Администрирование информационных систем

Механизмы обеспечения безопасности передачи данных

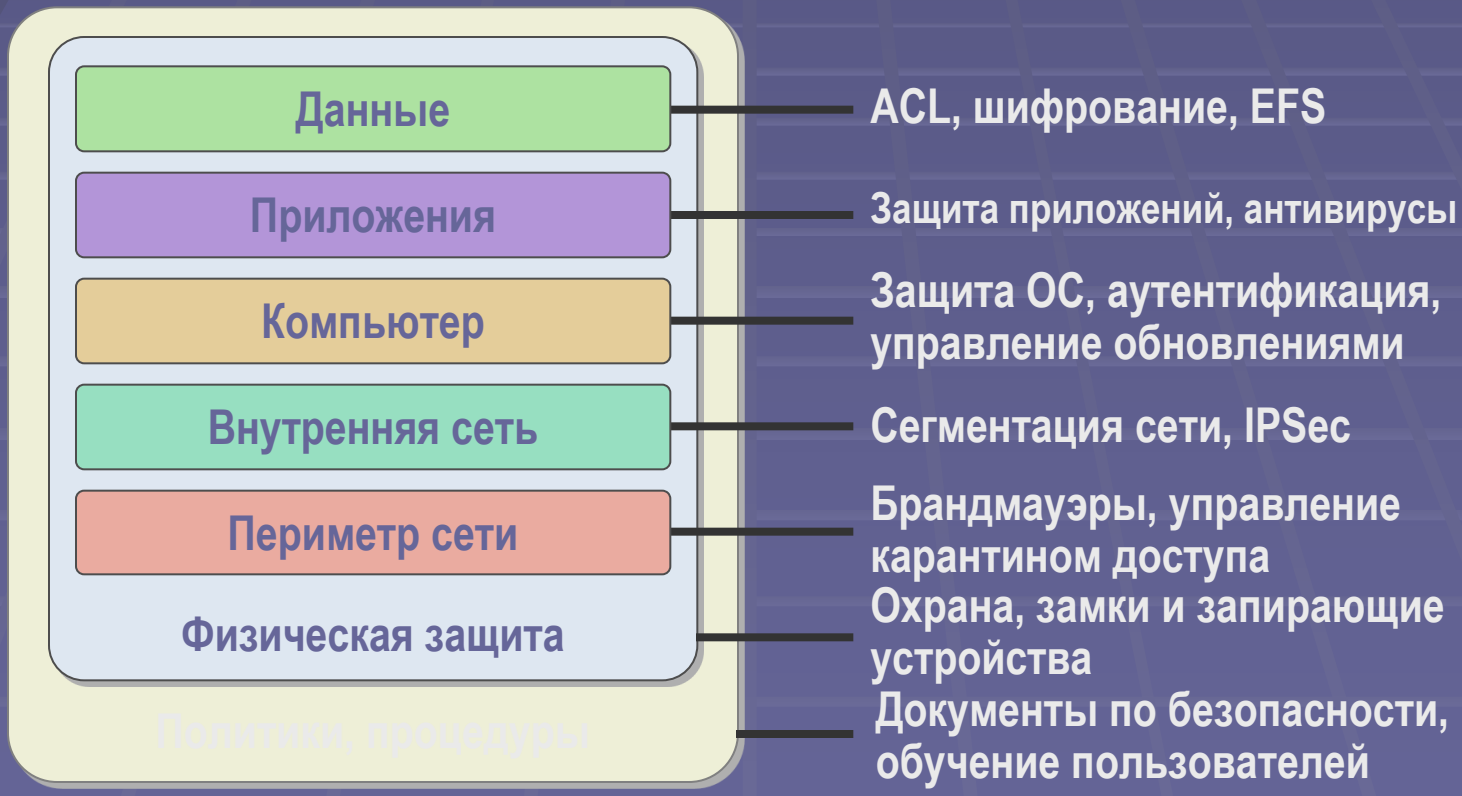
Цели обеспечения безопасности сети

	Защита периметра	Защита клиентов	Обнаружение вторжений	Контроль доступа к сети	Конфиден-циальность	Безопасность удаленного доступа
ISA Server	✔		✔	✔		✔
Windows Firewall		✔				
IPSec		✔			✔	✔
Network Access Quarantine				✔		✔

