Д. М. Максимов, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732

ОРГАНИЗАЦИЯ УДАЛЕННОГО БЕЗОПАСНОГО СОЕДИНЕНИЯ К СЕТИ ПРЕДПРИЯТИЯ СРЕДСТВАМИ FLEXVPN

Аннотация. *В статье рассмотрена возможность применения технологии FlexVPN от компании Cisco в рамках повышения уровня безопасности сети предприятия, отражена актуальность использования технологии, обеспечивающей удаленное безопасное соединение. В результате проделанной работы была построена практическая модель применения технологии FlexVPN в сети предприятия, обеспечивающая безопасное удаленное соединение между филиалами.*
Ключевые слова: *Cisco, Flex VPN, IPSEC, удаленный доступ.*

Введение. В связи с интенсивным развитием сети Интернет все чаще поднимается вопрос о построении VPN-сети. Эта технология, с помощью которой можно организовать сетевое соединение между несколькими удаленными сетями поверх другой сети, то есть, она дает возможность объединить удаленных пользователей в единую сеть без использования дополнительных физических каналов передачи данных. Одной из передовых подобных технологий является проприетарная технология FlexVPN компании Cisco.

VPN (Virtual Private Network) — это технология, которая использует публичную сеть для построения специальной частной сети [1], от безопасности которой зависит функционирование предприятия. Обеспечение безопасности в такой сети возможно с помощью протокола PPTP, с помощью которого организуется шифрованный тунель [2], или с помощью протокола SSL, благодаря которому обеспечивается безопасность управляющего канала и потока данных [3]. Однако ни один из предложенных подходов не дает должного уровня защиты удаленного доступа для операционной системы Cisco IOS, так как организация его безопасной работы на сетевом оборудовании Cisco имеет особенности, знание которых необходимо учитывать при его имплементации в корпоративную сеть.

Проблема исследования. Сегодня технологии, обеспечивающие безопасное удаленное соединение, уже широко применяются в сфере безопасности предприятий различного масштаба. Согласно подведенным итогам второго квартала 2021 г. от специалистов аналитической компании IDC, доля лидирующей компании Cisco на рынке маршрутизаторов оценивается в 34,2% [4].

Защита VPN-соединения является достаточно сложным и комплексным процессом, поэтому были выделены несколько задач:

1. Изучить теоретические особенности функционирования Flex VPN.
2. Сравнить современные протоколы обеспечения безопасности туннельных соединений.
3. Проанализировать методы защиты трафика, передаваемого посредством VPN.
4. Смоделировать компьютерную сеть организации, использующую технологи Flex VPN, в программном эмуляторе.

Материалы и методы. Методами данного исследования стали: наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для эмуляции компьютерной сети было выбрано программное средство GNS3 2.2.31.

Результаты. FlexVPN — это структура конфигурации (набор команд CLI/API), направленная на то, чтобы упростить настройку топологий remote access, site-to-site [5]. Это мощная и основанная на стандартах технология VPN, которая позволяет крупным компаниям безопасно устанавливать соединение между различными офисами и удаленными клиентами. Она обеспечивает превосходную экономию средств по сравнению с расходами на многочисленные отдельные типы виртуальных частных сетей (VPN), таких как GRE (generic routing encapsulation), crypto map и решения на базе virtual tunnel interface (VTI).

FlexVPN работает только на современном служебном протоколе IKEv2 и обратно не совместим с технологиями, использующими предыдущую версию IKEv1.

IKEv2 — это протокол туннелирования на основе IPsec, который обеспечивает безопасный канал связи VPN между одноранговыми

устройствами VPN и определяет согласование и аутентификацию для ассоциаций безопасности (SA) IPsec защищенным способом [6].

IPSec — это набор протоколов, используемых для создания безопасного интернет-соединения, передачи данных и коммуникаций. В этот набор протоколов входят протоколы: Internet Key Exchange (IKE), Authentication Header (AH), Encapsulating Security Payload (ESP). Перечисленные группы протоколов имеют следующие возможности: конфиденциальность и целостность данных, аутентификация узлов, защита от воспроизведения данных и доставка ключей.

В качестве примера спроектируем топологию сети малого предприятия с головным офисом и удаленным от него филиалом с использованием маршрутизаторов, поддерживающих функциональные возможности технологии FlexVPN (рис. 1).

