Настройка безопасности сети с помощью IPSec

Лаштанов И.Г.

Знакомство с протоколом IPSec

С развитием Интернета и интрасетей увеличилась потребность в защите информации.

Основные проблемы — это зашита сетевого трафика от:

• изменения данных в пути;

• перехвата, просмотра или копирова-шя данных;

• несанкционированного доступа.

IPSec — структура открытых стандартов для обеспечения частной защищенной связи по IP-сетям с помощью криптографических служб безопасности. Реализация IPSec в Microsoft Windows 2000 основана на стандартах, разработанных рабочей группой Internet Engineering Task Force **(IETF)** IPSec. IPSec выполняет две задачи:

1. зашищает пакеты протокола IP;

2. обеспечивает 1ащиту от сетевых атак.

Протокол IPSec

Обе задачи выполняются с помощью основанных на криптографии служб, протоколов безопасности и динамического управления ключами. Такой метод является достаточно мощным и гибким, чтобы обезопасить связь между компьютерами в частной сети, между удаленными узлами, соединенными через Интернет, а также между удаленными клиентами. IPSec также используют для фильтрования пакетов данных в сети.

IPSec основан на сквозной модели защиты. Это означает, что поддержка IPSec требуется лишь на принимающем и передающем компьютерах. Каждый из них управляет защитой со своей стороны, предполагая, что среда передачи данных небезопасна. Маршрутизаторы, переправляющие пакеты между источником и адресатом, для поддержки IPSec не требуются. Подобная модель позволяет успешно развернуть IPSec в имеющейся сети предприятия:

- ЛВС: клиент-сервер, одноранговая сеть;
- ГВС: маршрутизатор-маршрутизатор;
- удаленный доступ: удаленные клиенты и доступ из частных сетей через Интернет.

Преимущества IPSec

В Windows 2000 протокол IPSec реализован прозрачно для пользователя. Для связи с применением протокола IPSec от пользователей не требуется подключение к одному домену. Они могут находиться в любом из доверенных доменов сети предприятия. Утилита IPSec Management позволяет централизовать администрирование. Администраторы домена создают для обычных сценариев связи политику зашиты. Эта политика, привязанная к политике домена, хранится в службе каталогов.

При регистрации в домене каждый компьютер автоматически загружает его политику защиты, что устраняет необходимость в настройке отдельных систем.

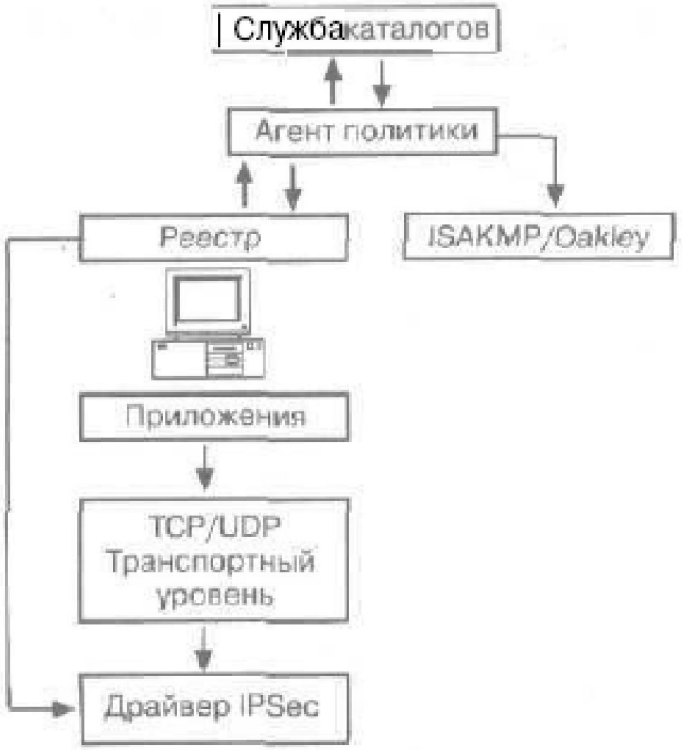
Преимущества IPSec

Протокол Windows 2000 IPSec обеспечивает следующие преимущества, позволяющие достичь высокого уровня безопасности связи при низкой цене использования:

- централизованное администрирование политики зашиты;
- прозрачность IPSec для пользователей и приложений;
- гибкость в настройке политики зашиты, что отвечает потребностям разных предприятий;
- наличие служб конфиденциальности, предотвращающих неавторизированный доступ к передаваемым по сети секретным данным;
- наличие служб аутентификации, проверяющих подлинность отправителя и получателя, что позволяет предотвратить использование подложных идентификационных сведений;
- . шифрование каждого пакета с использованием информации о времени, что пошоляет предотвратить перехват и последующую передачу данных (атаку повтора);
- высокая стойкость ключей и их динамическая смена в процессе коммуникаций позволяют защититься от атак;
- безопасные сквозные каналы для пользователей частной сети в пределах одного домена или любого доверенного домена сети предприятия;
- безопасные сквозные каналы, основанные на IP-адресе, между удаленными пользователями и пользователями в любом домене предприятия.

