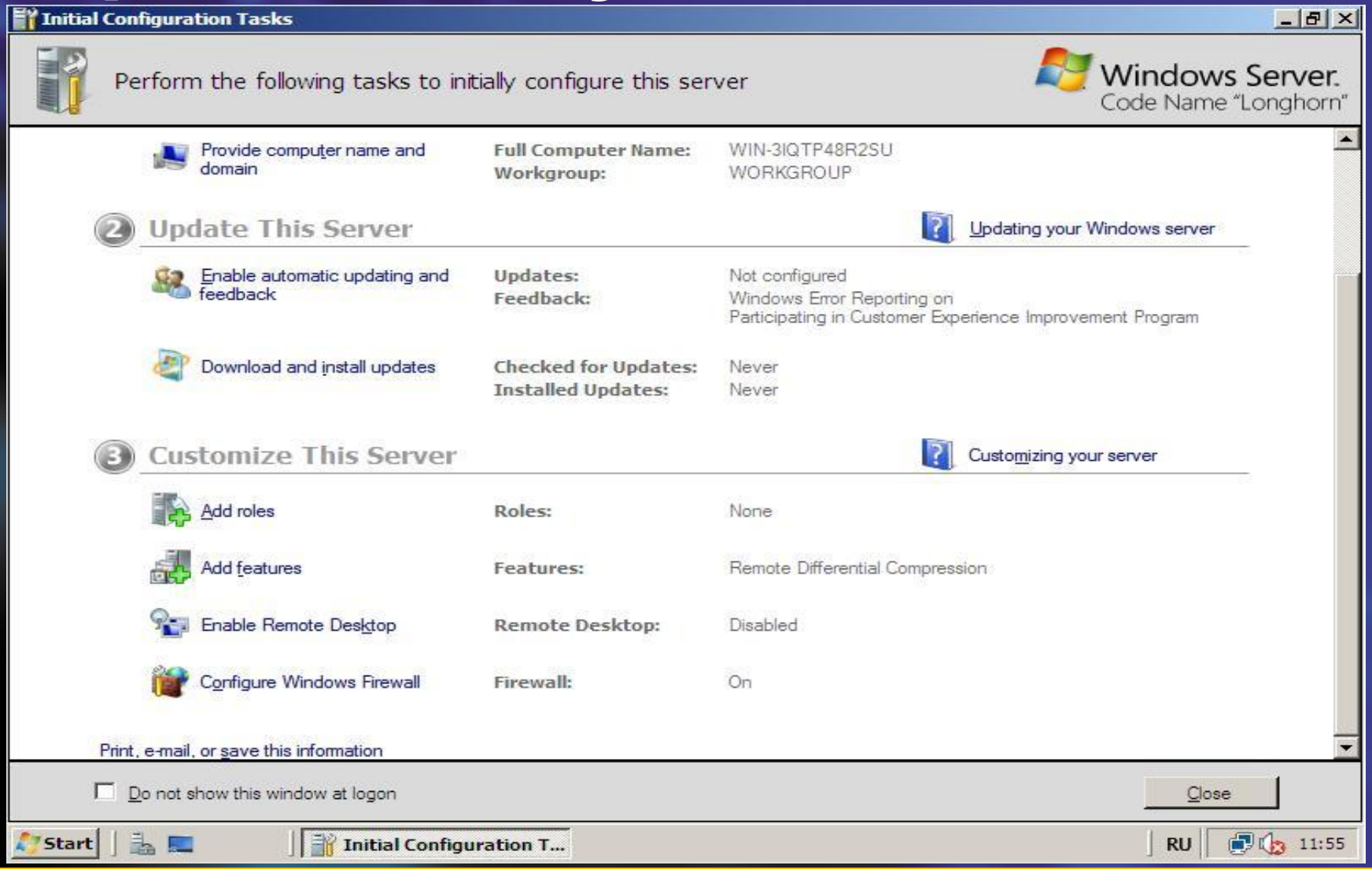
# Простота инсталляции



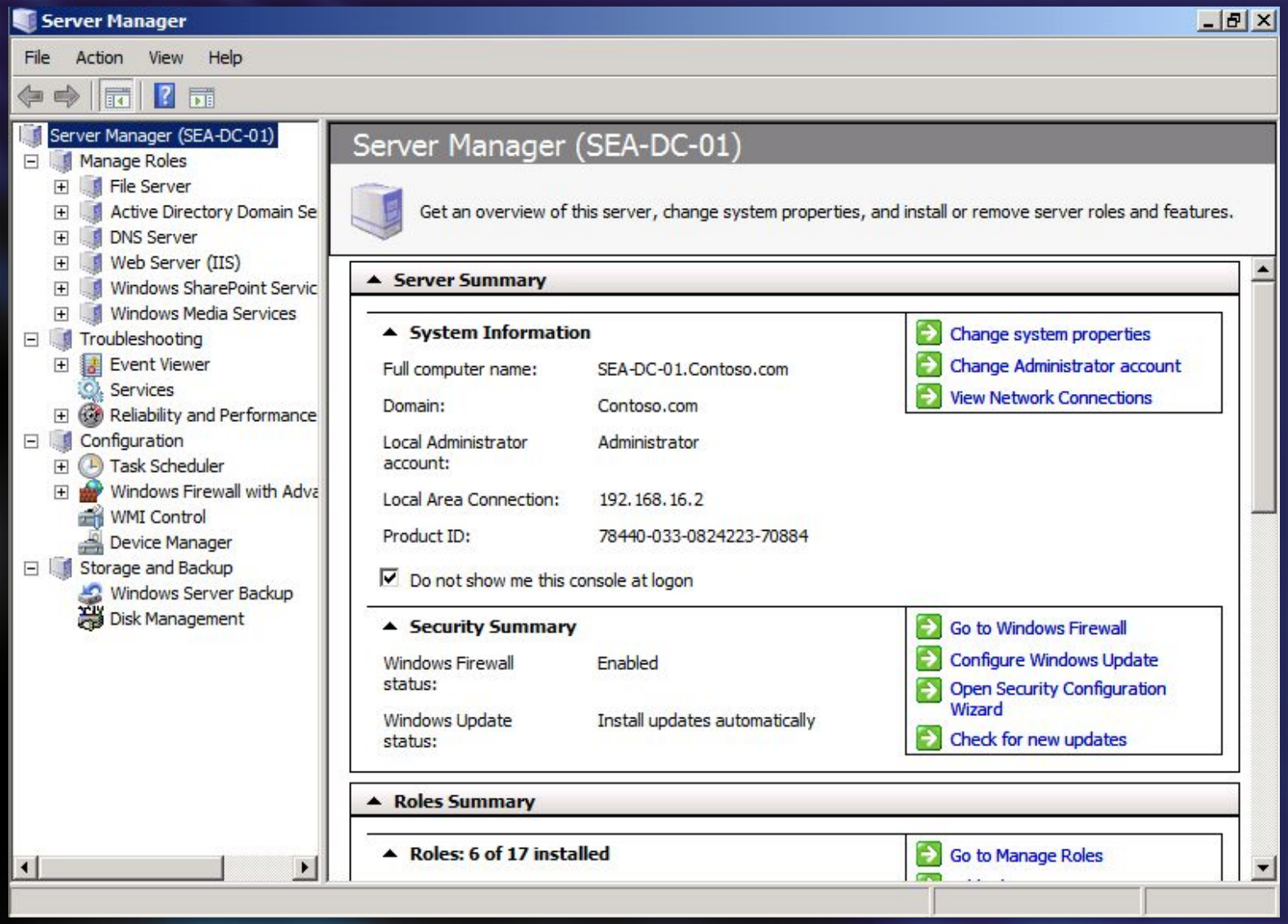
# Простота инсталляции



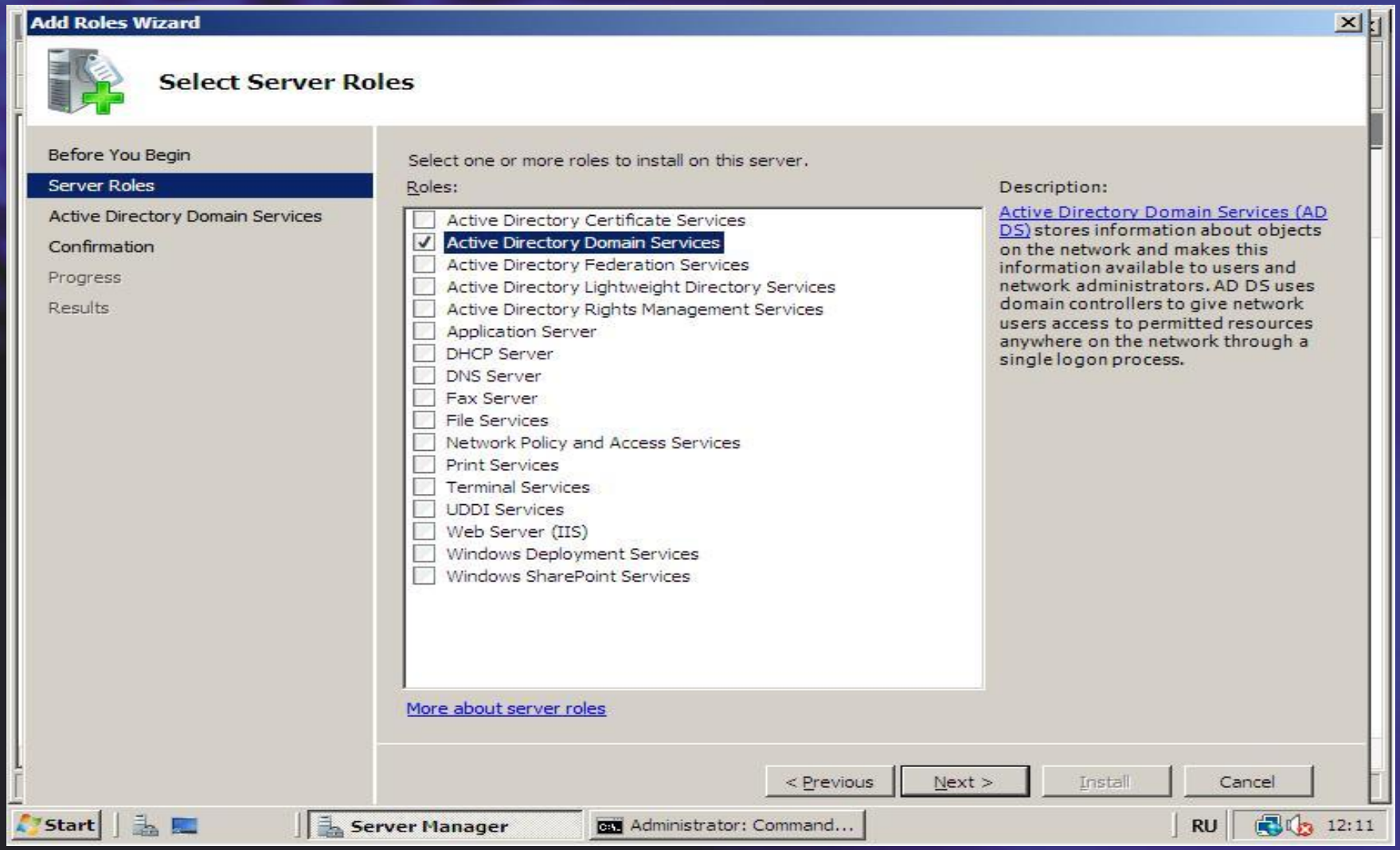
# Через 30 минут



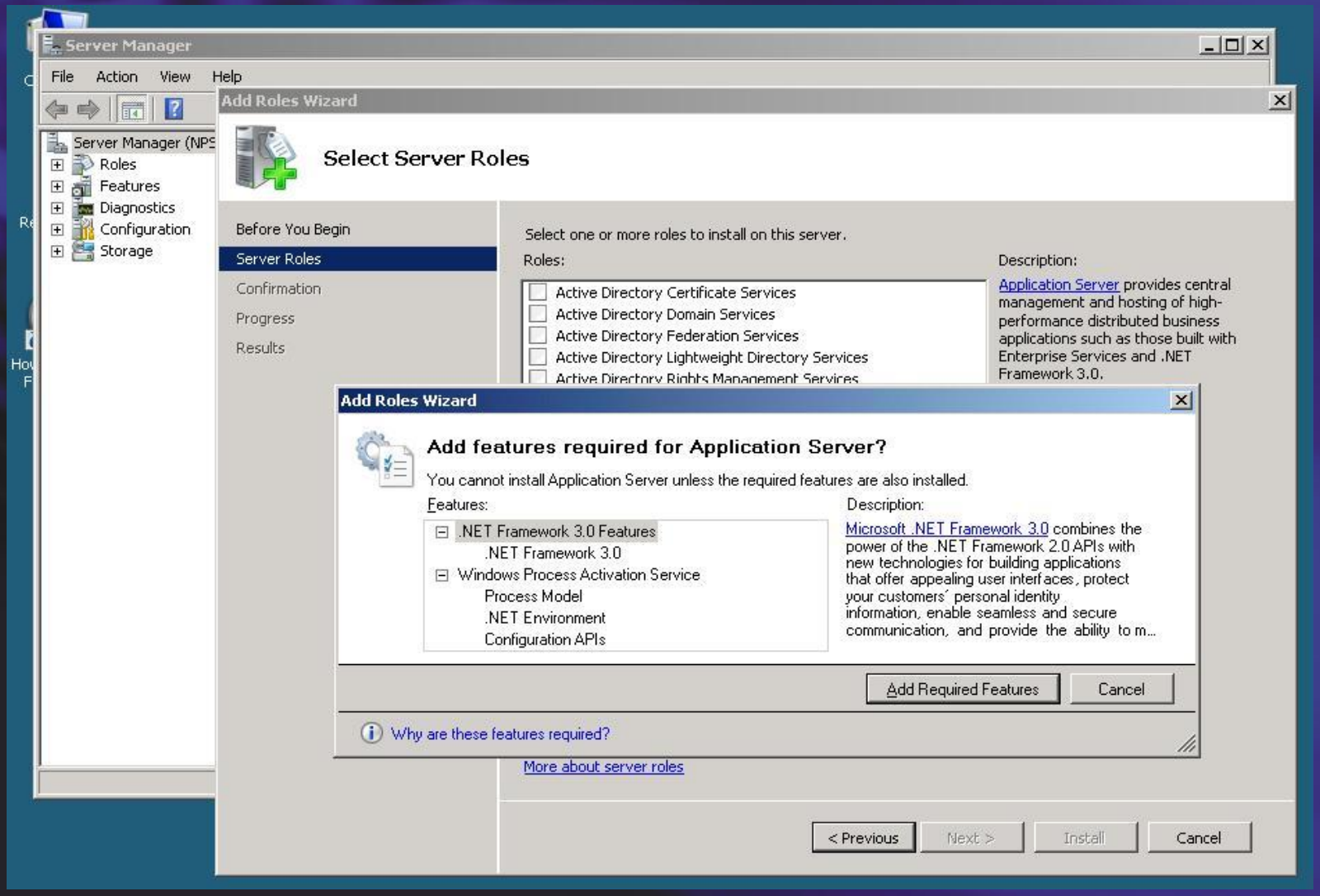
# Новый интерфейс управления



# Ролевые игры



# Ролевые игры



# Демонстрация механизма управления ролями сервера

# Безопасность сервисов

## Windows® XP SP2/Server 2003 R2

| Аккаунт | Сервисы | |
|---|---|---|
| **LocalSystem** | Wireless Configuration<br>System Event Notification<br>Network Connections (netman)<br>COM+ Event System<br>NLA<br>Rasauto<br>Shell Hardware Detection<br>Themes<br>Telephony<br>Windows Audio<br>Error Reporting<br>Workstation<br>ICS | RemoteAccess<br>DHCP Client<br>W32time<br>Rasman<br>browser<br>6to4<br>Help and support<br>Task scheduler<br>TrkWks<br>Cryptographic Services<br>Removable Storage<br>WMI Perf Adapter<br>Automatic updates<br>WMI<br>App Management<br>Secondary Logon<br>BITS |
| **Network Service** | DNS Client | |
| **Local Service** | SSDP<br>WebClient<br>TCP/IP NetBIOS helper<br>Remote registry | |

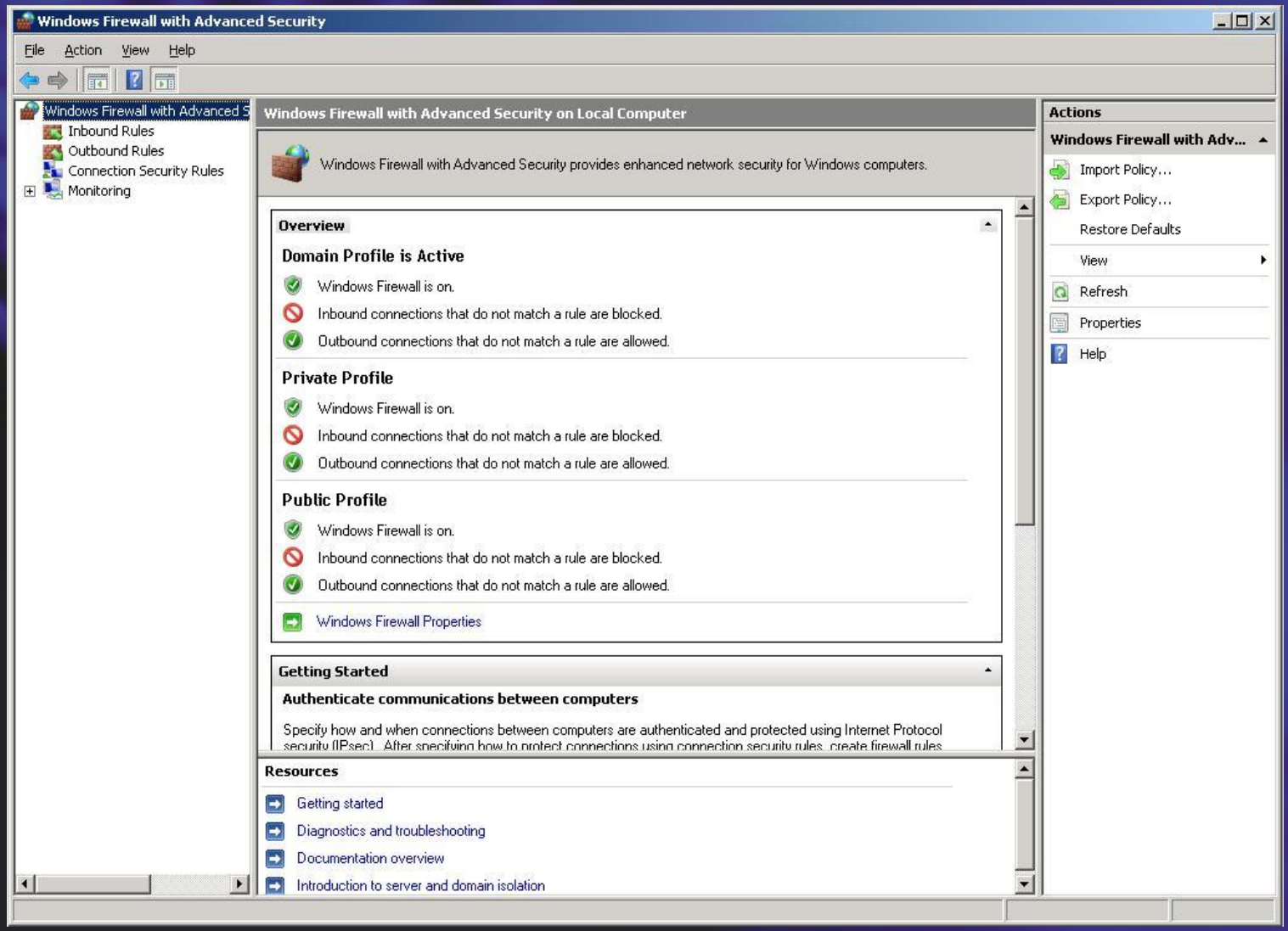
## Windows Vista/Windows Server 2008

| Аккаунт | Сервисы | |
|---|---|---|
