ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка
до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ТА ЗАСОБИ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ КОМЕРЦІЙНОЇ ОРГАНІЗАЦІЇ ІЗ ВИКОРИСТАННЯМ UMBRELLA CLOUD-DELIVERED FIREWALL (CDFW)»

Виконав студент 6 курсу, групи БСДМ - 63
спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Грищенко Я.О.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. З кожним роком в інформаційному просторі стає все більше загроз направлених на комерційні організації і тільки завдяки окремим технологіям захисту ми можемо мінімізувати їх вплив на захищену мережу.

Безпрецедентні зміни у сфері корпоративної безпеки та мережевих технологій не припиняються і до сьогодні, оскільки ринок постійно стимулює відділи безпеки використовувати хмарні технології. Широке використання хмарних технологій є основоположним для бізнесу.

Віддалені робочі місця стають дедалі поширенішим явищем в IT-компаніях. Традиційно, організації направляли інтернет-трафік з віддалених місць назад у центральне місце для забезпечення безпеки, але це стало непрактичним через високу вартість і проблеми з продуктивністю. Тому, реалізація технології Umbrella Cloud-Delivered Firewal (CDFW) є відмінним засобом у протидії даним загрозам для побудови захищеної мережі комерційної організації, також вона має багато сучасних функцій захисту, яких не мають її аналоги.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології захисту та побудови захищеної мережі комерційної організації на прикладі Umbrella Cloud-Delivered Firewall (CDFW)»

Об'єкт дослідження – захищена мережа комерційної організації.

Предмет дослідження – технології та засоби побудови захищеної мережі на основі Umbrella Cloud-Delivered Firewall.

Мета роботи – розробити рекомендації щодо застосування технології побудови захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewall.

Наукові завдання:

— дослідити технології та засоби побудови захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewal (CDFW).

— проаналізувати особливості побудови захищеної мережі комерційної організації;

— встановити сутність побудови захищеної мережі комерційної організації;

— проаналізувати основні функції та принципи реалізації захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewal (CDFW).

Методи дослідження – теорія інформації, теорія складних систем, теорія алгоритмів захисту інформації, вектори атак, опрацювання літератури за даною темою, аналіз міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: полягає в розробці рекомендації щодо застосування технології побудови захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewall.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на трьох конференціях:

1) Всеукраїнська науково-технічна конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 48-50 стр.

2) VI Міжнародної науково-практичної конференції «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2022), Навчально-науковий інститут інформаційних технологій, 23-25 червня 2022 р., 63-65 стр.

3) XIV Науково-технічна конференція студентів та молодих вчених навчально-наукового інституту інформаційних технологій державного університету телекомунікацій, 19 травня 2022 р., 12-13 стр.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ КОМЕРЦІЙНОЇ ОРГАНІЗАЦІЇ

1.1. Вплив атак на комерційні організації

Успішна кібератака може завдати серйозної шкоди комерційній організації. Вона може вплинути на підсумковий прибуток, а також на репутацію організації і довіру споживачів. Наслідки порушення безпеки можна розділити на три категорії: фінансові, репутаційні та юридичні.

Кібератаки часто призводять до значних фінансових втрат, що виникають унаслідок:

- крадіжки корпоративної інформації;
- крадіжки фінансової інформації (наприклад, банківських реквізитів або даних платіжних карт);
- крадіжки грошей;
- порушення торгових операцій (наприклад, неможливість здійснювати транзакції через Інтернет);
- втрата бізнесу або контракту;

Під час усунення порушення підприємства, як правило, також несуть витрати, пов'язані з ремонтом постраждалих систем, мереж і пристроїв.

Останнє опитування про порушення кібербезпеки у 2022 році урядом ЄС показало, що за останні 12 місяців 39 % організацій виявили кібератаки [1]. У цій групі були:

1. 31% підприємств вважають, що зазнавали атак не рідше ніж один раз на тиждень;
2. Кожен п'ятий заявив, що внаслідок атаки вони зіткнулися з негативними наслідками;

Що стосується матеріальних наслідків, то середня оціночна вартість кібератак за останні 12 місяців становить 20 млн доларів. Однак у групі середніх і великих підприємств ця цифра зростає до 80 млн [2].

Репутаційний збиток. Довіра - важливий елемент взаємин із клієнтами. Кібератаки можуть завдати шкоди репутації вашого підприємства і підірвати довіру клієнтів до вас. Це, своєю чергою, потенційно може призвести до:

- втрати клієнтів
- втрати продажів
- зниження прибутку

Репутаційний збиток може навіть вплинути на ваших постачальників або на відносини з партнерами, інвесторами та іншими третіми особами, зацікавленими у вашому бізнесі. Відповідно до останнього звіту охоронної компанії Comparitech за 2021 рік, ціни на акції компаній, які були скомпрометовані через витік даних, впали в середньому на 3,5%, що свідчить про втрату довіри до ринку.

Юридичні наслідки кіберзагрози. Закони про захист даних і конфіденційність вимагають від вас гарантувати безпеку всіх персональних даних, якими ви володієте, чи то дані ваших співробітників, чи то клієнтів. Якщо ці дані будуть випадково або навмисно скомпрометовані, а ви не вжили відповідних заходів безпеки, вам можуть загрожувати штрафи і санкції регулюючих органів.

Порушення операційної діяльності. Крім реального фінансового збитку, компанії часто стикаються з непрямими витратами від кібератак, такими як можливість серйозної перерви в роботі, що може призвести до втрати доходів. Кіберзлочинці можуть використовувати будь-яку кількість способів, щоб скувати нормальну діяльність компанії, чи то зараження комп'ютерних систем шкідливим ПЗ, що стирає цінну інформацію, чи то встановлення шкідливого коду на сервер, що блокує доступ до вашого сайту.

Наприклад, 2010 року хакери, які симпатизують WikiLeaks, помстилися гігантам кредитних карток Mastercard і Visa, провівши атаки, які тимчасово вивели з ладу їхні веб-сайти [3].

Рис.1.1. Логотипи компаній Mastercard і Visa

Вкрадена інтелектуальна власність. Певні види кіберзлочинів спрямовані на порушення або викрадення інтелектуальної власності компанії. Наприклад, сквотінг домену або кіберсквоттинг — це різновид кіберзлочинності, коли зловмисник реєструє доменне ім'я компанії (або його варіанти) до того, як компанія як власник торгової марки зможе це зробити. Не кажучи вже про те, що зараз багато компаній зберігають свою інтелектуальну власність і товарні знаки в хмарі, яка є вразливою для кіберзлочинів. Наприклад, майже 30% американських компаній повідомляють, що їхня інтелектуальна власність була вкрадена китайським контрагентом за останні 10 років.

Фінансові втрати для організації. Кіберзлочини можуть завдати великих фінансових збитків у різних формах:

- Порушення безпеки може призвести до втрати бізнесу, оскільки ваші клієнти більше не довіряють вам як бренду безпеки.
- Втрата конкурентної переваги, наприклад, якщо ваша цінова стратегія просочується до конкурентів.
- Порушення повсякденної діяльності може призвести до непрямих фінансових наслідків.
- Вимагання, наприклад, у вигляді програм-вимагачів.
- Наймання юристів, експертів з кібербезпеки та інших відповідних сторін для боротьби з кіберзлочинцями може потребувати значних витрат.

У 2017 році з системи Home Depot було викрадено інформацію про 50 мільйонів кредитних карток, що коштувало компанії 13 мільйонів доларів у Фонді розрахунків. Потенційні фінансові наслідки кіберзлочинності можуть бути серйозними, тому завжди краще запобігти атаці, ніж зменшувати збитки [4].

Викрадення даних. Одним із улюблених активів для зловмисників є особисті дані клієнтів. Їхню адресу/місцезнаходження, номери телефонів, електронні адреси чи навіть платіжну інформацію можна використати зловживати у формі соціальної інженерії чи іншими способами. Насправді організації, які мають доступ до камер, контактів, можуть створити ще більші проблеми для своїх користувачів.

Порушення роботи. Кібератаки, такі як DDoS та зараження зловмисним програмним забезпеченням, серед іншого, можуть призвести до серйозних перебоїв у повсякденній роботі організації, що може призвести не лише до втрати доходу, але й до потенційної шкоди репутації вашого бренду. Є кіберзлочинці, які спеціалізуються на атаках, щоб порушити звичайний бізнес, і є групи хактивістів, які активно атакують державні установи чи відомі підприємства, намагаючись протестувати проти передбачуваної неправомірності цільової компанії чи державного органу. Щоб відновити роботу після атаки, організація може вирішити зупинити операції та дії, доки не повернеться в нормальний стан, що призведе до значної затримки в робочих процесах.

1.2. Структура корпоративної мережі

Корпоративна мережа - це структурна мережа будь-якої організації, головною метою якої є створення ефективної внутрішньої та зовнішньої роботи цієї організації. По суті це взаємопов'язана сукупність локальних мереж під впливом глобальної мережі. Користувачами цієї мережі є виключно співробітники цієї організації. Часто корпоративна мережа включає охоплює офіси, відділення, підрозділи та інші структури організації в різних містах і країнах.

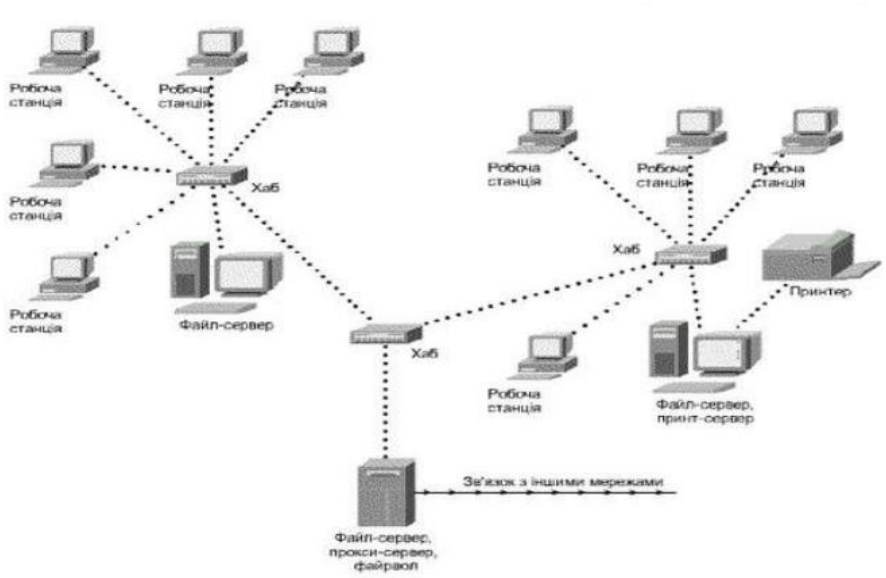


Рис.1.2. Структура корпоративної мережі

Термін «корпоративна мережа» означає фізичну, віртуальну або логічну інфраструктуру зв'язку, яка дозволяє системам і додаткам:

- Спілкуватися
- Обмінюватися інформацією
- Запускати служби та програми
- Аналізувати продуктивність системи

Корпоративна мережа фактично складається з інфраструктури, апаратних і програмних систем, а також комунікаційних протоколів, що використовуються для надання наскрізних послуг. Мережа (або її підмножина) може бути спроектована, розгорнута, оптимізована і налаштована для виконання унікального набору технічних завдань.

Основні елементи корпоративної мережі:

- Робочі станції
- Мережеве обладнання
- Сервери
- Поштовий сервер
- Сервер друку
- Сервер бази даних

- Файловий сервер
- Термінальний сервер (MS Office, 1C, Skype тощо)
- Web-сервер
- Сервер резервного копіювання
- Інші сервери

Основні компоненти локальної мережі підприємства:

- мережеві адаптери;
- концентратори;
- програмне забезпечення; програмне забезпечення;
- комутатори; програмне забезпечення; комутатори;
- маршрутизатор;
- кабельна система;

Типи корпоративних мереж. До найпоширеніших типів корпоративних мереж відносяться:

1. Локальні мережі
2. Глобальні мережі
3. Хмарні мережі

Локальна обчислювальна мережа (LAN). Локальна мережа - це комп'ютерна мережа, що об'єднує системи в межах невеликої будівлі або приміщення. Як правило, локальні мережі використовуються для особистих, некомерційних цілей, однак вони можуть також використовуватися як невеликі мережі для створення прототипів або тестування.

Також можна створювати локальні мережі логічно і віртуально в рамках більшої мережі. Наприклад, кожен відділ у мережі підприємства може керувати невеликою локальною мережею, у якій кілька комп'ютерів під'єднано до одного комутатора, але відокремлено від локальних мереж інших відділів [5].

Глобальна мережа (WAN). WAN відрізняється від локальних мереж протоколами і компонентами на всіх рівнях моделі OSI, використовуваними для передачі даних. У той час як технології локальних мереж використовуються для

передачі даних з високою швидкістю в межах близької відстані, глобальні мережі налаштовані для зв'язку на великі відстані.

Хмарні мережі (Cloud networks). Більшість корпоративних IT-послуг надаються з центрів обробки даних і хмарних мереж. IT-середовище може являти собою гібридне поєднання локальних серверів і хмарних мереж за межами підприємства. Хмарний стек може складатися з декількох моделей хмарних обчислень - приватної, публічної та гібридної хмари.

Інфраструктурні компоненти та програмні технології забезпечують зв'язок між обладнанням центру обробки даних, додатками та сервісами, що працюють у різних IT-середовищах. Доступ до хмарних ресурсів і служб, що працюють на обладнанні, і управління ними здійснюється через Інтернет, зазвичай приватними і захищеними мережевими каналами (якщо тільки вони не використовуються для публічних додатків).

Неодмінним атрибутом корпоративної мережі є високий ступінь гетерогенності. У корпоративній мережі використовуються різні типи комп'ютерів від мейнфреймів до персональних, кілька типів операційних систем і безліч різних додатків. Неоднорідні частини корпоративної мережі повинні працювати як єдине ціле, надаючи користувачам по можливості прозорий доступ до всіх необхідних ресурсів.

Ієрархія корпоративних мереж. Ієрархічна структура мереж підприємства є складним механізмом, який складається з кількох шарів, які постійно взаємодіють один з одним. Всю систему можна представити у вигляді піраміди, складові якої розташовані знизу вгору таким чином [6].

1. Комп’ютери, в яких зберігається та обробляється інформація, і транспортна підсистема, яка забезпечує швидкий пакетний канал доступ між комп'ютерами.

2. Рівень мережевих операційних систем, розташований над транспортним рівнем системи. Він відповідає за коректну роботу додатків в комп'ютерах і доставляє через транспортну систему дані для спільного використання ресурсів комп’ютера.

3. Особливим шаром корпоративної мережі є системні програми, які керують базами даних, зберігають їх у впорядкованому вигляді і дозволяють виконувати з ними різноманітні операції.

4. Наступним рівнем системи є системні служби, які вони використовують системи управління базами даних для пошуку та надання інформації користувачам зручним способом. Ці системи включають Інтернет, електронні пошти та інші корпоративні засоби.

5. На останньому рівні піраміди є конкретні системи, які виконують спеціальні завдання, необхідні компанії. Для таких завдань можна віднести автоматизацію банківських систем, автоматизацію різних процеси та подібні операції.

1.3. Типи атак, які використовуються для нападу на захищені мережі комерційної організації

1. **Вторгнення в мережу (Server access).** Вторгнення - це будь-яка несанкціонована діяльність у вашій мережі, крадіжка цінних ресурсів, унаслідок якої безпека вашої організації наражається на ризик. Існує низка поширених методів кібератак, які складають мережеві вторгнення, включно з багатомаршрутною маршрутизацією, прихованими сценаріями, видачею себе за протокол і переповненням трафіку. Мережеві вторгнення часто проявляються як незвичайна поведінка, але не обов'язково аномальна, що ускладнює їхнє виявлення і, таким чином, вислизає від ручного спостереження. У деяких випадках зловмисники використовували відомі вразливості, такі як CVE-2020-7961, які дозволяли віддалене виконання коду на сервері. Ця вразливість входить до 10 найкращих вразливостей 2021 року [7].

2. **Програма-вимагач (Ransomware).** Можливо, це найзлісніша із загроз безпеці, що створюються кіберзлочинцями, ransomware спрямоване на захоплення бізнес-систем з метою вимагання грошей у жертв. Це одна з найпоширеніших моделей кібератак, що використовуються сьогодні, багато в чому тому, що цей тип

атак успішний і часто призводить до виплат у десятки мільйонів. За минулі роки ми бачили кілька прикладів того, чому ransomware є одним із найефективніших і найнебезпечніших видів кібератак. Вірус Nyetya, він же Petya, зачепив багато компаній. Cisco виявила, як він отримав доступ до даних і що вкрав із комп'ютерів. Компанія встановила: вірус тільки маскувався під вимагача грошей, насправді він був руйнівником. 90 відсотків вимагачів використовують вразливість DNS.

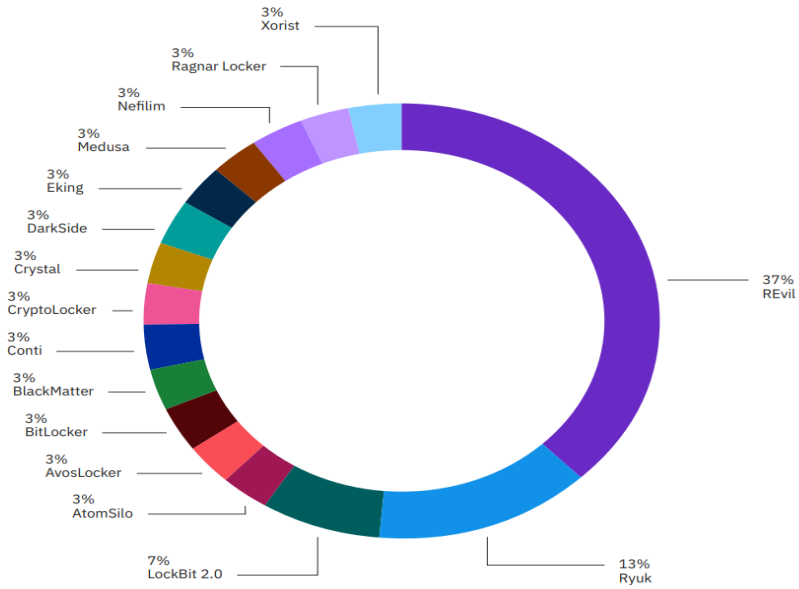


Рис. 1.3. Типи програм-вимагачів, що спостерігалися у 2021 році

3. **Інсайдерські загрози (Insider threats).** Інсайдерські загрози безпеці виникають, коли хтось із близьких співробітників організації з авторизованим доступом зловживає цим доступом для компрометації даних або критично важливих систем вашої компанії. Інсайдери не обов'язково мають бути співробітниками; вони також можуть видавати себе за партнерів, сторонніх постачальників і підрядників. Це найскладніший аспект виявлення внутрішньої загрози безпеці все починається з людей, а не з систем.

4. **Компрометація ділової електронної пошти (Business email compromise).** Компрометація ділової електронної пошти (BEC) - це вид шахрайства, спрямований на компанії, що здійснюють електронні перекази і мають постачальників за кордоном. Корпоративні або загальнодоступні облікові записи електронної пошти керівників або високопоставлених співробітників, пов'язаних із

фінансами або тих, що беруть участь у платежах з електронних переказів, або підміняють, або зламують за допомогою кейлогерів чи фішингових атак для здійснення шахрайських переказів, що призводить до втрат у сотні тисяч доларів. BEC була третьою за поширеністю атакою яку усуває Umbrella Cloud Delivered Firewall. Минулого року компанія Cisco, почала широке впровадження багатофакторної аутентифікації (MFA), що знижує кількість успішних атак, які можуть здійснити загрози BEC. Це впровадження у 2021 році показало найкращі результати, оскільки BEC-зловмисники не могли домогтися великого успіху, тому їм прийшлося змістити фокус своїх операцій на інші підприймства в іншому географічному полі. Завдяки даному рішенню відсоткова частка кількості атак у 2020 році становила 40%, а вже в 2021 році цей показник впав до 20% [8].

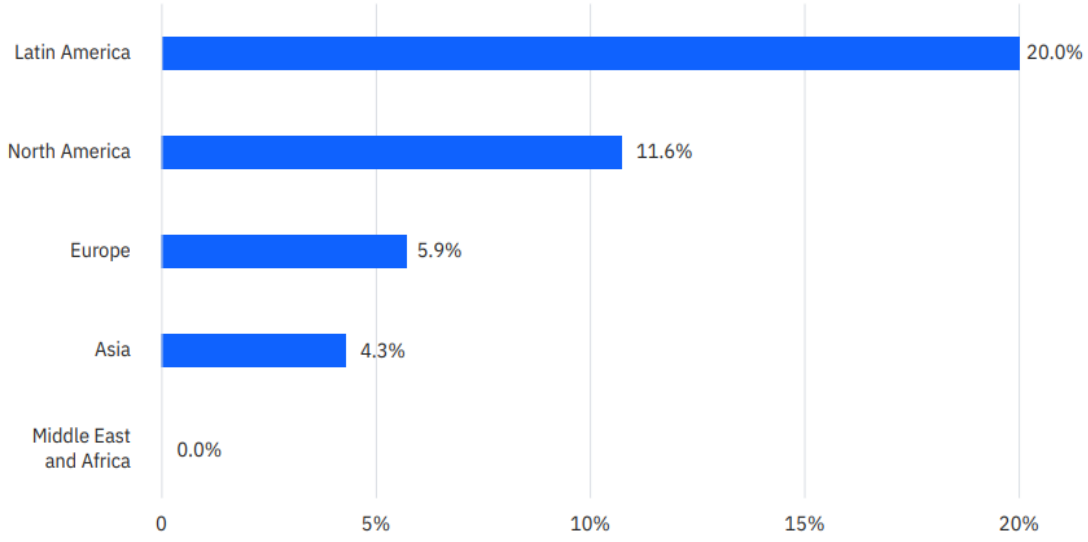


Рис. 1.4. Відсоток інцидентів, які були пов'язані з BEC у кожному регіоні на 2021 рік

5. **DDoS-атаки.** Розподілена атака типу «відмова в обслуговуванні» (DDoS) відбувається, коли зловмисники намагаються порушити нормальний трафік у мережі або на сервері чи системі. Зазвичай це робиться шляхом перевантаження інфраструктури об'єкта атаки потоком інтернет-трафіку.

