ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2025. Т. 7, № 2 (21). С. 134–142 http://siit.ugatu.su
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья

УДК 004.89 DOI 10.54708/2658-5014-SIIT-2025-no2-p134 EDN LIVHUK

Способы решения типовых проблем при построении VPN-туннелей на базе опорной сети разных провайдеров

Д. А. Любименко • А. Г. Кравец

Аннотация. В статье рассмотрены проблемы построения филиальной сети Site-to-Site и способы их решения при использовании протокола IKE (internet key exchange), входящего в стек IPSec. Построена типовая топология, применяемая на предприятиях оборонно-промышленного комплекса (обязательно соответствие шифрования ГОСТ 34.12-2018). Испытания проведены на реальных программно-аппаратных комплексах отечественного происхождения. Выполнено сравнение режимов прохождения трафика при использовании протоколов IKE v1 и IKE v2 (обычный и агрессивный режимы), определена возможность эксплуатации в условиях с длительным откликом, разными значениями параметра Maximum Transmission Unit. Полученные результаты подтвердились при проведении опытной эксплуатации в тестовой среде. На основе экспериментов определены основные проблемы интеграции сетей с использованием public key infrastructure (PKI) и методы их решения. Предположительно, рассмотренное техническое решение позволяет добиться стабильной передачи трафика между площадками даже при отсутствии «серого волокна», обеспечивающего задержки трафика менее 1 мс. Подтверждена высокая скорость работы при выполнении перечня обязательных технических условий. Это обеспечивает соединение между удаленными площадками для обычного и агрессивного режима соединения IKE.

Ключевые слова: IKE; IPSec; VPN; PKI; Site-to-Site.

Введение

Обязательное условие построения защищенного канала связи между удаленными площадками на предприятиях оборонно-промышленного комплекса (ОПК) – шифрование данных. Оно должно соответствовать требованиям, перечисленным в ГОСТ 34.12-2018 [1]. Таким требованиям удовлетворяет стек протоколов IPSec. Необходимо использовать доверенные программно-аппаратные комплексы (ПАК). Это касается всего телекоммуникационного оборудования.

Современное телекоммуникационное оборудование российского происхождения (ТОРП) для обеспечения защищенных каналов связи VPN использует стандартную инфраструктуру – IPSec. Процесс шифрования данных обеспечивается отдельным сервисом. Для его работы задействован IKE, выполняющий обмен ключами [2]. В процессе работы происходит аутентификация сторон. При обмене ключами выполняется согласование параметров, выбираются соответствующие ключи для алгоритмов шифрования [3]. Работа самого IKE построена на ISAKMP (Internet Security Association and Key Management Protocol). Задействован Oakley с модифицированным алгоритмом Диффи–Хеллмана. Последний формирует и управляет процедурой создания ключей шифрования. Oakley необходим для выполнения преобразований внутри сервиса IPSec [4]. Стек протоколов используется для формирования ассоциаций защиты между потенциальными сторонами IPSec.

IKE использует сравнительно простые математические модели. Первая – хэш-функция. Она обеспечивает устойчивость к коллизиям (невозможность совпадения двух сообщений m_1 и m_2) [5]:

$$H(m_2) = H(m_1). \quad (1)$$

В уравнении (1) H – обозначение хэш-функции. Ранее для решения задачи псевдослучайных функций использовались PRF (псевдослучайная функция). В современной реализации

протокола IKE задействуется HMAC – аутентификация с использованием хэш-функций [6]. Решение задачи предполагает наличие хэш-функции (*H*) и секретного ключа (*K*). Информация хэшируется с помощью процедуры сжатия. Длина каждого отдельного блока в байтах – *B*. Длина блоков после хэширования – *L*.

$$I_{\text{pad}} = \text{байт } 0\times36, \tag{2}$$

$$O_{\text{pad}} = \text{байт } 0\times5 \text{ с.} \tag{3}$$

В формулах (2) и (3) повторение было выполнено *B* раз. Расчет HMAC от произвольных данных «text» выполняется по формуле [7]:

$$H(K \text{ XOR } O_{\text{pad}}, H(K \text{ XOR } I_{\text{pad}}, \text{text})). \tag{4}$$

Цель исследования

Построение защищенных VPN-туннелей на базе опорной сети общего пользования требует определенной подготовки. Процесс создания зашифрованного канала подразумевает выполнения ряда требований, перечисленных в RFC 2405 [8]. Теоретически возможно использование IKE первой и второй версии в сетях с низкой пропускной способностью. Часто возникают вопросы, связанные с утилизацией канала. При высоком отклике (более 40 мс) скорость передачи при ширине канала 100 Мбит/с может составлять всего 3 %. Такие показатели – стандартные для сетей передачи данных общего пользования. При проведении опытной эксплуатации выбрано оборудование, обеспечивающее длительность задержи не более 10 мс, что позволяет утилизировать при использовании IKE v1 на 30–50 %. На стабильность передачи данных влияет maximal transmission unit (MTU). Дополнительные протоколы маршрутизации не использовались (OSPF, BGP). Требуемые задержки обеспечены с использованием базовых настроек провайдерского оборудования. Перед началом испытаний выполнены замеры задержек между отдельными узлами с помощью встроенной утилиты PING, отправляющей ICMP-запрос. Маршрут прохождения трафика включает 2 промежуточных узла. Такое количество позволяет обеспечить точность проведения всех замеров.

