Cisco Umbrella

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

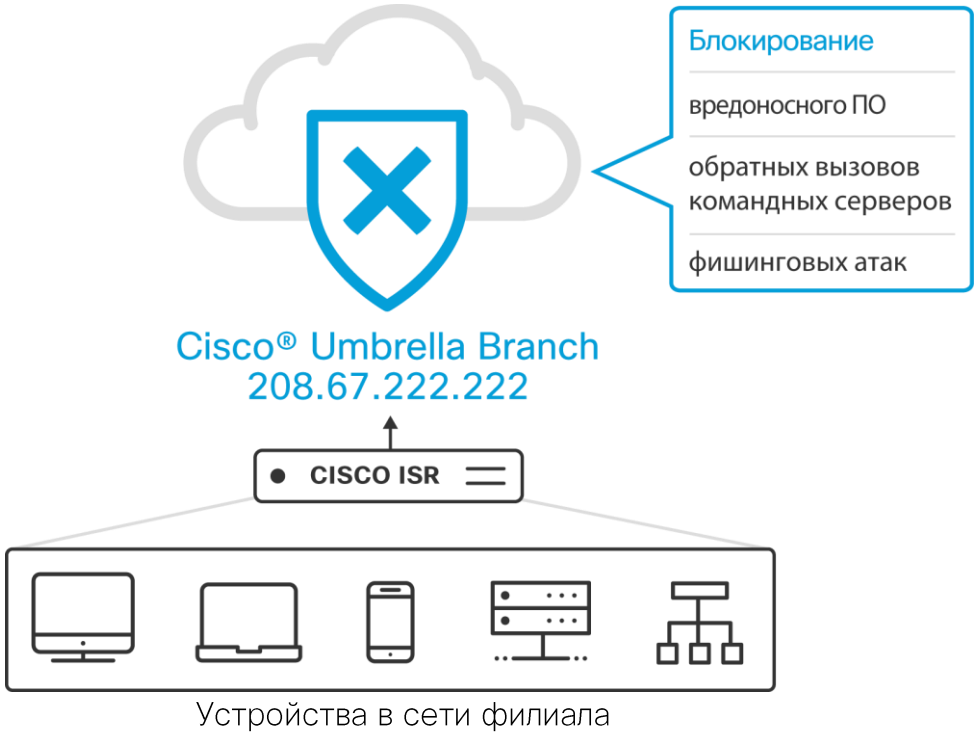
Cisco Umbrella: пакет Branch

Самый быстрый и простой способ защиты филиалов

Cisco Umbrella Branch – это облачное решение безопасности для маршрутизаторов с интегрированными сервисами Cisco (ISR) серии 4000. Оно служит первой линией обороны от угроз в филиалах. Это самый быстрый и простой способ обеспечить безопасность всех устройств в сети филиала. Мониторинг и применение политик на уровне DNS позволяют блокировать запросы к вредоносным доменам и IP-адресам до установления соединения.

Umbrella Branch обеспечивает защиту сотрудников и гостей в распределенных филиалах предприятий розничной торговли и гостиничного бизнеса, финансовых компаний, образовательных учреждений и других организаций. 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 через какой-либо порт невозможна. Umbrella Branch также обеспечивает простое в использовании решение для фильтрации контента в филиалах. Оно блокирует доступ гостевых пользователей Wi-Fi к неразрешенному контенту и не позволяет сотрудникам отвлекаться от рабочих обязанностей при подключении к Интернету. В результате ваши заказчики получают безопасный доступ в Интернет, а бизнес находится под надежной защитой.

Umbrella Branch – простейший способ обеспечить безопасность любого устройства в филиалах. Достаточно лишь обновить ПО на маршрутизаторах ISR 4000 – и можно начинать применять политики допустимого использования и блокировать вредоносное ПО, фишинговые атаки и обратные вызовы командных серверов. Никаких действий со стороны конечных пользователей при этом не требуется. Umbrella Branch обеспечивает простой, но очень эффективный способ защиты любых устройств, принадлежащих организации, сотрудникам или заказчикам.



Проблема

- 30% сложных целенаправленных атак попадают в сеть через филиалы, которые они используют в качестве точки входа.
- 70% филиалов в той или иной степени используют прямой доступ к Интернету[2].

