УДК 681.31

Георгій Яремович Криховецький

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ТЕХНОЛОГІЇ MPLS–VPN

Функціональність *MPLS-VPN* підтримує рівень безпеки, еквівалентний безпеці оверлейних віртуальних каналів у мережах *Frame Relay* і *ATM*. Безпека в мережах *MPLS-VPN* підтримується за допомогою сполучення протоколу *BGP* і системи дозволу *IP-адрес*.

BGP-протокол відповідає за поширення інформації про маршрути [1]. Він визначає, хто й з ким може зв'язуватися за допомогою багатопротокольних розширень і атрибутів *community*. Членство в *VPN* залежить від логічних портів, які поєднуються в мережу *VPN* і яким *BGP* привласнює унікальний параметр *Route Distinguisher* (*RD*). Параметри *RD* невідомі кінцевим користувачам, і тому вони не можуть одержати доступ до цієї мережі через інший порт і перехопити чужий потік даних. До складу *VPN* входять тільки певні призначені порти. У мережі *VPN* з функціями *MPLS* протокол *BGP* поширює таблиці *FIB* (*Forwarding Information Base*) з інформацією про *VPN* тільки учасникам даної *VPN*, забезпечуючи в такий спосіб безпеку передачі даних за допомогою логічного поділу трафіка.

Саме провайдер, а не замовник надає порти певній *VPN* під час її формування. У мережі провайдера кожен пакет асоційований з *RD*, і тому спроби перехоплення пакета або потоку трафіка не можуть привести до прориву хакера в *VPN*. Користувачі можуть працювати в мережі інтранет або екстранет, тільки якщо вони пов'язані з потрібним фізичним або логічним портом і мають потрібний параметр *RD*.

В опорній мережі інформація про маршрути передається за допомогою стандартного протоколу *Interior Gateway Protocol* (*IGP*), такого як *OSPF* або *IS-IS*. Прикордонні пристрої *PE* у мережі провайдера встановлюють між собою зв'язки-шляхи, використовуючи *LDP* для призначення міток.

Призначення міток для зовнішніх (користувальницьких) маршрутів поширюється між *PE-маршрутизаторами* не через *LDP*, а через багатопротокольні розширення *BGP*. Атрибут *Community BGP* обмежує рамки інформації про доступність мереж і дозволяє підтримувати дуже великі мережі, не перевантажуючи їхньою інформацією про зміни маршрутної інформації. *BGP* не оновляє інформацію на всіх периферійних пристроях *PE*, що перебувають у провайдерській мережі, а приводить у відповідність таблиці *FIB* тільки тих *PE*, які належать до конкретного *VPN*.

Якщо віртуальні канали створюються при оверлейній моделі, то інтерфейс, що виходить, будь-якого індивідуального пакета даних є функцією тільки вхідного інтерфейсу. Це означає, що *IP-адреса* пакета не визначає маршрут його передачі по магістральній мережі. Ця процедура запобігає також потраплянню несанкціонованого трафіка в мережу *VPN* і передачу несанкціонованого трафіка з неї.

У мережах *MPLS-VPN* пакет, що надходить у магістраль, у першу чергу асоціюється з конкретною мережею *VPN* на підставі того, по якому інтерфейсу (підінтерфейсу) пакет надійшов на *PE*-маршрутизатор [2]. Потім *IP-адреса* пакета звіряється з таблицею передачі (*forwarding table*) даної *VPN*. Зазначені в таблиці маршрути ставляться тільки до *VPN* прийнятого пакета. Таким чином, інтерфейс, що є вхідним, визначає набір можливих вихідних інтерфейсів. Ця процедура також запобігає як потраплянню несанкціонованого трафіка в мережу *VPN* і передачу несанкціонованого трафіка з неї.

При оцінці безпеки цієї технології *VPN* часто цитується дослідження компанії *Miercom* [3], головна думка якого полягає в тому, що технологію можна розглядати як надійну, оскільки зловмисник не в змозі одержати доступ до клієнтських *VPN* або магістралі. Однак, необхідно враховувати деякі особливості:

- трафік у віртуальних приватних мережах *MPLS* не шифрується. У цьому випадку *VPN* не означає нічого більше, крім поділу трафіка;
- маршрутизатор *PE* звичайно "ділиться" між різними клієнтами й — за певних

умов — завданнями. Виходячи з цього, атаки, наприклад "відмова в обслуговуванні" (*Denial of Service, Do*), із клієнтської мережі або — за умови відповідної досяжності — з *Internet* можуть мати побічний негативний вплив на безпеку або доступність інших клієнтів;

Метою даної статті є аналіз умов, *при яких системи, які застосовують технологію MPLS-VPN не будуть володіти властивостями конфіденційності та доступності.*

При застосуванні технології *MPLS-VPN* розрізняють мережі третього та другого рівнів.

