***Д. Е. Волков, А. М. Шабалин***
*Тюменский государственный университет, г. Тюмень*
**УДК 004.94**

# ОРГАНИЗАЦИЯ ЗАЩИЩЕННЫХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ СРЕДСТВАМИ АВТОМАТИЗАЦИИ В КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

**Аннотация.** В работе было проанализировано текущее состояние рынка сетевых устройств на корпоративном уровне, выбрана технология виртуальной частной сети с достаточной совместимостью, а также разработана технология автоматизации настройки сетевого оборудования. Результатом исследования стала разработка методики настройки защищенной корпоративной виртуальной сети на устройствах различных вендоров средствами современных решений автоматизации.

**Ключевые слова:** VPN, автоматизация, Cisco, Eltex, DMVPN, IPsec, VyOS, Ansible.

**Введение.** С 2022 года с российского рынка сетевых устройств начали уходить популярные зарубежные вендоры [1, 2]. Крупные корпорации с большим количеством филиалов потеряли возможность закупать оборудование одного вендора, чтобы продолжать масштабироваться. Возникла необходимость в смене оборудования, поскольку перспектива закупки устройств с наценкой от посредника без гарантии сервисного обслуживания может быть очень не выгодной. Замена всего сетевого оборудования является наихудшим вариантом для работоспособности действующей сети, поэтому компаниям приходится искать альтернативы, которые можно совместить с уже работающими решениями [3]. Кроме того, нужно поддерживать технологии безопасной передачи данных в виртуальных частных сетях (virtual private network, VPN) [4, 5], которые можно реализовать как на новом оборудовании, так и на имеющемся.

**Проблема исследования.** Проблемой является исследование технологий, позволяющих внедрить новое сетевое оборудование в существующую корпоративную сеть, а также возможности минимизация временных затрат на настройку сетевого оборудования средствами автоматизации. В ходе работы решался ряд задач:

1) сравнить доступные технологии для организации защищенных каналов передачи данных в сети средствами отечественного коммуникационного оборудования;
2) разработать алгоритм настройки защищенных каналов передачи на выбранном оборудовании;
3) разработать набор скриптов автоматизации, упрощающих настройку каналов передачи данных;
4) смоделировать корпоративную сеть компании в виртуальной среде;
5) апробировать алгоритм настройки защищенных каналов передачи.

**Материалы и методы.** Методами исследования являются анализ, изучение, моделирование. Апробация проводилась на виртуальных образах сетевого оборудования с использованием системы оркестрации EVE NG.

**Результаты.** Так как существуют различные способы создания защищенных каналов передачи данных для виртуальных частных сетей, был проведен сравнительно-сопоставительный анализ некоторых популярных технологий (см. табл. 1), при котором рассматривались те, которые обеспечивают безопасность и не требуют стороннего программного или аппаратного обеспечения.

Наиболее важными критериями сравнения являются поддержка технологии оборудованием различных вендоров и возможность настройки нового узла без изменения конфигурации других устройств. В результате анализа явными лидерами можно считать технологии от Cisco: DMVPN и FlexVPN. Однако и у них выявлены различия: FlexVPN, хоть и основан на открытых протоколах IPsec и GRE и даже поддерживается открытой операционной системой VyOS, имеет свои ограничения: в качестве сервера может быть использовано только оборудование Cisco. Кроме того, у отечественного оборудования Eltex нет поддержки технологии FlexVPN. Следовательно, чтобы воспользоваться всеми преимуществами этой технологии, нужно ограничить себя маршрутизаторами Cisco. DMVPN же не уступает FlexVPN в топологии с сетевыми устройствами от различных вендоров, но кроме того, в роли hub сможет выступать любое устройство, поддерживающее данную технологию.

По результатам сравнительного анализа была выбрана для апробации технология DMVPN.

*Таблица 1*

**Сравнение технологий виртуальных частных сетей**

| *Защищенный VPN* | *Протоколы* | *Подключение клиента без настройки сервера* | *Автоматические туннели между клиентами* |
|---|---|---|---|
| GRE over IPsec | GRE, IPsec | Нет | Нет |
| IPsec / VTI | IPsec, VTI | Нет | Нет |
| DMVPN + IPsec | GRE, NHRP, IPsec | Да | Да |
| FlexVPN | IPsec IKEv2, VTI, FlexVPN | Да | При использовании NHRP |

Для реализации технологии DMVPN требуется следующий стек протоколов:

1) Next Hop Resolution Protocol (NHRP) — разрешение следующего перехода до клиентского маршрутизатора;

2) Generic Routing Encapsulation (GRE) — построение туннелей;

3) динамическая маршрутизация.

