ПОРІВНЯЛЬНИЙ АНАЛІЗ VPN РІШЕНЬ ДЛЯ ЗВ'ЯЗКУ МІЖ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Садовніченко М.В., магістрант, sadovnichenko.max@gmail.com;
Воропаєва В.Я., к.т.н., доцент, viktoriya.voropayeva@donntu.edu.ua
ДВНЗ «Донецький Національний Технічний Університет»,
м. Луцьк, Україна

У теперішній час із запровадженням цифрових технології на об’єктах критичної інфраструктури є велика потреба в обміну інформації між цими об’єктами. До об’єктів критичної інфраструктури належать підприємства таких галузей як: енергетика, хімічна промисловість, транспорт тощо. Тобто це установи які є стратегічно важливими для функціювання економіки і безпеки держави і суспільства.

Якщо нема можливості для прокладення окремої лінії зв’язку між об’єктами, тоді приходиться використовувати загальнодоступні лінії зв’язку. Але ця мережа повинна відповідати наступним вимогам: своєчасність, достовірність і безпека зв’язку. Для налаштування безпечного і конфіденційного зв’язку в загальній доступній мережі існує технологія віртуальної приватної мережі(VPN).

Головне призначення VPN є побудова приватної мережі між віддаленими об’єктами без застосування виділеної ліній. За допомогою такого з’єднання досягається безпека зв’язку. В даному випадку це означає захист мережевого трафіку щодо конфіденційності, цілісності та автентифікації[1].

Існують наступні топології VPN мереж: однорангова, клієнт-сервер і Site to Site. Для потреб зв’язку між об’єктами доцільно використовувати саме останню топологію мережі. Під час такого з’єднання встановлюється безпечний тунель між 2 локальними мережами через мережу постачальника послуг, де кінцевими точками тунелю є сервер або маршрутизатор з функцією VPN.

Вибір протоколу VPN також залежить від типу трафіку, що надсилається через тунель. Протоколи VPN можна класифікувати відповідно до рівнів OSI отриманих пакетів які використовують для шифрування, і працюють на наступних рівнях: 2, 3, 4. Для наших вимог найкраще вибором будуть протоколи 2 рівня, оскільки він має кращий діапазон застосування і може передавати майже всі види пакетів які можуть генерувати датчики і інші пристрої на об’єктах. Вони можуть генерувати від простих даних, таких як показники лічильників. Але також можливі більш об’ємні дані, як відеозапис з камер. Що буде найкраще для мережі об’єктів критичної інфраструктури, так як можлива передача особливих пакетів даних між пристроями[2].

Головні вимоги до VPN мережі для зв’язку між об’єктами критичної інфраструктури є наступні: високі стандарти безпеки і/або високу якість об-

слуговування (QoS). Це залежить потреб самого зв'язку і які дані будуть відправлятися між об'єктами. Тому потрібно враховувати що висока пропускна здатність для таких мереж не є головним.

Серед доступних протоколів 2 рівня є наступні: PPTP, L2TP з IPSec, OpenVPN, PPP Bridging Control Protocol, EoIP з IPSec і MPLS VPLS. Розглянемо наступні пункти: QoS, аналіз пакетів і автентифікація з шифрування.

Під час аналізу трафіку через VPN мережу перевіряємо наступні параметри QoS. Пропускна здатність: 50 Мбіт/с, затримка: 20 мс, втрата пакетів: 0,1%. Далі наведена табл. 1 після проведення експерименту порівняння пропускної здатності між трафіком, не пов'язаними із VPN, і трафіком VPN на затримці 20 мс.

Таблиця 1

VPN	Пропускна здатність з VPN
PPTP-BCP	45.1 Мбіт/с
L2TP-BCP	45.2 Мбіт/с
L2TP-BCP-IPSec	44 Мбіт/с
OpenVPN	9.6 Мбіт/с
EoIP	46 Мбіт/с
EoIP_IPSec	45.1 Мбіт/с
MPLS VPLS	48 Мбіт/с

Можна побачити що майже всі протоколи мають зменшення пропускної здатності в VPN тунелі в діапазоні 5-12 %. І вони підходять для вибору проколу для зв'язку між об'єктами. Але пропускна здатність в протоколі OpenVPN зменшується аж на 80%. І якщо для зв'язку між об'єктами не потрібно велика пропускна здатність тунелю, також можна розглядати протокол OpenVPN для вибору.

Аналіз пакетів відбувається за допомогою програми Wireshark, який призначений для аналізу мережевих пакетів Ethernet. Аналізатор фіксує трафік саме в зашифрованому тунелі.

Такі протоколи як PPTP-BCP, L2TP-BCP, EoIP, MPLS VPLS мають наступні проблеми при передачі пакету в тунелі. А саме можна прослухати наступну інформацію: адреси джерела та призначення, і також який саме протокол використовується для шифрування. Найбільш захищений протокол є OpenVPN, завдяки надійному шифруванню в Wireshark відображаються лише те що використовується саме такий протокол без іншої додаткової інформації.

Таблиця 2

VPN	Шифрування	Аутентифікація
PPTP	MPPE128	Ім'я і пароль
L2TP	IPSec	Ім'я і пароль
OpenVPN	TLS(AES/BF)	TLS
EoIP	IPSec	Немає
MPLS VPLS	Немає	Немає

Кожен протокол має свій алгоритм шифрування і аутентифікації. Серед перелічених в табл.2 найкращі параметри безпеки має протокол OpenVPN. Який використовує TLS для шифрування і аутентифікації.

У висновку маємо наступні результат аналізу протоколів VPN. Найкращі параметри безпеки має саме протокол OpenVPN. Його набагато складніше прослухувати ніж інші, а також він має найвищий рівень аутентифікації і шифрування. Один із його недоліків саме нижчий рівень QoS. І якщо для об'єктів інфраструктури важливі високі показники QoS то можливо краще зупинити свій вибір на L2TP з підтримкою IPSec.

Література

1. Habibovic S. VIRTUAL PRIVATE NETWORKS: An Analysis of the Performance in State-of-the-Art Virtual Private Network solutions in Unreliable Network Conditions – URL:https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1367277&dswid=-8502

2. Dr.Manjaiah D.H. Technical Overview of Virtual Private Networks(VPNs) – URL: https://www.researchgate.net/publication/274929918_Technical_Overview_of_Virtual_Private_NetworksVPNs

3. Si Thu Aung, Thandar Thein. Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks – URL: https://www.researchgate.net/publication/339761254_Comparative_Analysis_of_Site-to-Site_Layer_2_Virtual_Private_Networks

Анотація

У статті був проведений аналіз наявних VPN рішень для використання зв'язку між об'єктами критичної інфраструктури. Був проведений аналіз в таких напрямках як QoS, аналіз пакету і автентифікація з шифрування. І вибір найкращого протоколу.

Ключові слова: VPN, QoS, шифрування, пакет, аутентифікація.

Abstract

The article analyzes the existing VPN solutions for the use of communication between critical infrastructure. The analysis was carried out in such areas as QoS, packet analysis and encryption authentication. And the choice of the best protocol.

Keywords: VPN, QoS, encryption, packet, authentication.