ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ РІШЕННЯ ВІДДАЛЕНОГО ДОСТУПУ VPN»

Виконав: студент 6 курсу, групи БСДМ-63
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Гінько А.О.
(прізвище та ініціали)

Керівник Довженко Н.М.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ВСТУП

Актуальність дослідження. З тих пір, як існує Інтернет, існувала потреба в протоколах для збереження конфіденційності та безпеки даних. Історія технології VPN (віртуальна приватна мережа) починається з 1996 року, коли співробітник Microsoft розробив протокол однорангового тунелювання або PPTP.

З розвитком Інтернету виник попит на більш складні системи безпеки. Антивірусне та пов'язане з ним програмне забезпечення може бути ефективним у запобіганні пошкодженням на рівні кінцевого користувача, але справді необхідно було покращити безпеку самого з'єднання. Ось тут і з'явилися VPN.

Мета VPN – створити приватне з'єднання між кількома людьми та пристроями в Інтернеті.

Сьогодні VPN використовуються для захисту інтернет-з'єднань, запобігання зловмисному програмному забезпеченню та злому, забезпечення цифрової конфіденційності, розблокування геообмеженого вмісту та приховування фізичного місцезнаходження користувачів. Простіший у використанні та доступніший, ніж будь-коли, VPN — це важливий інструмент для забезпечення безпеки в Інтернеті.

Об'єкт дослідження – забезпечення інформаційної безпеки корпоративної мережі.

Предмет дослідження – технології забезпечення безпеки корпоративної мережі на основі рішення віддаленого доступу VPN.

Мета роботи – розроблення рекомендацій щодо покрокового налаштування роботи рішення віддаленого доступу VPN у середовищі корпоративної мережі.

Наукові завдання:

- визначити проблематику інформаційного захисту корпоративних мереж;
- дослідити принципи роботи, функціональні особливості рішення віддаленого доступу VPN;

- інтегрування та оптимізація рішення віддаленого доступу VPN у середовищі корпоративної мережі.

Методи дослідження – методи теорії інформації, методи системного аналізу, алгоритми створення та роботи корпоративної мережі, вивчення принципів роботи рішення віддаленого доступу VPN.

Практичне значення одержаних результатів: дослідження роботи продукту та рекомендації щодо захисту можуть бути використані у сфері забезпечення кібербезпеки у корпоративних мережах.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ СУЧАСНИХ ЗАВДАНЬ ТА ЦІЛЕЙ ВИКОРИСТАННЯ VPN

1.1. VPN як рішення забезпечення безпеки корпоративної мережі

VPN — це як локальна мережа, мережа, у якій пристрої безпосередньо під'єднані до кожного, не потребуючи Інтернету, окрім використання Інтернету для встановлення з'єднань. Окрім протоколів тунелювання, які встановлюють безпечні з'єднання, приховуючи вихідне джерело, високорівневі стандарти шифрування гарантують, що навіть у разі втрати даних вони ніколи не будуть використані тими, хто їх не мав [1].

Переваги VPN для окремих користувачів Інтернету стали очевидними з самого початку, і це породило сучасний порив надавати найкращу технологію VPN. Протягом багатьох років розвиток VPN стимулювався вторгненнями цензорів у всьому світі та нескінченним бажанням зламувати будь-які пристрої та підключення, які вони можуть.

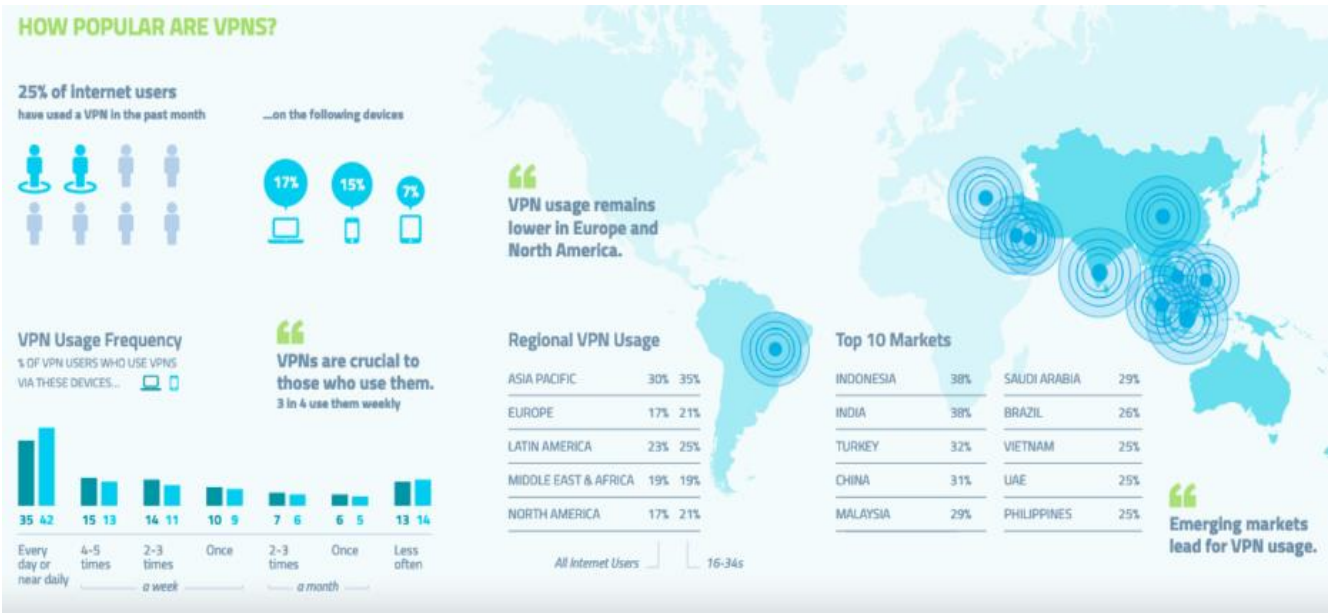

Рис. 1.1. Тенденція попиту VPN мереж

Цензура та геообмеження є однією з кількох проблем, які турбують Інтернет і стимулюють інновації в технології VPN. Історія цензури різниться від випадку

до випадку, але включає такі речі, як блокування соціальних медіа, неповний доступ до онлайн-каталогів медіа (звернути увагу на каталог Netflix США в порівнянні з каталогом, доступним для решти світу), відстеження активності користувачів, моніторинг електронних листів або повну відмову доступу до мережі Інтернет.

Терміни ретранслція та комутація пакетів є відмінною рисою технології віддаленого підключення та призвели до сучасних протоколів «точка-точка» та створення VPN. Інтернет дозволяє підключати все, а в рамках ширшої тканини глобального зв'язку розташовані менші виділені мережі, які забезпечують підвищену безпеку. Вони роблять це просто: VPN з'єднує віддалені місця через загальнодоступну мережу.

Існує два основних типи VPN: IPsec і SSL [2]:

- IPsec означає Internet Protocol Security і є стандартним типом VPN, який використовується для створення з'єднань між двома мережами та окремими пристроями з мережами. Цей трафік зашифрований і автентифікований, і, оскільки він працює на рівні IP, є найкращим доступним VPN загального призначення, що забезпечує наскрізну безпеку на всіх рівнях підключення. Єдина проблема з IPsec полягає в тому, що реалізація може відрізнятися від постачальника до постачальника, що спричиняє труднощі під час підключення. Рекомендується використовувати VPN з того самого джерела або мати під рукою IT-фахівця.

- SSL, Secure Socket Layer, є формою VPN, яку більшість користувачів Інтернету вже використовують і навіть не підозрюють про це. Цей протокол використовується для підключення одного користувача до веб-порталу, наприклад електронної комерції. Він створює зашифроване з'єднання VPN, захищаючи транзакції та втрату даних. SSL використовує веб-браузер для свого інтерфейсу, що полегшує розгортання малим і середнім підприємствам. Недоліком є обмеження функціональності, які роблять з'єднання IPsec більш практичним для складних програм.

VPN надають організації, які хочуть підтримувати віддалених працівників і сайти, кілька переваг, зокрема:

- Безпечне з'єднання: мережі VPN забезпечують зашифроване з'єднання між віддаленим користувачем і мережею підприємства. Це захищає від прослуховування та зменшує ризик зараження віддаленого користувача шкідливим програмним забезпеченням.
- Спрощені розподілені мережі: користувач, будь то віддалений працівник чи філія, має зашифроване з'єднання з мережею головного офісу. VPN-з'єднання забезпечують роботу користувача, майже ідентичну прямому підключенню до мережі штаб-квартири, що спрощує проектування та впровадження розподілених мереж.
- Контроль доступу: VPN вимагає автентифікації, перш ніж користувач зможе отримати доступ до ресурсів у корпоративній мережі. Це допомагає захистити від несанкціонованого доступу до корпоративних активів.
- Запобігання регулюванню даних: VPN обмежує доступ сторонніх до даних, що передаються через зашифрований канал. Це може допомогти захистити від обмеження певних типів мережевого трафіку.
- Зменшення витрат на підтримку: надаючи користувачам безпечний доступ до ресурсів корпоративної мережі та хмарної інфраструктури, VPN консолідують корпоративні активи, спрощуючи їх моніторинг і обслуговування.
- Масштабованість мережі: мережі VPN дозволяють організації легко об'єднувати розподілені мережі через загальнодоступний Інтернет за допомогою зашифрованих каналів. Це дає змогу організації легко масштабувати свою мережу, розглядаючи її як єдину приватну мережу.

Правильне безпечне рішення віддаленого доступу забезпечує значні переваги для організації, але неправильне рішення може стати серйозною проблемою. Деякі загальні недоліки рішень VPN включають:

- Низька швидкість з'єднання: VPN вимагає автентифікації та встановлення з'єднання між віддаленим користувачем і сервером VPN у

корпоративній мережі. Це може спричинити низьку швидкість з’єднання. Тайм-аути сеансу означають, що автентифікація може відбуватися часто.

- Складне налаштування та керування: VPN реалізує з’єднання «точка-точка», що підключає віддаленого користувача або сайт до корпоративної мережі. Це може створити складну мережеву інфраструктуру, яку важко розгорнути, налаштувати та керувати нею.
- Погана взаємодія з користувачем: деякі рішення VPN важко налаштувати, і вони можуть не підтримуватися на певних пристроях і операційних системах. Це призводить до поганої взаємодії з користувачем, що може спонукати користувачів порушувати корпоративну політику.
- Загрози безпеці: VPN призначений для надання віддаленому користувачеві безпечного з’єднання та повного доступу до корпоративної мережі. VPN не включає контроль доступу чи будь-яку перевірку безпеки, тобто не захищає від зламаних облікових записів, викрадання даних, зловмисного програмного забезпечення чи інших ризиків безпеці.

1.2. Основні складові VPN мереж

VPN базується на трьох основних методах, які застосовуються при реалізації заходів безпеки в мережах:

1. Тунелювання.
2. Аутентифікація.
3. Шифрування.

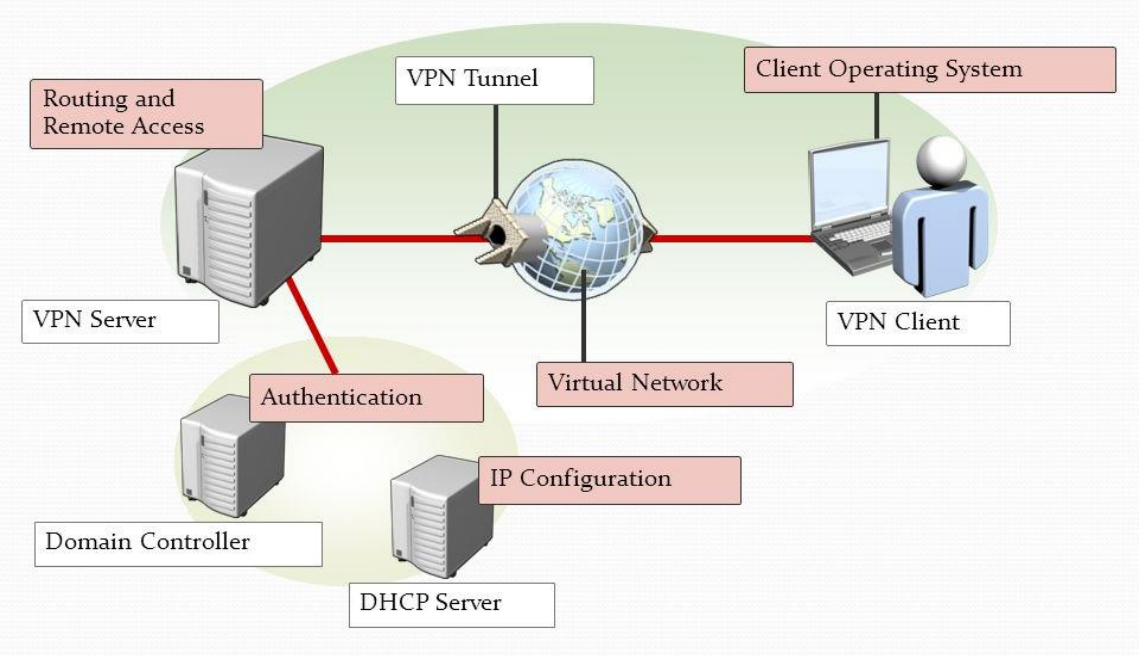

Рис. 1.2. Компоненти VPN

1.2.1. Тунелювання

Тунелювання забезпечує передачу шифрованих даних між двома точками - таким чином, що для выдправника і приймача даних виявляється прихованою вся мережева система, що лежить між ними цими точками.

Транспортне середовище тунелю, підхоплює дані використовуваного мережевого протоколу на вході в тунель і без змін доставляє їх до виходу. Побудови тунелю достатньо для того, щоб з'єднати два мережевих вузла так, що з точки зору працюючого на них програмного забезпечення вони виглядали підключеними до однієї (локальної) мережі. Однак не можна забувати, що насправді тунель з даними проходить через безліч проміжних маршрутизаторів відкритої глобальної мережі [3].

Такий стан справ має дві проблеми. Перша полягає в тому, що передається через тунель інформація може бути перехоплена правопорушниками. За допомогою тунелювання пакети даних транслюються через загальнодоступну мережу як по звичайному з'єднанню «точка-точка». Між кожною парою «відправник-отримувач даних» встановлюється своєрідний тунель - безпечне

логічне з'єднання, що дозволяє инкапсулировать дані одного протоколу в пакети іншого. Основними компонентами тунелю є [3]:

• відправник(ініціатор з'єднання);

• маршрутизатор мережі;

• тунельний комутатор;

• один або кілька тунельних термінаторів.

Якщо інформація конфіденційна (номери банківських карток, фінансові звіти, відомості особистого характеру), то цілком реальна загроза її компрометації, що вже неприємно. Гірше того, зловмисники мають можливість модифікувати передаються через тунель дані так, що одержувач не зможе перевірити їх достовірність.

Тунель в чистому вигляді придатний хіба що для деяких типів мережевих комп'ютерних ігор і не може претендувати на більш серйозне застосування. Обидві проблеми вирішуються сучасними засобами криптографічного захисту інформації. Щоб перешкодити внесенню несанкціонованих змін в пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису (ЕЦП). Суть методу полягає в тому, що кожен переданий пакет даних забезпечується додатковим блоком інформації, який виробляється у відповідності з асиметричним криптографічним алгоритмом і унікальний для вмісту пакета і секретного ключа ЕЦП відправника. Цей блок інформації є ЕЦП пакета і дозволяє виконати аутентифікацію даних одержувачем, якому відомий відкритий ключ ЕЦП відправника. Захист переданих через тунель даних від несанкціонованого перегляду досягається шляхом використання сильних алгоритмів шифрування.

1.2.2. Аутентифікація

Забезпечення безпеки є основною функцією VPN. Всі дані від комп'ютерів-клієнтів проходять через Internet до VPN-сервера. Такий сервер може знаходитися на великій відстані від клієнтського комп'ютера, і дані на шляху до мережі

організації проходять через обладнання безлічі провайдерів. Для цього застосовуються різні методи аутентифікації і шифрування.

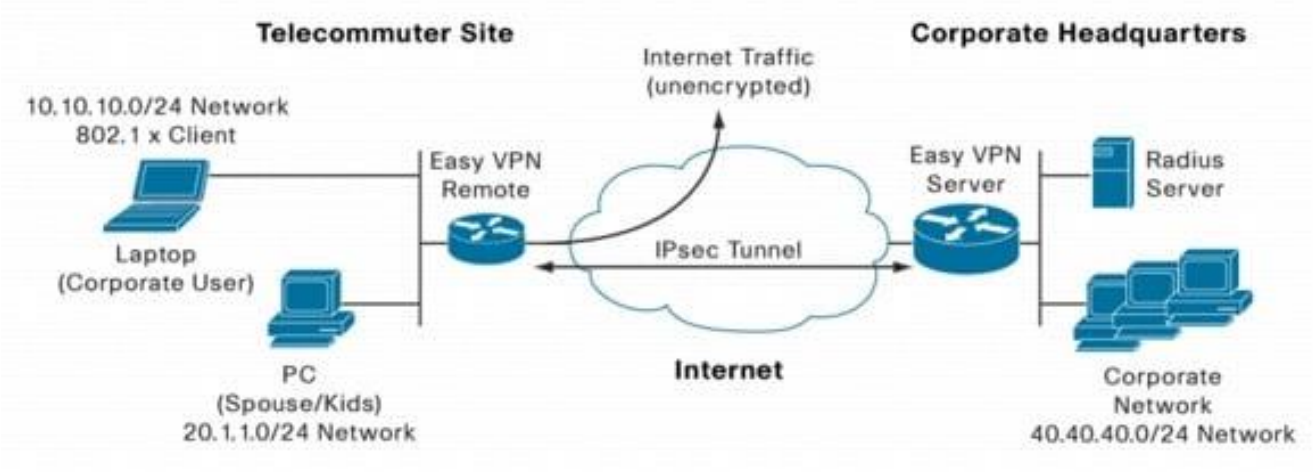

Рис. 1.3. Аутентифікація користувача в VPN мережах

Для аутентифікації користувачів PPTP може використовувати будь-який з протоколів [4]:

- EAP або Extensible Authentication Protocol;
- MSCHAP або Microsoft Challenge Handshake Authentication Protocol (версії 1 і 2);
- CHAP або Challenge Handshake Authentication Protocol;
- SPAP або Shiva Password Authentication Protocol;
- PAP або Password Authentication Protocol.

