



Усовершенствования системы безопасности Windows Server 2008

Семинары TechNet. Осень 2007

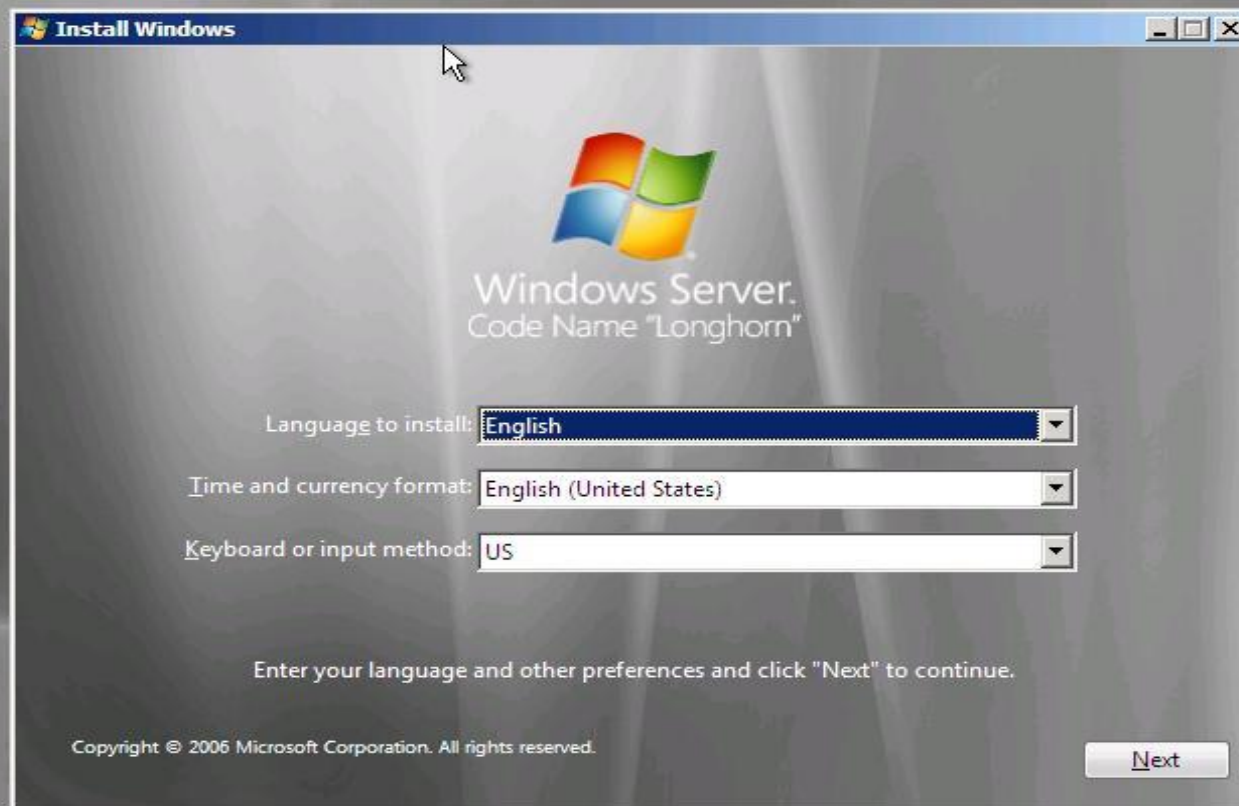
Краснодар, Казань, Новосибирск, Санкт-Петербург, Самара, Екатеринбург, Ростов-на-Дону, Н. Новгород,
Владивосток, Хабаровск