6. **Ексфільтрація даних (Data exfiltration).** Ексфільтрація даних - це несанкціоноване переміщення даних за межі вашої організації. Ця поширена

кібератака часто здійснюється вручну - наприклад, інформацію викрадають за допомогою принтера або флешки кимось, хто має доступ до систем компанії, або за допомогою зовнішніх зловмисників, які отримали доступ. Вона також може бути здійснена через вихідну електронну пошту, передана третій стороні у вигляді вкладення файлу або за допомогою передавання файлу на незахищений локальний пристрій, такий як смартфон, ноутбук, камера або зовнішній накопичувач.

7. **Шкідливе ПЗ (Malware).** Шкідливе програмне забезпечення - це код, розроблений зловмисниками і призначений для отримання несанкціонованого доступу до мережі або нанесення серйозної шкоди даним або системам. Шкідливе ПЗ зазвичай доставляється у вигляді посилання або файлу електронною поштою і вимагає від користувача натиснути на посилання або відкрити файл, щоб запустити шкідливе ПЗ. Це один із найстаріших типів загроз кібербезпеки (вперше з'явився в 1970-х роках), але залишається одним із найефективніших, оскільки використовує людську природу.

8. **Скомпрометовані облікові дані.** Компрометація облікових даних, також відома як «вкидання облікових даних», є, мабуть, найпоширенішою новою кіберзагрозою 2020 року, відповідальною за порушення в TurboTax, Disney+ і Ring. Уявіть, що ви є потоковою службою підписки, користувачі якої використовують одні й ті самі облікові дані для доступу до аналогічних служб або суміжних точок доступу, таких як Amazon або банківський рахунок. Злочинець може використовувати скомпрометовані облікові дані для злому цих систем і отримання подальшого доступу.

9. **Порушення політики (Violation of the policy).** Політики та керівництва з кібербезпеки визначають правила для таких елементів, як доступ до мережі, доступ до даних, використання паролів, шифрування, і диктують ієрархію дозволів на доступ - які надають користувачам доступ тільки до того, що необхідне для виконання їхньої роботи, - визначаючи ці правила для окремих осіб, а також груп осіб у межах компанії.

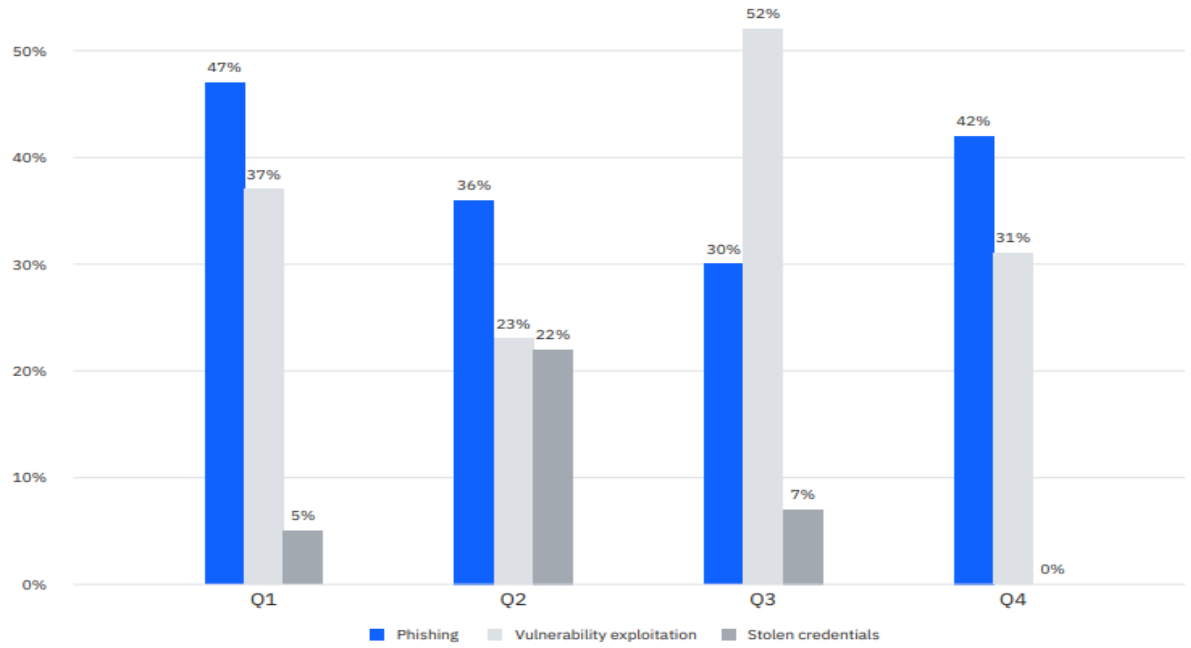


Рис. 1.5. Відсоток атак, пов'язаних з фішингом та використанням вразливостей викраденя облікових даних

10. **Боти/Ботнети (Bots).** Ботнет, скорочення від roBOT NETwork, - це група ботів, які є будь-яким типом комп'ютерної системи, під'єднаної до мережі, безпека якої була порушена. Як правило, ними керують віддалено.

Ботнет Mirai зміг отримати контроль над пристроями, під'єднаними до Інтернету речей (IoT), такими як відеореєстратор, домашній принтер, а також інтелектуальні прилади, ввівши ім'я користувача і пароль за замовчуванням, з якими поставляються пристрої. Загрозливі особи розгорнули DDoS-атаку (розподілену відмову в обслуговуванні), відправивши велику кількість даних на хостинг-компанію, що призвело до відключення багатьох популярних веб-сайтів.

11. **Атаки соціальної інженерії (Social Engineering Attacks).** Атаки соціальної інженерії стали популярним методом, використовуваним суб'єктами загроз для легкого обходу протоколів безпеки автентифікації та авторизації й отримання доступу до мережі.

За останні 5 років кількість таких атак значно зросла, перетворившись на прибутковий бізнес для хакерів. Внутрішні користувачі становлять найбільший ризик для безпеки організації, як правило, тому що вони неосвічені або не знають

про загрозу. Випадкове завантаження вкладення або перехід за посиланням на веб-сайт зі шкідливим кодом може коштувати тисячі збитків.

Наприклад, численні інциденти зі здирницьким ПЗ REvil, що спостерігалися у 2021 році, починалися з фішингового листа QakBot (електронного листа). Ці листи зазвичай містять дуже короткі повідомлення, часто посилаються на неоплачені рахунки, а іноді навіть перехоплюють поточні розмови електронною поштою і відповідають на всі листи тільки зі шкідливим вкладенням. Під час відкриття документа одержувач отримує інструкції з увімкнення макросів, які запускають банківський троян QakBot банківського трояна, який закріпиться в системі [9].

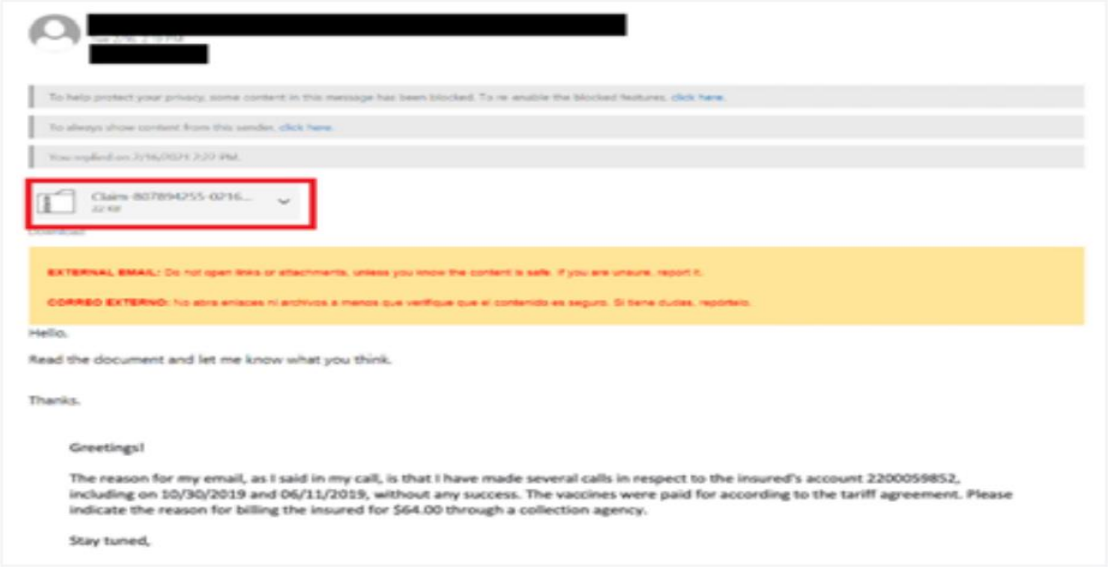


Рис. 1.6. Зразок фішингового листа QakBot

12. **Неправильно налаштовані брандмауери / операційні системи.** Однією з найбільш серйозних загроз для організації є вихід з ладу внутрішньої мережі або серверів для виходу в Інтернет. Коли дані відкриті і не шифруються, суб'єкти загроз легко можуть шпигувати за вашим трафіком, красти дані або компрометувати вашу мережу.

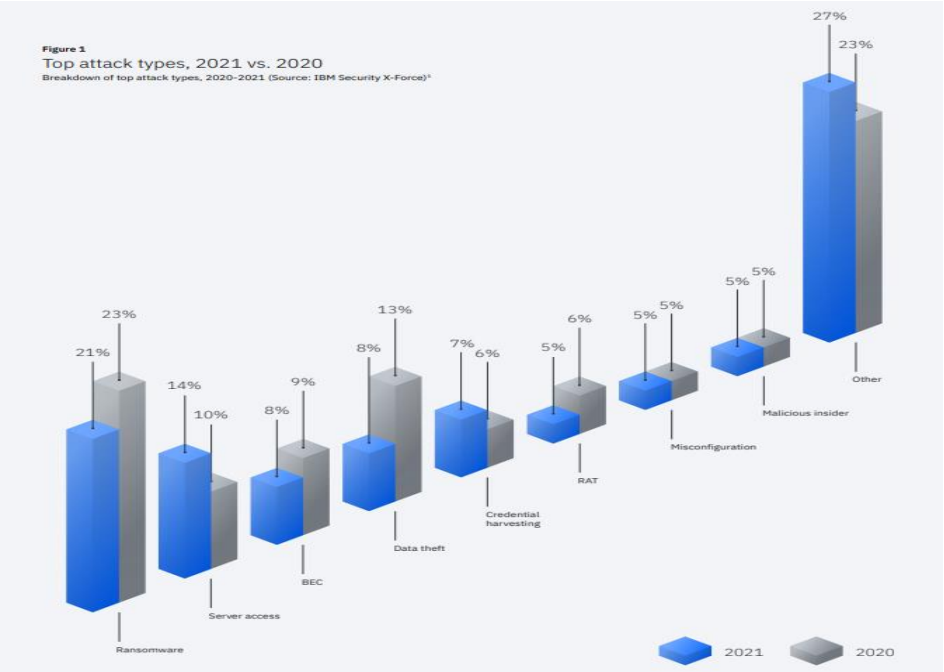


Рис. 1.7. Найпопулярніші типи атак на комерційні мережі порівняння 2021 року з 2020 роком

1.4. Класифікація атак на мережу та засоби їх протидії

Мережева атака - це навмисні дії третіх осіб, спрямовані на отримання контролю над локальним або віддаленим комп'ютером чи обчислювальною системою. В результаті зловмисники можуть порушити роботу мережі, змінити права доступу до облікових записів, отримати персональні дані користувачів та досягти інших цілей.

Види мережевих атак та їх наслідки мають суттєві відмінності один від одного. Сучасна класифікація загроз базується на наступних параметрах:

- характер впливу на мережу;
- мета впливу;
- наявність зворотного зв'язку з мережею, що атакується;
- умова початку атаки;
- місце розташування суб'єкта по відношенню до об'єкта атаки;
- рівень еталонної моделі ISO.

Основні види мережевих атак відповідно до зазначених категорій:

За характером впливу на мережу. Види мережевих атак за характером впливу на мережу, що атакується, можна поділити на активні та пасивні. Активна атака здійснюється з безпосереднім впливом на мережу, що може полягати в обмеженні її працездатності, модифікації налаштувань. Такий вплив обов'язково залишає сліди, тому при його плануванні спочатку передбачається їх виявлення. Пасивна атака здійснюється без прямого впливу на роботу мережі. Однак вона призводить до порушення безпеки мережі. Пасивну атаку набагато складніше виявити саме через відсутність прямого впливу. Прикладами таких загроз є стеження або прослуховування.

За метою атаки. Залежно від мети розрізняють види мережевих атак, спрямованих на порушення:

- функціонування
- конфіденційності;
- цілісність мережі, що атакується.

Основною метою є, як правило, несанкціонований доступ до секретної інформації шляхом її спотворення або перехоплення. У першому випадку інформація може бути змінена, у другому - доступ здійснюється без зміни даних.

За наявністю зворотного зв'язку з мережею, що атакується. Атака може здійснюватися зі зворотним зв'язком або без нього (односпрямована атака). У першому випадку зловмисник встановлює обмін даними з об'єктом атаки. В результаті зловмисники отримують актуальні дані про стан мережі. Односпрямована атака не передбачає встановлення зворотного зв'язку. Вона здійснюється тоді, коли цілі зловмисників не вимагають оперативного реагування на зміну стану об'єкта.

За умовою початку нападу. Існують різні умови початку атаки. В тому числі можна виділити види мережевих атак за цим критерієм:

- за запитом з боку об'єкта;
- за виконанням певної дії на стороні об'єкта;
- безумовні атаки.

Перші два види атак починаються після настання відповідної події, в той час як безумовні атаки починаються в будь-який момент.

За місцем розташування суб'єкта по відношенню до об'єкта атаки. За цим критерієм розрізняють мережеві атаки міжсегментного та внутрішньосегментного типів. Перший тип характеризується розташуванням суб'єкта та об'єкта в різних сегментах мережі. Другий тип характеризується їх розташуванням в одному сегменті. Сегмент мережі визначається як хости (комп'ютери), які фізично з'єднані між собою.

За рівнем еталонної моделі ISO/OSI. Атака на мережу може здійснюватися на різних рівнях еталонної моделі ISO/OSI.

До таких рівнів відносяться:

- фізичний;
- мережевий;
- транспортний;
- канальний;
- сеансовий;
- прикладний;
- представник.

Види мережевих атак та методи захисту від них. На сьогоднішній день відомі наступні види мережевих атак:

- поштове бомбардування;
- застосування спеціалізованих додатків;
- переповнення буфера;
- мережева розвідка (збір інформації за допомогою вільно розповсюджуваних програм);
- підміна IP-адреси (хакер видає себе за легітимного користувача);
- DDOS-атака (шляхом перевантаження унеможливлюється обслуговування нормальних користувачів);

- Man-in-the-Middle (проникнення з метою отримання пакетів, що передаються всередині системи);
- XSS-атака (клієнтські комп'ютери атакуються через уразливості в сервері);
- фішинг (обман жертви шляхом розсилання повідомлень з нібито знайомої адреси).

Методи захисту. Для захисту мереж від зовнішніх загроз можуть бути використані наступні основні методи і технології:

- використання портів з високим рівнем захисту, шифрування даних;
- використання ефективних антивірусів і сканерів;
- використання програмного або апаратного міжмережевого екрана;
- встановлення блокувальників руткітів та сніферів.

Різноманітність видів мережевих атак, яким можуть піддаватися корпоративні та приватні мережі, вимагає розробки ефективних заходів щодо їх захисту. Такі заходи повинні розроблятися і застосовуватися заздалегідь. Ефективний захист від загроз може допомогти зберегти конфіденційні дані в цілості і забезпечити безперебійну роботу мережі. Це може багаторазово окупити витрати, понесені на впровадження такого захисту [10].

1.5. Вразливості в комерційних мережах

Максимальне використання сучасних інформаційних і мережевих технологій є одним із пріоритетних завдань для будь-якої компанії. Розробка і впровадження комерційних проектів, використовуючи територіально рознесені філії та представництва по всьому світу, освоєння нових ринків і відкриття нових представництв неможливе без надійної і добре продуманої корпоративної мережі. Відомий аргумент для підвищення уваги до питань безпеки являє собою бурхливу розробку програмно-апаратних методів для захисту звичайного користувача системи від несанкціонованих дій зловмисника та збереження критичних властивостей інформації (конфіденційності, доступності, цілісності).

6-7 травня 2021 року компанія Colonial Pipeline Group стала об’єктом масштабної викрадення даних і атаки програм-вимагачів, яка призвела до зупинки комп’ютерних систем, які керують її конвеєром. Ця атака була здійснена східноєвропейською кіберзлочинною організацією під назвою DarkSide, яка погрожувала поділитися даними, а також тримати системи закритими, доки не буде сплачено викуп у розмірі 5 мільйонів доларів [11].

Хоча мережа не працювала лише на кілька годин, наслідки були надзвичайно важкими. Компанії довелося закрити всю конвеєрну систему, щоб запобігти поширенню програми-вимагача та не дати хакерам отримати додаткову інформацію. Коли мережа була відновлена, вона не працювала на належній швидкості, і протягом кількох днів трубопровід не працював повністю. Colonial Pipeline є одним із найбільших постачальників бензину в Техасі та на південному сході країни, аж до Нью-Йорка. Майже 45 відсотків палива, що використовується вздовж східного узбережжя та через південний схід, доставляється через систему Colonial Pipeline, тому закриття цієї системи призвело до значного дефіциту палива в усьому регіоні, що особливо сильно вдарило по Алабамі, Південній Каролініі, Джорджії та Північній Каролініі.

Уразливості мережі Colonial Pipeline зробили їх сприйнятливими до кібератак, але під загрозою знаходяться не лише великі компанії та корпорації. Насправді малі підприємства піддаються більшому ризику атаки, оскільки хакери припускають, що малі підприємства не мають заходів безпеки, щоб зупинити атаки. Наслідки цих нападів також можуть бути руйнівними. У 2018 році 41 відсоток малих підприємств заявили, що зазнали витоку даних, що призвело до фінансових збитків, які перевищили 50 тисяч доларів США, тоді як 60 відсотків малих підприємств закрилися протягом шести місяців після кібератаки через втрату даних, доходу та довіри клієнтів [12].

За останні п'ять років кількість вразливостей, виявлених в комерційних мережах, постійно і неухильно зростала. Ще більш тривожним є те, що кількість експлойтів і інструментів, які суб'єкти загроз можуть використати також постійно зростає, створюючи дедалі ширший спектр можливостей для використання

вразливостей. Варіантів для суб'єктів загроз, які прагнуть використовувати вразливості дуже багато. Компанія IBM Security спостерігала, як суб'єкти використовували безліч відомих вразливостей, таких як CVE-2021-35464 (уразливість де серіалізації Java) і CVE-2019-19781 (дефект обходу шляхів Citrix), для отримання початкового доступу до комерційних мереж, які їх цікавлять. Крім того, аналітики компанії навели дані, в яких продемонстрували, як хакери використовували вразливості нульового дня в таких великих компаніях як Microsoft, Google, Facebook, щоб отримати доступ до мереж і пристроїв жертв, які працювали на той час в підрозділах компанії. Уразливості, пов'язані з фішингом та експлуатацією вразливостей мережі зростають ще швидшими темпами, ніж загальна кількість вразливостей, причому ці дві категорії збільшили свій вплив на 50 відсотків порівняно з попередніми роками [13].

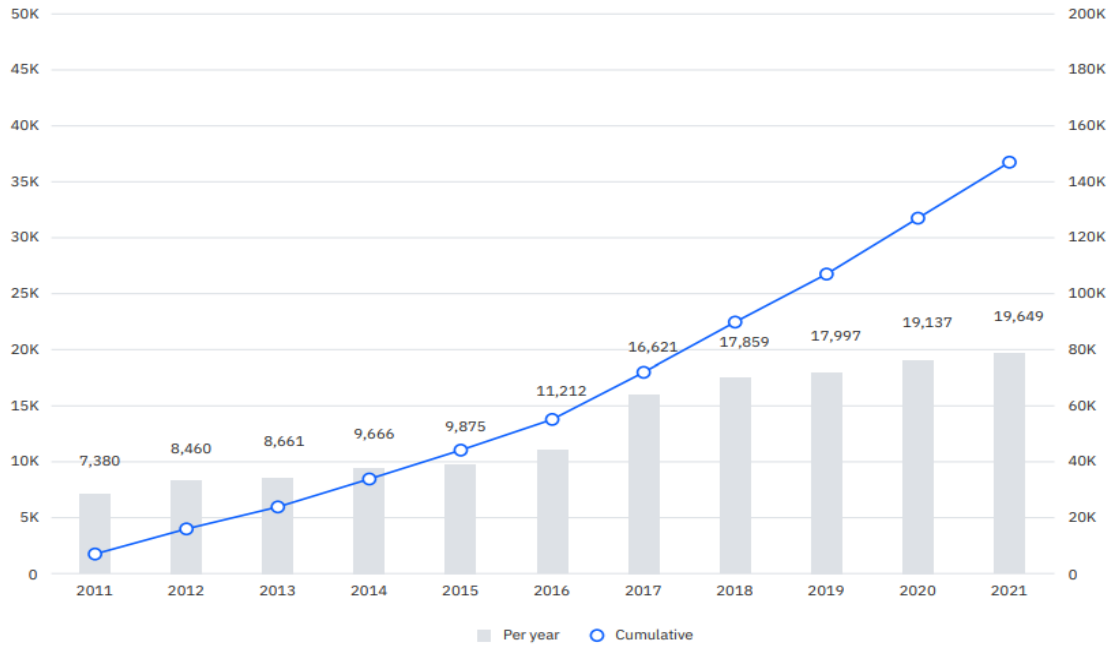


Рис. 1.8. Виявлені вразливості за роками з 2011 по 2021 рік

На додаток до вивчення кінцевої мети суб'єктів загроз компанія IBM security надала аналітично-статистичні дані в яких продемонструвала, як загрозливі суб'єкти отримують початковий доступ до мереж комерційних організацій. Найпоширенішими методами і вразливостями, які вони дослідили, є фішинг та експлуатація вразливостей. Третє місце займає використання вкрадених облікових

даних, потім груба сила, віддалені протоколи віддаленого робочого столу (RDP), підбір паролів становлять невеликий відсоток вторгнень.

