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 ПОБУДОВИ ЗАХИЩЕНОЇ ДИСТАНЦІЙНОЇ РОБОТИ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ DUO UMBRELLA»

Виконала студентка 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Шайкова А.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 роботи. Віддалена робота могла спочатку здаватися короткостроковою необхідністю, але реальність така, що все більше і більше віддаленої роботи стає тенденцією, яка буде зберігатися і надалі. Бізнес отримує цікаві переваги через віддалену роботу. Однією з переваг є можливість залучати та утримувати працівників у будь-якій точці світу. 54% офісних працівників кажуть вони покинули б свою роботу заради тієї, яка пропонує гнучкий графік роботи.

Заохочуючи більшу залученість співробітників, віддалена робота також призводить до додаткової переваги – підвищення продуктивності. Дослідження показують, що заохочення до роботи є найвищим серед працівників, які проводять 3 – 4 дні на тиждень, працюючи віддалено. Нарешті, віддалена робота дає бізнесу можливість зменшити вплив на навколишнє середовище, не зменшуючи при цьому продуктивності.

Не має значення, де ви працюєте: за кухонним столом чи на заводі, чи навіть у відкритому космосі. Сьогодні всі, від менеджерів по роботі з клієнтами до астронавтів, постійно потребують віддаленого доступу до цифрових ресурсів. Але якщо повернутися до реальності, то віддалена робота допомогла багатьом організаціям пережити глобальні перебої, що тривають, і, ймовірно, залишиться популярною, оскільки багато країн зараз запроваджують локдаун. У світлі цього, проблеми з роботою з дому зберігатимуться і надалі. Різниця між роботою з дому та роботою в офісі стає все менш значущою, оскільки сучасна робоча сила є динамічною, і багато працівників мають можливість працювати будь-де і будь-коли.

І ось, коли працівники стають менш статичними і все більш децентралізованими, поняття захисту стає ще більш актуальним, тому потрібно думати про те, як захистити працівників.

Об’єкт дослідження – захищена робота працівників.

Предмет дослідження – технології та засоби побудови захищеної роботи працівників.

Мета роботи – розробка рекомендацій для забезпечення безпечної дистанційної роботи працівників організації.

Завдання бакалаврської роботи:

- Дослідити загрози дистанційним працівникам.
- Ознайомитися з різними хмарними рішеннями для безпеки.
- Дослідити функціональні можливості Duo Umbrella.
- Розробити рекомендації щодо впровадження та використання рішення Duo Umbrella.

Методи дослідження – аналіз документації використаних рішень, проведення тестування інструментів, порівняльний аналіз сервісів.

Практичне значення отриманих результатів – дані рекомендації можуть бути використані для забезпечення кібербезпеки працівників організацій.

1 АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ БЕЗПЕКИ

1.1 Розширення просторів для атак

Організації почали використовувати більше кінцевих точок, мереж і програмного забезпечення для захисту в результаті збільшення кількості працівників, які роблять віддалено, що значно збільшує навантаження на команди безпеки, яка і без того перевантажена роботою. Ось кілька прикладів того, як віддалена робота розширює поле для атак [1]:

1) Коли працівники працюють з дому, вони можуть використовувати домашню мережу, яка не настільки захищена, як мережа в офісі. Це може полегшити зловмисникам доступ до мережі та скомпрометувати дані компанії.

Дистанційна робота збільшує ймовірність того, що працівники використовуватимуть незахищені мережі, такі як громадський Wi-Fi. Підключення до незахищених публічних мереж Wi-Fi може полегшити зловмисникам перехоплення даних та отримання доступу до систем компанії. Навіть домашні мережі часто вразливі до атак. Люди працюють вдома в середовищі, для захисту якого вони не мають достатнього технічного досвіду. Їм можуть сказати оновити маршрутизатори або використовувати VPN, але вони не матимуть технічних знань для цього. Загроза настільки значна, що «Агентство кібербезпеки і безпеки інфраструктури США» (CISA) підкреслило цей ризик у своїй рекомендації від червня 2022 року.

2) Багато віддалених працівників використовують хмарні додатки для доступу до даних компанії, що може призвести до появи нових вразливостей. Зловмисники можуть використовувати вразливості в цих додатках або застосовувати тактику соціальної інженерії, щоб отримати доступ до них.

3) Хоча VPN може допомогти віддаленим працівникам отримати безпечний доступ до ресурсів компанії, він також може створювати неочевидні вразливості. Зловмисники можуть скористатися вразливостями в програмному

забезпеченні VPN або використовувати викрадені облікові дані VPN, щоб отримати доступ до даних компанії.

Віддаленим працівникам рекомендується використовувати віртуальні приватні мережі (VPN) для доступу до систем компанії. VPN захищає інтернет-з'єднання, ускладнюючи хакерам можливість шпигувати за діями в Інтернеті або викрадати дані. Це особливо важливо, коли переглядаються конфіденційні дані або додатки чи використовують публічні мережі Wi-Fi.

Приховуючи IP-адресу та місцезнаходження, VPN може допомогти зберегти конфіденційність, запобігаючи відстеженню дій в Інтернеті веб-сайтами, рекламодавцями та іншими третіми сторонами.

Важливо вибрати надійного постачальника послуг і дотримуватися найкращих практик використання VPN, таких як оновлення програмного забезпечення та уникнення підозрілих веб-сайтів і завантажень.

4) Віддалені працівники часто використовують інструменти відеоконференцій для спілкування з колегами та клієнтами. Ці інструменти можуть створювати нові вразливості, такі як незахищені відеоконференції або фішингові атаки, замасковані під запрошення до відеоконференції.

Zoom-рейдерство – це тип кібератаки, коли зловмисник зриває відеоконференцію, приєднуючись до неї і беручи її під свій контроль, часто з образливим або неприйнятним контентом.

Підприємства все частіше використовують різні платформи для онлайн конференцій, а разом з ними і хакери. Злом веб-камери передбачає отримання зловмисниками несанкціонованого доступу до веб-камери віддаленого працівника, що дозволяє їм переглядати та записувати діяльність працівника без його відома чи згоди. Кіберзлочинці можуть саботувати або зривати онлайн-конференції, непомітно проникати в систему, щоб отримати інформацію, наприклад, службові дані або корпоративну електронну пошту, яку вони можуть використати на свою користь.

5) Віддалені працівники можуть не мати такого ж рівня фізичної безпеки, як офісні працівники. Наприклад, вони можуть працювати в громадських місцях,

де комусь легше вкрасти їхній ноутбук або отримати доступ до даних компанії, підгледівши дані для доступу в систему.

6) Робітники, що працюють дистанційно можуть використовувати слабкі паролі та не правильно їх використовувати, що може скомпрометувати дані компанії. Саме тому важливо встановити унікальний, складний пароль, який не дасть хакерам можливість отримати доступ до бізнес-даних. Всім відомо, що надійний пароль повинен складатися з десяти символів, включаючи цифри, символи, малі та великі літери, але ключовим моментом є часта зміна пароля. Це зменшує можливість доступу до даних для зловмисників.

Менеджери паролів – спеціалізовані сервіси для безпечного збереження всіх паролів. Паролі, логіни та інформація про сервіс, де ви маєте їх використовувати, надійно зашифровані.

Менеджер паролів можна використовувати через браузер, мобільний додаток, а також встановити як окрему програму на комп’ютер.

Можна безпечно збирати дані після реєстрації, під час якої потрібно створити пароль для входу. Деякі паролі можна інтегрувати в браузер, і при відвідуванні сайтів, навіть через мобільний додаток, дані з менеджера будуть «підтягуватися».

Сучасні органайзери виконують й інші корисні функції, окрім безпечного зберігання.

Синхронізація даних гарантує використання єдиного сервісу на різних платформах, включаючи комп’ютери, планшети та смартфони.

Здатність програми генерувати та аналізувати паролі дозволяє їй оцінювати складність паролів, створених користувачами, і створювати складні, унікальні паролі [6].

Сховища паролів, які використовують двофакторну автентифікацію, складніше зламати. Деякі з них також вимагають сканування відбитків пальців, введення коду цифр, який буде надіслано у вигляді SMS-повідомлення на підключений номер телефону, а також вставляння електронного ключа в USB-порт для доступу.

1.2 Брак кваліфікованих кадрів у сфері безпеки

Деякі компанії відчувають затримки з повним забезпеченням віддалених співробітників через кадрові проблеми. Компанія Fortinet, постачальник послуг з мережевої безпеки, виявила, що 60% з 1223 опитаних керівників у сфері IT та кібербезпеки заявили, що їм важко знаходити талановитих спеціалістів з кібербезпеки, 52% намагаються утримати кваліфікованих працівників, а 67% визнали, що брак кваліфікованих кандидатів у сфері кібербезпеки становить більші ризики для їхніх організацій. Ці висновки були оприлюднені у звіті «2022 Cybersecurity Skills Gap Global Research Report» [2].

Загальний план кібербезпеки компанії повинен включати навчання співробітників з питань кібербезпеки. Ризик виникнення проблем з безпекою через людський фактор, який часто є найслабшою ланкою в системі безпеки організації, можна зменшити, навчивши працівників розпізнавати та уникати кіберзагроз.

Найкращий захист від хакерських атак – це освіта. Вона допомагає зрозуміти, як діють зловмисники, які інструменти та методи вони будуть використовувати, щоб отримати доступ до ваших систем, або на що слід звертати увагу при фішингових аферах, а також уникати завантаження та встановлення програмного забезпечення з ненадійних джерел. Додатково, ризик фішингових схем можна зменшити, забезпечивши інформування всіх співробітників про найкращі практики роботи з електронною поштою.

Хакери стають все більш винахідливими, щоб використовувати перехід на дистанційну роботу в своїх цілях. «Незважаючи на всі зусилля захисників, кіберзлочинці продовжують успішно експлуатувати людський фактор для отримання фінансової вигоди», – йдеться у «2022 Social Engineering Report» [4] від постачальника програмного забезпечення для безпеки Proofpoint.

Соціальна інженерія – це тип кібератак, який покладається на людську взаємодію, щоб обманом змусити людей розголошувати конфіденційну інформацію або виконувати дії, які можуть поставити під загрозу їхню безпеку. У середовищі віддаленої роботи соціально інженерні атаки можуть бути особливо

ефективними, оскільки вони часто використовують довіру віддалених працівників до своїх колег, клієнтів або постачальників, а також їхнє незнання політик і процедур безпеки своєї організації.

Найкращий захист від соціальної інженерії – це усвідомлення ризиків, оскільки атаки соціальної інженерії спрямовані на людську психологію та почуття, а не на технічні недоліки, їх може бути складно виявити. Дотримання найкращих практик інформаційної безпеки, таких як обережність при відкритті електронних листів або переході за посиланнями з невідомих джерел, підтвердження особи тих, хто запитує конфіденційну інформацію, а також запровадження надійного контролю доступу та процедур автентифікації для запобігання несанкціонованому доступу до систем і даних, допоможе попередити страшні наслідки. Організації також можуть навчати своїх співробітників, як виявляти та протидіяти атакам соціальної інженерії.

1.3 Менший нагляд з боку служби безпеки

Не існує команд кібербезпеки, які б стежили за тим, що відбувається в приватній мережі співробітників. Дистанційна робота, за визначенням, виводить частину доступу до системи, мережевого трафіку і даних за межі традиційних периметрів корпоративного технологічного середовища і моніторингу безпеки в цьому середовищі. Загалом, компанії не в змозі розширити спостереження до всіх кінцевих точок і в усіх мережах, які зараз підтримують віддалену роботу.

Моніторинг працівників допомагає переконатися, що вони не відстають від графіка і виконують свою роботу швидко та ефективно. Це також може допомогти у виявленні та вирішенні проблем з продуктивністю або потенційних можливостей для вдосконалення.

Нагляд за працівниками може знизити ризики безпеки, виявляючи та реагуючи на потенційні інциденти з загрозою безпеці або її порушеннями, наприклад, коли працівники переглядають конфіденційні дані або беруть участь у ризикованих онлайн-діях.

Загалом, управління працівниками та забезпечення їх продуктивності, ефективність дотримання політик організації та вимог законодавства значною мірою залежить від контролю працівників та пильного нагляду за ними. Встановлення чітких правил та інструкцій щодо моніторингу та нагляду за працівниками допоможе досягти правильного балансу між моніторингом працівників і захистом їхнього приватного життя та свободи.

1.4 Неякісні інформаційні процеси та процедури роботи з даними

Співробітники можуть копіювати конфіденційну інформацію на свої локальні пристрої з різних причин, причому ця інформація може бути захищеною, а може і не бути. Не розуміючи ризиків, вони можуть обмінюватися конфіденційною бізнес-інформацією за допомогою незахищених методів, таких як незашифрована електронна пошта або файли. Дистанційні працівники можуть бути не так добре знайомі з процедурами роботи з даними компанії, тому можуть ненавмисно розкрити конфіденційну інформацію та поставити під загрозу безпеку даних компанії. Ось кілька поширених прикладів неналежних практик і процедур роботи з даними у віддаленому робочому середовищі [5]:

1) Віддалені працівники можуть підключатися до незахищених публічних мереж Wi-Fi, що може полегшити зловмисникам перехоплення даних і отримання доступу до систем компанії.

2) Не використання шифрування для захисту конфіденційних даних, таких як паролі або номери кредитних карток. Це може полегшити зловмисникам перехоплення даних і отримання доступу до систем компанії.

3) Віддалені працівники можуть використовувати незахищені пристрої, такі як особисті ноутбуки або смартфони, для доступу до даних компанії. Ці пристрої можуть не мати такого ж рівня безпеки, як пристрої, що належать компанії, і можуть бути більш вразливими до атак.

4) Працівники можуть використовувати слабкі паролі, наприклад, ті, що легко вгадати, або ті, що повторно використовуються в різних облікових записах.

5) Фахівці можуть ділитися даними компанії з неавторизованими особами або використовувати дані компанії в особистих цілях. Це може поставити під загрозу безпеку даних компанії та підвищити ризик їх витоку.

1.5 Вразливість до фішингових атак

Фішингові атаки – це тип кібератак, одна з найпоширеніших і найнебезпечніших загроз в кібербезпеці, що впливає як на окремих осіб, так і на організації. Небезпека фішингу все ще присутня і широко розповсюджена; достатньо одній людині помилково натиснути щось, чого вона не повинна була торкатися, щоб сталося дещо жахливе. І через те, що процедури, ймовірно, продовжуватимуть змінюватися, це приносить новизну, а новизна створює можливості для нових шахрайств.

