ISSN 2219-9365

https://doi.org/10.31891/2219-9365-2022-72-4-4
УДК 621.396.969.1

Юлій БОЙКО
Хмельницький національний університет
https://orcid.org/0000-0003-0603-7827
e-mail: boiko_julius@ukr.net
Богдана БІЛЯВЕЦЬ
Хмельницький національний університет
https://orcid.org/0000-0002-4330-3605
e-mail: dana.bilyavets@gmail.com

SAML: ДЕФІНІЦІЯ ТА ПРИНЦИП РОБОТИ ЧЕРЕЗ VPN ТУНЕЛЬ У ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖАХ

У статті піднімаються питання віддаленого підключення користувачів до робочих місць. Аналізуються технології досягнення безпечного підключення та реалізація двоетапної аутентифікації зареєстрованих осіб внутрішньої мережі, що дає можливість підвищити продуктивність працівників завдяки доступу до файлів і системних ресурсів. Розглянута технологія полегшує роботу з іншими колегами, які працюють в межах офісу або в інших місцях. Організації мають можливість найняти найкращих спеціалістів із будь-якої частини світу, що забезпечує покращену якість продукції без додаткових накладних витрат. Проведено аналіз принципів надання віддаленого доступу за допомогою VPN. Показано, що VPN було розроблено щоб дозволити філіям безпечно отримувати доступ до програм організації. Таким чином, він забезпечує зашифроване та безпечне підключення до мережі. Визначено особливості налаштування віддаленого доступу, що має важливе значення для віддалених працівників, оскільки воно дає їм прямий доступ до ресурсів організації, не перебуваючи в офісі. Користувачі можуть підключатися до мережі з різних областей у всьому світі за допомогою своїх пристроїв. Встановлено, що за наявності віддаленого доступу персонал може отримати доступ до віддаленого пристрою без фізичної присутності. Визначено, що безпека покращується завдяки інкапсуляції даних у зашифрованому тунелі, який захищає їх від перехоплення. Це особливо важливо для віддалених працівників, які часто підключаються через незахищену інфраструктуру, наприклад публічного Wi-Fi у готелі, аеропорту чи вдома. Доведено, що метод віддаленої роботи, запроваджений багатьма організаціями, має важливі переваги але супроводжується виникненням нових ризиків які можуть зруйнувати всю компанію. Описано вимоги до забезпечення належної корпоративної безпеки під час впровадження системи віддаленої роботи, керуючись протоколами підключення віддаленого доступу. З метою підтвердження припущення було проведено статистичний аналіз і порівняння показників обслуговування користувачів при використанні технологій IPSec VPN та SSL VPN.
Ключові слова: система VPN, SAML, двофакторна аутентифікація, віддалені робочі місця

Juliy BOIKO, Bohdana BILIAVETS
Khmelnytskyi National University

SAML: DEFINITION AND PRINCIPLES OF OPERATION THROUGH A VPN TUNNEL IN SECURE INFORMATION NETWORKS

The article raises issues of remote connection users to workplaces. The technologies for achieving a secure connection and the implementation of two-step authentication of registered persons of the internal network are analyzed, which allows increasing the productivity of workers through access to files and system resources. The considered technology makes it easier to work with other colleagues working in the office or in other places. Organizations can hire the best talent from anywhere in the world, delivering improved product quality without additional overhead. An analysis of the principles providing remote access using VPN has been carried out. VPN is shown to have been designed to allow branch offices to securely access an organization's programs. Thus, it provides an encrypted and secure connection to the network. The features of setting up remote access are determined, which is important for remote workers, since it gives them direct access to the organization's resources without being in the office. Users can connect to the network from different areas around the world using their devices. It has been determined that when setting up remote access, IT staff can access a remote device without being physically present. It is determined that security is improved by encapsulating the data in an encrypted tunnel that protects it from interception. This is especially important for remote workers, who often connect through insecure infrastructure, such as public Wi-Fi at a hotel, airport, or home. The method of remote work adopted by several organizations has been proven to have important benefits, but comes with new risks that can destroy the entire company. The requirements for ensuring proper corporate security when implementing a remote work system are described, guided by remote access connection protocols. It has been proven that secure data exchange is important in the conditions of modern information technologies, when real tasks are performed with the requirement of high efficiency. It is shown that due to the emergence of predictable threats to stay at the enterprise, it becomes necessary to study the secure connection and authorization of users to their workplaces.
Keywords: VPN system, SAML, two-factor authentication, remote workplaces

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Зловмисники вправно проникають у корпоративні та домашні інформаційні мережі з метою викрадення конфіденційної інформації. Метою є крадіжка особистих персональних та корпоративних даних,

таких як облікові дані з відповідним доступом, номера банківських карт, вилучення цінних документів з можливістю шантажування та викупу. Тому налаштування безпечної інформаційної мережі потребує відповідального ставлення до захисту особистих даних від кіберзлочинців.