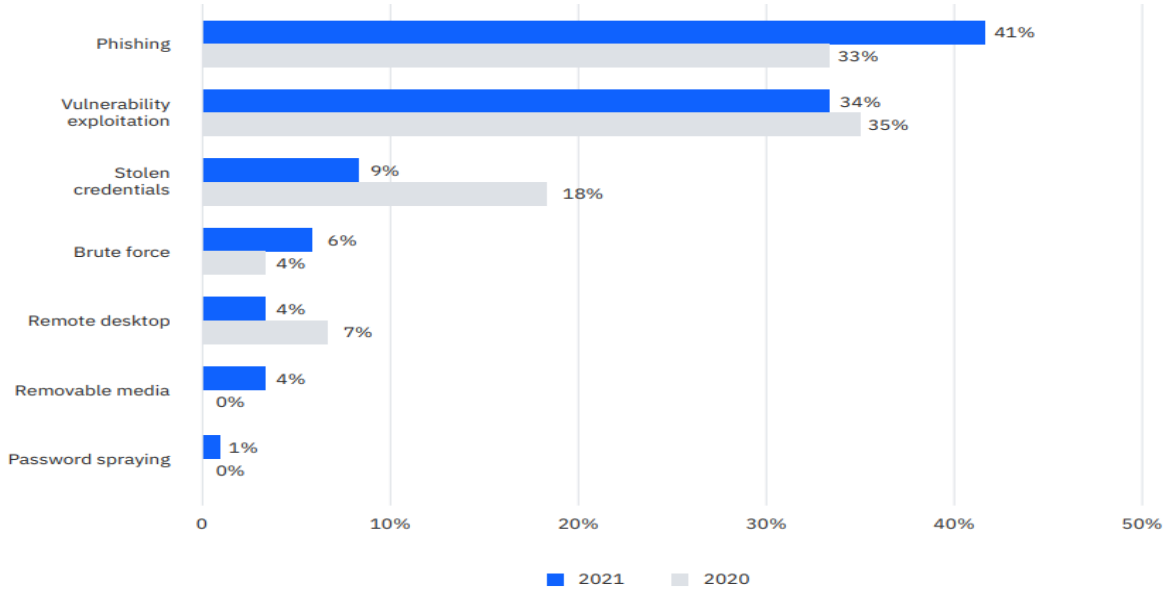


Рис. 1.9. Найпопулярніші вразливості в комерційних мережах (порівняння 2020 та 2021 років)

В інформаційній безпеці вразливість мережі – це слабке місце, яке може використовуватися загрозливим суб'єктом, наприклад зловмисником, для отримання несанкціонованого доступу до інформації або ресурсів. Щоб зрозуміти вразливі місця мережі, важливо спочатку зрозуміти, що таке мережі та як вони працюють. Мережі в широкому сенсі можна визначити як системи взаємопов'язаних комп'ютерів і пристроїв, які можуть обмінюватися даними та ресурсами. Найпоширенішим типом мережі є Інтернет, який є глобальною мережею комп'ютерів і пристроїв, яка дозволяє обмінюватися інформацією між користувачами.

Існує кілька типів найпоширеніших уразливостей мережі:

- Незахищені протоколи : протоколи – це правила, які регулюють спосіб обміну даними між комп'ютерами в мережі. Деякі протоколи безпечніші за інші, а незахищені протоколи можуть зробити мережі вразливими для атак.

- Погано налаштовані брандмауери: брандмауери використовуються для захисту мереж від несанкціонованого доступу. Якщо вони неправильно налаштовані, вони можуть зробити мережі вразливими для атак.
- Слабкі паролі: паролі використовуються для автентифікації користувачів і обмеження доступу до конфіденційної інформації. Якщо паролі слабкі або їх легко вгадати, вони можуть надати зловмисникам легкий доступ до мереж і даних.

Вразливості мережі, які впливають на організацію:

— **Застарілі або невиправлені програмні додатки.** Хоча більшість операційних систем і поширених програм, як-от Salesforce, Microsoft Office 365 і Google G Suite, загалом безпечні, величезний обсяг коду для їх запуску робить уразливості безпеки неминучими. У штаті цих компаній є розробники, які постійно шукають слабкі місця в своїх програмах і ОС і створюють патчі, щоб їх виправити. Після виявлення абсолютно необхідно встановити ці патчі, коли вони стануть доступними. Без цих патчів хакер може легко надіслати командний рядок, який викрадає дані або вимикає вашу систему. Крім того, запуск операційної системи або програмного забезпечення, яке більше не підтримується розробниками програмного забезпечення, означає, що виправлення чи оновлення для усунення вразливостей не надсилатимуться. Щоб зменшити ризики, важливо завжди переходити до поточних версій і виконувати сканування вразливостей (або доручати їх виконувати керованій службі безпеки мережі).

— **Слабкі паролі.** Якщо використовується слабкий пароль або пароль за замовчуванням у веб-програмі чи внутрішній програмі, велика ймовірність витоку даних. Прості паролі, як-от параметр за умовчанням, «пароль» або назва компанії, легко зламати зловмисним програмним забезпеченням або викрасти хакерам.

— **Однофакторна автентифікація.** Однофакторна автентифікація передбачає використання лише одного пароля для входу в програмне забезпечення, програму або файл. Навіть якщо виправити проблему зі слабким паролем вище, мати лише одну лінію захисту все одно легко зламати. Натомість ми рекомендуємо перейти до стратегії багатофакторної автентифікації, щоб покращити вашу

безпеку. Введення надійного пароля з подальшим використанням додаткового методу, наприклад коду текстового повідомлення, таємного запитання чи навіть сканування відбитків пальців, може майже унеможливити доступ для неавторизованого користувача.

— **Погана конфігурація брандмауера.** Брандмауер відстежує вхідний і вихідний мережевий трафік і дозволяє встановлювати правила доступу, які запобігають проникненню неавторизованих джерел у мережу або доступу людей. Це важлива частина безпеки, але її потрібно використовувати правильно, щоб блокувати загрози. Важливо перевірити базу правил – набір правил, які визначають, кому і що дозволено через брандмауер, а кому – ні, щоб переконатися, що вона не містить помилок конфігурації, таких як проблеми з класифікацією, друкарські помилки або надання більшого доступу, ніж необхідно.

— **Уразливості мобільних пристроїв.** Навіть якщо ваші офісні пристрої добре захищені брандмауерам і надійними паролями , мобільні пристрої, такі як телефони, планшети та ноутбуки, можуть зробити вас відкритими для кібератак. Використання Bluetooth або незахищеного з’єднання Wi-Fi відкриває двері для доступу до кешованих паролів у веб-браузері, інформації в електронних листах та іншої секретної інформації. Щоб захистити свої дані на мобільних пристроях, уникайте використання загальнодоступної мережі Wi-Fi, уникайте завантаження неперевірених програм і виходьте з облікових записів, коли ними не користуєтеся.

— **Відсутність резервного копіювання даних.** Хоча важливо зробити все можливе, щоб зупинити атаку, перш ніж вона станеться, для вашого бізнесу також важливо мати резервне копіювання та аварійне відновлення. Наприклад, навіть якщо у вас є надійні паролі з двофакторною автентифікацією, мобільні протоколи безпеки та оновлені програми, якщо хтось випадково завантажить файл із прикріпленим програмним забезпеченням-вимагачем і вимкне всю вашу систему, ваш бізнес пропаде. Регулярне резервне копіювання за межами сайту забезпечує безпеку ваших даних і їх легко відновити, запобігаючи простоям і катастрофам [14].

— **Незахищена електронна пошта.** Електронні листи зі спамом є поширеною вразливістю для бізнесу та неймовірно ефективним способом для хакерів доставити зловмисне програмне забезпечення, оскільки вони здатні імітувати та копіювати надійні джерела. Щойно співробітник відкриває електронний лист, він відкриває вашу мережу для атаки. Замість того, щоб ризикувати своєю організацією кожним електронним листом, установіть ефективний захист від електронної пошти та спаму, щоб ви та ваша команда відкривали повідомлення лише з надійних джерел.

Висновки до першого розділу

Досліджено та проаналізовано вплив атак на комерційні організації, а також висвітлено класифікацію цих атак на мережу та засоби протидії.

Виокремлено два питання, щодо типів атак, які використовуються для нападу на захищені мережі комерційної організації та вразливості, які використовують для злому.

Поставлено задачі на подальше дослідження і розробку рекомендації щодо застосування технології побудови захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewall.

Наведено аналітично-статистичні дані по типам атак, які мають найбільший вплив на комерційні мережі, в результаті чого було виявлено, що найбільших втрат компанії завдає неправильно налаштований брандмауер. Тому, реалізація технології Umbrella Cloud-Delivered Firewal (CDFW) є відмінним засобом у протидії даним загрозам для побудови захищеної мережі комерційної організації.

2 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ТА ЗАСОБІВ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ КОМЕРЦІЙНОЇ ОРГАНІЗАЦІЇ ІЗ ВИКОРИСТАННЯМ UMBRELLA CLOUD-DELIVERED FIREWAL (CDFW)

2.1. Дослідження технологій та засобів побудови захищеної мережі із використанням хмарного фаєрвола

Забезпечення надійного захисту корпоративної мережі – дуже складний процес, який являє собою безперервну і постійну послідовність дій по реалізації комплексу заходів спрямованих на безпеку.

В якості одного з базових засобів захисту корпоративних мереж сьогодні виступають системи виявлення атак, такі як хмарні брандмауери, що дають змогу своєчасно виявляти та блокувати атаки порушників.

Хмарний брандмауер — це продукт безпеки, який, як і традиційний брандмауер , фільтрує потенційно шкідливий мережевий трафік. На відміну від традиційних брандмауерів, хмарні брандмауери розміщені в хмарі.

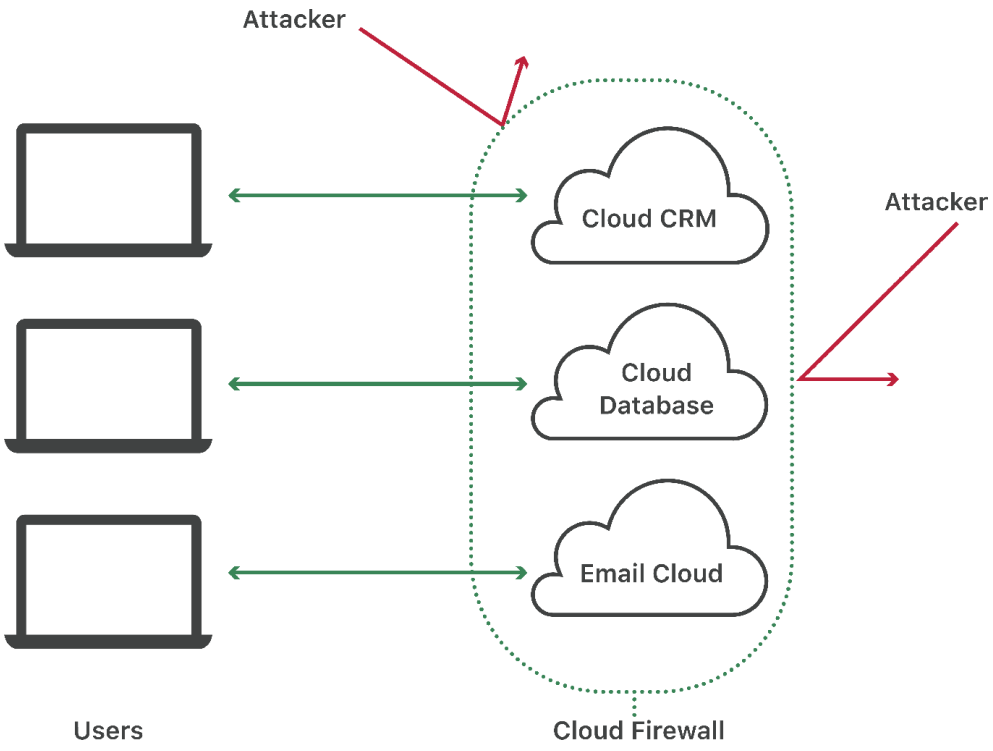


Рис. 2.1. Принцип роботи хмарного фаєрвола

Ця хмарна модель брандмауерів також називається брандмауер як послуга (FWaaS). Хмарні брандмауери створюють віртуальний бар'єр навколо хмарних платформ, інфраструктури та додатків так само, як традиційні брандмауери утворюють бар'єр навколо внутрішньої мережі організації. Хмарні брандмауери також можуть захистити локальну інфраструктуру.

Типи хмарного брандмауера. Існує два типи хмарних брандмауерів – відмінність визначається тим, для захисту чого користувачам потрібна допомога. Обидва типи існують як хмарне програмне забезпечення, яке відстежує всі вхідні та вихідні пакети даних і фільтрує цю інформацію відповідно до політик доступу з метою блокування та реєстрації підозрілого трафіку.

Брандмауери SaaS призначені для захисту мережі організації та її користувачів – на відміну від традиційного локального апаратного чи програмного брандмауера. Єдина відмінність полягає в тому, що його розгортають за межами хмари. Цей тип брандмауера можна назвати:

- Брандмауер програмного забезпечення як послуги (брандмауер SaaS)
- Безпека як послуга (SECaaS)
- Брандмауер як послуга (FWaaS)

Брандмауери нового покоління – це хмарні служби, призначені для розгортання у віртуальному центрі обробки даних. Вони захищають власні сервери організації в моделі платформи як послуги (PaaS) або інфраструктури як послуги (IaaS). Програма брандмауера існує на віртуальному сервері та захищає вхідний і вихідний трафік між хмарними програмами.

Переваги хмарних фаєрволів:

- Масштабованість: оскільки розгортання набагато простіше, організації можуть регулювати розмір свого рішення безпеки без проблем, пов'язаних із встановленням, обслуговуванням і оновленням на місці. У міру збільшення пропускної здатності хмарні брандмауери можуть автоматично налаштовуватися для підтримки паритету. Наприклад, розподілені атаки типу «відмова в обслуговуванні» (DDoS) можна пом'якшити, не турбуючись про обмеження пропускної здатності.

- Доступність: постачальники хмарних брандмауерів враховують вбудовану вартість високої доступності за рахунок підтримки інфраструктури. Це означає гарантування резервного живлення, опалення, вентиляції та кондиціонування повітря та мережевих служб, а також автоматизацію стратегій резервного копіювання на випадок збою сайту. Цю доступність важко порівняти з локальними рішеннями брандмауера через вартість і необхідну підтримку. Це також означає, що необхідні оновлення можна впровадити негайно, без необхідності великих системних завантажень або оновлень.
- Розширюваність: хмарні брандмауери можуть бути доступні та встановлені будь-де, де організація може забезпечити захищений шлях мережевого зв'язку. З локальним пристроєм ця можливість розширення обмежена доступними ресурсами організації, яка шукає рішення для брандмауера.
- Безпека міграції: хмарний брандмауер здатний фільтрувати трафік із різноманітних джерел; Інтернет, між віртуальними мережами, між орендарями або навіть віртуальним центром обробки даних. Він здатний гарантувати безпеку з'єднань між фізичними центрами обробки даних і хмарою – це дуже корисно для організацій, які шукають засоби перенесення поточних рішень із локального розташування до хмарної інфраструктури.
- Паритет безпечного доступу: хмарні брандмауери забезпечують такий самий рівень безпечного доступу, як і локальні брандмауери. Це означає розширену політику доступу, керування з'єднаннями та фільтрацію між клієнтами та хмарою. Це також поширюється на зашифрований вміст.
- Захист особистих даних: хмарні брандмауери можуть інтегруватися з постачальниками контролю доступу та надавати користувачам детальний контроль над інструментами фільтрації.
- Управління продуктивністю. Хмарні брандмауери надають інструменти для керування продуктивністю, видимістю, використанням, конфігурацією та журналюванням – усім тим, що зазвичай пов'язано з локальним рішенням.

Процес виявлення атак починається зі збору даних, необхідних для визначення факту атаки на ресурс мережі. Зокрема, можна аналізувати відомості про пакети даних, що надходять із зовнішньої мережі в корпоративну мережу компанії, продуктивність програмно-апаратних засобів (обчислювальне навантаження на вузли мережі, завантаженість оперативної пам'яті, швидкість роботи прикладного програмного забезпечення), відомості про доступ до певних файлів тощо. Корисно також мати повну інформацію про реєстрацію користувачів під час входу в корпоративну мережу [15].

Недоліки хмарних фаєрволів. Одним із потенційних недоліків будь-якої хмарної служби (особливо щодо хмарних брандмауерів) є те, що користувачі повинні покладатися на доступність свого постачальника FaaS. Будь-який рівень простою для постачальника послуг хмарного брандмауера може призвести до порушення безпеки в кількох організаціях без негайної безпеки. Через це багато постачальників послуг мають групи безпеки, відповідальні за реагування на серйозні проблеми.

Використання хмарного фаєрвола. Банки мають багато засобів фізичної безпеки. Більшість звичайних банків мають такі функції безпеки, як камери спостереження та куленепробивне скло. Охоронці та банківські працівники також допомагають зупиняти потенційних злодіїв, а готівка зберігається у надійних сейфах. Але уявіть, якби готівка кожного відділення банку не зберігалася в одному місці, а зберігалася в різних сейфах по всій країні, якими керує компанія, що спеціалізується на обслуговуванні сейфів. Це схоже на те, що роблять хмарні брандмауери. Хмара схожа на банк із розпорошеними ресурсами, але замість грошей хмара зберігає дані та обчислювальну потужність. Авторизовані користувачі можуть підключатися до хмари з будь-якого місця та майже в будь-якій мережі. Програми, які працюють у хмарі, можуть працювати будь-де, і це також стосується хмарних платформ та інфраструктури.

Хмарні брандмауери блокують кібератаки, спрямовані на ці хмарні активи. Розгортання хмарного брандмауера — це те саме, що замінити локальні камери безпеки банку та фізичну охорону на глобальний цілодобовий центр безпеки, який

має централізований персонал і камери безпеки отримують інформацію з усіх місць, де зберігаються активи банку.

Не потрібно забувати, що головним завданням, розв'язуваної на етапі проектування захищеної мережі є інформаційна безпека, а саме забезпечення безпеки інформації в комп'ютерних мережах, що передбачає створення перешкод для будь-яких несанкціонованих спроб розкрадання або модифікації даних, що передаються в мережі. Водночас дуже важливо зберегти такі властивості інформації, як доступність, цілісність і конфіденційність. Доступність інформації має на увазі забезпечення своєчасного і безперешкодного доступу користувачів до потрібних відомостей. Цілісність інформації полягає в її існуванні в неспотвореному вигляді, тобто незмінному щодо деякого фіксованого її стану. Конфіденційність передбачає необхідність введення обмежень доступу до даної інформації для певного кола користувачів [16].

Тому проблема захисту комерційної мережі під час взаємодії із зовнішніми чиниками успішно може бути вирішено за допомогою спеціалізованих програмно-апаратних комплексів, що забезпечують цілісний захист комп'ютерної мережі від потенційно ворожого зовнішнього середовища. Такі комплекси називають міжмережевими екранами, брандмауерами або системами Firewall.

Брандмауер - це пристрій мережевої безпеки, який контролює вхідний і вихідний мережевий трафік і дозволяє або блокує пакети даних на основі набору правил безпеки. Його мета - встановити бар'єр між внутрішньою мережею і вхідним трафіком із зовнішніх джерел (як-от Інтернет), щоб блокувати шкідливий трафік.

Як правило, цей кордон проводиться між корпоративною (локальною) мережею підприємства і глобальною мережею Internet, хоча її можна провести і всередині корпоративної мережі підприємства. Використання фаєрвола дає змогу організувати внутрішню політику безпеки мережі підприємства, розділивши всю мережу на сегменти, що дає змогу сформулювати основні принципи архітектури безпеки корпоративної мережі:

- Введення N категорій секретності та створення N виділених мережевих сегментів користувачів. При цьому кожен користувач усередині мережевого

сегмента має однаковий рівень секретності (допущений до інформації одного рівня секретності).

- Виділення в окремий сегмент усіх внутрішніх серверів компанії. Цей захід також дає змогу ізолювати потоки інформації між користувачами, які мають різні рівні доступу.
- Виділення в окремий сегмент усіх серверів компанії, до яких буде надано доступ з Інтернету (створення демілітаризованої зони для зовнішніх ресурсів).
- Створення виділеного сегмента адміністративного управління.
- Створення виділеного сегмента управління безпекою.

