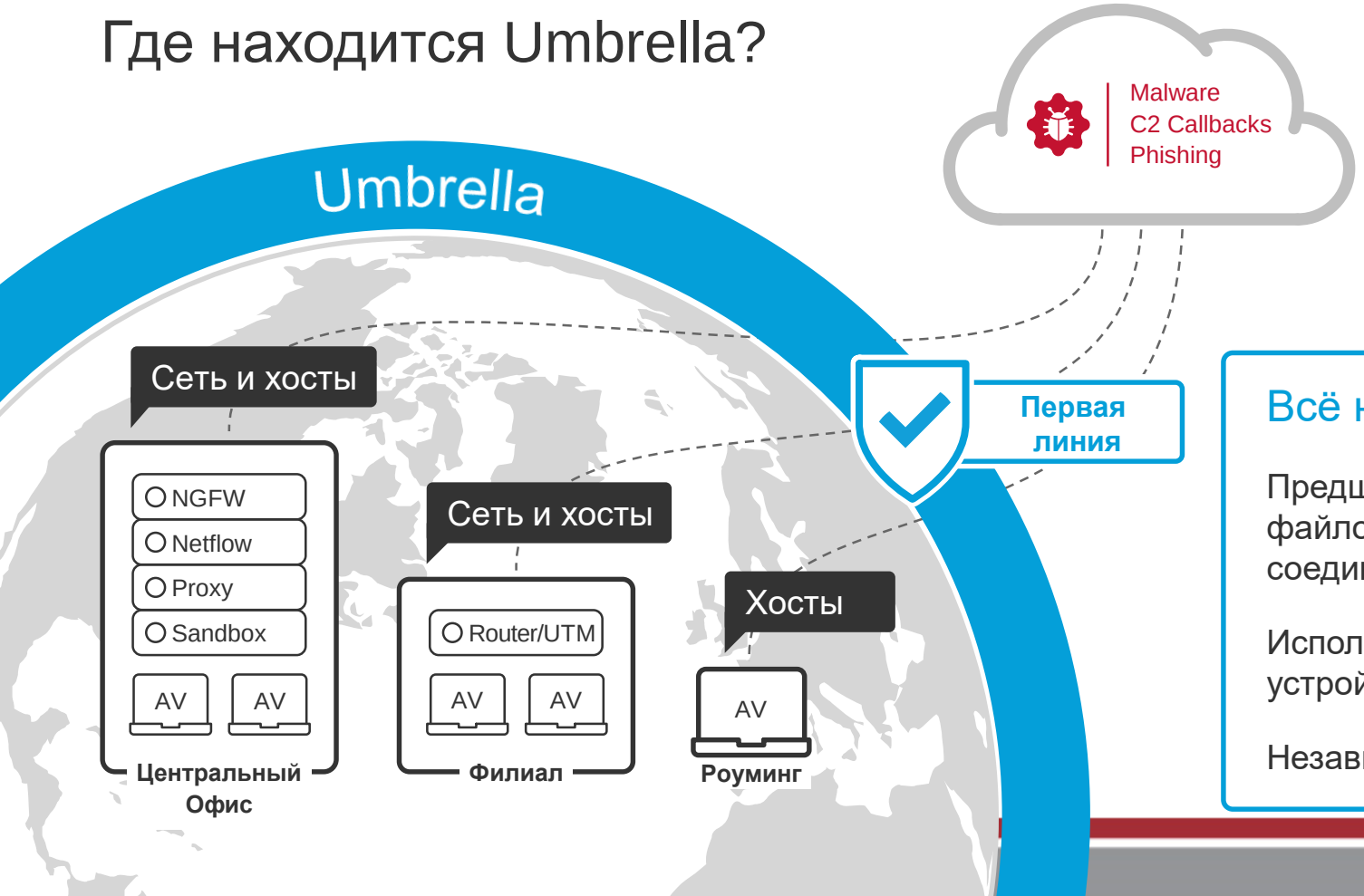
Cisco Umbrella – Первая линия обороны против интернет угроз

Евгений Лысенко

Старший инженер-консультант
Департамент телекоммуникаций
CCNP, CCDP, CCNP DC, CCNA Sec, CCNA Wireless
Evgeniy.Lysenko@it-integrator.ua

Где находится Umbrella?



