КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.19.3445
УДК 004.056

Тишик Іван Ярославович
кандидат технічних наук, доцент кафедри захисту інформації
Національний університет "Львівська політехніка", м. Львів, Україна
ORCID ID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

ВИБІР ТЕХНОЛОГІЇ ВІДДАЛЕНОГО ДОСТУПУ ДЛЯ ЕФЕКТИВНОЇ ОРГАНІЗАЦІЇ ЗАХИСТУ МЕРЕЖЕВИХ З'ЄДНАНЬ

Анотація. Розглянуто сучасні методи та засоби побудови сервісу віртуальних приватних мереж, проаналізовано шляхи їх реалізації апаратно-програмними засобами на прикладі приватної віртуальної мережі на основі CISCO FlexVPN. Для реалізації цього завдання використовувався протокол обміну ключами для забезпечення безпеки взаємодії у віртуальних мережах IKEv2. Примітно, що FlexVPN в IOS за замовчуванням вимагає мінімум дій з боку системного адміністратора для швидкого налаштування VPN. Для цього призначені так звані smart-defaults (заздалегідь налаштовані стандартні ikev2 proposal / policy / profile, ipsec profile та інші). В такій конфігурації за замовчуванням налаштовані: IKEv2 proposal, IKEv2 policy, IPSec transform-set і IPSec profile. Причому налаштовані вони так, що вищий пріоритет мають найбільш серйозні алгоритми, що, як правило, цілком влаштовує системного адміністратора. Природно, що найбільшу передбачуваність роботи VPN забезпечує ручне налаштування усіх параметрів. З огляду на сказане можна констатувати, що для побудови VPN-каналів найбільш прогресивною є технологія FlexVPN, оскільки володіє широкою масштабністю, гнучкістю, не накладає жодних обмежень на конфігурацію, а також має передбачений набір команд за замовчуванням Smart-defaults, який може значно полегшити завдання щодо налаштування відповідного комунікаційного обладнання на певних етапах. Головною особливістю ж цієї технології є поєднання двох основних типів побудови віртуальних приватних мереж: Site-to-site та Client-to-site. Модель, яка створена на основі програмного забезпечення GNS3, надає змогу більш детально розглянути основні кроки та загальний принцип налаштувань на пристроях створюваної мережі. Загалом продемонстровано актуальність використовуваної технології у контексті стрімко зростаючої конкуренції на ринку та необхідності надавати можливість віддаленим користувачам на безпечний доступ до віддалених корпоративних ресурсів. Як результат моделювання було створену віртуальну приватну мережу для корпорації, в якій реалізовано одночасно кілька захищених каналів зв’язку між структурними підрозділами, а також організований віддалений доступ для домашніх користувачів за допомогою технології Cisco AnyConnect.

Ключові слова: Віртуальна приватна мережа, обмін ключами в Інтернеті, інтерфейси віртуального тунелю, Адаптивний пристрій безпеки, Асоціація безпеки Інтернету та протокол керування ключами, Мережева операційна система.

ВСТУП

Нині у діловому світі спостерігається значне збільшення обсягу бізнес-процесів, які циркулюють в Інтернет та зростання ролі сучасних систем комунікації в ньому. Очевидно, що управління великою компанією може бути успішним лише в тому випадку, якщо дії її структурних підрозділів скоординовані, дані передаються вчасно, а їх конфіденційність та цілісність залишаються при цьому не порушеними. Крім того, Інтернет вже давно перестав бути просто мережею передачі даних, і навіть його цінність як джерела інформації, з точки зору бізнес-спільноти, також відходить на другий план.

Нині Інтернет є одночасно активним споживчим ринком і товарно-валютним обміном: мільйони транзакції відбуваються в ньому "онлайн" щодня.

Проте, слід зазначити, що безпека під час використання засобів комунікації є як ніколи актуальною. Безперечно, засобів захисту існує чимало, надійність кожного з них та галузь застосування відрізняються, але незаперечним залишається факт, що використання мереж VPN стає все більш популярним. На цей час головною особливістю мереж VPN є те, що багато з них можна використовувати безкоштовно і вони є легкодоступними.