Для протидії несанкціонованому міжмережевому доступу фаєрвол повинен розташовуватися між захищеною мережею організації, що є внутрішньою, і потенційно ворожою зовнішньою мережею (рис. 2.2).

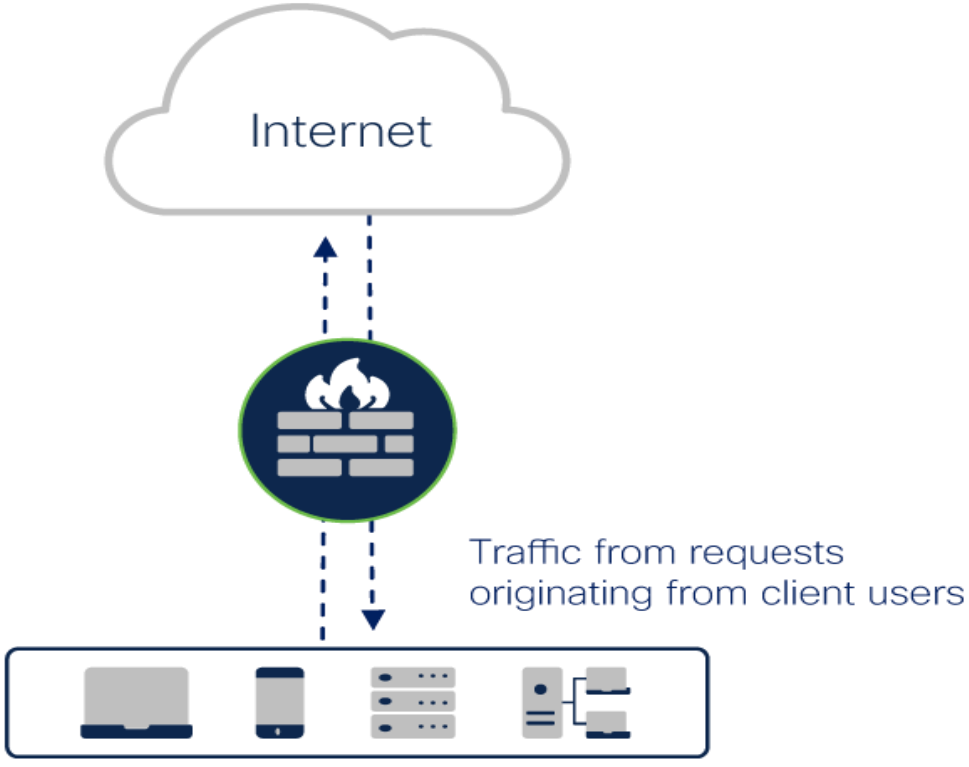


Рис. 2.2. Схема підключення хмарного брандмауера

Міжмережевий екран не є симетричним. Для нього окремо задаються правила, що обмежують доступ із внутрішньої мережі в зовнішню мережу і навпаки.

За необхідності доступу з внутрішньої мережі в зовнішню мережу або навпаки спочатку має бути встановлено логічне з'єднання з програмою-посередником, що функціонує на комп'ютері екрана. Брандмауер перевіряє допустимість запитаної міжмережевої взаємодії та за її дозволу сама встановлює окреме з'єднання з необхідним комп'ютером. Далі обмін інформацією між комп'ютерами внутрішньої і зовнішньої мережі здійснюється через програмного посередника, який може виконувати фільтрацію потоку повідомлень, а також здійснювати інші захисні функції.

До функцій посередництва в загальному випадку належать:

— **Ідентифікація та автентифікація користувачів.** Для високого ступеня безпеки необхідна ідентифікація та аутентифікація користувачів не тільки під час їхнього доступу із зовнішньої мережі у внутрішню мережу, а й навпаки. Пароль не повинен передаватися у відкритому вигляді через загальнодоступні комунікації. Оптимальним способом аутентифікації є використання одноразових паролів. Зручно і надійно також застосування цифрових сертифікатів, що видаються довірчими органами, наприклад, центром розподілу ключів. Більшість програм-посередників розробляються таким чином, щоб користувач аутентифікувався тільки на початку сеансу роботи з фаєрволом. Після цього від нього не вимагається додаткова автентифікація протягом часу, що визначається адміністратором.

— **Перевірка автентичності переданих даних.** Програми-посередники можуть здійснювати перевірку автентичності одержуваних і переданих даних. Це актуально не тільки для автентифікації користувачів, а й для програмних комплексів, які використовують технологію хмарного брандмауера стосовно яких може бути виконано підробку. Перевірка автентичності полягає в перевірці їхніх цифрових підписів.

— **Розмежування доступу до ресурсів внутрішньої мережі.** Ідентифікація та автентифікація користувачів при зверненні до міжмережевого екрана дає змогу розмежувати їхній доступ до ресурсів внутрішньої або зовнішньої мережі. Способи розмежування до ресурсів внутрішньої мережі нічим не відрізняються від способів розмежування, підтримуваних на рівні операційної системи.

Під час розмежування доступу до ресурсів зовнішньої мережі найчастіше використовується один із таких підходів:

- дозвіл доступу тільки за заданими адресами в зовнішній мережі;
- фільтрація запитів на основі оновлюваних списків неприпустимих адрес і блокування пошуку інформаційних ресурсів за небажаними ключовими словами;

Багато хмарних брандмауерів містять потужну систему реєстрації, збору та аналізу статистики. Облік може вестися за адресами клієнта і сервера, ідентифікаторами користувачів, часом сеансів, часом з'єднань, кількістю переданих/прийнятих даних, діями адміністратора і користувачів. Системи обліку дають змогу зробити аналіз статистики та надають адміністраторам докладні звіти. Внаслідок використання спеціальних протоколів посередники можуть виконати віддалене сповіщення про певні події в режимі реального часу [17].

2.2. Порівняльний аналіз використання Umbrella Cloud Delivered Firewall та Barracuda CloudGen Firewall

Хмарний брандмауер Umbrella Cloud Delivered Firewall забезпечує видимість і контроль вихідного інтернет-трафіку за всіма портами і протоколами. Він реєструє всю вихідну активність і блокує будь-який небажаний трафік за допомогою правил IP, портів і протоколів, а також за допомогою контролю та керування додатками.

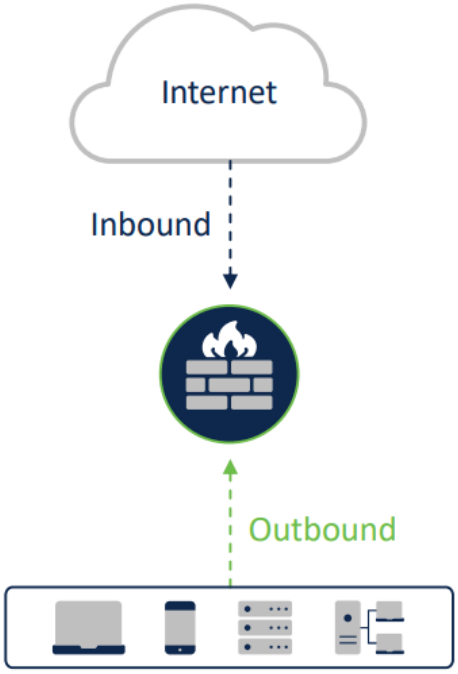


Рис. 2.3. Принцип роботи хмарного брандмауера Umbrella Cloud Delivered Firewall

Адміністратор даного рішення можете направити будь-який трафік у хмару для перевірки брандмауером, встановивши тунель IPSec з будь-якого мережевого пристрою, а також дає змогу інтегрувати Meraki VPN або Cisco SD-WAN. За допомогою функції видимості та контролю Umbrella Cloud Delivered Firewall розпізнає будь-які вебдодатки і зробить відповідні дії для їхнього блокування або дозволу на роботу. Хмарний брандмауер використовує сигнатурне виявлення для ідентифікації та блокування 2800 застосунків, які вже внесені до списку, і регулярно додаються нові.

Ось приклади того, що може блокувати хмарний брандмауер:

- Блокувати тіньові IT через веб порти: Він може блокувати або дозволяти будь-які SaaS додатки від MS Teams, WebEx або Google Hangouts тощо.
- Блокувати небезпечні додатки на нестандартних портах: Зупинити віддалене під'єднання віртуальних терміналів до інших мереж (приклад: Telnet або Зупинити передачу файлів).

- Блокувати несанкціонований трафік через не вебпорти: Це дасть змогу зупинити будь-який несанкціонований трафік, як-от піринговий трафік (наприклад, TOR або BitTorrent).

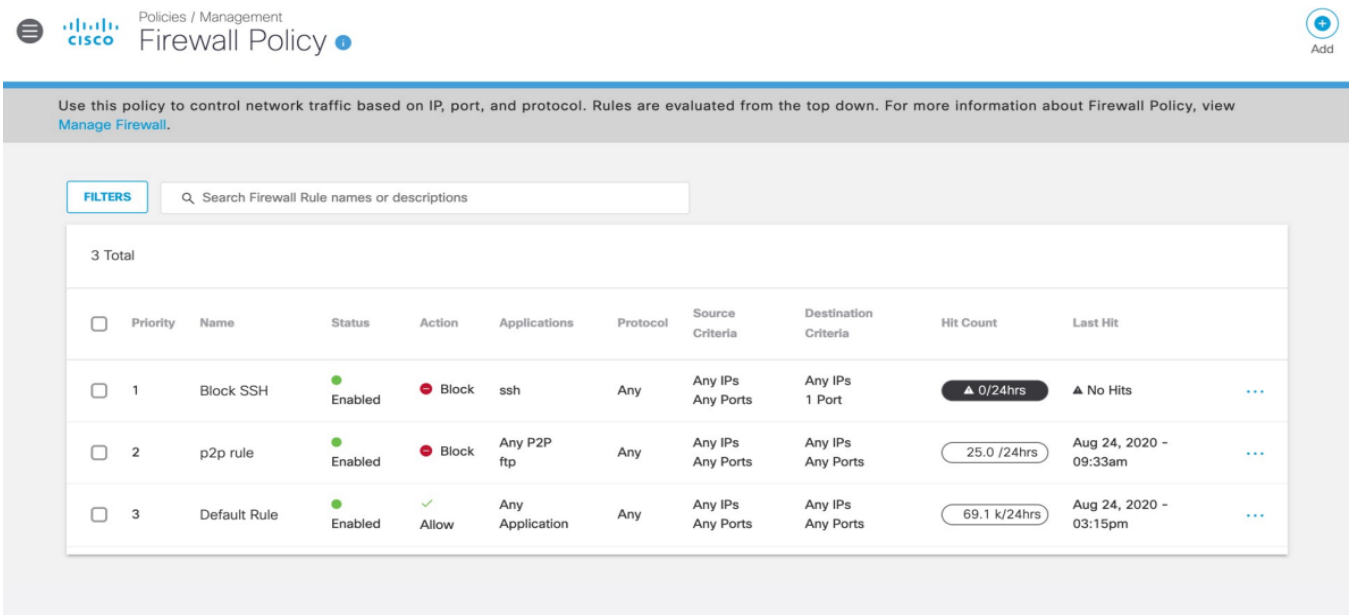


Рис. 2.4. Приклад роботи хмарного брандмауера Umbrella Cloud Delivered Firewall з вхідним трафіком

Переваги:

- Управління даним брандмауером здійснюється через робочу панель Cisco Umbrella, яка є дуже інтуїтивною для будь-якого спеціаліста;
- Хмарний міжмережевий екран Umbrella (CDFW) надає послуги міжмережевого екрана без необхідності розгортання;
- Обслуговування та оновлення баз даних фізичних або віртуальних пристроїв на об'єкті відбувається щосекунди;
- Umbrella CDFW підтримує видимість і контроль інтернет-трафіку у філіях, забезпечуючі безперервний захист мережі;
- Umbrella реєструє всю мережеву активність і блокує небажаний трафік, використовуючи критерії правил IP, портів і протоколів;
- Направити трафік в Umbrella CDFW з будь-якого мережевого пристрою, створивши тунель IPsec (Internet Protocol Security) і IKEv2 (Internet Key Exchange, версія 2), пристрої Cisco ASA, Cisco ISR та Cisco FTD;

- Перевірка і фільтрація на рівні 7 (рівень застосунків) з використанням механізму NBAR2;
- У міру додавання нових тунелів у політику брандмауера, Umbrella автоматично застосовує і послідовно виконує правила, визначені в політиці;
- Автоматизовані журнали звітів, включно з підрахунком влучень у політику;
- Моніторинг кількості ударів в реальному часі, які відображаються для кожної мережі;
- Перегляд журналів брандмауера у звітах;
- Перевірка протоколу вебтрафіку на постійній основі;
- Надійна інфраструктура і постійна підтримка 24/7;

Недоліки:

- Вимагає деякої спеціальної підготовки від спеціаліста;
- Максимально допустима смуга на кожен тунель 250 Мбіт/с;
- Якщо буде потрібно передавати більше трафіку, потрібно буде будувати додаткові тунелі і балансувати між ними навантаження;
- У політиці безпеки можна додавати Applications, але додавати групи користувачів AD не можна;
- 14-денна пробна ліцензія Cisco Umbrella;
- Може не підтримуватися функціонал залежно від ліцензії;
- За замовчуванням кількість правил брандмауера, які ви можете додати в політику брандмауера, становить 1000;
- Пакети повинні виходити від IP-адреси RFC1918 і призначатися для публічної IP-адреси. В іншому разі пакети відкидаються, але можна використовувати функцію Traffic Selector у налаштуванні тунелю;

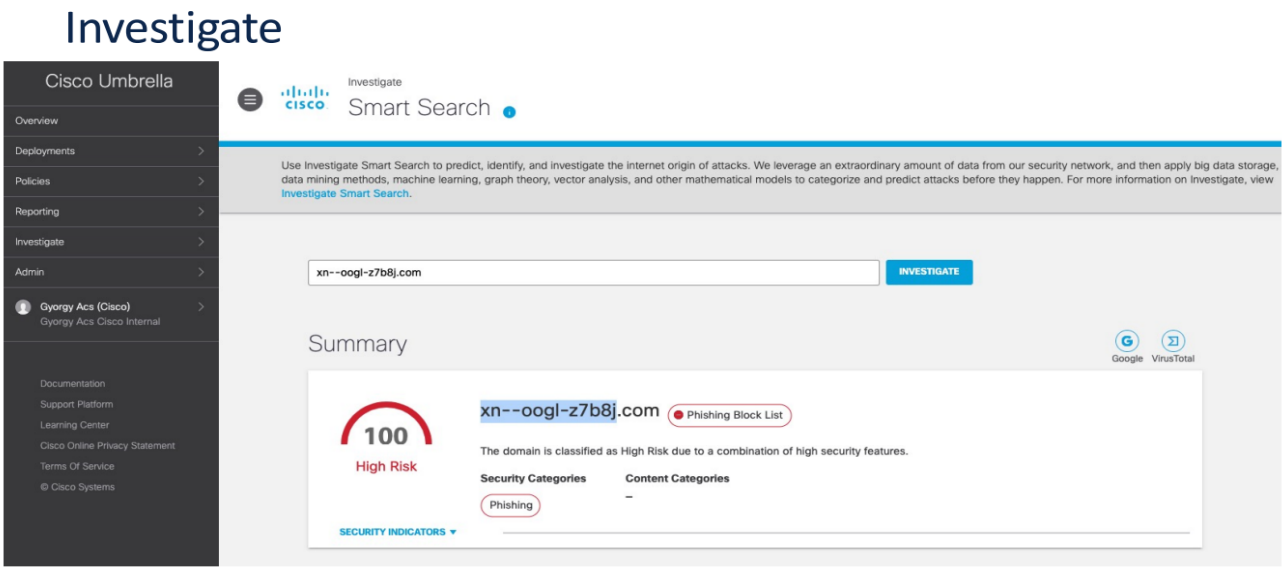


Рис. 2.5. Робоча панель Cisco Umbrella (CDFW)

Barracuda CloudGen Firewall пропонує повний набір технологій міжмережевому екрану нового покоління для забезпечення захисту мережі в режимі реального часу від широкого спектра мережевих загроз, вразливостей та експлойтів, включно з ін'єкціями SQL, міжсайтовим скриптінгом, атаками на відмову в обслуговуванні, троянами, вірусами, черв'яками, шпигунськими програмами та багатьом іншим. Також вона забезпечує кілька рівнів виявлення, включно з передовими сигнатурами загроз, поведінковим та евристичним аналізом.

Основна мета цього брандмауера - застосування політик доступу та безпеки до трафіку, що входить і виходить із ваших мереж. За це відповідають дві різні служби брандмауера, залежно від призначення трафіку:

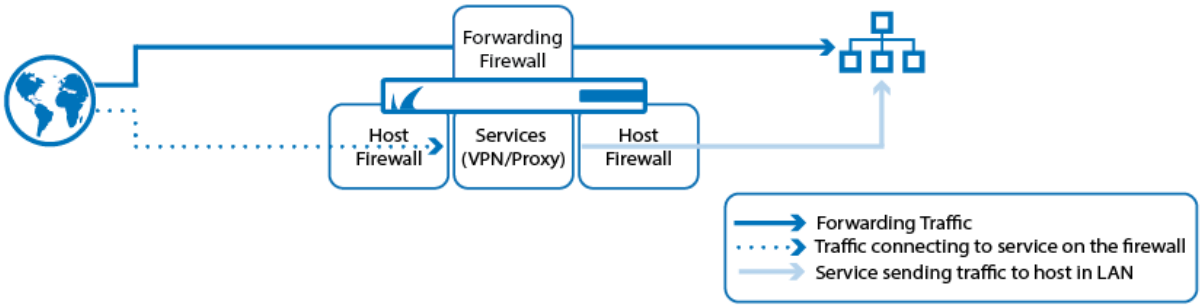
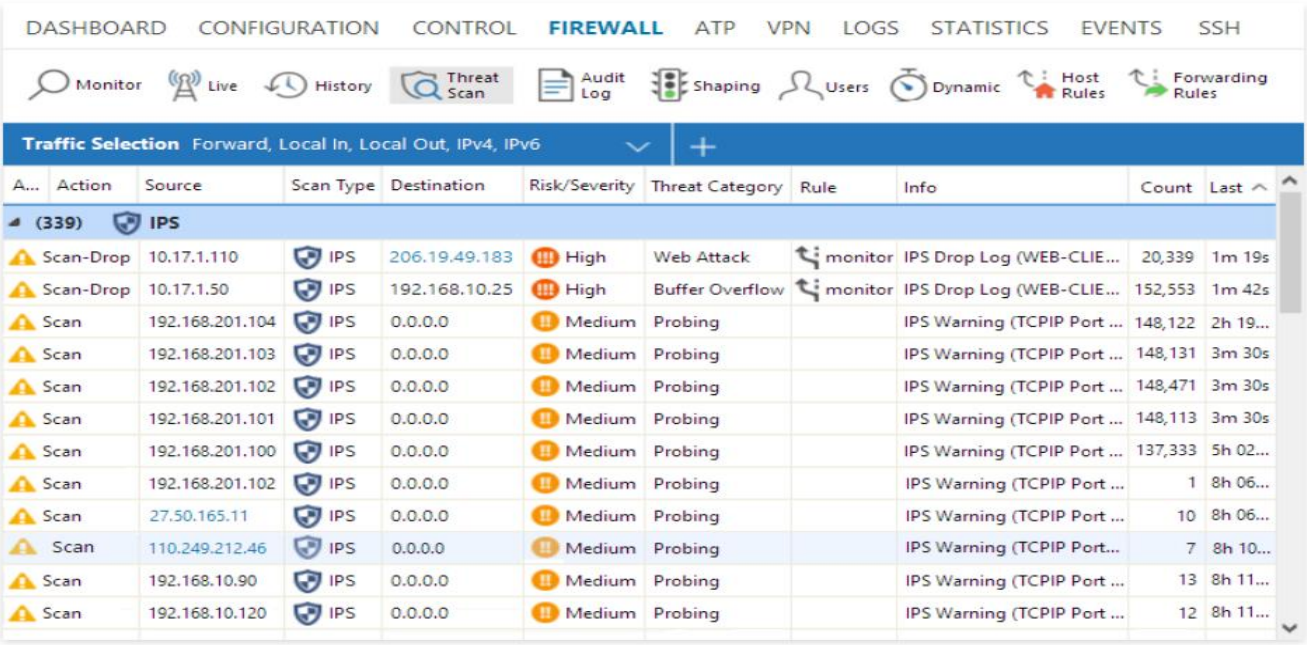


Рис. 2.6. Принцип роботи хмарного брандмауера Barracuda CloudGen Firewall

Хмарний брандмауер Barracuda CloudGen поєднують в собі механізми побудови надійних і захищених мереж з інтелектуальним управлінням трафіком і можливістю оптимізації маршрутів передачі даних. Це дає змогу скоротити витрати, збільшити загальну доступність мережі, поліпшити взаємодію між сайтами та забезпечити безперебійний доступ до додатків, розміщених у хмарі [18].

Технічні аспекти брандмауера:

- перевірка пакетів;
- повна ідентифікація користувача;
- IDS/IPS;
- фільтрація репутації DNS;
- динамічні правила / тригери за таймером;
- Єдиний об'єктноорієнтований набір правил для маршрутизації, мостів і маршрутизованих мостів;
- Виявлення та запобігання вторгнень;



A...	Action	Source	Scan Type	Destination	Risk/Severity	Threat Category	Rule	Info	Count	Last
(339)	IPS									
	Scan-Drop	10.17.1.110	IPS	206.19.49.183	High	Web Attack	monitor	IPS Drop Log (WEB-CLIE...	20,339	1m 19s
	Scan-Drop	10.17.1.50	IPS	192.168.10.25	High	Buffer Overflow	monitor	IPS Drop Log (WEB-CLIE...	152,553	1m 42s
	Scan	192.168.201.104	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	148,122	2h 19...
	Scan	192.168.201.103	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	148,131	3m 30s
	Scan	192.168.201.102	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	148,471	3m 30s
	Scan	192.168.201.101	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	148,113	3m 30s
	Scan	192.168.201.100	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	137,333	5h 02...
	Scan	192.168.201.102	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	1	8h 06...
	Scan	27.50.165.11	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	10	8h 06...
	Scan	110.249.212.46	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port...	7	8h 10...
	Scan	192.168.10.90	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	13	8h 11...
	Scan	192.168.10.120	IPS	0.0.0.0	Medium	Probing		IPS Warning (TCPIP Port ...	12	8h 11...