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

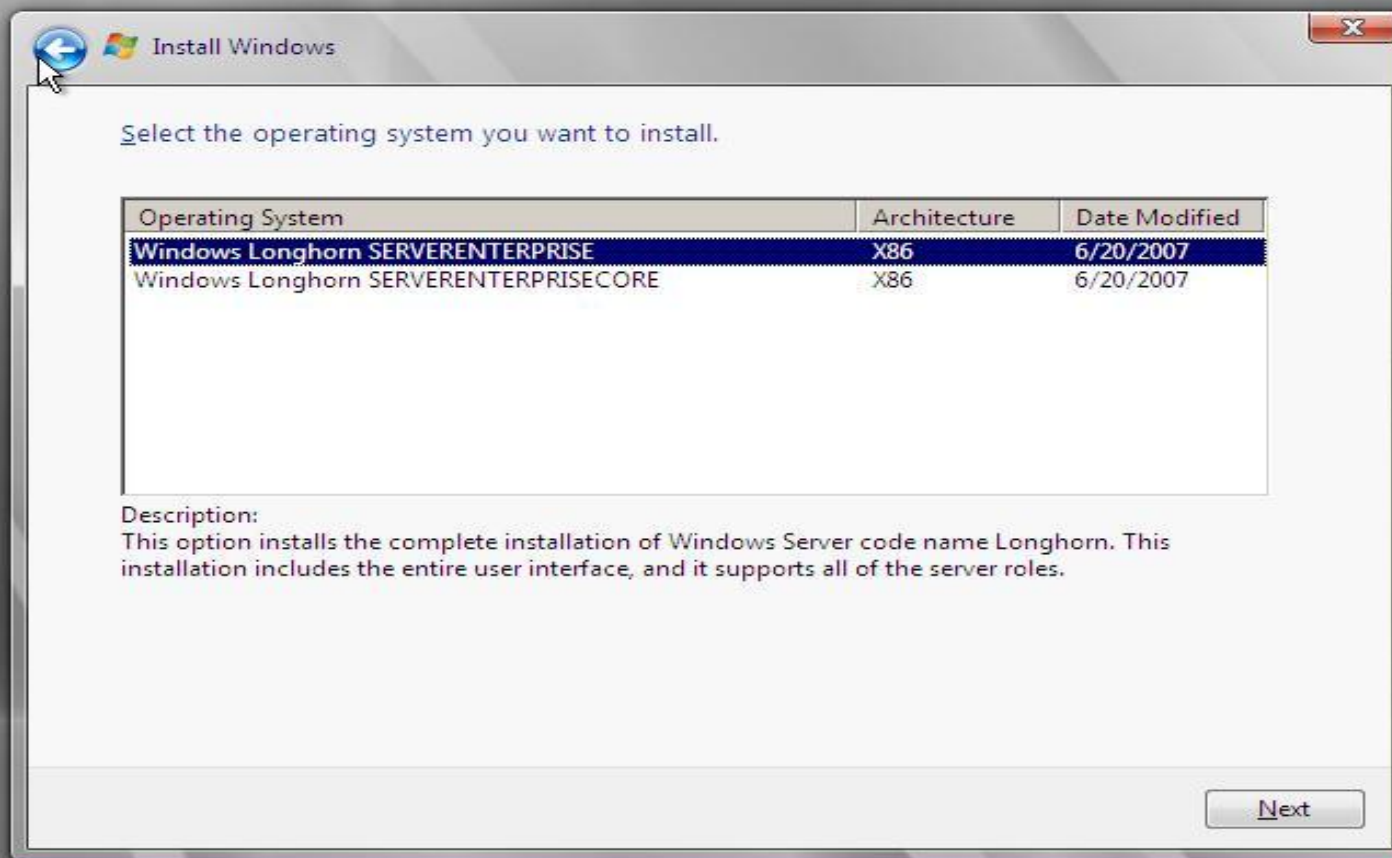


1

Collecting information

Installing Windows

Простота инсталляции



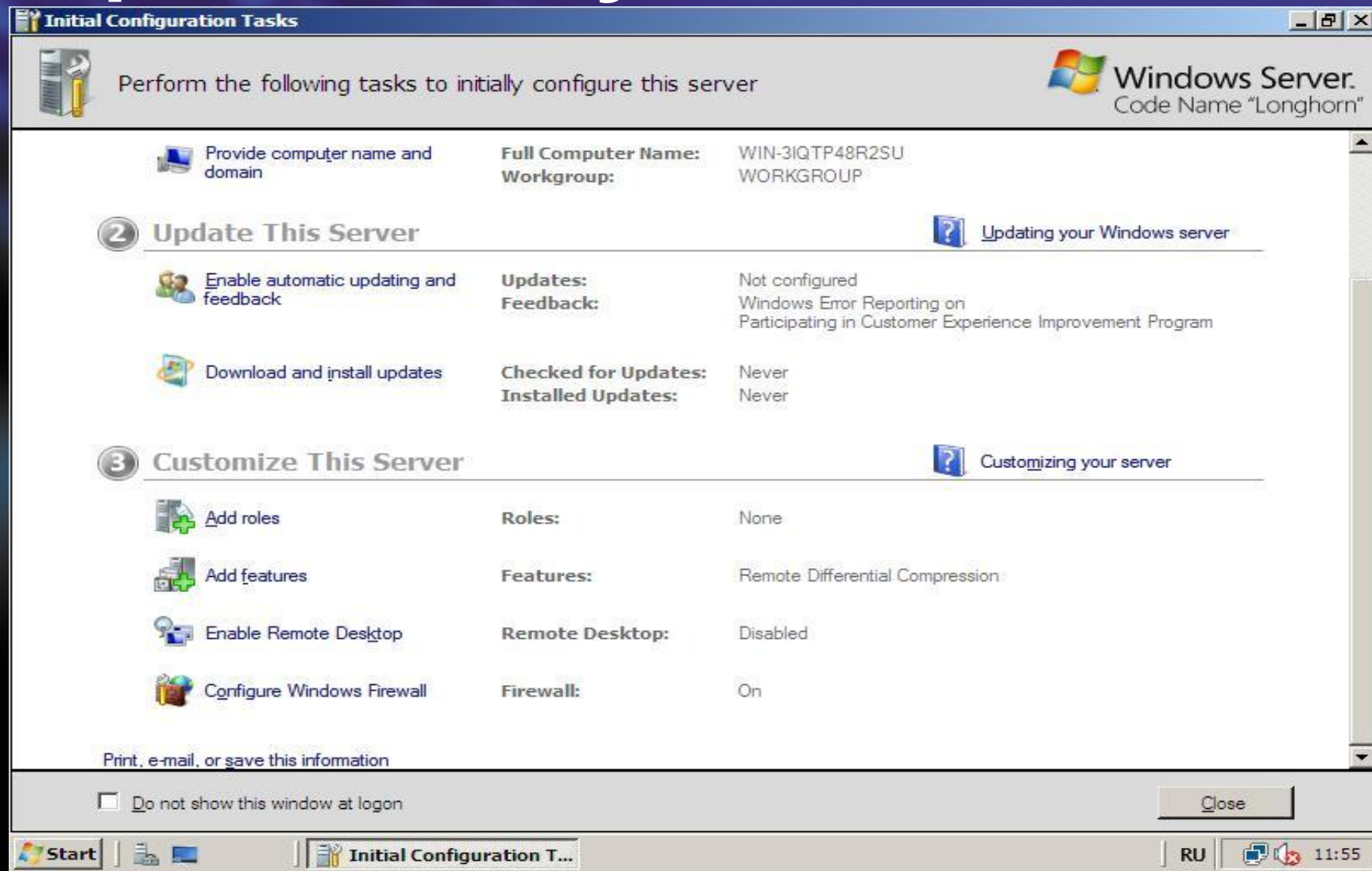
1

Collecting information

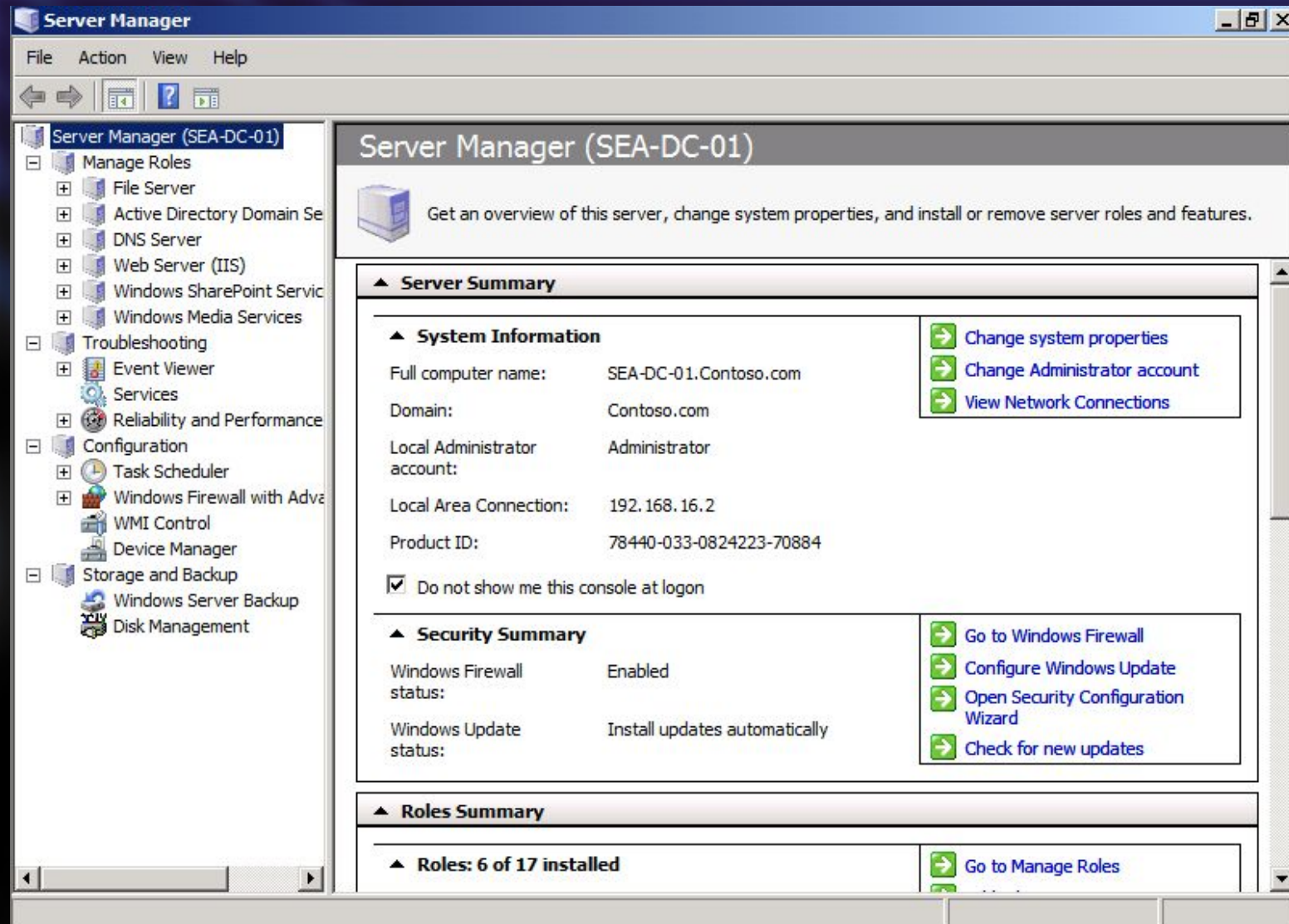
2

Installing Windows

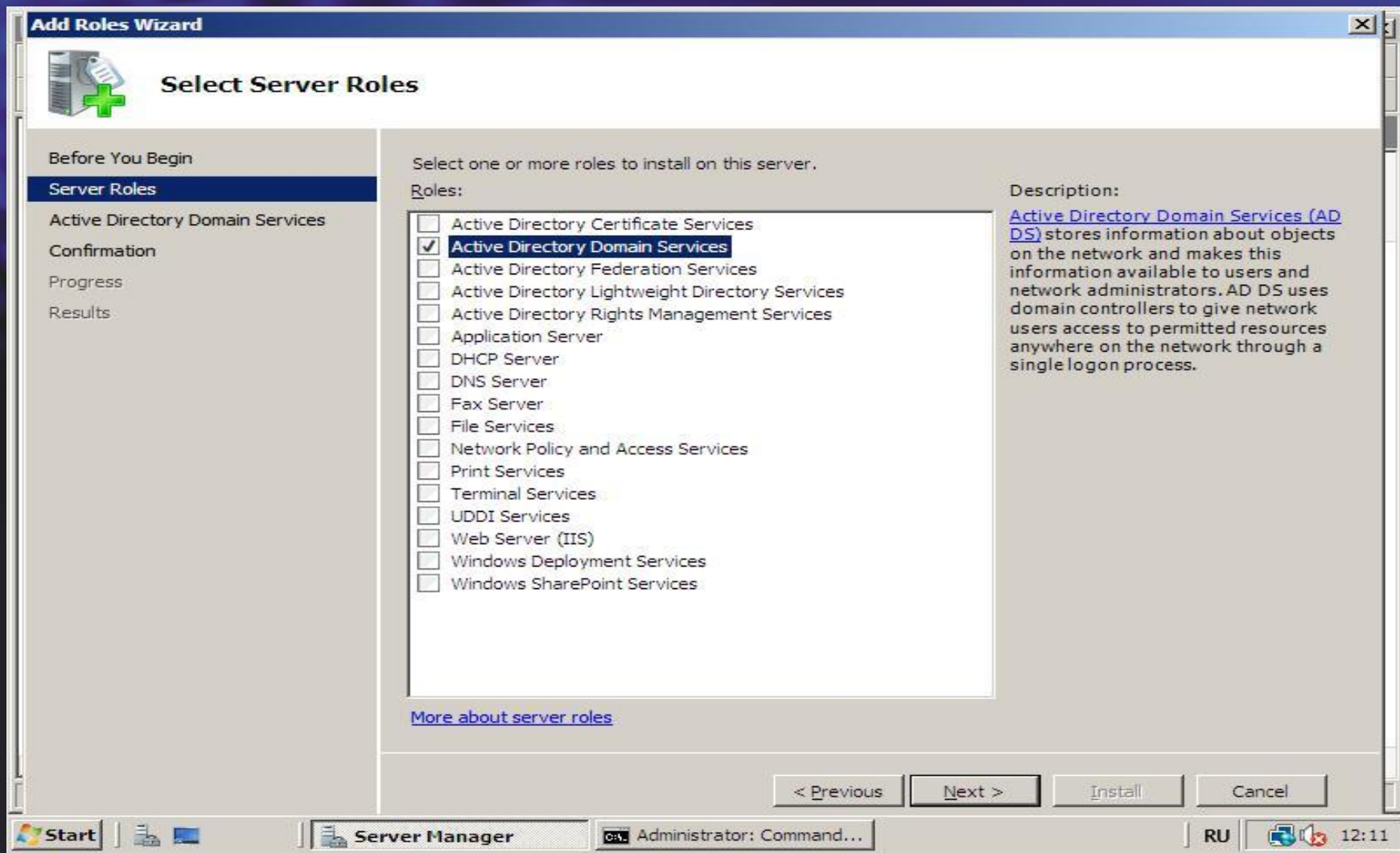
Через 30 минут



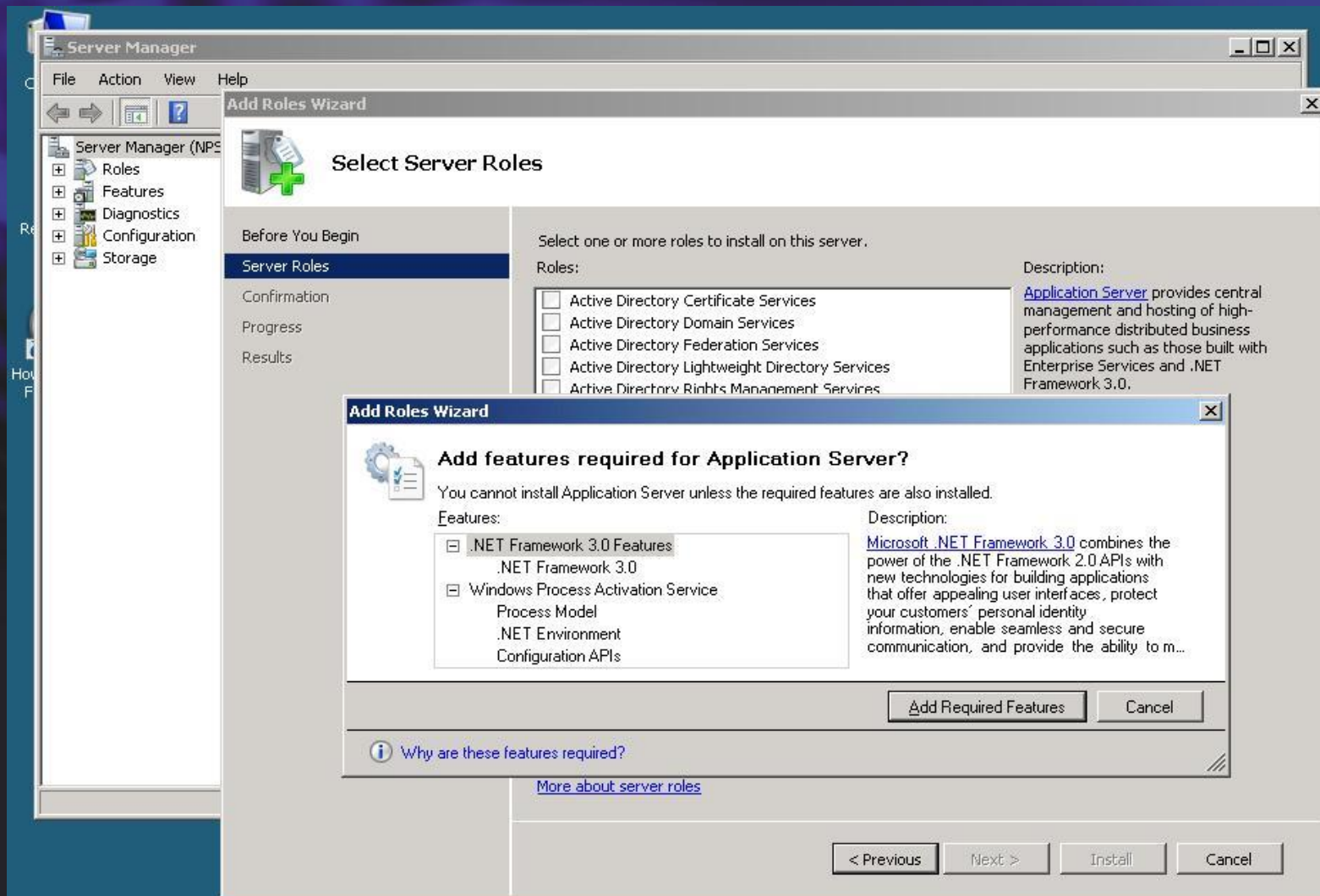
Новый интерфейс управления



Ролевые игры



Ролевые игры



Демонстрация механизма управления ролями сервера

Безопасность сервисов

Windows® XP SP2/Server 2003 R2

Аккаунт	Сервисы	
LocalSystem	Wireless Configuration 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
Network Service	DNS Client	
Local Service	SSDP WebClient TCP/IP NetBIOS helper Remote registry	

