ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення мережевого доступу з нульовою довірою на базі рішення Cisco»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Анастасія ШАЙКОВА
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ШАЙКОВА Анастасія
(прізвище, ім'я)

Керівник д.т.н., проф. ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ВСТУП

Актуальність роботи. Розвиток інформаційно-комунікаційних технологій у сучасному світі відкриває нові можливості для наукових досліджень, промисловості та суспільства в цілому. Безпеці інформаційних ресурсів серйозно загрожує зростання кількості кібератак, що збігається з перевагами цифрової трансформації. З появою хмарних технологій, мобільних пристроїв і віддаленої роботи кордони, що розділяють корпоративні мережі, стають все більш розмитими, що робить традиційні стратегії кібербезпеки, засновані на парадигмі «захисту периметра», застарілими. Ідея нульової довіри стає найпопулярнішою стратегією захисту даних і мереж у цих умовах.

Сучасна тактика, відома як «нульова довіра», ґрунтується на ідеї «перевіряй все, не довіряй нікому». Усунення неявної довіри до пристроїв і користувачів, як всередині, так і поза корпоративною мережею, є її основною концепцією. Це гарантує надійний захист даних і зменшує можливість небажаного доступу. Багатофакторна автентифікація, мікросегментація мережі, контроль доступу на основі ролей і динамічна оцінка ризиків – ось деякі з компонентів, що складають Zero Trust.

Завдяки своїй ефективності та креативності рішення Cisco для доступу до мережі з нульовою довірою (ZTNA) лідирують на ринку. Незалежно від місця розташування, такі інструменти, як Cisco Duo, Cisco Secure Access і Cisco Umbrella, пропонують комплексний підхід до захисту даних, додатків і пристроїв. Вони дозволяють компаніям створювати безпечну, масштабовану та адаптивну IT-інфраструктуру, яка відповідає сучасним стандартам кібербезпеки.

Метою цієї роботи є надання рекомендацій щодо розгортання технологій доступу до мережі з нульовою довірою на базі Cisco. Для цього розглядаються основні ідеї концепції Zero Trust, оцінюються поточні стратегії впровадження ZTNA та формулюються корисні пропозиції для організацій. Особливу увагу

приділено впливу Zero Trust на посилення безпеки та гарантування безперервності бізнес-процесів.

Об'єкт дослідження – забезпечення мережевого доступу з нульовою довірою.

Предмет дослідження – технологія забезпечення мережевого доступу з нульовою довірою на базі рішення Cisco.

Мета роботи – розробити порядок впровадження технології забезпечення мережевого доступу з нульовою довірою на базі рішення Cisco.

Наукові завдання:

дослідити сутність концепції нульової довіри (Zero Trust), зокрема її роль у забезпеченні безпеки інформаційних ресурсів в умовах сучасного цифрового середовища;

проаналізувати підходи до забезпечення безпечного мережевого доступу за принципами нульової довіри, включаючи ключові компоненти архітектури Zero Trust;

проаналізувати існуючі рішення для реалізації Zero Trust Network Access (ZTNA), зосередившись на рішеннях провідних постачальників, таких як Cisco, Fortinet, Palo Alto Networks, тощо;

дослідити методи та засоби забезпечення безпечного мережевого доступу на базі рішень Cisco, зокрема Cisco Secure Access та Cisco Umbrella;

розробити порядок впровадження технології забезпечення мережевого доступу з нульовою довірою на базі рішень Cisco, враховуючи практичні рекомендації з налаштування та управління.

Методи дослідження – вивчення літератури з питань мережевого доступу з нульовою довірою, вивчення інструкцій з експлуатації продуктів Cisco Secure Access та Cisco Umbrella, дослідження стандартів кібербезпеки. Для оцінки ефективності рішень та їх адаптації до сучасних вимог захисту інформаційних ресурсів організацій було використано порівняльний аналіз.

Практичне значення одержаних результатів: запропоновано процес впровадження технології доступу до мережі з нульовою довірою на базі Cisco. Результати роботи можуть бути використані в сучасних методах гарантування

безпеки даних у бізнес-мережах, посилення захисту в гібридному середовищі та підвищення рівня кіберстійкості організації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 КОНЦЕПЦІЯ НУЛЬОВОЇ ДОВІРИ (ZERO TRUST)

1.1 Що таке Zero Trust

Ідея нульової довіри існувала в кібербезпеці ще до того, як з'явилася фраза «zero trust». Міністерство оборони США та Агентство оборонних інформаційних систем (DISA) опублікували своє дослідження щодо більш безпечного підходу для підприємств, відомого як «чорне ядро» (BCORE). Частиною «чорного ядра» є перехід від підходу до безпеки, що базується на периметрі, до підходу, що ставить на перше місце безпеку транзакцій. Концепція деперіметризації – обмеження неявної довіри відповідно до місця розташування мережі та недоліки залежності від єдиного статичного захисту у великому сегменті мережі – була оприлюднена в роботі Форуму в Єрихоні в 2004 році (JERICHO). Пізніше Джон Кіндерваг розвинув ширшу ідею нульової довіри під час роботи в компанії Forrester [1], спираючись на ідеї деперіметеризації. Фраза «zero trust» була введена для позначення низки рішень з кібербезпеки, які змістили акцент безпеки від неявної довіри, заснованої на розташуванні мережі, до оцінки довіри за кожною транзакцією. Перехід від безпеки, що базується на периметрі, до підходу, заснованого на принципах нульової довіри, також відбувся в комерційному секторі та у вищій освіті.

Згідно з концепцією IT-безпеки, відомої як «безпека з нульовою довірою», всі пристрої та користувачі, які намагаються отримати доступ до ресурсів у приватній мережі, повинні пройти сувору перевірку особи, незалежно від того, чи знаходяться вони всередині або за межами периметра мережі. Хоча ZTNA є основною технологією, пов'язаною з архітектурою zero trust, zero trust – це комплексна стратегія мережевої безпеки, яка об'єднує низку інших технологій і концепцій.

Іншими словами, типова безпека IT-мереж передбачає, що все і всі в мережі заслуговують на довіру. В архітектурі з нульовою довірою ніщо і ніхто не заслуговує на довіру.

Парадигма «castle-and-moat» [2] (згідно з концепцією мережевої безпеки «castle-and-moat», кожен всередині мережі може отримати доступ до даних, але ніхто поза мережею не може. Уявіть собі периметр мережі як рів, а мережу організації – як фортецю (рис. 1.1). Як тільки підйомний міст опускається, будь-хто може безперешкодно увійти на територію замку. Відповідно до цієї парадигми, користувач може отримати доступ до всіх даних і додатків у мережі, як тільки він встановив з'єднання) є основою традиційної безпеки IT-мереж. При захисті за даним принципом усім всередині мережі автоматично довіряють, але доступ ззовні мережі ускладнений. Проблема цієї стратегії полягає в тому, що зловмисник отримує повний контроль над мережею, як тільки він потрапляє в неї.

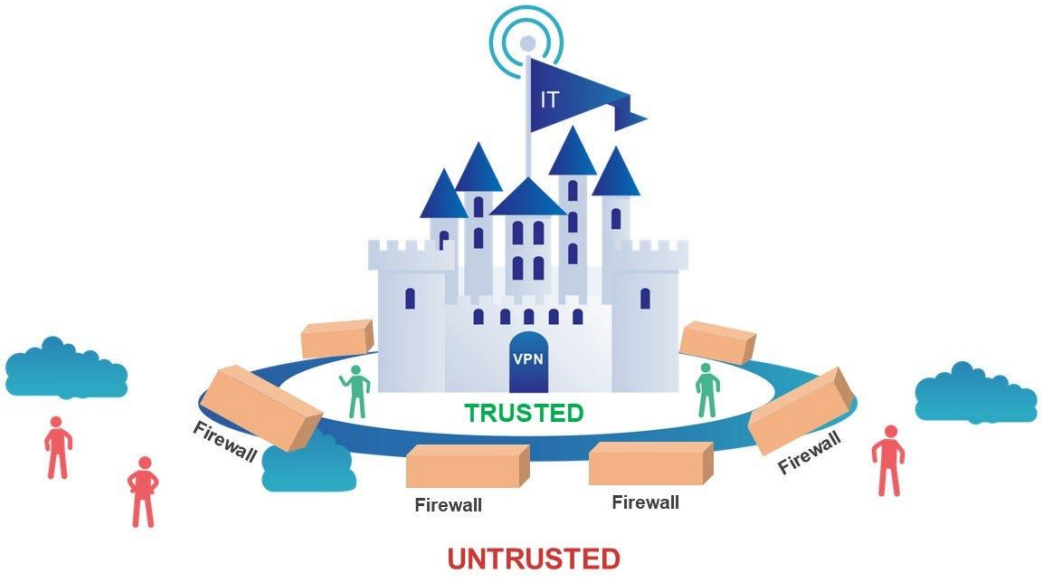

Рис. 1.1. Парадигма «castle-and-moat»

Той факт, що компанії більше не зберігають свої дані в одному місці, робить рішення з замкненим ровом набагато більш вразливими. Сьогодні дані часто розпорошені між хмарними провайдерами, що ускладнює встановлення єдиного контролю безпеки для всієї мережі.

Кожен, хто намагається отримати доступ до мережевих ресурсів, повинен підтвердити свою особу, оскільки безпека з нульовою довірою означає, що за замовчуванням нікому не довіряють ні в мережі, ні за її межами. Було продемонстровано, що цей додатковий рівень безпеки зупиняє вторгнення даних. Згідно з дослідженнями, один витік даних часто коштує понад 3 мільйони доларів. Не дивно, що з огляду на цю цифру, багато фірм зараз прагнуть впровадити стратегію безпеки zero trust.

У звіті Cisco «Security Outcomes for Zero Trust: Adoption, Access, and Automation Trends» детально описано, як компанії використовують безпеку з нульовою довірою для досягнення результатів. Існує безліч схвалених галузевих моделей зрілості для нульової довіри, від приватних дослідницьких фірм, таких як Forrester на рис. 1.2, до державних агентств, таких як CISA (Cybersecurity Infrastructure and Security Agency – Агентство з кібербезпеки та безпеки інфраструктури США). Звіт Cisco не має на меті замінити жодну з них. Компанія висвітлює історії та дані, що відображають те, як команди бачать власну організаційну зрілість на основі кейсів використання та можливостей, які вони розгорнули в рамках zero trust pillars. На рис. 1.3 показано відсоток організацій, які починають (яскраво-синій колір) або досягають зрілості (градієнт від синього до зеленого).

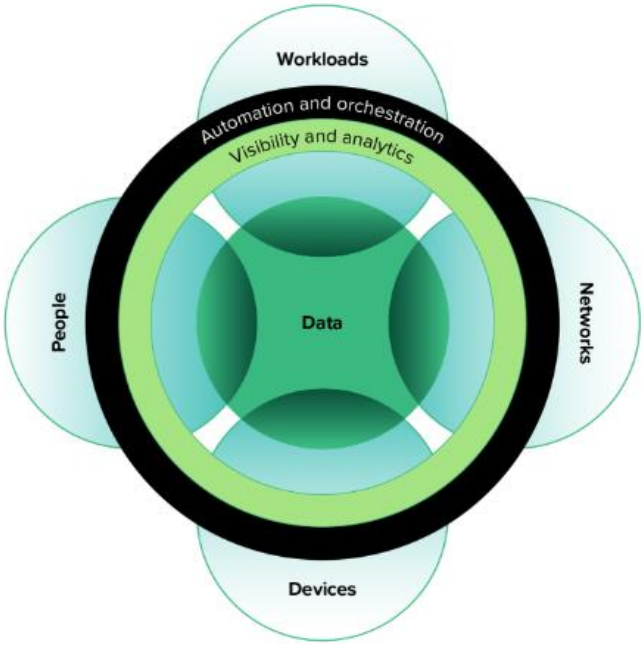

Рис. 1.2. Forrester’s Zero Trust Model Of Information Security

Серед основних положень можна виділити наступні:

1. Коли йдеться про запобігання атакам і зниження ймовірності інциденту, багатофакторна автентифікація (MFA) все ще залишається найефективнішим засобом контролю.

2. На сприйняття організаціями нульової довіри найбільше вплинуло використання автоматизації та оркестрування.

3. В організаціях, які впровадили всі компоненти нульової довіри, кількість проблем зі звітністю знизилася вдвічі – з 66% до 33%.

4. Компанії, які досягли прогресу в області ідентифікації, майже на 11% рідше стикаються з інцидентами, пов’язаними з вимогами викупу, ніж ті, які цього не зробили.

Принципи нульової довіри, які стосуються даного звіту:

- Identity

Multi-factor authentication (MFA)

Enterprise single sign-on (SSO)

Role-based access control (RBAC)

- Device

Continuous validation of users and devices

Endpoint detection and response (EDR)

Risk-based vulnerability management

- Network and Workload

Network detection and response (NDR)

Micro-segmentation of application workloads

- Automation and Orchestration

Orchestrated workflows

Automation and response

Security Orchestration and Automated Response (SOAR)

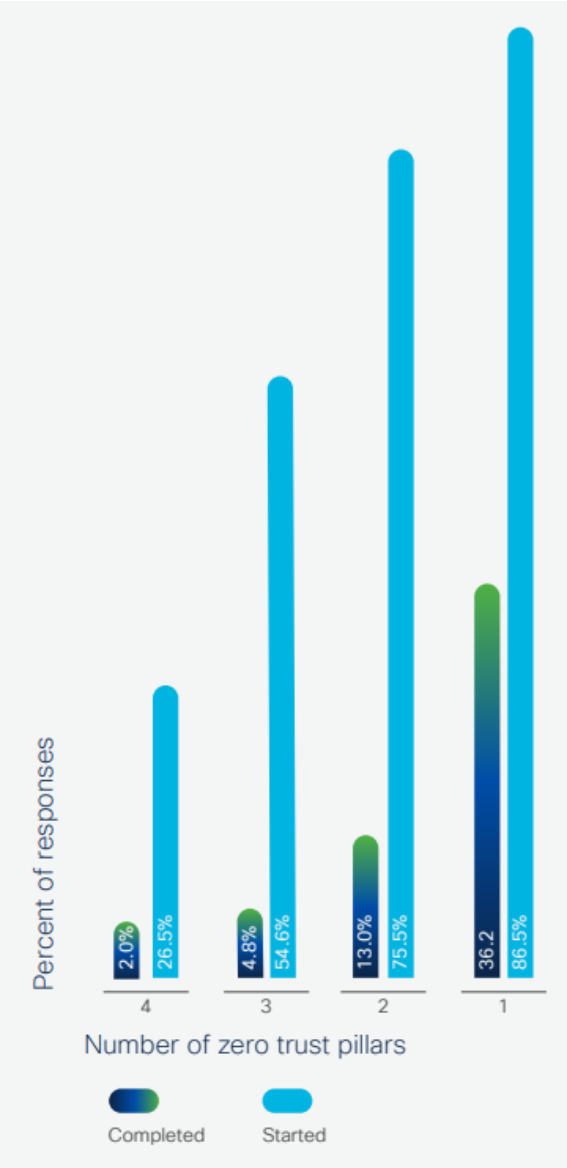

Рис. 1.3. Number of zero trust pillars

Було опитано 4751 активних фахівця з інформаційної безпеки з 26 країн. Інститут Cyentia провів незалежний аналіз даних опитування від імені Cisco і підготував усі результати (рис. 1.4).