Захищеність мережі асоціюється з розгортанням великої корпоративної мережі, до якої належать тисячі робочих місць. Однак, навіть кілька пристроїв підключених до домашнього роутера також вважаються мережею. Забезпечення їх безпеки не менш важливе, оскільки вони також містять конфіденційні файли.

Безпечний обмін даними є важливим з використанням сучасних інформаційних технологій, в ході виконання реальних завдань, коли вони потребують вирішення на високому рівні, що є можливе лише із врахуванням вимог до захисту інформації і даних. Аналізуючи наявність прогнозованих загроз захисту конфіденційної інформації, виникає необхідність дослідження безпечного підключення та авторизації користувачів до своїх робочих місць.

Метою статті є порівняльний аналіз і експериментальна перевірка віддаленого керування сервером авторизації на основі мови розмітки декларації безпеки SAML (Мови розмітки твердження безпеки).

Аналіз досліджень та публікацій

Організації все частіше починають використовувати незалежні джерела аутентифікації для програм та веб-порталів. Одним з дослідників SAML аутентифікації є викладач Луїсвільського університету Джеймс Левіс, який дослідив та підтвердив чимало її переваг, однією з яких є зменшення кількості звернень до служби технічної підтримки, що й досі актуально для функціонування багатьох організацій [1].

Виклад основного матеріалу

Структура інформаційних мереж в офісах приватних і державних компаній дозволяє працівникам отримати доступ до принтерів, підключитися до IT-ресурсів, передавати дані тощо. Загалом такий доступ є безпечним та захищає фірми і компанії від неоднозначних веб-сайтів. Організація корпоративної офісної мережі ґрунтується на принципі, коли всі працівники в офісі використовують локальну мережу. Це забезпечує їх ресурсами, а компанію – безпекою. Віддалені працівники не можуть увійти в систему, так як для цього потрібен віддалений доступ до робочого місця, що підводить до реалізації такого порталу.

Концепція VPN (віртуальної приватної мережі) віддаленого доступу означає, що віддалені співробітники можуть увійти в мережу конкретного офісу з будь-якого місця — з дому, у дорозі чи в будь-якому громадському місці, де є доступ до Інтернету. За таких умов вони отримають доступ до всіх ресурсів необхідної компанії, а корпоративні дані компанії, як і раніше, будуть захищені, навіть у випадку використання публічного Wi-Fi [2].

VPN використовують різні протоколи. Старіші протоколи, такі як PPP (протокол точка-точка) і PPTP(тунельний протокол типу точка-точка), вважаються менш безпечними. Розглянемо деякі типи протоколів безпеки.

PPTP був найпершим із протоколів безпеки та вперше випущений у Windows 95. Він вважається швидкісний, проте характеризується низьким рівнем шифрування.

IP Sec (безпека Інтернет-протоколу) — це популярний протокол, який захищає дані в транспортному або тунельному режимі.

Протокол тунелювання рівня 2 (L2TP)/IPSec. L2TP — це протокол VPN, який сам по собі не шифрує дані. У зв'язку з цим, він поєднується з шифруванням IPSec. Однією з його головних переваг є доступність для більшості пристроїв і операційних систем, які реалізовують високий рівень безпеки, але це може призвести до уповільнення з'єднань. В цьому випадку використовується процес подвійної інкапсуляції.

Secure Sockets Layer (SSL) і Transport Layer Security (TLS). SSL (рівень захищених сокетів) був протоколом шифрування VPN, який найчастіше використовувався до 2015 року. Подальшим його розвитком став протокол TLS(протокол захисту транспортного рівня) для шифрування даних, котрі передаються на сервер SSL VPN.

SSL — криптографічний протокол, який передбачає забезпечення більш безпечного зв'язку. По суті, це спосіб передачі інформації в Інтернеті, який характеризується прозорим шифрування даних. Протокол широко використовувався для обміну миттєвими повідомленнями та передачі голосу через IP (VoIP) у таких додатках, як електронна пошта, Інтернет-факс та інші. Згодом на підставі протоколу SSL 3.0 було розроблено та прийнято стандарт RFC (запити коментарів), який отримав назву TLS [3, 4].

TLS – протокол захисту транспортного рівня, який як і його попередник SSL – криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі Інтернет. SSL і TLS використовують для шифрування трафік в роботі з сайтами. Коли дані передаються за протоколом HTTPS (захищений протокол передачі гіпертексту), трафік шифрується сертифікатом який використовує той чи інший ресурс.

SSL-сертифікат — містить інформацію про власника, а також відкритий ключ, який використовується для створення захищеного каналу зв'язку. Організації та фізичні особи отримують підтвердження того, що сайт чи інший ресурс дійсно підтримують такий сертифікат і не відносяться до підробленого ресурсу. Сертифікати отримують або купують у авторизованих довірених центрах сертифікації.

