



# Усовершенствования системы безопасности Windows Server 2008

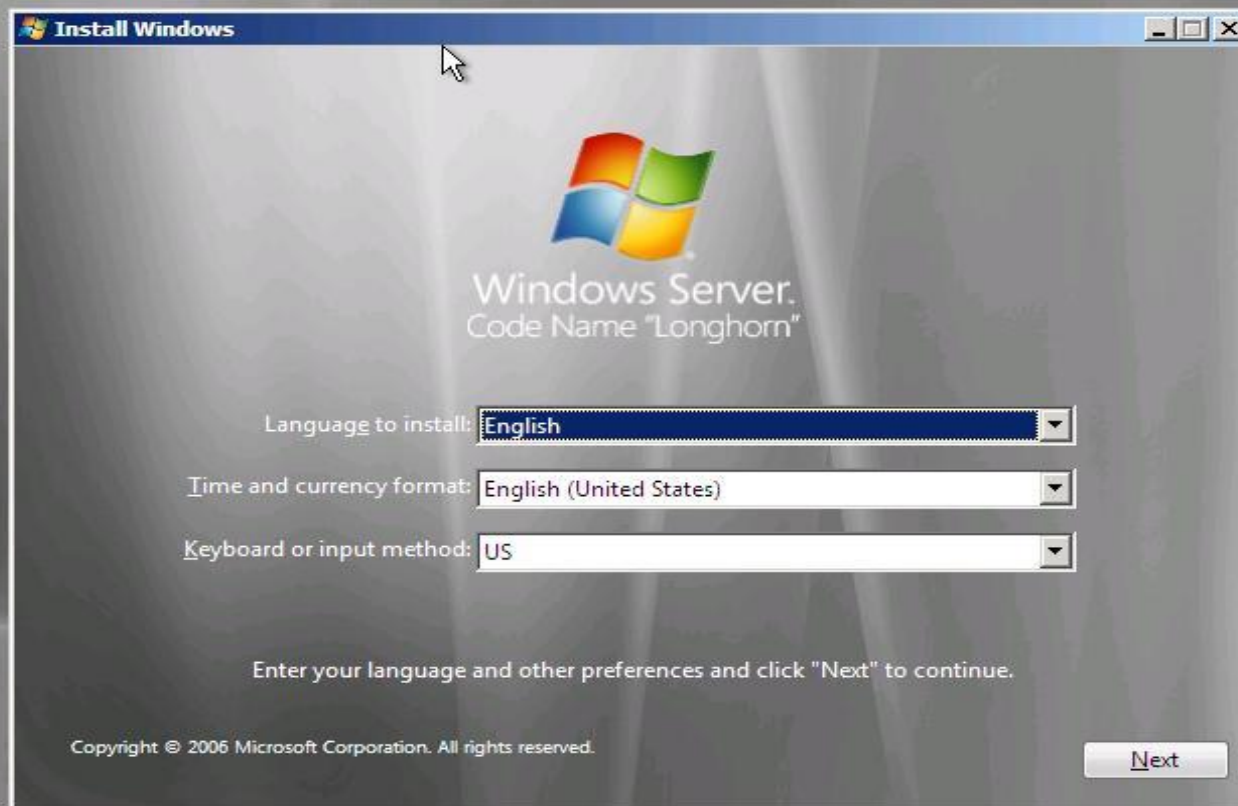
**Семинары TechNet. Осень 2007**

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

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

- Отвечаем на 4 простых вопроса и идем пить кофе.

# Простота инсталляции




# Простота инсталляции

Install Windows

## Type your product key for activation

You can find your product key on your computer or on the installation disc holder inside the Windows package. Although you are not required to enter your product key now to install, failure to enter it may result in the loss of data, information, and programs. You may be required to purchase another edition of Windows. We strongly advise that you enter your product identification key now.

The product key sticker looks like this:



Product key (dashes will be added automatically):

  
 [Automatically activate Windows when I'm online](#)

[What is activation?](#)

[Read our privacy statement](#)

Next

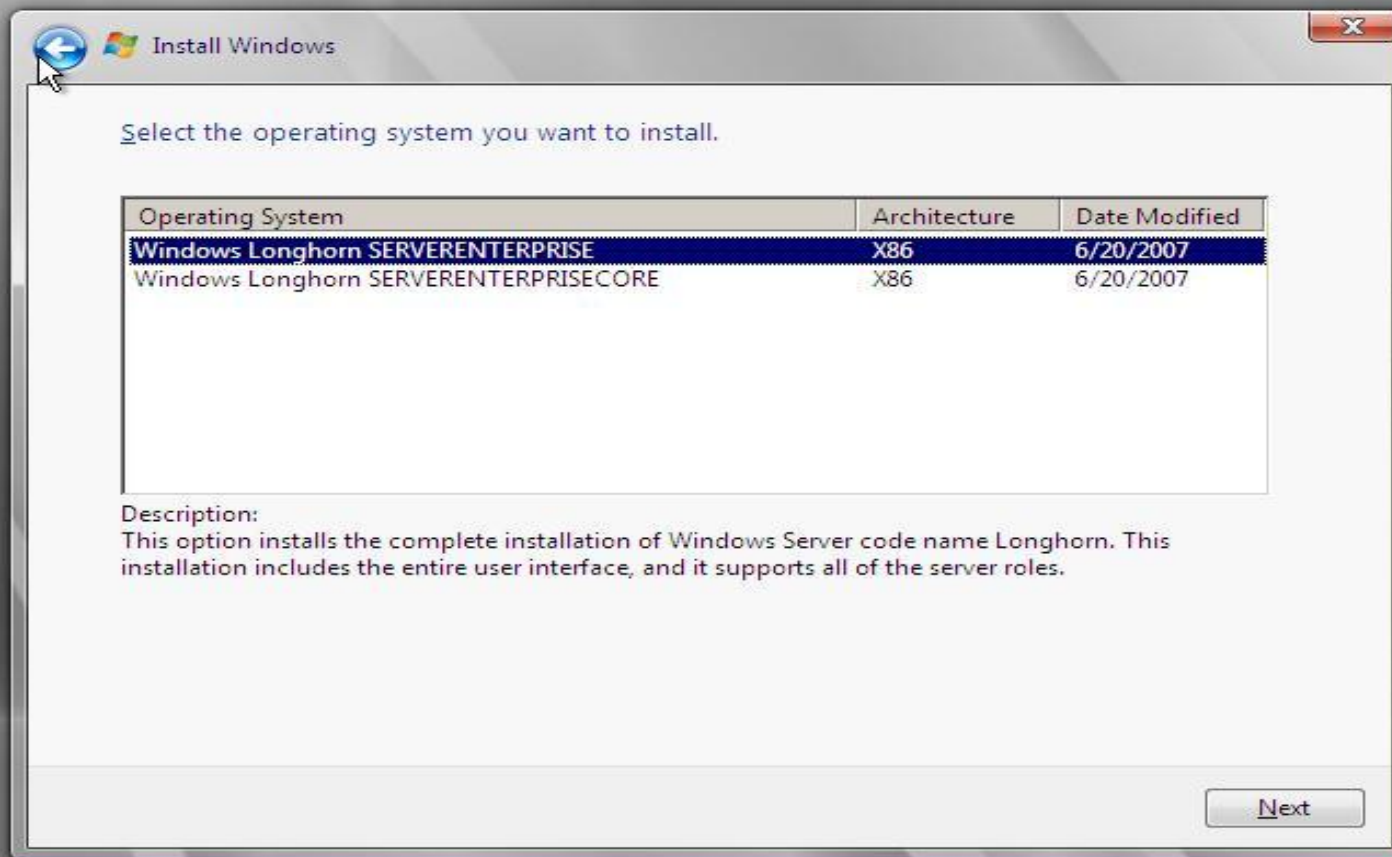
1

Collecting information

Installing Windows



# Простота инсталляции



1 Collecting information

Installing Windows

# Через 30 минут

**Initial Configuration Tasks**

Perform the following tasks to initially configure this server

Windows Server  
Code Name "Longhorn"

**1 Provide computer name and domain**

<b>Full Computer Name:</b>	WIN-3IQTP48R2SU
<b>Workgroup:</b>	WORKGROUP

**2 Update This Server** [Updating your Windows server](#)

<b>Enable automatic updating and feedback</b>	<b>Updates:</b>	Not configured
	<b>Feedback:</b>	Windows Error Reporting on Participating in Customer Experience Improvement Program
<b>Download and install updates</b>	<b>Checked for Updates:</b>	Never
	<b>Installed Updates:</b>	Never

**3 Customize This Server** [Customizing your server](#)

<b>Add roles</b>	<b>Roles:</b>	None
<b>Add features</b>	<b>Features:</b>	Remote Differential Compression
<b>Enable Remote Desktop</b>	<b>Remote Desktop:</b>	Disabled
<b>Configure Windows Firewall</b>	<b>Firewall:</b>	On

Print, e-mail, or save this information

Do not show this window at logon

Close

Start | Initial Configuration T... | RU | 11:55

# Новый интерфейс управления

The screenshot shows the Windows Server Manager interface for a server named SEA-DC-01. The interface is divided into a left-hand navigation pane and a main content area. The navigation pane lists various server management tasks such as Manage Roles, Troubleshooting, Configuration, and Storage and Backup. The main content area displays a 'Server Summary' section with three sub-sections: System Information, Security Summary, and Roles Summary. Each sub-section provides key system details and offers quick links to perform common administrative tasks.

**Server Manager (SEA-DC-01)**

Get an overview of this server, change system properties, and install or remove server roles and features.