| **LocalSystem**<br>*Защищено брандмауэром* | WMI Perf Adapter<br>Automatic updates<br>Secondary Logon | App Management<br>Wireless Configuration |
| **LocalSystem** | BITS<br>Themes<br>Rasman<br>TrkWks<br>Error Reporting | 6to4<br>Task scheduler<br>RemoteAccess<br>Rasauto<br>WMI |
| **Network Service**<br>*Полностью изолированы* | DNS Client<br>ICS<br>DHCP Client | browser<br>Server<br>W32time |
| **Network Service**<br>*Network Restricted* | Cryptographic Services<br>Telephony | PolicyAgent<br>Nlasvc |
| **Local Service**<br>*без доступа к сети* | System Event Notification<br>Network Connections<br>Shell Hardware Detection | COM+ Event System |
| **Local Service**<br>*Полностью изолированы* | Windows Audio<br>TCP/IP NetBIOS helper<br>WebClient<br>SSDP | Event Log<br>Workstation<br>Remote registry |

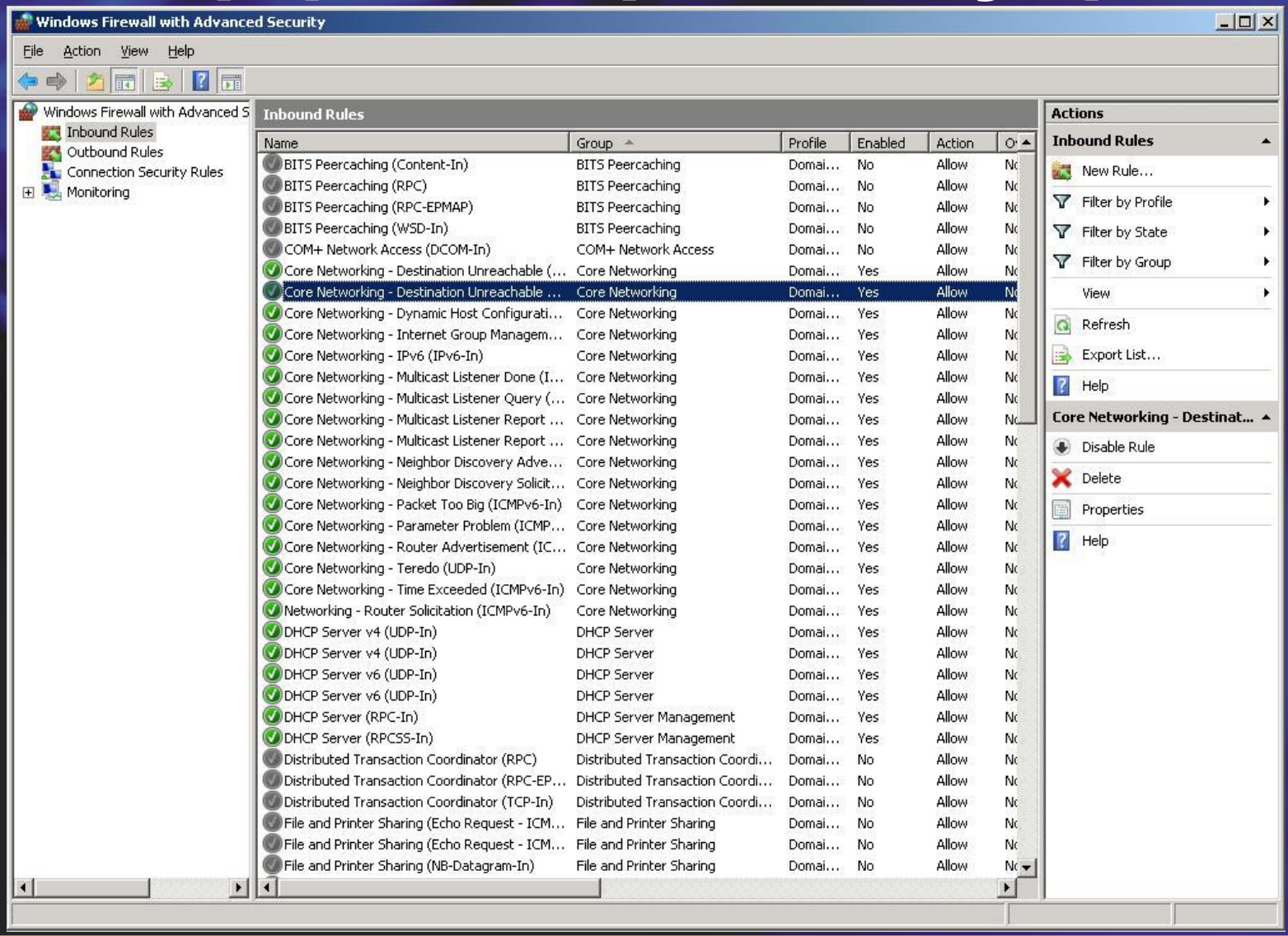
# Новый брандмауэр

- Единый интерфейс управления брандмауэром и IPsec
- Правила фильтрации трафика стали более интелектуальными
- Управление правилами на уровне компьютеров и групп пользователей Active Directory
- Двунаправленная фильтрация трафика
- Набор предустановленных правил
- Переключаемые профили
- Поддержка IPv6
- Управление с командной строки