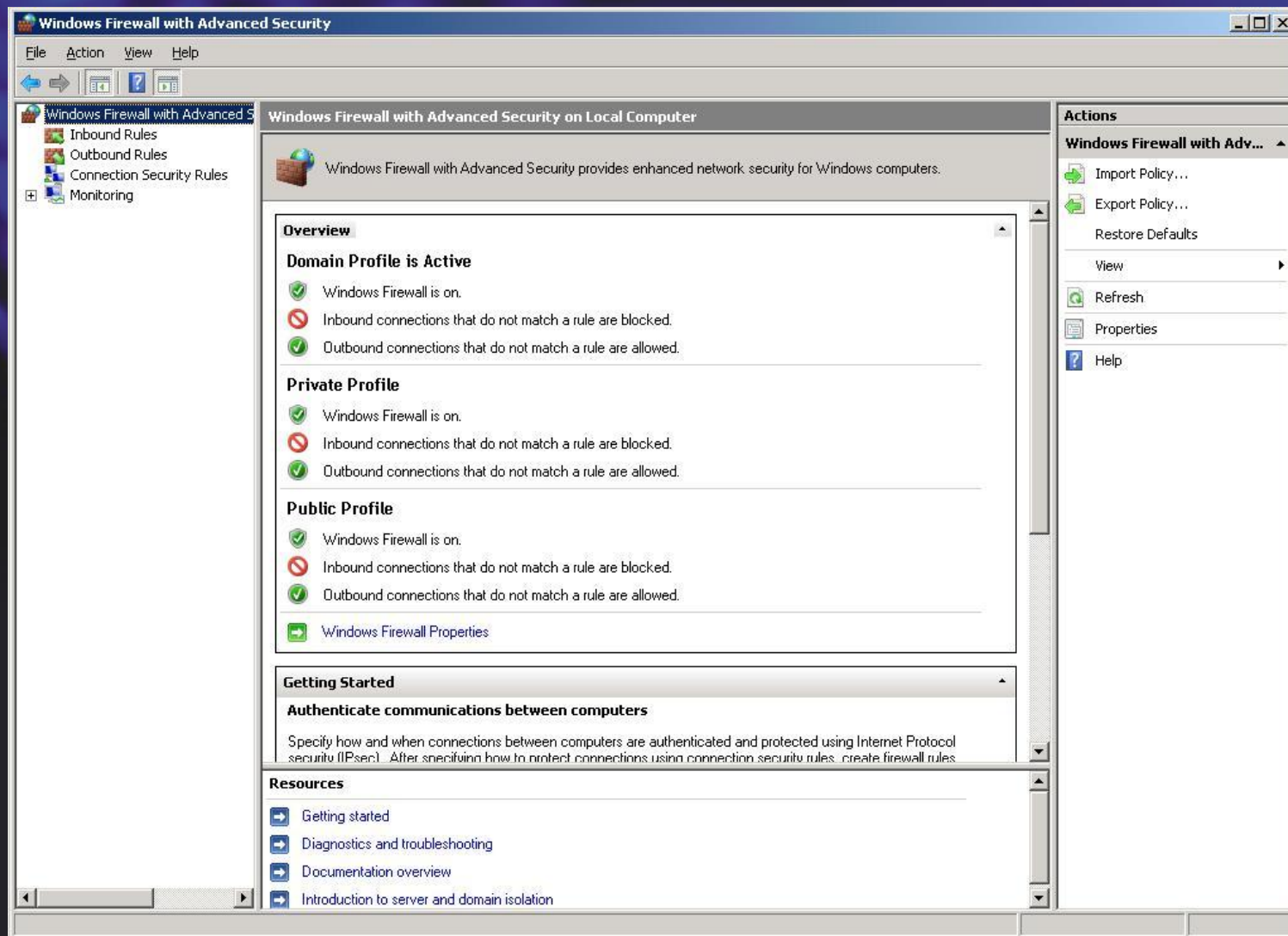
Windows Vista/Windows Server 2008

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

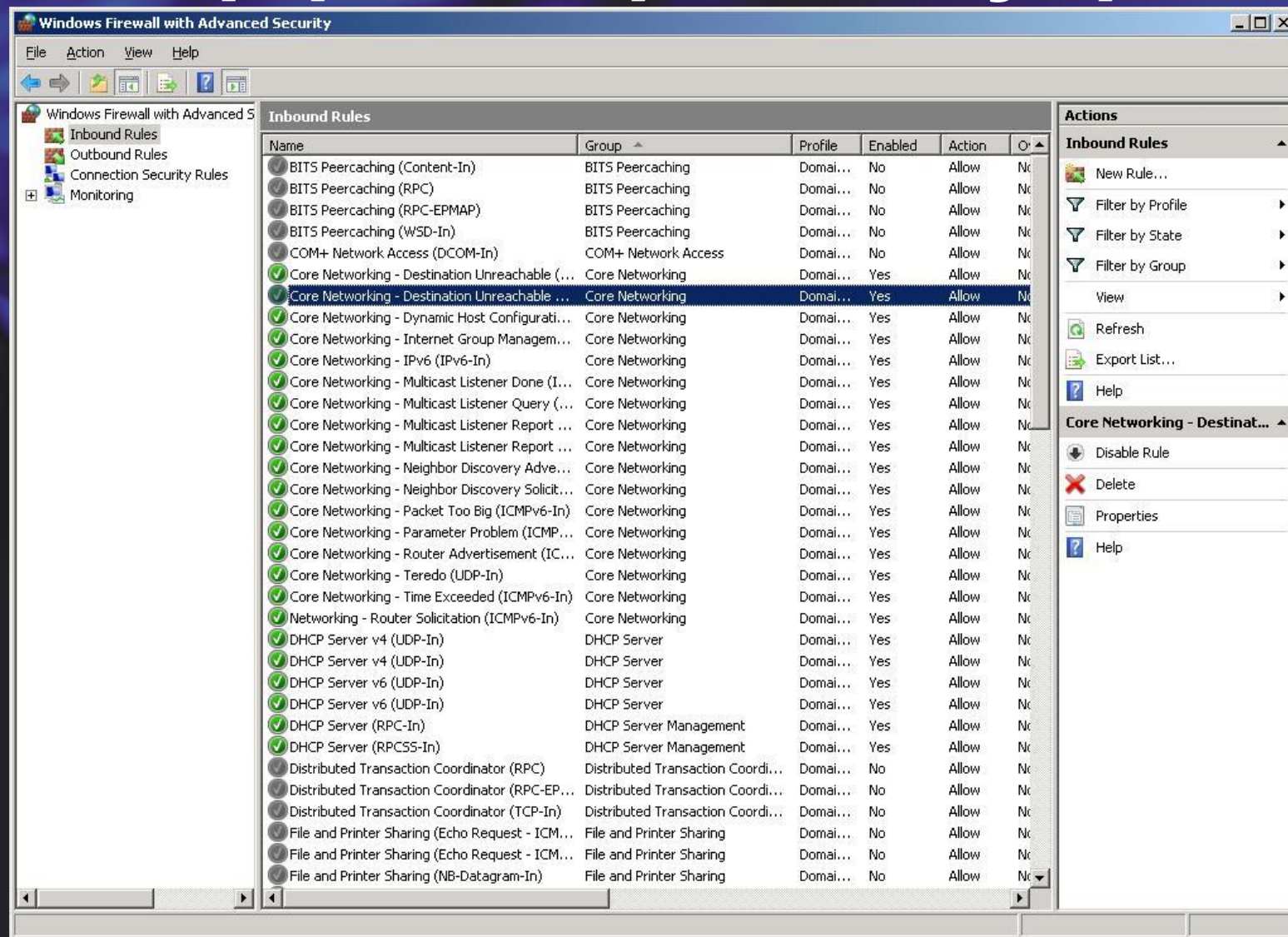
Новый брандмауэр

- 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

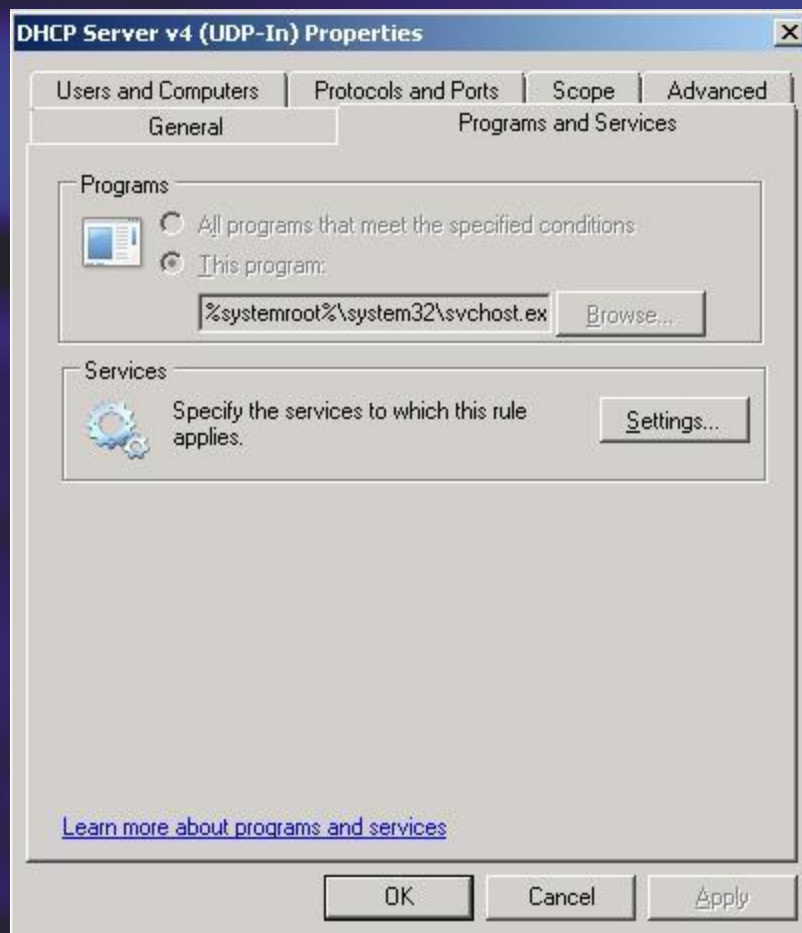
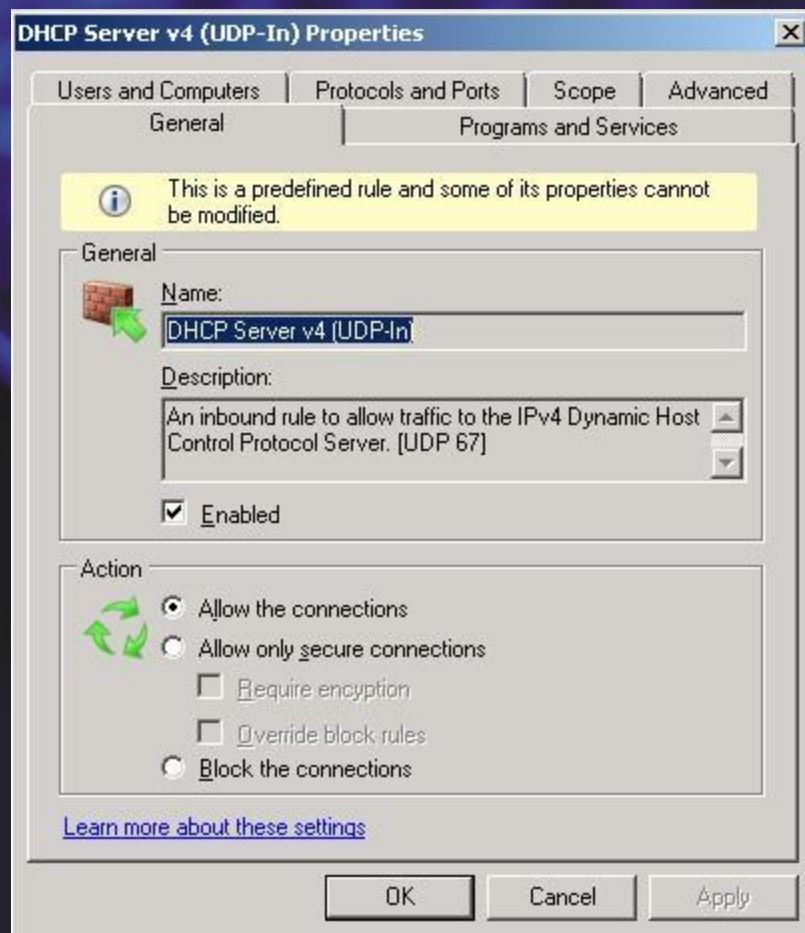
Интерфейс Брандмауэра



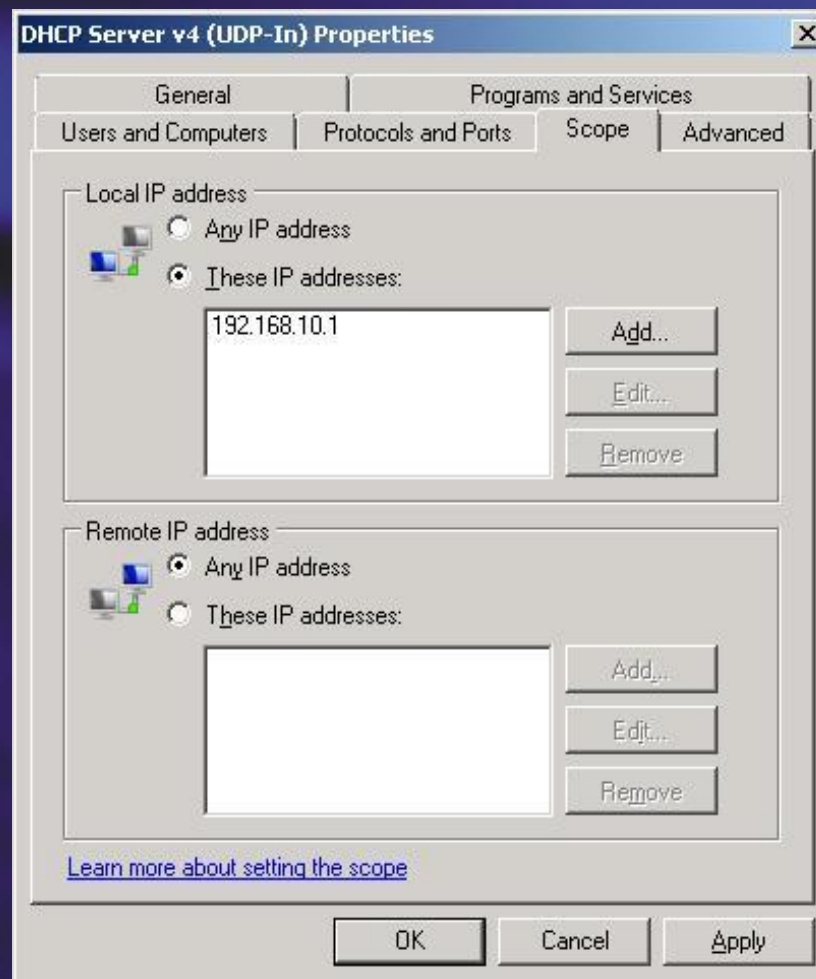
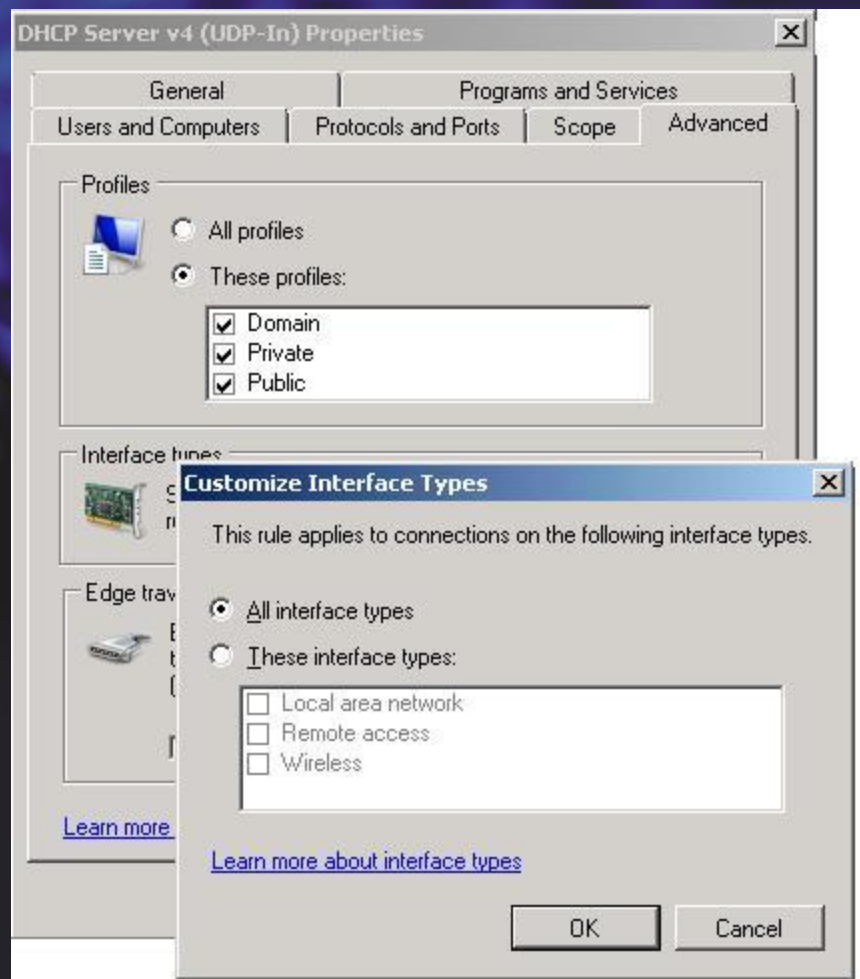
Интерфейс Брандмауэра