**Server Summary**

**System Information**

Full computer name:	SEA-DC-01.Contoso.com	<a href="#">Change system properties</a>
Domain:	Contoso.com	<a href="#">Change Administrator account</a>
Local Administrator account:	Administrator	<a href="#">View Network Connections</a>
Local Area Connection:	192.168.16.2	
Product ID:	78440-033-0824223-70884	

Do not show me this console at logon

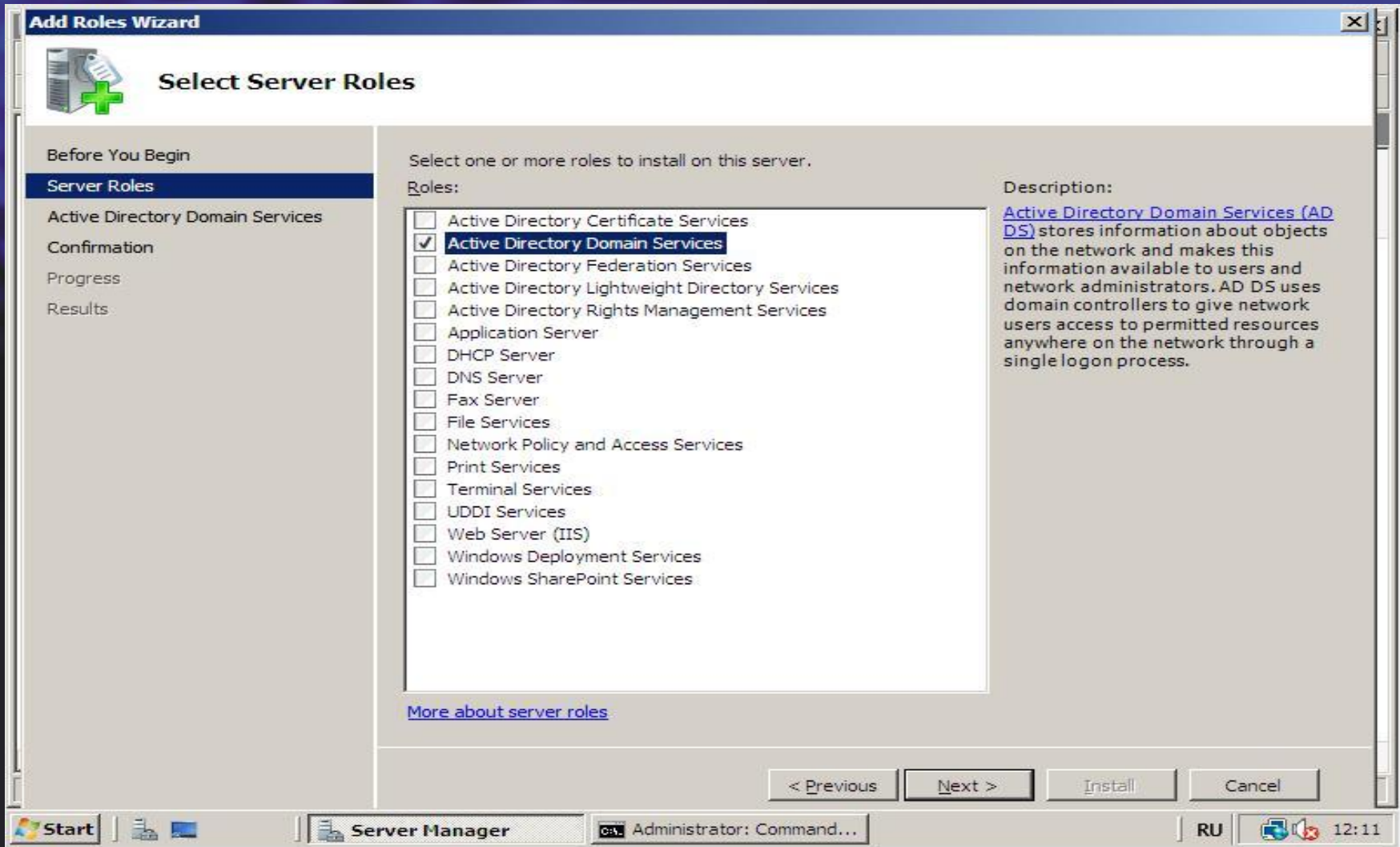
**Security Summary**

Windows Firewall status:	Enabled	<a href="#">Go to Windows Firewall</a>
Windows Update status:	Install updates automatically	<a href="#">Configure Windows Update</a>
		<a href="#">Open Security Configuration Wizard</a>
		<a href="#">Check for new updates</a>

**Roles Summary**

**Roles: 6 of 17 installed** [Go to Manage Roles](#)

# Ролевые игры



**Add Roles Wizard**

## Select Server Roles

Before You Begin

**Server Roles**

- Active Directory Domain Services
- Confirmation
- Progress
- Results

Select one or more roles to install on this server.

Roles:

- Active Directory Certificate Services
- Active Directory Domain Services**
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- DHCP Server
- DNS Server
- Fax Server
- File Services
- Network Policy and Access Services
- Print Services
- Terminal Services
- UDDI Services
- Web Server (IIS)
- Windows Deployment Services
- Windows SharePoint Services

Description:

[Active Directory Domain Services \(AD DS\)](#) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

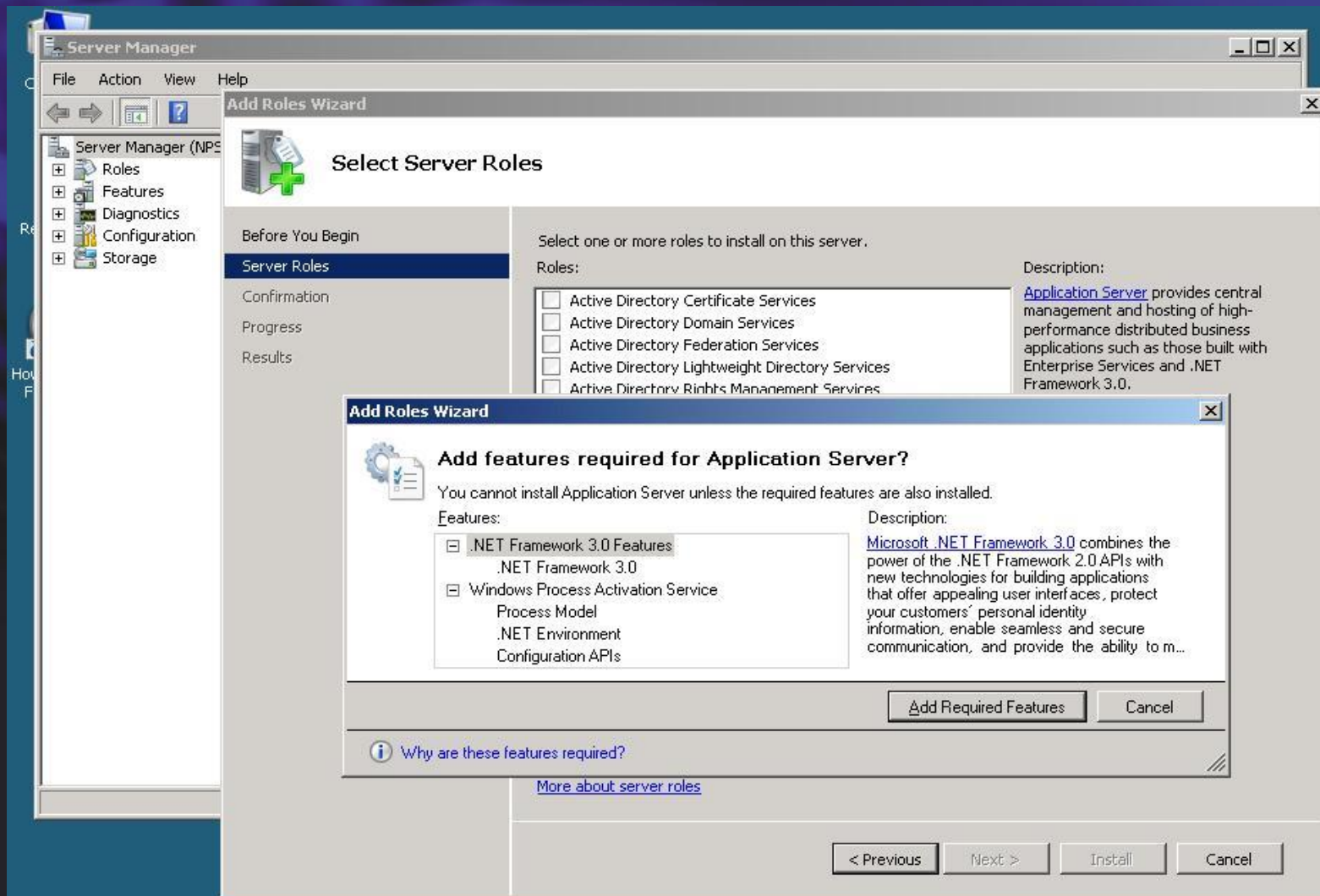
[More about server roles](#)