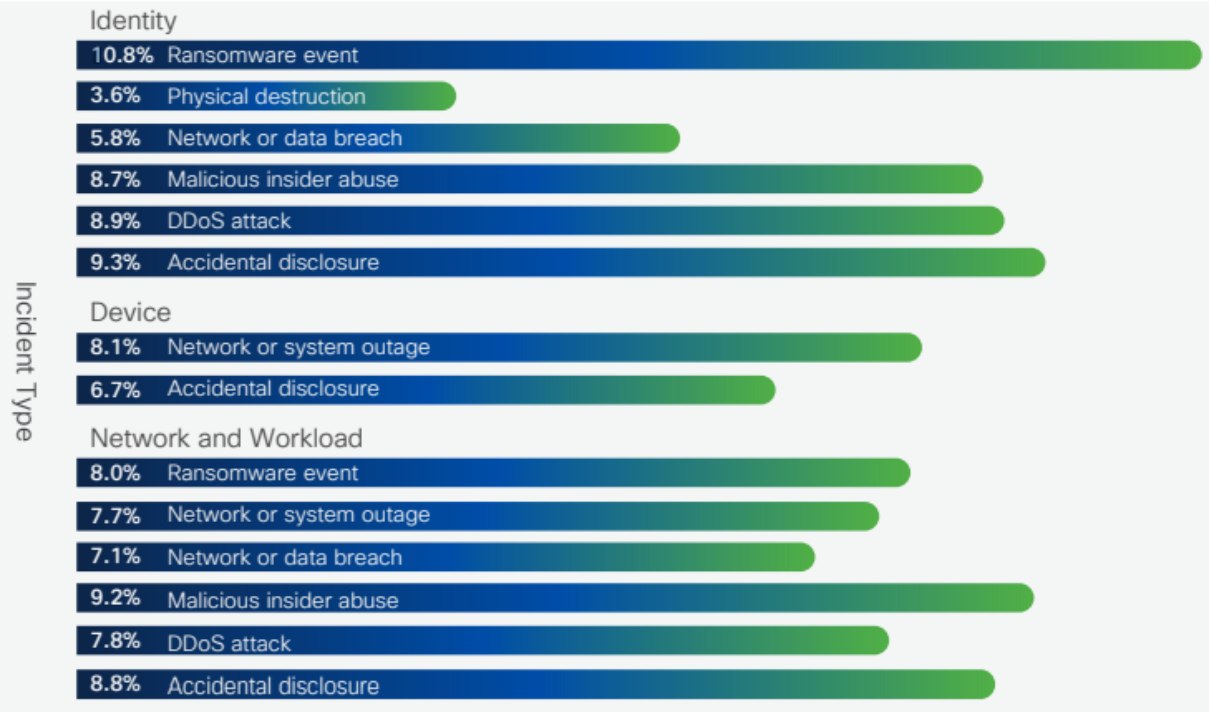

Рис. 1.4. Зменшення ймовірності інцидентів у відсотках

1.2 Аналіз загроз та ризиків ZTNA

Технологія Zero Trust Network Access (ZTNA) пропонує високий рівень безпеки, але вона також має певні загрози та вразливості. Ось основні з них:

- Фішингові атаки

Одним з найпопулярніших способів компрометації облікових даних залишається фішинг, який становить значний ризик для ZTNA. Спроби фішингу, такі як підроблені електронні листи або фальшиві сторінки входу, які створюють видимість безпечного середовища, все ще можуть впливати на користувачів навіть із ZTNA. Зловмисник може спробувати отримати доступ, використовуючи отримані облікові дані, якщо атака буде успішною. Однак ймовірність таких атак зменшується завдяки постійній автентифікації та верифікації ZTNA.

- Соціальна інженерія

Оскільки навіть найзахищеніші мережі вразливі до психологічних маніпуляцій, які можуть призвести до передачі паролів або інших конфіденційних даних, соціальна інженерія також становить серйозний ризик. Наприклад, щоб

обійти систему безпеки, зловмисники можуть прикидатися співробітниками технічної підтримки і випитувати важливу інформацію.

Identity (тобто користувач та його пристрій) – це периметр для атак. Постійний рух до цифрової трансформації, перехід до хмарних технологій, гібридна робота, взаємозв'язок бізнесу (ланцюжок поставок) і мобільність – все це розмиває класичні мережеві кордони. Користувач є першою, останньою, а іноді і єдиною лінією оборони організації між зловмисником і ресурсами, на які він націлений.

Зловмисники активно використовують прогалини та слабкі місця в цій розширеній поверхні атаки, а не лише в самій технології. Зловмисники успішно знаходять способи обійти слабші реалізації безпеки, включаючи автентифікацію та управління доступом. Тепер сама поведінка користувачів стає більш цілеспрямованою, що є ризиком, який, ймовірно, тільки зростатиме, оскільки інструменти для цього прості у використанні. Бар'єри для складних атак знижуються завдяки AI/ ChatGPT, які просувають фішингові електронні листи, push-фішингові атаки та набори для крадіжки облікових даних. Деякі з цих злочинних організацій навіть мають технічну підтримку.

- Зловживання привілеями

Користувачі високого рівня, які навмисно або ненавмисно зловживають своїми привілеями для доступу до ресурсів або приватних даних поза межами своїх службових обов'язків, становлять таку небезпеку. Коли користувачі намагаються збільшити свій рівень доступу для виконання дій, до яких вони не мають права. Це може включати спроби обійти обмеження системи безпеки або отримати адміністративний доступ до ресурсів. Користувачі мають можливість взаємодіяти з даними або системами, що не входять у їхні безпосередні обов'язки. Надмірний доступ створює додатковий вектор для зловживань.

- Недосконалість налаштувань політик доступу

Небезпечний доступ до життєво важливих ресурсів, ненавмисне надання надмірних прав або нездатність виявити незвичні дії можуть бути наслідком неправильно встановлених політик доступу або рідкісних перевірок. Користувачі

можуть взаємодіяти з ресурсами, які їм не потрібні для виконання своїх посадових обов'язків, коли права доступу обмежені неналежним чином. Це підвищує ймовірність зловживання доступом або несанкціонованого доступу до приватної інформації. Регулярне оновлення політик доступу необхідне, щоб врахувати зміни в кадровому складі, обов'язках та загрозах. Якщо цього не робити, може накопичитися занадто багато надмірних або неактуальних доступів.

1.3 Архітектура та ключові аспекти

Наскрізна стратегія захисту бізнес-ресурсів і даних, архітектура нульової довіри охоплює ідентифікацію (як людей, так і об'єктів), облікові дані, контроль доступу, операції, кінцеві точки, хостингові середовища та інфраструктуру, яка їх з'єднує. Обмеження доступу до ресурсів лише тими, кому вони потрібні, і надання лише мінімальних привілеїв (читання, запис і видалення), необхідних для досягнення мети, має бути першочерговим пріоритетом. Установи (і бізнес-мережі загалом) історично надавали пріоритет захисту периметру, а після входу у внутрішню мережу аутентифіковані користувачі отримують дозволений доступ до широкого спектру послуг. Тому несанкціонована латеральна мобільність у середовищі є однією з головних проблем, з якими стикаються державні органи.

Це визначення зосереджується на головній меті – запобігти несанкціонованому доступу до даних і сервісів, а також забезпечити контроль доступу настільки точно, наскільки це можливо. Іншими словами, лише уповноважені та схвалені суб'єкти – користувач, додаток, служба та пристрій – можуть отримати доступ до даних, виключаючи всіх інших суб'єктів або зловмисників. Якщо піти далі, то ZT можуть стосуватися доступу до ресурсів (таких як принтери, обчислювальні ресурси і виконавчі пристрої Інтернету речей), а не просто доступу до даних, використовуючи словосполучення «ресурс» замість «дані».

Основна увага приділяється аутентифікації, авторизації та зменшенню неявних зон довіри при збереженні доступності та зменшенні часових затримок у

методах аутентифікації з метою зменшення невизначеності (оскільки їх неможливо повністю усунути). Для того, щоб забезпечити мінімальні права, необхідні для виконання дії в запиті, правила доступу робляться настільки деталізованими, наскільки це можливо.

Згідно з абстрактною концепцією доступу на рис. 1.5, суб'єкт повинен мати доступ до ресурсу підприємства. Policy decision point [3] (PDP – системний об'єкт, який оцінює застосовну політику та приймає рішення про надання дозволу. Цей термін визначено спільними зусиллями робочої групи IETF Policy Framework та Distributed Management Task Force) та відповідна policy enforcement point [3] (PEP – системний об'єкт, який виконує контроль доступу, роблячи запити на прийняття рішень і забезпечуючи виконання рішень про авторизацію. Цей термін також визначено спільними зусиллями робочої групи IETF Policy Framework та Distributed Management Task Force).

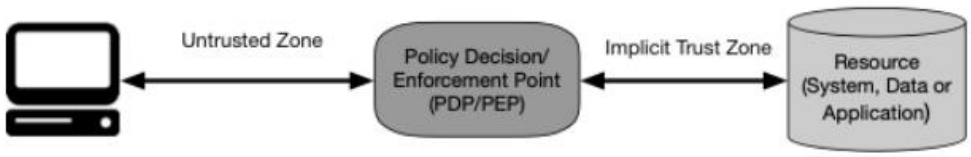

Рис. 1.5. Zero Trust Access

Коли організація обирає нульову довіру як основний підхід, вона створює архітектуру нульової довіри, тобто план, заснований на принципах нульової довіри. Потім організація може використовувати цей план для створення середовища нульової довіри.

Система повинна перевірити, що запит є законним, а тема – реальною. Суб'єкт отримує доступ до ресурсу після того, як PDP/PEP виносить відповідне рішення [3]. Це означає, що дозвіл і автентифікація є двома фундаментальними сферами, де застосовується нульова довіра. Наскільки достовірною є ідентифікація суб'єкта конкретного запиту? З огляду на ступінь довіри до ідентифікації суб'єкта, чи дозволений доступ до ресурсу? Чи має пристрій, на якому виконується запит, належний рівень безпеки? Чи існують якісь додаткові змінні (такі як час,

місцезнаходження суб'єкта або стан його безпеки), які слід взяти до уваги і які змінюють ступінь довіри?

Загалом, підприємствам необхідно розробити та підтримувати динамічні політики доступу до ресурсів на основі оцінки ризиків, а також створити систему, яка забезпечить правильне та послідовне застосування цих політик для окремих запитів на доступ до ресурсів. Це означає, що підприємство не повинно покладатися на надійність, що може бути виявлена тільки через свої зв'язки з іншими об'єктами чи процесами, за якої, якщо суб'єкт пройшов базовий рівень автентифікації (наприклад, увійшов до ресурсу), всі наступні запити на доступ до ресурсу вважаються однаково дійсними.

Ідея відмови від широкомасштабного захисту периметра (наприклад, бізнес-фаєрволів) підкреслюється в багатьох визначеннях ZT і дискусіях. Однак, як частина функціональних можливостей ZTA, більшість цих визначень все ж таки посилаються на периметри (наприклад, мікроперіметри – дрібніші, контрольовані межі всередині мережі або мікросегментацію – поділ мережі на ізольовані сегменти; див. Розділ 3.1). Це спроба описати ZT та ZTA з точки зору фундаментальних принципів, які мають бути включені, а не того, що не включено. Ці принципи представляють найкращий спосіб дій, однак, не кожен принцип може бути використаний у своїй найчистішій формі для конкретної стратегії.

Архітектура нульової довіри розробляється і розгортається з дотриманням наступних основних принципів нульової довіри:

1. **Всі джерела даних та обчислювальні сервіси вважаються ресурсами.** Мережа може складатися з декількох класів пристроїв. У мережі також можуть бути малогабаритні пристрої, які надсилають дані до агрегаторів/сховищ, програмне забезпечення як послуга (SaaS), системи, що надсилають інструкції виконавчим механізмам, та інші функції. Крім того, підприємство може вирішити класифікувати особисті пристрої як ресурси, якщо вони можуть отримати доступ до ресурсів, що належать підприємству.

2. **Уся комунікація захищена незалежно від місця розташування мережі.** Місцезнаходження мережі саме по собі не означає довіру. Запити на доступ

до ресурсів, розташованих у мережевій інфраструктурі підприємства (наприклад, всередині периметра застарілої мережі), повинні відповідати тим самим вимогам безпеки, що й запити на доступ і зв'язок з будь-якої іншої мережі, що не належить підприємству. Іншими словами, довіра не повинна надаватися автоматично на основі того, що пристрій знаходиться в мережевій інфраструктурі підприємства. Вся комунікація повинна здійснюватися у найбільш безпечний спосіб, захищати конфіденційність і цілісність, а також забезпечувати автентифікацію джерела.

3. **Доступ до окремих ресурсів підприємства надається на основі сеансу.** Перед наданням доступу оцінюється довіра до заявника. Доступ також повинен надаватися з найменшими привілеями, необхідними для виконання завдання. Це може означати лише «нещодавно» для цієї конкретної транзакції і не відбуватися безпосередньо перед ініціюванням сеансу або виконанням транзакції з ресурсом. Однак автентифікація та авторизація на одному ресурсі не надають автоматично доступ до іншого ресурсу.

4. **Доступ до ресурсів визначається динамічною політикою, що включає спостережуваний стан ідентичності клієнта, програми/сервісу та ресурсу, що запитує, а також може включати інші поведінкові та середовищні атрибути.** Організація захищає ресурси, визначаючи, які ресурси вона має, хто є її членами (або можливість автентифікації користувачів з об'єднаної спільноти), і який доступ до ресурсів потрібен цим членам. Для нульової довіри ідентифікація клієнта може включати обліковий запис користувача (або ідентифікатор служби) і будь-які пов'язані з ним атрибути, призначені підприємством для цього облікового запису, або артефакти для автентифікації автоматизованих завдань. Запит стану активу може включати характеристики пристрою, такі як встановлені версії програмного забезпечення, мережеве розташування, час/дату запиту, поведінку, що спостерігалася раніше, та встановлені облікові дані. Поведінкові атрибути включають, але не обмежуються автоматизованою аналітикою суб'єктів, аналітикою пристроїв і виміряними відхиленнями від спостережуваних шаблонів використання. Політика – це набір правил доступу, заснованих на атрибутах, які організація призначає суб'єкту, активу даних або додатку. Атрибути середовища

можуть включати такі фактори, як місцезнаходження мережі запитувача, час, повідомлення про активні атаки тощо. Ці правила та атрибути базуються на потребах бізнес-процесу та прийнятному рівні ризику. Політики доступу до ресурсів і дозволів на дії можуть відрізнятися залежно від чутливості ресурсу/даних. Принцип найменших привілеїв застосовується для обмеження як видимості, так і доступності.

5. **Підприємство контролює та вимірює цілісність та рівень безпеки всіх власних та пов'язаних з ними активів.** Довіра не притаманна жодному активу. Оцінюючи запит на ресурси, організація враховує стан захищеності активу. Організація, що використовує ZTA, повинна створити систему безперервної діагностики та усунення наслідків (CDM) або аналогічну систему, щоб відстежувати стан пристроїв і додатків та застосовувати патчі або виправлення в разі потреби. Пристрої, що належать підприємству або пов'язані з ним, які вважаються найбільш захищеними, можуть мати інший режим, ніж активи, які піддаються підриву, мають відомі вразливості та/або не управляються підприємством. Таке ставлення може включати заборону всіх підключень до ресурсів підприємства. Це також може стосуватися пов'язаних пристроїв (наприклад, приватних пристроїв), яким може бути дозволено доступ до одних ресурсів, але не до інших. Для того, щоб запропонувати дієві дані про поточний стан корпоративних ресурсів, також має бути створена потужна система моніторингу та звітності.

6. **Вся автентифікація та авторизація ресурсів є динамічною і суворо виконується перед тим, як доступ до них буде дозволено.** Доступ отримано, небезпеки просканована та оцінено, внесено корективи, а впевненість у безперервному зв'язку постійно переоцінюється. Системи управління ідентифікацією, обліковими даними та доступом (ICAM) і управління активами повинні бути впроваджені до того, як організація впровадить ZTA. Використання багатофакторної автентифікації (MFA) для отримання доступу до деяких або всіх ресурсів організації є частиною цього процесу. Згідно з політикою (наприклад, на основі часу, запиту нового ресурсу, модифікації ресурсу, виявлення аномальної

активності суб’єкта), безперервний моніторинг з можливою повторною аутентифікацією та повторною авторизацією відбувається протягом усіх транзакцій користувача, щоб досягти балансу між безпекою, доступністю, зручністю використання та економічною ефективністю.

7. **Підприємство збирає якомога більше інформації про поточний стан активів, мережевої інфраструктури та комунікацій і використовує її для покращення стану своєї безпеки.** Організація повинна збирати інформацію про мережевий трафік, стан захищеності активів та запити на доступ, аналізувати цю інформацію та використовувати нові знання для покращення розробки та впровадження політик. Запити суб’єктів на доступ також можна контекстуалізувати, використовуючи ці дані.

Висновки до першого розділу

У першій частині було детально розглянуто ідею нульової довіри та її функції в сучасній кібербезпеці, основні небезпеки та загрози, пов’язані з ZTNA, а також основні компоненти архітектури, які складають цю модель. В основі нульової довіри лежить ідея, що жоден пристрій або користувач не повинен автоматично отримувати доступ до ресурсів без попереднього проходження відповідного процесу автентифікації та верифікації. Це дозволяє захиститися від несанкціонованого доступу та значно знизити ризики, пов’язані з внутрішніми та зовнішніми загрозами. Завдяки використанню таких елементів, як багаторівнева автентифікація, динамічний контроль доступу та мікроперіметри, ZTNA дозволяє створити надійний бар’єр, який успішно захищає важливу інформацію та системи.

2 РІШЕННЯ ZTNA

2.1 Огляд рішень від Cisco

Cisco пропонує комплексні рішення для впровадження доступу до мережі з нульовою довірою (ZTNA) на практиці. Використовуючи принципи нульової довіри, ZTNA гарантує надійну безпеку доступу до корпоративних ресурсів.

