***А. Л. Петченко, А. М. Шабалин***
*Тюменский государственный университет, г. Тюмень*
**УДК 004.732**

# ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ В КОМПЬЮТЕРНОЙ СЕТИ СРЕДСТВАМИ РЕШЕНИЙ OPEN SOURCE

**Аннотация.** В статье рассмотрена возможность применения Open Source решений для организации безопасной маршрутизации протокола EIGRP. Представлено сравнение различных программных пакетов для осуществления маршрутизации. Проверена совместимость с устройствами Cisco с целью возможной миграции. В результате проведенной работы построен виртуальный стенд на платформе GNS3 с настроенными конфигурациями для каждого устройства.
**Ключевые слова:** EIGRP, Cisco, FRR, Open Source-маршрутизация.

**Введение.** В связи с уходом крупных вендоров из России, в том числе и компании Cisco, появилась проблема замены импортного программного обеспечения и сетевых операционных систем. И здесь могут помочь решения Open Source [1].

В последние несколько лет наблюдается тенденция роста использования программного обеспечения с открытым исходным кодом. И, исходя из отчета Red Hat 2022 года [2], в ближайшие несколько лет данная тенденция сохранится. При сравнении Open Source-продуктов с проприетарным программным обеспечением можно выделить следующие преимущества: низкая стоимость, отсутствие лишнего функционала и зависимости от поставщика оборудования.

С целью борьбы с вредоносной сетевой активностью обычно применяются прокси-серверы, межсетевые экраны, системы обнаружения вторжений и так далее [3]. Установлено, что данные средства защиты могут быть применимы в компьютерной сети, но при этом не менее важна защита самого процесса маршрутизации [4].

Для повышения уровня безопасности применяют аутентификацию, шифрование, пассивные интерфейсы, списки контроля доступа и т. д. [5].

**Проблема исследования.** Для реализации безопасной маршрутизации проприетарного протокола Cisco EIGRP с применением программного обеспечения Open Source были поставлены следующие задачи:

- изучить угрозы и способы защиты, характерные для маршрутизации динамического протокола;
- выявить решения Open Source, способные осуществлять маршрутизацию по протоколу EIGRP;
- разработать алгоритм настройки безопасной маршрутизации, используя программное обеспечение с открытым исходным кодом;
- реализовать разработанный алгоритм в виде виртуального стенда и проверить совместимость Open Source с решениями Cisco.

**Материалы и методы.** Методами данного исследования стали наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для построения модели компьютерной среды было выбрано программное средство GNS3 2.2.31.

**Результаты.** При работе с маршрутизаторами выделяют три плоскости, безопасность которых необходимо обеспечить:

- management plane — трафик, который генерирует администратор, когда осуществляет настройку и мониторинг устройства;
- control plane — трафик, принадлежащий устройству;
- data plane — пользовательский трафик, проходящий через устройство.

В данной статье наше внимание акцентируется защите control plane, с помощью которого осуществляется маршрутизация в компьютерной сети.

Основными угрозами при работе динамического протокола маршрутизации являются спуффинг, анализ трафика и фальсификация данных, хранящихся в таблице маршрутизации. Для защиты от подобного рода атак на тупиковых сетях применяются пассивные интерфейсы и списки контроля доступа. При защите транзитных областей используется концепция доверия и шифрования трафика, а также различные виды аутентификации, где самым надежным считается аутентификация key-chain.

Помимо этого, для увеличения уровня защищенности применяют технологию VRF, благодаря которой, например, можно изолировать административный и транзитный трафики, проходящие через маршрутизатор.

Среди программных продуктов Open Source, способных осуществлять маршрутизацию, можно выделить FRRouting (форк Quagga) [6], Bird, Gobgp и Openbgpd.

Gobgp и Openbgpd — это сервисы, способные обеспечить работу BGP-маршрутизации, но, исходя из исследований бывшего сетевого инженера AWS Джастина Питча [7], они очень уступают по многим параметрам своим аналогам. FRR и Bird во многом схожи, однако есть и отличия. Bird имеет более функциональный сервис, FRR же реализует большее количество протоколов маршрутизации, в том числе поддерживает EIGRP. Также FRR, в отличие от Bird, имеет Cisco-подобную командную строку.

Таким образом, для данной работы была использована операционная система Debian 11.6 с установленным на ней пакетом FRRouting 7.5.1.