Всё начинается с DNS

Предшествует открытию файлов и установлению IP соединения

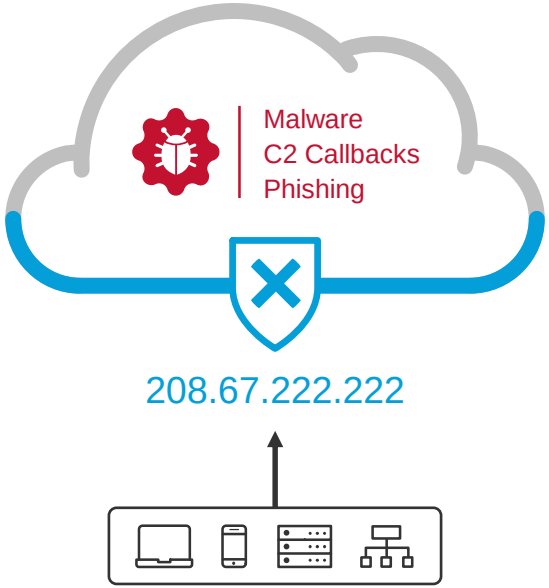
Используется всеми устройствами

Независимо от порта

IT.Integrator

Cisco Umbrella

Облачная платформа безопасности



Встроен в саму основу Интернет

Интеллект позволяющий видеть угрозу до атаки

Видимость и защита везде

Развертывание на всю сеть за минуты

Интеграция для расширения текущих возможностей

Видение Интернет

80 МЛРД.
Запросов в день

65 МЛН.
Активных пользователей ежедневно

12 ТЫС.
Корпоративных заказчиков

160+
Стран по всему миру

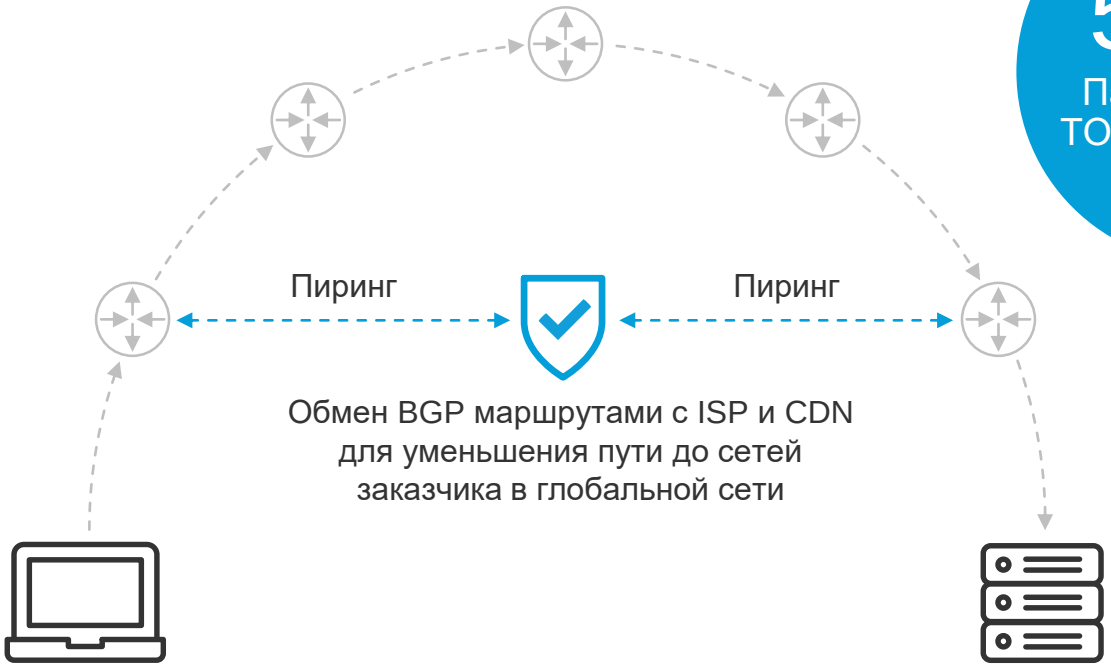
Эффективность

ЦОД расположены в основных точках обмена трафиком IXPs

25
ЦОД по всему миру

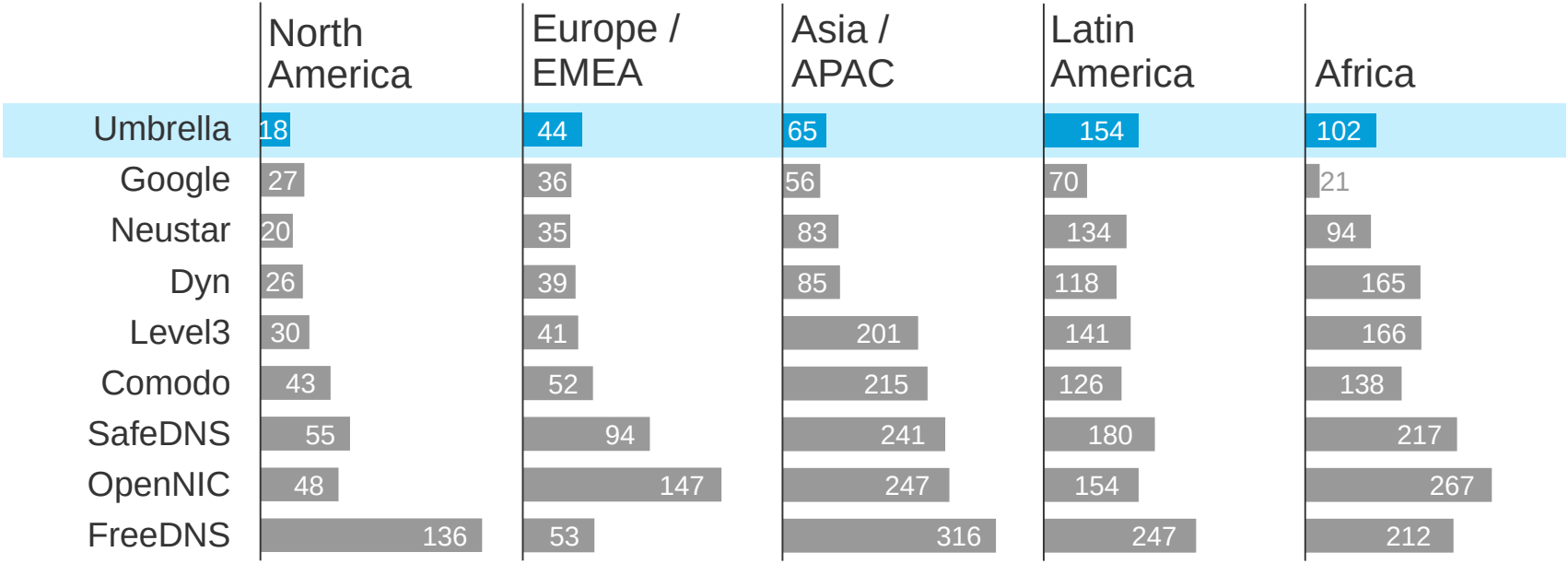
BGP пиринг для скорости

500+
Партнерство с
ТОП ISP и CDNS



Обмен BGP маршрутами с ISP и CDN
для уменьшения пути до сетей
заказчика в глобальной сети

Как быстро Umbrella резолвит DNS запросы?



