CISCO
SECURE

The bridge to possible

Cisco Umbrella

Спрощуємо безпеку

Pavel Rodionov . CCIE 11155, CISSP, GREM
Technical Solutions Architect, Cisco Security Solutions

Summer 2023

Use Umbrella DNS
208.67.222.222
208.67.220.220

Agenda

- Umbrella. Огляд
- Глобальна хмарна архітектура
- Кібераналітика
- Компоненти Umbrella / основний функціонал
  - Підключення, інтеграції та журналювання
  - DNS безпека
  - ~~Secure web gateway~~
  - ~~Хмарний міжмережевий екран~~
  - ~~Cloud access security broker (CASB)~~
  - ~~Cisco SecureX~~
- Umbrella інтеграції в мережу

Огляд Umbrella

Umbrella: Єдина глобальна рекурсивна служба DNS

Use Umbrella DNS
208.67.222.222
208.67.220.220

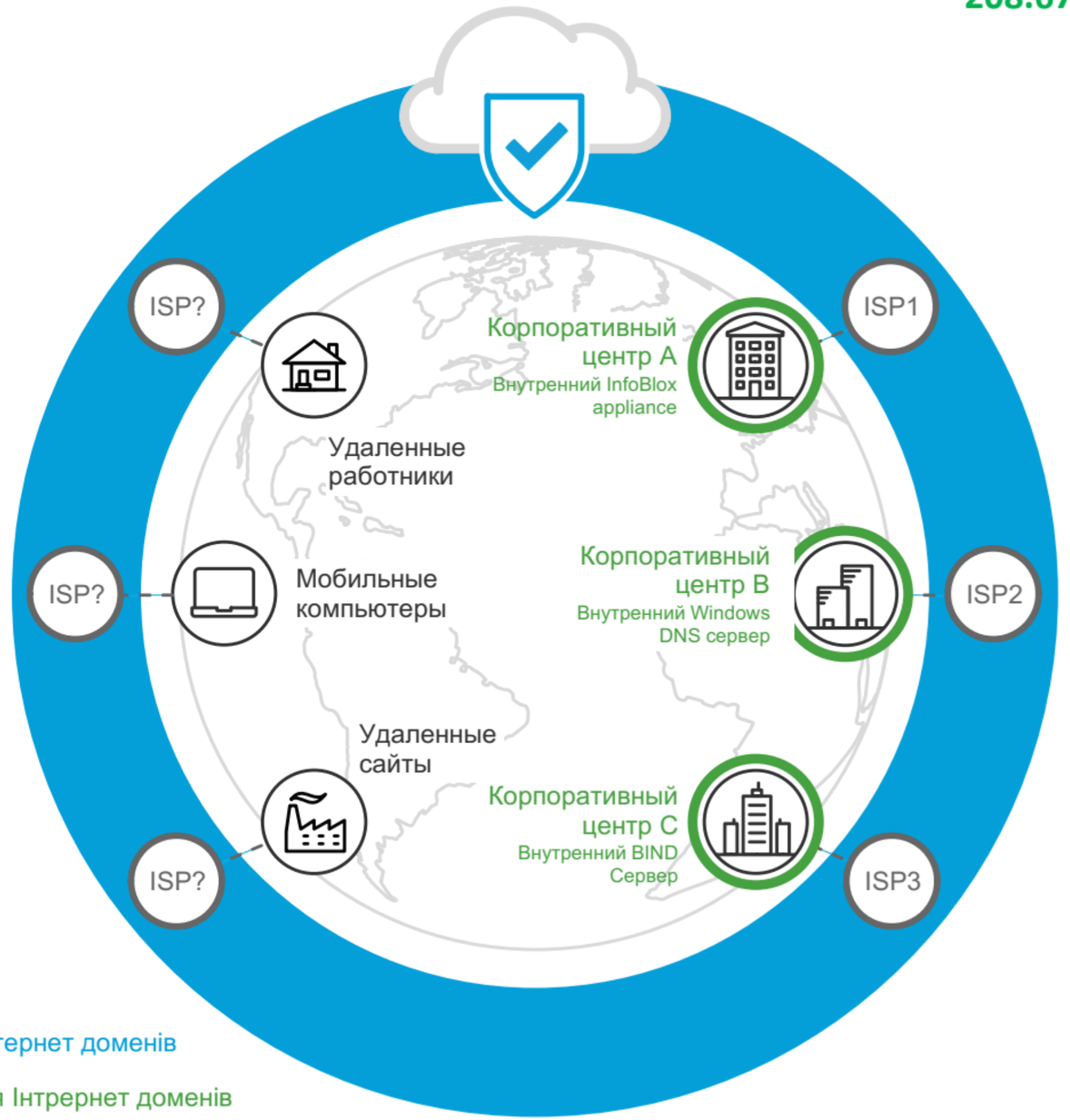
Переваги

Глобальна видимість інтернет-активності

Безпека мережі без додавання затримок

Комплексне застосування політик

Видимість інтернету з хмари



Рекурсивний DNS для Інтернет доменів

Авторитативний DNS для Інтрернет доменів

Use Umbrella DNS
208.67.222.222
208.67.220.220

Cisco Umbrella еволюція

DNS resolution

DNS + безопасность

Набор сервисов безопасности, интегрированный в облаке

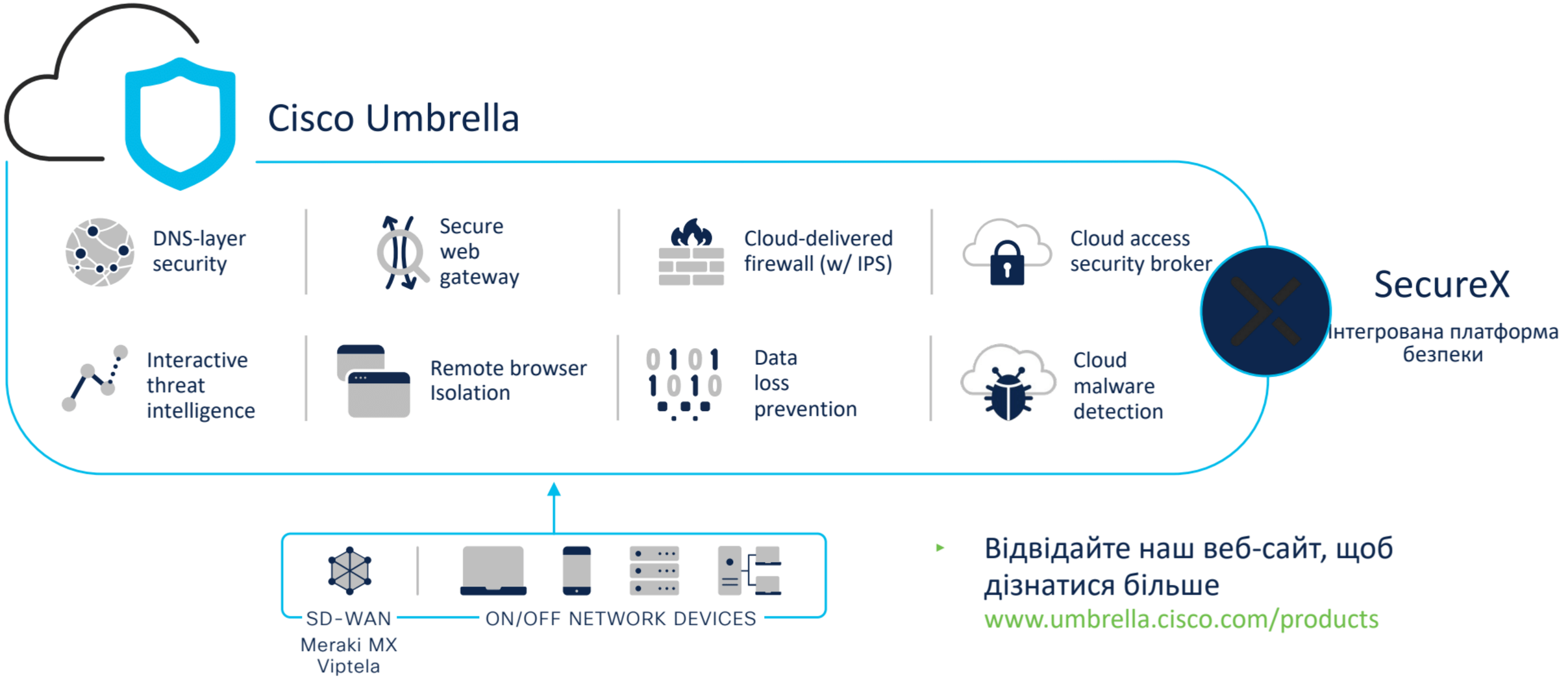
SIG

Многофункциональная безопасность и SD-WAN

Эволюция в сторону облачной, многофункциональной безопасности и сетевых услгу

SASE

Cisco Umbrella



- Відвідайте наш веб-сайт, щоб дізнатися більше
  www.umbrella.cisco.com/products

Ключові можливості Cisco Umbrella

Безпечний доступ до internet та використання хмарних додатків

Видимість

- В та поза корп.мережею
- Весь інтернет та веб-трафік
- Усі програми
- Всі пристрої
- Розшифровка SSL
- Тіньове IT
- Конфіденційні дані, що передаються

Захист

- Захист рівня DNS
- Веб-інспекція
- Перевірка файлів & пісочниця
- Запобігання втраті даних
- Перевірка невеб-трафіку
- Система запобігання вторгнень
- Віддалена ізоляція браузера
- Дані в стані спокою хмарне сканування шкідливих програм

Контроль

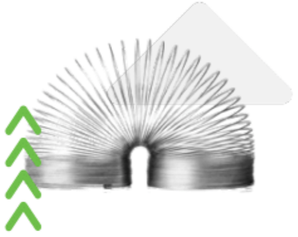
- Списки URL block/allow
- Правила порту та протоколу
- Детальні елементи керування програмами
- Фільтрація вмісту
- Блокування додатків
- Елементи керування клієнтом

Вбудована платформа розширеного виявлення та реагування (XDR) з Cisco SecureX

Глобальна хмарна архітектура Umbrella

Народжені в глобальній хмарній архітектурі

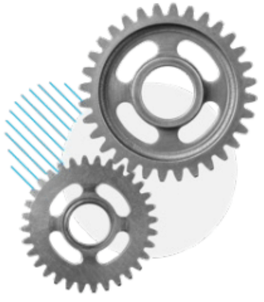
Швидка масштабованість, постійні інновації, висока продуктивність – без збоїв



Контейнерна, multi-tenant архітектура забезпечує масштабованість і надійність

Гнучка інфраструктура забезпечує безперервні інновації без простоїв клієнтів

Перевірений послужний список з 2006 року з глобальними центрами обробки даних на шести континентах



Низька затримка забезпечує високу продуктивність і до 73% скорочення затримки

Широке, глобальне покриття

38+

Центрів обробки даних по всьому світу

100%

Час безвідмовної роботи бізнесу з 2006 року

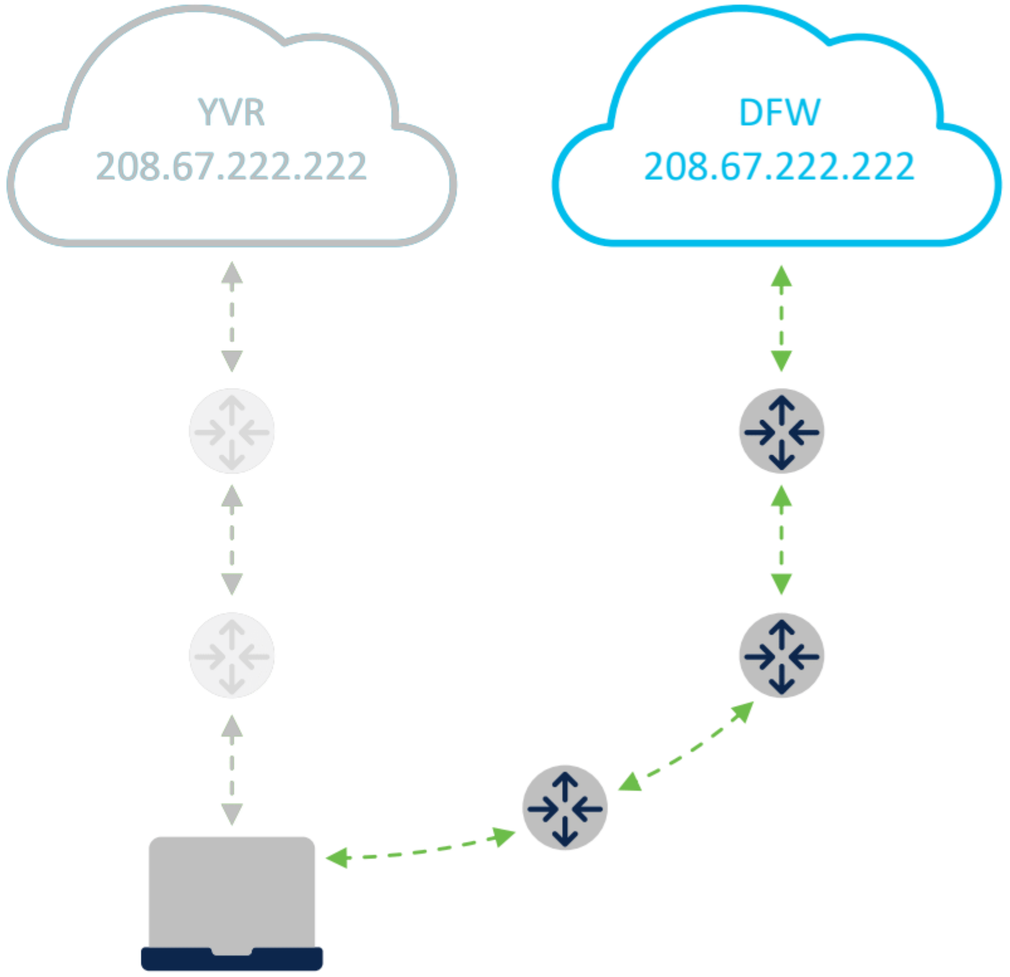
Затримка та оптимізація середньої милі - це те, що найважливіше враховувати при виборі постачальника SASE: https://umbrella.cisco.com/blog/how-to-measure-cloud-security-performance

Use Umbrella DNS
208.67.222.222
208.67.220.220

Маршрутизація Anycast IP для надійності

Захист рівня DNS

- Усі центри обробки даних оголошують однакову IP-адресу
- Клієнт спрямовує DNS на нашу IP-адресу
- Запити прозоро перенаправляються в найближчий доступний дата-центр з автоматичним перемиканням



Безпека DNS

Use Umbrella DNS
208.67.222.222
208.67.220.220

Перевірений лідер у сфері хмарної безпеки

620 млрд

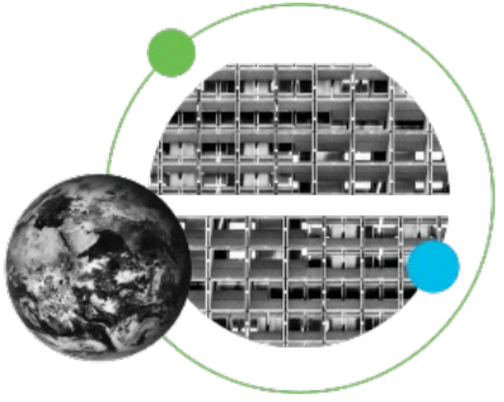
запитів на день

500 млн

Події аутентифікації щомісяця

500K

Глобальні клієнти



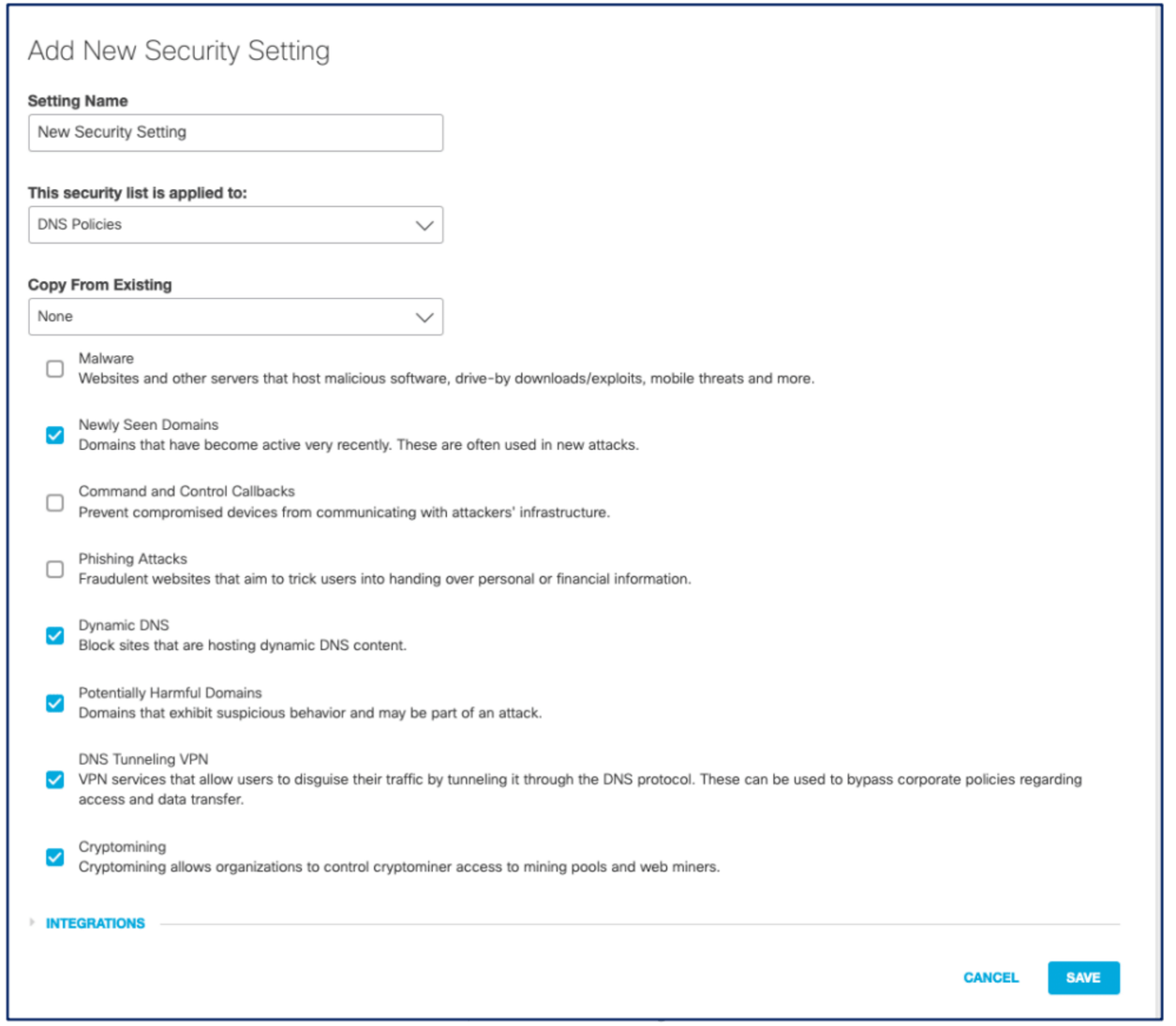
96%

Найвищий рівень виявлення загроз*

* 7% better than the 2nd rated and 32% better than the 3rd rated vendors.

Use Umbrella DNS
208.67.222.222
208.67.220.220

Унікальний захист для безпеки рівня DNS



- **Добре:** Безпека на рівні Umbrella DNS
- **Краще:** хмарний серві безпеки Umbrella з secure web gateway (повний проксі) та firewall.
- **Найкраще:** все

✓ Безпека рівня DNS пропонує унікальний захист

Use Umbrella DNS
208.67.222.222
208.67.220.220

DNS: освітня програма

Реєстратор доменів

Зіставлення записів імен з IP в "телефонній книзі"

GoDaddy

Авторитативний DNS

Публікація «телефонної книги» та володіння єю

amazon web services Route 53

Рекурсивний DNS

Шукає та зберігає записи для кожного імені

Cisco Umbrella

Use Umbrella DNS
208.67.222.222
208.67.220.220

Хто вирішує ваші запити DNS?