Кращими вважаються протоколи MSCHAP версії 2 і Transport Layer Security (EAP-TLS), оскільки вони забезпечують взаємну аутентифікацію, тобто VPN-сервер і клієнт ідентифікують один одного. У всіх інших протоколах тільки сервер проводить аутентифікацію клієнтів.

Хоча PPTP це один із найстаріших протоколів VPN забезпечує достатній ступінь безпеки, але все ж L2TP поверх IPSec надійніше.

Таблиця 1.1.

Характеристики протоколу PPTP

Сумісність платформи	Windows, macOS, Android, iOS, Linux та ін
Шифрування VPN	До 128-розрядних
Шифрування стандарту безпеки VPN	Відомі вразливості
Швидкість VPN	Висока швидкість через нижчий рівень шифрування.

L2TP поверх IPSec забезпечує аутентифікацію на рівнях «користувач» і «комп'ютер», а також виконує аутентифікацію і шифрування всіх даних.

Аутентифікація здійснюється або в відритому вигляді (clear text password), або за наступною схемою: запит-відгук. Клієнт посилає серверу пароль. Сервер порівнює це з своєю таблицею і або забороняє доступ, або відповідає підтвердженням. Відкрита аутентифікація практично не зустрічається.

Схема запит-відгук набагато більш застосована. В загальному вигляді вона виглядає так [2]:

- клієнт посилає серверу запит (request) на аутентифікацію;

- сервер повертає свій відгук (challenge);

- клієнт знімає зі свого пароля хеш (хешем називається результат хеш-функції, яка перетворює вхідний масив даних довільної довжини в вихідну бітову комбінацію фіксованої довжини), шифрує їм challenge і передає його серверу;

- те ж саме проробляє і сервер, порівнюючи отриманий результат з відповіддю ініціатора;

- якщо зашифрований запит збігається, аутентифікація вважається успішною.

На першому етапі аутентифікації клієнтів і серверів VPN, L2TP поверх IPSec використовує локальні сертифікати, отримані від служби сертифікації. Клієнт і сервер обмінюються сертифікатами і створюють захищений коннект ESP SA (security association). Після того як L2TP (поверх IPSec) завершує процес аутентифікації комп'ютера, виконується аутентифікація на рівні користувача. Для аутентифікації можна задіяти будь-який протокол, навіть PAP, що передає ім'я

користувача та пароль у незашифрованому вигляді. Це цілком безпечно, так як L2TP поверх IPSec шифрує всю сесію. Проте проведення аутентифікації користувача при допомоги MSCHAP, що застосовує різні ключі шифрування для аутентифікації комп'ютера і користувача, може посилити захист.

Таблиця 1.2.

Характеристики протоколу L2TP/IPsec

Сумісність із платформою	Windows, macOS, Android, iOS, Linux та ін
Шифрування VPN	До 256-бітного
Сильне шифрування VPN Security	Сильна цілісність даних
Швидкість VPN	Відносно повільна завдяки обробці даних процесором

1.2.3. Шифрування

Шифрування гарантує, що майже ніхто не зможе отримати доступ до пакетів при пересиланні через Internet.

В даний час підтримуються два методи шифрування [4]:

1. Протокол MPPE шифрування або Microsoft Point-to-Point Encryption сумісний тільки з MSCHAP.

2. EAP-TLS автоматично вибирає довжину ключа шифрування при узгодженні параметрів між клієнтом і сервером.

MPPE працює з ключами довжиною 32, 40, 56, 64, 72, 128 або 256 біт. Операційні системи Windows підтримують шифрування з довжиною ключа тільки 32 та 40 біт, тому в змішаному середовищі Windows слід вибирати довжину ключа яка підтримується усіма пристроями.

Протокол MPPE розроблявся для каналів зв'язку точка-точка, в яких пакети передаються послідовно, і втрата пакетів неможлива. У цій ситуації значення ключа для чергового пакета залежить від результатів дешифрування попереднього пакета. При побудові віртуальних мереж через мережі загального доступу цих умов дотримуватися неможливо, так як пакети даних часто приходять до одержувача не в тій послідовності, в якій були відправлені.

Тому PPTP використовує для зміни ключа шифрування порядкові номери пакетів. Це дозволяє виконувати дешифрацію незалежно від попередніх прийнятих пакетів.

Таким чином, зв'язка тунелювання-автентифікація-шифрування» дозволяє передавати дані між двома точками через мережу загального користування, моделюючи роботу приватної (локальної) мережі. Іншими словами, розглянуті засоби дозволяють побудувати віртуальну приватну мережу.

Додатковим приємним ефектом VPN-з'єднання є можливість (і навіть необхідність) використання системи адресації, прийнятої в локальній мережі.

Реалізація віртуальної приватної мережі на практиці виглядає таким чином. У локальній обчислювальній мережі офісу фірми встановлюється сервер VPN. Віддалений користувач (або маршрутизатор, якщо здійснюється з'єднання двох офісів) з використанням клієнтського програмного забезпечення VPN ініціює процедуру з'єднання з сервером.

Відбувається аутентифікація користувача - перша фаза встановлення VPN-з'єднання. У разі підтвердження повноважень настає друга фаза - між клієнтом і сервером виконується узгодження деталей забезпечення безпеки з'єднання. Після цього організується VPN-з'єднання, що забезпечує обмін інформацією між клієнтом і сервером у формі, коли кожен пакет з даними проходить через процедури шифрування / дешифрування та перевірки цілісності - аутентифікації даних.

Основною проблемою мереж VPN є відсутність установлених стандартів аутентифікації і обміну шифрованого інформацією. Ці стандарти все ще знаходяться в процесі розробки і тому продукти різних виробників не можуть встановлювати VPN-з'єднання і автоматично обмінюватися ключами.

Дана проблема тягне за собою уповільнення розповсюдження VPN, так як важко змусити різні компанії користуватися продукцією одного виробника, а тому ускладнений процес об'єднання мереж компаній-партнерів в, так звані, extranet-мережі.

1.3. Вектори атак

Починаючи з віддаленого користувача та після підключення до даних або служби, віддалений доступ може бути скомпрометовано в будь-якому з наступних моментів:

• Користувача або систему можна видати за себе, щоб обдурити цільову систему;

• Зловмисник може використовувати захоплені або вгадані облікові дані, щоб видати себе за користувача;

• Зловмисник може залякати або змусити користувача надати дійсні облікові дані або виконати дії на вимогу зловмисника;

• Пристрій доступу користувача (ноутбук, КПК тощо) може бути атаковано та скомпрометовано та використано для доступу до мережі системи управління;

• Зловмисник може видати себе за цільову систему, щоб обдурити користувача й таким чином отримати вигоду-облікові дані або інша інформація з системи користувача;

• Комунікація може бути прослухана третіми особами будь-де вздовж комунікації ланцюга;

• Зв'язок може бути перерваний або забитий;

• Зловмисники можуть вводити дані в комунікації [6];

• Зв'язок може бути зламаний після того, як він був ініційований (не покладається на видавання себе за іншу особу) або перехоплено під час ініціації (видавати себе за користувача та ціль, також відома як атака «людина посередині»);

• Частини повідомлення можуть бути відтворені для цілі, навіть якщо зловмисник не може розшифрувати вміст (також відомий як атака повтору);

• Цільове комунікаційне програмне забезпечення, яке прослуховує запити, може зазнати атаки та потенційно скомпрометоване;

• Зловмисник може видати себе за дійсний комунікаційний вузол і отримати доступ до базового середовища зв'язку;

• Атака типу «відмова в обслуговуванні» на сервер автентифікації (наприклад, радіус-сервер або RAS);

• Атака типу «відмова в обслуговуванні» на пристрій зовнішнього зв'язку (наприклад, банк модемів, зовнішній маршрутизатор для віддаленого доступу) [5].

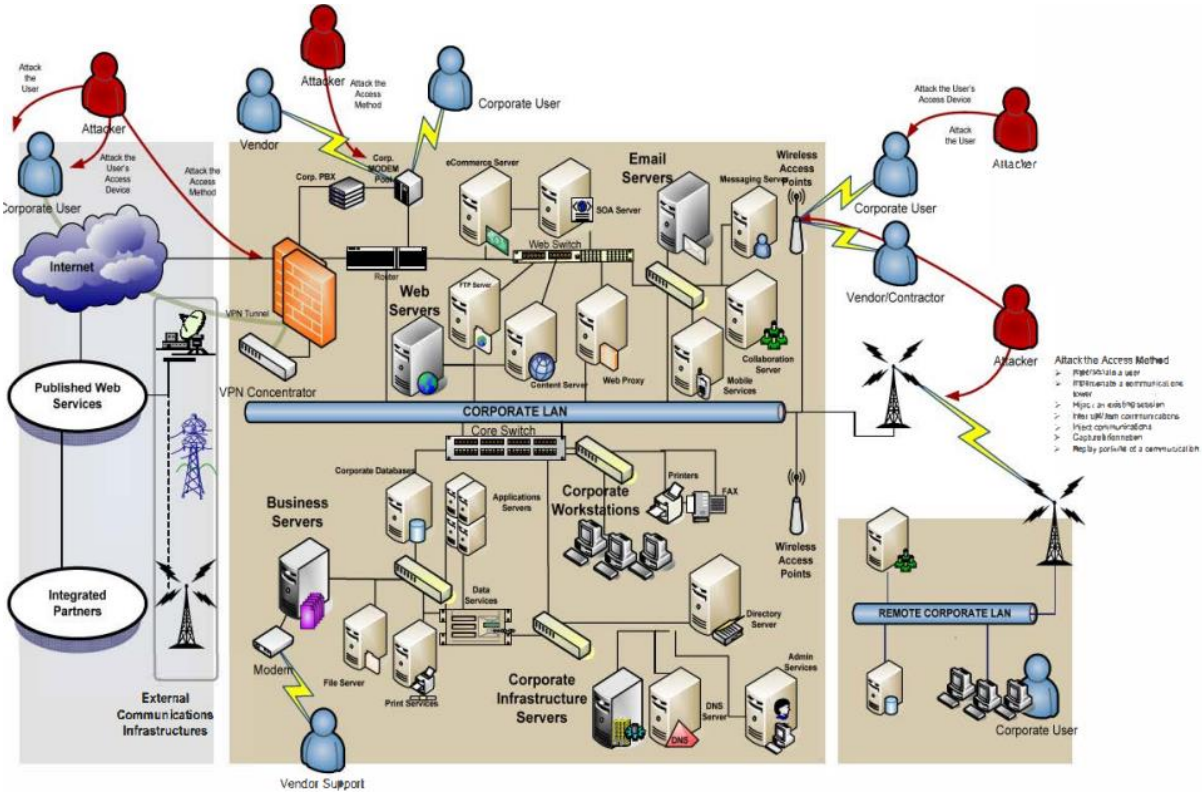

Рис. 1.4. Вектори атак каналу VPN мережах

Висновки до першого розділу

Розглянуто загальну технологію організації VPN підключення до мережі передачі даних, побудову розподільної мережі та віддалений доступ до мережі.

Досліджено, що схеми віддаленого доступу можуть відрізнятися також і типом служб, які підтримуються для віддаленого клієнта. Найчастіше використовується віддалений доступ до файлів, баз даних, принтерів в тому ж стилі, до якого користувач звик при роботі в локальній мережі.

Зазначено, що при віддаленому доступі реалізується обмін з центральною мережею повідомленнями електронної пошти, за допомогою якого можна в автоматичному режимі отримати запрошувані корпоративні дані.

Розглянуто, що особливе місце серед всіх видів віддаленого доступу до комп'ютера є спосіб, при якому користувач має можливість віддалено працювати з комп'ютером таким самим чином, ніби він управляв їм за допомогою локального підключеного терміналу. У цьому режимі він може запускати виконання програми на віддаленому комп'ютері і бачити результати роботи у прямому часі. При цьому прийнято розділяти такий спосіб доступу на термінальний доступ і віддалене управління.

2 ДОСЛІДЖЕННЯ РІШЕННЯ ВІДДАЛЕНОГО ДОСТУПУ VPN У ЯКОСТІ МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ТА КОНТРОЛЮ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

2.1. Віддалений доступ IPSec VPN

Віддалений доступ IPSec VPN забезпечує безпечні зашифровані з’єднання між приватною мережею компанії та віддаленими користувачами шляхом встановлення зашифрованого тунелю IPSec через Інтернет за допомогою широкосмугового кабелю, DSL або комутованого з’єднання [7].

Віддалений доступ IPSec VPN складається з клієнта VPN і головного пристрою VPN або шлюзу VPN. Клієнтське програмне забезпечення VPN знаходиться на робочій станції користувача та ініціює доступ через тунель VPN до корпоративної мережі. На іншому кінці VPN-тунелю знаходиться VPN-шлюз на краю корпоративного сайту [8].

Коли клієнт VPN ініціює підключення до пристрою шлюзу VPN, узгодження складається з автентифікації пристрою через Інтернет-обмін ключами (IKE), а потім автентифікації користувача за допомогою розширеної автентифікації IKE (Xauth). Далі профіль групи надсилається VPN-клієнту за допомогою конфігурації режиму, і для завершення VPN-з’єднання створюється асоціація безпеки IPsec (SA).

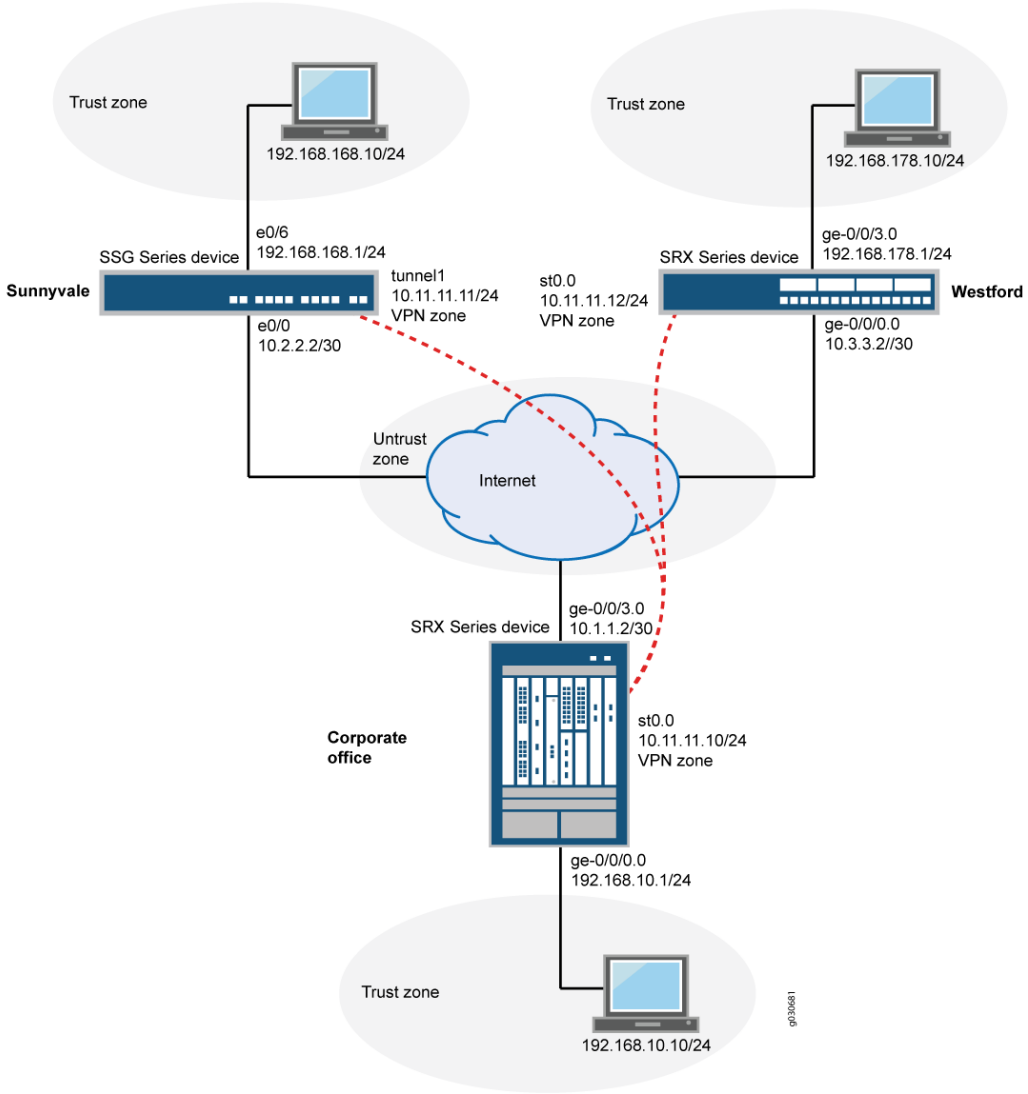

Рис. 2.1. Віддалений доступ IPSec VPN

Для віддаленого доступу IPSec VPN для безпечного доступу використовується AAA (автентифікація, авторизація та облік). При автентифікації користувача перед встановленням з'єднання потрібно ввести дійсне ім'я користувача та пароль.