Віддалені працівники часто більш вразливі до фішингових атак, оскільки вони працюють за межами традиційного офісного середовища і можуть бути більш вразливими до тактик соціальної інженерії. Чому віддалені працівники можуть бути більш вразливими до фішингових атак [7]:

1) Віддалені працівники можуть бути більш розслаблені під час роботи, що може зробити їх більш вразливими до фішингових атак. Вони можуть частіше перевіряти особисту електронну пошту або акаунти в соціальних мережах у робочий час, що може підвищити ймовірність натискання на фішингове посилання. Оскільки працівники більше покладаються на електронну пошту, ризик зростає, коли вони працюють поза офісом, оскільки вони з меншою ймовірністю розпізнають добре сплановану фішингову атаку, яка видає себе за справжній діловий запит.

2) Віддалені працівники можуть не мати такого ж рівня підготовки з кібербезпеки, як офісні працівники, що може зробити їх вразливими до даного типу атак. Без належної підготовки вони не зможуть розпізнати фішингові електронні листи та уникнути переходу за шкідливими посиланнями.

3) Віддалених спеціалістів легше відволікти, ніж офісних, що може зробити їх більш вразливими до фішингових атак. Вони можуть працювати в режимі багатозадачності, в шумному середовищі або мати інші відволікаючі фактори, які можуть полегшити зловмисникам завдання: змусити їх перейти за фішинговим посиланням.

1.6 Незахищене та вразливе обладнання

Раптовий перехід на віддалену роботу на початку пандемії означав, що багато працівників використовували свої особисті пристрої для виконання своєї роботи, незалежно від того, чи мали вони навички забезпечення своєчасного оновлення та захисту своїх домашніх роутерів, ноутбуків і смартфонів. Віддалені працівники можуть:

– Не отримувати оновлення безпеки так само регулярно, як офісні, оскільки вони не підключені до мережі компанії. Це може зробити їхні пристрої вразливими до атак, які вже були додані та вирішені в нових версіях програмного забезпечення або прошивки.

– Ділитися пристроями з іншими особами, наприклад, членами сім’ї або сусідами по кімнаті. Це може збільшити ризик несанкціонованого доступу до даних компанії.

– Загубити свої пристрої або їх можуть вкрасти. Це може поставити під загрозу безпеку даних компанії, якщо пристрої не захищені або не зашифровані належним чином.

Щоб захиститися від небезпек в Інтернеті, на робочих пристроях зазвичай встановлюють заходи безпеки, такі як брандмауери та антивірусне програмне забезпечення. Це може зменшити ризик виникнення проблем з безпекою, спричинених використанням співробітниками потенційно небезпечних особистих гаджетів.

Роботодавці можуть заохочувати узгодженість і командну роботу, гарантуючи, що всі їхні співробітники використовують однакове програмне

забезпечення, додатки та інструменти. Це може спростити процеси та зменшити кількість помилок і непорозумінь.

ІТ-відділ або служба підтримки зазвичай обслуговує пристрої компанії і може запропонувати технічну підтримку або усунення несправностей за потреби. Це може зменшити затримку та підвищити продуктивність.

Щоб гарантувати, що працівники ознайомлені з найкращими практиками користування пристроями та їх безпеки, організації повинні розробити чіткі політики та інструкції щодо роботи з корпоративними пристроями.

1.7 Неправильні конфігурації в публічній хмарі

Хмара є важливою технологією для віддаленої роботи, але вона також пов’язана з певними ризиками. Один з таких ризиків полягає в неправильних конфігураціях, особливо тих, що стосуються доступу. Організації можуть ненавмисно надати користувачам занадто великий доступ або не впровадити контроль доступу. Згідно з «2022 Cloud Security Report» [3], підготовленим постачальником програмного забезпечення для мережевої безпеки Check Point Software Technologies, понад чверть опитаних фахівців з інформаційної безпеки заявили, що їхні організації зіткнулися з інцидентом безпеки в інфраструктурі публічної хмари протягом минулого року, і основною причиною цього були неправильні конфігурації безпеки.

Хмарні сховища можуть бути незахищеними або загальнодоступними, що дозволяє несанкціонований доступ до конфіденційних даних.

Функції реєстрації та моніторингу можуть бути не увімкнені або налаштовані неправильно, що ускладнює виявлення та реагування на інциденти, пов’язані з безпекою. А також, на хмарних ресурсах може використовуватися застаріле програмне забезпечення, що робить їх вразливими до атак, які використовують відомі вразливості.

Висновки до першого розділу

Визначено основні загрози дистанційним працівникам організації, через які вони потребують захисту в кіберпросторі. Зазначено, що збільшилися простори.

Простежено, що через брак кваліфікованих працівників, відбуваються неякісні інформаційні процеси.

Проаналізовано необхідність проведення навчання для працівників.

2 ДІЄВІ РІШЕННЯ ДЛЯ ВІДДАЛЕНИХ ПРАЦІВНИКІВ

2.1 Використання перевірених рішень

Щоб захистити дистанційних працівників організації потрібно дотримуватися певних правил «кібергігієни», таких як: використовувати VPN, налаштувати політики віддаленого доступу та відстежувати активність працівників. Для спрощення всіх цих процесів потрібно використовувати хмарні рішення для безпеки.

Потрібно обирати надійних постачальників і товари, які пройшли тестування та сертифікацію незалежними організаціями, коли йдеться про рішення для забезпечення безпеки. Використовувати продукти, які добре зарекомендували себе та часто оновлюються, щоб протистояти новим загрозам.

Використання перевірених рішень є важливим першим кроком у захисті комп’ютера, але це лише один з елементів великого плану безпеки, який також повинен включати постійне спостереження та обслуговування, щоб захистити комп’ютер від нових загроз.

Такі рішення з більшою ймовірністю будуть сумісні з вашою операційною системою та іншими програмними додатками. Це зменшує ризик виникнення проблем сумісності, які можуть призвести до збою або несподіваної поведінки вашого комп’ютера. Вони зазвичай постачаються зі спеціальними командами технічної підтримки та обслуговування клієнтів, які можуть допомогти вирішити будь-які питання або проблеми, з якими є можливість зіткнутися. Це особливо важливо, якщо користувачі не знайомі з рішенням або його функціоналом.

Але навіть перевірені рішення можуть мати недоліки, якими можуть скористатися зловмисники, тому дуже важливо пам’ятати про це, використовуючи їх для захисту свого комп’ютера. Щоб захистити свій комп’ютер від відомих вразливостей, потрібно бути в курсі найновіших виправлень та оновлень безпеки.

2.2 Cisco Umbrella

Cisco Umbrella є добре відомим інструментом захисту, який використовується багатьма компаніями по всьому світу.

Gartner Peer Insights – це платформа для оцінювання та огляду корпоративних технологічних рішень від користувачів для майбутніх користувачів. Огляди Gartner Peer Insights є суб'єктивними думками, заснованими на їх власному досвіді. Клієнти та професіонали галузі дали рішенню Umbrella (рис.2.1) схвальні оцінки та відгуки, вони високо оцінили платформу за простоту використання, надійність та ефективність у блокуванні загроз.

Рис.2.1. Рейтинг Cisco Umbrella

Деякі компанії віддають перевагу Cisco Umbrella над іншими системами захисту з наступних причин:

1. Захист від сучасних загроз: Cisco Umbrella використовує дані про загрози з різних джерел, щоб виявляти та зупиняти сучасні загрози, такі як програми-вимагачі, фішингові атаки та ботнети.

Сповіщення від різних систем завалюють команди безпеки. Є можливість програмно завантажити контекстну інформацію про загрози з глобальної мережі у середовище для управління безпекою або реагування на інциденти. Кожне попередження супроводжується глобальним контекстом для команди IT-безпеки. Команда матиме більше часу, щоб сконцентруватися на важливих ситуаціях,

оскільки менше часу витрачатиметься на перемикання між інструментами розвідки.

2. Простота в управлінні та впровадженні: це хмарна система, що робить її простою в управлінні та встановленні. Оновлення впроваджуються миттєво, без будь-якої ручної допомоги.

В умовах розосередженої мережі конфігурація та управління безпекою є складним завданням. Може бути важко визначити, які політики впроваджуються і в якій послідовності, оскільки різні офіси мають різні середовища. Партнери та фахівці можуть автоматизувати адміністрування та змінювати налаштування в середовищі Umbrella програмно.

3. Глобальна мережа: незалежно від місцезнаходження користувача або пристрою, який він використовує, Cisco Umbrella має глобальну мережу комп'ютерів, які можуть швидко реагувати на ризики безпеки[8].

Процес надсилання трафіку на хмарну платформу простий. Можна швидко забезпечити тисячі мережевих виходів і роумінгових ноутбуків, використовуючи наявну мережу Cisco, захистивши користувачів поза мережею, філіали та користувачів Wi-Fi за лічені хвилини.

Для більшої прозорості, контролю та безпеки Umbrella надає хмарний проксі-сервер, який може реєструвати та аналізувати весь ваш інтернет-трафік. Трафік може надсилатися через тунелі IPsec, PAC-файли та ланцюжок проксі для повної видимості, обмежень на рівні URL-адрес і додатків та покращеного запобігання загрозам.

Основні функції включають в себе (рис.2.2):

– Блокування веб-сайтів [9], які порушують правила або не відповідають вимогам законодавства, шляхом перевірки вмісту за категоріями або окремими URL-адресами.

– Використовуючи механізм Cisco Secure Endpoint (раніше Cisco AMP) [9] і зовнішні ресурси, є можливість швидко перевірити будь-який файл, який завантажується, на наявність шкідливого програмного забезпечення та інших небезпек.

– На зміну Threat Grid прийшов Cisco Secure Malware Analytics [9], який швидко аналізує підозрілі файли (необмежена кількість зразків). Наприклад, блокує завантаження файлів .exe,

– У деяких програмах можна заблокувати певні дії користувачів за допомогою гранульованих обмежень, наприклад, завантаження файлів у Dropbox, вкладення у Gmail, публікації та поширення у Facebook [9].

– Докладні звіти, включають зовнішню IP-адресу, ідентифікацію мережі, повні URL-адреси, а також дозволені або заблоковані дії.

4. Співпраця з іншими програмами безпеки [8]: Cisco Umbrella працює разом з іншими програмами безпеки Cisco, включаючи Cisco Secure Email і Cisco Secure Endpoint, щоб запропонувати компанії комплексну програму безпеки.

Щоб об’єднати хмарні рішення для забезпечення IT-безпеки та аналітики, Umbrella співпрацює з провідними IT-компаніями.

Щоб захистити користувачів і дані, фахівці з безпеки використовують широкий спектр методів. Інтегровані засоби захисту, на відміну від тих, що потребують 100+ годин роботи експертів, забезпечують кращий захист. Мета бути «простими в розгортанні та простими в управлінні» є фундаментальним компонентом їхньої партнерської програми. Мета – зробити використання платформи максимально простим для партнерів і клієнтів.

Клієнти можуть захистити кожну людину та будь-який пристрій у будь-якому місці, розширивши свій периметр до хмари за допомогою Umbrella та партнерів з посилення захисту від загроз.

Основоположними компонентами архітектури безпечного доступу Cisco (SASE), яка об’єднує мережеві та безпекові операції, є Umbrella і SD-WAN [9]. Завдяки поєднанню Umbrella і Cisco SD-WAN можна швидко і легко встановити Umbrella в усій мережі і отримати вигоду від надійного хмарного захисту для захисту від онлайн-атак і забезпечення безпечного доступу до хмарних сервісів. Розгортати та адмініструвати середовище безпеки в десятках, сотнях і навіть тисячах віддалених локацій дуже просто завдяки найкращій в галузі автоматизації.

На інформаційній панелі Umbrella вільно встановлюються політики безпеки, виходячи з необхідного вам рівня захисту та наочності.

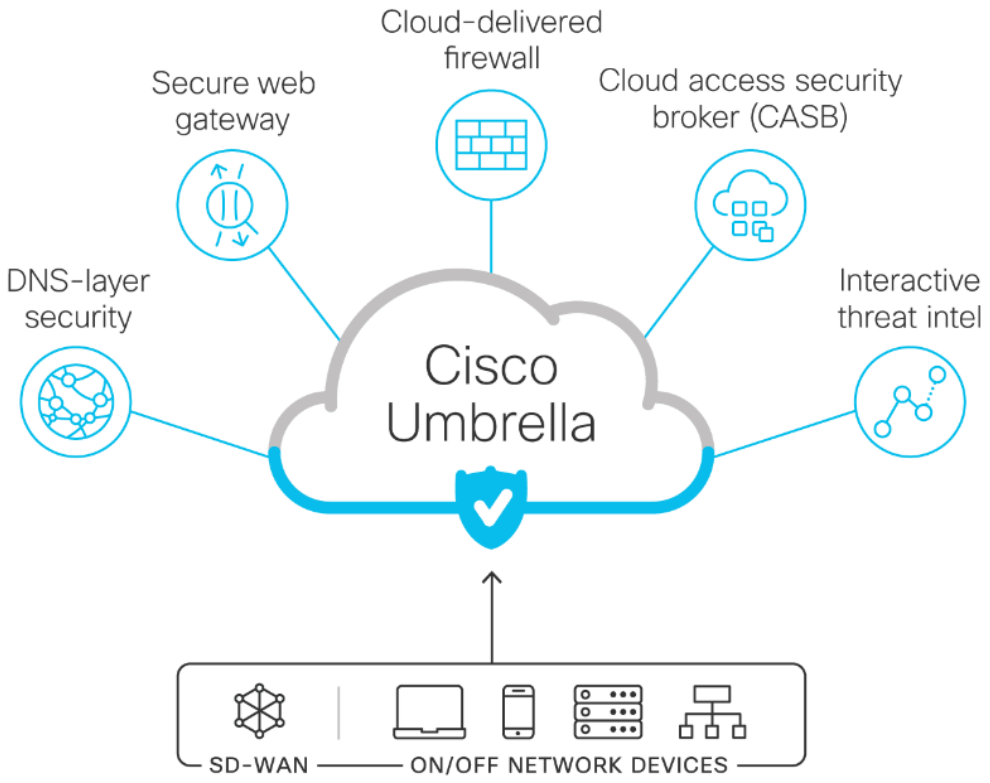

Рис.2.2. Функції безпеки Cisco Umbrella

2.3 OpenDNS

З метою надання всім користувачам безпечнішого, швидшого та якіснішого інтернет-серфінгу, OpenDNS було створено у 2006 році. Спочатку OpenDNS запропонувала рекурсивну службу DNS для домашнього використання, а в 2009 році запустила послугу, орієнтовану на бізнес. У 2012 році OpenDNS представила Umbrella, програмне забезпечення для безпеки бізнесу. Завдяки швидкому зростанню та залученню клієнтів компанія Cisco придбала OpenDNS у 2015 році [10].