В качестве протокола маршрутизации могут быть использованы OSPF, EIGRP и BGP. Протокол EIGRP может быть реализован только на оборудовании Cisco. OSPF и BGP — открытые решения, которые могут работать на оборудовании различных вендоров, но в сочетании с протоколом NHRP, который является основой технологии DMVPN, для построения динамических туннелей функционально более подходит протокол BGP.

Поскольку протокол GRE не обеспечивает защиты передаваемой в туннеле информации, то такие данные могут быть перехвачены, и для обеспечения безопасности используется дополнительная защита в виде протокола IPsec, отвечающего за шифрование данных.

Следовательно, нами для моделируемой корпоративной сети было выбрано оборудование компании Cisco, так как оно является одним из наиболее самых распространенных на территории России и оборудование Eltex, как самое перспективное в настоящее время на отечественном рынке, а также — операционная система Vyos в качестве маршрутизатора, поскольку она распространяется в свободном доступе и имеет открытый код, а значит, является вполне приемлемой альтернативой маршрутизатору для небольшого филиала корпоративной

сети. Перечисленное выше аппаратное и программное обеспечение обладает поддержкой протоколов NHRP, mGRE, IPsec, BGP, что позволяет реализовать технологию DMVPN на этих устройствах.

Были изучены принципы настройки этих протоколов на выбранном оборудовании, на основе которых впоследствии была разработана методика настройки технологии DMVPN, включающая в себя способы настройки протоколов NHRP, mGRE, BGP для обеспечения связности между оборудованием различных вендоров и IPsec для обеспечения защиты передаваемых данных.

Используя систему оркестрации EVE NG, нами была создана сетевая топология (рис. 1), моделирующая реальную сеть крупной компании с филиалами, соединенными между собой через Интернет. В топологии есть один филиал с маршрутизатором Cisco на границе, другой филиал с маршрутизатором Eltex, а также небольшой филиал с сервером Vyos в роли пограничного маршрутизатора.