< Previous   Next >   Install   Cancel

Start | Server Manager | Administrator: Command... | RU | 12:11



# Ролевые игры



# Демонстрация механизма управления ролями сервера

# Безопасность сервисов

## Windows® XP SP2/Server 2003 R2

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

## Windows Vista/Windows Server 2008

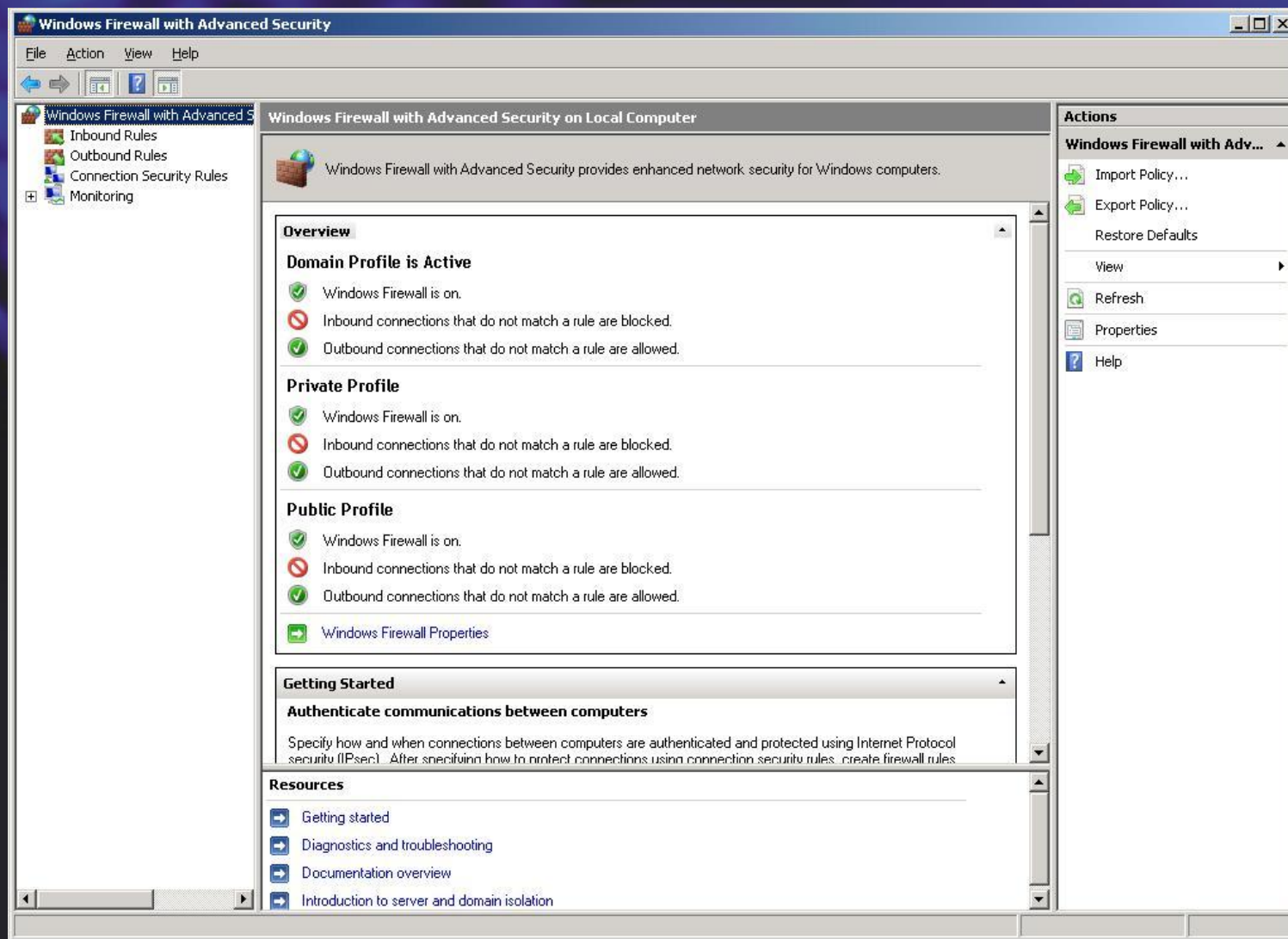
Аккаунт	Сервисы	
<b>LocalSystem</b> <i>Защищено брандмауэром</i>	WMI Perf Adapter Automatic updates Secondary Logon	App Management Wireless Configuration
<b>LocalSystem</b>	BITS Themes Rasman TrkWks Error Reporting	6to4 Task scheduler RemoteAccess Rasauto WMI
<b>Network Service</b> <i>Полностью изолированы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

# Новый брандмауэр

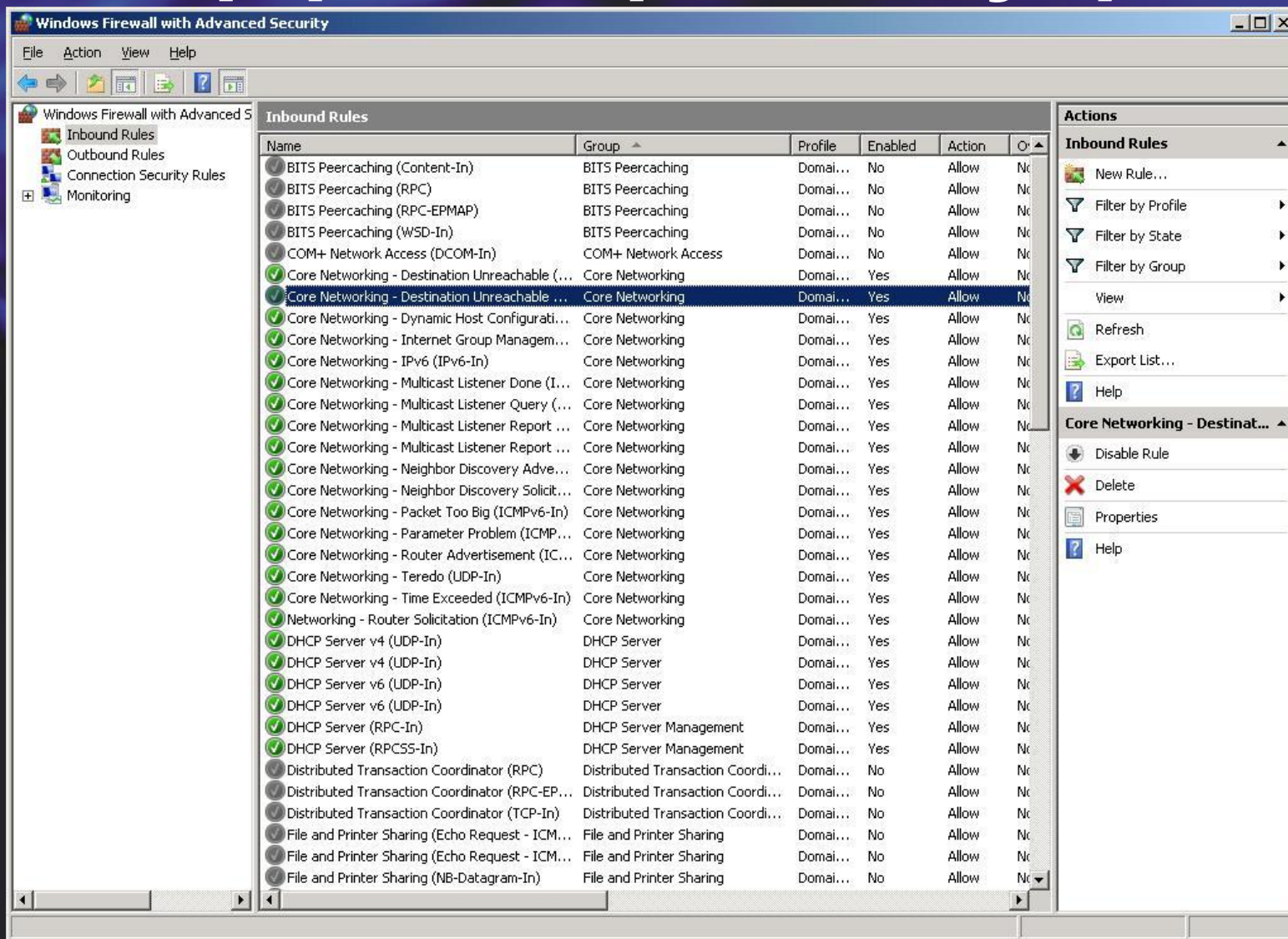
- Единый интерфейс управления брандмауэром и IPsec
- Правила фильтрации трафика стали более интеллектуальными
- Управление правилами на уровне компьютеров и групп пользователей Active Directory
- Двухнаправленная фильтрация трафика
- Набор предустановленных правил
- Переключаемые профили
- Поддержка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



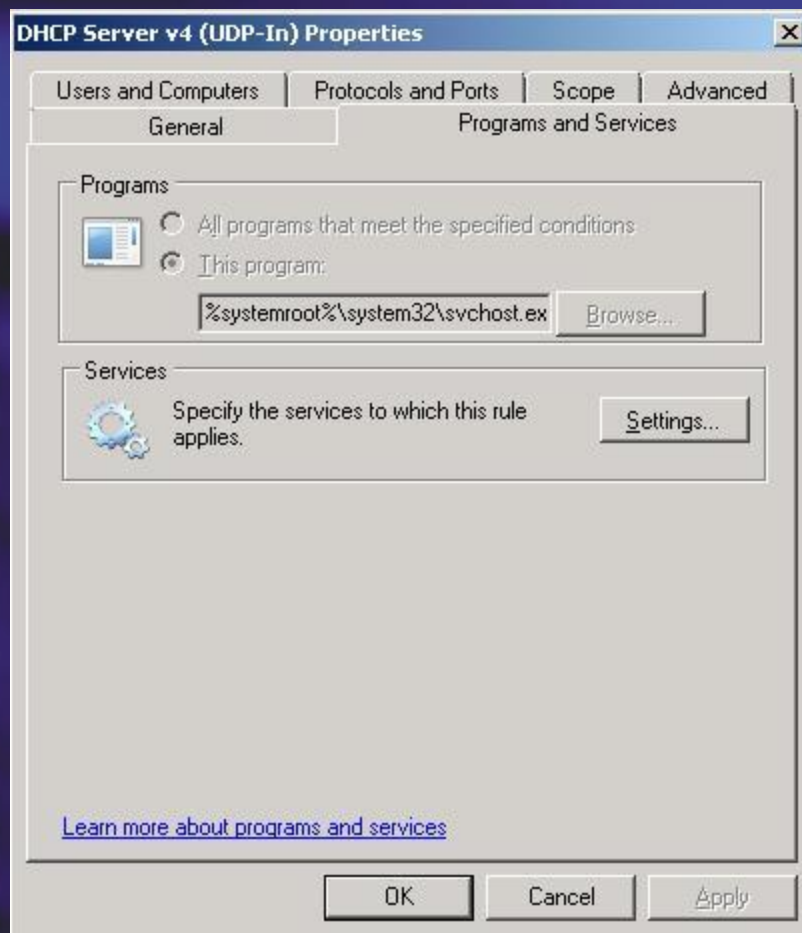
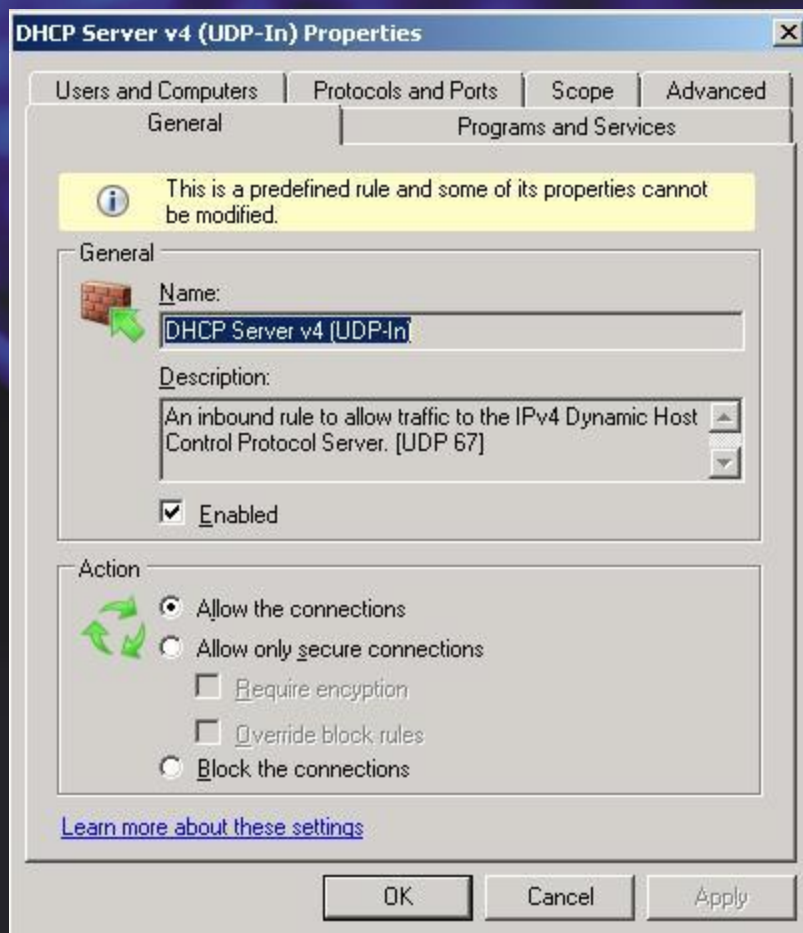
# Интерфейс Брандмауэра