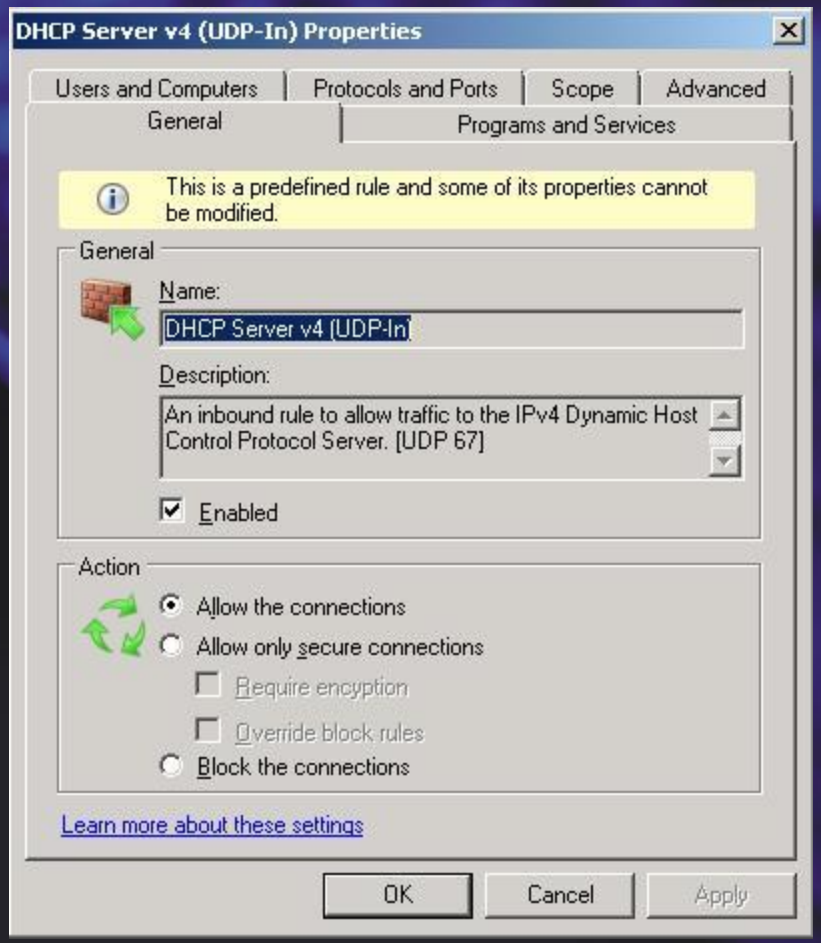
# Интерфейс Брандмауэра

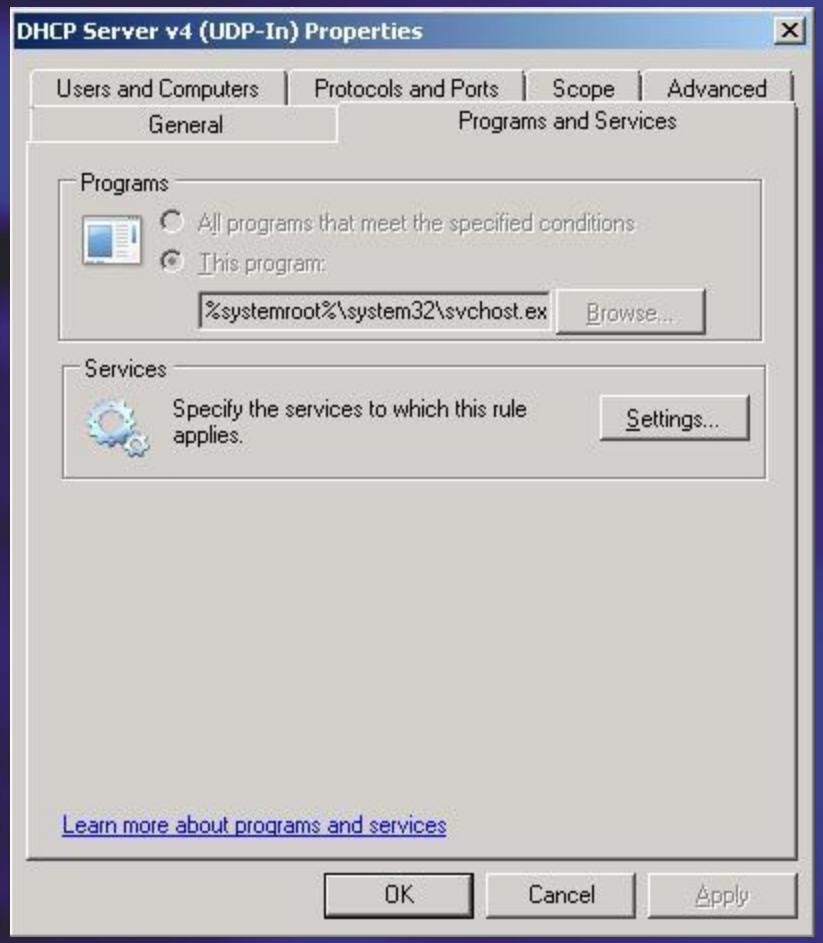


# Интерфейс Брандмауэра

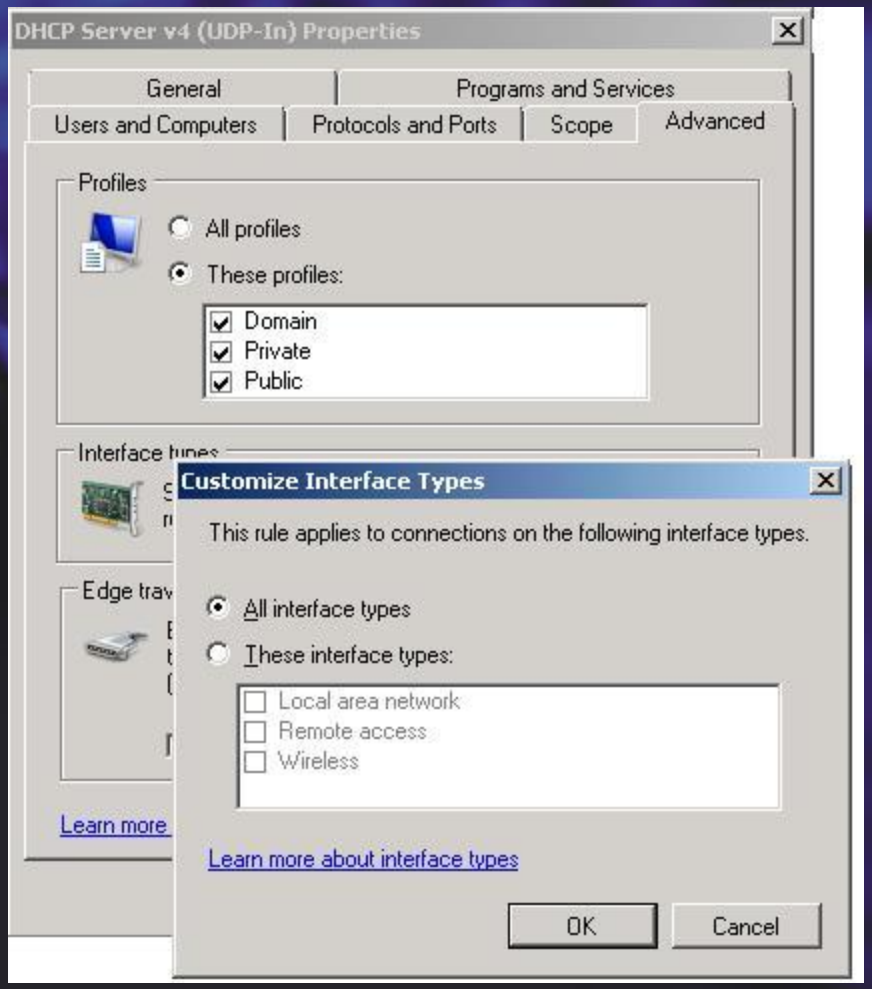


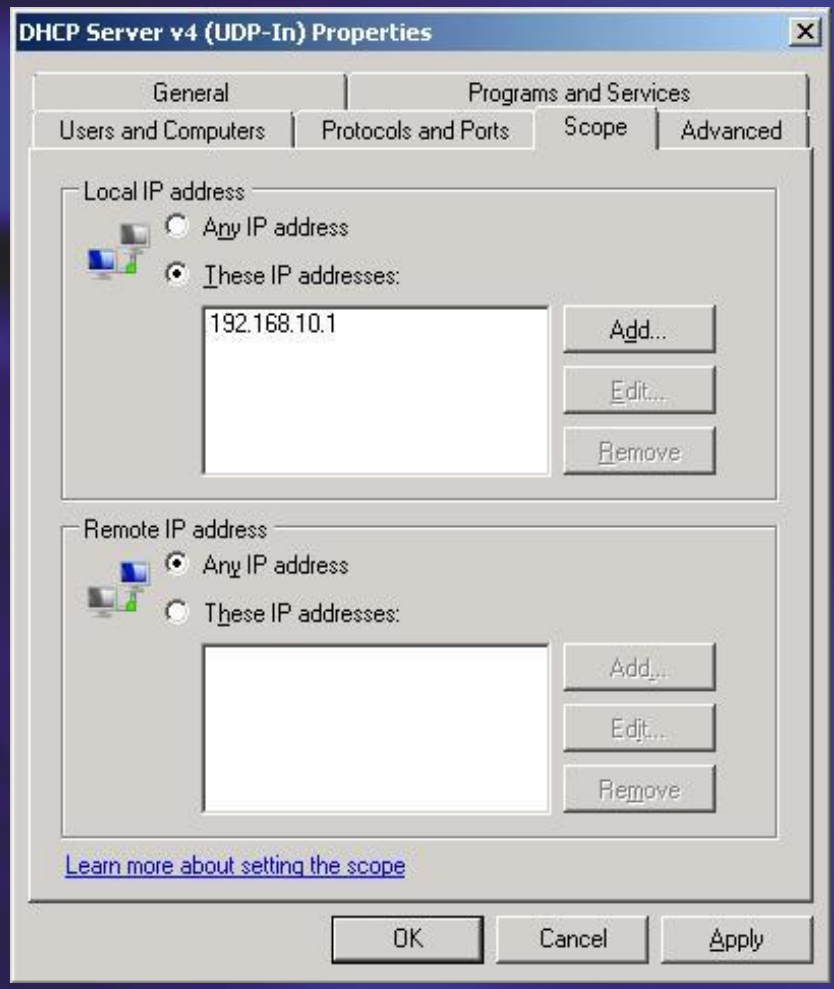
# Интерфейс Брандмауэра



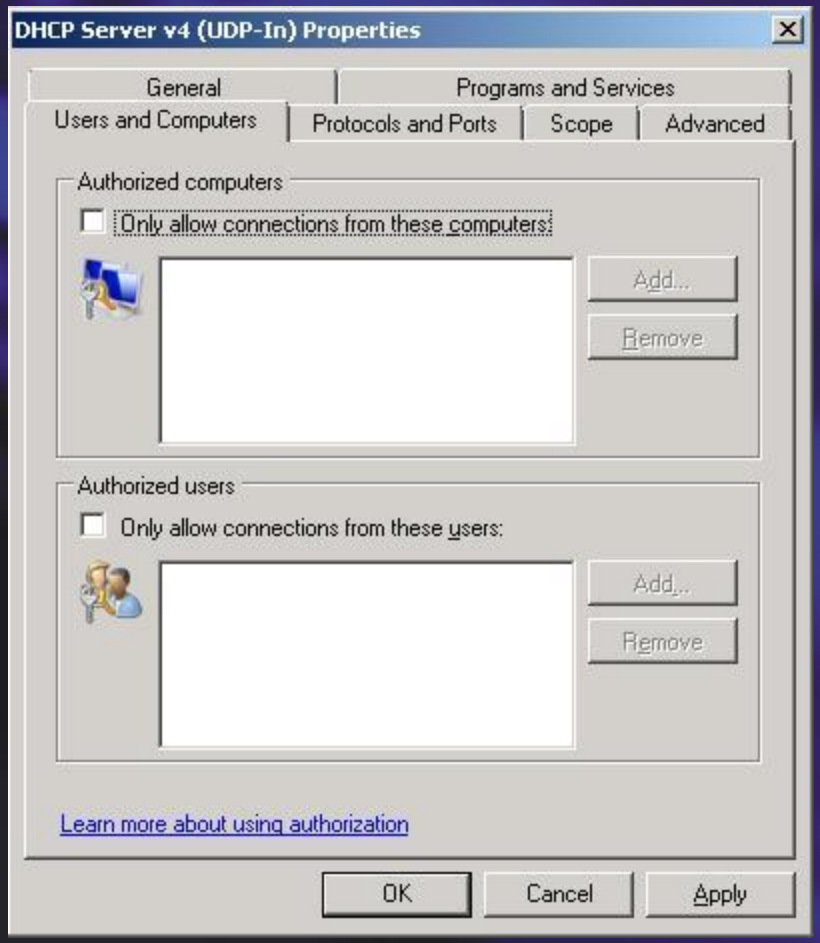



# Интерфейс Брандмауэра



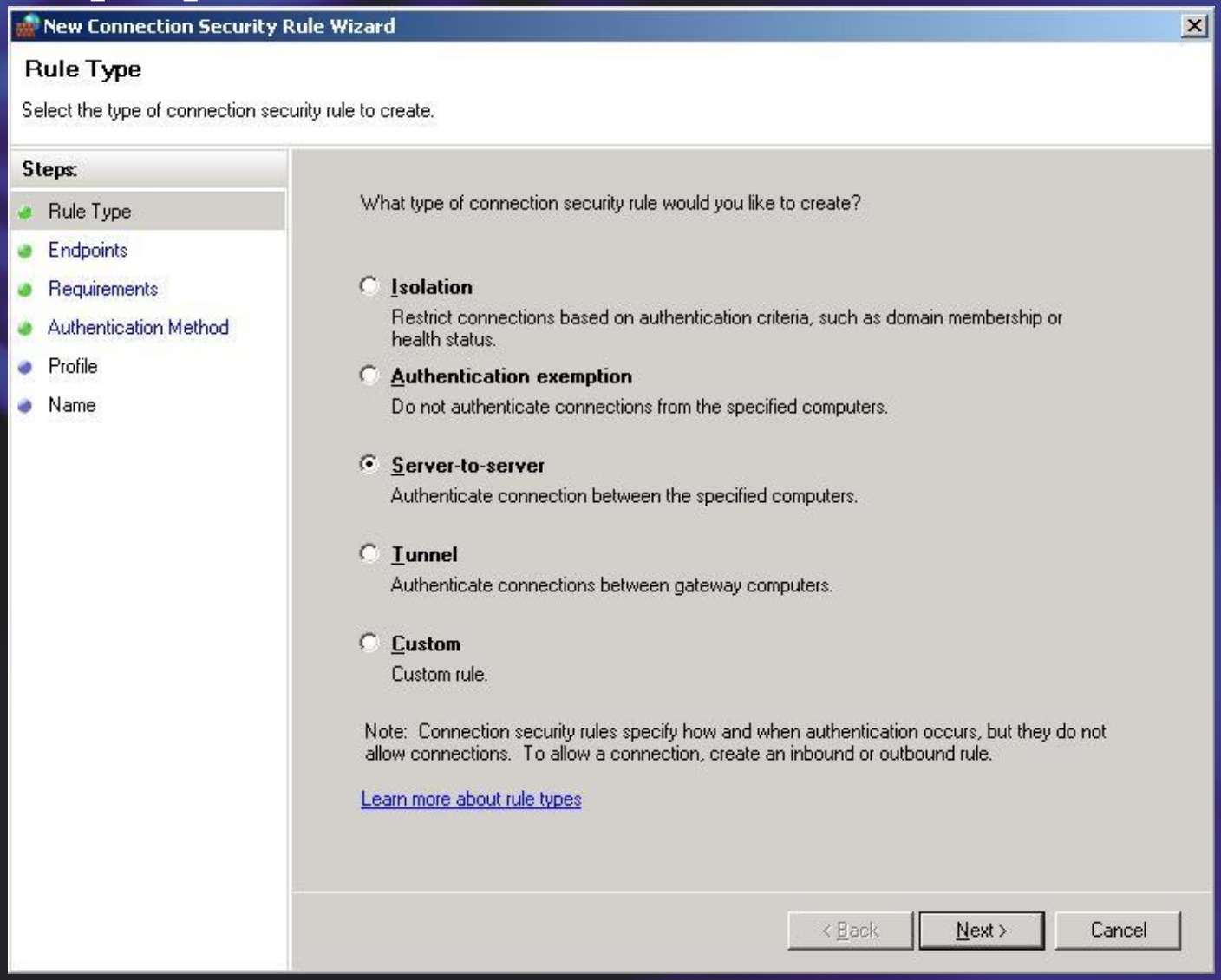
# Интерфейс Брандмауэра



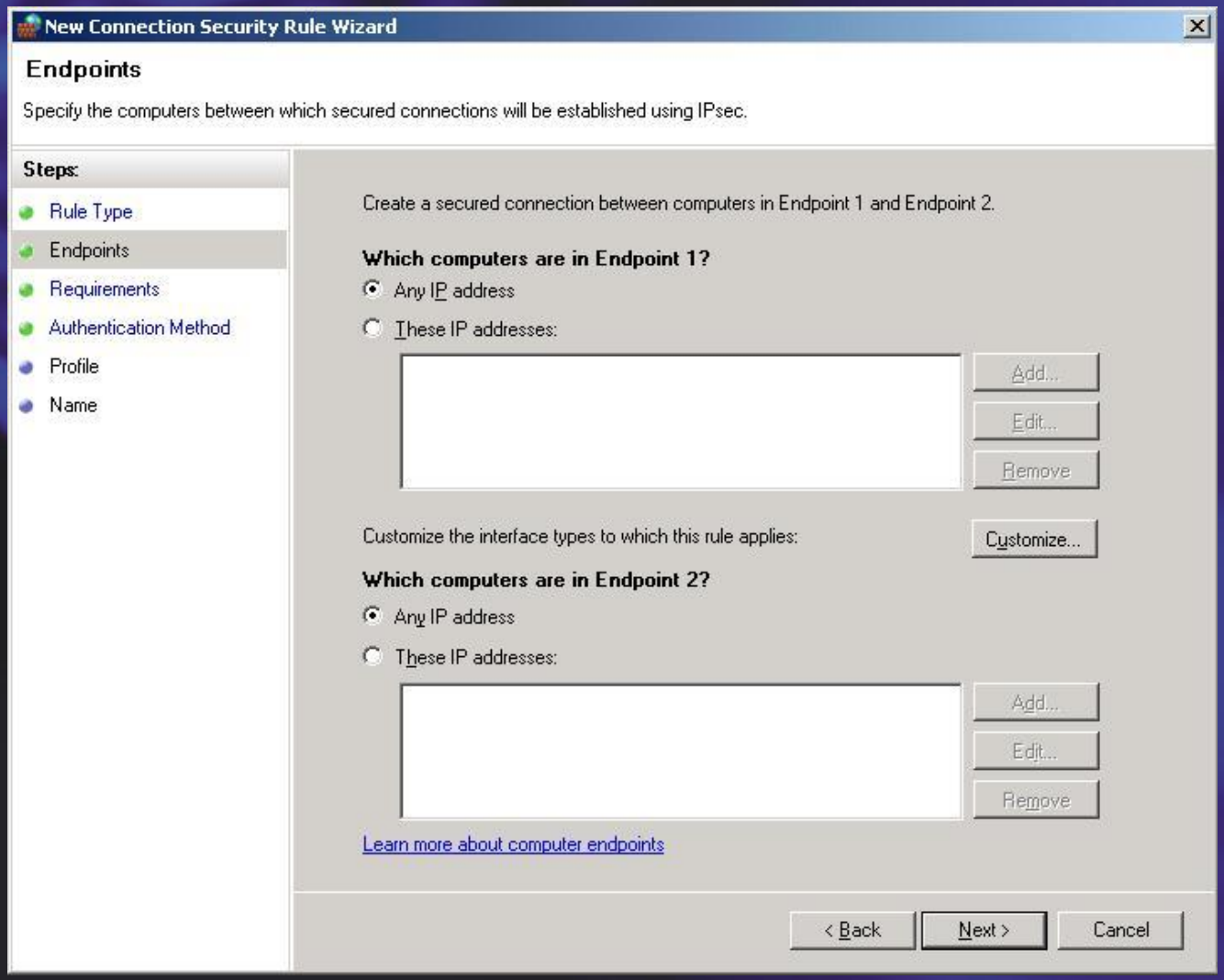
# Улучшение IPsec

| Улучшение | Эффект |
| --- | --- |
| Упрощение политик | • Облегчение создания политик за счет непротиворечивости и снижения необходимости в исключениях<br>• Значительное упрощение поддерки и обслуживания |
| Поддержка IPv6 | • Обработка IPsec IPv6 трафика идентична IPSec IPv4 |
| Балансировка нагрузки с помощью WLB | • Уменьшает время переключения каналов в Microsoft Clustering & NLB |
| Защита трафика между клиентом и DC | • Защита IPv4 и IPv6 траффика в момент присоединения клиента к домену |
| Стойкие криптоалгоритмы | • AES, Elliptic Curve |