Модель многослойной защиты

Использование многослойной модели защиты позволяет:

- **Уменьшить шанс успеха атаки**
- **Увеличить вероятность обнаружения атаки**



Модель многослойной защиты

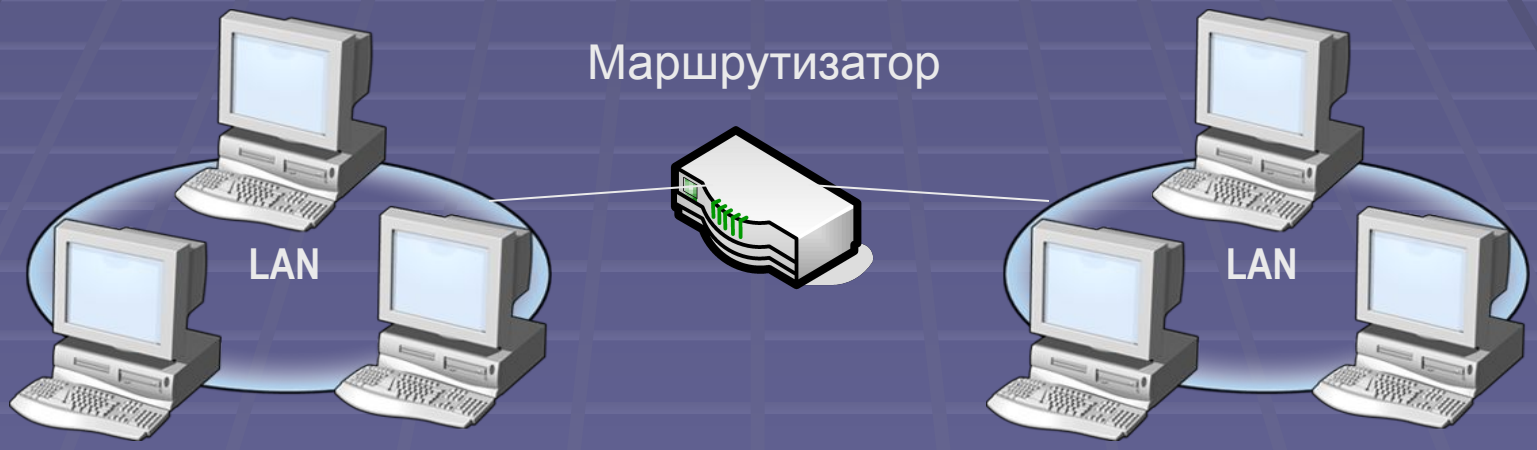
Использование многослойной модели защиты позволяет:

- **Уменьшить шанс успеха атаки**
- **Увеличить вероятность обнаружения атаки**

Сегментация сети

- Одним из средств защиты передачи данных является механизм сегментации сети (деление на подсети).
- Механизм разделения общей сети на отдельные подсети предприятия позволяет скрывать детали отдельных подсетей, обеспечивает возможность контроля трафика на границе подсети.

Сегментация сети



Отдельные сегменты сети

Сегментация сети

- Для обеспечения разделения внутренней сети организации на отдельные сегменты возможно использование аппаратных (коммутаторы) и программно-аппаратных (маршрутизаторы) решений.
- Серверная платформа Windows 2000/2003 позволяет создание эффективного маршрутизатора с возможностями усиления безопасности на границах сетей. Инструментом является служба **Удаленный доступ и маршрутизация (RRAS)**.