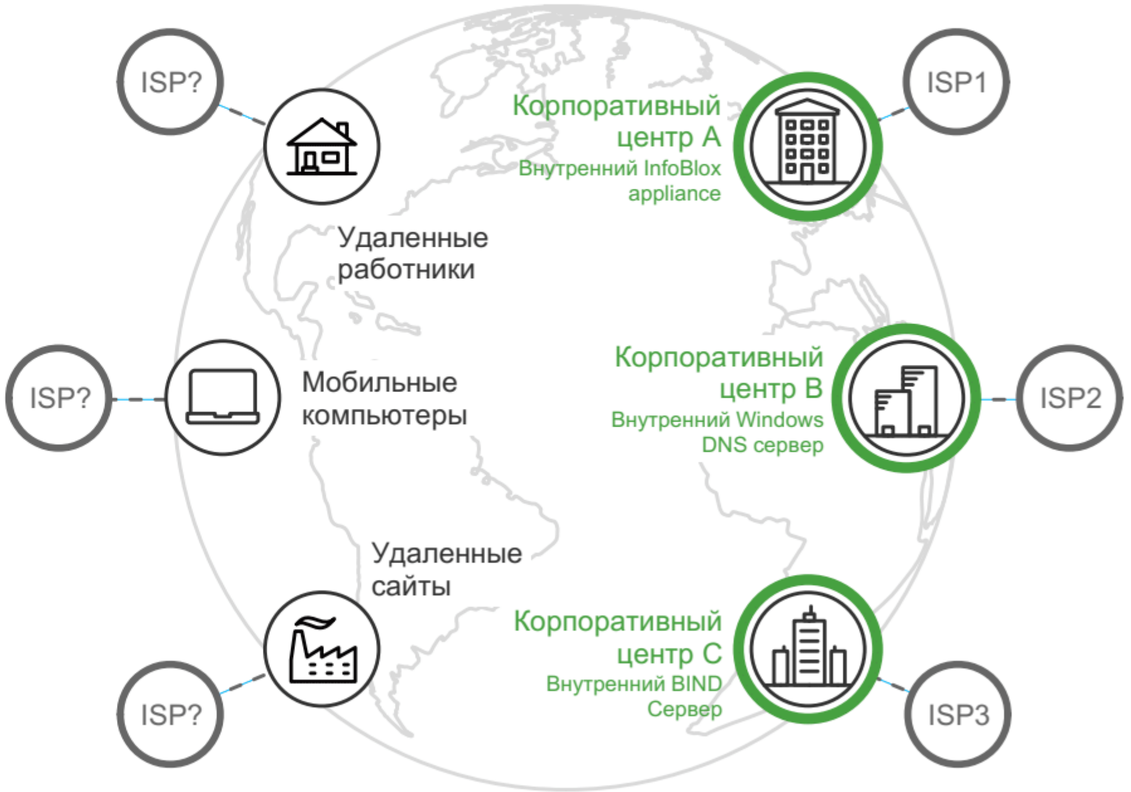
Проблеми

Багато інтернет-провайдерів

Пряме з'єднання філій

Користувачі забувають завжди вмикати VPN

Різні формати журналів DNS



Рекурсивный DNS для Интернет доменов

Авторитативный DNS для интранет доменов

Umbrella: Єдина глобальна рекурсивна служба DNS

Use Umbrella DNS
208.67.222.222
208.67.220.220

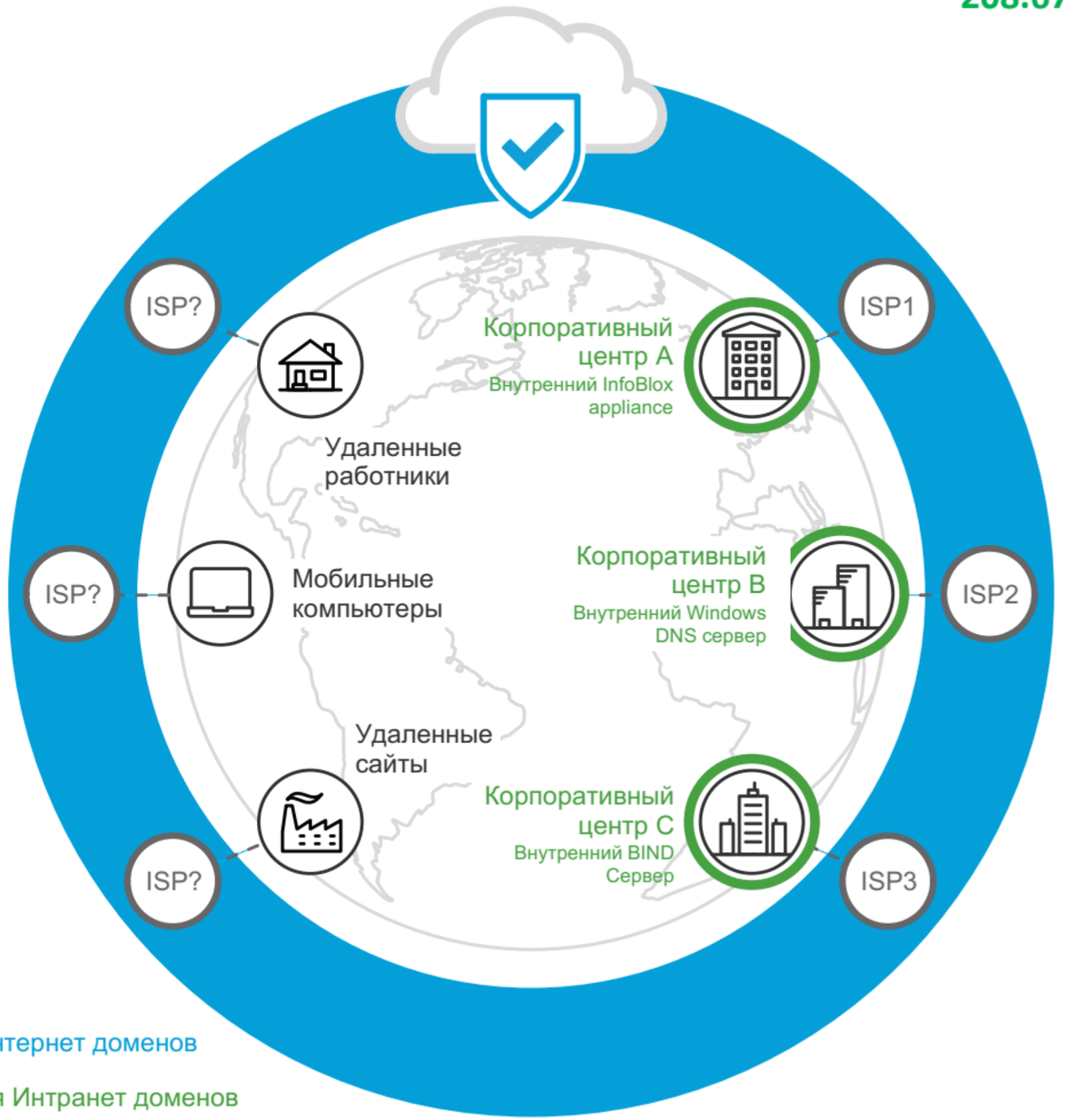
Переваги

Глобальна видимість інтернет-активності

Безпека мережі без додавання затримок

Комплексне застосування політик

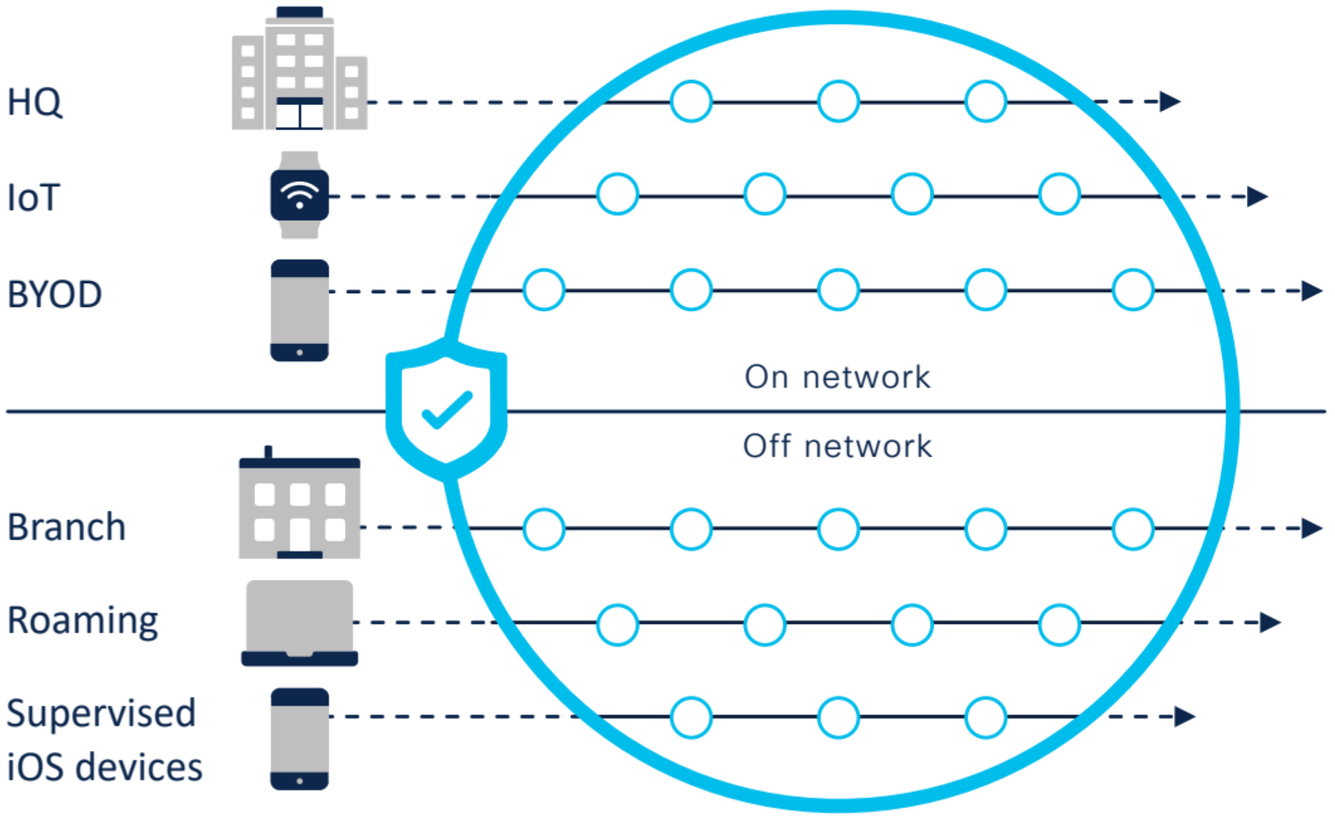
Видимість інтернету з хмари



Use Umbrella DNS
208.67.222.222
208.67.220.220

DNS безпека

Видимість і захист всієї діяльності, з будь-якого місця



- Всі офіси
- Будь-який пристрій в мережі
- Роумінг-пристрої
- Мобільні пристрої - iOS і Android
- Кожен порт і протокол

Use Umbrella DNS
208.67.222.222
208.67.220.220

Вбудовані в ядро Інтернету

Призначення

Вихідне місце призначення або заблокована сторінка

Контроль безпеки

- Правила DNS та IP
- Проксі-перевірка ризикових доменів
- Доступна розшифровка SSL

Інтернет-трафік

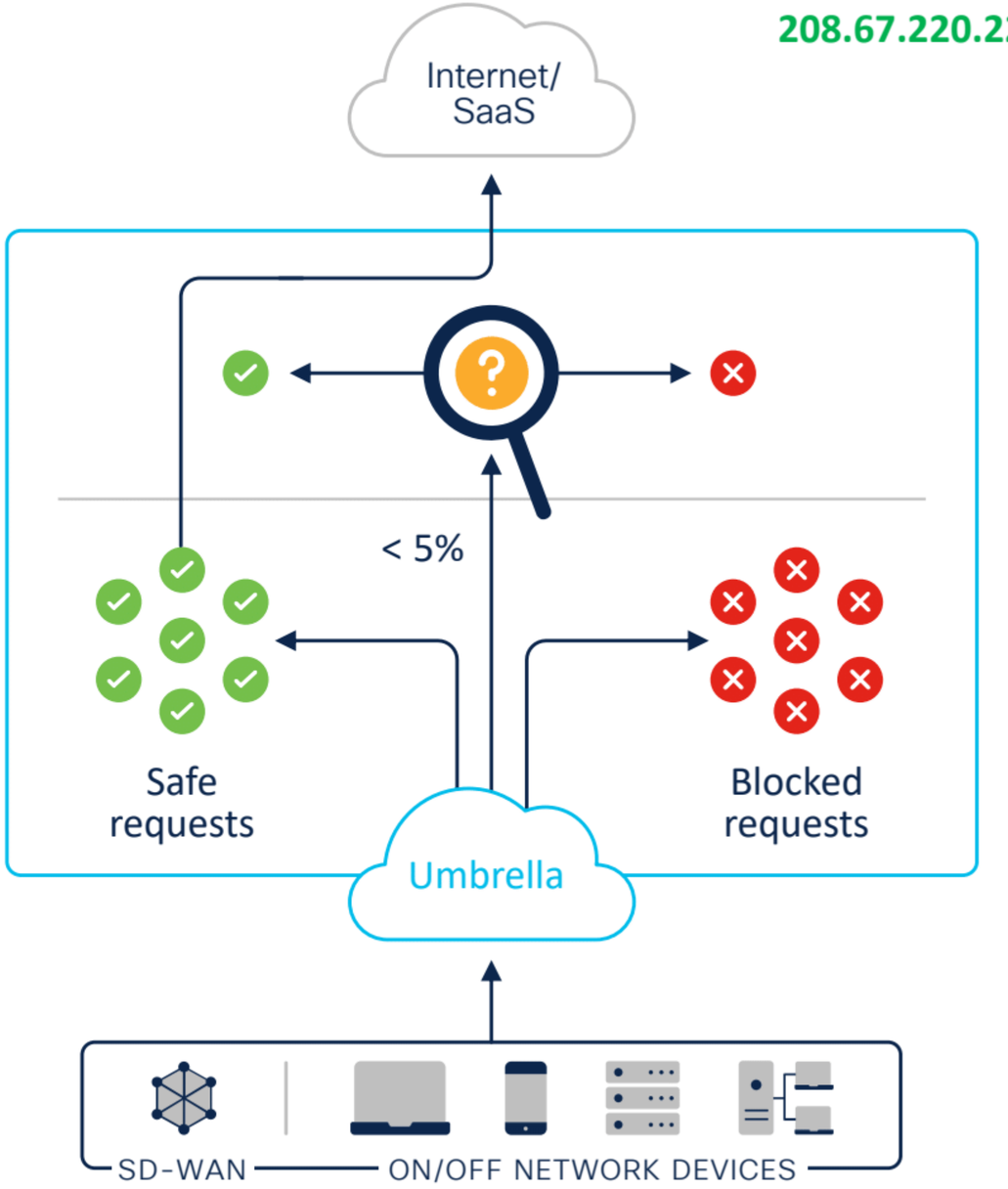
Мережевий та позамережевий

Use Umbrella DNS
208.67.222.222
208.67.220.220

Захист рівня DNS

Перша лінія оборони

- Розгортання по всьому підприємству за лічені хвилини
- Блокування доменів, пов'язаних зі malware, фішингом, викликами C&C
- Припинення загроз на самих ранніх етапах і стримування шкідливих програм, які вже знаходяться всередині
- Прискорення реагування на загрози за допомогою інтегрованої платформи безпеки



Use Umbrella DNS
208.67.222.222
208.67.220.220

Широта для охоплення всіх портів і глибина для перевірки протоколів

DNS і рівень IP

- Запит домену
- Відповідь IP (рівень DNS) або підключення (рівень IP)

Umbrella/Talos та партнерські канали

Спеціальні списки доменів

Спеціальні списки IP-адрес

Оновлення

Моделі Umbrella: статистичне та машинне навчання

Allow, block, proxy

Інтернет-телеметрія

HTTP/S layer

- URL запит
- Хеш файлу

WBRS/Talos + партнерские фиды

Кастомные списки URL

AV

Secure Endpoint
(AMP)

Allow або block

Use Umbrella DNS
208.67.222.222
208.67.220.220

Запобігає з'єднанням до та під час атаки

Інфікування через Web- та Email-

- Malvertising / exploit kit
- Фішинг / веб-посилання
- Компрометація «waterhole»

Атаки Command and control

- Завантажити шкідливе розширення
- Ключі шифрування
- Оновлена інструкція

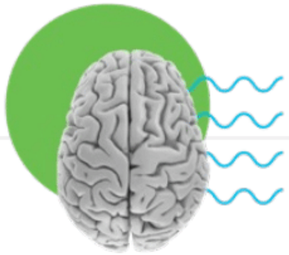
Зупиніть ексфільтрацію даних і виконання шкідливих програм

Use Umbrella DNS
208.67.222.222
208.67.220.220

Беззаперечна інформаційна база

Масивні та різноманітні дані

- >Сотні млрд запитів на день
- Сотні мільйонів активних користувачів, сотні тисяч комерційних підприємств
- З 190+ країн
-



Дослідники безпеки

- Відомі дослідники
- Побудова моделей, які автоматично класифікують і оцінюють домени та IP
-

Моделі

- Десятки моделей постійно аналізують мільйони «живих» подій в секунду.
- Автоматичне виявлення malware, ransomware та інших загроз

Use Umbrella DNS
208.67.222.222
208.67.220.220

Багатогранна кібераналітика

Use Umbrella DNS
208.67.222.222
208.67.220.220

Umbrella Investigate

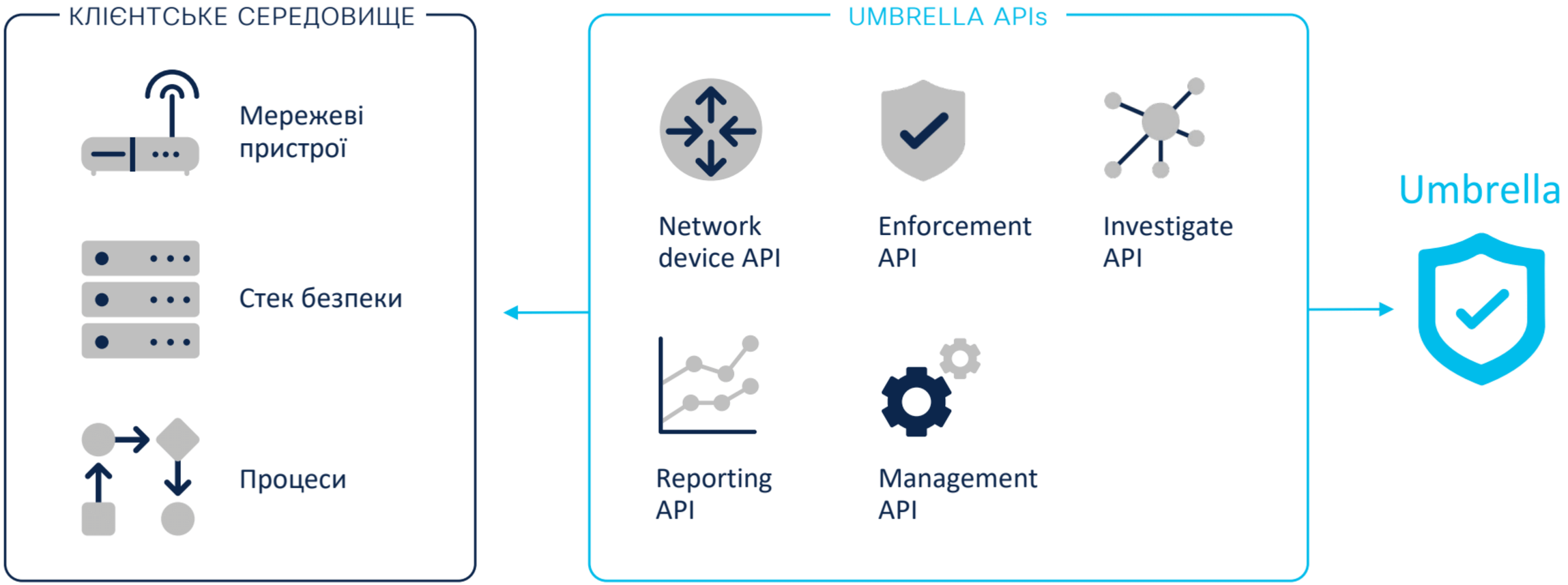
Велика інформація для швидкого сортування

- Отримайте глибоку видимість загроз з найбільш повним оглядом Інтернету
- Прискорення розслідування та реагування на інциденти
- Виявлення та прогнозування шкідливих доменів та IP
- Збагачуйте дані та сповіщення у вашій інфраструктурі за допомогою глобальної інформаційної системи

Use Umbrella DNS
208.67.222.222
208.67.220.220

API для легкої інтеграції

Збагачуйте дані та розширюйте захист для існуючих інструментів та процесів

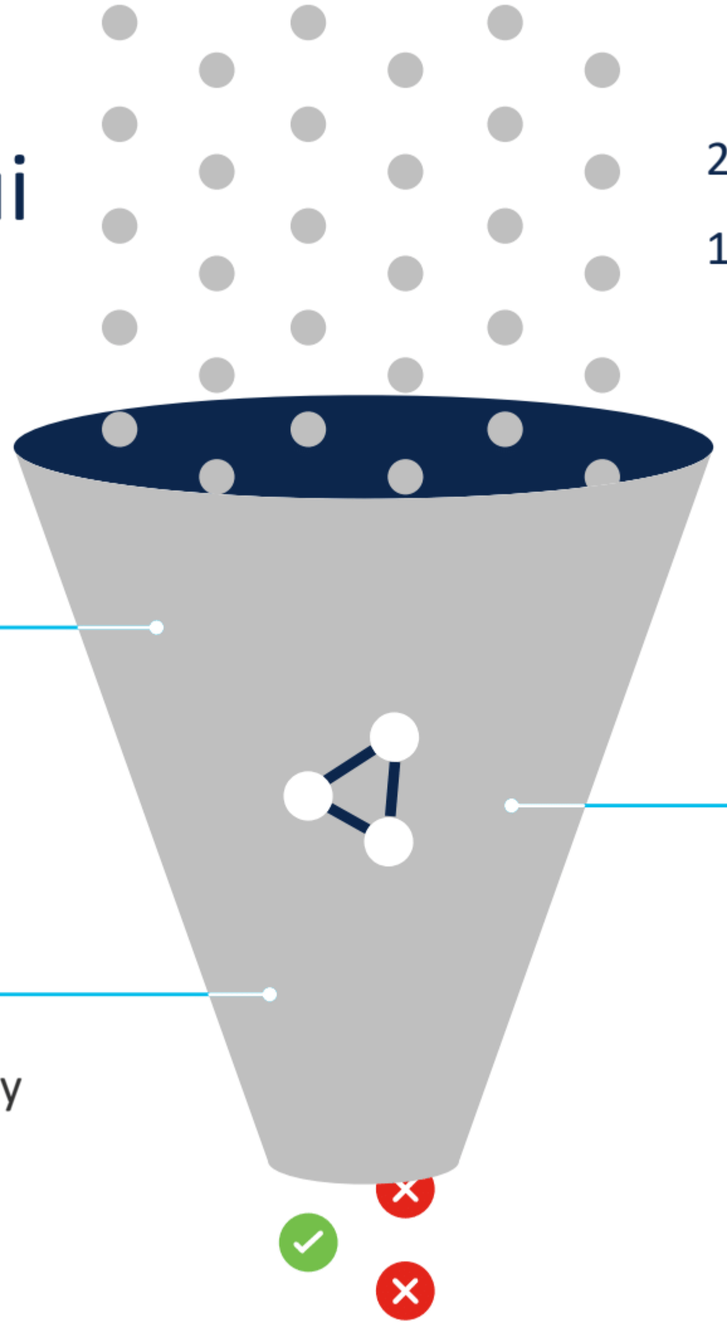


Use Umbrella DNS
208.67.222.222
208.67.220.220

Статистичні моделі

2 мільйон+ подій за секунду

11 мільярдів+ історичних подій



За висновком

- Модель спільних подій
- Sender rank model
- Secure rank model

За асоціацією

- Пасивне моделювання IP-простору
- Кореляція пасивних DNS і WHOIS

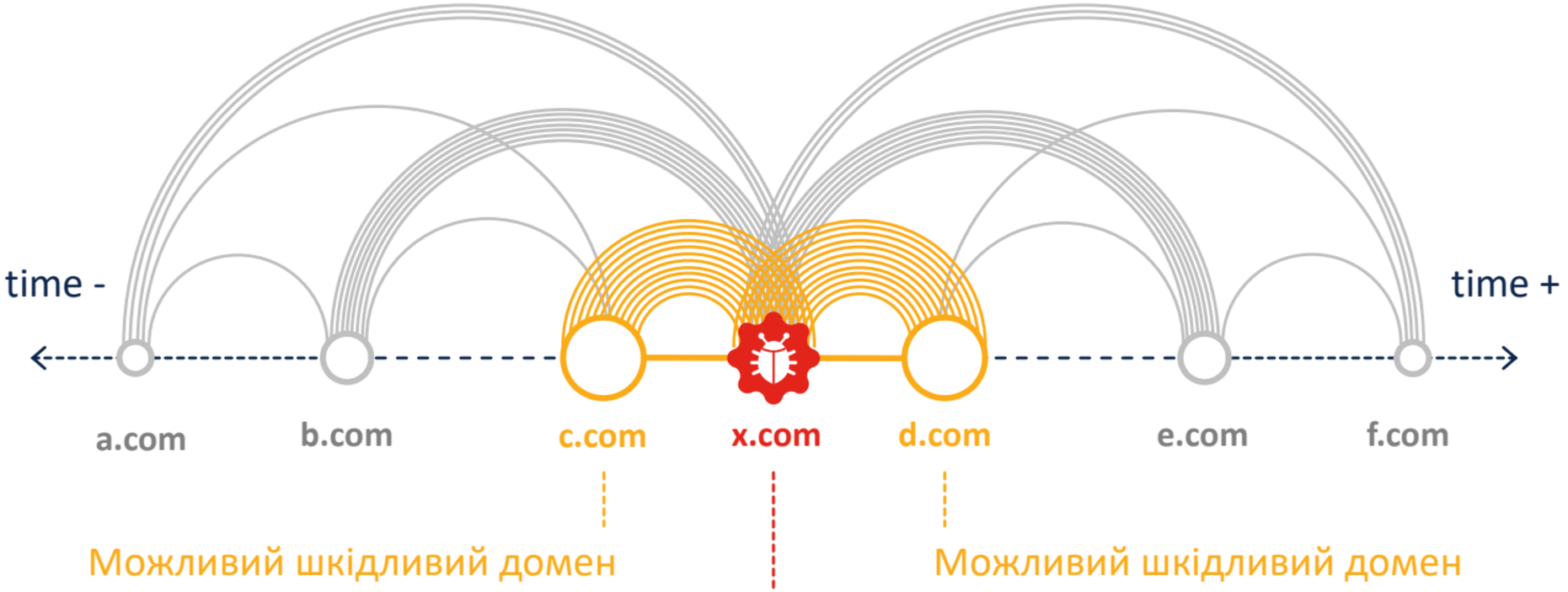
Шаблони звинувачень

- Модель пікового ранжирування
- Модель ранжирування NLP
- Передбачення DGA
- DNS тунелювання

Use Umbrella DNS
208.67.222.222
208.67.220.220

Модель спільних подій

Домени «звинувачуються» при за подіями



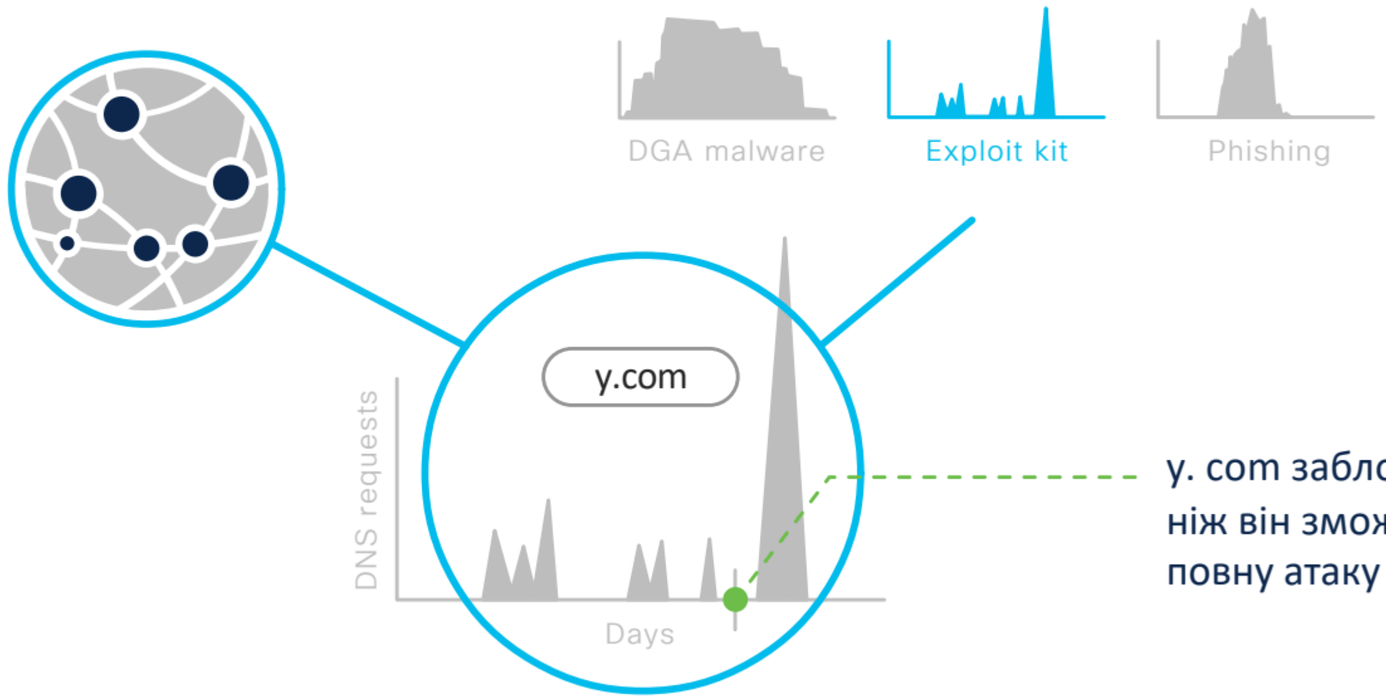
Спільні доменні події означають, що статистично значуща кількість об'єктів була запитана обома доменами одночасно за короткий проміжок часу

Use Umbrella DNS
208.67.222.222
208.67.220.220

Модель пікового ранжирування

Шаблони звинувачень

Збирається та аналізується величезний обсяг запитів DNS



y. com заблоковано, перш ніж він зможе розпочати повну атаку

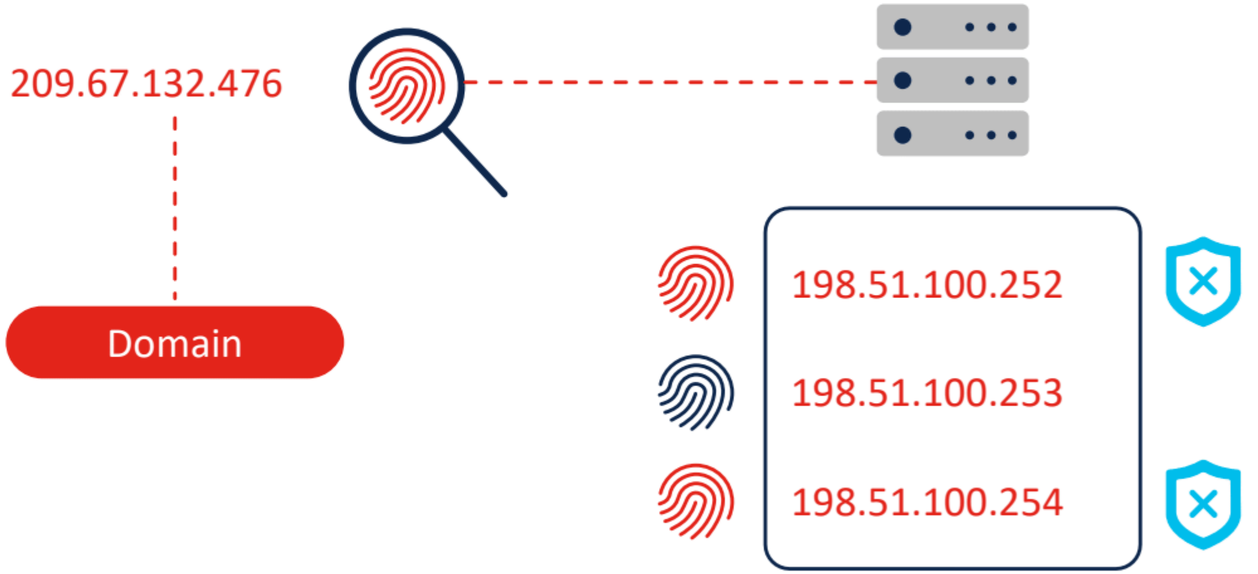
Обсяг DNS-запитів збігається з шаблоном відомого комплекту експлойтів і пророкує майбутню атаку