Хмарна служба безпеки DNS під назвою OpenDNS пропонує фільтрацію веб-трафіку та захист від низки небезпек в Інтернеті, таких як шкідливе програмне забезпечення, фішинг і програми-вимагачі. Щоб відфільтрувати потенційно

шкідливі веб-сайти та матеріали до того, як вони потраплять на пристрій кінцевого користувача, ця служба перенаправляє веб-трафік через свої сервери.

Здатність OpenDNS захищати віддалених співробітників є однією з його основних переваг. Це пов’язано з тим, що її легко налаштувати для захисту таких пристроїв, як ноутбуки, планшети і мобільні телефони, які не підключені до корпоративної мережі. Застосовуючи правила веб-фільтрації, які запобігають доступу до шкідливих веб-сайтів, фішингових схем та інших ризиків, OpenDNS можна використовувати для захисту цих пристроїв.

Як адміністратори, так і кінцеві користувачі вважають OpenDNS простим у використанні. Адміністратори можуть просто налаштувати параметри і ввести необхідні зміни завдяки можливості встановлення та адміністрування правил з центральної панелі. Щоб скористатися перевагами безпеки, кінцевим користувачам достатньо підключитися до Інтернету за допомогою серверів OpenDNS; ніякого додаткового програмного забезпечення або конфігурації не потрібно.

В цілому, OpenDNS є хорошим варіантом для захисту віддалених співробітників і захисту від інтернет-загроз, оскільки він ефективний і простий у використанні. Функції веб-фільтрації та захисту від загроз допомагають забезпечити безпечний перегляд веб-сторінок для співробітників, незалежно від того, де вони працюють, а хмарна архітектура робить його простим у розгортанні та управлінні.

Рішення OpenDNS містить наступний функціонал [10]:

– Security Graph – це технологія, яка автоматизує захист від відомих та нових загроз. Вона аналізує зріз світової інтернет-активності, щоб спостерігати за підготовкою атак ще до того, як вони будуть здійснені. Цей предиктивний інтелект лежить в основі їхнього продукту для корпоративної безпеки – Umbrella.

– Інфраструктура OpenDNS, відома як Глобальна мережа, надійно обслуговує понад 2% всіх щоденних інтернет-запитів з усього світу. Вона миттєво охоплює кожен пристрій в будь-якій точці світу, забезпечуючи дотримання стандартів безпеки без будь-яких затримок.

– Інтерактивний движок візуалізації даних з відкритим вихідним кодом під назвою OpenGraphiti, що дозволяє аналітикам з безпеки, дослідникам і фахівцям з обробки даних поєднувати візуалізацію з великими даними для побудови 3D-зображень небезпек. Подібно до того, як вірусологи можуть ідентифікувати певний вірус, використовуючи відомі картини хвороби, OpenGraphiti може знаходити складні моделі поведінки та зв'язки, пов'язані з нападами.

Згідно з дослідженнями, багато людей швидше сприймають інформацію, коли вона подається у візуальному стилі, а не словами. Одне з досліджень показало, що людська сітківка може передавати інформацію зі швидкістю, подібною до швидкості Ethernet-з'єднання. Рушій OpenGraphiti використовує метод, який найчастіше використовується в індустрії відеоігор, щоб об'єднати обчислювальні можливості центральних процесорів (CPU) і графічних процесорів (GPU) для представлення даних у 2D і 3D форматі. Движок дозволяє відображати будь-які дані, незалежно від того, наскільки дотично вони пов'язані, у форматі, який простий у створенні, використанні та поясненні.

OpenDNS проаналізував кілька загроз, включаючи ботнет Kelihos, шкідливе програмне забезпечення Red October, програми-вимагачі Cryptolocker і CryptoDefense та інші загрози, використовуючи движок і методологію OpenGraphiti. Навіть візуалізація окремих місій Сирійської електронної армії (SEA) стала доступною.

– DNSCrypt. DNS (Domain Name System) – це важливий компонент архітектури інтернету, який перетворює доменні імена на зрозумілі машині IP-адреси. DNS необхідна для того, щоб інтернет-дані потрапляли туди, куди вони прямують, але вона також може бути атакована різноманітними загрозами, включаючи перехоплення DNS, тунелювання DNS та інше.

Оскільки будь-яка атака, пов'язана з DNS, може дозволити зловмиснику перехопити, перенаправити або змінити інтернет-дані, безпека DNS має вирішальне значення. Це може призвести до численних небажаних наслідків, зокрема крадіжки даних, незаконного доступу до мереж і переривання роботи

інтернет-сервісів. Атаки на DNS іноді використовуються для запуску більш складних операцій, таких як програми-вимагачі або DDoS-атаки.

DNSCrypt перетворює звичайний DNS-трафік у зашифрований DNS-трафік, захищений від підслуховування та атак «man-in-the-middle», так само, як SSL перетворює веб-трафік HTTP у зашифрований веб-трафік HTTPS. Це лише спосіб безпечного шифрування зв'язку між клієнтами та DNS-серверами в центрах обробки даних, який не вимагає жодних змін у доменних іменах або їхньому функціонуванні. Вихідний код продукту DNSCrypt є загальнодоступним на GitHub.

Безпека та конфіденційність кожного інтернет-користувача в Інтернеті може бути значно підвищена завдяки DNSCrypt, який може стати значущою розробкою в галузі інтернет-безпеки.

2.4 Zscaler

Хмарна платформа безпеки Zscaler пропонує веб-фільтрацію, запобігання втраті даних та інші функції безпеки, щоб захистити користувачів від ризиків в Інтернеті. Це досягається шляхом надсилання інтернет-трафіку через хмарну платформу, де він перевіряється на наявність шкідливого коду та інших проблем безпеки перед тим, як потрапити на пристрій кінцевого користувача [11].

Здатність Zscaler захищати віддалених співробітників є однією з його головних переваг. Це пов'язано з тим, що його легко налаштувати на захист таких пристроїв, як ноутбуки, мобільні телефони та планшети, які не підключені до корпоративної мережі. Завдяки хмарному дизайну Zscaler, віддалені співробітники можуть отримати доступ до Інтернету через сервери Zscaler і отримати такий же рівень безпеки, як якщо б вони були фізично підключені до мережі компанії.

Zscaler простий у використанні як для адміністраторів, так і для кінцевих користувачів. Адміністратори можуть швидко впроваджувати політики безпеки та відстежувати ризики в режимі реального часу, керуючи політиками та конфігураціями з єдиної панелі. Кінцевим користувачам не потрібно

встановлювати додаткове програмне забезпечення або налаштовувати свої комп'ютери, щоб підключитися до Інтернету за допомогою серверів Zscaler.

Zscaler є хорошим інструментом для захисту віддалених співробітників і захисту від онлайн-небезпек, оскільки він добре працює і простий у використанні. В той час як його розширені функції захисту від загроз допомагають забезпечити безпечний перегляд веб-сторінок для співробітників, незалежно від того, де вони працюють, його хмарна архітектура (Рис.2.3) робить його простим у розгортанні та управлінні.

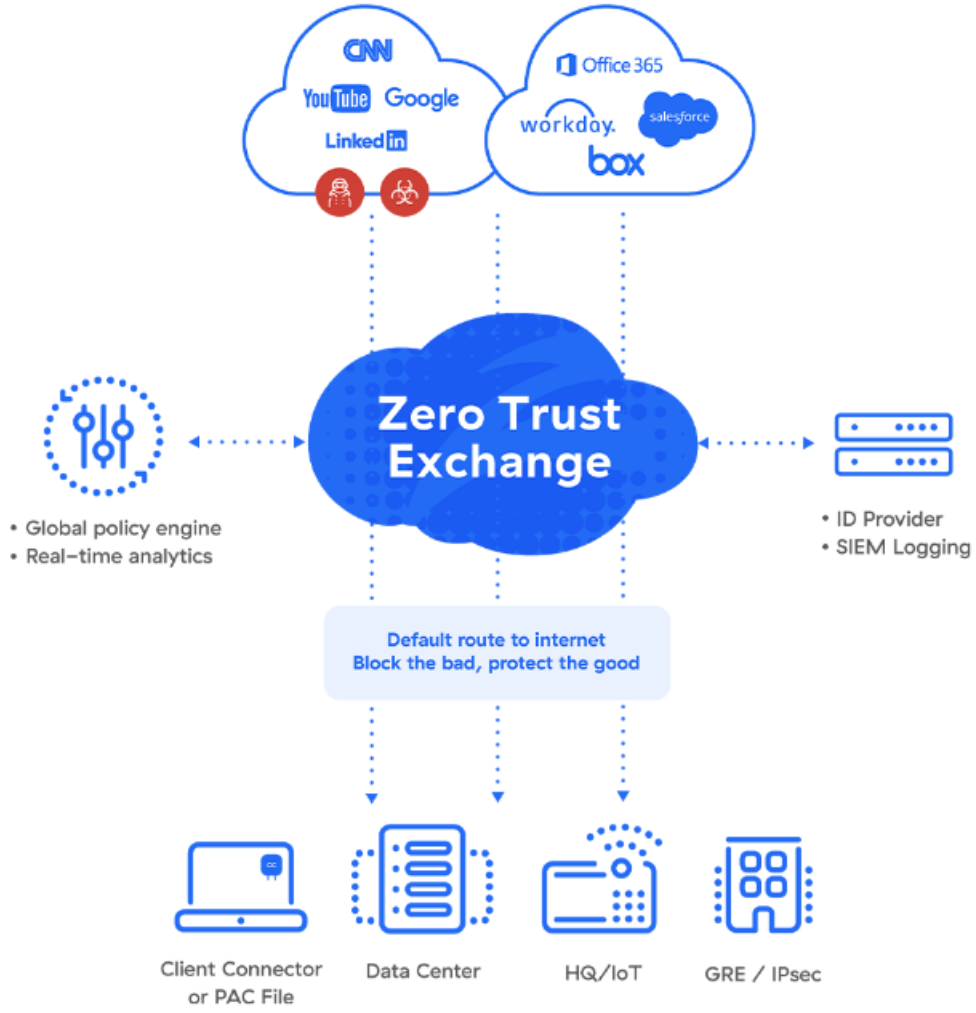

Рис.2.3. Архітектура SASE від Zscaler

SWG забороняє доступ до шкідливих веб-сайтів і посилань або з них. Як шлюз безпеки, він забезпечує дотримання детальних правил використання та запобігає отриманню доступу до онлайн-додатків, перевіряючи веб-трафік та інтернет-трафік на рівні додатків.

SWG і мережеві екрани виконують схожі функції, але це не одне і те ж саме. Мережеві екрани перевіряють вміст вхідних пакетів лише на мережевому рівні і звіряють свої результати з сигнатурами відомих загроз. SWG функціонують на рівні додатків і, залежно від політики використання Інтернету на підприємстві, можуть обмежувати або дозволяти з'єднання [11].

Потреба в хмарних рішеннях безпеки зростає в результаті популяризації віддаленої роботи та швидкого впровадження SaaS. Організаціям також потрібен захист від загроз, захист від шкідливого програмного забезпечення, ізольованість, захист даних за допомогою брокерів безпеки хмарного доступу (CASB), запобігання втраті даних (DLP) і хмарний DLP, а також послуги ізоляції браузерів на додаток до запобігання вторгненням. Вони також повинні мати можливість перевіряти SSL-зашифрований трафік та будь-який інший трафік.

Для успішного захисту хмарних ресурсів рішення безпеки повинні бути побудовані з використанням парадигми Gartner's secure access service edge (SASE) [11]. Конструкції на основі пристроїв багатьох із запропонованих сьогодні «хмарних сервісів безпеки» мають обмеження, особливо для завдань, які вимагають великої обчислювальної потужності, включаючи дешифрування та перевірку SSL-шифрування.

Різноманітні послуги, такі як захист DNS, SWG, доступ до мережі з нульовою довірою (ZTNA) та запобігання втраті/витоку даних (DLP), об'єднуються в одну платформу за допомогою хмарної архітектури SASE.

2.5 Forcepoint ONE Secure Web Gateway

Хмарна технологія безпеки під назвою Forcepoint ONE Secure Web Gateway пропонує [12] інструменти веб-фільтрації, захисту від загроз і запобігання втраті даних, щоб захистити клієнтів від небезпек в Інтернеті. Це досягається шляхом надсилання інтернет-трафіку через хмарну платформу, де він перевіряється на наявність шкідливого коду та інших проблем безпеки, перш ніж потрапити на пристрій кінцевого користувача. У результаті SWG весь інтернет-трафік, як

правило, змушений проходити через централізований центр обробки даних, що збільшує затримку і може серйозно перешкоджати роботі поточних веб-додатків. Крім того, багатьом постачальникам SWG не вистачає широко розосереджених хмарних архітектур, і натомість вони керують застарілим обладнанням, яке має внутрішні вузькі місця в мережі. SWG у Forcepoint, навпаки, має розподілену архітектуру (Рис.2.4), яка не лише пропонує більш гнучку хмарну архітектуру з більш ніж 300 точками присутності по всьому світу, але і йде далі, пропонуючи альтернативний варіант, щоб надати клієнтам ще більшу гнучкість – агент на пристрої, який усуває «вузькі місця» і може забезпечити вдвічі більшу пропускну здатність для чутливого до продуктивності веб-контенту і додатків, ніж конкуруючі SWG.

Можливість захистити віддалених співробітників є однією з переваг Forcepoint ONE Secure Web Gateway. Це пов’язано з тим, що його легко налаштувати на захист таких пристроїв, як ноутбуки, планшети і мобільні телефони, які не підключені до корпоративної мережі. Завдяки хмарному дизайну Forcepoint, віддалені співробітники можуть отримати доступ до Інтернету через сервери Forcepoint і отримати такий же рівень безпеки, як якщо б вони були фізично підключені до мережі компанії. Інтернет може бути неприємним ресурсом, який не завжди використовується в професійних цілях. Завдяки повному управлінню маршрутами [12], SWG в Forcepoint дозволяє вам забороняти або дозволяти відвідувачам невідповідні веб-сайти. При управлінні доступом можна враховувати групу користувачів, стан пристрою, місцезнаходження, категорію URL-адреси, оцінку репутації та оцінку ризиків корпоративних додатків. Адміністратори можуть застосовувати різні обмеження для різних каталогів.

