ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА"

Факультет инфокоммуникационных сетей и систем

Кафедра программной инженерии и вычислительной техники

ОТЧЁТ О

НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

Вариант №12

Выполнил:

студент 3 курса

группы ИКПИ-11

Крылов Артём Вячеславович

Принял:  
кандидат технических наук,

доцент кафедры ПИиВТ

Журавель Евгений Павлович

\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург

2024 год

Содержание

[Введение 3](#__RefHeading___Toc894_3576477318)

[Обзор научных статей 4](#__RefHeading___Toc896_3576477318)

[Проектирование двухканального общего GRE через IPSec VPN в сетях P2MP 4](#__RefHeading___Toc896_3576477318_Copy_1)

[Исследование и применение зашифрованной передачи данных на основе IPSec. 7](#__RefHeading___Toc898_3576477318)

[Отслеживание IP-адресов за VPN/прокси-серверами 9](#__RefHeading___Toc900_3576477318)

[Методы двустороннего применения политики качества обслуживания в динамически формируемых наложенных виртуальных частных сетях 12](#__RefHeading___Toc902_3576477318)

[Использование IPSec VPN для защиты сетевых коммуникаций в умной сети 15](#__RefHeading___Toc904_3576477318)

[Заключение 18](#__RefHeading___Toc906_3576477318)

[Список использованных источников 19](#__RefHeading___Toc908_3576477318)

# **Введение**

Виртуальная частная сеть на 3 уровне ЭМВОС (**Layer 3 Virtual Private Network**, L3VPN), также известная как маршрутизируемый VPN, является типом виртуальной частной сети, которая работает на сетевом уровне модели OSI. Она использует IP-маршрутизацию и обеспечивает безопасную и эффективную передачу данных между серверами, расположенными в различных локациях через общедоступные или частные сети. Отличительная черта L3VPN — возможность интеграции разнообразных сетевых ресурсов и услуг на уровне IP.

Задачи исследования в области L3VPN включают в себя:

1. **Исследование архитектуры и протоколов**: В данной области проводится всестороннее исследование различных моделей построения L3VPN. Используются BGP, MPLS, IPSec, а также протоколы маршрутизации OSPF, IS-IS, EIGRP. Изучаются механизмы разделения виртуальных маршрутных таблиц (VRF) и процессы управления ими на маршрутизаторах провайдера.
2. **Оптимизация управления трафиком**: Этот аспект исследований включает разработку алгоритмов маршрутизации и управления ресурсами сети с использованием VPN. Цель состоит в повышении производительности, надежности и безопасности сетевых соединений путём оптимизации маршрутов и распределения нагрузки в сети.
3. **Поддержка новых сервисов и технологий**: Исследования в этой области направлены на обеспечение совместимости и эффективного взаимодействия виртуальных частных сетей с новыми технологиями, такими как облачные вычисления, виртуализация, программно-определяемые сети (SDN) и виртуальные сетевые функции (NFV).
4. **Исследование проблем безопасности**: В данной области исследуются уязвимости сетевой инфраструктуры, а также разрабатываются методы защиты от них. Для безопасной работы L3VPN важно обеспечить надёжную идентификацию пользователей и филиалов, контролировать их доступ, а также защищать передаваемые данные от несанкционированного доступа.

Цель данного отчёта состоит в ознакомлении с актуальными направлениями исследований в области виртуальных частных сетей, выявлениями основных проблем и трудностей, а также представлении возможных путей их решения.