Основная цель исследования: определить на практике факторы, влияющие на устойчивость канала связи, скорость передачи между хостами, расположенными за разными узлами, между которыми построены туннели. Работа современных ИТ-систем требует устойчивого соединения, производительности канала связи. Особенно это касается высоконагруженных систем. Классические серверные конфигурации (включающие в себя 3 сервера с базами данных, 2 сервера приложений, 2 веб-сервера), являющиеся георазпределенными и катастрофоустойчивыми, реплицируются [9]. Базы данных могут иметь размер в несколько десятков гигабайт, что вкупе с одновременной работой через каналы связи обычных пользователей и других систем предполагает необходимость высокой скорости соединения.

Построение VPN-туннеля часто происходит с использованием сети двух провайдеров. Наличие стыка может увеличить длительность задержки. Для тестирования нагрузки канала применяется утилита iperf. На рис. 1 представлена упрощенная модель соединения двух серверов с базами данных, между которыми выполняется репликация [10].

Программа испытаний в частном случае предполагает построение туннеля IPSec с использованием IKE разных версий, выгрузку дампа трафика и анализ результатов, полученных в процессе опытной эксплуатации туннеля [11].

Построение туннеля: фазы IPSec и требования L2TP

Набор защищенных протоколов передачи данных IPSec позволяет осуществлять транспорт по незащищенным сетям, не беспокоясь о конфиденциальности. Функционал реализован на третьем уровне OSI. Приложения, работающие на уровнях выше, не замечают работу данного протокола [12].

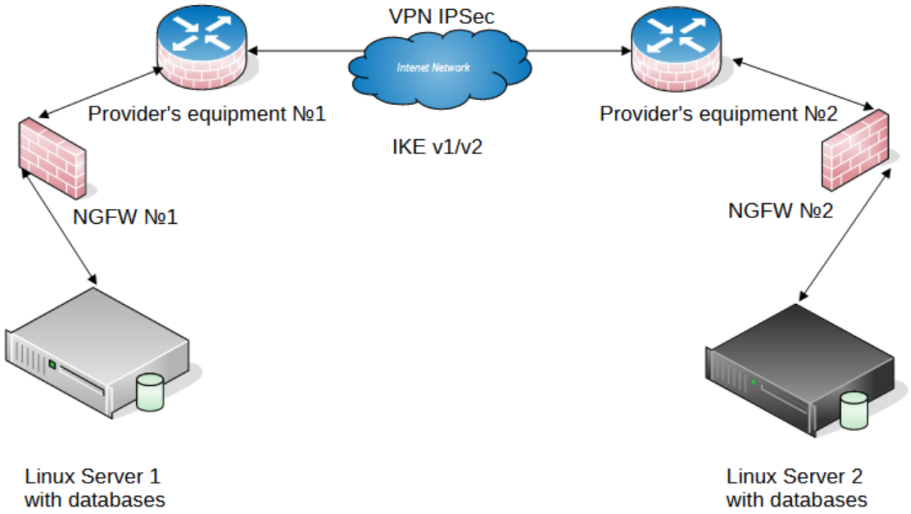

Рис. 1 Типовая схема построения VPN-туннеля через двух провайдеров

Процесс согласования включает 2 фазы:

- первый этап: взаимно определяют метод идентификации, алгоритм хэша и шифрования, группу Диффи–Хелмана;
- второй этап: генерация ключей.

Сертифицированные Федеральной службой по техническому и экспортному контролю (ФСТЭК) устройства не всегда поддерживают работу IPSec без L2TP. Последний обязательно требует инкапсуляции данных. Процесс туннелирования и инкапсуляции предполагает выполнение требований к качеству канала связи. При величине задержки более 10 мс возможно уменьшение скорости прохождения трафика через туннель [13].

Сложности построения возникают на этапе установления туннеля средствами протокола Internet Key Exchange (IKE). Первая версия протокола IKE более чувствительная к задержкам трафика за счет использования инкапсуляции. В IKE v1 закреплен режим шифрования. Внесение в него изменений не предполагается, что создало сложности с сертификацией. Вторая версия протокола была создана в 2005 году. Отличается гибкостью настройки, структурированностью. Реализовано разделение отдельных элементов протокола. Опции позволяют настраивать функционал (основное отличие от IKE v1) [14]. Сложность использования IKE v2 обусловливается необходимостью применения Public Key Infrastructure (PKI). При отсутствии собственного центра сертификации задействуется свободное программное обеспечение (OpenSSL или аналогичное). Недостаток Open Source Software – вероятность наличия программных закладок.