- **Cisco Duo**

Cisco Duo є системою багатофакторної автентифікації (MFA), яка підвищує безпеку доступу, підтверджуючи особи користувачів перед наданням їм доступу до ресурсів. Гарантуючи, що люди і пристрої авторизовані і підтверджені в кожній точці доступу, вона відповідає парадигмі безпеки Zero Trust (нульова довіра).

Багатофакторна автентифікація – це система управління доступом, яка використовує два або більше факторів перевірки для підтвердження особи користувача під час входу в систему. Додаючи додатковий рівень безпеки до даних користувача або компанії, MFA допомагає зупинити атаки програм-вимагачів, фішингу та шкідливого програмного забезпечення. Завдяки Cisco Duo MFA стало простіше використовувати, інтегрувати та впроваджувати. New York Times Wirecutter визнав Duo Mobile найкращим додатком для двофакторної автентифікації (2FA) [4].

Завдяки своїй великій масштабованості та простоті інтеграції як із замовленими, так і зі стандартними додатками, Duo дозволяє розгортати рішення для безпечного доступу з мінімальною допомогою IT-спеціалістів.

Багатофакторна автентифікація Duo пропонує цілий ряд потужних методів автентифікації на вибір та комбінування, таких як біометричні дані, токени, паролі, мобільний додаток Duo Push та інші.

За допомогою мобільного додатку MFA від Duo користувачі можуть швидко і легко впровадити MFA. Спрощуючи процес автентифікації за допомогою легкої верифікації з мобільних пристроїв.

Адаптивна автентифікація Duo – це вдосконалений тип MFA, який дозволяє створювати власні політики доступу на основі контекстних факторів, таких як роль, програма, географічне розташування, мережа та стан пристрою.

Особливості Duo:

- Перевірка надійності будь-якого пристрою. Важливим компонентом підходу нульової довіри є контроль над гаджетами, що є першим кроком до побудови довіри до них. Duo проводить перевірку стану при кожній спробі входу в систему та надає інформацію про кожен пристрій, підключений до мережі. Щоб гарантувати відповідність вимогам і налаштувати параметри доступу для кожного випадку, Duo допомагає виявити можливі небезпеки. Дане рішення спрощує моніторинг правил безпеки та виявлення незвичної поведінки користувачів завдяки надійним функціям звітності та зручній для адміністратора інформаційній панелі.

- Гнучкий доступ. Підхід нульової довіри змінює ступінь довіри або доступу відповідно до контекстної інформації про пристрій або користувача, який запитує доступ. Крім того, він дозволяє доступ лише тим, кому він справді потрібен. За допомогою Duo ви можете керувати правилами по всьому світу або для певних програм чи груп користувачів, а також швидко створювати комплексні політики за допомогою простої адміністративної панелі. Під час кожного входу система визначає місцезнаходження користувача, його пристрій, роль тощо. Ці характеристики слугують основою для політик безпеки.

- **Cisco Identity Intelligence**

Cisco Identity Intelligence – це рішення на основі штучного інтелекту, яке безперешкодно надає інформацію про безпеку найвищого рівня, долаючи розрив між автентифікацією та доступом [5].

Дане рішення надає повну картину активності облікових записів, де можна очистити/видалити вразливі акаунти, усувати ризиковані привілеї та блокувати спроби доступу з високим ступенем ризику.

Завдяки безшовному розгортанню рішення Cisco Identity Intelligence забезпечує роботу інших систем безпеки Cisco, що дає змогу розширити функціональність і забезпечити правильну реакцію на будь-яку загрозу.

- **Cisco Secure Access**

Cisco Secure Access – це універсальне рішення для забезпечення безпеки доступу всіх ваших користувачів, захисту внутрішніх активів від кібератак і запобігання їхньому виявленню за допомогою одного рішення [6].

Рішення SSE допомагає організаціям забезпечити безпечне підключення для гібридної робочої сили, одночасно захищаючи корпоративні ресурси від кібератак і втрати даних. Воно об’єднує кілька функцій безпеки в єдину хмарну службу, яка захищає доступ користувачів до Інтернету, загальнодоступних SaaS-додатків і приватних додатків, захищаючи їх від складних загроз, що постійно розвиваються.

Будучи конвергентним хмарним сервісом, заснованим на нульовій довірі і керованим централізовано, SSE ефективно захищає сучасні гіперрозподілені середовища, одночасно підвищуючи продуктивність, знижуючи складність, обмежуючи витрати і знижуючи ризики, а також підвищуючи безпеку.

Cisco Secure Access поєднує в собі унікальний рівень простоти використання та IT-ефективності для безперешкодного доступу до всіх додатків (а не до деяких) із сучасними засобами безпеки, які задовольняють користувачів і розчаровують зловмисників. Використовуючи хмаро орієнтований підхід до впровадження політик безпеки, заснований на нульовій довірі, Secure Access захищає користувачів, дані та пристрої під час безпечного доступу до Інтернету, додатків SaaS і всіх приватних додатків як з корпоративної мережі, так і з-за її меж. Забезпечуючи безперешкодний і безпечний доступ з будь-чого і будь-де, це рішення забезпечує безперебійну роботу кінцевих користувачів, спрощує IT-операції та знижує ризики завдяки деталізованому контролю та посиленому захисту.

Забезпечуючи суворий захист, Secure Access також спрощує та покращує роботу кінцевого користувача завдяки єдиному загальному підходу до доступу, який уможливлює безперешкодну роботу. Це простий, безпроблемний користувацький досвід для щасливіших, продуктивніших користувачів і команд.

Переосмисліть взаємодію з користувачем і впевнено підключайтеся до будь-чого таким чином, щоб забезпечити безпечний доступ до будь-яких додатків, через

будь-яку мережу, де б не працювали користувачі. Cisco Secure Access – це рішення для будь-якого керівника служби безпеки: Захистити роумінгових користувачів, які отримують доступ до Інтернету, додатків SaaS і приватних додатків Захистити користувачів, які підключаються з філій/місцезнаходжень до того ж широкого спектру пунктів призначення Дозволити співробітникам легко отримувати доступ до необхідних ресурсів, без проблем, з високою продуктивністю Перестати турбуватися про порушення безпеки, які несуть серйозні бізнес-ризики Знизити операційні витрати Зменшити складність IT, звільнивши команди безпеки, щоб приділяти більше часу вирішенню важливих завдань.

Cisco Secure Access забезпечує [6]:

– *Secure private access:* Усі приватні програми, навіть нестандартні, однорангові, багатоканальні або ті, що використовують інші порти чи протоколи, надійно захищені. Для найширшого доступу до приватних додатків використовуються VPNaaS і Zero Trust Network Access (ZTNA), які безперешкодно надаються.

– *Secure internet access*: Захищає доступ до Інтернету та контролює використання загальнодоступних SaaS-додатків/хмарних сервісів у мережах, філіях і роумінгових користувачах.

– *Unified console*: Визначає політику для будь-якого користувача в будь-якій програмі, спрощуючи процес побудови політик безпеки та забезпечуючи узгодженість у визначенні політик – і все це в єдиній консолі.

– *AI Assistant*: Автоматично перетворює розмовні англійські фрази в політики безпеки, щоб заощадити час, підвищити операційну ефективність і зменшити складність.

– *App connectors*: Забезпечує безпечне з’єднання та спрощує адміністративні завдання зі встановлення з’єднання з приватними додатками.

– *Full proxy/SWG*: Забезпечує глибокий, детальний контроль веб-трафіку, включаючи гнучкі політики для вибіркового розшифрування зашифрованого трафіку.

– *Data loss prevention (DLP)*: Аналізує конфіденційні дані в режимі реального часу через проксі-сервер SWG та поза смугою пропускання через API, щоб захистити конфіденційну інформацію від витоку з вашої організації, в тому числі під час використання додатків генеративного ШІ.

– *Cloud access security broker (CASB)*: Виявляє тіньові IT, надаючи можливість виявляти хмарні додатки, що використовуються у вашому середовищі, та створювати звіти про них, щоб краще керувати впровадженням хмарних технологій, знижувати ризики та обмежувати або блокувати додатки.

– *Firewall-as-a-Service (FWaaS)*: Блокує більше, бачачи більше, завдяки глибокій видимості та контролю трафіку на всіх портах і протоколах для підвищення безпеки

– *Experience Insights*: Відстежує стан і продуктивність кінцевих точок, програм і мережевого з'єднання для оптимізації продуктивності користувачів і спрощення пошуку та усунення несправностей.

– *DNS-layer security*: Блокує інтернет-запити на шкідливі та небажані адреси ще до встановлення з'єднання – зупиняє загрози через будь-який порт або протокол до того, як вони потраплять у вашу мережу або на кінцеві точки.

– *Remote browser isolation (RBI)*: Ізолює веб-трафік від пристрою користувача та загрози, щоб користувачі могли безпечно отримувати доступ до ризикованих веб-сайтів.

– *Secure malware analytics*: Поєднує вдосконалену ізольовану роботу з аналітикою загроз в одному уніфікованому рішенні для захисту організацій від зловмисного програмного забезпечення.

– *Cloud malware detection*: Виявляє та видаляє шкідливе програмне забезпечення з хмарних додатків і гарантує, що програми залишаються захищеними від шкідливих програм.

- **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 [7].

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 [7], 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) [7] 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 [7], 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 [7].

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

4. Співпраця з іншими програмами безпеки [7]: 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 [7]. 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.

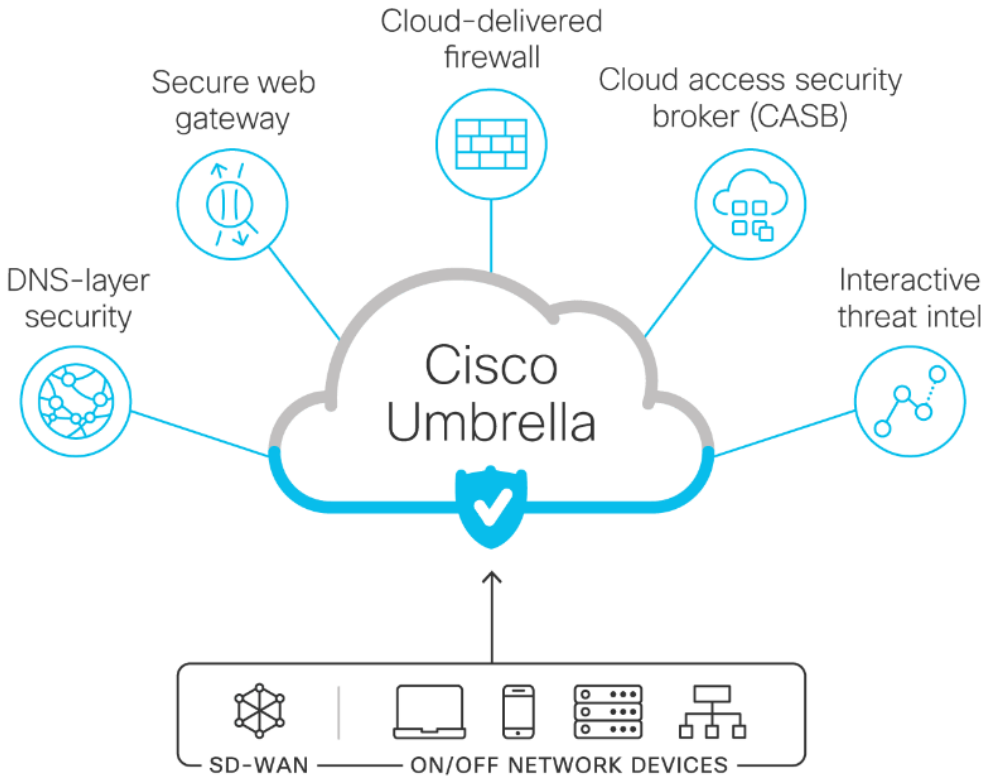

Рис. 2.2. Функції безпеки Cisco Umbrella

2.2 Порівняння з іншими рішеннями

Для розгортання та розвитку архітектури нульової довіри (ZT) організації розробляють плани та стратегії. Багато з цих підприємств мають недоліки в системі безпеки, можливості, що перетинаються, та велику кількість постачальників. Не жертвуючи функціональністю, необхідно об’єднати технології, полегшити інтероперабельність і консолідувати контроль.

Платформи нульової довіри (ZTP) забезпечують єдиний, всеохоплюючий метод для введення в дію технологічної екосистеми ZT, що дозволяє досягти результатів у бізнесі та безпеці ZT.

ZTP об’єднують розрізнені види діяльності та пропонують додаткові можливості та послуги для покращення міжфункціональних операцій та

спрощення впровадження ZT, незалежно від того, чи це на початку шляху до ZT, чи в міру того, як важливі сфери стають зрілими.

Всі функції, необхідні для успішної архітектури ZT, не можуть бути забезпечені одним рішенням. ZTP усувають потребу в окремому кріпильному обладнанні, поєднуючи в собі основні функції ZT. Завдяки власним та стороннім інтеграціям, які мають на меті закріпити та сконцентрувати, а не розірвати та замінити, це створює більш гармонійну архітектуру.

У зв'язку з цим клієнтам ZTP доводиться шукати постачальників, які:

1. Полегшують централізоване управління та зручність використання. Мало хто з постачальників пропонує єдиний універсальний користувацький інтерфейс (UI) і користувацький досвід (UX) для різних компонентів ZT, незважаючи на те, що деякі з них обіцяють централізоване адміністрування. Єдина видимість, адміністрування та виконання елементів керування, які підвищують досвід аналітика (AX), знижують складність і покращують аналітику, є перевагою для фахівців з безпеки та ризиків. Спрощення робочого процесу аналітика та надання детальних інструкцій щодо інструментів і процедур є важливими для вдосконалення AX. Завдяки простоті використання централізованого адміністрування фахівці з розвідки та безпеки можуть знаходити, досліджувати, класифікувати, приймати рішення і виконувати дії без запуску декількох різних користувацьких інтерфейсів або інших консолей. Найкращі практики ZT відповідають галузевим нормам і правилам, оскільки консолідація, яка також створює єдину площину управління і власні інструменти та сервіси для допомоги, навчання та підвищення обізнаності з питань кібергігієни.

2. Пропонують гнучкі моделі розгортання з підтримкою різноманітних гібридних архітектур. Підприємства більше не живуть і не функціонують за межами традиційного захисту мережі на основі периметра. Компанії все ще переносять свої ресурси в хмару і використовують хмарне програмне забезпечення і сервіси. Деякі компанії або не можуть мігрувати в хмару, або вважають за краще мати певний контроль над своїми ресурсами, зберігаючи їх локально. В осяжному майбутньому більшість компаній будуть контролювати та захищати гібридні

архітектури, які поєднують віртуальні та локальні системи. Пропонуючи гнучкі режими розгортання основних компонентів безпеки, якими можна керувати з хмарного інтерфейсу користувача (UI) або розгорнути локально, щоб задовольнити конкретні потреби підприємств, постачальники ZTP адаптують свої продукти для хмарних, віртуальних і локальних систем.

3. Інтегрують можливості ZTNA та/або мікросегментації за замовчуванням. Фундаментальні принципи ZT – застосування повної видимості, неявна відмова в доступі та забезпечення найменших привілеїв – стали можливими завдяки доступу до мережі з нульовою довірою (ZTNA) та мікросегментації, які є ключовими технологіями або можливостями. Пропонуючи безпечний наскрізний доступ до хмарних, програмних як послуга (SaaS) і локальних ресурсів, ZTNA зменшує залежність від застарілих VPN. Встановлюючи мікропериметри, мікросегментація дозволяє здійснювати гранульований контроль доступу до ресурсів і додатків. Завдяки цим технологіям організації можуть впроваджувати ZT-контроль без негативного впливу на моральний дух співробітників або діяльність компанії.

Оцінка Forrester Wave™ на рис. 2.3 виокремлює лідерів, сильних виконавців, претендентів і тих, хто кидає виклик. Це оцінка найкращих постачальників на ринку; вона не відображає весь ландшафт постачальників [8].