При атаках на *VPN третього рівня* першочергова мета зловмисника — читання трафіка або неавторизований доступ. Всі атаки можна розділити на атаки "ззовні" і атаки "зсередини" (з магістралі *MPLS*).

Атаки "ззовні" можна розділити на дві складові: атаки із клієнтської мережі й атаки з *Internet*.

Інжекція (введення) попередньо маркірованого трафіка із клієнтської мережі. Зловмисник, що перебуває в клієнтській мережі, може спробувати проникнути в іншу віртуальну приватну мережу, передавши "своєму" пристрою *PE* пакети, що вже містять мітку. Мова йде про мітку, на підставі якої пакет направляється в іншу *VPN*. Але як написано в *RFC* 2547: "Пакети з мітками з джерел, які не заслуговують довіри, не приймаються магістральними маршрутизаторами".

З погляду провайдера, клієнтська мережа ніколи "не заслуговує довіри", а виходить, такі пакети повинні відхилятися маршрутизатором *PE*.

Інжекція (введення) уже маркірованого трафіка з Internet. Зловмисник може спробувати відправити на маршрутизатор *PE* вже маркіровані пакети з *Internet*, з метою передати їх у клієнтську мережу. Для цього йому необхідно довідатися або вгадати використовувані мітки й *IP-адреси*, що цілком можливо.

Маркіровані відповідним чином пакети необхідно доставити точки, яку атакують, що (що малоймовірно), а маршрутизтор, що атакує *PE*, повинен бути досяжний з *Internet* (що залежить від організації конкретної мережі провайдера) — тільки тоді атака буде успішною. Але завдяки тенденції до концентрації все більшої кількості функцій на все меншому числі багатофункціональних пристроїв, такі умови не можна повністю виключати.

Однак, як уже згадувалося, *RFC* 2547 вимагає, щоб пакети з мітками з джерел, які не заслуговують довіри, до яких, безумовно, відноситься *Internet*, відкидалися.

Атаки "зсередини" на відміну від перерахованих атак передбачають знаходження зловмисника на магістралі. Для початку необхідно коротенько пояснити цю умову. Якщо зловмисник контролює один з вузлів магістралі, то в нього з'являється можливість для проведення цілої низки різних атак. Звичайно, насамперед весь минаючий через цей вузол трафік, якщо він додатково не зашифрований, піддається загрозі зчитування. Як правило, таке шифрування забезпечити можливо, однак нерідко від нього відмовляються заради економії й простоти адміністрування віртуальної приватної мережі *MPLS*, чого не скажеш про *VPN* на базі *IPsec*, — як відомо, *MPLS VPN* покликані замінити *IPSec VPN*.

Атаки "зсередини" можна розділити на наступні складові:

- скомпрометовані провайдерські пристрої;
- експлуатовані клієнтами пристрої *PE*;
- зламані станції управління;
- атаки на транзитні вузли між провайдерами;
- неправильно сконфігуровані пристрої провайдерів;
- модифікація міток на магістралі;
- модифікація маршрутизації *MP-BGP*.

Скомпрометовані провайдерські пристрої. Даний вид атаки полягає в тому, що провайдерські пристрої можуть бути зламані, після чого зломщик (хакер) може отримати доступ до всієї конфіденційної інформації.

Експлуатовані клієнтами пристрої *PE*. Якщо клієнт самостійно експлуатує пристрій *PE*, це ставить під загрозу всю модель безпеки магістралі, оскільки в нього з'являється потенційна можливість доступу до віртуальних приватних мереж інших клієнтів.

Зламані станції управління. Якщо співробітник провайдерскї компанії входить в *Internet* з того ж комп'ютера, з якого він звертається до інструментів управління із графічним інтерфейсом для побудови *VPN*, то потенційно зловмисник може одержати доступ до системи управління — з усіма наслідками, що випливають, для безпеки *VPN*, що управляються.

Атаки на транзитні вузли між провайдерами. Для того щоб пропонувати віртуальні приватні мережі *MPLS* у світовому масштабі, багато операторів погоджують між собою контракти, завдяки яким вони можуть будувати віртуальні приватні мережі *MPLS*, що простираються за межі їхньої власної мережі, і одночасно обмінюватися маркірованими пакетами. *RFC* 2547 описує різні моделі, і серед них щонайменше одна — найбільш масштабована — може бути по суті своїй ненадійною. Окрім того, у точках обміну трафіком (*Internet Exchange Points, IXP*) оператори часто організують

міжз'єднання на базі *Ethernet*, у результаті чого потенційно створюються умови для атак на інтерфейс даних на другому рівні.