Использование IKE v1 для построения туннеля: замеры задержек и нагрузочное тестирование

Для проведения тестирования построен туннель с применением протокола IKE v1. Для этого использованы отечественные межсетевые экраны Usergate (appliance-образы) (рис. 2).

Согласно RFC 2405, ключевым параметром для стабильного соединения является величина задержки трафика. Посчитаем среднюю величину задержки между двумя серверами с адресами 10.10.3.20 и 10.10.20.20 с помощью утилиты ping. Отправим 9 эхо-запросов (рис. 3) [15]. Средняя величина задержки между серверами при использовании IKE v1 составляет 3.2 мс. Данный параметр укладывается в нормы RFC 2405. Требования к отклику описаны также в RFC 4306. Если ответ не получен в течение заданного времени, запрашивающий узел может просто повторить свой запрос. Но повторный либо последующий за ним запрос станут причиной снижения скорости передачи данных. По этой причине шифрование такого типа используют для эксплуатации внутри топологии с минимальными задержками.

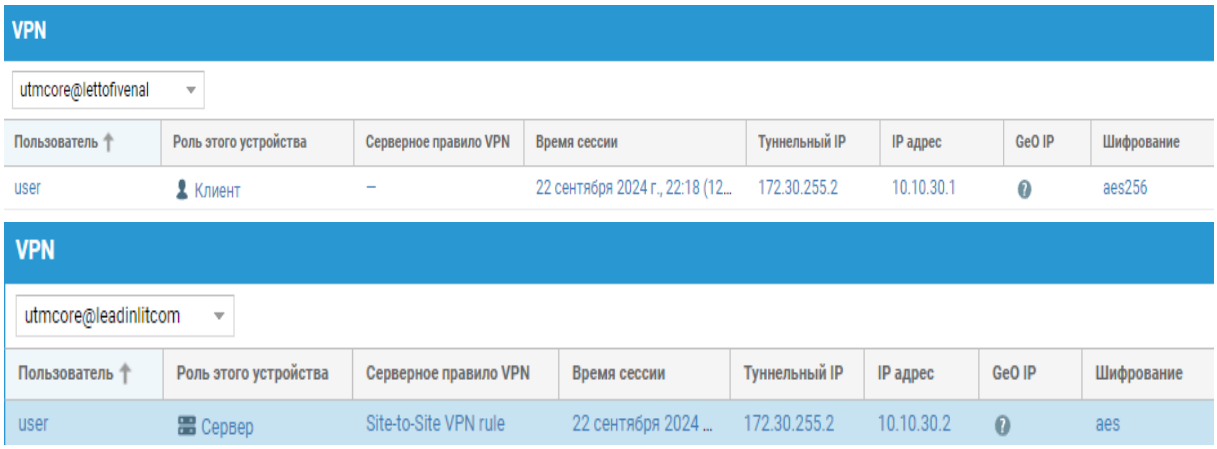

Рис. 2 Иллюстрация подключения, адресация, тип шифрования

```
lyubimenko@ubuntu-2:~$ ping -c 9 10.10.3.20
PING 10.10.3.20 (10.10.3.20) 56(84) bytes of data.
64 bytes from 10.10.3.20: icmp_seq=1 ttl=62 time=2.88 ms
64 bytes from 10.10.3.20: icmp_seq=2 ttl=62 time=2.98 ms
64 bytes from 10.10.3.20: icmp_seq=3 ttl=62 time=3.58 ms
64 bytes from 10.10.3.20: icmp_seq=4 ttl=62 time=1.88 ms
64 bytes from 10.10.3.20: icmp_seq=5 ttl=62 time=2.61 ms
64 bytes from 10.10.3.20: icmp_seq=6 ttl=62 time=4.45 ms
64 bytes from 10.10.3.20: icmp_seq=7 ttl=62 time=3.64 ms
64 bytes from 10.10.3.20: icmp_seq=8 ttl=62 time=2.03 ms
64 bytes from 10.10.3.20: icmp_seq=9 ttl=62 time=5.15 ms
```

Рис. 3 Отправка 9 эхо-запросов с сервера 10.20.20.20 на сервер 10.10.3.20

Альтернатива IKE v1 и IKE v2 – протокол «Магма». Внутри него задействовано 32 раунда шифрования. Он менее чувствителен к задержкам, но требует глубокого понимания алгоритма шифрования. Протокол «Магма» задействуется в межсетевых экранах нового поколения «Континент». Отличительная особенность продукта – отсутствие возможности подключения устройств стороннего производителя. Usergate (используется для опытной эксплуатации) поддерживает работу с различными производителями межсетевых экранов, что подтверждается наличием преднастроенных профилей безопасности. Базовая конфигурация включает в себя наличие стандартных настроек для подключения оборудования Cisco, Fortinet. Отсутствуют сложности с работой туннелей VPN между Mikrotik и Usergate (рис. 4).