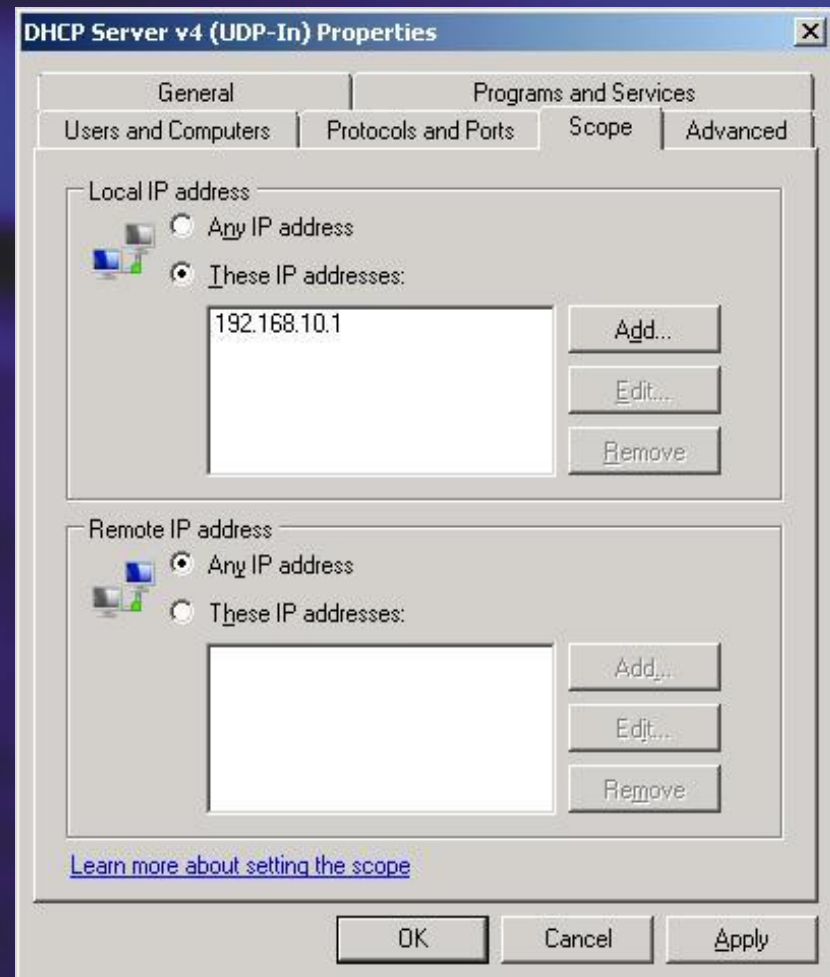
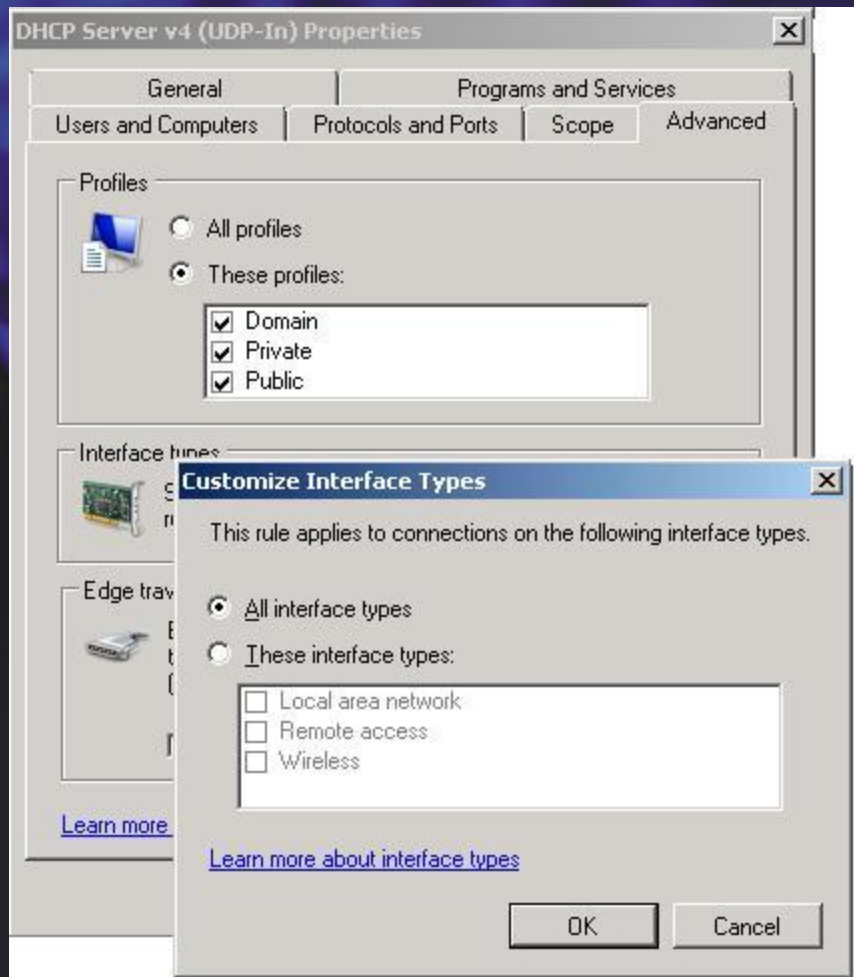
# Интерфейс Брандмауэра



# Интерфейс Брандмауэра

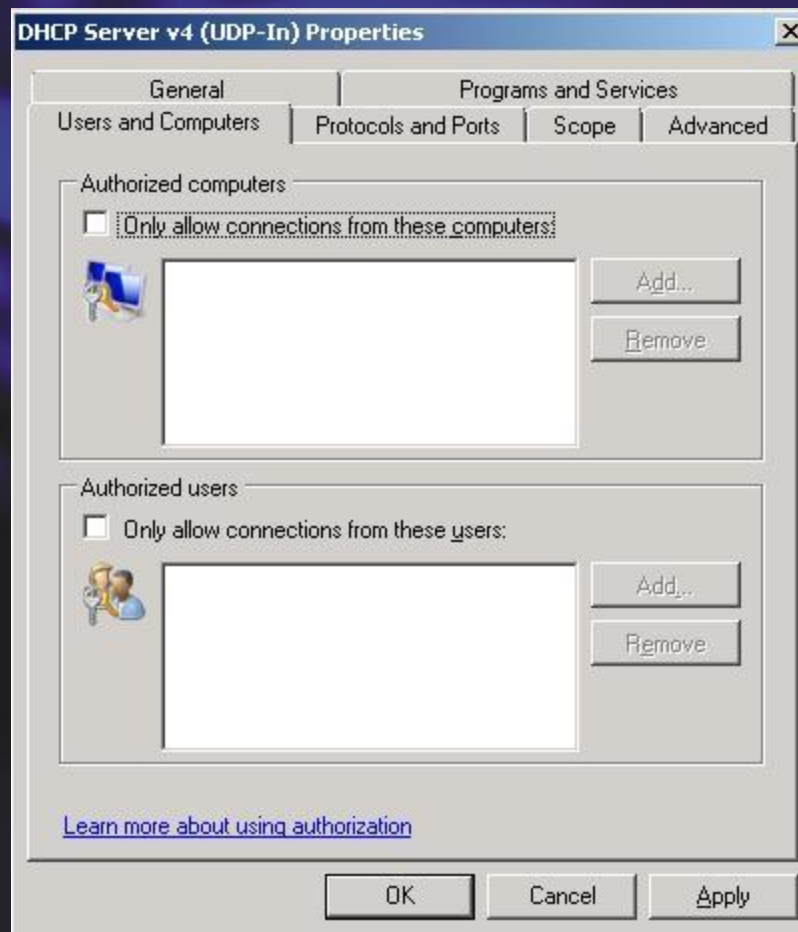


# Интерфейс Брандмауэра





# Интерфейс Брандмауэра



# Улучшение IPsec

## Улучшение

## Эффект

Упрощение политик

- Облегчение создания политик за счет непротиворечивости и снижения необходимости в исключениях
- Значительное упрощение поддержки 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 трафика в момент присоединения клиента к домену

Стойкие криптоалгоритмы

- AES, Elliptic Curve

# Интерфейс IPSec

**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?

- I**solation  
Restrict connections based on authentication criteria, such as domain membership or health status.
- A**uthentication exemption  
Do not authenticate connections from the specified computers.
- S**erver-to-server  
Authenticate connection between the specified computers.
- T**unnel  
Authenticate connections between gateway computers.
- C**ustom  
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

# Интерфейс IPSec

**New Connection Security Rule Wizard** [X]

## Endpoints

Specify the computers between which secured connections will be established using IPsec.

