ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ РІШЕННЯ CISCO UMBRELLA»

Виконав студент 4 курсу, групи БСД-44
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Головань В.В.
(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.*Розвиток сучасних інформаційних технологій веде до того, що відбувається поступовий перехід до об'єднання автономних комп'ютерів і локальних мереж в єдину мережу. Якщо до недавнього часу подібні мережі створювалися тільки в специфічних і вузьконаправлених цілях, то розвиток Інтернету і аналогічних систем привів до використання глобальних мереж передачі даних в повсякденному житті практично кожної людини. Інтернет спочатку був заснований на відкритих стандартах, які забезпечували простоту зв'язку. Були упущені деякі ключові компоненти захисту, до яких, наприклад, можна віднести контроль віддаленого доступу, таємницю комунікацій і так далі. Необхідність захисту комунікацій викликала бурхливий розвиток технологій захисту мереж.

Об’єкт дослідження–корпоративні мережі.

Предмет дослідження –методи захисту корпоративних мереж.

Мета роботи –розроблення рекомендацій щодо захисту корпоративних мереж за допомогою Cisco Umbrella.

Завдання бакалаврської роботи:

– проаналізувати існуючі вразливості корпоративних мереж;

– визначити наявні уязвимості корпоративних мереж;

– дослідити існуючі засоби боротьби з небезпеками корпоративних мереж;

– виокремити Cisco Umbrella, як дієве рішення для захисту мережі;

– розробити рекомендації щодо застосування Cisco Umbrella.

Методи дослідження –опрацювання технічної літератури за даною темою,аналіз експлуатаційної документації інструментів,порівняльний аналіз сервісів.

Практичне значення одержаних результатів: рекомендації щодо захисту корпоративних мереж за допомогою Cisco Umbrella.

1 АНАЛІЗ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Поняття корпоративної мережі

Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям або користувачам.

Залежно від масштабу підприємства, а також від складності і різноманіття вирішуваних завдань розрізняють мережі відділу, мережі кампусу і корпоративні мережі (термін «корпоративні» в даній класифікації набуває вузького значення — мережу великого підприємства). На рисунку 1.1 продемонстровано загальну схему всіх корпоративних мереж[1].

Рис. 1.1. Схема корпоративної мережі

Будь-яка організація - це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи зв'язані між собою функціонально, тобто вони виконують окремі види робіт в рамках єдиного бізнес

процесу, а також інформаційно, обмінюючись документами, факсами, письмовими і усними розпорядженнями і так далі крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційною, так і функціональною. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися - для урядової установи, банку, промислового підприємства, комерційної фірми і так далі.

Такий загальний погляд на організацію дозволяє сформулювати деякі загальні принципи побудови корпоративних інформаційних систем, тобто інформаційних систем в масштабі всієї організації. Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP. і використовує комунікаційні стандарти Інтернету, а також сервісні застосування, що забезпечують доставку даних користувачам мережі. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків і інших службових документів. Службовці здійснюють доступ до необхідних документів за допомогою засобів (коштів) проглядання Web.

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послугам Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення і звукозаписи), надання необхідних ресурсів по запитах клієнтів Web, а також здійснення доступу до баз даних. У цьому керівництві всі служби публікації називаються службами інтернету, незалежно від того, де вони використовуються (у інтернеті або корпоративній мережі).

Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднуючою офіси, підрозділи і інші структури, що знаходяться на значному віддаленні один від одного. Принципи, по яких будується корпоративна мережа, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні. Для підключення віддалених користувачів до корпоративної мережі найпростішим і найдоступнішим варіантом є використання телефонного зв'язку.

Там, де це можливо, можуть використовуватися мережі ISDN[3]. Для об'єднання вузлів мережі найчастіше використовуються глобальні мережі передачі. Навіть там, де можливе прокладання виділених ліній (наприклад, у межах одного міста) використання технологій пакетної комутації дозволяє зменшити кількість необхідних каналів зв'язку і – що важливо – забезпечити сумісність системи з існуючими глобальними мережами.

Підключення корпоративної мережі до Internet виправдане, якщо вам потрібний доступ до відповідних послуг. У багатьох роботах існує думка з приводу підключення до Internety: Використовувати Internet як середовище передачі даних варто тільки тоді, коли інші способи недоступні та фінансові міркування переважують вимоги надійності та безпеки. Якщо використовувати Internet лише як джерело інформації, краще скористатися технологією з'єднання за запитом (*dial-on-demand*), тобто. таким способом підключення, коли з'єднання з вузлом Internet встановлюється тільки за вашою ініціативою і на потрібний час. Це різко знижує ризик несанкціонованого проникнення у мережу ззовні.

Для передачі даних усередині корпоративної мережі варто використовувати віртуальні канали мереж пакетної комутації. Основні переваги такого підходу - універсальність, гнучкість, безпека.

Багато чого в IT-інфраструктурі змінилося за ці роки. Але щеє багато, чому можна навчитися, вивчаючи моделі, які існують протягом тривалого часу. У цьому випадку трирівнева модель ієрархічного дизайну Cisco може надати величезну інформацію про управління корпоративною мережею. «Трирівнева модель є концептуальною структурою», — каже Cisco. «Це абстрактна картина мережі, схожа на концепцію еталонної моделі взаємозв’язку відкритих систем (OSI).»

Будь-який IT-фахівець, який пройшов складну сертифікацію CiscoCertifiedNetworkAssociate (CCNA), знатиме про трирівневу систему керування мережею компанії. Задовго до того, як віртуалізація, хмарні обчислення та інші технології почали змінювати уявлення людей про IT-інфраструктуру, техніки, знайомі з підходом Cisco, скористалися його логічною організацією. (Для

отримання додаткової інформації про нові способи концептуалізації мереж див. Віртуалізація мережі: нова структура.)

Кінцеві пристрої, такі як робочі станції користувачів, забезпечують трафік до мережі на рівні доступу. Cisco називає це «двері до мережі». Традиційні технології фіксованого зв'язку включають Frame Relay, ISDN і виділені лінії. Рівень розподілу, який іноді називають рівнем агрегації, збирає та контролює потік трафіку, що надходить від рівня доступу, і пересилає його до ядра. Цей середній рівень фільтрує та маршрутизує пакети та обмежує доступ на основі визначених політик. Основний рівень забезпечує високу швидкість передачі даних між основними комутаторами та маршрутизаторами. Ієрархічна модель відображає мультиплексування та демультиплексування протоколів, які розпізнаються в моделі OSI. На рисунку 1.2. представлено сім шарів моделі OSI.

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

452 × 401

Рис.1.2. Модель OSI

Інформація передається від одного рівня до іншого, і кожен рівень реалізує свій власний набір протоколів, щоб зробити таку передачу можливою. Інформаційний потік починається з рівня програми і перетікає від рівня до рівня, поки не досягне останнього фізичного рівня, звідки він досягає місця призначення.

Досягнувши місця призначення, інформація переходить з фізичного рівня на рівень програми, щоб доставити інформацію користувачеві в місце призначення.

У корпоративних умовах центри обробки даних, філії, загальнодоступні та приватні хмари, пристрої Інтернету речей (IoT) і окремі співробітники організації потребують надійних мережевих з'єднань. Ці з'єднання дозволяють підприємствам обмінюватися даними, запускати бізнес-процеси та аналізувати те, що відбувається в мережі — по суті, мережа робить можливим ведення бізнесу.

На відміну від Інтернету, корпоративні мережі не відкриті для будь-кого, хто хоче підключитися. Корпоративні мережі обмежують підключення до певних користувачів, пристроїв і засобів. Вони часто шифрують дані, які передаються через них, використовуючи віртуальні приватні мережі (VPN) або шифрування безпеки транспортного рівня (TLS).

Корпоративна мережа також відрізняється від інших типів мереж через свій масштаб. Звичайна людина може мати доступ до домашньої локальної мережі, яка підключає кілька пристроїв до Інтернету через один маршрутизатор. Але підприємства використовують внутрішні мережі, які з'єднують тисячі пристроїв між собою та з Інтернетом. (Деякі корпоративні мережі достатньо великі та підключені, щоб їм було призначено номер автономної системи або ASN — дізнайтеся більше про ASN.)

Протягом багатьох років основним фокусом корпоративних мереж було підключення всіх і всього до локальних централізованих центрів обробки даних, де зберігалися дані та запускалися програми. Цей доступ забезпечувався шляхом підключення користувачів і пристроїв до локальної мережі в корпоративному офісі. Локальна мережа кожного офісу була з'єднана з іншими офісами через глобальну мережу великого підприємства, яка зазвичай створювалася за допомогою виділених маршрутів багатопротокольної комутації міток (MPLS).

Модель мережі Hub-and-Spoke, трафік через центральний центр обробки даних.

Інфраструктура корпоративної мережі складалася з фізичних пристроїв, підключених один до одного та до персональних комп'ютерів, принтерів і

пристроїв Інтернету речей за допомогою комбінації кабелів Ethernet і сигналів WiFi. Використовувані мережеві пристрої включали:

Маршрутизатори надсилають дані з однієї мережі в іншу, забезпечуючи підключення між мережами та доступ до Інтернету.

Шлюзи забезпечують з'єднання між різними мережами за допомогою кількох протоколів і на кількох рівнях моделі OSI.

Брандмауери обробляють весь трафік, що надходить і виходить з мережі, щоб блокувати потенційні атаки.

Балансувальники навантаження розподіляють мережевий трафік між декількома серверами в центрі обробки даних, щоб уникнути перевантаження сервера (балансувальники навантаження можуть робити те саме для веб-додатків).

VPN-сервери встановлюють і припиняють VPN-з'єднання, щоб забезпечити безпечний доступ до внутрішньої мережі.

Часто підключення до корпоративної мережі вимагає підключення до VPN. VPN зашифрував трафік між користувачем і сервером VPN, після чого користувач міг отримати доступ до внутрішньої локальної мережі.

Корпоративна мережа сьогодні дуже відрізняється від того, як корпоративна мережа працювала лише кілька років тому. Поєднання хмарної міграції та нових викликів безпеці призвело до того, що модель корпоративної мережі, описана вище, не відповідає потребам сучасного бізнесу, навіть якщо вона все ще використовується багатьма організаціями.

Тепер співробітники, швидше за все, підключаються до мережі як всередині, так і поза офісом. Вони підключаються до хмари та локальних центрів обробки даних (модель гібридної хмари) або виключно до хмари. Це робить централізовану мережеву інфраструктуру неефективною, оскільки мережа стає вузьким місцем для трафіку, що надходить до хмари та з неї.

Центр обробки даних стає вузьким місцем для хмарного трафіку. MPLS-з'єднання між дата-центром, офісами, віддаленими користувачами.

Крім того, багато апаратних засобів, описаних вище, тепер доступні як програмне забезпечення або віртуалізовані хмарні служби. Розширення мережі за

допомогою апаратної інфраструктури потребує придбання та активації додаткового обладнання. Але масштабування мережі за допомогою інфраструктури на основі програмного забезпечення (наприклад, SD-WAN) можливе за допомогою недорогого стандартного обладнання замість обладнання певного постачальника. А масштабувати за допомогою хмарної інфраструктури (наприклад, якщо використовується NaaS — див. нижче) так само просто, як придбати більше послуг у хмарного постачальника.

З огляду на всі ці постійні тенденції, ефективна сучасна мережева архітектура підприємства може виглядати приблизно так:

Центр обробки даних стає вузьким місцем для хмарного трафіку. MPLS-з'єднання між дата-центром, офісами, віддаленими користувачами.

Gartner, глобальна дослідницька та консультаційна фірма, ввела термін безпечний доступ до послуг (SASE) для опису цієї нової моделі мережі. У SASE мережеві служби тісно інтегровані зі службами безпеки, і доступ до мережі більше не є централізованим у кількох фізичних місцях.

SASE об’єднує декілька технологій і послуг на одній платформі:

Програмно визначена WAN (SD-WAN): SD-WAN дозволяє використовувати кілька різних методів підключення на додаток до MPLS.

Захищений веб-шлюз (SWG): SWG фільтрує загрози з веб-трафіку незалежно від того, звідки підключаються співробітники.

Брандмауер як послуга (FWaaS): FWaaS — це хмарний брандмауер, який замінює старі апаратні брандмауери, що використовуються в традиційних корпоративних мережах.

Посередник безпеки доступу до хмари (CASB): CASB поєднує кілька функцій безпеки для хмарних програм та інфраструктури.

Доступ до мережі з нульовою довірою (ZTNA): ZTNA запобігає витоку даних, постійно перевіряючи користувачів і пристрої та дозволяючи доступ лише за потреби.

Разом ці технології створюють ефективні сучасні корпоративні мережі. Проте сьогодні більшість підприємств все ще перебувають між старою та новою моделями, тому повне впровадження SASE ринком займе деякий час.

Оскільки багато підприємств все ще частково покладаються на застарілу локальну інфраструктуру, їм потрібно переконатися, що вони впровадили платформу SASE, яка може працювати як із традиційними центрами обробки даних, так і з хмарою.

Незалежно від того, що чекає в майбутьому, IT-фахівці повинні залишатися напоготові, щоб зустрітися з труднощами роботи в корпораціях. Труднощі виникають як у технічному, так і в соціальному середовищі. А зміни є невід'ємною частиною гри в інформаційних технологіях. Будь-хто, хто не вміє справлятися з ударами, адаптуватися до передових технологій або мати справу зі складними людьми, може обірвати кар'єру. З іншого боку, ті, хто демонструє технічний професіоналізм, можуть зайняти собі нішу в підтримці мінливих корпоративних мереж.

1.2 Існуючі загрози для функціонування корпоративних мереж

Вразливість мережі – це слабке місце або недолік у програмному забезпеченні, апаратному забезпеченні чи організаційних процесах, які, якщо їх скомпрометовано загрозою, можуть призвести до порушення безпеки. На рисунку 1.3 продемонстровано основні вразливості, з якими має справу корпоративна мережа[2].