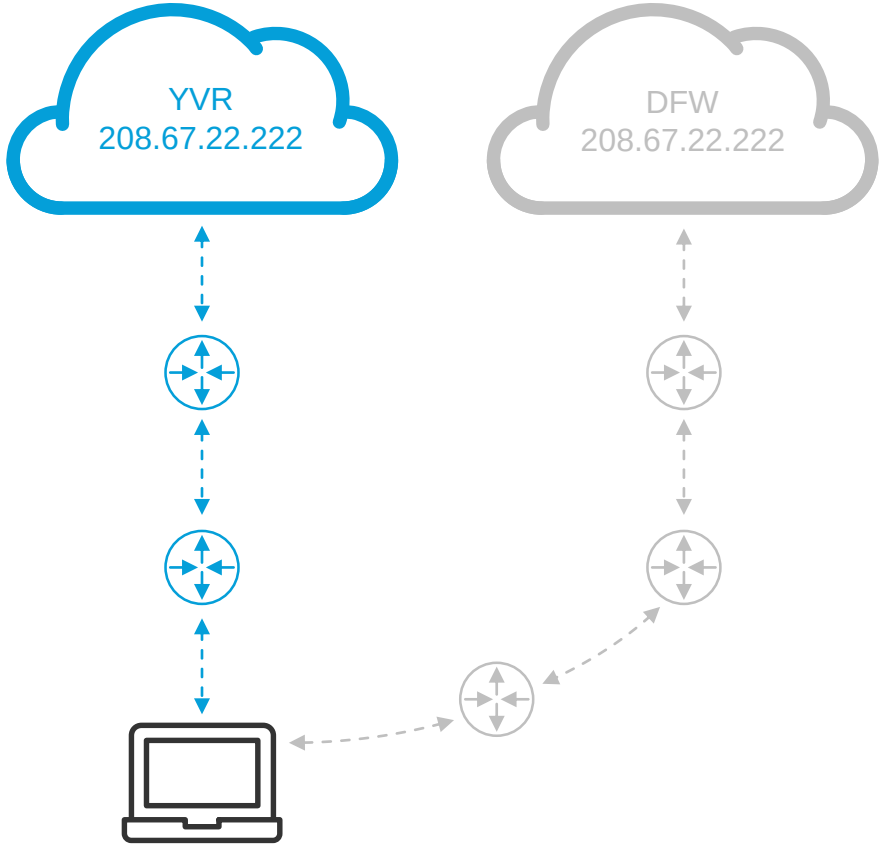
Измерение в миллисекундах

Source: MSFT Office 365 Researcher, ThousandEyes Blog Post, May 2015

Anycast IP маршрутизация для скорости

Все ЦОД анонсируют одинаковые IP адреса

Запросы прозрачно отсылаются в самый быстрый из доступных



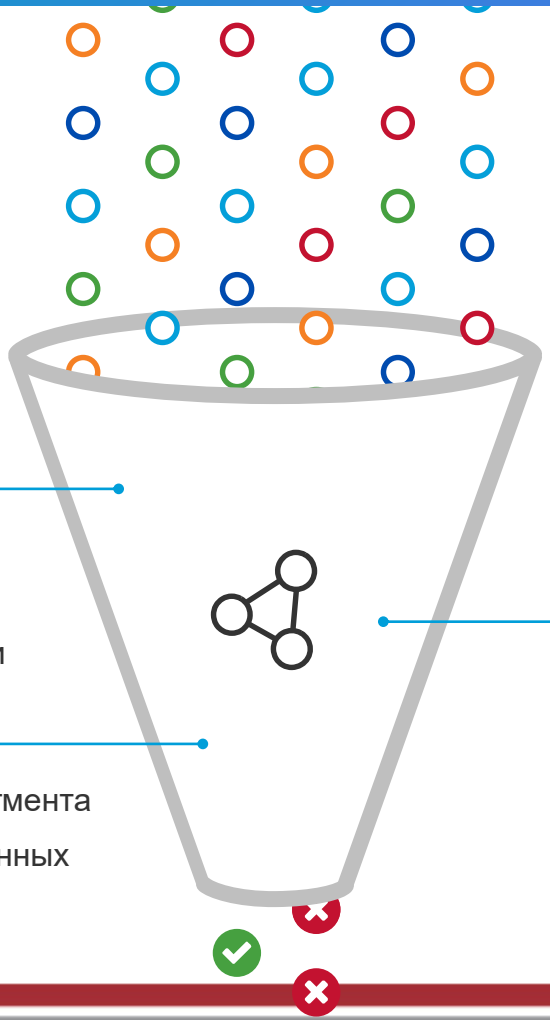
Anycast IP маршрутизация для доступности

100%

Аптайм с 2006

500+ Гб/с емскость, DDoS защита и глобальная отказоустойчивость

Статистическое моделирование



2M+ событий в секунду

11B+ исторических событий

Виновен по поведению

- Модель совместных запросов
- Геолокационная модель
- Модель индекса безопасности

Виновен по связям

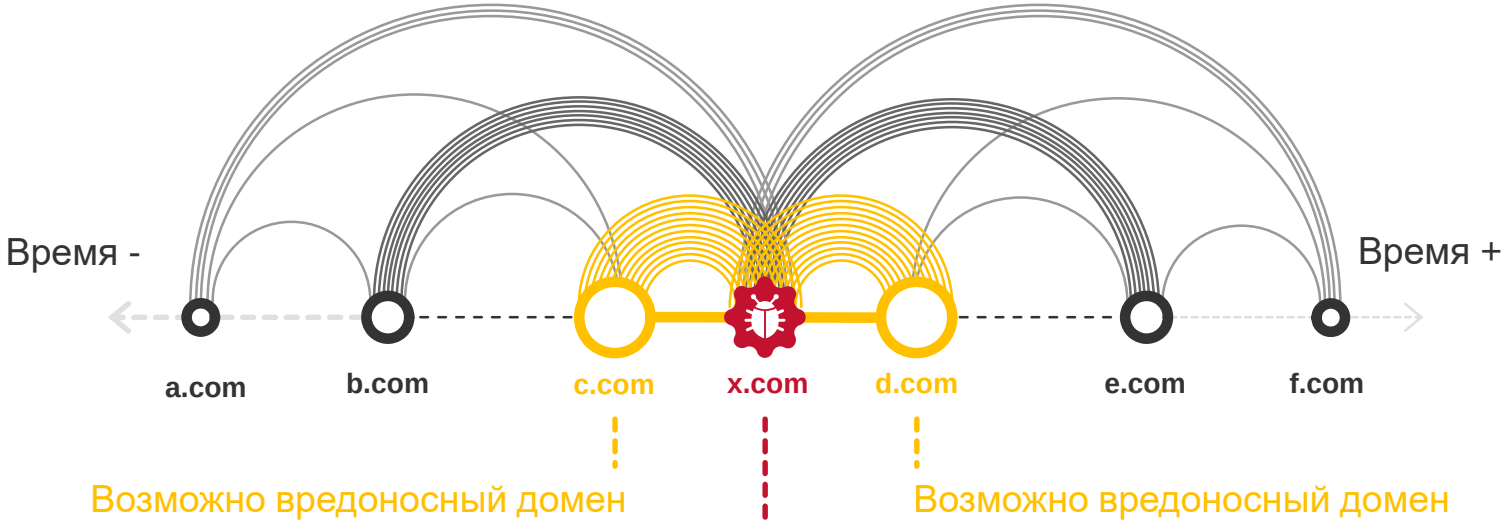
- Модель предсказуемого IP сегмента
- Корреляция DNS и WHOIS данных