**Steps:**

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

Create a secured connection between computers in Endpoint 1 and Endpoint 2.

**Which computers are in Endpoint 1?**

Any IP address

These IP addresses:

Add...  
Edit...  
Remove

Customize the interface types to which this rule applies:

**Which computers are in Endpoint 2?**

Any IP address

These IP addresses:

Add...  
Edit...  
Remove

[Learn more about computer endpoints](#)

< Back   Next >   Cancel



# Интерфейс IPSec

**New Connection Security Rule Wizard**

**Requirements**

Specify the authentication requirements for connections that match this rule.

**Steps:**

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

When do you want authentication to occur?

- Request authentication for inbound and outbound connections**  
Authenticate whenever possible but authentication is not required.
- Require authentication for inbound connections and request authentication for outbound connections**  
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.
- Require authentication for inbound and outbound connections**  
Both inbound and outbound connections must be authenticated to be allowed.

[Learn more about authentication requirements](#)

< Back    Next >    Cancel

# Интерфейс IPSec

**New Connection Security Rule Wizard**

## Authentication Method

Specify how authentication is performed for connections that match this rule.

**Steps:**

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

What authentication method would you like to use?

**Computer certificate**  
Restrict communications to connections from computers that have a certificate from this certification authority (CA).

CA name:

Accept health certificates only  
These certificates are issued by Network Access Protection health certificate servers.

**Preshared Key (not recommended)**

Key:

Preshared key authentication is less secure than other authentication methods.  
Preshared keys are stored in plaintext.

**Advanced**  
Specify custom first and second authentication settings.

[Learn more about authentication methods](#)

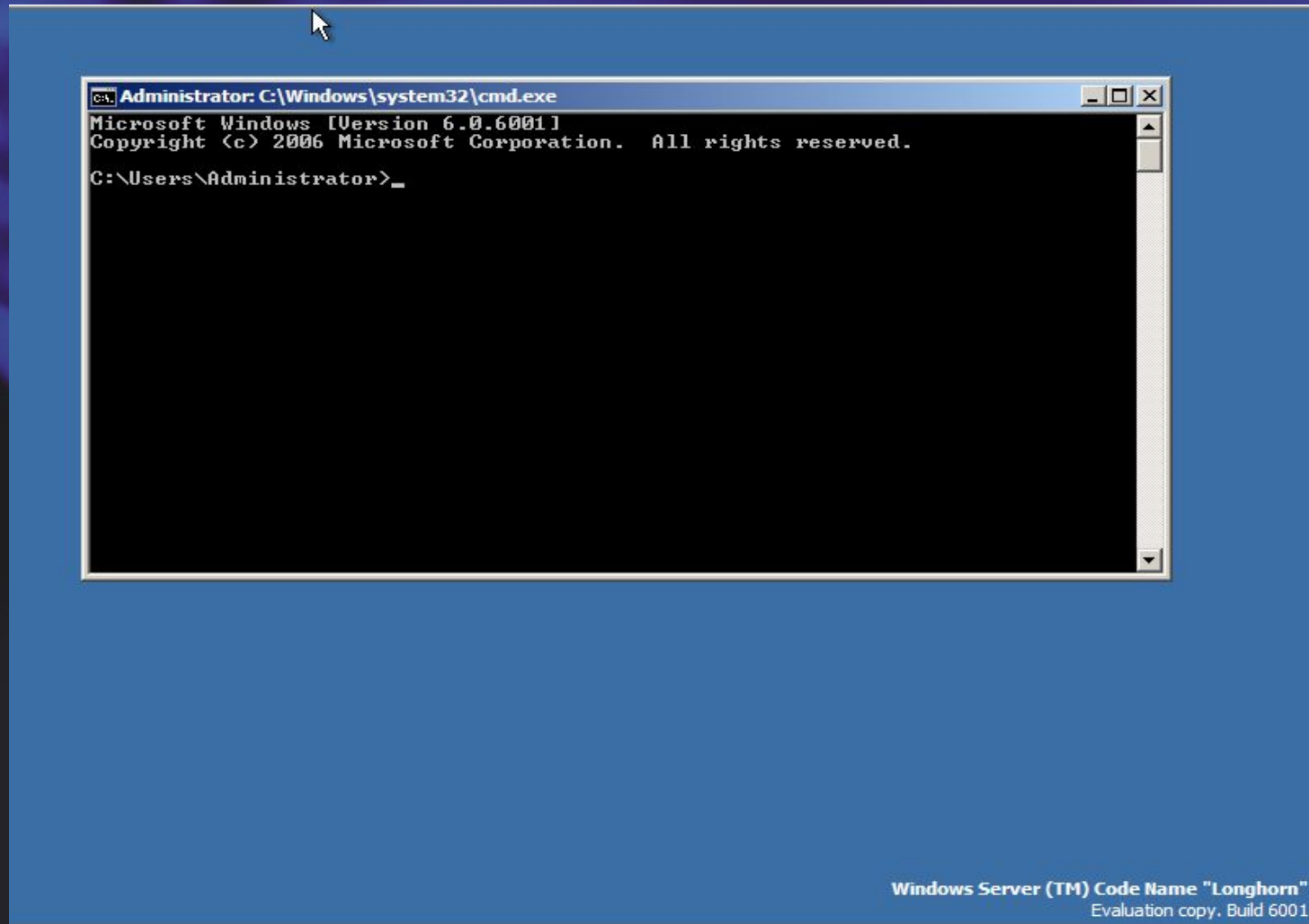
< Back    Next >    Cancel

# 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
- Ограниченный набор ролей
- Упрощение обслуживания и управления
- Меньше возможностей для атаки

## Роли Server Core

DNS

DHCP

File

AD

## Server Core

Security, TCP/IP, File Systems, RPC,  
стандартные подсистемы Core Server

## Роли WindowsServer 2008

TS

IAS

Web  
Server

Share  
Point®

и.т.д...

## Server

WinFx, Shell, GUI, и.т.д.

~~GUI, CLR,  
Shell, IE,  
Media, OE,  
и.т.д.~~

# 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:

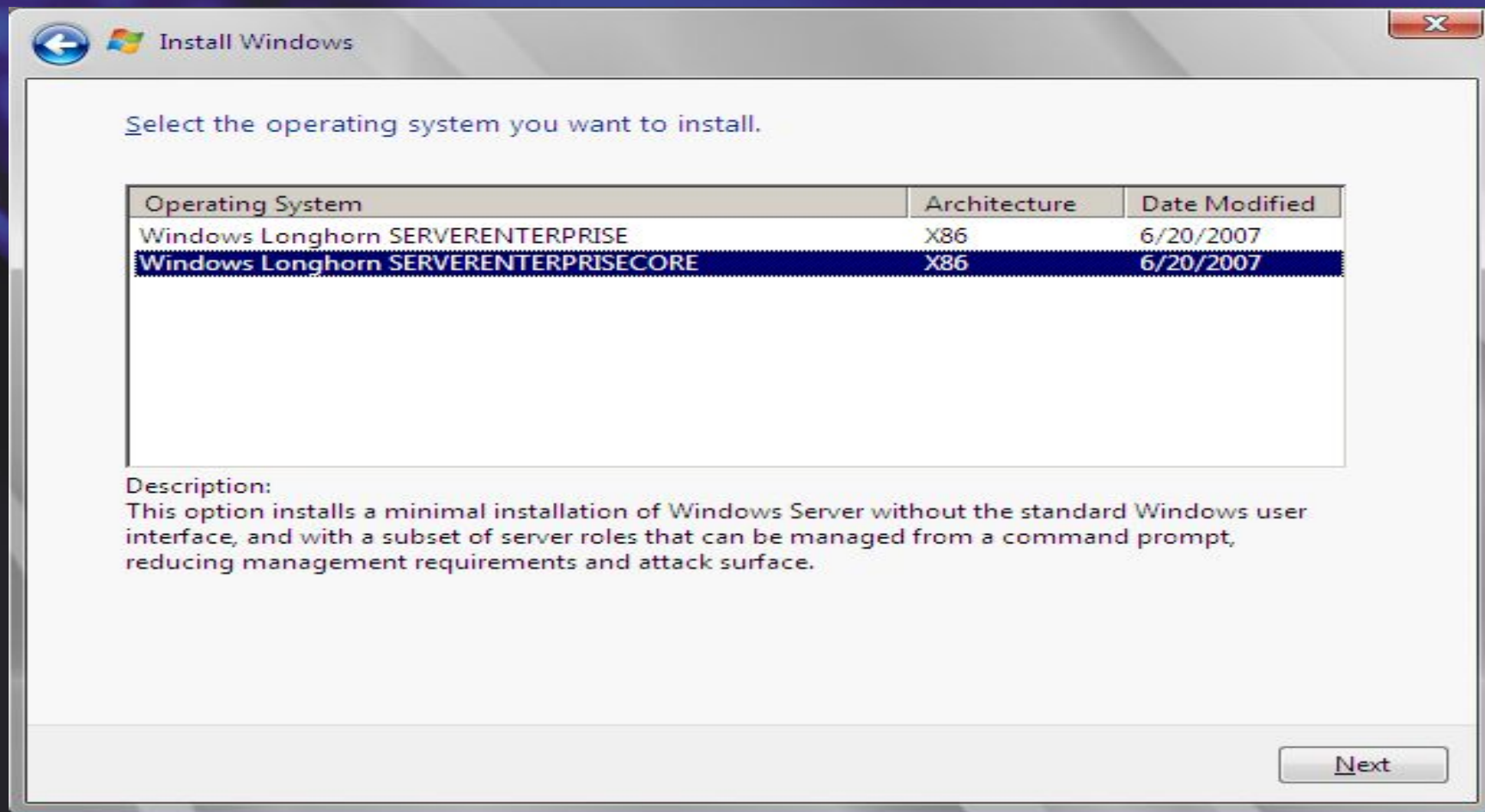
- Инсталляция с носителя Windows Server 2008.
- Версии Enterprise и Standard Edition.
- Обновление до Server Core R2.