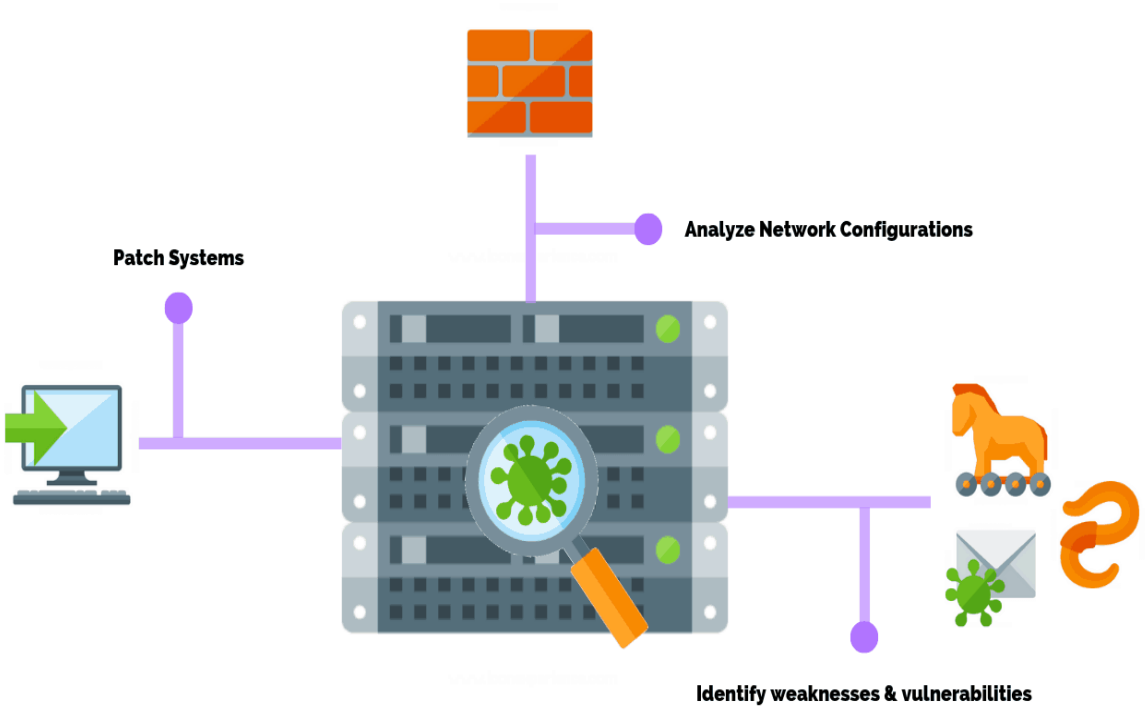

Рис. 1.3. Вразливості мережі

Вразливості мережі можуть поставити під загрозу всю систему. У результаті, конфіденційні дані можуть бути втрачені або, що ще гірше, викрадені кіберзлочинцями. Витік даних може завдати серйозної шкоди репутації вашої компанії та завдати значних фінансових збитків.

Ці вразливості постійно розвиваються. Хакери мають перевірені методи проникнення в, здавалося б, безпечну мережу та використовують різні прийоми, пристрої та інформацію, щоб виконати роботу.

Тому моніторинг внутрішньої мережі та сканування вразливостей є надзвичайно важливими. Важливо також проводити регулярне тестування на проникнення та оцінку вразливості, щоб виявити недоліки IT-безпеки у вашій мережі, операційних системах, брандмауерах і обладнанні.

Уразливості нефізичної мережі пов’язані з даними та програмним забезпеченням. Наприклад, операційні системи, які IT-відділ не оновлює, залишать всю мережу вразливою для загроз. Наприклад, якщо вірус або шкідливе програмне забезпечення завантажується в застарілу операційну систему, воно може заразити всю мережу.

Уразливості фізичної мережі передбачають заходи безпеки для фізичного захисту активу. Ці заходи включають камери безпеки, замикання сервера в шафі-стійці та захист точок входу за допомогою картки-ключа.

Уразливості мережі не тільки класифікуються на фізичні та нефізичні. також визначаються три широкі категорії вразливостей мережевої безпеки: апаратне забезпечення, програмне забезпечення та вразливість людини.

Будь-який пристрій у мережі може бути проблематичним, якщо IT-відділ не знає про цей пристрій і підтримує кожне з них із останніми оновленнями мікропрограми для виправлення помилок і вразливостей.

Уразливості апаратної мережі вимагають захисту всіх ваших пристроїв, маршрутизаторів, серверів та інших ресурсів. Впровадження патчів безпеки та фізичний захист пристроїв від несанкціонованого доступу є першою лінією захисту.

Ноутбуки, смартфони та інші мобільні пристрої найбільш вразливі до крадіжок і порушень безпеки. Крім того, пристрої IoT мають датчики та програмне забезпечення, які дозволяють їм підключатися до системи, мережі чи пристрою та передавати дані через Інтернет. Ці пристрої IoT також потребуватимуть уваги.

Практично кожна мережа використовує програмне забезпечення, здатне запускати різні операційні системи та програми; це програмне забезпечення також вразливе до кібератак.

Найпоширенішими вразливими місцями програм є несправні, некеровані або застарілі програми. Застосування відповідних політик безпеки та використання найновіших програмних рішень може обмежити ризик поширених уразливостей усистемі.

Крім того, конфігурацію програмного забезпечення слід виконувати обережно. Наприклад, замість використання налаштувань за замовчуванням змінюємо ім’я кожного облікового запису адміністратора та обмежуємо доступ працівників до конфіденційних даних.

Зловмисники завжди переслідують найслабшу ланку.Найчастіше найслабшою ланкою є люди, які користуються мережею.Незважаючи на всі спроби

захистити комп’ютерні системи, люди зобов’язані керувати ними, і люди обов’язково припускаються помилок.

Організація вразлива до атак зловмисного програмного забезпечення, рекламного ПЗ, розподіленої системи відмови в обслуговуванні (DDOS) і програм-вимагачів, коли співробітники використовують слабкі паролі, переходять за посиланнями на підозрілі веб-сайти та стають жертвами фішингових атак.Ось чому навчання співробітників має бути головним пріоритетом: щоб усі розуміли важливість захисту безпеки та контролю.

Вразливі місця мережі — це недоліки або слабкі місця в операційних системах, комп’ютерних мережах, апаратному забезпеченні чи інших цифрових процесах, які використовує ваша компанія. Уразливі місця мережі, скомпрометовані кіберзагрозами, можуть призвести до витоку даних. Уразливість мережі — це ненавмисна помилка в проектуванні системи, бізнес-операціях, встановленому програмному забезпеченні та конфігурації мережі.

З іншого боку, мережева атака намагається отримати несанкціонований доступ до мережі компанії з метою викрадення даних або іншої деструктивної поведінки. Воно є навмисним і може бути активним або пасивним.

Уразливості безпеки не були б проблемою, якби не існувало кіберзагроз. Однак кіберзлочинці та хакери можуть використовувати різноманітні тактики та інструменти, щоб зламати ваші системи та використати дані вашої компанії. У широких категоріях є чотири основні типи атак, на які варто звернути увагу:

Атаки шкідливих програм. Зловмисне програмне забезпечення — це скорочення від зловмисного програмного забезпечення, наприклад троянських коней, вірусів і черв’яків, які встановлюються на комп’ютер користувача чи хост-сервер.

Атаки соціальної інженерії. Фішингові атаки та інші методи соціальної інженерії мають на меті змусити користувачів надати інформацію для автентифікації, таку як імена користувачів і паролі. Ця помилка дає поганим акторам доступ до системи.

Невиправлене або застаріле програмне забезпечення. Застарілі версії програмного забезпечення наражають IT-системи (і, можливо, всю мережу) на відомі вразливості.

Неправильно налаштовані брандмауери. Брандмауер є буфером між Інтернетом і внутрішньою мережею, а неправильно налаштований брандмауер може ненавмисно викрити вашу мережу.

Зловмисне програмне забезпечення – це зловмисне програмне забезпечення, яке несвідомо купується, завантажується або встановлюється.

До найпоширеніших типів шкідливих програм належать:

1.Віруси

2.Кейлоггери

3.Черви

4.Трояни

5.програми-вимагачі

6.Логічні бомби

7.Боти/ботнети

8.Рекламне та шпигунське ПЗ

9.Руткіти

10.Зловмисне програмне забезпечення часто розгортається через фішингові електронні листи. Коротше кажучи, зловмисники надсилають співробітникам електронні листи, що містять посилання на веб-сайти, або вкладені файли в самому листі. У разі виконання певної дії, як-от натискання посилання або завантаження вкладеного файлу, зловмисний код виконується, і ви можете вважати себе зламаним.

Вірус є найпоширенішим типом атаки зловмисного програмного забезпечення. Для того, щоб вірус заразив систему, користувачеві потрібно клацнути або скопіювати його на носій або хост. Більшість вірусів саморозмножуються без відома користувача. Ці віруси можуть поширюватися з однієї системи на іншу через електронну пошту, миттєві повідомлення, завантаження з веб-сайтів, знімні носії (USB) і мережеві з’єднання.

Деякі типи файлів більш сприйнятливі до вірусних інфекцій – .doc/docx, .exe, .html, .xls/.xlsx, .zip. Віруси зазвичай залишаються бездіяльними, доки не поширяться в мережі або на кількох пристроях, перш ніж доставити корисне навантаження.

Клавіатурний журнал або захоплення клавіатури реєструє натискання клавіш користувача та надсилає дані зловмиснику. Користувачі зазвичай не знають, що їхні дії контролюються. Хоча є випадки використання роботодавцями клавіатурних шпигунів для відстеження діяльності співробітників, вони здебільшого використовуються для викрадення паролів або конфіденційних даних. Кейлоггери можуть являти собою фізичний дріт, непомітно підключений до периферійного пристрою, як-от клавіатура, або встановлений трояном.

Подібно до вірусу, хробак також може самовідтворюватися та поширювати свої повні копії та сегменти через мережеві з’єднання, вкладення електронної пошти та миттєві повідомлення. Однак, на відміну від вірусів, хробак не потребує хост-програми для роботи, самовідтворення та розповсюдження. Хробаки зазвичай використовуються проти серверів електронної пошти, веб-серверів і серверів баз даних. Після зараження хробаки швидко поширюються через Інтернет і комп’ютерні мережі.

Троянські програми — це зловмисне програмне забезпечення, яке маскується під законне програмне забезпечення. Троянська програма ховатиметься на вашому комп’ютері, доки її не викличуть. Після активації трояни можуть дозволити зловмисникам шпигувати за вами, викрадати ваші конфіденційні дані та отримувати бекдорний доступ до вашої системи.

Трояни зазвичай завантажуються через вкладення електронної пошти, завантаження з веб-сайту та миттєві повідомлення. Тактика соціальної інженерії зазвичай використовується, щоб обманом спонукати користувачів завантажувати та запускати троянські програми в їхніх системах. На відміну від комп'ютерних вірусів і хробаків, трояни не здатні до саморозмноження.

Програми-вимагачі – це різновид зловмисного програмного забезпечення, призначеного для блокування доступу користувачів до їхніх систем або заборони

доступу до даних, доки не буде сплачено викуп. Крипто-зловмисне програмне забезпечення – це тип програм-вимагачів, які шифрують файли користувача та вимагають оплати протягом певного часу та часто через цифрову валюту, як-от біткойн.

Атаки програм-вимагачів можуть мати руйнівний вплив. Наприклад, поточні оцінки атаки програм-вимагачів у Балтіморі становлять до 18 мільйонів доларів США. Подібно до вірусів, хробаків і троянів, програмне забезпечення-вимагач доставляється через вкладення електронної пошти, завантаження з веб-сайту та миттєві повідомлення та поширюється через фішингові електронні листи або заражені веб-сайти. Немає гарантії, що сплата викупу надасть доступ до ваших файлів/даних, а процес відновлення може бути складним і дорогим.

Логічні бомби – це тип зловмисного програмного забезпечення, яке активується, лише коли спрацьовує, наприклад у певну дату/час або під час 25-го входу в обліковий запис. Віруси та хробаки часто містять логічні бомби для доставки свого корисного навантаження (шкідливого коду) у заздалегідь визначений час або коли виконується інша умова.

Шкода, завдана логічними бомбами, варіюється від зміни байтів даних до того, що жорсткі диски стають нечитабельними. Антивірусне програмне забезпечення може виявляти найпоширеніші типи логічних бомб під час їх виконання. Однак, доки вони не зроблять, логічні бомби можуть бездіяльно перебувати в системі тижнями, місяцями чи роками.

Ботнет, скорочення від roBOT NETwork, — це група ботів, які є будь-яким типом комп’ютерної системи, підключеної до мережі, безпеку якої було порушено.

Висновки до першого розділу

Проаналізовано, що корпоративна мережа - це комунікаційна мережа, призначена для використання підприємствами та організаціями. Це дозволяє співробітникам та іншим авторизованим користувачам отримувати доступ до таких ресурсів, як файли, принтери, програми та бази даних з будь-якого місця в мережі.

Досліджено, що безпека корпоративних мереж є критично важливим аспектом, оскільки вони зазвичай зберігають і передають конфіденційну інформацію.

Зазначено, що вони часто мають кілька рівнів заходів безпеки, таких як брандмауери, системи виявлення та запобігання вторгненням, віртуальні приватні мережі (VPN) і шифрування, щоб гарантувати запобігання несанкціонованому доступу та підтримку конфіденційності, цілісності та доступності даних.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ БОРОТЬБИ З ВРАЗЛИВІСТЮ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Дослідження особливостей виявлення вразливостей корпоративних мереж.