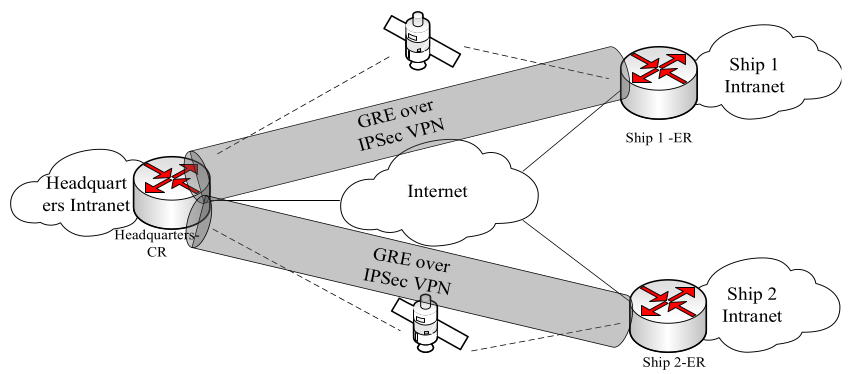
# **Обзор научных статей**

## **Проектирование двухканального общего GRE через IPSec VPN в сетях P2MP**

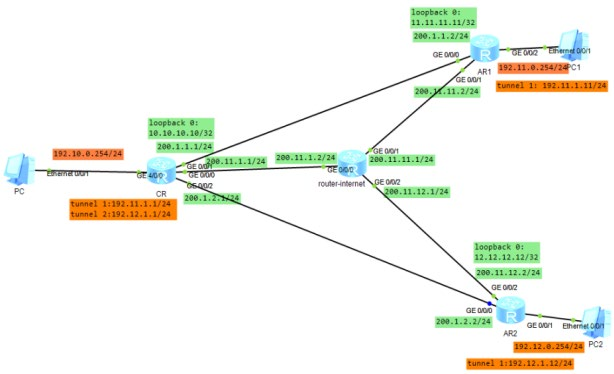
В статье [1] рассматривается проблема огранизации безопасной связи между головным офисом и несколькими филиалами предприятия. Авторы статьи предлагают дизайн двухканального общего GRE через IPSec VPN в сети P2MP (point-to-multipoint, точка-многоточка), чтобы обеспечить безопасный канал для одноадресной и многоадресной передачи данных как для двусторонней, так и для односторонней связи.

Для предотвращения прослушивания или взлома связи между головным офисом и филиалами могут использоваться выделенные линии, обеспечивающие безопасность содержания связи. Однако использование выделенных линий является дорогостоящим и недоступным для большого числа компаний, а если связь осуществляется через Интернет, который представляет собой прозрачную и открытую среду, могут возникнуть риски для безопасности связи. Кроме того, связь посредством беспроводных каналов, например, между кораблями или между сушей и кораблями, также находится в открытом и трудноконтролируемом состоянии. Технология IPSec (IP Security) VPN может решить текущую дилемму, независимо от того, передаётся ли она через Интернет или по беспроводным каналам. IPSec предоставляет услуги безопасности данных на уровне IP, предотвращая подделку и перехват IP-пакетов с помощью алгоритмов аутентификации и шифрования. Однако у IPSec есть и некоторые недостатки. Например, большое количество операций потребляют сетевые ресурсы, увеличивают задержку передачи данных, что не способствует передаче услуг с жесткими требованиями реального времени. Кроме того, IPsec предоставляет только услуги безопасности «точка-точка» и не поддерживает многоадресную рассылку.

Модель, использованная в статье [1], представляет собой P2MP сеть судоходной компании, в которой наземный штаб должен поддерживать связь с каждым из двух грузовых судов. Как показано на рис. 1, между штаб-квартирой и каждым судном существует два канала связи, один из которых спутниковая связь во время плавания судна, еще один — доступ в Интернет по оптоволоконному кабелю, когда судно находится в порту. Оба канала открыты и небезопасны, поэтому между штаб-квартирой и каждым судном необходимо установить соединение GRE через IPSec VPN, чтобы обеспечить безопасность одноадресной и многоадресной связи.

*Рис. 1. Проектирование двухканального общего GRE через IPSec VPN в сети P2MP*

Для экспериментальной проверки используется платформа моделирования Huawei eNSP. Экспериментальная топология показана на рисунке 2. Прямое соединение выходного маршрутизатора представляет собой канал спутниковой связи, а «маршрутизатор-Интернет» представляет собой Интернет. Туннель IPSec устанавливается с использованием ESP, туннельного режима, автоматического согласования IKE (двусторонняя связь) или ручной настройки (односторонняя связь).



*Рис. 2 Экспериментальная топология*

В заключении авторы статьи [1] подводят итоги исследования и обсуждают его значимость. Предложенное применение технологии туннелирования GRE через IPSec к сети P2MP на основе многоканального совместного использования между сторонами связи позволяет обеспечить безопасную связь «один ко многим» без снижения надежности каналов связи.

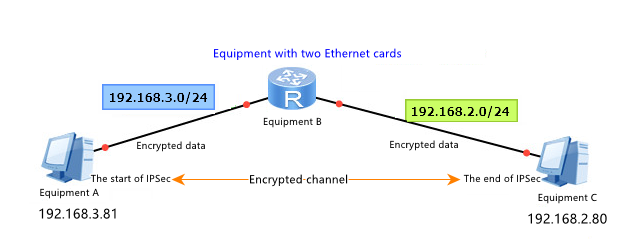
## **Исследование и применение зашифрованной передачи данных на основе IPSec**

В статье [2] рассматривается проблема безопасности передачи данных между сетями. В замен использования алгоритмов шифрования, таких как RSA и AES, авторы предлагают установить собственный зашифрованный канал на стороне отправки и получения данных. Благодаря зашифрованному каналу может быть гарантирована безопасность передачи данных, даже если они проходят через несколько устройств в среде Интернета.

