ДОСЛІДЖЕННЯ ОРГАНІЗАЦІЇ VPN НА БАЗІ MPLS-ТЕХНОЛОГІЙ

Чистик І.М., студент, група ТКРм-20, ivan.chystyk@donntu.edu.ua
Воропаєва А.О., к.т.н., доцент, anna.voropaieva@donntu.edu.ua
Донецький національний технічний університет,
м. Покровськ, Україна

Потреба у використані віртуальної приватної мережі(VPN) зараз виникає як у звичайного користувача, який хоче створили безпечне з'єднання для власних цілей, так і у великих корпорацій, підрозділи яких знаходяться на великий відстані один від одного для безпечного обміну цінною інформацією. Існує декілька шляхів створення та надання такої послуги. Побудова VPN на базі мультипротокольної комутації за мітками(MPLS) є одним із найбільш вдалих рішень, оскільки має рядь вагомих переваг з точки зору процесу створення, обслуговування та отриманого результату. Можливість роботи на різних типах середи передачі даних, різних поколінь та типів зумовлена особливістю MPLS і рівнях моделі OSI, на яких і відбувається процес налаштування, незалежно від фізичного і канального рівнів. Тому в даній статі приведене дослідження особливостей організації VPN на базі MPLS-технологій та її налаштування.

До кожного об'єкта віртуального маршрутизатора(VRF – англ. Virtual Routing and Forwarding)на кожному граничному маршрутизаторі провайдера(PE) прив'язується дві множини атрибутів ідентифікаторів, що описують правила експорту та імпорту(RT): import та export. Множина може містити один чи більше атрибутів RT. Правила розподілу маршрутної інформації виглядають наступним чином:

Всі маршрути, отримані від граничного маршрутизатора клієнта(CE), що належать VRF X, передаються іншим PE з додаванням безлічі атрибутів RT "export" VRF X.

Маршрут, отриманий від іншого PE, буде доданий до VRF-таблиці Y, тільки якщо безліч RT атрибутів отримане з маршрутом і безліч "import" VRF- Y мають хоча б один загальний атрибут.

Таблиця 1 – Конфігурація VRF на PE1

VRF	import	export	значення RD
A	1:1, 2:1	2:1	6:1
B	1:1, 3:2	3:2	7:2
C	2:2, 3:1, 4:5	6:2, 6:4	7:1

Маршрутизатор PE1 отримує по граничному протоколу шлюзу(iBGP) від маршрутизатора PE2 інформацію про маршрути VPN

Таблиця 2 – Маршрутна інформація, що отримується PE1 від PE2 по BGP

Префікс	Атрибути RT	Next-hop	VPN-label
8:1:10.2.1.0/24	4:2, 2:1	172.16.1.1	100
8:1:10.2.1.0/24	3:1	172.16.1.1	200
8:3:172.16.1.0/24	1:1, 7:1	172.16.1.1	300

Значення атрибута next-hop однакове у всіх маршрутів, тому що маршрутна інформація отримана від PE2 і це віртуальний інтерфейс PE2, від якого організовується сесія iBGP

З таблиці видно, що маршрути VPN є парою «дискримінатор маршрутної інформації(RD):префікс». Префікси 8:1:10.2.1.0/24 та 8:2:10.2.1.0/24 відрізняються лише значенням RD, отже різні маршрути, належать різним VPN і мають різний набір атрибутів. RT префікси розподіляються за таблицями маршрутизації наступним чином:

- 8:1:10.2.1.0/24 - VRF A, оскільки RT 2:1 входить до множини import VRF A.;
- 8:2:10.2.1.0/24 - VRF C, оскільки RT 3:1 входить до множини import VRF C;
- 8:3:172.16.1.0/24 - VRF A і B, тому що RT 1:1 входить у безліч import VRF A і B.

Таблиця 3 - Таблиця маршрутизації VRF на PE1

VRF-таблиця	Протокол	Префікс	Вихідний інтерфейс	Next-hop	Мітки для комутації
A	iBGP	10.2.1.0/24	Int3	172.16.1.1	100/1001
A	iBGP	172.16.1.0/24	Int3	172.16.1.1	300/1001
A	OSPF	10.1.1.0/24	Int2	CE1	Hi
B	iBGP	172.16.1.0/24	Int3	172.16.1.1	300/1001
B	OSPF	10.3.1.0/24	Int1	CE2	Hi
C	iBGP	10.2.1.0/24	Int3	172.16.1.1	200/1001
C	RIP	10.1.1.0/24	Int0	CE3	Hi

Значення мітки при комутації пакета від PE1 до PE2, дорівнює 1001. Тобто мітка 1001 визначає шлях перемикання міток(LSP) від PE1 до PE2. При проходженні через MPLS домен, VPN пакетам призначаються мітки: зовнішня, що визначає LSP між PE та внутрішня, що визначає VRF або інтерфейс на PE, до якого приєднаний абонент.