Все це застосовується для обмеження несанкціонованого доступу особам, які потрапляють в канал зв'язку між адресатами з метою заволодіння інформацією або з метою її змінити, рис. 1.

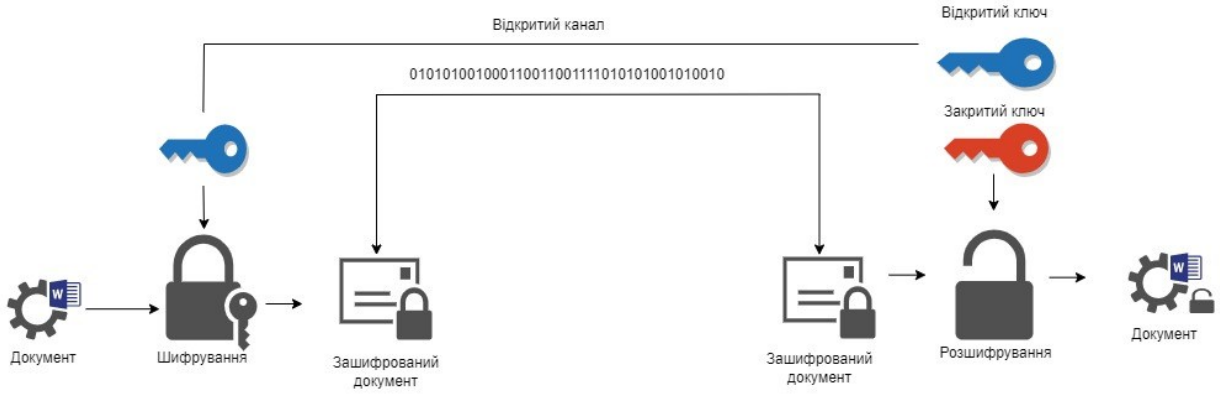

Рис. 1. Схема асиметричного шифрування документу при передачі файлів

У випадку асиметричного шифрування використовуються два різні ключі: один для шифрування (відкритий), інший для розшифровування (закритий).

Аутентифікація є невід'ємною частиною кожного з'єднання TLS. Розглянемо найпростіший процес аутентифікації між двома користувачами, рис. 2.

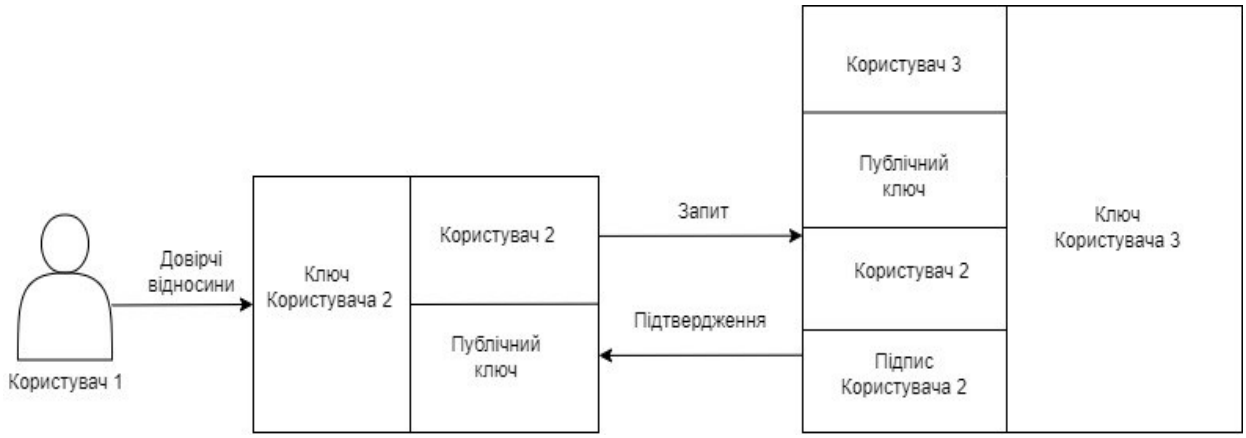

Рис. 2. Схема побудови довірчих відносин між користувачами

Обидва користувачі системи генерують власні відкриті та закриті ключі. Вони обмінюються відкритими ключами. Один з них генерує повідомлення, шифрує його своїм закритим ключем та відправляє іншому. Користувач 2 використовує отриманий від Користувача 1 ключ для розшифрування повідомлення і таким чином перевіряє справжність отриманого повідомлення.

Очевидно, що ця схема побудована на довірі між користувачами мережі. Передбачається, що обмін відкритими ключами відбувся, наприклад, під час особистої зустрічі. Таким чином, перший користувач впевнений, що отримав ключ саме від другого, тобто між ними побудовані довірчі відносини.