Рис. 2.7. Приклад роботи хмарного брандмауера Barracuda CloudGen Firewall з вхідним трафіком

Переваги:

- Масштабоване централізоване управління допомагає знизити адміністративні витрати в умовах розподіленої мережі в комерційній організації;
- NGFW Barracuda ідеально підходять для підприємств зі складною, розподіленою мережевою інфраструктурою;
- Обробляє весь трафік, для якого пункт призначення не збігається з прослуховуваним сокетом на брандмауері - іншими словами, весь трафік, що проходить через CloudGen Firewall;
- Barracuda CloudGen Firewall автоматично перемикає сеанси некритично важливого бізнес-трафіку на вторинні канали, щоб звільнити пропускну здатність для критично важливого трафіку;
- Брандмауер Barracuda CloudGen Firewall поєднує в собі повний набір розширених функцій безпеки з можливостями підтримки програмно визначеної глобальної мережі (SD-WAN);
- Коли загрози вражають вашу мережу, Barracuda показує ступінь ризику, джерело загрози й те, яка служба її виявила.
- Збереження пропускної здатності та прискорення роботи критично важливих додатків для забезпечення безперервності бізнесу;

Недоліки:

- Програмне управління - це те, що розуміють тільки певні люди (фахівці). Іноді вона працює за власною логікою. Використовувати її дуже складно;
- Складна в плані виконання простих речей;
- Вона могла б бути зручнішою для користувача і логічнішою;
- Найвища ціна, ніж в інших вендорів;
- Для кожного CloudGen Firewall дозволена тільки одна служба Forwarding Firewall, як наслідок втрачаємо функціонал;
- Брандмауер обробляє тільки IP-протоколи. IP-трафік, такий як протокол Spanning Tree Protocol або IPX/SPX, не пересилається;

- Рішення можна було б поліпшити, якби в трафіку було видно інформацію про те, що відбувається в цей момент часу.
- Я вважаю, що аналітика слабка, і хоча здається, що вона виконує свою роботу, важко зрозуміти, що саме вона робить.
- Відтворення всього трафіку та обсягу пропускної здатності в реальному часі не відображається для кожної мережі окремо.

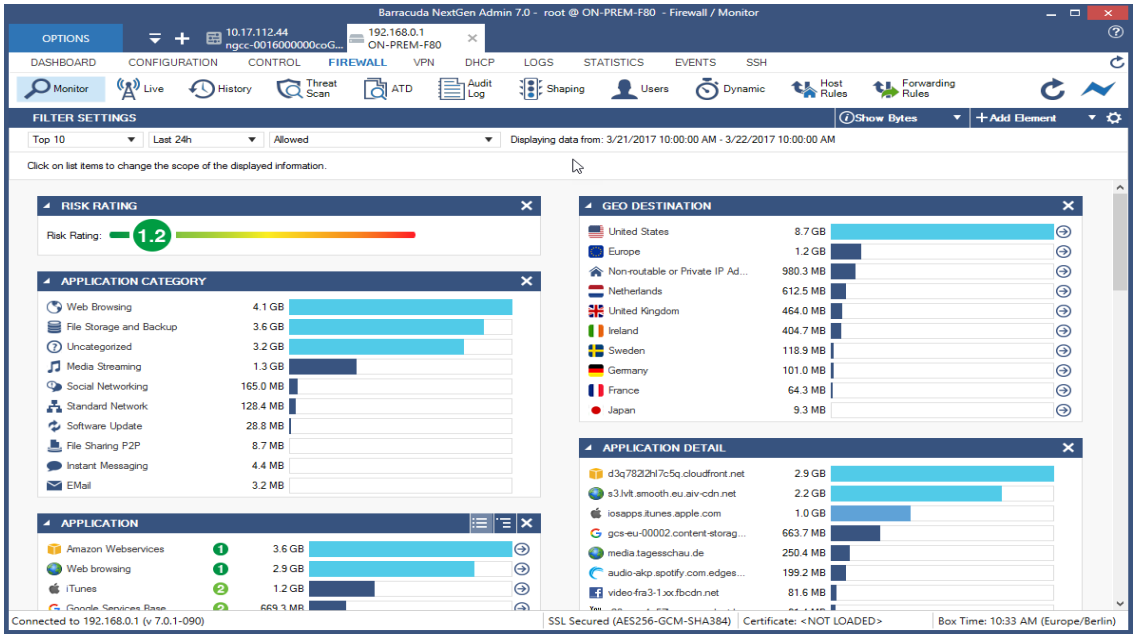


Рис. 2.8. Робоча панель Barracuda CloudGen Firewall

Враховуючи результати наведених вище порівнянь Umbrella Cloud Delivered Firewall та Barracuda CloudGen Firewall. Можна зробити висновок, що найкращим рішенням для побудови захищеної мережі комерційної організації буде використання Umbrella Cloud Delivered Firewall.

Оскільки завдяки вище перечисленим перевагам таким як: підтримка видимості та контролю інтернет-трафіку у філіях, забезпечується безперервним захистом мережі, а послуги міжмережевого екрана не потребують постійного розгортання і мають дуже гнучке налаштування. Тим паче достатня кількість фахівців з інформаційної безпеки також рекомендують до використання Umbrella Cloud Delivered Firewall для захисту комерційної мережі.

2.3. Призначення, можливості та функції Umbrella Cloud Delivered Firewall

Мінливий ринок стимулює безпеку використовувати хмарні технології. Безпрецедентні зміни у сфері корпоративної безпеки та мережевих технологій не припиняються і до сьогодні. Широке використання хмарних технологій призвело до використання додатків, які є основоположними для бізнесу. Віддалені місця розташування працівників компанії, які переміщуються, стають дедалі поширенішим явищем.

Традиційно, організації спрямовували інтернет-трафік з віддалених місць назад у центральне місце для забезпечення безпеки, однак це стало непрактичним через високу вартість і проблеми з продуктивністю. Тому на допомогу їм приходить Cisco Umbrella: який має багато функцій безпеки в тому числі й хмарний фаєрвол.

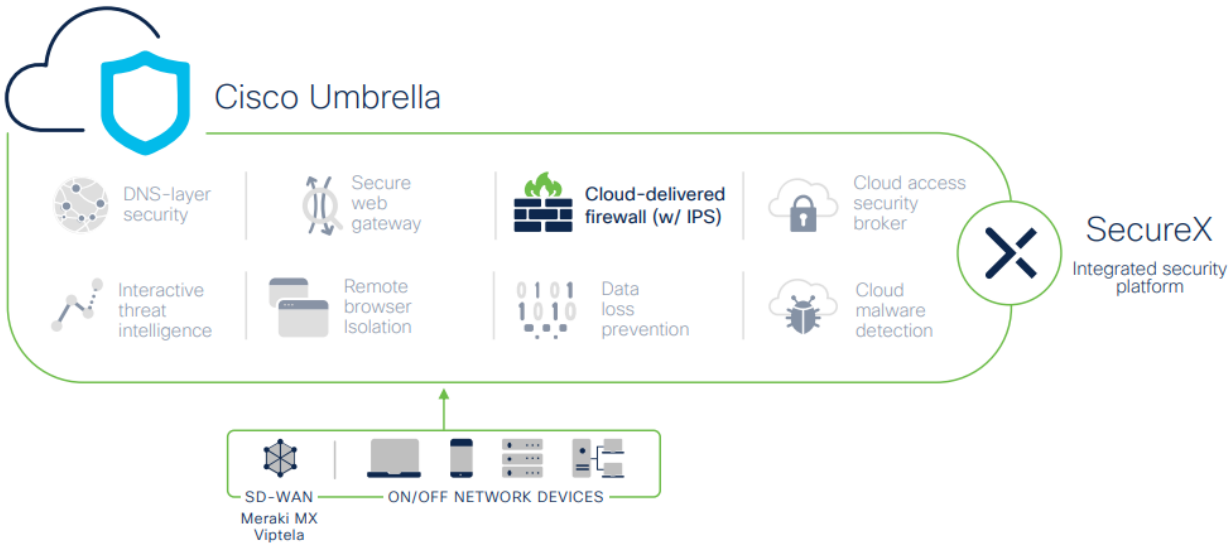


Рис. 2.9. Cisco Umbrella

Cisco Umbrella об'єднує безліч функцій безпеки в єдиній хмарній службі для забезпечення безпеки доступу до Інтернету та контролю використання хмарних застосунків у мережах, філіях і роумінгу.

На відміну від розрізнених засобів безпеки, Umbrella об'єднує безпечний веб-шлюз, хмарний брандмауер, брандмауер рівня DNS, функції брокера безпеки хмарного доступу. Завдяки тому, що все це можна отримати з єдиної приладової панелі, Umbrella є актуальною як ніколи, Даний програмний комплекс скорочує час, гроші та ресурси, необхідні для розгортання, налаштування та вирішення завдань [19].

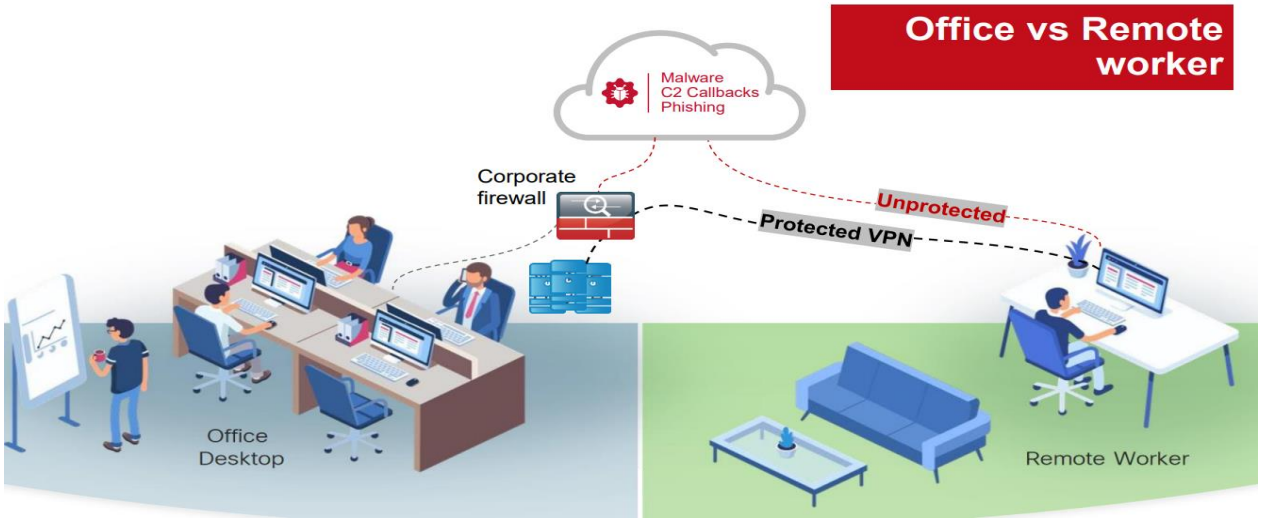


Рис. 2.10. Різниця між захищеною офісною мережею та стаціонарною

Umbrella Cloud Delivered Firewall - це брандмауер, що працює в хмарі, сьогодні він необхідний, але в майбутньому його важливість значно зросте. Оскільки Umbrella (CDFW) спрямовує трафік до ідеальної системи безпеки, вже зараз можна побачити як 70% сервісів використовують дану технологію.

Хмарний міжмережевий екран Umbrella (CDFW) забезпечує видимість і контроль трафіку, що виходить від клієнтського запиту в Інтернет, за всіма портами та протоколами. Він реєструє всю активність і блокує небажаний трафік, використовуючи правила IP, портів і протоколів (міжмережевий екран рівня 3/4), правила застосунків (рівень 7 видимості та контролю застосунків) і правила системи запобігання вторгненням (IPS). Надсилання трафіку на хмарний міжмережевий екран, можна зробити просто налаштувавши тунель IPSec з будь-якого мережевого пристрою.

Основні можливості хмарного брандмауера Umbrella Cloud Delivered Firewall:

- Umbrella розпізнає близько 2 800 загроз (регулярно додаються нові) і робить відповідні дії щодо їх блокування або дозволу. Це розширює виявлення і блокування застосунків з рівня безпеки DNS і безпечного веб-шлюзу Umbrella;
- Підтримка IPSec тунелю включаючи AnyConnect;
- Блокує тіньовий IT трафік через не веб-порти;
- Блокує небезпечні додатки на нестандартних портах;
- Блокує несанкціонований трафік через не мережеві порти;
- Налаштування політика міжмережевого екрана;
- IPS Сигнатурні списки;
- Додавання та видалення правил брандмауера (За допомогою правил брандмауера, написаних на приладовій панелі Umbrella, ви можете фільтрувати трафік на рівнях 3 і 4) ;
- Зміна пріоритету брандмауера;
- Перегляд журналів брандмауера у звітах;
- Перевірка протоколу веб-трафіку;

Основні функції хмарного брандмауера Umbrella Cloud Delivered Firewall:

- Видимість і контроль інтернет-трафіку через усі порти й протоколи.
- Налаштовувані політики IP, портів, протоколів і застосунків на приладовій панелі Umbrella
- Підтримка тунелів IPsec для безпечної маршрутизації трафіку в хмарну інфраструктуру
- Автоматизовані журнали звітів
- Фільтрацію через тунель IPsec з будь-якого мережевого пристрою.
- При створенні нових тунелів, потрібно налаштувати політику безпеки, яка потім автоматично буде застосовуватися у всьому середовищі.
- Якщо в Cloud Delivered Firewall відбуваються збої в роботі системи або виникають інші критичні проблеми, на сторінці стану з'являються червоні

повідомлення про зниження активності. У більшості випадків це означає, що основні функції не працюють належним чином, або відбувається якась інша серйозна подія, що впливає на клієнта.

2.4. Компоненти та архітектура рішення Umbrella Cloud Delivered Firewall

Архітектура рішення Umbrella (CDFW):

1. Ідентифікатори

- Мережевий тунель використовується як основна ідентифікація;

- Підтримка SAML (SAML (Security Assertion Markup Language) є відкритим стандартом на основі XML, який призначений для обміну даними автентифікації та авторизації між сторонами процесу);

2. Інфраструктура

- Підтримка декількох центрів обробки даних;

- Автоматичне відновлення після відмови центра зберігання та обробки даних;

3. Ведення журналів і звітність

- Журнали брандмауера включені як частина Activity Search;

- Підтримується експорт журналів через S3 (Simple Storage Service) - протокол передавання даних);

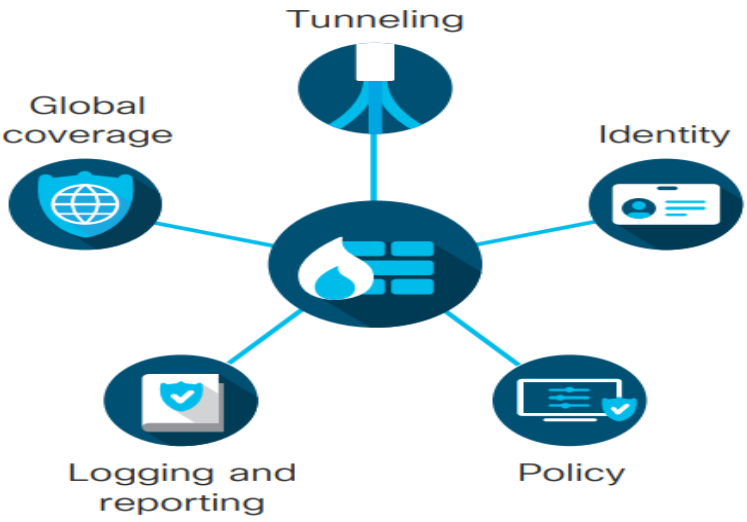


Рис. 2.11. Приклад Архітектури рішення Umbrella (CDFW)

Priority	Name	Enabled	Protocol	Source Criteria	Destination Criteria	Action
1	Port Block - 444	Enabled	Any	any IPs any Ports	any IPs 1 Port	Block
2	ICMP Block Outbound	Enabled	ICMP	any IPs any Ports	any IPs any Ports	Block
3	Block Destination IP	Enabled	Any	any IPs any Ports	1 IP any Ports	Block
4	Default Rule	Enabled	Any	any IPs any Ports	any IPs any Ports	Allow

Рис. 2.12. Політика брандмауера в Umbrella (CDFW)

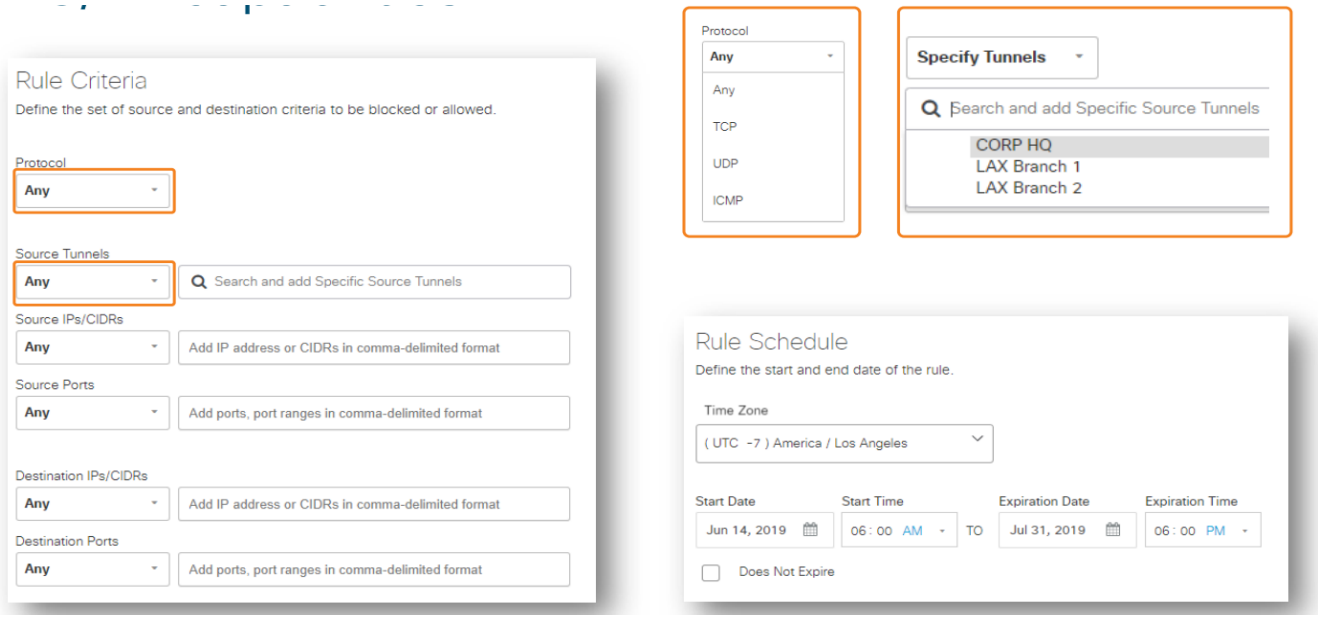


Рис. 2.13. Налаштування L3/L4 в Umbrella (CDFW)

Фільтр за IP-адресами, портами, протоколами АБО перегляд відомостей про IP-адреси в розділі «Розслідування»

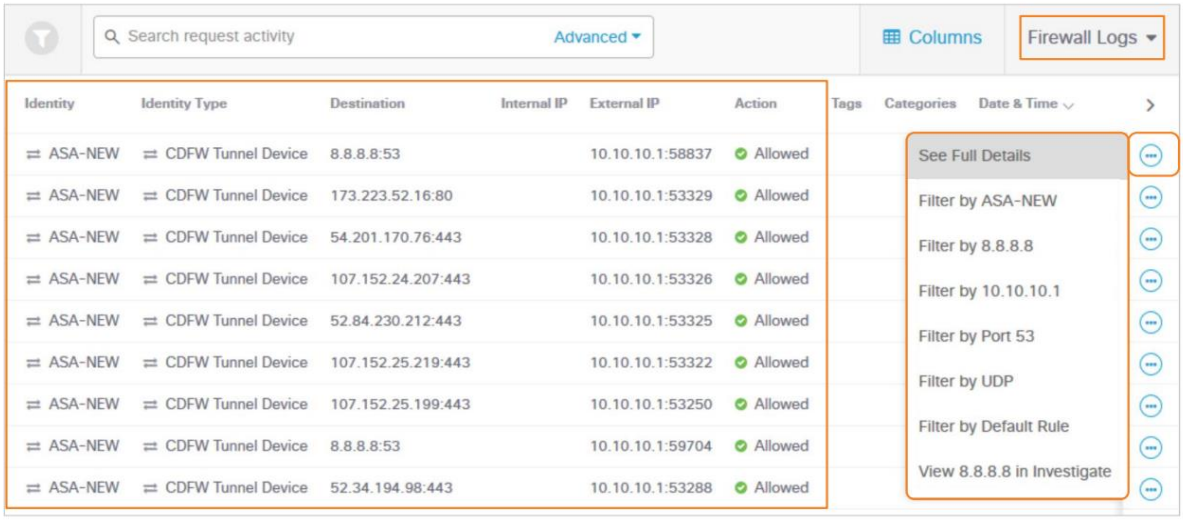


Рис. 2.14. Звітність в Umbrella (CDFW)

Експортується в Cisco або власне сховище S3

- **Timestamp**—The timestamp of the request transaction in UTC.
- **originId**—The unique identity of the network tunnel.
- **Identity**—The name of the network tunnel.
- **Identity Type**—The type of identity that made the request. Should always be "CDFW Tunnel Device".
- **Direction**—The direction of the packet. It is destined either towards the internet or to the customer's network.
- **ipProtocol**—The actual protocol of the traffic. It could be TCP, UDP, ICMP.
- **packetSize**—The size of the packet that Umbrella CDFW received.
- **sourceIp**—The internal IP address of the user generated traffic towards the CDFW. If the traffic goes through NAT before it comes to CDFW, it will be the NAT IP address.
- **sourcePort**—The internal port number of the user generated traffic towards the CDFW.
- **destinationIp**—The destination IP address of the user generated traffic towards the CDFW.
- **destinationPort**—The destination port number of the user generated traffic towards the CDFW.
- **dataCenter**—The name of the Umbrella Data Center that processed the user generated traffic.
- **ruleId**—The ID of the rule that processed the user traffic.
- **verdict**—The final verdict whether to allow or block the traffic based on the rule.