Система виявлення вторгнень — це програмний засіб, який використовується для виявлення несанкціонованого доступу до комп'ютерної системи чи мережі. Система виявлення вторгнень здатна виявляти всі типи зловмисного мережевого трафіку та використання комп'ютера. Це включає мережеві атаки на вразливі служби, атаки на програми, керовані даними, атаки на хост, такі як підвищення привілеїв, несанкціонований вхід і доступ до конфіденційних файлів, а також зловмисне програмне забезпечення.

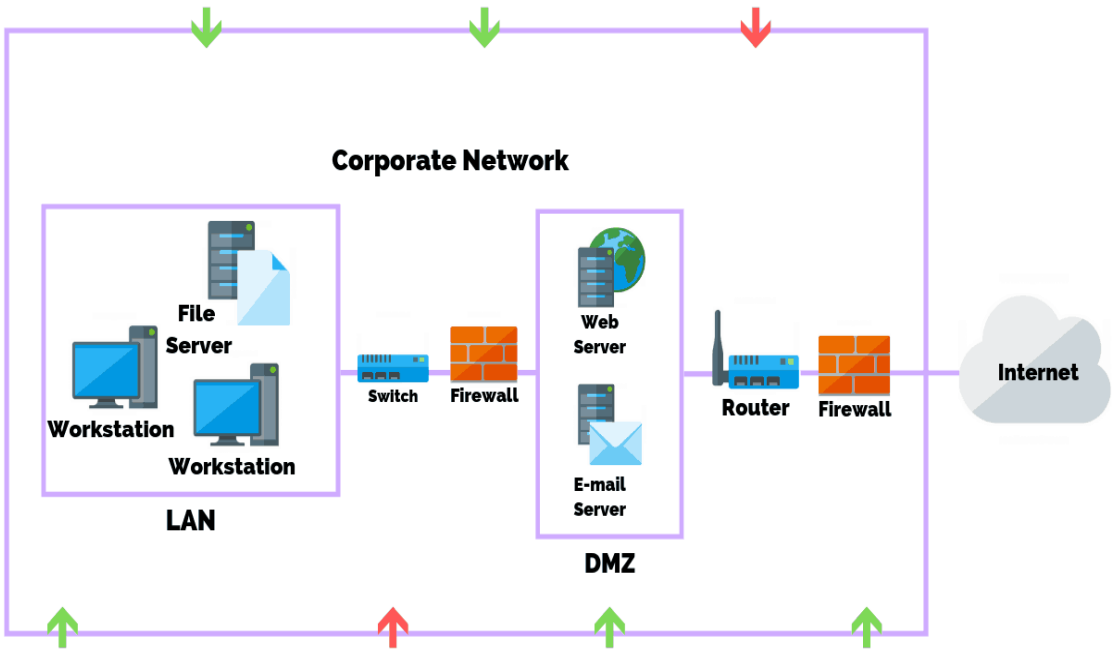

Рис. 2.1. Створення безпеки

За останні двадцять років системи виявлення вторгнень повільно еволюціонували від додатків, призначених для хостів і операційних систем, до

розподілених систем, які включають широкий спектр операційних систем. Перед наступним поколінням систем виявлення вторгнень і, точніше, перед системами виявлення аномалій, постає багато проблем. Перш за все, традиційні системи виявлення вторгнень не адаптувалися належним чином до нових мережевих парадигм, таких як бездротові та мобільні мережі.

Підхід до виявлення аномалій зазвичай складається з двох етапів: етапу навчання та етапу тестування. У першому визначається нормальний профіль трафіку; в останньому вивчений профіль застосовується до нових даних.

Оскільки прогрес у мережевих технологіях допомагає з'єднати віддалені куточки земної кулі та оскільки Інтернет продовжує розширювати свій вплив як засіб комунікації та торгівлі, загроза з боку спамерів, зловмисників і злочинних організацій також зростає відповідно. Саме поширеність таких загроз змусила системи виявлення вторгнень — еквівалент кіберпростору охоронній сигналізації — приєднатися до брандмауерів як однієї з основних технологій безпеки мережі. Проте сучасні комерційно доступні системи виявлення вторгнень – це переважно системи виявлення вторгнень на основі сигнатур, які призначені для виявлення відомих атак за допомогою сигнатур цих атак. Такі системи вимагають частих оновлень бази правил і оновлень сигнатур і не здатні виявляти невідомі атаки. Навпаки, системи виявлення аномалій, підгрупа систем виявлення вторгнень, моделюють нормальну поведінку системи/мережі, що дає їм змогу бути надзвичайно ефективними у пошуку та запобіганні як відомим, так і невідомим атакам або атакам «нульового дня». Хоча системи виявлення аномалій концептуально привабливі, необхідно подолати безліч технологічних проблем, перш ніж вони зможуть бути широко впроваджені. Ці проблеми включають: високий рівень помилкових тривог, неможливість масштабування до гігабітної швидкості тощо. У цій статті ми надаємо комплексний огляд систем виявлення аномалій і гібридних систем виявлення вторгнень нещодавнього минулого та сьогодення. Ми також обговорюємо останні технологічні тенденції у виявленні аномалій та визначаємо відкриті проблеми та виклики в цій галузі.

Сьогодні Інтернет разом із корпоративною мережею відіграє важливу роль у створенні та просуванні нових напрямків бізнесу. Потреби бізнесу спонукали підприємства та уряди в усьому світі розробляти складні інформаційні мережі. Такі мережі включають різноманітний набір технологій, включаючи розподілені системи зберігання даних, методи шифрування та автентифікації, передачу голосу та відео через IP, віддалений і бездротовий доступ, а також веб-сервіси. Крім того, корпоративні мережі стали більш доступними; наприклад, більшість підприємств надають своїм партнерам доступ до своїх послуг у внутрішніх мережах через екстранет, дозволяють клієнтам взаємодіяти з мережею через транзакції електронної комерції та дозволяють співробітникам підключатися до систем компанії через віртуальні приватні мережі. На рисунку 2.2 показана статистика кіберінцидентів останніх років.

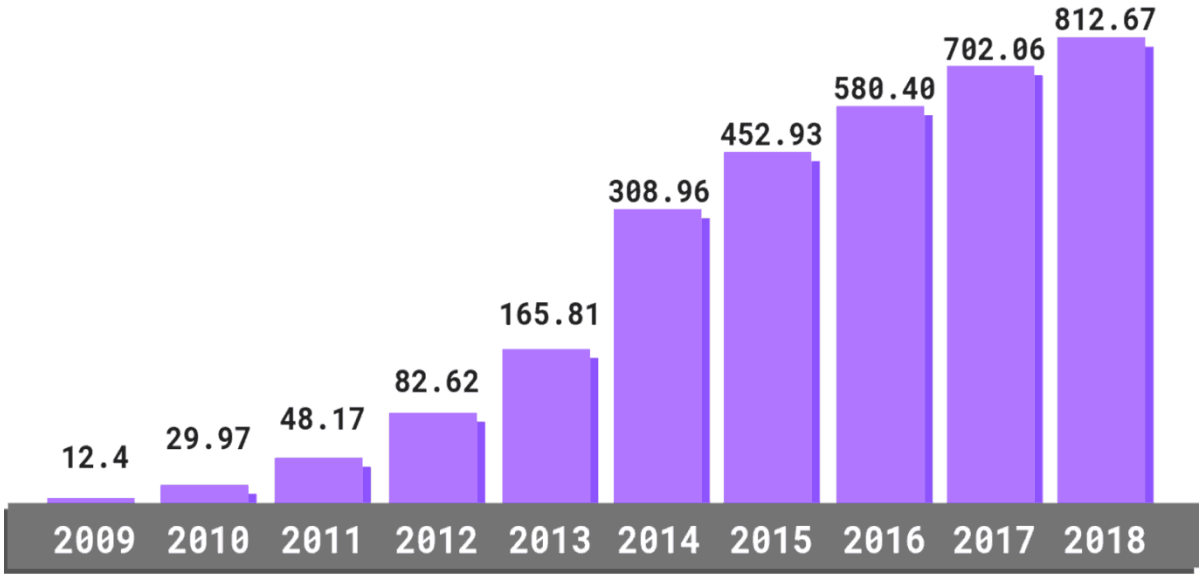

Рис. 2.2. Статистика

Вищезгадані точки доступу роблять сучасні мережі більш уразливими до вторгнень і атак. Кіберзлочин більше не є прерогативою стереотипного хакера. До хакерів приєдналися незадоволені співробітники, неетичні корпорації та навіть терористичні організації. Зважаючи на вразливість сучасного програмного забезпечення та протоколів у поєднанні зі зростаючою складністю атак, не дивно, що мережеві атаки зростають. Щорічне дослідження комп'ютерної злочинності та безпеки за 2005 рік, спільно проведене Інститутом комп'ютерної безпеки та ФБР,

показало, що фінансові збитки, понесені компаніями-респондентами через мережеві атаки/вторгнення, становили 130 мільйонів доларів США. В іншому опитуванні, проведеному на замовлення VanDyke Software у 2003 році, близько 66% компаній заявили, що вважають проникнення в систему найбільшою загрозою для своїх підприємств. Незважаючи на те, що 86% респондентів використовували брандмауери, вони погодилися, що брандмауери самі по собі недостатні для забезпечення належного захисту. Крім того, згідно з останніми дослідженнями, щомісяця виявляється в середньому від двадцяти до сорока нових уразливостей у широко використовуваних мережевих і комп'ютерних продуктах. Такі широко поширені вразливості програмного забезпечення доповнюють сучасне небезпечне обчислювальне/мережне середовище. Це незахищене середовище породило сферу виявлення та запобігання вторгненням, що постійно розвивається. У кіберпросторі еквівалент охоронної сигналізації, системи виявлення вторгнень доповнюють обложений брандмауер.

Система виявлення вторгнень збирає й аналізує інформацію з різних областей комп'ютера чи мережі, щоб виявити можливі порушення безпеки. Іншими словами, виявлення вторгнення – це акт виявлення дій, які намагаються порушити конфіденційність, цілісність або доступність системи/мережі.

Традиційно системи виявлення вторгнень класифікуються як сигнатурні системи виявлення, системи виявлення аномалій або гібридні/комбіновані системи виявлення. Система виявлення сигнатур визначає шаблони трафіку або даних програми, які вважаються зловмисними, тоді як системи виявлення аномалій порівнюють дії з «нормальною» базовою лінією. З іншого боку, гібридна система виявлення вторгнень поєднує методи двох підходів. Системи виявлення сигнатур і виявлення аномалій мають свої переваги та недоліки. Основна перевага сигнатурного виявлення полягає в тому, що відомі атаки можна досить надійно виявляти з низьким рівнем хибних спрацьовувань. Головним недоліком підходу до визначення сигнатур є те, що такі системи зазвичай вимагають визначення підпису для всіх можливих атак, які зловмисник може розпочати проти мережі.

Системи виявлення аномалій мають дві основні переваги перед системами виявлення вторгнень на основі сигнатур. Першою перевагою, яка відрізняє системи виявлення аномалій від систем виявлення сигнатур, є їх здатність виявляти невідомі атаки, а також атаки «нульового дня». Ця перевага пояснюється здатністю систем виявлення аномалій моделювати нормальну роботу системи/мережі та виявляти відхилення від них. Друга перевага систем виявлення аномалій полягає в тому, що вищезазначені профілі нормальної активності налаштовані для кожної системи, програми та/або мережі, і тому зловмиснику дуже важко точно знати, які дії він може виконувати без виявлення. Однак підхід до виявлення аномалій також має свої недоліки. Наприклад, внутрішня складність системи, високий відсоток помилкових тривог і пов’язана з цим складність визначення конкретної події, яка викликала ці тривоги, є одними з багатьох технічних проблем, які необхідно вирішити, перш ніж системи виявлення аномалій можуть бути широко впроваджені.

2.2 Методи та засоби боротьби зі стороннім втручанням до корпоративної мережі

Способи захисту інформації на підприємстві, також як і способи її видобутку, постійно змінюються. Регулярно з'являються нові пропозиції від компаній, що надають послуги із захисту інформації. Панацеї звичайно немає, але є кілька базових кроків побудови захисту інформаційної системи підприємства, на які вам обов'язково потрібно звернути увагу.

Багатьом напевно знайома концепція глибокої захисту від злому інформаційної мережі. Основна її ідея полягає в тому, щоб використовувати кілька рівнів оборони. Це дозволить, як мінімум, мінімізувати збитки, пов'язані з можливим порушенням периметра безпеки інформаційної системи.

Рис. 2.3. Захист мережі

Розглядаючи загальні аспекти комп'ютерної безпеки, а також створимо якийсь чекліст, службовець в якості основи для побудови базової захисту інформаційної системи підприємства.

Основною частиною уникнення загроз безпеці мережі є поділ мережі на зони відповідно до вимог безпеки. Це можна зробити за допомогою підмереж в одній мережі або шляхом створення віртуальних локальних мереж (VLAN)[4], кожна з яких веде себе як окрема мережа. Сегментація обмежує потенційний вплив атаки однією зоною та вимагає від зловмисників вжити спеціальних заходів для проникнення та отримання доступу до інших зон мережі.

Заборона користувачам мережі доступ до Інтернету без прапорців. Передача всіх запититів через прозорий проксі та використання його для контролю та моніторингу поведінки користувачів. Переконайтеся, що вихідні з’єднання дійсно виконує людина, а не бот чи інший автоматизований механізм. Білий список

доменів, щоб корпоративні користувачі мали доступ лише до веб-сайтів, які ви явно схвалили.