Служба Маршрутизация и удаленный доступ

- Служба **Маршрутизация и удаленный доступ** (Routing and Remote Access, RRAS) в Windows 2003 представляет собой программный многопротокольный маршрутизатор, который может быть объединен с другими функциями ОС, такими как учетные записи и групповые политики.
- Служба поддерживает маршрутизацию между различными ЛВС, между ЛВС и WAN-каналами, VPN- и NAT- маршрутизацию в IP-сетях.

Особенности Службы маршрутизации и удаленного доступа

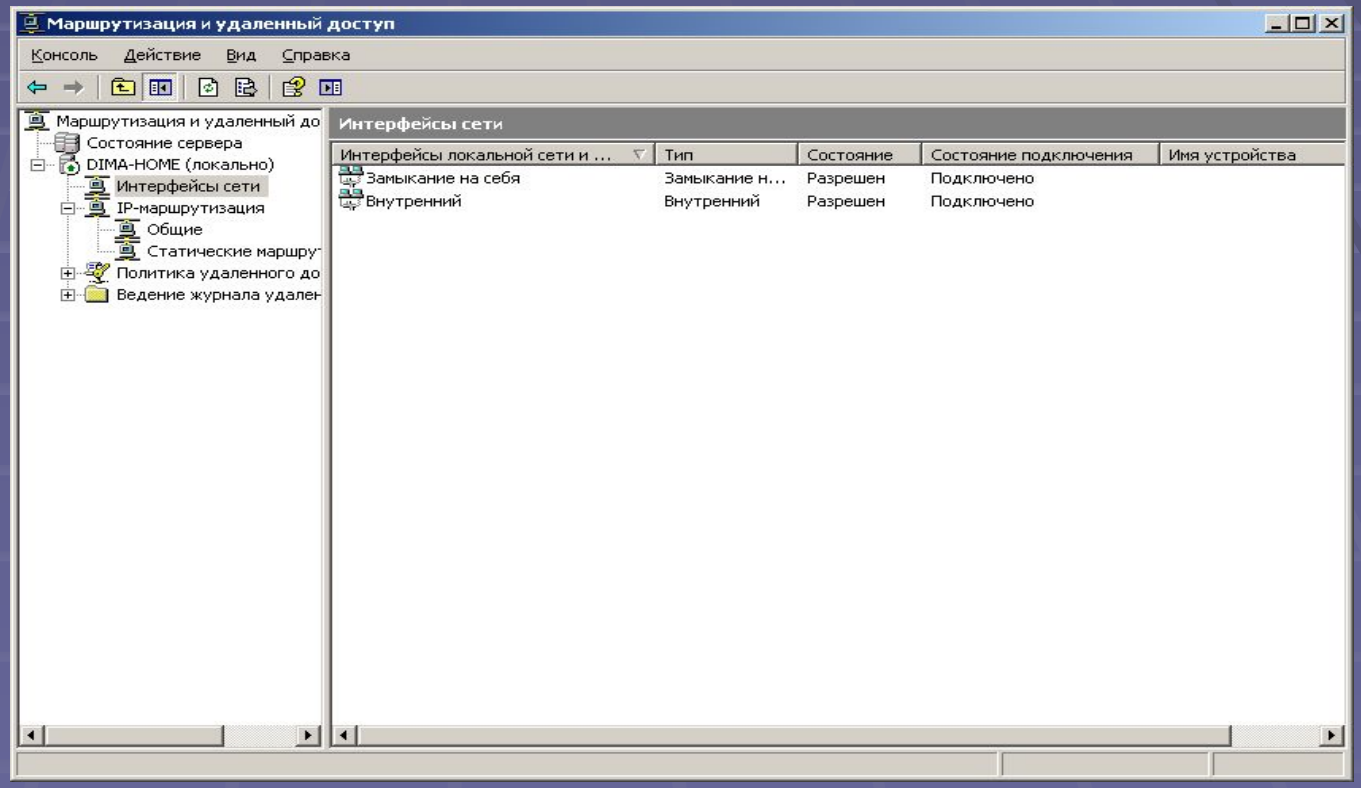
- Кроме того, служба может быть сконфигурирована для особого вида маршрутизации:
  - Многоадресные ip-рассылки;
  - Маршрутизация вызовов по требованию;
  - Ретрансляция DHCP;
  - Фильтрация пакетов
- В службу включена поддержка протоколов динамической маршрутизации – RIP (routing information protocol) и OSPF (open shortest path first).

