



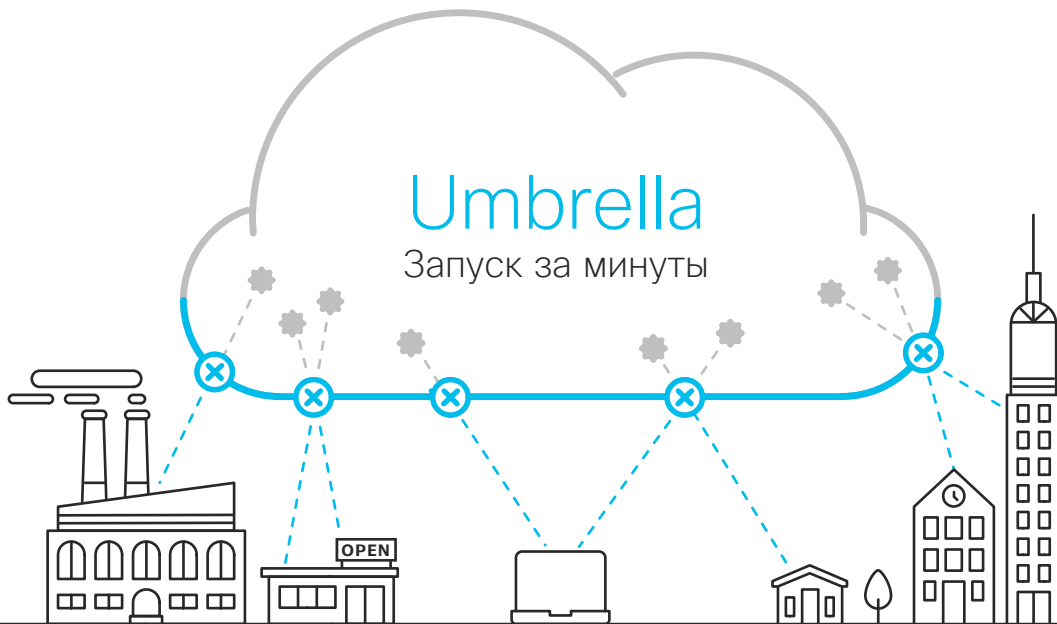
Cisco Umbrella

Упрощаем безопасность

- Один маленький клик
- Огромный труд тысяч сотрудников

Umbrella для Заказчика выглядит просто

- 1 Подпишитесь
- 2 Укажите ваш DNS
- 3 ВСЕ!!!



Давайте посмотрим, что там?
За линией защиты Umbrella

Наш взгляд на Internet

200млрд

запросов в день

100млн

активных
пользователей
ежедневно

225тыс

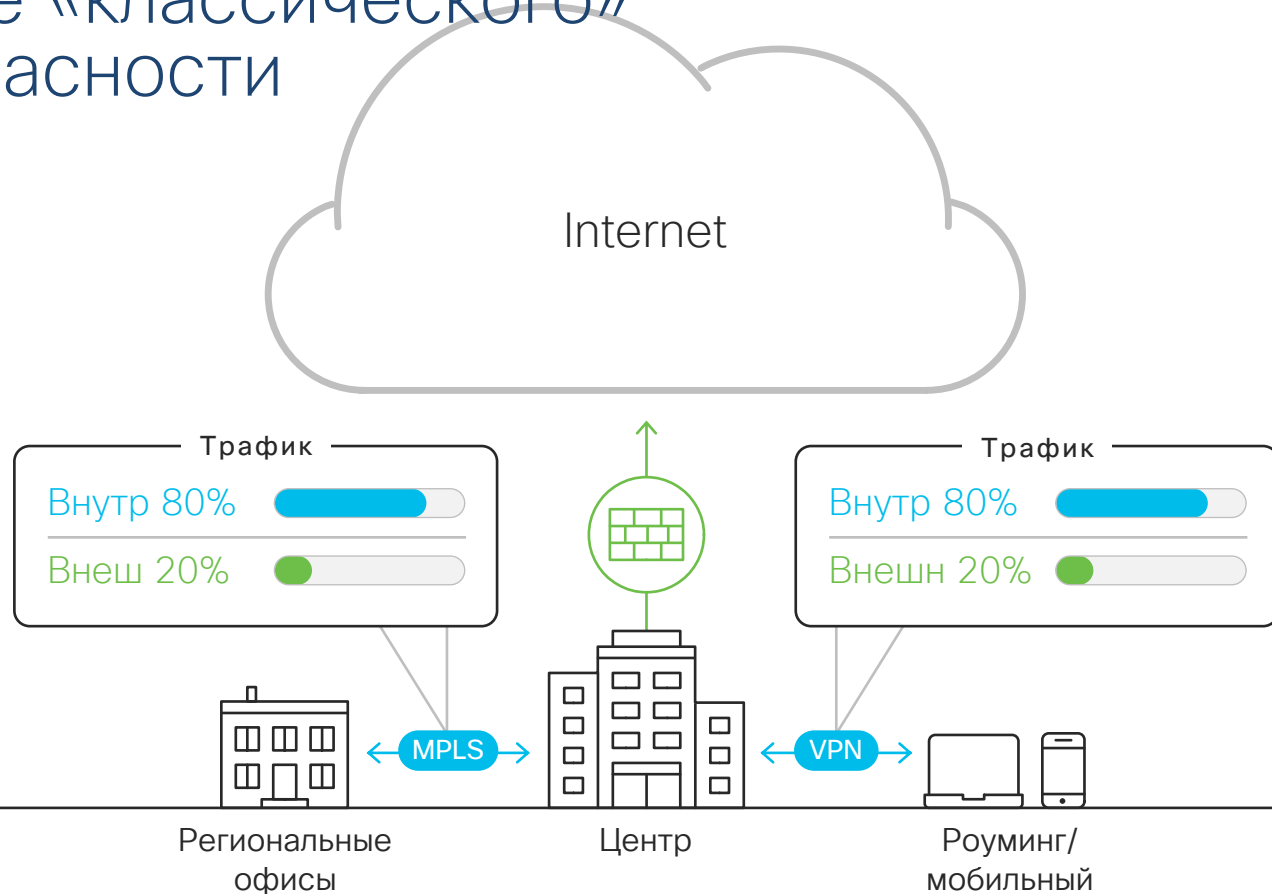
корпоративных
клиентов

190+

стран



Устаревание «классического» стека безопасности



Изменения типа и путей трафика

Проблемы:

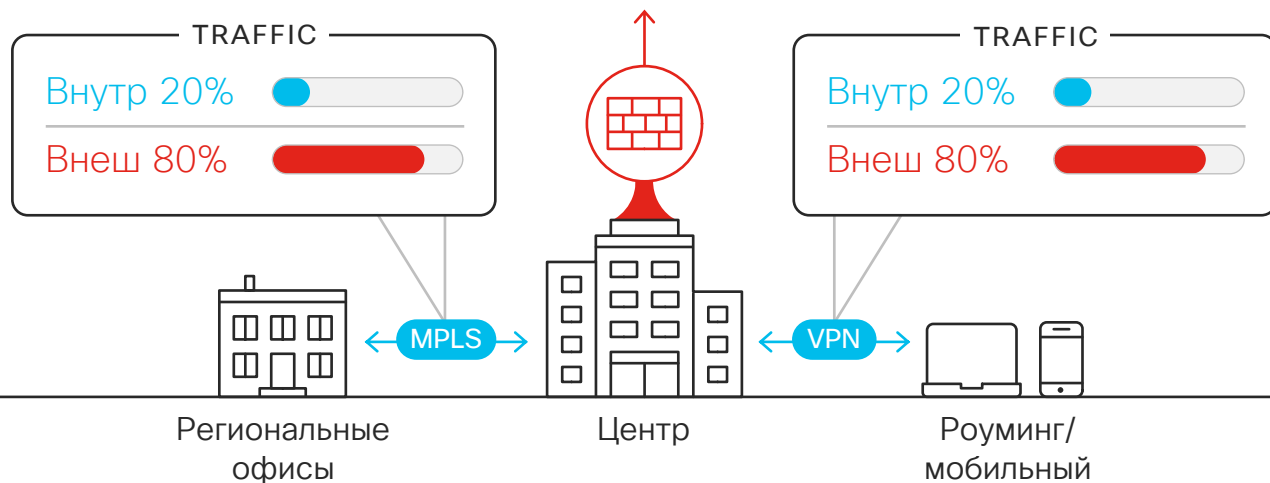
Стоимость

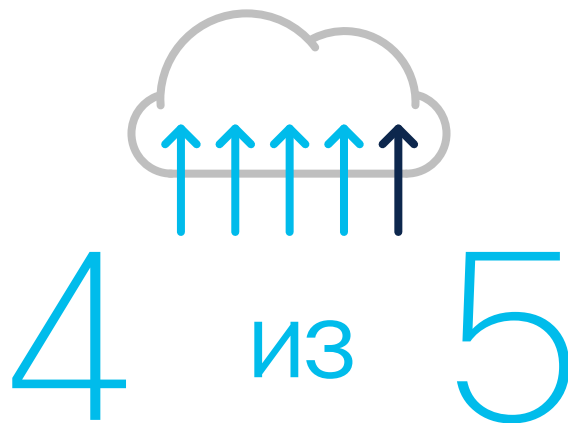
Производительность

вендоров/
инструментов

Интеграция

Обслуживание





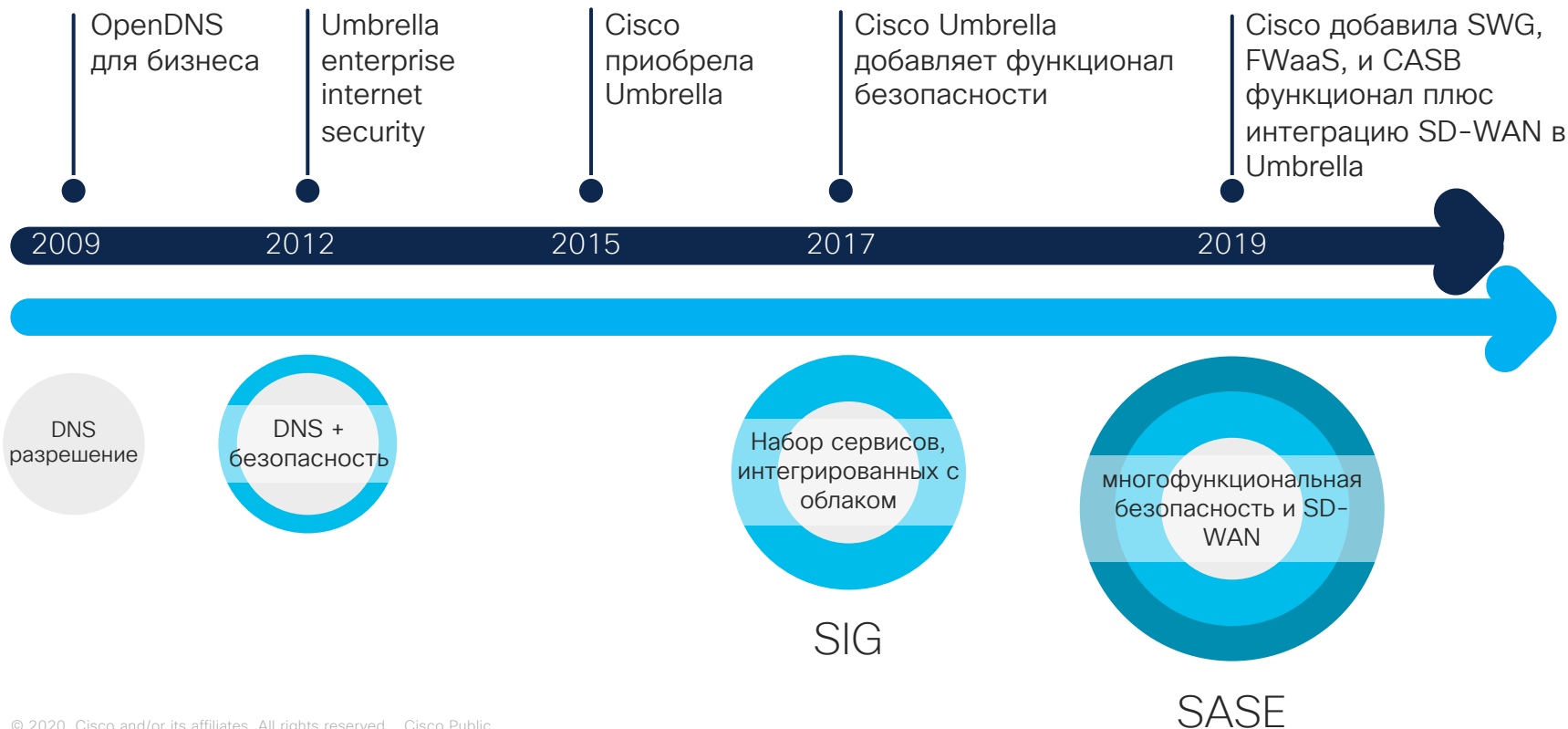
организаций переходят на прямой доступ
Direct Internet Access (DIA)

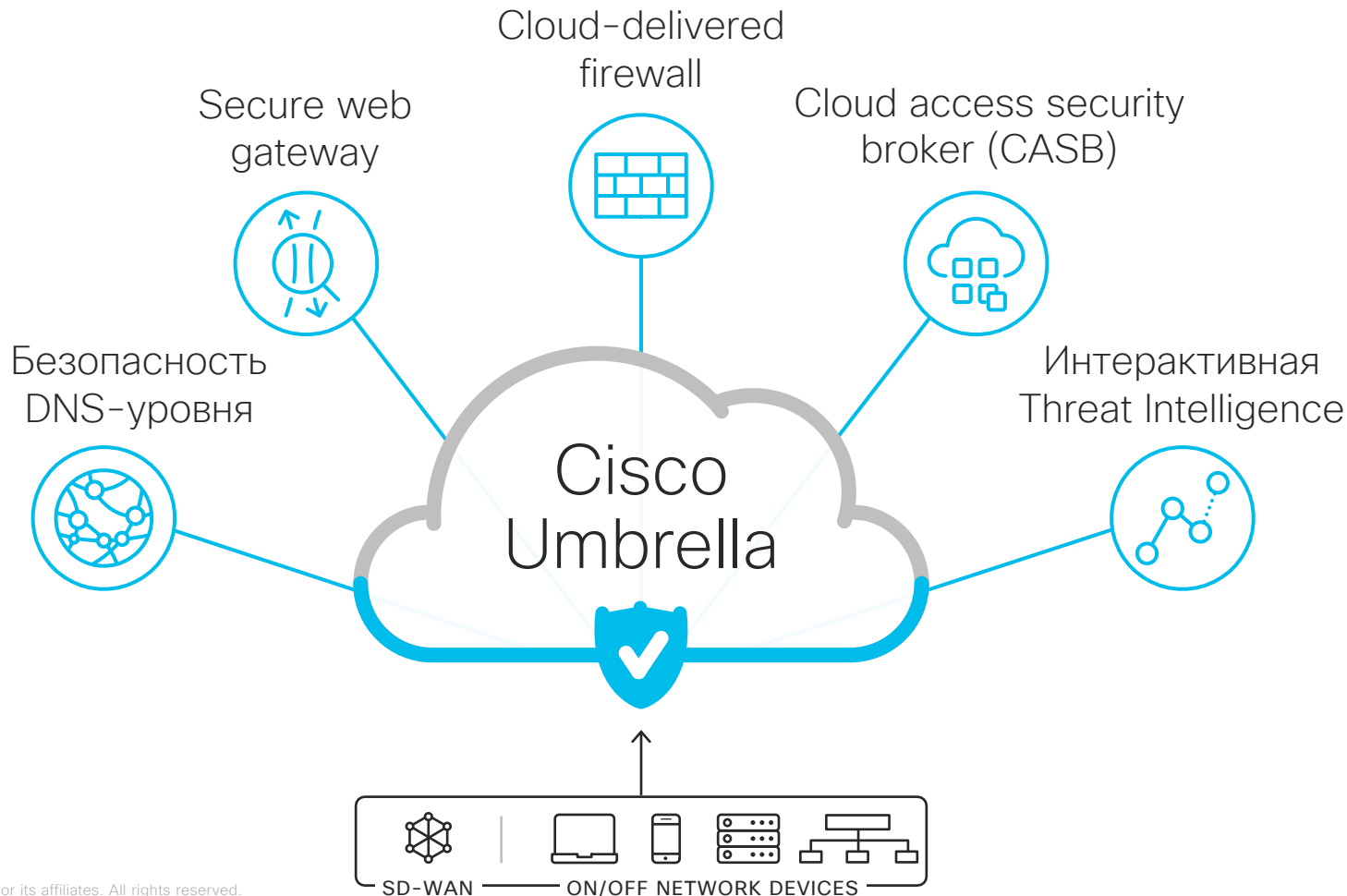
Безопасность должна подстраиваться под новый
ПОДХОД

Source: ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019

Обзор продукта

Эволюция Cisco Umbrella





Cisco Umbrella

Безопасное подключение к Internet, везде



Видимость

В сети и вне ее

Весь трафик Internet и Web

Все приложения

Все устройства

SSL расшифровка



Защита

Безопасность DNS уровня

Веб инспекция

Инспекция файлов

Песочница

Доступ к Threat intel



Контроль

Списки URL block/allow

Правила портов/протоколов

Фильтр контента

Блокировка приложений

Детальный контроль
приложений

Поддерживается Cisco Talos threat intelligence

DNS безопасность

Краткое введение в DNS



Регистратор доменов

Сопоставляет записи имен к адресам в “телефонной книге”



Авторитативный DNS

Владеет и публикует “телефонную книгу”



Рекурсивный DNS

Ищет и хранит адреса для каждого имени



Кто проводит разрешение Ваших DNS запросов?