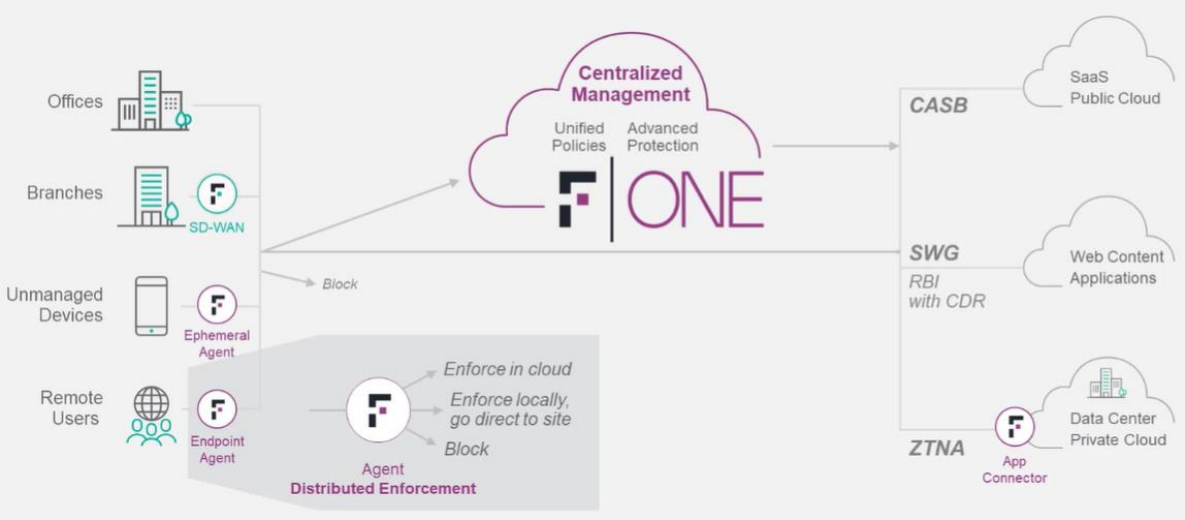

Рис.2.4. Архітектура Forcepoint ONE SWG

Як адміністратори, так і кінцеві користувачі розуміють простоту використання захищеного веб-шлюзу Forcepoint. Адміністратори можуть швидко впроваджувати політики безпеки і відстежувати ризики в режимі реального часу, керуючи політиками і конфігураціями з єдиної панелі. Кінцевим користувачам не потрібно ніякого додаткового програмного забезпечення або налаштувань для підключення до Інтернету за допомогою серверів Forcepoint.

Forcepoint ONE Secure Web Gateway - це ефективне і просте рішення для захисту віддалених співробітників і захисту від онлайн-загроз з урахуванням усіх обставин. В той час як його розширені функції захисту від загроз допомагають забезпечити безпечний перегляд веб-сторінок для співробітників, незалежно від того, звідки вони працюють, хмарна архітектура робить його простим у розгортанні та управлінні.

2.6 Symantec Web Security Service

Розгалужена мережа акредитованих міжнародних центрів обробки даних забезпечує безпеку онлайн і хмарних додатків за допомогою Symantec Cloud SWG, багатокористувацької хмарної платформи (Рис.2.5). Адміністратори можуть встановити правила безпеки один раз і поширити їх на всі свої шлюзи,

використовуючи можливості Universal Policy Enforcement (UPE). Підприємства можуть бути впевнені в тому, що існує послідовний захист, незалежно від того, де зберігаються дані – локально або в хмарі. Захищений веб-шлюз – це розумний вибір для компаній, які шукають засоби захисту корпоративного класу в хмарному сервісі, завдяки найкращому в своєму класі набору функцій, потужним інтегрованим рішенням, можливостям мережевої безпеки корпоративного класу та гнучкій моделі ціноутворення на підписку.

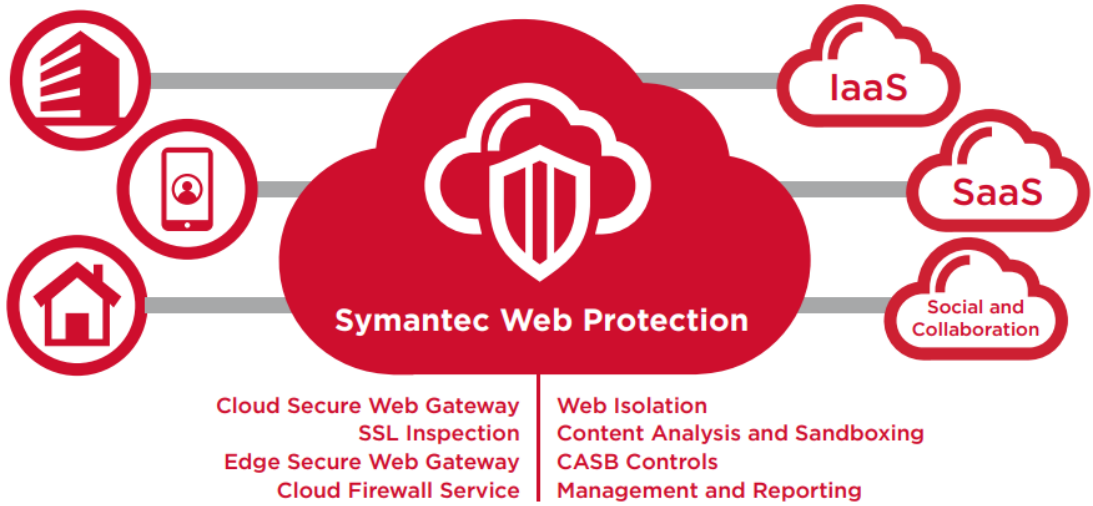

Рис.2.5. Складові Symantec Web Security Service

Ваші дані та програми переходять у хмару, а з ними і ваша безпека. Перехід до хмарних технологій створює нові проблеми з дотриманням нормативних вимог і безпекою, але також відкриває світ нових можливостей для захисту. Хмарна мережева безпека підвищує продуктивність і забезпечує гнучкість, захищаючи користувачів від загроз і гарантуючи, що їхні дані відповідають нормативним вимогам, де б вони не знаходилися.

Завдяки хмарному проксі, програмно визначеному периметру, антивірусному скануванню, пісочниці, веб-ізоляції, запобіганню втрати даних (DLP) та захисту електронної пошти, Symantec Cloud Secure Web Gateway (SWG) пропонує широкий спектр передових функцій. Можна розширити єдині політики, які слідуватимуть за конфіденційними даними, куди б вони не потрапляли, коли користувачі безпосередньо працюють в Інтернеті.

Де б це не було потрібно – на високопродуктивному обладнанні, у вигляді віртуального пристрою або в інфраструктурі приватної хмари – компанія Symantec пропонує високопродуктивне рішення Edge Secure Web Gateway (SWG) на основі проксі-серверів. Проксі-сервер від Symantec захищає бізнес в мобільних мережах, соціальних мережах і Інтернеті. У поєднанні з хмарним SWG від Symantec це гібридне рішення веб-безпеки можна централізовано керувати, щоб захистити всіх співробітників, де б вони не знаходилися.

Рішення SWG від Symantec пропонується у вигляді хмарного сервісу, фізичного пристрою та віртуального пристрою. В основі всіх рішень Symantec для веб-безпеки лежить глобальна мережа Symantec Global Intelligence Network, яка забезпечує захист від вірусів у реальному часі та фільтрацію URL-адрес у реальному часі. Системи також забезпечують перевірку шкідливого програмного забезпечення в режимі реального часу на основі репутації, що сприяє ранньому виявленню нових цілеспрямованих атак.

Щоб запобігти доступу шкідливого програмного забезпечення з веб-сайтів до ваших пристроїв, Symantec Web Isolation [13] виконує веб-сеанси за межами кінцевих точок і надсилає до браузерів користувачів лише безпечне відображення контенту. Політики спрямовують трафік з некатегоризованих веб-сайтів або URL-адрес із сумнівними або потенційно небезпечними профілями ризику через ізоляцію для безпечного серфінгу в поєднанні з безпечними веб-шлюзами Symantec Secure Web Gateways. Web Isolation відокремлює URL-адреси в електронних листах, щоб запобігти фішинговим атакам на облікові дані, інтегруючись із продуктами Symantec для обміну повідомленнями. При поєднанні Web Isolation і Symantec Secure Web Gateway користувачі захищені від атак з некатегоризованих веб-сайтів або URL-адрес з потенційно небезпечними профілями ризику завдяки рівню ізоляції, який поповнюється аналітикою рівня веб-ризиків з глобальної аналітичної мережі Symantec Global Intelligence Network.

Функції та можливості [13]:

– Фільтрація та категоризація URL-адрес: використання динамічних рейтингів ризику URL-адрес у режимі реального часу на основі актуальних даних

про глобальні загрози дозволяє обробляти понад 6 мільярдів веб-запитів щодня та зупиняти мільйони веб-атак і шахрайських дій із використанням соціальної інженерії.

Класифікація URL-адрес за однією або кількома з 72 категорій контенту категорій безпеки (6 заблоковані за замовчуванням), що охоплюють понад 60 мов.

– Удосконалений захист від загроз: запобігання шкідливому програмному забезпеченню завдяки поєднанню евристичного аналізу з подвійним багаторівневим антивірусним захистом. Налаштований аналіз репутації файлів і функції дозволу/заборони списків. Настроювана політика з використанням даних про географічне розташування IP-адреси та рівень ризику загроз.

– Глибока перевірка файлів [13]: блокування файлів у режимі реального часу та складний аналіз (статичний код, правила YARA, поведінковий) використовуються для протидії загрозам.

– Управління зашифрованим трафіком [13]: пошук ризиків і можливо небезпечних матеріалів, прихованих у зашифрованому трафіку, перехоплення і декодування SSL і TLS-трафіку. Самокеровані сертифікати, що спрощують керування клієнтською PKI.

– Cloud Access Security Broker (CASB) [13]: оцінюйте ризики десятків тисяч (30 000+) різних хмарних додатків, які використовуються, одночасно визначаючи програми та сервіси, які використовуються в даний момент. Захист від загроз, безпека даних і поточна видимість під час використання будь-яких хмарних додатків з керованих і некерованих кінцевих точок.

– Запобігання втраті даних (DLP) [13]: використовуючи сучасні механізми зіставлення та розпізнавання DLP, відстежуються та захищаються конфіденційні дані на мобільних пристроях, локально та в хмарі. Розширення можливостей DLP, для отримання прямого доступу до матеріалів у більш ніж 60 хмарних додатках, зокрема Office 365, Box, Dropbox, Google Apps і Salesforce, і керувати ними.

– Просте впровадження для філіалів і мобільних користувачів [13]: забезпечує комплексний захист для мережі та кінцевих точок за допомогою

Symantec Endpoint Security, спростивши керування програмами для мобільних пристроїв. Інтеграція з провідними рішеннями SD-WAN.

2.7 BlueCat Edge

BlueCat Edge – це DNS-розв'язувач від BlueCat, що забезпечує видимість і контроль DNS-трафіку для оптимізації та захисту мережі.

Ключові особливості [14]:

– Підвищення продуктивності: зменшує перенавантаження мережі, забезпечує декілька оптимізованих шляхів роздільної здатності та спрощення зон перекриття для підвищення продуктивності мережі.

– Розгортання без агентів: BlueCat DNS Edge забезпечує видимість, захист і контроль будь-якого пристрою, що використовує DNS, без необхідності розгортання та управління агентами на цих пристроях.

– Простота експлуатації: отримання інформації про загрози від третіх сторін, щоб блокувати відомі небезпечні домени. Інтеграція з провідними SIEM для кореляції даних DNS з іншими даними безпеки.

– Масштабованість і доступність: побудована на базі перевіреної корпоративної хмарної інфраструктури, яка динамічно масштабується для задоволення будь-яких потреб у зборі, зберіганні та обробці даних без перебоїв.

Одна з перших функцій при вході в DNS Edge є інформаційна панель. На карті інформаційної панелі (Рис.2.6) відображаються точки, які представляють кластери сайтів, а також кількість сайтів, згрупованих у цьому географічному регіоні. Якщо точка не має номера, це означає, що в цьому кластері є лише один сайт. В області Активність політики/запитів відображається інформація про загальну кількість запитів і відповідей на них за останні 24 години. В області IP Engagement показано загальну кількість IP-клієнтів, які надсилали запити за той самий період. Також на карті існує Топ-5 найпопулярніших доменів за останні 24 години.

Рис.2.6. Карта інформаційної панелі

Точки обслуговування виконують оновлення в послідовному форматі, де точки обслуговування оновлюються одна за одною. Під час оновлення точки обслуговування продовжуватимуть обробляти інформацію запиту, що не призведе до простою.

Коли версія точки обслуговування сайту оновлюється в результаті автоматичного оновлення на всіх сайтах або ручного оновлення вибраних сайтів, точки обслуговування, розгорнуті на цих сайтах, розпізнають, що оновлення доступне під час наступного періодичного опитування до хмари DNS Edge Cloud. Потім точка обслуговування отримує оновлення з хмари DNS Edge Cloud і послідовно починає виконувати оновлення до нової версії точки обслуговування.

Налаштування оновлення точок обслуговування дозволяють контролювати, чи будуть точки обслуговування автоматично оновлюватися з кожним випуском нової версії точки обслуговування. За замовчуванням точки обслуговування налаштовано на автоматичне оновлення.

Якщо вимкнути автоматичне оновлення точок обслуговування, вони залишаться з поточними версіями точок обслуговування і їх потрібно буде оновлювати вручну на кожному сайті. За допомогою цієї функції можна оновити точки обслуговування, пов’язані з тестовим сайтом, щоб переконатися, що новіші

оновлення точок обслуговування не порушують існуючу функціональність, перш ніж розгорнути оновлення для решти організації. Також наявна більша гнучкість для розгортання оновлень точок обслуговування під час контрольованого вікна обслуговування.

Є можливість створення списків доменів, які допоможуть створити політики. Наприклад, організації може знадобитися список сайтів соціальних мереж для політики блокування, або короткий список сайтів, до яких можуть мати доступ касові апарати, для політики дозволу. Ви також можете додавати списки доменів до просторів імен як у вигляді списків збігів, так і у вигляді списків винятків, щоб контролювати пересилання запитів [14].

Існує можливість додавати домени для блокування, дозволу або спостереження вручну або створити список доменів у форматі .csv чи текстового файлу і завантажити його.

Приватні віртуальні мережі, розгорнуті в хмарних налаштуваннях, негайно вирішуються за допомогою BlueCat Cloud Resolver. Після встановлення він отримує доступ до хмари і знаходить кожну DNS-зону, присутню в хмарній архітектурі. Для вирішення запитів будь-якою кінцевою точкою в центрі обробки даних або хмарі, виявлені DNS-зони додаються в єдиний список доменів BlueCat Edge. Оскільки Cloud Resolver орієнтований на хмару, він дозволяє мережевим командам використовувати будь-яку комбінацію постачальників приватної хмари, не заплутуючись у правилах умовної переадресації DNS.

Надається доступ до інформації про екземпляр Cloud Resolver, як тільки він буде запущений і почне надавати дані про список доменів для вашого середовища Edge. Крім того, можна вибрати домен зі списку, натиснувши хмару Cloud Resolver.

Також існує можливість визначити політики для контролю доступу до певних списків доменів, типів запитів, вихідних IP-адрес і IP-адрес відповідей.