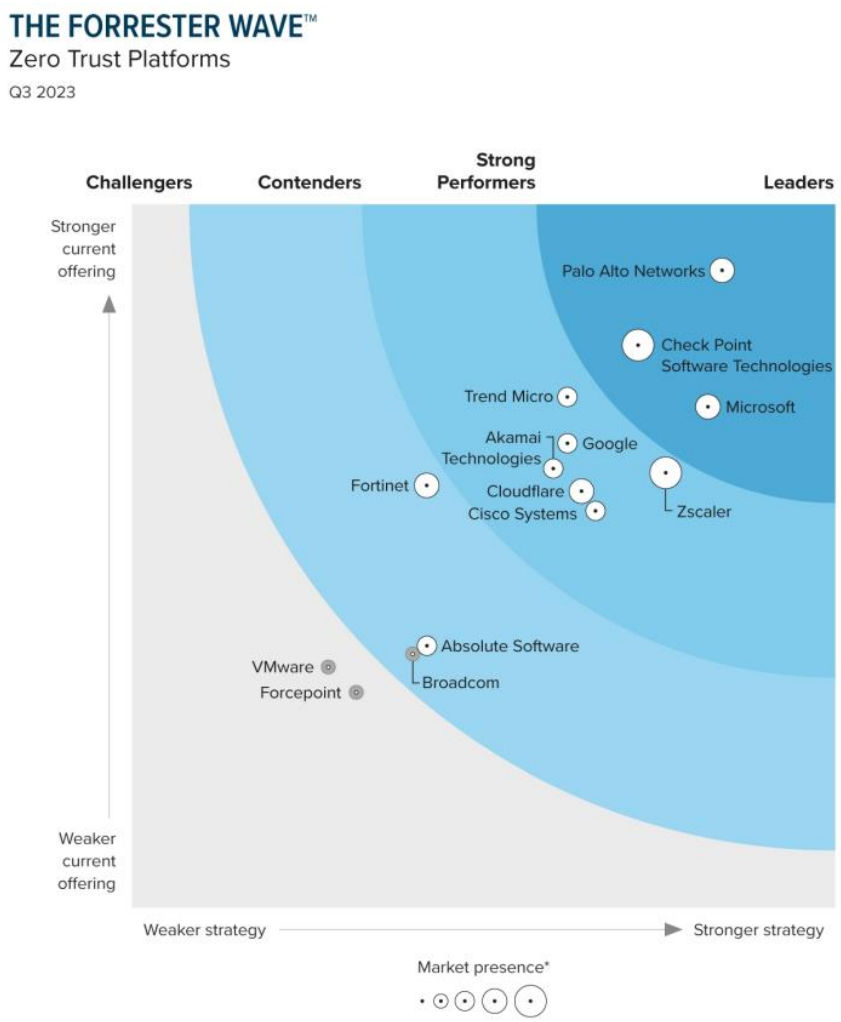

Рис. 2.3. Forrester Wave™: Zero Trust Platform Providers

- **Palo Alto Networks**

Компанія Palo Alto Networks завжди випереджала час з моменту свого заснування понад вісімнадцять років тому. Це почалося у 2008 році [8], коли було представлено перший в галузі брандмауер нового покоління. Використовуючи рішення Prisma, Strata і Cortex з уніфікованим адмініструванням і деякими елементами штучного інтелекту для IT-операцій, постачальник продовжує розвивати цей підхід, пропонуючи мережеві та безпекові можливості через свою Zero Trust Framework. Основна мета Palo Alto Networks – допомогти компаніям розпочати свій шлях до ZT – вирішує проблему, з якою компанії стикаються під час переходу від планування до виконання. Однак її траєкторія є більш амбітною і здебільшого залежить від довгострокових зобов’язань щодо розширення можливостей AI/ML, які виходять за рамки автоматизованої розробки політик.

Пропонуючи найменш привілейований прямий доступ до додатків, необхідний сучасній гібридній робочій силі, ZTNA стала основним методом зменшення поверхні атаки в спробі відновити контроль над швидко зростаючою поверхнею атак. Раннє рішення ZTNA, або 1.0, не відповідало принципу нульової довіри, про що свідчать помітні обмеження зображені на рис. 2.4. Очевидно, що потрібна нова стратегія, і ZTNA 2.0 є такою [9].

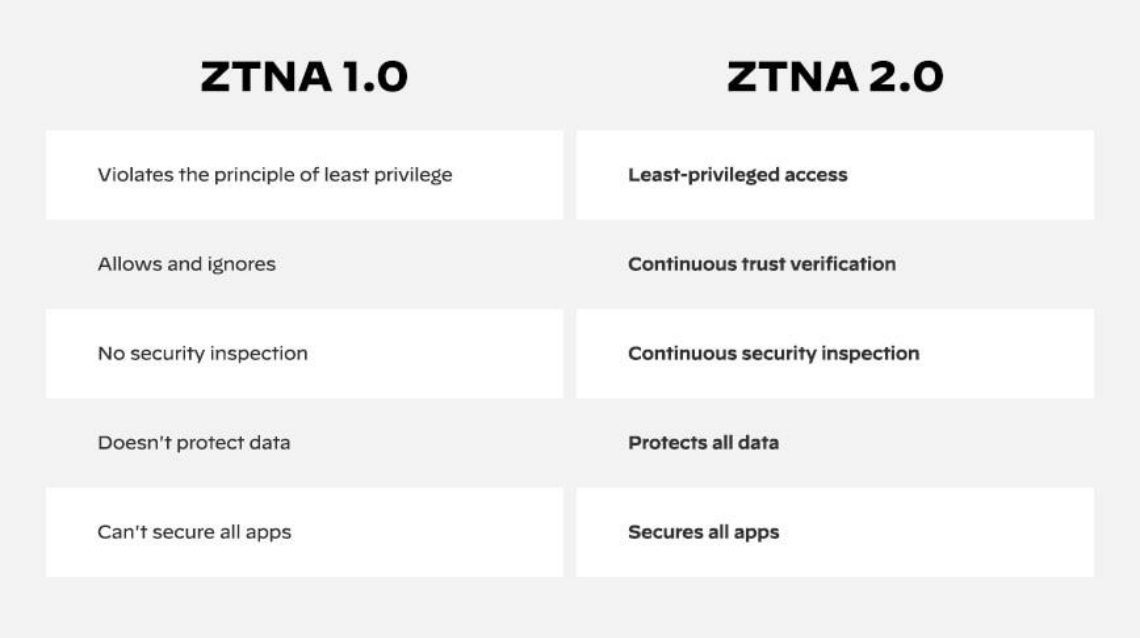

Рис. 2.4. Порівняння функціоналу ZTNA 1.0 та ZTNA 2.0

Долаючи недоліки попередніх систем ZTNA, Zero Trust Network Access 2.0 пропонує безпечні з'єднання, які покращують результати безпеки для компаній зі змішаним складом працівників. ZTNA 2.0 забезпечує [9]:

- *True least-privileged access*: Використовуються ідентифікатори додатків для ідентифікації додатків. Це дає змогу точно регулювати доступ на рівні додатків і піддодатків, незалежно від мережевих структур, таких як IP-адреси та номери портів.
- *Continuous trust verification*: Після надання доступу до додатку довіра постійно оцінюється на основі змін у положенні пристрою, поведінці користувача та поведінці додатку. Якщо виявлено будь-яку підозрілу поведінку, доступ можна відкликати в режимі реального часу.

- *Continuous security inspection*: Щоб зупинити всі загрози, включаючи загрози нульового дня, виконується ретельна і безперервна перевірка всього трафіку, навіть для дозволених з'єднань. Це особливо важливо в ситуаціях, коли легітимні облікові дані користувачів викрадають і використовують для запуску атак на додатки або інфраструктуру.
- *Protect all data*: Завдяки єдиній політиці DLP дані послідовно контролюються в усіх бізнес-системах, включно з SaaS і приватними додатками.
- *Secure all apps*: Усі додатки, що використовуються в компанії, постійно захищені, включаючи SaaS, старі приватні та сучасні хмарні додатки, а також ті, що використовують динамічні порти та з'єднання, ініційовані сервером (рис. 2.5).

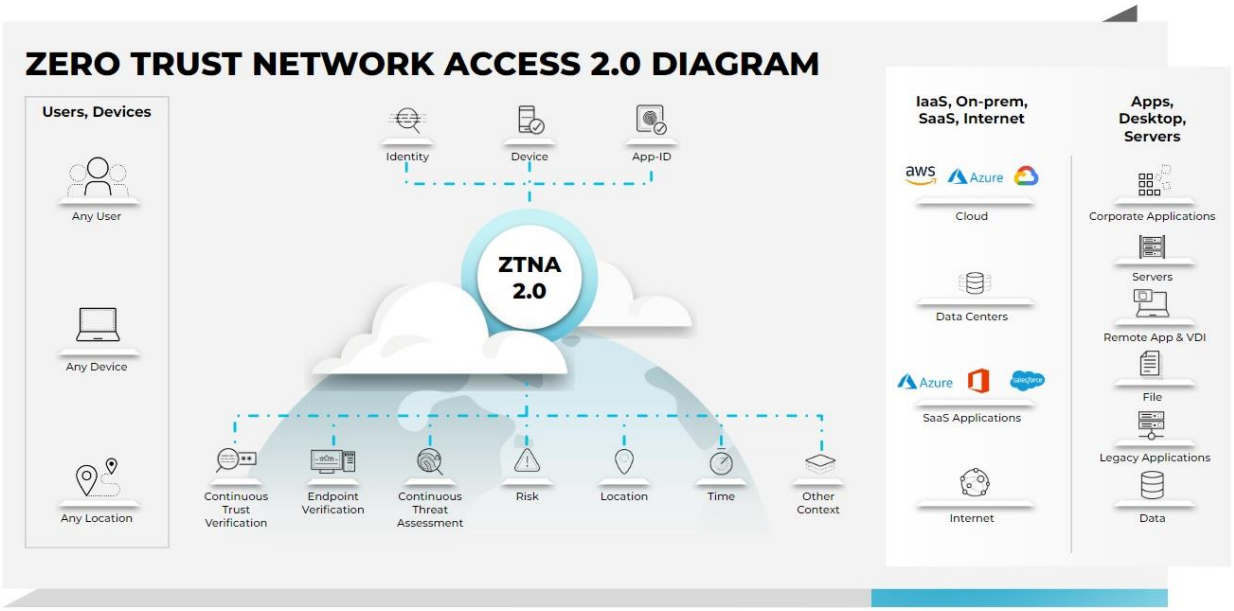

Рис. 2.5. ZTNA 2.0 Diagram

- **Check Point Software**

Лідер у галузі мережевої безпеки, який пропонує апаратні та програмні рішення, забезпечує захист мережі вже трохи більше 30 років [8]. Check Point Software Technologies продовжує відстежувати поточні та майбутні вимоги до підтримки ZT в гібридній архітектурі, навіть в той час, коли багато постачальників звертають свою увагу на повністю хмарні рішення.

Щоб задовольнити конкретні архітектурні потреби, частини ZTP розгортаються в цифровому вигляді, в хмарі SaaS і локально у вигляді апаратного

або програмного забезпечення. Технологічна дорожня карта (Technology roadmap) Check Point [10] фокусується на мережевих стратегіях і стратегіях безпеки для просування глибокого навчання і штучного інтелекту для кращої ідентифікації та запобігання векторів загроз.

Незалежно від того, чи використовує адміністратор Infinity Portal або інші компоненти, користувальницький інтерфейс Check Point пропонує єдиний досвід. Фахівці з мережевої безпеки можуть виконувати повсякденну роботу легше і простіше, використовуючи Check Point Infinity Portal, усуваючи необхідність відкривати кілька вікон або вкладок. Щоб зробити доступ до різних рішень менш складним, кожен компонент згрупований в стовпи і централізовано адмініструється через єдину адміністративну панель (рис. 2.6).

Хоча функція мікросегментації Check Point використовує Azure для спрощення інсталяцій на рівні мережі, вона не має впізнаваної функції мікросегментації на рівні хоста [10].

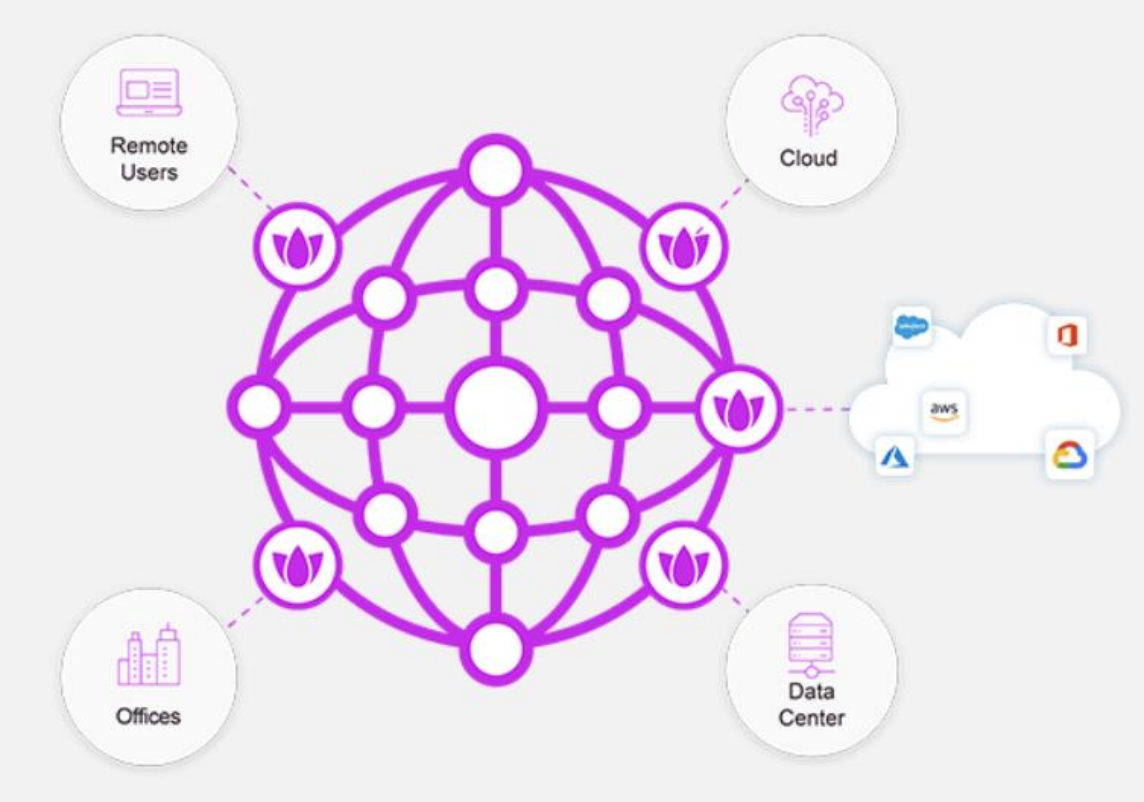

Рис. 2.6. Granular, Secure Remote Access

– Zero Trust Data. Це захист даних, які постійно передаються між робочими станціями, мобільними пристроями, серверами додатків, базами даних, додатками SaaS, корпоративними та загальнодоступними мережами. Check Point Infinity забезпечує багаторівневий захист даних, попереджаючи крадіжку, пошкодження та ненавмисну втрату даних, де б вони не знаходилися. Шифруйте дані, де б вони не знаходилися або передавалися, щоб зробити викрадені дані марними. Відстежуйте і контролюйте переміщення даних по мережі, щоб гарантувати, що конфіденційна інформація не покине організацію. Забезпечуйте найменш привілейований доступ до конфіденційних даних в додатках і керуйте станом безпеки даних.

– Zero Trust People. Традиційної автентифікації на основі імені користувача та пароля вже недостатньо, оскільки 81% крадіжок даних включають викрадення облікових даних. Рішення Identity Awareness від Check Point гарантує, що тільки авторизовані люди отримають доступ до важливих даних після ретельної перевірки їх особистих даних. Виявлення аномалій, контекстно-залежні правила (наприклад, час і місце з'єднання), єдиний вхід і багатофакторна автентифікація – все це частина процесу. Застосування найменш привілейованого доступу до будь-якого організаційного ресурсу – який може охоплювати як внутрішні, так і зовнішні ідентичності – покращить управління доступом, орієнтоване на ідентичність.

– Перевірка стану пристроїв. Перш ніж дозволити пристроям приєднатися до мережі, переконайтеся, що вони відповідають вимогам безпеки компанії. Це потрібно робити постійно, щоб переконатися, що стан пристроїв не змінюється.

– Єдина хмарна інформаційна панель. Ви можете керувати мережею за допомогою єдиного зручного інтерфейсу. Додавання або видалення прав, додавання додаткових мереж для посилення захисту, а також приєднання та відсторонення користувачів – все це прості процеси.

– Керування доступом за програмами. Користувачі повинні підключатися до програм, а не до всієї мережі. Правила доступу з нульовою

довірою гарантують, що працівники мають доступ до інструментів, необхідних для виконання своїх обов'язків. Ні більше, ні менше.

– Управління інвентаризацією пристроїв. Дізнавайтеся про контрольовані пристрої, які підключаються до вашої мережі, та їхній стан здоров'я на даний момент.

- **Microsoft**

Комплексний і сучасний підхід Microsoft до ZT розроблявся протягом багатьох років [8]. Постачальник та інші учасники цього оцінювання представляють свою хмарну організацію як ZTP, підкреслюючи свої спроби інтегрувати методологію та концепції ZT у функції Azure. Тема Copilot поширюється на важливу мету – запропонувати вичерпні покрокові інструкції з використання ШІ для досягнення ZT. Таким чином, клієнти можуть наслідувати приклад корпорації Майкрософт, коли вони починають свій шлях до ZT. Дорожня карта Microsoft, яка включає Security Copilot і публічні попередні версії ZTNA, ще більше демонструє її мету. Ціноутворення та ліцензування ZT, яке враховує окремі незалежні компоненти Azure, такі як Sentinel, все ще залишається складним і вимагає багато часу та роботи для правильного складання бюджету [11].