Запуск службы Маршрутизация и удаленный доступ

- При установки Windows server 2003 служба Маршрутизация и удаленный доступ отключена.
- Ее активация выполняется с помощью Мастера настройки сервера маршрутизации и удаленного доступа.
- Если сервер маршрутизации является рядовым членом домена Active Directory, то он должен быть включен в группу Серверы RAS и IAS.
- Контроллеры домена в дополнительной настройке не нуждаются.

Консоль управления Маршрутизация и удаленный доступ

- Консоль управления Маршрутизация и удаленный доступ представляет собой стандартную оснастку консоли управления в Windows. В конфигурации по умолчанию поддерживается маршрутизация в ЛВС.

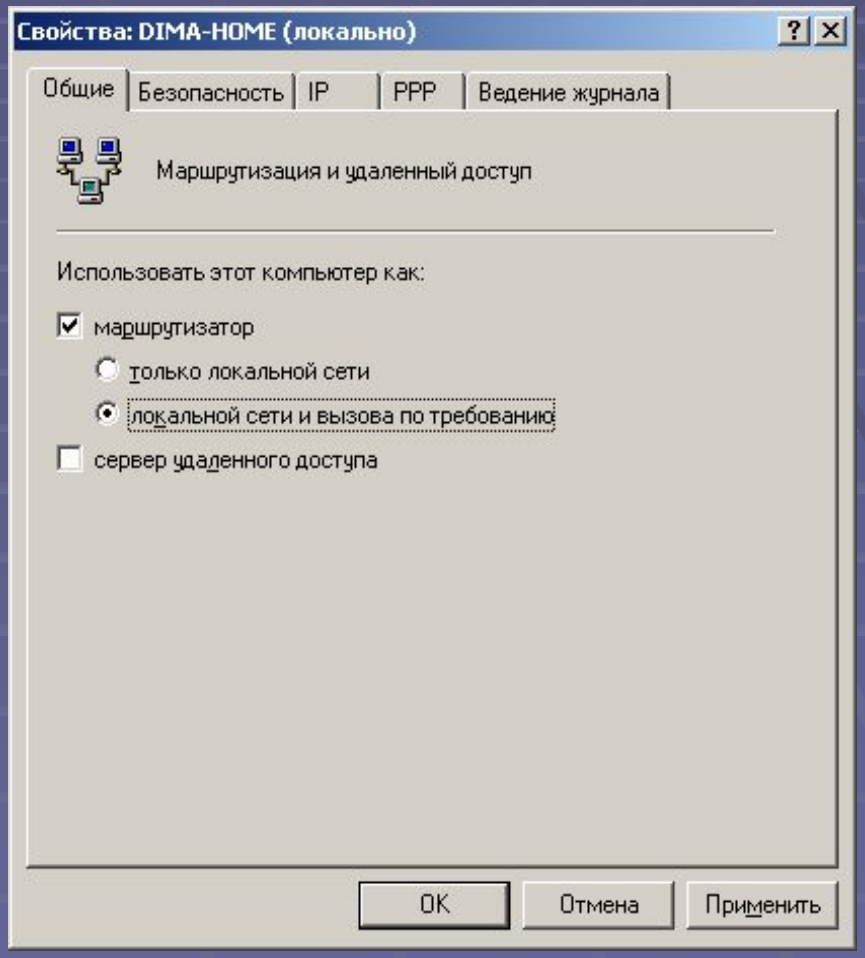


Создание интерфейсов

- Сетевой интерфейс в консоли управления – программный компонент, подключаемый к физическому устройству (модему или сетевой плате).
- В процессе настройки необходимо, чтобы все интерфейсы, через которые необходимо маршрутизировать трафик присутствовали в консоли управления.
- Если необходимо сконфигурировать маршрутизацию через подключение по требованию или постоянное подключение по коммутируемой линии, VPN или PPOE-подключение (Point-to-Point Protocol over Ethernet), необходимо выполнить конфигурирование интерфейсов в ручную.