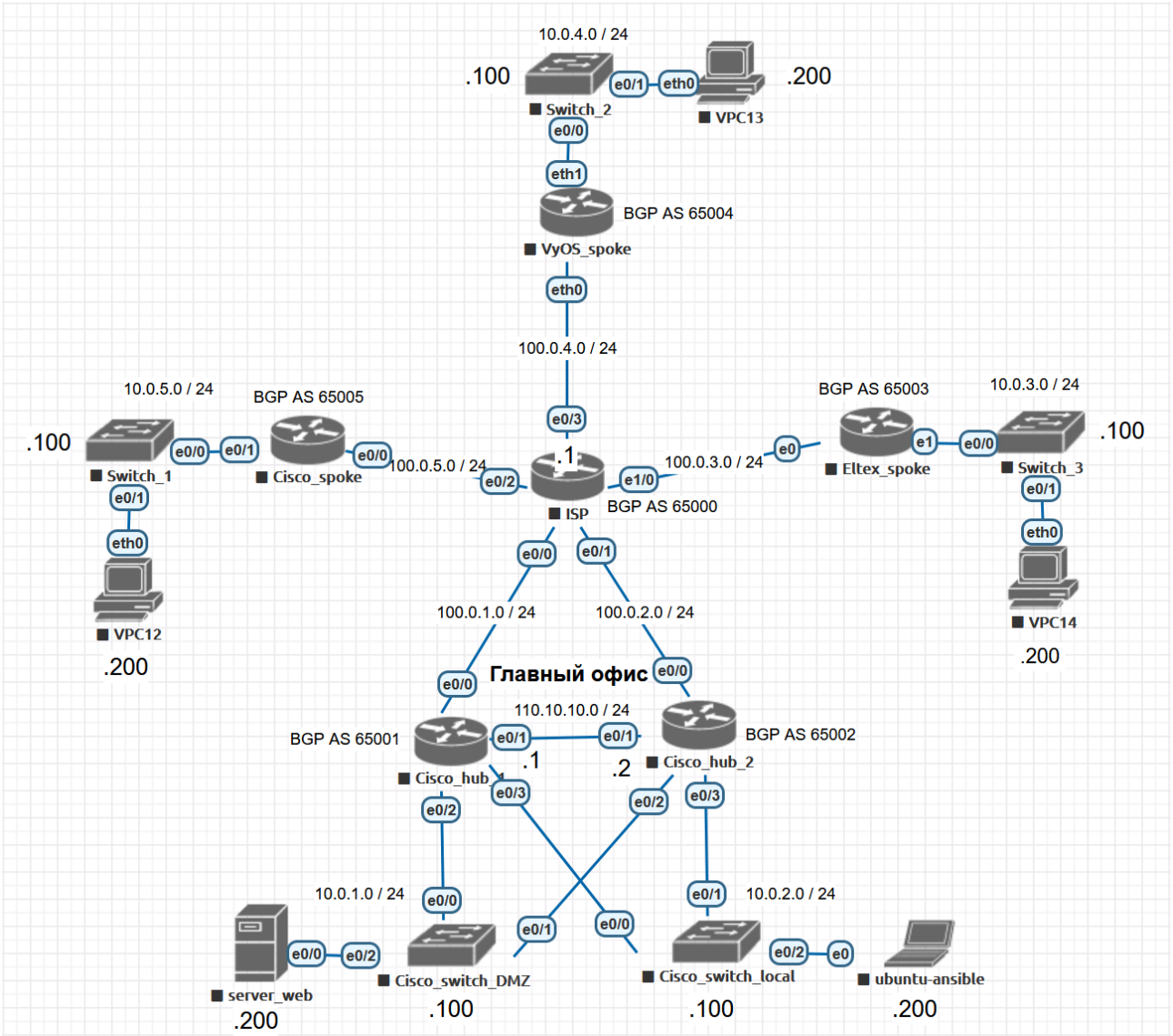


*Рис. 1.* Логическая топология сети нескольких филиалов

На представленной топологии была апробирована методика создания сети DMVPN, в результате чего она показала себя перспективной для потенциального внедрения.

На основе данной методики были разработаны ansible-скрипты, позволяющие автоматически настроить подключение к виртуальной сети DMVPN и вносить крупные изменения в конфигурацию массива сетевых устройств. Для их работы достаточно иметь SSH-подключение и настроить переменные для конфигурируемых устройств, после чего Ansible сможет отправить на маршрутизатор конфигурационные файлы, которые настроят необходимые протоколы и создадут защищенный канал до центрального узла. Нами были написаны 3 сценария (playbook) для подключения к корпоративной сети в роли spoke-маршрутизаторов Cisco, Eltex и VyOS соответственно. Такая автоматизация конфигурации скриптами помогает решить ряд проблем:

- избежать задержки в работе сети во время обновления конфигурации оборудования;
- исправить ошибки при конфигурации;
- уменьшить объем однотипной работы сетевого администратора.

**Заключение.** Таким образом, в процессе исследования нами были изучены принципы настройки протоколов технологии DMVPN на различном оборудовании, что позволило организовать защищенные каналы связи в корпоративной сети средствами современных технологий VPN, совместимых с оборудованием различных вендоров, а также разработать набор Ansible-скриптов, который позволяет минимизировать временные затраты на настройку сетевого оборудования и свести к минимуму ошибки в уже работающей корпоративной сети.

**СПИСОК ЛИТЕРАТУРЫ**


1. Суслов Н.С. Импортозамещение на примере ERP системы: нюансы, задачи и подходы / Н.С. Суслов, А.М. Хафизов // Информационные технологии. Проблемы и решения. — 2023. — № 4 (25). — С. 18-21. — EDN DIXRJQ. URL: https://elibrary.ru/item.asp?id=55925346.
2. Ковпотина Е.А. Направления и методы защиты информации для бизнеса в условиях санкций / Е.А. Ковпотина, П.С. Мороз // Современные проблемы науки и образования: Материалы VIII ежегодной международной научно-практической конференции, Ессентуки, 28 декабря 2022 года. — Ессентуки: Ессентукский институт управления, бизнеса и права, 2022. — С. 159-168. — EDN YGQETY. — URL: https://elibrary.ru/item.asp?id=50744979.
3. Петрова К.С. Россия и путь к безопасному Интернету / К.С. Петрова, С.Ю. Землянская // Наука, образование, транспорт: актуальные вопросы, приоритеты, векторы взаимодействия: Материалы II Международной научно-методической конференции: в 3 ч. Оренбург, 08-09 ноября 2023 г. — Оренбург: Самарский государственный университет путей сообщения, 2023. — С. 80-84. — EDN KESPJO. — URL: https://elibrary.ru/item.asp?id=60028051.
4. Pshenitsyna, E. I. Real and virtual computer networks as a factor of causally sustainable competitiveness of modern companies / E. I. Pshenitsyna, A. V. Sigarev // Мировая экономика: проблемы безопасности. — 2018. — No. 1. — P. 76-81. — EDN YUYWJO. URL: https://elibrary.ru/item.asp?id= 32747721.
5. Бабушкин, Н. С. Необходимость компьютерной безопасности в корпоративной сети / Н. С. Бабушкин // Евразийский научный журнал. — 2017. — № 5. — С. 202-203. — EDN YUAJER. URL: https://elibrary.ru/item.asp?id=29429875.