Імена користувачів і паролі можна зберігати на самому пристрої VPN або на зовнішньому сервері AAA, який може забезпечувати автентифікацію для багатьох інших баз даних. Щоб отримати додаткові відомості про використання серверів AAA.

2.2. Віддалений доступ SSL VPN

Функція SSL VPN дозволяє користувачам отримувати доступ до корпоративних мереж з будь-якого місця з підтримкою Інтернету, використовуючи лише веб-браузер, який нативно підтримує шифрування Secure Socket Layer (SSL), без необхідності програмного чи апаратного клієнта.

Використовуючи веб-браузер із підтримкою SSL, віддалений користувач встановлює з'єднання зі шлюзом SSL VPN. Після автентифікації віддаленого користувача на безпечному шлюзі через веб-браузер встановлюється сеанс SSL VPN, і користувач може отримати доступ до внутрішньої корпоративної мережі. Сторінка порталу дозволяє користувачам отримати доступ до всіх ресурсів, доступних у мережах SSL VPN.

На пристроях ASA віддалені користувачі встановлюють безпечний VPN-тунель віддаленого доступу до пристрою безпеки за допомогою веб-браузера. Протокол SSL забезпечує безпечне з'єднання між віддаленими користувачами та певними підтримуваними внутрішніми ресурсами, які ви налаштовуєте на центральному сайті. Пристрій безпеки розпізнає з'єднання, які потребують проксі-сервері, а сервер HTTP взаємодіє з підсистемою автентифікації для автентифікації користувачів.

Автентифікація користувача може здійснюватися за допомогою імен користувачів і паролів, сертифікатів або обох [9].

Працівник може отримати доступ до захищених ресурсів із головного офісу та філій. З'єднання IPsec між основними та віддаленими сайтами не змінюється. Для безпечного доступу до корпоративної мережі працівнику потрібен лише доступ до Інтернету та підтримуване програмне забезпечення (веб-браузер і операційна система) (рис.2.2).

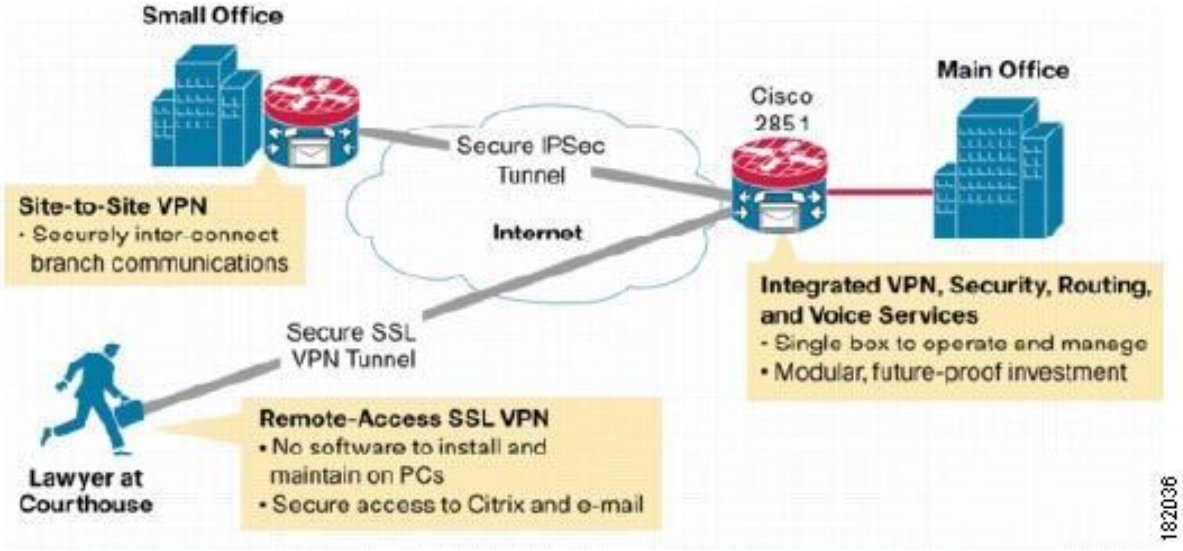

Рис. 2.2. Захищений доступу SSL VPN

SSL VPN забезпечує три режими віддаленого доступу на маршрутизаторах IOS: Clientless, Thin Client і Full Client. На пристроях ASA є два режими: безклієнтський (включає переадресацію портів без клієнта та тонкого клієнта) і клієнт AnyConnect (який замінює повний тунель) [10]:

1. *Безклієнтський режим доступу*. У безклієнтському режимі віддалений користувач отримує доступ до внутрішньої або корпоративної мережі за допомогою веб-браузера на клієнтській машині. Завантажувати аплет не потрібно.

Безклієнтський режим корисний для доступу до більшості вмісту, який очікується у веб-браузері, наприклад доступу до Інтернету, баз даних та онлайн-інструментів, які використовують веб-інтерфейс. Він підтримує перегляд веб-сторінок (за допомогою HTTP і HTTPS), обмін файлами за допомогою загальної файлової системи Інтернету (CIFS) і електронну пошту Outlook Web Access (OWA).

Користувачі SSL VPN на основі браузера, які підключаються з операційних систем Windows, можуть переглядати спільні файлові системи та виконувати такі операції: переглядати папки, переглядати властивості папок і файлів, створювати, переміщувати, копіювати, копіювати з локального хоста на віддалений хост, копіювати з віддалений хост на локальний хост і видалити. Internet Explorer вказує, коли веб-папка доступна. Під час доступу до цієї папки відкривається

інше вікно, що забезпечує перегляд спільної папки, у якій користувачі можуть виконувати функції веб-папки, припускаючи, що властивості папок і документів це дозволяють.

2. *Режим доступу тонкого клієнта*. Режим тонкого клієнта, також званий перенаправленням портів TCP, передбачає, що клієнтська програма використовує TCP для підключення до добре відомого сервера та порту. У цьому режимі віддалений користувач завантажує аплет Java, натиснувши посилання на сторінці порталу. Аплет Java діє як TCP-проксі на клієнтській машині для служб, налаштованих на шлюзі SSL VPN. Аплет Java запускає нове підключення SSL для кожного підключення клієнта.

Аплет Java ініціює запит HTTP від клієнта віддаленого користувача до шлюзу SSL VPN. Ім’я та номер порту внутрішнього сервера електронної пошти включено до запиту HTTP. Шлюз SSL VPN створює TCP-з’єднання з цим внутрішнім сервером електронної пошти та портом.

Режим тонкого клієнта розширює можливості криптографічних функцій веб-браузера, щоб забезпечити віддалений доступ до програм на основі TCP, таких як протокол поштового відділення версії 3 (POP3), простий протокол передачі пошти (SMTP), протокол доступу до повідомлень в Інтернеті (IMAP), Telnet і Secure Shell (SSH).

Використовуючи режим тонкого клієнта необхідно розуміти [11]:

- Віддалений користувач має дозволити завантажувати та інсталювати аплет Java.
- Щоб програми переадресації портів TCP працювали безперебійно, віддаленим користувачам мають бути дозволені адміністративні привілеї.
- Неможливо використовувати режим тонкого клієнта для таких програм, як FTP, де порти узгоджуються динамічно. Тобто ви можете використовувати переадресацію портів TCP лише зі статичними портами [12].

3. *Повний тунельний режим клієнтського доступу*. Режим повного тунельного клієнта забезпечує повний доступ до корпоративної мережі через тунель SSL VPN, який використовується для переміщення даних на рівні мережі

(IP). Цей режим підтримує більшість IP-програм, таких як Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail і Telnet. Бути частиною SSL VPN є абсолютно прозорим для програм, які працюють на клієнті. Завантажується аплет Java для тунелювання між клієнтським хостом і шлюзом SSL VPN. Користувач може використовувати будь-яку програму так, ніби клієнтський хост знаходиться у внутрішній мережі.

Тунельне підключення визначається конфігурацією групової політики. Клієнт SSL VPN (SVC) завантажується та встановлюється на віддаленому клієнті, а тунельне з'єднання встановлюється, коли віддалений користувач входить до шлюзу SSL VPN. За замовчуванням SVC видаляється з віддаленого клієнта після закриття з'єднання, але ви можете залишити його встановленим, якщо потрібно.

2.3. Керування файлами підтримки SSL VPN

SSL VPN іноді потребують допоміжних файлів, які зберігаються у флеш-пам'яті пристрою. Особливо це стосується SSL VPN, налаштованих на пристроях ASA. Допоміжні файли включають пакети Cisco Secure Desktop (CSD), образи клієнтів AnyConnect і файли плагінів. Security Manager містить багато з цих файлів для корпоративного використання. Однак деякі допоміжні файли, такі як графічні файли, використовуються для сторінок порталу, або профілі клієнтів, які використовуються для клієнтів AnyConnect, не надаються Security Manager.

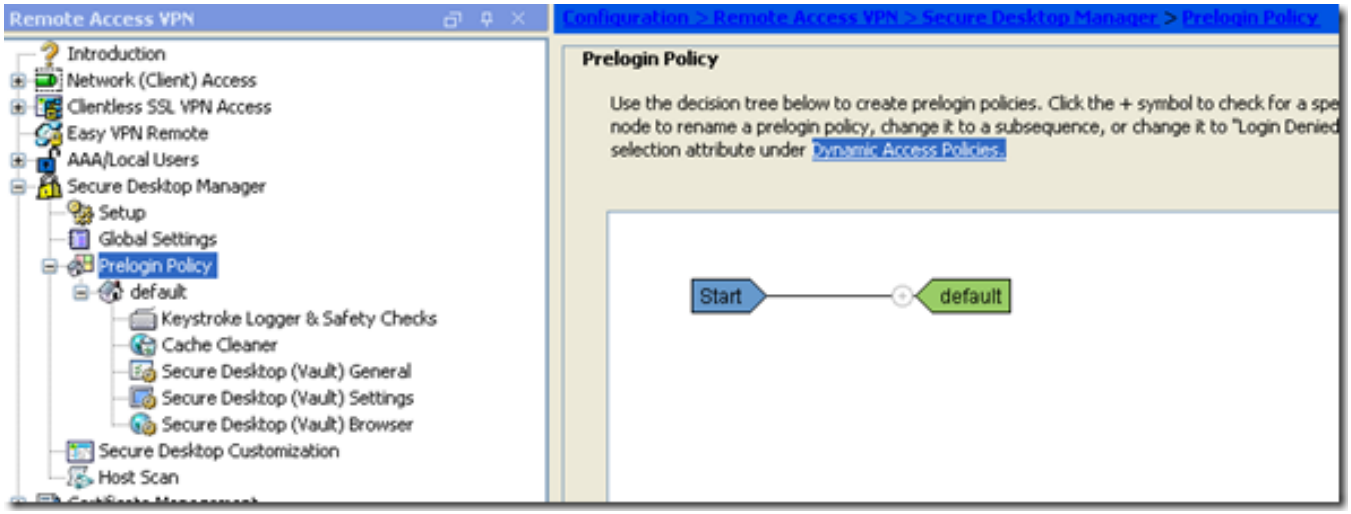

Рис. 2.3. Керування файлами підтримки SSL VPN

Як правило, потрібно створити об’єкт File, щоб указати допоміжний файл, а потім вибрати об’єкт File під час створення політики, яка посилається на нього. Можливо створити об’єкти файлів, які необхідні під час створення політик, або можливо створити їх до початку визначення політик.

Коли розгортаються політики на пристроях, усі допоміжні файли, на які посилаються корпоративні політики, копіюються на пристрій і розміщуються у флеш-пам’яті в папці \csm. Здебільшого співробітнику не потрібно виконувати ручну роботу, щоб це сталося. Нижче наведено кілька ситуацій, коли може знадобитися ручна робота [13]:

• Якщо необхідно виявити існуючі політики SSL VPN або знову відкрити їх, посилання на файли з політик SSL VPN мають бути правильними.

• Якщо налаштований пристрій ASA у конфігурації Active/Failover, необхідно отримати допоміжні файли на пристрій відновлення після відмови. Допоміжні файли не копіюються на пристрій відновлення після відмови під час відновлення. Варіанти передачі файлів на пристрій відновлення після відмови:

– Вручну скопіювати файли з папки \csm на активному пристрої до блоку відновлення після відмови.

– Після розгортання політик на активному блоці примусово перемикатися після відмови та повторно розгорнути політики на тепер активному блоці.

- Якщо використовується кластер VPN для балансування навантаження, однакові допоміжні файли мають бути розгорнуті на всіх пристроях у кластері.

2.4. Параметри клієнта SSL VPN

Клієнт VPN Cisco AnyConnect забезпечує безпечні з’єднання SSL із пристроєм безпеки для віддалених користувачів. Клієнт надає віддаленим користувачам переваги клієнта SSL VPN без необхідності мережевим адміністраторам встановлювати та налаштовувати клієнти на віддалених комп’ютерах.

Без попередньо встановленого клієнта віддалені користувачі вводять IP-адресу у своєму браузері інтерфейсу, налаштованого на прийом з'єднань SSL VPN. Якщо пристрій безпеки не налаштовано на перенаправлення запитів http:// на https://, користувачі повинні вводити URL у формі https:// <*адреса*-> .

Після введення URL-адреси браузер підключається до цього інтерфейсу та відображає екран входу. Якщо користувач виконує вхід і автентифікацію, а пристрій безпеки визначає, що користувач потребує клієнта, він завантажує клієнт, який відповідає операційній системі віддаленого комп'ютера. Після завантаження клієнт інсталюється та налаштовується, встановлює безпечне з'єднання SSL і залишається або видаляється (залежно від конфігурації пристрою безпеки), коли з'єднання припиняється.

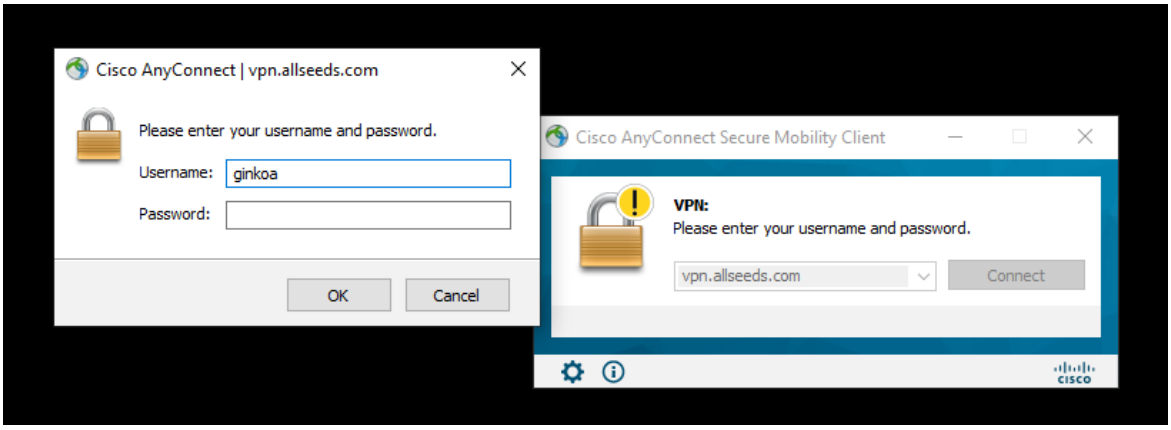

Рис. 2.4. Форма VPN Cisco AnyConnect

У випадку попередньо встановленого клієнта, коли користувач автентифікується, пристрій безпеки перевіряє версію клієнта та оновлює клієнта за необхідності.

Коли клієнт узгоджує з'єднання SSL VPN із пристроєм безпеки, він підключається за допомогою безпеки транспортного рівня (TLS) і, за бажанням, захисту транспортного рівня датаграм (DTLS). DTLS дозволяє уникнути проблем із затримкою та пропускною здатністю, пов'язаних із деякими з'єднаннями SSL, і покращує продуктивність програм реального часу, чутливих до затримок пакетів.

Клієнт AnyConnect можна завантажити з пристрою безпеки або вручну встановити на віддаленому ПК системним адміністратором.

Пристрій безпеки завантажує клієнт на основі групової політики або атрибутів імені користувача користувача, який встановлює з’єднання. Можливо налаштувати пристрій безпеки на автоматичне завантаження клієнта або налаштувати його так, щоб віддалений користувач запитував, чи слід завантажувати клієнт. В останньому випадку, якщо користувач не відповідає, можливо налаштувати пристрій безпеки або на завантаження клієнта після періоду очікування, або на показ сторінки входу [14].

AnyConnect Essentials — це окремо ліцензований SSL VPN-клієнт, повністю налаштований на пристрої адаптивної безпеки, який надає повні можливості AnyConnect, за такими винятками:

- Без CSD (включаючи HostScan/Vault/Cache Cleaner)
- Без клієнтської SSL VPN
- Додаткова підтримка Windows Mobile

Профіль клієнта AnyConnect — це група параметрів конфігурації, що зберігаються у файлі XML, які клієнт використовує для налаштування записів підключення, які відображаються в інтерфейсі користувача клієнта. Ці параметри (теги XML) містять імена та адреси хост-комп’ютерів і налаштування для ввімкнення додаткових функцій клієнта.