## 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

## Главный офис



- ✓ Полноценный DC
- ✓ Защищенная серверная

Интернет

## Филиал



- ✓ DC, DNS только для чтения
- ✓ Односторонняя реплика
- ✓ Кэширование критичных данных
- ✓ локальный администратор

### Копия базы AD только для чтения

- Может содержать все объекты 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

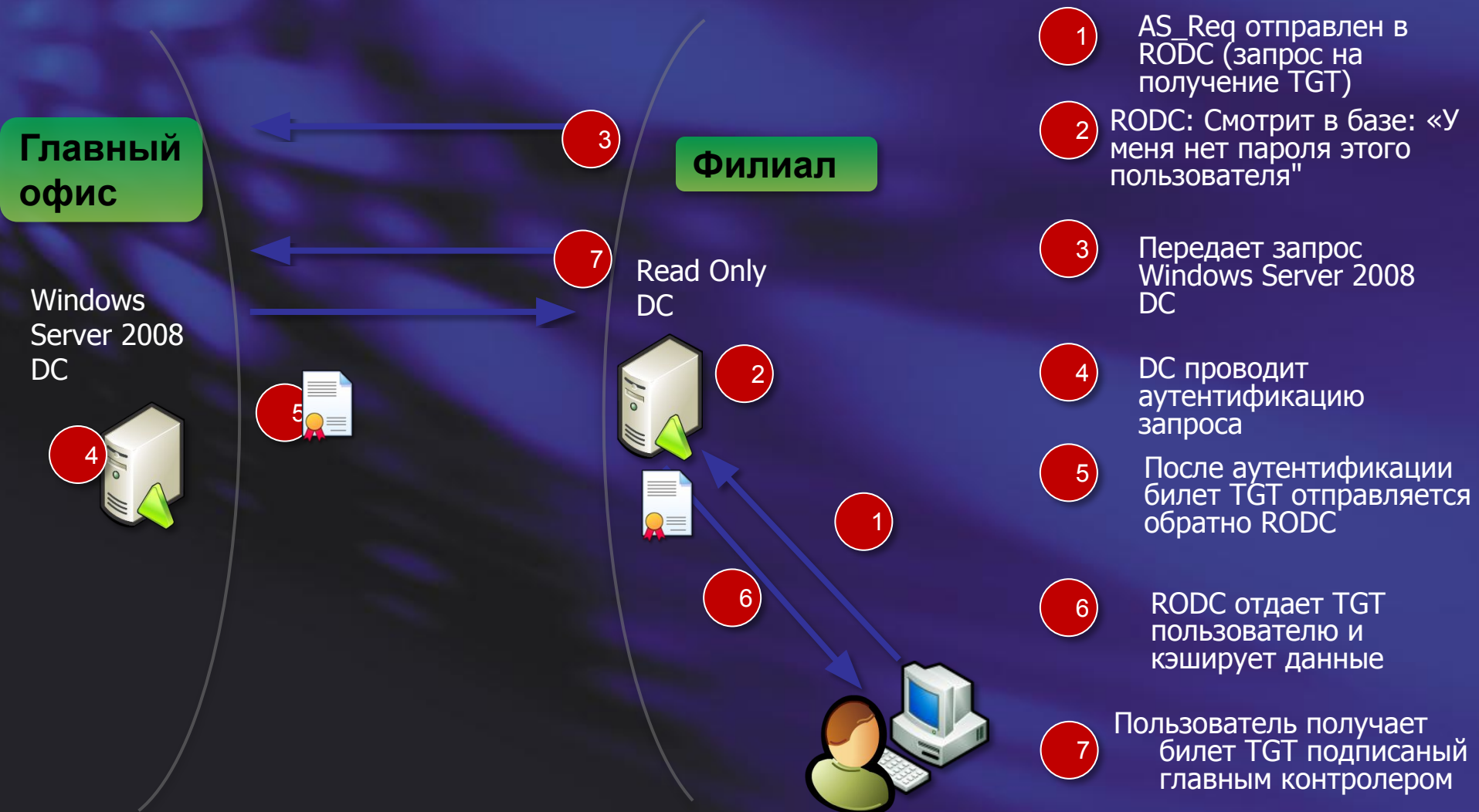
- Не хранит паролей пользователей (по умолчанию)
- RODC выдает только локальные билеты

### Разделение административных ролей

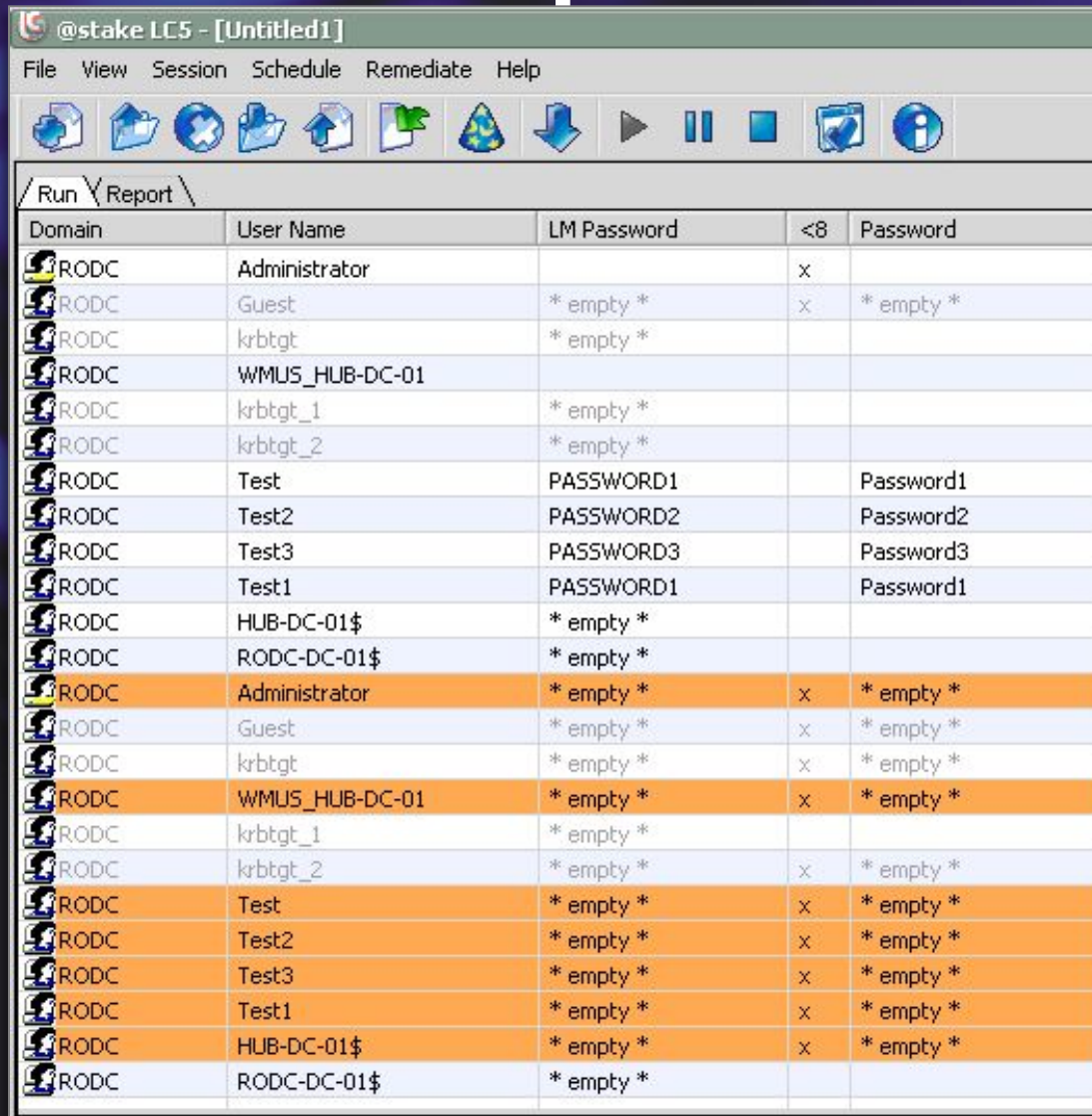
- Управление от имени локального пользователя
- Администратор локального контролера не является администратором глобального DC



# Как RODC функционирует



# 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** [X]

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



```
Windows PowerShell
PS D:\> get-service
```

- 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

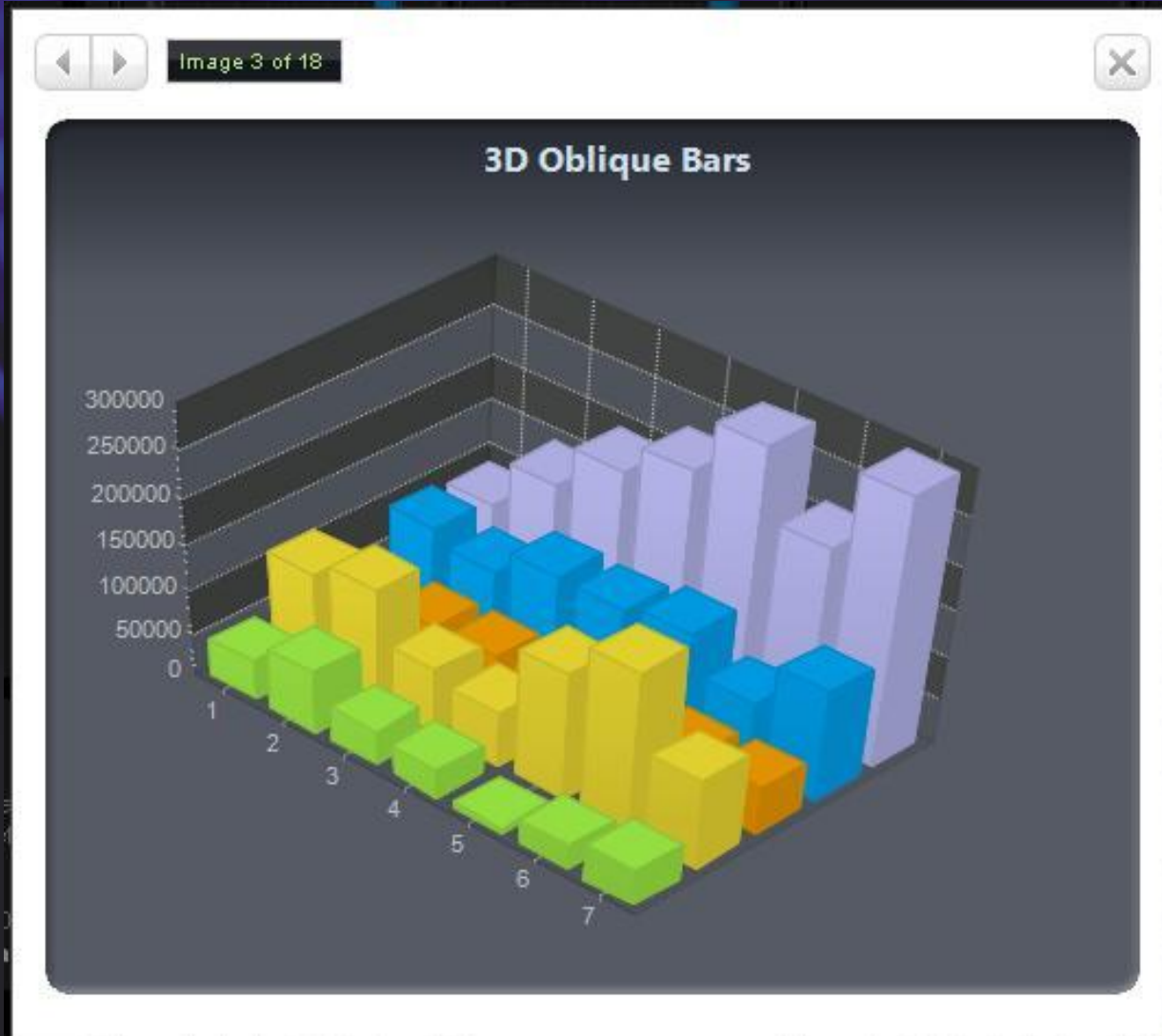
Используется в следующих проектах:

- 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

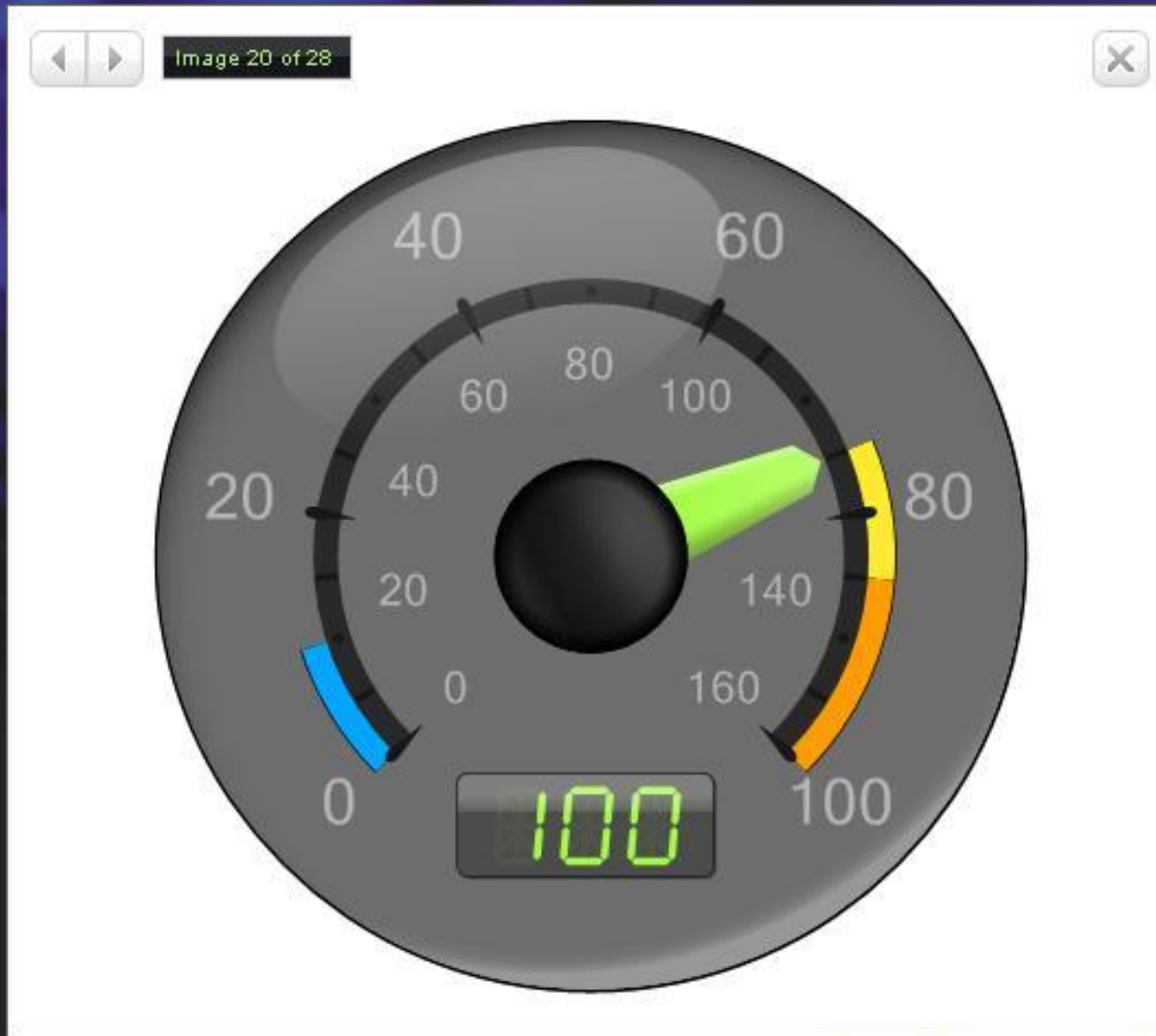
# Демонстрация Powershell



# PowerShell + PowerGadgets



# PowerShell + PowerGadgets



# PowerShell + PowerGadgets

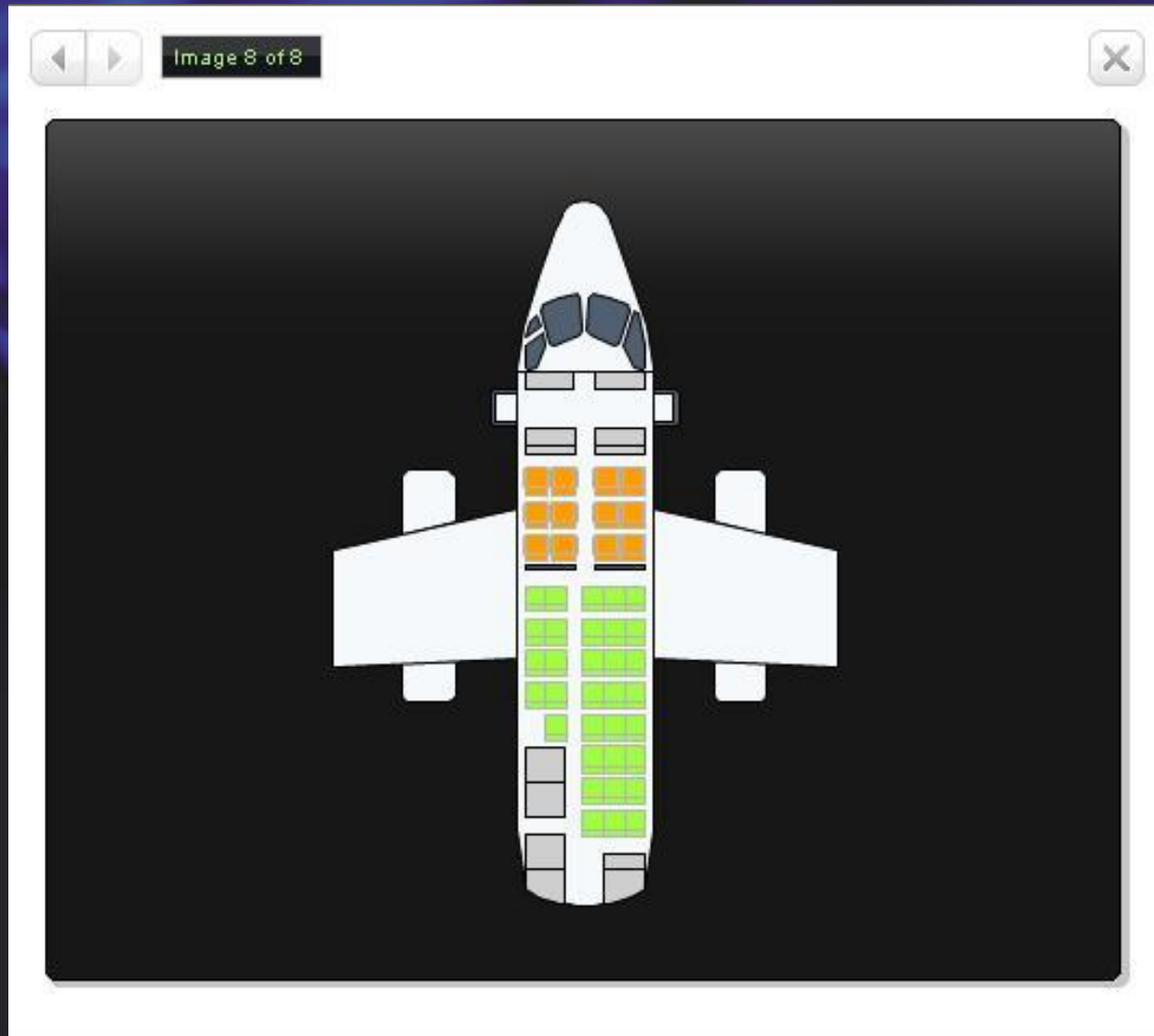


# PowerShell + PowerGadgets





# PowerShell + PowerGadgets



# PowerShell + PowerGadgets



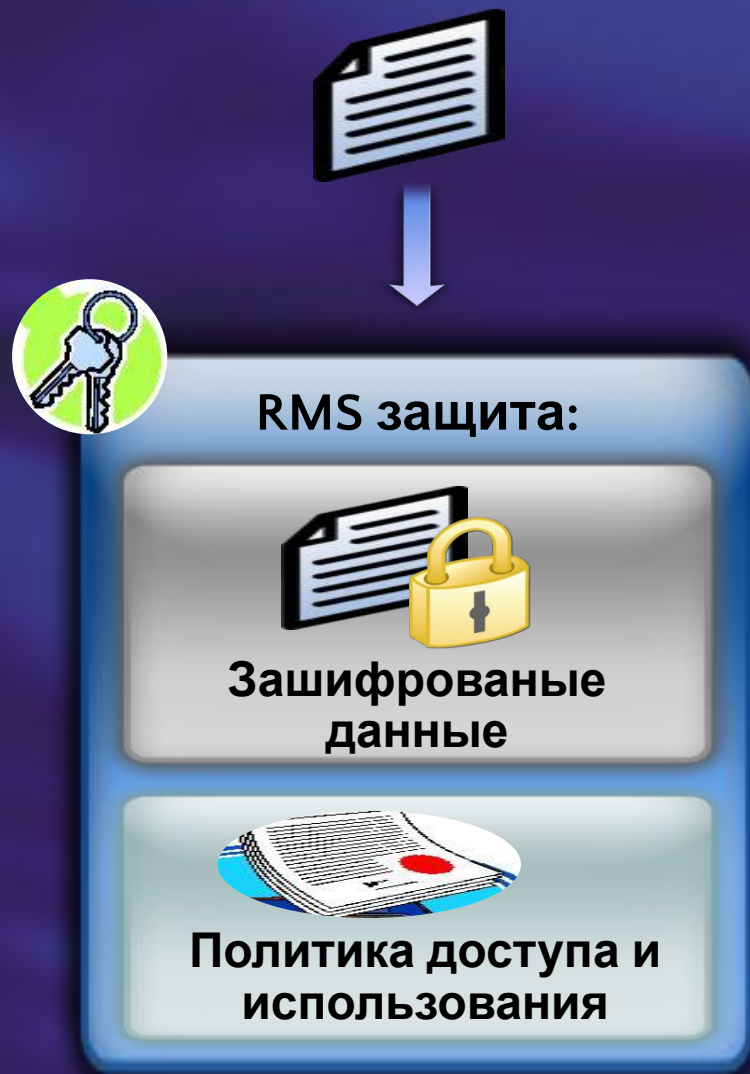
# Цель Rights Management Service:

Дать возможность защитить важную информацию в течении жизненного 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 централизованно реализовать политику организации