Існує три категорії політик [14]:

Довіра: дозволяє визначати певні домени, які можуть бути заблоковані, покладаючись на довіру до них. Наприклад, можна розробити політику довіри, яка дозволяє доступи до доменів, які могли бути помилково заблоковані правилами

виявлення загроз. BlueCat рекомендує налаштувати глобальну політику довіри, яка охоплює внутрішні домени, що можуть бути класифіковані як тунельні або DGA.

Блокування: списки доменів, типи запитів, IP-адреси джерела або IP-адреси відповіді, які додалися до політики, – недоступні. Застосування політики, яка обмежує доступ до списку доменів URL-адрес соціальних мереж, є одним із підходів, щоб обмежити доступ до доменів.

Моніторинг: дозволяє відстежувати доступ до домену, не впливаючи на відповідь DNS.

2.8 Infoblox Secure DNS

Кіберзагрози на основі DNS стають дедалі небезпечнішими. Найпоширенішою точкою входу для шкідливого програмного забезпечення, програм-вимагачів і DDoS-атак є DNS. Як наслідок, компанії в усьому світі поспішають зрозуміти, яку роль DNS відіграє в сучасних кіберзагрозах і як з ними боротися.

Продукти безпеки Infoblox включають в себе:

– BloxOne Threat Defense [15]. BloxOne Threat Defense працює на рівні DNS, щоб виявляти загрози, які інші рішення пропускають, і запобігати атакам на ранніх стадіях їхнього життєвого циклу (Рис.2.7). Він підвищує ефективність поточного стеку безпеки, захищає цифрові операції та роботу з будь-якого місця, а також знижує загальні витрати на кібербезпеку завдяки повсюдній автоматизації та інтеграції в екосистему. Покращує видимість і контроль навіть дуже ухильної активності загроз протягом усього життєвого циклу загрози.

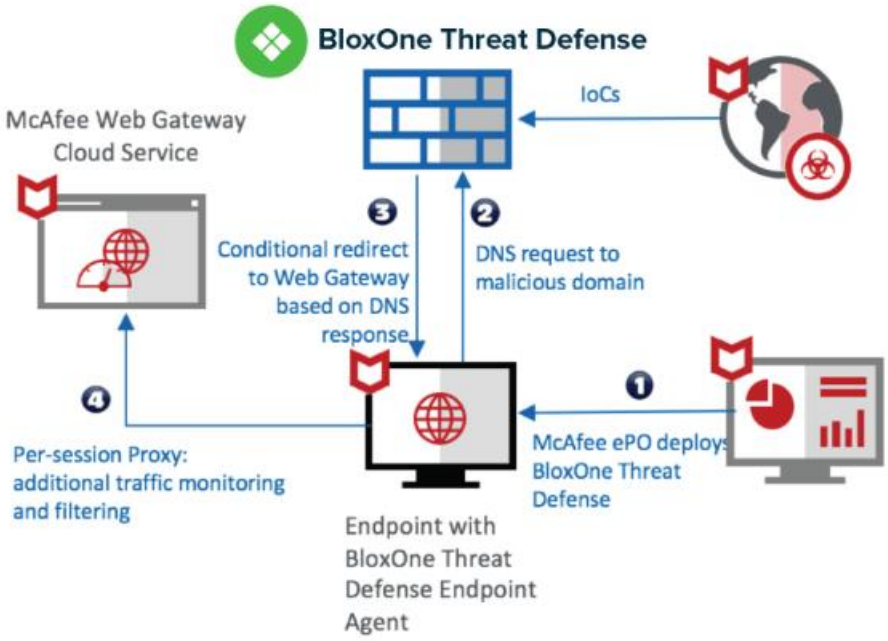

Рис.2.7. Архітектура BloxOne Threat Defense

Надає користувачам і пристроям надійний і точний захист підприємства незалежно від їхнього місцезнаходження. Дозволяє стороннім інструментам безпеки працювати в унісон, щоб краще виявляти та усувати загрози завдяки широкій автоматизації. Скорочує час на розслідування загроз і забезпечує ефективніше реагування на інциденти завдяки швидкому доступу до цінних даних.

– Threat Intelligence [15]. Інформація про загрози є важливим фактором ефективності системи безпеки. Команди безпеки можуть збирати, стандартизувати і поширювати високоточні дані про загрози з різних джерел, використовуючи можливості Infoblox BloxOne Threat Defense, зміцнюючи весь стек безпеки і захищаючи DNS. Завдяки додатковим можливостям SecOps може прискорити розслідування загроз і реагування на них на дві третини. Завжди надає актуальні дані про загрози. Адаптує аналітику до конкретних потреб. Використовує комплексний контекст для прийняття швидких та ефективних рішень. Має легке та автоматичне розповсюдження по всьому стеку безпеки.

Усі можливості BloxOne Threat Defense значною мірою залежать від автоматизації, яка прискорює очищення та зменшує адміністративне навантаження. Щоб забезпечити захист, дані про загрози автоматично збираються,

стандартизуються та передаються. Вся екосистема безпеки може бути використана для ініціювання автоматизованих реакцій. Доступ до всіх релевантних даних про загрози, які доступні в контексті, прискорює розслідування та усунення наслідків.

– Advanced DNS Protection [15]. Усуває об’ємні атаки, перехоплення DNS, отруєння кешу та інші DNS-специфічні експлойти, які можуть вивести бізнес з ладу. Переконується, що клієнти завжди на відміну від підходів, які покладаються на надмірне резервування інфраструктури або просте обмеження швидкості відповіді, ADP інтелектуально виявляє і пом’якшує DNS-атаки, реагуючи тільки на законні запити, використовуючи постійно оновлювану інформацію про загрози, без необхідності розгортати патчі безпеки.

Постійний моніторинг, виявлення та запобігання загрозам, здатність розпізнавати і запобігати DNS-атакам, як об’ємним, так і необ’ємним, а також реагування на справжні запити. Автоматично зупиняє атаки до того, як вони досягнуть програмного забезпечення DNS-сервера, за допомогою спеціалізованого обладнання для перевірки мережевих пакетів. Автоматичне оновлення захисту на основі сторонніх досліджень та аналізу методів атак, що розвиваються, інформації, отриманої з клієнтських розгортань, і даних, отриманих від модифікацій конфігурації DNS.

– Cybersecurity Ecosystem [15]. Ручне управління десятками технологій безпеки та щоденне реагування на сотні і тисячі оповіщень стають тягарем для команд кібербезпеки через значні локальні та публічні/гібридні хмарні корпоративні налаштування. За допомогою Ecosystem Exchange від Infoblox команди безпеки можуть покінчити з ізольованістю, підвищити рентабельність інвестицій в екосистему кібербезпеки та оптимізувати свої рішення для автоматизації та реагування на загрози (SOAR). Завдяки покращеній автоматизації та двосторонньому обміну даними в режимі реального часу по всій екосистемі, що стало можливим завдяки комплексним API, це рішення скорочує час і витрати на реагування на загрози. Скорочує час усунення несправностей на дві третини. Зменшує витрати, пов’язані з ручним втручанням та людськими помилками.

Організації повинні подолати ізольованість, отримати видимість майже в режимі реального часу і зібрати важливу криміналістичну інформацію та мережеві дані про інциденти, щоб прискорити реагування на інциденти. Для такого важливого мережевого контексту BloxOne Threat Defense використовує дані DNS, DHCP і IPAM. Потім він автоматично передає цю інформацію до ширшої екосистеми безпеки і запускає автоматичну реакцію на події безпеки. У випадках, пов’язаних з активністю Advanced Persistent Threat (APT) і шкідливими доменами, BloxOne Threat Defense автоматично обмінюється інформацією з передовими рішеннями для виявлення загроз. Потім Infoblox автоматично зупиняє роботу, реєструє події або реагує на ці ризики в міру необхідності.

Висновки до другого розділу

Досліджено хмарні рішення для забезпечення захищеної роботи працівників. Проведено аналіз їх основних компонентів та методів роботи.

Обґрунтовано, що потрібно використовувати перевірені рішення, з гарною репутацією, які пройшли тестування та сертифікації.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОЇ ВІДДАЛЕНОЇ РОБОТИ ПРАЦІВНИКІВ НА БАЗІ РІШЕННЯ DUO UMBRELLA

3.1 Переваги Cisco Umbrella

Cisco Umbrella має низку переваг над іншими рішеннями безпеки на основі DNS, зокрема:

Глобальне покриття: Cisco Umbrella використовує найбільшу і найсучаснішу в світі мережу розвідки безпеки, яка надає інформацію про загрози в режимі реального часу і дозволяє Umbrella блокувати загрози на рівні DNS. Таке глобальне покриття гарантує, що користувачі захищені від загроз незалежно від того, де вони знаходяться.

Інтеграція з продуктами безпеки Cisco: Cisco Umbrella є частиною екосистеми безпеки Cisco і може інтегруватися з іншими продуктами Cisco, такими як Cisco SecureX, для забезпечення більш комплексного рішення безпеки.

Предиктивний інтелект: Cisco Umbrella використовує машинне навчання і предиктивну аналітику для виявлення і блокування загроз ще до того, як вони потраплять в мережу. Такий проактивний підхід до безпеки допомагає захистити користувачів від атак нульового дня та нових загроз.

Простота використання: Cisco Umbrella просте у розгортанні та управлінні, його можна налаштувати відповідно до конкретних потреб безпеки кожної організації. Його хмарна архітектура означає, що не потрібно встановлювати апаратне чи програмне забезпечення, а доступ до нього можна отримати з будь-якого місця.

Гнучкість: Cisco Umbrella пропонує гнучкі варіанти розгортання, включаючи переадресацію DNS, роумінговий клієнт Umbrella і віртуальний пристрій Umbrella. Ця гнучкість дозволяє організаціям вибирати метод розгортання, який найкраще відповідає їхнім потребам.

Гранульований контроль політики: Cisco Umbrella забезпечує гранульований контроль політик, дозволяючи адміністраторам створювати політики на основі конкретних користувачів, груп, місцезнаходжень і додатків. Це дозволяє організаціям впроваджувати політики безпеки, які відповідають їхнім унікальним потребам.

В цілому, глобальне покриття Cisco Umbrella, предиктивна аналітика, простота використання, гнучкість і гранульований контроль політик роблять Cisco Umbrella потужним рішенням для забезпечення безпеки на основі DNS, яке може допомогти організаціям захистити свої мережі і користувачів від широкого спектру загроз.

3.2 Overview

Umbrella – це хмарна платформа безпеки, яка забезпечує першу лінію захисту від загроз в Інтернеті, де б не перебували користувачі, аналізуючи та вивчаючи моделі поведінки в інтернеті. Вона автоматично блокує шкідливі запити до того, як вони потраплять до мережі або кінцевих точок клієнта.

Панель приладів – одна з речей яку отримують, купуючи Umbrella (Рис.3.1).

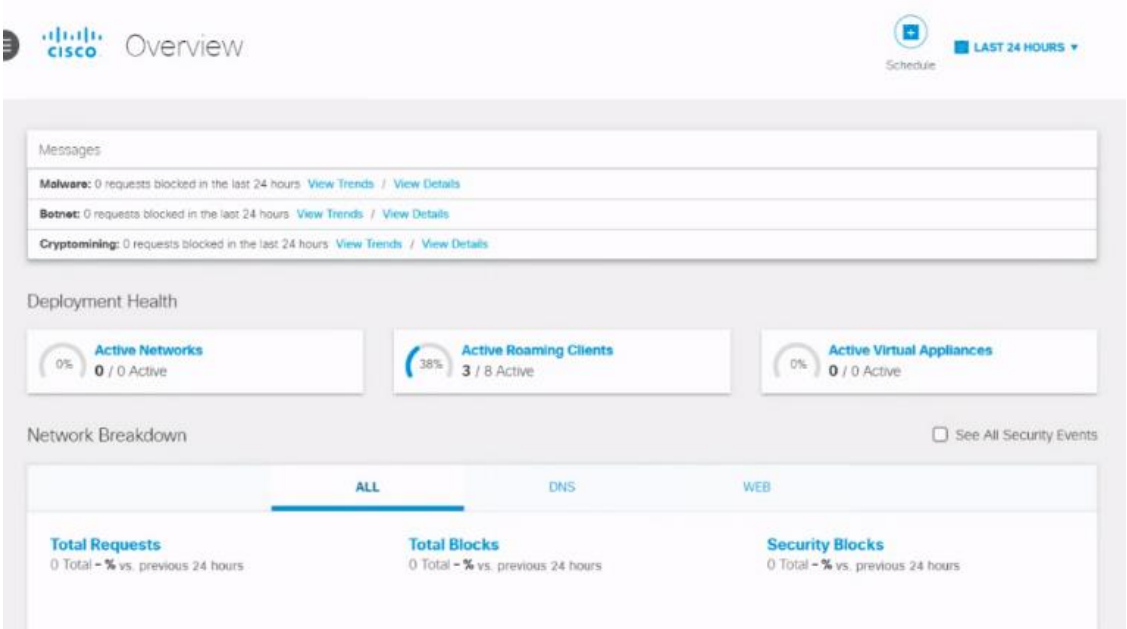

Рис.3.1. Dashboard

Це повна інформаційна панель, яка дає багато даних про посилання, на які переходять користувачі, та які програми вони використовують. Тут можна встановити різні політики для різних типів користувачів, щоб рішення могло інтегруватися в Active Directory**.**

У верхній частині відображаються повідомлення, які дають швидкий огляд подій. Іноді тут можна побачити додаткові банери, якщо є сповіщення та попередження. Уся сторінка Overview і більшість контенту на ній прив’язані до часу, і є можливість вибрати показ активності за останні 24 години, вчора, за останні сім днів або за останні 30 днів.

Стан розгортання дає нам інформацію про стан мережі та клієнтів, якими керують, а саме: скільки активних мереж ідентифікували, скільки зареєстрованих клієнтів перебувають поза мережею і скільки віртуальних пристроїв розгорнуто.

Розбивка мережі показує загальну кількість запитів і загальну кількість блоків. Прокручуючи вниз, можна побачити деталізацію блоків безпеки: блоки шкідливого програмного забезпечення, фішингові блоки, блоки криптомайнінгу, тощо. Загальні блоки також фокусуються на поведінці користувачів.