Інсталяція клієнта AnyConnect включає шаблон профілю під назвою *AnyConnectProfile.tmpl* , який можна редагувати за допомогою текстового редактора та використовувати як основу для створення інших файлів профілю.Можливо встановити додаткові параметри, недоступні через інтерфейс користувача. Інсталяція також включає повний файл схеми XML під назвою *AnyConnectProfile.xsd* .

Після створення профілю необхідно завантажити файл на пристрій безпеки та налаштувати пристрій безпеки для завантаження його на віддалені клієнтські ПК. Після завантаження файлу в кеш-пам'ять профіль стає доступним для групових політик і атрибутів імен користувачів клієнтів.

2.5. Групові політики (ASA)

Коли налаштовується підключення IPSec або SSL VPN віддаленого доступу, необхідно створити групи користувачів, до яких належатимуть віддалені клієнти. Групова політика користувача — це набір орієнтованих на користувача пар атрибут/значення для VPN-з'єднань віддаленого доступу, які зберігаються або внутрішньо (локально) на пристрої, або зовні на сервері AAA. Профіль підключення використовує групову політику користувачів, яка встановлює умови підключення користувачів після встановлення підключення. Групові політики дозволяють застосовувати цілі набори атрибутів до користувача або групи користувачів замість того, щоб вказувати кожен атрибут окремо для кожного користувача [15].

Політики динамічного доступу мають пріоритет над груповими політиками. Якщо параметр не вказано в політиці динамічного доступу, пристрій ASA перевіряє групові політики, які визначають цей параметр

Група користувачів ASA містить такі атрибути:

- Джерело групової політики — визначає, чи зберігаються атрибути та значення групи користувачів внутрішньо (локально) на пристрої безпеки чи зовні на сервері AAA. Якщо група користувачів зовнішнього типу, для неї не потрібно налаштовувати інші параметри.
- Параметри конфігурації клієнта, які визначають параметри клієнта Cisco для групи користувачів у Easy VPN або VPN віддаленого доступу.
- Атрибути брандмауера клієнта, які налаштовують параметри брандмауера для клієнтів VPN у Easy VPN або VPN віддаленого доступу.
- Атрибути апаратного клієнта, які налаштовують параметри апаратного клієнта VPN 3002 у Easy VPN або VPN віддаленого доступу.
- Параметри IPsec, які визначають протоколи тунелювання, фільтри, параметри підключення та сервери для групи користувачів у Easy VPN або VPN з віддаленим доступом.

- Безклієнтські налаштування, які налаштовують безклієнтський режим доступу до корпоративної мережі в SSL VPN для групи користувачів ASA.
- Параметри повного клієнта, які налаштовують повний клієнтський режим доступу до корпоративної мережі в SSL VPN для групи користувачів ASA.
- Загальні налаштування, необхідні для безклієнтської переадресації/переадресації портів у SSL VPN.
- Параметри DNS/WINS, які визначають сервери DNS і WINS, а також ім’я домену, яке слід надсилати віддаленим клієнтам, пов’язаним із групою користувачів ASA.
- Розділене тунелювання, яке дозволяє віддаленому клієнту умовно направляти пакети через тунель IPsec або SSL VPN у зашифрованому вигляді або до мережевого інтерфейсу у відкритому текстовому вигляді.
- Параметри підключення сеансу віддаленого доступу або SSL VPN для групи користувачів ASA.

Сертифікат до політики карти профілю підключення використовуються для розширеної автентифікації сертифіката на пристроях ASA.

Сертифікат політики карти профілю підключення – це унікальна ідентифікація, що складається з окремих полів, які можна використовувати як ідентифікатор під час зіставлення користувачів із профілем підключення.

Політики відображення профілю підключення до сертифіката дозволяють визначати правила для відповідності сертифіката користувача групі дозволів на основі вказаних полів. Щоб встановити автентифікацію, можливо використовувати будь-яке поле сертифіката або ви можете надати всім користувачам сертифіката спільну групу дозволів.

Щоб зіставити групи дозволів користувачів на основі полів сертифіката, визначаються правила, які вказують поля для відповідності для групи, а потім необхідно увімкнути кожне правило для цієї вибраної групи. Профіль з’єднання вже має існувати в конфігурації, перш ніж буде можливість створити для нього правило.

Після визначення правил необхідно налаштувати політику відповідності груп сертифікатів, щоб визначити метод ідентифікації груп дозволів користувачів сертифікатів. Необхідно зіставити групу з правил DN, поля організаційного підрозділу (OU), ідентифікатора IKE або IP-адреси однорангового пристрою [16].

2.6. Розуміння проксі та правил обходу проксі

Пристрій безпеки може завершувати з'єднання HTTPS і пересилати запити HTTP/HTTPS на проксі-сервери HTTP та HTTPS. Ці сервери діють як посередники між користувачами та Інтернетом. Вимагання всього доступу до Інтернету через сервер, яким ви керуєте, надає ще одну можливість для фільтрації для забезпечення безпечного доступу до Інтернету та адміністративного контролю.

Можна вказати файл автоконфігурації проксі (PAC) для завантаження з проксі-сервера HTTP; однак ви не можете використовувати автентифікацію проксі під час вказівки файлу PAC.

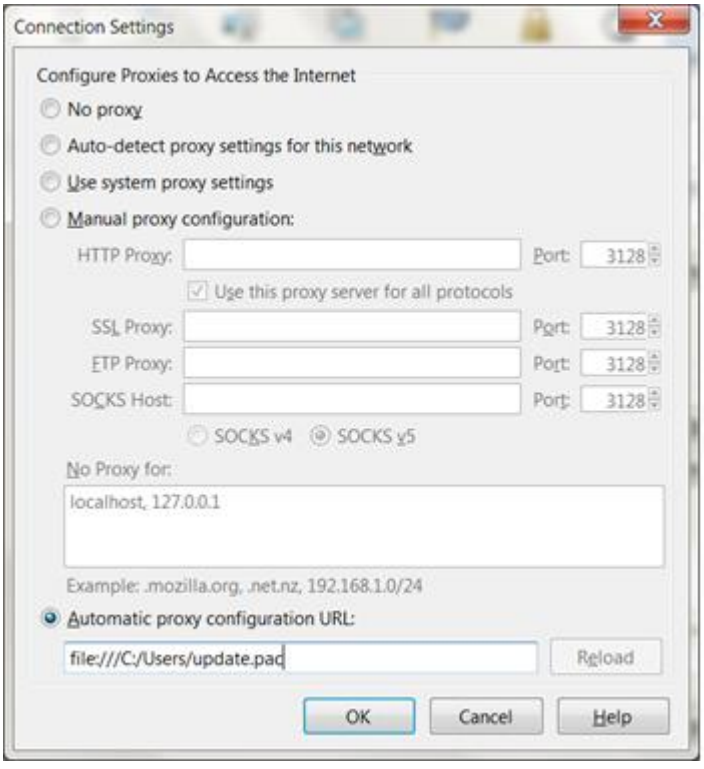

Рис. 2.5. Файл автоконфігурації проксі

Можливо налаштувати пристрій безпеки на використання обходу проксі-сервера, коли програми та веб-ресурси краще працюють із перезаписом вмісту, який забезпечує ця функція. Обхід проксі – це альтернативний метод перезапису вмісту, який вносить мінімальні зміни до вихідного вмісту. Це корисно для спеціальних веб-додатків.

Можна налаштувати кілька записів обходу проксі. Порядок, у якому ви їх налаштовуєте, не має значення. Інтерфейс і маска шляху або інтерфейс і порт унікально визначають правило обходу проксі.

Якщо необхідно налаштувати обхід проксі-сервера за допомогою портів, а не масок шляхів, залежно від конфігурації мережі, вам може знадобитися змінити конфігурацію брандмауера, щоб дозволити цим портам доступ до пристрою безпеки. Щоб уникнути цього обмеження, використовуйте маски шляху. Однак необхідно мати на увазі, що маски шляху можуть змінюватися, тому може знадобитися використовувати кілька операторів маски шляху, щоб вичерпати можливості.

Висновки до другого розділу

Досліджено види віддаленого доступу такі як: IPSec VPN та SSL VPN, що дозволяють користувачам отримувати доступ до корпоративних мереж з будь-якого місця з підтримкою Інтернету. Розглянуто принципи їх роботи та зазначено основні переваги та недоліки.

Проаналізовано можливості керування файлами підтримки SSL VPN та параметри клієнта, що забезпечує безпечні з’єднання.

Розглянуто особливості групових політик (ASA) та сформовано розуміння проксі і правил його обходу.

3 ОРГАНІЗАЦІЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ОПТИМІЗАЦІЯ ПРОДУКТИВНОСТІ РОБОТИ НА ОСНОВІ РІШЕННЯ ВІДДАЛЕНОГО ДОСТУПУ VPN

3.1. Використання майстра конфігурації віддаленого доступу VPN

Майстер конфігурації віддаленого доступу VPN дозволяє швидко та легко налаштувати пристрій як сервер віддаленого доступу IPSec VPN. Після того, як політики налаштовані, певні параметри безпеки, визначені в цих політиках, надсилаються сервером клієнту, мінімізуючи конфігурацію на клієнті.

Залежно від типу пристрою та типу VPN (IPSec або SSL), майстер проведе в через и для налаштування базової VPN віддаленого доступу.

Щоб отримати доступ до майстра налаштування віддаленого доступу:

- У вікні «Пристрій» вибрати пристрій, який потрібно налаштувати як сервер віддаленого доступу.
- Обрати Remote Access VPN --> Configuration Wizard у полі вибору політики.
- Обрати перемикач, що відповідає типу VPN віддаленого доступу, який необхідно створити: Remote Access SSL VPN або Remote Access IPSec VPN
- Натиснути Майстер налаштування віддаленого доступу.

3.1.1. Створення SSL VPN за допомогою майстра конфігурації VPN віддаленого доступу (пристрої IOS)

Ця процедура описує, як створювати або редагувати SSL VP**N** на пристроях IOS за допомогою майстра конфігурації VPN віддаленого доступу:

1. У вікні «Пристрій» вибрати потрібний пристрій IOS.
2. У вибірці політики обрати Remote Access VPN --> Configuration Wizard.
3. Обрати перемикач Remote Access SSL VPN.

4. Натиснути Майстер налаштування віддаленого доступу. Відкриється сторінка «Шлюз і контекст».

5. Обрати шлюз, який буде використовуватися як проксі для підключень до захищених ресурсів у корпоративній SSL VPN.

Варіанти:

- Використовувати наявний шлюз — дозволяє використовувати існуючий шлюз для корпоративної SSL VPN. Якщо вибрано цей параметр, указати назву шлюзу.
- Створити за допомогою IP-адреси — дозволяє налаштувати новий шлюз за допомогою доступної (публічної, статичної) IP-адреси на маршрутизаторі [17].
- Create Using Interface — дозволяє налаштувати новий шлюз за допомогою загальнодоступної статичної IP-адреси інтерфейсу маршрутизатора.

Якщо було прийнято рішення створити новий шлюз за допомогою IP-адреси або інтерфейсу:

- Указати номер порту, який передаватиме трафік HTTPS (між 1024 і 65535). Значення за замовчуванням — 443, якщо не ввімкнуто переспрямування порту HTTP. У цьому випадку стандартним номером порту HTTP є 80.
- Ввести цифровий сертифікат, необхідний для встановлення безпечного з'єднання. Якщо потрібно налаштувати певний сертифікат ЦС, під час активації шлюзу SSL VPN генерується самопідписаний сертифікат. Усі шлюзи на маршрутизаторі можуть використовувати той самий сертифікат.

6. Ввести назву контексту, який визначає ресурси, необхідні для підтримки тунелю SSL VPN між віддаленими клієнтами та корпоративною або приватною внутрішньою мережею.

7. Ввести URL-адресу, яка відображатиметься на сторінці порталу для доступу до шлюзу SSL VPN.

8. Ввести назви групових політик, які використовуватимуться у корпоративному SSL VPN-з’єднанні, і вкажіть, чи ввімкнено або вимкнено для них режим повного тунельного доступу.

9. Ввести назву групи серверів автентифікації (LOCAL, якщо користувачів визначено на локальному пристрої).

10. Ввести список або метод для віддаленої автентифікації користувача SSL VPN.

11. Ввести назву групи серверів обліку.

12. Натиснути «Далі» . Відкриється сторінка налаштування сторінки порталу.

13. Ввести заголовок, який буде відображатися в рядку заголовка сторінки порталу. Назва за замовчуванням – «SSL VPN Service».

14. Ввести логотип, який буде відображатися в рядку заголовка сторінки входу SSL VPN і порталу. Варіанти:

- None — логотип не відображається.
- За замовчуванням — використовувати стандартний логотип.
- Спеціальний — якщо вибрано, ви можете вказати власний логотип. У полі «Файл логотипу» вказати вихідний файл зображення для логотипу або натиснути «Вибрати», щоб вибрати файл зображення.

Вихідним файлом зображення для логотипу може бути файл GIF, JPG або PNG із назвою файлу довжиною до 255 символів і розміром до 100 кілобайт.

15. Ввести повідомлення, яке відображатиметься користувачеві після входу.

16. Ввести колір основного та додаткового рядків заголовків на сторінках входу та порталу SSL VPN.

17. Ввести колір тексту в основному та додатковому рядках заголовків сторінок входу та порталу. Варіанти: білий або чорний (за замовчуванням).

18. Якщо необхідно попередньо переглянути, як буде виглядати сторінка порталу, натиснути «Попередній перегляд» .

19. Натиснути «Готово», щоб зберегти корпоративне визначення локально в клієнті Security Manager і закрити діалогове вікно.

3.1.2. Створення IPSec VPN за допомогою майстра конфігурації VPN віддаленого доступу (пристрої IOS)

Ця процедура описує, як створювати або редагувати IPSec VPN на пристроях IOS за допомогою майстра конфігурації VPN віддаленого доступу.

1. У вікні «Пристрій» обрати потрібний пристрій IOS.
2. У вибірці політики обрати Remote Access VPN --> Configuration Wizard .
3. Обрати перемикач Remote Access IPSec VPN .
4. Натиснути Майстер налаштування віддаленого доступу . Відкриється сторінка групової політики користувача.
5. Обрати потрібні групи користувачів зі списку Доступні групи користувачів і натиснути ->-> .

Якщо потрібної групи користувачів немає в списку, натиснути «Створити», щоб відкрити діалогове вікно «Редактор груп користувачів», у якому можна створити або відредагувати об’єкт групи користувачів.

6. Натиснути «Далі» . Відкриється сторінка за замовчуванням.
7. Ввести параметри за замовчуванням, які будуть використовуватися для цього IPSec VPN.
8. Натиснути «Готово» , щоб зберегти корпоративне визначення локально в клієнті Security Manager і закрити діалогове вікно.

3.1.3. Створення SSL VPN за допомогою майстра конфігурації VPN віддаленого доступу (пристрої ASA)

Ця процедура описує, як створювати або редагувати SSL VPN на пристроях ASA за допомогою майстра конфігурації VPN віддаленого доступу [18]:

1. У вікні «Пристрій» обрати потрібний пристрій ASA.
2. У вибірці політики обрати Remote Access VPN -> Configuration Wizard .
3. Обрати перемикач Remote Access SSL VPN .

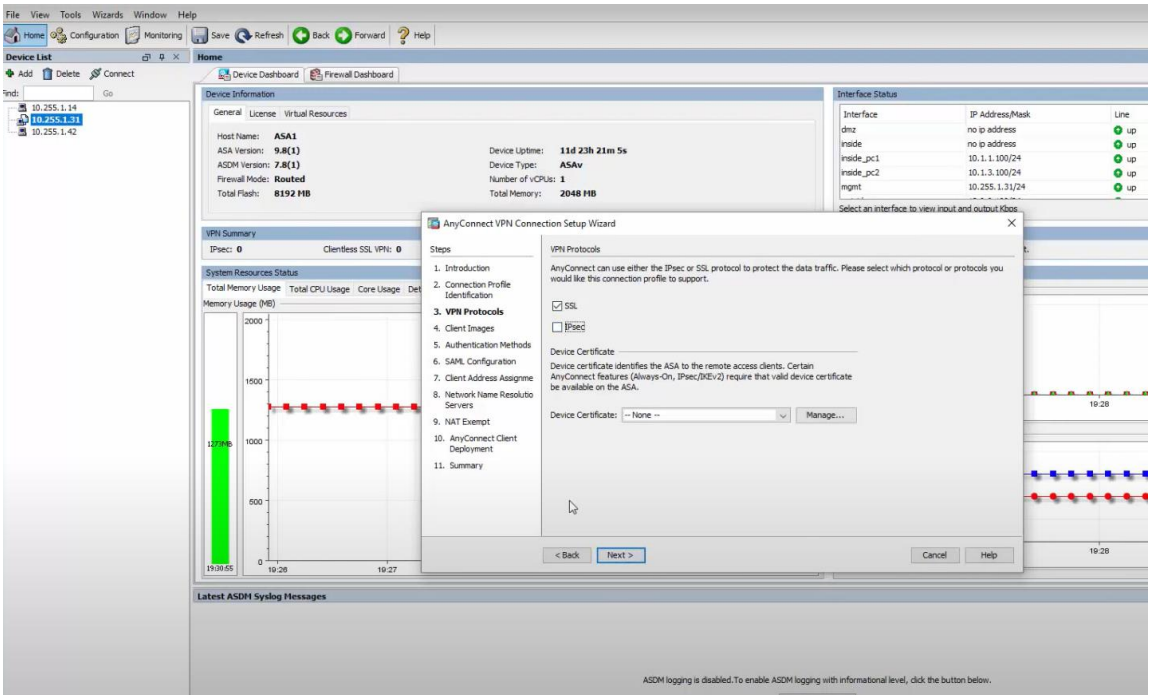

Рис. 3.1. Налаштування SSL VPN на пристроях ASA

4. Натиснути Майстер налаштування віддаленого доступу . Відкриється сторінка доступу.