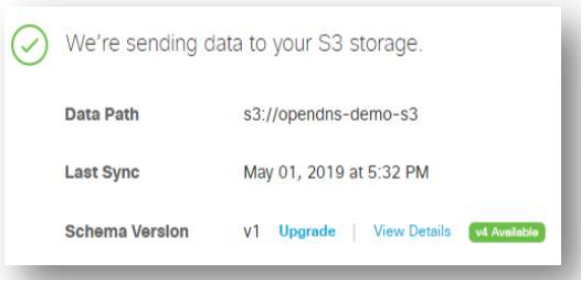


Рис. 2.15. Експорт журналу в Umbrella (CDFW)

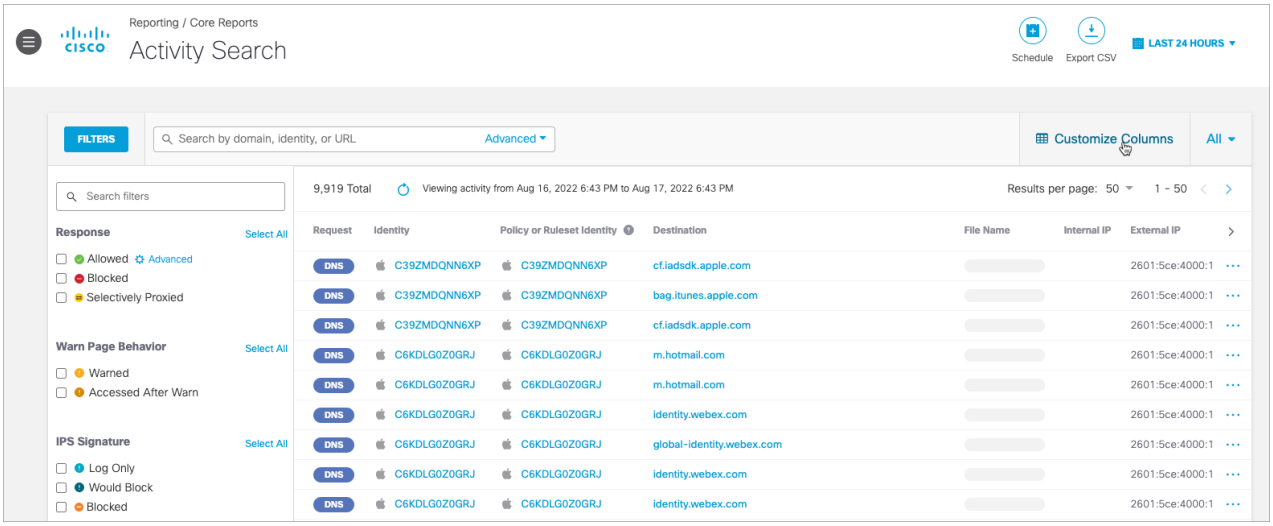


Рис. 2.16. Перевірка протоколу веб-трафіку в Umbrella (CDFW)

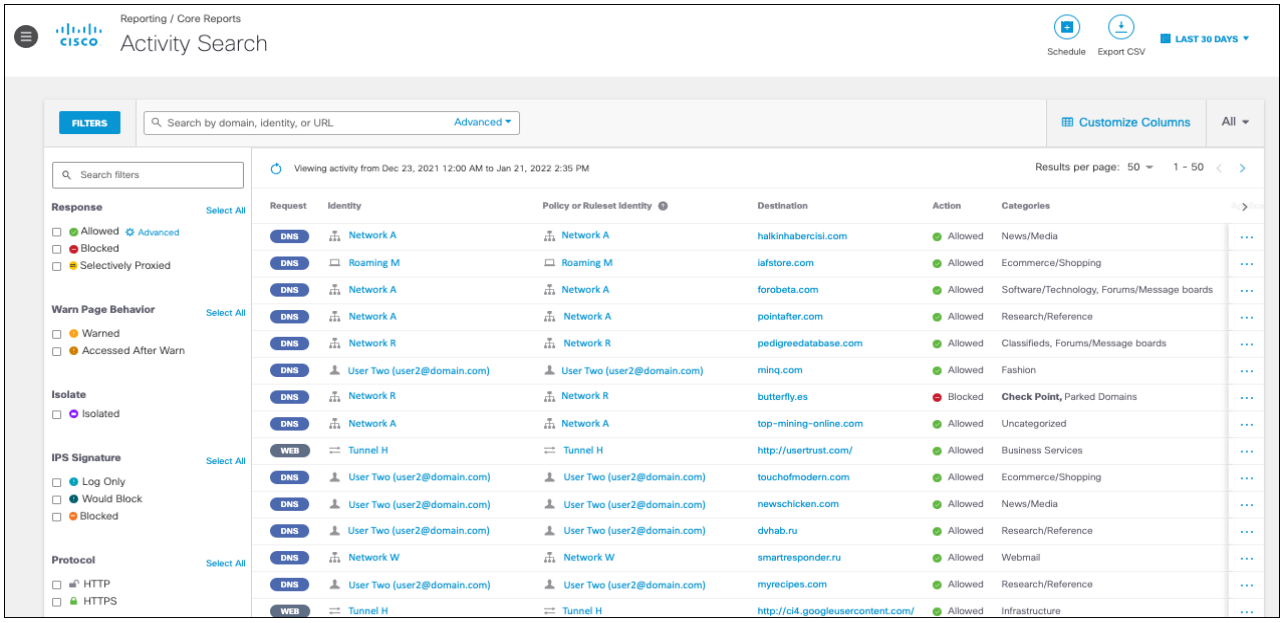


Рис. 2.17. Перегляд журналів брандмауера у звітах в Umbrella (CDFW)

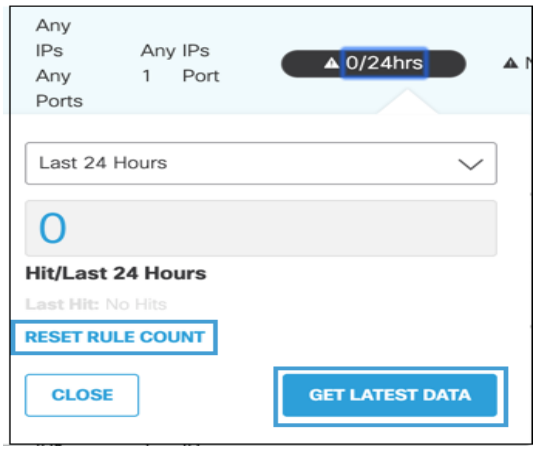


Рис. 2.18. Редагування кількості переглядів в Umbrella (CDFW)

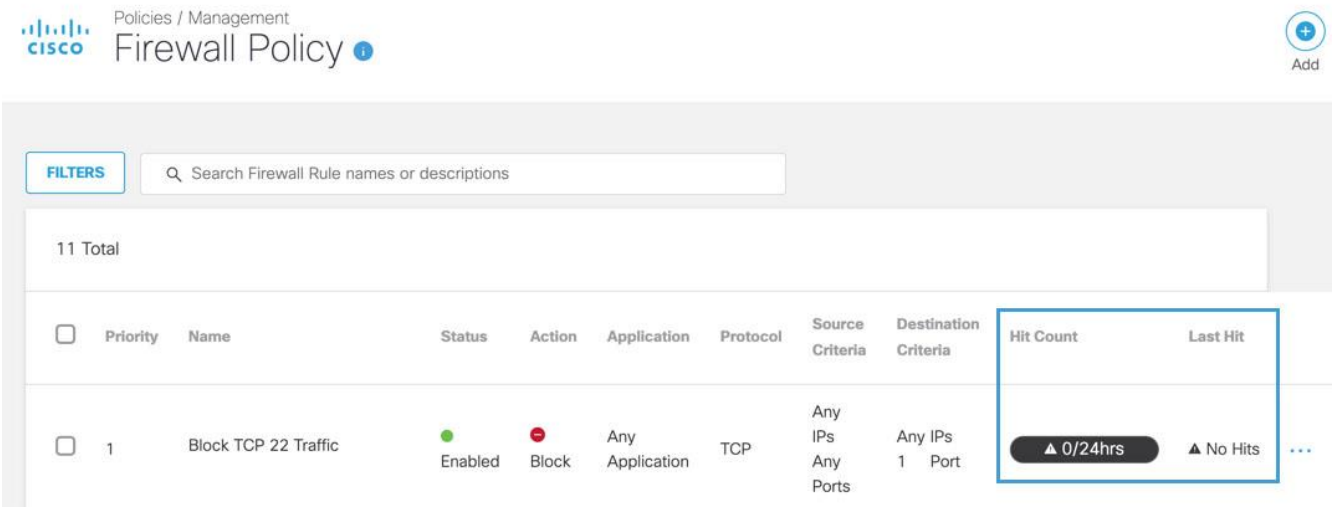


Рис. 2.19. Моніторинг кількості влучень в Umbrella (CDFW)

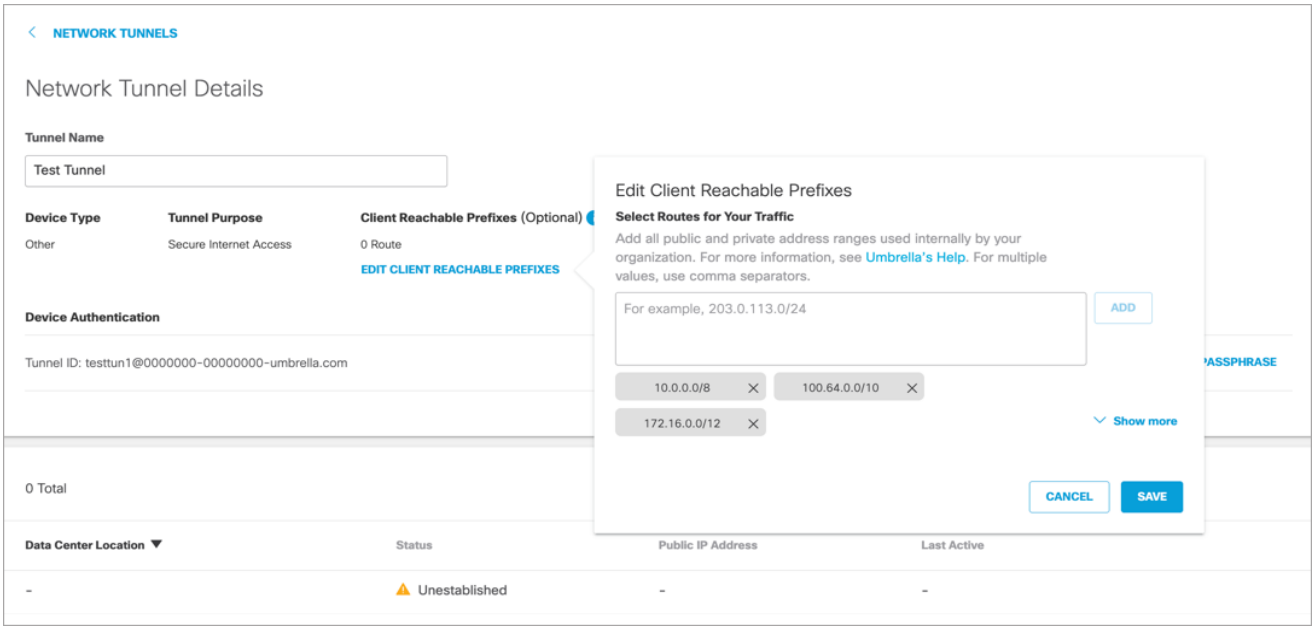


Рис. 2.20. Конфігурація мережевого тунелю в Umbrella (CDFW)

Висновки до другого розділу

Проаналізовано та досліджено технології та засобів для побудови захищеної мережі із використанням хмарного фаєрвола.

Виконано порівняльний аналіз використання двох хмарних фаєрволів Umbrella Cloud Delivered Firewall та Barracuda CloudGen Firewall. Виокремлено переваги та недоліки у функціоналі між Umbrella Cloud Delivered Firewall та Barracuda CloudGen Firewall.

Досліджено та проаналізовано призначення, можливості та функції Umbrella Cloud Delivered Firewall.

Виокремлено компоненти та архітектурні рішення в Umbrella Cloud Delivered Firewall. Одночасно з розвитком корпоративної мережі в комерційній організації, необхідно, щоб система антивірусного захисту, у кращому разі, випереджала її розвиток на крок або ж змінювалася одночасно та відповідно до розширення кількості або якості сервісів, які надаються користувачам цієї мережі.

3 ТЕХНОЛОГІЯ ТА ЗАСОБИ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ КОМЕРЦІЙНОЇ ОРГАНІЗАЦІЇ ІЗ ВИКОРИСТАННЯМ UMBRELLA CLOUD-DELIVERED FIREWALL (CDFW)

3.1. Вимоги до системи для інсталяції Cisco Umbrella та компонента Cloud Delivered Firewall

Cisco Umbrella - це хмарний захищений інтернет-шлюз Cisco Secure Internet Gateway (SIG), який забезпечує кілька рівнів захисту від інтернет-загроз. Umbrella інтегрує в собі функції безпечного веб-шлюзу, брандмауера, захисту на рівні DNS та брокера безпеки хмарного доступу (CASB) для захисту вашої мережі від загроз.

Найшвидший спосіб розпочати роботу - відкрити браузер, увійти до панелі управління Umbrella за адресою http://dashboard.umbrella.com, зареєструвати мережу, додавши ідентифікатор мережі, а потім вказати DNS для Cisco Umbrella [20].

Загальнодоступний IP-трафік від користувачів SIG буде відображатися як такий, що надходить з діапазонів адрес 146.112.0.0/16 та 155.190.0.0/16. Залежно від організації, може знадобитися повідомити постачальників послуг, до яких отримується доступ через службу Umbrella, про ці додаткові діапазони IP-адрес. Наприклад, деякі постачальники послуг вимагають попереднього повідомлення про діапазони використовуваних IP-адрес, перш ніж дозволити доступ до їхніх послуг.

Перед початком використання Cisco Umbrella, є кілька перших кроків, які необхідно зробити, щоб Cisco Umbrella могла почати захищати систему та організацію.

1. Зареєструвати мережу, додавши ідентифікатор мережі. Ідентифікатор - це об'єкт, який Umbrella захищає за допомогою політик і контролює за допомогою звітів.

2. Налаштувати DNS на Umbrella. Потрібно чітко вказати налаштування DNS операційної системи або апаратного брандмауера/маршрутизатора на IP-адреси сервера імен Umbrella та вимкнути автоматичні DNS-сервери, що надаються провайдером Інтернет-послуг. Umbrella підтримує адреси IPv4 та IPv6.

3. Додавання та налаштування політик. За допомогою політик необхідно визначити, як Umbrella застосовує засоби контролю безпеки та доступу до ідентичностей, визначаючи, чи буде трафік перевірений і заблокований або дозволений. Існує три типи політик, які можна додати:

- Політика DNS - забезпечує видимість, безпеку і застосування DNS-рівня з можливістю вибіркового проксі-сервера для ризикованих доменів для додаткової безпеки.
- Політика брандмауера - забезпечує фільтрацію і перенаправлення вашого веб-трафіку.
- Веб-політика - забезпечує видимість, безпеку і контроль веб-трафіку на рівні URL-адрес.

4. Знайти ідентифікатор організації. Кожна організація Umbrella (Org) є окремим екземпляром Umbrella і має власну інформаційну панель. Організації ідентифікуються за назвою облікового запису та унікальним ідентифікатором організації (Org ID). Org ID використовується для ідентифікації вашої організації під час розгортання таких компонентів, як віртуальні пристрої, і часто запитується службою підтримки, щоб допомогти ідентифікувати ваше розгортання Umbrella.

Порядок дій:

- Входимо до інформаційної панелі Umbrella.

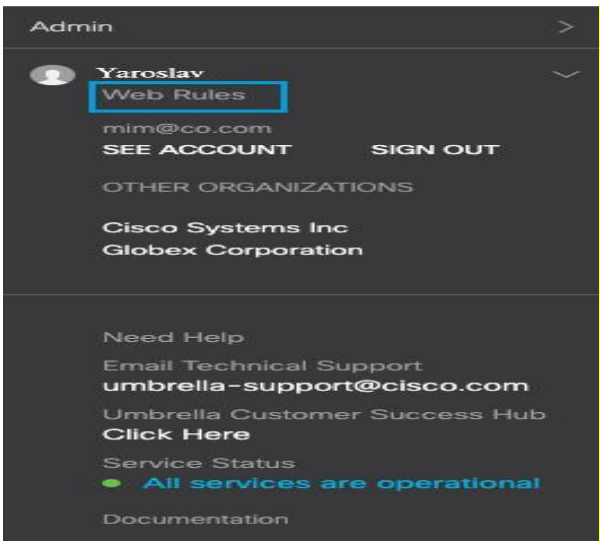


Рис. 3.1. Навігаційне меню Cisco Umbrella

- У навігаційному меню необхідно розгорнути назву облікового запису та переконатися, що здійснено вхід до інформаційної панелі Umbrella. Назва організації вказана під назвою облікового запису. Інші організації, до яких можна отримати доступ, перераховані в розділі (Інші організації).
- Після входу в потрібну інформаційну панель перевірте URL-адресу в адресному рядку: https://dashboard.umbrella.com/o/<*OrgID*>/#/<*page*>.

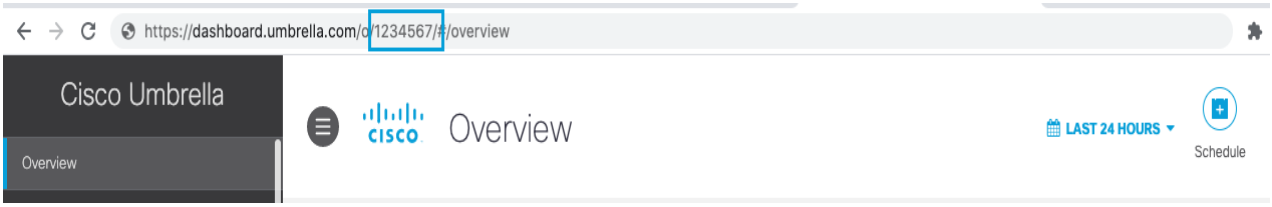


Рис. 3.2. Перевірка URL-адреси в адресному рядку

5. Наступним кроком потрібно визначити поточний пакет. Не всі функції Cisco Umbrella доступні для всіх пакетів Cisco Umbrella. Ліцензійний пакет визначає, які функції Cisco Umbrella доступні для користувача, а також рівень підтримки, який доступний. Поточний пакет вказано на сторінці ліцензування Cisco Umbrella. Треба зазначити, зо з роками пакети Cisco Umbrella змінюються. Залежно від того, коли вперше почали використовувати Cisco Umbrella, вказаний ліцензійний пакет може відрізнятися від того, що був доступний для нових розгортань Cisco Umbrella.

- Адміністрування > вкладка Ліцензування.

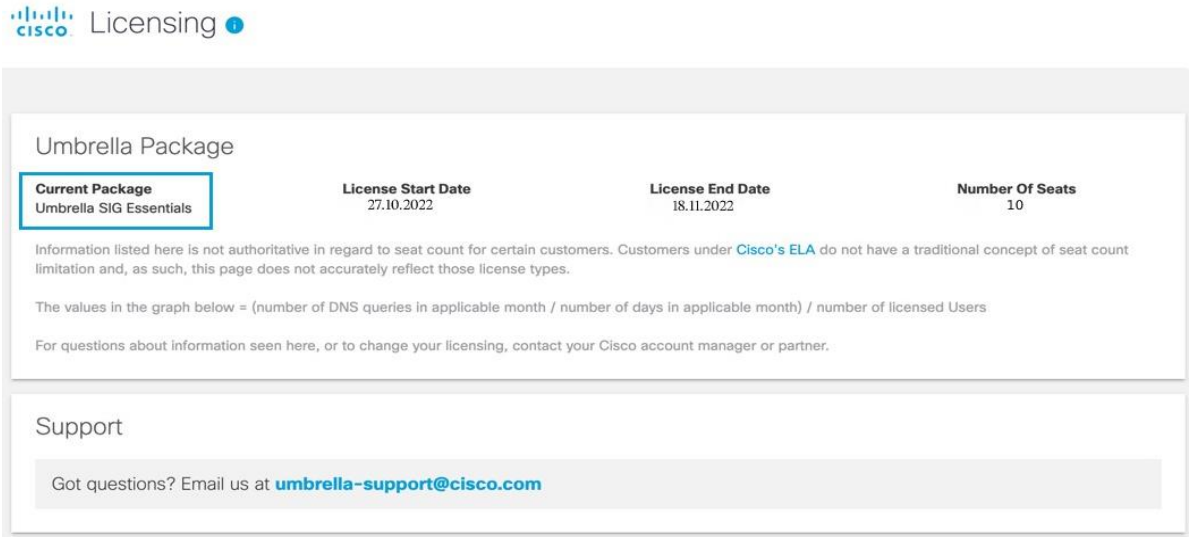


Рис. 3.3. Вкладка Ліцензування

6. При цьому необхідно переглянути статус служби хмарного захисту. Cisco Cloud Security Service Status надає інформацію про стан сервісних платформ Cisco Umbrella та Cisco Cloudlock в режимі реального часу (рис.3.4.). В системі доступна можливість перегляду стану компонентів Cloud Security, служб, API та світових центрів обробки даних, а також доступна інформація про нещодавні події з технічного обслуговування та сервісу [21].

