



IS-S 205: Обеспечение безопасной работы удаленных офисов и филиалов

Юрий Осипов
Microsoft

Содержание

- Для чего удаленный доступ компаниям?
- Сценарии удаленной работы
 - Доступ удаленных пользователей
 - Подключение удаленных офисов
- Продукты Microsoft
 - ISA Server 2006;
 - Intelligent Application Gateway 2007
 - Семейство Microsoft Forefront;
 - Windows Server 2008;

Три вопроса к аудитории

- Кто из вас участвовал в прошлогодней Платформе?
- Кто уже присутствовал на аналогичном докладе в прошлом году?
- У кого есть потребность (задача) обеспечения удаленного доступа к ресурсам компании?

Организация удаленного доступа

Цели и задачи

- Создание единой среды компании
 - Сбор, организация хранения и обеспечение сохранности электронных ресурсов
 - Стандартизация и унификация рабочих процессов в компании
- Обеспечение единых правил безопасности
 - защита от несанкционированного доступа и изменения данных
 - Обнаружение попыток вторжения
 - Контроль передаваемой информации
- Оптимизация издержек бизнеса
 - Управление объемом сетевого трафика

Конфиденциальная информация

- Персональные данные
- Коммерческая тайна
- Данные, составляющие тайну следствия и судопроизводства
- Служебная тайна
- Сведения связанные с профессиональностью, доступ к которым ограничен законом (нотариальная, адвокатская, врачебная тайна, тайна переписки, телефонных переговоров, телеграфных и почтовых отправок и т.д.)

Правовая составляющая

- **Федеральный закон Российской Федерации от 10 января 2002 г. N 1-ФЗ
Об электронной цифровой подписи**
 - **Федеральный закон Российской Федерации от 29 июля 2004 г. N 98-ФЗ
О коммерческой тайне**
 - **Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ
О персональных данных**
- и другие законодательные акты и постановления Правительства РФ, относящиеся к сфере деятельности компании**

Организация удаленного доступа

- Тип данных
- Куда?
 - Периметр
 - Внутренняя сеть
 - Приложения
- Каким образом?
 - Устройства
 - Приложения
 - Протоколы