Работа протокола IPSec

- Пакет IP сравнивается с IP-фильтром, являющимся частью политики IPSec.
- Политика IPSec может включать несколько дополнительных методов зашиты. Драйверу IPSec требуется знать, какой метод использовать для защиты пакета. Для согласования метода и ключа защиты драйвер IPSec опрашивает Internet Security Association and Key Management Protocol (ISAKMP).
- ISAKMP определяет метод зашиты и передает его вместе с ключом защиты драйверу IPSec.
- Метод и ключ становятся *сопоставлением безопасности* (security association. SA) IPSec. Драйвер IPSec сохраняет это SA в с носи базе данных.
- Обоим сообщающимся компьютерам требуется шифровать или расшифровывать трафик IP, поэтому им необходимо знать и хранить SA.



Архитектура IPSec

Протокол IPSec реализован в Windows 2000 с использованием следующих компонентен:

- агента **политики** IPSec;
- службы ISAKMP/Oakley Key Management;
- драйвера IPSec;
- модели IPSec.

Когда следует использовать IPSec

Протокол IPSec шифрует исходящие пакеты, и это сказывается на производительности компьютеров. IPSec осуществляет симметричное шифрование сетевых данных, что очень эффективно. Тем не менее для серверов, поддерживаюших множество параллельных сетевых подключений, издержки на шифрование весьма существенны, и поэтому перед внедрением IPSec проверьте, как сервер справится е шифрованием информации, сымитировав сетевой трафик. Кроме того, если для IP-безопасности вы используете аппаратные средства и программные продукты сторонних фирм, не поленитесь провести предварительное тестирование. Для каждого домена можно определить собственную политику IPSec.

Внедрение IPSec

Политику IPSec по умолчанию можно просмотреть в оснастке Group Policy (Групповая политика). Политики отображаются и узле IP Security Policies, который расположен в подузле Computer Configuration\ Windows Settings\Security Settings\IP Security Policies (Конфигурация компьютера\Конфигурация Windows\ Пара метры безопасности\Политики безопасности IP).

Кроме того, для просмотра лолитики IPSec можно воспользоваться оснасткой IP Security Policy Management (Управление политикой безопасности IP). Каждая политика IPSec основывается на правилах, определяющих порядок ее применения. Щелкните значок политики правой кнопкой мыши и в контекстном меню выберите команду Properties. На вкладке Rules (Правила) перечислены правила политики. Правила можно разделить на списки фильтров, действия фильтров и дополнительные свойства. Оснастка по умолчанию запускается из меню Administrative Tools и позволяет конфигурировать политику только для локального компьютера. Для централизованного управления политиками нескольких компьютеров добавьте в консоль оснастку IP Security Management.

Настройка политики IPSec

Политики по умолчанию не изменяются независимо от того, является ли полигика IPSec локальной или хранится n Active Directory как часть политики группы. В этом примере политика IPSec является локальной политикой рядового сервера.

- Политика Client (Respond Only) допускает связь без шифрования данных, но отвечает на запросы IPSec и не отвергает попытки согласовать параметры безопасности. Для аутентификации используется протокол Kerberos V5.
- Политика Server (Request Security) заставляет сервер каждый раз устанавливать защищенную связь. Если сданным компьютером связь пытается установить клиент, не поддерживающий IPSec. сеанс будет разрешен.
- Политика Secure Server (Require Security) требует доверительных отношений Kerteros для всех IP-пакетов, посланных с этого компьютера, за исключением широковещательных и многоадресных пакетов, а также пакетов протокола Resource Reserviition Setup Protocol (RSVP) и службы ISAKMP. Данная политика не позволяет устанавливать незащищенную связь с клиентами. В итоге все клиенты, подключающиеся к серверу с политикой IPSec, должны поддерживать IPSec.

Чтобы отредактировать политику, щелкните ее значок правой кнопкой и в контекстном меню выберите команду Properties.

Типы подключений

Вкладка Connection Type (Тип подключения) доступна в диалоговом окне Edit Rule Properties (Свойства: Изменить правило) (рис. 5-6). Кроме того, она отображается в мастере создания правила.