Use Umbrella DNS
208.67.222.222
208.67.220.220

Прогнозний моніторинг IP-простору

Звинувачення за асоціацією

- Позначення підозрілого домену та відстеження відбитків IP-адрес
- Ідентифікація інших IP-адрес, які розміщені на тому ж сервері та мають однакові відбитки пальців
- Блокування підозрілих IP-адрес і відповідних доменів



Use Umbrella DNS
208.67.222.222
208.67.220.220

Аналіз геолокації IP

інфраструктура вузлів

Розташування IP-адрес для конкретного домену

Хостинг по 28+ стран

DNS Запити

Розташування мережі та автономних пристроїв, які запитують домен

Только US клиенты запрашивают .RU TLD

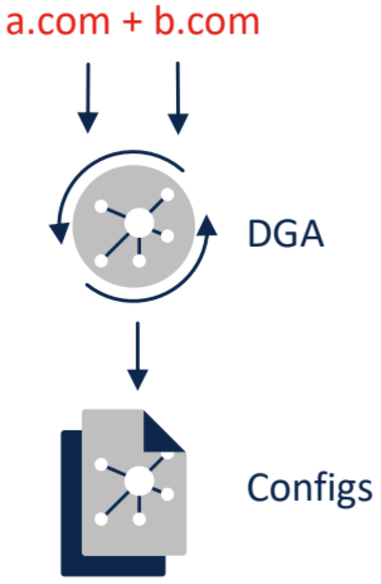
Use Umbrella DNS
208.67.222.222
208.67.220.220

«Живе» передбачення DGA

Автоматизація в безпрецедентних масштабах

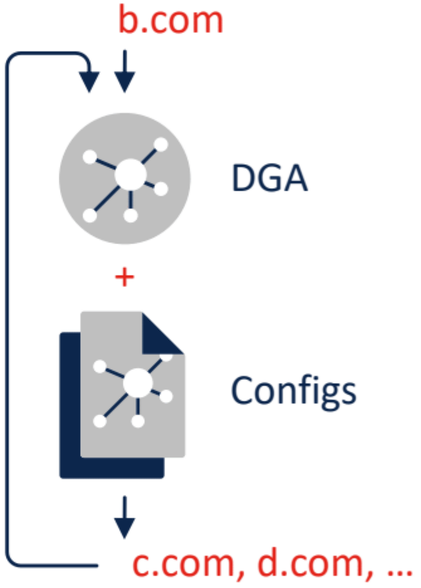
Живий потік журналів DNS

Визначення мільйонів доменів, багато з яких є DGA



Автоматичний реверс-інжинірінг

Об'єднання пар доменів C2 і відомих DGA для виявлення невідомих конфігурацій



Передбачення 100,000s майбутніх доменів

Інтеграція нових ідентифікованих конфігурацій з DGA для постійної ідентифікації доменів C2

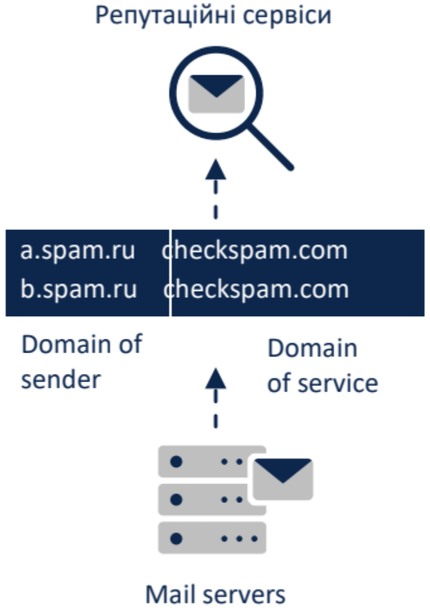
Автоблокування доменів пулу C2

Використовується тисячами зразків malwarezараз і в майбутньому

Use Umbrella DNS
208.67.222.222
208.67.220.220

Модель ранжирування відправника

Прогнозування доменів, пов'язаних зі спамерами



Визначення запитів на виявлення спам-служб

Користувачі DNS 85M+ піддаються атакам різних спам-кампаній і користуються послугами репутації

Модель агрегує графіки доменів щогодини

Короткі тиражі тисяч спам-листів використовують багато FQDN, щоб сховатися від репутаційних сервісів

Модель ідентифікує власників доменів Hailstorm

Після підтвердження запит на запис WHOIS для отримання реєстратора

Блокуйте доменів до того, як відбудеться атака

Зловмисники часто реєструють більше доменів для введення фішингових посилань або закликів C2 до шкідливого програмного забезпечення

Use Umbrella DNS
208.67.222.222
208.67.220.220

Категорія "Нові домени"

Знижує ризик невідомості

1. May have predictively blocked it already, and likely the first requestor was a free user 2. E.g. domain generated for CDN service 3. Usually 24 hours, but modified for best results, as needed.

Use Umbrella DNS
208.67.222.222
208.67.220.220

Новий аналіз і категорії

Для боротьби з тунелюванням даних DNS

500B+ DNS-запитів щодня

Потокові сигнатурні події

Автоматична ідентифікація шкідливої або навмисної ексфільтрації даних або інструментів з відкритим кодом (наприклад, DNS2TCP).

Автоматизуйте поведінковий аналіз та роботу аналітиків

Ручна ідентифікація комерційних послуг (наприклад, ваша свобода) або норми. користувачів щогодини.

Машинне навчання виявляє велику кількість піддоменів з даними кодування символів. Plus виявляє клієнтів, які запитують велику кількість субдоменів

Undetermined

Malware
(e.g. PisLoader)

Potentially harmful domains*

DNS туннелирование VPN*

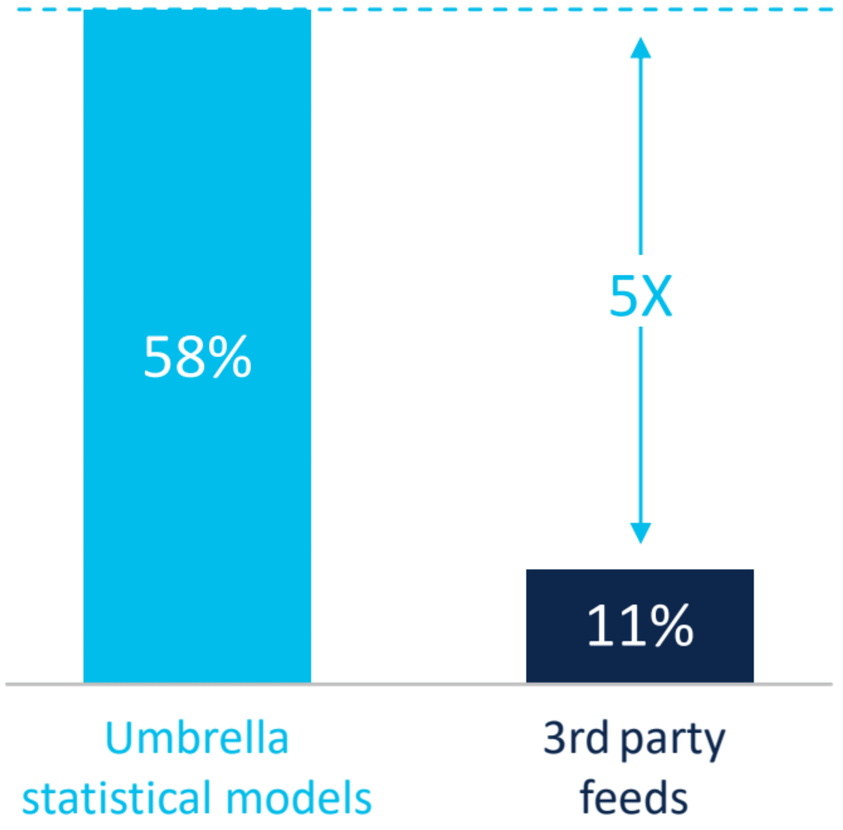
Скрытый белый список
(e.g. AV updates)

*New categories: These are allowed by default, but can be blocked. And domains in these categories may have already been categorized as Malware or Botnet (a.k.a. C2 callbacks) by many other Umbrella statistical models.

Use Umbrella DNS
208.67.222.222
208.67.220.220

Статистичні моделі Umbrella IT в 5 разів більш релевантні, ніж зовнішні бази даних

- Релевантність вимірює, наскільки кожне джерело, що пропонує інформацію, блокує активні загрози нашій клієнтській базі
- Вища релевантність – краще охоплення від активних загроз
- Статистичні моделі Umbrella IT мають більш високу актуальність, оскільки моделі швидко адаптуються до мінливого ландшафту загроз.



Інтерактивна кібераналітика

Use Umbrella DNS
208.67.222.222
208.67.220.220

Cisco Talos: найбільша організація з кібераналітики на планеті

- 400+ дослідників та аналітиків
- 5 млрд запитів на репутацію, 2 млрд щоденних зразків шкідливого пз
- 5 млрд реакції категоризації, 200 млн IPs та URLs блокується щоденно.

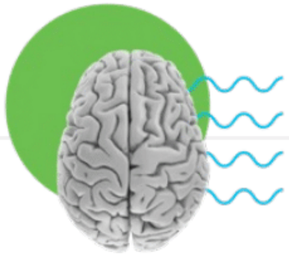
Ми бачимо більше, щоб ви могли більше блокувати та швидше реагувати на загрози.

Use Umbrella DNS
208.67.222.222
208.67.220.220

Статистичні моделі та машинне навчання

Масивна і розподілена видимість

- 5 мільярдів щоденних запитів на репутацію
- 2 млрд обробляються щоденні зразки malware
- 200+ нові виявлені вразливості на рік



Дослідники

- Провідні аналітики та дослідники
- Розробити навчальні моделі, які автоматично класифікують та оцінюють домени та IP-адреси

Моделі

- Десятки моделей, які безперервно аналізують мільйони живих подій в секунду
- Автоматичне визначення malware, ransomware, та інших загроз

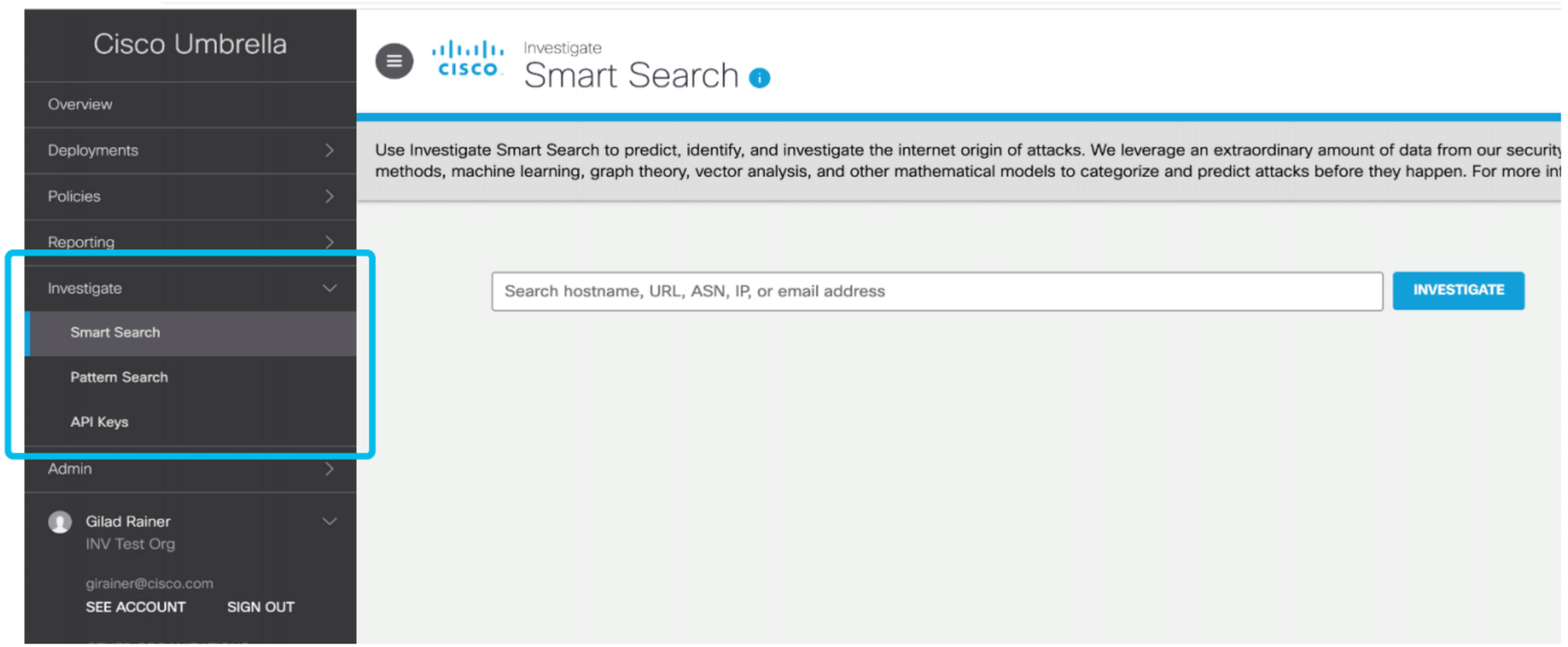
Use Umbrella DNS
208.67.222.222
208.67.220.220

Багатогранна кібераналітика

Use Umbrella DNS
208.67.222.222
208.67.220.220

Прозора навігація

Investigate вбудован в Umbrella



- Доступ до Investigate з IT-консолі Umbrella спрощений. Тепер користувачі можуть швидко перемикатися на Investigate і запускати Smart Search або Pattern Search.
- Клієнти можуть швидко знайти ключі API для своїх організацій

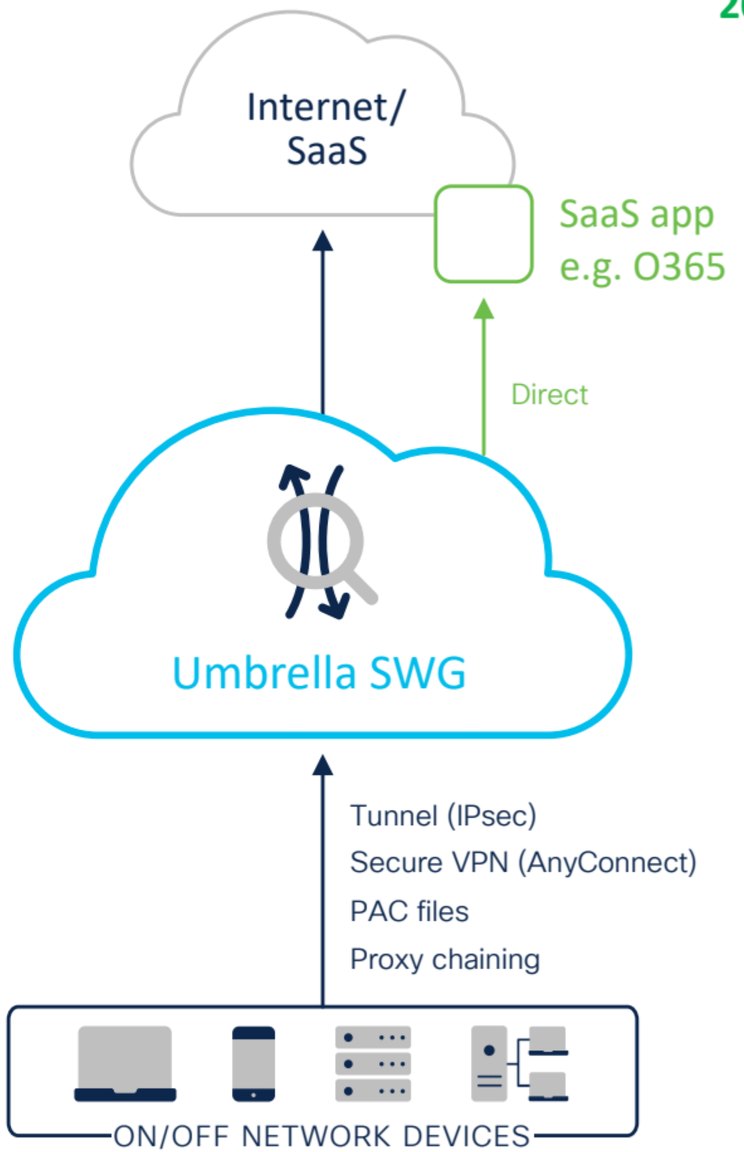
Secure Web Gateway

Use Umbrella DNS
208.67.222.222
208.67.220.220

Umbrella SWG

Багато функцій і зведена звітність з єдиної хмарної консолі

- Сканування malware, яке включає два антивіруси Cisco Antimalware (AMP)
- Елемент керування типом файлу
- Повне або вибіркове розшифровка SSL
- Фільтрування категорій або URL-адрес для керування вмістом
- Сканування файлів у пісочниці Secure Malware Analytics (ThreatGrid)
- Видимість застосування і детальний контроль
- Повна звітність на рівні URL-адрес

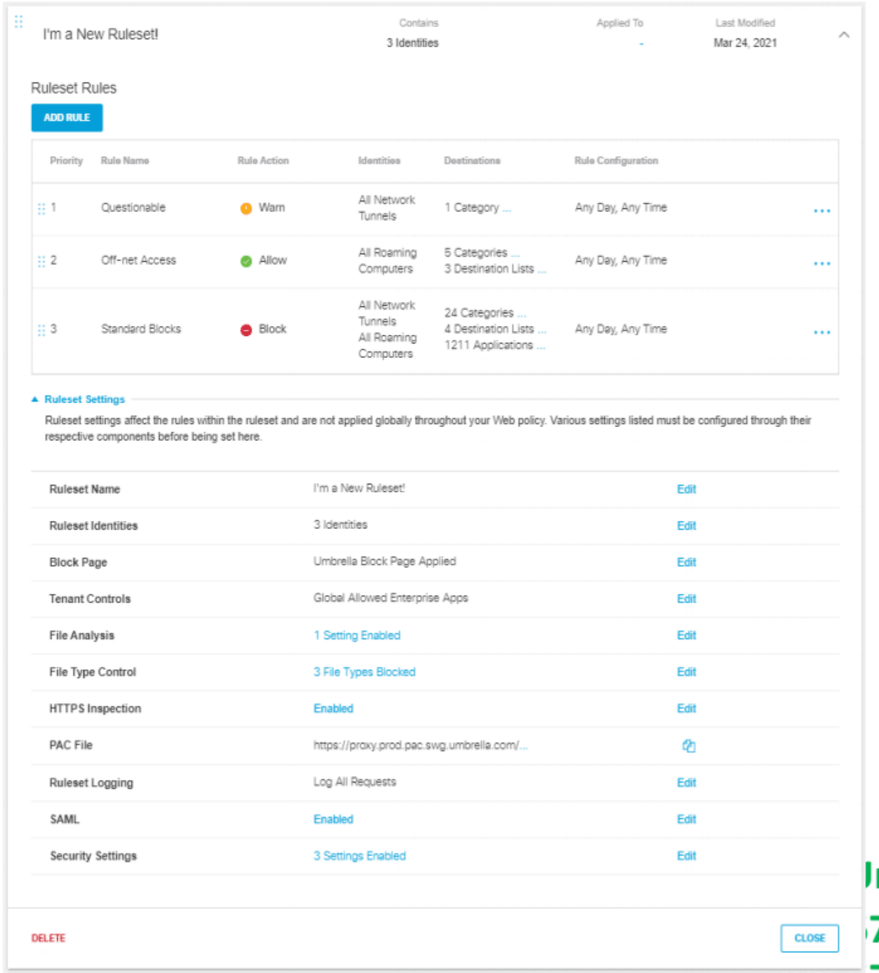


Правила Umbrella

Огляд: *Набори правил Umbrella забезпечують детальний контроль і дозволяють створювати більш складні стратегії*

Можливості

- Створення певних правил, які дозволяють, забороняють або забороняють доступ до певних ресурсів
- Пошук правил за identity і метою
- Гнучкість у створенні веб-політик
- Створення винятків

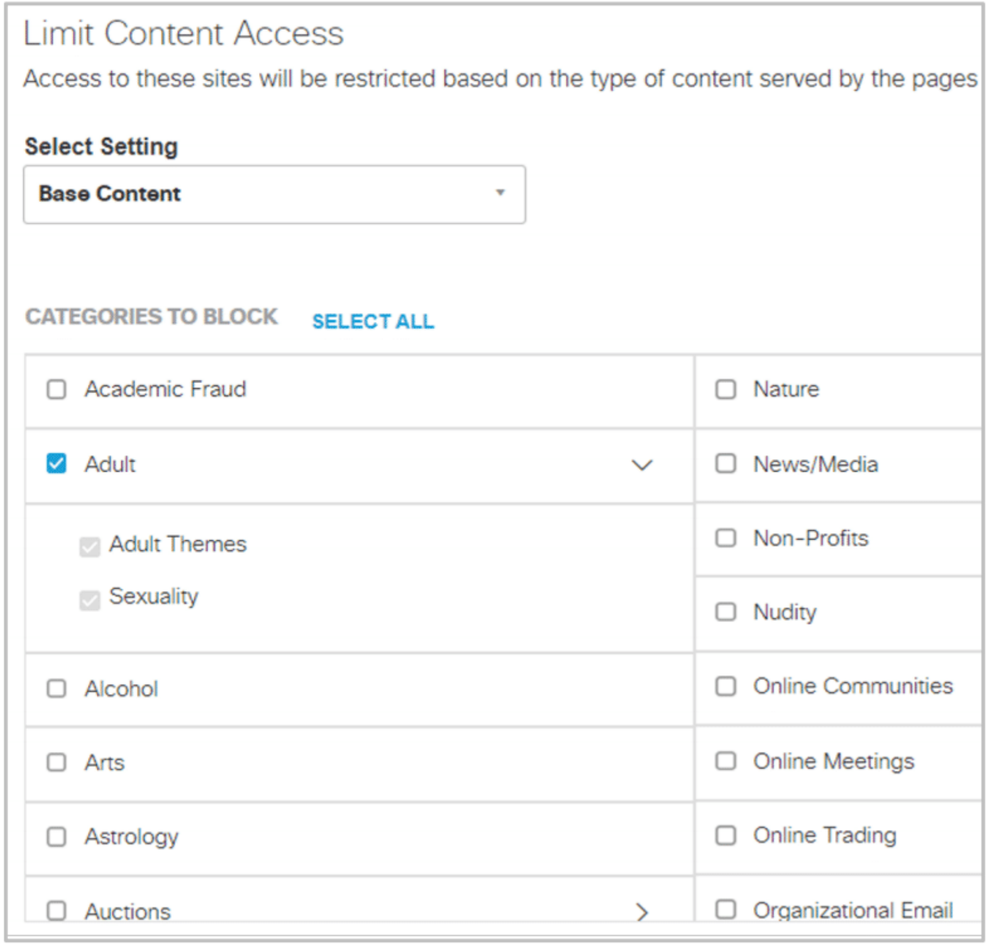


Umbrella DNS
7.222.222
208.67.220.220

Use Umbrella DNS
208.67.222.222
208.67.220.220

Категорія

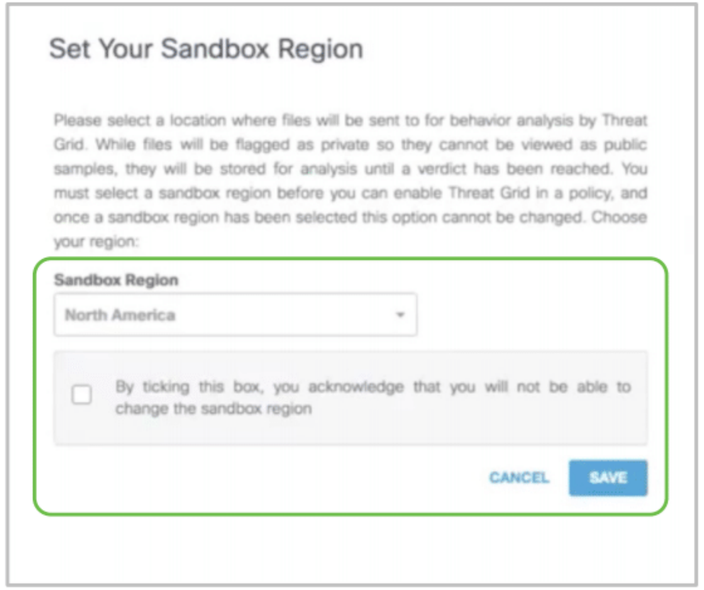
- Застосування політик до великої кількості сайтів
  - Категорії вмісту використовуються для політик використання (“acceptable use policies”)
  - Категорії безпеки для політик безпеки
- Umbrella SWG використовує категорії Talos для вмісту та безпеки
- Понад 100+ категорій
- Динамічні хмарні оновлення
-



Use Umbrella DNS
208.67.222.222
208.67.220.220

Песочница Cisco Secure Malware Analytics (Threat Grid)

- Можливість виявлення прихованих загроз у завантажуваних файлах
- Набір нових файлів або файлів з високим ризиком розміщується в ізольованому середовищі та сканується на наявність шкідливої активності/вміст
- Для файлу, у якому відображаються підозрілі дії, відображаються попередженн
- Для цього файлу оновлюється Umbrella кібераналітика



Регионы:
Европа или Северная Америка

SIG Essentials имеет ограничения Cisco Secure Malware Analytics 500 файлов/день

SIG Advantage включает неограниченное количество файлов и доступ к полному варианту консоли для 3 пользователей

Use Umbrella DNS
208.67.222.222
208.67.220.220

Secure Malware Analytics (Threat Grid)

Огляд в пісочниці

- Файли, які пройшли через антивірус та інші інструменти (менше, ніж 50 Мб)
- Файли, яких ми раніше не бачили в Cisco Secure Malware Analytics і які мають атрибути, змодельовані в цільовій моделі Cisco Secure Malware Analytics
- Щоб визначити тип файлу, ми використовуємо libmagic та розширення