Через свою широку присутність на ринку, Microsoft повинна узгоджувати свої пропозиції SaaS з міжнародними нормами, законами та правилами. Категоризація постачальника та видимість ризиків і загроз спрощують управління, особливо щодо комплексної безпеки даних. Завдяки інтеграції та сумісності з іншими постачальниками Microsoft розширює можливості екосистеми ZT, пропонуючи більш точний контроль над передачею та споживанням даних. За словами референтних клієнтів, ZTP – це скромне поєднання важливих рішень, які не повністю підпадають під ліцензію E5. Вона також ще не має справжнього рішення ZTNA або переконливої мікросегментації. Згідно з дорожньою картою, постачальник має намір завершити розробку цих функцій. Компанії, які в даний час використовують ліцензії Microsoft E5 для цілей безпеки, мають хорошу можливість почати свій шлях до ZT раніше за допомогою аддонів Microsoft.

Зони захисту Zero Trust Microsoft [11]:

1. Identity

Усі пристрої, облікові записи служб, що використовуються для програм і процесів, а також співробітники отримують ідентичності та умовні обмеження доступу за допомогою Azure Active Directory, хмарної служби ідентичностей.

Важливо, що Azure AD може запропонувати єдину площину контролю ідентичностей зі стандартними службами автентифікації та авторизації для всіх ваших програм і служб, включно з відомими програмами SaaS, а також хмарними та локальними програмами для окремих галузей бізнесу. Це не обмежується лише службами Microsoft.

Це запобігає використанню декількох облікових даних і слабких паролів у різних службах і допомагає вам повсюдно застосовувати надійні методи автентифікації, такі як безпарольна багатофакторна автентифікація для ваших користувачів.

Крім того, є можливість використовувати умовний доступ в Azure AD, щоб використовувати аналітику в режимі реального часу під час входу, щоб зменшити настирливість процесу автентифікації для користувачів.

За допомогою умовного доступу можна створювати політики для оцінки рівнів ризику. Платформа пристрою, місце входу, програми, а також користувач або вхід можуть піддаватися ризику, приймаючи рішення про точку входу й застосовуючи політики доступу в режимі реального часу, щоб надати доступ, але вимагати додатковий фактор автентифікації, обмежити його, наприклад, до привілеїв лише для перегляду, або заблокувати доступ і вимагати скидання пароля.

2. Endpoints

Кінцеві точки користувачів можуть не належати і не контролюватися компанією, коли використовують ресурси, такі як ваші дані та програми. Кінцеві точки вразливі до витоку даних з невідомих програм або сервісів, якщо вони не оновлені або не захищені належним чином.

Незалежно від того, чи належить пристрій користувачеві або компанії, можна використовувати Microsoft Endpoint Manager, щоб переконатися, що він і програми,

інстальовані на ньому, відповідають вимогам політики безпеки компанії та відповідності.

Незалежно від того, чи підключено пристрій зсередини периметра мережі, через VPN, домашню мережу або загальнодоступний Інтернет, цей захист залишається чинним.

3. Network

Завдяки сучасній архітектурі та гібридним сервісам, які включають численні хмарні сервіси, віртуальні мережі, або VNET, VPN та локальні сервіси, ми надаємо вам декілька засобів керування, починаючи з цього: 1. Сегментація вашої мережі для зменшення радіусу ураження та бокового переміщення атак. 2. Захист від загроз для зміцнення мережевого периметра від грубої сили або DDoS-атак, з подальшою можливістю оперативного виявлення та вирішення проблем. 3. Шифрування всього мережевого трафіку, незалежно від того, чи є він внутрішнім, вхідним або вихідним.

Фаєрвол Azure та захист від DDoS-атак Azure – це дві технології мережевої безпеки від Microsoft, які можуть допомогти захистити ваші ресурси Azure VNET.

Важливо, що рішення XDR та SIEM від Microsoft, яке включає Azure Sentinel та Microsoft Defender, допомагає швидко виявляти та локалізувати проблеми з безпекою.

- **Zscaler**

Zscaler досягла значного успіху з ZTNA, пропонуючи безпечний доступ для віддалених працівників підприємств у розпал спалаху COVID-19, але їм було важко боротися за використання локальних кейсів. Допомога клієнтам оптимізувати цінність їхніх розгортань Zscaler за допомогою навчання, успіху клієнтів, конфігурації продукту та аудиту безпеки, а також надання розширених можливостей у пакетах початкового рівня є основною тактикою постачальника для збільшення кількості клієнтів та проникнення на ринок. Забезпечення безперебійної, безпечної передачі інформації та «нульовий дотик, нульова довіра» – це дві стратегії розщеплення повідомлень, які пропонує постачальник; перша з них є більш практичним і здійсненним підходом [8].

Zero Trust Exchange (ZTP) від Zscaler об’єднує брокер безпеки хмарного доступу (CASB), запобігання втрати даних (DLP), безпечний веб-шлюз (SWG) і продукти ZTNA. Клієнти можуть підтримувати безпеку продукту за допомогою вичерпної інформації, яка включає SKU, субкомпоненти та ліцензії, завдяки готовності надавати специфікацію програмного забезпечення під час підписання контракту. За допомогою Client Connector, який використовує єдиного агента для адміністрування та контролю Zscaler Internet Access (ZIA) та Zscaler Private Access (ZPA), компанія Zscaler намагається консолідуватися [12].

Однак той факт, що ZIA і ZPA все ще розглядаються як окремі частини, а не як єдине рішення, дратує користувачів: Клієнти скаржаться на те, що їм доводиться мати справу з двома різними консолями, які «дещо перетинаються». Крім того, за винятком Branch Connector, Zscaler Zero Trust Exchange все ще залишається хмарним рішенням, яке не має життєздатних варіантів розгортання на місці. Компанії, які бажають розпочати або продовжити свій шлях до ZT, можуть звернутися до Zscaler, якщо вони мігрують до хмари і не мають потреби в підтримці застарілих систем.

- **Cloudflare**

Cloudflare Access – це гнучкий рівень агрегації, який постійно перевіряє детальний контекст, наприклад, ідентифікаційні дані та стан пристрою, щоб забезпечити простий і безпечний доступ до всіх ресурсів організації, створюючи програмно-визначений периметр [8]. Коли користувач проходить автентифікацію та відповідає всім критеріям політики доступу, Access видає підписаний веб-токен JSON, дійсний протягом визначеного часу сеансу. Ми виконуємо однопрохідну перевірку всіх запитів користувачів за допомогою нашу гнучку платформу, а наш досвід централізованого адміністрування політик дозволяє профілювати зміни політик в глобальному масштабі за лічені секунди завдяки нашій унікальній мережевій архітектурі Anycast.

Уніфікована безклієнтська та клієнтська робота працює з усіма типами пристроїв. Використовується один пристрій клієнт для всіх сервісів Zero Trust, який шифрує трафік до нашої мережі, щоб зберегти конфіденційність даних клієнтів.

Також надається простий і безпечний доступ до пристроїв за межами підприємства за допомогою безклієнтського налаштування. Послуги ZTNA, DNS та провідні на ринку WAF і DDoS ZTNA та провідні на ринку послуги захисту від атак DDoS працюють разом, створюючи та захищаючи публічні імена хостів, доступні стороннім користувачам і гібридним співробітникам на будь-якому пристрої. А варіанти автентифікації без участі користувача (токени або сертифікати mTLS) також підходять для автоматизованих сервісів та пристроїв Інтернет речей.

Для контролю нульової довіри ресурси використовують загальнодоступні імена хостів для зворотного проксі до самостійно розміщених додатків (хмарних/стаціонарних) або браузерного SSH/VNC, проксі з ідентифікацією до додатків SaaS, або приватна маршрутизація на основі клієнта/тунелю через прямий проксі L4-7 на будь-який веб або не-веб-сайт (наприклад, довільний TCP/UDP) ресурс у приватній підмережі [13]. Глобальна мережа та коннектор додатків підтримують будь-яке обчислювальне середовище (рис. 2.7) – публічну хмару, включаючи Kubernetes і контейнери або застарілі локальні мережеві ресурси – без необхідності використання інфраструктури віртуальних машин і без обмежень пропускної здатності, на відміну від інших постачальників Zero Trust.

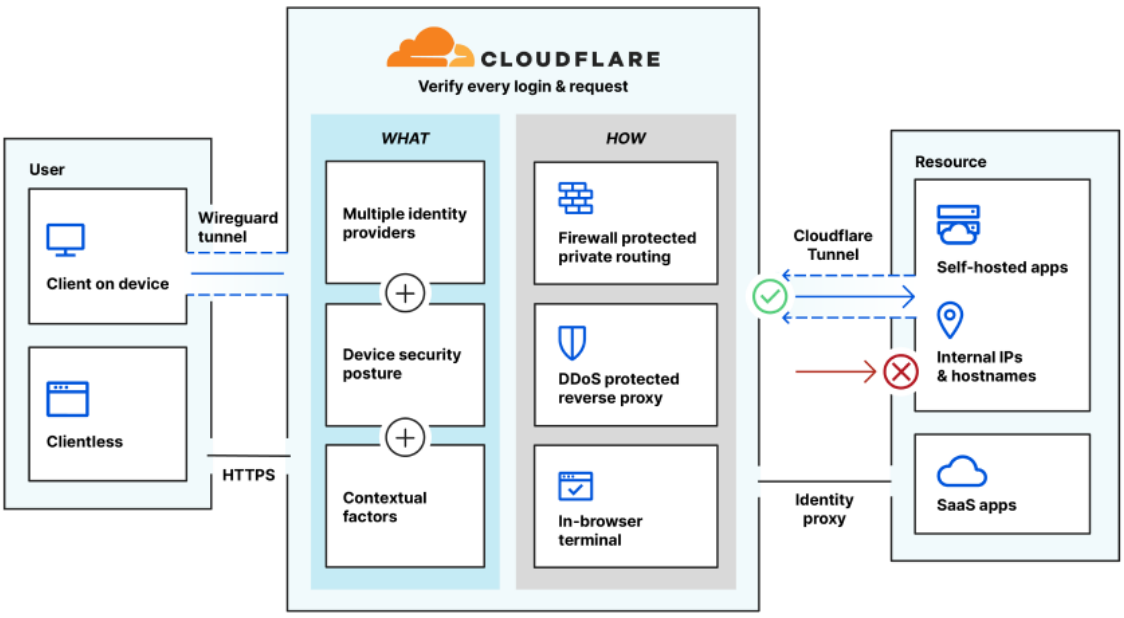

Рис. 2.7. Топологія Cloudflare

Сторонні інструменти ідентифікації, кінцевих точок, розгортання мережі, ведення журналів/аналітики та SIEM інтегровані в інформаційну панель разом із власними опціями для клієнта пристрою та аналітики, що дозволяє адміністраторам залишатися гнучкими і розвиватися разом з інструментами, які вони вже використовують.

Cloudflare регулярно бачить, як підприємства починають з ZTNA, оскільки вона передбачає доступні та практичні дії для IT-команд і демонструє значний короткостроковий комерційний ефект, тоді як SSE та SASE, як правило, передбачають багаторічну стратегічну подорож. На шляху до консолідації IT-керівники прагнуть убезпечити гібридні операції, захиститися від атак і захистити свої дані, і вони все частіше обирають Cloudflare як надійного партнера [13].

Будь-яке підприємство може захистити та підвищити продуктивність пристроїв, додатків та цілих мереж завдяки гнучкості розгортання та модульній архітектурі Cloudflare, гарантуючи, що гібридна робота залишається безпечною та ефективною. Для цього надають веб-ізоляцію без клієнтів для блокування небезпечного трафіку, підключення без агентів для кінцевих користувачів, а також уніфіковану панель управління, яка надає адміністраторам і користувачам доступ до всіх служб безпеки і мережі з будь-якого місця. Завдяки розгалуженій всесвітній мережі Cloudflare, безпека може бути реалізована ближче до кінцевих користувачів, зменшуючи затримки та пропонуючи безперебійне робоче середовище для співробітників. Уникаючи перебоїв в Інтернеті, архітектура Anycast підтримує команди в режимі онлайн і сприяє безперервності бізнесу.

Політики ZTNA, CASB, DLP і SWG мають спільний контекст з уніфікованою платформою SSE і SASE, що підвищує рівень безпеки і спрощує встановлення за допомогою стандартизованого процесу адміністрування. Політики доступу для ZTNA, CASB і SWG можуть ґрунтуватися на одних і тих самих змінних ідентичності та стану пристроїв, що спрощує керування політиками в різних компаніях.

Поєднання ZTNA, RBI та захисту електронної пошти може також захистити користувачів від шкідливої інформації (вкладень, посилань), яку вони бачать в

електронній пошті та інструментах для спільної роботи, надаючи при цьому умовний доступ до ресурсів. Щоб уникнути витоку даних, підрядникам і користувачам на некерованих пристроях можна надати обмежений доступ до ресурсів компанії. Крім того, різні політики L7 DLP можуть бути впроваджені для виявлення конфіденційних даних, а дії користувачів (такі як завантаження, вивантаження, копіювання та вставка) можуть бути заблоковані.

- **Akamai Technologies**

Купівля Guardicore компанією Akamai Technologies у 2021 році сприяла позиціонуванню виробника як конкурентоспроможного постачальника ZTP [8]. Для досягнення спільної, але традиційної мети – оптимізації ZT – корпорація продовжує свою стратегію злиття та поглинання, додаючи нові можливості та вдосконалюючи існуючі. Вибір компанії створити спеціальний бізнес-підрозділ ZT на чолі з колишнім генеральним директором Guardicore для розширення можливостей Akamai Technologies та інтеграції з перспективою ZT є найбільш привабливим кроком [14].

З точки зору спеціалізованої підтримки бізнесу, який починає або активно впроваджує архітектуру ZT, цей підрозділ в основному займається внутрішніми дослідженнями та розробками. Плани щодо збільшення інтеграції, покриття, масштабу, зручності використання та безпеки відображені в дорожній карті Akamai Technologies.

Технології ZTNA, SWG і мікросегментації разом з такими інтеграціями, як багатофакторна автентифікація (MFA) і рішення WAF (захист веб-додатків і API), складають платформу Zero Trust Security від Akamai Technologies. Компанії, які бажають отримати наочність і вбудовані можливості брандмауера для мікросегментації, продовжують вважати рішення Akamai Guardicore Segmentation цінним інструментом.

Завдяки тому, що сегментація «накладається на щось без необхідності перепроектування системи», референтні клієнти повідомляють про покращення безпеки та зручності роботи користувачів DevOps.

Сторонні рішення також інтегровані в технологічну екосистему Akamai Technologies (рис. 2.8). Однак паритет функцій і повна інтеграція ще не були продемонстровані.

Референтні клієнти висловили незадоволення вимогою утримувати багато агентів і незалежних служб підтримки. Організації, які хочуть зняти стрес від мікросегментації, можуть скористатися платформою Zero Trust Security від Akamai Technologies [14].