Таким чином, IP пакету, проходячи від CE1, призначається стек з двох міток: внутрішня 100 - ідентифікатор VRF на PE2 і "зовнішня" 1001, що визначає LSP до PE2.

Також префіксам 10.2.1.0/24 у різних VRF-таблицях (A та C) встановлюється різна "внутрішня" мітка. Це означає, що IP пакет, призначений для підмережі 10.2.1.0/24, прийде від CE1, його буде направлено далі з "внутрішньою" міткою 100, а прийшов від CE3 з "внутрішньою" міткою 200, тому ці пакети потраплять у різні VRF на PE2 і, відповідно, будуть направлені різним CE. Таким чином, MPLS/VPN дозволяє об'єднувати вузли з адресними просторами, що перетинаються, в різні VPN.

Розглянемо приклад маршрутної інформації, що передається від PE1 до PE2 за протоколом BGP. PE1 отримує, від підключених до нього CE, три префікси. Кожен префікс належить певному VRF, кожному префіксу призначається RD і безліч атрибутів RT. Мітка призначається автоматично залежно від режиму призначення міток: або VRF, або інтерфейсу, через які отримано маршрут. Оскільки VPN маршрути утворюються на PE1, то значення атрибута next-hop встановлюється рівним 172.16.1.2 - віртуальний інтерфейс, від якого PE1 встановлює iBGP сесію.

Таблиця 4 – Маршрутна інформація, що передається по BGP від PE1 до PE2

Джерело маршруту	VRF	Префікс	Префікс+RD	Заданий RT	Задана VPN мітка	Next-hop
CE1	A	10.1.1.0/24	6:1:10.1.1.0/24	2:1	200	172.16.1.2
CE2	B	10.3.1.0/24	7:2:10.3.1.0/24	3:2	400	172.16.1.2
CE3	C	10.1.1.0/24	7:1:10.1.1.0/24	6:2,6:4	100	172.16.1.2

PE1 отримує маршрут 10.1.1.0/24 від двох CE (CE1 і CE3), але ці CE належать різним VRF, тому префіксам призначаються різні RD, безліч RT і VPN мітка. Серед переваг організації VPN на базі MPL можна виділити:

- масштабованість;
- можливість перетину адресних просторів, вузлів підключених до різних VPN;
- ізоляція трафіку VPN один від одного на другому рівні моделі OSI.

Стисло підсумки даної роботи можна описати так: передача VPN пакетів через MPLS домен відбувається з двома мітками - "зовнішньої" та "внутрішньої", які визначають LSP від одного PE до іншого та LSP від одного PE до іншого відповідно, а правила імпорту маршрутної інформації задаються значенням множин VRF import і export.

Література

1. MPLS – режим доступу до ресурсу: https://ru.wikipedia.org/wiki/MPLS
2. Организация VPN на базе MPLS – режим доступу до ресурсу: https://docstore.mik.ua/manuals/ru/mpls/testbed1.html
3. Configuring a Basic MPLS VPN – режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html

Анотація

Розвиток світу інформаційних технологій, збільшення послуг і, відповідно, вимог до компаній від клієнтів задає необхідність у створені зручного, надійного та ефективного рішення створення безпечного доступу до мережі. Організація VPN на базі MPLS-технологій відповідає всім цим критеріям.

Ключові слова: MPLS, VPN

Аннотация

Развитие мира информационных технологий, увеличение услуг и, соответственно, требований к компаниям от клиентов задает необходимость в создании удобного, надежного и эффективного решения создания безопасного доступа к сети. Организация VPN на базе MPLS-технологий отвечает всем этим критериям.

Ключевые слова: MPLS, VPN

Abstract

The development of the world of information technology, the increase in services and, accordingly, the requirements for companies from customers make it necessary to create a convenient, reliable and effective solution for creating secure access to the network. The organization of VPN based on MPLS technologies meets all these criteria.

Keywords: MPLS, VPN