File Retrospective

Recent Retrospective Events

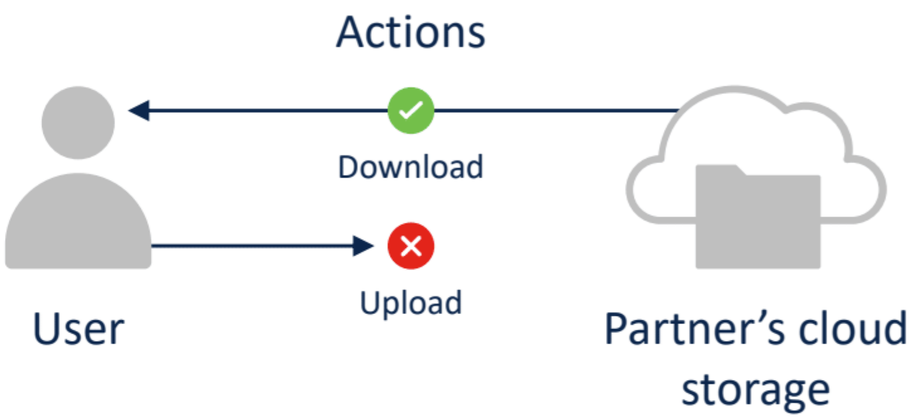
SHA256	Threat Score	Malware Name	Date Detected
7638f6d4a9cd3ea5fa88f9958da6e6e745b2931b96ecea...	100	W32.7638F6D4A9-100.SBX.TG	Jul 30, 2019 at 3:22 AM
526b2cad716f7dc1e568d5e68b8a251d19e129308806b...	100	W32.526B2CAD71-100.SBX.TG	Jul 27, 2019 at 3:23 AM
1a27fdf68d61964ddc13a62a75b15b7c94978def0b014...	100	W32.1A27FDF68D-100.SBX.TG	Jul 26, 2019 at 3:24 AM
49ade947bb9de7ce36f9735f90758d8425f939c2ce84b6...	100	W32.49ADE947BB-100.SBX.TG	Jul 25, 2019 at 4:31 AM
f9f23288188bc1a959e890084cc685db4ff9c50b95a52a...	100	W32.F9F2328818-100.SBX.TG	Jul 24, 2019 at 3:26 AM

1 - 5 of 32

Use Umbrella DNS
208.67.222.222
208.67.220.220

Детальний контроль популярних SaaS-додатків

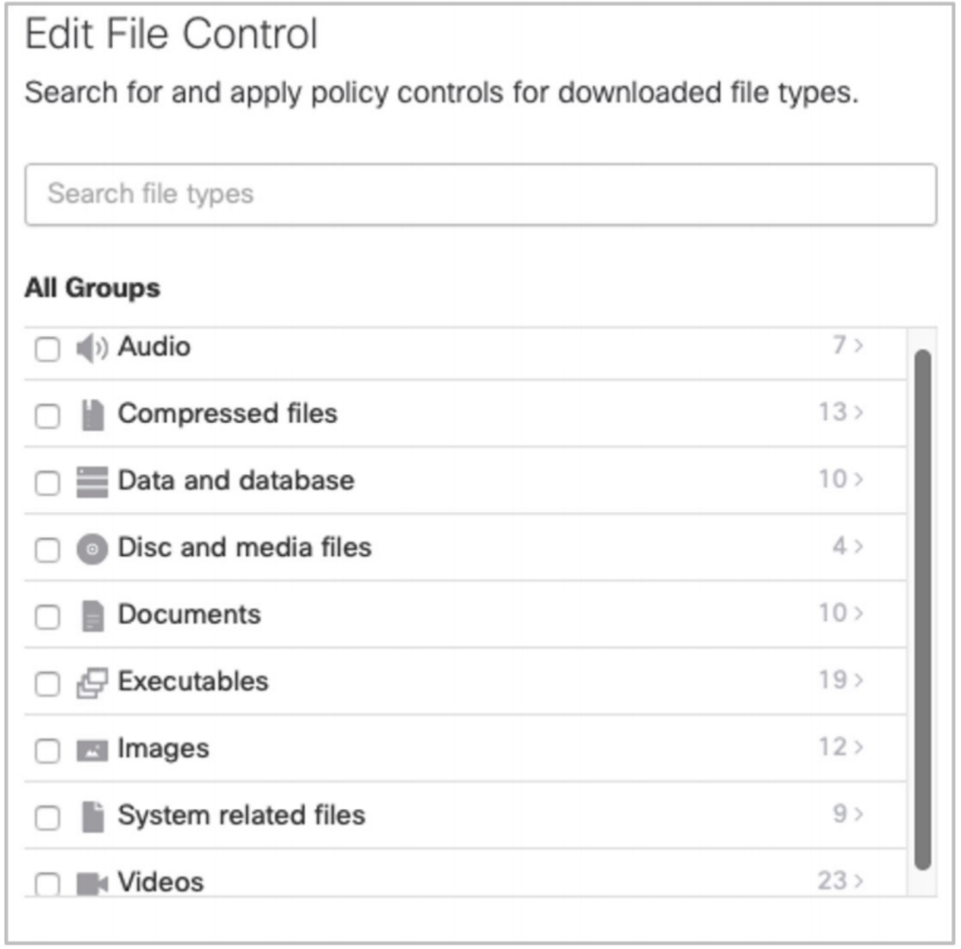
- Блокування постів/обмінів додатків соцмереж
- Блокування приєднаних файлів для webmail
- Блокування вивантаження на хмарне сховище, програми для спільної роботи, офісні програми для керування вмістом тощо.

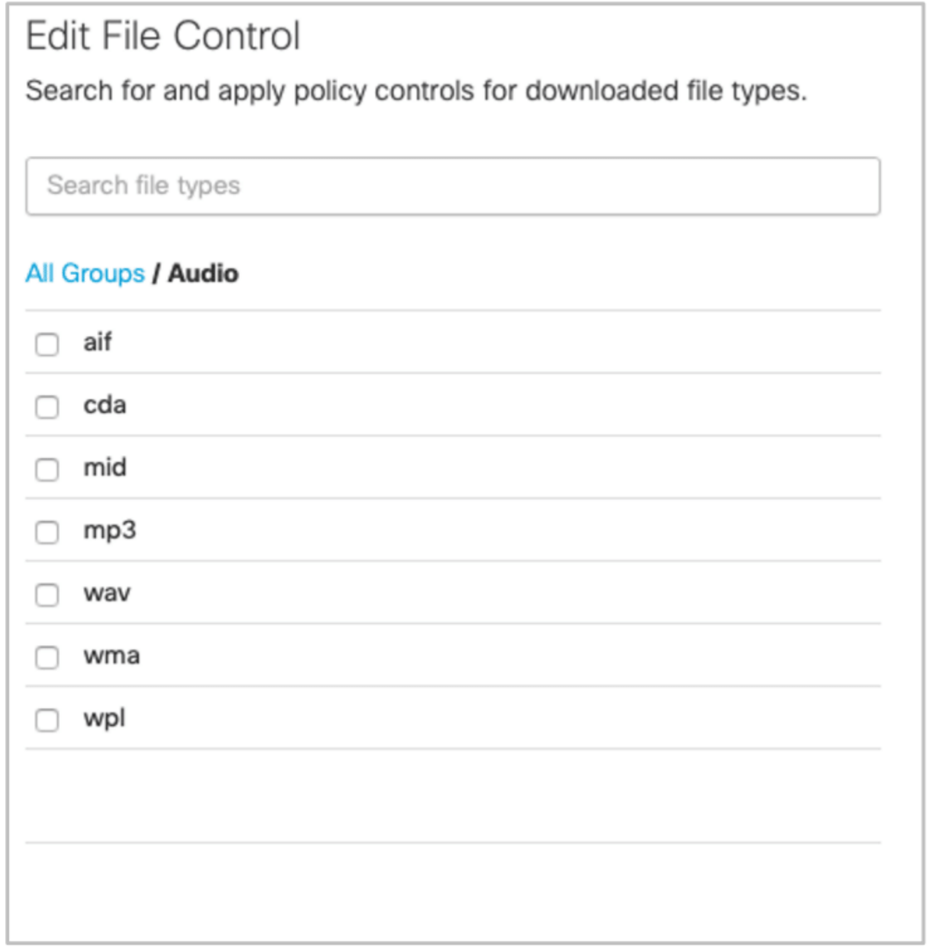


box twitter Dropbox Pinterest Messenger Gmail facebook LinkedIn slack
Instagram Google Drive SlideShare YouTube vimeo WhatsApp smartsheet PASTEBIN

Use Umbrella DNS
208.67.222.222
208.67.220.220

File type control – категорії та типи файлів

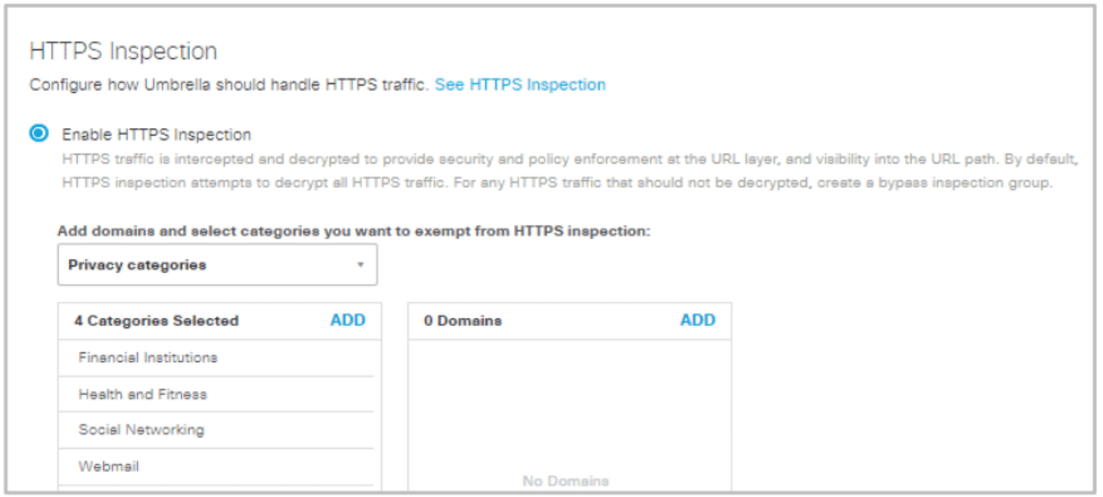




Use Umbrella DNS
208.67.222.222
208.67.220.220

Хмарна розшифровка SSL/HTTPS

- Видимість і набір правил безпеки для зашифрованого веб-трафіку
- Дешифруйте, повідомляйте та перевіряйте зашифрований трафік і файли
  - Не потрібне дороге обладнання
  - Нео проблеми з масштабуванням, коли збільшується обсяг зашифрованого інтернет-трафіку
  - Можливість вибіркової вишивки
  -



Use Umbrella DNS
208.67.222.222
208.67.220.220

Режим сумісності з Microsoft

- Організації, які покладаються на M365 у своїх робочих процесах і потребують високої продуктивності
- Microsoft не рекомендує перевірку трафіка для M365

- ✔ Режим сумісності гарантує, що трафік M365 прозоро проходить через Umbrella, але ви все одно отримаєте покращення продуктивності завдяки використанню Umbrella Backbone
- ✔ Використання API Microsoft для визначення доменів для виключення
- ✔ Якщо цю функцію ввімкнуто, політики не застосовуватимуться до трафіку M365
- ✔ Але Umbrella все одно буде реєструвати весь трафік на ці домени.

Use Umbrella DNS
208.67.222.222
208.67.220.220

Атрибуція та аутентифікація користувачів

- Security Assertion Markup Language (SAML 2.0)
  - Service Provider (SP) – Umbrella
  - Identity Provider (IdP) –PingID, Okta, Azure, Duo, OpenAM, ADFS, та інші в основній підтримці
- Варіанти підтримки surrogates
  - Cookie surrogate – вимагає інспекції HTTP/HTTPS, ви можете вказати час завершення
  - IP surrogate - Перевірка HTTPS не потрібна, більш безшовна аутентифікація userID
- Призначений для браузерів, може не працювати з “desktop apps”

Use Umbrella DNS
208.67.222.222
208.67.220.220

Атрибуція користувача з одного сайту

- Citrix/TS може мати багато користувачів за одним IP
- Secure web gateway використовує SAML аутентифікацію через cookie surrogate
- Cookie surrogate підтримує багато користувачів за одним IP
- Підтримує virtual desktops (Citrix/TS) та published browsers (Citrix)

Use Umbrella DNS
208.67.222.222
208.67.220.220

SWG користувачі та групи

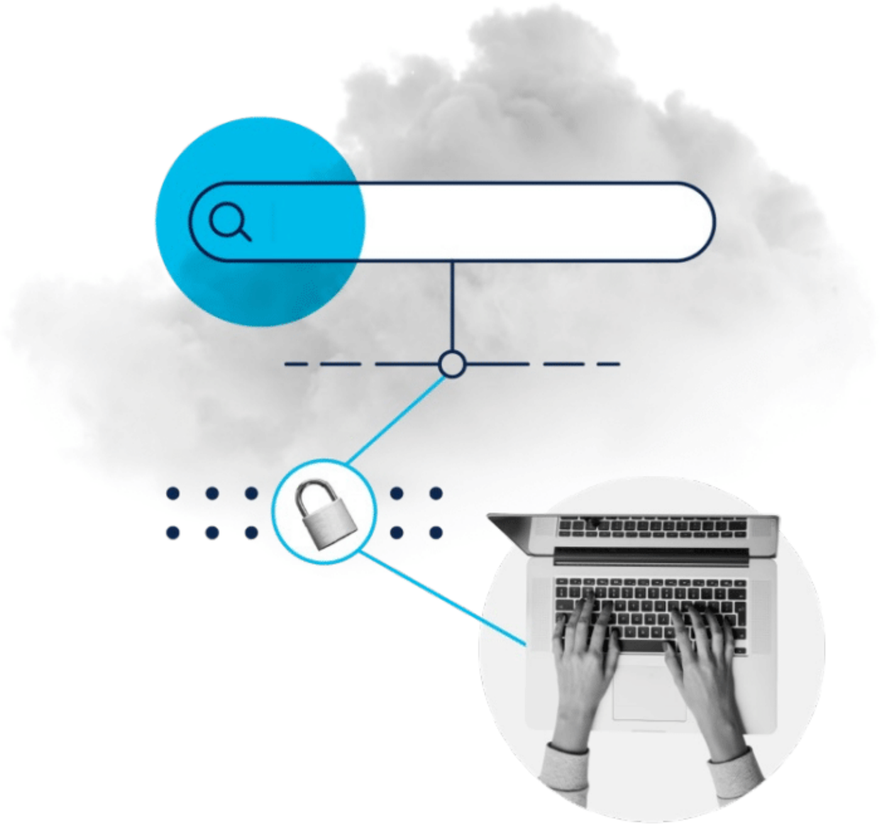
- CSV вивантаження
  - Рекомендоване використання CSVDE на Windows Domain Controller
- AD конектор Active Directory sync
  - Фільтрування груп підтримується
  - Встановлення стандартного конектора AD 1.3.8+
  - Треба один Domain Controller,
    не треба VA

Use Umbrella DNS
208.67.222.222
208.67.220.220

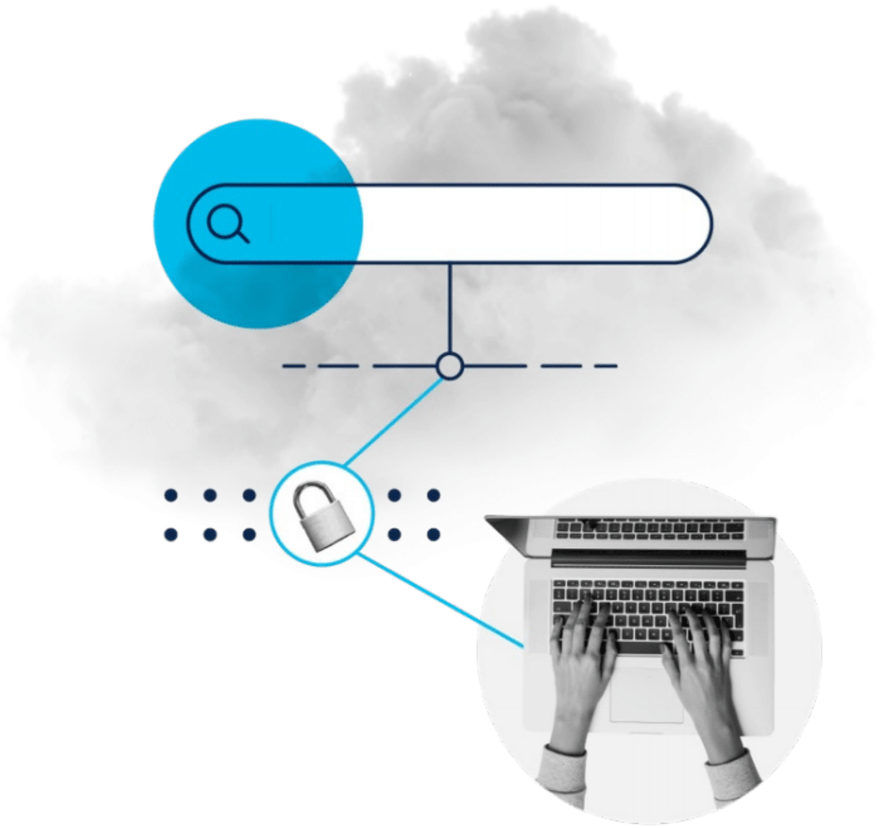
НОВЕ!
Umbrella remote browser isolation (RBI)

Новий рівень безпеки для підозрілих користувачів і сайтів

- Забезпечити ізоляцію між призначеним для користувача пристроєм і загрозами, яким піддається браузер
- Швидке розгортання, не змінюючи наявну конфігурацію
- Забезпечує безпечний перегляд із захистом від загроз нульового дня



Use Umbrella DNS
208.67.222.222
208.67.220.220



Remote browser isolation

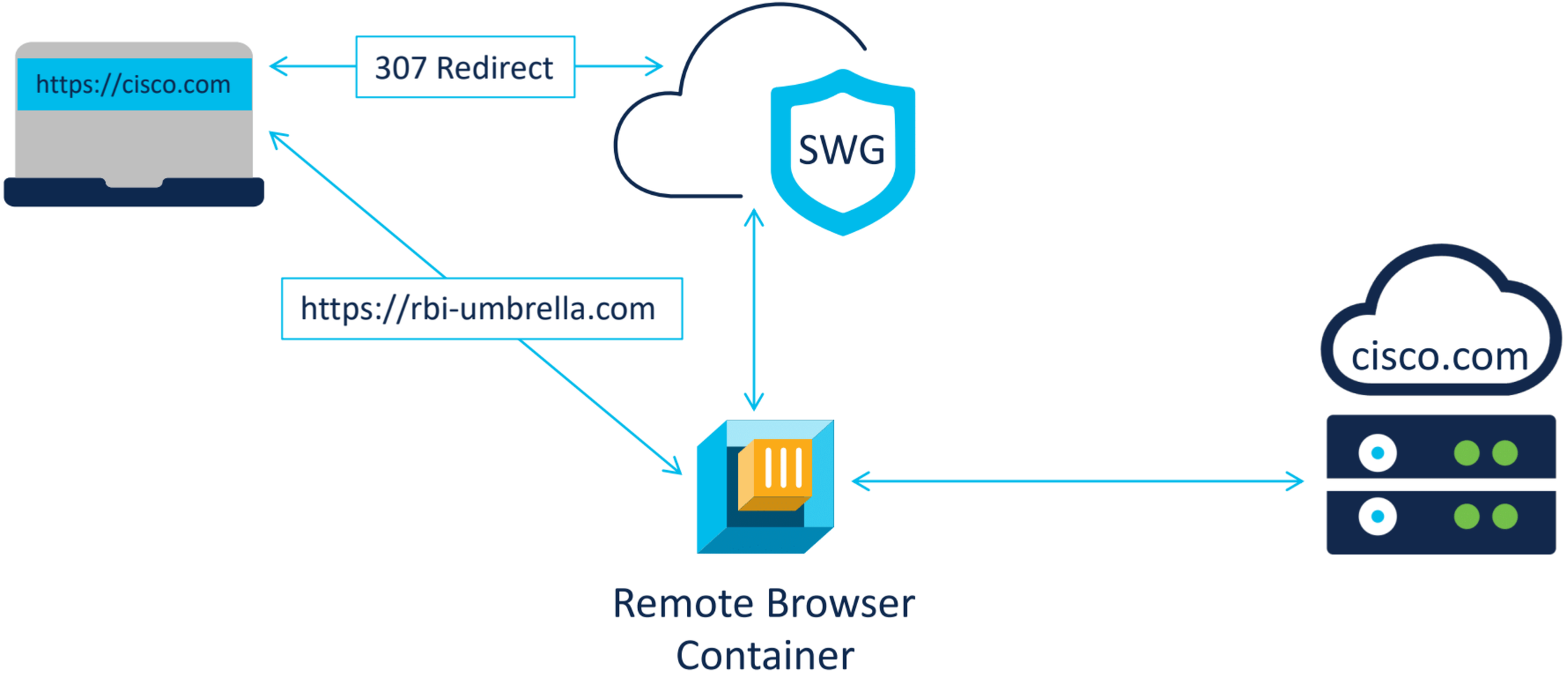
Завдання

Забезпечте безпечний перегляд веб-сторінок із захистом від загроз нульового дня

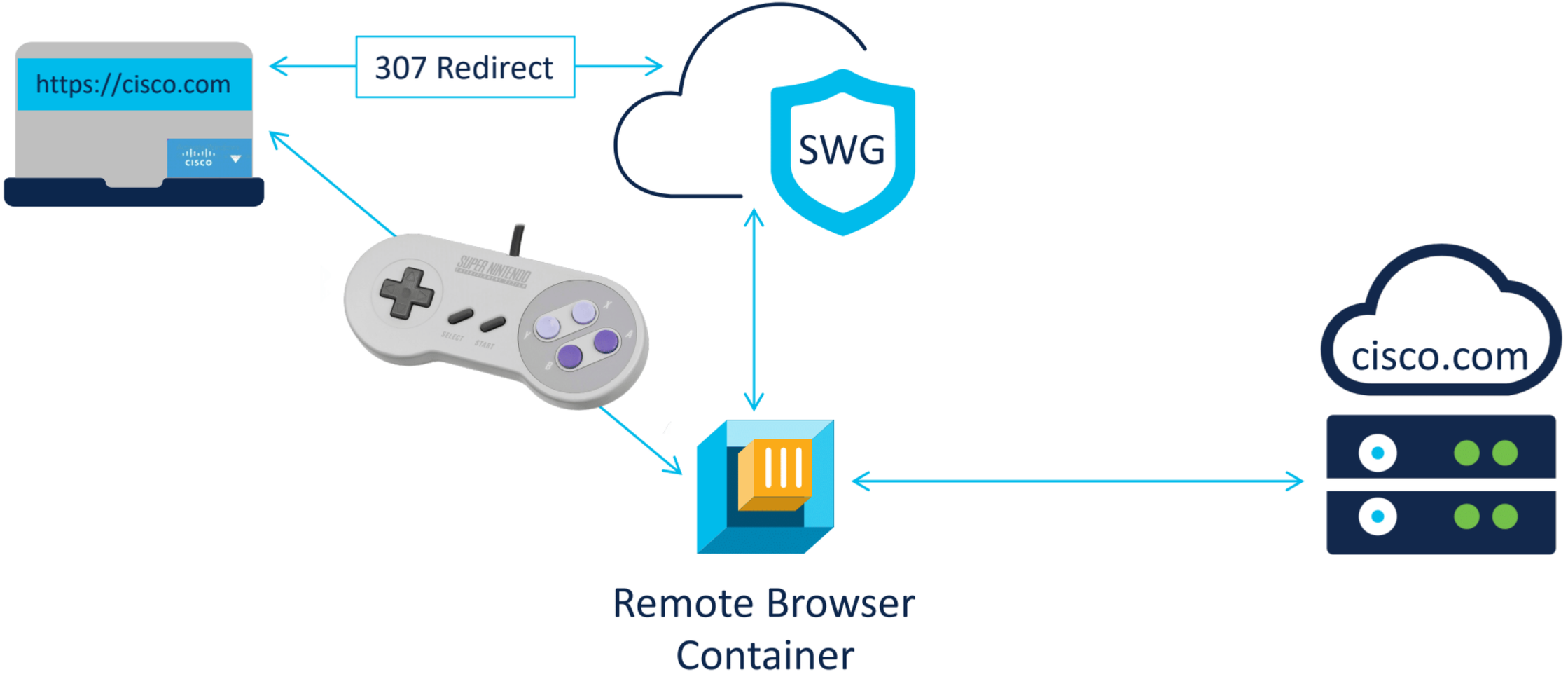
Use Umbrella DNS
208.67.222.222
208.67.220.220