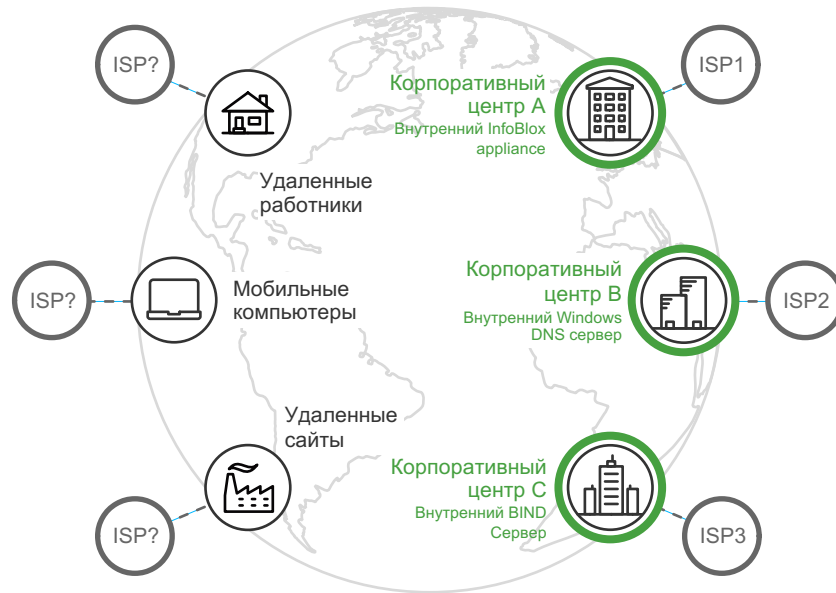
Проблемы

Множество Интернет провайдеров

Прямое подключение филиальных офисов

Пользователи забывают всегда включать VPN

Различные форматы DNS логов



○ Рекурсивный DNS для Интернет доменов

○ Авторитативный DNS для интранет доменов

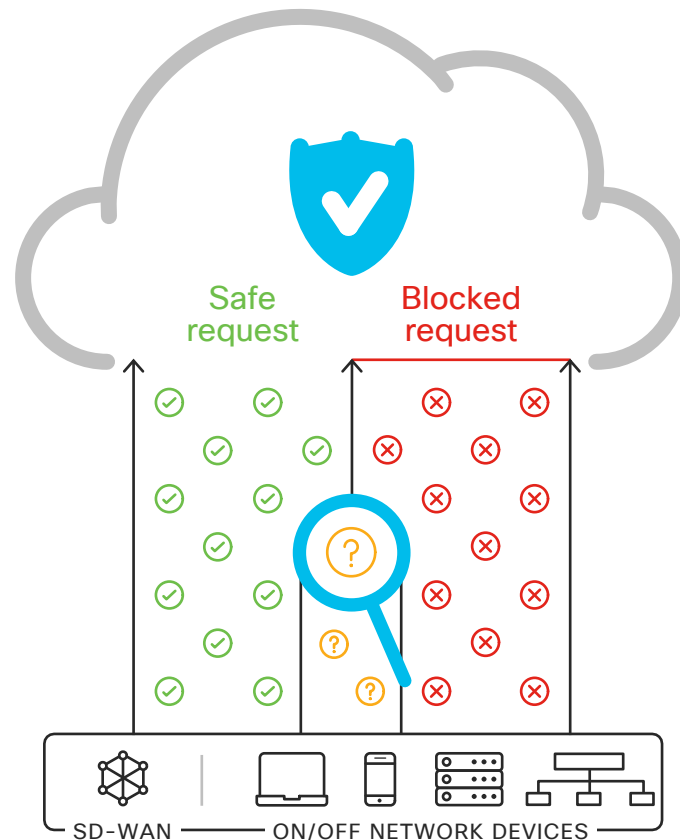
Безопасность DNS уровня

Первая линия защиты Internet-доступа

Развертывание за минуты для всей сети

Блокировка доменов, ассоциированных с malware, фишингом, вызовами command and control из сети и вне ее

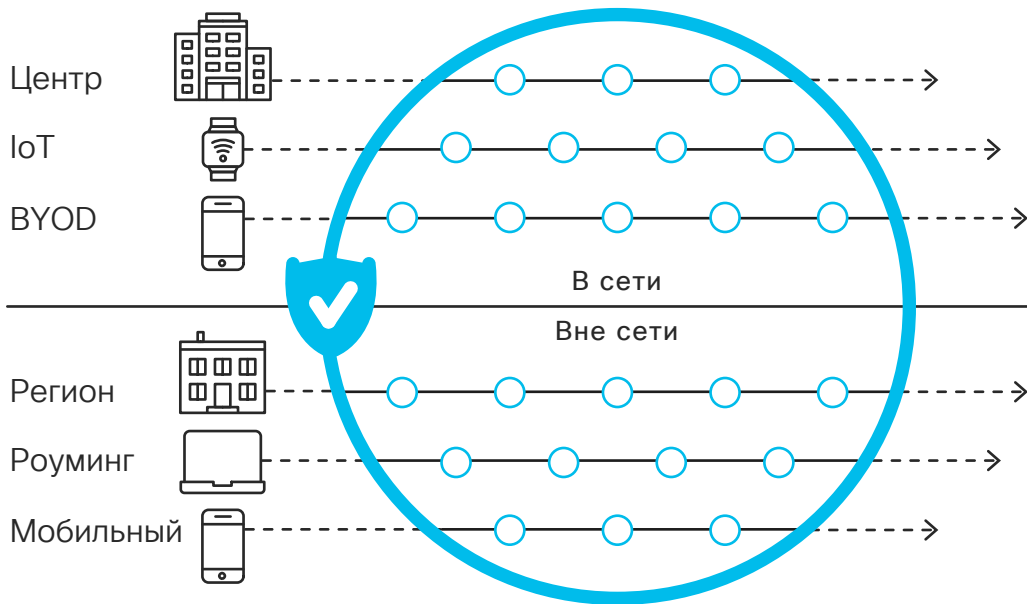
Более 95% malware использует DNS для коммуникации, что позволяет остановить распространение на самой ранней стадии и сдерживание malware, если оно уже попало внутрь



DNS безопасность

Видимость и защита любой активности, везде

Umbrella



Все офисные локации

Любое устройство в сети

Роуминг компьютеры и
мобильные устройства

Каждый порт и протокол

Встроено в основу Internet

Назначение

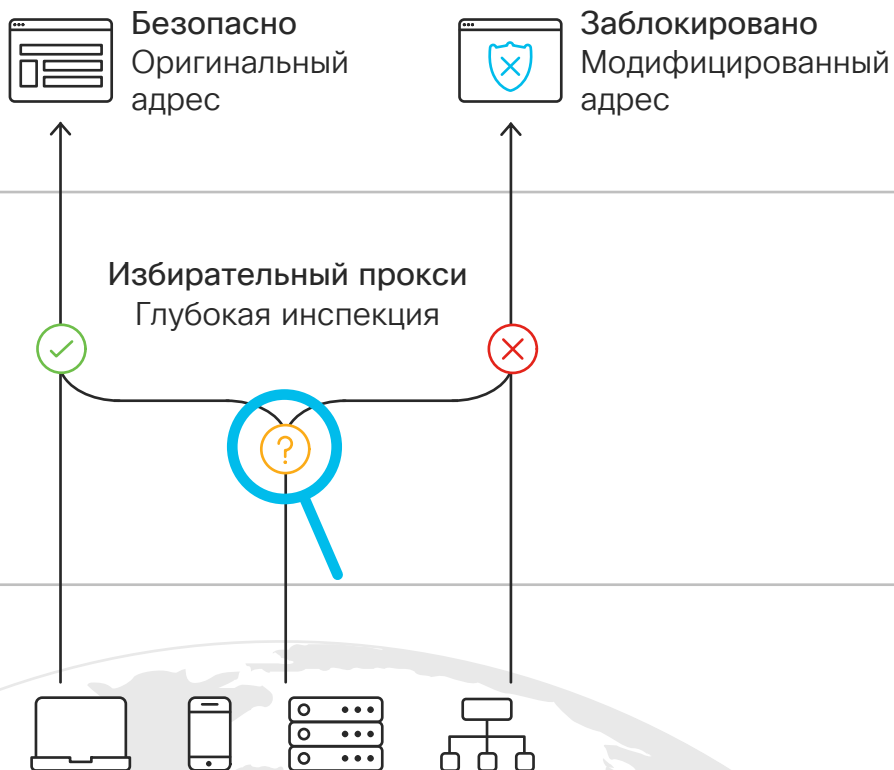
Оригинальное назначение или страница блокировки

Контроли безопасности

- Правила DNS и IP
- Инспекция рискованных доменов через прокси
- Доступна SSL расшифровка