5. Указати інтерфейси, на яких потрібно ввімкнути профілі підключення SSL VPN.

Можна натиснути «Вибрати», щоб відкрити діалогове вікно, у якому можна вибрати інтерфейс зі списку інтерфейсів або об’єктів ролі інтерфейсу.

6. Указати номер порту, який необхідно використовувати для сеансів SSL VPN.

Стандартний порт 443 для трафіку HTTPS. Номер порту може бути 443 або в діапазоні 1-65535. Якщо змінити номер порту, усі поточні з’єднання SSL VPN припиняються, і поточні користувачі повинні повторно підключитися.

Якщо переспрямування порту HTTP увімкнено, номер порту HTTP за умовчанням становить 80.

Можна натиснути «Вибрати», щоб відкрити діалогове вікно «Вибір списку портів», у якому можна зробити вибір або створити новий список портів.

7. Щоб дозволити користувачам вибирати групу тунелів зі списку профілів підключення групи тунелів, налаштованих на пристрої під час входу, установіть

прапорець « Дозволити користувачам вибирати профіль підключення на сторінці порталу».

8. Щоб увімкнути функцію AnyConnect на пристрої ASA, необхідно встановити прапорець Enable AnyConnect Access .

9. Натиснути «Далі». Відкриється сторінка профілю підключення.

10. Ввести назву для цього профілю з'єднання.

11. Ввести або обрати назву тунельної групи, яка містить політики для цього профілю підключення SSL VPN.

12. Вказати стандартну групову політику, пов'язану з пристроєм. Можна натиснути «Редагувати», щоб відкрити засіб вибору групової політики. Якщо потрібної групової політики немає в списку, Натиснути кнопку «Створити», щоб відкрити майстер створення групи користувачів, у якому можна створити групову політику.

Якщо необхідно змінити властивості групової політики у списку, обрати її та Натиснути «Редагувати» . Відкриється діалогове вікно Редагування груп користувачів, у якому можна редагувати об'єкт групової політики.

13. Вказати профіль налаштування, який визначає зовнішній вигляд сторінки порталу, що дозволяє віддаленому користувачеві отримати доступ до всіх ресурсів, доступних у мережах SSL VPN.

Можна натиснути «Вибрати», щоб відкрити діалогове вікно «Вибір налаштування SSL VPN», у якому перераховано всі доступні об'єкти налаштування, з яких ви можете зробити свій вибір.

Можна налаштувати різні вікна входу для різних груп, використовуючи комбінацію профілів налаштування та груп тунелів. Наприклад, припустивши, що створили профіль налаштування під назвою salesgui, ви можете створити тунельну групу SSL VPN під назвою sales, яка використовує цей профіль налаштування.

14. Обрати протокол (http або https) зі списку та вказати URL-адресу, включаючи назву профілю підключення, у відповідному полі.

Вказати URL-адресу, пов’язану з профілем підключення. Ця URL-адреса надає користувачам прямий доступ до сторінки порталу профілю підключення. URL-адреса складається з імені хоста або IP-адреси пристрою ASA та номера порту, а також псевдоніма, який використовується для ідентифікації профілю підключення SSL VPN.

Якщо не вказати URL-адресу, можна отримати доступ до сторінки порталу, ввівши URL-адресу сторінки порталу, а потім вибравши псевдонім профілю підключення зі списку налаштованих псевдонімів профілю підключення, налаштованих на пристрої.

15. Вказати пули адрес, з яких будуть призначені IP-адреси. Сервер використовує ці пули в зазначеному порядку. Якщо всі адреси в першому пулі були призначені, він використовує наступний пул і так далі. Ви можете вказати до шести пулів.

Якщо необхідно використати інший пул адрес або вибрати додаткові пули адрес, натиснути «Вибрати», щоб відкрити селектор «Мережа/Хости», з якого буде можливість зробити вибір.

16. Ввести назву групи серверів автентифікації (LOCAL, якщо тунельну групу налаштовано на локальному пристрої). Можна натиснути «Вибрати», щоб відкрити діалогове вікно зі списком усіх доступних груп серверів AAA, у якому можна створити об’єкти групи серверів AAA.

17. Якщо вибрано зовнішню групу серверів AAA, можна ввімкнути резервний доступ до локальної бази даних для автентифікації, якщо вибрана група серверів автентифікації не вдасться.

18. Ввести назву групи серверів авторизації (LOCAL, якщо тунельну групу налаштовано на локальному пристрої). Можна натиснути «Вибрати», щоб відкрити діалогове вікно зі списком усіх доступних груп серверів AAA, у якому можна створити об’єкти групи серверів AAA.

19. Ввести назву групи серверів обліку. Можна натиснути «Вибрати», щоб відкрити діалогове вікно зі списком усіх доступних груп серверів AAA, у якому можна створити об’єкти групи серверів AAA.

20. Натиснути «Готово» , щоб зберегти визначення локально в клієнті Security Manager і закрити діалогове вікно

3.1.4. Створення IPSec VPN за допомогою майстра конфігурації VPN віддаленого доступу (ASA Devices)

Ця процедура описує, як створювати або редагувати IPSec VPN на пристроях ASA за допомогою майстра конфігурації VPN віддаленого доступу [18]:

1. У вікні «Пристрій» обрати потрібний пристрій ASA.
2. У вибірці політики обрати Remote Access VPN -> Configuration Wizard .
3. Обрати перемикач Remote Access IPSec VPN .
4. Натиснути Майстер налаштування віддаленого доступу . Відкриється сторінка профілю підключення.
5. Ввести ім’я для профілю з’єднання IPSec VPN.
6. Вказати стандартну групову політику, пов’язану з пристроєм. Можливо натиснути «Вибрати», щоб відкрити засіб вибору груп користувачів ASA, у якому можна вибрати групу користувачів зі списку об’єктів.

Якщо потрібної групи користувачів за замовчуванням немає в списку, Натиснути «Створити», щоб відкрити майстер створення групи користувачів.

Якщо необхіднозмінити властивості групи користувачів у списку, обрати її та Натиснути Редагувати . Відкриється діалогове вікно Редагування груп користувачів.

7. Ввести пули адрес, з яких буде призначено IP-адреси. Сервер використовує ці пули в зазначеному порядку. Якщо всі адреси в першому пулі були призначені, він використовує наступний пул і так далі. Можна вказати до 6 пулів.

Якщо необхідно використати інший пул адрес або вибрати додаткові пули адрес, натиснути «Вибрати», щоб відкрити селектор «Мережа/Хости», з якогови можна зробити вибір.

8. Ввести назву групи серверів автентифікації (LOCAL, якщо тунельну групу налаштовано на локальному пристрої). Можна натиснути «Вибрати», щоб відкрити діалогове вікно зі списком усіх доступних груп серверів AAA, у якому можна створити об’єкти групи серверів AAA.

9. Якщо обаний LOCAL для групи серверів автентифікації, можна ввімкнути відкат до локальної бази даних для автентифікації, якщо вибрана група серверів автентифікації не вдасться.

10. Ввести назву групи серверів авторизації (LOCAL, якщо тунельну групу налаштовано на локальному пристрої). Можна натиснути «Вибрати», щоб відкрити діалогове вікно зі списком усіх доступних груп серверів AAA, у якому можна створити об’єкти групи серверів AAA.

11. Ввести назву групи серверів обліку. Можна натиснути «Вибрати», щоб відкрити діалогове вікно зі списком усіх доступних груп серверів AAA, у якому можна створити об’єкти групи серверів AAA.

12. Натиснути Далі. Відкриється сторінка налаштувань IPSec.

13. Ввести значення попереднього ключа для групи тунелів. Максимальна довжина спільного ключа становить 127 символів.

14. Ввести ім’я точки довіри, якщо будь-яку точку довіри налаштовано. Точка довіри представляє пару ЦС/ідентифікатор і містить ідентичність ЦС, специфічні параметри конфігурації ЦС і асоціацію з одним зареєстрованим сертифікатом ідентифікації.

15. Обрати, чи перевірка ідентифікатора однорангового вузла IKE ігнорується, потрібна чи перевіряється, лише якщо підтримується сертифікатом. Під час переговорів IKE партнери повинні ідентифікувати себе один перед одним.

16. Щоб увімкнути надсилання ланцюжка сертифікатів для авторизації, установити прапорець Увімкнути надсилання ланцюжка сертифікатів . Ланцюжок сертифікатів включає кореневий сертифікат ЦС, сертифікат ідентифікації та пару ключів.

17. Щоб увімкнути оновлення паролів за допомогою протоколу автентифікації RADIUS, установити прапорець « Увімкнути оновлення пароля за допомогою автентифікації RADIUS ».

18. Вказати такі параметри ISAKMP Keepalive:

• Щоб налаштувати IKE Keepalive як механізм відновлення після відмови та маршрутизації за замовчуванням, установіть прапорець Monitor Keepalive .

• Ввести кількість секунд, протягом яких пристрій очікує між надсиланням пакетів підтримки активності IKE.

• Ввести кількість секунд, протягом яких пристрій чекає між спробами встановити з'єднання IKE з віддаленим вузлом. За замовчуванням 2 секунди.

19. Налаштувати певний рівень версії та URL-адресу зображення клієнтів VPN.

20. Натиснути «Далі» . Відкриється сторінка за замовчуванням.

21.. Ввести параметри за замовчуванням, які будуть використовуватися для цього IPSec VPN.

22. Натиснути «Готово» , щоб зберегти корпоративномуі визначення локально в клієнті Security Manager і закрийте діалогове вікно.

3.1.5. Налаштування глобальних параметрів VPN віддаленого доступу

На сторінці «Глобальні параметри VPN» можливо визначити глобальні параметри для IKE, IPsec, NAT і фрагментації, які застосовуються до пристроїв у корпоративномуій VPN віддаленого доступу [19]:

Глобальні налаштування VPN включають:

• Параметри ISAKMP/IPsec, які дають змогу налаштувати параметри ISAKMP (IKE) і IPsec, які дозволяють узгодженим вузлам узгодити встановлення тунелю VPN у VPN віддаленого доступу.

• Параметри трансляції мережевих адрес (NAT), щоб дозволити пристроям, які використовують внутрішні IP-адреси, надсилати та отримувати дані через Інтернет.

• Загальні параметри, включаючи параметри фрагментації та параметри обробки максимальної одиниці передачі (MTU), які можна налаштувати на пристроях у корпоративномуій VPN віддаленого доступу. Для отримання додаткової інформації див.

1. У вікні «Пристрій» обрати потрібний пристрій.

2. Обрати «Віддалений доступ до VPN» -> «Глобальні налаштування» в полі вибору політики.

Відкриється сторінка глобальних налаштувань VPN із вкладкою налаштувань ISAKMP/IPsec.

3. На вкладці «Параметри ISAKMP/IPsec» Вказати глобальні параметри для IKE та IPsec, як описано нижче:

- Обрати «Увімкнути Keepalive» , щоб налаштувати IKE Keepalive як механізм відновлення після відмови та маршрутизації за замовчуванням для корпоративномуих пристроїв. (Застосовується до маршрутизаторів Cisco IOS, пристроїв Catalyst 6500/7600 і брандмауерів PIX версії 6.3.)
- Ввести кількість секунд, протягом яких пристрій повинен чекати між надсиланням пакетів підтримки активності IKE.
- Ввести кількість секунд, протягом яких пристрій повинен чекати між спробами встановити з’єднання IKE з віддаленим вузлом.
- Обрати «Періодичний», якщо необхідно надсилати повідомлення про виявлення мертвих однорангових пристроїв (DPD), навіть якщо немає вихідного трафіку для надсилання (для маршрутизаторів, крім 7600).
- Вказати, чи використовує пристрій IP-адресу чи ім’я хоста для ідентифікації під час узгодження IKE. Також можна вказати використання розрізняючого імені (DN) для ідентифікації імені групи користувачів.
- Вказати максимальну дозволену кількість запитів SA, перш ніж IKE почне їх відхиляти (для маршрутизаторів, крім 7600).
- Вказати відсоток системних ресурсів, який можна використовувати до того, як IKE почне відхиляти нові запити SA (для маршрутизаторів Cisco IOS і пристроїв Catalyst 6500/7600).

- Обрати «Увімкнути термін служби», щоб налаштувати глобальні параметри терміну служби для крипто IPsec SA на пристроях віддаленого доступу VPN.

- Вказати кількість секунд, протягом яких SA існуватиме до закінчення терміну дії.

- Вказати обсяг трафіку (у кілобайтах), який може проходити між одноранговими IPsec за допомогою даного SA до закінчення терміну його дії.

- Вказати час очікування Xauth, тобто кількість секунд, протягом яких пристрій чекатиме відповіді системи на виклик Xauth (маршрутизатори Cisco IOS і пристрої Catalyst 6500/7600).

- Вказати максимальну кількість SA, які можна ввімкнути одночасно на пристрої (лише для пристроїв ASA або PIX 7.0).

- Обрати «Увімкнути IPsec через Sysopt» , щоб указати, що будь-який пакет, який надходить із тунелю IPsec, буде неявно довіреним (лише для пристроїв PIX 6.3, PIX 7.0 і ASA).

4. Натиснути вкладку Параметри NAT , щоб визначити глобальні параметри NAT, які застосовуються до пристроїв, які використовують внутрішні IP-адреси для надсилання та отримання даних через загальнодоступний Інтернет [19]:

- Обрати Enable Traversal Keepalive для передачі повідомлень Keepalive, коли пристрій (іменований проміжним пристроєм), розташований між підключеним через VPN концентратором і роз’ємом, виконує NAT у потоці IPsec.

- Вказати інтервал (від 5 до 3600 секунд) між сигналами підтримки активності, які надсилаються між роз’ємом і середнім пристроєм, щоб вказати, що сеанс активний.

- Обрати «Увімкнути проходження через TCP» (лише для пристроїв ASA або PIX 7.0), щоб інкапсулювати протоколи IKE та IPsec у TCP-пакет і ввімкнути безпечне тунелювання через пристрої NAT і PAT і брандмауери.

- Ввести порти TCP, для яких потрібно ввімкнути проходження NAT (лише для пристроїв ASA або PIX 7.0).

5. Натиснути вкладку «Загальні налаштування», щоб визначити фрагментацію та інші глобальні параметри на пристроях у корпоративномуій VPN віддаленого доступу.

- Обрати режим фрагментації з наступних параметрів:

• Без фрагментації — обрати, якщо не потрібно фрагментувати перед інкапсуляцією IPsec.

• Наскрізне виявлення MTU — обрати використання повідомлень ICMP для виявлення MTU.

• Локальна обробка MTU — обрати, щоб установити MTU локально на пристроях. Цей параметр зазвичай використовується, коли ICMP заблоковано.

- Вказати розмір MTU (від 68 до 65535 байт залежно від інтерфейсу VPN).

- Обрати необхідне налаштування для біта DF (для маршрутизаторів Cisco IOS, пристроїв ASA або PIX 7.0) — Copy , Set або Clear .

- Обрати «Увімкнути фрагментацію перед шифруванням» (для маршрутизаторів Cisco IOS, пристроїв ASA або PIX 7.0), щоб фрагментувати перед шифруванням, якщо очікуваний розмір пакета перевищує MTU (тільки для маршрутизаторів Cisco IOS).

- Обрати «Увімкнути сповіщення про відключення», щоб повідомити кваліфікованих однорангових користувачів про сеанси, які незабаром будуть відключені.

- Обрати «Увімкнути зв’язок «Спілка-спілка» через концентратор (лише для пристроїв ASA або PIX 7.0), щоб увімкнути прямий зв’язок між стрілками в топології VPN «концентратор і стрілка», у якій концентратором є пристрій ASA або версія брандмауера PIX 7.0.

- Обрати «Увімкнути маршрут за замовчуванням» (лише для маршрутизаторів Cisco IOS), щоб використовувати налаштований зовнішній інтерфейс пристрою як вихідний маршрут за замовчуванням для всього вхідного трафіку.

3.1.6. Створення групових політик (ASA)

Сторінка «Групова політика» використовується, щоб створити групову політику для пристроїв ASA, які використовуються у віддаленому доступі IPSec або SSL VPN [19]:

1. У вікні «Пристрій» обрати потрібний пристрій ASA.

2. Обрати Remote Access VPN -> Group Policies у селекторі Policy.

Відкриється сторінка групових політик.

3. Натиснути «Створити», щоб відкрити діалогове вікно, у якому можна вибрати групу користувачів зі списку попередньо визначених об’єктів групи користувачів ASA або за потреби створити нові.

4. Обрати потрібну групу користувачів ASA зі списку та натиснути OK , або, якщо потрібної групи користувачів ASA не існує, створити її, натиснувши «Створити».

З’явиться діалогове вікно «Додати групу користувачів ASA», у якому показано список параметрів, які можна налаштувати для об’єкта групи користувачів ASA.

5. Ввести назву об’єкта.

6. (необов’язково) Ввести опис, який допоможе вам ідентифікувати об’єкт. Дозволено максимум 1024 символи та спеціальні символи. Якщо введено опис, під час перегляду таблиці груп користувачів ASA відображається піктограма.