Remote Browser Container

Use Umbrella DNS
208.67.222.222
208.67.220.220

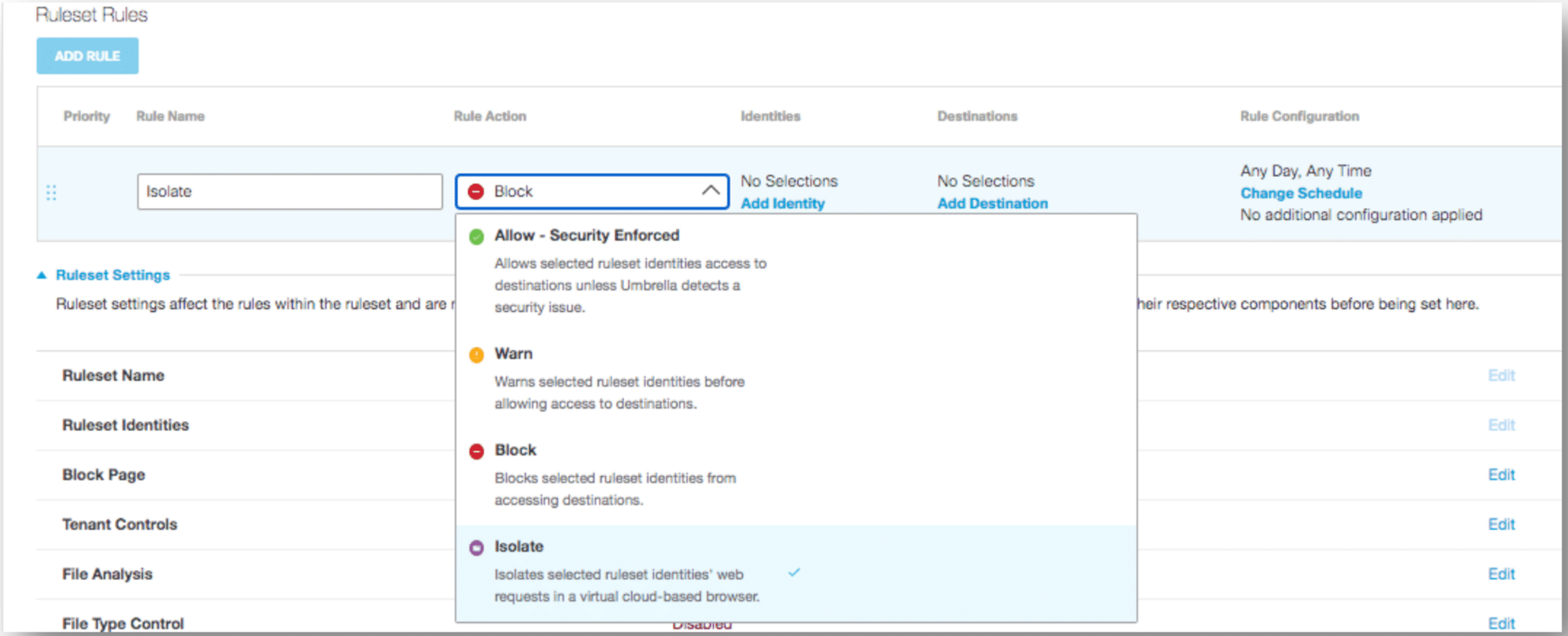


Use Umbrella DNS
208.67.222.222
208.67.220.220



Use Umbrella DNS
208.67.222.222
208.67.220.220

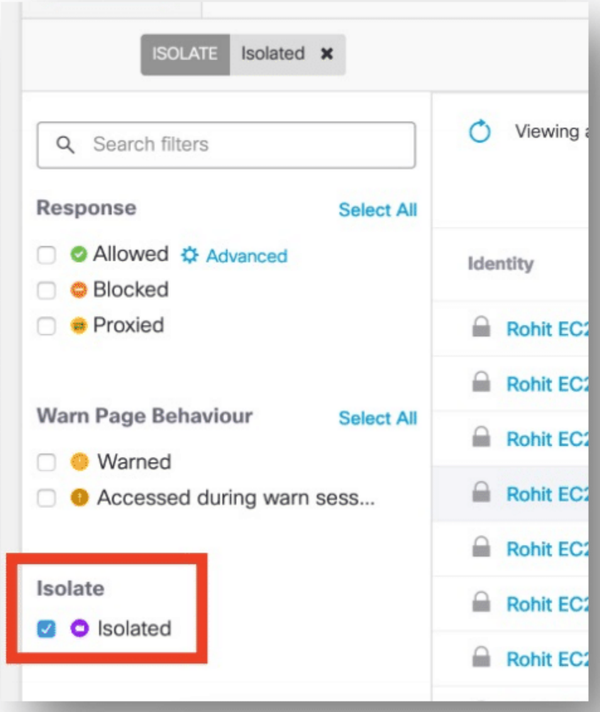
Browser Isolation

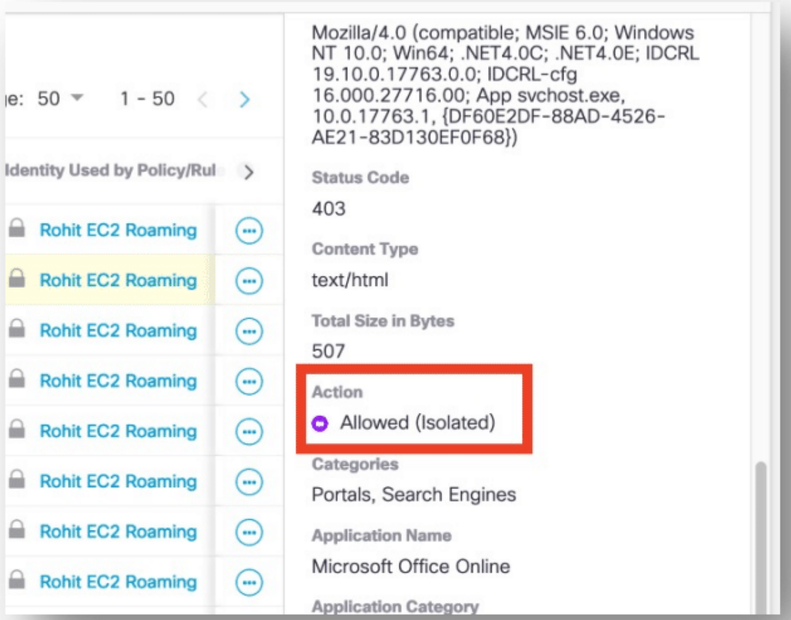


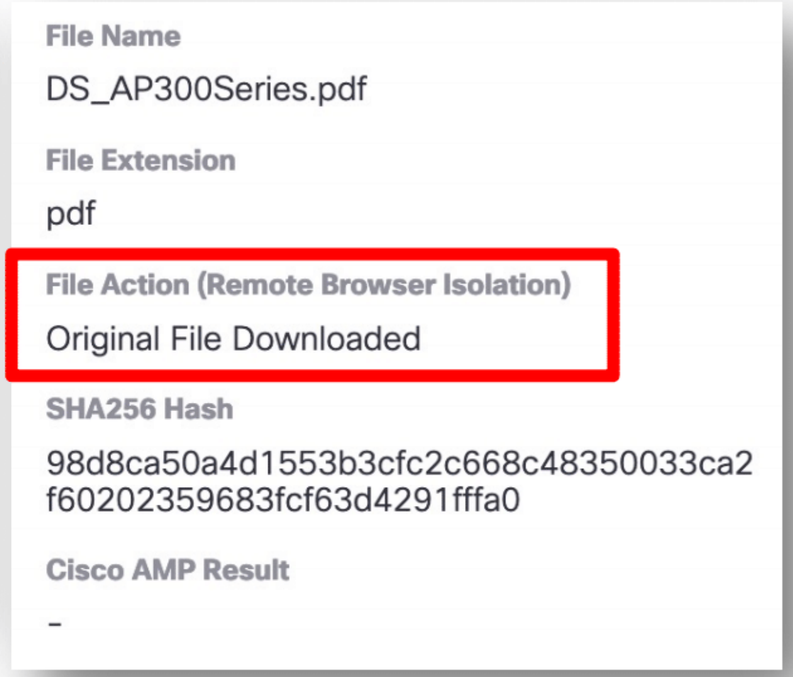
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Umbrella DNS
208.67.222.222
208.67.220.220

RBI Reporting





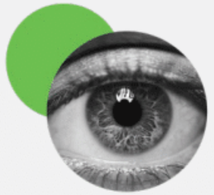


Identity	Destination	Action	Identity Used by Policy/Rule	Internal IP	External IP	Categories
Rohit EC2 Roaming	https://us-west-1-02760011-inspect.rbi-umbrella.com/safeview-auth-server/c...	Allowed	Rohit EC2 Roaming	172.31.13.61	34.208.29.202	Uncategorized
Rohit EC2 Roaming	https://www.facebook.com/pages/create/	Allowed (Isolated)	Rohit EC2 Roaming	172.31.13.61	34.208.29.202	Social Networ
Rohit EC2 Roaming	https://www.facebook.com/	Allowed (Isolated)	Rohit EC2 Roaming	172.31.13.61	34.208.29.202	Social Networ
Rohit EC2 Roaming	https://us-west-1-02760011-inspect.rbi-umbrella.com/safeview-auth-server/c...	Allowed	Rohit EC2 Roaming	172.31.13.61	34.208.29.202	Uncategorized

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Umbrella DNS
208.67.222.222
208.67.220.220

Порівняйте опції RBI



Ізолювати ризиковані

- Security Categories: Malware, Command and Control Callbacks, Phishing Attacks, Potentially Harmful
- Content Categories: Uncategorized

Ізолювання веб-додатків

- Content Categories: Chat, File Storage, File Transfer Services, Instant Messaging, Organizational Email Professional Networking, Social Networking, Webmail
- Applications: Various from Cloud Storage, Collaboration, Office Productivity, and Social Media categories

Ізолювання будь-яких

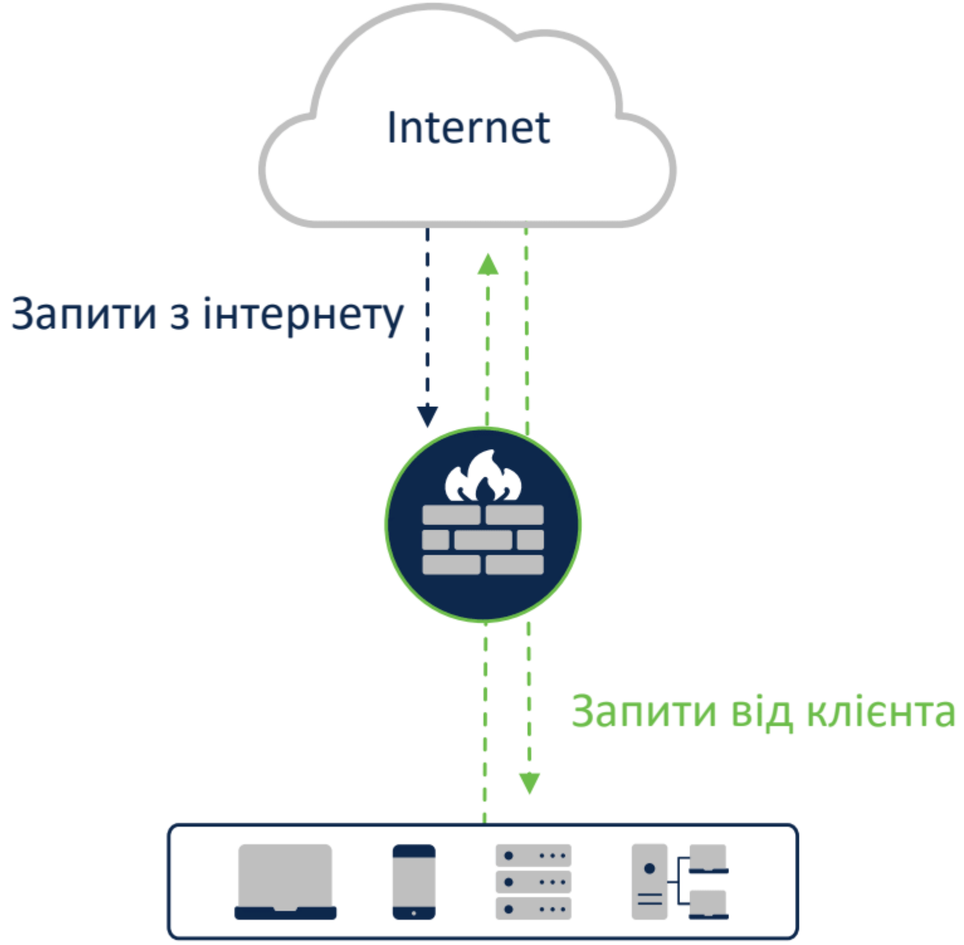
- Any security categories, content categories, applications, and destination lists can be isolated

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Хмарний міжмережевий екран

Use Umbrella DNS
208.67.222.222
208.67.220.220

Umbrella firewall захищає запити, які ініціює клієнт



Firewall обробляє запити, що ініційовані внутрішнім користувачем і які необхідні для захисту доступу до інтегратора і контролю використання хмарних додатків

Policies / Management

Firewall Policy

Add

Use this policy to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. For more information about Firewall Policy, view Manage Firewall.

FILTERS

Search Firewall Rule names or descriptions

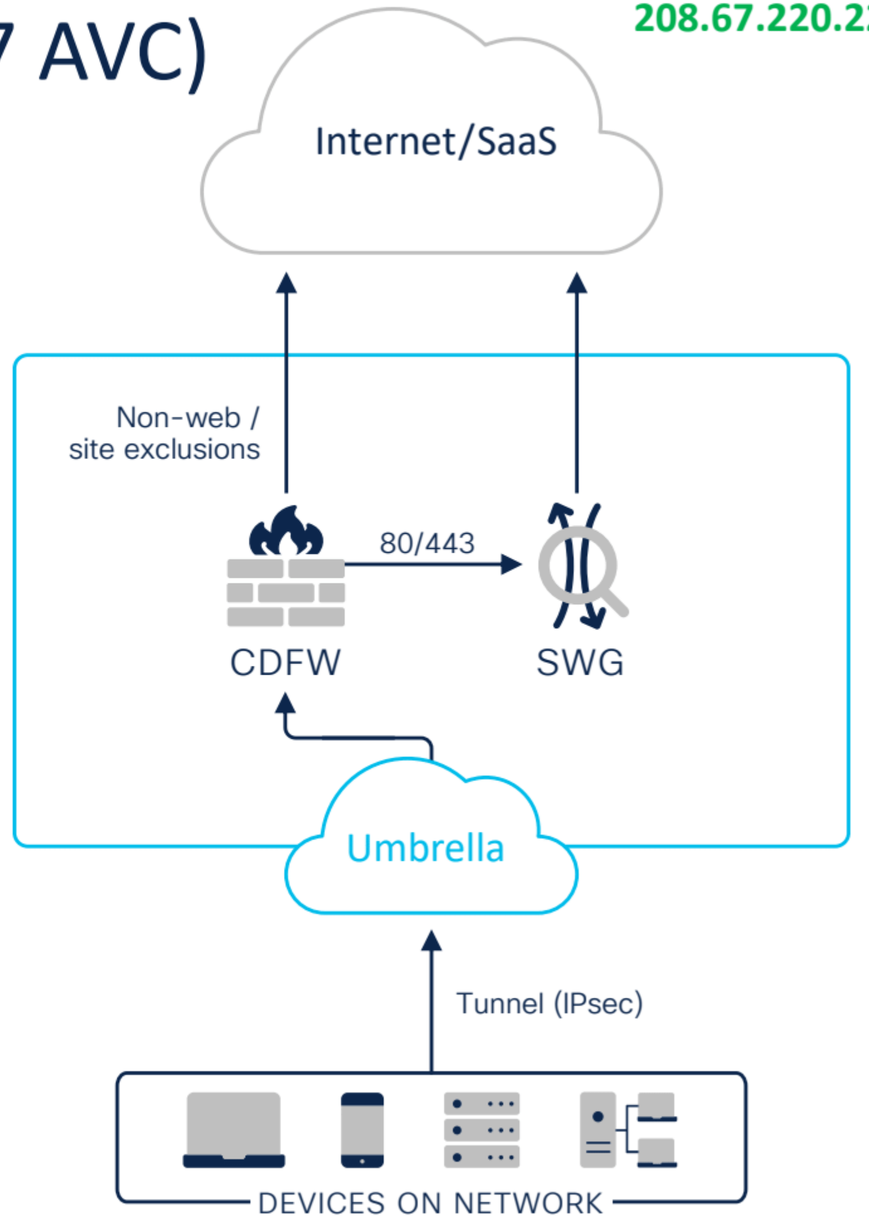
3 Total

Priority	Name	Status	Action	Applications	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit
1	Block SSH	Enabled	Block	ssh	Any	Any IPs Any Ports	Any IPs 1 Port	▲ 0/24hrs	▲ No Hits
2	p2p rule	Enabled	Block	Any P2P ftp	Any	Any IPs Any Ports	Any IPs Any Ports	25.0 /24hrs	Aug 24, 2020 - 09:33am
3	Default Rule	Enabled	Allow	Any Application	Any	Any IPs Any Ports	Any IPs Any Ports	69.1 k/24hrs	Aug 24, 2020 - 03:15pm

Use Umbrella DNS
208.67.222.222
208.67.220.220

Видимість і контроль додатків (Layer 7 AVC)

- Тунелювання всього трафіку на Umbrella IT
- Блокування ризикованих додатків і протоколів (видимість і контроль додатків 7-го рівня)
- Централізоване управління IP, портами, протоколами і додатками (рівень 3, 4 і 7)
- Перенаправлення веб-трафіку (порти 80/443) для захисту веб-шлюзу
- Вимагає використання IPsec тунелів



Use Umbrella DNS
208.67.222.222
208.67.220.220

Application visibility and control

Розширення для всіх точкок застосування

Захист рівня DNS

- Видимість хмарних додатків у вашій організації
- Визначте потенційний ризик і заблокуйте конкретні програми (виявлення 16 000 додатків)

Хмарний firewall

- Layer 7 Application Visibility and Control
- Розширює видимість, захист і контроль на:
  - Не-веб (не-HTTP/S) трафік
  - Додатки, які використовують зареєстровані IP-адреси і не роблять DNS-запити
  - Програми, у яких для виявлення потрібне виявлення підпису

Secure web gateway

Детальний контроль веб-додатків через HTTP/S (порти 80/443):

- Блокування передавання в хмарні програми
- Блокування публікацій в соцмережах
- Блокування атачів для webmail
- Обмеження використання (Tenant)

Use Umbrella DNS
208.67.222.222
208.67.220.220

Основні варіанти використання

Layer 7 application visibility and control

Блокування Shadow IT

Приклад: Припиніть використання неавторизованих SaaS-програм

- WebEx дозволений
- MS Teams відео заборонено
- Google meets заборонений

Блокування незахищених додатків на нестандартних портах

Приклад: Зупинка віддаленого віртуального терміналу в інших мережах

- Наприклад, нестандартний порт telnet 8080

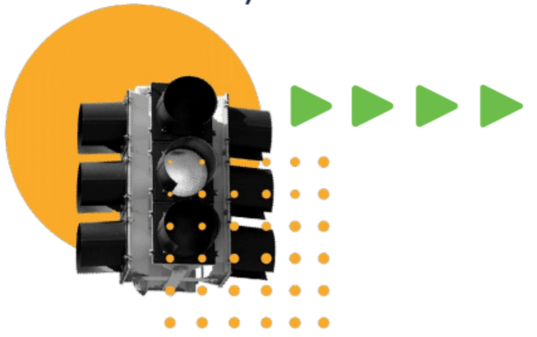
Приклад: зупинка передавання файлів

- Такі як FTP через нестандартний порт 1003

Блокувати несанкціонований трафік через нестандартний порт

Приклад: Припиніть використовувати заборонений трафік

- Блокування всього peer-to-peer трафіку (наприклад, TOR або BitTorrent)



Use Umbrella DNS
208.67.222.222
208.67.220.220

Система запобігання вторгнень Umbrella (IPS)

Доступно з липня 2021 року

Можливості

- Посилює захист Umbrella Firewall для трафіку клієнтів
- Використовує сигнатурний аналіз (Snort 3) для аналізу мережевих потоків і захисту від експлуатації вразливостей
- Додає рівень захисту від шкідливих програм, ботнетів, фішингу тощо.
- Використовує 40K+ правил Cisco Talos для виявлення та співвіднесення загроз у режимі реального часу

Результати

- ✔ Просте управління з єдиного інтерфейсу Umbrella
- ✔ Видаліть обмеження продуктивності готельних пристроїв, використовуючи масштабовану хмарну ємність
- ✔ Зупиніть більше загроз за допомогою найефективнішої системи інформування про загрози
- ✔ Виявлення та блокування використання вразливостей

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public
69

Use Umbrella DNS
208.67.222.222
208.67.220.220

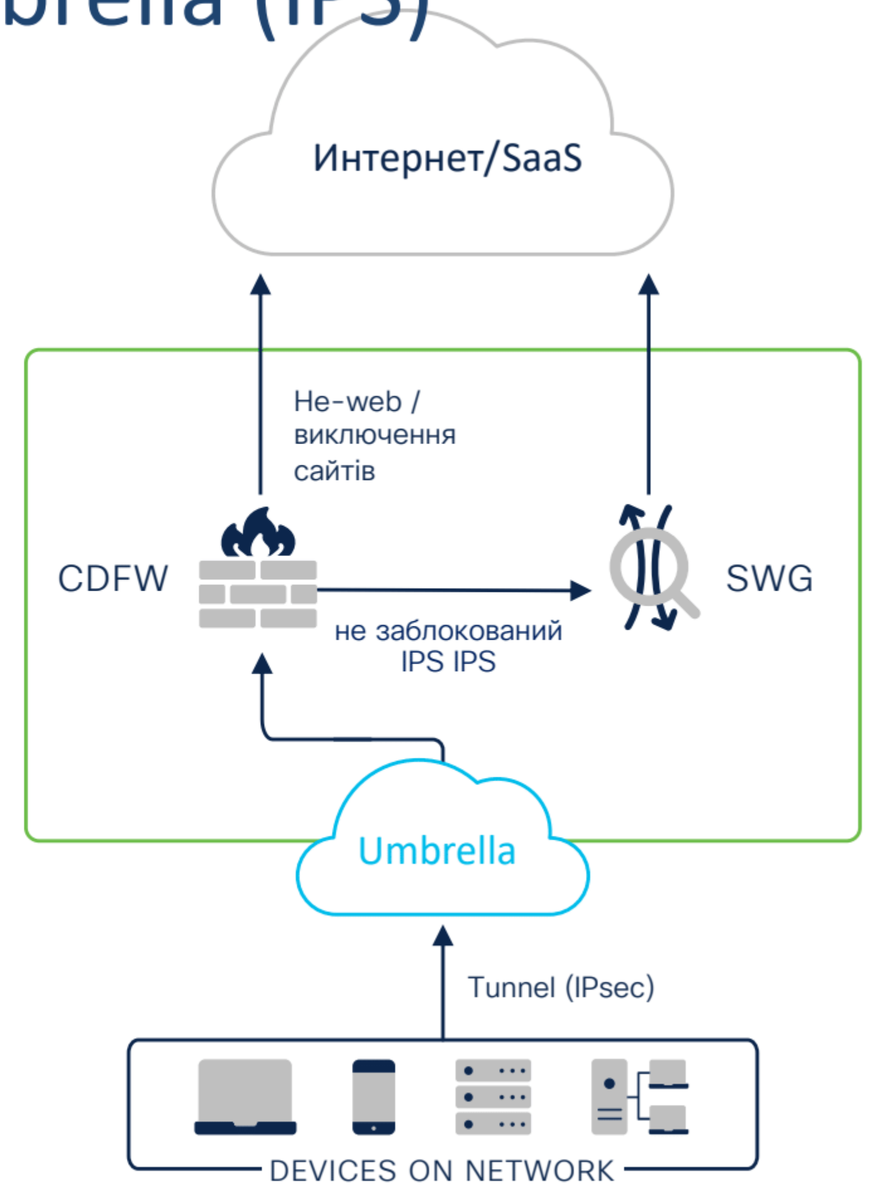
Система запобігання вторгнень Umbrella (IPS)

Рівні безпеки для кращого захисту

IPS з сігнатурним аналізом

Layer 7 обізнаність і контроль додатків

Layer 3 / 4 МСЭ : правила по IP, порту, протоколу



Ключові переваги Umbrella IPS

Use Umbrella DNS
208.67.222.222
208.67.220.220

Простота

Правила IPS можуть бути складними

- Єдиний уніфікований дашборд для управління
- Прості глобальні правила з налаштуванням за лічені секунди
- Унікальні метадані Cisco допоможуть вам легко налаштовувати правила та керувати ними

Продуктивність

Безпека за стабільною ціною

- IPS може погіршити продуктивність локального брандмауера
- Хмарна IPS забезпечує гарантовану продуктивність без шкоди для безпеки

Ефективність

Мінливий ландшафт загроз

- Інформація про загрози від Cisco Talos (Правила 40K+)
- Легко отримайте новітні технології Snort 3 для більшої ефективності
- Автоматичне отримання оновлень Snort 3
-

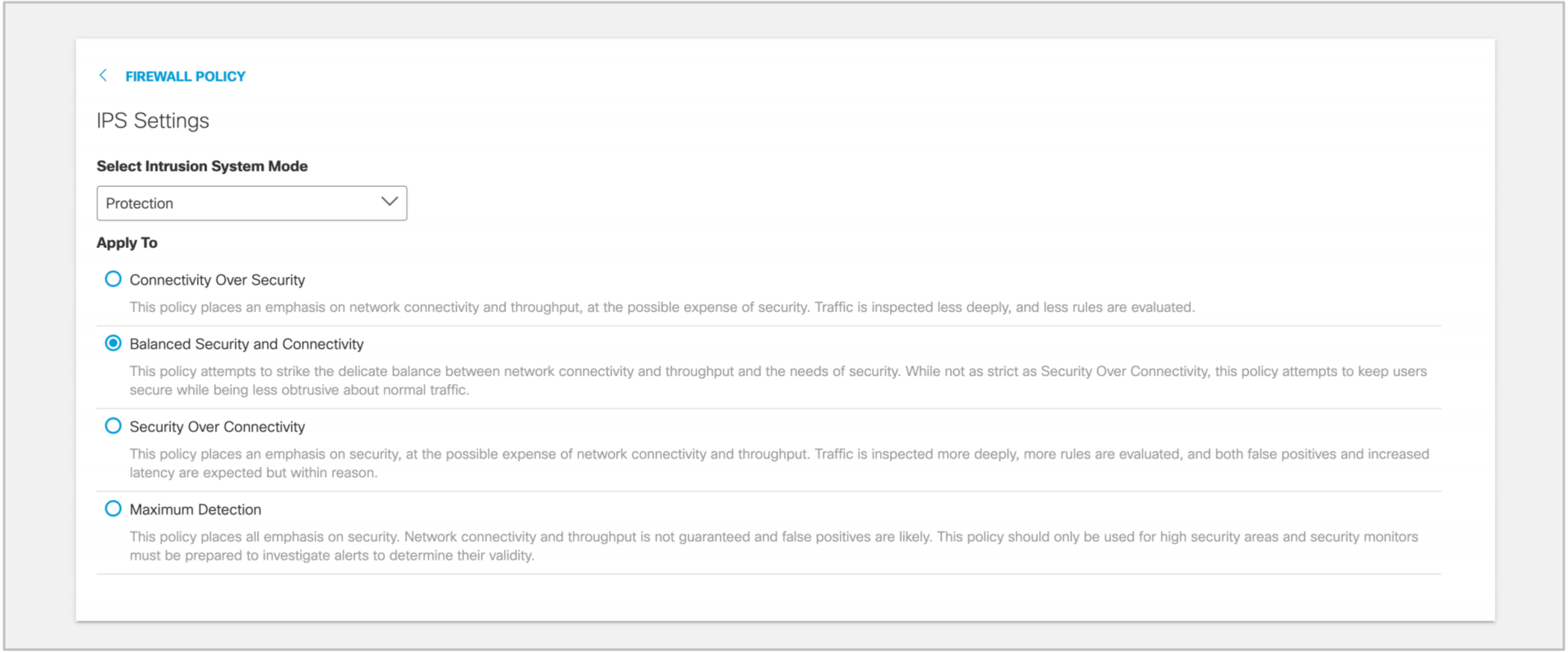
Надійність

Відмовостійка конструкція

- Глобальна присутність центру обробки даних
- Висока доступність з Anycast для автоматизації відновлення та краща доступність