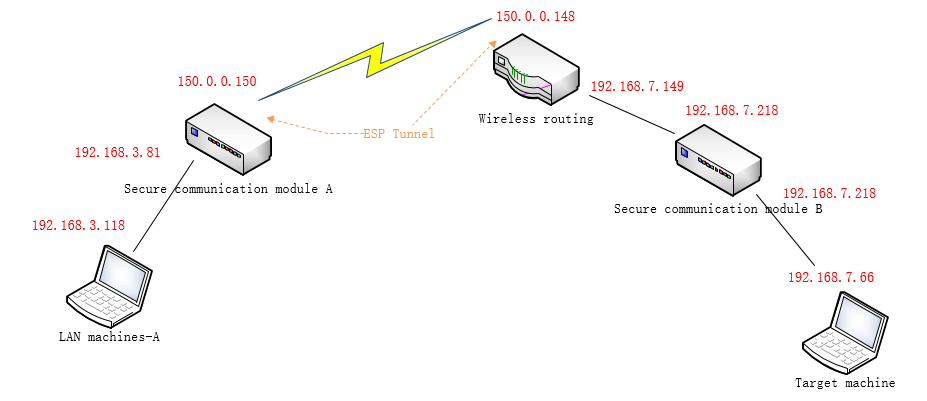
В современную эпоху популяризации Интернета концепция информационной безопасности привлекает все больше внимания. Обеспечение безопасной передачи данных на целевое устройство среди большого количества интернет-устройств — это новая задача. Люди предлагают и разрабатывают новые технологии, структуры и даже протоколы для постоянного удовлетворения соответствующих потребностей в безопасности. В действительности сообщения между устройствами передаются через сетевые кабели и множество промежуточных узлов (включая, помимо прочего, коммутаторы, маршрутизаторы, межсетевые экраны и другие устройства), прежде чем они наконец достигнут целевой сети. Эти устройства необходимы для точной передачи данных по адресу назначения, но в то же время они представляют собой серьёзную угрозу утечки данных. Если во время передачи данных возникнут такие проблемы, как потеря пакетов данных, подделка или утечка данных, то это создаст угрозу безопасности. Обычный способ обеспечить безопасность данных — зашифровать и затем передать их. Однако если все данные зашифрованы, объём информации будет очень большим. Кроме того, шифрование и дешифрование займут много времени, что серьёзно повлияет на пользовательский опыт.

В статье [2] авторы предлагают решить эту проблему с помощью другого подхода: вместо использования зашифрованных данных происходит попытка установить зашифрованный канал на сетевом уровне. Данный подход практически не влияет на работу пользователя и обеспечивает шифрованную передачу данных без снижения скорости передачи, что значительно снижает риск незаконной кражи данных.

Работа IPSec рассмотрена на примере модели, показанной на рисунке 3. Устройство A в сегменте сети слева должно связаться с устройством C в сегменте сети справа. Поскольку задействованы разные сегменты сети, требуется переход к маршрутизации с использованием устройства B.

*Рис. 3. Топология сети устройства A и устройства C с использованием IPSec*

В дополение к вышеупомянутой модели авторы статьи [2] приводят пример использования IPSec с технологией NAT.

*Рис. 4. Схема топологии сети с использованием NAT*

В заключении статьи [2] авторы подводят итоги, подчёркивая преимущества предложенного ими способа передачи данных. Введение туннельного режима IPSec показывает, что данная технология может эффективно гарантировать безопасность данных без значительного снижения скорости их передачи.

## **Отслеживание IP-адресов за VPN/прокси-серверами**

В статье [3] рассматривается многоуровневый механизм обнаружения истинной идентичности интернет-злоумышленников, использующих VPN и прокси-сервера для достижения корыстных целей.