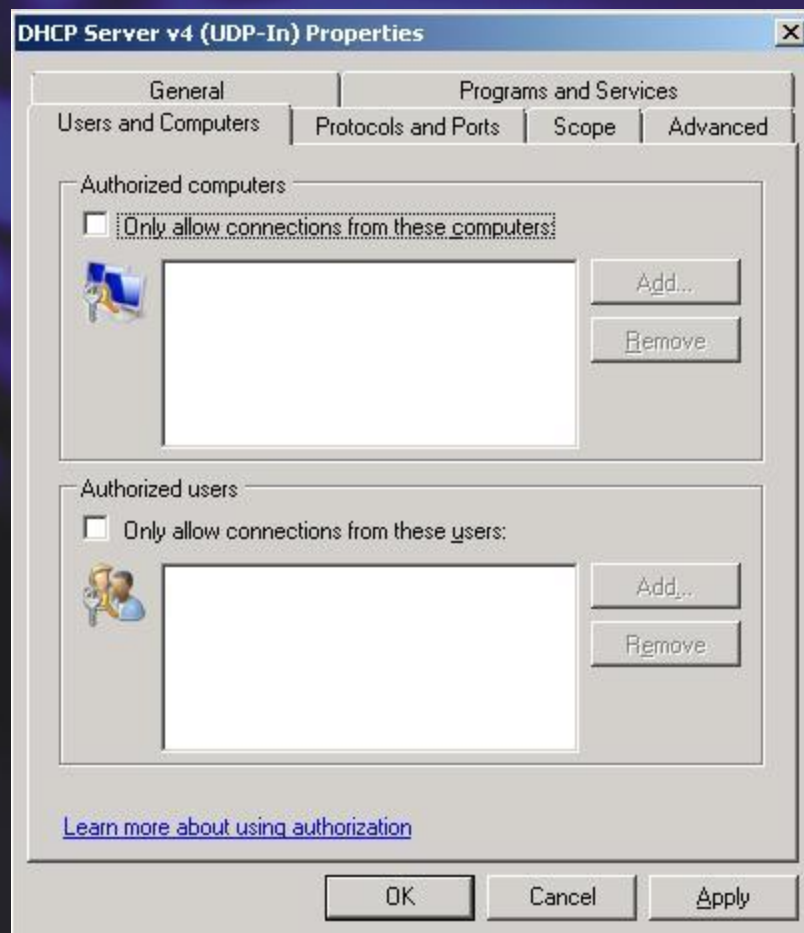
Интерфейс Брандмауэра



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

The screenshot shows the 'New Connection Security Rule Wizard' window. The title bar reads 'New Connection Security Rule Wizard'. The main heading is 'Rule Type', with the instruction 'Select the type of connection security rule to create.' Below this is a 'Steps' pane on the left with a list of steps: 'Rule Type' (selected with a green dot), 'Endpoints', 'Requirements', 'Authentication Method', 'Profile', and 'Name'. The main area asks 'What type of connection security rule would you like to create?' and lists five options with radio buttons: 'Isolation' (restrict connections based on authentication criteria), 'Authentication exemption' (do not authenticate connections from specified computers), 'Server-to-server' (selected, authenticate connection between specified computers), 'Tunnel' (authenticate connections between gateway computers), and 'Custom' (custom rule). A note at the bottom states: '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.' A link 'Learn more about rule types' is provided. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

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

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

The screenshot shows the 'New Connection Security Rule Wizard' window, specifically the 'Requirements' step. The window has a title bar with the text 'New Connection Security Rule Wizard' and a close button. Below the title bar, the 'Requirements' section is highlighted. The main area contains a question 'When do you want authentication to occur?' followed by three radio button options. The first option is 'Request authentication for inbound and outbound connections' with the description 'Authenticate whenever possible but authentication is not required.' The second option is 'Require authentication for inbound connections and request authentication for outbound connections' with the description 'Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.' The third option is 'Require authentication for inbound and outbound connections' with the description 'Both inbound and outbound connections must be authenticated to be allowed.' At the bottom of the main area is a link 'Learn more about authentication requirements'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

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.

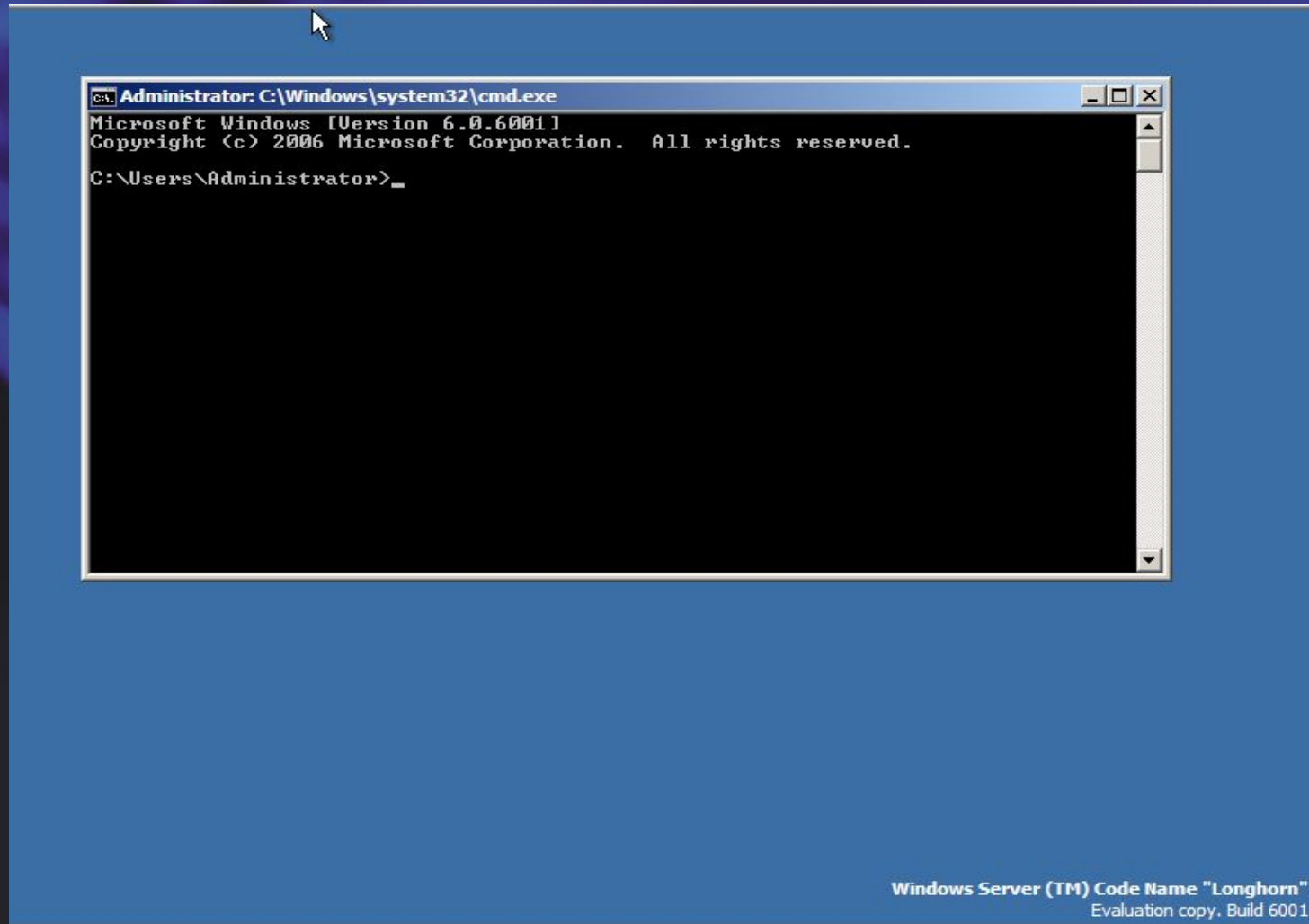
[Learn more about authentication methods](#)

< 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

Роли Windows Server 2008

TS

IAS

Web
Server

Share
Point®

и.т.д...

Server

WinFx, Shell, GUI, и.т.д.