7. Обрати, чи зберігати атрибути та значення групи користувачів ASA локально на пристрої чи на зовнішньому сервері.

Якщо обрано зберігати атрибути групи користувачів ASA на зовнішньому сервері, тоді не потрібно налаштовувати параметри технології. Після того, як вкажеться група серверів AAA, яка використовуватиметься для автентифікації, і пароль до сервера AAA, Натиснути OK , щоб зберегти визначення та закрити діалогове вікно групи користувачів ASA.

8. Якщо обрано локальне зберігання атрибутів групи користувачів ASA на пристрої, обрати тип VPN, для якого створюється групу користувачів ASA, зі списку технологій.

9. Щоб налаштувати групу користувачів для Easy VPN або IPSec VPN, у папці Easy VPN/IPSec VPN на панелі налаштувань:

- Обрати «Конфігурація клієнта» , щоб налаштувати параметри клієнта Cisco для групи користувачів ASA.
- Обрати «Атрибути брандмауера клієнта», щоб налаштувати параметри брандмауера для клієнтів VPN для групи користувачів ASA.
- Обрати «Атрибути апаратного клієнта», щоб налаштувати параметри апаратного клієнта VPN 3002 для групи користувачів ASA.
- Обрати IPsec, щоб указати протоколи тунелювання, фільтри, параметри підключення та сервери для групи користувачів ASA.

10. Щоб налаштувати групу користувачів для SSL VPN, у папці SSL VPN на панелі налаштувань:

- Обрати «Без клієнта», щоб налаштувати безклієнтський режим доступу до корпоративної мережі в SSL VPN для об’єкта групи користувачів ASA.
- Обрати «Повний клієнт», щоб налаштувати повний клієнтський режим доступу до корпоративної мережі в SSL VPN для об’єкта групи користувачів ASA.
- Обрати Параметри , щоб налаштувати загальні параметри, необхідні для режимів доступу без клієнта та тонкого клієнта в SSL VPN для об’єкта групи користувачів ASA.

11. Вказати такі параметри для групи користувачів ASA в конфігурації Easy VPN, IPSec VPN або SSL VPN на панелі налаштувань:

- Обрати DNS/WINS, щоб визначити сервери DNS і WINS, а також доменне ім’я, яке потрібно надіслати клієнтам, пов’язаним із групою користувачів ASA.

- Обрати розділене тунелювання, щоб указати безпечний тунель до центрального сайту та одночасні тунелі з відкритим текстом до Інтернету.
- Обрати «Загальні параметри» , щоб налаштувати параметри з’єднання SSL VPN для групи користувачів ASA, наприклад час очікування сеансу та простою, включно з текстом банера.

12. Обрати групу користувачів ASA зі списку та Натиснути OK.

3.1.7. Налаштування правил відображення профілів підключення (ASA)

Ця процедура описує, як налаштувати правила та параметри сертифіката для карти профілю підключення для будь-якого віддаленого клієнта, який намагається підключитися до пристрою сервера ASA [18,19]

1. У вікні «Пристрій» обрати потрібний пристрій ASA.

2. Обрати Remote Access VPN -> IPSec VPN -> Certificate to Connection Profile Maps -> Rules у виборці Policy. Відобразиться сторінка «Правила відображення профілю підключення до сертифіката».

3 Натиснути «Створити» на верхній панелі, щоб налаштувати пріоритет і відображення профілю підключення для корпоративних правил відповідності. Відкриється діалогове вікно «Правило відображення».

4. Обрати профіль підключення зі списку.

5. Ввести номер пріоритету для правила відповідності. Менше число має вищий пріоритет.

6. Натиснути OK. Правило відображається у верхній частині сторінки.

7. Обрати правило, створене на верхній панелі, щоб відобразити деталі на нижній панелі.

8. Натиснути «Створити» на нижній панелі, щоб налаштувати правило відповідності сертифіката та профілю з’єднання, яке має бути виконано для підключення віддаленого клієнта до пристрою. Відкриється діалогове вікно «Правило відображення».

9. Обрати поле сертифіката зі списку.

10. Обрати компонент правила, який потрібно налаштувати.

11. Обрати оператор правила.

12. Ввести значення для правила відповідності.

13. Натиснути OK . Параметри правила відображаються в нижній частині сторінки.

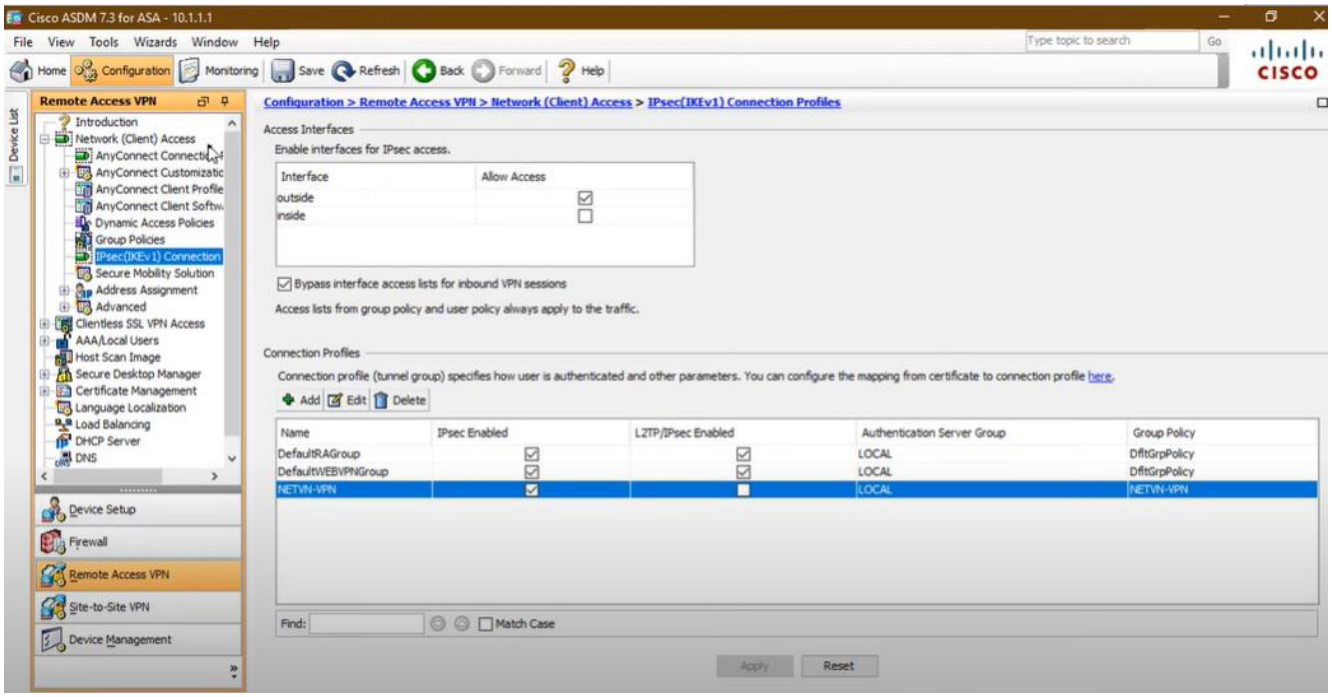

Рис. 3.2. Налаштування правил відображення профілів підключення (ASA)

Налаштувати політику доступу на пристрої ASA:

1. У вікні «Пристрій» обрати потрібний пристрій ASA.

2. Обрати Remote Access VPN -> SSL VPN -> Access у полі вибору політики. З’явиться сторінка доступу.

3. З таблиці можна створити інтерфейс або відредагувати існуючий, на якому можна встановити з’єднання SSL VPN, як показано нижче:

- Натиснути «Додати рядок» під таблицею або обрати рядок у таблиці та натиснути «Редагувати рядок». Відкриється діалогове вікно конфігурації інтерфейсу доступу.

- Вказати інтерфейс, на якому необхідно налаштувати доступ до VPN. Можна натиснути «Вибрати», щоб відкрити діалогове вікно, у якому можна вибрати інтерфейс зі списку інтерфейсів або об’єктів ролі інтерфейсу.

- Ввести або обрати визначену точку довіри, яку потрібно призначити цьому інтерфейсу.
- Якщо балансування навантаження налаштовано, можна ввести або вибрати додаткову точку довіри балансування навантаження, яку потрібно призначити цьому інтерфейсу.
- Обрати «Дозволити доступ», щоб увімкнути доступ до VPN через цей інтерфейс. Якщо цей параметр не вибрано, доступ налаштовується в інтерфейсі, але він вимкнений.
- Обрати «Увімкнути DTLS», щоб увімкнути з'єднання DTLS із клієнтом AnyConnect в інтерфейсі та дозволити клієнтам AnyConnect VPN встановлювати з'єднання SSL VPN за допомогою двох одночасних тунелів — тунелю SSL і тунелю DTLS.
- Обрати «Перевірити сертифікат клієнта», щоб вимагати від клієнта дійсний цифровий сертифікат для підключення.
- Натиснути OK .

4. Вказати номер порту для сеансів SSL VPN. Можна натиснути «Вибрати», щоб відкрити діалогове вікно «Вибір списку портів», у якому можна зробити свій вибір.

5. Вказати окремий порт UDP для з'єднань DTLS із клієнтом AnyConnect. Ви можете натиснути «Вибрати» , щоб відкрити діалогове вікно «Вибір списку портів», у якому можна зробити свій вибір.

6. Вказати резервну точку довіри для використання для інтерфейсів, яким не призначено точку довіри.

7. Вказати проміжок часу в секундах, протягом якого сеанс SSL VPN може бути неактивним, перш ніж пристрій безпеки завершить сеанс.

8. Вказати максимальну кількість сеансів SSL VPN, які необхідно дозволити.

9. Обрати «Дозволити користувачам вибирати профіль підключення на сторінці порталу», щоб включити список налаштованих груп тунелів в інтерфейс

кінцевого користувача SSL VPN, з якого користувачі можуть вибрати профіль підключення під час входу.

10. Обрати «Увімкнути доступ AnyConnect» , щоб увімкнути VPN-клієнт Cisco AnyConnect або застарілий клієнт Cisco SSL VPN (SVC) на інтерфейсах, визначених у пристрої безпеки для підключень SSL VPN.

11. Обрати «Увімкнути AnyConnect Essentials» , щоб увімкнути SSL VPN-клієнт AnyConnect Essentials.

3.1.8. Налаштування інших параметрів SSL VPN

У Security Manager можна визначити глобальні параметри SSL VPN, які застосовуються до всіх пристроїв у корпоративній топології SSL VPN. Ці налаштування включають кешування, перезапис вмісту, кодування символів, проксі та визначення обходу проксі, плагіни браузера та зображення та профілі клієнтів AnyConnect.

1. Кешування підвищує продуктивність SSL VPN. Він зберігає часто повторно використовувані об’єкти в системному кеші, що зменшує необхідність повторного перезапису та стиснення вмісту. Це зменшує трафік між SSL VPN і віддаленими серверами та браузерами кінцевих користувачів, у результаті чого багато програм працюють набагато ефективніше:

- У вікні «Пристрій» обрати потрібний пристрій ASA.
- Обрати Remote Access VPN -> SSL VPN -> Other Settings у полі вибору політики.
- Відкриється сторінка «Інші налаштування» з відкритою за замовчуванням вкладкою «Продуктивність».
- Установіть прапорець «Увімкнути», щоб увімкнути кешування на пристрої безпеки.
- Вказати мінімальний розмір документа, який пристрій безпеки може кешувати. Діапазон 0-10000 Кб. За замовчуванням 0 Кб. Максимальний розмір об’єкта має бути більшим за мінімальний розмір об’єкта.

- Вказати максимальний розмір документа, який пристрій безпеки може кешувати. Діапазон від 0 до 10000 Кб. За замовчуванням 1000 Кб.
- Вказати ціле число, щоб установити політику повторної перевірки для кешування об’єктів, які мають лише позначку часу останньої зміни, і не мають інших встановлених сервером значень терміну дії. Діапазон 1-100. За замовчуванням 20.
- Ввести ціле число, щоб встановити кількість хвилин для кешування об’єктів без їх повторної перевірки. Дійсні значення в діапазоні від 0 до 900. За замовчуванням одна хвилина.
- Установити прапорець Cache Compressed Content , щоб кешувати стислий вміст.
- Установити прапорець «Кешувати статичний вміст», щоб кешувати статичний вміст.

2. SSL VPN обробляє трафік програми за допомогою механізму перетворення/перезапису вмісту, який включає розширені елементи (наприклад, JavaScript, VBScript, Java та багатобайтові символи) для проксі-трафіку HTTP залежно від того, чи використовує користувач програму всередині чи незалежно від неї. Пристрій SSL VPN.

Якщо не потрібно, щоб деякі програми та веб-ресурси, наприклад загальнодоступні веб-сайти, проходили через пристрій безпеки, можна створити правила перезапису, які дозволять користувачам переглядати певні сайти та програми без використання самого пристрою безпеки. Це схоже на розділене тунелювання у з’єднанні IPsec VPN.

На вкладці «Перезапис вмісту» сторінки «Інші налаштування SSL VPN» можна налаштувати кілька правил перезапису вмісту. На вкладці Content Rewrite перераховано всі програми, для яких увімкнено або вимкнено перезапис вмісту:

- У вікні «Пристрій» обрати потрібний пристрій ASA.
- Обрати Remote Access VPN -> SSL VPN -> Other Settings у полі вибору політики.

- На сторінці «Інші налаштування» натиснути вкладку «Перезапис вмісту». Відкриється вкладка Content Rewrite, на якій відображаються всі програми, для яких увімкнено або вимкнено перезапис вмісту.
- На вкладці «Перезапис вмісту» Натиснути «Створити» або обрати правило перезапису в таблиці та Натиснути « Редагувати » .
- Відкриється діалогове вікно Add/Edit Content Rewrite.
- Установити прапорець « Увімкнути », щоб увімкнути перезапис вмісту для цього правила перезапису.
- Ввести число для цього правила. Цей номер визначає позицію правила в списку. Правила без номера знаходяться в кінці списку. Діапазон від 1 до 65534.
- Ввести назву програми або ресурсу, до якого застосовується правило (до 300 символів).
- Ввести додаток або ресурс для правила.
- Натиснути OK . Діалогове вікно «Додати правило перезапису вмісту» закривається, а правило перезапису вмісту додається до таблиці.

3. Визначення проксі та правил обходу проксі. Ця процедура показує, як визначити проксі та правила обходу проксі для корпоративного SSL VPN.

- У вікні «Пристрій» обрати потрібний пристрій ASA.
- Обрати Remote Access VPN -> SSL VPN -> Other Settings у селекторі Device Policies.
- На сторінці «Інші параметри» натиснути вкладку «Проксі».
- Обрати тип зовнішнього проксі-сервера, який буде використовуватися для підключень SSL VPN, як описано нижче:

• HTTP Proxy — дає змогу використовувати зовнішній проксі-сервер для обробки HTTP-запитів і активує всі поля під ним, які визначають властивості HTTP-сервера.

• Проксі-сервер HTTPS — дає змогу використовувати зовнішній проксі-сервер для обробки запитів HTTPS і активує всі поля під ним, які визначають властивості сервера HTTPS.

- Файл автоконфігурації проксі- сервера — дає змогу вказати файл автоконфігурації проксі (PAC) для завантаження з проксі-сервера HTTP у браузер.

- Якщо обраний HTTP Proxy як тип проксі-сервера, виконати такі дії, щоб установити тип конфігурації для HTTP-сервера [20]:

- Вказати IP-адресу зовнішнього проксі-сервера HTTP, на який пристрій безпеки пересилає HTTP-з'єднання. Ви можете натиснути «Вибрати», щоб зробити вибір зі списку об'єктів мережевого хосту.

- Вказати порт, який прослуховує HTTP-запити. Стандартним портом є 80. Ви можете натиснути «Вибрати», щоб зробити вибір у діалоговому вікні «Вибір списку портів».

- У полі «Список адрес винятків» ввести URL-адресу або список кількох URL-адрес, розділених комами, щоб виключити їх із тих, які можна надіслати на проксі-сервер HTTP. Ви можете натиснути «Вибрати», щоб відкрити засіб вибору списку URL-адрес, у якому можна зробити вибір зі списку об'єктів списку URL-адрес.

- Вказати ім'я користувача, яке супроводжуватиме кожен запит проксі-сервера HTTP паролем для забезпечення базової автентифікації проксі-сервера.

- Ввести пароль для надсилання на проксі-сервер з кожним запитом HTTP. Повторно Ввести пароль, щоб підтвердити його.

- Якщо обраний HTTPS Proxy як тип проксі-сервера, виконати такі дії, щоб установити тип конфігурації для HTTPS-сервера.

- Вказати IP-адресу зовнішнього проксі-сервера HTTPS, на який пристрій безпеки пересилає HTTP-з'єднання. Можна натиснути «Вибрати», щоб зробити вибір зі списку об'єктів мережевого хосту.

- Вказати порт, який прослуховує запити HTTPS. Стандартним портом є 443. Можна натиснути «Вибрати», щоб зробити вибір у діалоговому вікні «Вибір списку портів».

- У полі «Список адрес винятків» ввести URL-адресу або список кількох URL-адрес, розділених комами, щоб виключити їх із тих, які можна надіслати на проксі-сервер HTTPS. Можна натиснути «Вибрати», щоб відкрити

засіб вибору списку URL-адрес, у якому можна зробити вибір зі списку об’єктів списку URL-адрес.