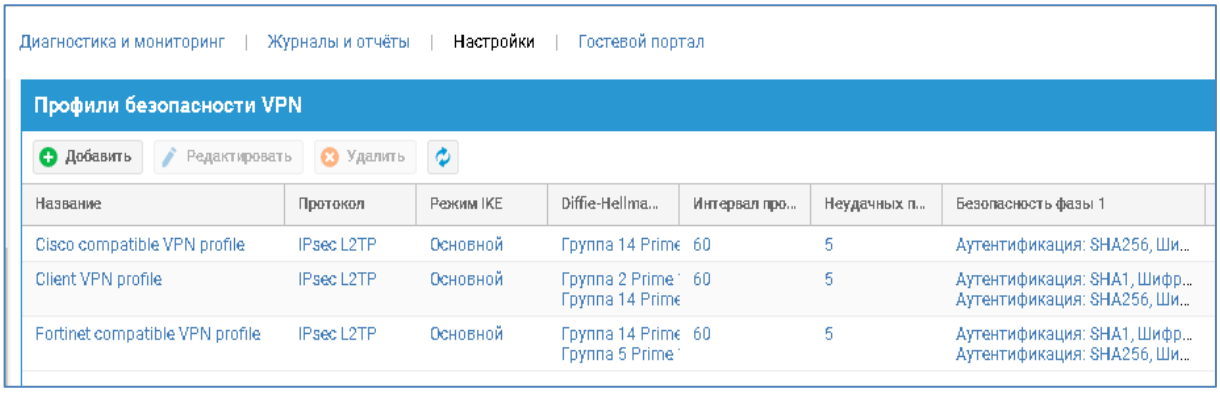

Рис. 4 Преднастроенные профили безопасности

Запустим нагрузочное тестирование для канала связи между двумя узлами. Утилита iperf используется для генерации трафика. В качестве клиента будет выступать сервер с адресом 10.10.20.20. В качестве сервера – 10.10.3.20. При отличных MTU (1360, 1400, 1500) [16]

различия в скорости передачи данных не обнаружены. Может использоваться основной режим (main mode) и агрессивный (aggressive mode). Основной режим задействует 6 сообщений. Канал реализован на базе ISAKMP SA. На первом этапе происходит согласование алгоритмов обмена данными, хэширования. Включается алгоритм Диффи–Хеллмана (задействуются случайные числа). Только на третьем этапе происходит рукопожатие, завершение проверки подлинности сторон. Процедура циклична. Агрессивный режим задействует 3 сообщения. На первом этапе передаются все данные, необходимые для создания соединения. Вторая сторона следующим шагом также высылает генерацию. Третий этап – создание соединения. Опасность агрессивного режима заключается в большом количестве технической информации, передаваемой вместе с сообщением. Нагрузочное тестирование было выполнено в основном и агрессивном режимах. Полученные результаты представлены в табл. 1.

Таблица 1

Результаты нагрузочного тестирования утилитой iperf с использованием IKE v1

ID	Interval, sec	Transfer, Gb	Bandwidth, Mbits/sec
1	0.0000–10.0192	1.05	896
2	0.0000–10.0277	1.04	888
3	0.0000–10.0255	1.05	827
4	0.0000–10.0248	1.13	969
5	0.0000–10.0326	1.02	874

ИСПОЛЬЗОВАНИЕ IKE v2 ДЛЯ ПОСТРОЕНИЯ ТУННЕЛЯ: ЗАМЕРЫ ЗАДЕРЖЕК И НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ

Для проведения тестирования построен VPN-туннель с использованием IKE v2. Коммутация между двумя устройствами с использованием данного протокола требует наличия сертификатов сервера и клиента. Выпуск можно осуществить с использованием утилиты OpenSSL [16]. В процессе формирования сертификата необходимо указывать вместо FQDN (Fully Qualified Domain Name) ip адрес внешнего интерфейса зоны Untrusted. В случае указания FQDN при попытке генерации из запроса возникает ошибка вида

error:22098080:X509 V3 routines:X509V3_EXT_nconf:error
in extension:v3_conf.c:93:name=subjectAltName.