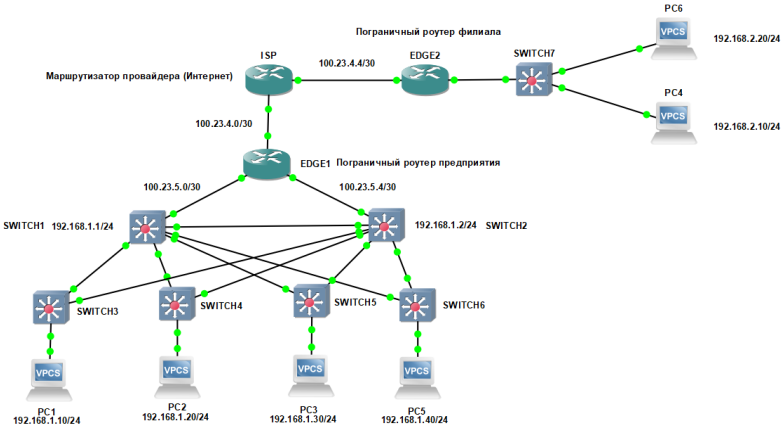

Рис. 1. Топология сети предприятия с использованием устройств, поддерживающих технологию FlexVPN

На рис. 1 устройства, обозначенные словом EDGE, — это пограничные маршрутизаторы предприятия, между которыми установлено VPN-соединение (рис. 2).

Рис. 2. Активное VPN-соединение и используемые алгоритмы безопасности

Создана закрытая внутренняя сеть, где все офисы подключены между собой и весь трафик, который ходит между ними, зашифрован (рис. 3).

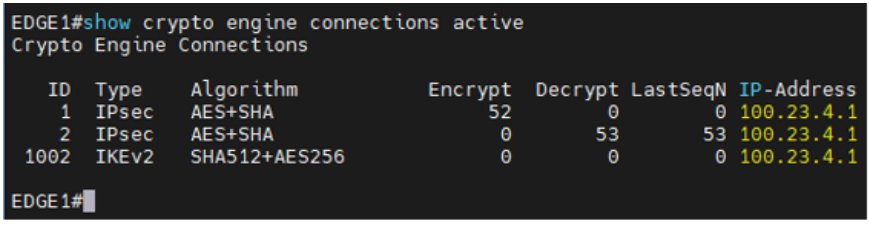

Рис. 3. Шифрование передаваемого в туннеле трафика

Заключение. В результате проведенной работы была смоделирована защита VPN-соединения средствами современной проприетарной технологии от компании Cisco. Также в статье были рассмотрены теоретические особенности функционирования Flex VPN и проанализированы современные протоколы, с помощью которых данная технология работает. В статье предложены конкретные безопасные алгоритмы криптографии и хэширования информации, результаты их применения были апробированы в среде эмуляции.

СПИСОК ЛИТЕРАТУРЫ

1. Губарев Е. А. Моделирование GRE OVER IPSEC VPN сети предприятия в среде CISCO PACKET TRACER / Е. А. Губарев. — Текст : электронный // Инновационные технологии: теория, инструменты, практика. — 2017. — № 1. — URL: https://www.elibrary.ru/download/elibrary_34876914_92461678.pdf (дата обращения: 02.05.2022).

2. Рощин Д. VPN на основе протокола PPTP: как повысить безопасность? / Д. Рощин. — Текст : электронный // Системный администратор. — 2007. — № 4. — URL: https://www.elibrary.ru/download/elibrary_20394452 _21186501.pdf (дата обращения: 04.05.2022).
3. Киселев С. С. Протокол SSL/TLS как основа технологии VPN / С. С. Киселев, С. В. Пилькевич, Н. В. Салко. — Текст : электронный // Труды военно-космической академии имени А. Ф. Можайского. — 2011. — № 630. — URL: https://www.elibrary.ru/download/elibrary_21050527_ 24730965.pdf (дата обращения: 05.05.2022).
4. Продажи коммутаторов Ethernet корпоративного уровня за год. — Текст : электронный // https://www.ixbt.com : новостной ресурс. — 2021. — URL: https://www.ixbt.com/news/2021/09/10/ethernet-10-8.html (дата обращения: 14.05.2022).
5. Cisco FlexVPN DMVPN, Part 1 — Overview and Design / M. Kashin. — URL: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design (date of the application: 10.05.2022). — Text : electronic.
6. IKEv2 VPN Protocol Explained / Miklos Zoltan. — URL: https://www.privacyaffairs.com/ikev2-vpn-protocol (date of the application: 11.05.2022). — Text : electronic.

Ю. Ю. Михайлов, Д. С. Топкасов, Т. И. Паюсова
Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ФИЛЬТРАЦИИ НЕЖЕЛАТЕЛЬНОГО КОНТЕНТА В ИНТЕРНЕТЕ

Аннотация. *В статье обоснована необходимость фильтрации контента, а также перечислены требования, которым должен удовлетворять программный комплекс для фильтрации нежелательного контента в Интернете.*

Ключевые слова: *обработка естественных языков, фильтрация контента, информационная безопасность, законодательство РФ, нежелательный контент.*

Введение. Информационная безопасность — это защита не только информации, но и от нее. Точнее, от ее воздействия.

Эта сфера регулируется различными федеральными законами и нормативными правовыми актами Российской Федерации.