Нехай тепер Користувач 1 отримує повідомлення від Користувача 3, з яким він не знайомий, але який стверджує, що має довірчі відносини із Користувачем 2. Щоб це довести, Користувач 3 заздалегідь попросив підписати власний відкритий ключ закритим ключем Користувача 2 і прикріпив цей підпис до повідомлення Користувачу 1. У цьому разі Користувач 1 спочатку повинен перевірити підпис Користувача 2 на ключі Користувача 3, та переконатись у дійсності налагоджених довірчих відносин.

Описана вище схема є технологію створення «ланцюжка довіри».

У протоколі TLS дані ланцюга довіри засновані на сертифікаті автентичності, який надається спеціальними органами які називаються центрами сертифікації (CA). Центри сертифікації проводять перевірку та у випадку, якщо виданий сертифікат скомпрометований, виконується процедура відкликання

сертифікату [5-7]. З виданих сертифікатів складається вже розглянутий ланцюжок довіри. Ключовим елементом підтвердження ступеня довіри є сертифікат Root CA certificate (головний центр сертифікації), який підписаний авторизованим центром сертифікації, довіра до якого незаперечна. В загальному вигляді організація ланцюжка довіри виглядає так, як представлено на рис. 3.

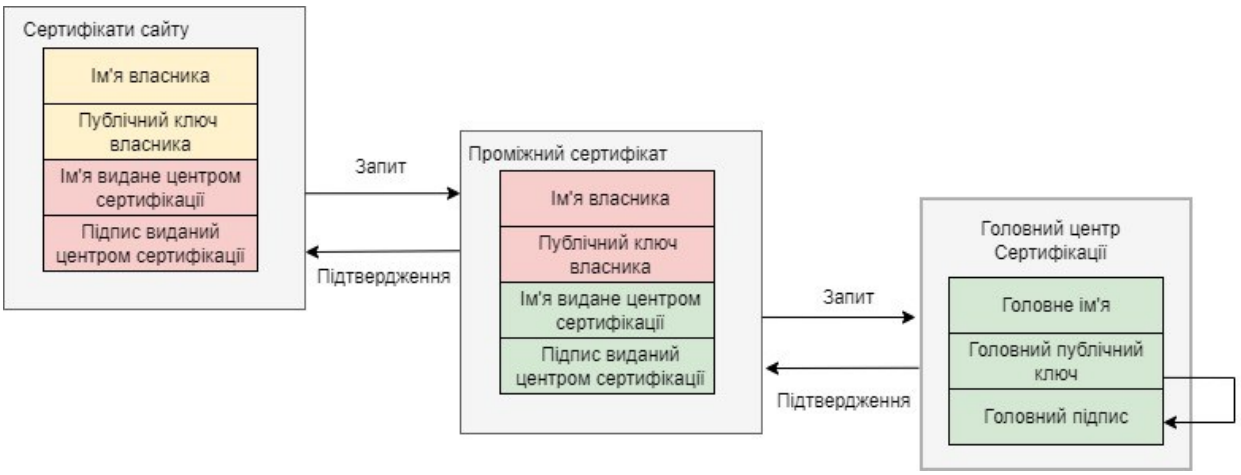

Рис. 3. Схема обміну сертифікатами для налаштування довірчих відносин

Розглянемо віддалений доступ VPN в умовах вже наявного підключення. Найбільш логічним і популярним способом передачі інформації є загальнодоступний Інтернет, тому VPN передає інформацію використовуючи його ресурси. Однак в цьому випадку, доступ до всієї інформації, яка передається через Інтернет і не є захищеною може отримати зловмисник. Наприклад, будь-хто у локальній мережі Wi-Fi може організувати підслуховування або доступ до інформації. Дієвим способом запобігання таких протиправних дій є застосування ефективних методів шифрування [7-9].

Процедура шифрування використовується на сервері доступу. Таким чином, будь-який контент, який передається через корпоративну мережу Wi-Fi піддається шифруванню. Така особливість забезпечує захист інформації та дозволяє доступ до читання даних лише в межах корпорації, окреслених мережевих меж офісу. Для інших осіб, непов’язаних з структурою офісних мереж доступ до інформації буде закрито.

Доступ до інформації можна отримати на основі серверу доступу. Сервер доступу володіє ключем для розшифрування зашифрованої інформацій [8]. В цьому випадку, будь-яка інформація, яка далі надсилається назад на певний пристрій із сервера доступу, також піддається шифруванню, а отже, все, що надходить через таке з’єднання в будь-якому напрямку неможливо прочитати іншим стороннім особам.

Завдяки параметрам на сервері персонал може використовувати доступе їм програмне забезпечення. Сервер доступу можна налаштувати для роботи в режимі первинного-вторинного відновлення після відмови для розгортання локальної мережі, щоб підтримувати високу доступність яка необхідна для цілодобової роботи без вихідних.