Internet traffic

В сети и вне ее



Информация чтобы увидеть атаки перед запуском

Данные

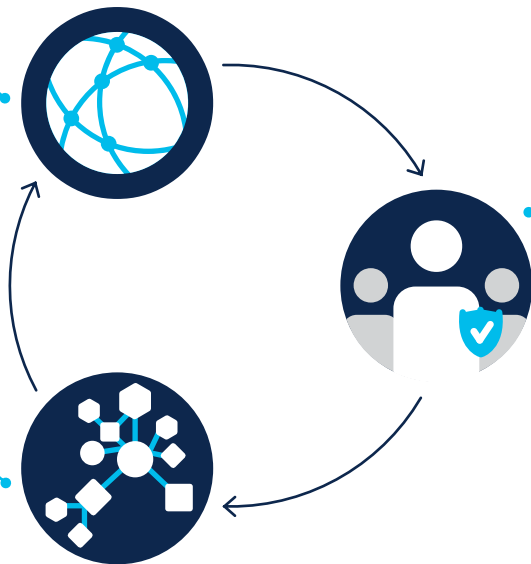
- Данные Umbrella DNS – 200 млрд запросов в день
- Данные Cisco Talos о вредносных доменах, IP, и URL

Модели

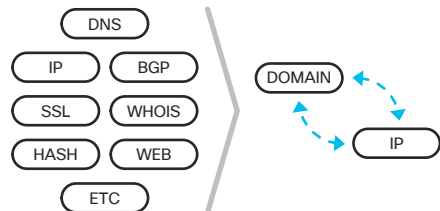
- Десятки моделей постоянно анализируют миллионы событий в секунду
- Автоматически обнаруживает malware, ransomware, другие угрозы

Люди

- Исследователи безопасности
- Построение моделей, которые автоматически классифицируют и оценивают домены и IP



Многоуровневая информация об угрозах



Лексическая ●

Живое пресказание DGA



Детектор аномалий ●

Новые домены

Модель ранжирования пиков



Предиктивный IP ●

Предиктивный мониторинг IP пространства



Графы ●

Модель совпадений



Botnet ●●●



Crimeware ●●●



Exploit Kit ●●●



Phishing ●●●



Ransomware ●●●



Spam ●●●



Trojan ●●●

Umbrella

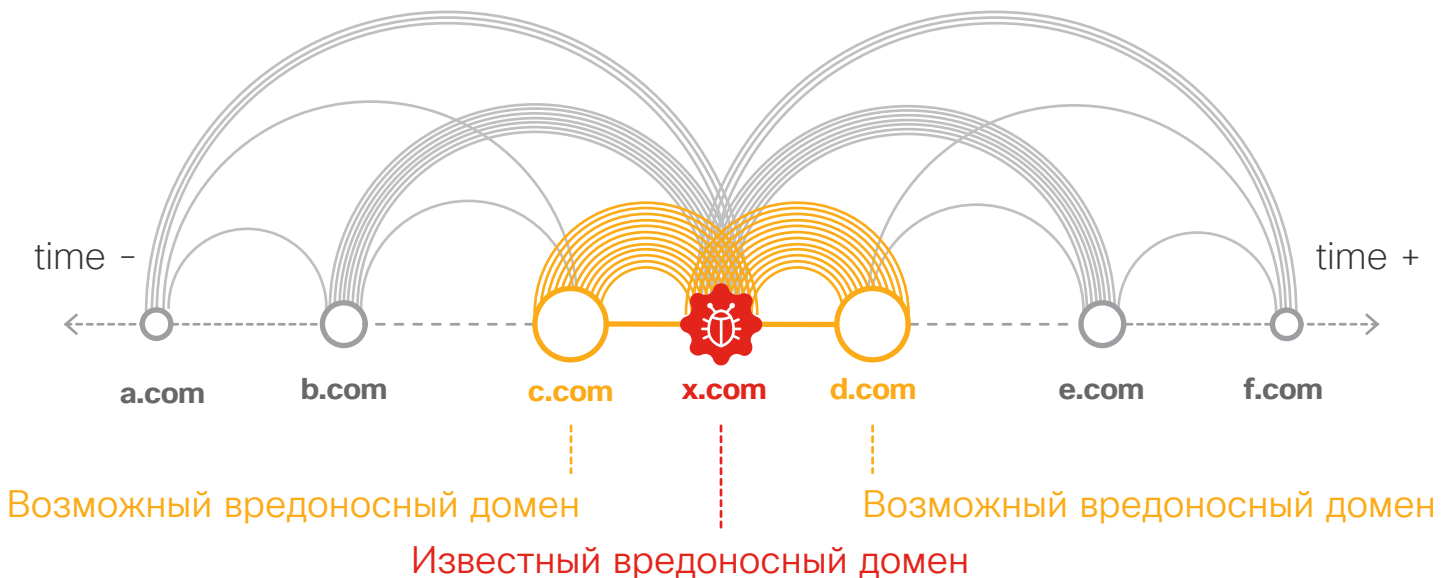


Investigate



Модель совпадений

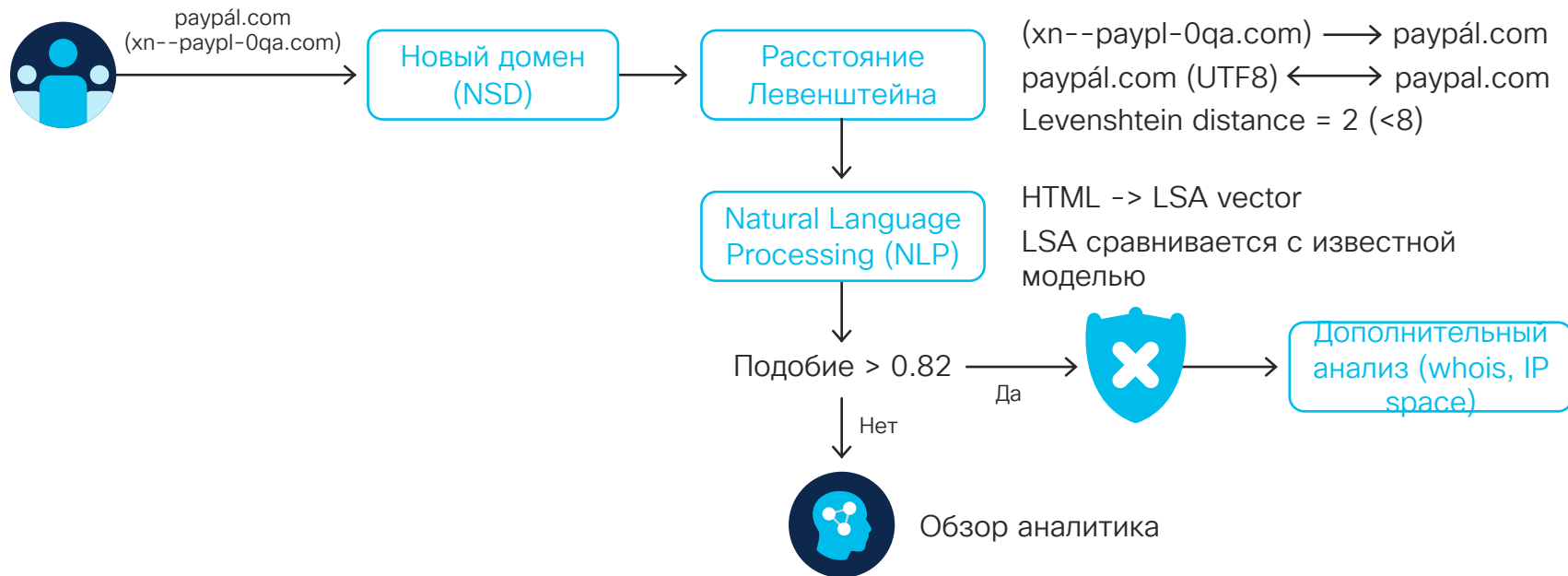
Обвинение по следствию



Совпадение доменов означает, что статистически существенное количество пользователей одновременно запросило два домена в короткое время

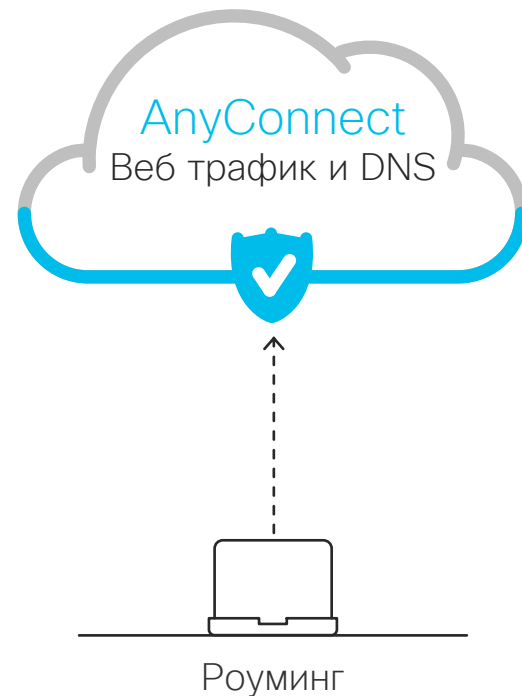
Одна из наших статистических моделей – Punycode

Что мы делаем?