Віртуальні приватні мережі можна вважати повноцінним видом транспорту для передачі трафіку, лише якщо є гарантії пропускної здатності та інших параметрів продуктивності, а також безпека переданих даних.

Хоча технологія VPN давно відома, віддалений доступ VPN як послуга є сучасним рішенням безпеки мережі для повсякденних потреб бізнесу. Команди авторизованого користувача повинні безпечно працювати будь-де, будь-коли та на будь-якому пристрої. VPN віддаленого доступу створює зашифрований тунель між ресурсами організації, кінцевими пристроями в мережі та співробітниками, які їх використовують, захищаючи всю онлайн-активність від зовнішніх користувачів та конфіденційні зони мережі.

Нині існує достатньо велика кількість параметрів, за якими можна класифікувати існуючі методи та засоби реалізації однієї і тієї самої технології. Пропозицій на ринку чимало, проте, при виборі технології слід виділити ту, яка є достатньо новою, активно підтримується розробником, дозволяючи користувачам максимально гнучко налаштовувати під свої потреби системну конфігурацію вузлів своєї мережі та будувати унікальні системи для захищеної передачі даних на віддалений хост.

Такою технологією є Cisco FlexVPN, так як поєднує технологію Site-to-site VPN з Remote-access VPN для різних типів їх підключення [1-4].

Постановка проблеми. З огляду на сказане, постає завдання демонстрації актуальності використовуваної технології, в якій реалізовано одночасно кілька захищених каналів зв’язку між структурними підрозділами для забезпечення віддаленим користувачам безпечного доступу до віддалених корпоративних ресурсів.

Аналіз останніх досліджень і публікацій. Свого часу експерти проаналізували близько трьохсот VPN-додатків, розміщених в Google Play і App Store. Дослідження щодо завантажень VPN додатків охопило 73 країни (рис.1)

В цілому протягом року користувачі скачали більш 480 млн VPN-додатків, що на 54% більше, ніж роком раніше, коли обсяг завантажень вимірювався 311 млн.

Велика частина установок такого програмного забезпечення − 75% від загальної кількості − припадає на власників Android-пристроїв. Вони завантажили 358,3 млн додатків, що дозволяють обходити блокування сайтів. Власники iPhone і планшетів здійснили понад 121,9 мільйонів завантажень VPN-сервісів різного типу [1].

Country	Downloads (12 Mths)	Growth (YOY)	Free Downloads (12 Mths)
Indonesia	75,463,349	111%	72,599,298
United States	74,554,690	17%	50,585,819
India	57,003,606	405%	50,657,702
United Arab Emirates	30,627,589	32%	26,821,969
Brazil	23,500,424	76%	21,189,143
Saudi Arabia	19,923,733	14%	18,877,623
Turkey	16,357,471	39%	15,058,458
United Kingdom	13,993,181	33%	9,032,697
Pakistan	10,384,873	60%	9,210,565

Рис 1. Кількість завантажень VPN додатків у світі за інформацією Top10VPN

Країною з найбільшою популярністю VPN-сервісів названа Індонезія, де за 12-місячний проміжок часу місцеві жителі скачали близько 75,5 млн мобільних VPN-додатків, що на 111% перевищує показник річної давності.

У трійку лідерів також потрапили США та Індія, де зафіксовано 74,6 і 57 мільйонів завантажень подібного програмного забезпечення відповідно.

Порівнюючи приватні та віртуальні приватні мережі, слід виділити ряд безперечних переваг VPN:

• Технологія VPN може значно знизити витрати на обслуговування мережі: користувач сплачує лише плату за оренду каналу, організація якої не викликає жодних труднощів через великий масштаб Інтернету.

• зручність та легкість в організації та перебудові структури мережі;

Розробка єдиної моделі віртуальної приватної мережі може спростити мережеві операції, але такий підхід не може відповідати різним вимогам клієнтів, оскільки вони унікальні. Кожен клієнт висуває свої вимоги щодо безпечного передавання трафіку, доступ до кількості сайтів, складності маршрутизації, критичних ситуацій, моделей та обсягів трафіку. Для задоволення широкого спектру вимог постачальники послуг повинні пропонувати клієнтам різні моделі надання послуг.