Шаблон виновности

- Модель всплесков активности
- Модель оценки языкового шаблона (NLP)
- Обнаружение DGA

Модель совместных запросов

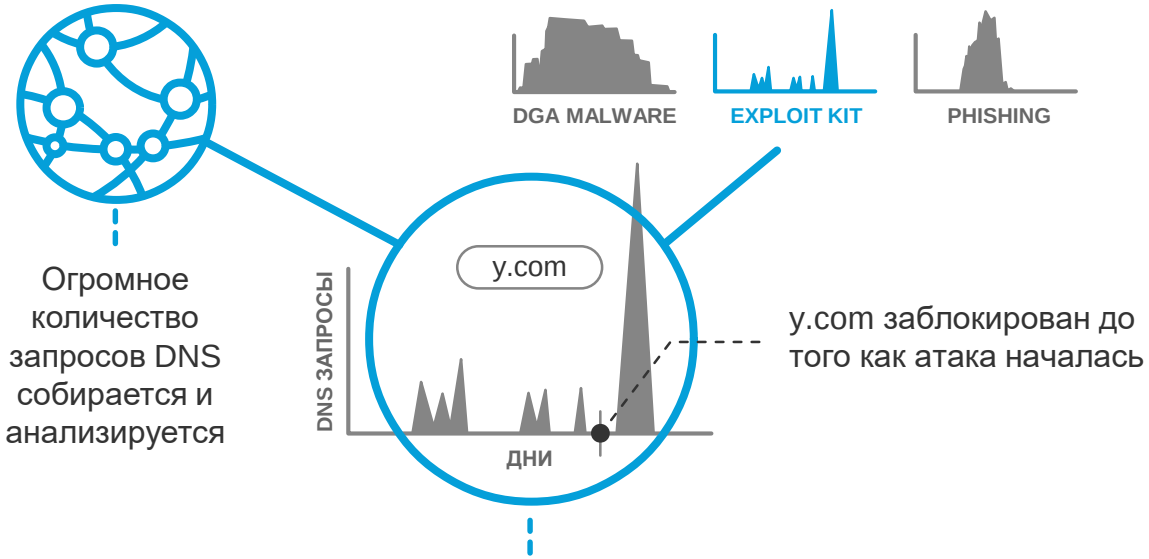
Домены виновные по модели связанных вызовов



Совместное появление доменов означает что статистически значимое количество хостов запросило оба домена одновременно в короткий промежуток времени

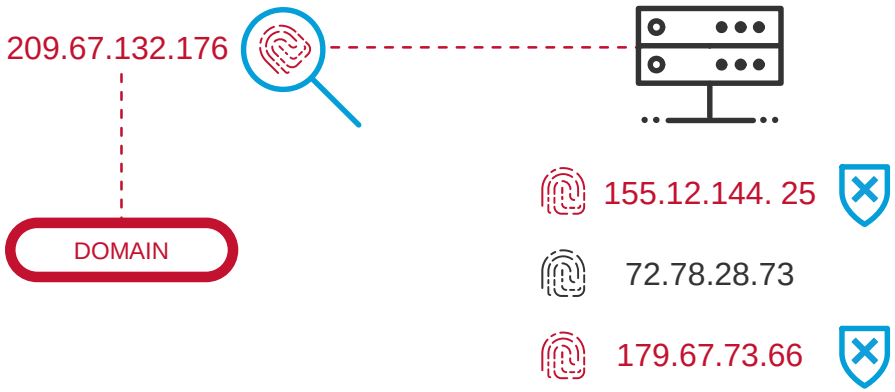
Модель всплесков активности

Шаблоны виновности



Мониторинг предсказуемого IP сегмента

Виновен по ассоциации

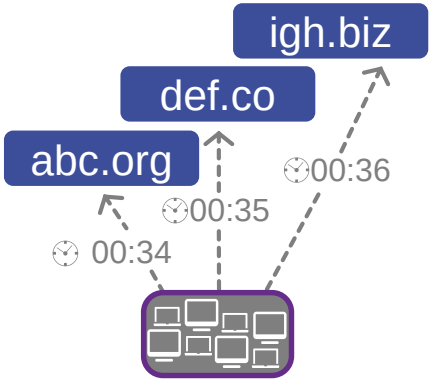


Обнаруживает подозрительные домены,
и изучает их IP отпечатки

Идентифицирует другие IP (хостящиеся на том же сервере) которые имеют схожие отпечатки