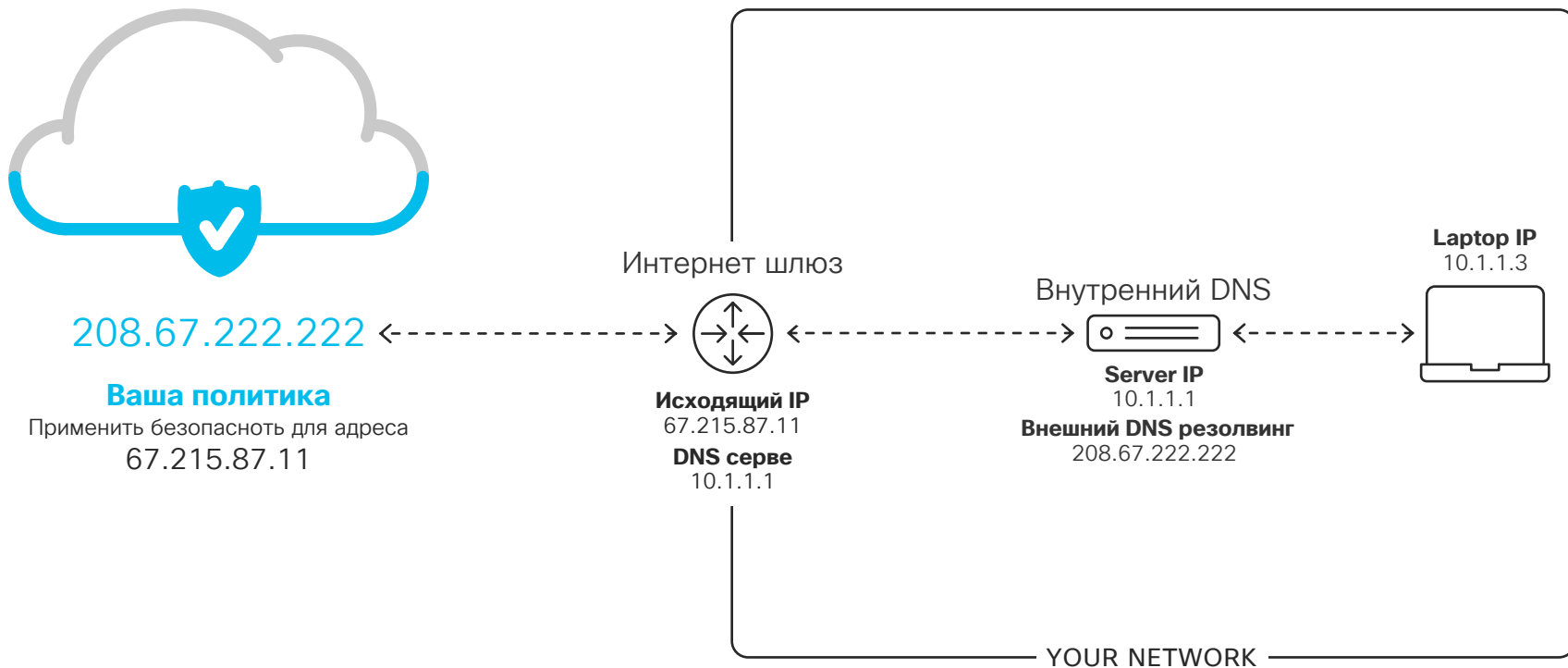


Подключения, интеграции
и журналирование

Гибкие методы подключения



Защита устройств внутри сети с помощью DNS



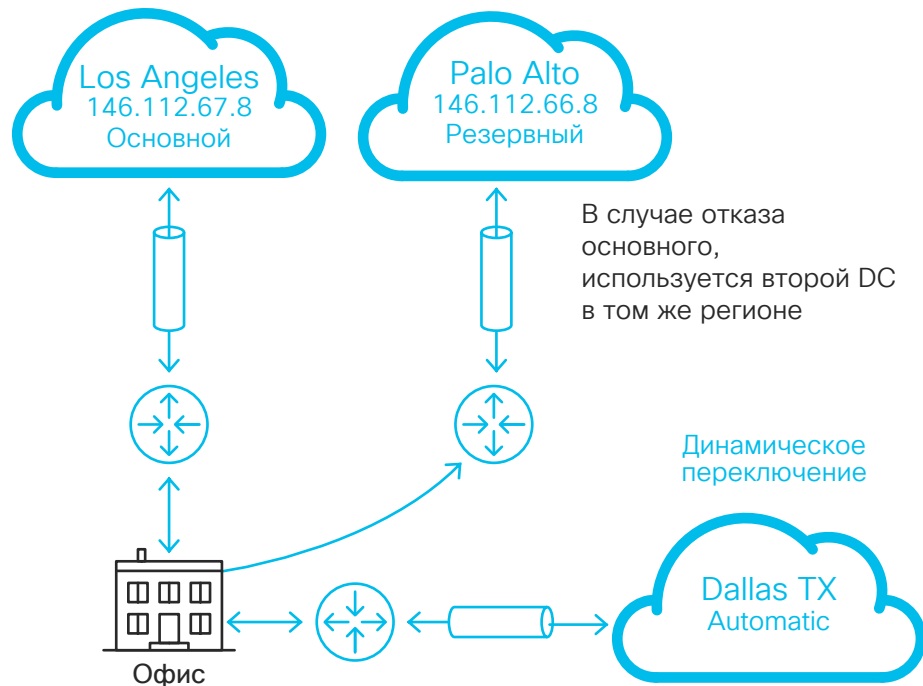
Производительность и отказоустойчивость туннелей

Емкость IPSEC

- >250 мбит/туннель в каждом направлении с будущим развитием для увеличения емкости
- Для большей емкости можно использовать несколько туннелей

Доступность

- Конфигурирование основного и резервного
- Переключение на резерв и на DR сайт автоматическое
- Если настроен только основной туннель, осуществляется переключение на резервный.
- Использует anycast и IKE DPD.



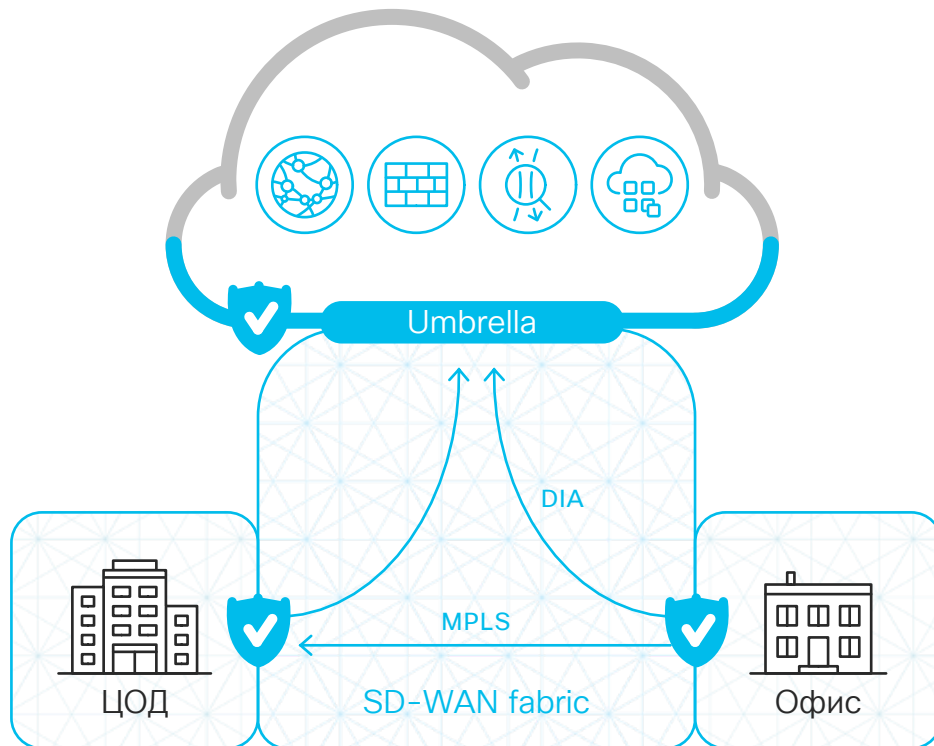
Интеграция Cisco SD-WAN

Простая, эффективная безопасность для Cisco SD-WAN (работа на Viptela)

Автонастройка и развертывание
высокодоступных туннелей в
несколько кликов

По умолчанию отказоустойчивость
между регионами

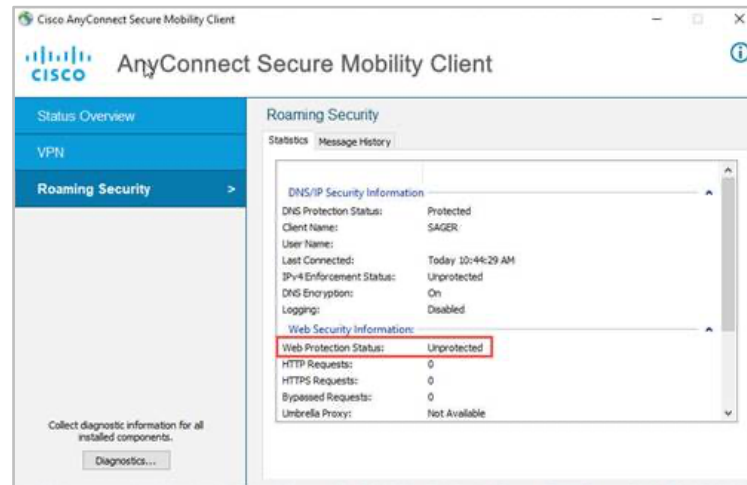
Глубокая инспекция и контроль с
облачным Firewall и Secure Web
Gateway