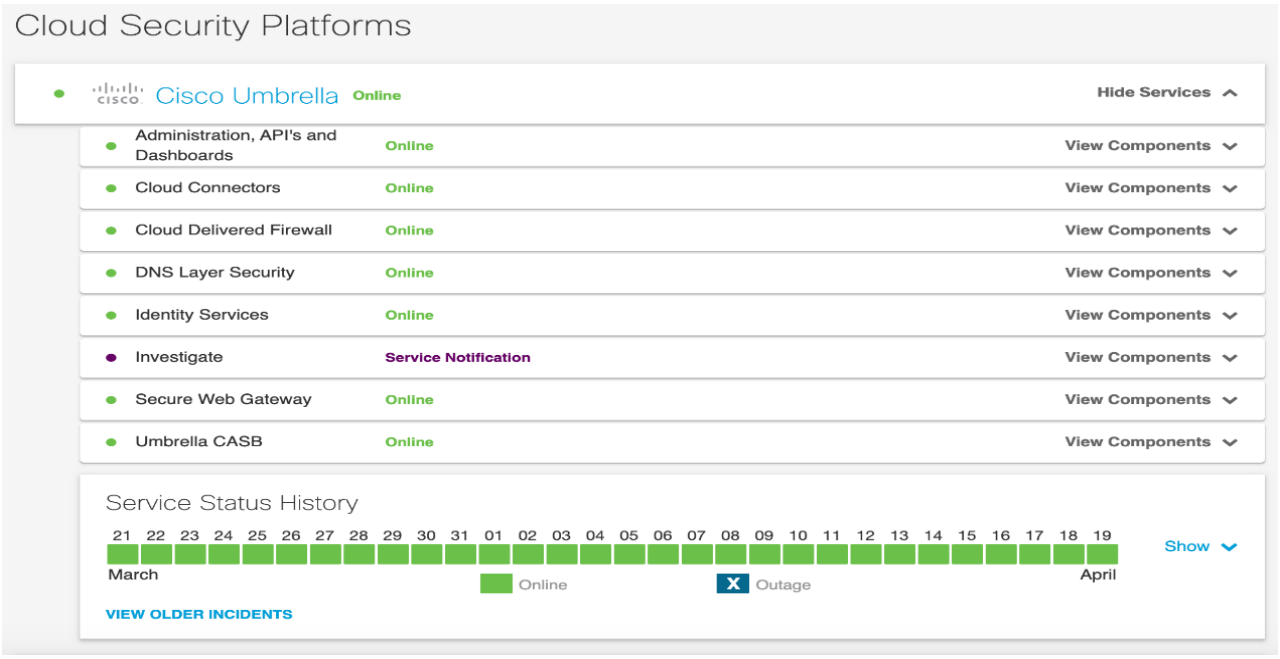


Рис. 3.4. Переглядаємо статус компонентів сервісної платформи Cisco Umbrella

7. Початок роботи. Щоб розпочати захист системи, необхідно увімкнути захист Cisco Umbrella на рівні DNS та налаштувати веб-безпеку за допомогою захищеного веб-шлюзу Cisco Umbrella та хмарного брандмауера Umbrella Cloud Delivered Firewall. Після того, як здійснено налаштування параметрів DNS, потрібно перейти на сторінку http://welcome.umbrella.com. Якщо вірно вказані дані DNS щодо серверів Cisco Umbrella, з'явиться вітальна сторінка. Це буде означити, що всі вимоги перед використанням продукту були виконані вірно.

3.2. Налаштування програмного продукту Cisco Umbrella та компонента Cloud Delivered Firewall для мінімізації атак на мережеву інфраструктуру

Коли користувач намагається потрапити на якийсь ресурс по домену, незалежно від протоколу, здійснюється резервування доменного імені, тобто перетворення його в IP-адресу. Можна обмежувати доступ до ресурсів на основі URL (фактично вже HTTP-трафік), а можна робити це на крок раніше, виходячи з з політики брандмауера.

Рішення може детектувати та блокувати DNS-звернення за такими категоріями:

- скомпрометовані системи;
- зв'язок із серверами управління (C2C);
- Malware та Phishing;
- автозгенеровані домени;
- нові домени;
- побудова DNS-тунелів (DNS Exfiltration).

Головна вимога – це захист користувачів. Особливо за умов масового переходу на віддалений формат роботи, цього також потребують віддалені користувачі. Користувачів якось потрібно перенаправити в хмару для аналізу їхніх DNS-запитів, і тут є два способи.

1) У користувачів на майданчиках прописаний локальний DNS (зазвичай адреса домену-контролера). Це досить просто потрібно прописати адреси в Cisco Umbrella у налаштуваннях DNS Forwarders;

2) Віддаленим користувачам достатньо встановити AnyConnect (модуль Roaming Client) або налаштувати основну політику брандмауера, через Cloud Delivered Firewall.

Доступність зазначених адрес 208.67.222.222 та 208.67.220.220 забезпечується за допомогою BGP Anycast (коли одні й самі маршрути анонсуються з різних географічних точок). Таким чином, при зверненні на ці адреси для зменшення затримок ви будете направлені до найближчого дата центру (ЦОД) залежно від свого географічного розташування.

З боку Cisco Umbrella достатньо додати лише особисту білу IP адресу (або кілька адрес) для переходу до списку Networks, для roaming clients (віддалених користувачів) нічого додатково додавати не треба.

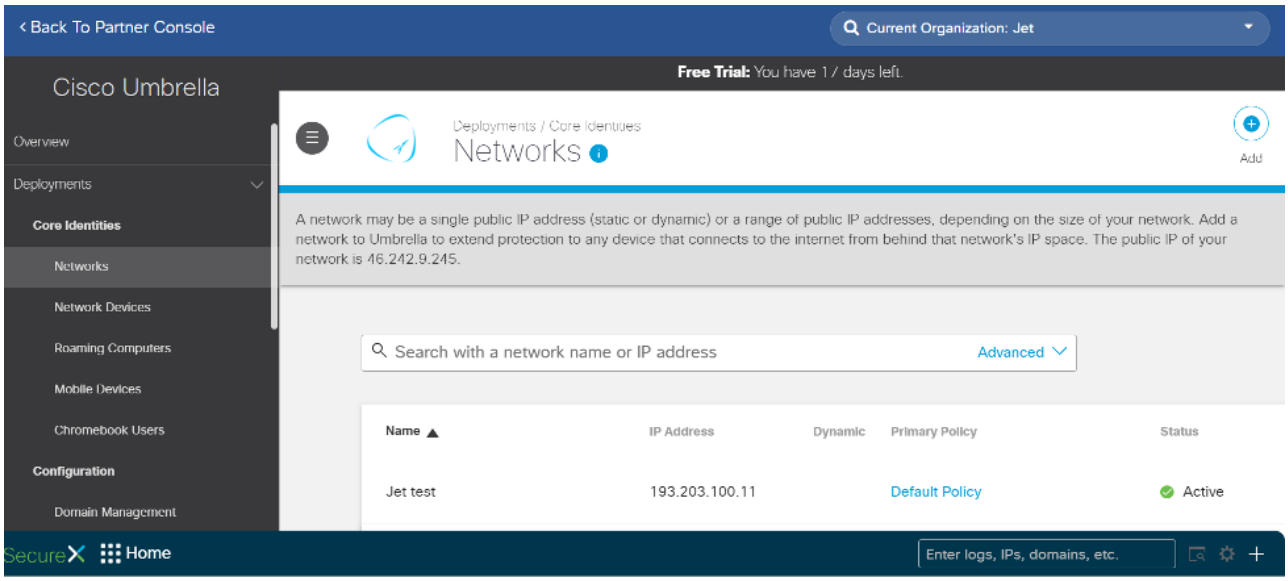


Рис. 3.5. Перевірка статусу IP адреси

Коли на домен-контролері налаштовані DNS-forwarders, а у віддалених користувачів встановлений Roaming Client, можна перевірити, чи використовується захист Cisco Umbrella, перейшовши за адресою https://welcome.umbrella.com.

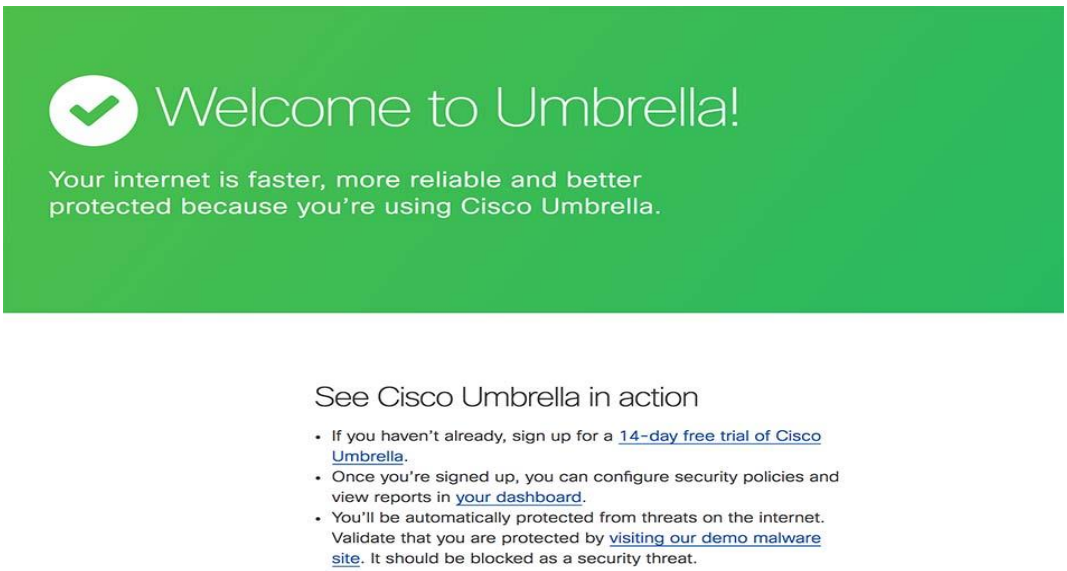


Рис. 3.6. Перевірка статусу Cisco Umbrella (Все ви під захистом!)

Як вже раніше зазначалося внаслідок масового переходу на відалений формат роботи, постає питання захисту мережі комерційної організації від атак на інфраструктуру. Тому на допомогу проходить хмарний брандмауер Umbrella Cloud Delivered Firewall, який надає послуги брандмауера без необхідності розгортання, обслуговування та оновлення фізичних або віртуальних пристроїв.

Також, дане рішення може додатково виступати в ролі L3/L4/L7 міжмережевого екрана в хмарі, для цього потрібно загорнути трафік з майданчика через IPSec-тунель. Такий хмарний фаєрвол може в принципі підійти тим організаціям, на майданчиках яких немає свого брандмауера і є лише канал в інтернет (тобто, немає виділених каналів до ЦОД, де можна централізовано випускати користувачів в інтернет).

За допомогою правил брандмауера, записаних на інформаційній панелі Cisco Umbrella, можна фільтрувати трафік на рівнях 3 і 4, який проходить з внутрішньої мережі, але призначений для Інтернету [22].

Необхідні умови:

- Підключення до мережі Інтернет, яке дозволяє вихідний IPsec-трафік.
- Обліковий запис Umbrella з увімкненою функцією хмарного брандмауера.
- Мережевий пристрій, здатний створити тунель IPsec IKEv2.

- Парольна фраза тунелю, отримана з інформаційної панелі Umbrella.
- Наявність підключення принаймні до одного тунелю.

Процедура додавання правил брандмауера:

1. Політики > Керування > Політика брандмауера і натисніть Додати.

Рис. 3.7. Налаштування Політики брандмауера

Якщо Umbrella відображає повідомлення «Вам не вистачає тунельного з'єднання», необхідно натиснути «Додати тунель».

Тунелі необхідні для правил брандмауера.

Рис. 3.8. Кнопка «Додати тунель»

2. Визначення основних характеристик правил брандмауера:

- вибір назви та опису;
- вибір порядку пріоритету. Порядок пріоритету розташовує правила в політиці брандмауера в тому порядку, в якому вони оцінюються, а потім застосовуються. Правила застосовуються послідовно, при цьому правило за замовчуванням завжди знаходиться в останній позиції.
- ввімкнення або вимкнення правил брандмауера.

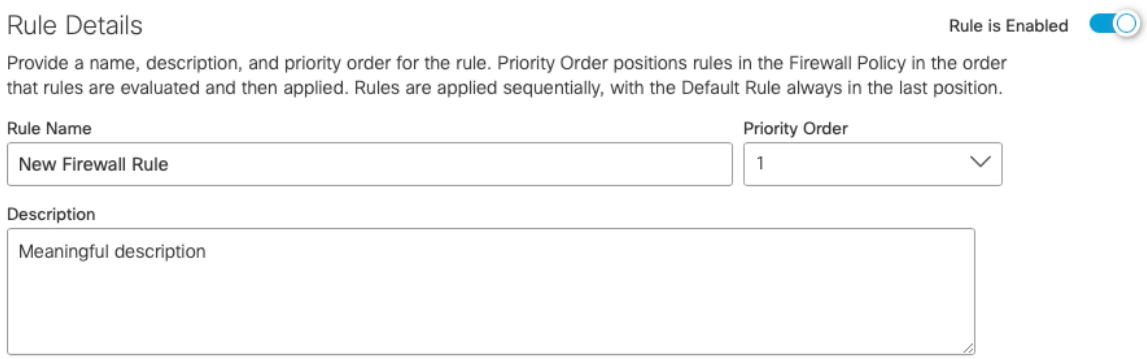


Рис. 3.9. Кнопка вмикання або вимикання правила брандмауера

3. У розділі Дія правила необхідно обрати Дозволити або Заблокувати.

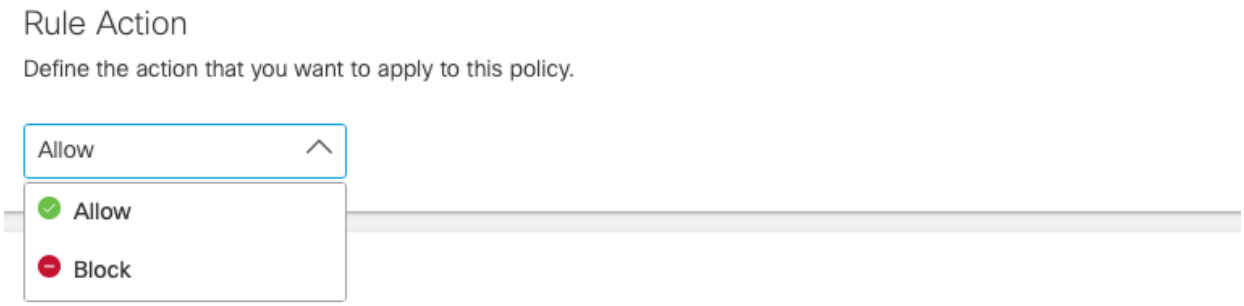


Рис. 3.10. Дозволити або Заблокувати правило брандмауера

4. Вибір критеріїв правил:

- Протокол - протоколи, до яких застосовується правило. Можливі варіанти: TCP, UDP, ICMP або будь-який інший.
- Програми - програми та категорії програм, до яких застосовується правило. Для отримання додаткової інформації див.
- Вихідні тунелі - вихідний тунель, до якого застосовується правило. До трьох тунелів відображаються динамічно, коли ви починаєте вводити текст.
- IP-адреси джерела CIDR - IP-адреси джерела тунелю (IP або CIDR), до яких застосовується правило. Можна вказати IP і додати кожну IP-адресу CIDR, або вибрати будь-яку іншу.
- Вихідні порти - вихідні порти тунелю, до яких застосовується правило. Можна вибрати Specify Port (Вказати порт) і ввести порти або діапазони портів в текстовому списку через кому або вибрати Any (Будь-який).
- IP-адреси призначення CIDR - адреси призначення тунелю (IP або CIDR), до яких застосовується правило. Можна вибрати Вказати IP і додати кожну IP-адресу CIDR, або вибрати будь-який інший.
- Порти призначення - порти призначення тунелю, до яких застосовується правило. Можна вибрати Specify Port (Вказати порт) і ввести порти або діапазони портів в текстовому списку, розділеному комами, або вибрати Any (Будь-який).

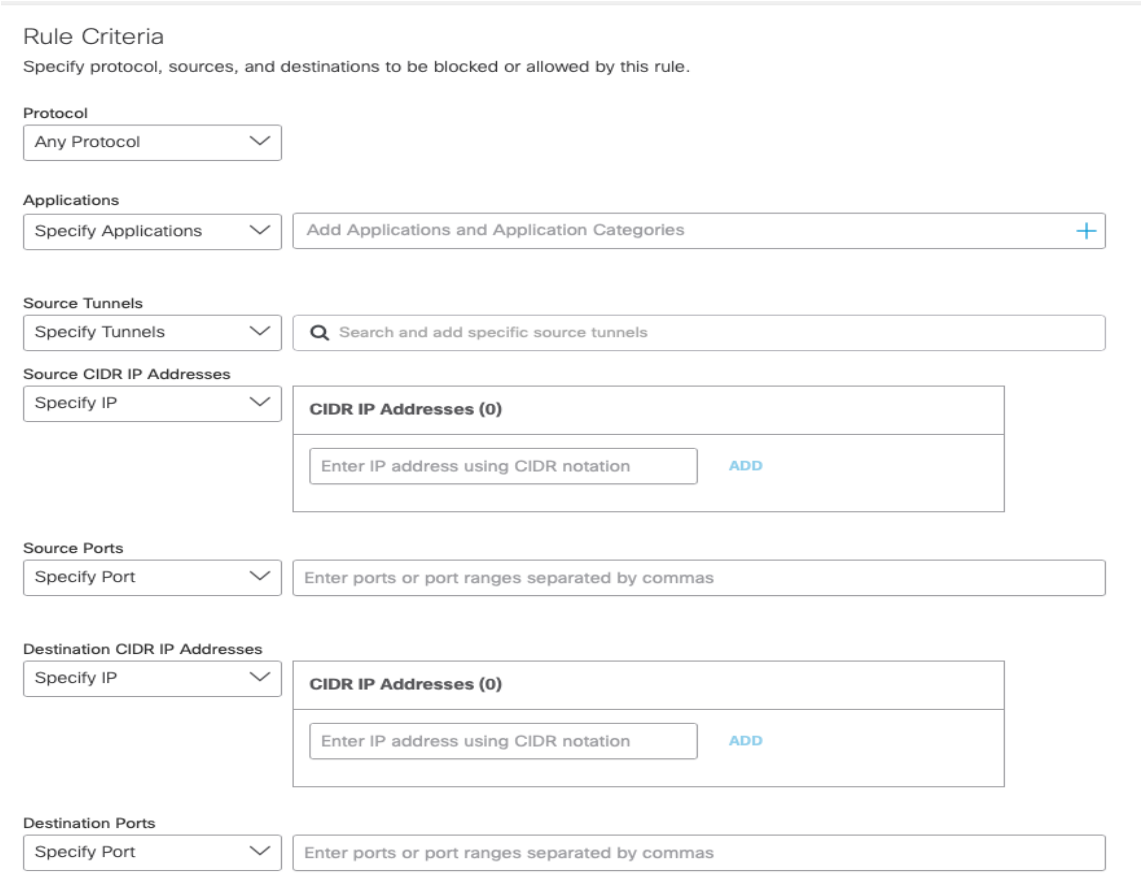


Рис. 3.11. Налаштування критеріїв правил

5. Вибір часового поясу і налаштування дати, часу початку і закінчення дії правила. За бажанням, можна встановити прапорець Does Not Expire, щоб термін дії правила не закінчувався.

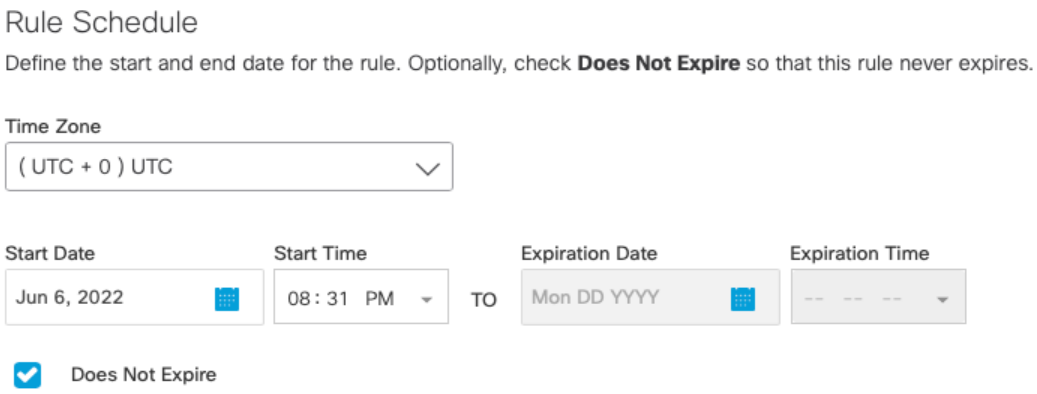


Рис. 3.12. Налаштування часового поясу, дати, часу початку і закінчення дії правила

6. Вибір інтервалу для лічильника відвідувань. Якщо вимкнути ведення журналу для цього правила брандмауера, лічильник потраплянь також буде вимкнено.