Одна з них є Site-to-site VPN (Virtual Private Network) − спосіб реалізації технології OpenVPN, призначений для створення захищеного віртуального тунелю між кількома приватними мережами, що може бути корисною опцією при об'єднанні у віртуальну приватну мережу віддалених філій компанії або відділів, що знаходяться в одному будинку, але в різних мережах зокрема, за різними роутерами, які не підтримують режим точки доступу [5].

При використанні Site-to-Site VPN відсутня необхідність окремо налаштовувати параметри підключення для кожного конкретного клієнтського пристрою. Тут достатньо налаштувати по одному VPN-шлюзу з боку кожної з об’єднуваних мереж. Point-to-Site доцільний при підключенні конкретних віддалених співробітників до VPN-сервера корпорації з відповідним налаштуванням параметрів як сервера, так і їх клієнтських частин [6].

Зазвичай віддалений користувач не має статичної адреси та підключається до захищених ресурсів не через виділений VPN-пристрій, а за допомогою спеціального програмного забезпечення, встановленого на його пристрої. Відносини підприємства з провайдером відіграють важливу роль у створенні VPN, зокрема, розподіл між ними функцій для налаштування та роботи VPN-пристроїв. Під час створення захищених

каналів інструменти VPN можуть розташовуватися як у середовищі обладнання постачальника, так і в обладнанні підприємства. Залежно від цього, існує два варіанти побудови VPN:

• схема користувача (VPN, що надається клієнтом)

• схема провайдера (VPN, що надається постачальником)

Крім наведеної класифікації, всі варіанти створення VPN можна розділити на дві категорії: програмні рішення − це готові програми, які встановлюються на момент сканування комп'ютерної мережі за допомогою стандартного програмного забезпечення, апаратні рішення VPN, які включають комп'ютер, операційну систему, спеціальне програмне забезпечення.

Кожен виробник мережевого устаткування пропонує свої рішення для організації VPN каналів. У тому числі і компанія Cisco. Деякі з цих рішень різних виробників сумісні між собою, а деякі працюють тільки на обладнанні одного виробника. Технології побудови VPN на обладнанні Cisco можна класифікувати за технологією побудови каналу [6, 8].

Технологія Cisco FlexVPN підтримує IKEv2 (Internet Key Exchange Version 2) та IKEv1, які є саме тими протоколами, які входять до групи протоколів безпечної асоціації (SA). Завдання IKEv2 є забезпечити автентифікаційне узгодження ключів в рамках фреймворка (програмного каркасу) ISAKMP (англ. Internet Security Association and Key Management Protocol, Інтернет протокол асоціацій безпеки та керування ключами). Опублікований IETF в уже досить далекому 2005 році (IKEv1 - 1998р.). У жовтні 2014 року в редакції RFC 7296 вийшла виправлена версія стандарту, що описує IKEv2.

Протоколи IKEv1 та IKEv2 працюють за UDP / 500 (4500 у випадку з NAT-T), але між собою несумісні, тобто неможливою є ситуація при якій на одному кінці тунелю був би IKEv1, а на іншому − IKEv2. При цьому один і той же роутер може мати налаштованими на собі як IKEv2 так і IKEv1 тунелі одночасно. У заголовках IKEv1 і IKEv2 досить відмінностей для того, щоб роутер зміг визначити з чим має справу, не зважаючи на те що обидва протоколи будуть використовувати одні і ті ж порти.

У IKEv2 більше немає таких понять як aggressive / main mode (Ці режими використовуються в IKEv1. Aggressive mode використовує три повідомлення (замість шести в main-режимі). При цьому той, хто ініціює з'єднання, віддає всі свої дані разом, а також свою частину обміну DH. Потім сторона, яка надсилає відповідь, відразу завершує свою частину генерації DH. У підсумку в цьому режимі всього два етапи. Тобто перші два етапи з main mode (узгодження хешів і обмін DH) спресовуються в один. В результаті цей режим значно небезпечніше з тієї причини, що у відповідь приходить багато технічної інформації в plaintext файлі. І найголовніше - VPN-шлюз може надіслати хеш пароля, який використовується для автентифікації на першій фазі (цей пароль ще часто називається pre-shared key або PSK)., що є одним з аспектів, які роблять протокол простішим для розуміння.