SAML, як вже будо зазначено вище, скорочення від Security Assertion Markup Language (Мова розмітки декларації безпеки). ЇЇ ключова роль у забезпеченні мережевої безпеки полягає в тому, що її застосування дозволяє отримати доступ до декількох додатків на основі використання одного набору облікових даних для авторизації. Така схема працює за допомогою обміну автентифікаційною інформацією у певному форматі між учасниками, зокрема між системою управління доступом та веб-додатком.

SAML представляє собою відкритий стандарт обміну даними автентифікації, що базується на мові XML (розширювана мова розмітки). Веб-програми використовують SAML, щоб передавати автентифікаційні дані між сторонами процесу: а саме між системою керування доступом та провайдером послуг. Для прикладу розглянемо використання в якості провайдера послуг FortiClient.

SAML з'явився в індустрії високих технологій для спрощення процесу автентифікації, коли користувачам потрібно було отримати доступ до кількох незалежних веб-додатків у різних доменах. До появи SAML, технологія єдиного входу цілком виконувала поставлені задачі, проте базувалася на файлах cookies, які були актуальними лише в межах одного домену.

При використанні SAML технологія входу досягається за рахунок узгодження процесу автентифікації із системою управління доступом. Веб-програми можуть використовувати SAML, через систему керування доступом. Такий метод автентифікації означає, що користувачам більше не потрібно запам'ятовувати численні комбінації логінів та паролів. Більш того, він має безперечну перевагу для провайдера, у вигляді підвищення рівня безпеки платформи, переважно завдяки тому, що усунуто необхідність зберігання паролів та процесів їх відновлення.

Концепція SAML працює шляхом обміну інформацією користувача (логіни, стан автентифікації, ідентифікатори та інші дані) між системою управління доступом та постачальником послуг. В результаті, це спрощує і забезпечує безпеку процесу автентифікації, так як в такому випадку користувачеві необхідно увійти в систему тільки один раз з використанням одного набору даних для входу. Таким чином, коли користувач надає запит для отримання доступу до сайту, SAML передає аутентифікаційні дані постачальника послуг, які в результаті дозволяють доступ користувачеві [10].

Процес двоетапної автентифікації починається в той момент, коли користувач намагається увійти в додаток, службу або систему, доки йому не буде надано доступ для використання. Алгоритм аутентифікації виглядає наступним чином:

- Крок 1. Користувач відкриває програму або веб-сайт, до якої він хоче отримати доступ. Здійснює введення облікових даних для входу.
- Крок 2. Далі він зазначає свої дані, якими звичайно є ім'я користувача та пароль. Додаток або веб-сайт підтверджує деталі та розпізнає, що було введено правильні дані початкової автентифікації на сервері авторизації в нашому випадку за протоколом SAML.
- Крок 3. Якщо програма або веб-сайт не використовує облікові дані для входу з паролем, буде згенеровано ключ безпеки для користувача. Ключ буде оброблено інструментом автентифікації, а сервер перевірить початковий запит.
- Крок 4: Користувачеві пропонується надіслати другий фактор аутентифікації. Очевидно, що таким фактором буде підтвердження прав власності. Наприклад, додаток або веб-сайт надішле унікальний код на мобільний пристрій користувача.
- Крок 5: Користувач вводить код у програму або на веб-сайт, і якщо код буде схвалено, він буде автентифікований і отримає доступ до системи.

Модель налаштування SAML для SSL VPN представлена на рис. 4.

