УДК 391.39

МЕТОД ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СЕРВІСІВ VPN НА ОСНОВІ ТЕХНОЛОГІЇ MPLS РІВНЯ ISP

Денисюк С.В, Осокін М.Г.
Інститут телекомунікаційних систем КПІ імені Ігоря Сікорського
E-mail: serhiy.denysiuk@gmail.com

Method of providing VPN security services based on MPLS technology ISP level

VPN services based on MPLS technology are very. They can give all that have given older 2 layer technologies, like ATM and Frame relay, and even more. Except basic VPN concepts, MPLS provide more better quality security options.

Впродовж довгого часу традиційні технології другого рівня, такі як ATM або Frame Relay лишалися домінуючими у наданні послуг приватних мереж (VPN), проте з приходом технології Multiprotocol Label Switching (MPLS) все більше компаній схиляються саме до сервісів, побудованих на основі цієї технології. Їхній вибір можна пояснити не тільки зрозумілою, добре продуманою архітектурою мереж на базі MPLS, але і їх поширенням та забезпеченням високої якості обслуговування (QoS).

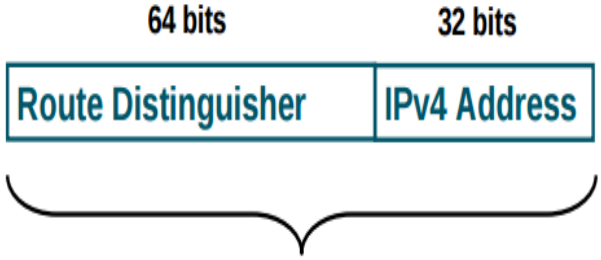

Рис. 1. Додавання розпізнавача маршрутів до маршруту IPv4.

Одним з перших пунктів, які потрібно передбачити при побудові сервісів даного типу, це розділення адресного простору між різними незалежними VPN. З точки зору маршрутизації це означає, що кожна кінцева система в VPN має свою унікальну адресу, і всі маршрути до цієї адреси вказують на ту ж кінцеву систему. Це досягається додаванням 64-розрядного розпізнавача маршрутів (рис. 1) до кожного маршруту IPv4, що робить унікальними адреси VPN в ядрі MPLS.

Також використовується спосіб розділення маршрутів між VPN. В такому випадку кожен маршрутизатор PE підтримує окремий екземпляр віртуальної маршрутизації і перенаправлення (VRF) для кожної підключеної VPN. Кожна VRF (рис. 2) на маршрутизаторі PE заповнюється маршрутами з однієї VPN, відповідно, не буде ніяких завад між віртуальними частинами VPN та маршрутизаторами PE.

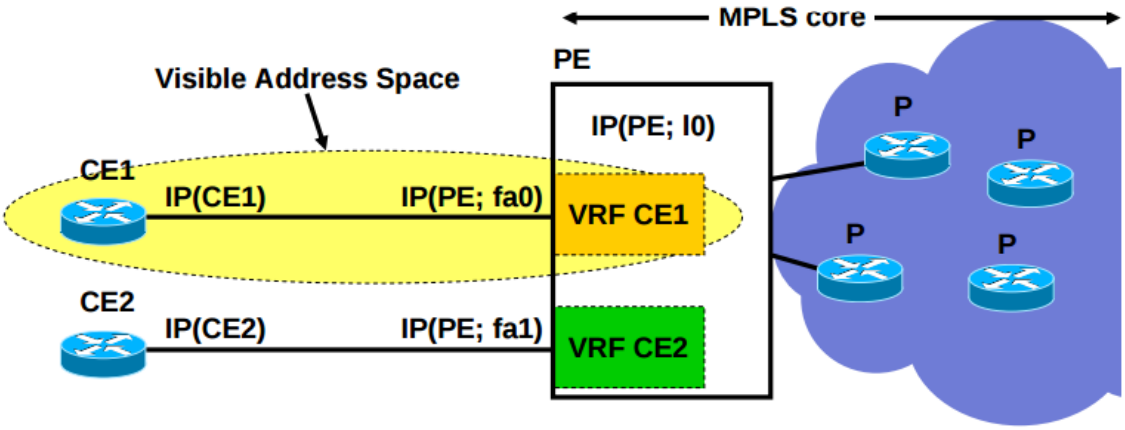

Рис. 2. Застосування VRF для відокремлення трафіку кожної VPN.

Крім того, слід зробити так, щоб крайні елементи мережі провайдера (PE) не були видимі для зовнішніх мереж (1). Це не обов'язково, але зрозуміло, що якщо ці адреси будуть доступні зовнішньому світові, то їх простіше буде атакувати. Відповідно, потрібно показати таку ж структуру, як і при звичайному інтернет-сервісі. Як варіант, можна використовувати NAT для подальшого приховування адреси. Для запобігання загрозам від атак, застосовують методи фільтрації пакетів з використанням мережевих екранів, списків керування доступом, а також приховуванням адрес від зовнішнього світу.