У IKEv2 термін «Фаза 1» замінений на «IKE_SA_INIT» (обмін двома повідомленнями, що забезпечує узгодження протоколів шифрування / хешування і генерацію DH ключів), а «Фаза 2» − на «IKE_AUTH» (теж два повідомлення, які реалізують безпосередньо автентифікацію пірів та генерацію ключів для ESP). Обмін даними в «IKE_AUTH» завжди зашифрований за допомогою SA, сформованими «IKE_SA_INIT». ISAKMP SA тепер називаються IKEv2 SA, а IPSec SA - Child SA.

У IKEv2 метод автентифікації між пірами більше не узгоджується автоматично і не прив'язаний до тих чи інших політик IKEv2. Тобто якщо раніше в IKEv1 кожної ISAKMP policy був рядок authentication, де вказувалося, який буде тип автентифікації, в разі якщо буде обрана саме ця policy, то тепер метод автентифікації задається вручну і явно

визначається з яким конкретним піром буде автентифікація за сертифікатами, а ось з цим - по pre-shared key. Крім того, в IKEv2 стала можлива асиметрична автентифікація. Тобто можна зробити так, що кінцева точка «А» буде автентифікувати кінцеву точку «В» за сертифікатами, в той час як «В» буде автентифікувати «А» по pre-shared ключу. Або ж «А» автентифікує «В» за допомогою pre-shared key1, в той час як «В» автентифікує «А» за допомогою pre-shared key2. Можливі й інші варіанти, в тому числі. автентифікація з використанням різних методів EAP.

Mode Config (режим, який в IKEv1 називається phase 1.5 і використовується для налаштування віддалених підключень RAVPN / EasyVPN), NAT-T і keepalives тепер безпосередньо описаний в специфікації протоколу і є його невід'ємною частиною. Раніше ж відповідальними за реалізацію цих речей були виробники і продавці які створювали їх кожен по-своєму у міру необхідності.

У IKEv2 додався додатковий механізм захисту control-plane (services plane) від DoS атак. Суть його полягає в тому, що перш ніж відповідати на кожен запит у встановленні захищеного з'єднання (IKE_SA_INIT) IKEv2 VPN-шлюз надсилає джерелу певний тестовий cookie, і чекає, що той відповість тим же. Якщо джерело відповіло, то це означає, що можна починати з ним генерацію DH. Якщо ж джерело не відповідає (у випадку з DoS атакою так і відбувається, і це можна порівняти з TCP SYN flood attack), VPN-шлюз просто забуває про нього і закриває зв’язок.

VPN використовується для зменшення ризику втрати внутрішніх даних, полегшити роботу віддаленої робочої сили та захистити від зловмисних атак. Як частина надійного рішення безпеки, наприклад NordLayer, VPN віддаленого доступу для бізнесу пропонують компаніям гнучкий і економічно ефективний спосіб убезпечити свої віддалені команди, задовольнити їхні поточні потреби та захистити критично важливі активи [9, 10].

Мета статті. Для обґрунтування вибору технології безпечного віддаленого доступу існує достатньо велика кількість параметрів, за якими можна класифікувати способи її реалізації. Оскільки пропозицій готових рішень реалізації безпечного віддаленого доступу на ринку чимало, варто виділити технологію, яка є достатньо новою, активно підтримується розробниками, дозволяє користувачам максимально гнучко налаштовувати під свої потреби системну конфігурацію вузлів мережі та будувати унікальні системи для захищеної передачі даних на віддалений хост, має покращений захист від DDoS-атак. Такою технологією є FlexVPN, обґрунтування вибору та реалізація якої для забезпечення безпечного обміну даними і є метою цієї статті.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ FLEXVPN

Основною особливістю FlexVPN є те, що одна і та ж конфігурація VPN-шлюзу дозволяє прикріпити до нього різні типи тунелів (Remote Access, Site-to-Site та інші). Тобто це єдина технологія, яка дозволяє поєднати різні типи підключення до віртуальної приватної мережі без застосування надлишкової конфігурації системи, ускладнення її розуміння та зниження ефективності взаємодії між сегментами мережі.