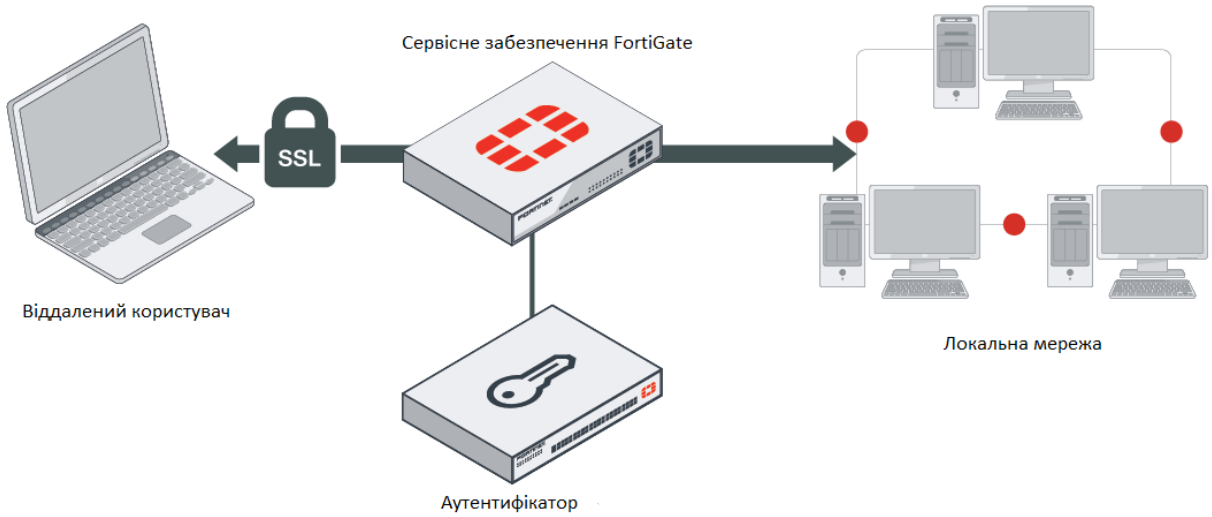

Рис. 4. Модель мережевого підключення обладнання сімейства FortiGate

Розглянемо процес мережевого підключення в наступній послідовності:

1. Адміністратор або кінцевий користувач налаштовує з'єднання SSL VPN із увімкненим SAML SSO.
2. FortiClient підключається до FortiGate.
3. FortiGate повертає посилання перенаправлення на сторінку авторизації SAML IdP.
4. FortiClient відображає сторінку авторизації IdP у вбудованому вікні браузера.
5. Кінцевий користувач вводить свої облікові дані у вікні для входу.
6. Після успішної спроби входу FortiClient встановлює тунель до FortiGate.

У такій схемі FortiGate налаштовується як SP (постачальник послуг), а FortiAuthenticator — як IdP (постачальник ідентифікаційної інформації).

Загалом, безпечне віддалене підключення можна реалізувати великим набором способів, використовуючи протоколи, а також групові чи індивідуальні політики безпеки [6, 11]. Потрібно наголосити, що особливість несанкціонованого входу зумовлюється і тим, що внаслідок витоку інформації можливий вільний доступ до облікових даних, і в цьому випадку такі дані можуть бути використані без відома особи власника та зокрема в злочинних цілях.

Головною відмінністю між SSL VPN та IPSec VPN є те, що IPSec будує захищене з'єднання між віддаленою локальною мережею та клієнтським робочим місцем дозволяючи отримати повний доступ до віддаленої мережі так, наче клієнтське робоче місце безпосередньо підключене до неї та надає всі доступні ресурси мережі. SSL VPN же для побудови захищеного з'єднання використовує браузер клієнтського робочого місця, завдяки чому надається доступ тільки до веб-ресурсів віддаленої локальної мережі [12, 13]. Враховуючи сучасні тенденції, більшість систем є веб-орієнтованими та надають доступ до своїх ресурсів за допомогою браузера, що полегшує взаємодію користувача з системою та не вимагає додаткових зусиль з боку користувача. У випадку поєднання SSL VPN з SAML авторизацією, зникає необхідність запам'ятовування безлічі облікових даних віддалених ресурсів, до яких надається доступ шляхом використання параметрів єдиного входу. Також, на відміну від IPSec, SSL VPN здійснює безпечне підключення тільки до веб додатків, що забезпечує додатковий рівень захисту віддаленої мережі та не дозволяє отримувати доступ до інших ресурсів, які не є веб орієнтованими та не потрібні користувачу.

Налаштуємо FortiGate SP як користувача SAML. Ми повинні налаштувати віддалений сертифікат IdP від FortiAuthenticator на FortiGate [11]:

```
config user saml
edit "saml-user"
set cert "Fortinet_Factory"
set entity-id "http://172.17.61.59:11443/remote/saml/metadata/"
set single-sign-on-url "https://172.17.61.59:11443/remote/saml/login/"
set single-logout-url "https://172.17.61.59:11443/remote/saml/logout/"
set idp-entity-id "http://172.17.61.118:443/saml-idp/101087/metadata/"
set idp-single-sign-on-url "https://172.17.61.118:443/saml-idp/101087/login/"
set idp-single-logout-url "https://172.17.61.118:443/saml-idp/101087/logout/"
set idp-cert "REMOTE_Cert_4"
next
end
```

Додаємо користувача SAML до групи користувачів:

```
config user group
edit "saml_grp"
set member "saml-user"
next
end
```

Встановлюємо групу SAML у налаштуваннях SSL VPN:

```
config vpn ssl settings
config authentication-rule
edit 1
set groups "saml-group"
set portal "full-access"
next
next
end.
```

Для проведення практичного порівняння початкове підключення користувачів було налаштовано за допомогою технології IPSec VPN. Впродовж 10 днів було зафіксовано подані заявки для відновлення паролів до віддалених робочих місць, які може змінювати лише адміністратор безпеки компанії, на відміну від доменного паролю, який користувач має можливість змінювати самостійно (рис. 5).