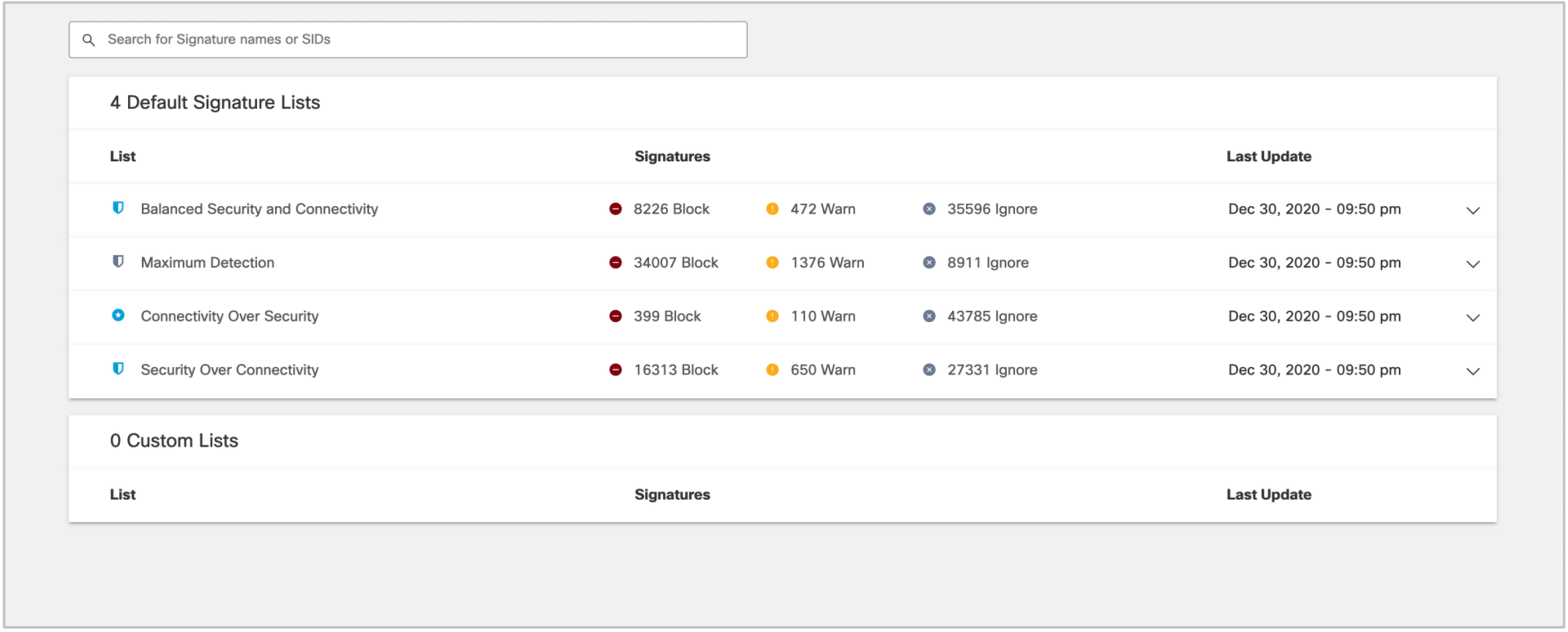
Use Umbrella DNS
208.67.222.222
208.67.220.220

Політика Firewall



Use Umbrella DNS
208.67.222.222
208.67.220.220

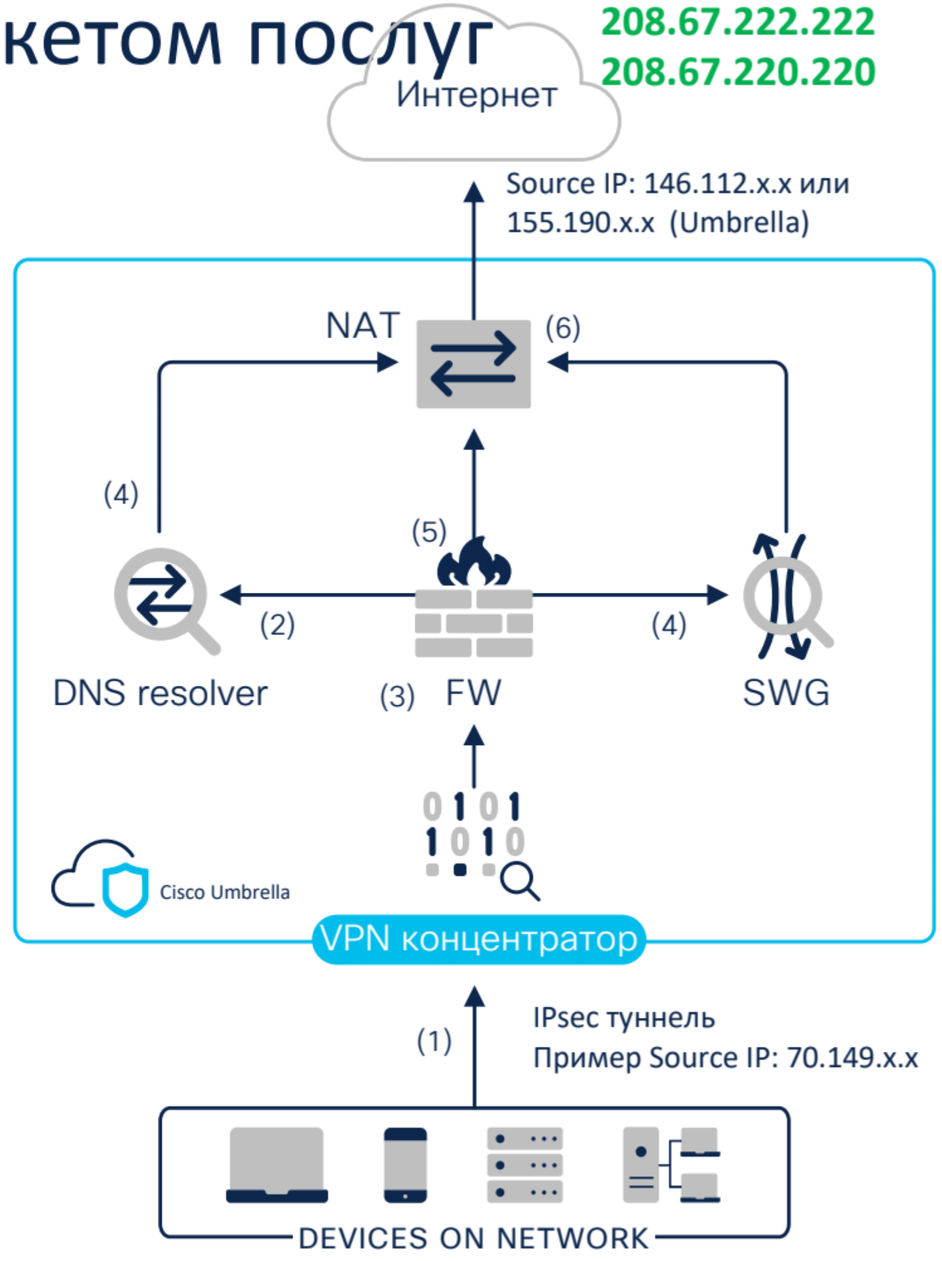
Списки правил Snort IPS



Як ваша програма працює з повним пакетом послуг

Правила DNS, SWG і CDFW

1. Надсилайте трафік всередині тунелю IPSec у хмару
2. Резолвінг імен в Umbrella DNS безпека відповідно до політики. Трафік реєструється.
3. Трафік перевіряється в CDFW (рівні 3, 4, AVC і IPS). Веб, який не заблокований у CDFW, надсилається до SWG (4). Весь інший трафік перевіряється firewall (крок 5). Трафік реєструється.
4. SWG перевіряє відповідно до політики. Трафік реєструється.
5. «Дозволений» трафік проходить через NAT



Функціональність CASB

Use Umbrella DNS
208.67.222.222
208.67.220.220

Основні типи багаторежимного CASB

In-band/proxy

- Високий вплив на розгортання
- Агент або перенаправлення трафіку
- Немає API для захисту програм
- Обмежена ретроспектива
- Правила роботи в режимі реального часу
- Схід-захід або хмара в хмару
- Усі програми

Out-of-band/API

- Низький вплив
- Без агентів
- Покладається на API хмарних додатків
- Ретроспективний
- Правила «майже» реального часу
- Універсальне покриття
- Авторизовані програми

Use Umbrella DNS
208.67.222.222
208.67.220.220

Типи CASB (продовження)

In-band/proxy

Umbrella

- Видимість і блокування додатків
- Контроль додатків
  - Блокування вивантаження файлів (Dropbox/Box)
  - Блокування приєднань файлів (webmail)
- Контроль Tenants
- In-band DLP

Out-of-band/API

Umbrella

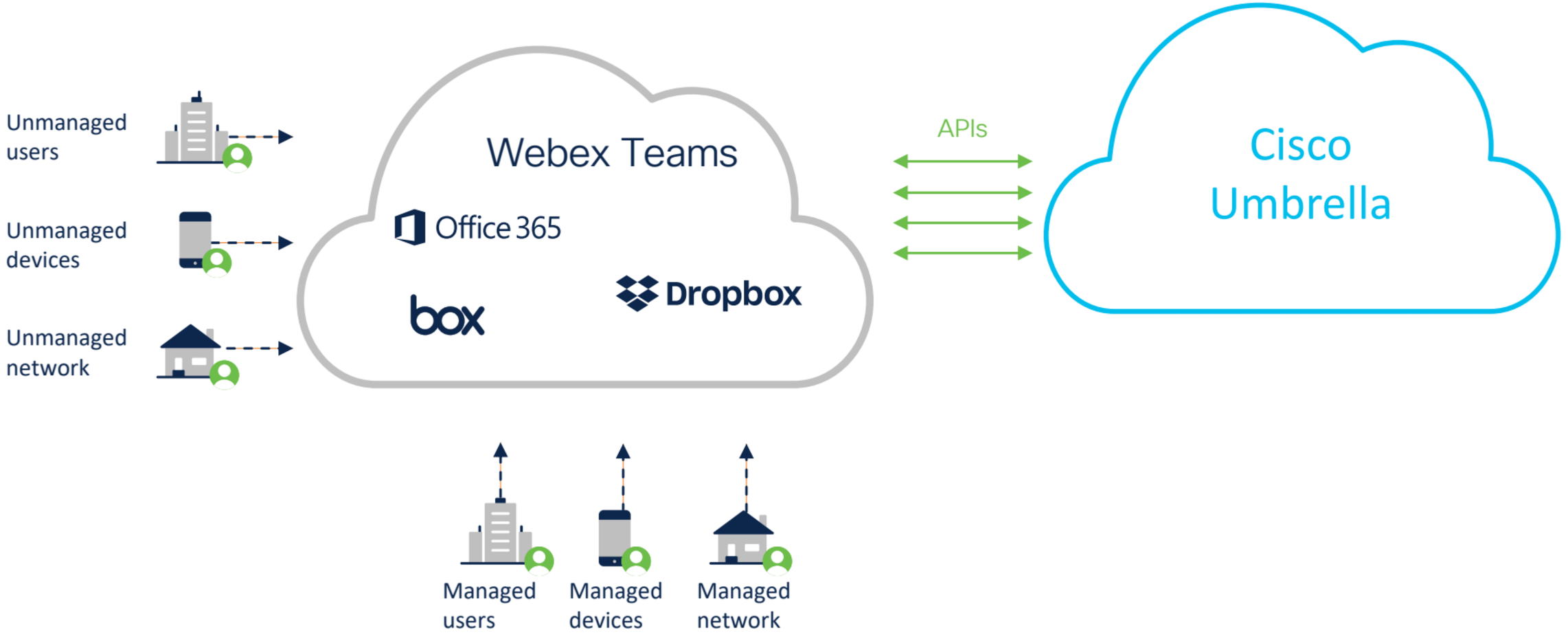
- Виявлення malware в хмарних сховищах

Cloudlock

- Моніторинг/запобігання поведінці користувачів
- Політики хмарного сховища
- Карантин та відкликання DLP (out-of-band)
- App OAuth: видимість і контроль
-

Use Umbrella DNS
208.67.222.222
208.67.220.220

Сканування шкідливих програм працює з api, міжхмарне

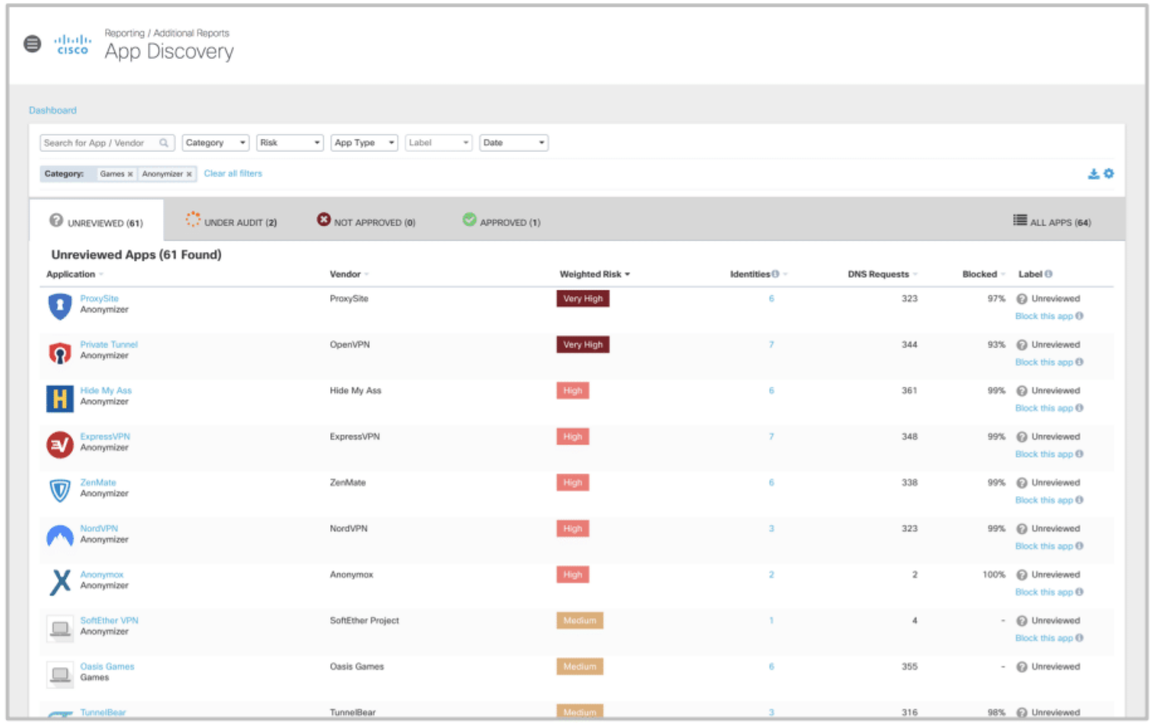


Use Umbrella DNS
208.67.222.222
208.67.220.220

Виявлення та керування додатками

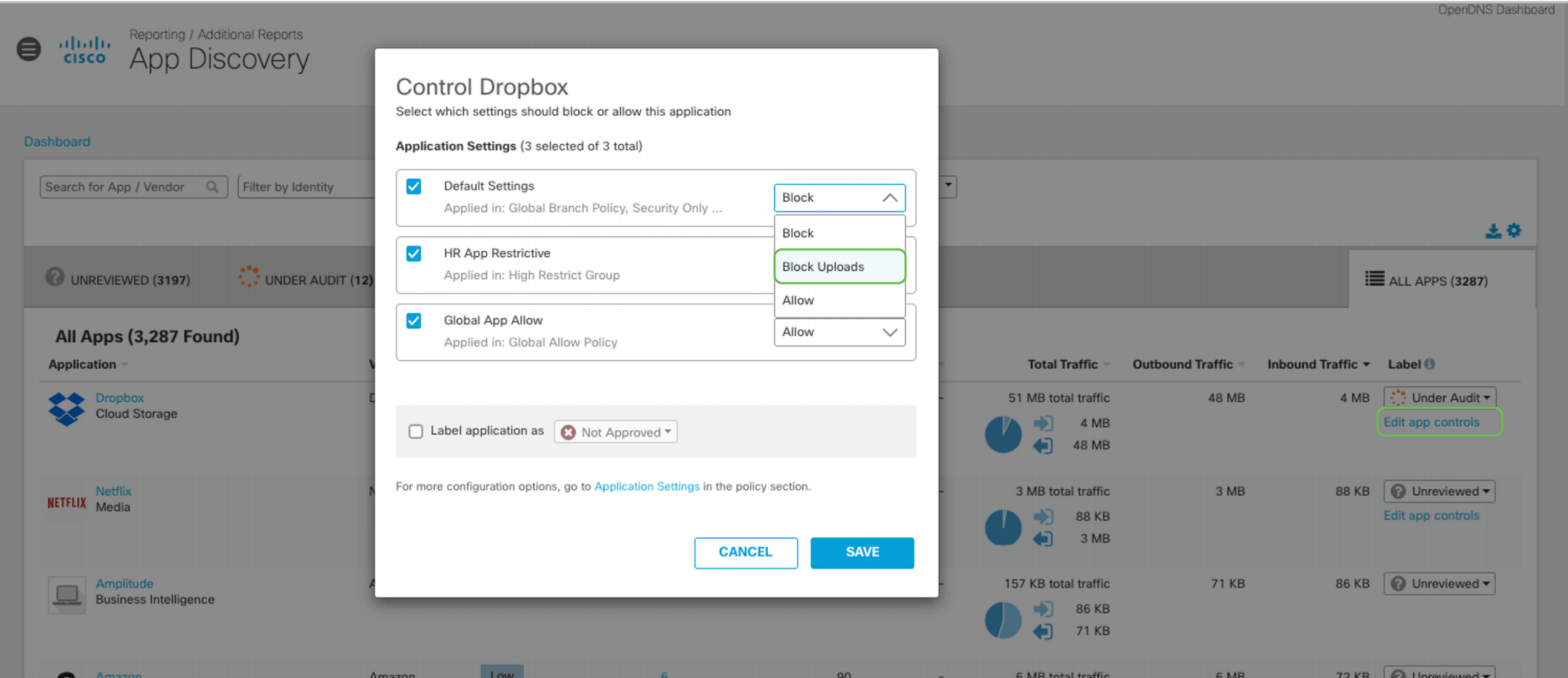
Видимість «тіньової» IT та керування хмарними додатками

- Повний список використовуваних хмарних додатків
- Звіти про категорії та ризики
- Кількість користувачів та обсяг трафіку
- Блокування за категоріями або програмами



Use Umbrella DNS
208.67.222.222
208.67.220.220

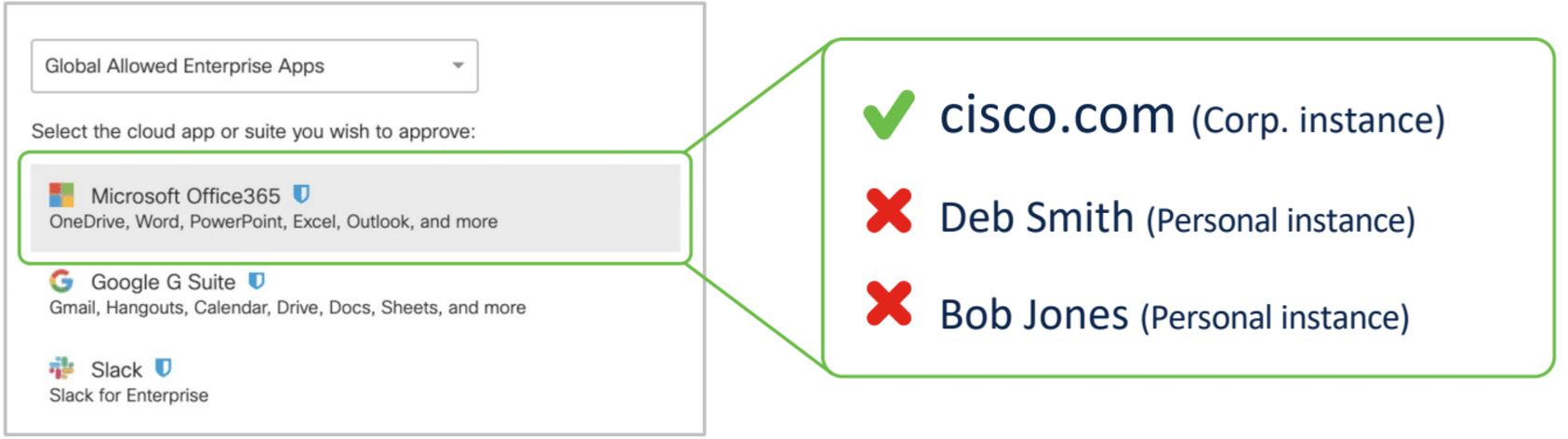
Детальний контроль додатків



Use Umbrella DNS
208.67.222.222
208.67.220.220

Контроль доступу до Tenants

Вибір об'єкта ключових SaaS-додатків, які можуть використовуватися користувачами або групами



Основні сфери застосування

Безпека
Забезпечення того, що конфіденційні дані можуть створюватися та зберігатися лише в дозволених об'єктах

Продуктивності
Надання доступу лише до параметрів корпоративних програм saaS

Use Umbrella DNS
208.67.222.222
208.67.220.220

Inline DLP

Хмарний проксі DLP

Використовує SWG для підключення, маршрутизації та дешифрування SSL

Класифікація DLP

80+ вбудованих класифікаторів

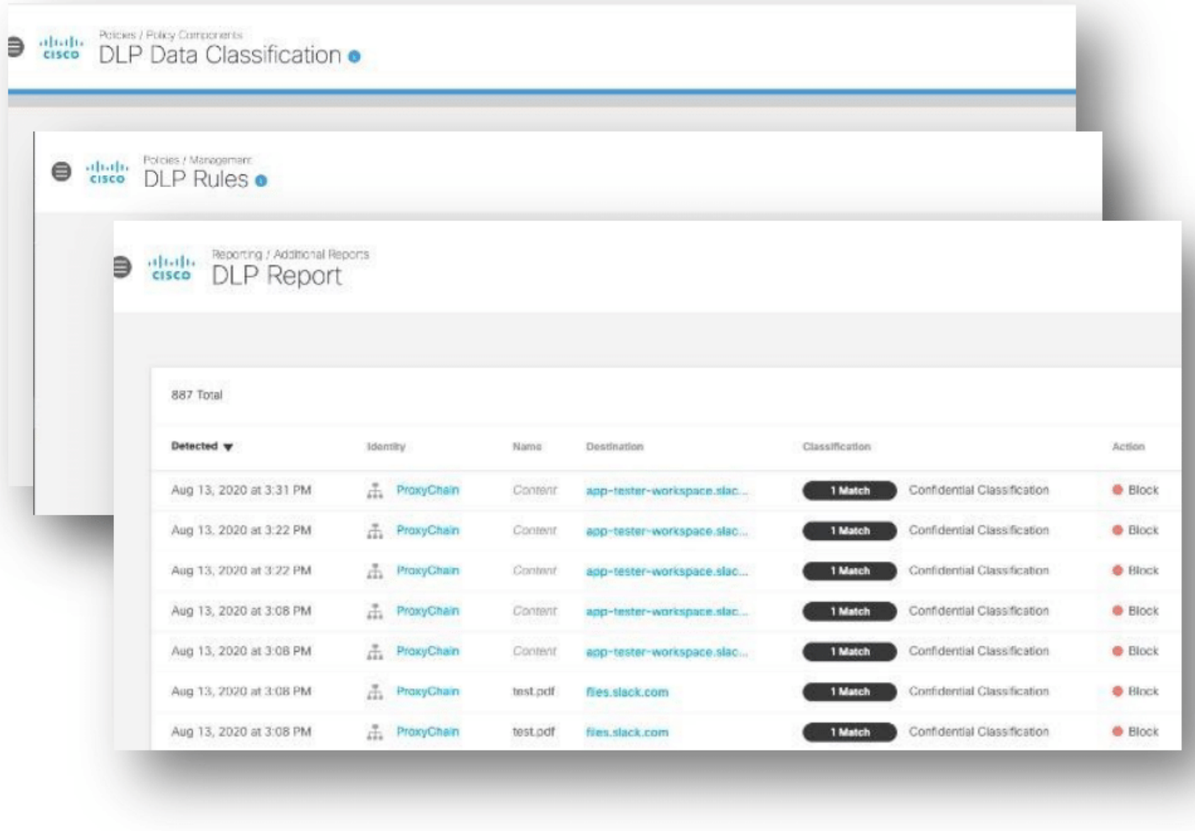
Настроювання та додавання власного

Гнучка політика DLP

Можливість застосовувати специфічні класифікатори до конкретних користувачів

Вбудована звітність

Включає користувача, ім'я файлу, класифікацію, шаблон збігу, винятки тощо.