Использование ip позволяет избежать ошибки. Процесс выпуска сертификата представлен ниже. На рис. 5 обозначены основные параметры корневого сертификата, самоподписного.

```
lyubimenko@ubuntu-240401:~$ sudo openssl genrsa -aes256 -passout pass:1234 -out rootCA.key 4096
[sudo] password for lyubimenko:
lyubimenko@ubuntu-240401:~$ sudo openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem -subj "/C=RU/ST=Vlg/L=Vlg/O=server/OU
=10.10.30.1/CN=QA"
Enter pass phrase for rootCA.key:
```

Рис. 5 Генерация самоподписного сертификата для сервера

На основе созданного корневого сертификата генерируются сертификаты для VPN-сервера. Создается приватный ключ с расширением pem. Полученная ключевая пара подгружается на серверный узел. Аналогичная процедура выполняется на клиентском узле [17]. Построение туннеля требует предварительной настройки узлов. Создаются дополнительные подсети, прописываются маршруты, профили безопасности (рис. 6).

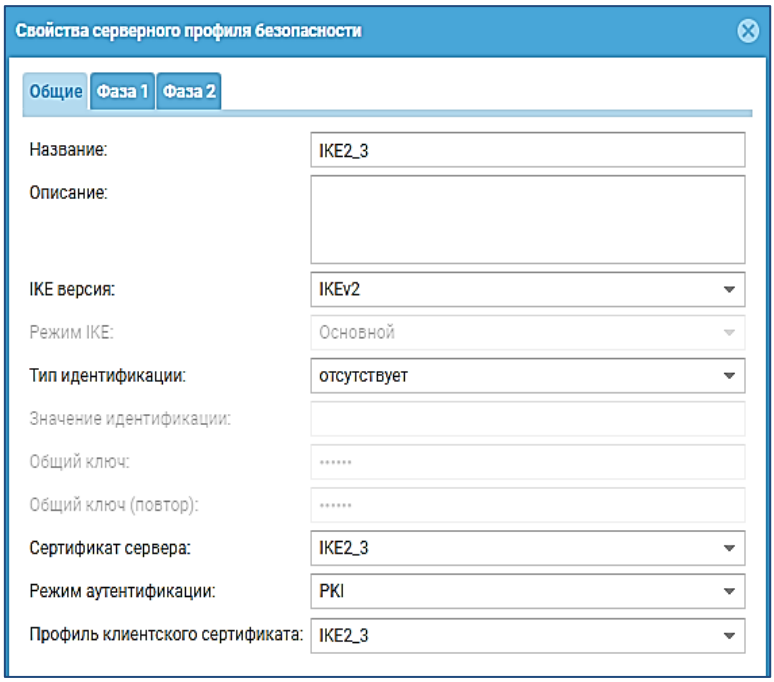

Рис. 6 Настройка профиля безопасности

Построение туннеля выполнено, подключение произошло. Для проверки внутрь туннеля был запущен ICMP-запрос. Средняя величина отклика составила 3.2 мс – аналогично тестированию, проведенному для испытаний IKE v1, что позволяет добиться максимальной чистоты эксперимента [18]. Согласно утверждению вендора, пропускная способность туннеля VPN при использовании IKE v2 должна увеличиться вдвое [19]. Для проверки проведем замер пропускной способности между двумя виртуальными машинами Linux с помощью утилиты iperf. Нагрузочное тестирование на канал выполняется 5 раз. В качестве принимающей стороны трафика выступает хост с адресом 10.10.1.6. Клиент – 10.10.2.5. Результат тестирования в реальном времени частично представлен на рис. 7 и в табл. 2 (работа серверной части утилиты iperf).

```
lyubimenko@ubuntu-1:~$ sudo iperf -s
[sudo] пароль для lyubimenko:
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size:  128 KByte (default)
------------------------------------------------------------
[  1] local 10.10.1.6 port 5001 connected with 10.10.1.5 port 38292 (icwnd/mss/irtt=14/1448/56
9)
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.0230 sec  1.88 GBytes  1.61 Gbits/sec
[  2] local 10.10.1.6 port 5001 connected with 10.10.1.5 port 52306 (icwnd/mss/irtt=14/1448/39
2)
[ ID] Interval       Transfer     Bandwidth
[  2] 0.0000-10.0083 sec  1.88 GBytes  1.61 Gbits/sec
[  3] local 10.10.1.6 port 5001 connected with 10.10.1.5 port 41038 (icwnd/mss/irtt=14/1448/12
9)
[ ID] Interval       Transfer     Bandwidth
[  3] 0.0000-10.0165 sec  1.85 GBytes  1.59 Gbits/sec
```

Рис. 7 Нагрузочное тестирование канала
с использованием протокола шифрования IKE v2

В процессе опытной эксплуатации на интерфейсах межсетевых экранов были задействованы разные MTU (1360, 1400, 1500). Отличия в скорости передачи данных отсутствовали [20]. На туннельных интерфейсах задействован MTU 1420. На физических портах установлен MTU 1500. Пример конфигурации параметров MTU на разных портах представлен на рис. 8.