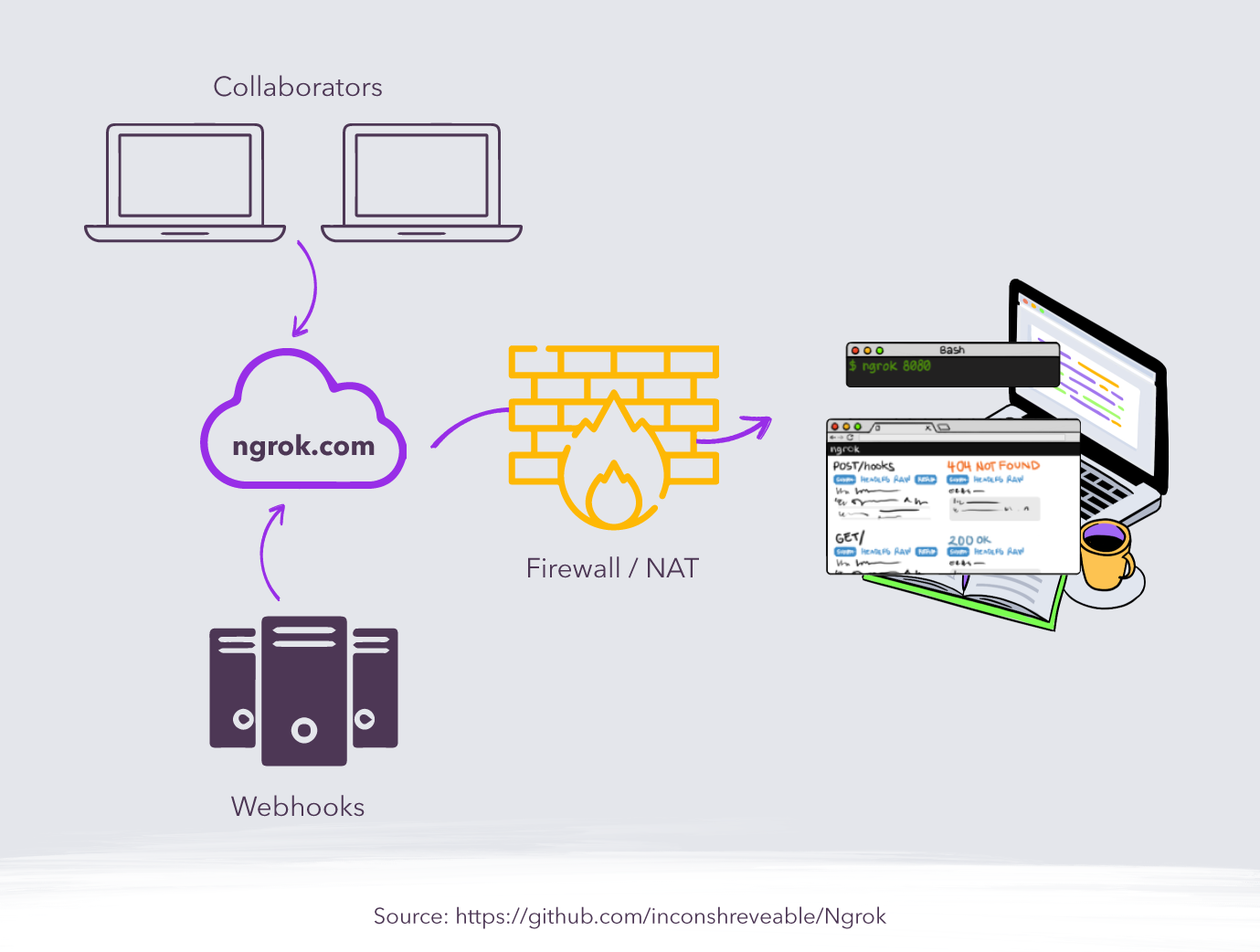
Виртуальная частная сеть (VPN) и прокси - два популярных инструмента, используемых для безопасного и анонимного доступа в Интернет. VPN - это сетевая технология, которая создает частное и зашифрованное соединение между устройством пользователя и VPN-сервером, обеспечивая анонимность и защиту от онлайн-угроз. С другой стороны, прокси-сервер действует как посредник между устройством пользователя и Интернетом, позволяя пользователям анонимно получать доступ к веб-сайтам и службам, скрывая свой IP-адрес. И VPN, и прокси-серверы имеют свои уникальные функции и преимущества. VPN обеспечивают лучшую безопасность и конфиденциальность, тогда как прокси-серверы настраиваются быстрее и проще. Кроме того, VPN позволяют пользователям получать доступ к заблокированным веб-сайтам и сервисам в определенных странах, а прокси-серверы предоставляют простой способ обойти фильтры веб-сайтов и брандмауэры. В конечном счёте, выбор между VPN и прокси-серверами зависит от конкретных потребностей и предпочтений пользователя, а также от желаемого уровня безопасности и анонимности.

Конфиденциальность в Интернете становится все труднее и труднее поддерживать. По этой причине люди используют VPN, которые отлично защищают своих пользователей от онлайн-слежения, шпионажа, сбора данных и навязчивой рекламы. Киберпреступники будут использовать прокси-сервисы для сокрытия своего настоящего IP-адреса и проведения мошеннических транзакций. Задача состоит в том, чтобы найти их и отследить их подлинный IP-адрес. Раскрытие вашей личной информации в Интернете - это самый быстрый способ ее распространения. Вредоносное ПО, файлы cookie или вход в учётные записи - это основные способы, с помощью которых кто-то может узнать, чем вы занимаетесь в Интернете, помимо того факта, что вы используете VPN.

Чтобы скрыть свою личность, хакер использует поддельный IP-адрес, например VPN/прокси. Авторы статьи [3] предлагают побудить пользователя получить доступ к веб-сайту, чтобы, пока пользователь выполняет какие-либо действия на веб-сайте, был сгенерирован токен, содержащий учётные данные пользователя. Существующие проекты используют анализ заголовков пакетов, многочисленные методы создания сценариев и анализ маршрутизации, чтобы выяснить, находится ли пользователь за прокси-сервером или нет. В настоящее время некоторые сайты используют фильтрацию URL-адресов, но, с другой стороны, в развёртываниях фильтрации URL-адресов отсутствуют необходимые функции для полного контроля веб-серфинга и предотвращения угроз.

В статье [3] описывается улучшенный метод, целью которого является постоянное отслеживание злоумышленников, даже если «отпечатки пальцев» браузера со временем меняются. Авторы использовали прототип системы для проверки точности их стратегии, включая второстепенные функции, используя механизмы хранения данных в браузере и разрабатывая алгоритмы корреляции. Согласно экспериментальным результатам, предложенный авторами метод может объединять различные отпечатки пальцев с одной платформы на 24,5% точнее, чем традиционные методы снятия отпечатков пальцев, при выявлении анонимных веб-злоумышленников.

