СЕКЦІЯ: КОМП'ЮТЕРНО-ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ ЗВ'ЯЗКУ

УДК 004.3

Н. А. Шевченко, Г. В. Шимчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПІДВИЩЕННЯ СТІЙКОСТІ БАГАТОКОЛІЙНОЇ МАРШРУТИЗАЦІЇ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ МЕРЕЖЕВОЇ ВІРТУАЛІЗАЦІЇ VRF

N. A. Shevchenko, G. V. Shymchuk

IMPROVING MULTIPATH ROUTING RESILIENCE USING VRF NETWORK VIRTUALIZATION TECHNOLOGY

Розділення трафіку на віртуальні мережі (Virtual Routing and Forwarding, VRF) – це метод, який використовується в мережевих пристроях, таких як маршрутизатори та комутатори, для створення окремих ізольованих мереж в одній фізичній інфраструктурі. Кожна VRF має свої власні таблиці маршрутизації, інтерфейси та інші параметри, що відокремлюють їх один від одного. Цей метод дозволяє розділити мережевий трафік на декілька незалежних сегментів, які можуть мати різні політики маршрутизації та безпеки.

Основні переваги використання VRF включають:

– Ізоляція. Кожна VRF має власну таблицю маршрутизації, тому трафік, що проходить через різні VRF, не взаємодіє один з одним і залишається ізольованим.

– Розділення ресурсів. Використання VRF дозволяє виділити окремі фізичні або логічні інтерфейси для кожної VRF, що дозволяє краще керувати ресурсами та пропускною здатністю мережі.

– Маршрутизація. Кожна VRF може мати свою власну політику маршрутизації, що дозволяє керувати шляхами для різних сегментів мережі.

– Безпека. Використання VRF допомагає в мережевій безпеці, оскільки розділяє трафік між різними сегментами мережі, ускладнюючи потенційні атаки.

Для налаштування VRF використовуються команди на маршрутизаторах і комутаторах. Кожна VRF має унікальне ім'я і пов'язану з нею таблицю маршрутизації. Віртуальні інтерфейси (наприклад, sub-interfaces для маршрутизаторів) можуть бути призначені для конкретної VRF. Крім того, можна налаштовувати маршрутизаційні протоколи, такі як OSPF або BGP, для роботи в межах певної VRF.

Приклад налаштування VRF на маршрутизаторі Cisco показано на рисунку 1.

```
Router(config)# ip vrf VRF_NAME
Router(config-vrf)# rd ROUTE_DISTINGUISHER
Router(config-vrf)# route-target both ROUTE_TARGET
Router(config-vrf)# interface GigabitEthernet0/0.1
Router(config-if)# encapsulation dot1Q 10
Router(config-if)# ip vrf forwarding VRF_NAME
Router(config-if)# ip address 192.168.10.1 255.255.255.0
```

Рисунок 1. Налаштування VRF на маршрутизаторі Cisco

У цьому прикладі створюється VRF з ім'ям "VRF_NAME", призначається інтерфейсу GigabitEthernet0/0.1, і налаштовується маршрутна інформація для цієї VRF.

Використання різних фізичних інтерфейсів в мережевих з'єднаннях може бути корисним для різноманітних цілей, таких як розділення трафіку, підвищення надійності та забезпечення різних видів послуг в мережі.

Щоб підвищити надійність мережі, проводиться використання різних фізичних інтерфейсів у режимі «резерву». Якщо один інтерфейс відмовить, резервний інтерфейс може автоматично бути активований, забезпечуючи безперервну роботу мережі.

Різні фізичні інтерфейси можуть мати різну пропускну здатність. Ви можете використовувати інтерфейси з великим обсягом каналу для обробки великого обсягу трафіку, такого як відеопотоки, і менших інтерфейсів для менш вимогливих завдань.

При розширені мережі фізичні інтерфейси дозволяють підключати різні типи пристроїв до мережі. Наприклад, ви можете підключати сервери через 10-гігабітні інтерфейси, а клієнтські пристрої через 1-гігабітні інтерфейси.

Забезпечення безпеки в VRF (Virtual Routing and Forwarding) дуже важливе для збереження конфіденційності, цілісності та доступності даних у віртуальних мережах. Ось кілька кроків і рекомендацій щодо забезпечення безпеки в VRF:

1. Використання Access Control Lists (ACL).
2. Використання Firewall або Intrusion Detection/Prevention Systems (IDS/IPS).
3. Шифрування трафіку.
4. Segmentation (Сегментація).
5. Моніторинг безпеки.
6. Автентифікація та авторизація.
7. Оновлення та патчі.
8. Фізична безпека.
9. Освіта та навчання персоналу.

Наявність VRF дозволяє відокремити різні сегменти мережі на одному фізичному маршрутизаторі. Використовуючи VRF, можна створювати віртуальні мережі зі своїми власними таблицями маршрутизації, що дозволяє ефективно відокремлювати різні частини мережі.

Кожна VRF може мати власну адресну простору та незалежні маршрутизаційні таблиці. Це забезпечує високий рівень конфіденційності та дозволяє використовувати однакові IP-адреси в різних VRF без конфліктів.

Забезпечення безпеки в VRF включає в себе контроль доступу, моніторинг та шифрування трафіку. Використовуючи комбінацію Access Control Lists (ACL), firewall, VPN та систем виявлення вторгнень, можна захищати дані та ресурси в межах VRF.

Моніторинг і виявлення загроз важливі для вчасної реакції на потенційні проблеми безпеки. Системи моніторингу та виявлення вторгнень допомагають вчасно виявляти та реагувати на загрози безпеки в VRF.

Оновлення програмного забезпечення та фізична безпека мають велике значення. Регулярне оновлення ПЗ маршрутизаторів та забезпечення фізичної безпеки обладнання важливо для забезпечення безпеки мережі.

Враховуючи ці аспекти, можна створити безпечну та добре відокремлену мережу з використанням VRF на маршрутизаторах Cisco. Важливо постійно оновлювати свої знання та практики в області безпеки для забезпечення оптимального рівня захисту.

Література

1. Lasserre, M., Balus, F., Morin, T., Bitar, N., and Y. Rekhter, "Framework for Data Center (DC) Network Virtualization", RFC 7365, DOI 10.17487/RFC7365, October 2014.

2. Garg, P., Ed., and Y. Wang, Ed., "NVGRE: Network Virtualization Using Generic Routing Encapsulation", RFC 7637, DOI 10.17487/RFC7637, September 2015.

3. Black, D., Hudson, J., Kreeger, L., Lasserre, M., and T. Narten, "An Architecture for Data-Center Network Virtualization over Layer 3 (NVO3)", RFC 8014, DOI 10.17487/RFC8014, December 2016.