Клиент AnyConnect

Поддержка DNS и SWG

- AnyConnect может использоваться по всей организации
- Текущие AnyConnect клиенты могут расширить поддержку, право на использования AC включено в лицензию
- Сервисы Umbrella DNS и Web Gateway services сосуществуют
- Защита активов в сети и вне ее
- Простая и согласованная атрибуция пользователей

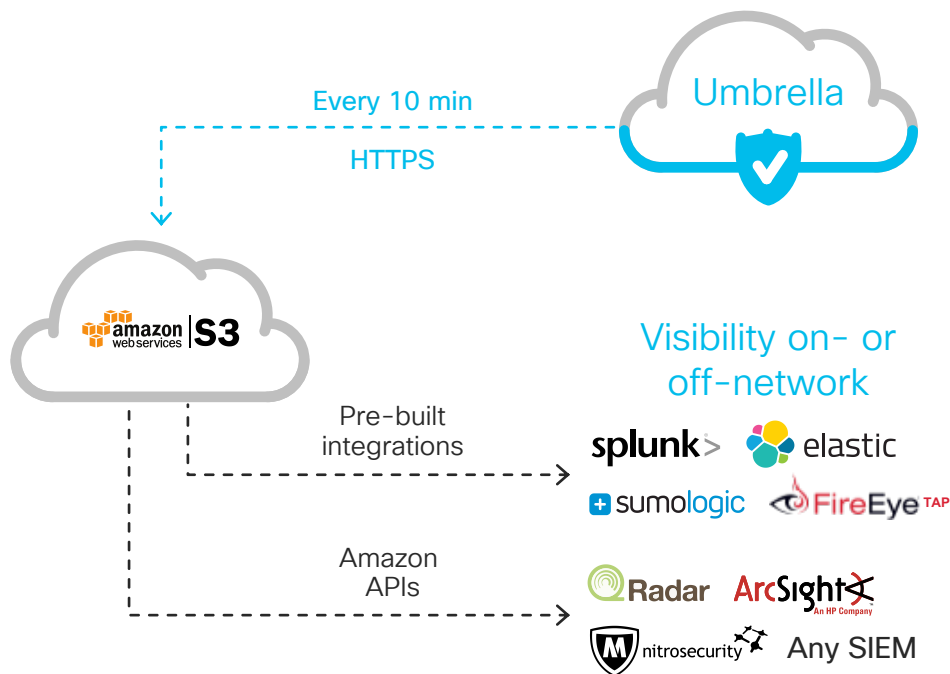


Не требуется identity



Поддержка Windows и Mac

Хранение журналов на Amazon S3



S3 преимущества

- Отказоустойчивое и шифрованное хранилище
- Встроенная интеграция с SIEM / аналитикой журналов
- Использование собственных или Cisco хранилищ
- Централизованные журналы S3

Доступно хранилище в EU

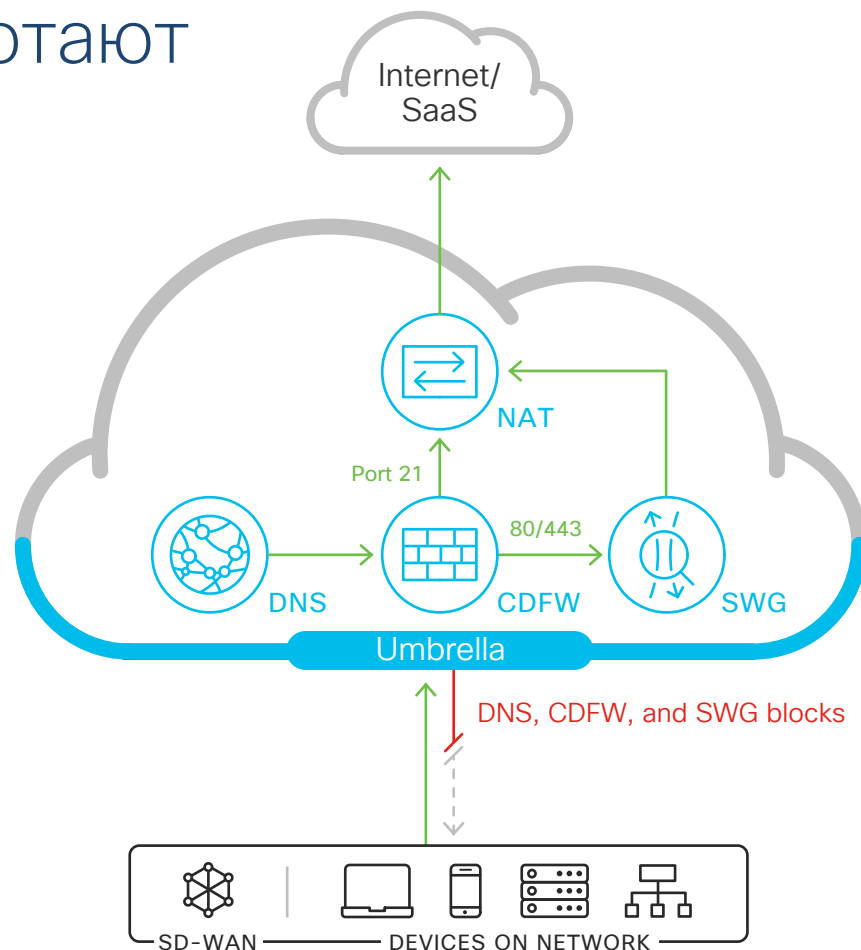
- Упрощает регуляторику
- Хранение данных в EU

Политики, которые работают вместе

Безопасность уровня: Во первых блокируются домены, которые ассоциированы с malware или политикой

Cloud-delivered firewall (CDFW): Затем проверка правил IP, порт, протокол

Secure web gateway (SWG): В конце проверяется трафик Web на предмет наличия malware или нарушений политик



Secure Web Gateway

Umbrella SWG



Защита от вирусів и malware

- Сканирование и обнаружение широкого диапазона malware и вирусов для того, чтобы избежать инфицирования и остановить атаки

- Umbrella secure web gateway с Advanced Malware Protection (AMP) и сторонними антивирусными движками

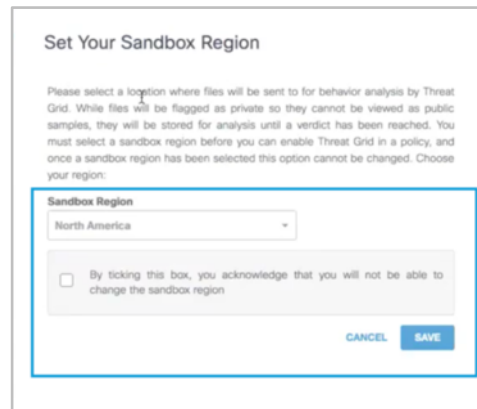
- Отчеты активности показывают детали каждого обнаруженного события

[illegible]

Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action	Categories
Jumper	google-profiles.com	Jumper		54.183.40.98	Blocked	Malware, Parked Domains
Jumper	11bmasdtp9ifjaposdfjhgosurijfaewrrwegwea.com	Jumper		54.183.40.98	Blocked	Malware, Computer Security
Jumper	google-profiles.com	Jumper		54.183.40.98	Blocked	Malware, Parked Domains
Jumper	vpnoverdns.com	Jumper		54.183.40.98	Blocked	DNS Tunneling VPN, Software/Tec

Песочница Threat Grid

- Возможность обнаружить скрытые угрозы в загружаемых файлах
- Набор новых или рискованных файлов помещаются в песочницу и проверяются на предмет вредоносной активности или контента
 - Для файлов публикуются предупреждения
 - Обновляется информация Umbrella threat intelligence



Regions:
Europe or
North America

SIG Essentials имеет ограничение 200 файлов в день для Threat Grid.
Для увеличения необходимо приобретение еще одного SKU.

Анализ файлов Threat Grid

Инспекция Threat Grid:

- Файлы, которые прошли через антивирус и сканирование AMP
- Неизвестные файлы, которые имеют атрибуты для помещения в песочницу

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 < >					

Детальный контроль приложений

Reporting / Additional Reports
App Discovery

Dashboard

Search for App / Vendor Filter by Identity

UNREVIEWED (3197) UNDER AUDIT (12)

All Apps (3,287 Found)

Application

Dropbox Cloud Storage

Netflix Media

Amplitude Business Intelligence

Amazon E-Commerce

Control Dropbox

Select which settings should block or allow this application

Application Settings (3 selected of 3 total)

- ☒ Default Settings
Applied in: Global Branch Policy, Security Only ...
Block
- ☒ HR App Restrictive
Applied in: High Restrict Group
Block Uploads
- ☒ Global App Allow
Applied in: Global Allow Policy
Allow

☐ Label application as

For more configuration options, go to [Application Settings](#) in the policy section.