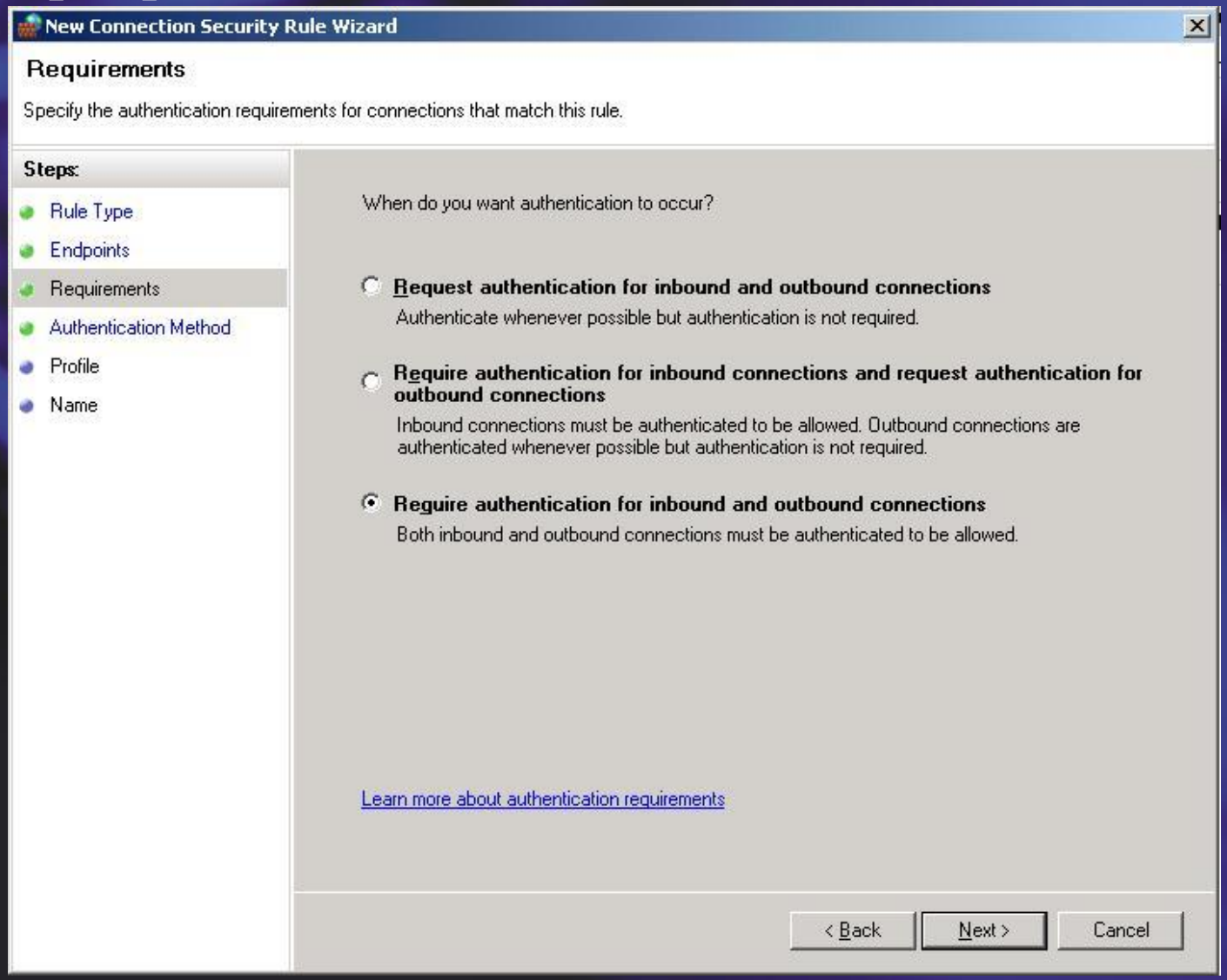
# Интерфейс IPSec



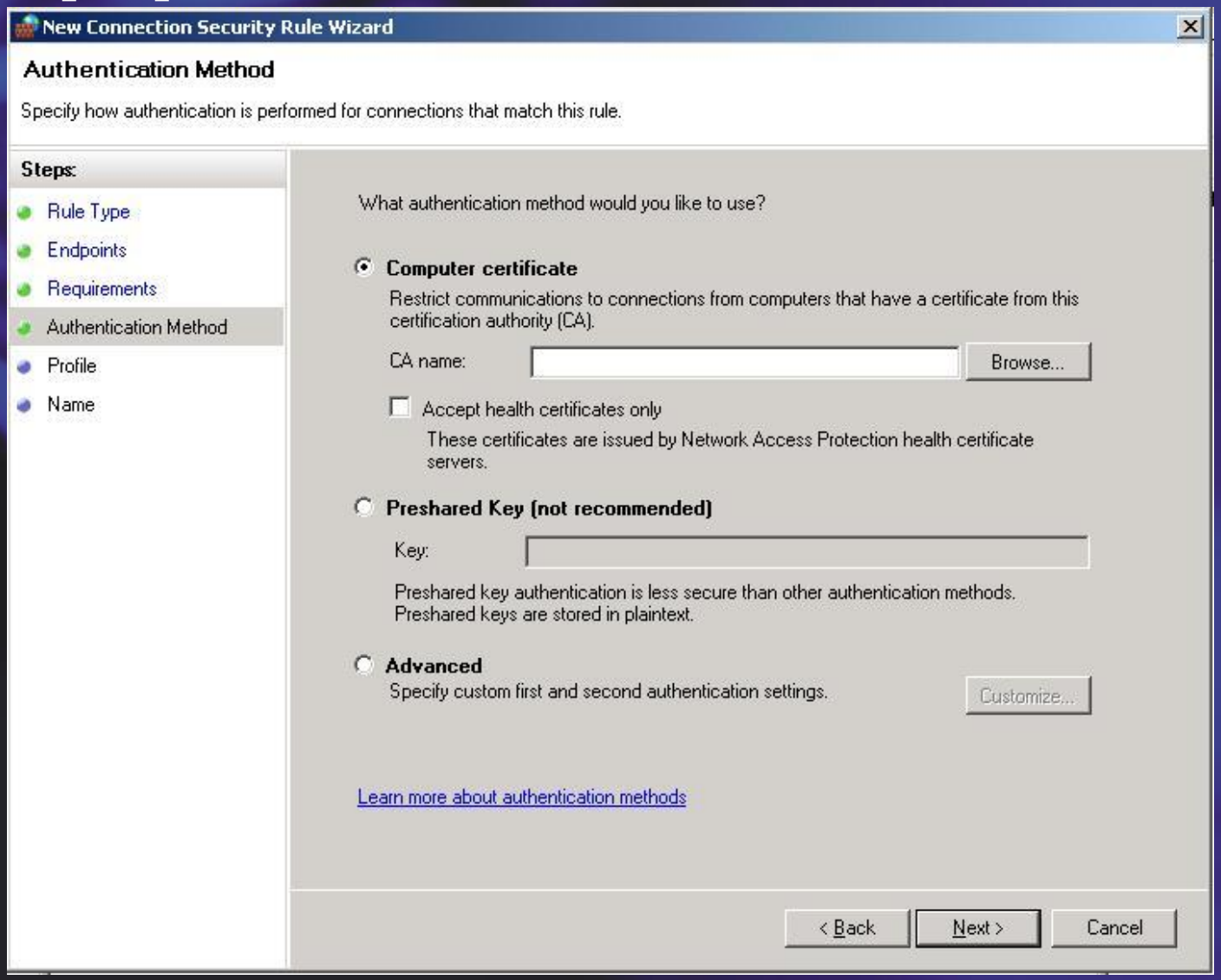
# Интерфейс IPSec



# Интерфейс IPSec



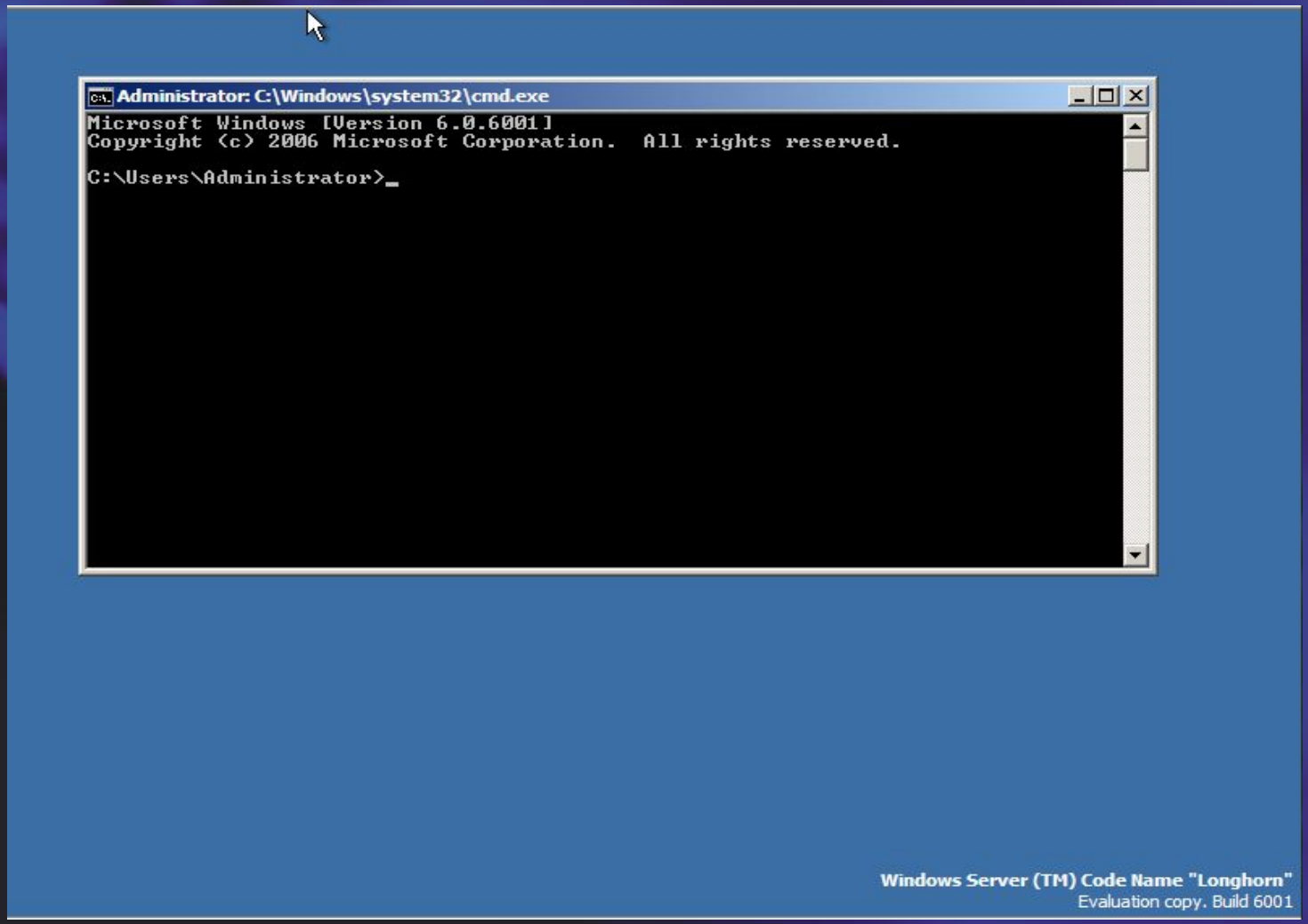
# Интерфейс IPSec



# Демонстрация интерфейса управления брандмауэром и IPsec

# Server Core – хватит и половины дозы.....

# Server Core – Windows без окон



# Server Core – Windows без окон

GUI почти - нет.

Windows Explorer – нет.

Internet Explorer & Media Player – нет.

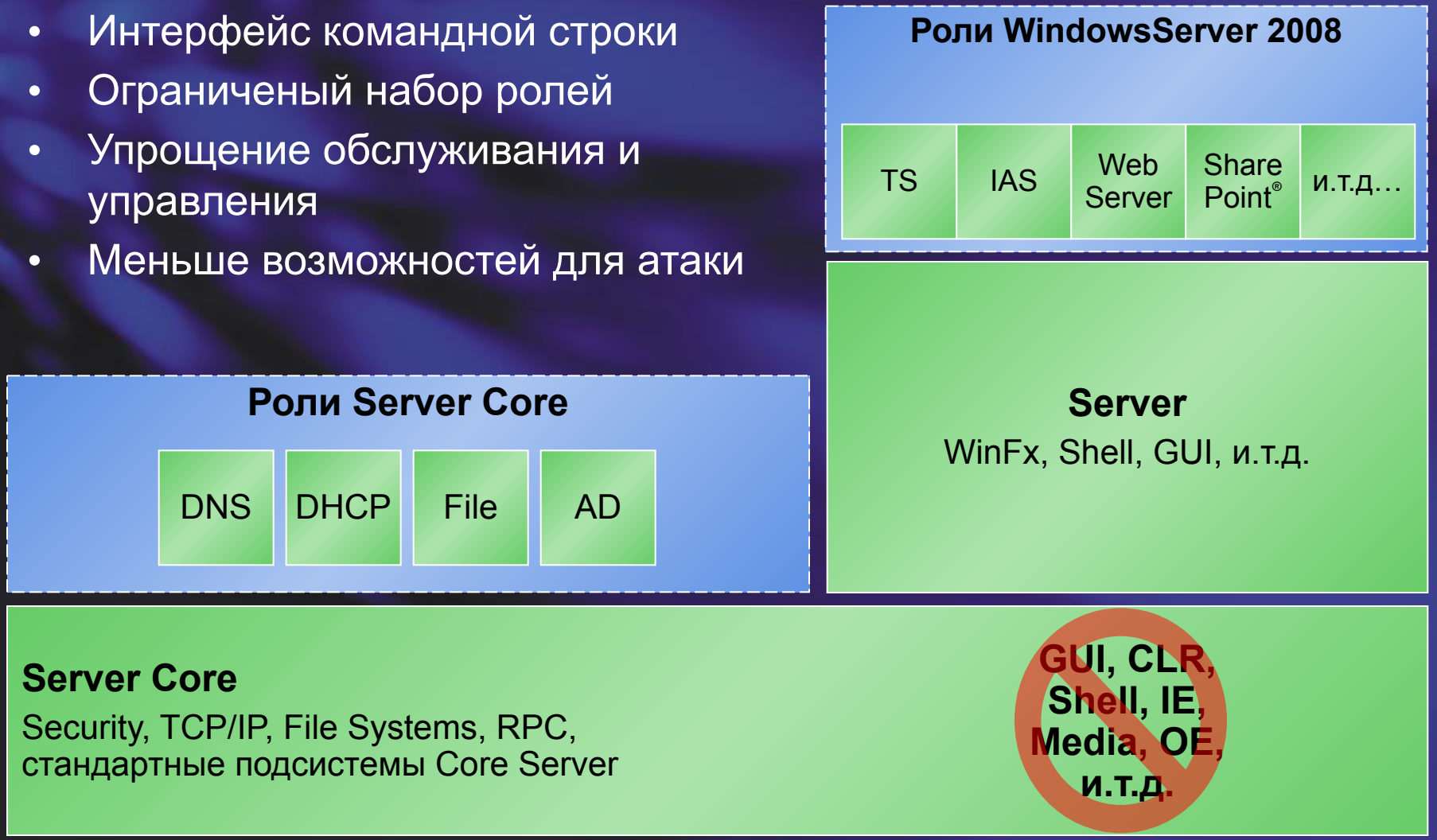
.Net Framework, PowerShell – тоже нет.

MMC – снова нет.

UAC – нет.

# Server Core

- Минимальная инсталляция
- Интерфейс командной строки
- Ограниченый набор ролей
- Упрощение обслуживания и управления
- Меньше возможностей для атаки



# Server Core поддерживает роли

- Active Directory Domain Services - ADDS
- Active Directory Lightweight Directory Service – ADLDS
- Domain Name System Server - DNS
- Dynamic Host Configuration Protocol Server - DHCP
- File Services
- Internet Information Services (IIS7)
- Print Server
- Streaming Media Services
- Windows Server Virtualization* - WSv
  - Будет доступна через 180 после релиза Windows Server 2008.

# Опциональные компоненты и возможности

- BitLocker
- Клиент NFS
- DFS Server и репликатор
- Failover Cluster
- FRS
- LPD Print Service
- MultipathIO
- Network Load Balancing
- Removable Storage Management
- Сервер NFS
- SNMP
- Система совместимости с UNIX приложениями
- Клиент Telnet
- Windows Server Backup
- WINS
- Run Once

# Управление и мониторинг

- Будут поддерживаться агенты System Center, MOM, SMS
- Функционал доступный агентам и инструментам управления:
  - Локальное исполнение команд
  - Terminal Server
  - Веб сервисы для дистанционного управления (WS-Management)
  - Windows Remote Shell (WinRS)
  - WMI
  - Task Scheduler
  - RPC и DCOM
  - SNMP
  - Дистанционное управление с помощью MMC

# Аппаратные требования

| Server Core | | | |
|---|---|---|---|
| Компонент | Минимум | Рекомендовано | Оптимально |
| Процессор | 1 GHz | 2 GHz | 3 GHz |
| ОЗУ* | 512 MB | 512 MB | 1 GB |
| Жесткий диск** | 8 GB | 8 GB | 40 GB |
| Windows Server 2008 | | | |
| Процессор | 1 GHz | 2 GHz | 3 GHz |
| ОЗУ | 512 MB | 1 GB | 2 GB |
| Жесткий диск | 8 GB | 40 GB | 80 GB |

* В режиме бездействия Server Core занимает 184 MB ОЗУ, Windows Server 2008 соответственно 308 MB.
** Пространство на диске без учета фалов подкачки, временных файлов хранящих содержимое оперативной памяти в режиме сна. Обычно для Server Core требуется приблизительно 1.5 GB. Те же файлы для Windows Server 2008 занимают примерно 7.5 GB.