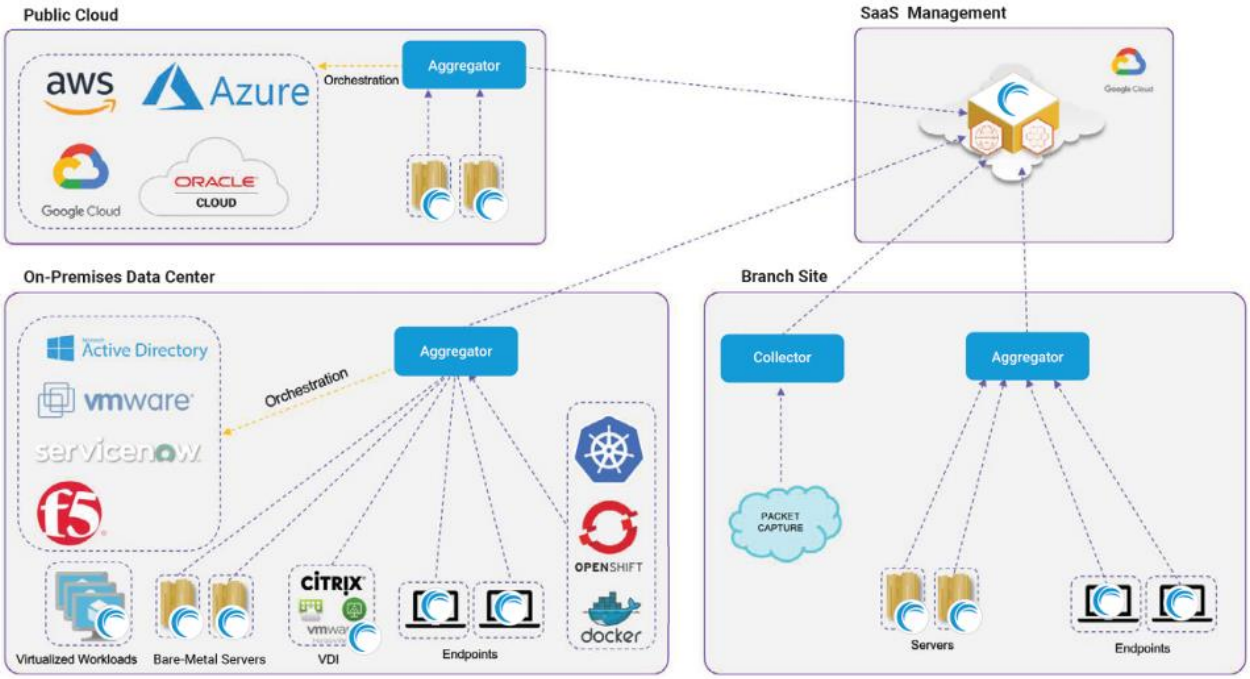

Рис. 2.8. Infrastructure topology

Secure the workload

Провідна в галузі технологія мікросегментації, Akamai Guardicore Segmentation, призначена для запобігання поширенню програм-вимагачів та інших шкідливих програм. На додаток до забезпечення безпечного контролю доступу, програмне забезпечення пропонує розуміння та видимість робочих навантажень, процедур і додатків.

Secure the user

Одним із варіантів хмарного безпечного веб-шлюзу є безпечний доступ до Інтернету. Він перевіряє кожен веб-запит, який роблять користувачі, і застосовує аналітику загроз у режимі реального часу та передові методи аналізу шкідливого

програмного забезпечення, щоб гарантувати, що доставляється лише безпечний вміст. Шкідливі запити та вміст проактивно блокуються.

Облікові записи співробітників захищені від фішингу та інших атак типу «машина посередині» за допомогою Akamai MFA. Це гарантує уникнення захоплення облікових записів співробітників, заборону стороннього доступу, а також те, що лише працівники, які пройшли надійну автентифікацію на основі ідентифікаційних даних, можуть отримати доступ до облікових записів, які вони контролюють.

Secure the network and network access

Для надійної ідентифікації користувачів була створена технологія Zero Trust Network Access від Akamai, яка виконує роль звичайної технології VPN. Доступ до корпоративних додатків дозволяє користувачеві отримати доступ в залежності від конкретного додатку, який користувач повинен використовувати для виконання певної функції, уникаючи ризику для всієї мережі. Контроль доступу до корпоративних додатків забезпечує надійну автентифікацію та ідентифікацію, а також прозорість ідентифікації користувачів.

Track and monitor

Команда мисливців за загрозами найвищого рівня компанії Akamai постійно шукає вразливості, незвичайні шаблони атак і складні загрози, які часто вислизають від звичайних рішень мережевої безпеки, що працюють за принципом «завжди припускати наявність порушень». Про будь-яку серйозну подію, виявлену у вашій мережі, наші мисливці за загрозами негайно повідомляють вам, а потім безпосередньо співпрацюють з вашою командою для вирішення проблеми.

Висновки до другого розділу

У другому розділі розглядаються сучасні рішення для доступу до мережі з нульовою довірою (ZTNA), з акцентом на платформах Cisco та порівнянням з іншими провідними виробниками. Для створення політики нульової довіри технології Cisco, такі як Duo, Umbrella і Secure Access, демонструють велику

гнучкість та інтеграцію, надаючи як локальним, так і віддаленим користувачам безпечний доступ до ресурсів компанії.

Акцент на хмарній інтеграції, мікросегментації, штучному інтелекті для аналітики та автоматизації виявилися загальними тенденціями в галузі ZTNA порівняно з іншими постачальниками, включаючи Palo Alto Networks, Check Point Software, Microsoft, Zscaler, Cloudflare та Akamai Technologies. Однак кожне рішення пропонує унікальні переваги та недоліки, що підкреслює необхідність вибору постачальника на основі вимог та архітектури організації.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОГО ДОСТУПУ З НУЛЬОВОЮ ДОВІРОЮ НА БАЗІ РІШЕННЯ CISCO

3.1 Технологія впровадження рішення Cisco Secure Access

Щоб розпочати роботу з Cisco Secure Access, виконайте наступні кроки [15]:

1. **Початок процесу налаштування**: Перейдіть до розділу «Get Started» у Cisco Secure Access, щоб розпочати процес налаштування.
2. **Крок 1 – Налаштування мережевих підключень**: Визначення та налаштування мережевих підключень, які будуть використовуватися для підключення до Cisco Secure Access.
3. **Крок 2 – Налаштування доступу до ресурсів**: Визначення ресурсів, до яких користувачі матимуть доступ, та налаштування політики доступу до них.
4. **Крок 3 – Налаштування підключення кінцевих користувачів**: Налаштування способів підключення кінцевих користувачів до системи, включаючи методи автентифікації та авторизації.
5. **Крок 4 – Налаштування кінцевих точок та мережевих джерел**: Визначення та налаштування кінцевих точок (пристроїв користувачів) та мережевих джерел, які будуть використовуватися в системі.

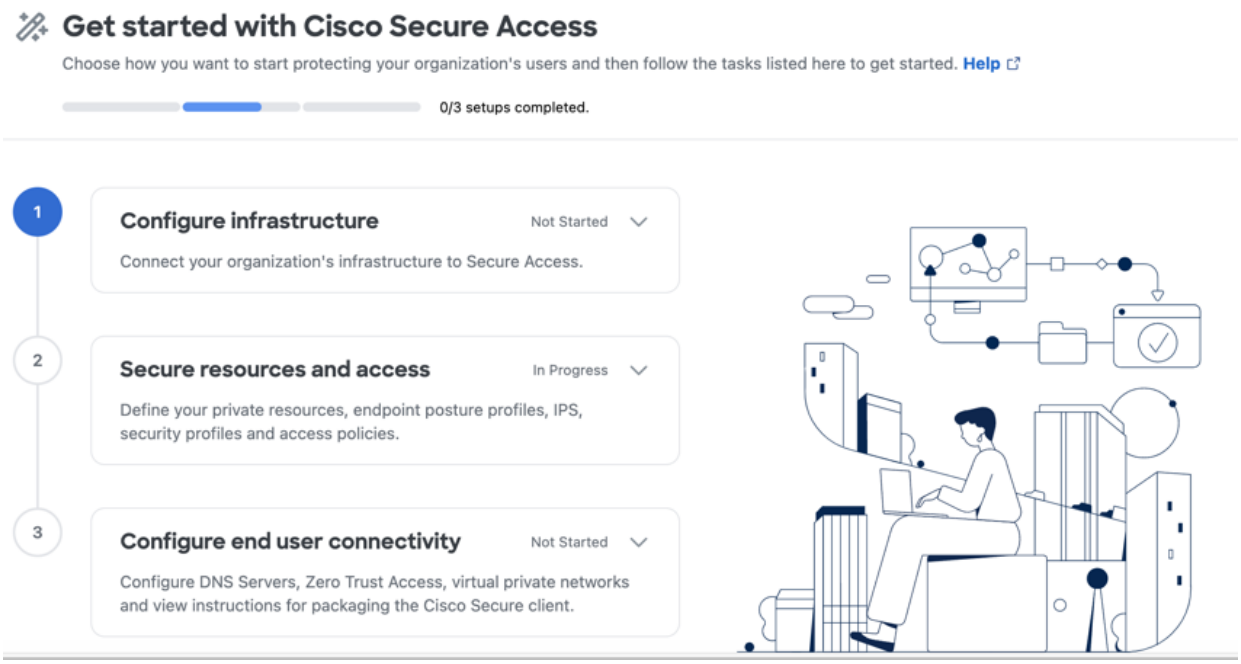

Рис. 3.1. Початок процесу налаштування

- **Крок 1 – Налаштування мережевих підключень**

  Add Network Tunnel Groups:

Впровадження групи мережевих тунелів у компанії, а також впровадження та контроль тунелів IPsec. Після створення тунелю IPsec він може полегшити підключення до мережевих ресурсів через віртуальну приватну мережу (VPN) або до приватних ресурсів у мережі, захищених за допомогою мережевого доступу з нульовою довірою (ZTNA).

Add Resource Connector Groups:

Додавання групи коннекторів ресурсів до організації, де група коннекторів включає принаймні два коннектори ресурсів. Група коннекторів ресурсів підтримує віддалені мережеві підключення за допомогою Zero Trust Network Access (ZTNA) до приватних ресурсів, що працюють у приватних хмарах або локальних центрах обробки даних.

Provision Users and Groups:

Надання користувачам і групам з організації доступ до Захищеного доступу. Є можливість налаштувати користувачів і групи за допомогою інтеграції з постачальниками ідентичностей (IdP) або вручну імпортувати список користувачів

і груп з файлу значень, розділених комами (CSV). Після створення користувачів ви можете налаштовувати і керувати ними в профілях, які захищають і маршрутизують трафік з пристроїв користувачів.

Configure Integrations with SAML Identity Providers

За допомогою Cisco Secure Access ви можете отримати безпечний доступ до Інтернету, веб-ресурсів у публічних і приватних хмарах, програм як послуги (SaaS) і локальних приватних ресурсів вашої компанії. Ви повинні інтегрувати постачальника ідентифікаційних даних (IdP) на основі мови розмітки тверджень безпеки (SAML) із захищеним доступом, щоб встановити детальніші правила політики та дозволити захищеному доступу автентифікувати користувачів, які підключаються з мереж, мережевих тунелів або за допомогою нульової довіри (ZT). Автентифікація з єдиним входом (SSO) пропонується SAML IdP. Secure Access будує відносини довіри з IdP.

Secure Access підтримує мову розмітки Security Assertion Markup Language (SAML) для автентифікації користувачів за допомогою єдиного входу (SSO). Azure Active Directory (Azure AD), Duo, Okta, Ping Identity, Active Directory Federation Services (AD FS) і OpenAM – це лише деякі з SAML 2.0 IdP, з якими взаємодіє Secure Access.

SAML IdP обробляє всі запити на автентифікацію, коли користувачі у вашій компанії налаштовані на використання SSO. Після автентифікації за допомогою SSO IdP користувачеві надається дозвіл на підключення до певних ресурсів і він негайно входить до Secure Access.

- **Крок 2 – Налаштування доступу до ресурсів**

Set Up Private Resources:

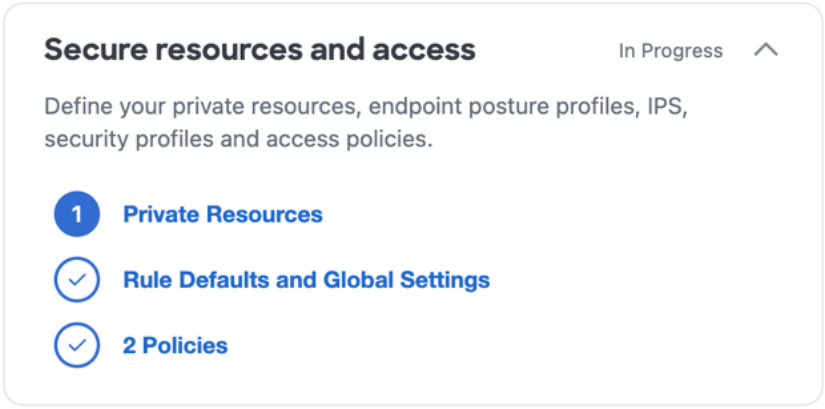

Рис. 3.2. Налаштування доступу до ресурсів

Перейдіть до розділу «Resources» у панелі управління Cisco Secure Access.

Натисніть «Add Resource» та введіть необхідну інформацію про ресурс, включаючи його назву, тип (наприклад, веб-додаток, сервер) та IP-адресу або доменне ім’я.

Збережіть налаштування, щоб додати ресурс до системи.

Приватні ресурси – це програми, мережі або підмережі, які є внутрішніми ресурсами, розміщеними у вашій приватній хмарі або центрі обробки даних, що мають сторінку входу, до якої неможливо отримати доступ ззовні мережі.

Коли відбувається налаштування приватного ресурсу, Secure Access автоматично додає запис для кожної налаштованої адреси ресурсу для клієнтського доступу з нульовою довірою на сторінку Керування трафіком, щоб спрямовувати трафік кінцевого користувача до ресурсу.

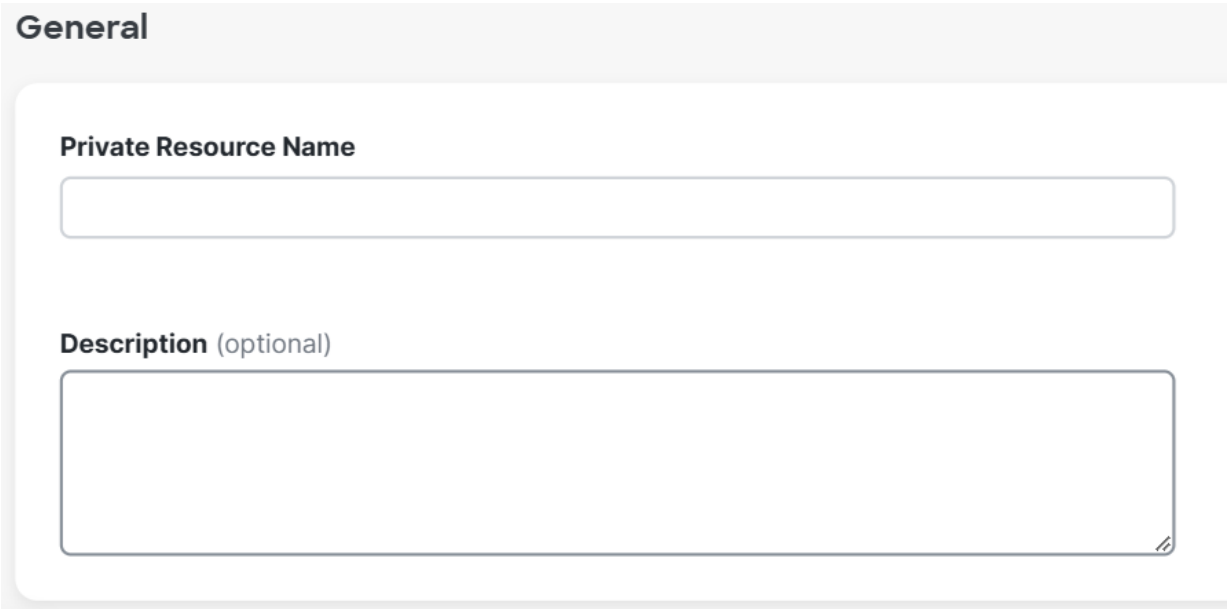

Рис. 3.3. Створення приватного ресурсу

Add a Policy Rule

Одним із ключових етапів є створення правил доступу, які визначають, хто саме матиме доступ до ресурсів. Це дозволяє контролювати доступність ресурсів для користувачів і пристроїв. Також важливо забезпечити правильне налаштування клієнта Cisco Secure, який встановлюється на пристрої користувачів для підтримки Zero Trust Access. У випадках, коли використання клієнта неможливе, можна надати URL-адреси для браузерного доступу.

- **Крок 3 – Налаштування підключення кінцевих користувачів**

Configure DNS servers

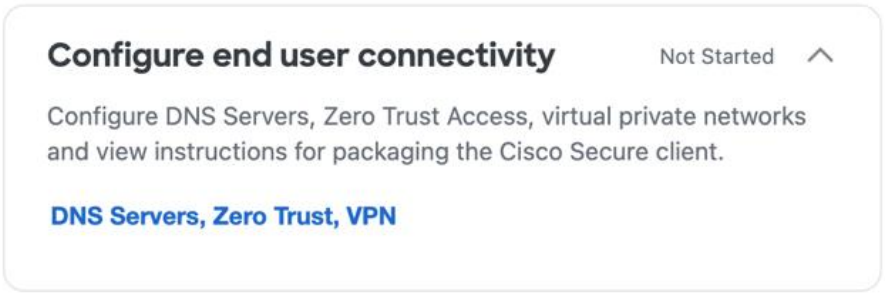

Рис. 3.4. Підключення кінцевих користувачів

Cisco Secure Access захищає трафік DNS в організації. Додайте DNS-сервери для вирішення DNS-запитів до інтернет-ресурсів. При додаванні цих DNS-серверів

DNS-сервер 1 виконує обробку перед DNS-сервером 2. Якщо можливо, вкажіть DNS-сервери, які можуть обробляти IPv4 і IPv6.