Розміщення брандмауера на кожному з'єднанні мережевих зон, а не лише на краю мережі. Якщо немає можливості скрізь розгорнути повноцінні брандмауери, скористайтеся вбудованою функцією брандмауера своїх комутаторів і маршрутизаторів. Розгорніть пристрої для захисту від DDoS або хмарні служби на межі мережі. Ретельно подумайте, де розмістити стратегічні пристрої, як-от балансувальники навантаження – якщо вони знаходяться за межами демілітаризованої зони (DMZ), вони не будуть захищені вашим пристроєм безпеки мережі.

Трансляція мережевих адрес (NAT) дозволяє переводити внутрішні IP-адреси в адреси, доступні в загальнодоступних мережах. Ви можете використовувати його для підключення кількох комп'ютерів до Інтернету за допомогою однієї IP-адреси. Це забезпечує додатковий рівень безпеки, оскільки будь-який вхідний або вихідний трафік має проходити через пристрій NAT, а IP-адрес менше, через що зловмисникам важко зрозуміти, до якого хоста вони підключаються.

Переконайтеся, що у вас є повна видимість вхідного, вихідного та внутрішнього мережевого трафіку з можливістю автоматичного виявлення загроз і розуміння їх контексту та впливу. Поєднуйте дані з різних інструментів безпеки, щоб отримати чітку картину того, що відбувається в мережі, усвідомлюючи, що багато атак охоплюють кілька IT-систем, облікових записів користувачів і векторів загроз.

Жодні заходи захисту мережі не є 100% успішними, і зловмисникам врешті-решт вдасться проникнути у вашу мережу. Визнайте це та запровадьте технологію обману, яка створює приманки у вашій мережі, спокушаючи зловмисників «напасти» на них і дозволяючи вам спостерігати за їхніми планами та техніками. Ви можете використовувати приманки для виявлення загроз на всіх етапах життєвого циклу атаки: файли даних, облікові дані та мережеві з'єднання.

Брандмауер або файрвол - це перша лінія оборони, яка зустрічає непрошених гостей.

У найпростішому випадку фільтрація мережевих пакетів відбувається відповідно до встановлених правил, тобто на основі адрес джерела і призначення мережевих пакетів, номерів мережевих портів;

Брєндмауери, що працює на сеансовому рівні (stateful). Він відстежує активні сполуки і відкидає підроблені пакети, що порушують специфікації TCP / IP;

Файрвол, що працює на прикладному рівні. Виробляє фільтрацію на основі аналізу даних програми, що передаються всередині пакету.

Підвищена увага до мережевої безпеки і розвиток електронної комерції призвело до того, що все більше число користувачів використовують для свого захисту шифрування з'єднань (SSL, VPN). Це досить сильно ускладнює аналіз трафіку проходить через міжмережеві екрани. Як можна здогадатися, тими ж технологіями користуються розробники шкідливого програмного забезпечення. Віруси, які використовують шифрування трафіку, стали практично не відрізняються від легального трафіку користувачів.

Ситуації, коли співробітнику необхідний доступ до ресурсів компанії з громадських місць (Wi-Fi в аеропорту або готелі) або з дому (домашню мережу співробітників не контролюють ваші адміністратори), особливо небезпечні для корпоративної інформації. Для їх захисту просто необхідно використовувати шифровані тунелі VPN. Ні про який доступ до віддаленого робочого столу (RDP) безпосередньо не використовує шифрування даних не може бути й мови. Це ж стосується використання стороннього ПЗ: Teamviewer, Aammy Admin і т.д. для доступу до робочої мережі. Трафік через ці програми шифрується, але проходить через непідконтрольні вам сервера розробників цього ПО.

До недоліків VPN можна віднести відносну складність розгортання, додаткові витрати на ключі аутентифікації і збільшення пропускної здатності інтернет каналу. Ключі аутентифікації також можуть бути скомпрометовані. Вкрадені мобільні пристрої компанії або співробітників (ноутбуки, планшети, смартфони) з попередньо налаштованими параметрами підключення VPN можуть стати потенційною діркою для несанкціонованого доступу до ресурсів компанії.

Система виявлення вторгнень (IDS - англ .: Intrusion Detection System) - програмне або апаратне засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (Мережа), або несанкціонованого управління такою системою. У найпростішому випадку така система допомагає виявити сканування мережевих портів вашої системи або спроби увійти на сервер. У першому випадку це вказує на первинну розвідку зловмисником, а в другому спроби злому вашого сервера. Також можна виявити атаки, спрямовані на підвищення привілеїв в системі, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення. Просунуті мережеві комутатори дозволяють підключити систему виявлення вторгнень, використовуючи віддзеркалення портів, або через ответвители трафіку.

Система запобігання вторгнень (IPS - англ .: Intrusion Prevention System) - програмні або апаратна система забезпечення безпеки, активно блокує вторгнення в міру їх виявлення. У разі виявлення вторгнення, підозрілий мережевий трафік може бути автоматично перекритий, а повідомлення про це негайно відправлено адміністратору.

Антивірусне програмне забезпечення є основним рубежем захисту для більшості сучасних підприємств. За даними дослідницької компанії Gartner, обсяг ринку антивірусного ПО за підсумками 2012 року склав $ 19,14 млрд. Основні споживачі - сегмент середнього і малого бізнесу.

Перш за все антивірусний захист націлена на клієнтські пристрої та робочі станції. Бізнес-версії антивірусів включають функції централізованого управління для передачі оновлень антивірусних баз клієнтські пристрої, а також можливість централізованої настройки політики безпеки. В асортименті антивірусних компаній присутні спеціалізовані рішення для серверів.
З огляду на те, що більшість заражень шкідливим ПО відбувається в результаті дій користувача, антивірусні пакети пропонують комплексні варіанти захисту. Наприклад, захист програм електронної пошти, чатів, перевірку відвідуваних користувачами сайтів. Крім того, антивірусні пакети все частіше включають в себе

програмний брандмауер, механізми проактивного захисту, а також механізми фільтрації спаму.

Існують два основні підходи до інформаційної безпеки. Перший підхід передбачає, що в операційній системі за замовчуванням дозволено запуск будь-яких додатків, якщо вони раніше не внесені до чорного списку. Другий підхід, навпаки, передбачає, що дозволений запуск тільки тих програм, які заздалегідь були внесені до білого списку, а всі інші програми за замовчуванням блокуються. Другий підхід до безпеки звичайно більш кращий в корпоративному світі. Білі списки можна створити, як за допомогою вбудованих засобів операційної системи, так і за допомогою стороннього ПО. Антивірусне ПЗ часто пропонує дану функцію в своєму складі. Більшість антивірусних програм, що пропонують фільтрацію по білому списку, дозволяють провести первинне налаштування дуже швидко, з мінімальним увагою з боку користувача.

Проте, можуть виникнути ситуації, в яких залежно файлів програми з білого списку були правильно визначені вами або антивірусним ПЗ. Це призведе до збоїв програми або до неправильної його установці. Крім того, білі списки безсилі проти атак, що використовують уразливості обробки документів програмами з білого списку. Також слід звернути увагу на найслабша ланка в будь-якому захисті: самі співробітники в поспіху можуть проігнорувати попередження антивірусного ПО і додати в білий список шкідливе програмне забезпечення.

Спам розсилки часто застосовуються для проведення фішинг атак, що використовуються для впровадження троянця або іншого шкідливий в корпоративну мережу. Користувачі, які щодня обробляють велику кількість електронної пошти, більш сприйнятливі до фішинг-повідомленнями. Тому завдання IT-відділу компанії - відфільтрувати максимальну кількість спаму із загального потоку електронної пошти.

Своєчасне оновлення програмного забезпечення і застосування актуальних латочок безпеки - важливий елемент захисту корпоративної мережі від несанкціонованого доступу. Виробники ПЗ, як правило, не надають повну інформацію про нову знайденої дірі в безпеці. Однак зловмисникам вистачає і

загального опису уразливості, щоб буквально за пару годин після публікації опису нової дірки і латки до неї, написати програмне забезпечення для експлуатації цієї уразливості.

Насправді це досить велика проблема для підприємств малого та середнього бізнесу, оскільки зазвичай використовується широкий спектр програмних продуктів різних виробників. Часто оновлень всього парку ПО не приділяється належної уваги, а це практично відкрите вікно в системі безпеки підприємства. В даний час велика кількість ПО самостійно оновлюється з серверів виробника і це знімає частину проблеми. Тому що сервера виробника можуть бути зламані і, під виглядом легальних оновлень, ви отримаєте свіже шкідливе ПЗ. А також і самі виробники часом випускають оновлення, що порушують нормальну роботу свого ПО. На критично важливих ділянках бізнесу це неприпустимо. Для запобігання подібних інцидентів все одержувані поновлення, по-перше, повинні бути застосовані відразу після їх випуску, по-друге, перед застосуванням вони обов'язково повинні бути ретельно протестовані.

Фізична безпека корпоративної мережі є одним з найважливіших факторів, який складно переоцінити. Маючи фізичний доступ до мережних пристроїв зловмисник, в більшості випадків, легко отримає доступ до вашої мережі. Наприклад, якщо є фізичний доступ до комутатора і в мережі не проводиться фільтрація MAC-адрес. Хоча і фільтрація MAC в цьому випадку вас не врятує. Ще однією проблемою є крадіжка або недбале ставлення до жорстких дисків після заміни в сервері або іншому пристрої. З огляду на те, що знайдені там паролі можуть бути розшифровані, серверні шафи і кімнати або ящики з обладнанням повинні бути завжди надійно захищені від проникнення сторонніх.

Це лише деякі з найбільш поширених аспектів безпеки. Важливо також звернути увагу на навчання користувачів, періодичний незалежний аудит інформаційної безпеки, створення і дотримання надійної політики інформаційної безпеки.

Захист корпоративної мережі є досить складною темою, яка постійно змінюється. Ви повинні бути впевнені, що компанія не залежить лише від одного-

двох рубежів захисту. Завжди прагніть стежити за актуальною інформацією і свіжими рішеннями на ринку інформаційної безпеки.

Висновки до другого розділу

Проаналізовано, що захист корпоративних мереж має важливе значення для захисту цінних цифрових активів організації та конфіденційної інформації від різних загроз безпеці, які можуть завдати шкоди репутації організації, фінансовій стабільності та навіть юридичним зобов’язанням.

Досліджено, чому важливо захищати корпоративні мережі. Зазначено, що захист корпоративних мереж має вирішальне значення для забезпечення безпеки, відповідності та безперервності діяльності організації, а також захисту її репутації та активів.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ТА ВПРОВАДЖЕННЯ CISCO UMBRELLA ДЛЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Загальна інформація про Cisco UMBRELLA

CiscoUmbrella[7] – це хмарна платформа, завдяки якій щодня більше 100 мільйонів користувачів підключаються до Інтернету за найзахищенішим, надійним та швидким каналам. До складу Umbrella входять міжмережевий екран, захищений веб-шлюз, система захисту на рівні DNS,[6] брокер безпечного доступу до хмари (CASB) та рішення для аналізу загроз. З таким пакетом коштів захистити свою мережу від різних загроз зможе організація будь-якого розміру. Сьогодні багато компанії вибирають прямий доступ до Інтернету, і Umbrella дозволяє їм легко розширити периметр захисту для охоплення віддалених користувачів та філій.

Посилення захисту завдяки більш докладній аналітиці У систему Umbrella завантажуються аналітичні звіти CiscoTalos, однієї з найбільших у світі комерційних організацій з аналізу загроз, де працюють понад 300 дослідників. Завдяки цим даним Umbrella під час атак виявляє і блокує безліч шкідливих доменів, IP та URL-адрес, а також файлів. Крім того, аналізуються величезні обсяги інформації про активність у мережі Інтернет, перетворюючи їх на статистичні моделі та алгоритми машинного навчання, тому Umbrella дозволяє виявляти і нові, тільки атаки, що готуються.

Просте блокування шкідливого ПЗ Інтернет-протоколи є однією з базових складових Umbrella, і щодня рішення обробляє 180 мільярдів інтернет-запитів від більш ніж 18500 організацій. Завдяки реалізації захисту на рівні DNS та IP-адрес Umbrella блокує запити до шкідливого ПЗ, програм здирників, фішингових програм та ботнетів до ще установки підключення, запобігаючи загрозам до того, як вони досягнуть мережі або кінцевих пристроїв. Захищений та розгорнутий у хмарі веб-шлюз реєструє та аналізує весь веб-трафік, що гарантує прозорість, контроль над інцидентами та захист.

Хмарний міжмережевий екран дозволяє записувати та блокувати трафік з використанням узгоджених правил для IP-адрес,[8] портів і протоколів у масштабі всього середовища. Швидше та точніше реагування на інциденти Umbrella класифікує активність у мережі Інтернет та зберігає все необхідні дані, щоб спростити вивчення інцидентів та прискорити реагування ними. Завдяки використанню консолі UmbrellaInvestigate та API-інтерфейсу для запиту додаткових відомостей ви можете у будь-який момент переглянути аналітику (історію та контекст), а потім визначити важливість інциденту та швидше обробити його. Наше рішення легко інтегрується з іншими джерелами аналітичних даних та засобами оркестрації захисту, що підвищує ефективність управління.

3.2 Переваги та основні принципи захисту мережі

Безпека, яка забезпечується із самого інтернету Система доменних імен (DNS) – базовий компонент Інтернету, який зіставляє доменні імена з IP-адресами. Коли користувач переходить за посиланням або вводить URL-адресу, запит DNS ініціює підключення пристрою до Інтернету. Umbrella використовує DNS як один із головних механізмів для передачі трафіку на хмарну платформу, а також для застосування політик безпеки. Отримавши DNS-запит, Umbrella оцінює його на основі даних аналітики як безпечний, шкідливий або пов'язаний із ризиком (коли домен містить і шкідливий, і легітимний контент). Безпечні запити передаються зазвичай, шкідливі блокуються, а пов'язані з ризиком перенаправляються на хмарний проксі-сервер для поглибленого аналізу. Проксі-сервер Umbrella використовує дані CiscoTalos про репутацію веб-ресурсів та інші сторонні канали для перевірки URL-адреси. За допомогою антивірусних систем та рішення Cisco[9] для захисту від складного шкідливого програмного забезпечення (AMP) проксі-сервер також аналізує файли, які користувачі намагалися завантажити з сумнівних веб-сайтів. За результатами аналізу підключення дозволяється чи блокується.