Currently LA. GA target July 2021

Use Umbrella DNS
208.67.222.222
208.67.220.220

Data-at-rest, виявлення malware (API-based)

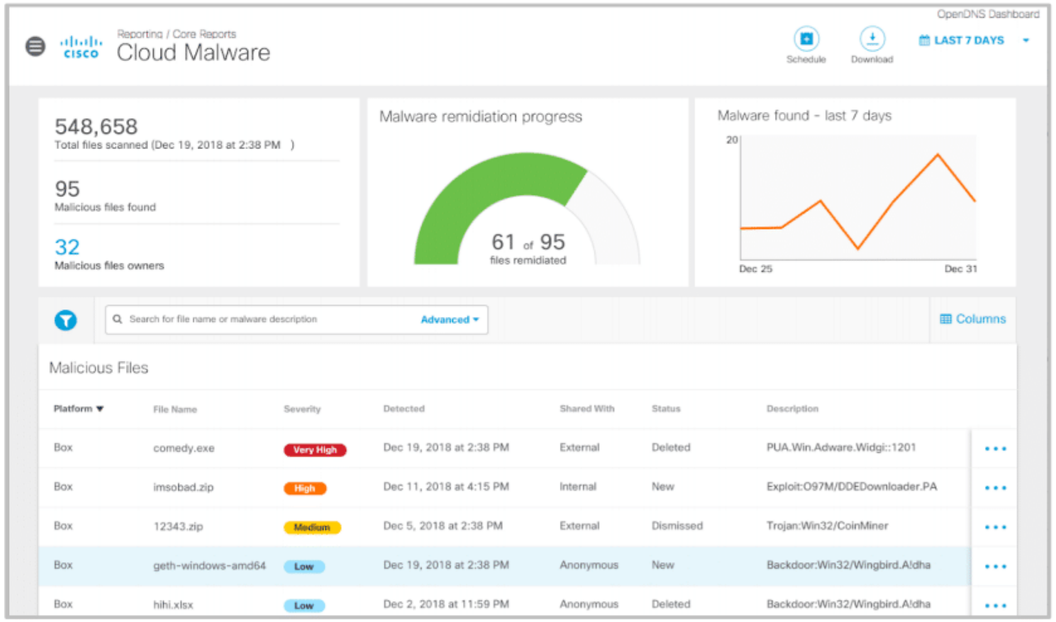
Файли, які містять malware в хмарних сховищах, можуть завдати значної шкоди

Malware входить/виходить через:

- Вузли, на яких не встановлений Cisco Secure Endpoint (AMP)
- Некеровані пристрої
- Зовнішні пристрох

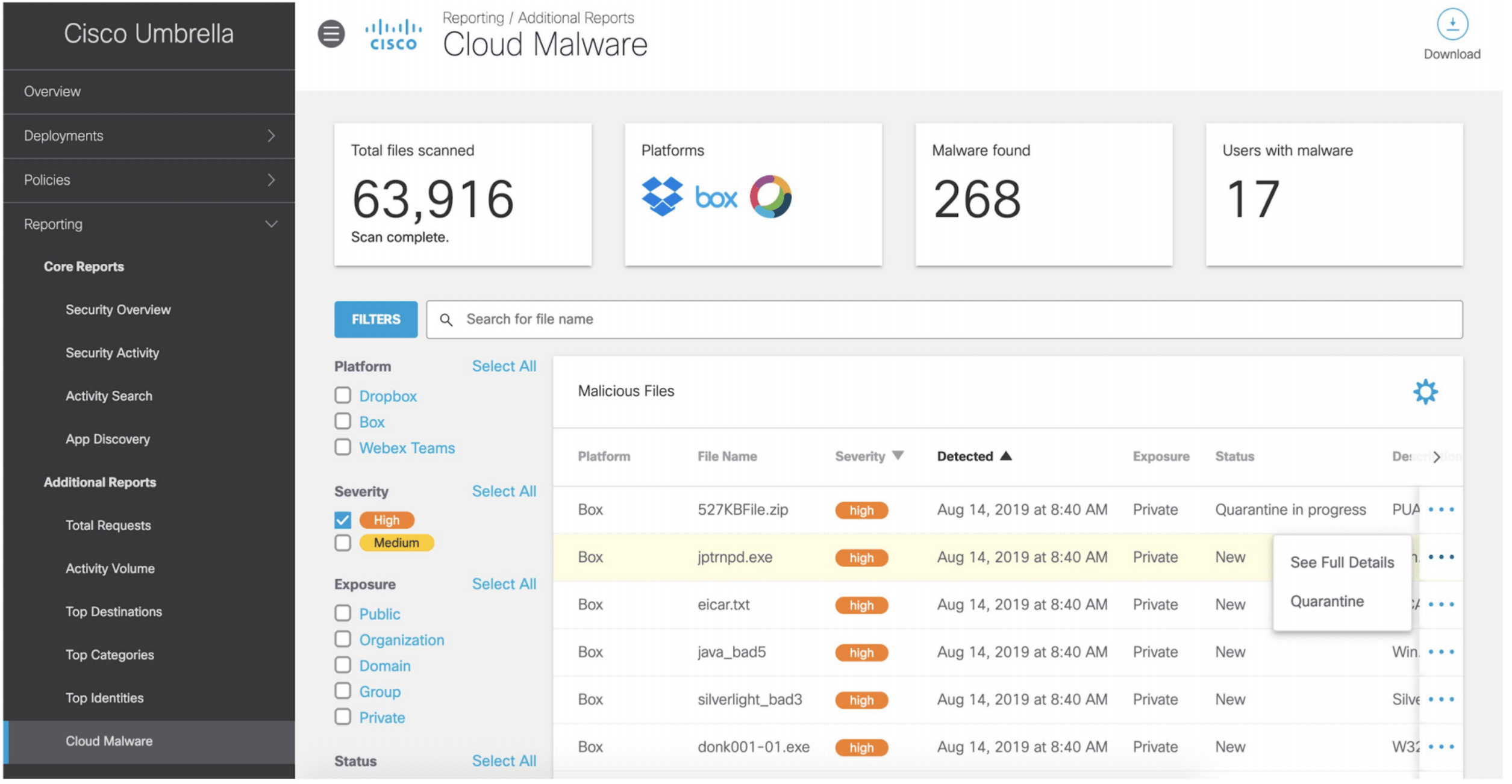
Рішення:

- Сканування репозиторіїв і перевірка файлів



Запобігання поширенню malwari між сайтами та користувачами

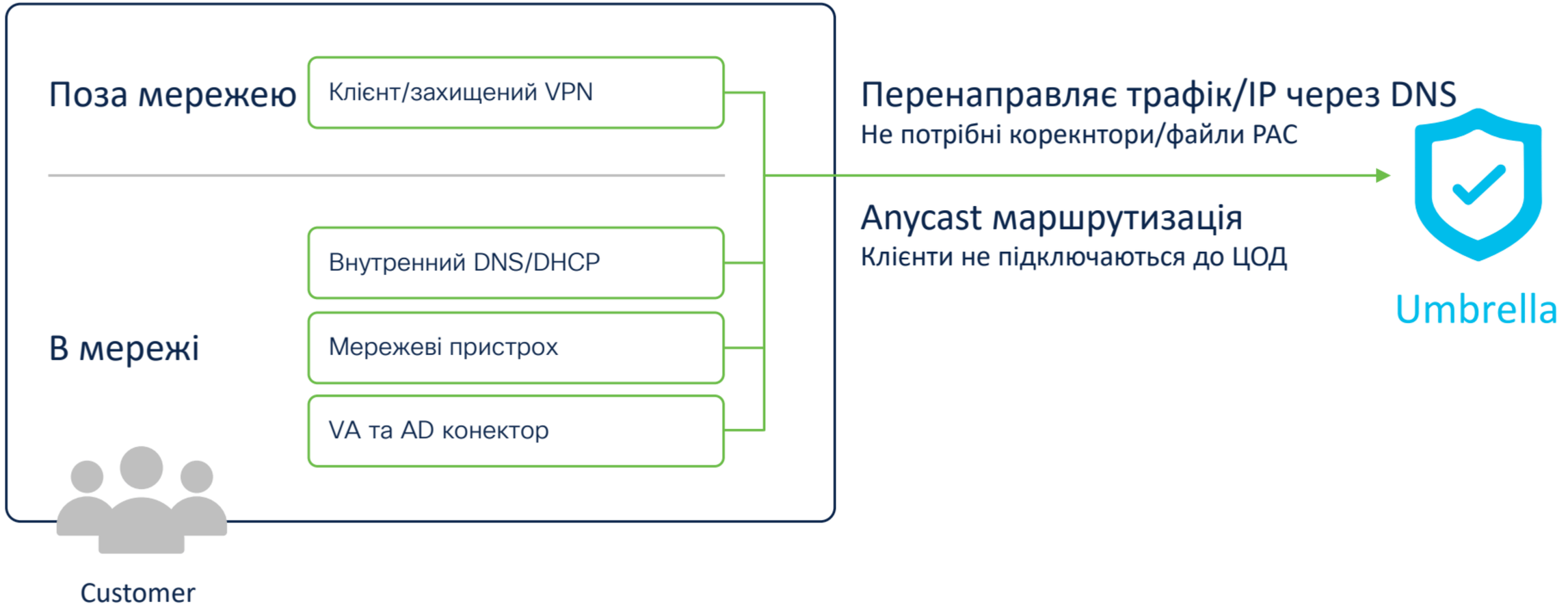
Two apps included in SIG Essentials
All available apps included in SIG Advantage


Cisco Umbrella
Overview
Deployments
Policies
Reporting
Core Reports
Security Overview
Security Activity
Activity Search
App Discovery
Additional Reports
Total Requests
Activity Volume
Top Destinations
Top Categories
Top Identities
Cloud Malware
Reporting / Additional Reports
Cloud Malware
Download
Total files scanned
63,916
Scan complete.
Platforms
box
Malware found
268
Users with malware
17
FILTERS
Search for file name
Platform
Select All
Dropbox
Box
Webex Teams
Severity
Select All
High
Medium
Exposure
Select All
Public
Organization
Domain
Group
Private
Status
Select All
Malicious Files
Platform
File Name
Severity
Detected
Exposure
Status
Box 527KBFile.zip high Aug 14, 2019 at 8:40 AM Private Quarantine in progress PUA
Box jptrnpd.exe high Aug 14, 2019 at 8:40 AM Private New
See Full Details
Quarantine
Box eicar.txt high Aug 14, 2019 at 8:40 AM Private New
Box java_bad5 high Aug 14, 2019 at 8:40 AM Private New Win
Box silverlight_bad3 high Aug 14, 2019 at 8:40 AM Private New Silve
Box donk001-01.exe high Aug 14, 2019 at 8:40 AM Private New W32

Підключення та інтеграція

Use Umbrella DNS
208.67.222.222
208.67.220.220

Підключення до Umbrella



Use Umbrella DNS
208.67.222.222
208.67.220.220

Розгортання по всій мережі за лічені хвилини

DNS/DHCP сервери, Wi-Fi APs

Проста зміна конфігурації для маршрутизації DNS

EXISTING

ISR1K / 4K

SD-WAN (Viptela)

WLC

Meraki MR

- Налаштувати політики для VLAN/SSID; додавання тегів для детальної фільтрації та звітування
- Вбудована інтеграція (Доступний віртуальний прилад для Umbrella)

НАСТРОЮВАННЯ МЕРЕЖІ

Secure VPN (AnyConnect) roaming module

iOS and Android apps

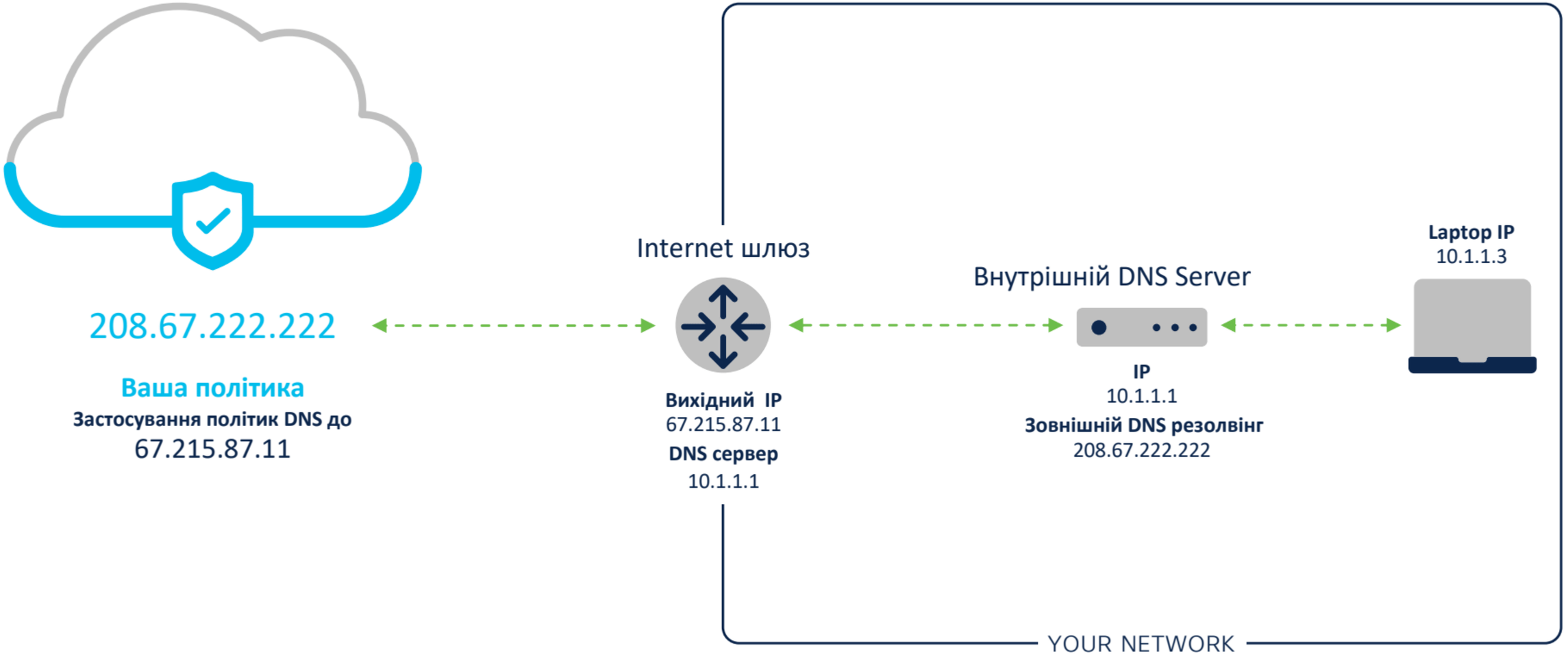
Umbrella Android client

Детальна фільтрація та звітування в мережі та поза нею

НАЛАШТУВАННЯ ENDPOINT

Use Umbrella DNS
208.67.222.222
208.67.220.220

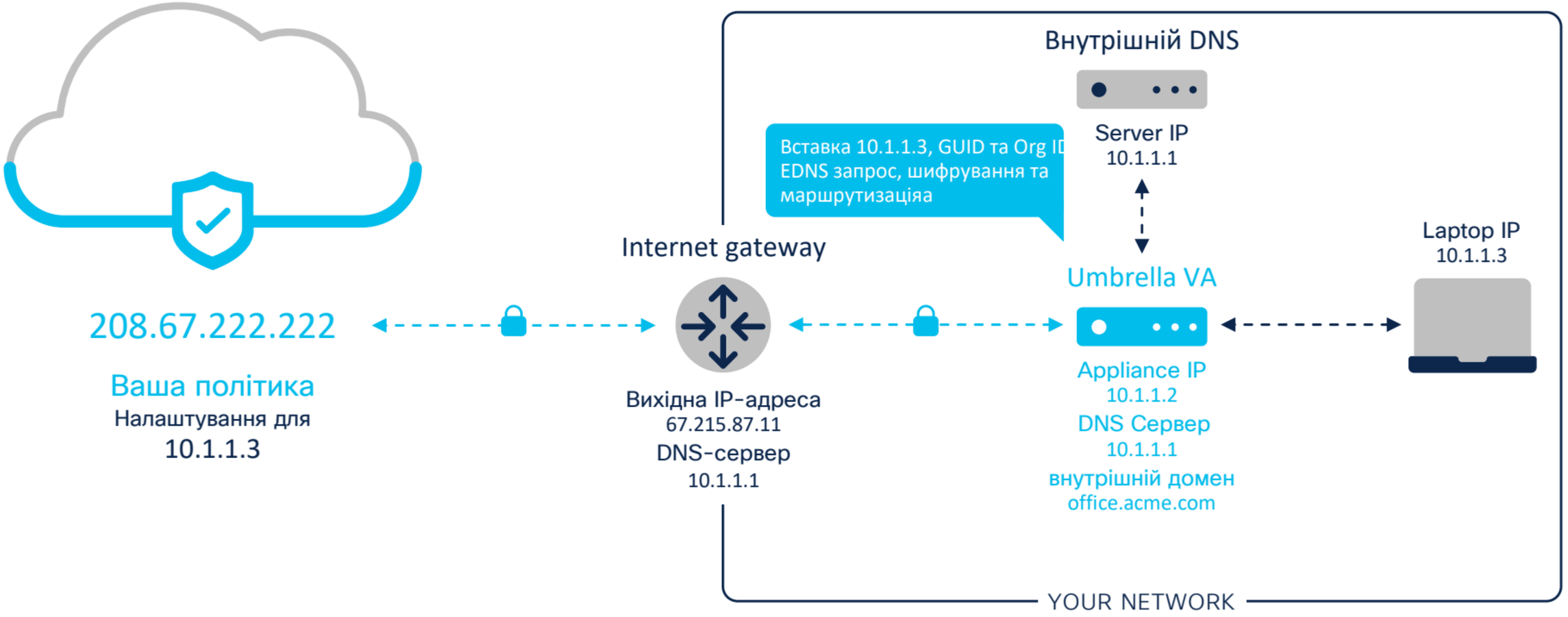
Захист мережі за допомогою DNS-сервера



Use Umbrella DNS
208.67.222.222
208.67.220.220

Внутрішній моніторинг мережі

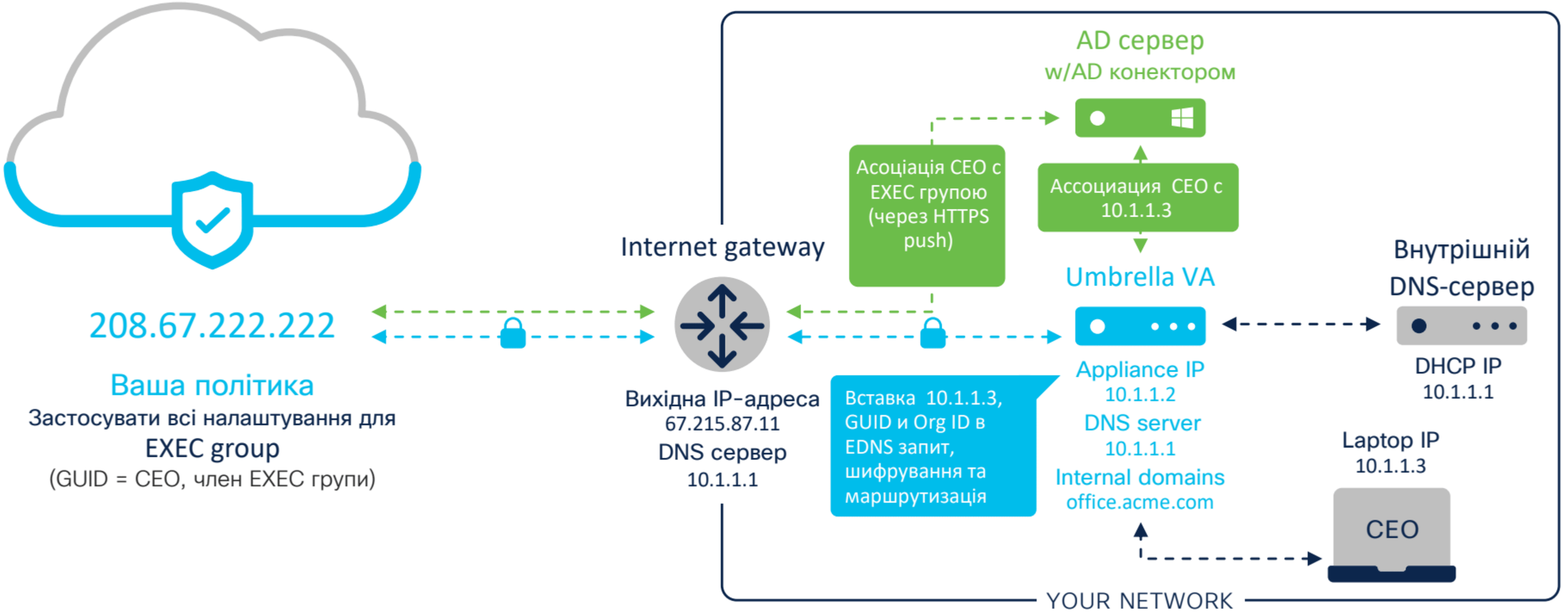
3 Umbrella virtual appliance



Use Umbrella DNS
208.67.222.222
208.67.220.220

Інтеграція з AD

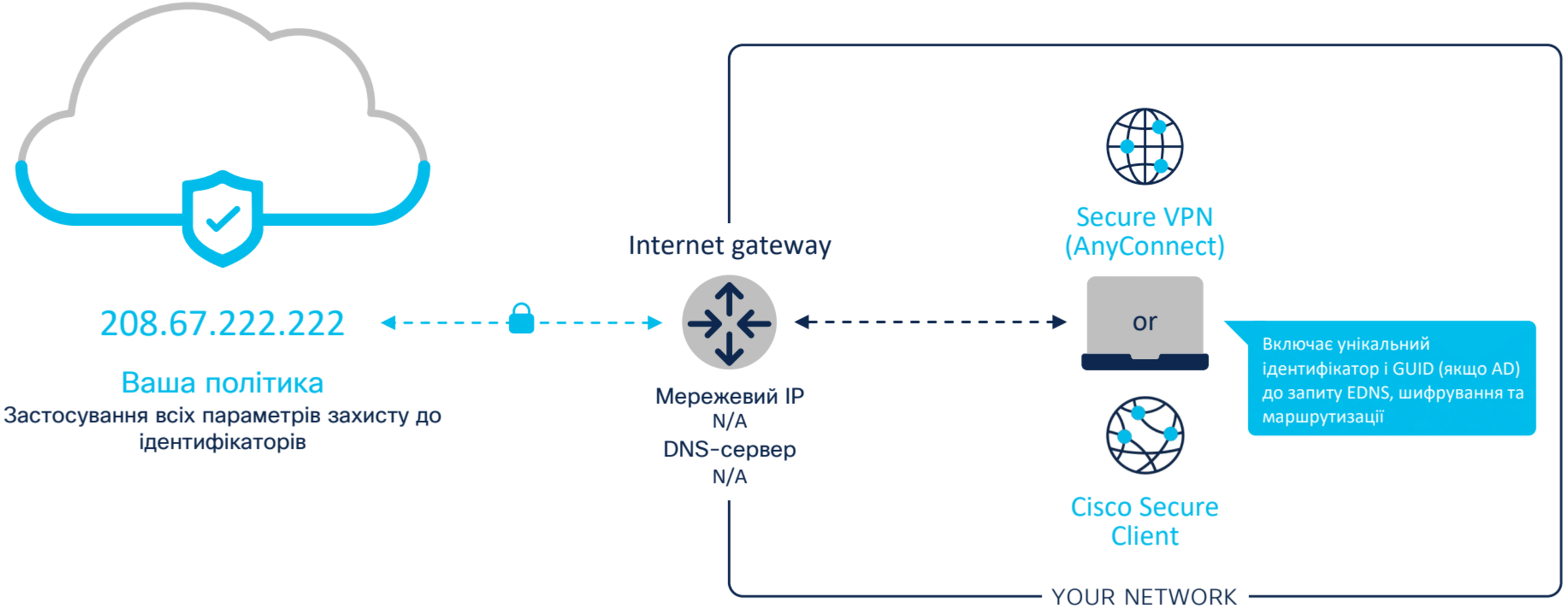
Через конектор та Umbrella virtual appliance



Use Umbrella DNS
208.67.222.222
208.67.220.220

Захист позамережевих Win/Macs

Через Cisco Secure Client



Use Umbrella DNS
208.67.222.222
208.67.220.220

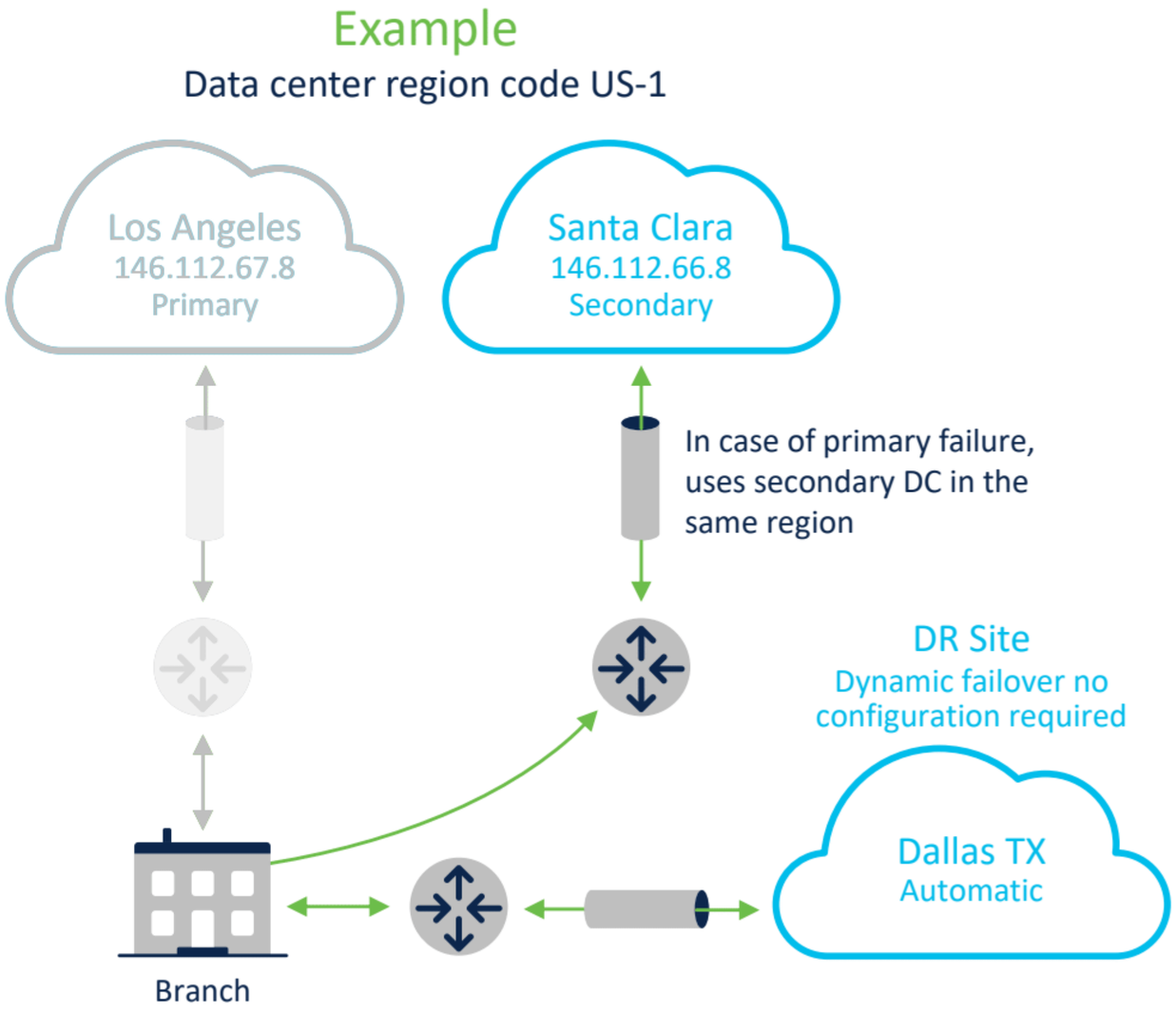
Тунелювання трафіку

Пропускна здатність IPsec

- 250 Mbps за замовчуванням, з можливим збільшенням
- Можна використовувати кілька тунелів

Спеціальні можливості

- Підтримка primary і secondary DC
- Failover на другий ЦОД за допомогою Anycast
- Виявлення помилок через IKE dead peer detection