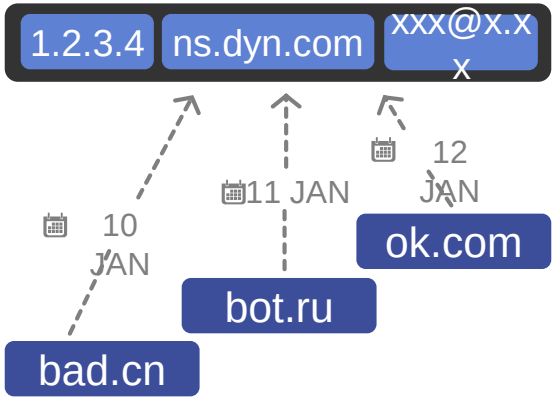
Блокируем эти IP и их ассоциированные домены

Сила корреляции DNS, WHOIS, и BGP блоков данных



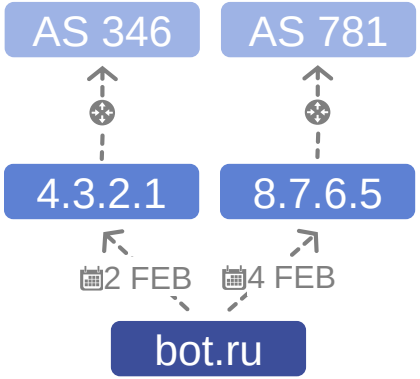
СОВМЕСТНЫЕ ЗАПРОСЫ

Запросы вида домен-к-домену через рекурсивный DNS



ПАССИВНЫЙ DNS И WHOIS

Текущие и прошлые связи для домен-к-IP/nameserver/email через authoritative DNS и DNS registrars



ИНФРАСТРУКТУРЫ

Домен-к-IP-к-AS взаимоотношения через графы BGP данные маршрутов

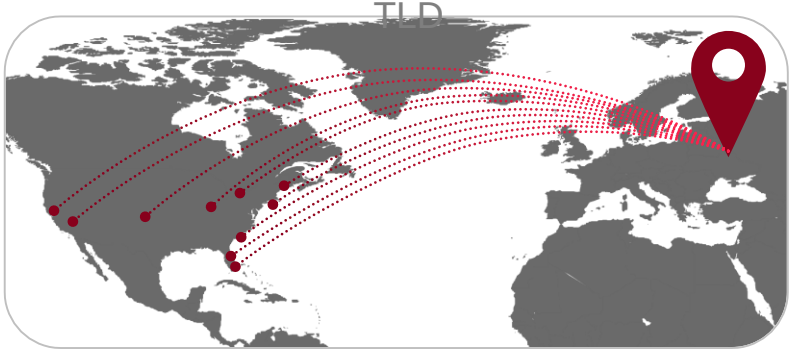
IP ГЕО-локационный анализ

Хостится в более чем 28+ странах

ХОСТ ИНФРАСТРУКТУРА

Расположение сервера IP адреса связанные с доменом

Только заказчики из US связываются с .RU TLD



DNS ЗАПРОШИВАЮЩИЕ ХОСТЫ

Расположение сетевые и вне-сетевые IP адреса запрашивающих домен

Модель языкового моделирования (NLPRank)

Идентификация вредоносных доменов и направленных C2 или фишинговых доменов

1

Читаем APT отчет

2

Шаблоны в доменах используемых для атаки

- Подлог домена использован для спуфинга
- Частые имена брендов и слово “update”
- Примеры:
  update-java[.]net
  adobe-update[.]net

3

Проверили данные и подтвердили опасения

- Словарные слова и имена компаний слитно
- Измененные строчные буквы # на символы для сокрытия
- Домены хостятся на ASNах не ассоциированных с компанией
- Изменённые отпечатки WEB страниц

4

Построили модель и продолжаем подстройку

Обнаружение доменов для фрода:

1linkedin.net

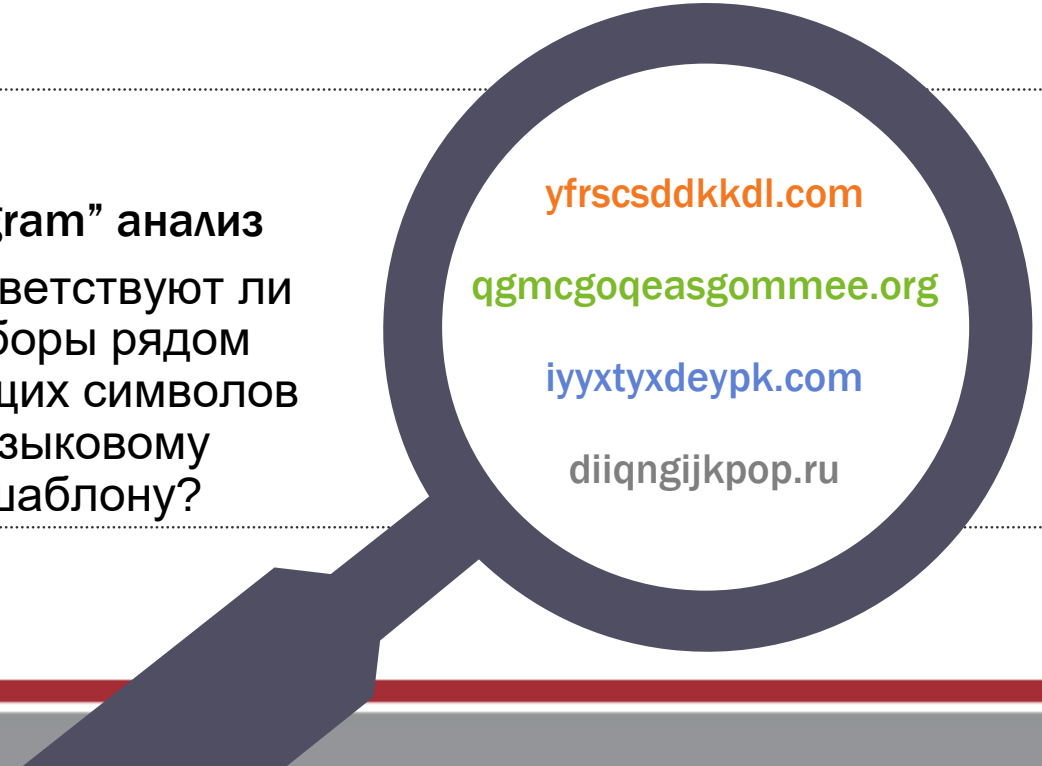
linkedin.com

Обнаружение алгоритмов генерации доменов DGA

Domain Generation Algorithms: техника избежания задания статичных имен доменов в вредоносе

“N-gram” анализ

Соответствуют ли наборы рядом стоящих символов языковому шаблону?

