Cisco Umbrella

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

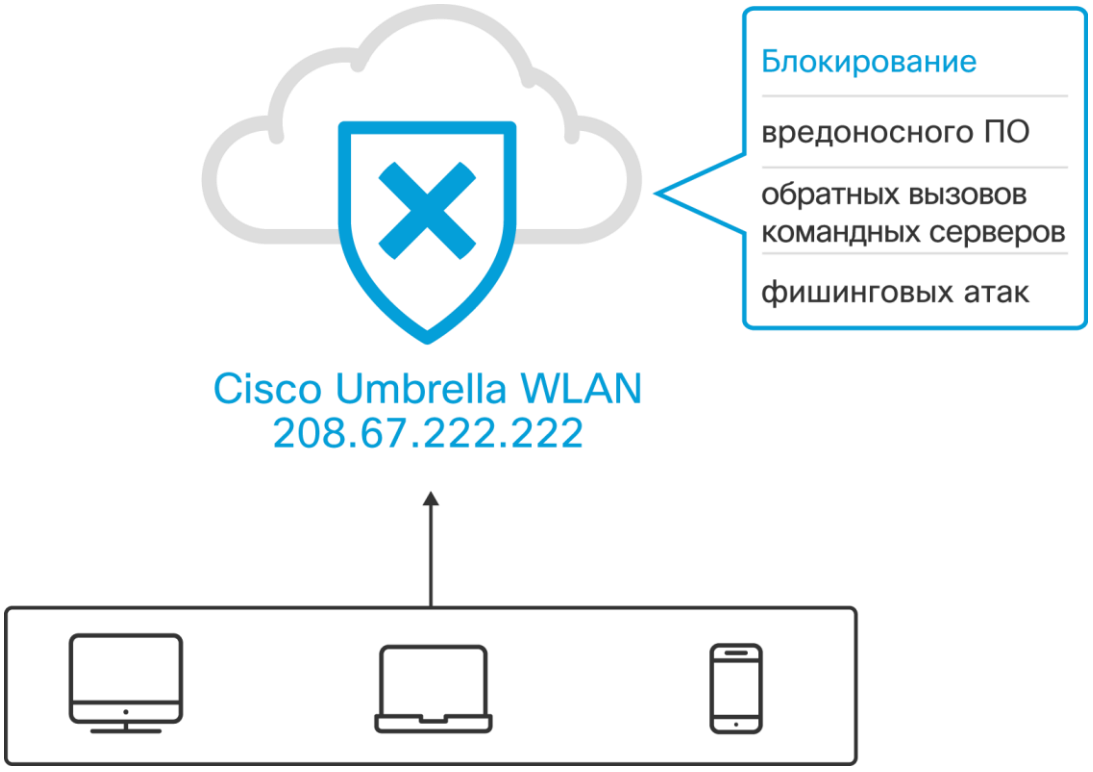
Cisco Umbrella: пакет Wireless LAN

Защита корпоративного и гостевого доступа к Wi-Fi

Пакет Cisco Umbrella Wireless LAN (WLAN) служит первой линией обороны от угроз для подключений Wi-Fi. Это самый быстрый и простой способ обеспечить безопасность всех пользователей в сети Wi-Fi.

Umbrella WLAN обеспечивает сотрудникам и гостям защищенное подключение к Интернету из точек беспроводного доступа. Применение политик безопасности на уровне DNS исключает возможность подключения к сомнительным сайтам и загрузки вредоносных файлов. Таким образом, вредоносное ПО не может проникнуть на устройства, и утечка данных в результате атаки через какой-либо порт или протокол невозможна. Umbrella WLAN также обеспечивает простое в использовании решение для фильтрации контента в сети Wi-Fi. Оно блокирует доступ гостевых и корпоративных пользователей к неразрешенному контенту в соответствии с политикой компании. В результате пользователи получают безопасный доступ в Интернет, а ваш бизнес находится под надежной защитой.

Umbrella WLAN – простейший способ обеспечить безопасность любого устройства, подключающегося к вашей беспроводной сети. Никаких действий конечных пользователей при этом не требуется. Umbrella WLAN обеспечивает простой, но очень эффективный способ защиты любых устройств, принадлежащих организации, сотрудникам или заказчикам.



Преимущества Umbrella WLAN

- Интеграция с контроллерами беспроводных локальных сетей Cisco (WLC), точками доступа Aruba, Cradlepoint и Aerohive упрощает развертывание и управление политиками.
- Поскольку плата взимается за каждую точку доступа, вы можете обеспечить защиту неограниченного числа пользователей.

Совместимость с решениями

Контроллеры беспроводных локальных сетей

Другие точки доступа

Решение, созданное для вашей беспроводной среды

Платформа Umbrella WLAN совместима со многими контроллерами беспроводных сетей и точками доступа. Встроенная интеграция с решениями Cisco для беспроводной связи и другими продуктами еще больше упрощает эксплуатацию и обеспечивает детальный контроль.

Контроллеры беспроводных локальных сетей Cisco (WLC)

Мониторинг и управление политиками выполняются для каждого устройства, общедоступного IP-адреса и идентификатора SSID. Динамические общедоступные IP-адреса автоматически обновляются. Защиту всех DNS-запросов обеспечивает программа DNSCrypt, которая предотвращает перехват информации и атаки через посредника.
Развертывание за считанные минуты:

1. Обновите свой контроллер беспроводной локальной сети Cisco (WLC) до AireOS 8.4 или более поздней версии.
2. Настройте коннектор Umbrella на контроллере Cisco WLC.
3. Создайте политики безопасности и фильтрации контента (если необходимо).
4. WLC регистрируется в Umbrella WLAN, и политика активируется.

Точки доступа Aruba, Cradlepoint или Aerohive

Организации, использующие точки доступа Aruba, Cradlepoint или Aerohive, получают преимущества от мониторинга и управления политиками для каждого устройства и общедоступного IP-адреса. Динамические общедоступные IP-адреса автоматически обновляются.

Другие точки доступа

Мониторинг и управление политиками выполняются для каждого общедоступного IP-адреса. Динамическими общедоступными IP-адресами управляет пользователь.

Функции решения

Защита

Защита всех гостей, сотрудников и устройств в беспроводной сети от вредоносного ПО, программ-вымогателей, фишинга и обратных вызовов командных серверов

Блокирование запросов к вредоносным доменам и IP-ответов на уровне DNS

Применение политик допустимого использования по 60 категориям контента

Мониторинг

Все события безопасности, произошедшие за день, неделю или месяц, можно просмотреть в вашей папке входящих сообщений или на панели управления Umbrella

Вы можете увидеть, растет или сокращается число угроз в вашей среде, и быстро реагировать на инциденты за счет полного анализа действий в конкретном домене

Можно просмотреть подробные сведения об интернет-трафике реального времени за последние 30 дней и при желании отфильтровать их по времени, домену, категории, устройству или IP-адресу

Управление

Создание настраиваемых списков запрещенных и разрешенных ресурсов и вариантов обхода для администраторов Разработка настраиваемых страниц блокировки для конечных пользователей

Как Umbrella заблаговременно прогнозирует угрозы

Ежедневно наша глобальная сетевая инфраструктура обрабатывает более 100 млрд DNS-запросов, что обеспечивает нам уникальный обзор Интернета. На основании шаблонов интернет-трафика Umbrella выявляет инфраструктуру злоумышленников, подготовленную для очередной атаки. Мы пропускаем огромные массивы данных через модели на основе статистических методов и машинного обучения, чтобы обнаруживать текущие и новые угрозы и заранее блокировать доступ пользователей к вредоносным узлам.

Cisco Umbrella