Задача — отслеживать их реальный IP-адрес и местоположение, даже если они используют VPN/прокси. Первым шагом для осуществления этого процесса является веб-хостинг. Создать веб-сайт с использованием HTML и разместить его на сервере с помощью ngrok, чтобы пользователь мог получить к нему доступ. Кроссплатформенная программа под названием ngrok позволяет программистам легко подключить локальный сервер разработки к Интернету. На рис. 5 показан рабочий процесс сервера Ngrok.



*Рис. 5. Работа ngrok*

Заставляя ваш локально размещённый веб-сервер притворяться, что он размещен на субдомене ngrok.com, программное обеспечение устраняет необходимость в общедоступном IP-адресе или доменном имени локального компьютера. Этот локальный сервер предназначен только для тестирования, чтобы узнать, доступен ли веб-сайт через Интернет. Для глобального распространения авторы статьи [3] используют веб-платформу с открытым исходным кодом под названием 000webhostapp, на которой они развернули веб-сайт. 000webhost — это услуга веб-хостинга, которая предлагает владельцам веб-сайтов платформу для бесплатного размещения их веб-сайтов. 000webhost предлагает своим пользователям ряд функций, включая конструктор веб-сайтов, круглосуточную поддержку клиентов и удобную панель управления, которая позволяет легко управлять веб-сайтом. Платформа также предлагает установку в один клик для популярных систем управления контентом (CMS), таких как WordPress, Joomla и Drupal, что позволяет пользователям легко настраивать свои веб-сайты. Кроме того, 000webhost предоставляет своим пользователям 99% времени безотказной работы и высокоскоростные серверы, гарантируя, что веб-сайт всегда доступен для пользователей. Однако, будучи бесплатным сервисом, 000webhost имеет некоторые недостатки, такие как ограниченное пространство для хранения и пропускная способность, а также отсутствие расширенных функций, таких как шифрование SSL. Несмотря на эти ограничения, 000webhost остается популярным вариантом для новичков или тех, кто хочет разместить личный веб-сайт или блог без каких-либо затрат на хостинг. Это также отличный вариант для пользователей, которые хотят протестировать свой веб-сайт или опробовать различные конструкторы веб-сайтов, прежде чем переходить на платный хостинг.

После полного размещения веб-сайта выполняется веб-отслеживание. На сайт вставляется фрагмент XML-кода, позволяющий отслеживать активность пользователей с помощью инструмента-анализатора, такого как Google Analytics. Google Analytics – это платформа под брендом Google для маркетинга, которая измеряет и сообщает о посещаемости веб-сайта. После приобретения Urchin компания Google представила эту услугу в ноябре 2005 года. По состоянию на 2019 год она является наиболее используемым онлайн-сервисом веб-аналитики.

После завершения части процесса, заключающейся в отслеживании местоположения пользователя, следующий шаг — захват «токена-канарейки», чтобы записывать информацию о пользователе после того, как им было выполнено какое-либо действие.

В заключении авторы статьи [3] подводят итоги исследования и предоставляют рекомендацию использовать передовые технологии определения местоположения для борьбы с злоумышленниками.

## **Методы двустороннего применения политики качества обслуживания в динамически формируемых наложенных виртуальных частных сетях**

В статье [4] рассматривается организация внутренней сети крупного предприятия с головным офисом и множеством филиалов. Все сайты подключены к одному и тому же интернет-провайдеру, а MPLS Layer 3 VPN используется для обеспечения IP-маршрутизации между сайтами клиентов.

Современные виртуальные частные сети (VPN) строятся на базе различных соединений «последней мили». Физические скорости передачи данных могут не соответствовать скорости, оговоренной клиентом. Это приводит к падению трафика со стороны поставщика услуг, когда клиент отправляет трафик на линейной скорости. Служба VPN по таким линиям может испытывать прерывания соединения и потерю пакетов и никогда не сходиться в худшем случае. Крупные предприятия одновременно используют несколько VPN-подключений в разных транспортных сетях. Каждая сеть может иметь разные физические свойства и требует отдельной политики качества обслуживания (QoS). Его необходимо настроить в обоих направлениях: от клиента к поставщику услуг и от поставщика услуг к клиенту. Используя оверлейную VPN, клиенты могут настраивать детальные и симметричные политики QoS. Это обеспечивает планирование мощности и хорошее качество опыта. Для FlexVPN, основанного на технологии IKEv2 и IPSec, симметричное качество обслуживания легко достижимо и подходит для крупномасштабных развертываний. Атрибуты могут храниться локально или получаться с внешнего сервера. Для конфигурации, которую необходимо применить вручную к большому количеству сетевых устройств, можно использовать платформу сетевой автоматизации, чтобы ускорить развертывание конфигурации и избежать проблем с неправильной конфигурацией. Nornir — одна из сред автоматизации, которая в настоящее время широко используется для развертывания конфигурации.