Для реализации базовых настроек EIGRP была спроектирована топология сети (рис. 1), включающая в себя два маршрутизатора Cisco и две виртуальные машины Debian с установленным на них пакетом FRRouting.

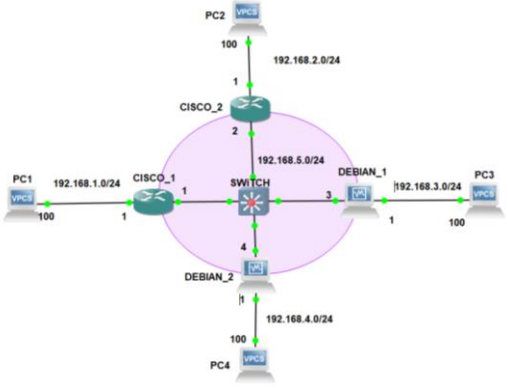


*Рис. 1.* Топология сети

На всех устройствах был настроен протокол EIGRP с аутентификацией key-chain, установлены пассивные интерфейсы на тупиковые сети и реализована изоляция трафика EIGRP посредством технологии VRF. Пример конфигурации на виртуальной машине Debian_1 представлен на рис. 2.

В результате выполненных настроек было установлено EIGRP-соседство между всеми устройствами (рис. 3).

```
debian(config)# do sh running-config
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname debian
no ipv6 forwarding
service integrated-vtysh-config
!
key chain keys
 key 1
  key-string cisco
 exit
!
interface enp0s3 vrf vrf_eigrp
 ip address 192.168.5.3/24
 ip authentication key-chain eigrp 1 keys
 ip authentication mode eigrp 1 md5
!
interface enp0s8 vrf vrf_eigrp
 ip address 192.168.3.1/24
!
router eigrp 1 vrf vrf_eigrp
 eigrp router-id 2.2.2.2
 passive-interface enp0s8
 network 192.168.5.0/24
 network 192.168.3.0/24
!
line vty
!
end
debian(config)# _
```

*Рис. 2.* Конфигурация debian_1

```
cisco_1(config)#do sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
2   192.168.5.3             Et0/0                    13 00:00:51    1  5000  1  0
1   192.168.5.4             Et0/0                    11 00:00:53    1  5000  1  0
0   192.168.5.2             Et0/0                    14 00:00:53   16   100  0  11
```

*Рис. 3.* EIGRP-соседство на устройстве debian_1

**Заключение.** В результате проведенной работы были рассмотрены угрозы для протоколов динамической маршрутизации и возможности защиты от этих угроз; найдены решения, позволяющие реализовать работу динамического протокола маршрутизации EIGRP; обеспечена реализация и защита данного протокола, а также проверена совместимость работы решений Open Source с решениями Cisco с целью возможной последующей миграции.

## СПИСОК ЛИТЕРАТУРЫ


1. Бережной А. Особенности перехода на бесплатные решения Open Source / А. Бережной // Системный администратор. — 2012. — № 1-2(110-111). — С. 38-42. — EDN RFVIKN.
2. The State of Enterprise Open Source: A Red Hat report. — Текст : электронный // redhat.com : [сайт]. — URL: https://www.redhat.com/en/resources/state-of-enterprise-open-source-report-2022 (дата обращения: 29.04.2023).
3. Смирнов В. М. Состояние и тренды сетевой безопасности / В. М. Смирнов, Я. В. Цыганкова, И. А. Нестеров // Евразийский союз ученых. — 2019. — № 9-2(66). — С. 42-43. — EDN IYPIWL.
4. Дубенко К. И. Статические и динамические методы маршрутизации / К. И. Дубенко // Наука, образование и культура. — 2018. — № 10(34). — С. 9-11. — EDN YSGECL.
5. Байсаева М. У. Методы и технологии защиты компьютерных сетей (сетевой, транспортный и прикладной уровни) / М. У. Байсаева // Международный журнал прикладных наук и технологий Integral. — 2020. — № 3. — С. 27. — EDN WDDJNX.
6. FRRouting Project. — Текст : электронный // FRRouting : [сайт]. — URL: https://frrouting.org/ (дата обращения: 29.04.2023).
7. Comparing Open Source BGP stacks. — Текст : электронный // The Elegant Network : [сайт]. — URL: https://elegantnetwork.github.io/posts/comparing-open-source-bgp-internet-routes (дата обращения: 29.04.2023).