CANCEL SAVE

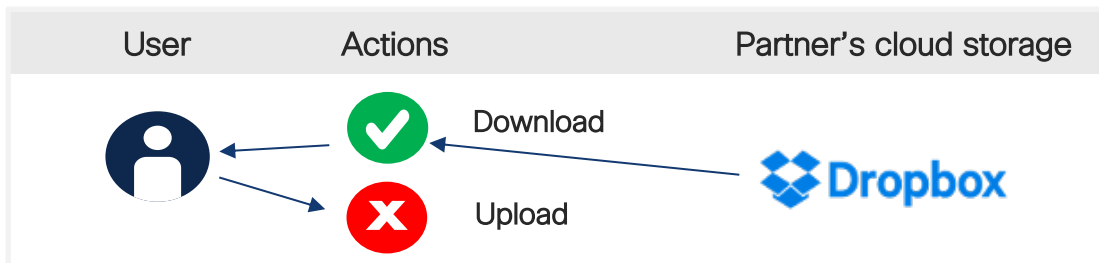
OpenDNS Dashboard

ALL APPS (3287)

Total Traffic	Outbound Traffic	Inbound Traffic	Label
51 MB total traffic 4 MB 48 MB	48 MB	4 MB	Under Audit Edit app controls
3 MB total traffic 88 KB 3 MB	3 MB	88 KB	Unreviewed Edit app controls
157 KB total traffic 86 KB 71 KB	71 KB	86 KB	Unreviewed
6 MB total traffic 72 KB	6 MB	72 KB	Unreviewed Control this app

Детальный контроль для приложений SaaS

- Блокировка постов в СОЦСЕТИ
- Блокировка аттачей в вебмейл
- Блокировка загрузок на облачные хранилища, офисные приложения, приложения медиа и т.д.



Расшифровка SSL/HTTPS в облаке

- Видимость и набор правил безопасности для все увеличивающегося объема зашифрованного веб трафика
- Расшифровка, отчетность и инспекция зашифрованного веб трафика и файлов
 - Нет расходов на железо
 - Нет проблем с масштабированием
 - Возможность избирательной расшифровки

The screenshot shows the 'HTTPS Inspection' configuration page in the Umbrella cloud console. It includes a toggle to 'Enable HTTPS Inspection' with a descriptive paragraph. Below, there are two sections for exemptions: 'Privacy categories' with a dropdown menu and a list of selected categories (Financial Institutions, Health and Fitness, Social Networking, Webmail), and 'Domains' with an 'ADD' button and a 'No Domains' message.

HTTPS Inspection

Configure how Umbrella should handle HTTPS traffic. [See HTTPS Inspection](#)

☒ Enable HTTPS Inspection

HTTPS traffic is intercepted and decrypted to provide security and policy enforcement at the URL layer, and visibility into the URL path. By default, HTTPS inspection attempts to decrypt all HTTPS traffic. For any HTTPS traffic that should not be decrypted, create a bypass inspection group.

Add domains and select categories you want to exempt from HTTPS inspection:

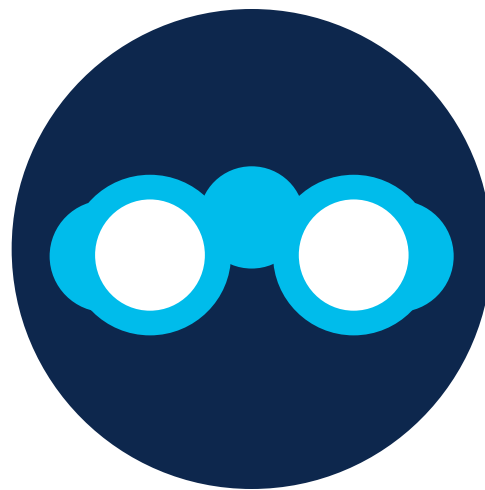
Privacy categories ▾

4 Categories Selected ADD	0 Domains ADD
Financial Institutions	
Health and Fitness	
Social Networking	
Webmail	
	No Domains

Использование AMP, Threat Grid и Umbrella Threat Intelligence для защиты зашифрованного трафика

Требования к видимости HTTPS трафика и URL

- Детальный контроль приложений
- Блокировка URL категорий
- Полная видимость URL
- AV сканирование, репутация и песочница
- Отображение страниц блокировки
- Практически все, что нельзя сделать на dns уровне



Контроль типов файлов– SWG

The screenshot displays the Cisco Umbrella settings interface. On the left, a list of security settings includes:

- 1 Identity Affected** (1 Network) with an [Edit Identity](#) link.
- No Security Settings Applied** with an [Enable](#) link.
- No Content Settings Applied** with an [Enable](#) link.
- No Application Settings Applied** with an [Enable](#) link.

On the right, additional settings are shown:

- 0 Destination List Enforced** with an [Enable](#) link.
- File Analysis Enabled** (File Inspection Enabled, Threat Grid Malware Analysis Not Enabled) with an [Edit](#) link.
- Umbrella Default Block Page Applied** with [Edit](#) and [Preview Block Page](#) links.
- File Type Control Enabled** (gif, jpeg, jpg, ai and 8 more will be blocked.) with [Edit](#) and [Disable](#) links. This section is highlighted with a blue border and a line pointing to the 'Требуется инспекция HTTPS.' text.

At the bottom, the **ADVANCED SETTINGS** section is expanded, showing the **HTTPS Inspection** toggle switch, which is currently turned on. A line points from this toggle to the 'Требуется инспекция HTTPS.' text.

Требуется инспекция HTTPS.

Контроль типов файлов – категории и типы файлов

Edit File Control

Search for and apply policy controls for downloaded file types.

Search file types

All Groups

☐  Audio	7 >
☐  Compressed files	13 >
☐  Data and database	10 >
☐  Disc and media files	4 >
☐  Documents	10 >
☐  Executables	19 >
☐  Images	12 >
☐  System related files	9 >
☐  Videos	23 >



Edit File Control

Search for and apply policy controls for downloaded file types.

Search file types

All Groups / Audio

☐ aif
☐ cda
☐ mid
☐ mp3
☐ wav
☐ wma
☐ wpl

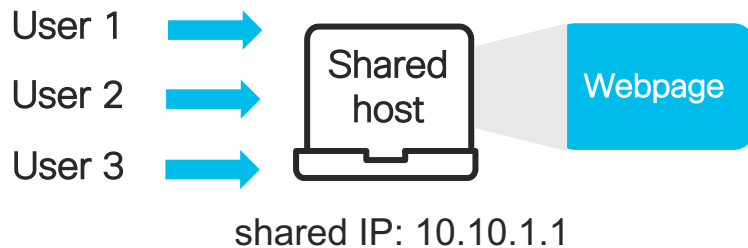
Аттрибуция и аутентификация пользователей

- Security Assertion Markup Language (SAML)
 - Service Provider (SP) – Umbrella
 - Identity Provider (IdP) – сторонний
- Cookie суррогаты
 - Требуется инспекция HTTPS
- Подразумевается поддержка браузеров, может не работать для «десктопных приложений»



Несколько пользователей из одного хоста

- VA с AD коннектором может только поддерживать одного пользователя на IP адрес
- У Citrix/TS множество пользователей подключаются из одного IP
- Secure web gateway использует SAML аутентификацию с суррогатами cookie
- Суррогаты Cookie поддерживают несколько пользователей из одного IP
- Поддержка виртуальных десктопов (Citrix/TS) и браузеров (Citrix)