Создание интерфейсов по вызову

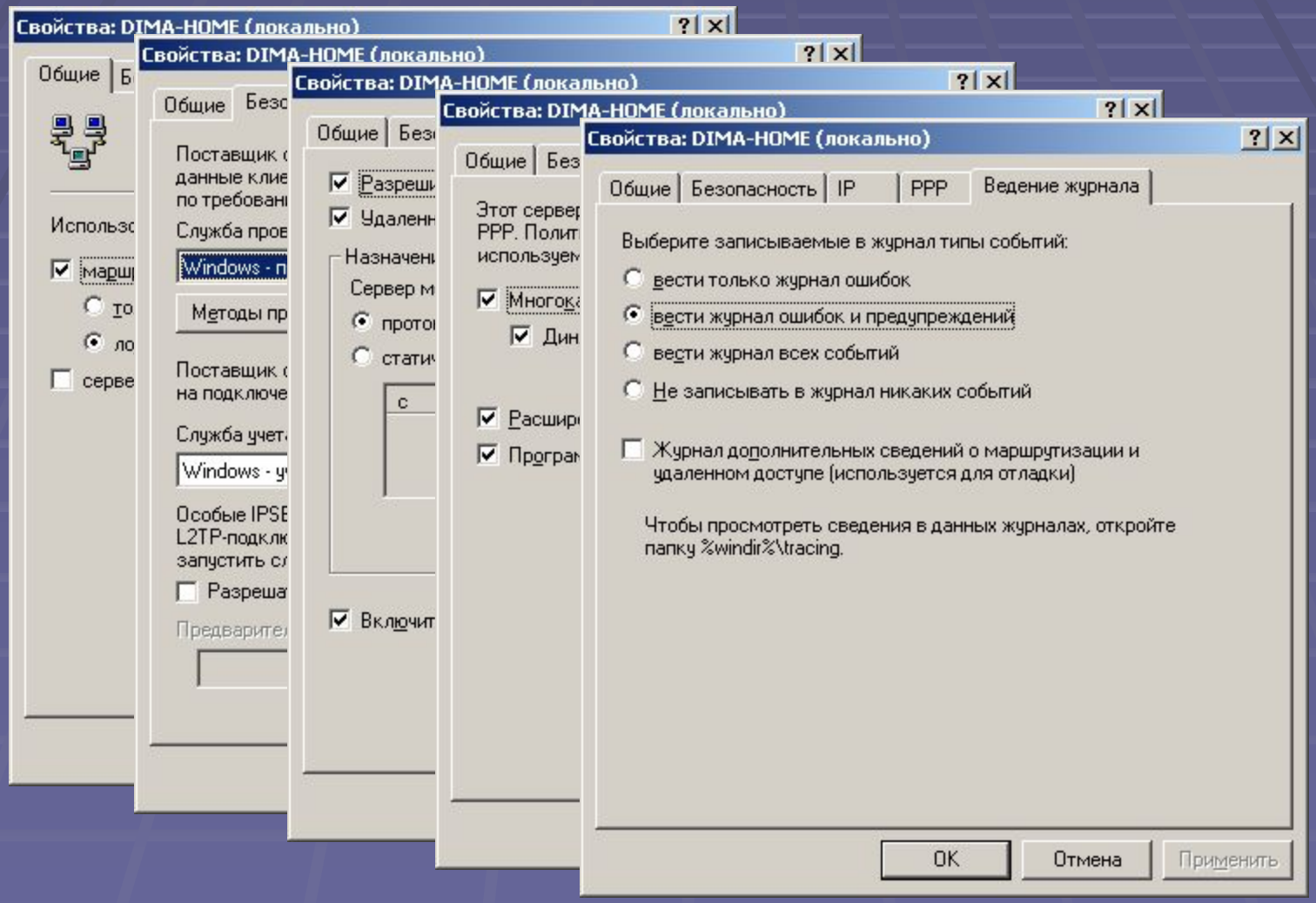
- Для создания интерфейса по вызову, необходимо включить такую возможность в Свойствах сервера маршрутизации.
- Для создания подключения используется Мастер интерфейса по требованию