SD-WAN

Безпечний SD-WAN

Гнучка архітектура Cisco для мереж на основі намірів

Будь-яке розгортання

Management & Analytics

On-premise | Cloud | Multi-tenant

Automation | Network Insights | Machine Learning | AI

Open | Programmable | Scalable

Будь-яка послуга

Multicloud Optimization

Multi-Layer Security

ThousandEyes Analytics

Voice

SaaS Optimization O365, Webex

Будь-який транспорт

Satellite

Internet

MPLS

5G/ LTE

SDCI*

Будь-яке місце

Branch

Colocation

AWS

Azure

Cloud

Remote Work

* Software Defined Cloud Interconnect

Вибір: Viptela або Meraki

Meraki Full Stack

Простий та інтуїтивно

зрозумілий

Швидке розгортання

Оптимізований за вартістю HW

Powered by

cisco Meraki

cisco

SD-WAN

Вимагає командної роботи

UTM

Сегментація

IPv6

Складна маршрутизація

Cloud On-Ramp

SASE ready

IBN Multidomain

Гнучкі дизайни

SRST/UC

FEC / Packet Duplication/DRE

SDCI

Powered by

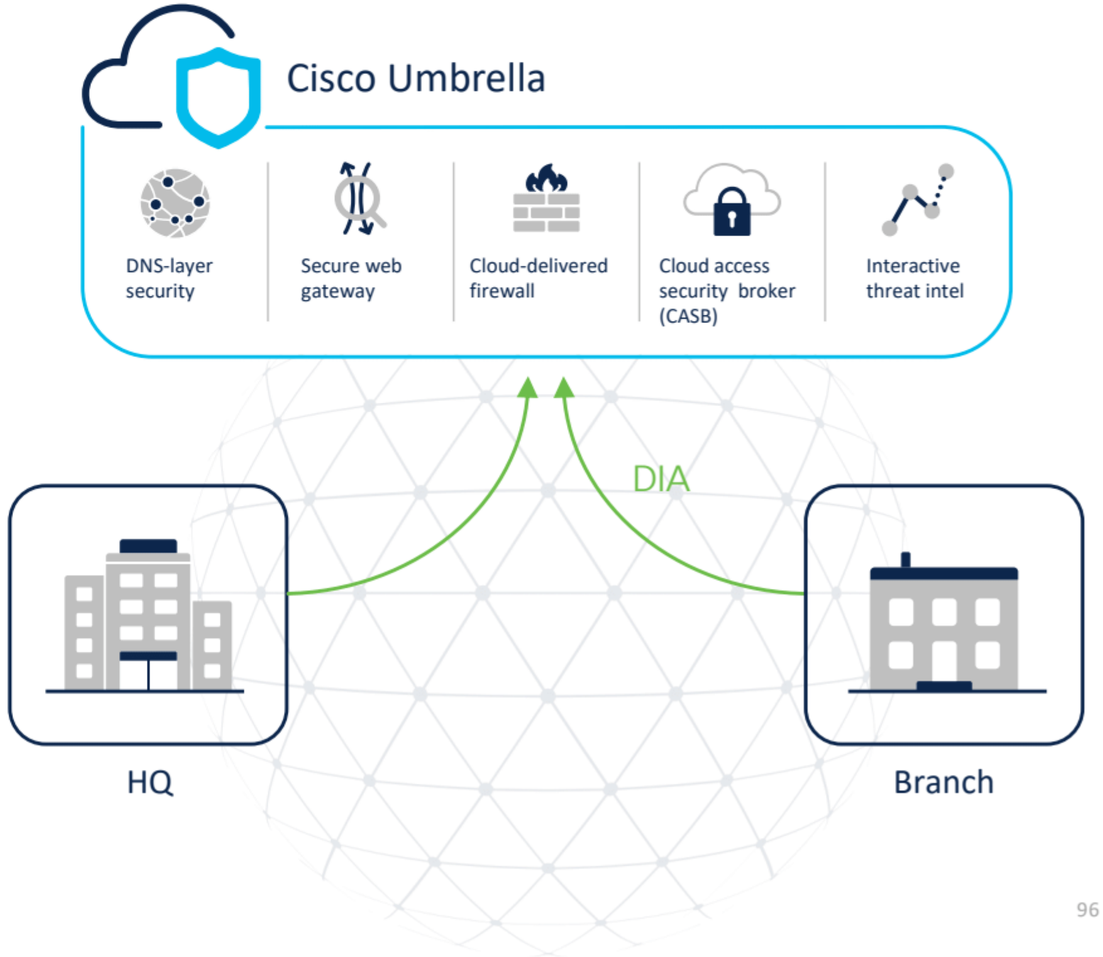
viptela

Use Umbrella DNS
208.67.222.222
208.67.220.220

Umbrella для Cisco SD-WAN

Автоматична безпека для **SASE**

- Вбудована автоматизація: розгортання IPsec-тунелів на тисячах вузлів за лічені хвилини
- Спрощене управління: Одна консоль для всіх офісів, включаючи автономні пристрої
- Поглиблений огляд і контроль: SWG, CASB, і хмарний Firewall на рівнях 3, 4 і 7

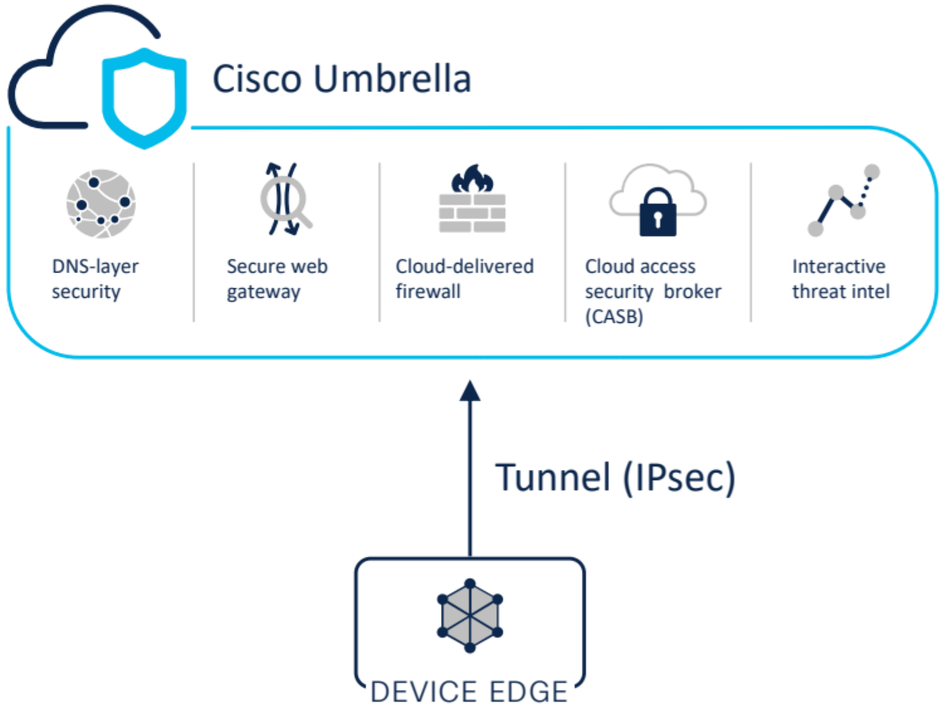


Use Umbrella DNS
208.67.222.222
208.67.220.220

Автоматичне створення IPsec тунелів

Cisco SD-WAN SASE

- Надіславши шаблон функції SIG, адміністратори можуть встановити тунель IPsec в Umbrella SIG
- без цього рішення клієнти повинні вручну встановити тунель для кожного пристрою в мережі



З такими можливостями SD-WAN дозволяє швидко і прозоро інтегруватися з Umbrella

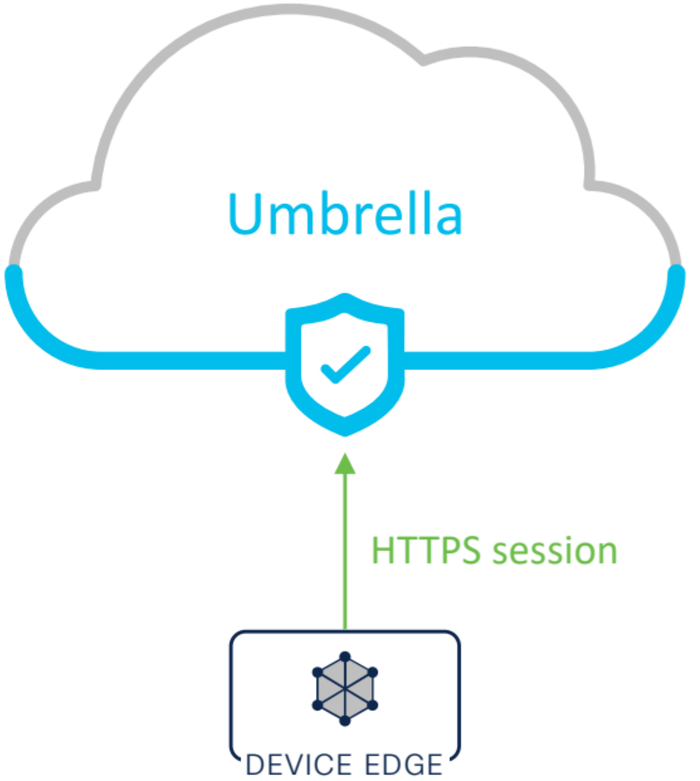
Use Umbrella DNS
208.67.222.222
208.67.220.220

Швидке впровадження: прискорення безпеки та ROI

Cisco SD-WAN SASE

Розгортання SD-WAN займає лічені хвилини:

- SD-WAN Edge автоматично реєструється в Umbrella
- Не треба вводити ключі API
- Захищений ключ API автоматично налаштовується на edge пристрої

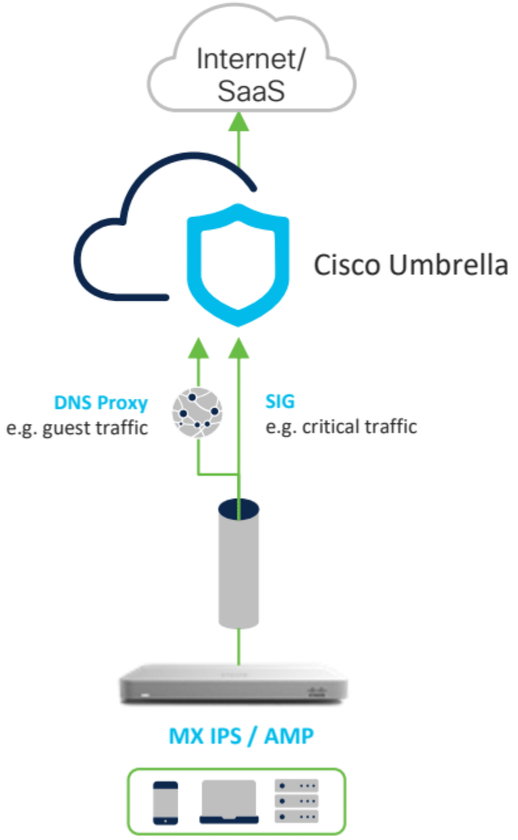


New DNA-Premier package

Use Umbrella DNS
208.67.222.222
208.67.220.220

Варіанти інтеграції Meraki MX та Umbrella

Фаза 1
Meraki dashboard and user interface simplify tunnel creation



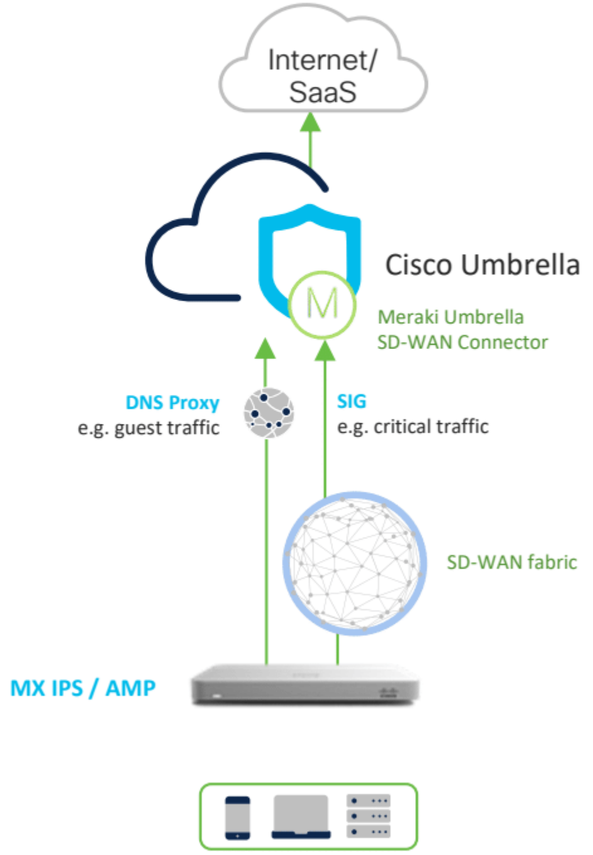
IPsec Tunnel Connectivity

Choose per site

Flexible security options

Automated SD-WAN fabric integration

Фаза 2
Auto VPN extends Meraki's SD-WAN fabric into the Umbrella cloud



SD-WAN Fabric Integration

Use Umbrella DNS
208.67.222.222
208.67.220.220

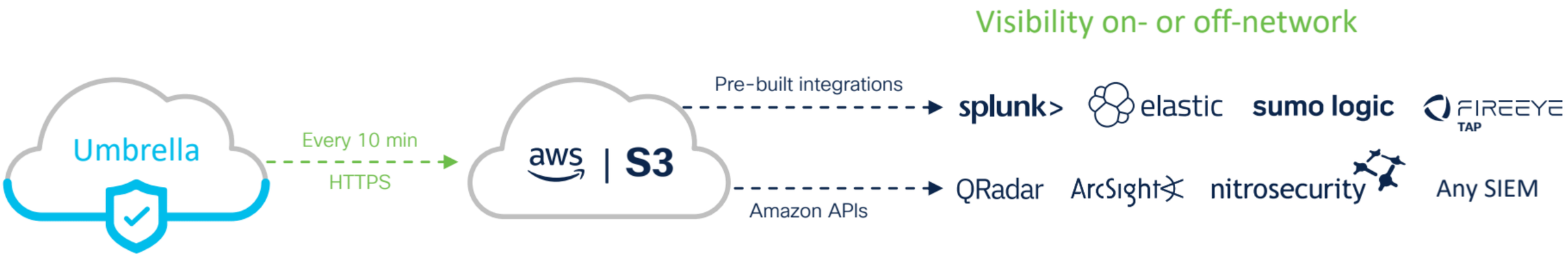
Журнали зберігаються в Amazon S3

S3 Переваги

- Зашифроване сховище з потрійним резервуванням
- Вбудована інтеграція SIEM/log аналітики
- Використовуйте персональний bucket, або Cisco bucket
- Централізованне керування журналами S3

Сховище доступне в ЄС

- Зменшує занепокоєння щодо зберігання даних
- Зберігає дані до ЄС

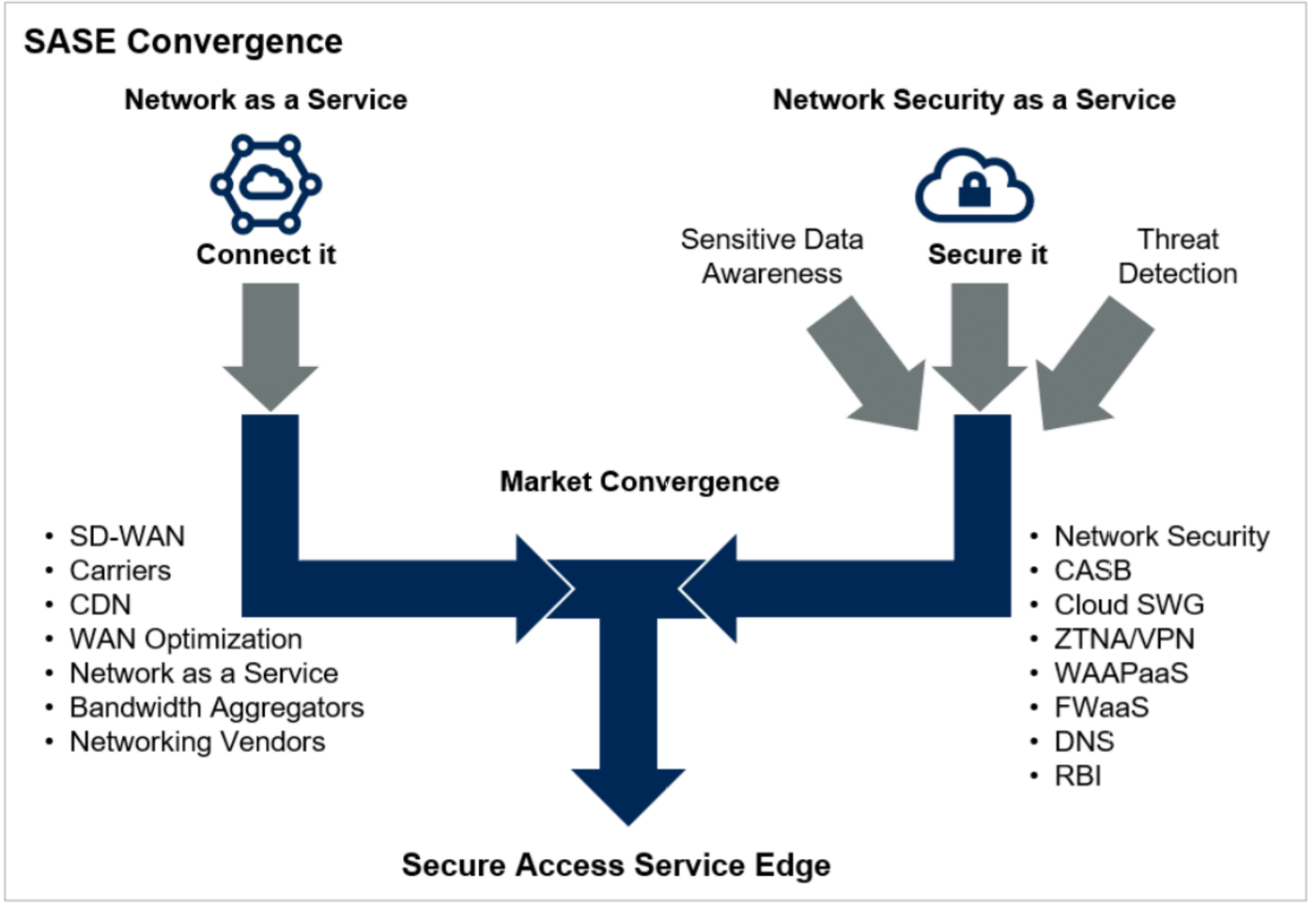


Secure Access Services Edge

Use Umbrella DNS
208.67.222.222
208.67.220.220

Gartner: Secure Access Service Edge (SASE)

Конвергенція сервісів мережі та безпеки, включаючи
SWG, CASB, DNS, firewall-as-a-services, SD-WAN та архітектури zero trust



Gartner, The Future of Network Security Is in the Cloud, Neil MacDonald, Aug 30, 2019

Use Umbrella DNS
208.67.222.222
208.67.220.220

SASE повертає вам контроль над ситуацією

Надання безпечного доступу з будь якої точки

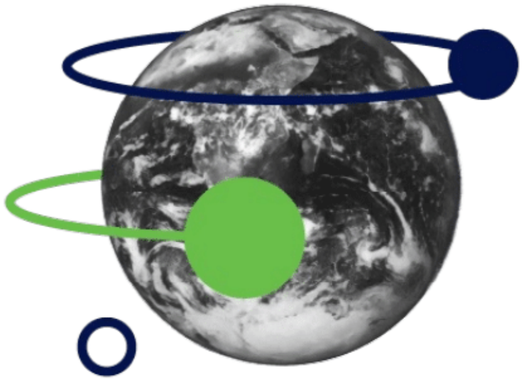
Робить ваш бізнес більш гнучким

Переміщує елемент керування доступом до граничного рівня мережі

Ефективна модель як послуги

З рішеннями Cisco ми маємо унікальні позиції

Use Umbrella DNS
208.67.222.222
208.67.220.220



Мережі

Найбільший постачальник рішень SD-WAN

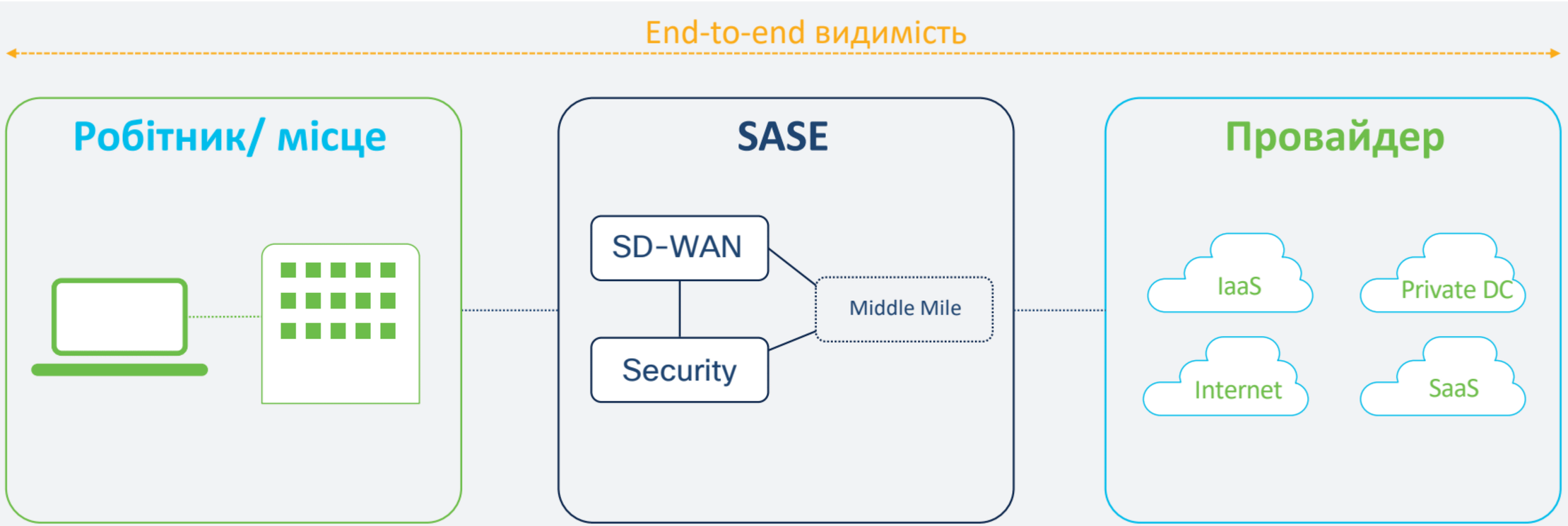
Безпека

Захист 100%
Fortune 100

Zero Trust

Лідер Zero Trust вже кілька років поспіль

Use Umbrella DNS
208.67.222.222
208.67.220.220



Reduce cost

Improve OpEx with circuit consolidation and consolidation of UI touchpoints

Improve user experience

Bring services closer to user and leverage middle-mile partnerships + password-less authentication to optimize connections

Minimize risk

Decryption & inspection addressing data loss, leveraging a true zero-trust approach across the IT diameter

Use Umbrella DNS
208.67.222.222
208.67.220.220

SASE Software defined WAN

Software Defined Connectivity

Automation and Cloud-Based orchestration	Cloud On-Ramp and Multi-Cloud access	Middle mile optimization	Integrated security and macro/micro segmentation	Dynamic performance routing	Analytics, SaaS Telemetry, Smart thresholds
Zero touch онбординг та забезпечення	Єдина консоль оркестрування хмарних мереж	Гнучкі та програмовані варіанти взаємозв'язку	Інтегровані елементи керування безпекою та мережевою політикою	Передбачувана продуктивність додатків і користувальницький досвід	Проактивне забезпечення мережі та мережеві операції

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Umbrella DNS
208.67.222.222
208.67.220.220

SASE Cloud security (Security Service Edge)

Хмара забезпечує захист від загроз

DNS-layer security	Cloud-delivered firewall	Secure web gateway	Cloud App & Data Security (CASB & DLP)	Remote Access	Interactive threat intel	SecureX Platform
Припиніть загрози до того, як трафік потрапить до мережі	L7 безпека на всіх сайтах, щоб зупинити невеб-загрози	Повна видимість/контроль URL-адреси для забезпечення виконання політики блокування попередніх загроз	Виявлення, звітування та керування використанням хмарних додатків	Хмарний безпечний віддалений доступ	Контекст загрози в режимі реального часу, що прискорює розслідування та реагування на інциденти	Видимість по всьому стеку безпеки за допомогою автоматизованих дій

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Umbrella DNS
208.67.222.222
208.67.220.220

SASE Zero trust

Хмарна ідентифікація та можливості довіри

Adaptive MFA

Переконайтеся, що користувачі є тими, за кого себе видають

Device posture and health

Оцініть і застосуйте перевірку endpoint перед входом в систему

Least privileged access

Zero Trust - забезпечити безпеку та позицію при КОЖНОМУ вході в програму

Continuous verification

Кожен логін отримує постійний аналіз безпеки

Behavior analytics

Виявляйте та повідомляйте про аномальну, незвичайну та підозрілу активність у вході/доступі

Кожен користувач. Кожен пристрій. Кожна програма.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Umbrella DNS
208.67.222.222
208.67.220.220

SASE Visibility

Корисна інформація, яку команди IT та Ops використовують для вирішення інцидентів швидко з кращими результатами для користувача

App performance	Path visualization	Internet and WAN health	BGP route monitoring	Remote worker experience
Ізоляція проблем із застосунками від проблем із мережею	Визначте проблеми, пов'язані з постачальником послуг, розташуванням та інтерфейсом	Інтернет - це ваша нова глобальна мережа. Контролюйте його продуктивність	Переконайтеся, що проблеми з маршрутизацією в Інтернеті не впливають на користувачів і служби	Бізнес-програми мають бути доступними, коли співробітники працюють з дому

Correlated insights to take action

Видимість від кожного користувача, до будь-якої програми, через будь-яку мережу.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Umbrella DNS
208.67.222.222
208.67.220.220

SASE Агент

Уніфікований агент, що поєднує безпеку та видимість

Advanced VPN	Endpoint Compliance	Network Visibility	Cloud Edge / SASE	End to end Encryption
✓	✓	✓	✓	✓
Корпоративний доступ за допомогою розширеного контролю доступу	Перевірка endpoint posture у дротових, бездротових мережах та мережах VPN	Фіксує кінцеву точку та поведінку користувачів	Інтегрується з хмарним компонентом безпеки SASE DNS Security і SWG-контентом	Зменшуйте ризики за допомогою наскрізного шифрування data-in-motion

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Umbrella DNS
208.67.222.222
208.67.220.220

Cisco SASE Архітектура

Reduce cost

- Improve OpEx through circuit consolidation
- Reduce IT complexity and improve OpEx by consolidating UI touchpoints and leveraging centralized policy

Improve user experience

- Leverage password-less authentication measures to streamline workflows
- Leverage Cisco® SD-WAN + middle-mile partnership to optimize connections and reduce latency

Minimize risk

- Proxy-based architecture decrypts, inspects, and assists with data loss prevention to protect brand
- Leverage a true zero-trust approach by securing workplace and off-premises workforce to workloads

Demo Time

SECURE