Глобальна мережа Umbrella, на основі якої побудовано службу рекурсивних DNS- запитів, щодня обробляє мільярди інтернет-запитів від мільйонів

користувачів по всьому світу. Cisco аналізує цей величезний обсяг даних, щоб виявити шаблони та виявити інфраструктуру зловмисників. Всі дані про інтернет-трафік у режимі реального часу передаються в графову базу даних і потім безперервно пропускаються через моделі на основі статистичних методів та машинного навчання. Цю інформацію також постійно вивчають аналітики безпеки Umbrella, доповнюючи її відомостями від групи CiscoTalos. Успішно поєднуючи досвід фахівців Cisco з машинним навчанням, Umbrella виявляє шкідливі сайти (домени, IP-адреси або URL-адреси) по всьому Інтернету.

Сумісність з іншими рішеннями Umbrella інтегрується з існуючим стеком рішень безпеки, включаючи пристрої захисту, аналітичні платформи та брокери безпечного доступу до хмарної інфраструктури (CASB, CloudAccessSecurityBroker). Umbrella може передавати дані журналів про інтернет-трафіку до систем управління подіями та даними безпеки (SIEM) або системи управління журналами. Використовуючи API-інтерфейс, можна запрограмувати відправлення шкідливих доменів до Umbrella для блокування. Це дозволяє посилити наявні засоби забезпечення безпеки та легко розширити комплексний захист. Розгортання у всій організації за лічені хвилини Umbrella - найшвидший і найпростіший спосіб забезпечити безпеку всіх користувачів за лічені хвилини. Так як це хмарне рішення, не потрібно встановлювати жодне обладнання та вручну оновлювати програмне забезпечення. Для того щоб швидко ініціалізувати всі пристрої всередині мережі, включаючи особисті пристрої співробітників та пристрої Інтернету речей, та використовувати існуючі рішення Cisco – AnyConnect, маршрутизатори з інтегрованими сервісами (ISR) серії 4000 та контролери бездротових локальних мереж моделей 5520 та 8540 – для оперативної підготовки тисяч пристроїв , що залишають мережу, та ноутбуків у роумінгу. Переваги: Зниження витрат на відновлення та шкоди внаслідок порушення безпеки. Оскільки CiscoUmbrella — це перша лінія оборони, скорочується кількість заражень шкідливим програмним забезпеченням, що потребують усунення, і загрози вдається нейтралізувати до того, як вони завдадуть шкоди. Прискорення виявлення та стримування загроз. CiscoUmbrella блокує зворотні дзвінки командних серверів

через будь-який порт і протокол і надає звіти про ці дії в режимі реального часу. Покращення моніторингу інтернет-трафіку для всіх користувачів у будь-якій точці. CiscoUmbrella забезпечує моніторинг, необхідний для оперативного реагування на інциденти, і дає впевненість у повному контролі над обстановкою. Виявлення хмарних програм, що використовуються в компанії. CiscoUmbrella[10] дозволяє контролювати дозволені та нерозв'язані хмарні сервіси, що використовуються на підприємстві: можна зрозуміти, які нові сервіси та ким використовуються, а також пов'язаний з цим потенційний ризик.

Відправна точка – величезний масив різнорідних даних. У 2006 році компанія Cisco[11] почала створювати найбільшу у світі мережу інтернет-безпеки для накопичення глобальних аналітичних даних. На сьогоднішній день понад 65 мільйонів активних користувачів із більш ніж 160 країн щодня направляють свій DNS-трафік до глобальної мережі Cisco. Це дозволяє відстежувати понад 100 мільярдів інтернет-запитів на день. Крім того, понад 500 пірінг-партнерів обмінюються із CiscoBGP-маршрутами. В результаті виходить повна картина зв'язків та відносин між різними мережами в Інтернеті. Цей величезний масив різноманітних даних забезпечує безпрецедентний огляд всього Інтернету.

Застосування статистичних моделей. Щоб виявляти шаблони та виявляти аномалії даних, були розроблені статистичні моделі для категоризації та оцінки. Декілька прикладів перераховано нижче: Багато моделей аналізують просторові відносини. Приклад – графічне відображення відносин між мережами в Інтернеті; Деякі моделі аналізують часові відносини. Приклад - виявлення причинно-наслідкового зв'язку переходу між доменами в результаті послідовних DNS-запитів, які багаторазово надсилають тисячі користувачів за короткі інтервали часу; Інші моделі аналізують статистичні відхилення від нормальної активності. Приклад - оцінка географічного розподілу IP-мереж, які запитують доменне ім'я;

Використовуючи обробку природної мови, модель NLPRank виявляє фішингові домени, які імітують фірмові найменування, аналізуючи їхню лексичну структуру та розташування в Інтернеті. Використання досвіду та знань фахівців. Перелічені моделі створені та налагоджені групою CiscoUmbrella, до якої входять

фахівці з обробки та аналізу даних, інженери, математики та аналітики з інформаційної безпеки. За допомогою 3D-візуалізації, численних методів інтелектуального аналізу даних та експертних знань у галузі інформаційної безпеки аналітики Umbrella удосконалюють моделі та додають додатковий контекст до результатів їх застосування. Фахівці постійно знаходять нові способи аналізу даних для виявлення нових взаємозв'язків та шаблонів. Результат: прогнозна аналітика. Результати цього аналізу дозволяють нам точно виявляти шкідливі домени, IP-адреси, мережі та хеш-суми файлів в Інтернеті та навіть прогнозувати джерела майбутніх атак. Варіанти використання Investigate

Веб-консоль забезпечує доступ до всієї аналітики в режимі реального часу та можливість інтерактивної комбінації різних елементів даних під час розслідування. В Investigate можна створити запит на точні збіги доменних імен, IP-адрес, адрес електронної пошти, номерів ASN і хеш-сум файлів або використовувати пошук за шаблоном, формуючи гнучкіші запити певних термінів, фірмових найменувань, зразків та неточних збігів. RESTAPI-інтерфейс. Investigate надає доступ до API-інтерфейсу для передачі контекстних даних у систему управління подіями та даними безпеки, платформу аналітики загроз або процес обробки інцидентів. Це прискорює виявлення серйозних безпекових порушень. Можливості продукту: Зв'язування атак з певними доменами, IP-адресами, номерами ASN[12] та шкідливим програмним забезпеченням для визначення плану інфраструктури зловмисників; Відображення підозрілих піків у кількості глобальних DNS-запитів до певного домену; Прогнозування джерел майбутніх атак шляхом виявлення доменів та IP-адрес, пов'язаних із шкідливим ПЗ; Дослідження поведінкових індикаторів та мережевих підключень зразків шкідливого програмного забезпечення з використанням даних від CiscoAMPThreatGrid; використання даних WHOIS для визначення власників доменів та виявлення шкідливих доменів, зареєстрованих з однаковими контактними даними; застосування системи оцінки ризику до різних атрибутів доменів з метою виявити серед них підозрілі; Виявлення доменів, які використовують FastFlux, та доменів, створених за допомогою

алгоритмів генерації доменних імен; Доступ до найбільшої пасивної бази даних DNS та WHOIS для перегляду ретроспективних даних про домени.

3.3 Впровадження Cisco Umbrella для захисту від можливих загроз

Клієнт роумінгу Umbrella[13] — це дуже легкий DNS-клієнт, який працює на комп'ютерах Windows або macOS. Це не клієнт VPN або локальний антивірусний механізм, він дозволяє застосовувати безпеку Umbrella та захист на основі політики, включаючи інтелектуальний проксі. Umbrella забезпечує дотримання правил, що були встановленні. Він включає в себе можливість надавати деталізовану політику застосування та повідомляти інформацію про особу конкретного комп'ютера або навіть користувача Active Directory, який увійшов у систему.

У Windows роумінговий клієнт Umbrella прив'язується до 127.0.0.1:53 (localhost для IPv4) і [::1]:53 (localhost для IPv6) і встановлюється як ексклюзивний DNS-сервер для кожного мережевого підключення на комп'ютері, гарантуючи, що всі DNS запити відносяться до близьколежачого центру обробки даних Umbrella, при цьому витончено обробляючи ресурси локальної мережі за допомогою внутрішніх доменів. Для macOS роумінговий клієнт Umbrella прив'язується лише до 127.0.0.1:53 (localhost для IPv4).

DNS-запити, надіслані через Umbrella, шифруються, автентифікуються та перевіряються, щоб забезпечити безпеку та фільтрацію вмісту, що диктується адміністратором вашої організації. Якщо комп'ютер ставить до того, що його Umbrella або ваша організація-адміністратор вважає небезпечним, браузер комп'ютера може бути включений у безпечній блоковій сторінці.

Варіанти гарантій безпеки, що забезпечується Umbrella[14], рис 3.1:

1.Захищений рекурсивний DNS;

2.Веб-проксі з можливістю надсилання підозрілих файлів на аналіз до пісочниці;

3.L3/L4/L7 міжмережевий екран (Cloud Delivery Firewall);

4.Cloud Access Security Broker (CASB);

5.Інструмент для проведення розслідувань.

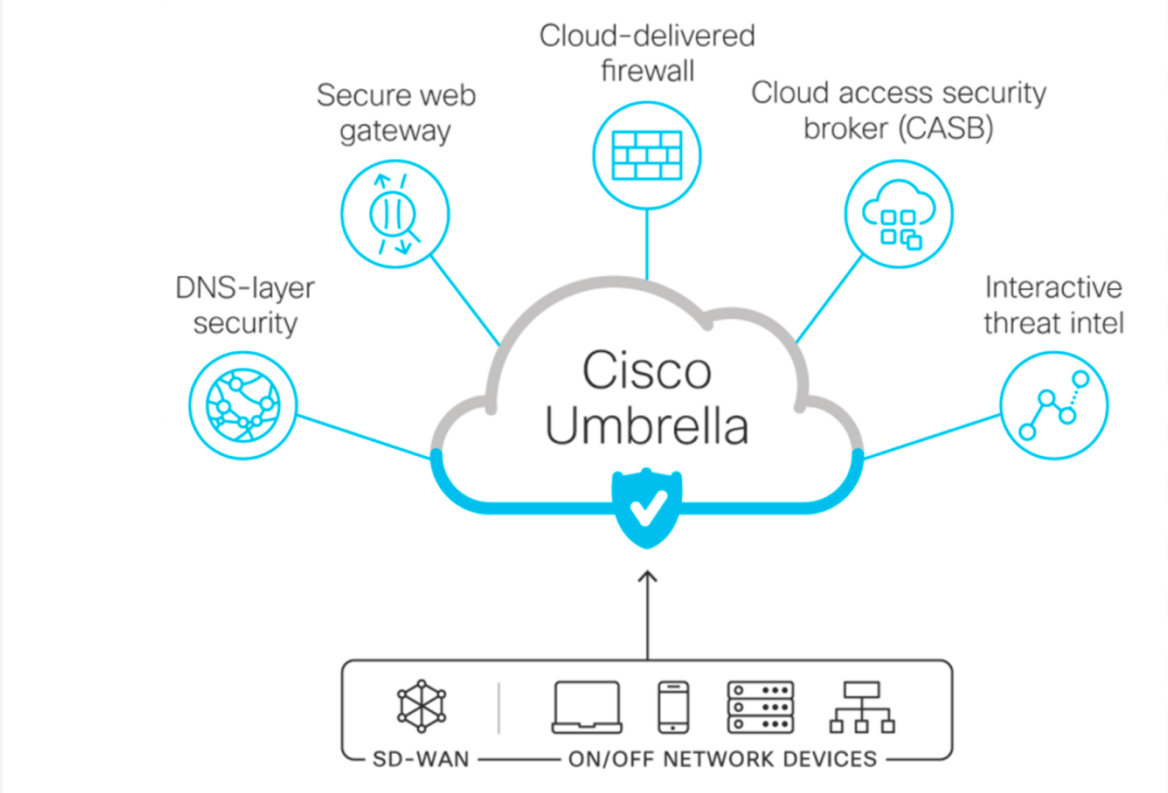

Рис. 3.1. Види захисту

Захищений рекурсивний DNS рис.3.2. Коли ми намагаємося потрапити на якийсь ресурс по домену, незалежно від протоколу, ми резолвуємо доменне ім'я, тобто перетворимо 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 DNS-запиту. Cisco Umbrella у разі виступає як хмарний рекурсивний DNS. 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).