IP - маршрутизация

- Узел ip – маршрутизация используется дла настройки основных параметров по протоколу IP.
- По умолчанию содержится три подузла:
  - Общие
  - Статические маршруты
  - NAT / простой брандмауэр

Настройка параметров службы маршрутизации и удаленного доступа



Управление таблицей маршрутизации

- Мрашрутизаторы считывают адреса назначения пакетов и переправляют пакеты в соответствии с информацией, хранящейся в таблицах маршрутизации.
- Отдельные записи таблицы маршрутизации называются маршрутами.
- Существуют три типа маршрута:
  - Маршрут узла – определяет ссылку на определенный узел или широковещательный адрес. Маска маршрута – 255.255.255.255;
  - Маршрут сети – определяет маршрут к определенной сети, а соответствующее поле в таблицах маршрутизации может содержать произвольную маску;
  - Маршрут по умолчанию – один маршрут, по которому отправляются все пакеты, чей адрес не совпадает ни с одним адресов таблицы маршрутизации.
- Просмотр таблицы маршрутизации может быть выполнен с помощью команд
  - **route print**
  - **netstat -r**

Защита периметра сети

- Защита периметра сети предусматривает создание условий препятствующих проникновению постороннего трафика из внешней сети во внутреннюю сеть организации (и возможно ограничение трафика из внутренней сети во внешнюю).
- Одним из средств защиты является использование брандмауэров.

Функции сетевых брандмауэров

- Фильтрация пакетов
- Проверка установки соединений
- Проверка трафика на уровне приложений

Защита клиентов

Метод	Описание
Прокси-функции	**Обработка всех запросов клиентов и запрет прямых соединений**
Поддержка клиентов	**Возможность поддержки подключений клиентов без специального ПО. Использование специального ПО (ISA Firewall) обеспечивает дополнительную функциональность**
Правила	**Доступ к веб-ресурсам может быть ограничен на основе имени пользователя, IP-адреса клиента, URL сервера или по расписанию**
Add-ons	**Дополнительные компоненты обеспечвают расширение функциональности брандмауэра и возможность использования решений третих фирм**

Защита веб-серверов

- Правила веб-публикаций
  - Защита веб-серверов, находящихся позади брандмауэра предотвращает внешние атаки на сервера путем проверки HTTP входящего трафика
- Проверка Secure Socket Layer (SSL) трафика
  - Расшифровка и проверка входящего зашифрованного веб-трафика на предмет соответствия заданным правилам и стандартам
  - Возможна перешифровка трафика перед пересылкой на веб-сервер

HTTP фильтрация

- Интернет приложения используют HTTP для туннелирования трафика приложений
- ISA Server 2004 включает HTTP фильтры для:
  - Обеспечения контроля за всем HTTP трафиком
  - Обеспечения URLScan функциональности по периметру сети организации
  - Возможность объединения с URLScan внутренних веб-серверов для обеспечения согласования разрешенного трафика
- HTTP фильтры могут обеспечить фильтрацию:
  - На основе анализа HTTP запросов, ответов, заголовков и содержания контента
  - На основе расширений файлов, методов передачи и цифровых подписей