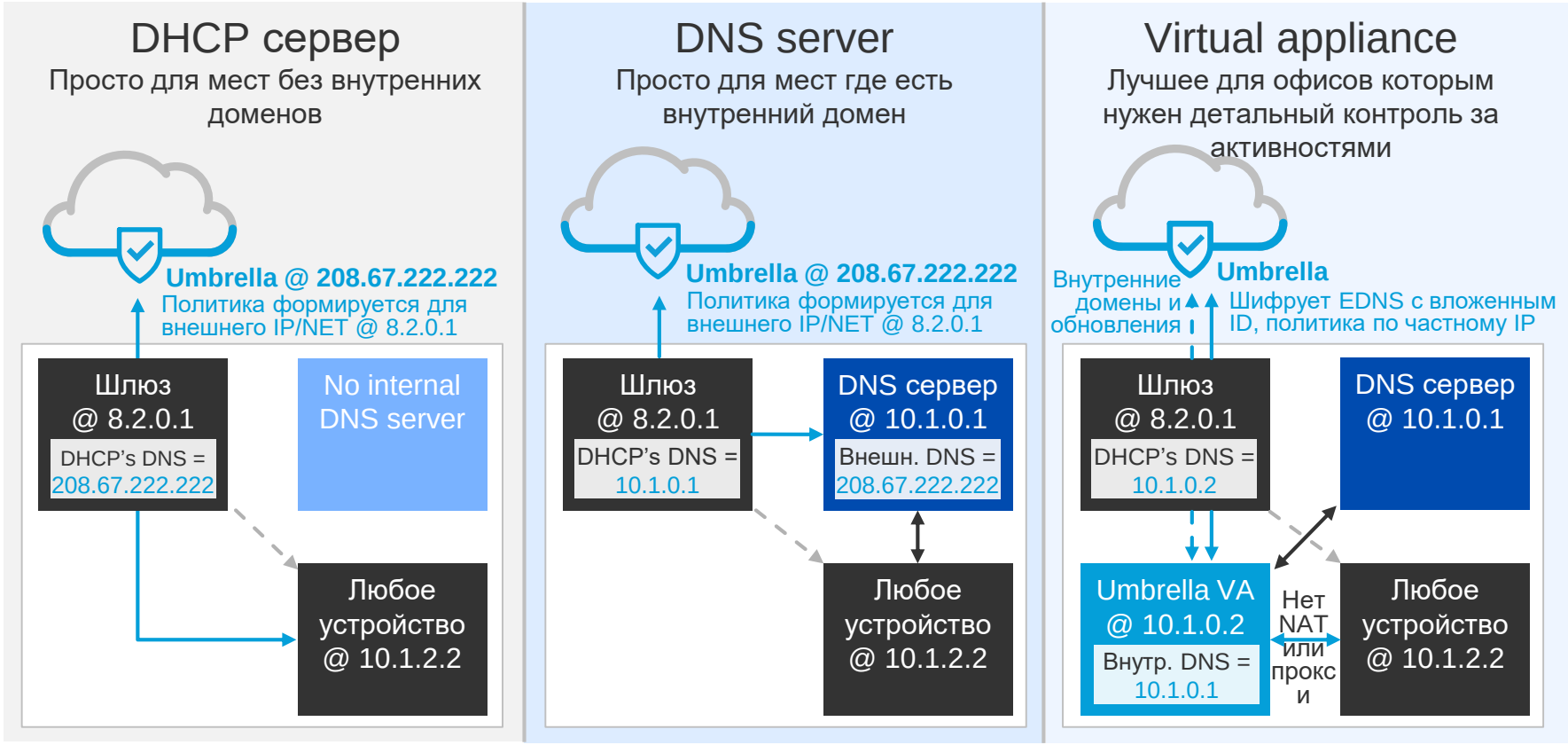


Анализ энтропии

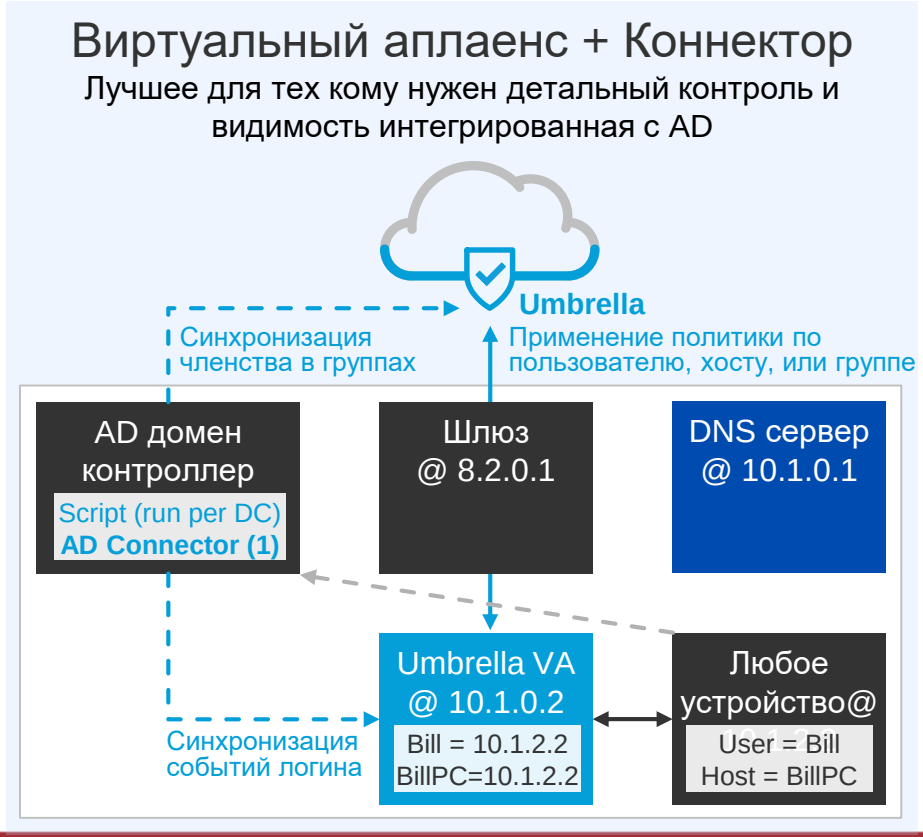
Не выглядит ли распределение символов случайным?