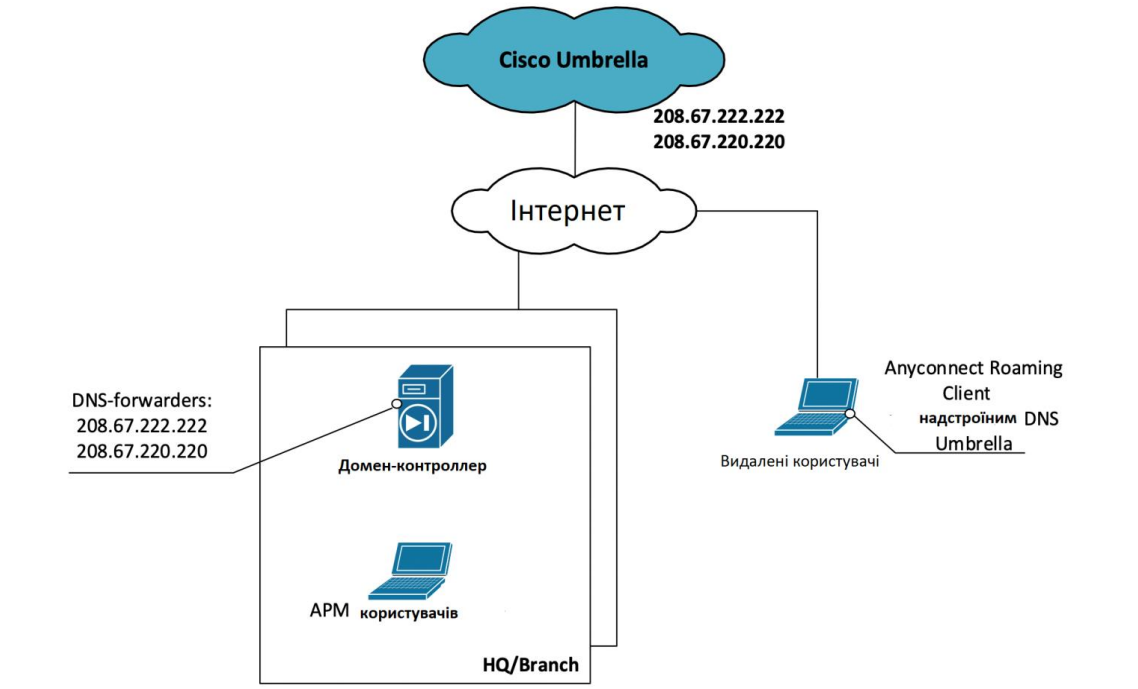

Рис. 3.2. Рекурсивний DNS

Політика за умовчанням та її основні компоненти. Ось так виглядає основне меню налаштування політики за промовчанням (рис.3.3).

Також передбачего велику кількість інших політик, які встанувлюються індивідуально, рис 3.4.

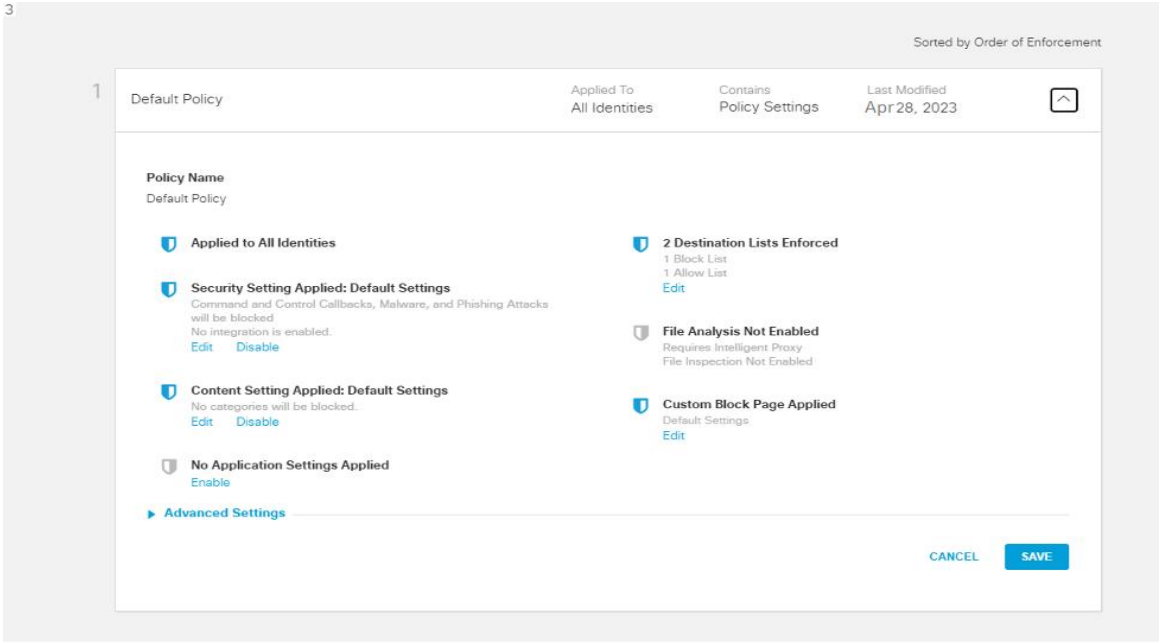

Рис. 3.3. Базова сторінка

Applied to All Identities означає, що політика застосовується до всіх, хто надсилає запити через Umbrella (у межах організації). Якщо робити власну політику, можна вказати багато різних типів, до чого її застосовувати: ID групи користувачів, Roaming Computers, IP-адреси та ін.

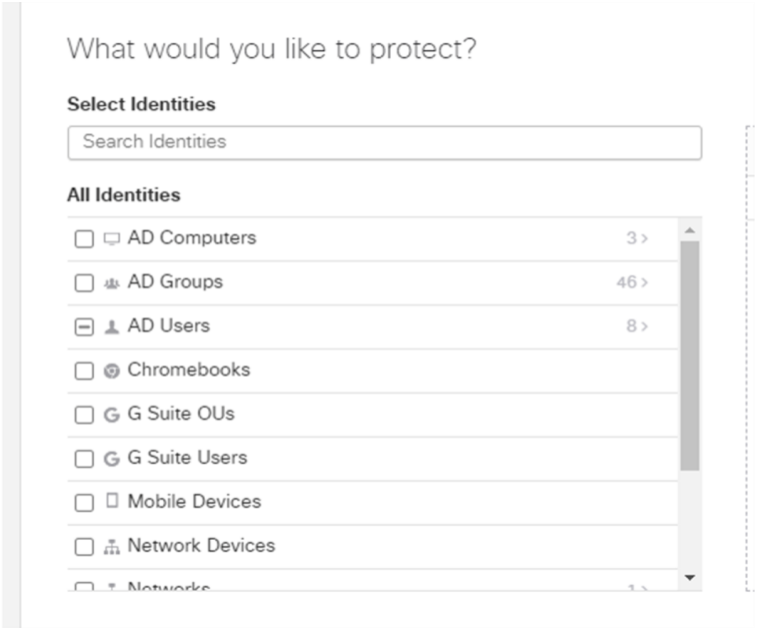

Рис.3.4. Види політик

Security Setting Applied означає блоковані категорії рис 3.5:

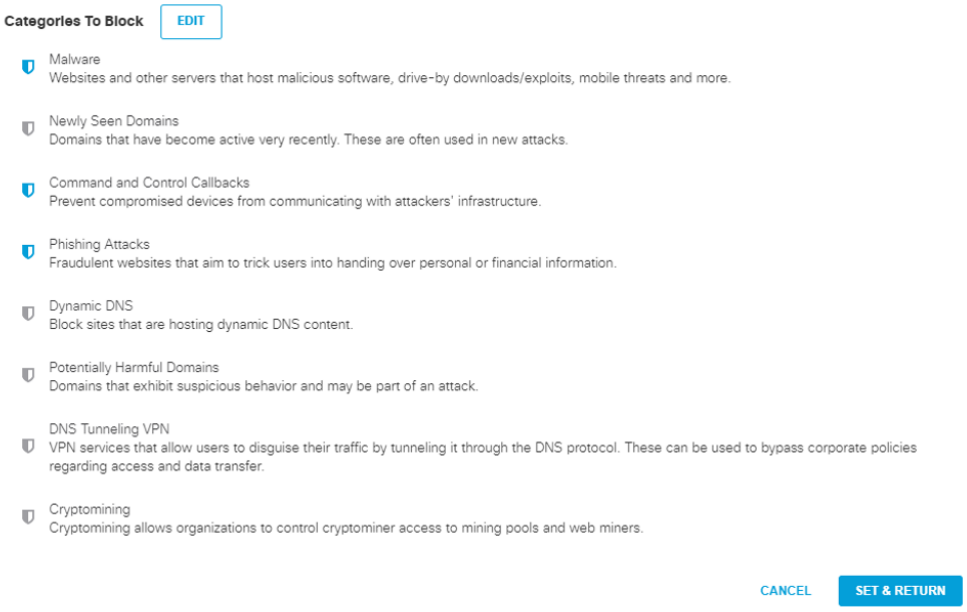

Рис. 3.5. Блоковані категорії

Також варто звернути увагу на те, що DNS-політика не будується за принципом «implicit deny», блокуються тільки категорії Malware, C2C, Phishing Attacks рис 3.6.

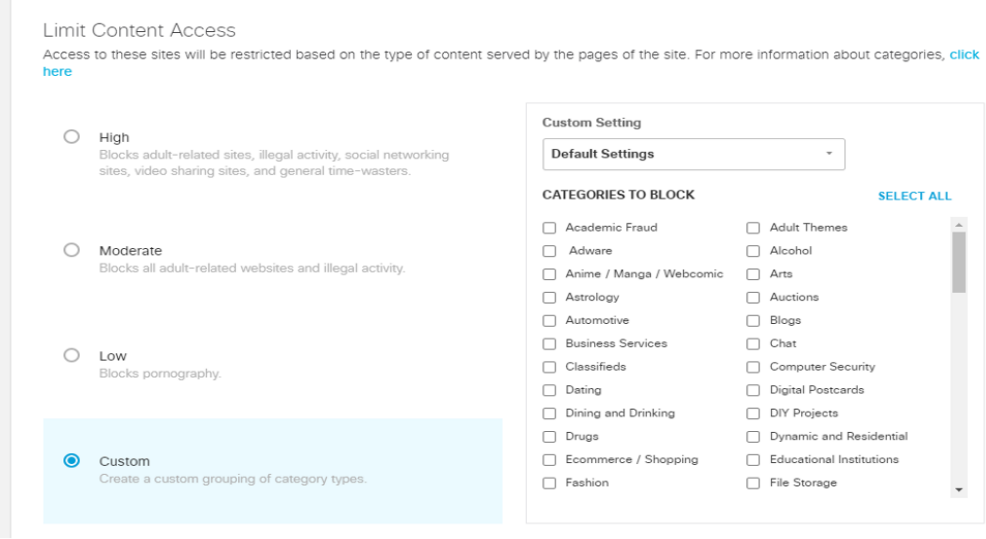

Рис. 3.6. Види блокувань

Якщо домен категоризований як Drugs рис.3.7, він буде повністю потрапляти в цю категорію, навіть якщо за посиланням www.example.com/Sports буде розміщуватися спортивний вісник про останні досягнення місцевої команди. А от якщо блокування на основі контенту буде застосовуватись у Web Policy, а не DNS Policy, то тут буде розмежування залежно від конкретного URL. Application Settings Applied означає блокування залежно від використовуваної програми.

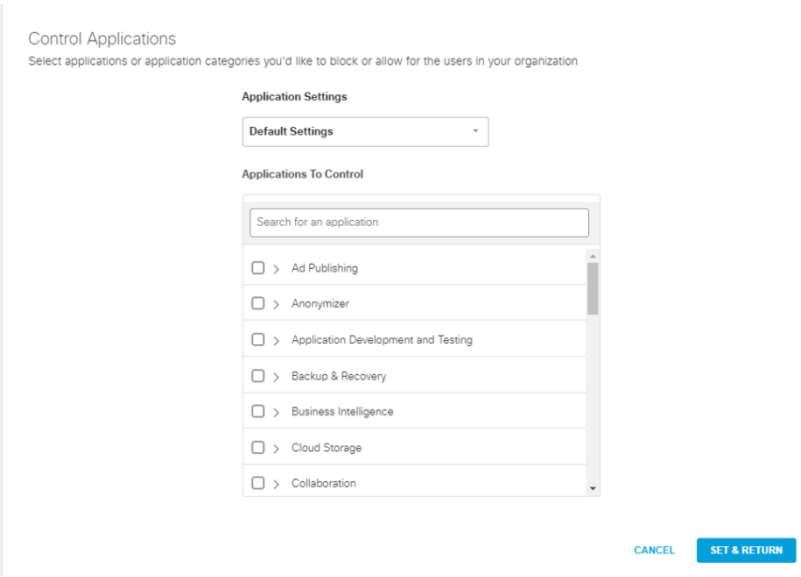

Рис. 3.7. Блокування за типом

Destination list – це вид блокування за конкретним FQDN, IP-адресою, URL (для Web-Policy) Рис 3.8.

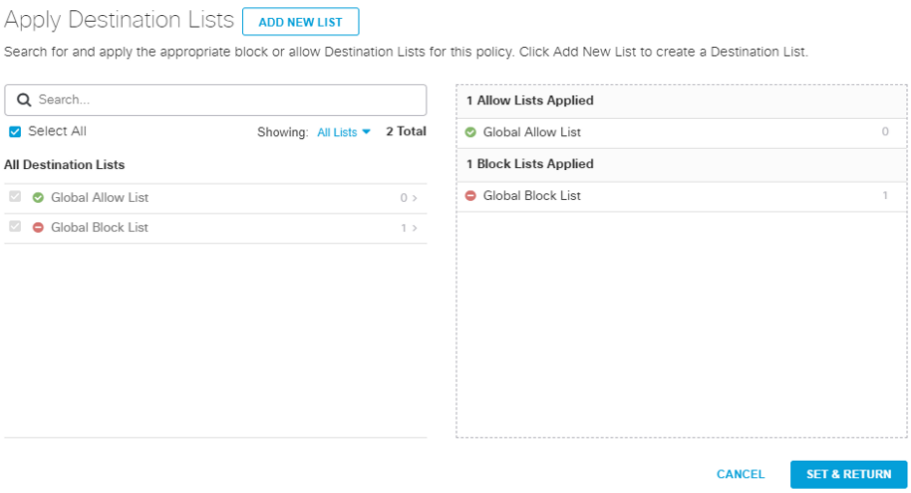

Рис. 3.8. Destinationlist

Додавши щось у Global Allow List у вигляді IP-адреси або, наприклад, FQDN, то цей ресурс за категорією чи контентом вже не буде блокуватися (якщо він підпадає під цю категорію/контент). Налаштування File Analysis[15] доступне, якщо увімкнути в Advanced Settings функцію Intelligent Proxy.За замовчуванням її вимкнено Рис. 3.9.