Организация удаленного

доступа

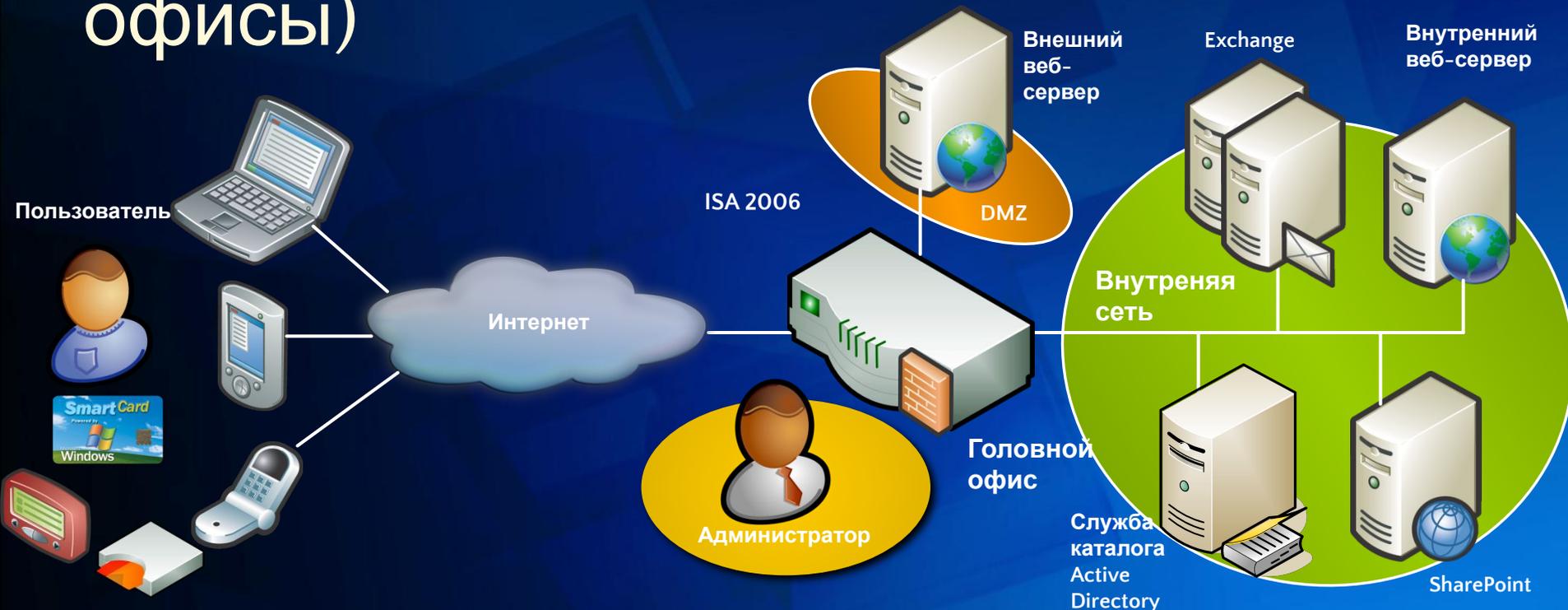
• Организация VPN

- Для создания VPN соединения пользователю и серверу необходимо подтвердить свою подлинность, чтобы исключить атаку типа "человек-в-середине".
- Публикация приложений
- Терминальная служба
- Мобильные технологии
 - Outlook Web Access
 - Outlook Mobile Access
 - RPC over HTTP
 - Active Sync

Но сначала...

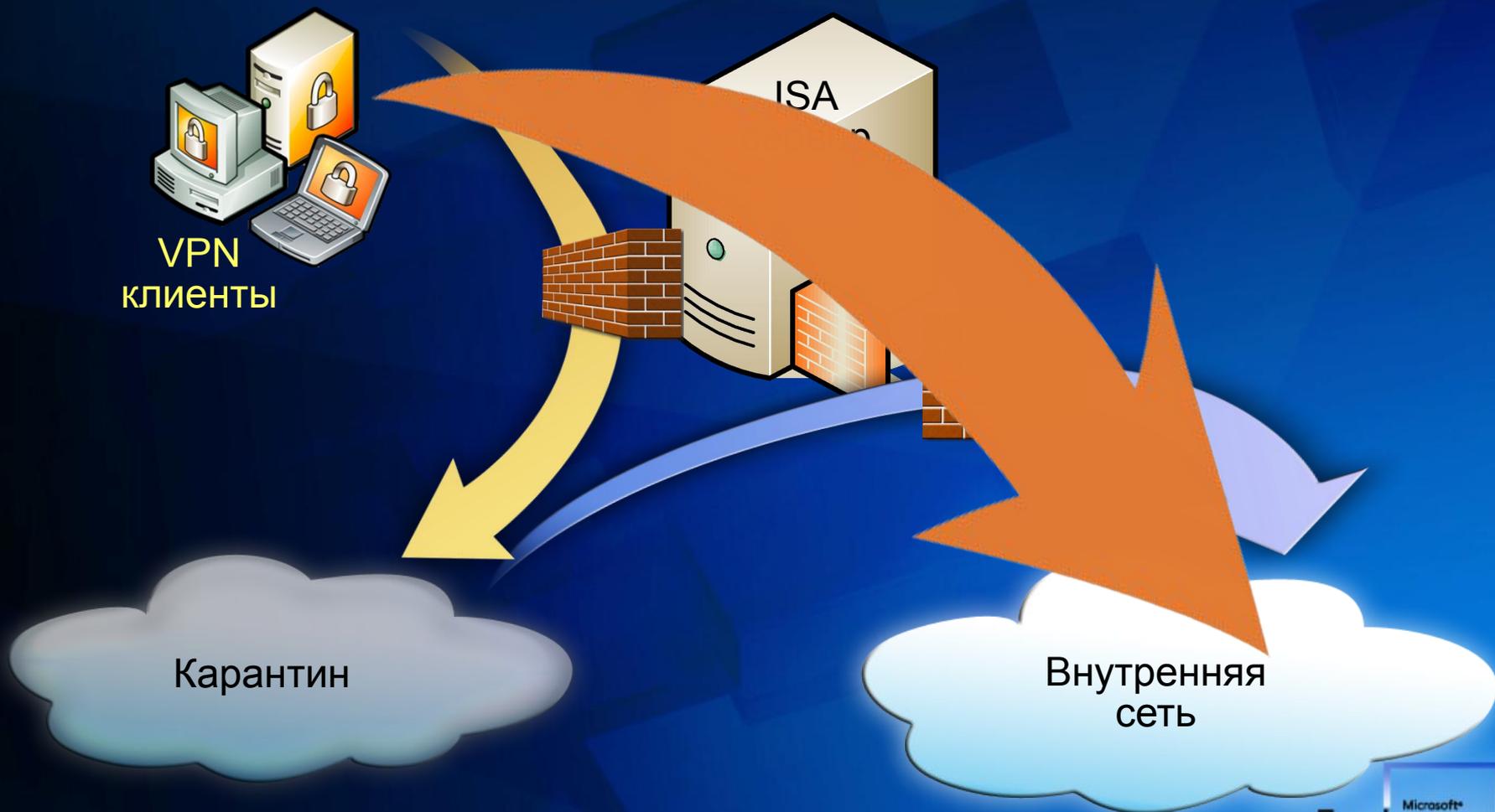
- ... надо определить защищаемые ресурсы...
- ...и организовать надежную аутентификацию пользователей
 - Многофакторную
 - Алгоритмами, гарантирующими заданную стойкость
 - и соответствующими требованиями законодательства

