Cisco Umbrella

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Cisco Umbrella: пакет Roaming

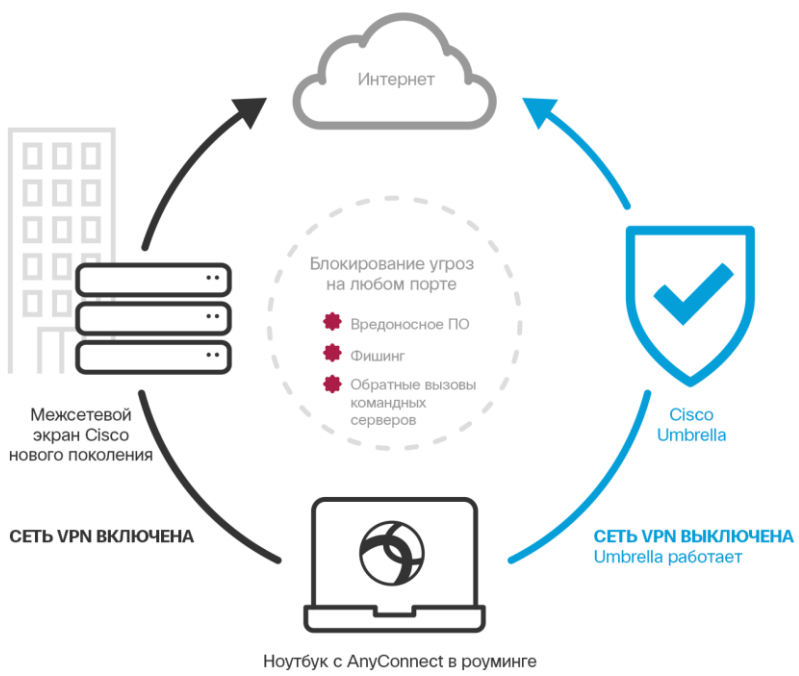
Самый быстрый и простой способ постоянной защиты пользователей

Облачный сервис обеспечения безопасности для межсетевого экрана Cisco нового поколения

Umbrella Roaming обеспечивает безопасность сотрудников, когда они подключаются к сети без использования VPN. Решение блокирует запросы к вредоносным доменам и IP-ответы в процессе обработки DNS-запросов. Применение политик безопасности на уровне DNS исключает возможность подключения к сомнительным сайтам и загрузки вредоносных файлов. Вредоносное ПО не сможет заразить ноутбуки, и в результате обратных вызовов командных серверов или фишинга не произойдет утечки данных через какой-либо порт. Кроме того, вы сможете контролировать зараженные ноутбуки и их связи с командной инфраструктурой злоумышленника в режиме реального времени.

Защита мобильных сотрудников без дополнительных агентов и действий пользователя

Весь интернет-трафик, который обходит средства защиты периметра, теперь направляется через нашу службу безопасности, устраняя невидимые зоны вне вашей сети. Решение Umbrella Roaming полностью интегрируется с AnyConnect для Windows или Mac OS X. В отличие от использования VPN, оно не требует от конечных пользователей никаких новых действий и не снижает производительность[2].



Способы работы изменились

82% сотрудников признают, что не всегда используют сеть VPN[2]

Сотрудники используют больше облачных приложений для работы, а свои рабочие ноутбуки – для личных целей, причем не каждое подключение осуществляется через сеть VPN. Ваши средства безопасности (как и сама сеть) должны выйти за пределы периметра.

49% персонала – это мобильные сотрудники, которые недостаточно защищены[3]

Пик заражения новым вредоносным ПО приходится на ночное время и выходные, когда пользователи перемещаются, и злоумышленники знают об их уязвимости. В 22% случаях пользователи переходят по вредоносным ссылкам в электронной почте, будучи в роуминге[4]. Пусть система безопасности не сможет отразить абсолютно все угрозы, но она должна работать постоянно.