# Установка Server Core

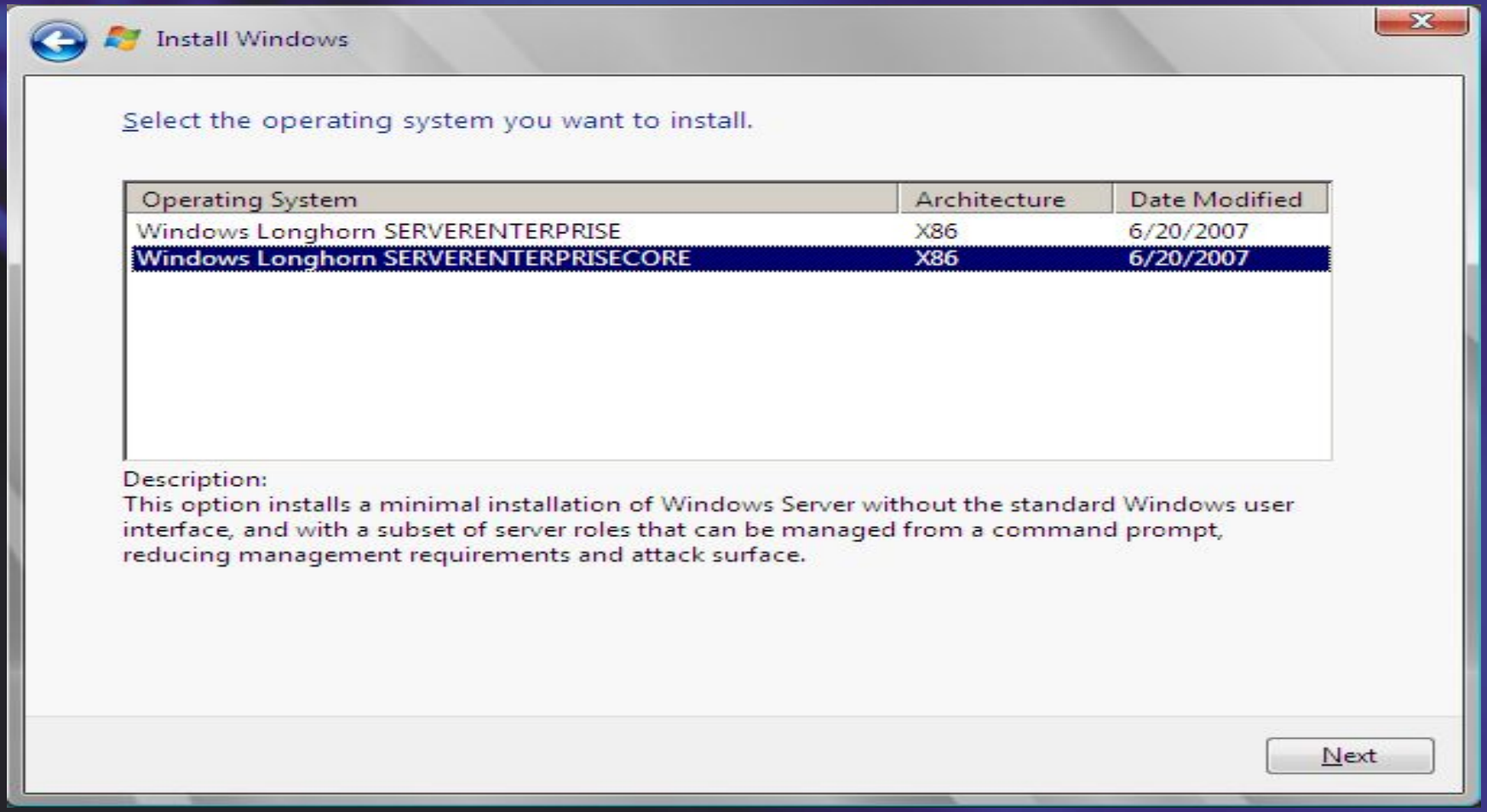
## Можно:

- Инсталляция с носителя Windows Server 2008.
- Версии Enterprise и Standard Edition.
- Обновление до Server Core R2.

## Нельзя:

- Обновление с предыдущих версий Windows
- Конвертировать инсталляцию Windows Server 2008 в Server Core,
- Превратить Server Core в Windows Server 2008

# Установка Server Core



# Демонстрация Server Core

# Read-Only Domain Controller – безопасный контролер домена для филиала ...

# Read-Only Domain Controller

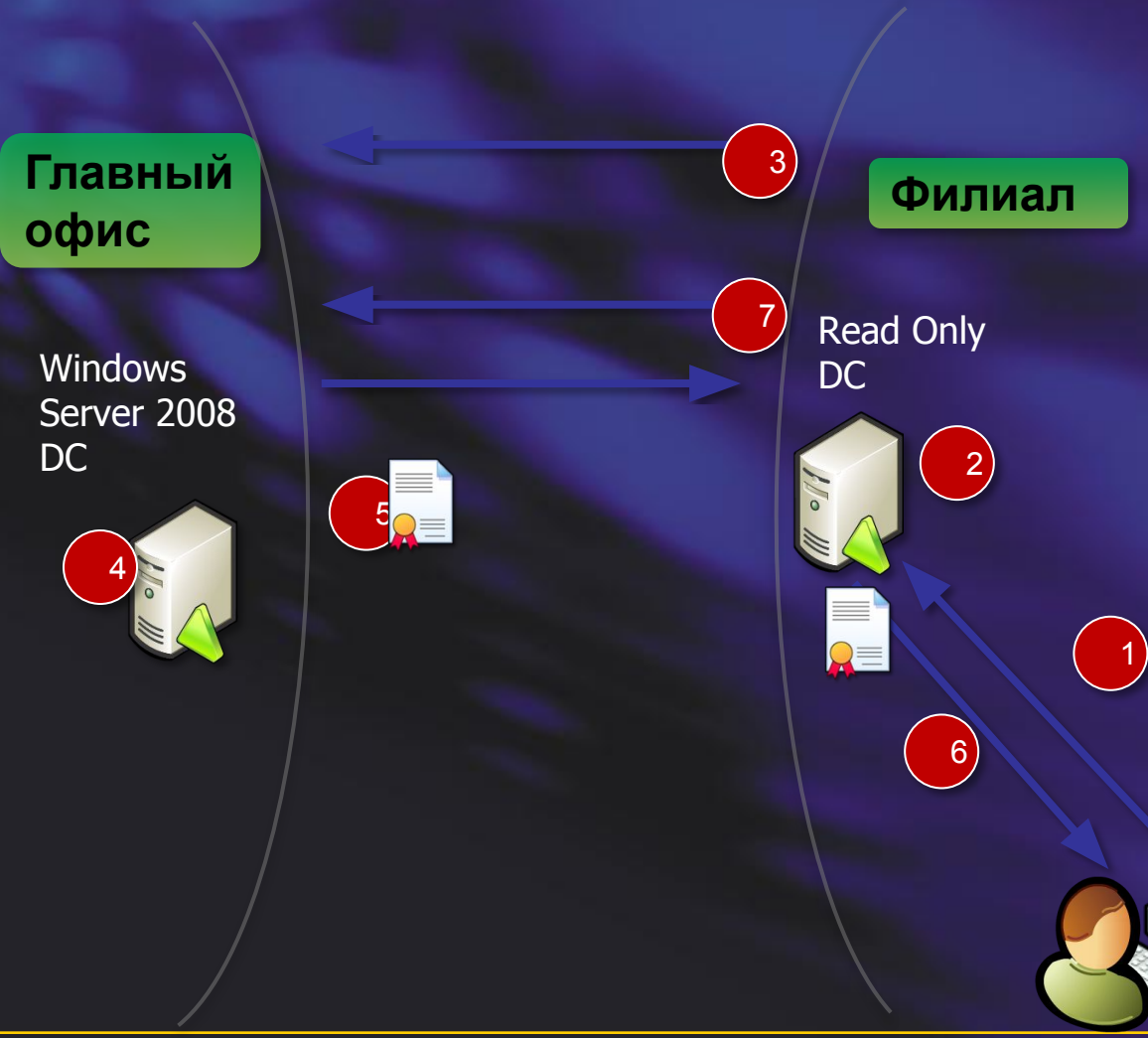

**Копия базы AD только для чтения**
- Может содержать все обеъкты и атрибуты
- DNS зоны только для чтения

**Односторонняя репликация**
- Изменения вносятся только в главном офисе
- Гибкая настройка параметров репликации – экономия сетевого трафика

**Данные авторизации и аутентификации**
- Не хранит паролей пользователей (по умолчанию)
- RODC выдает только локальные билеты

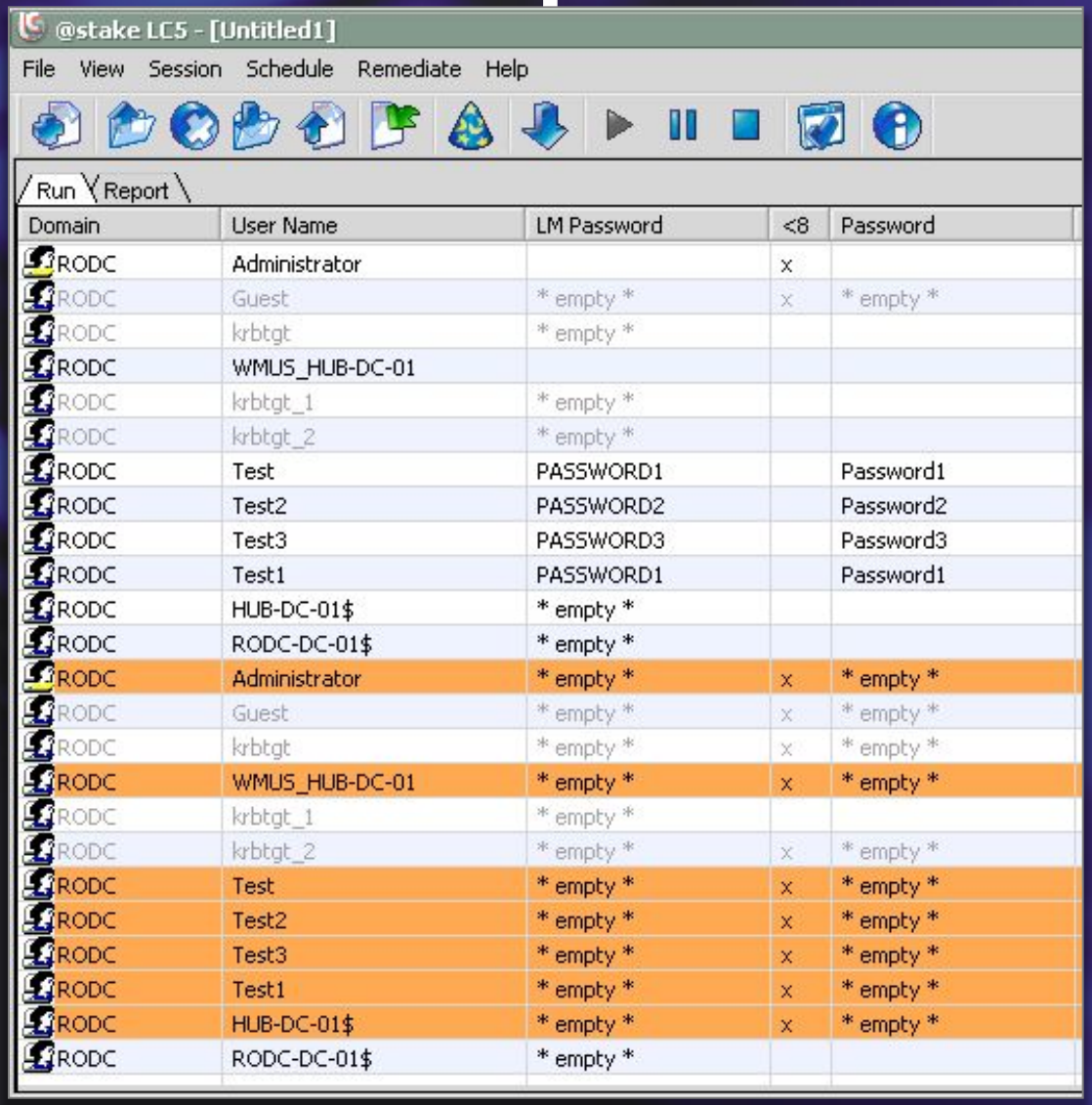
Разделение административных ролей
- Управление от имени локального пользователя
- Администратор локального контролера не является администриатором глобального DC

# Как RODC функционирует



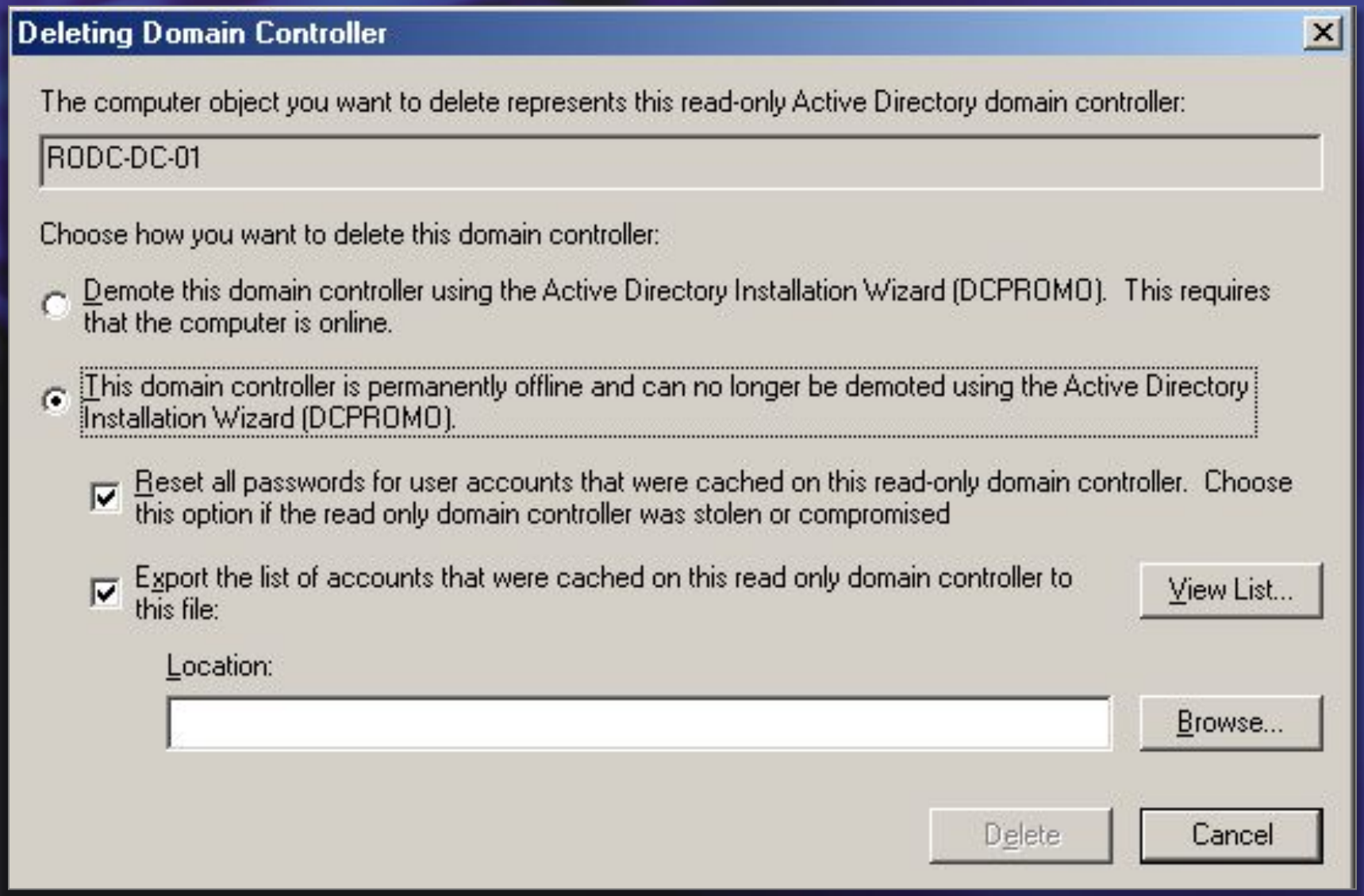

1. AS_Req отправлен в RODC (запрос на получение TGT)
2. RODC: Смотрит в базе: «У меня нет пароля этого пользователя"
3. Передает запрос Windows Server 2008 DC
4. DC проводит аутентификацию запроса
5. После аутентификации билет TGT отправляется обратно RODC
6. RODC отдает TGT пользователю и кэширует данные
7. Пользователь получает билет TGT подписаный главным контролером