Неправильно сконфігуровані пристрої провайдерів. У більшості випадків пристрої провайдерів обслуговуються людьми, які можуть робити ненавмисні помилки. За певних умов навіть стає можливим порушення цілісності магістралі *MPLS*. Якщо ж віртуальні приватні мережі *MPLS* використовуються в рамках корпоративних мереж, тоді немає майже ніякої різниці між "клієнтськими пристроями" і "безумовно надійними провайдерськими пристроями" — щонайменше в тому, що стосується обслуговуючого персоналу.

Модифікація маршрутизації *MP-BGP*. Коли зловмисник у стані втрутитися в первісний інформаційний обмін в *Multiprotocol BGP*, він може додавати у віртуальну приватну мережу "додаткові філії", і вже через них одержати неавторизований доступ до систем. Причому треба не тільки перебувати на магістралі, але й мати в наявності додаткові інструменти для точкового доступу до трафіка *BGP*, що вимагає значних зусиль.

Модифікація міток на магістралі. Цей тип атаки також передбачає знаходження атакуючого на магістралі. Якщо йому вдається змінити мітку пакета, то останній нескладно перенаправляти в іншу віртуальну приватну мережу. Крім того, в існуючі *VPN* можна ввести будь-які пакети.

Хоча для проведення подібних атак інструментів поки не існує, навіть однобічна інжекція пакетів у віртуальну приватну мережу може мати серйозні наслідки. Її виявляється досить, приміром, для атак на основі *SNMP* — серед яких є відкидання конфігураційного файлу пристрою — або для запуску "хробаків" на основі *UDP* ("хробаки" *SQL*).

Під терміном *"віртуальна приватна мережа другого рівня"* у контексті *MPLS* звичайно розуміється передача довільного трафіка по *MPLS* (*Any Transport over MPLS, ATo*). Тоді по магістралі *MPLS* передаються не пакети, а цілі блоки другого рівня, наприклад осередку *ATM*, кадри *Ethernet* або *Frame Relay*.

При допомозі міток створюються так звані "псевдопровода": вони утворять логічні канали, по яких і передаються відповідні кадри. Зловмисникові доступ до магістралі дає ті ж можливості для атаки, що й описані слабкі місця віртуальних приватних мереж третього рівня.

Але в технології *ATo* є дві модифікації, які становлять особливий інтерес у рамках розмови про безпеку: *Ethernet* поверх *MPLS* (*Ethernet over MPLS, EoMPLS*) і служба віртуальної приватної локальної мережі (*Virtual Private LAN Service, VPLS*).

У випадку *EoMPLS* дві філії підключають до магістралі комутатори й передають, відповідно, кадри *Ethernet*. Для обох сторін це виглядає так, немов між ними побудований прямий канал другого рівня без проміжної інфраструктури глобальної мережі. Всі системи можуть користуватися загальними віртуальними локальними мережами або підмережами *IP*.

EoMPLS являє собою двухточечну технологію з'єднання. Підключення додаткової філії припускає побудову від неї нового тунелю до всіх існуючих офісів, що обмежує масштабованість *EoMPLS*. Саме цей недолік і повинна виправити служба віртуальної приватної локальної мережі. При її застосуванні будь-яка кількість філій утворюють загальну мережу *Ethernet* із многоточечними з'єднаннями. При додаванні філії "псевдопроводи" створюються автоматично за допомогою спеціальної системи сигналізації — однак необхідна протокольна база ще не специфікована повністю. Всі філії з'єднуються одна з одною "нібито" прямо, тому хмару *MPLS/VPLS* часто характеризують як "великий віртуальний комутатор". Прикордонними пристроями на стороні клієнта в *EoMPLS* або *VPLS* найчастіше служать комутатори.

Однак, якщо хмара дійсно поводиться зовсім прозоро, як це, приміром, має місце у випадку реалізації *VPLS* від компанії *Juniper*, тоді можуть проявлятися два ефекти, що істотно впливають на безпеку мережі.

1. Оскільки різні філії утворять тепер загальну мережу (*Ethernet*), на кожну віртуальну мережу вибирається лише один корінь *STP* (тільки в одній філії). При надлишковому підключенні філії (приміром, з міркувань підвищення готовності) це потенційно веде до того, що внутрішні канали філії між комутаторами виявляються заблокованими.