Сети передачи данных в настоящее время проектируются с учетом требований быстро развивающегося бизнеса и должны быть высоконадежными, ориентированными на приложения и сервисы. Существует как минимум две точки зрения на сеть передачи данных: поставщик услуг Интернета (ISP) и клиент.

Интернет-провайдер обеспечивает соединение последней мили в соответствии с параметрами, связанными с контрактом, такими как пропускная способность, доступность и другие аспекты соглашения об уровне обслуживания (SLA). Может случиться так, что соединения последней мили, поддерживающие физическую скорость, не соответствуют контракту; например, клиент приобрел у интернет-провайдера соединение с полосой пропускания 200 Мбит/с. Если последней милей будет Ethernet, то необходимо использовать как минимум соединение 1000BASE. Оставленное без присмотра такое соединение открывает интернет-провайдеру возможность нарушения договора со стороны клиента, поскольку он будет иметь доступ к полной скорости линии. Чтобы обеспечить соблюдение контрактной скорости, интернет-провайдер должен настроить базовую политику качества обслуживания (QoS) как для входящего, так и для исходящего трафика. Эта настроенная политика будет служить функцией кондиционирования трафика, сокращая избыточную полосу пропускания и может изменять данные кодовых точек DS для дальнейшей защиты сети поставщика услуг и обеспечения справедливого использования услуг. С точки зрения интернет-провайдера этого достаточно для обеспечения стабильного обслуживания в соответствии с соглашением. При подключении последней мили к сотовой сети могут возникать аналогичные проблемы в зависимости от того, используется ли для подключения внешний сотовый модем или он встроен в маршрутизатор виртуальной частной сети (VPN). При использовании внешнего сотового модема несоответствие скорости передачи данных между поставщиком услуг мобильной связи и внутренним Ethernet-соединением может стать проблемой. В настоящее время соединения по локальной сети (LAN) 1000BASE распространены повсеместно и могут использоваться для подключения сотового модема к локальной сети. Таким образом, клиент сможет отправлять исходящий трафик поставщику услуг на линейной скорости и, возможно, нарушать контрактную скорость передачи данных. Если интернет-провайдер решит отбросить избыточный трафик или сеть перегружена, это приведет к потере пакетов или задержке.

Чтобы обеспечить безопасную связь между сайтами клиентов, к маршрутизатору головного офиса с каждого маршрутизатора сайта филиала клиента создается динамическое наложенное VPN-соединение. Штаб-квартира служит центром VPN, а филиалы — лучами. VPN построен с использованием FlexVPN, поскольку он предлагает множество преимуществ для динамической настройки атрибутов подключения.

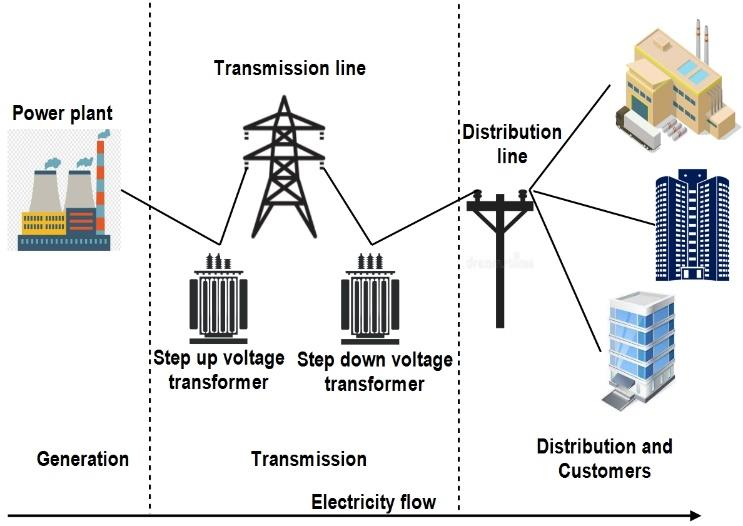
Привязка клиентского трафика к VPN-соединению обеспечивается за счет применения технологии VRF (виртуальная маршрутизация и переадресация). Изоляция трафика гарантирована, и как входящий, так и исходящий трафик должен пересекать VPN-туннель. Это позволяет использовать потуннельное качество обслуживания со стороны штаб-квартиры, а трафик, отправляемый из штаб-квартиры в филиалы, может быть ограничен по скорости, чтобы соответствовать контрактной скорости «последней мили» удалённого сайта, что обеспечивает лучшее качество обслуживания для конечных пользователей. Если каждый филиал имеет разную скорость последней мили, то для каждого ограничения скорости необходимо настроить отдельную политику QoS, а затем применить ее к соответствующему VPN-подключению. Каждый филиал должен иметь уникальный идентификатор, чтобы политика QoS могла быть сопоставлена и применена к динамически формируемому туннелю.