  - RMS протоколирование позволяет отслеживать потоки информации
- Расширяемая платформа
  - Основная возможность платформы разработки от MS
  - Поддерживается приложениями Microsoft и других поставщиков

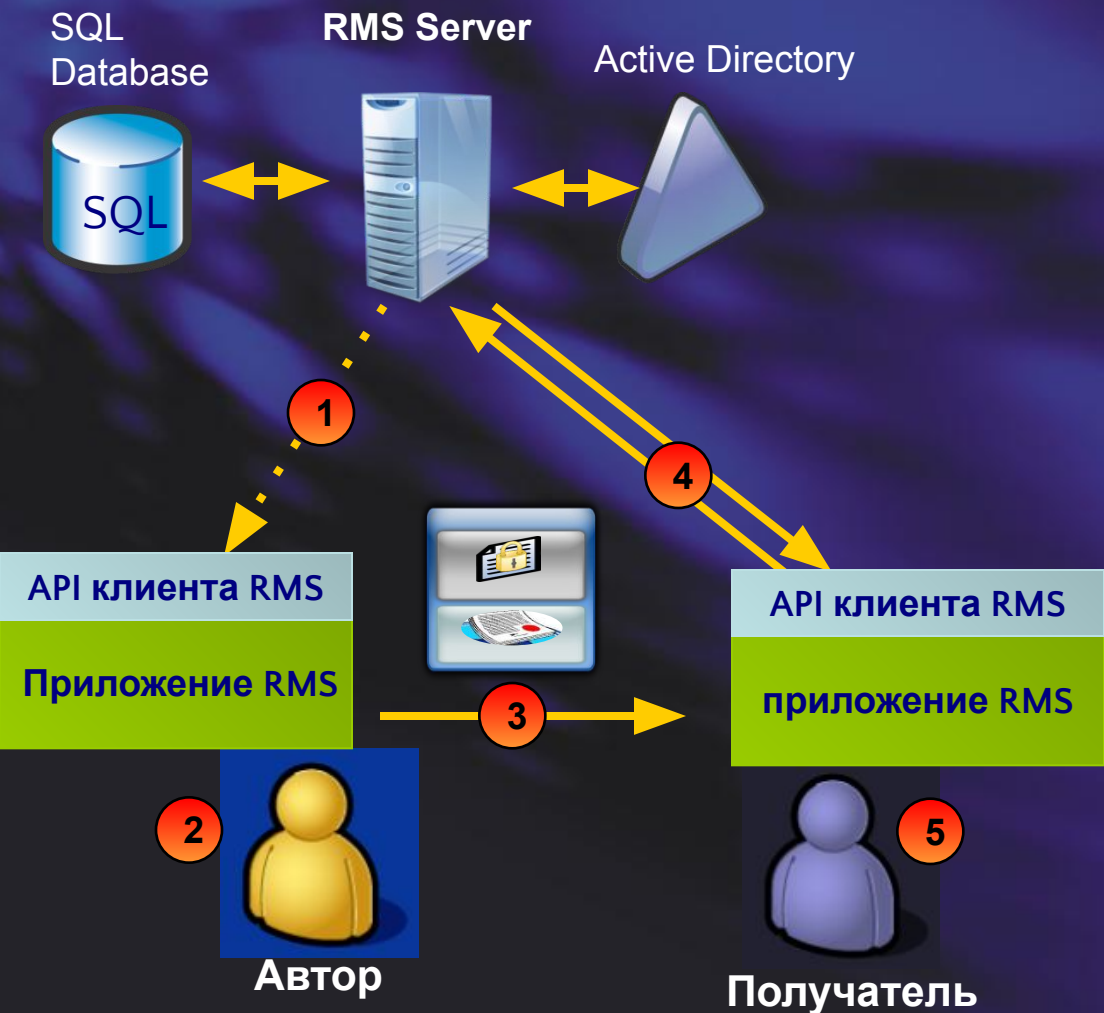
# Как RMS защищает данные?

- RMS защищает с помощью
  - Сильного шифрования
    - Симметричная и асимметричная 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



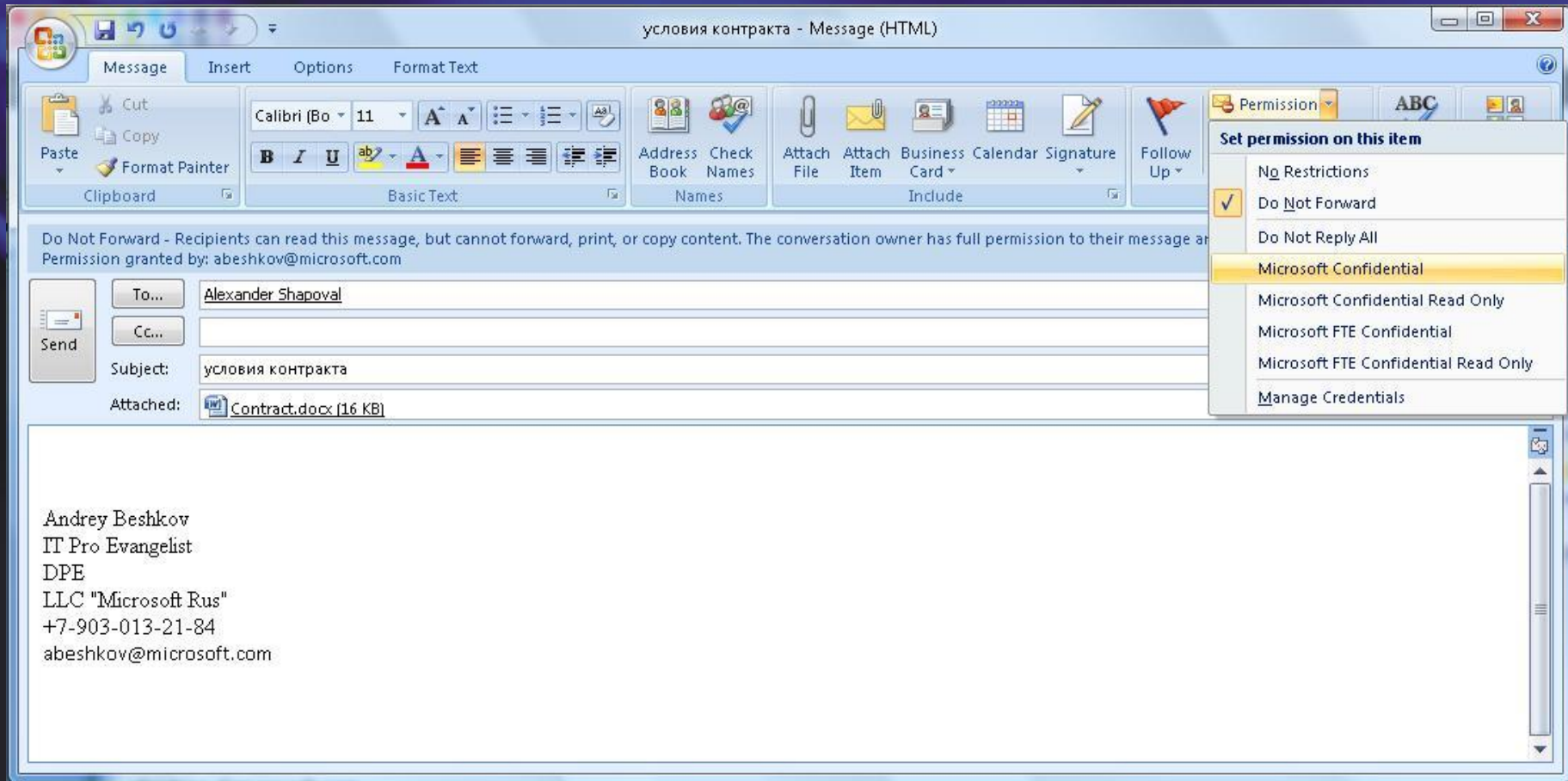


# Пример работы RMS



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; шифрованный 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<sup>®</sup>**

*Your potential. Our passion.<sup>™</sup>*