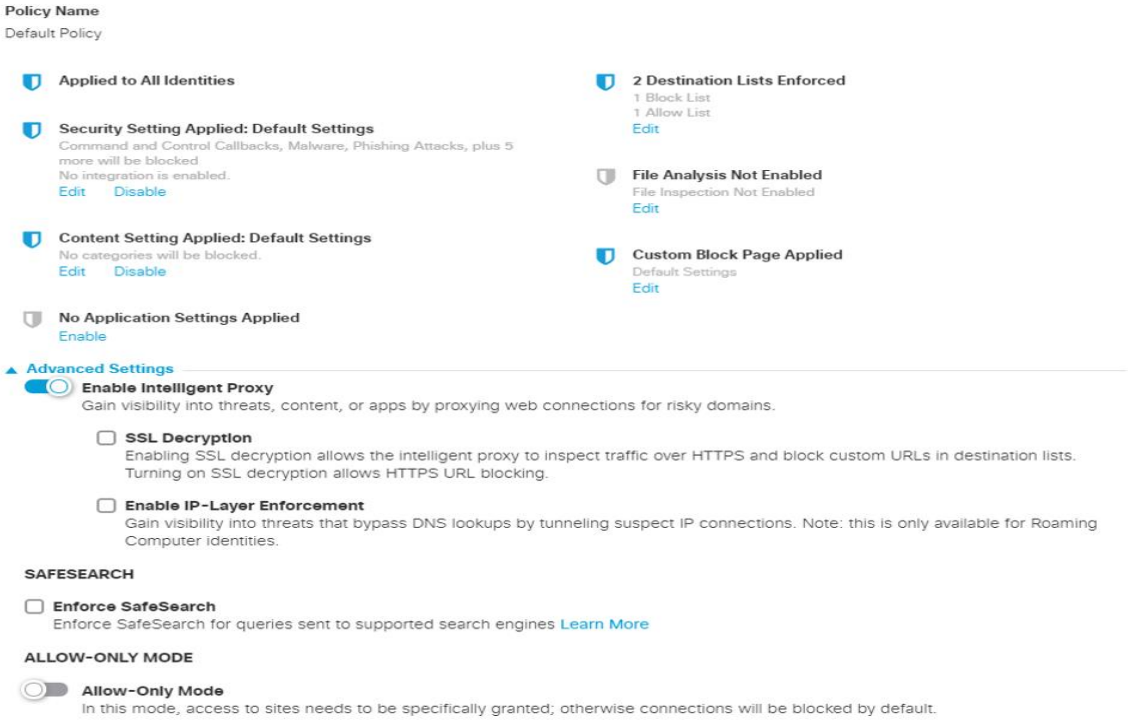

Рис. 3.9. Додаткові налаштування

Intelligent Proxy призначений для роботи з так званими grey доменами, коли на них може бути розміщений небажаний контент або шкідливі файли, але блокувати домен не можна або немає необхідності. У звичайному режимі роботи Umbrella або повертає в DNS-відповіді адресу цільового ресурсу, або на блокуючу сторінку.

При включеній же опції Intelligent Proxy Umbrella повертатиме вам адресу хмарної проксі, через яку проксуватиметься трафік із сертифікатом Cisco (потрібно встановити сертифікат Cisco у довірені та включити опцію SSL Decryption).Велика кількість дуже популярних доменів, наприклад Google або Facebook, не проксується через низьку ймовірність розміщення там шкідливого контенту.

Block Page — веб-сторінка, яка відображатиметься у користувача під час блокування запиту.Налаштувати відображувану сторінку можна у розділі «Block Page Appearance».

Можна модифікувати сторінку блокування Рис.3.10, наприклад, відобразити, що запит заблокований через віднесення до конкретної категорії або контенту, що міститься, вказати e-mail адміна для контакту.

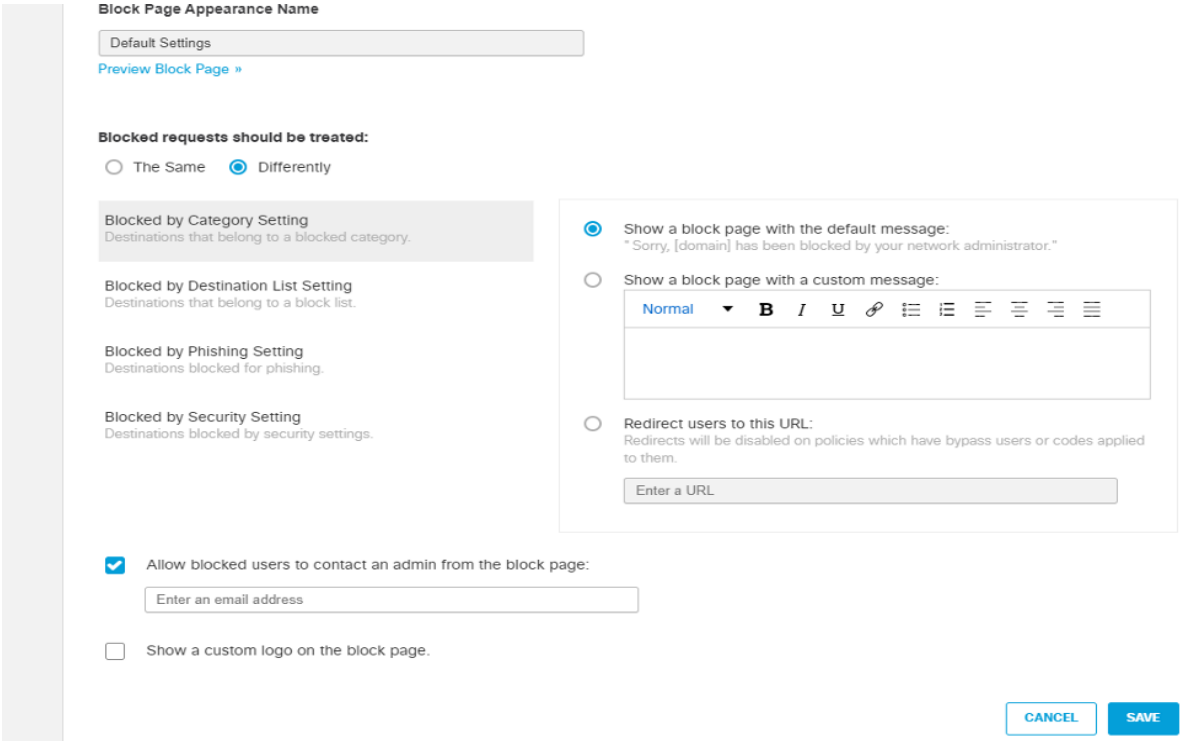

Рис. 3.10. Налаштування сторінки блокування

Робота в режимі веб-проксі Рис 3.12. Рішення може працювати не тільки як рекурсивний DNS, а й як хмарний веб-проксі. Трафік у хмарний веб-проксі від користувачів прямує так само, як і в земний – за допомогою PAC-файлів (proxy auto-config).Сам PAC-файл можна розмістити у Umbrella.Проксірується лише HTTP/HTTPS-трафік (TCP 80/443).

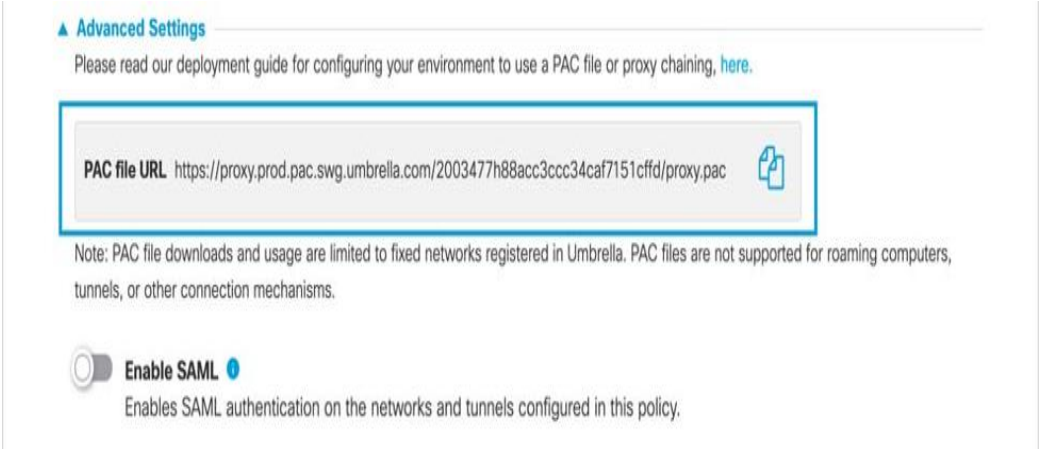

Рис. 3.10. Saml

Щоб аутентифікувати користувачів у хмарному проксі застосувується технологія SAML Рис. 3.11.

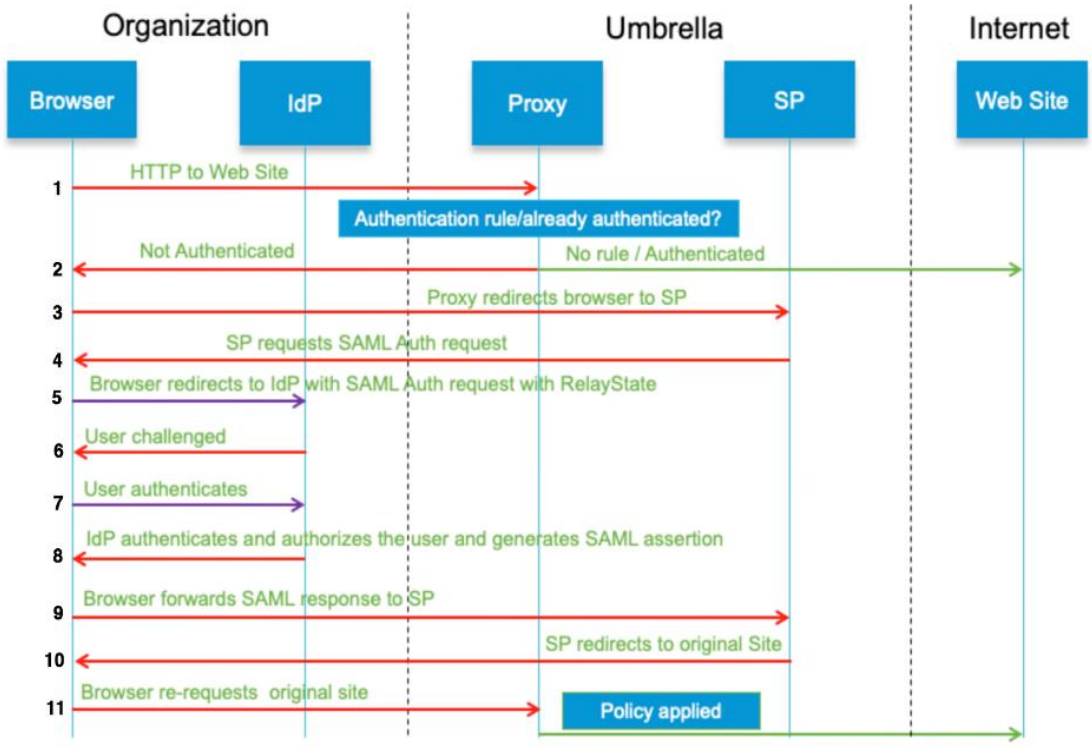

Рис.3.11. Веб проксі

В якості IDP (Identity Provider) використовується якраз земний AD (ADFS) із встановленим AD-конектором, який я розглядав у розділі захисту DNS. У веб-політиках можна використовувати те ж саме, що і в DNS-політиках, а також:

1) Антивірусний захист файлів за допомогою движка Cisco AMP (Advanced Malware Protection) та відправлення їх у пісочницю Threat Grid Malware Analysis.Обмеження тут – максимум 200 файлів на день із розміром файлу не більше 50 Мб.

2) Контроль за типами файлів (File Type Control).Дозволяє блокувати завантаження залежно від категорії (виконувані файли, зображення, аудіо тощо) та конкретного розширення (js, jpeg, exe тощо).

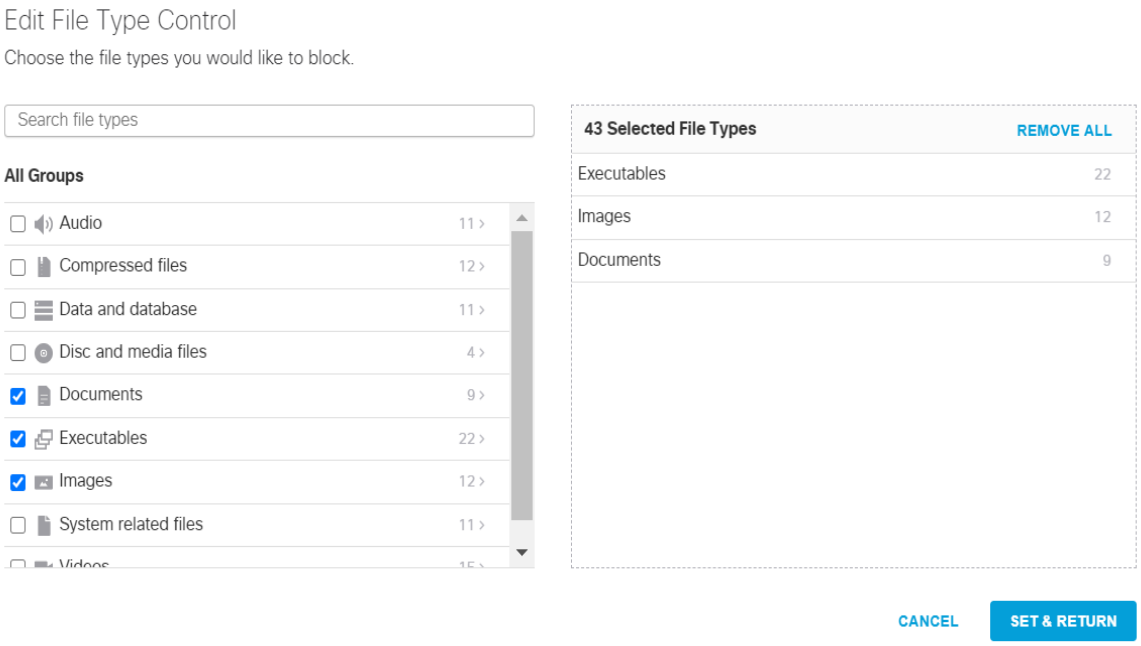

Рис. 3.12. Налаштування дозволених типів

Cloud Delivery Firewall. Рішення може додатково виступати в ролі L3/L4/L7 міжмережевого екрану в хмарі, для цього потрібно загорнути трафік з майданчика через IPSec-тунель Рис. 3.13.

