УДК 004.772

АНАЛІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СЕРВІСІВ MPLS VPN

Тимофеєв Є.М., Созонник Г.Д.
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
E-mail: timofeeevzh@gmail.com

SECURITY ANALYSIS OF MPLS VPN SERVICES

Analyzes modern technologies to ensure the security of the service of building virtual private networks, technical solutions of VPN technologies on the example of the organization of a private virtual network based on MPLS network. Reasons for the need to protect against attack. The technique of complex data protection of the enterprise at the organization of VPN security service is offered.

Здійснено аналіз сучасних технологій щодо надання безпеки сервісу побудови віртуальних приватних мереж, технічних рішень технології VPN на прикладі організації приватної віртуальної мережі на основі мережі MPLS. Встановлено причини необхідності захисту від атак. Запропоновано методику комплексного захисту даних підприємства при організації безпечного сервісу VPN.

VPN (Virtual Private Network – віртуальна приватна мережа) – це приватна мережа, побудована в рамках загальнодоступної мережевої інфраструктури, такої як глобальний Інтернет. VPN означає не тільки ізоляцію комунікацій, а скоріше контрольоване сегментування для спільнот, що становлять інтерес, через спільну інфраструктуру. Технологія VPN стала однією з найважливіших послуг у транснаціональних компаніях по всьому світу завдяки своїй безпеці, зручності та низькій вартості розгортання [1].

MPLS (Multiprotocol Label Switching – багатопротокольна комутація по мітках) є основною магістральною технологією нового століття.

Технологія, заснована на MPLS VPN, базується на чіткому розмежуванні між постачальником послуг мережі (P-мережа) та мережі споживача (C-мережа), як показано на рисунку 1 [2]. У порівнянні з традиційною технологією VPN, MPLS VPN є справді хорошим рішенням і має свої технологічні особливості та функції, такі як FEC, VRF, MPBGP, VPNv4-адреса тощо для подолання недоліків власне тунелювання.

Найважливішою характеристикою будь-якої системи передачі, незалежно від її складності і призначення, є безпека циркулюючої в ній інформації. Високий ступінь автоматизації, до якої прагне людство, широке впровадження дешевих комп'ютерних систем масового застосування та попиту роблять їх надзвичайно вразливими по відношенню до деструктивних дій, ставлять сучасне суспільство в залежність від ступеня безпеки використовуваних інформаційних технологій. Загальна комп'ютеризація несе з собою численні проблеми, найбільш складною з яких є проблема інформаційної безпеки.

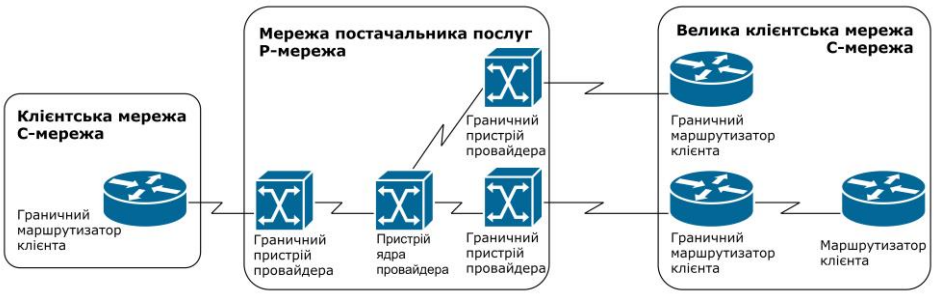

Рис.1. Мережа постачальника послуг та клієнтів на основі MPLS.

Мета створення систем безпеки – попередження або оперативне усунення наслідків умисних (навмисних) і випадкових деструктивних впливів, наслідком яких можуть бути руйнування, модифікація або витік інформації, а також дезінформація [3].

