Конфигурирование безопасной передачи информации

Использование протоколов IPsec. IPsec (Internet Protocol security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Представляет собой стандарт конфиденциальной передачи данных по сетям IP и позволяет осуществлять подтверждение подлинности, проверку целостности и (или) шифрование IP-пакетов. IPsec также включает в себя протоколы для защищенного обмена ключами в Интернете. В основном используется для организации VPN-соединений (Virtual Private Network).

Конфигурирование безопасной передачи информации

Virtual Private Network (виртуальная частная сеть) — технология, позволяющая обеспечить одно или несколько сетевых соединений поверх другой сети.

IPsec появился, когда Интернет стал публичным и начал активно развиваться. Возникла необходимость построения защищенных протоколов, так как безопасность организовывалась на уровне физической изоляции объектов от посторонних лиц. Доступ к Сети имело ограниченное число машин.

Конфигурирование безопасной передачи информации

В 1994 г. Совет по архитектуре Интернет (IAB) выпустил отчет «Безопасность архитектуры Интернет», который стал предпосылкой создания стандартов защищенных протоколов: RFC2401—RFC2412, используемых и в настоящее время.

Конфигурирование безопасной передачи информации

IPsec является частью IPv6-протокола или расширением протокола IPv4. IPsec располагается на сетевом уровне (3-й уровень в модели ISO/OSI), используя самый распространенный протокол этого уровня — IP, что делает IPsec более гибким. Он мо жет использоваться для защиты любых протоколов, базирующихся на семействе протоколов TCP/IP, и не требует внесения изменений в существующие приложения или ОС.

Конфигурирование безопасной передачи информации

Уровень TCP/IP	Уровень ISO/OSI
4. Прикладных программ	7. Прикладных программ 6. Представление данных
3. Транспортный	5. Сеансовый 4. Транспортный
2. Межсетевой	3. Сетевой
1. Доступа к сети	2. Канальный 1. Физический

Конфигурирование безопасной передачи информации

Протокол IPsec в большинстве случаев не требует установки нового оборудования или замены старого, что снижает стоимость его внедрения. Протокол является стандартным и открытым и поставляется практически со всеми современными ОС. Таким образом, данный протокол позволяет сохранить конфиденциальность данных и обеспечить проверку подлинности пользователей в ранее незащищенной сети без дополнительных затрат на сетевое оборудование.

Конфигурирование безопасной передачи информации

Набор IPsec включает в себя три протокола:

1) *Authentication Header* (AH) — обеспечивает целостность виртуального соединения, аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов;

2) *Encapsulating Security Payload* (ESP) — обеспечивает конфиденциальность передаваемой информации, ограничение потока конфиденциального трафика;

Конфигурирование безопасной передачи информации

3) *Internet Security Association and Key Management Protocol* (ISAKMP) — протокол, используемый для первичной настройки соединения, взаимной аутентификации конечными узлами друг друга и обмена секретными ключами.

Протоколы Authentication Header и Encapsulating Security Payload могут использоваться как совместно для обеспечения наибольшего уровня безопасности, так и независимо друг от друга.

Конфигурирование безопасной передачи информации

Работа протокола IPsec возможна в двух режимах: транспортном и туннельном. Функции протоколов, входящих в набор IPsec, в разных режимах отличаются.

Конфигурирование безопасной передачи информации

Транспортный режим используется для установления безопасного соединения между двумя компьютерами с помощью шифрования полезных данных IP, при этом IP-заголовок остается доступным только для чтения. Протокол Authentication Header защищает данные от целенаправленных изменений. Протокол Encapsulating Security Payload обеспечивает конфиденциальность полезных данных IP, но не заголовка IP.

Конфигурирование безопасной передачи информации

Туннельный режим используется, когда необходимо зашифровать весь исходный IP-пакет. Этот режим позволяет организовать защищенную связь преимущественно средствами VPN-туннелей для передачи данных через открытые каналы связи. Протокол Authentication Header шифрует весь пакет, а затем инкапсулирует его в поле данных нового пакета, при этом данные остаются доступными для чтения.

Конфигурирование безопасной передачи информации

Протокол Encapsulating Security Payload помещает исходный пакет между заголовком ESP и трейлером проверки подлинности ESP, одновременно шифруя эти данные и создавая новый заголовок IP. Сервер туннеля на другой стороне канала расшифровывает и передает пакет получателю.