Сценарии развертывания

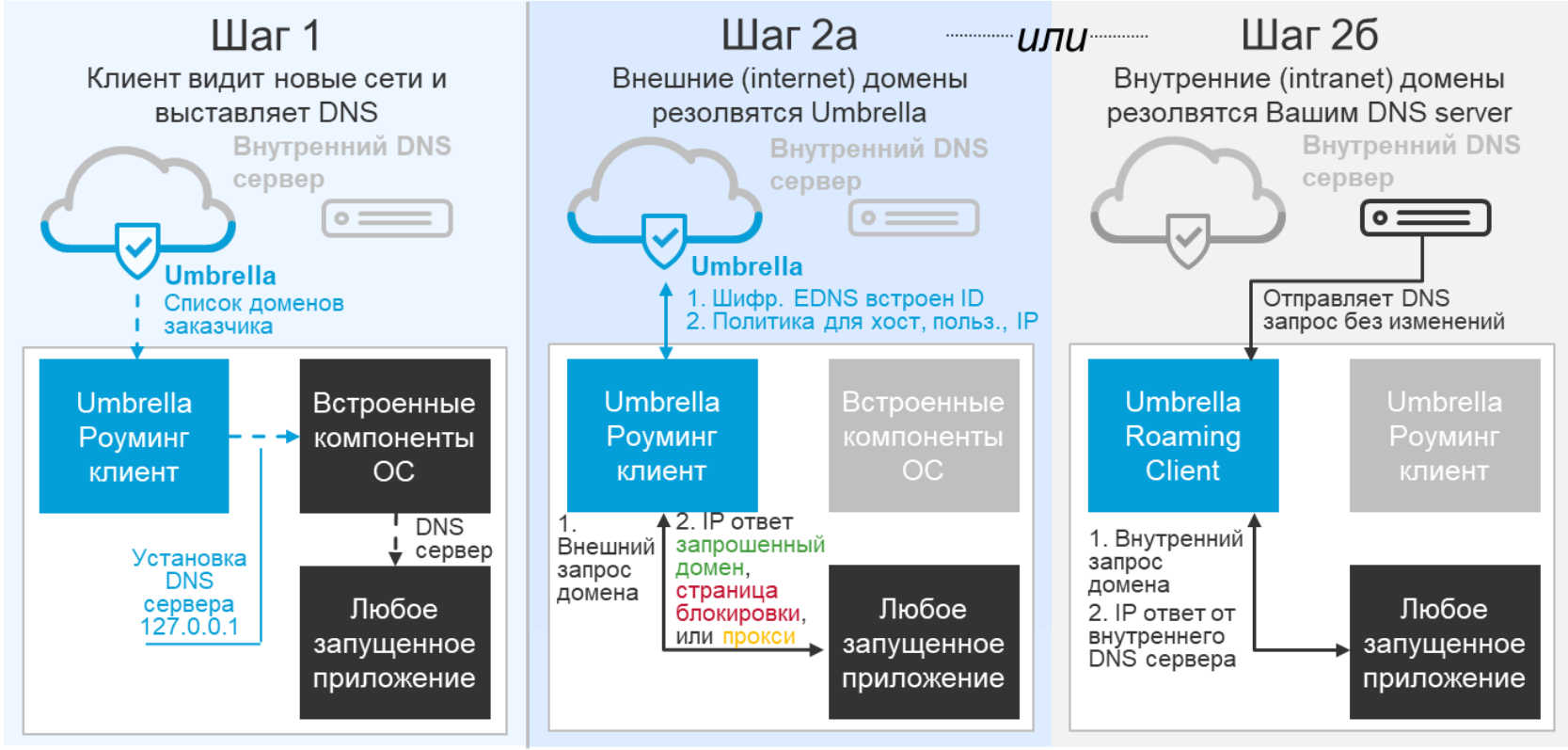
Внутри сети: Просто указать внешний DNS без клиентов