Кількість заявок про втрату паролю становила 53 з 500 підключених користувачів. В результаті реалізації SS VPN технології SAML, яка отримує дані про користувачів з Active Directory, тобто авторизація користувачів відбувається через доменне ім’я без використання додаткових облікових записів, зафіксована кількість заявок – 18. Отримані дані зведено до табл. 1

Таблиця 1

Порівняння показники технологій IPSec VPN та SSL VPN

Технологія	Кількість заявок	Відсоткове відношення %
IPSec VPN	53	10,6
SSL VPN	18	3,6

Проаналізувавши отримані дані, отримаємо результат у вигляді економії часу адміністратора на виконання заявок майже у 3 рази, рис. 6.

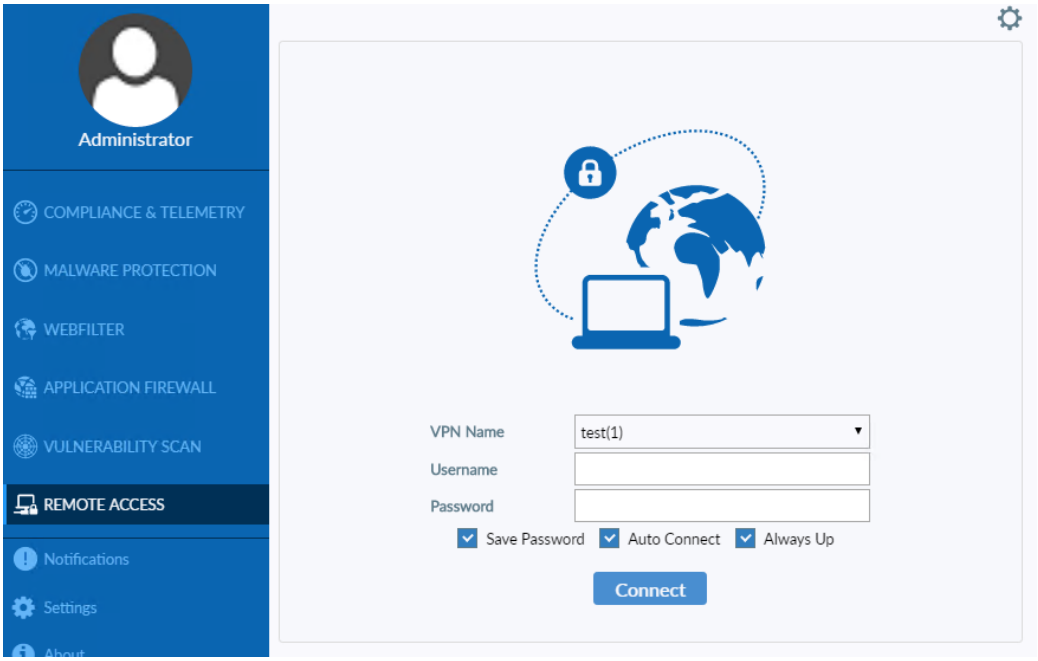

Рис. 5. Віддалене підключення за допомогою FortiClent

Рис. 6. Діаграма відсоткового співвідношення

Висновки з даного дослідження і перспективи подальшого розвитку у даному напрямі

Проведено порівняльний аналіз віддаленого підключення з використанням технології IPSec VPN та SSL VPN, з можливістю реалізації незалежного серверу авторизації. В ході вивчення питання, було виявлено, що налаштування SAML серверу можливе лише на базі протоколу SSL, відповідно до технічної документації та доступних функцій. Під час перевірки було виявлено можливість реалізації єдиного входу за доменним обліковим записом, що економить час для додаткового адміністрування, а також зберігання лог-файлів з діями користувачів в одному місці. Перевіривши на практиці віддалене підключення, за двома протоколами, отримано аналітику з якої встановлено, що підключення через SSL VPN створювало додаткове використання людського ресурсу.

Отже, підсумовуючи, потрібно наголосити на наявності існуючої значної кількості протоколів безпеки. У зв'язку з цим до вибору необхідного протоколу безпеки потрібно підходити індивідуально, тобто обирати найбільш зручний спосіб для кожного конкретного підприємства, врахувавши особливості побудови локальної мережі та задачі, які покладаються на неї. Перспективами подальших досліджень вважаємо використання хмарних рішень з можливістю розташування незалежних серверів авторизації, VPN-тунелю та зберігання домен-контролерів з даними про користувачів мережі.

Література

1. Дослідження аутентифікації SAML [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML (date of appeal: 5.11.2022).

2. Горбатий І. В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи / І. В. Горбатий, А. П. Бондарєв. – Львів : Львівська політехніка, 2016. - 336 с.

3. Смірнов О.А. Інформаційна безпека в комп'ютерних мережах: навчальний посібник /О.А. Смірнов, С.А. Конопліцька-Слободенюк, К.О. Смірнов, Т.В. Буравченко, Л.І. Смірнова [та інш.]. – Кропивницький : Центральноукраїнський національний університет, 2020. - 295 с.