# RODC с точки зрения атакующего




| Domain | User Name | LM Password | <8 | Password |
|---|---|---|---|---|
| RODC | Administrator | | x | |
| RODC | Guest | * empty * | x | * empty * |
| RODC | krbtgt | * empty * | | |
| RODC | WMUS_HUB-DC-01 | | | |
| RODC | krbtgt_1 | * empty * | | |
| RODC | krbtgt_2 | * empty * | | |
| RODC | Test | PASSWORD1 | | Password1 |
| RODC | Test2 | PASSWORD2 | | Password2 |
| RODC | Test3 | PASSWORD3 | | Password3 |
| RODC | Test1 | PASSWORD1 | | Password1 |
| RODC | HUB-DC-01$ | * empty * | | |
| RODC | RODC-DC-01$ | * empty * | | |
| RODC | Administrator | * empty * | x | * empty * |
| RODC | Guest | * empty * | x | * empty * |
| RODC | krbtgt | * empty * | x | * empty * |
| RODC | WMUS_HUB-DC-01 | * empty * | x | * empty * |
| RODC | krbtgt_1 | * empty * | | |
| RODC | krbtgt_2 | * empty * | x | * empty * |
| RODC | Test | * empty * | x | * empty * |
| RODC | Test2 | * empty * | x | * empty * |
| RODC | Test3 | * empty * | x | * empty * |
| RODC | Test1 | * empty * | x | * empty * |
| RODC | HUB-DC-01$ | * empty * | x | * empty * |
| RODC | RODC-DC-01$ | * empty * | | |

# Украли RODC?


Deleting Domain Controller
The computer object you want to delete represents this read-only Active Directory domain controller:
RODC-DC-01
Choose how you want to delete this domain controller:
Demote this domain controller using the Active Directory Installation Wizard (DCPROMO). This requires that the computer is online.
This domain controller is permanently offline and can no longer be demoted using the Active Directory Installation Wizard (DCPROMO).
Reset all passwords for user accounts that were cached on this read-only domain controller. Choose this option if the read only domain controller was stolen or compromised
Export the list of accounts that were cached on this read only domain controller to this file:
View List...
Location:
Browse...
Delete
Cancel

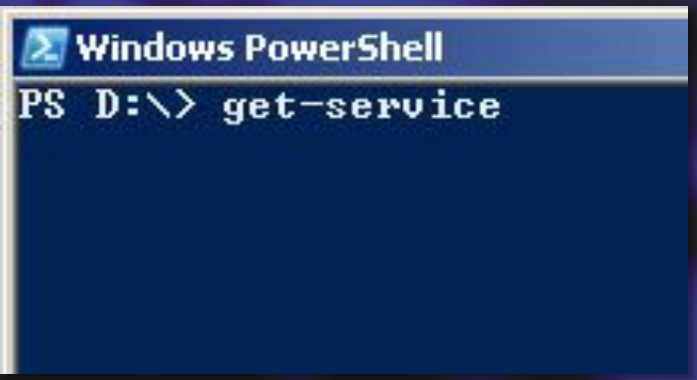
# Варианты управления RODC

- **Учетные записи пользователей не хранятся в RODC**( по умолчанию)
  - **За**: Наиболее безопасно
  - **Против**: Никто не сможет работать если WAN неисправен
- **Большинство учетных записей хранятся в RODC**
  - **За**: Облегчается управление паролями. Управляемость важнее безопасности.
  - **Против**: Больше паролей «оседают» в RODC
- **Хранятся учетные записи пользователей филиала в RODC**
  - **За**: В случае аварии WAN местные пользователи продолжают работать, сохраняется безопасность остальных учетных записей
  - **Против**: Усложнение администрирования
    - Необходимо сопоставить имена компьютеров контролерам филиала

# Powershell – скриптовый язык моей мечты.....

# Windows PowerShell

## Новый интерфейс командной строки и новый системный скриптовый язык Scripting Language




- Ускоряет автоматизирование типичных задач системного администратора
- Прост и интуитивно понятен
- Работает с унаследованными скриптами VBS, WSH
- Объектно ориентирован
- 130 стандартных инструментов

## Перспективы

- Будет входить в поставку Windows 2008 Server
- Большинство административных интерфейсов будет лишь прослойкой над PowerShell:

# Windows PowerShell

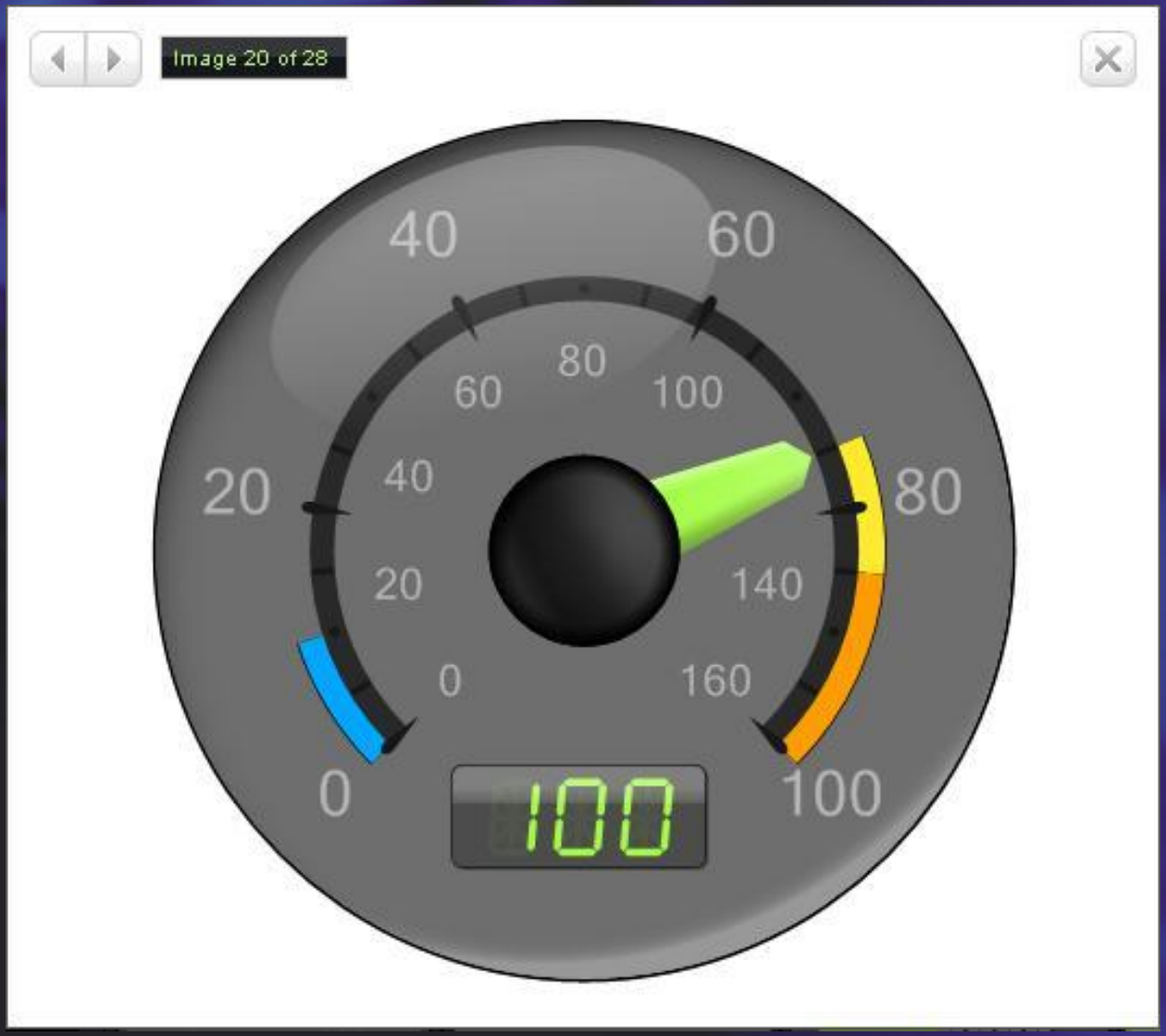
**Используется в следующих проектах:**

- Exchange 2007
- System Center Operations Manager 2007 (SCOM 2007)
- System Center Virtual Machine Manager 2007 (VMM)
- System Center Data Protection Manager 2007 (DPM)
- Microsoft Transporter Suite for Lotus Domino
- Windows Compute Cluster Tool Pack
- Windows Server 2008