1. cs.co/gartner-prediction 2. cs.co/IDG-survey 3. cs.co/sans-survey 4. cs.co/proofpoint-repott 5. cs.co/dns-latency,

Проблема

Межсетевые экраны нового поколения не контролируют 25% трафика[1]

Не весь трафик (проходящий через все порты в каждый момент времени) пропускается через средства защиты периметра, использующие Cisco AnyConnect VPN. Это связано со следующими причинами:

- Использование приложений и данных в облаке
- Просмотр веб-страниц в личных целях
- Настройка разделенных туннелей

Защиты оконечных устройств (например, с помощью антивирусных программ) недостаточно для обеспечения безопасности мобильных сотрудников.

Решение

Межсетевой экран Cisco нового поколения + Cisco Umbrella Roaming

- Безопасность при отсутствии подключения к сети VPN
- Не требуется никаких действий конечных пользователей
- Защита от угроз, проникающих через любой порт
- Для ноутбуков в роуминге, работающих под управлением Windows и Mac OS X

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

Заблаговременное прогнозирование угроз

Разнообразные данные реального времени позволяют определить шаблоны интернет-трафика

Сопоставление DNS-запросов, записей WHOIS, маршрутов BGP, данных по расположению на основе IP-адресов, сертификатов SSL и фактов доступа к файлам создает полную картину доменов и IP-адресов, являющихся источниками будущих угроз.

Автоматизированные статистические модели 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, подготовленную для новой атаки.

Узнайте, как нам удается обеспечить такую быстроту и надежность

- Для специалистов по обслуживанию сетей: перейдите на страницу cs.co/pointdns, чтобы узнать, как мы сохраняем стопроцентную отказоустойчивость с 2006 г.
- Для системных администраторов: перейдите на страницу cs.co/roaming, чтобы узнать, почему не используются практически никакие ресурсы ПК.

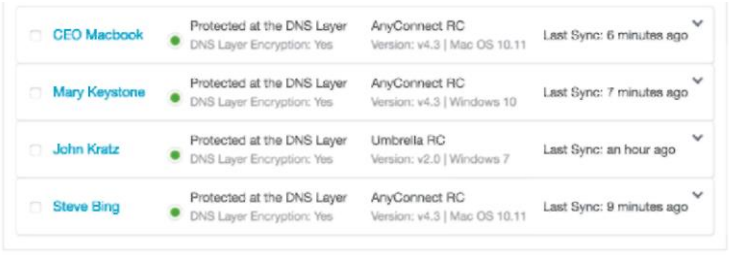
Простота использования для служб безопасности и системных администраторов

Реализация защиты в роуминге за считанные минуты

- Просто активируйте модуль Roaming Security в Cisco AnyConnect версии 4.3 или более поздней для Windows или Mac OS X.

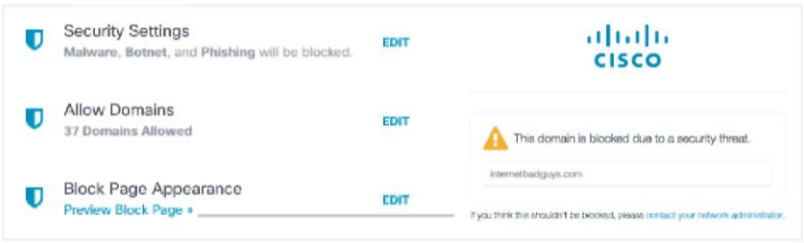
ИЛИ

- Разверните автономный клиент Umbrella Roaming для Windows или Mac OS X наряду с любым другим клиентом VPN для удаленного доступа.



Глобальная защита по умолчанию

- Сразу после активации модуль Roaming Security обеспечивает защиту мобильных сотрудников от вредоносного ПО.
- 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 пределами сети за день, неделю или месяц, можно просмотреть в вашей папке входящих сообщений или на нашей панели управления.
- Можно узнать, растет или уменьшается число угроз, 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-ое число основных сводных отчетов хранится до двух лет. Можно запланировать их отправку в папку входящих сообщений – вашу или других пользователей.