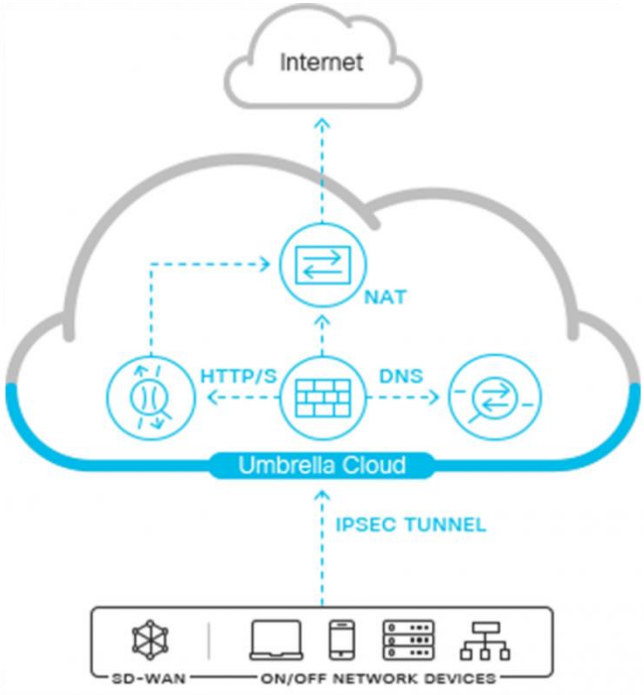

Рис. 3.13. Міжмережевий екран

Важливе обмеження: у політиках MCE вписуються лише приватні IP-адреси, у полі Source та публічні адреси у полі Destination і інакше.Тобто застосувується тут цілком конкретне лише обмеження доступу для внутрішніх ресурсів назовні. Ще один нюанс: максимально допустима смуга на кожний тунель 250 Мбіт/с.Якщо потрібно передавати більше трафіку, потрібно буде будувати додаткові тунелі та балансувати між ними навантаження (наприклад, ECMP). У політиках можна додавати Applications, але додавати групи користувачів AD не можна. Приклад настроєного правила (Рис.3.14):

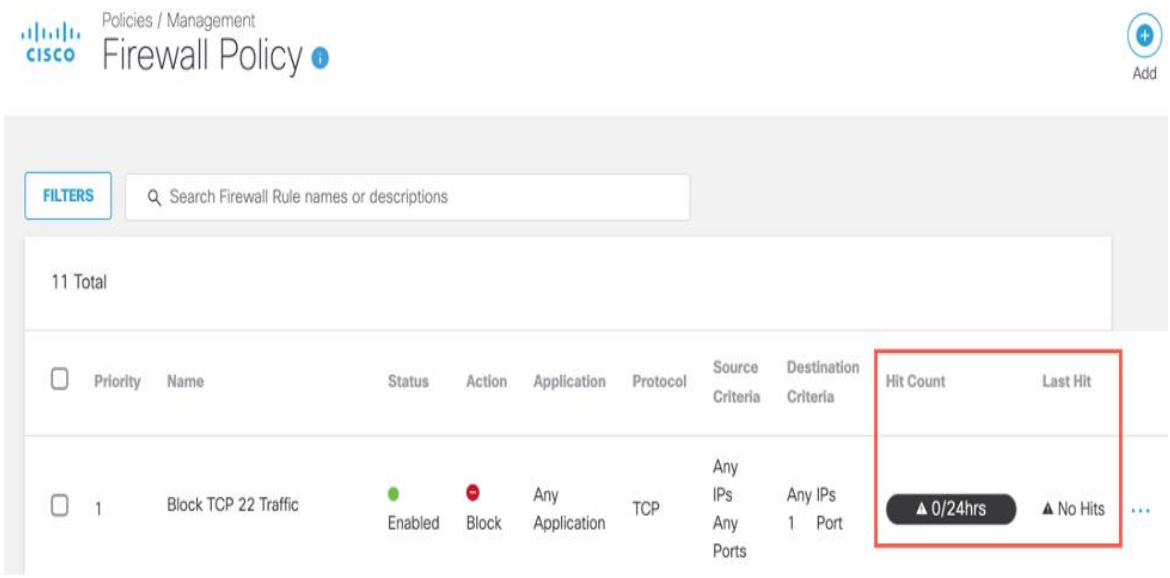

Рис. 3.14. Правило

Робота зі звітністю та розслідуваннями. У Umbrella представлений досить хороший функціонал для проведення розслідувань та аналізу звітності. Можна дивитися як загальний стан компанії, так і детально Рис. 3.15.

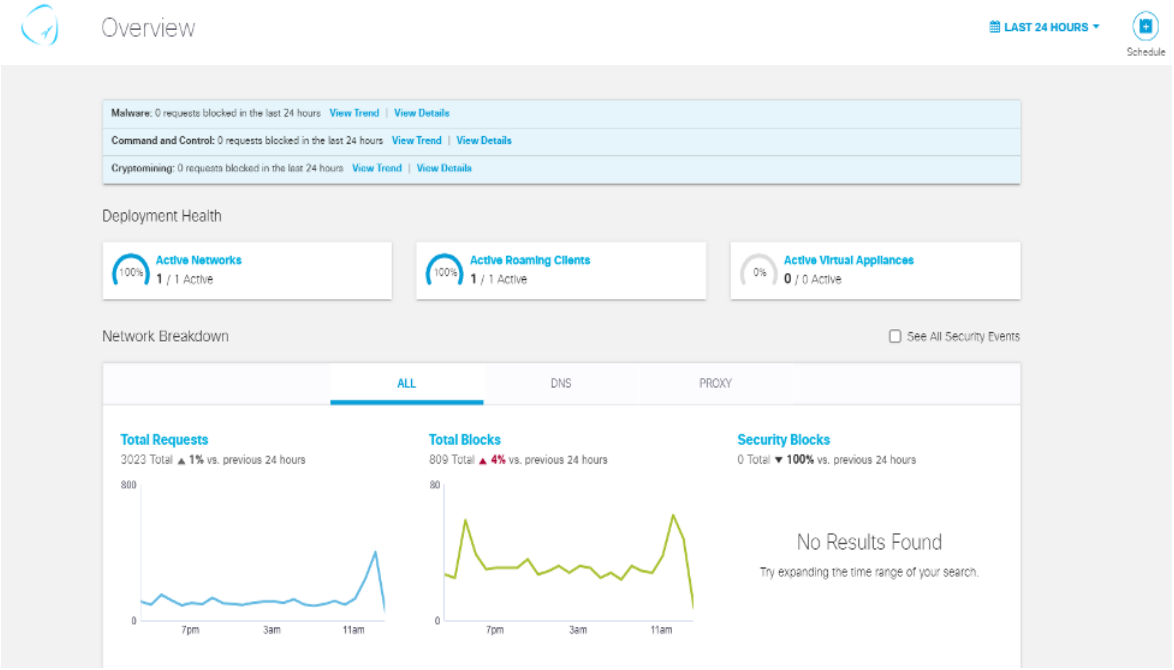

Рис. 3.15. Стан мережі

Є багато різних типів звітів (App Discovery, Threats, Top Destinations та інші).Звіти можна вивантажувати у форматах csv та pdf, вивантаження звітів можна

робити автоматично, наприклад, щотижня з відправкою на пошту. Приклад витримки із звіту App Discovery рис. 3.16.

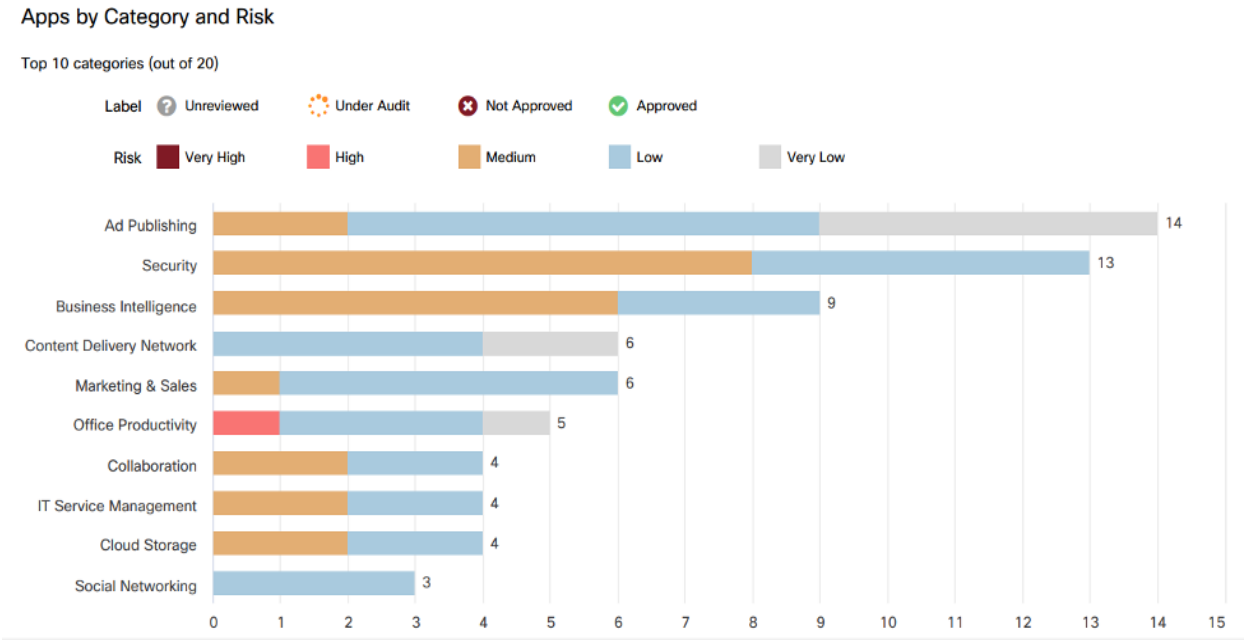

Рис. 3.16. Звіт

Висновки до третього розділу

Проаналізовано, що Cisco Umbrella — це хмарна платформа безпеки, яка забезпечує першу лінію захисту від кіберзагроз для користувачів у корпоративній мережі та поза нею. Він пропонує низку функцій безпеки, які допомагають захистити від зловмисного програмного забезпечення, фішингу та інших зловмисних дій, блокуючи доступ до відомих зловмисних доменів і IP-адрес до встановлення будь-якого з'єднання.

Досліджено основні переваги та засоби забезпечення безпеки цього рішення.Cisco Umbrella використовує DNS (систему доменних імен) для блокування доступу до зловмисних доменів і IP-адрес до встановлення будь-якого з'єднання, запобігаючи зараженню шкідливим програмним забезпеченням та іншим кіберзагрозам.

Зазначено, що веб-фільтрація забезпечує можливості, які дозволяють організаціям блокувати доступ до неприйнятних або не пов'язаних з бізнесом веб-сайтів, захищаючи користувачів від веб-загроз і підвищуючи продуктивність.

Підкреслено, що Cisco Umbrella базується на хмарі, її легко розгортати та керувати нею, не вимагаючи встановлення апаратного чи програмного забезпечення. Він надає дані про загрози в режимі реального часу та автоматичні оновлення, щоб захистити організації від останніх загроз. Cisco Umbrella інтегрується з іншими рішеннями безпеки Cisco, такими як Cisco SecureX і Cisco AnyConnect, щоб забезпечити комплексну безпеку для організацій.

Зазначено, що загалом Cisco Umbrella забезпечує надійне хмарне рішення безпеки, яке може допомогти організаціям захищатися від ряду кіберзагроз і покращити рівень безпеки.

ВИСНОВКИ

В бакалаврській роботі отримано наступні теоретичні та наукові результати:

– досліджено, що корпоративні мережі є дуже вразливими для шахраїв, та мають необхідність у своєму захисті, в останні роки злам корпоративних мереж став буденним явищем, характерним як для розвинутих країн, так і для країн, що розвиваються. Основним об'єктом бажань зловмисників, природно, є інформація, оброблювана в корпоративній мережі.

– проаналізовано**,** що Cisco Umbrella може стати ефективним інструментом для захисту корпоративних мереж від широкого спектру кіберзагроз. Забезпечуючи безпеку на основі DNS і діючи як захищений інтернет-шлюз, він може допомогти запобігти зараженню зловмисним програмним забезпеченням, фішинговим атакам та іншим зловмисним діям, перш ніж він зможе потрапити в корпоративну мережу.

– зазначено, що згідно з проведенною роботою, рекомендується застосовувати Cisco Umbrella як ефективний засіб для захисту корпоративних мереж від широкого спектру кіберзагроз, включаючи зараження зловмисним програмним забезпеченням, фішингові атаки та іншу шкідливу діяльність. Він надає дані про загрози в режимі реального часу та автоматичні оновлення, щоб захистити організації від останніх загроз.