# Демонстрация Powershell

# PowerShell + PowerGadgets

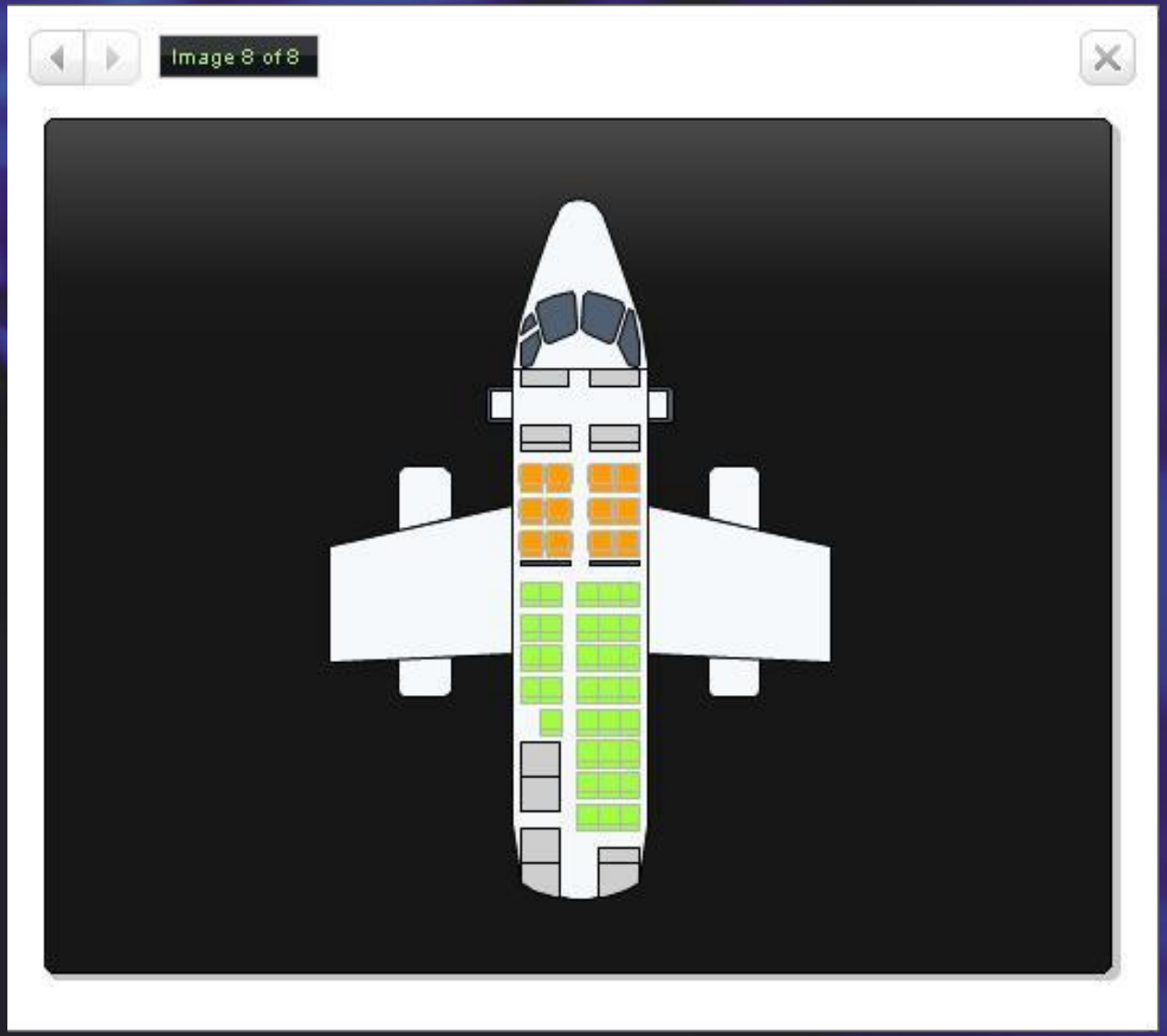
# PowerShell + PowerGadgets



# PowerShell + PowerGadgets

# PowerShell + PowerGadgets

# PowerShell + PowerGadgets



# PowerShell + PowerGadgets

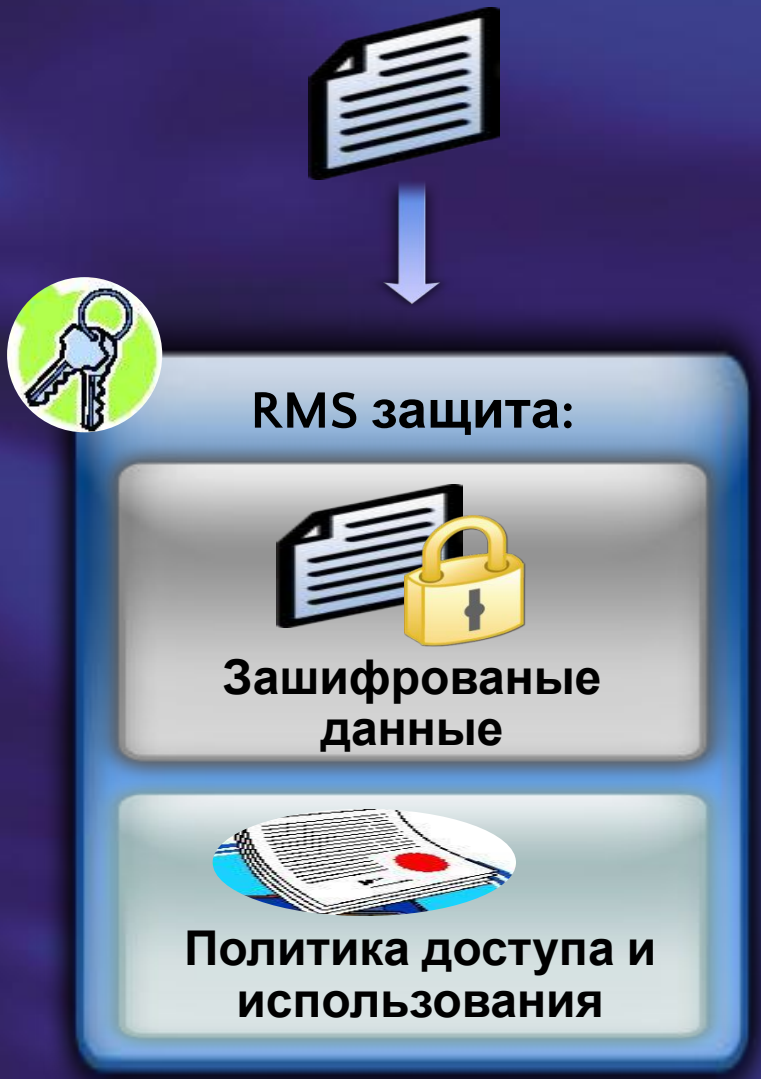
# Цель Rigths Management Service:

Дать возможность защитить  важную информацию в течении жизненого цикла

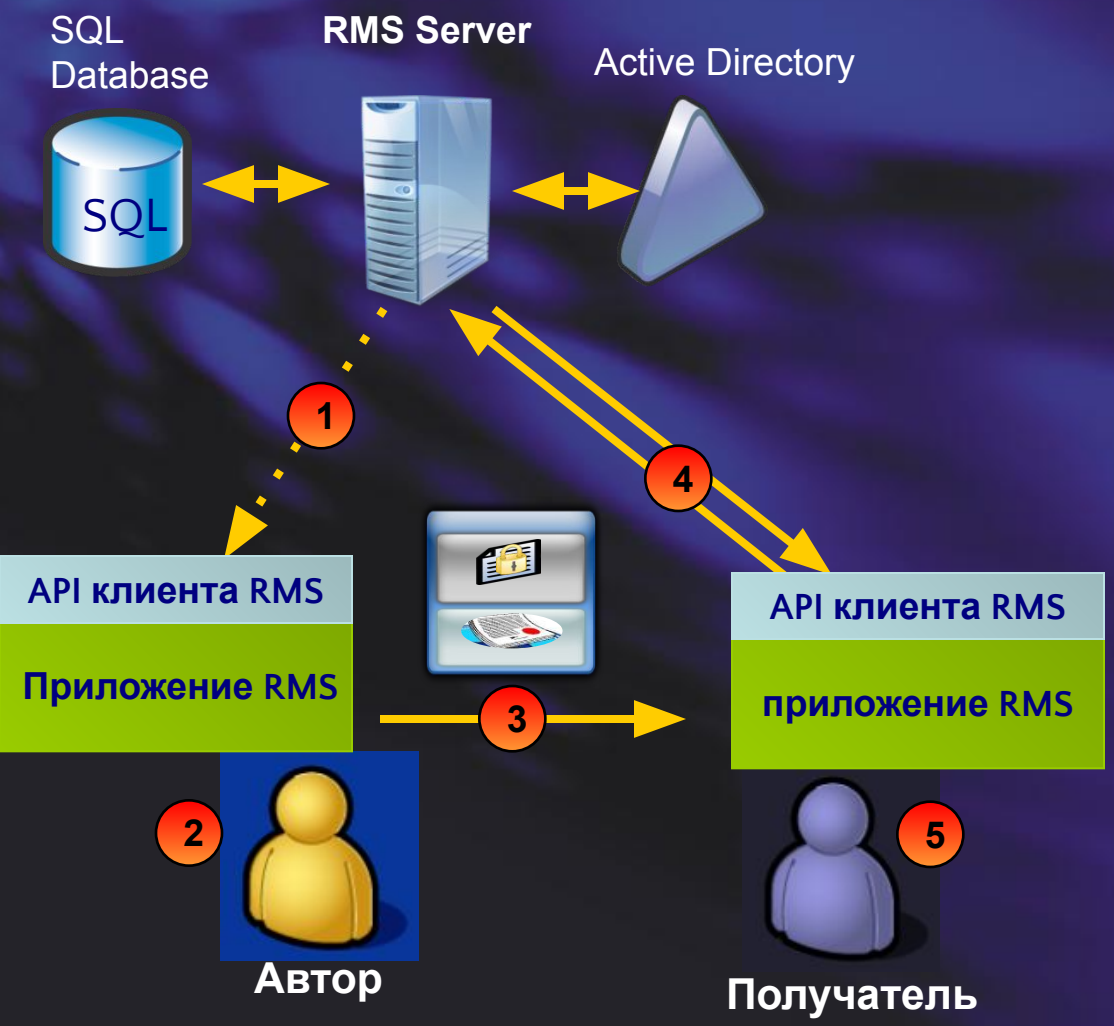
- Защита информации
  - Данные защищены во время хранения, передачи, обработки
  - Защита данных как внутри организации так и снаружи
- Соответствие организационным политикам
  - Постоянный контроль за тем кто, когда получает доступ к данным и что с ними делает
- Organizational
- Control
  - ИТ департамент может централизовано реализовать политику организации
  - RMS протоколирование позволяет отслеживать потоки информации
- Расширяемая платформа
  - Основная возможность платформы разработки от MS
  - Поддерживается приложениями Microsoft и других поставщиков

# Как RMS защищает данные?

- RMS защищает с помощью
  - Сильного шифрования
    - Симетричная и асиметричная криптография
  - Контроль доступа
    - Пользователи и Группы
    - Временные условия
    - Разрешенные применения
  - Политика использования
    - Только для чтения, Редактирования, Экспорта, Печать, Сохранение, …
  - Аудит доступа
    - Журналы сервера хранят подробную информацию о доступе
- Защита RMS постоянна
  - Во время хранения, при передаче и использовании данных

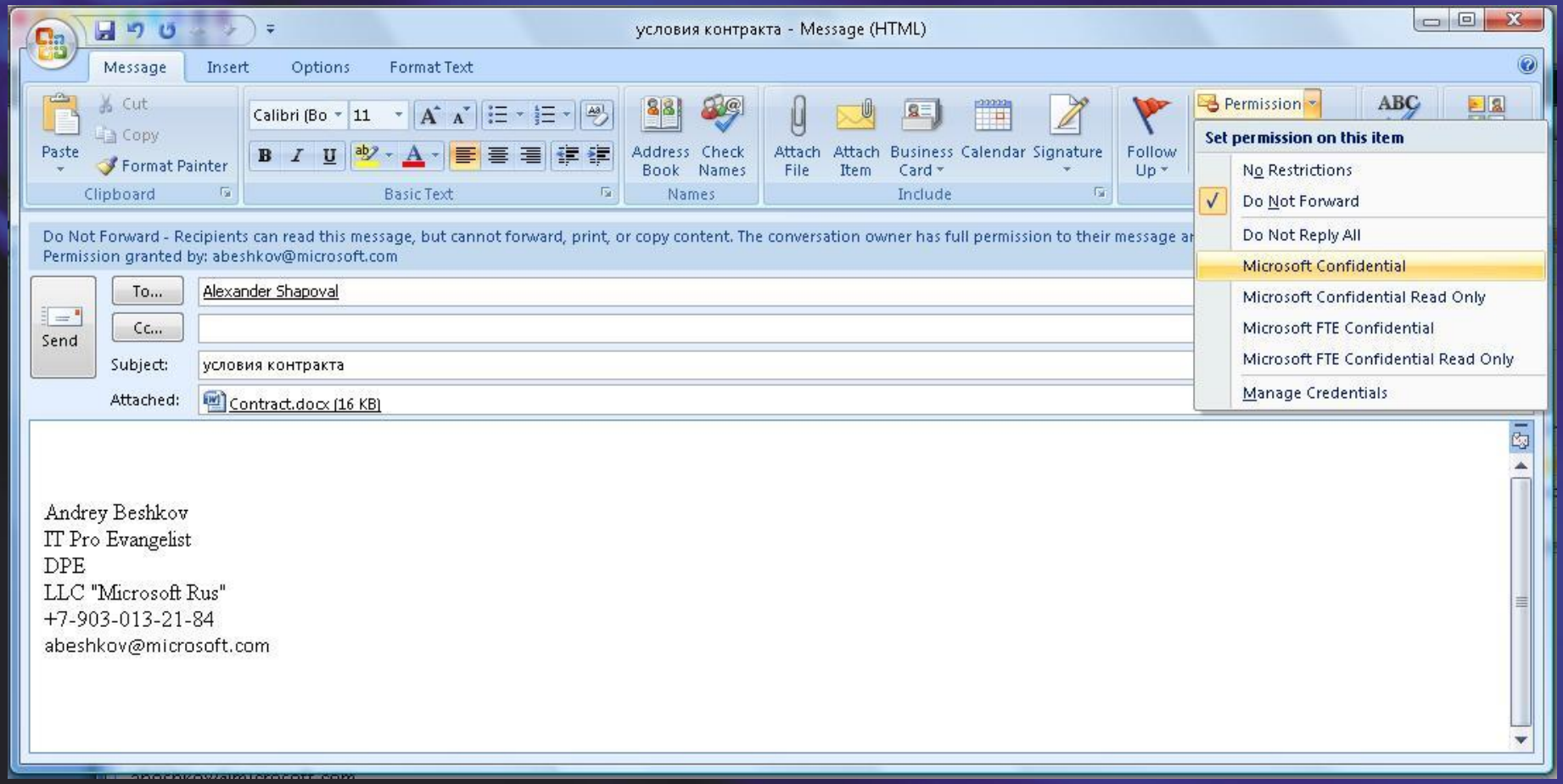


# Пример работы RMS




1. При первом обращении к RMS автор получает ключи и в случае необходимости политики защиты данных
2. Автор применяет политики к данным; приложение используя API RMS шифрует данные и применяет к ним политики; шифрованый контейнер данных и политик сохраняется в файле.
3. Автор распространяет файл
4. Получатель открывает файл; приложение обращается к серверу RMS которые авторизует пользователя и выдает ему лицензию на использование данных
5. Приложение отображает файл применяет права и ограничивает получателя; RMS клиент удостоверяет что среда достаточно защищена

# Пример работы RMS



# Дополнительная информация

**Документация**

- http://www.microsoft.com/windowsserver2008/
- http://www.microsoft.com/powershell

**Блоги**

- http://blogs.technet.com/abeshkov/
- http://blogs.technet.com/ashapo/
- http://blogs.technet.com/windowsserver/

Microsoft®

Your potential. Our passion.™