В заключении статьи [4] автор подводит итоги, подчёркивая своё положительное отношение к технологиям FlexVPN и Nornir.

## **Использование IPSec VPN для защиты сетевых коммуникаций в умной сети**

В статье [5] рассматривается применение технологии IPSec в «умных электросетях», использующих информационные и коммуникационные технологии.

Традиционная электрическая сеть состоит из трех частей: сетей генерации, передачи высокого напряжения и распределительных сетей низкого напряжения, как показано на рисунке 6.



*Рис. 6. Инфраструктура традиционной сети*

Производство электроэнергии – это сердцебиение электросети. Электричество вырабатывается в ядре электростанции путем сжигания угля или природного газа. Традиционная электросеть содержит ряд электростанций вдали от населённых пунктов, чтобы защитить их от загрязнения, возникающего в результате производства электроэнергии, например, загрязнения воздуха выбросами углекислого газа и звукового загрязнения. В 2020 году процент выбросов углерода в США от производства электроэнергии достиг 25% от общего объёма выбросов углерода, и ожидается, что этот показатель увеличится в ближайшие годы, если ученые не найдут других решений для производства электроэнергии.

Роль линий электропередачи высокого напряжения заключается в передаче электроэнергии от площадки электростанции к распределительной площадке через трансформаторы. Подстанция содержит трансформаторы, установленные рядом с электростанциями, которые должны повышать напряжение, затем высокое напряжение течёт по линиям, преодолевая большие расстояния, а в конце пути возле места потребления трансформатор снижает напряжение передачи электроэнергии к распределительным линиям низкого напряжения.

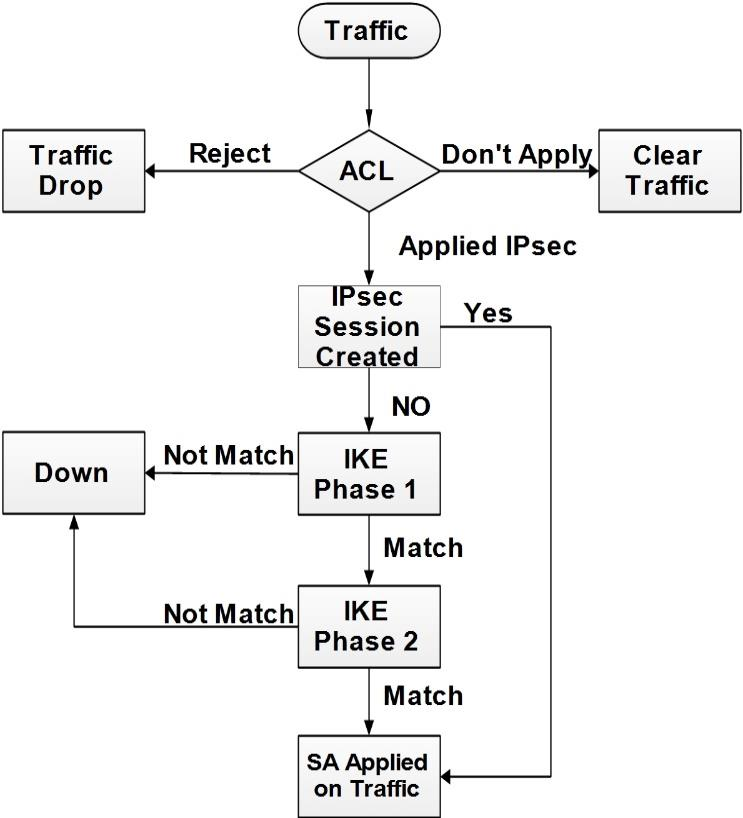
Распределительные линии, поставляющие электроэнергию, имеют низкое напряжение для потребления, и напряжение снижается, когда требуется обслуживание. Распределительные трансформаторы снижают напряжение до уровня, используемого в освещении, промышленном оборудовании, коммерческой и бытовой технике. Линии распределения электроэнергии представляют собой трёхфазные силовые кабели, находящиеся, как правило, на обочинах дорог в городах и деревнях, поскольку эти места находятся ближе всего к потребителю для подачи электроэнергии.

Умная сеть — это новое поколение электросетей, которое можно объединить с классической сетью, чтобы обеспечить поток энергии и связь в обоих направлениях между коммунальными предприятиями и потребителями. Она использует коммуникационные технологии, серверы, компьютеры, Интернет вещей и управляющее программное обеспечение. Анализируя автоматически собираемые данные со всех частей умной электросети, она способствует эффективной и гибкой работе сети при удовлетворении потребностей пользователей в электроэнергии как в пиковое, так и в непиковое время. Чтобы предотвратить перебои в подаче электроэнергии в случае выхода из строя оборудования из-за стихийного бедствия или перебоев по любой другой причине, умная сеть имеет возможность автоматически перенаправлять электроэнергию, чтобы сократить период простоя и повысить гибкость для пострадавшего района.