- Вказати ім’я користувача, яке супроводжуватиме кожен запит проксі-сервера HTTPS із паролем для забезпечення базової автентифікації проксі-сервера.
- Ввести пароль для надсилання на проксі-сервер з кожним запитом HTTPS. Повторно ввести пароль, щоб підтвердити його.

- Якщо обраний файл автоматичної конфігурації проксі як тип проксі-сервера, обрати параметр «Указати URL-адресу файлу PAC» і вказати файл PAC для завантаження в браузер. Після завантаження файл PAC використовує функцію JavaScript для визначення проксі-сервера для кожної URL-адреси.

- У таблиці «Обхід проксі» натиснути « Створити» або обрати правило в таблиці та натиснути «Редагувати» .
- Відкриється діалогове вікно Add/Edit Proxy Bypass.
- Вказати назву інтерфейсу на пристрої безпеки для обходу проксі. Можна натиснути «Вибрати», щоб зробити вибір зі списку інтерфейсу та об’єктів ролі інтерфейсу.
- Обрати необхідну опцію обхідного трафіку , як показано нижче:

• На порту — щоб указати номер порту, який використовуватиметься для обходу проксі. Дійсні номери портів: 20000-21000. Можна натиснути «Вибрати» , щоб відкрити діалогове вікно «Вибір списку портів», у якому можна зробити свій вибір.

• Шаблон визначення відповідності — щоб указати URL-шлях для відповідності для обходу проксі.

- У полі URL -адреси обрати протокол http або https і Ввести URL-адресу, до якої потрібно застосувати обхід проксі-сервера.
- Установити прапорець «Переписати XML», щоб переписати сайти та програми XML, які будуть обходити пристрій безпеки.
- Установити прапорець Rewrite Hostname , щоб переписати абсолютні зовнішні посилання.

4. Розуміння плагінів. Плагін браузера — це окрема програма, яку веб-браузер викликає для виконання спеціальної функції, наприклад підключення клієнта до сервера у вікні браузера. Пристрій безпеки дозволяє імпортувати плагіни для завантаження у віддалені браузери в безклієнтських сеансах SSL VPN. Звичайно, Cisco тестує плагіни, які вона розповсюджує, а в деяких випадках перевіряє підключення плагінів, які не можемо розповсюджувати. Однак наразі не рекомендується імпортувати плагіни, які підтримують потокове медіа.

Відповідно до Загальної публічної ліцензії GNU (GPL) Cisco розповсюджує додаткові модулі, не вносячи в них жодних змін. Відповідно до GPL, Cisco не може безпосередньо покращувати ці плагіни.

Пристрій безпеки виконує такі дії, коли встановлюється плагін на флеш-пристрій:

- (Лише плагіни, що розповсюджуються Cisco) Розпаковує файл jar, указаний у URL-адресі.
- Записує файл у каталог csco-config/97/plugin у файловій системі пристрою безпеки.
- Вмикає плагін для всіх майбутніх безклієнтських сеансів SSL VPN і додає опцію головного меню та опцію до спадного меню поруч із полем «Адреса» на сторінці порталу.

Коли користувач у безклієнтському сеансі SSL VPN клацає пов’язану опцію меню на сторінці порталу, на сторінці порталу відображається вікно інтерфейсу та відображається панель довідки. Користувач може вибрати протокол, який відображається в спадному меню, і ввести URL-адресу в поле «Адреса», щоб встановити з’єднання.

Деякі плагіни Java можуть повідомляти про стан підключення або онлайн, навіть якщо сеанс до цільової служби не налаштовано. Плагін із відкритим кодом повідомляє про стан, а не пристрій безпеки.

Безклієнтська SSL VPN має бути ввімкнена на пристрої безпеки, щоб забезпечити віддалений доступ до плагінів. Мінімальні права доступу, необхідні для віддаленого використання, належать до гостьового режиму привілеїв. Плагіни

автоматично встановлюють або оновлюють необхідну версію Java на віддаленому комп’ютері. Перехід із збереженням стану не зберігає сеанси, встановлені за допомогою плагінів. Користувачі повинні повторно підключитися після відновлення після відмови.

Перед встановленням плагіна підготувати пристрій безпеки таким чином:

- Переконатися, що безклієнтську SSL VPN ("webvpn") увімкнено в інтерфейсі пристрою безпеки. Для цього ввести команду show running-config .
- Установити сертифікат SSL на інтерфейс пристрою безпеки, до якого віддалені користувачі використовують для підключення повне доменне ім’я (FQDN).

Не вказувати IP-адресу як загальну назву (CN) для сертифіката SSL. Віддалений користувач намагається використовувати FQDN для зв’язку з пристроєм безпеки. Віддалений комп’ютер має мати можливість використовувати DNS або запис у файлі System32\drivers\etc\hosts для вирішення FQDN.

На вкладці Plug-in сторінки глобальних налаштувань SSL VPN можна переглянути поточні налаштовані плагіни браузера для безклієнтського доступу браузера SSL VPN. На цій вкладці можна створювати або редагувати файли плагіна, як описано в наведеній нижче процедурі.

Надання доступу до плагінів, розповсюджених Cisco. Створити тимчасовий каталог під назвою «plugins» на комп'ютері, який ви використовуєте для встановлення сеансів Security Manager із пристроєм безпеки. Потім завантажити потрібні плагіни з веб-сайту Cisco до каталогу «плагіни». Cisco розповсюджує наступні компоненти з відкритим вихідним кодом на основі Java, доступ до яких здійснюється як плагіни для веб-браузерів у безклієнтських сеансах SSL VPN:

- rdp-plugin.jar — плагін Remote Desktop Protocol дозволяє віддаленому користувачеві підключатися до комп’ютера, на якому запущено Microsoft Terminal Services. Cisco розповсюджує цей плагін без будь-яких змін відповідно до GNU General Public License. Веб-сайт, на якому міститься джерело розповсюдженого плагіна, – http://properjavardp.sourceforge.net/ .

• ssh-plugin.jar — плагін Secure Shell-Telnet дозволяє віддаленому користувачеві встановлювати з'єднання Secure Shell або Telnet з віддаленим комп'ютером. Cisco розповсюджує цей плагін без будь-яких змін відповідно до GNU General Public License. Веб-сайт, на якому міститься джерело розповсюдженого плагіна, — http://javassh.org/ .

• vnc-plugin.jar — плагін Virtual Network Computing дозволяє віддаленому користувачеві використовувати монітор, клавіатуру та мишу для перегляду та керування комп'ютером із увімкненим спільним доступом до віддаленого робочого столу. Cisco розповсюджує цей плагін без будь-яких змін відповідно до GNU General Public License. Веб-сайт, на якому міститься джерело розповсюдженого плагіна, – http://www.tightvnc.com .

- У вікні «Пристрій» обрати потрібний пристрій ASA.
- Обрати Remote Access VPN -> SSL VPN -> Other Settings у полі вибору політики.
- На сторінці «Інші налаштування» натиснути вкладку «Плагін».
- Натиснути «Створити» або обрати плагін у таблиці та Натиснути «Редагувати» .
- Відкриється діалогове вікно Add/Edit Plug-in.
- У списку плагінів обрати тип плагіна, який потрібно завантажити з сервера Security Manager на пристрій
- У полі «Файл плагіна» Ввести ім'я об'єкта «Файл», який ідентифікує файл плагіна, або Натиснути «Вибрати» , щоб вибрати об'єкт. Також можна створити об'єкт File за допомогою селектора об'єктів.
- Натиснути OK .

3.1.9. Налаштування параметрів клієнта SSL VPN

Ця процедура показує, як визначити зображення та профілі клієнта SSL VPN і налаштувати кеш-пам'ять для клієнта SSL VPN і зображень Cisco Secure Desktop на пристрої безпеки [20]:

1. У вікні «Пристрій» обрати потрібний пристрій ASA.
2. Обрати Remote Access VPN -> SSL VPN -> Other Settings .
3. На сторінці «Інші параметри» натиснути вкладку «Параметри клієнта».
4. У таблиці «Зображення клієнта AnyConnect» можна додати нове зображення або відредагувати наявне, як описано нижче:

- Натиснути «Створити» під таблицею або обрати зображення в таблиці та натиснути «Редагувати» . З'явиться діалогове вікно Add/Edit AnyConnect Client Image.
- У полі «Зображення клієнта AnyConnect» ввести ім'я об'єкта «Файл», який ідентифікує клієнт AnyConnect, або Натиснути «Вибрати» , щоб вибрати об'єкт. Також можна створити об'єкт File за допомогою селектора об'єктів..
- Ввести порядок, у якому пристрій безпеки завантажує клієнтські зображення на віддалений ПК. Спочатку завантажується зображення у верхній частині таблиці. Тому вам слід ввести нижче значення для образу, який використовується найбільш часто зустрічається операційною системою.
- Натиснути OK , щоб зберегти зміни.

5. У таблиці «Профіль клієнта AnyConnect» можна створити новий профіль або відредагувати шлях до наявного, як описано нижче:

- Натиснути «Створити» під таблицею або обрати профіль у таблиці та натиснути «Редагувати» . З'явиться діалогове вікно Add/Edit AnyConnect Client Profile.
- Ввести назву профілю клієнта.
- У полі «Профіль клієнта AnyConnect» ввести ім'я об'єкта «Файл», який ідентифікує профіль клієнта AnyConnect, або натиснути «Вибрати», щоб вибрати об'єкт. Також можна створити об'єкт File за допомогою селектора об'єктів..
- Натиснути OK , щоб зберегти зміни.

6. У полі «Максимальний розмір» вказати розмір кеш-пам'яті в МБ, який буде виділено для клієнта SSL VPN і образів CSD на пристрої.

3.2. Оптимізація використання рішення віддаленого доступу VPN

3.2.1. Тунелювання трафіку

AnyConnect тунелює весь трафік за замовчуванням. Зв’язок з Інтернетом також тунелюється, тому під час доступу до веб-сайту через внутрішній проксі продуктивність VPN віддаленого доступу та швидкість доступу до веб-сайту буде знижена.

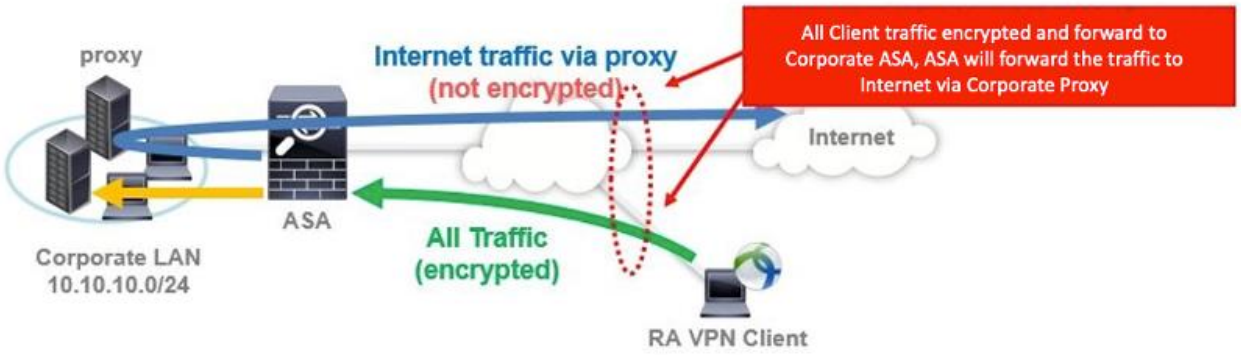

Рис. 3.3. Тунелювання трафіку

Одним із найпростіших і найефективніших способів максимізації продуктивності корпоративних пристроїв та ASA є «тунелювання лише того трафіку, який дійсно потрібен». Очікується, що ця підтримка зменшить трафік між терміналом AnyConnect і ASA, і, як очікується, покращить продуктивність як терміналу, так і ASA [18, 19].

Приклад використання розділеного тунелю, який є технологією, яка розділяє зв’язок для певних пунктів призначення, а також заходи безпеки терміналу під час використання цієї функції:

1. Тільки внутрішній зв'язок є розділеним тунелюванням

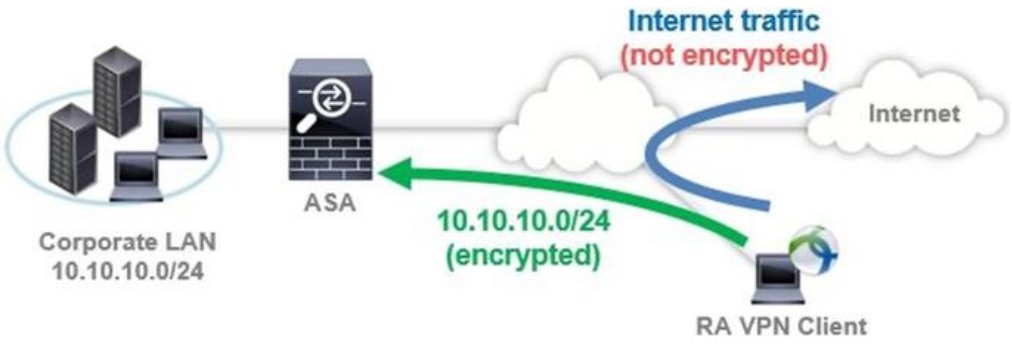

Рис. 3.4. Внутрішній зв'язок є розділеним тунелюванням

Можна очікувати покращення продуктивності як клієнта, так і ASA, дозволивши клієнту отримати прямий доступ до Інтернету та тунелюючи лише зв’язок із компанією.

2. Виключити тунелювання лише для зв’язку з певним доменом (динамічне розділене тунелювання)

Рис 3.5. Динамічне розділене тунелювання

Під час тунелювання всіх комунікацій можуть виникнути випадки, коли потрібно отримати прямий доступ до Інтернету лише для хмарних програм, таких як Office 365 і Webex, або для зв’язку з визначеними доменами чи FQDN. У цьому випадку та під час використання AnyConnect можна виключити лише вказаний домен із цільового тунелювання за допомогою функції динамічного розділеного тунелювання. Максимальна довжина символів динамічного розділеного тунелювання (DST) може становити до 5000 символів, за винятком роздільників (приблизно 300 доменних імен звичайного розміру). Якщо необхідно налаштувати багато доменів/FQDNS довжиною понад 5000 символів, необхідно

використовувати «Статичне розділене тунелювання, щоб не тунелювати весь інтернет-трафік» і «Umbrella» замість DST.

3. Заходи безпеки терміналу

Для підприємств, які часто виходять в Інтернет, наприклад у хмарі, за допомогою ефективного використання розділених тунелів можна тунелювати лише необхідний трафік і значно підвищити продуктивність терміналу та ASA. Однак прямий доступ до Інтернету з пристрою безпосередньо наражає пристрій на загрози.

Наступні додаткові модулі доступні для AnyConnect для захисту корпоративномуого пристрою.

- Cisco Umbrella - веб-безпека DNS. Шкідлива URL-адреса, довільна URL-адреса, фільтрація програм тощо.
- Cisco AMP - Розширений захист від шкідливих програм. Підтримує машинне навчання, інтегроване керування та візуалізацію шляхів зараження.

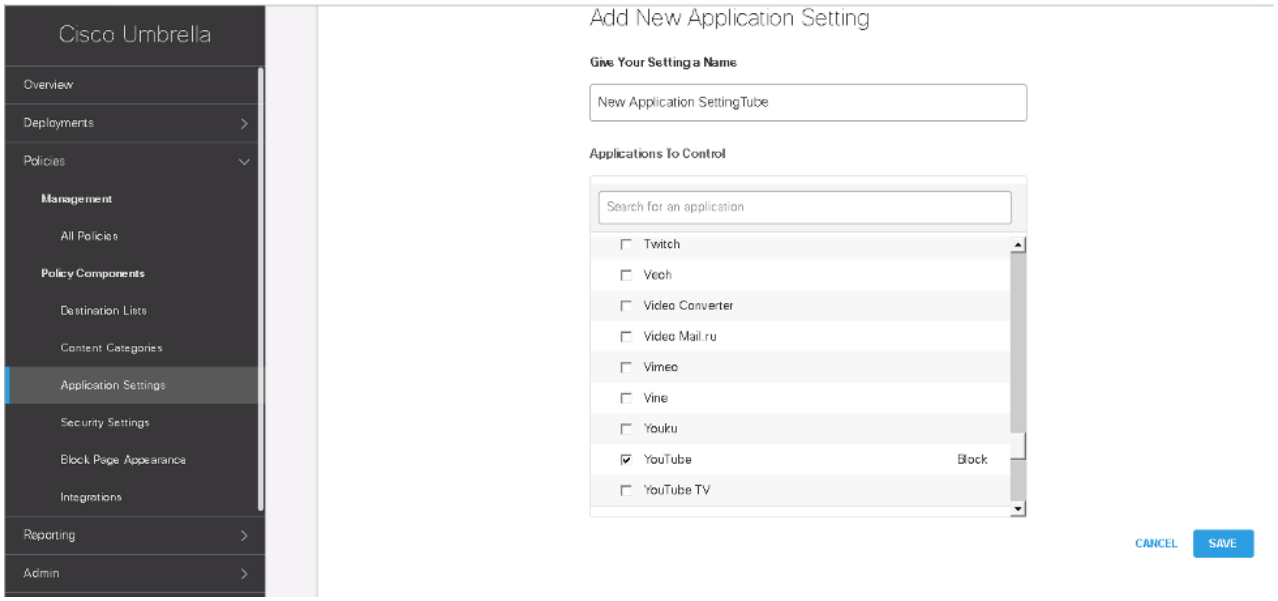

Рис. 3.6. Керування доступом програми YouTube з панелі керування Umbrella

3.2.2. Використання DTLS

Підключення ASA клієнта AnyConnect виконується за такими кроками:

1. Встановити сеанс, підключившись до ASA за допомогою SSL (TCP443) і обмінявшись сертифікатами, автентифікацією, інформацією профілю тощо.