Server Core

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

~~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

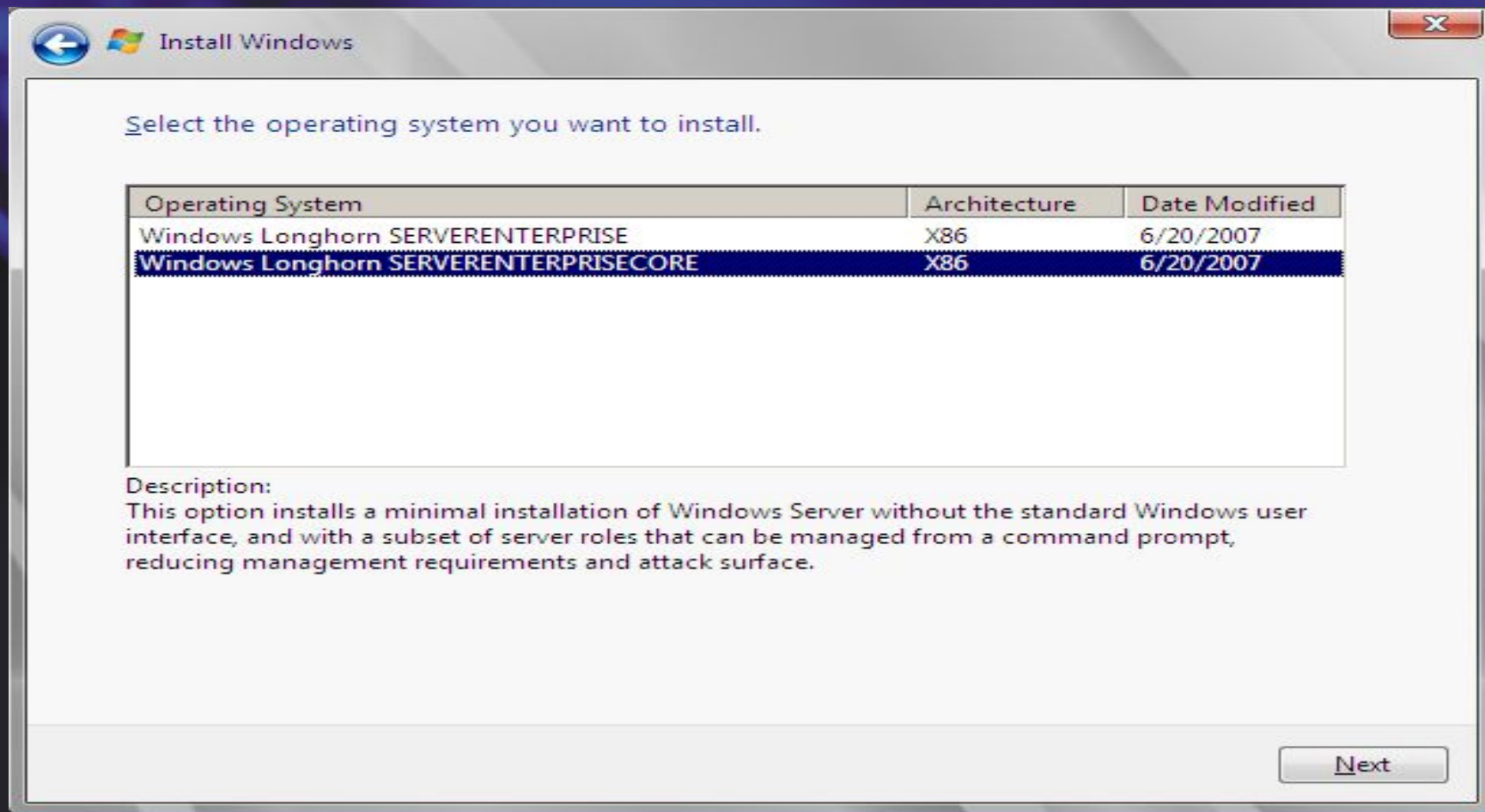
Можно:

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

Нельзя:

- Обновление с предыдущих версий Windows
- Конвертировать установку 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

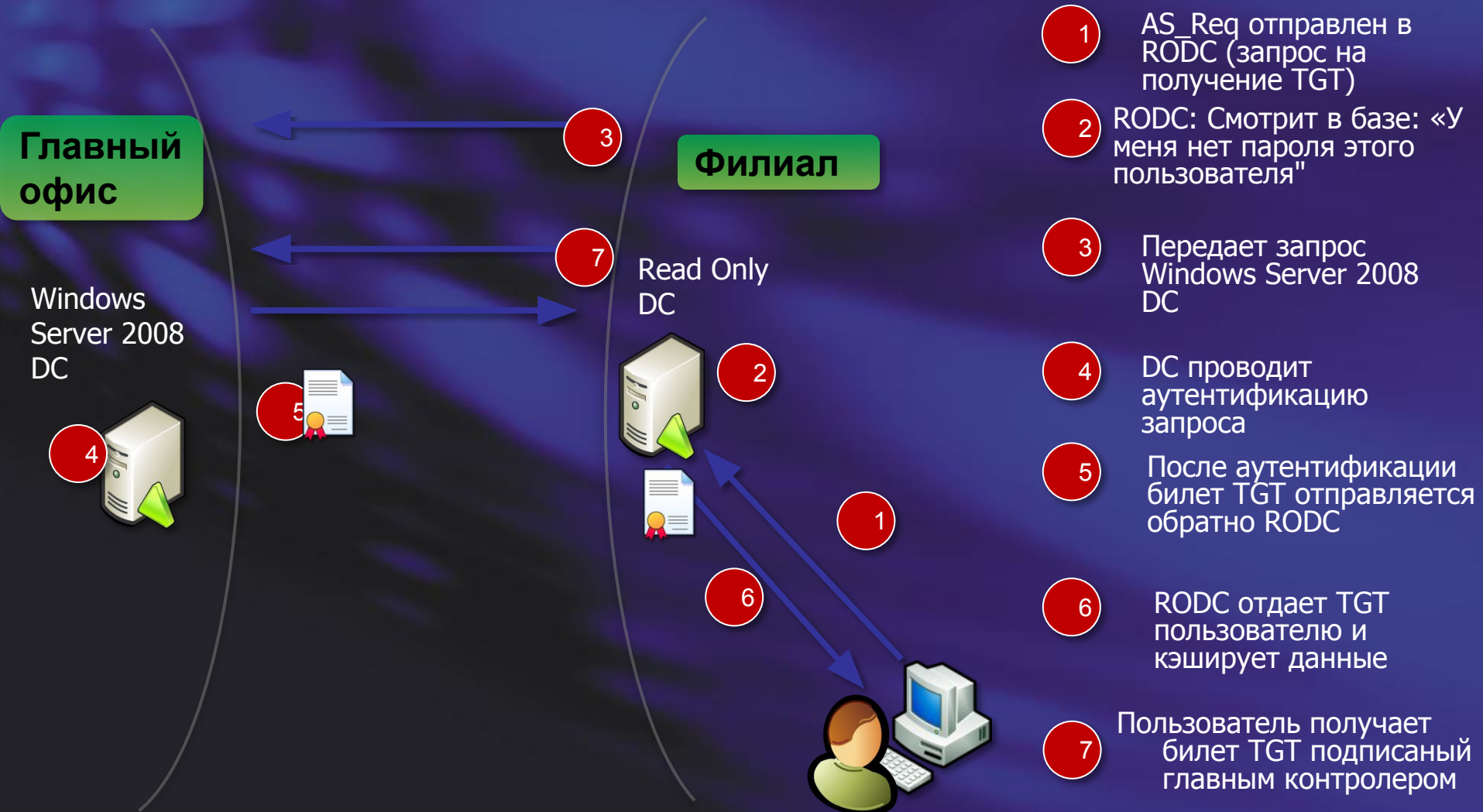
Данные авторизации и аутентификации

- 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

@stake LC5 - [Untitled1]

File View Session Schedule Remediate Help

Run Report

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



- 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:

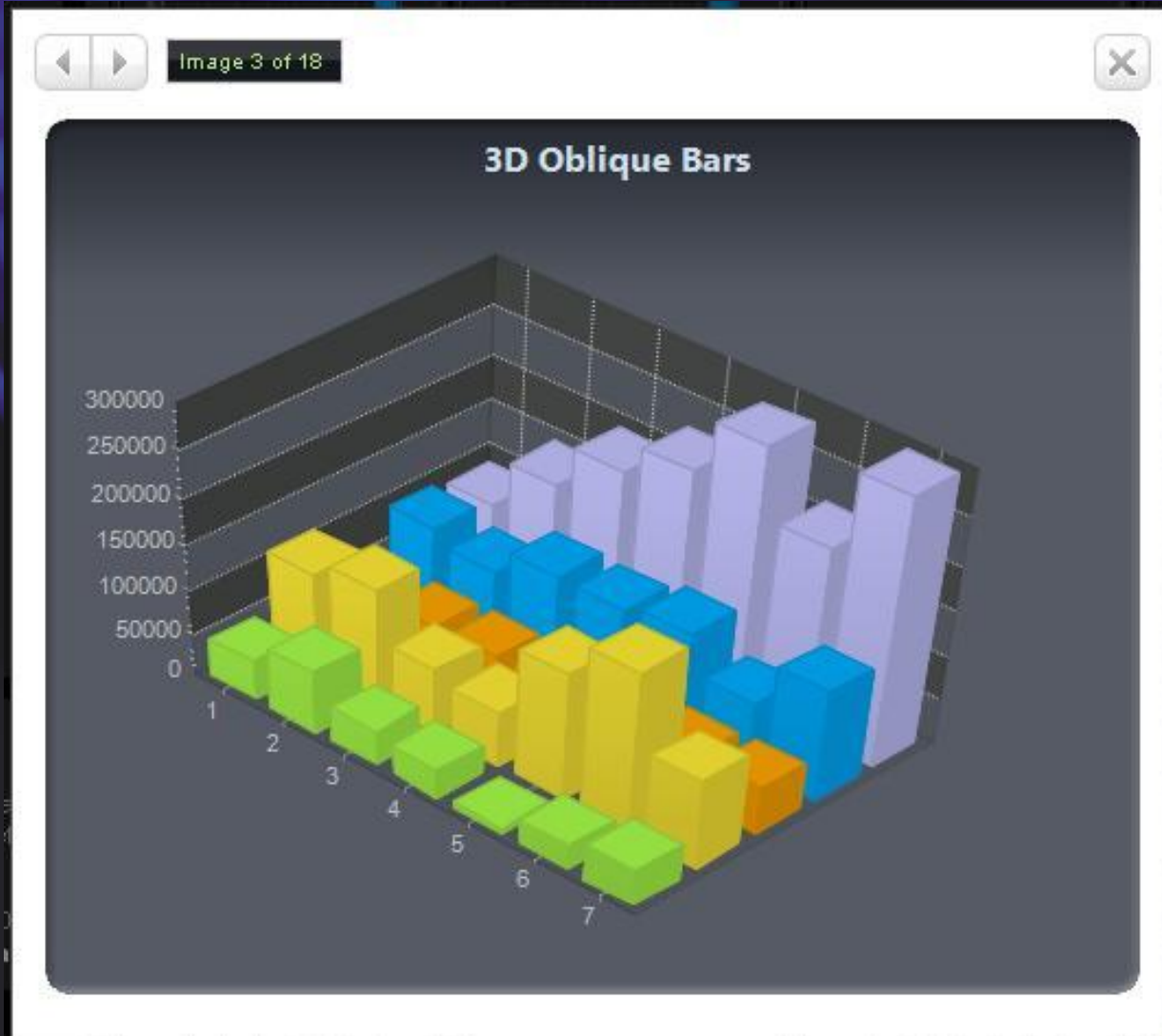
Windows PowerShell

Используется в следующих проектах:

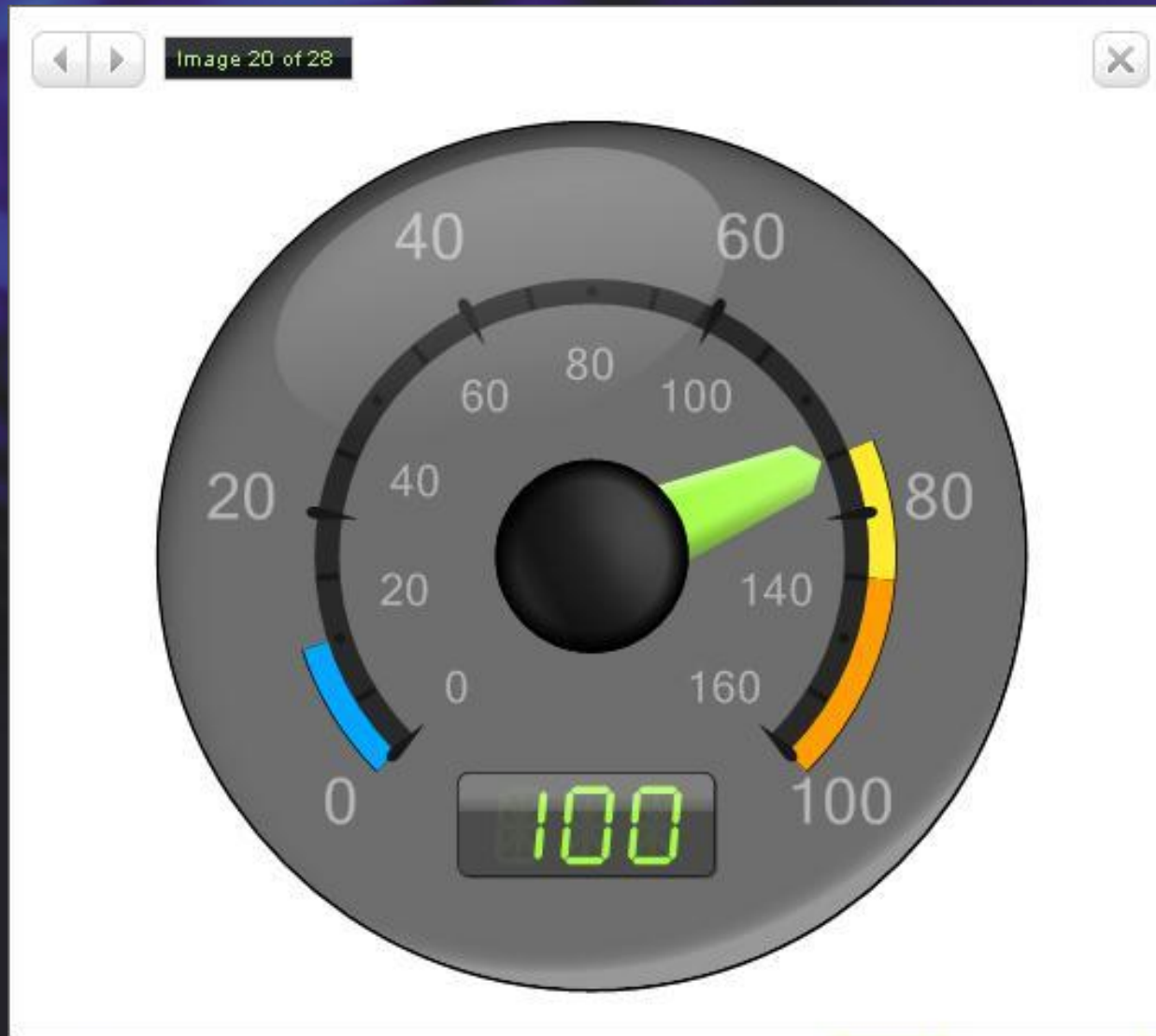
- Exchange 2007
- System Center Operations Manager 2007 (SCOM 2007)
- System Center Virtual Machine Manager 2007 (VMM)
- System Center Data Protection Manager 2007 (DPM)
- Microsoft Transporter Suite for Lotus Domino
- Windows Compute Cluster Tool Pack
- Windows Server 2008