Manage Traffic Steering

Елементи керування трафіком на сторінці Підключення кінцевого користувача > Нульова довіра охоплюють лише клієнтські з'єднання з нульовою довірою до внутрішніх пунктів призначення, які налаштовано як приватні ресурси.

Щоб спрямувати трафік кінцевого користувача до приватного ресурсу, Безпечний доступ автоматично додає елемент для кожної адреси ресурсу, налаштованої для клієнтського нульової довіри, на сторінку Керування трафіком.

Хоча ви можете ознайомитися з правилами керування трафіком, загалом не варто їх змінювати.

Найкращі практики:

1. Не варто додавати пункти призначення безпосередньо на сторінку керування трафіком з нульовим рівнем довіри. Замість цього додайте приватний ресурс.

2. Не слід редагувати записи на сторінці керування трафіком з нульовою довірою, за винятком таких випадків: а) Редагуйте записи на сторінці керування трафіком з нульовою довірою, якщо ви налаштували адресу доступу до приватного ресурсу як шаблонний FQDN у форматі *.example.com і хочете виключити вказані субдомени з клієнтського доступу з нульовою довірою.

3. Кількість напрямків на сторінці керування трафіком обмежена.

- **Крок 4 – Налаштування кінцевих точок та мережевих джерел**

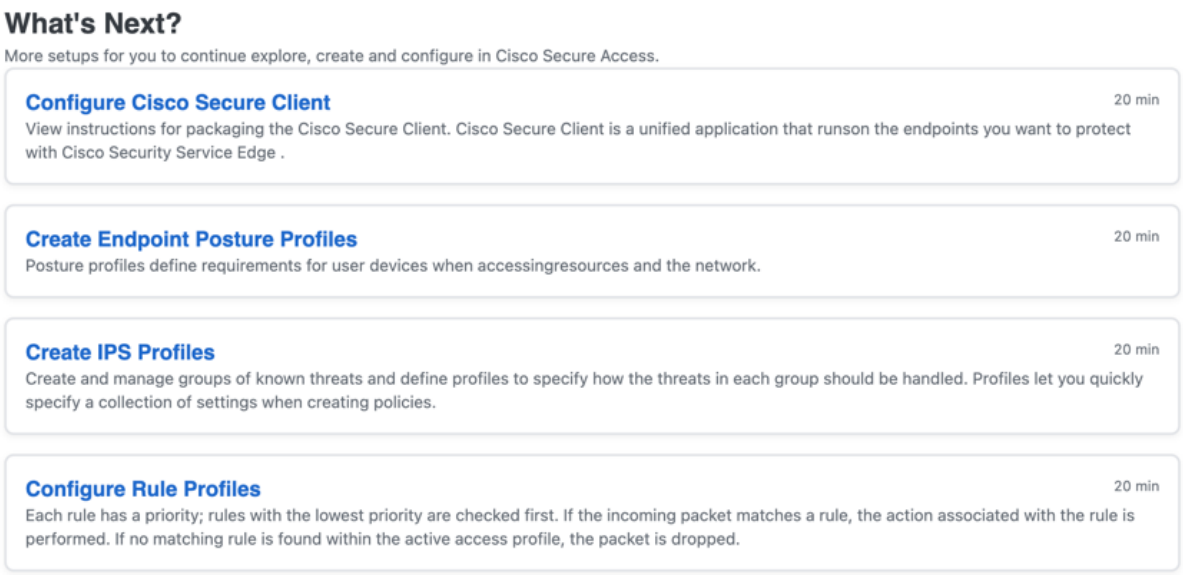

Рис. 3.5. Налаштування кінцевих точок та правил

Можна дозволити безпечний доступ з керованих і некерованих пристроїв до приватних і загальнодоступних ресурсів, використовуючи мережевий доступ з нульовою довірою (ZTNA).

Користувачі можуть отримати доступ до цифрових приватних ресурсів за допомогою:

- ZTNA – на основі клієнта
- ZTNA – на основі браузера
- VPNaaS

Клієнтська версія ZTNA використовує провідний у галузі модуль під назвою Cisco Secure Client (раніше відомий як AnyConnect Client).

Cisco Secure Client забезпечує безпеку користувацьких пристроїв у будь-якій мережі, незалежно від того, чи підключається пристрій до приватних ресурсів за допомогою Zero Trust Access або VPN, чи безпечно під’єднаний до Інтернету за допомогою захисту на рівні DNS і захищеного веб-шлюзу (SWG).

Щоб використовувати Cisco Secure Client з Zero Trust Access на підтримуваних пристроях, користувач повинен зареєструвати клієнт у Zero Trust Access.

1. Інсталяція Cisco Secure Client

Для успішного запуску модуля Secure Client може знадобитися розгортання певного профілю. Диспетчер конфігурації системи або система віддаленого моніторингу та керування (RMM) може завантажити, інсталювати та розгорнути Secure Client на пристроях користувачів організації.

2. Реєстрація в Zero Trust Access

Перш ніж користувачі зможуть отримати доступ до ресурсів за допомогою клієнтського Zero Trust Access, вони повинні зареєструватися. Після встановлення Cisco Secure Client на кінцевих пристроях користувачів, потрібно запросити кінцевих користувачів в організації зареєструватися в Zero Trust Access на захищеному клієнті на своєму пристрої. Існує інструкція, якої необхідно дотримуватися користувачам, щоб зареєструвати свої пристрої для доступу з нульовою довірою.

Наступний крок – захистити свої цифрові ресурси за допомогою політик доступу (Access Policies).

Ресурс – це об’єкт під управлінням вашої організації, який має доступ до Інтернету. Щойно ресурс додано до Cisco Secure Access, конфігурації безпеки, описані в правилах політики, захищають його від загроз і атак. Безпечний доступ може підтримувати як високорівневі об’єкти у компанії, як-от внутрішні або зареєстровані мережі, так і дуже деталізовані об’єкти, як-от окремий користувач, підключений до Microsoft Office 365.

Одна публічна статична або динамічна IP-адреса, або набір IP-адрес, представляє собою зареєстрований мережевий ресурс. Cisco Secure Access підтримує як статичні IP-адреси IPv4 і IPv6, так і динамічні IP-адреси IPv4. Весь трафік, що надходить з публічного IP-простору, розпізнається як такий, що надходить з цієї мережі в рамках безпечного доступу. Обсяг мережевого ресурсу визначається загальнодоступним IP-простором, часто відомим як IP-діапазон.

Ви можете налаштувати Secure Web Gateway, IPS, профілі стану кінцевих точок (endpoint posture profiles) і налаштування безпеки для пунктів призначення (security settings for destinations).

3.2 Налаштування політик та управління доступом

За допомогою Cisco Umbrella ми можемо налаштувати роботу з мережевими та хмарними додатками. Для цього необхідно буде створити політики у вкладці Policies.

Вона ділиться на дві основні категорії: Management та Policy Components (Рис. 3.6).

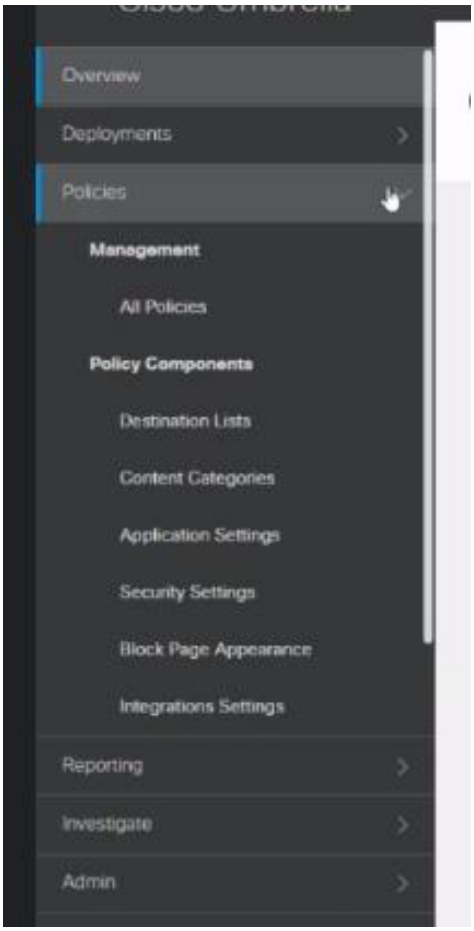

Рис. 3.6. Категорії та підкатегорії Policies

В **Management** можна створити власну політику або використати ту, що стоїть за замовчуванням (Рис. 3.7).

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

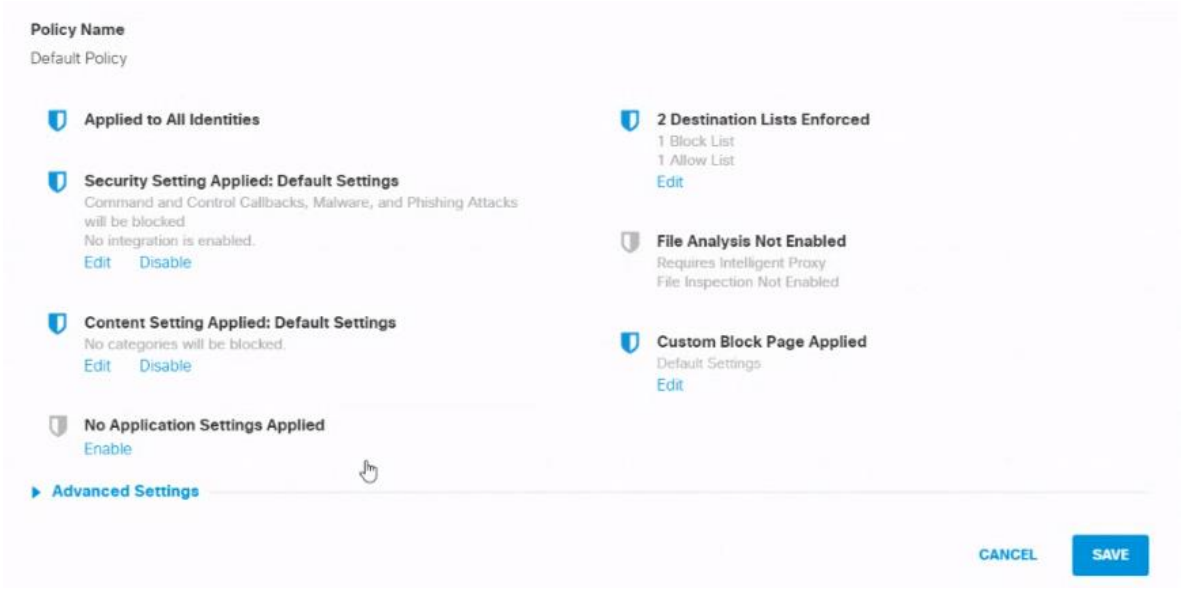

Рис. 3.7. Політика за замовчуванням

Поетапне створення політики:

Для початку потрібно визначити, що саме потребуватиме захисту: мережі, користувачі чи групи, пристрої чи Chromebooks (Рис. 3.8).

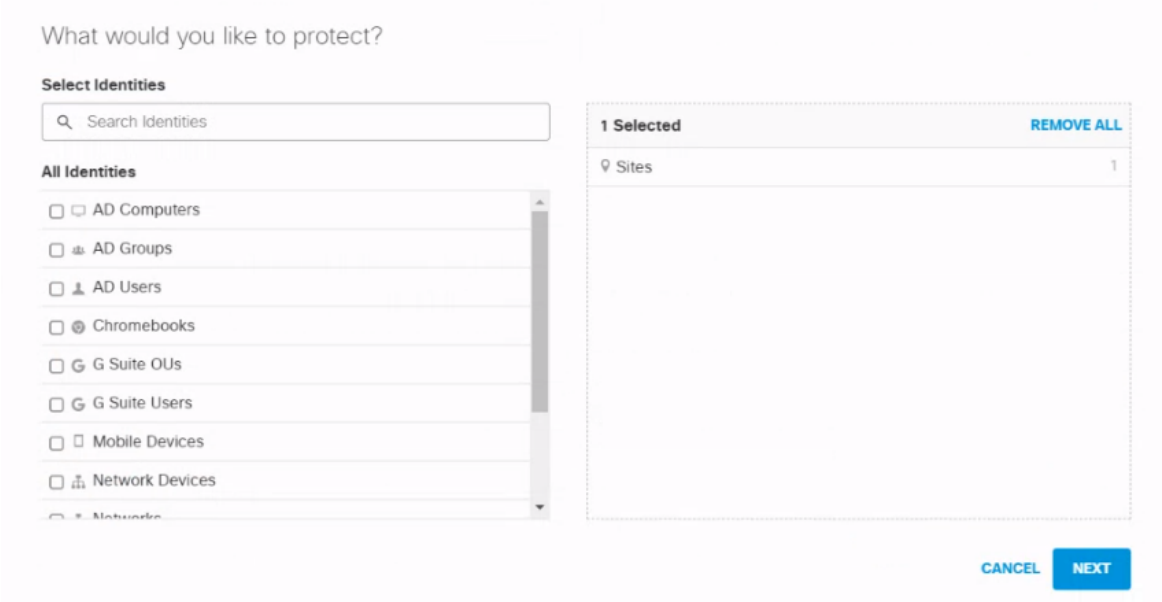

Рис. 3.8. Обрання об’єктів для захисту

Після обрання всіх ключових об’єктів натискаємо **Next**. Далі потрібно обрати функціонал даної політики (Рис. 3.9). 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.

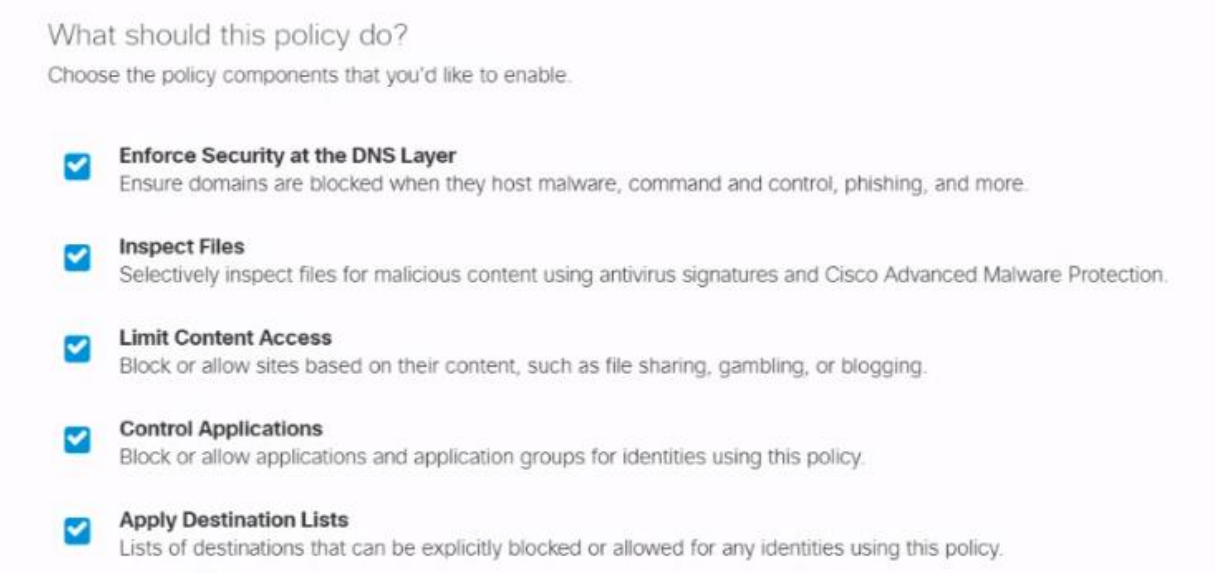

Рис. 3.9. Компоненти політики

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. 3.10).