Основні компоненти конфігурації IKEv2 в Cisco IOS є: Proposal, Policy, Keyring, Profile.

IKEv2 proposal визначає, які алгоритми будуть задіяні для встановлення IKE_SA_INIT фази. Його особливість в тому, що в один proposal можна помістити відразу кілька алгоритмів шифрування і виглядає наступним чином:

crypto ikev2 proposal PROP_1

encryption aes-cbc-256 aes-cbc-128 3des
group 14 5 2
integrity sha 256 sha1 md5

Перша відмінність від isakmp policy в тому, що в один proposal можна помістити відразу кілька алгоритмів / довжини ключів шифрування / DH / хешування. Друга відмінність − відсутній рядок authentication, оскільки тепер автентифікація є окремим питанням. Третя відмінність − proposal не є самостійною частиною конфігурації і він поміщений у policy.

IKEv2 Policy є контейнером (місце зберігання) для proposal. Як приклад:

crypto ikev2 policy POLICY_1
match vrf VRF1
match address local 203.0.113.10
proposal PROP_1

Як видно з прикладу policy посилається на proposal. Але, при цьому надається можливість вибрати той чи інший proposal в залежності від:

1) того в якому VRF знаходиться інтерфейс, до якого підключається віддалений корстувач.

2) до якого типу локальної адреси підключається віддалений пір.

Таким чином є змога гнучко конфігурувати необхідні політики доступу в залежності від потреб користувача

IKEv2 Keyring є репозиторієм (місце для зберігання), в якому зберігаються pre-shared ключі. Очевидно, що keyring має сенс лише при попередньому виборі методу автентифікації на основі pre-shared ключів. У разі, якщо для автентифікації використовується PKI, потрібно налаштовувати не keyring, а Trustpoint. У IKEv2 ж з'явився своєрідний контейнер keyring, завдяки чому конфігурація виглядає більш структурованою.

IKEv2 profile лежить в основі FlexVPN і є основною його складовою. Він визначає політику віддаленого доступу до VPN-шлюзу. За своїм призначенням IKEv2 profile є повністю аналогічний IKEv1 isakmp profile в Cisco IOS або tunnel-group (connection profile) у міжмережевих екранах ASA, проте надає більше можливостей і є більш гнучким в налаштуванні. Це своєрідний репозиторій параметрів, які не узгоджуються учасниками VPN-взаємодії в автоматичному режимі, а визначаються статично.

IKEv2, як і IKEv1, ISAKMP і декілька інших, менш відомих, є саме тими протоколами, які входять до групи SA протоколів. Завдання IKEv2 є забезпечити автентифікаційне узгодження ключів в рамках фреймворка (програмного каркасу) ISAKMP.

Примітно, що FlexVPN в IOS за замовчуванням вимагає мінімум дій з боку системного адміністратора для швидкого налаштування VPN. Для цього призначені так звані smart-defaults (заздалегідь налаштовані стандартні ikev2 proposal / policy / profile, ipsec profile та інші). В такій конфігурації за замовчуванням налаштовані: IKEv2 proposal, IKEv2 policy, IPSec transform-set і IPSec profile. Причому налаштовані вони так, що вищий пріоритет мають найбільш серйозні алгоритми, що, як правило, цілком влаштовує системного адміністратора. Природно, що найбільшу передбачуваність роботи VPN забезпечить ручне налаштування усіх параметрів.

ISSN 2663 - 4023

РЕАЛІЗАЦІЯ SITE-TO-SITE FLEXVPN З PRE-SHARED АВТЕНТИФІКАЦІЄЮ

У цьому випадку налаштовано IKEv2 тунель між маршрутизаторами Site1Router і Site2Router (рис.2,3) і забезпечено взаємну доступність loopback-ів кожного з маршрутизаторів через тунель з використанням динамічного протоколу маршрутизації.