Таке поводження хоча й відповідає принципам сполучного дерева, як вони описані в стандарті, але при цьому відповідальний за безпеку на підприємстві часто забуває про те, що внутрішній трафик філії передається по провайдерській мережі в незашифрованому виді й залежно від інфраструктури може проходити через країни, де діють закони про допустимість читання минаючого трафіка державними органами й/або "поширене інше відношення до поняття інтелектуальної власності".

2. Проблеми з безпекою виникають і у зв'язку з віртуальними локальними мережами. Якщо, приміром, у двох філіях існують однакові номери віртуальних мереж, то ці *VLAN* після з'єднання філій за допомогою *EoMPLS/VPLS* будуть "бачити" один одного. Коли в одній філії є *VLAN 10 для серверів, а в іншому — VLAN 10* для

бездротової мережі, всі користувачі бездротової мережі другої філії будуть одержувати широкомовний трафік *Windows* першої філії, і в зловмисника, що перебуває в бездротовій мережі, з'явиться доступ до сервера іншої філії.

Перераховані вище аспекти відповідають самому звичайному поводженню мережі або протоколів, однак дуже впливають на мережну безпеку. У випадку використання віртуальних приватних мереж другого рівня на базі *MPLS* про них завжди необхідно пам'ятати й ураховувати при оцінці ризику.

Доступність до інформаційних ресурсів можливо оцінити за допомогою визначення функціональної живучості телекомунікаційної мережі, що використовує технологію *MPLS*.

Зазначені мережі не будуть володіти властивістю функціональної живучості у випадках, коли [4].

1. Імовірність отримання пакета прикордонним комутуючим маршрутизатором телекомунікаційної мережі буде дорівнювати нулю. Тобто

$$P_{ПТ}(b_{ij}) = \prod_{l=1}^{r} (P_{НВ_l}(b_{ij}) + P_{ПП_l}(b_{ij})) = 0 \qquad (1)$$

де $P_{НВ_i}(b_{ij})$ — імовірність не виявлення завадостійким кодом помилки в пакеті i-того пріоритету, при проходженні ним j-тим каналом зв'язку;
$P_{ПП_l}(b_{ij})$ — імовірність правильного прийому пакета i-того пріоритету, при проходженні ним j-тим каналом зв'язку.

Для визначення можливості настання такої події проаналізуємо складові виразу (1). Для завадостійких кодів, що працюють у режимі одночасного виявлення й виправлення помилок імовірність не виявлення завадостійким кодом помилки в прийнятому пакеті (імовірність пропуску помилки) становить значення

$$P_{НВ}(n) = \sum_{i=(d-t)}^{n} \frac{e(i)}{i} P(i, n) \qquad (2)$$

де $e(i)$ — число помилок кратності i, що приводять до неправильного декодування;
d — мінімальна кодова відстань;
$t = \dfrac{d-1}{2}$ — найвища кратність помилок, що гарантовано виправляються.

Оскільки в режимі одночасного виправлення і виявлення помилок до неправильного декодування приводять помилки, що відповідають не тільки першому рядку стандартного розміщення коду, але і помилки, що відповідають ще $\sum_{i=1}^{t} c_n^i$ рядкам, то при розрахунках можна використовувати наближену формулу:

$$P_{НВ}(n) \approx \frac{\sum_{i=0}^{t} c_n^i}{2^{n-r}} P(\geq (d-t), n) \qquad (3)$$

Імовірність правильного прийому пакету визначається як

$$P_{ПП}(n) = \sum_{i=0}^{t} P(i, n) = 1 - P(\geq t+1, n) \qquad (4)$$

Отже, при імовірності появи помилок, кількість яких перевищує найвищу кратність помилок, що гарантовано виправляються, у пакеті з n символів рівній одиниці шлях телекомунікаційної мережі, у відповідності до алгоритму передачі і захисту інформації від помилок, прийнятому в технології *MPLS,* не володіє властивістю функціональної живучості.

2. Імовірність безвідмовної роботи комутуючих маршрутизаторів (*LSR*) через переповнення вхідного буфера накопичувача буде дорівнювати нулю. Тобто

$$P_{вх}(a_j) = 0 \qquad (5)$$

Для визначення можливості настання такої події проаналізуємо організацію процесів масового обслуговування пакетів на вході *LSR*. При використанні механізмів *QoS* вибір пакетів, що відкидаються, залежить від їхнього пріоритету. Використання зазначених методів приводити до того, що на інформаційних напрямках, які здійснюють передачу пакетів з низькими пріоритетами, обмін інформацією стає проблематичним через постійне відкидання цих пакетів на комутаційних маршрутизаторах. Тобто для визначених категорій терміновості $q P_{вх}(a_j)$ буде прагнути, але не дорівнювати нулю (завдяки використанню методу *CBWFQ).*

Висновки.