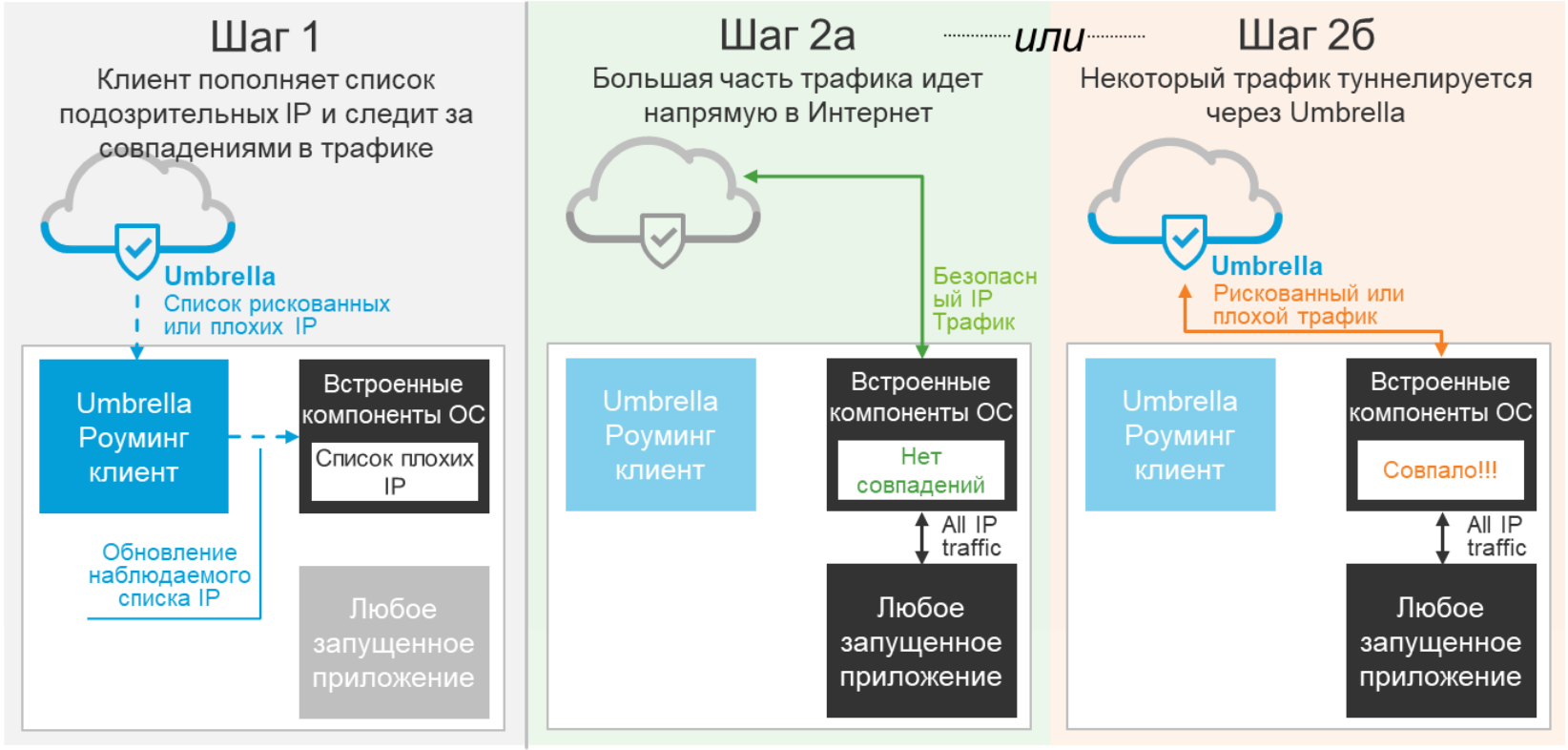
Внутри сети: Добавление политик по пользователям без агентов



Роуминг: Защита уровня DNS с Umbrella роуминг клиентом



Роуминг: добавление уровня фильтрации без полного VPN туннелирования

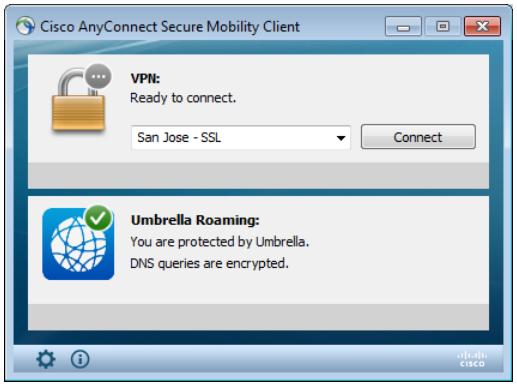


Cisco AnyConnect модуль

Защита мобильных хостов без доп. агентов

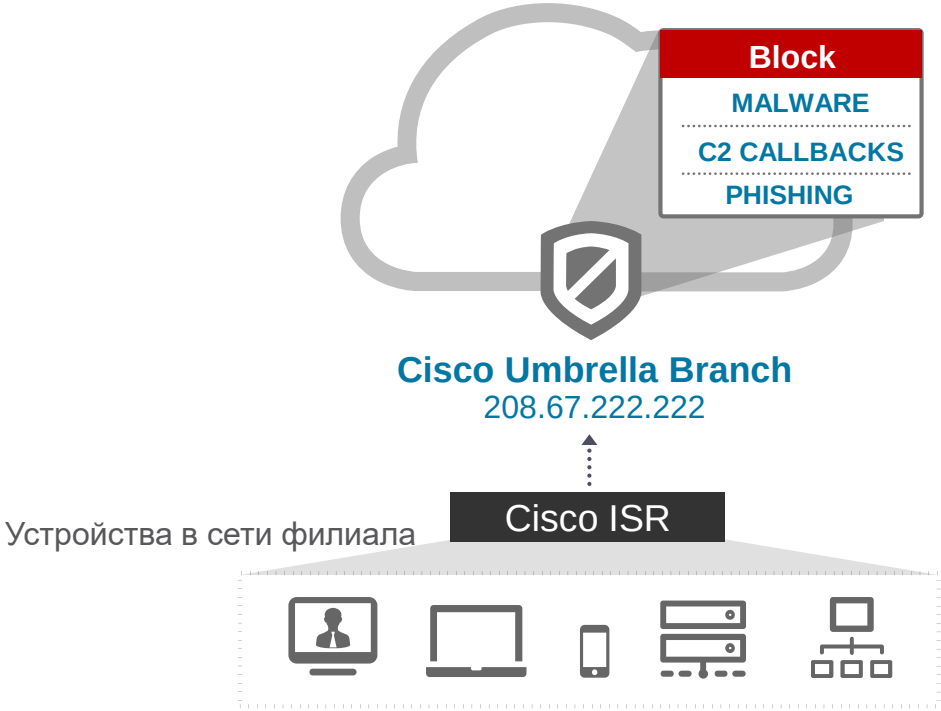
1. Включить модуль роуминга
2. Настроить политику роуминга в Umbrella
3. Увидеть интернет активности и детальные логи для разбора инцидентов

208.67.222.222



Cisco Umbrella Branch

Ваш первый уровень защиты для филиала



- Видимость и фильтрация на уровне DNS
- Блокировка запросов к вредоносным доменам и IP
- Контентная фильтрация для гостей и корпоративных пользователей

Спасибо
за внимание!