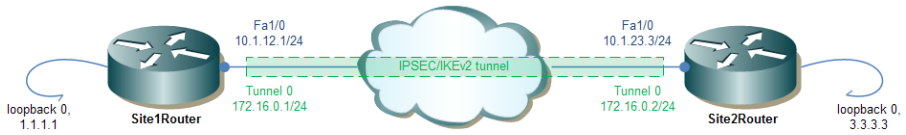

Рис. 2 Конфігурація Site-to-siteFlexVPN

На цьому прикладі конфігурація має відношення до налаштування IKEv2 і IPSec виділений кольором. У прикладі задіяні ті самі smart-defaults, які задають параметри за замовчуванням для IKEv2 policy / proposal, IPSec transform-set. IPSec profile теж використовується по замовчуванню. У конфігурації він посилається на профіль ikev2 і прикріплений на тунельний інтерфейс для його захисту. В результаті конфігурація виходить досить компактною і легко читається. Як видно з прикладу, налаштування всього, що в IKEv1 мало відношення до другої фази, аналогічна такій в IKEv2. Тобто створюється такий же crypto ipsec transform set (тут взято стандартний), цей transform-set разом з ikev2 профілем прив'язується до ipsec профілію, ipsec-профіль прикріплений на інтерфейс, що працює в режимі ipsec ipv4 (VTI).

Site1Router	Site2Router

crypto ikev2 keyring KEYRING
 peer Site2Router
  address 10.1.23.3
  identity address 10.1.12.1
  pre-shared-key local cisco1
  pre-shared-key remote cisco2
!
crypto ikev2 profile IKEV2PROF
 match identity remote address 10.1.23.3 255.255.255.255
 identity local address 10.1.12.1
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
!
crypto ipsec profile default
 set ikev2-profile IKEV2PROF
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf 10 area 0
!
interface Tunnel0
 ip address 172.16.0.1 255.255.255.0
 ip ospf 10 area 0
 tunnel source FastEthernet1/0
 tunnel mode ipsec ipv4
 tunnel destination 10.1.23.3
 tunnel protection ipsec profile default
!
interface FastEthernet1/0
 ip address 10.1.12.1 255.255.255.0
!
router ospf 10
 	
ip route 0.0.0.0 0.0.0.0 10.1.12.2
	crypto ikev2 keyring KEYRING
	 peer Site1Router
	  address 10.1.12.1
	  identity address 10.1.23.3
	  pre-shared-key local cisco2
	  pre-shared-key remote cisco1
	!
	crypto ikev2 profile IKEV2PROF
	 match identity remote address 10.1.12.1 255.255.255.255
	 identity local address 10.1.23.3
	 authentication remote pre-share
	 authentication local pre-share
	 keyring local KEYRING
	!
	crypto ipsec profile default
	 set ikev2-profile IKEV2PROF
	!
	interface Loopback0
	 ip address 3.3.3.3 255.255.255.0
	 ip ospf network point-to-point
	 ip ospf 10 area 0
	!
	interface Tunnel0
	 ip address 172.16.0.2 255.255.255.0
	 ip ospf 10 area 0
	 tunnel source FastEthernet1/0
	 tunnel mode ipsec ipv4
	 tunnel destination 10.1.12.1
	 tunnel protection ipsec profile default
	!
	interface FastEthernet1/0
	 ip address 10.1.23.3 255.255.255.0
	!
	router ospf 10
	
	ip route 0.0.0.0 0.0.0.0 10.1.23.2

Рис.3. Налаштування VPN кожного з маршрутизаторів

ISSN 2663 - 4023

На цьому прикладі конфігурація має відношення до налаштування IKEv2 і IPSec виділений кольором. У прикладі задіяні ті самі smart-defaults, які задають параметри за замовчуванням для IKEv2 policy / proposal, IPSec transform-set. IPSec profile теж використовується по замовчуванню. У конфігурації він посилається на профіль ikev2 і прикріплений на тунельний інтерфейс для його захисту. В результаті конфігурація виходить досить компактною і легкою для читання. Як видно з прикладу, створений transform-set разом з ikev2 профілем прив'язується до IPSec профілїю, прикріпленого до відповідного інтерфейсу.