4. Ільченко М.Ю. Телекомунікаційні системи /М.Ю. Ільченко, С.О. Кравчук. – Київ: Наукова думка, 2017. - 305 с.

5. Мирошниченко В. Використання сучасних інформаційних технологій. Формування мультимедійної компетентності / В. Мирошниченко. - Центр навчальної літератури, 2017. - 296 с.

6. Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security (date of appeal: 5.11.2022).

7. iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс]. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html (date of appeal: 5.11.2022).

8. SAML 2.0: A Clear and Concise Reference Paperback – 2021. – 187 p.

9. Open Source Security Testing Methodology Manual (OSSTMM) [Електронний ресурс]. – Режим доступу: https://www.isecom.org/OSSTMM.3.pdf (date of appeal: 5.11.2022).

10. A Framework for IP Based Virtual Private Networks / B. Gleeson, A. Lin, J. Heinanen. [Електронний ресурс]. — http://www.ietf.org/rfc/rfc2764.txt (date of appeal: 5.11.2022)

11. Настанова з налаштування обладнання сімейства FortiNet [Електронний ресурс]. – Режим доступу: https://docs.fortinet.com/document/fortigate/7.0.2/administration-guide/989067/configuring-saml-sso-in-the-gui (date of appeal: 5.11.2022).

12. Бойко Ю.М. Концептуальні особливості реалізації безпровідних сенсорних мереж / Ю.М. Бойко, В.М. Локазюк, В.В. Мішан // Вісник Хмельницького національного університету. – 2010. – № 2. – С. 94–97.

13. Boiko J.M. Solutions improve signal processing in digital satellite communication channels /J. M. Boiko, A. I. Eromenko //20th International Conference on Microwaves, Radar and Wireless Communications. MIKON 2014. June, Gdansk – Poland. - 2014. – PP. 126-129.

References

1. Research on SAML authentication [Electronic resource]. – Access mode: https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML (date of appeal: 5.11.2022).

2. Horbatyi I. V. Telekomunikatsiini systemy ta merezhi. Pryntsypy funktsionuvannia, tekhnolohii ta protokoly / I. V. Horbatyi, A. P. Bondariev. – Lviv : Lvivska politekhnika, 2016. - 336 s.

3. Smirnov O.A. Informatsiina bezpeka v kompiuternykh merezhakh: navchalnyi posibnyk /O.A. Smirnov, S.A. Konoplitska-Slobodeniuk, K.O. Smirnov, T.V. Buravchenko, L.I. Smirnova [ta insh.]. – Kropyvnytskyi : Tsentralnoukrainskyi natsionalnyi universytet, 2020. - 295 s.

4. Ilchenko M.Iu. Telekomunikatsiini systemy /M.Iu. Ilchenko, S.O. Kravchuk. – Kyiv: Naukova dumka, 2017. - 305 s.

5. Myroshnychenko V. Vykorystannia suchasnykh informatsiinykh tekhnolohii. Formuvannia multymediinoi kompetentnosti / V. Myroshnychenko. - Tsentr navchalnoi literatury, 2017. - 296 s.

6. Audyt informatsiinoi bezpeky informatsiinykh system ta informatsiino-telekomunikatsiinykh system [Electronic resource]. – Access mode: http://www.uss.gov.ua/audit-of-information-security (date of appeal: 5.11.2022).

7. iWar: A new threat, its convenience and our increasing vulnerability [Electronic resource]. – Access mode: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html (date of appeal: 5.11.2022).

8. SAML 2.0: A Clear and Concise Reference Paperback - 2021. - 187 p.

9. Open-Source Security Testing Methodology Manual (OSSTMM) [Electronic resource]. – Access mode: https://www.isecom.org/OSSTMM.3.pdf (date of appeal: 5.11.2022).

10. A Framework for IP Based Virtual Private Networks / B. Gleeson, A. Lin, J. Heinanen. [Electronic resource]. — http://www.ietf.org/rfc/rfc2764.txt (date of appeal: 5.11.2022)

11. Fortinet family equipment configuration manual [Electronic resource]. – Access mode: https://docs.fortinet.com/document/fortigate/7.0.2/administration-guide/989067/configuring-saml-sso-in-the-gui (date of appeal: 5.11.2022).

12. Boiko J. M. Kontseptualni osoblyvosti realizatsii bezprovidnykh sensornykh merezh /J.M. Boiko, V.M. Lokaziuk, V.V. Mishan // Herald of Khmelnytskyi national university. – 2010. – № 2. – S. 94–97.

13. Boiko J.M. Solutions improve signal processing in digital satellite communication channels /J. M. Boiko, A. I. Eromenko //20th International Conference on Microwaves, Radar and Wireless Communications. MIKON 2014. June, Gdansk – Poland. - 2014. – PP. 126-129.