Доступ удаленных пользователей (мобильные пользователи, малые офисы)



Основной критерий для внедрения:
невозможность развернуть собственную инфраструктуру

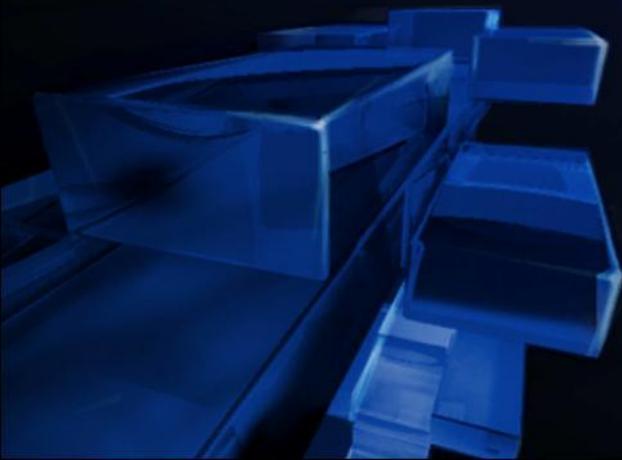
Карантин VPN





Доступ удаленных
пользователей

ДЕМОНСТРАЦИЯ



ISA Server 2006 и eToken NG-OTP для безопасности удалённого доступа

Строгая двухфакторная аутентификация
(по сертификату и закрытому ключу)



Клиент Microsoft Windows xp Интернет

Windows Mobile

Беспроводная сеть



Двухфакторная аутентификация
(по одноразовому паролю)

Сервер удаленного доступа, межсетевой экран, публикация приложений



Microsoft ISA Server 2006

Внутренняя сеть



Служба каталога Microsoft AD



Центр сертификации Microsoft CA



Сервер приложений

Сервер аутентификации RADIUS



Microsoft Internet Authentication Service (IAS)