3.3 Deployments

Ділиться на дві основні категорії (Рис.3.2): Core Identities та Configuration. В свою чергу, кожна з них поділяється ще на декілька підкатегорій:

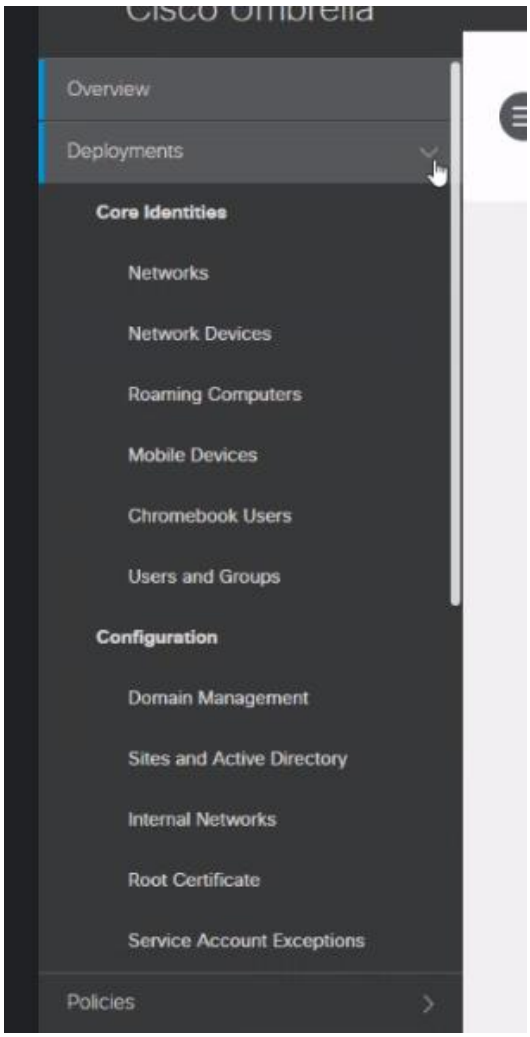

Рис.3.2. Категорії та підкатегорії Deployments

Core Identities:

Networks: в цій вкладці видно всі додані мережі, за якими ведеться спостереження. Тут дуже легко додати нову мережу. Все, що потрібно зробити це назвати мережу, обрати версію інтернет-протоколу, що буде використовуватися – IPv4 або IPv6 та ввести потрібну IP-адресу (Рис.3.3).

Network Devices: тут можна буде спостерігати за всіма пристроями, що підключені до однієї з мереж в попередній підкатегорії.

Roaming Computers: щоб не відслідковувати весь трафік мережі, на пристрій установлюється Umbrella Roaming Client, завдяки чому, відбувається моніторинг лише на певному пристрої.

Mobile Devices: ідентично до попередньої підкатегорії, тільки клієнта буде встановлено на мобільний девайс.

Chromebook Users: Chromebook – це пристрої виробництва фірми Google, що працюють на операційній системі Chrome. На них теж установлюється клієнт, за допомогою якого відбувається моніторинг.

Users and Groups: тут створюються окремі користувачі та групи цих користувачів, щоб стежити за ними.

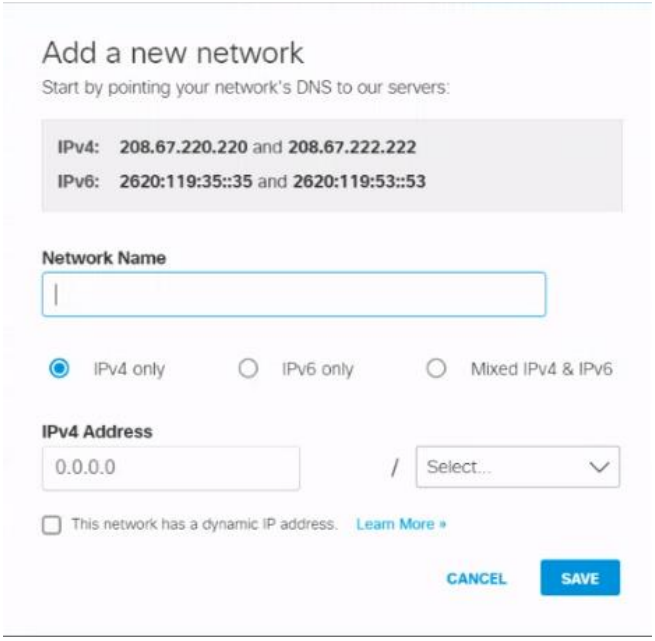

Рис.3.3. Додавання мережі

Configuration:

Domain Management: управління корпоративним доменом або доменами, підтримка їх у безпечному, стабільному стані для забезпечення роботи веб-сайту або веб-сайтів.

Sites and Active Directory: можна налаштувати так, щоб на панелі керування було видно імена користувачів, а не тільки IP-адреси. Це допоможе отримати більш повне уявлення про те, хто і коли намагався отримати доступ до різних сайтів. Також, адміністратором може бути доданий код розблокування. Якщо доступ до певного веб-ресурсу був обмежений спеціально чи випадково, через недогляд, і комусь знадобився тимчасовий доступ до того сайту, за допомогою коду можна буде його розблокувати.

Internal Networks: так само як в Networks є можливість додати мережу та моніторити її. Відмінність полягає в тому, що до цієї мережі є можливість застосувати політики.

Root Certificate: можна скачати сертифікат для підтвердження захищеного з’єднання.

Service Account Exceptions: налаштування подій, що не будуть відслідковуватися.

3.4 Policies

Ділиться на дві основні категорії: Management та Policy Components (Рис.3.4).

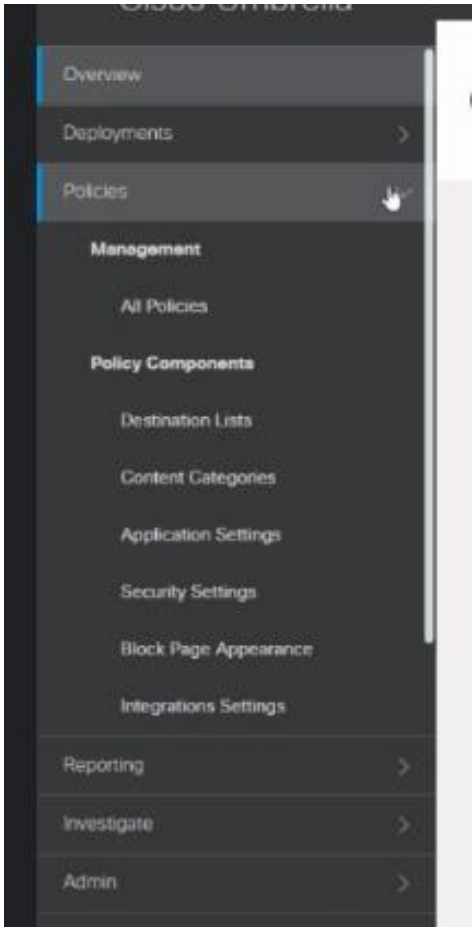

Рис.3.4. Категорії та підкатегорії Policies

В **Management** можна створити власну політику або використати ту, що стоїть за замовчуванням (Рис.3.5).

Політика за замовчуванням буде застосована для всіх об’єктів, а інші компоненти будуть використовувати налаштування за замовчуванням.

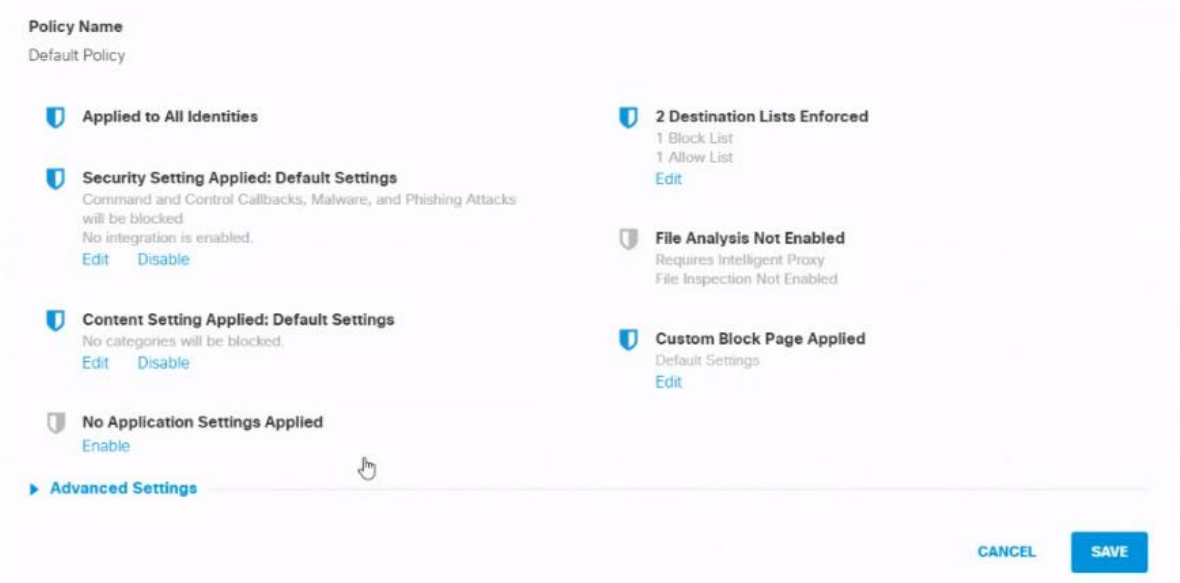

Рис.3.5 Політика за замовчуванням

Поетапне створення політики:

Для початку потрібно визначити, що саме потребуватиме захисту: мережі, користувачі чи групи, пристрої чи Chromebooks (Рис.3.6).

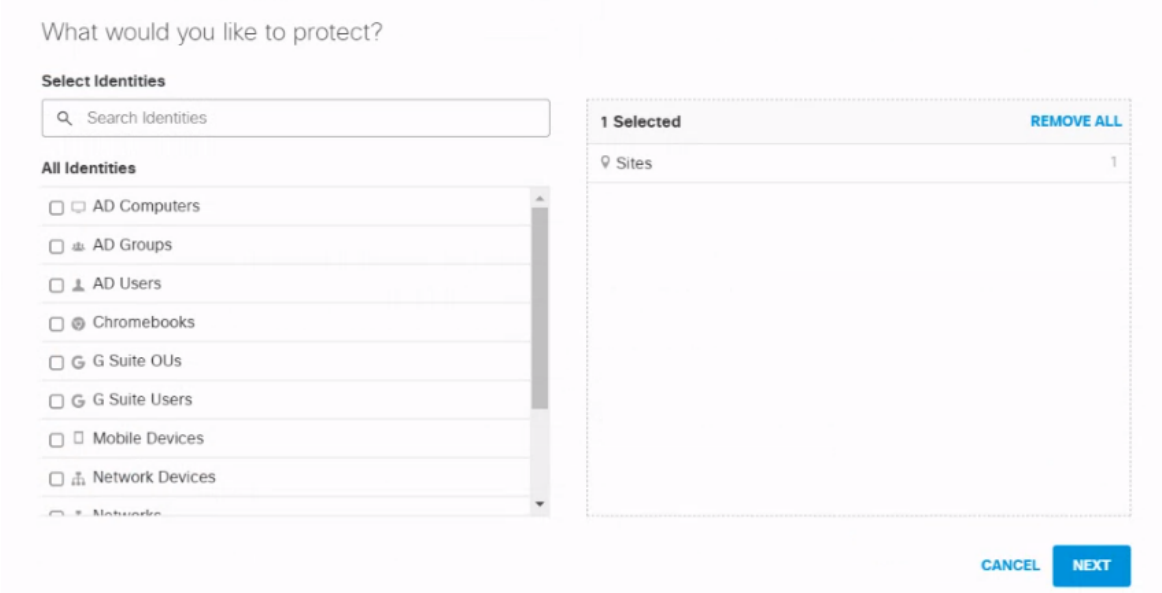

Рис.3.6. Обрання об’єктів для захисту

Після обрання всіх ключових об’єктів натискаємо **Next**. Далі потрібно обрати функціонал даної політики (Рис.3.7). Є п’ять основних компонентів:

– Забезпечення безпеки на рівні DNS: блокування всіх доменів, що містять шкідливе програмне забезпечення, якщо це фішингові сайти та інше.

– Перевірка файлів: вибірково перевіряє файли на наявність шкідливого вмісту за допомогою антивірусних сигнатур і розширеного захисту від шкідливих програм від Cisco.

– Обмеження доступу до вмісту: блокує або дозволяє сайти на основі їхнього вмісту.

– Керування додатками: блокує або дозволяє додатки або групи додатків для об’єктів, обраних даною політикою.

– Застосування списків призначення: блокує або дозволяє IP-адреси, домени або URL-адреси.

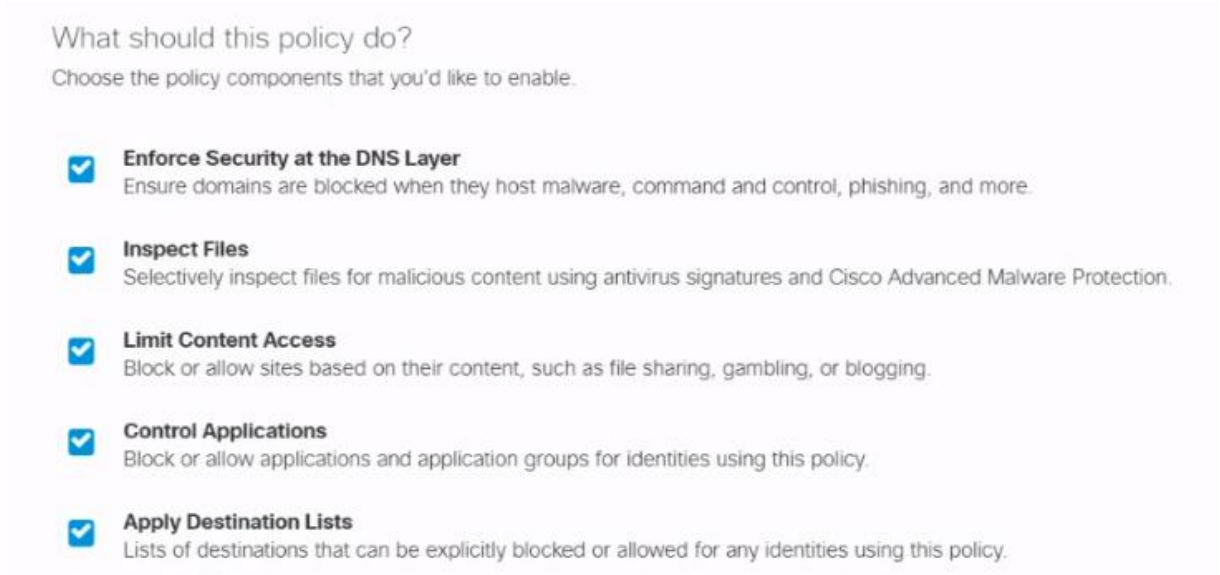

Рис.3.7. Компоненти політики

Після визначення функціоналу, який потрібно застосувати до нової політики натискаємо **Next**. Наступний крок – обрання категорій, які потрібно буде блокувати. Представлені наступні категорії:

– Шкідливе програмне забезпечення: сайти та інші сервіси, на яких розміщено шкідливе програмне забезпечення, скачування за замовчуванням, мобільні загрози та інше.