Після успішного встановлення тунелю отримано наступний вивід від команди *show crypto ipsec sa*:

```
Site1Router#sh crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.12.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 10.1.23.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1680, #pkts encrypt: 1680, #pkts digest: 1680
    #pkts decaps: 1678, #pkts decrypt: 1678, #pkts verify: 1678
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.23.3
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0x31A6B95A(833010010)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xE6E9033F(3874030399)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 11, flow_id: 11, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4268866/1723)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x31A6B95A(833010010)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 12, flow_id: 12, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4268866/1723)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

Вивід sh crypto ipsec sa такий самий як при налаштуванні традиційного Ikev1, оскільки ESP все одно, хто для нього готує ключову інформацію − IKEv2 або IKEv1.

Site1Router#sh crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
1 10.1.12.1/500 10.1.23.3/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/12375 sec
CE id: 1003, Session-id: 2
Status Description: Negotiation done
Local spi: 1625F2D9751CC54F Remote spi: B9C9990767BC0006
Local id: 10.1.12.1
Remote id: 10.1.23.3
Local req msg id: 2 Remote req msg id: 6
Local next msg id: 2 Remote next msg id: 6
Local req queued: 2 Remote req queued: 6
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

Тут вже бачимо специфічну для IKEv2 інформацію − використані алгоритми шифрування / хешування / DH групи. Задіяно смарт-дефолт (Smart Defaults), що дозволяє мінімізувати кількість рядків конфігу за рахунок використання параметрів за замовчуванням, які, до того ж, можна налаштувати під власні потреби. Видно також, що ініціатором з'єднання був Site2Router.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З огляду на сказане можна констатувати, що для побудови VPN-каналів найбільш прогресивною є технологія FlexVPN, оскільки володіє широкою масштабністю, гнучкістю, не накладає жодних обмежень на конфігурацію, а також має передбачений набір команд за замовчуванням Smart-defaults, який може значно полегшити завдання щодо налаштування відповідного комунікаційного обладнання на певних етапах. Головною особливістю ж цієї технології є поєднання двох основних типів побудови віртуальних приватних мереж: Site-to-site та Client-to-site. Модель, яка створена на основі емулятора GNS3, надає змогу більш детально розглянути основні кроки та загальний принцип налаштувань на пристроях створюваної мережі. Загалом продемонстровано актуальність використовуваної технології у контексті стрімко зростаючої конкуренції на ринку та необхідності надавати можливість віддаленим користувачам на доступ до корпоративних ресурсів

Напрямки подальших досліджень можуть бути спрямовані на підвищення надійності FlexVPN шляхом підтвердження усіх операцій від іншої сторони VPN-з’єднання та покращення захисту від DDoS-атак.

ISSN 2663 - 4023

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Санникова, О. (2018). *Новые технологии создания корпоративных виртуальных сетей FlexVPN*. VPN Expo.
2 Andrew119 «IKEv2 и Flex VPN средствами Cisco IOS. Синтаксис и логика работы» habr.com/ru/post/186126/
3 Настройка соединения через протокол IPSec между двумя маршрутизаторами и Cisco VPN Client 4.x. www.cisco.com/
4 Rodrigues, A., Krupa, Jan. FlexVPN: AnyConnect IKEv2 Remote Access with Local User Database. www.cisco.com/
5 Skendzic, A., Kovacic, B. (2017). Open source system OpenVPN in a function of Virtual Private Network. *IOP Conference Series: Materials Science and Engineering*, *200*, 012065. https://doi.org/10.1088/1757-899x/200/1/012065
6 FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS XE Everest 16.6. www.cisco.com
7 *Public Key Infrastructure Configuration Guide, Cisco IOS XE Release 3S - Configuring Certificate Enrollment for a PKI [Support]*. Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book/sec-cert-enroll-pki.html
8 Anwar, S. J., Ahmad, I. (2019). Design and Deployment of IPSec VPN Using CISCO Network Infrastructure. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 237–247. https://doi.org/10.32628/cseit195630
9 https://telecom-sales.ru/content/stati/tehnologii-cisco-vpn-vidy-i-tipy-udalennogo-dostupa/