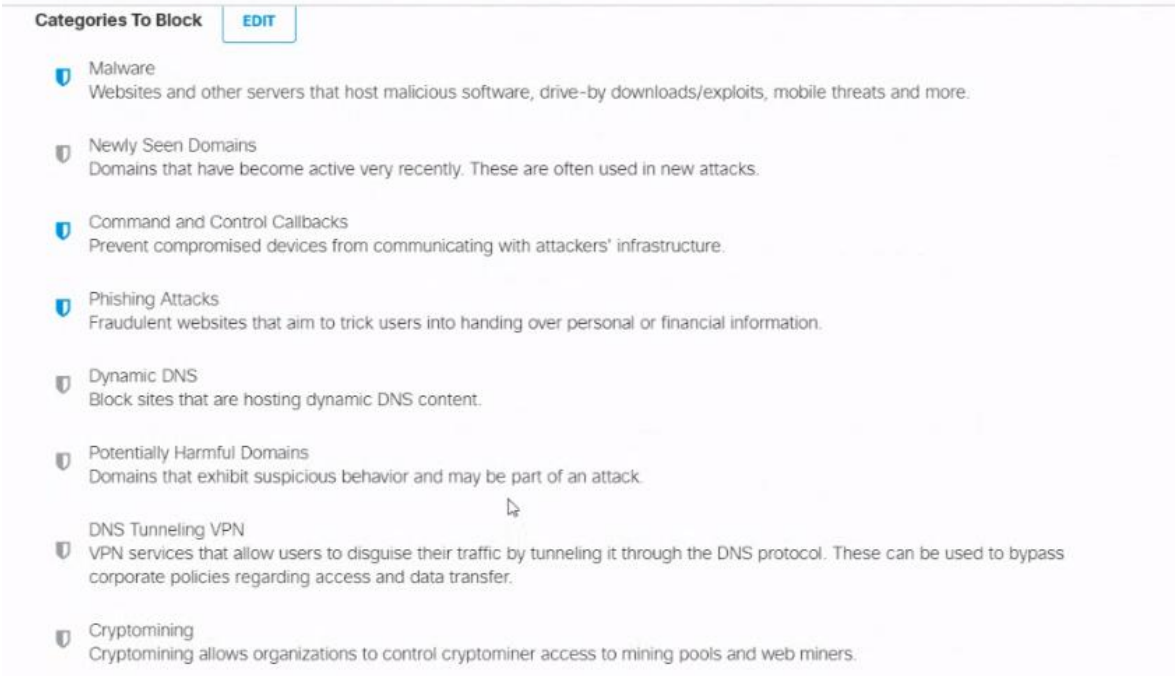

Рис. 3.10. Категорій блокування

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. 3.11):

– 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.

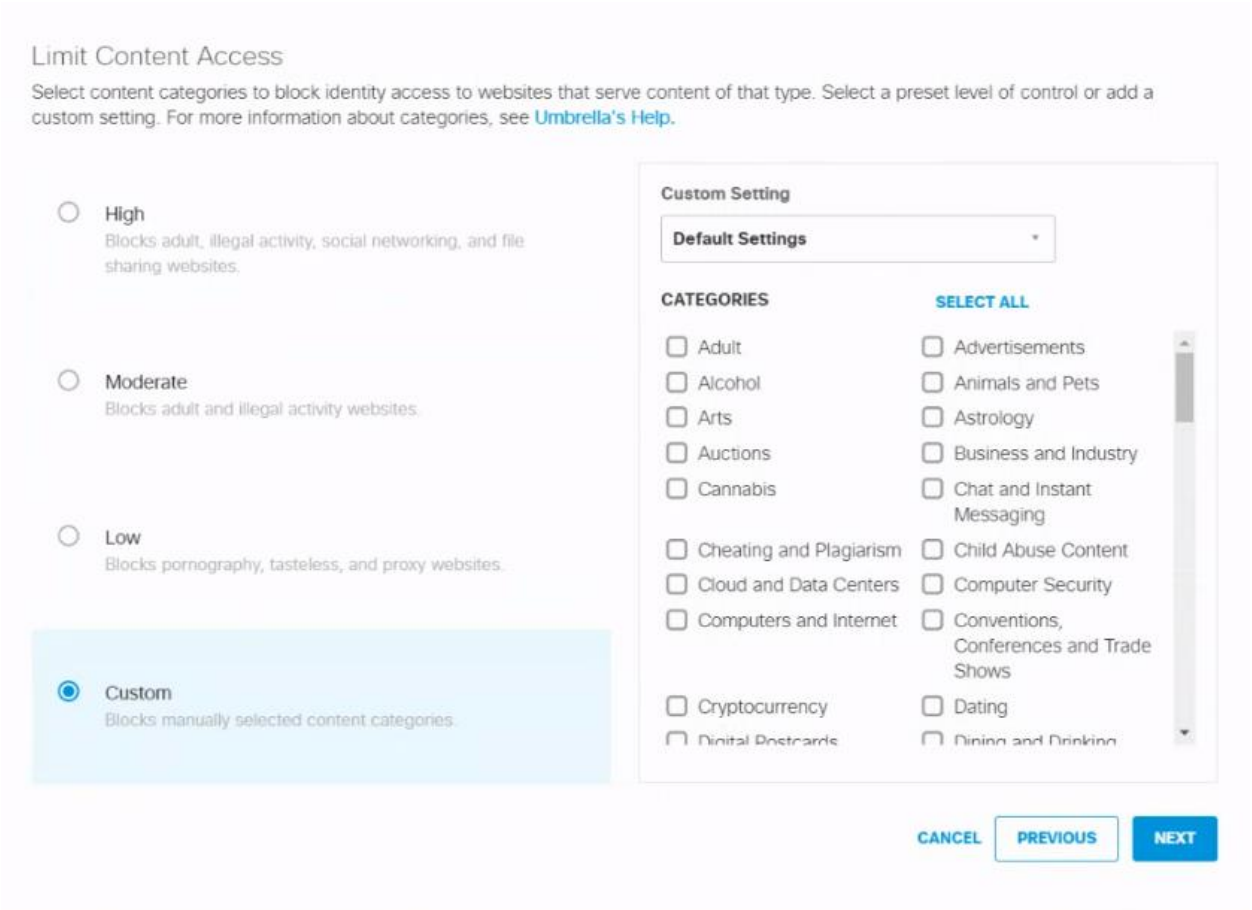

Рис. 3.11. Категорії обмеження

Натискаємо **Next**. Переходимо до наступної функції Контроль програм (Рис. 3.12). Тут потрібно обрати програми або категорії програм, які ми хочемо заблокувати або, навпаки, дозволити користувачам в компанії.

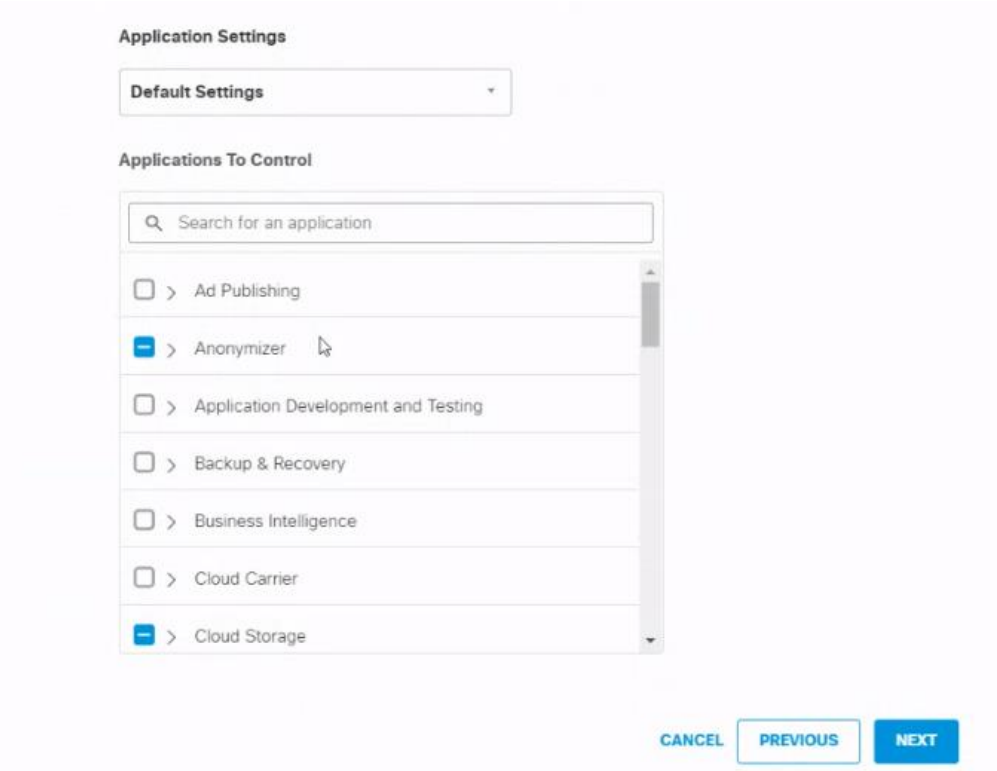

Рис. 3.12. Категорії програм для контролю

Після цього потрібно застосувати списки призначення (Рис. 3.13). 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.

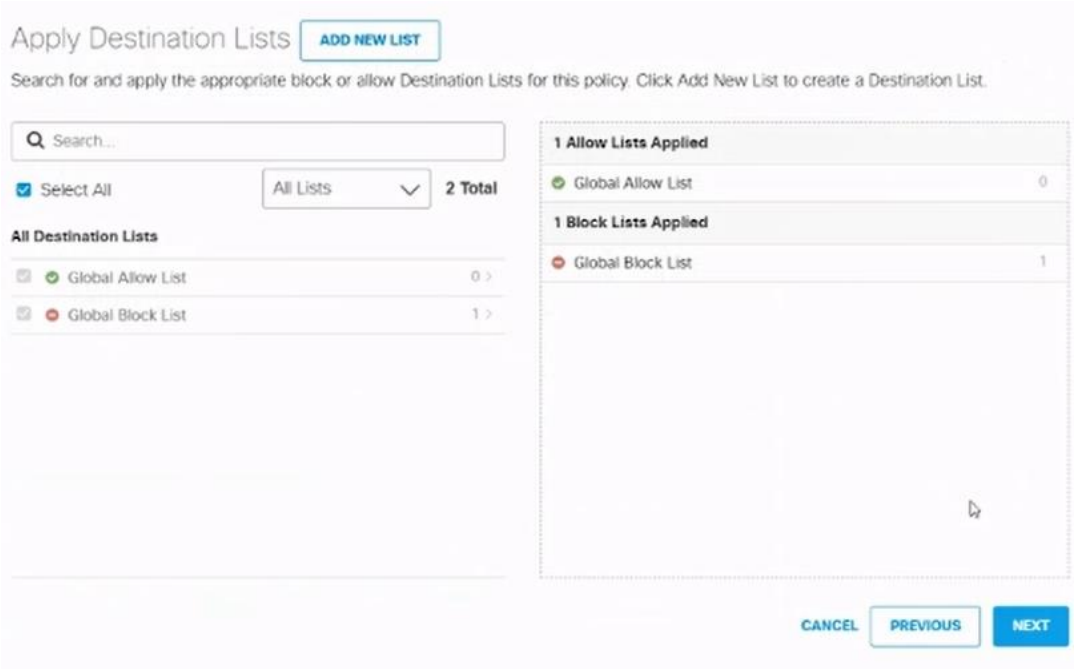

Рис. 3.13. Обрання списків

Далі обираємо чи потрібен нам аналіз файлів (Рис. 3.14). 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. 3.14. Аналіз файлів

Потім обираємо налаштування сторінки блокування (Рис. 3.15). Є можливість обрати сторінку за замовчуванням (Рис. 3.16) або ж індивідуальний зовнішній вигляд.

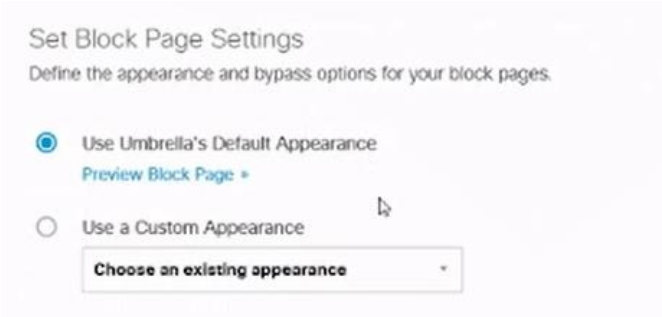

Рис. 3.15. Налаштування сторінки блокування

Рис. 3.16. Сторінка блокування за замовчуванням

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

Висновок до третього розділу

В результаті дослідження було створено ґрунтовну стратегію надання доступу до мережі з нульовою довірою на основі рішення Cisco. Встановлення мережевих з'єднань, створення та захист доступу до ресурсів, впровадження правил доступу для кінцевих користувачів та інтеграція клієнта Cisco Secure відповідно до політики нульової довіри – все це є частиною цієї стратегії. Розглянуті технології, такі як Cisco Umbrella та Secure Access, що мінімізують небезпеку небажаного доступу, пропонуючи багаторівневий захист і дозволяючи ефективно контролювати доступ до ресурсів організації. В результаті,

використовуючи цю стратегію, підприємства можуть побудувати масштабовану та безпечну IT-інфраструктуру.

ВИСНОВКИ

В рамках кваліфікаційної роботи було проведено ґрунтовний аналіз проблеми гарантування безпечного доступу до мережі на основі використання концепції нульової довіри. Визначено мету роботи, наукові завдання та актуальність теми в сучасному цифровому світі, який характеризується збільшенням кількості кібератак, використанням розподілених мереж та гібридних IT-інфраструктур.

В роботі висвітлено основи Zero Trust, а також його головні ідеї та архітектурні стратегії. Усунення неявної довіри до людей і технологій, незалежно від того, де вони знаходяться, є основою ідеї. Zero Trust пропонує постійний моніторинг і перевірку транзакцій замість традиційного захисту периметра, акцентуючи увагу на рольовому контролі доступу, мікросегментації, багатофакторній автентифікації та динамічній оцінці ризиків.

Продукти Cisco, а саме Cisco Duo, Cisco Secure Access та Cisco Umbrella, використовуються як приклад у дослідженні рішень для розгортання мережевого доступу з нульовою довірою (Zero Trust Network Access, ZTNA). Описано основні цілі цих технологій, а також їхні переваги для надання безпечного доступу до приватних мереж, хмарних додатків і ресурсів компанії. Розглянуто потенціал моніторингу мережевого трафіку, адаптивного контролю доступу, ізоляції браузерів, запобігання шкідливому програмному забезпеченню та багатофакторної автентифікації.

Розглянуто стратегію і тактику впровадження нульової довіри на базі технологій Cisco. Запропонований процес впровадження технології на практиці передбачає встановлення мережевих з’єднань, контроль доступу до ресурсів, встановлення правил безпеки та інтеграцію технологій Cisco в більш широку IT-архітектуру організації. Проведено тестування рішень та надано корисні поради щодо їх використання.

Впровадження технології нульової довіри на базі рішень Cisco забезпечує багаторівневий захист даних і додатків компанії, підвищує стійкість організації до сучасних атак і забезпечує безперервність бізнес-процесів. Щоб зберегти свою високу ефективність у мінливих умовах, системи Cisco повинні забезпечувати гнучку модифікацію політик доступу відповідно до змін у бізнес-середовищі.

На основі висновків було розроблено рекомендації для спеціалістів з кібербезпеки щодо використання мережевого доступу з нульовою довірою. Ці рекомендації спрямовані на зниження ризику небажаного доступу, зменшення залежності від звичайних VPN і підвищення загального рівню безпеки для інформаційних активів компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Zero Trust security | What is a Zero Trust network? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-zero-trust/.
2. What is the castle-and-moat network security model? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/access-management/castle-and-moat-network-security/.
3. eXtensible Access Control Markup Language (XACML) Version 2.0 [Електронний ресурс] – Режим доступу до ресурсу: https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.
4. The Best Two-Factor Authentication App [Електронний ресурс] – Режим доступу до ресурсу: https://www.nytimes.com/wirecutter/reviews/best-two-factor-authentication-app/.
5. Cisco Identity Intelligence [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/site/us/en/solutions/security/identity-intelligence/index.html.
6. Endpoint security built for resilience [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html.
7. Cloud security services for your business [Електронний ресурс] – Режим доступу до ресурсу: https://umbrella.cisco.com/products/cloud-security-service.
8. The Forrester Wave™: Zero Trust Platform Providers, Q3 2023 [Електронний ресурс] – Режим доступу до ресурсу: https://www.checkpoint.com/kr/downloads/resources/forrester-q3-2023-ztp.pdf.
9. What Is Zero Trust Network Access (ZTNA) [Електронний ресурс] – Режим доступу до ресурсу: https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna.

10. Zero Trust Security Solutions [Електронний ресурс] – Режим доступу до ресурсу: https://www.checkpoint.com/solutions/zero-trust-security/.

11. Protect and modernize your org with a Zero Trust strategy [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/en-us/security/business/zero-trust.

12. Secure Private Access with ZTNA [Електронний ресурс] – Режим доступу до ресурсу: https://www.zscaler.com/products-and-solutions/zscaler-private-access.

13. Zero Trust Network Access (ZTNA) [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/products/zero-trust/zero-trust-network-access/.

14. Getting Started with Your Zero Trust Strategy [Електронний ресурс] – Режим доступу до ресурсу: https://www.akamai.com/glossary/where-to-start-with-zero-trust.

15. Cisco Secure Access Help [Електронний ресурс] – Режим доступу до ресурсу: https://docs.sse.cisco.com/sse-user-guide/docs/begin-get-started-with-secure-access-workflow.