Демонстрация Powershell

PowerShell + PowerGadgets



PowerShell + PowerGadgets



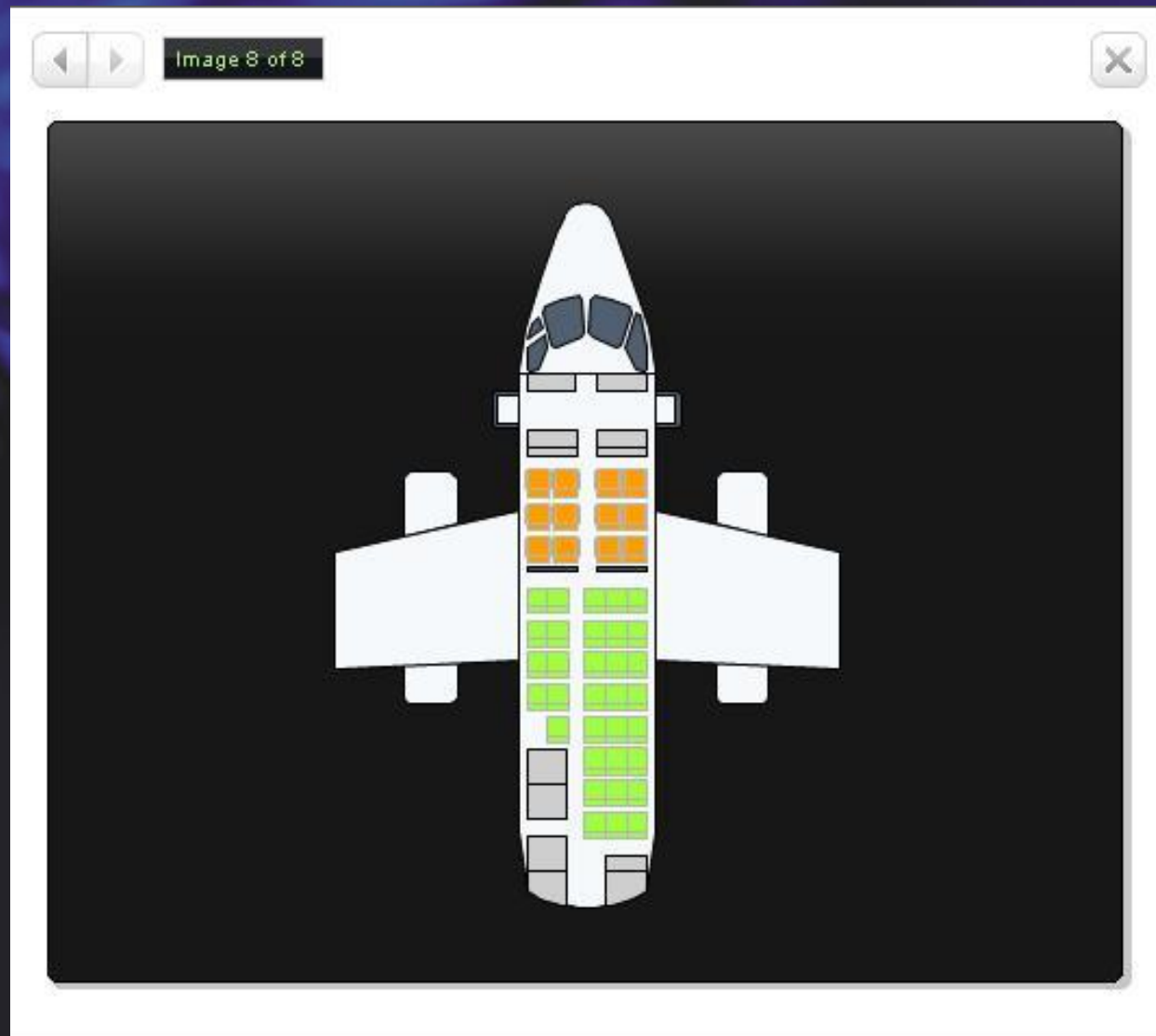
PowerShell + PowerGadgets



PowerShell + PowerGadgets



PowerShell + PowerGadgets



PowerShell + PowerGadgets



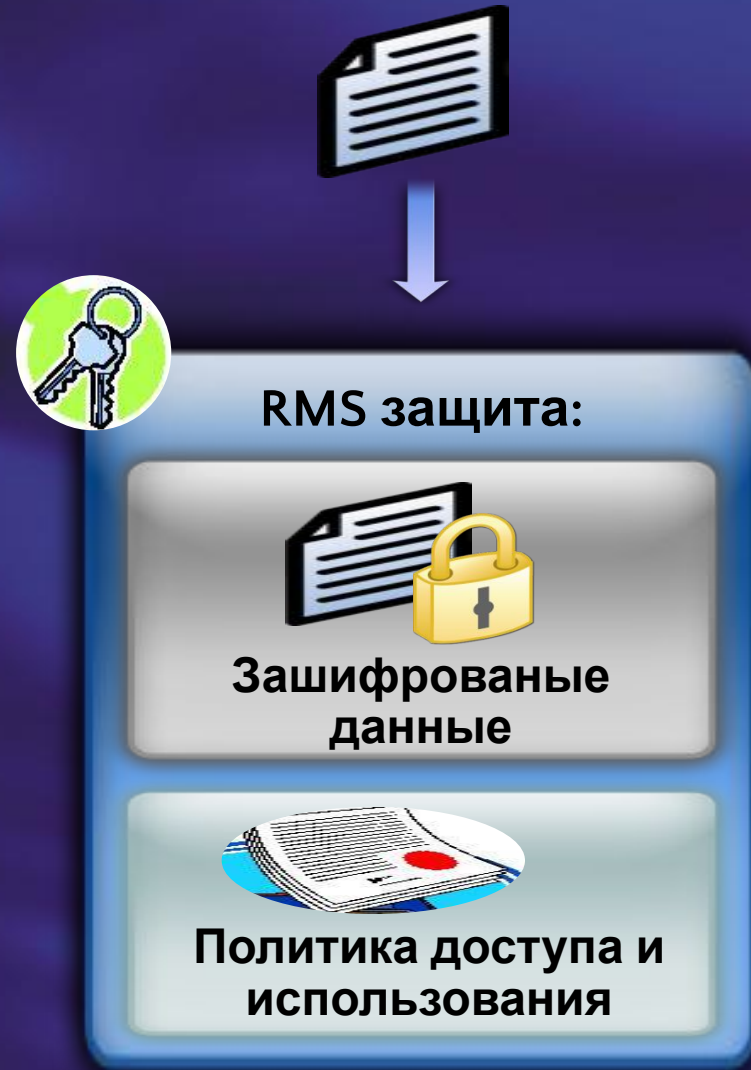
Цель Rights Management Service:

Дать возможность защитить важную информацию в течении жизненного цикла

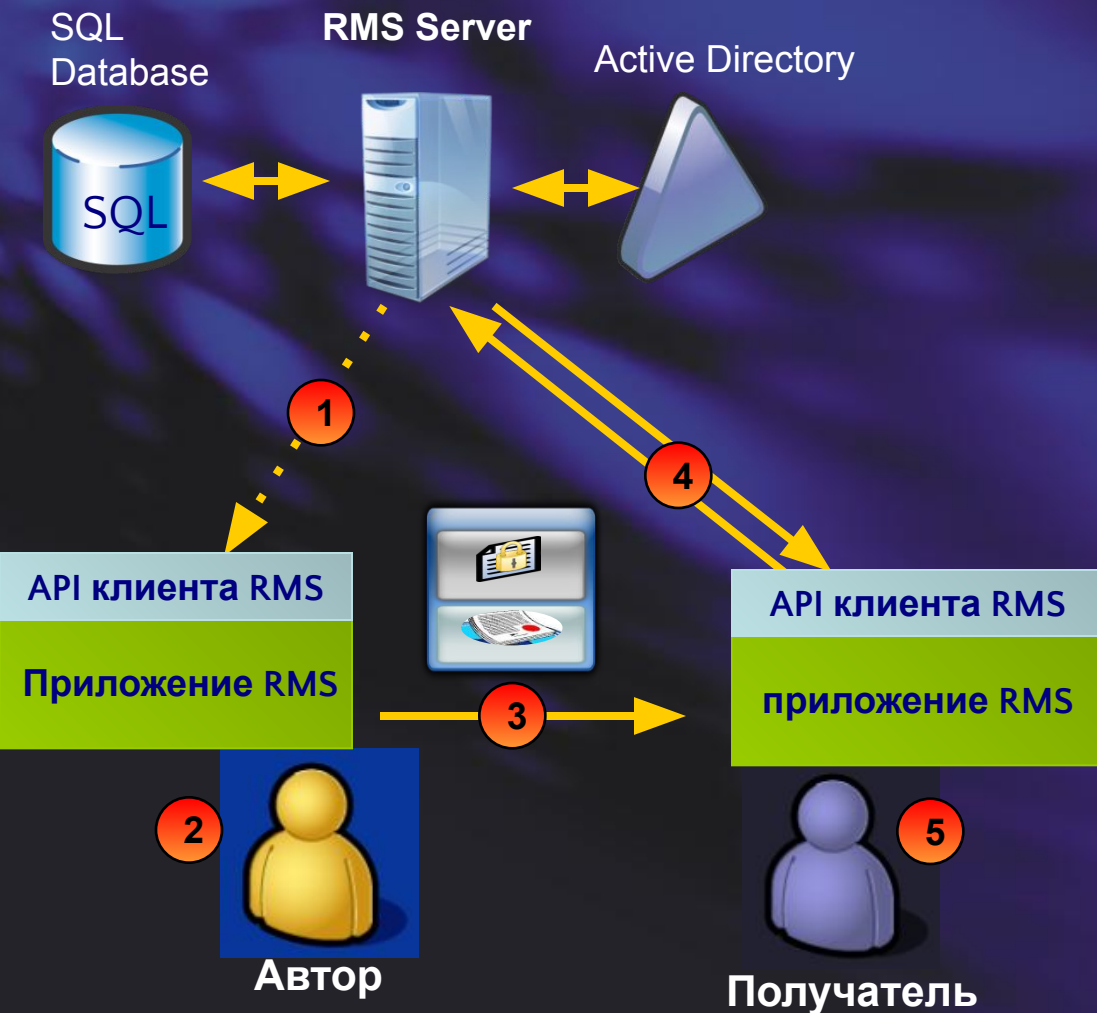
- Защита информации
 - Данные защищены во время хранения, передачи, обработки
 - Защита данных как внутри организации так и снаружи
- Соответствие организационным политикам
 - Постоянный контроль за тем кто, когда получает доступ к данным и что с ними делает
- Organizational
- Control
 - ИТ департамент 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

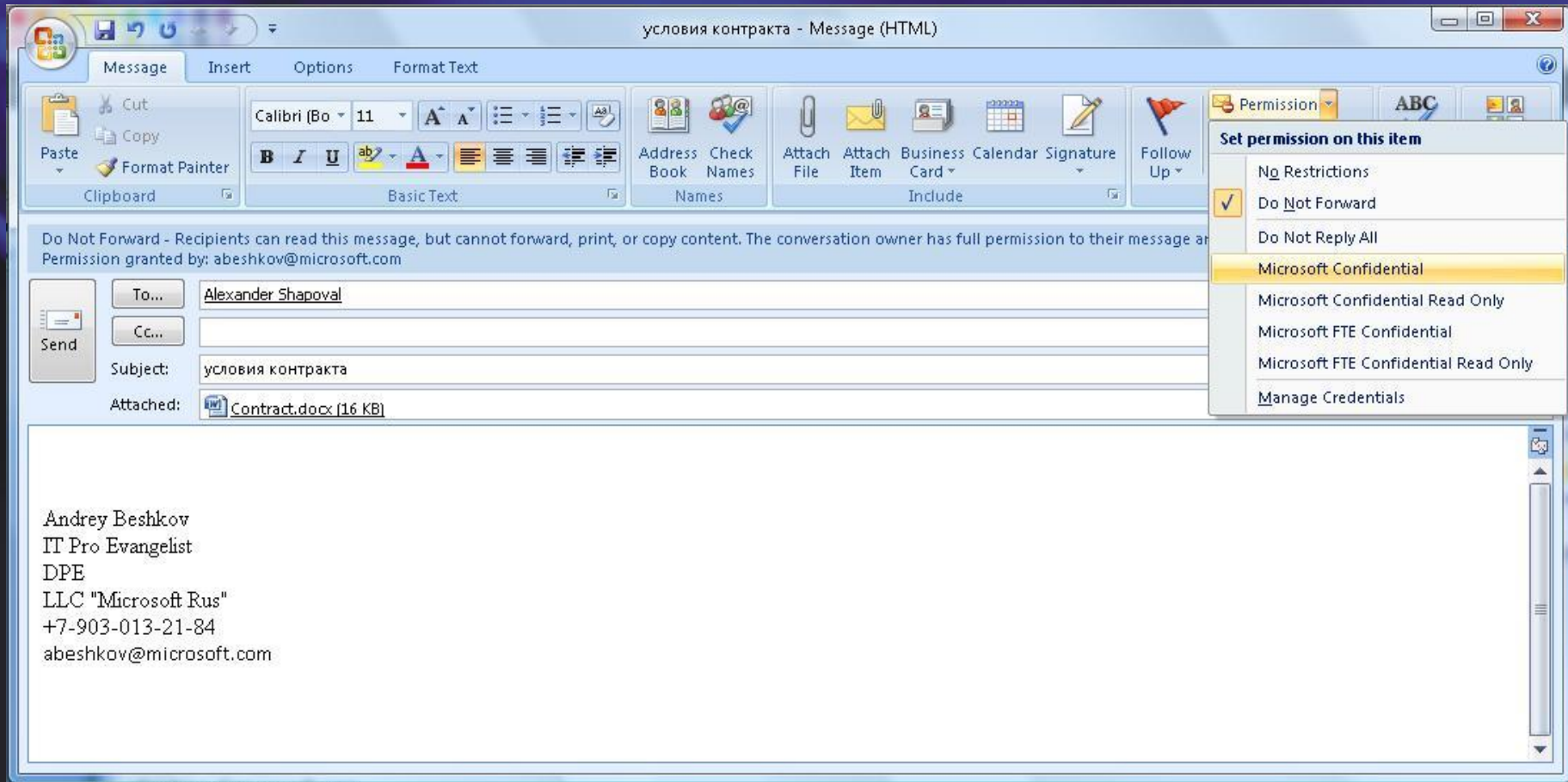


Пример работы RMS



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[®]

Your potential. Our passion.[™]