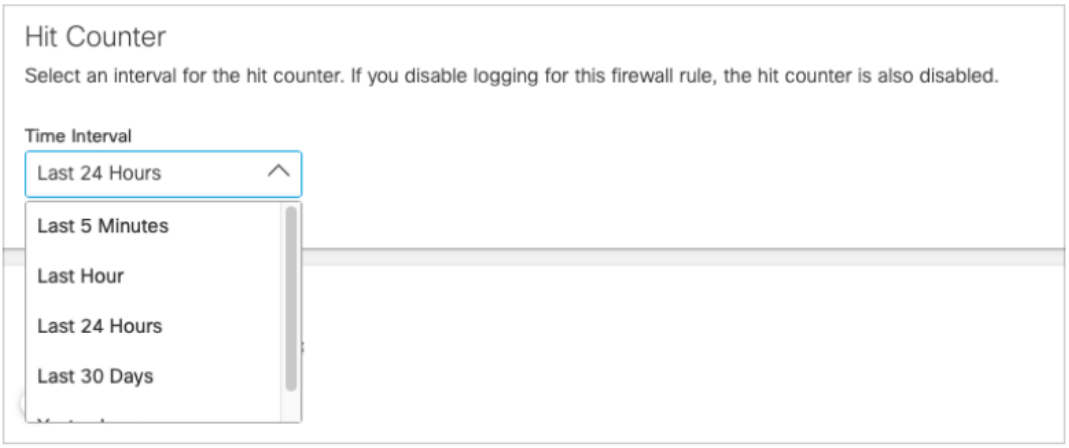


Рис. 3.13. Налаштування лічильника відвідувань

7. Увімкнення або вимкнення ведення журналу. За замовчуванням ведення журналу відключено. Якщо вимкнути ведення журналу, відвідувань також буде відключений, тому це дуже важливо.

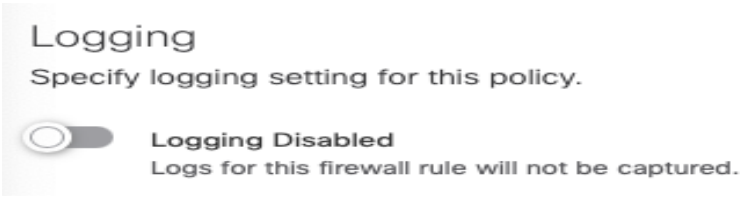


Рис. 3.14. Налаштування ведення журналу

8. Натискаємо «Зберегти». Тепер можна додавати ідентифікатори мережевих тунелів і визначати дії, порти, протоколи та програми в правилі брандмауера. Umbrella оцінює кожне правило брандмауера, починаючи з правила з найвищим рейтингом. Коли ідентифікатор і пункт призначення збігаються з правилом, також Umbrella застосовує дію, визначену в правилі. Наприклад, якщо ідентифікатор запитує веб-додаток через порт 80 або 443, Umbrella спочатку перевіряє наявність відповідного правила брандмауера. Якщо Umbrella знаходить відповідне правило брандмауера, хмарний брандмауер (CDFW) застосовує дію, визначену в правилі [23].

3.3. Налаштування параметрів безпеки на мережевих пристроях за допомогою Umbrella Cloud Delivered Firewall

Брандмауер Umbrella Cloud Delivered Firewall дозволяє організації тунелювати весь інтернет-трафік до Umbrella Cloud та реєструвати усі дії. Політика Umbrella (CDFW) може фільтрувати рівні 3 і 4, щоб блокувати загрози на основі IP, порту та протоколу. Для перенаправлення трафіку в Umbrella Cloud створюються VPN-тунелі IKEv2/IPSec. Umbrella (CDFW) також підтримує мережеві тунелі на пристроях SDWAN (vEdge і cEdge), Cisco ASA, Cisco ISR і Cisco FTD [24].

Весь трафік, окрім трафіку DNS, тунелюватиметься через Umbrella CDFW. DNS-трафік спрямовуватиметься безпосередньо на сервери Umbrella DNS із загальнодоступною IP-адресою маршрутизатора, що дає змогу застосовувати політику DNS на основі політик організації. Без обходу трафіку DNS хмарний брандмауер обробить запит, і трафік буде направлено за публічною IP-адресою на Umbrella (CDFW) [25].

Реєстрація мережі:

1. Вхід на інформаційну панель Umbrella
2. Розгортання > Основні ідентифікатори > Мережі

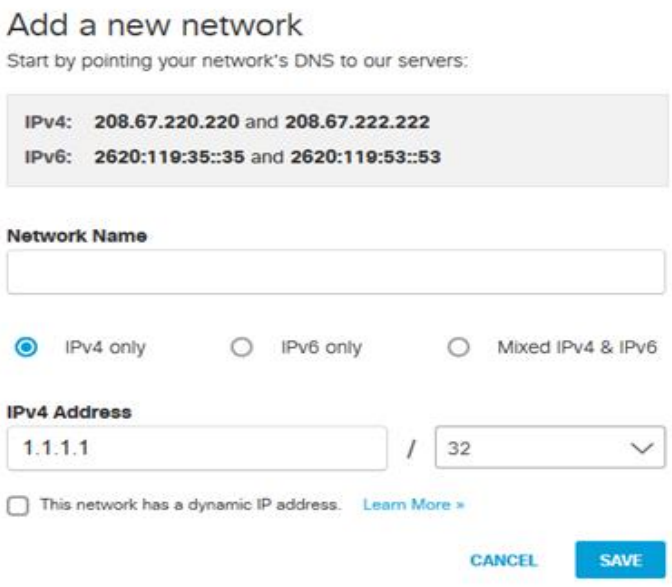


Рис. 3.15. Приклад додавання нової мережі

3. Додати

4. Визначається IPv4-адреса зовнішнього інтерфейсу маршрутизатора ISR (інтерфейс DNS-трафік буде джерелом)
5. Зберегти.

Мережевий тунель:

1. Розгортання > Основні ідентифікатори > Мережеві тунелі;
2. Додати;
3. Необхідно називати тунель відповідно, як вказано на рис.3.2;
4. Обрати тип пристрою зі спадного списку;
5. Натиснули «Зберегти»;
6. Обрати ідентифікатор тунелю;
7. Обрати парольну фразу та підтверджуємо;
8. Натиснути «Зберегти»;
9. Скопіювати ідентифікатор тунелю;
10. Натиснути «Готово».

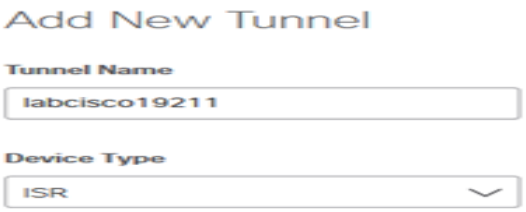


Рис. 3.16. Додаємо новий мережевий тунель

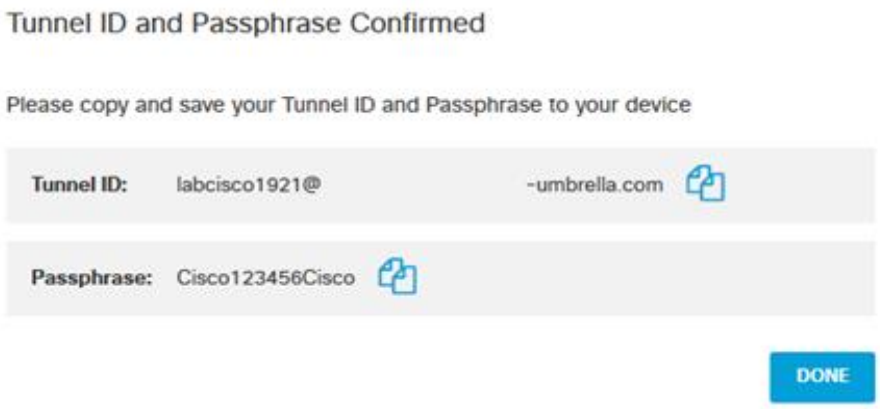


Рис. 3.17. Введення ідентифікатора тунелю та визначення парольної фрази

Списки місць призначення:

1. «Політики» > «Компоненти політики» > «Списки призначення»;

2. Обрати глобальний список блокувань;

3. Визначення тестового домену який буде заблокований, наприклад fox.com;

4. Натиснути «Додати»

5. Натиснути «Зберегти» (Глобальний список блокувань буде ввімкнено за умовчанням у політиці DNS)

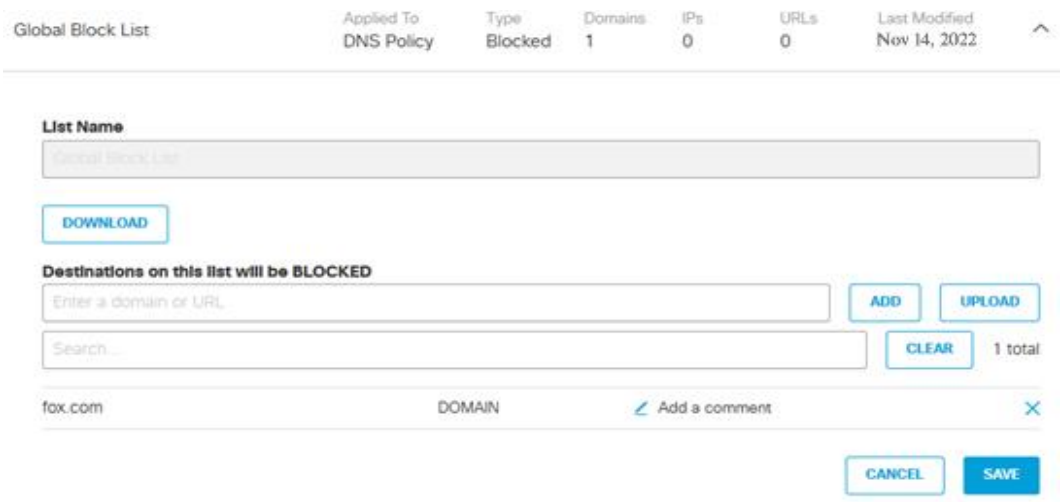


Рис. 3.18. Визначення тестового домену який буде заблокований

Політика брандмауера. Визначення основної політики брандмауера, щоб дозволити індефікувати весь трафік HTTP/HTTPS

1. «Політики» > «Керування» > «Політика брандмауера»;

2. Натиснути «Додати»;

3. Визначати відповідну назву правила, тобто веб-трафік;

4. У списку «Протокол» обирати TCP;

5. У списку «Порти призначення» обрати «Вказати порт» і ввести порти 80, 443;

6. Обрати «Дія правила» та переконатися, що вибрано «Дозволити трафік».

7. Додатково ввімкнути журналювання

8. Натиснути «Зберегти»

2 Total

	Priority	Name	Status	Action	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit	
☐	1	Web Traffic	Enabled	Allow	TCP	Any IPs Any Ports	Any IPs 2 Ports	337.0 /24hrs	Nov 14, 2022 - 04:10pm	···
☐	2	Default Rule	Enabled	Block	Any	Any IPs Any Ports	Any IPs Any Ports	1.5 k/24hrs	Nove 14, 2022 - 04:09pm	···

Рис. 3.19. Визначення основної політики брандмауера

Налаштуваня конфігурації маршрутизатора IKEv2/IPSec

```
crypto ikev2 proposal UMBRELLA_PROPOSAL
 encryption aes-gcm-256 aes-gcm-128
 prf sha256
  group 19 20
!
crypto ikev2 policy UMBRELLA_POLICY
 proposal PROPOSAL
```

Рис. 3.20. Створення пропозиції та політики IKEv2

```
crypto ikev2 keyring UMBRELLA_KEY
 peer UMBRELLA_LONDON
  address 146.112.97.8
  pre-shared-key Cisco123456Cisco
```

Рис. 3.21. Визначення IKEv2

Як зазначено під час налаштування мережевого тунелю на інформаційній панелі Umbrella (CDFW). Вказати однорангову адресу за допомогою списку IP-адрес Umbrella DC.

```
crypto ikev2 profile UMBRELLA
 match identity remote address 146.112.97.8 255.255.255.255
 identity local email labcisco1921@xxxxxxxx-xxxxxxxxxx-umbrella.com
 authentication local pre-share
 authentication remote pre-share
 keyring local UMBRELLA_KEY
 dpd 10 2 periodic
```

Рис. 3.22. Створення профілю IKEv2

Визначення локальної ідентифікації, як визначеної конфігурації мережевого тунелю на інформаційній панелі Umbrella (CDFW).

```
crypto ipsec transform-set UMBRELLA_IPSEC_POLICY esp-gcm 256
 mode tunnel
!
crypto ipsec profile UMBRELLA
 set transform-set UMBRELLA_IPSEC_POLICY
 set ikev2-profile UMBRELLA
```

Рис. 3.23. Створення набору перетворень IPSec

Інтерфейс тунелю

```
interface Tunnel1
 ip unnumbered GigabitEthernet0/0 <WAN INTERFACE>
 tunnel source GigabitEthernet0/0 <WAN INTERFACE>
 tunnel mode ipsec ipv4
 tunnel destination 146.112.97.8
 tunnel protection ipsec profile UMBRELLA
 end
```

Рис. 3.24. Налаштування інтерфейсу тунелю

Спочатку необхідно переконатися, що IP-інтерфейс не має номера, а джерелом тунелю є зовнішній інтерфейс. Вказується пункт призначення тунелю як найближчий DC (той самий DC, який налаштовано в бірці ключів IKEv2).

Трансляція мережевих адрес (NAT)

```
ip access-list extended NAT_ACL
 permit ip 192.168.0.0 0.0.255.255 any
 permit ip 10.0.0.0 0.255.255.255 any
```

Рис. 3.25. Створення розширеного ACL (Access Control List)

Для того, щоб, дозволити весь внутрішній мережевий трафік бути ідентифікованим.

```
ip nat inside source list NAT_ACL interface GigabitEthernet0/0 overload
```

Рис. 3.26. Створення правил NAT (Network Address Translation)

Посилаючись на створений раніше ACL NAT для всього вихідного трафіку NAT.

```
interface GigabitEthernet0/0
 description ---| WAN Interface |---
 ip address 1.1.1.1 255.255.255.0
 ip nat outside
!
interface GigabitEthernet0/1
 description ---| Internal Interface |---
  ip address 192.168.247.1 255.255.255.0
 ip nat inside
```

Рис. 3.27. Налаштування NAT на зовнішньому та внутрішньому інтерфейсах

Маршрутизація. Трафік направляється до VPN (Virtual Private Network) за допомогою маршрутизації на основі політики. Трафік DNS не слід надсилати через

тунель VPN до Umbrella Cloud. Якщо DNS-трафік направляється через тунель, трафік піддаватиметься NAT, і тому DNS-трафік не відповідатиме вихідній IP-адресі організації, а згодом політики DNS не застосовуватися.

```
ip access-list extended UMB_TRAFFIC_ACL
 deny ip any host 208.67.220.220
 deny ip any host 208.67.222.222
 permit ip 192.168.10.0 0.0.0.255 any
 deny ip any any
```

Рис. 3.28. Визначається карта маршруту

При налаштуванні ACL, необхідно переконатися, що DNS-серверам Umbrella заборонено доступ, але дозволено маршрутизацію всього іншого трафіку через Umbrella CDFW.

```
route-map UMB_ROUTE_MAP permit 10
 match ip address UMB_TRAFFIC_ACL
 set interface Tunnel1
```

Рис. 3.29. Налаштування внутрішнього інтерфейсу для використання карти маршруту

Посилаючись на наведений вище ACL, який визначає трафік, який буде направлено до Umbrella CDFW через інтерфейс тунелю.

```
interface GigabitEthernet0/1
 ip policy route-map UMB_ROUTE_MAP
```

Рис. 3.30. Налаштування внутрішнього інтерфейсу для використання карти маршруту

Тестування/перевірка

- Необхідно переконатися, що локальний DNS-сервер використовує DNS-сервери Umbrella Cloud 208.67.220.220 і 208.67.222.222.
- Після всіх налаштуваннь, здійснити спробу зайти на домен FOX.COM або інший домен, який було внесено до глобального списку блокувань.

Рис. 3.31. Спроба зайти на домен FOX.COM

3.4. Рекомендації щодо застосування технології побудови захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewall

Виходячи з аналітики першого розділу та порівняльного аналізу другого розділу, можна виокремити наступні рекомендації:

1. Величезне значення має добре налаштована система реєстрації всіх мережевих запитів, оскільки вона дає змогу адміністратору вчасно ідентифікувати загрозу та вжити відповідних заходів щодо її усунення;

2. Важливо регулярно переглядати журнальні файли за найменшої ознаки вторгнення або спроби злому. Оскільки деякі зловмисники намагатимуться

приховати свої сліди шляхом редагування журнальних файлів, бажано захищати ці файли;

3. Необхідно виділити публічні ресурси в DMZ-зону й обмежити до неї доступ із загальної мережі;

4. Необхідно забезпечити повну сегментацію мережі за допомогою технології VLAN;

5. Необхідно розглянути можливість розгортання мережевих і вузлових систем виявлення вторгнень (IDS) для визначення і повідомлення про атаки в корпоративній мережі;

6. Рекомендується вимкнути широкомовну розсилку SSID у бездротовій мережі та використовувати стійкі алгоритми шифрування;

7. Рекомендується регулярно проводити аудит віддалених користувачів на предмет актуальних оновлень своїх систем;

8. Рекомендується вивчати потоки трафіку і робити автоматичні дії для перехоплення або відкидати небезпечні пакети до того, як вони досягнуть мети стосується адміністраторів;

9. Рекомендується дотримуватися нормативних вимог, щоб забезпечити додатковий рівень виявлення та блокування шкідливого ПЗ, ботнетів, фішингу і т.д.;

10. Припинити використання недозволених SaaS додатків;

11. Зупинити віддалений virtual terminal в інші мережі такі як telnet нестандартний порт 8080;

12. Зупинити передачу файлів такі як FTP через нестандартний порт 1003;

13. Припинити використання забороненого трафіку та заблокувати весь трафік peer to-peer (TOR або BitTorrent);

14. Застосовувати додаткову перевірку за допомогою проксі;

Виконання цих рекомендацій надасть змогу істотно поліпшити безпеку захищеної мережі комерційної організації.

При використанні даного продукту адміністратору необхідно дотримуватися певних правил:

1. Персоналізований адміністративний доступ. Заборонити використання загальних адміністративних облікових записів;

2. Заборона здійснювати регулярні завдання по використанню адміністративних облікових записів. Адміністратори повинні працювати на своїх ПК під стандартними обліковими записами з правами доступу;

3. Заборона використання облікових записів адміністраторів або домену для завдань, не пов'язаних з адмініструванням контролерів доменів;

4. Облікові записи для функціонування різних служб і ПО повинні мати мінімально необхідний рівень прав, достатній для роботи конкретного сервісу;

5. Регулярне навчання та підвищення кваліфікації спеціалістів у цій галузі та адміністраторів даних рішень у сфері сучасних загроз і методів захисту систем, що використовуються в організації;

6. Адміністратор підсистеми безпеки повинен знати, що конфіденційна інформація компанії може бути надіслана співробітником компанії електронною поштою через мережу. Для виявлення таких фактів підсистема безпеки повинна включати засоби моніторингу вмісту електронних повідомлень;

Висновки до третього розділу

Проаналізовано та досліджено вимоги до системи для інсталяції Cisco Umbrella та компонента Cloud Delivered Firewall.

Виконано налаштування програмного продукту Cisco Umbrella та компонента Cloud Delivered Firewall для мінімізації атак на мережеву інфраструктуру.

Виконано налаштування параметрів безпеки на мережевих пристроях за допомогою Umbrella Cloud Delivered Firewall.

Розроблено рекомендації щодо застосування технології побудови захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewall.

Виокремлено правила, яких потрібно дотримуватися при використанні даного продукту адміністратором мережі.

ВИСНОВКИ

В магістерській роботі отримано наступні наукові та науково-практичні результати:

1.Проаналізовано та досліджено вплив атак на комерційні організації, а також висвітлено класифікацію цих атак на мережу та засоби їх протидії.

2.Наведено аналітично-статистичні дані по типам атак, які мають найбільший вплив на комерційні мережі, в результаті чого було виявлено, що найбільших втрат компанії завдає неправильно налаштований брандмауер.

3.Виконано порівняльний аналіз двох хмарних фаєрволів Umbrella Cloud Delivered Firewall та Barracuda CloudGen Firewall.

4.Виокремлено переваги та недоліки у функціоналі між Umbrella Cloud Delivered Firewall та Barracuda CloudGen Firewall.

5.Досліджено та проаналізовано призначення, можливості та функції Umbrella Cloud Delivered Firewall.

6.Проаналізовано та досліджено вимоги до системи для інсталяції Cisco Umbrella та компонента Cloud Delivered Firewall.

7.Виконано налаштування програмного продукту Cisco Umbrella та компонента Cloud Delivered Firewall для мінімізації атак на мережеву інфраструктуру.

8.Виконано налаштування параметрів безпеки на мережевих пристроях за допомогою Umbrella Cloud Delivered Firewall.

9. Розроблено рекомендації щодо застосування технології побудови захищеної мережі комерційної організації із використанням Umbrella Cloud-Delivered Firewall.