2. Під час передачі даних за допомогою SSL, якщо UDP443 доступний, він автоматично перемикається на передачу даних за допомогою тунелю DTLS за допомогою UDP443.

3. Якщо UDP443 не можна використовувати, необхідно продовжити передачу даних за допомогою тунелю SSL (TLS), який використовує TCP443

Насправді замість SSL використовується більш безпечний TLS, але на дисплеї CLI використовується SSL.

Причина переходу на використання DTLS, коли UDP443 доступний, полягає в тому, що, оскільки UDP є високошвидкісним протоколом з невеликими накладними витратами, можна очікувати ефективності передачі даних. Клієнт AnyConnect активно намагатиметься передати дані через тунель DTLS, якщо UDP443 доступний [15].

У разі передачі даних за допомогою TLS на основі TCP відбувається обробка, характерна для TCP, наприклад контроль послідовності та порядку, і особливо у випадку низької якості або перевантаженої мережі, повторна передача та затримка через відкидання пакетів або зміну порядку тощо. Також відбуваються, і це покращить продуктивність. Це стає фактором зниження. Залежно від середовища зв’язку продуктивність TLS може бути меншою, ніж уполовину, ніж DTLS.

Якщо необхідно встановити з’єднання AnyConnect за допомогою DTLS, маршрут має дозволяти як SSL (TCP 443), так і DTLS (UDP 443). Наприклад, якщо дистанційний працівник підключається віддалено, треба переконатися, що корпоративний маршрутизатор підтримує UDP443, а також TCP443.

Можна перевірити спосіб підключення та статус обміну даними за допомогою DTLS за допомогою команди show vpn-sessiondb detail anyconnect. На рисунку можна побачити, що клієнт AnyConnect підключено за допомогою

DTLSv1.2, шифрування виконується за допомогою AES-GCM-256, і є близько 400 Мбайт надсилання (Tx) і близько 6 Мбайт отримання (Rx) [14, 15].

На стороні терміналу AnyConnect можна перевірити, чи DTLS чи TLS використовується для з'єднання, на вкладці «Статистика» розширеного вікна. Якщо пристрій підключається за допомогою TLS, можливо, UDP 443 заблоковано десь на шляху між пристроєм і ASA.

Рис. 3.7. Використання DTLS (UDP443) для передачі даних

Крім того, особливо в середовищі, до якого багато користувачів, як великі компанії та провайдери Інтернету, мають віддалений доступ, UDP443 заборонений у деяких середовищах зв'язку кінцевих користувачів (або UDP забувається), а також DTLS і нерідко є змішані з'єднання TLS. Важко зробити всі

з’єднання лише з’єднаннями DTLS, але можна очікувати покращення продуктивності, збільшивши коефіцієнт підключення DTLS.

3.2.3. Використання правильного MTU

Загалом, чим більший розмір пакета, тим більше даних можна надіслати за один раз, і тим легше отримати хорошу продуктивність. Крім того, чим більший обсяг даних можна надіслати за один раз, тим меншою кількістю пакетів потрібно обмінюватися, що зменшує кількість разів шифрування та дешифрування кожного пакета та покращує продуктивність ASA. Однак, якщо розмір пакета перевищує MTU маршруту, потрібні фрагментація (розподіл пакетів) і повторне збирання (повторне збирання пакетів), і продуктивність, швидше за все, погіршиться. Таким чином, легше отримати високу продуктивність, використовуючи розміри пакетів, які не є фрагментованими.

Під час використання DTLS MTU між терміналами AnyConnect налаштовується автоматично, тому індивідуальне налаштування зазвичай не потрібно. Оскільки максимальні накладні витрати на інкапсуляцію та шифрування DTLS становлять 94 байти, термінал AnyConnect використовує значення, отримане шляхом віднімання 94 байтів із MTU мережевого адаптера, який буде використано, а також автоматично перевіряє, чи є проблема з MTU маршруту. Наприклад, якщо фізичний адаптер терміналу має MTU 1300, AnyConnect спочатку спробує використати (1300-94) MTU 1206. Якщо MTU1206 виявить фрагменти в маршруті, він автоматично налаштується на використання нижчого MTU [10].

Навіть якщо використовується TLS, підтримується автоматичне налаштування MTU, але якщо клієнтське середовище не дозволяє DTLS (UDP443), щоб уникнути проблеми з повторним підключенням через 1 хвилину, доступне налаштування статичного AnyConnect MTU.

Слід зауважити, що з'єднання AnyConnect також підтримує IKEv2, але при використанні IKEv2 воно не сумісне з автоматичним налаштуванням MTU, тому потрібне налаштування вручну.

Можна перевірити MTU за замовчуванням у меню Конфігурація -> Віддалений доступ VPN -> Мережевий (клієнтський) доступ -> Групова політика. MTU за замовчуванням становить 1406.

Рис. 3.8. Перевірка MTU

Можна налаштувати MTU для кожної групової політики в меню Додатково -> Клієнт AnyConnect.

Можна налаштувати MTU для кожного локального користувача в меню Конфігурація -> Віддалений доступ VPN -> AAA/Локальні користувачі -> Локальні користувачі та Політика VPN -> Клієнт AnyConnect.

3.2.4. Зменшення непотрібних функцій і налаштувань

Оскільки багато функцій ASA обробляються програмним забезпеченням, продуктивність потроху знижується зі збільшенням кількості використовуваних функцій, встановленого обсягу та частоти використання (сеанси AnyConnect і кількість підключень).

Наприклад, якщо ASA використовується не лише як завершення VPN віддаленого доступу, але й як пристрій PAT / брандмауер для доступу до Інтернету для внутрішнього зв’язку, продуктивність ASA також використовується для обробки NAT і брандмауера. Це зменшує резерв продуктивності для. І навпаки, якщо ви використовуєте ASA як машину віддаленого доступу VPN лише для завершення, ви можете максимізувати продуктивність обробки VPN віддаленого доступу ASA.

Наприклад, під час використання фільтра VPN для контролю доступу AnyConnect навантаження перевірки ACL для кожного з’єднання збільшується зі збільшенням кількості рядків налаштування ACL. Наприклад, навантаження на перевірку ACL можна зменшити, зменшивши кількість параметрів ACL, реалізувавши «Контроль на основі сегмента за сегментом, а не на основі IP, наскільки це можливо» та «Контроль портів призначення якомога менше». Крім того, навантаження доступу на ASA зменшується або мінімізується, а керування доступом ACL виконується на призначеній IP-адресі іншим пристроєм на маршруті (наприклад, комутатором або маршрутизатором), що зменшує навантаження на обробку ASA. Можливо.

Наприклад, якщо використовується політика динамічного доступу (DAP), необхідно зменшити кількість записів максимум до 20-30, щоб покращити продуктивність контрольної точки (CP) і запобігти проблемам, налаштувавши DAP.

Наприклад, у середовищі, де інтенсивно використовується функція Syslog, налаштування Syslog, які виводять величезну кількість журналів, можуть призвести до зниження продуктивності через обробку генерації Syslog і тиску пропускної здатності через повідомлення Syslog. Можна зменшити навантаження на логування, встановивши відповідний рівень. Наприклад, не вмикати логування на консолі/моніторі, слід уникати логування налагодження під час нормальної роботи та зменшити кількість серверів системного журналу, якщо налаштовано (рис.3.9).

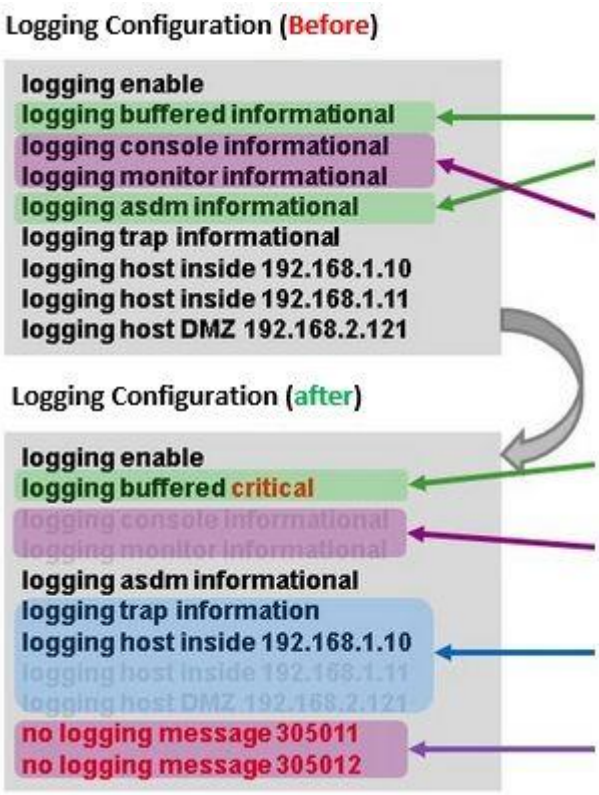

Рис. 3.9. Логування

Навантаження на обробку функцій керування зв’язком, таких як ACL і DAP, і функцій керування, таких як Syslog, невелике. Однак, якщо кількість підключень різко зростає через швидке збільшення кількості користувачів через дистанційну роботу, і якщо для кожного підключення виконується великий обсяг контролю, наприклад ACL і DAP, або виникає величезна кількість протоколювання зв’язку, навантаження може збільшуватися мультиплікативним чином, що призводить до незначного навантаження. Збереження простої конфігурації та оптимізація ASA для зосередження на обробці VPN-з’єднань віддаленого доступу може покращити продуктивність ASA [19].

3.2.5. Перевірка та відключення користувачів із високим трафіком

Якщо шукати сеанси з високим трафіком і спостерігати надмірне використання, яке може вплинути на загальну продуктивність, можна заохотити

користувачів із високим трафіком утриматися від їх використання або змусити їх відключитися:

1. Перевірити наявність сеансів AnyConnect із великим трафіком

Необхідно виконати команду show vpn-sessiondb anyconnect | in Username | Bytes | Duration, щоб перевірити обсяг трафіку та час підключення для кожного імені користувача. У наведеному нижче прикладі вихідних даних співрробітник (ginko) має час з'єднання приблизно 10 хвилин і близько 5 ГБ (≈ 5 156 556 220) даних надсилається (Tx) з ASA, а Cisco має час з'єднання приблизно 1 хвилину. Можна констатувати, що ASA отримує (Rx) дані розміром 23 МБ (≈23 545 802).

ASAv10(config)# show vpn-sessiondb anyconnect | in Username|Bytes|Duration
Username : ginko Index : 35
Bytes Tx : 5156556220 Bytes Rx : 75519009
Duration : 0h:10m:31s
Username : cisco Index : 36
Bytes Tx : 661625 Bytes Rx : 23545802
Duration : 0h:01m:08s
ASAv10(config)#

Можна від'єднати сеанс AnyConnect із вказаним іменем користувача за допомогою команди vpn-session logoff name <Username->.

ASAv10 (config) # vpn-session logoff name ginko
Do you want to logoff the VPN session (s)? [Confirm]
INFO: Number of sessions with name "ginko" logged off: 1

Після від'єднання термінал AnyConnect висвітить причину від'єднання «Захищений шлюз припинив з'єднання VPN. Від захиеного шлюзу було отримано таке повідомлення: Скидання адміністратора».

Навіть якщо від'єднатися, клієнт AnyConnect може повторно підключитися до ASA. Якщо потрібно завжди відхиляти підключення цього користувача, потрібно вжити додаткових заходів, таких як видалення або призупинення облікового запису користувача.

Під час використання ASDM можна перевірити статус зв'язку з користувачем і від'єднати зазначеного користувача з Моніторинг-> VPN-> Статистика VPN-> Сеанси.

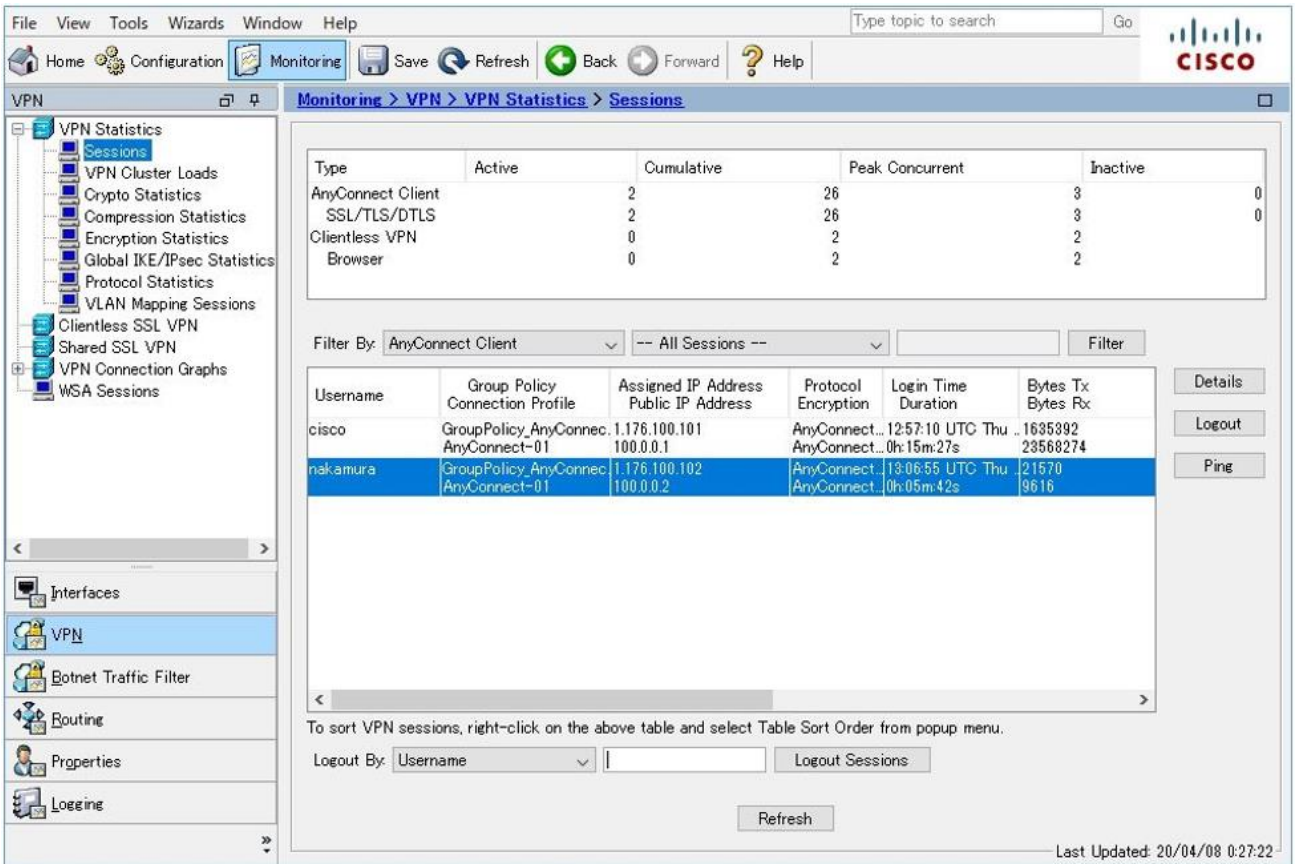

Рис. 3.10. Моніторинг

Висновки до третього розділу

Досліджено Cisco Security Manager, що дозволяє налаштувати як IPSec VPN віддаленого доступу, так і SSL VPN віддаленого доступу. Security Manager забезпечує гнучку конфігурацію та керування VPN віддаленого доступу.

Вивчено існуючі політики конфігурації VPN віддаленого доступу з існуючих живих пристроїв або з конфігураційних файлів. Можна змінити та розгорнути нові або оновлені політики, якщо це необхідно.

Проаналізовано функції та можливості, яких потребує корпоративна мережа.

Налаштовано використання майстра для створення базового VPN віддаленого доступу та додаткові функції, які не входять у програму окремо.

Зазначено, що Cisco Security Manager забезпечує гнучкість призначення політик конфігурації VPN віддаленого доступу: перегляд пристрою або режим перегляду політики. Для деяких політик можна також призначити стандартну політику (приватну політику) або спільну політику.

Показано можливості оптимізації роботи віддаленого доступу VPN у межах середовища корпоративної мережі.

ВИСНОВКИ

В магістерскій роботі отримано наступні теоретичні та теоретично-практичні результати:

1. Розглянуто питання організації та забезпечення інформаційної безпеки в корпоративній мережі, були вивчені основні вектори втрат даних по каналу рішення віддаленого доступу VPN

2. Досліджено основні технології тунелювання, визначені принципи їх роботи, призначення та сфери застосування у віртуальних приватних мережах.

3. Зазначено, що VPN використовують тунелювання за допомогою протоколів IPsec, L2TP, PPTP та SSL, шифрування трафіку для забезпечення конфіденційності даних, аутентифікацію користувача та алгоритми забезпечення цілісності даних.

4. Наведено та продемонстровано налашутування видів віддаленого доступу VPN, а саме IPSec VPN та SSL VPN. Наведено принципи роботи на налаштування групових політик ASA та проксі, можливості його обходу.

5. Приділено увагу особливостям роботи рішення та надано практичні рекомендації щодо оптимізації використання: тунелювання трафіку, використання DTLS, використання вірного MTU, поведінковий аналіз трафіку користувачів.