1. Використання технології *MPLS* у телекомунікаційних мережах спеціального призначення можливе лише у випадках, коли в якості середовища передавання даних використовуються волоконно-оптичні кабелі. Оскільки вони нечутливі до електромагнітних завад [5], виникнення подій, при яких шляхи телекомунікаційної мережі не будуть володіти властивістю живучості стають неможливими.

2. Технологію *MPLS* у телекомунікаційних мережах спеціального призначення необхідно використовувати лише з *QoS*, що надасть змогу підтримувати різні види трафіка (дані, голос і відео) у єдиній мережній архітектурі, а також надавати споживачам гарантовану якість послуг і підтримувати додатки, що мають критично важливе значення для окінцевого користувача, при цьому пограничні комутатори *PE* повинні належати сайту спеціального призначення (рис. 1).

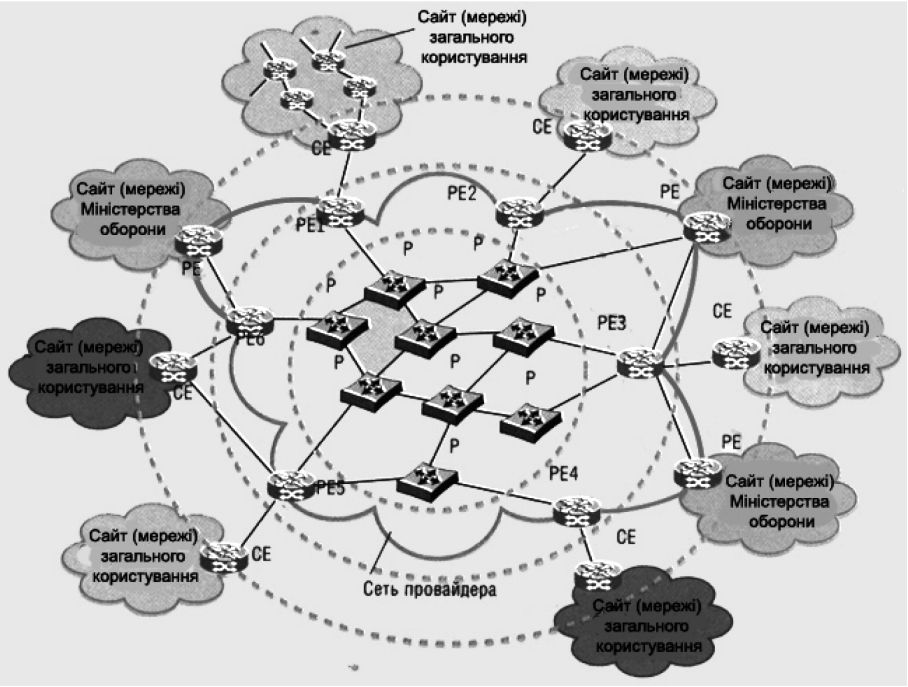

Рис. 1. Склад компонентів мережі побудованої з використанням технології MPLS

Література

1. В. Олифер, Н. Олифер. *MPLS* на службе *VPN* / В.Олифер, Н. Олифер // Журнал сетевых решений *LAN*. — 2002, март. — С. 40—47. **2. М. Захватов.** Построение виртуальных частных сетей (*VPN*) на базе технологи *MPLS*. Техническое описание *Cisco Systems* // М. Захватов. — М. : *Cisco Systems Inc*., 2001. — 48 с. **3. Э. Рей,** П. Фирс. Технология *MPLS* и сценарии нападения. Доклад на конференции *Blackhat,* 2006. **4. Колачов С. П.** Дослідження можливості використання технологій *Frame Relay* та *ATM* у проводовій телекомунікаційній мережі спеціального призначення / С.П. Колачов. — К. : Труди академії, 2008. — С. 125—132. **5. Буров Є.** Комп'ютерні мережі. — 2-ге оновлене і доповн. вид. / Є. Буров. — Львів : БаК, 2003. — 584 с.

В статье определены критерии, при которых системы, использующие технологию MPLS-VPN, потеряют свойства конфиденциальности и доступности. Автор делает вывод о возможности использования рассмотренной технологии в автоматизированных системах управления специального назначения.

Ключевые слова: технология MPLS-VPN, конфиденциальность, доступность системы, автоматизированные системы управления специального назначения.