Выбор типа подключения для отдельных правил определяет, на какие подключения (через сетевые адаптеры или модемы) распространяется политика IPSec. У каждого правила есть свойство подключения, указывающее, применяется ли правило к ЛВС-подключениям, удаленным подключениям или всем сетевым подключениям.

Фильтрование пакетов IP

IPSec распространяется на принимаемые и передаваемые пакеты. Исходящие пакеты проверяются на соответствие заданным фильтрам и по результатам сравнения шифруются, блокируются или передаются открытым текстом. Входящие пакеты также проверяются на соответствие фильтрам, и по результатам сравнения производится обмен параметрами безопасности, пакет блокируется или пропускается в систему.

Отдельные фильтры группируются в список, что позволяет группировать и управлять сложными шаблонами трафика как единым именованным списком фильтров, например, «Файловые серверы здания *1»* или «Блокируемый трафик». Списки фильтров при необходимости могут совместно использовать разные правила IPSec одной или разных политик IPSec. Спецификации фильтров устанавливаются отдельно для входящего и исходящего трафика.

- Фильтры входа, распространяющиеся на входящий трафик, позволяют получателю сравнивать трафик со списком фильтров IP. отвечать на запросы об установлении защищенной связи, а также сравнивать трафик с имеющимся соглашением безопасности и расшифровывать защищенные пакеты.
- Фильтры выхода, применяемые к исходящему трафику, вызывают согласование параметров защиты, необходимое для отсылки трафика.

Работа фильтра

Действие фильтра определяет, что предпринимает система защиты при срабатывании фильтра: следует ли блокировать или разрешить трафик или согласовать параметры безопасности для данного подключения. Согласование включает поддержку *только* подлинности и целостности данных с использованием протокола *заголовки аутентификации* {authentication header. AH) или поддержку целостности и конфиденциальности данных с использованием протокола Encapsulating Security Payload (ESP). Действие фильтра можно изменять в соответствии с вашими потребностями, что позволяет администратору определить протоколы, требующие подлинности, и протоколы, требующие конфиденциальности.

Можно задать одно или несколько согласованных действий фильтра.

Политика IPSec

Именованный набор правил и параметров обмена ключами. Политику IPSec можно назначить как политику безопасности домена или отдельного компьютера. При входе в домен компьютер домена автоматически наследует политику IPSec, назначенную домену. Если компьютер не подключен к домену (например изолированный сервер), политика IPSec хранится и считывается из системного реестра компьютера.

Это обеспечивает большую гибкость в настройке политики зашиты для групп схожих компьютеров или отдельных компьютеров со специфическими требованиями. Например, можно определить единую политику защиты для всех пользователей одной сети или всех пользователей из конкретного отдела. Для создания политик IPSec на рядовых серверах Windows 2000 применяется оснастка IPSec Management.

Правила

Определяют порядок использования протокола **IPSec.** Правило содержит список фильтров IP и задает действия, предпринимаемые системой безопасности в случае соответствия пакета'определенному фильтру. Правило — это набор:

- IP-фильтров;
- политик согласования параметров связи;
- методов аутентификации;
- атрибутов 1P-туннелирования;
- типов адаптеров.

Каждая политика защиты может включать несколько правил. Это позволяет назначать одну политику IPSec нескольким компьютерам с различными сценариями связи. Например, одна политика распространяется на всех пользователей отдела или сети, однако для установки связи может требоваться множество правил: одно будет управлять связью по интрасети, другое — коммуникациями через Интернет, требующими туннелирования, и т. д.

Методы защиты

Каждый метод защиты определяет уникальный уровень зашиты связи. Чтобы повысить вероятность нахождения двумя компьютерами обшего метода зашиты, в политику согласования параметров связи можно включать несколько методов защиты. Служба ISAKMP/Oakley на каждом компьютере перебирает список методов зашиты в порядке убывания, пока не находит общий метод. Вы можете использовать предопределенный или собственный метод зашиты связи.

- **Высокая степень защиты.** Протокол IP ESP обеспечивает конфиденциальность, целостность и аутентификацию данных, а также зашиту против атак повтора.
- **Средняя степень зашиты.** Протокол мщиты IP AH обеспечивает целостность и аутентификацию данных, а также зашиту против атак повтора. Конфиденциальность данных не обеспечивается.
- **Настраиваемая зашита.** В дополнение к выбору между ESP и AH опытные пользователи могут сами определить алгоритмы аутентификации, целостности и конфиденциальности данных.