– Нові домени: домени, що з’явилися недавно, можуть бути використані для нових атак.

– Зворотній контроль та команди: запобігає зв’язку скомпрометованих пристроїв з інфраструктурою зловмисників.

– Фішинг: шахрайські веб-сайти, які обманом змушують користувачів надати особисту чи фінансову інформацію.

– Динамічний DNS: блокує сайти, що містять динамічний DNS.

– Потенційно шкідливі домени: домени, які демонструють підозрілу поведінку та можуть бути частиною атаки.

– DNS тунелювання VPN: служби VPN, які дозволяють користувачам маскувати свій трафік, тунелюючи його через протокол DNS, адже їх можна використовувати для обходу корпоративної політики щодо доступу та передачі даних.

– Криптомайнінг: дозволяє організаціям контролювати доступ криптомайнерів до криптовалютних ферм та веб-майнерів.

На слайді представленому нижче видно категорії обрані за замовчуванням (Рис. 3.8).

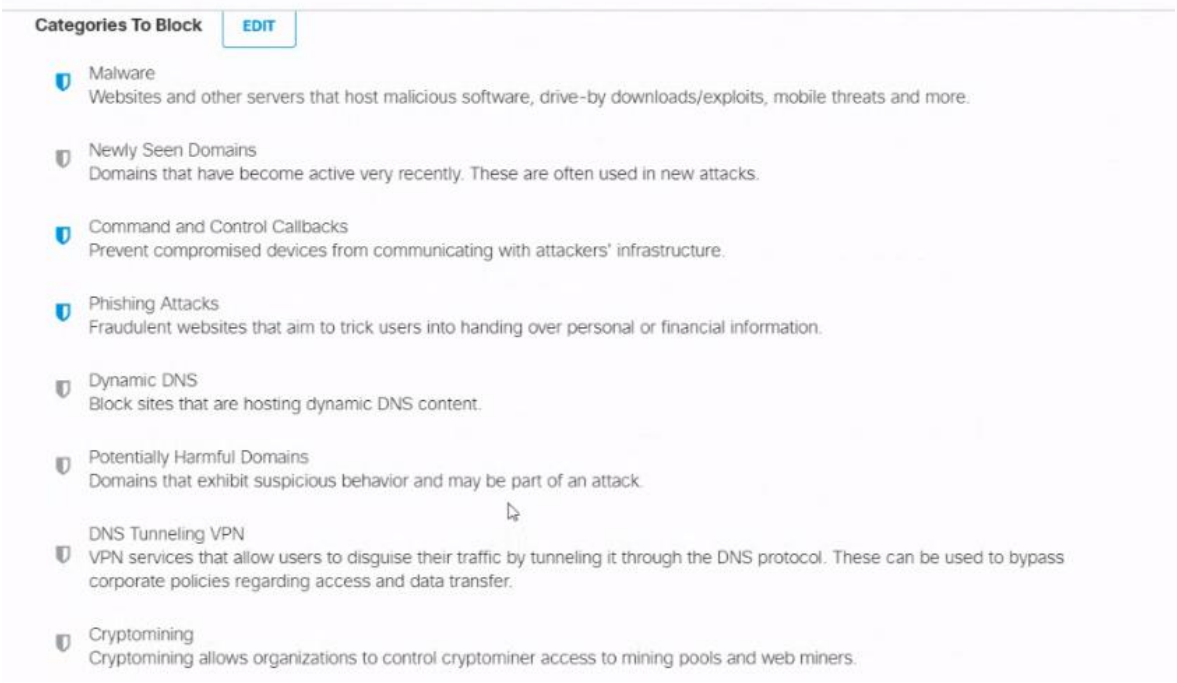

Рис.3.8. Категорій блокування

Обравши всі потрібні категорії, натискаємо **Next**. Далі обмежуємо доступ до контенту. Обираються категорії, щоб блокувати об’єктам доступ до веб-сайтів, які мають вміст такого типу. Є можливість обрати попередньо встановлені рівні контролю (Рис.3.9):

– High: блокує дорослий контент, незаконну активність, соціальні мережі та сайти, де можна ділитися файлами.

– Moderate: блокує дорослий контент та незаконну активність.

– Low: tasteless (до цієї категорії відносяться сайти, які містять образливі або насильницькі висловлювання, в тому числі в жартах, коміксах або сатирі, а також надмірне використання ненормативної лексики), дорослий контент та проксі веб-сайти.

Якщо ж ніякий з перелічених раніше рівнів контролю не задовольняє, можна створити власний з власноруч обраними категоріями: Custom.

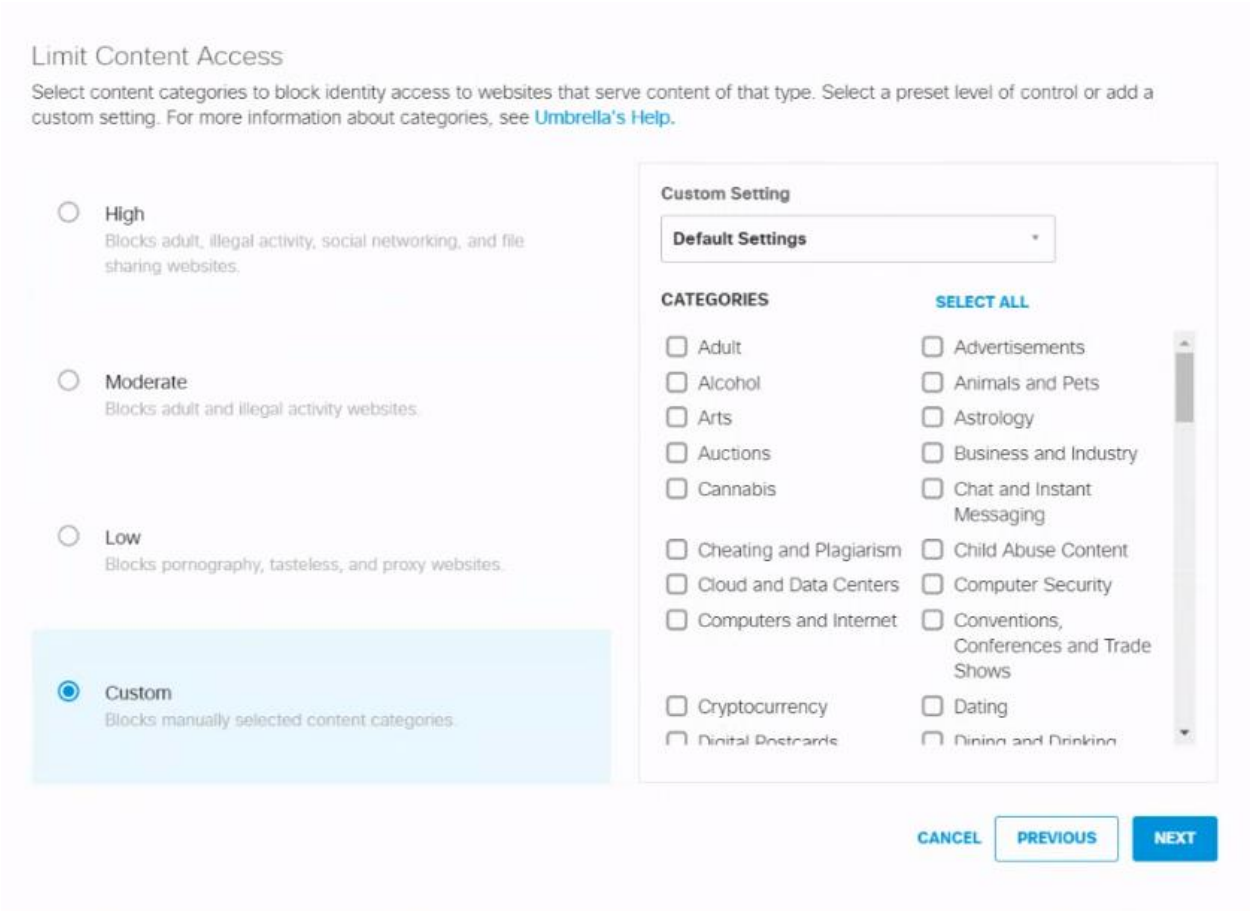

Рис.3.9. Категорії обмеження

Натискаємо **Next**. Переходимо до наступної функції Контроль програм (Рис.3.10). Тут потрібно обрати програми або категорії програм, які ми хочемо заблокувати або, навпаки, дозволити користувачам в компанії.

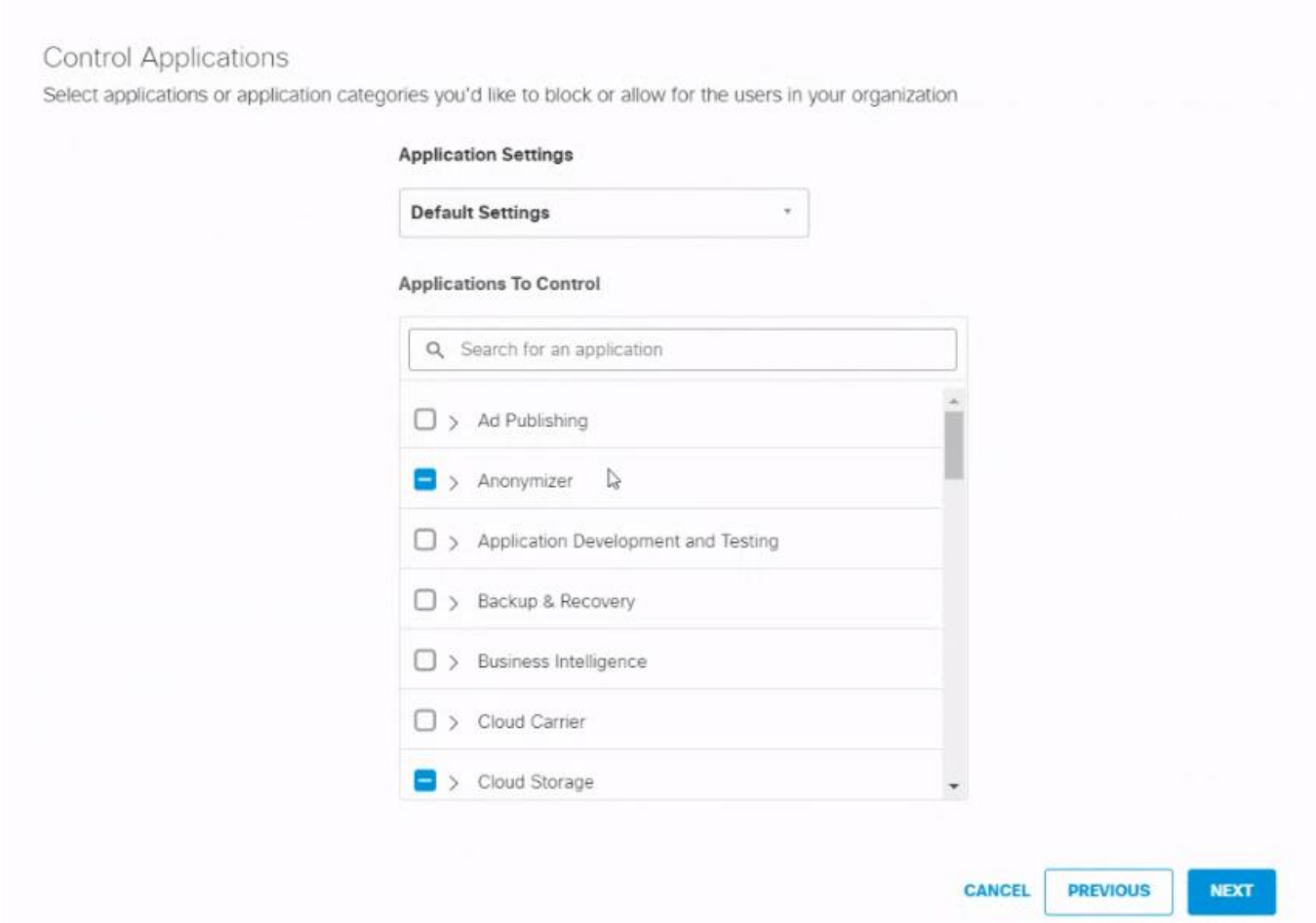

Рис.3.10. Категорії програм для контролю

Після цього потрібно застосувати списки призначення (Рис.3.11). Тут визначаються IP-адреси, домени або URL-адреси, які будуть дозволятися або блокуватися. Вони додаються в спеціальні списки Global Allow List та Global Block List – ці списки створені за замовчуванням. За потреби, є можливість створити нові списки.

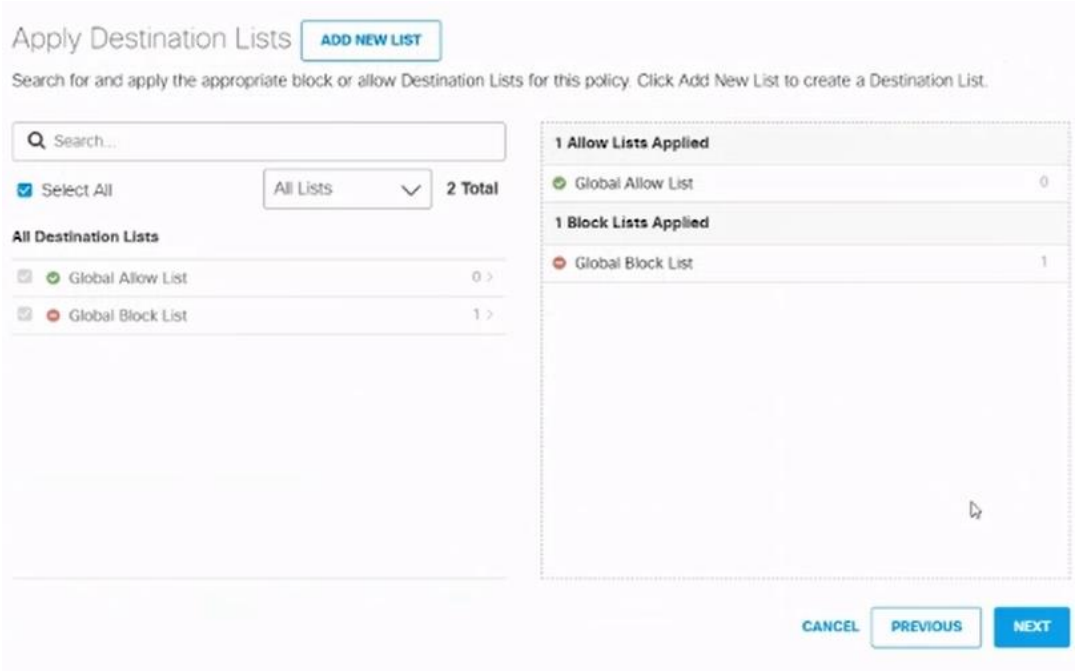

Рис.3.11. Обрання списків

Далі обираємо чи потрібен нам аналіз файлів (Рис.3.12). Буде відбуватися дослідження файлів на наявність підозрілої або шкідливої поведінки, використовуючи методи статичного та динамічного аналізу, також, буде братися до уваги репутація файлу та розширена евристика.