Таблица 2

Результаты нагрузочного тестирования утилитой iperf с использованием IKE v2

ID	Interval, sec	Transfer, Gb	Bandwidth, Gbits/sec
1	0.0000–10.0230	1.88	1.61
2	0.0000–10.0083	1.88	1.61
3	0.0000–10.0165	1.85	1.59
4	0.0000–10.0100	1.83	1.57
5	0.0000–10.0066	1.89	1.62

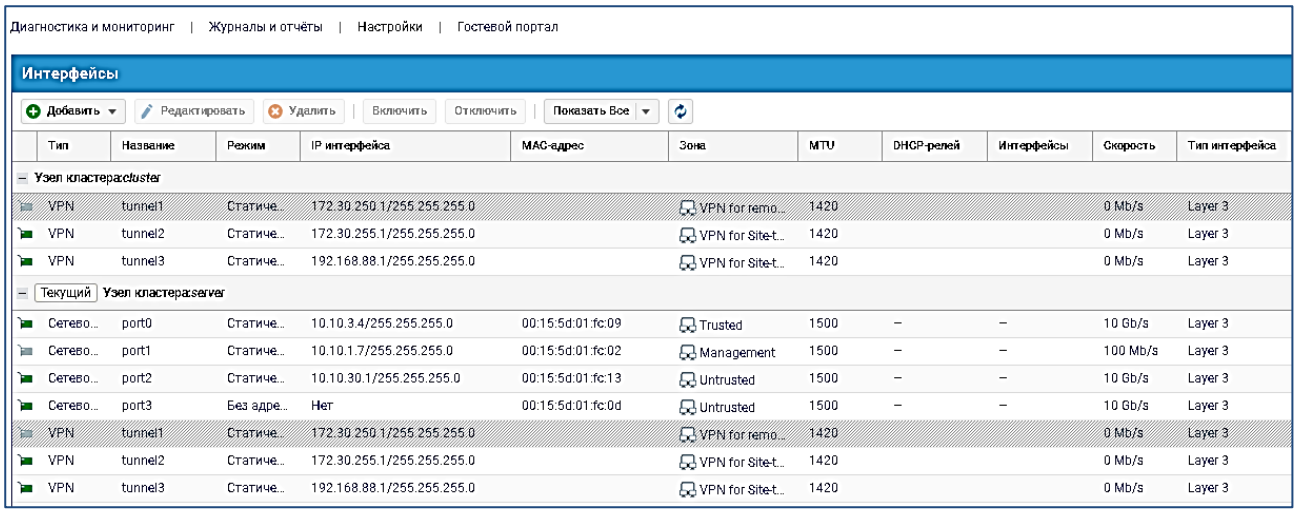

Рис. 8 Настройка MTU на физических и туннельных интерфейсах

Заключение

В работе рассмотрено проектирование топологии VPN с использованием разных протоколов шифрования (IKE v1 и IKE v2), соответствующих ГОСТ 34.12-2018. Для проверки соответствия данных, представленных в описании RFC 2409 и RFC 7296, построены тестовые туннели на базе NGFW отечественного производства Usergate (имеет сертификаты ФСТЭК № 3905). Задействованы разные значения Maximum Transmission Unit. Работа с разным MTU на физических и туннельных интерфейсах штатная. Какие-либо отличия отсутствуют.

При проведении опытной эксплуатации получены результаты тестирования канала с максимальной нагрузкой и длительностью задержки более 1 мс (параметр соответствует аналогичному показателю в сетях общего пользования). На основании полученных результатов можно сделать вывод о полном соответствии описанию RFC 2409, 7296 и возможности эксплуатации VPN IKE v2 в сети Интернет.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

[1] Деундяк В. М., Таран А. А. Система распределения ключей на дизайнах // Моделирование и анализ информационных систем. 2019. Т. 26. № 2. С. 229–243. DOI 10.18255/1818-1015-2019-2-229-243. EDN RYJIBR. [[Deundyak V. M., Taran A. A. “Key distribution system based on designs” // Modeling and Analysis of Information Systems. 2019. Vol. 26, no. 2, pp. 229–243. DOI 10.18255/1818-1015-2019-2-229-243. EDN RYJIBR. (In Russian).]]

[2] Diffie W., Hellman M. E. “New directions in cryptography” // IEEE Transactions on Information Theory. 1976. Vol. 22. No. 6. Pp. 644–654. DOI 10.1109/TIT.1976.1055638.

[3] Шуравин А. С., Лепешкин О. М., Курило А. А. Анализ сетей связи специального назначения с точки зрения угроз безопасности информации // Радиолокация, навигация, связь: Сб. тр. XXV Междунар. науч.-техн. конф. 2019. С. 90–93. EDN VSYVLY. [[Shuravin A. S., Lepeshkin O. M., Kurilo A. A. “Analysis of special-purpose communication networks from the point of view of information security threats” // Radar, Navigation, Communication: Proc. XXV Int. Conf. 2019. Pp. 90–93. EDN VSYVLY. (In Russian).]]