Решение

Cisco ISR серии 4000 и выше
Cisco Umbrella Branch

Простая и эффективная защита каждого пользователя в каждом филиале.

Лучшее сочетание эффективности и производительности

№ 1	по скорости и надежности обработки DNS-запросов от более 85 млн активных пользователей ежедневно
Более 100 млрд	ежедневных интернет-запросов и подключений
Более 3 млн	новых доменных имен, выявляемых ежедневно
Более 60 тыс.	вредоносных узлов, обнаруживаемых ежедневно
Более 7 млн	одновременно блокируемых вредоносных узлов при обработке DNS-запросов

[1] cs.co/gartner-branch [2] cs.co/Forrester-BranchOffices [3] cs.co/tech-target

Тенденции в филиалах

80% сотрудников и клиентов обслуживаются в филиалах[3]

Гостевым пользователям нужен удобный доступ к Wi-Fi, а сотрудникам требуется подключение к сети для эффективной работы. Однако в большинстве филиалов используется прямой доступ в Интернет, и сложные угрозы целенаправленно поражают уязвимые места. По мере того как все больше пользователей подключаются к незащищенным сетям филиалов, последние становятся еще более привлекательными для злоумышленников.

Заблаговременное прогнозирование угроз

Разнообразные данные реального времени позволяют определить шаблоны интернет-трафика

Ежедневно наша глобальная сетевая инфраструктура обрабатывает более 100 млрд DNS-запросов, что обеспечивает нам уникальный обзор Интернета. Сопоставляя DNS-запросы, записи WHOIS, маршруты BGP, данные по расположению на основе IP-адресов, сертификаты SSL, факты доступа к вредоносным файлам и другие сведения, Umbrella создает полную картину доменов и IP-адресов, задействованных в атаках.

Автоматизированные модели на основе статистических методов и машинного обучения обнаруживают вредоносные узлы

Подобно тому, как Amazon анализирует модели покупательского поведения для предложения следующего товара, а Pandora на основании музыкальных предпочтений пользователя выбирает очередную композицию для воспроизведения, мы изучаем шаблоны интернет-трафика и затем, руководствуясь полученными знаниями, выявляем инфраструктуру злоумышленников, которая подготавливается для новой атаки. Мы пропускаем данные через модели на основе статистических методов и машинного обучения, чтобы обнаруживать текущие и новые угрозы и заранее блокировать доступ пользователей к вредоносным узлам.

Простота использования для служб безопасности и системных администраторов

Реализация защиты за считанные минуты

Минимум усилий:

1. настройка коннектора ISR (предоставляется централизованно через Cisco Prime);
2. создание защищенного туннеля с Cisco Umbrella (только для внешнего трафика DNS);
3. создание политик безопасности и фильтрации контента (если необходимо);
4. регистрация ISR и добавление политики.

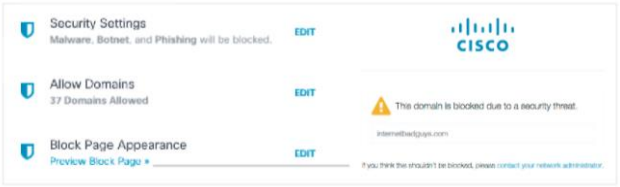
Все готово.

Глобальная защита по умолчанию

Сразу после активации Umbrella Branch обеспечивает защиту от вредоносного ПО всех пользователей, гостей и сотрудников.

Если вредоносный контент запрашивается через веб-браузер, для конечных пользователей отображается настраиваемая страница блокировки.

Чтобы немедленно открыть доступ к заблокированному сайту, нужно просто добавить домен в список разрешенных.



Мгновенное обнаружение угроз

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

Можно узнать, растут или сокращаются угрозы, а также выявить домены и ноутбуки с максимальным числом событий безопасности.

Полный анализ действий в конкретном домене или на конкретном ноутбуке позволяет эффективно реагировать на инцидент.

Подробные журналы для реагирования на инциденты

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

N-е число основных сводных отчетов хранится до двух лет. Вы можете запланировать их отправку в свою папку входящих сообщений.

cisco Cisco Umbrella