10 *FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS XE Everest 16.6 - Configuring Internet Key Exchange Version 2 [Cisco ASR 1000 Series Aggregation Services Routers]*. Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-6/sec-flex-vpn-xe-16-6-book/sec-cfg-ikev2-flex.html#GUID-5C063DFB-B2F2-40C1-85F9-741C0035C979

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

Ivan Tyshyk
Ph.D, Docent, Associate Professor at the Department of Information Security
National University Lviv Polytechnic, Lviv, Ukraine
ORCID ID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

CHOICE OF REMOTE ACCESS TECHNOLOGY FOR EFFECTIVE ORGANIZATION OF PROTECTION OF NETWORK CONNECTIONS

Abstract. Modern methods and means of building a service of virtual private networks are considered, the ways of their realization with the help of hardware and software on the example of a private virtual network based on CISCO FlexVPN are analyzed. To implement this task, the key exchange protocol was used to ensure the security of interaction in IKEv2 virtual networks. It is noteworthy that FlexVPN in IOS by default requires minimal action from the system administrator to quickly configure the VPN. The so-called smart-defaults are intended for this (standard ikev2 proposal / policy / profile, ipsec profile and others are configured in advance). In such a configuration, the following are configured by default: IKEv2 proposal, IKEv2 policy, IPSec transform-set, and IPSec profile. Moreover, they are configured so that the most serious algorithms have the highest priority, which, as a rule, suits the system administrator. Naturally, the greatest predictability of VPN operation will be provided by manual setting of all parameters. In view of the above, it can be stated that the FlexVPN technology is the most progressive for building VPN channels, as it has a wide scale, flexibility, does not impose any restrictions on the configuration, and also has a set of default commands called Smart-defaults, which can greatly facilitate the task regarding the configuration of the relevant communication equipment at certain stages. The main feature of this technology is the combination of two main types of construction of virtual private networks: Site-to-site and Client-to-site. The model, which is created on the basis of the GNS3 software, allows you to consider in more detail the main steps and the general principle of settings on the devices of the network being created. In general, the relevance of the technology used in the context of rapidly growing competition on the market and the need to provide remote users with secure access to remote corporate resources is demonstrated. As a result of the simulation, a virtual private network was created for the corporation, which provides both secure communication channels between departments, as well as organized remote access for employees using Cisco AnyConnect technology.

Keywords: Virtual Private Network, Internet Key Exchange, Virtual tunnel interfaces, Adaptive Security Appliance, Internet Security Association and Key Management Protocol. Interworking Operation System

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Sannikova, O. (2018). *New technologies for creating corporate virtual networks FlexVPN*. VPN Expo
2 Andrew119 «IKEv2 и Flex VPN средствами Cisco IOS. Sintaksis i logika raboty» habr.com/ru/post/186126/
3 Nastrojka soedineniya cherez protokol IPSec mezhdu dvumya marshrutizatorami i Cisco VPN Client 4.x. www.cisco.com/
4 Rodrigues, A., Krupa, Jan. FlexVPN: AnyConnect IKEv2 Remote Access with Local User Database. www.cisco.com/
5 Skendzic, A., Kovacic, B. (2017). Open source system OpenVPN in a function of Virtual Private Network. *IOP Conference Series: Materials Science and Engineering, 200,* 012065. https://doi.org/10.1088/1757-899x/200/1/012065
6 FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS XE Everest 16.6. www.cisco.com
7 *Public Key Infrastructure Configuration Guide, Cisco IOS XE Release 3S - Configuring Certificate Enrollment for a PKI [Support]*. Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book/sec-cert-enroll-pki.html

8 Anwar, S. J., Ahmad, I. (2019). Design and Deployment of IPSec VPN Using CISCO Network Infrastructure. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 237–247. https://doi.org/10.32628/cseit195630

9 https://telecom-sales.ru/content/stati/tehnologii-cisco-vpn-vidy-i-tipy-udalennogo-dostupa/

10 *FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS XE Everest 16.6 - Configuring Internet Key Exchange Version 2 [Cisco ASR 1000 Series Aggregation Services Routers]*. (б. д.). Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-6/sec-flex-vpn-xe-16-6-book/sec-cfg-ikev2-flex.html#GUID-5C063DFB-B2F2-40C1-85F9-741C0035C979