Критерієм при прийнятті будь-якого рішення щодо систем безпеки є цінність інформації. При цьому розрізнюють чотири види загроз:

1. Викрадення інформації: проникнення в приватну мережу для отримання конфіденційної інформації, яка може бути використана або продана з різними цілями. Приклад: розкрадання конфіденційної інформації, що належить організації, наприклад, відомості про науково-технічні розробки.

2. Крадіжка особистої інформації для подальшого її використання. Використовуючи викрадені дані можна отримати юридичні документи, подати заяву на кредит та здійснити несанкціоновані покупки через Інтернет [4]. Проблема крадіжки особистої інформації продовжує загострюватися, а фінансові втрати становлять мільярди доларів в рік.

3. Втрата даних або маніпуляція даними: проникнення з метою знищення або зміни записів даних. Приклади втрати даних: передача вірусу, що «затирає» жорсткий диск комп'ютера. Приклад неправомірного використання даних - проникнення в систему зберігання даних з метою зміни даних, наприклад ціни виробу.

4. Припинення обслуговування: заборона доступу правомочних користувачів до служб, для використання яких їм має бути надане право. Приклад: атаки типу «відмова в обслуговуванні» (DoS-атаки) на сервери, мережеві пристрої і канали обміну даними по мережі.

Таким чином, навіть у невеликих мережах необхідно враховувати загрози безпеці та вразливості при плануванні впровадження мережі.

Для створення захищеного каналу VPN використовуються процедури шифрування, аутентифікації і авторизації. Методів шифрування досить багато, тому важливо, щоб на кінцях тунелю використовувався один і той же алгоритм шифрування. Крім того, для успішного дешифрування даних джерела і одержувача даних необхідний обмін ключами шифрування. Під аутентифікацією розуміється визначення користувача або кінцевого пристрою. Аутентифікація дозволяє встановлювати з'єднання лише між легальними користувачами і, відповідно, запобігає доступ до ресурсів мережі несанкціонованих користувачів. У процедурі беруть участь дві сторони: одна доводить свою автентичність, а інша її перевіряє і приймає рішення.

Найчастіше для аутентифікації використовується пароль, але можуть застосовуватися інші докази. Недоліками застосування паролів є їх розкриття, що пояснюється їх простотою. Аутентифікація даних свідчить про їх цілісність, а також про те, що вони надійшли від одного з користувачів. Авторизація передбачає надання абонентам різних видів послуг. Кожному користувачеві надаються певні адміністратором права доступу. Ця процедура виконується після процедури аутентифікації і дозволяє контролювати доступ санкціонованих користувачів до ресурсів мережі. Взагалі, процедури аутентифікації і авторизації виконують одну задачу і до них пред'являються однакові вимоги. Цілісність переданих даних дозволяє забезпечити застосування електронного підпису.

Для забезпечення комплексного захисту інформації підприємства пропонується наступна стратегія: забезпечення безпечного доступу у будь-який час співробітників підприємства до мережевих ресурсів; забезпечення протидії атакам на DHCP сервер; впровадження в мережі функції IP Source Guard та DAI; забезпечення запобігання переповненню CAM таблиць комутаторів; використання мережевого екрану; організація Site-to-Site IPsec VPN зв'язку.

Висновок. Розглянуто сучасні методи організації безпеки віртуальних приватних мереж на основі MPLS. Описано процес створення захищеного VPN каналу та процедур шифрування, аутентифікації і авторизації. Запропонована методика комплексного підходу для забезпечення безпеки інформації підприємства.

Література

1. P. Ferguson, G. Huston, What is a VPN? Internet, https://www.potaroo.net/papers/vpn.pdf, April 1998.
2. I. Pepelnjak, J. Guichard, J. Apcar, MPLS and VPN Architectures, Volume II. Cisco Press, 2003.
3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: Кудиц - Образ, 2001. — 363 с.
4. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков; под общ. ред. Н. И. Синадского. – Екатеринбург: Изд-во Урал. ун-та, 2016. – 180с.