Microsoft Windows Server 2003

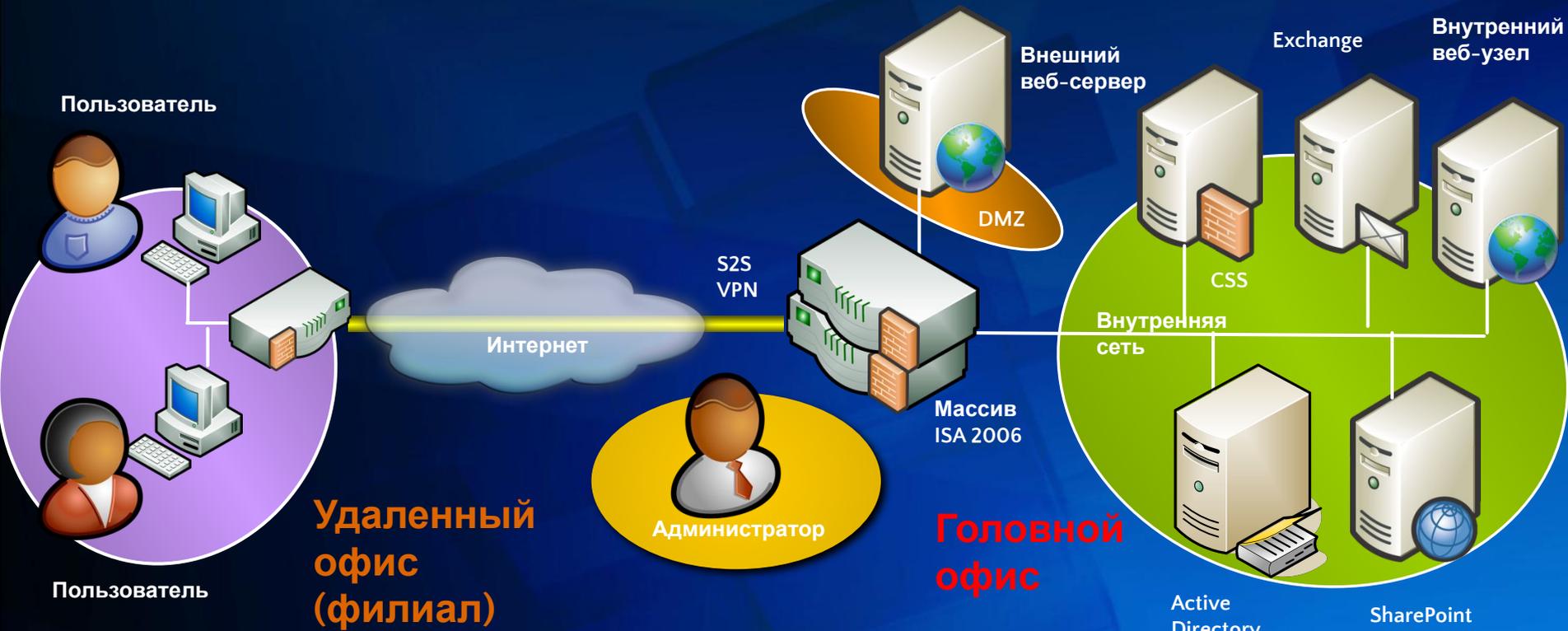
Список базовых продуктов и технологий

- Платформа – Microsoft Windows Server 2003 или Microsoft Windows Server 2008
 - Служба каталога Active Directory
 - Служба управления сертификатами
 - Служба аутентификации IAS
- Межсетевой экран – Microsoft ISA Server 2006
- Продукты третьих фирм (на примере Aladdin)
 - Носители – смарт-карты, токены, генераторы одноразовых паролей
 - Система управления жизненным циклом

Сертификат или одноразовый пароль?

- Сертификат
 - Требует наличия драйверов на устройстве
 - Обеспечивает прозрачную аутентификацию
 - Может быть использован для Single Sign On (SSO)
- Одноразовый пароль
 - Не требует установки драйверов и используется при доступе через любое устройство
 - Обеспечивает аутентификацию на периметре
 - Требует введения имени и пароля пользователя для доступа к ресурсам

Подключение удаленных офисов

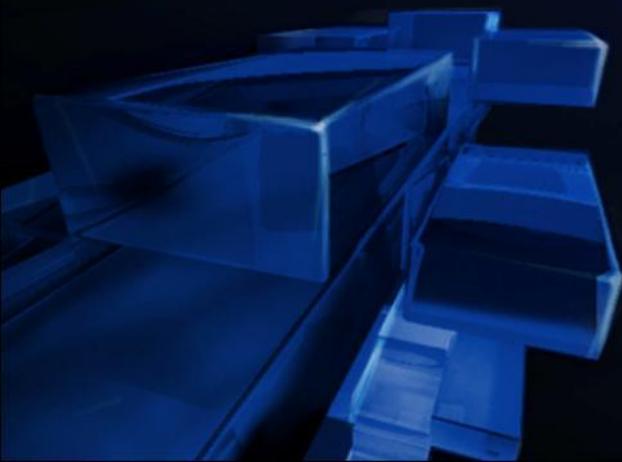


Основной критерий для внедрения:
возможность разворачивания собственной инфраструктуры



Подключение удаленных офисов

ДЕМОНСТРАЦИЯ



Windows Server 2008 в филиале

- Read-only Domain Controller
 - Возможность делегировать администрирование сервера локальным специалистам
 - Единые политики безопасности
 - Экономия внешнего трафика
- Network Access Protection (NAP)
 - Единые политики безопасности
- Сервисы безопасности
 - Rights Management Services (RMS)

Что ждет впереди?

- Новое поколение продуктов защиты периметра:
 - Новая версия ISA Server
 - Новая версия IAG

Дополнительная информация

ISA Server

- www.microsoft.com/rus/isaserver

Forefront

- www.microsoft.com/rus/forefront
- www.microsoft.com/rus/clientsecurity

Antigen

- www.microsoft.com/rus/antigen

Общая информация по безопасности

- www.microsoft.com/rus/security

Дополнительная информация о продуктах и технологиях Microsoft

- Портал TechNet:
 - <http://www.microsoft.com/rus/technet>
- Рассылка TechNet Flash:
 - http://www.microsoft.com/rus/technet/flash_register.aspx
- Интерактивные веб-трансляции:
 - http://www.microsoft.com/rus/technet/events_and_webcasts.aspx
- Форумы TechNet:
 - <http://www.microsoft.com/rus/forums>
- Блоги сотрудников Microsoft:
 - <http://www.microsoft.com/rus/blogs>
- Независимые сообщества ИТ-специалистов:
 - http://www.microsoft.com/rus/technet/community_overview.aspx



ВОПРОСЫ?

Юрий Осипов

Microsoft

i-yuryo@microsoft.com

Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