В умной сети протокол TCP/IP используется для передачи данных между различными доменами или в пределах одного домена. Протокол IP, являющийся частью стека TCP/IP, работает на сетевом уровне, но не обеспечивает никакой защиты при передаче данных. Для решения этой проблемы применяется протокол IPSec, который реализует такие важные аспекты безопасности, как конфиденциальность, целостность, аутентификация и защита от повторного воспроизведения на сетевом уровне стека TCP/IP.

IPSec можно использовать между двумя шлюзами домена умной сети для создания VPN, которая называется VPN типа «сеть-сеть», между шлюзами или брандмауэром и хостом для создания VPN, которая называется VPN удаленного доступа, а также внутри того же домена, например, операционного домена, используемого для создания VPN между серверами и терминалами операторов для защиты небезопасного соединения, такого как Telnet.

Пакет обмена ключами в Интернете (IKE) используется для создания IPSec VPN в два этапа, как показано на рис. 7. Первый этап называется IKE 1 и отвечает за согласование управления между двумя узлами для аутентификации друг друга и создания защищенного туннеля. Фаза 2 IKE отвечает за создание туннеля IPsec в туннеле фазы 1 IKE для передачи согласованных данных и обеспечения согласования параметров безопасности, таких как протоколы шифрования, хеширования и аутентификации. Эти параметры называются ассоциацией безопасности (SA).



*Рис. 7. Фазы IKE согласовываются*

Пакет IKE отвечает за создание туннелей и не обеспечивает шифрование данных и аутентификацию узлов. Для выполнения этих задач используются протоколы заголовка аутентификации (AH) и инкапсулирующей полезной нагрузки безопасности (ESP). AH обеспечивает аутентификацию и целостность, но ESP обеспечивает аутентификацию, целостность, а также шифрование в качестве дополнительной функции.

В заключении статьи [5] автор подводит итоги исследования и обсуждает его значимость. Информация, передаваемая между частями умной сети, должна быть безопасной, чтобы защитить сеть от любых атак. IPSec VPN обеспечивает эту цель посредством шифрования, проверки целостности отправленных сообщений и аутентификации узлов перед любым соединением.

# **Заключение**

Статья [1] рассматривает проблему организации безопасной связи в предприятии. Предложенное применение технологии туннелирования GRE через IPSec к сети P2MP на основе многоканального совместного использования между сторонами связи позволяет обеспечить безопасную связь «один ко многим» без снижения надежности каналов связи.

Статья [2] поднимает вопрос безопасности передачи данных между сетями. Введение туннельного режима IPSec показывает, что данная технология может эффективно гарантировать безопасность данных без значительного снижения скорости их передачи.

Статья [3] исследует многоуровневый механизм обнаружения истинной идентичности интернет-злоумышленников. Предложенный способ позволяет отслеживать их реальный IP-адрес и местоположение, даже если они используют VPN/прокси.

В статье [4] рассматривается организация внутренней сети крупного предприятия с головным офисом и множеством филиалов. Разработанное решение использует Nornir и FlexVPN.

В завершение, статья [5] затрагивает применение технологии IPSec в «умных электросетях». IPsec VPN обеспечивает безопасную передачу информации посредством шифрования, проверки целостности отправленных сообщений и аутентификации узлов перед любым соединением.

Текущее состояние исследований в области L3VPN указывает на значительный прогресс в разработке инструментов управления и защиты сетей. Однако, с учетом динамичного характера цифровых технологий, дальнейшее развитие направления требует постоянного совершенствования методов и алгоритмов, а также активного внедрения результатов исследований в практику. Перспективы дальнейшего развития L3VPN включают в себя углубление исследований в области безопасности и оптимизации управления трафиком.

# **Список использованных источников**

1. W. He, Y. Zhao, Z. Liu, Q. Li, B. Yu and H. Zhang, "Design of Dual-link Shared GRE over IPSec VPN on P2MP Networks," 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA), Shenyang, China, 2023, pp. 1781-1783, doi: 10.1109/ICPECA56706.2023.10075987.
2. S. Qu, Y. Cheng and X. Bai, "Research and application of encrypted data transmission based on IPSec," 2023 IEEE 3rd International Conference on Data Science and Computer Application (ICDSCA), Dalian, China, 2023, pp. 348-352, doi: 10.1109/ICDSCA59871.2023.10393329.
3. T. Nithesh Aravind, A. Mukundh and R. Vijayakumar, "Tracing Ip Addresses Behind Vpn/Proxy Servers," 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 2023, pp. 1-10, doi: 10.1109/ICNWC57852.2023.10127335.
4. I. Meijers, "Two-Way Quality of Service Policy Enforcement Methods in Dynamically Formed Overlay Virtual Private Networks," 2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, 2023, pp. 1-4, doi: 10.1109/ITMS59786.2023.10317738.
5. M. H. A. Hamied, "Using an IPsec VPN to Secure The Network Communication in The Smart Grid," 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 2023, pp. 1-5, doi: 10.1109/ICAISC56366.2023.10085145.