[4] Гребнев С. В., Лазарева Е. В. и др. Интеграция отечественных протоколов выработки общего ключа в протокол TLS 1.3 // Прикладная дискретная математика. Приложение. 2018. № 11. С. 62–65. DOI 10.17223/2226308X/11/19. EDN XYMQAP. [[DOI 10.17223/2226308X/11/19. EDN XYMQAP. (In Russian).]]

[5] Eronen P., Laganier J., and Madson C. IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2). RFC 5739. Internet Engineering Task Force (IETF), 2010. DOI 10.17487/rfc5739.

[6] Информационная безопасность открытых систем. Т. 2. Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. М.: Горячая линия-Телеком, 2018. 558 с. [[Information Security of Open Systems. Vol. 2. Means of Protection in Networks / S. V. Zapechnikov, N. G. Miloslavskaya, A. I. Tolstoy, D. V. Ushakov. Moscow: Goryachaya Liniya-Telecom, 2018. (In Russian).]]

[7] Гришина Н. В. Информационная безопасность предприятия: Учеб. пос. М.: Форум, 2018. 118 с. EDN ZAFTOX. [[Grishina N. V. Information Security of the Enterprise: textbook. Moscow: Forum, 2018. EDN ZAFTOX. (In Russian).]]

[8] Будко П. А., Кулешов И. А., Курносов В. И., Мирошников В. И. Инфокоммуникационные сети: Энциклопедия. Кн. 4. Гетерогенные сети связи принципы построения, методы синтеза, эффективность, цена, качество. М.: Наука, 2020. 683 с. [[Budko P. A., Kuleshov I. A., Kurnosov V. I., Miroshnikov V. I. Infocommunication Networks: encyclopedia. Book 4. Heterogeneous Communication Networks: Design Principles, Synthesis Methods, Efficiency, Price, Quality. Moscow: Nauka, 2020. (In Russian).]]

[9] Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности. СПб.: Питер, 2018. 256 с. EDN LEVPBQ. [[Rodichev Yu. A. Regulatory Framework and Standards in the Field of Information Security. St. Petersburg: Piter, 2018. EDN LEVPBQ. (In Russian).]]

[10] Сычев К. И. Многокритериальное проектирование мультисервисных сетей связи. СПб., 2018. 272 с. [[Sychev K. I. Multicriteria Design of Multiservice Communication Networks. St. Petersburg, 2018. (In Russian).]]

[11] Nencioni G. & Helvik B. & Gonzalez A. & Heegaard P. & Kamisiński A. Impact of SDN Controllers Deployment on Network Availability. 2016. DOI 10.48550/arXiv.1703.05595.

[12] Власенко А. В. Событийное реагирование на инциденты информационной безопасности // Цифровая трансформация науки и образования. 2021. С. 230–236. EDN YPQINH. [[Vlasenko A. V. “Event-based response to information security incidents” // Digital Transformation of Science and Education. 2021. Pp. 230–236. EDN YPQINH. (In Russian).]]

[13] Виноградено А. М. Методология интеллектуального контроля технического состояния автоматизированной системы связи специального назначения. СПб.: Наукоемкие технологии, 2020. 80 с. [[Vinogradenko A. M. Methodology of Intelligent Control of the Technical Condition of an Automated Special-Purpose Communication System. St. Petersburg: Science-intensive technologies, 2020. (In Russian).]]

[14] Николаенко Е. П. Управление инцидентами информационной безопасности // ЭМПИ: экономика, менеджмент, прикладная информатика: Мат-лы IV Всеросс. конф. Брянск, 5 марта 2019 г. Брянск: Брянск. гос. техн. ун-т, 2019. С. 207–210. EDN PKPLYA. [[Nikolaenko E. P. “Information security incident management” // EMPI: Economics, Management, Applied Informatics: Proc. IV All-Russian Conf. Bryansk, March 5, 2019. Bryansk, 2019, pp. 207–210. EDN PKPLYA. (In Russian).]]

[15] Porsev K. I., Sorokin A. V. “Management of innovations and knowledge in the structure of the enterprise integrated information environment” // Proc. 2020 Int. Conf. Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2020. Pp. 283–285. DOI 10.1109/ITQMIS51053.2020.9322865. EDN GPDGYR.

[16] Budko P. A. et al. “Method of adaptive control of technical states of radioelectronic systems” // Advances in Signal Processing. Theories, Algorithms, and System Control. Intelligens Systems Reference Library. Springer-Verlag 2020. Vol. 184. Chapter 11. Pp. 137–151. DOI 10.1007/978-3-030-40312-6_11. EDN MHPZXO.