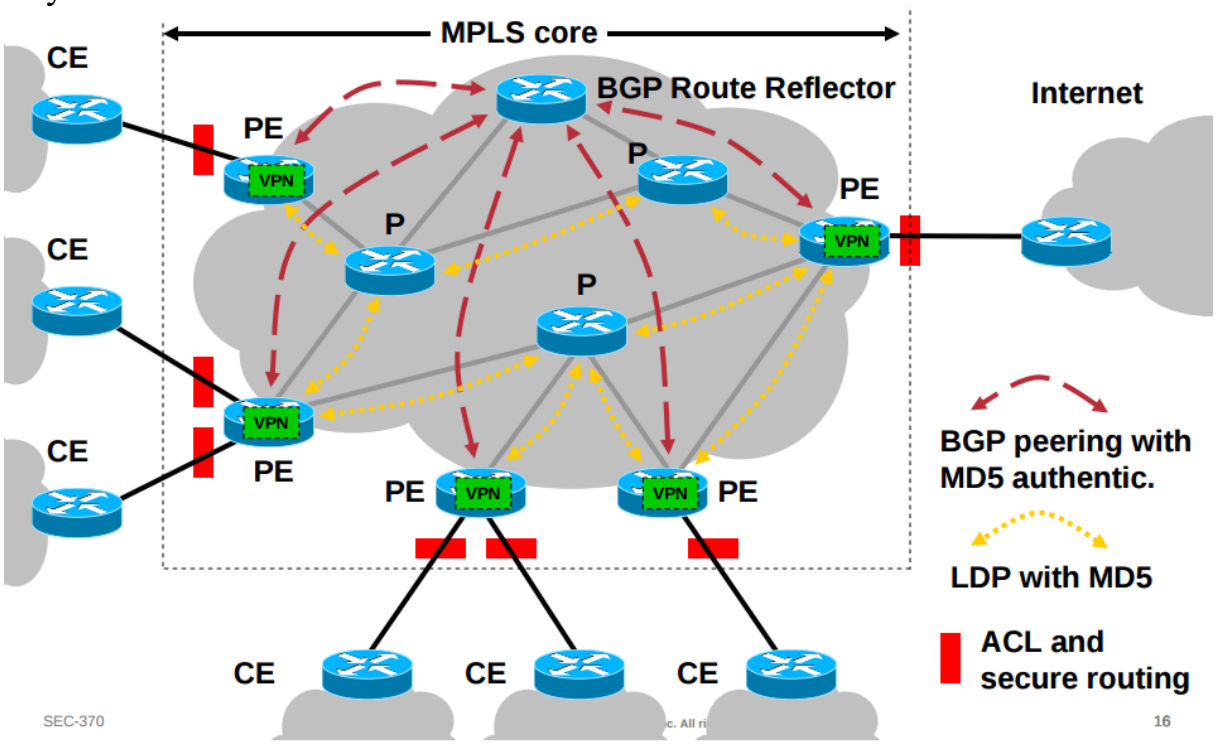

Рис. 3. Засоби захисту ядра MPLS.

У звичайній IP-мережі дуже просто підробити IP-адреси. Враховуючи те, що MPLS працює всередині з мітками замість IP-адрес, виникає питання, чи можливо підробити мітки. Припускаючи розділення адрес та

маршрутизації, зловмисник може спробувати отримати доступ до інших VPN, вставивши пакети з міткою, якою не полодіє. Це може бути проблеми з-зовні, наприклад, маршрутизатор іншого клієнта, або з середини ядра MPLS. В принципі, інтерфейс між будь-яким маршрутизатором CE та його піринговим PE-маршрутизатором являється IP-інтерфейсом. Маршрутизатор CE не знає про ядро MPLS і думаю, що відправляє IP-пакети на звичайний маршрутизатор. Додавання ж мітки (2) до пакету відбувається на самому PE-пристрої. У цілях безпеки, маршрутизатор PE ніколи не повинен приймати пакет з міткою від маршрутизатора CE. В більшості рішень від провідних вендорів, пакети, які приходять на інтерфейс CE з міткою, будуть видалені. Лишається варіант підміни IP-пакету, але, враховуючи розділення адрес та застосування VRF, це нанесе шкоди тільки тій VPN, із якої прийшов пакет, відповідно, це вже питання захисту окремої мережі окремого клієнта.

Інтерфейс CE/PE має ключове значення для безпеки мереж MPLS. Пакетні фільтри (ACL) повинні бути налаштовані так, щоб було дозволено тільки один конкретний протокол маршрутизації для пірингового інтерфейсу маршрутизатора PE і тільки з маршрутизатора CE. Увесь інший трафік на маршрутизатор та мережу ISP повинен бути заборонений. Так як маршрутизація являється сигнальним механізмом між CE та PE, вона є найкращим способом ввести фіктивну інформацію у ядро. Відповідно (рис.3), всі протоколи маршрутизації повинні бути сконфігуровані у відповідності до опції аутентифікації у відношенні CE і будь-якого Інтернет з'єднання: CE/PE - з аутентифікацією BGP MD5, PE/P – аутентифікацією MD5.

Що стосується атак з середини ядра MPLS, всі класи VPN (MPLS, FR, ATM) мають одну і ту ж проблему (3): якщо зловмисник може встановити сніффер (замінник мітки), він або вона може читати інформацію в усіх VPN. Він може виконувати велику кількість атак, від підробки пакетів до впровадження нового однорангового маршрутизатора.

Таким чином, MPLS забезпечує повне розділення адрес і маршрутизації, як в традиційних VPN-службах рівня 2. Він дозволяє приховати структури адресації ядра і інших віртуальних приватних мереж, і в сьогоднішньому розумінні неможливо з боку вторгнутися в ядро або інші VPN, зловживаючи механізмами MPLS. Крім того, неможливо проникнути в ядро MPLS, якщо воно надійно закріплене. Відповідно, інфраструктура MPLS відзначається таким же рівнем безпеки, як і класичні ATM або Frame Relay.

Література

1. http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a85c5.shtml.
2. http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/ multiprotocol-label-switching-mpls/prod_presentation0900aecd80312062.pdf.
3. http://searchenterprisewan.techtarget.com/guides/MPLS-VPN-fundamentals.