Рис.3.12. Аналіз файлів

Потім обираємо налаштування сторінки блокування (Рис.3.13). Є можливість обрати сторінку за замовчуванням (Рис.3.14) або ж індивідуальний зовнішній вигляд.

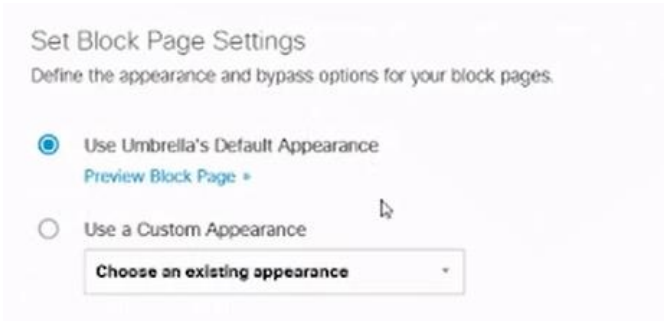

Рис.3.13. Налаштування сторінки блокування

Рис.3.14. Сторінка блокування за замовчуванням

Policy Components використовуються для того, щоб змінити вже існуючу політику, адже тут містяться всі функції, що використовувалися для створення політики.

3.5 Reporting

Ділиться на три основні категорії: Core Reports, Additional Reports та Management. В свою чергу, кожна з них поділяється ще на декілька підкатегорій (Рис.3.15):

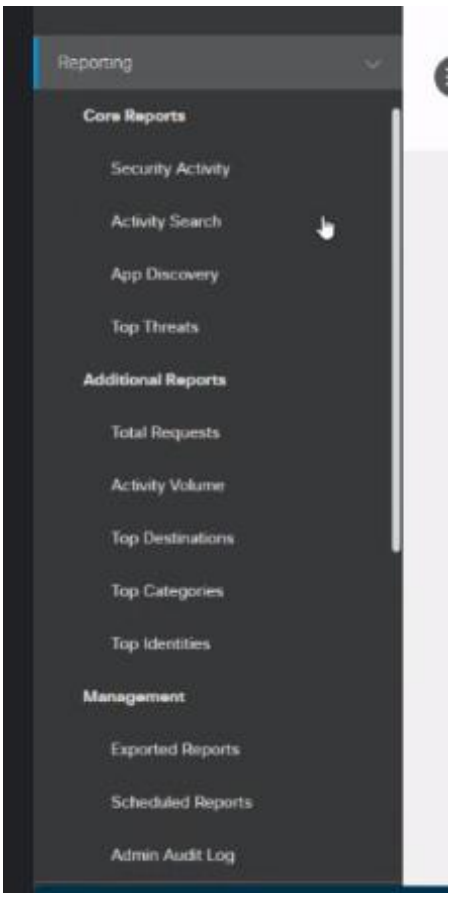

Рис.3.15. Категорії та підкатегорії Reporting

Core Reports:

Security Activity: показує небезпечну активність (Рис.3.16). Можна обрати час за який відбувалася ця активність: в останню годину, останні 24 години, вчора, цього тижня або останні 30 днів. Також, можна обрати тип активності, який цікавить нас, наприклад, антивірус схильний до шкідливих дій.

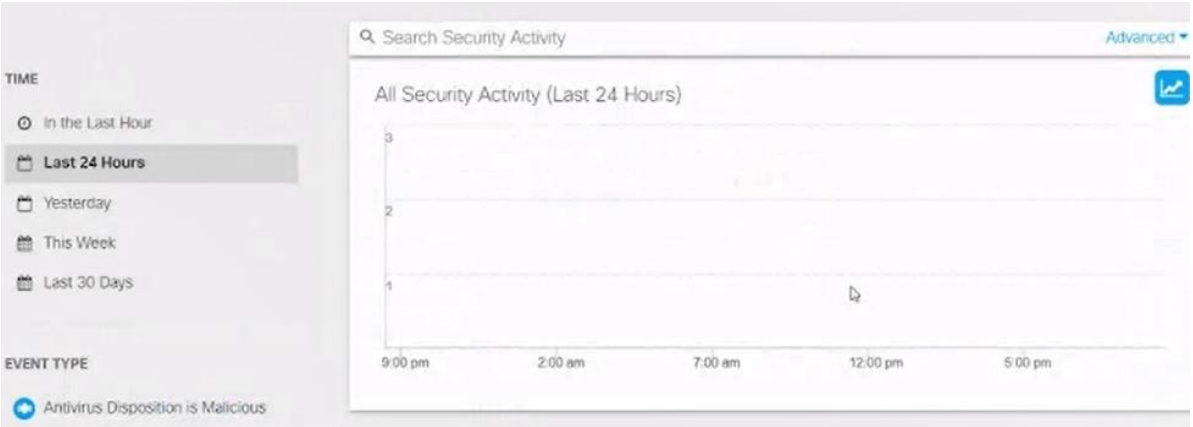

Рис.3.16. Показник небезпечної активності

Activity Search: на даній вкладці будуть відображатися всі шкідливі IP-адреси, домени та URL-адреси. Також, буде видно, які об’єкти намагалися отримати доступ до цих сайтів, яка саме шкідлива активність відбувалася на сайті. Можна обрати протокол HTTP або HTTPS, тип події та була ця подія заблокована чи дозволена.

App Discovery (Рис.3.17): на даній вкладці можна побачити які додатки зафіксувало дане рішення (Рис.3.18), їхню позначку (Unreviewed, Under Audit, Not Approved, Approved) та їх ризик (Very High, High, Medium, Low, Very Low).

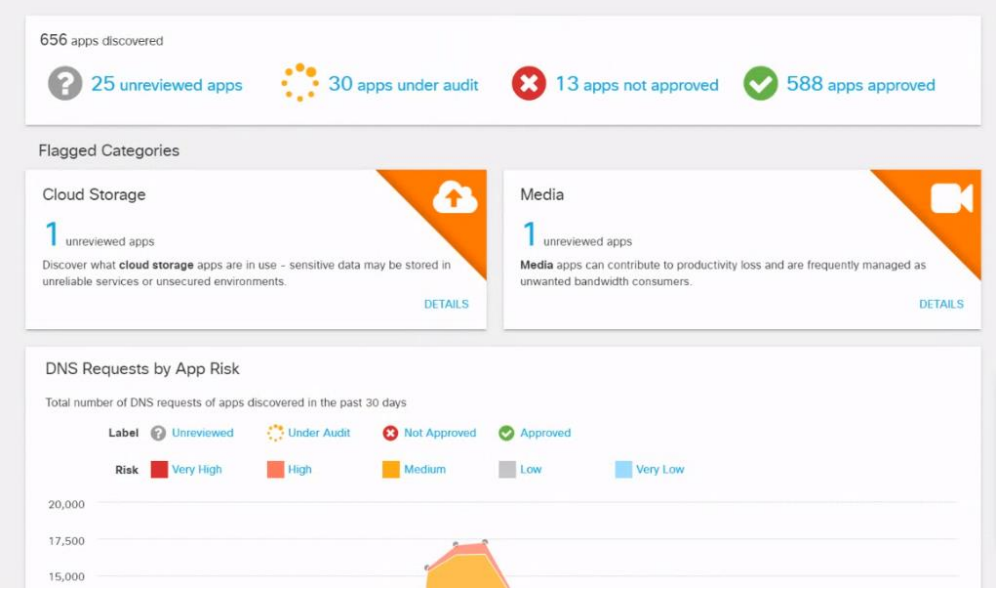

Рис.3.17. Зафіксовані додатки

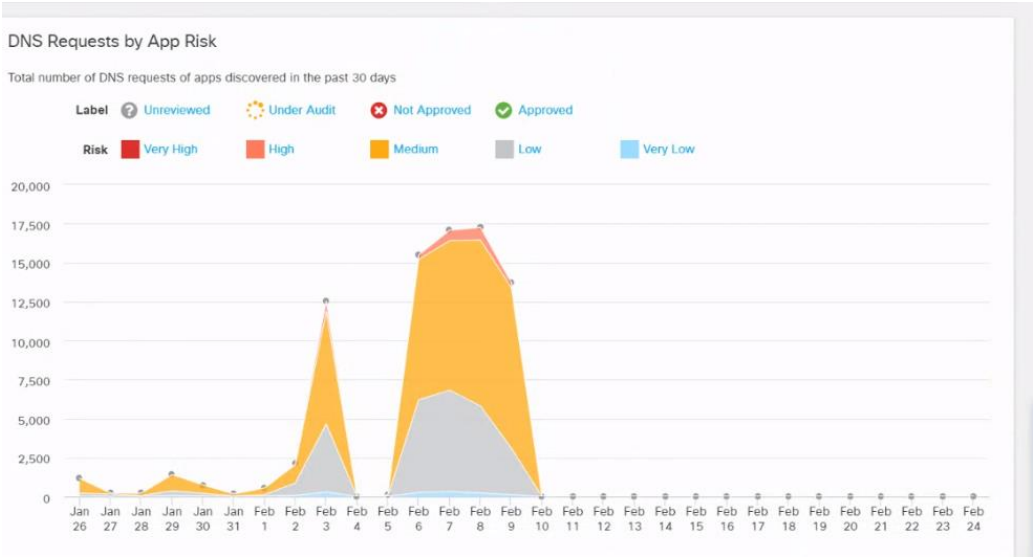

Рис.3.18. Час активності зафіксованих додатків

Top Threats (Рис.3.19): будуть відображатися всі загрози в середовищі.

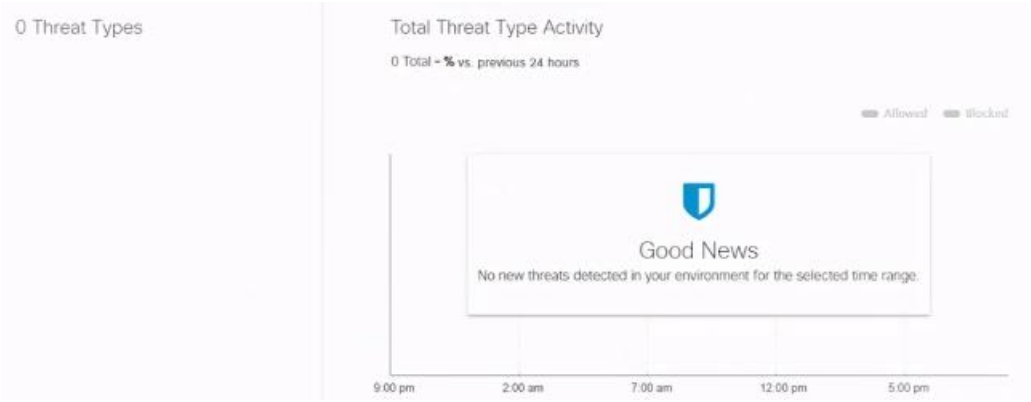

Рис.3.19. Результат перевірки на загрози в середовищі

Additional Reports:

Top Categories: показує, як багато хмарних застосунків було використано. У верхній частині таблиці наведені додатки з високим ступенем ризику, деякі з них є цілком законними, і в них немає нічого поганого, але вони все одно можуть бути ризикованими, якщо ними користується не та людина. Може показати репутацію продукту, а також те, чи має він якесь відношення до бізнесу та чи відповідає він вимогам постачальника. Можете встановити всі види політик і категорій як для додатків, так і для URL-адрес.

Activity Volume: можна побачити скільки загроз було зупинено та попереджено.

Management:

В даній вкладці можна створити звіт, експортувати його та запланувати його створення.

3.6 Duo

Завдяки зручним функціям для безпечного доступу, надійної автентифікації та моніторингу пристроїв, рішення для додатків і доступу MFA (багатофакторна автентифікація) і 2FA (двофакторна автентифікація) від Duo можуть полегшити забезпечення стійкості системи безпеки для компанії. Щоб підключитися до консолі Umbrella використовується двофакторна автетифікація від Duo. Дає змогу

підтвердити особу користувача будь-яким зручним методом двофакторної автентифікації, які ви можете налаштувати самі за допомогою push-сповіщень, біометрії, ключа безпеки, методами без під'єднання до мережі і не тільки.

Функції Duo:

– Перевірка довіри до будь-якого пристрою (Рис.3.20). Отримання контролю над пристроями – це перший крок до встановлення довіри до пристроїв, і це важливий аспект стратегії нульової довіри. Duo забезпечує видимість кожного пристрою у мережі та виконує перевірку стану при кожній спробі входу в систему. Duo допоможе виявити потенційні ризики, щоб була змога забезпечити відповідність вимогам і налаштувати параметри доступу для будь-якої ситуації. Завдяки потужним можливостям звітування та зручній для адміністратора інформаційній панелі, Duo дозволяє легко контролювати політики безпеки та виявляти аномальну активність входу в систему.

Рис.3.20. Перевірка пристрою від Duo

– Адаптивний доступ. Стратегія нульової довіри змінює рівень доступу або довіри на основі контекстних даних про користувача або пристрій, який хоче отримати доступ. Вона також надає доступ лише тим користувачам, яким він дійсно потрібен. За допомогою Duo можна налаштувати детальні політики за лічені хвилини за допомогою простої панелі адміністратора, а також керувати правилами глобально або для певних додатків чи груп користувачів. Визначає

місцезнаходження користувача, пристрій, роль і багато іншого при кожному вході. Політики безпеки встановлюються на основі цих атрибутів

Висновки до третього розділу

Розглянуто принципи налаштування та компоненти Cisco Umbrella та Duo.

Показано поетапне створення політики, перевірка заблокованого сайту та налаштована перевірка пристрою від Duo.

Розроблено рекомендації щодо впровадження даного рішення в організації.

ВИСНОВКИ

У бакалаврській роботі отримано наступні теоретичні та наукові результати:

– проаналізовано, які є види атак та загроз для віддаленої роботи, які є методи запобігання та виявлення цих загроз;

– визначено, що людський фактор є джерелом кіберзагроз, через недостатній рівень професійної підготовки, що призводить до завдання збитків компаніям;

– розглянуто хмарні рішення для забезпечення захищеної роботи працівників організації;

– досліджено рішення Cisco Umbrella та Duo, розглянуто принципи налаштування та компоненти;

– розроблено рекомендації щодо забезпечення захищеної віддаленої роботи працівників на базі рішення Duo Umbrella.