[17] Виноградено А. М., Будко Н. П. Адаптивный контроль технического состояния сложных технических объектов на основе интеллектуальных технологий // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 1. С. 25–35. DOI 10.36724/2072-8735-2020-14-1-25-35. EDN KEFCQK. [[Vinogradenko A. M., Budko N. P. “Adaptive control of the technical condition of complex technical objects based on intelligent technologies” // T-Comm: Telecommunications and Transport. 2020. Vol. 14, no. 1, pp. 25-35. DOI 10.36724/2072-8735-2020-14-1-25-35. EDN KEFCQK. (In Russian).]]

[18] Turskis Z., Goranin N., Nurusheva A., Boranbayev S. “Information security risk assessment in critical infrastructure a hybrid MCDM approach” // Informatica. 2019. Vol. 30(1). Pp. 187–211. DOI 10.15388/Informatica.2019.203. EDN BHGEIB.

[19] Koushika A. M., Selvi S. T. "Load balancing using software defined networking in cloud environment" // Recent Trends in Information Technology (ICRTIT). 2014. Int. Conf. IEEE. 2019. DOI 10.1109/ICRTIT.2014.6996164.

[20] Кузьмина Н. А. Системы фиксации и распознавания несанкционированного проникновения в охраняемую зону как элемент эффективной безопасности объекта транспортной инфраструктуры // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 5. С. 47–52. DOI 10.24411/20728735201810086. EDN UUGNBC. [[Kuzmina N. A. “Systems for recording and recognizing unauthorized entry into a protected area as an element of effective security of a transport infrastructure facility” // T-Comm: Telecommunications and Transport. 2018. Vol. 12, no. 5, pp. 47–52. DOI 10.24411/20728735201810086. EDN UUGNBC. (In Russian).]]

Поступила в редакцию 6 марта 2025 г.

МЕТАДАННЫЕ / METADATA

Title Typical problems and ways to solve them when building VPN tunnels based on the backbone network of different providers.

Abstract The article discusses the problems of building a Site-to-Site branch network and ways to solve them when using the IKE (internet key exchange) protocol included in the IPSec stack. A typical topology used at enterprises of the military-industrial complex is built (encryption must comply with GOST 34.12-2018). Tests were carried out on real software and hardware systems of domestic origin. A comparison of traffic flow modes using the IKE v1 and IKE v2 protocols (normal and aggressive modes) was performed, the possibility of operation in conditions with a long response, different values of the Maximum Transmission Unit parameter was determined. The results obtained were confirmed during trial operation in a test environment. Based on the experiments, the main problems of network integration using public key infrastructure (PKI) and methods for solving them were determined. Presumably, the technical solution considered allows achieving stable traffic transmission between sites even in the absence of "gray fiber", which provides traffic delays of less than 1 ms. High speed of operation is confirmed when fulfilling the list of mandatory technical conditions. This provides connectivity between remote sites for normal and aggressive IKE connection modes.

Key words IKE; IPSec; VPN; PKI; Site-to-Site.

Язык статьи / Language Русский / Russian.

Поддержка/Support государственное задание для высших учебных заведений № FEUE-2023-0007.

Об авторах / About the authors:

ЛЮБИМЕНКО Дмитрий Анатольевич
Волгоградский государственный технический университет,
Россия.
Аспирант кафедры систем автоматизированного проектирования и поискового конструирования. Магистр информатики и вычислительной техники (Волгогр. гос. ун-т, 2023). Иссл. в обл. кибербезопасности.
E-mail lubimenko-d@bk.ru

КРАВЕЦ Алла Григорьевна
Волгоградский государственный технический университет,
Россия.
Проф. каф. систем автоматизированного проектирования и поискового конструирования. Д-р техн. наук (Волгоград. гос. ун-т, 2008). Иссл. в обл. искусственного интеллекта и кибербезопасности.
E-mail AllaGKravets@yandex.ru
ORCID https://orcid.org/ 0000-0003-1675-8652

LYUBIMENKO Dmitrij Anatol'evich
Volgograd State Technical University,
Russia.
Master of Computer Science and Engineering (Volgograd State Univ., 2023). He is a postgraduate student of the Dept of Computer-Aided Design and Search Engineering Systems (Volgograd State Techn. Univ., 2025). Research in the field of cybersecurity.
E-mail lubimenko-d@bk.ru

KRAVEC Alla Grigor'evna
Volgograd State Technical University,
Russia.
Prof., Department of Computer-Aided Design and Search Engineering. Doctor of Technical Sciences (Volgograd State University, 2008). Research in the field of artificial intelligence and cybersecurity.
E-mail AllaGKravets@yandex.ru
ORCID https://orcid.org/ 0000-0003-1675-8652