ЗАЩИТА СЕТЕВОГО УРОВНЯ ПРИ ПОМОЩИ ПРОТОКОЛОВ GRE OVER IPSEC

Сакович Д.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шевчук О. Г. − к. т. н., доцент

В нынешнее время многие компании столкнулись с проблемой организации удалённого доступа между филиалами. Для этого многие из них прибегают к использованию инфраструктуры провайдера для соединения. Однако данная сеть небезопасна для использования в коммерческих целях. Для повышения защиты используется технология туннелирования при помощи протоколов GRE и IPSec.

Использование туннелей GRE вместе с IPSec дает несколько преимуществ, прежде всего потому, что IPSec не поддерживает трафик, отличный от одноадресной. Это может привести к проблемам, если планируется использоваться службы, требующие такого типа трафика, например, протоколы динамической маршрутизации, такие как OSPF или EIGRP, что можно увидеть на рисунке 1.

Благодаря процессу инкапсуляции GRE широковещательный и многоадресный трафик инкапсулируется в одноадресный пакет, который может обрабатываться IPSec, что делает возможной динамическую маршрутизацию между одноранговыми узлами, разделенными небезопасной сетевой областью.

Кроме того, туннели GRE обеспечивают более высокий уровень отказоустойчивости, чем на самом деле пакеты поддержки активности IKE.

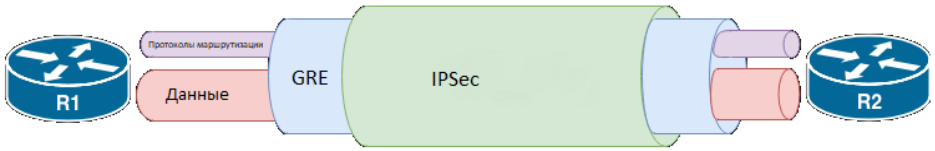

Рисунок 1 – Структура GRE over IPSec туннеля

Для развертывания на сетях был выработан алгоритм, по которому будет организовываться защита сетевого уровня. Данный алгоритм можно увидеть на рисунке 2.

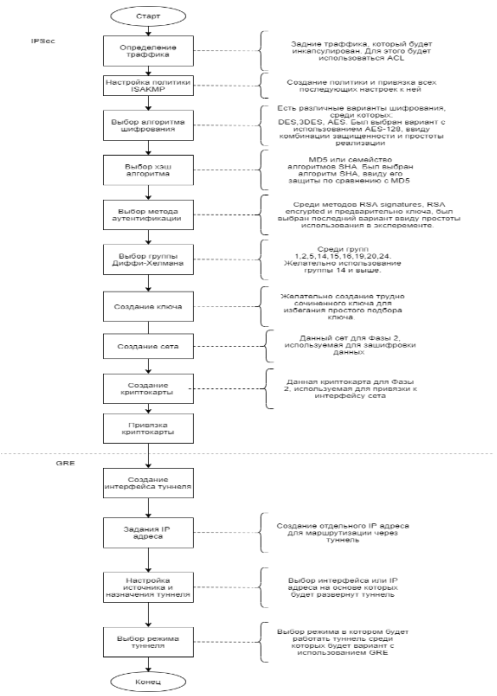

Рисунок 2 – Алгоритм установления защиты при помощи GRE over IPSec

По каждому шагу можно понять какие методы были использованы для инициализации туннелирования.

Данный алгоритм был использован и протестирован смоделированной сети при помощи перехвата пакетов для оценки его. Для моделирования сети был использован программа для эмуляции Cisco Packet Tracer. Результат перехвата одного из пакетов представлен на рисунке 3.

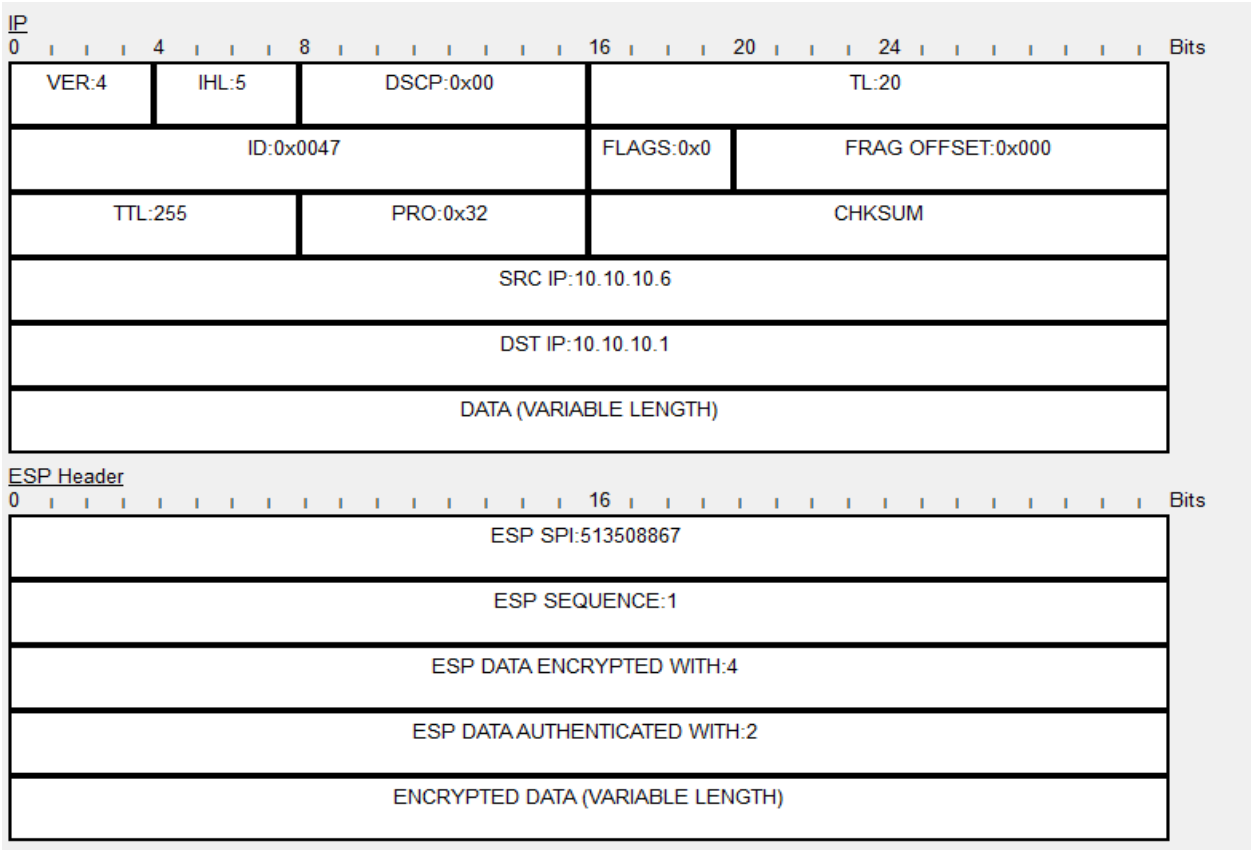

Рисунок 3 - Перехваченный инкапсулированный пакет

При перехвате пакета был получен результат, что данные находятся в зашифрованном и инкапсулированном состояние.

Таким образом, данный метод защиты не даёт возможность злоумышленнику узнать данные передаваемые по сетевому уровню IP.

Список использованных источников:

1. RFC 4301 Security Architecture for the Internet Protocol / S. Kent, K. Seo, december 2005.
2. RFC 1701 – Generic Routing Encapsulation (GRE) / Stan Hanks, october 1994