SWG пользователи и группы

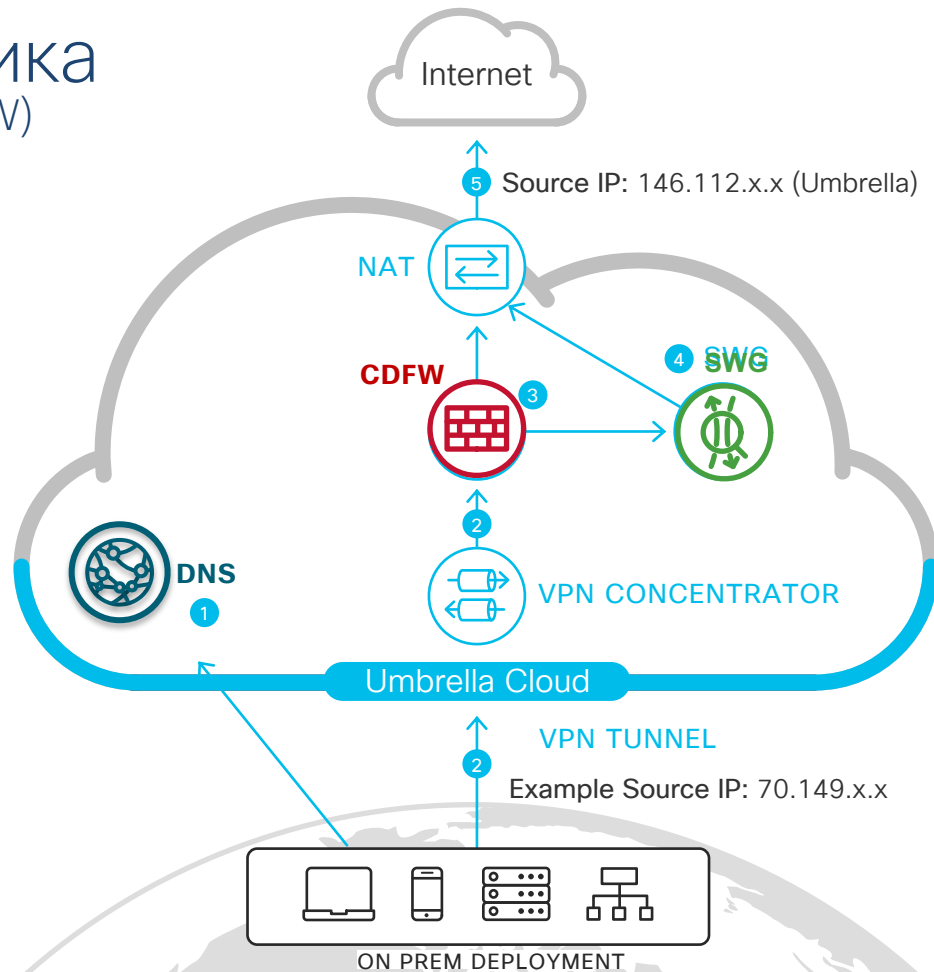
- CSV выгрузка
 - Рекомендуется инструмент CSVDE на контроллере домена Windows
- Синхронизация AD коннектора Active Directory sync
 - Фильтрация групп
 - Версия стандартного AD коннектора версии 1.3.8+
 - Требуется только DC, не требуется VA



Cloud-Delivered Firewall

Туннелирование трафика (DNS вне туннеля, SWG, и правил CDFW)

1. Резолвинг Umbrella DNS по политике, allow/block
2. Разрешенный трафик отправляется по туннелю на Umbrella
3. Инспекция трафика в CDFW. Если веб трафик разрешен по портам 80/443, он отправляется на SWG, другой трафик инспектируется CDFW. Трафик журналируется согласно политике
4. SWG инспектирует и журналирует трафик.
5. Разрешенный трафик пропускается через NAT



Кратко о Umbrella cloud-delivered firewall

Возможности

- L3/L4 FW; L7 возможности (пока в ограниченной доступности)
- Поддержка через туннель IPSec

Identities

- Туннель как основное Identity

Инфраструктура

- Поддержка нескольких DC
- Автоматическая отказоустойчивость с помощью Anycast

Журналирование и отчетность

- Журналы Firewall как часть Activity Search
- Экспорт логов поддерживается через Amazon S3



Варианты использования cloud-delivered firewall

Опасения: гостевой Wi-Fi



Подключение с
инфицированными
устройствам



Нелегальный обмен файлами
(пиратство, нарушения
законодательства)



Доступ к
нежелательному
контенту

Эти активности могут негативно повлиять на организацию

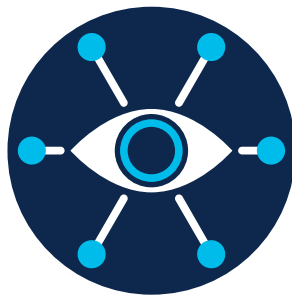
- Связано с рейтингами безопасности, такими как BitSight
- Может привлечь внимание правоохранителей

Варианты использования cloud-delivered firewall

Firewall для границы сети



Защита трафика
DIA в
региональном
офисе



Видимость и управление
приложениями



Согласованный
пользовательский
опыт для web/не веб

Функциональность CASB

Типы CASB



Внеполосный/API

- Cloudlock UEBA
- Cloudlock DLP
- Cloudlock Apps Firewall – OAuth-connected apps
- Umbrella cloud malware protection (LA)



Inline/Proxy

- Umbrella App Discovery & blocking
- Umbrella Advanced App Control
 - Блокировка выгрузок Dropbox/Box
 - Блокировка обмена файлами Webmail
- Umbrella Inline DLP (roadmap)

Обнаружение приложений и детальный контроль (proxy)

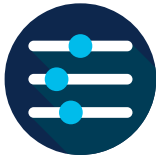
Решение основных проблем, относящихся к «скрытому» IT



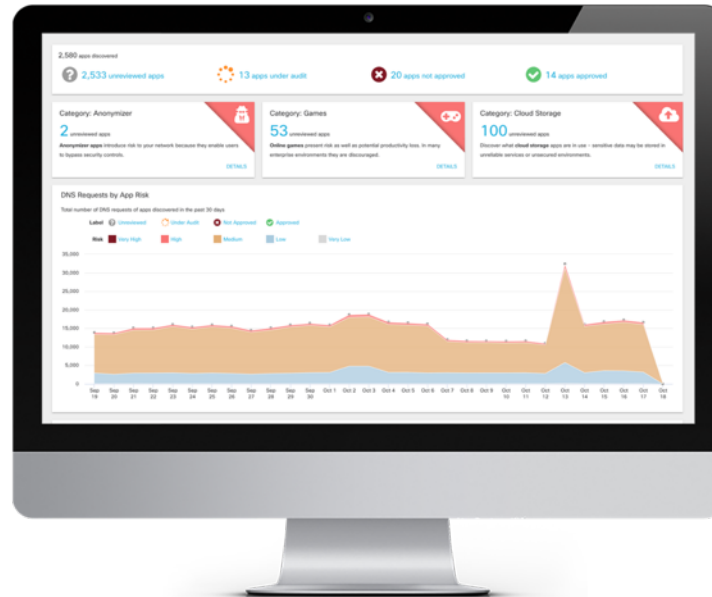
Видимость



Приложения и риск

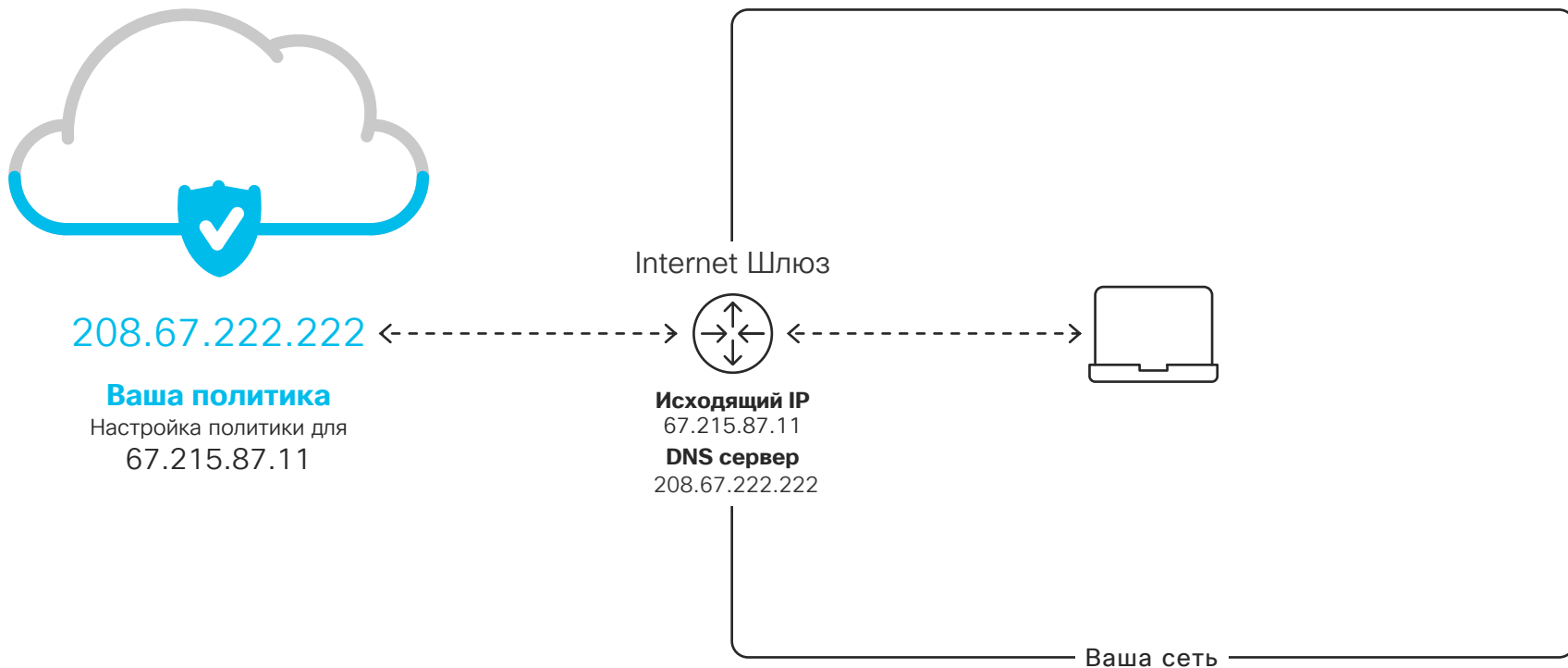


Оптимизация и
блокирование

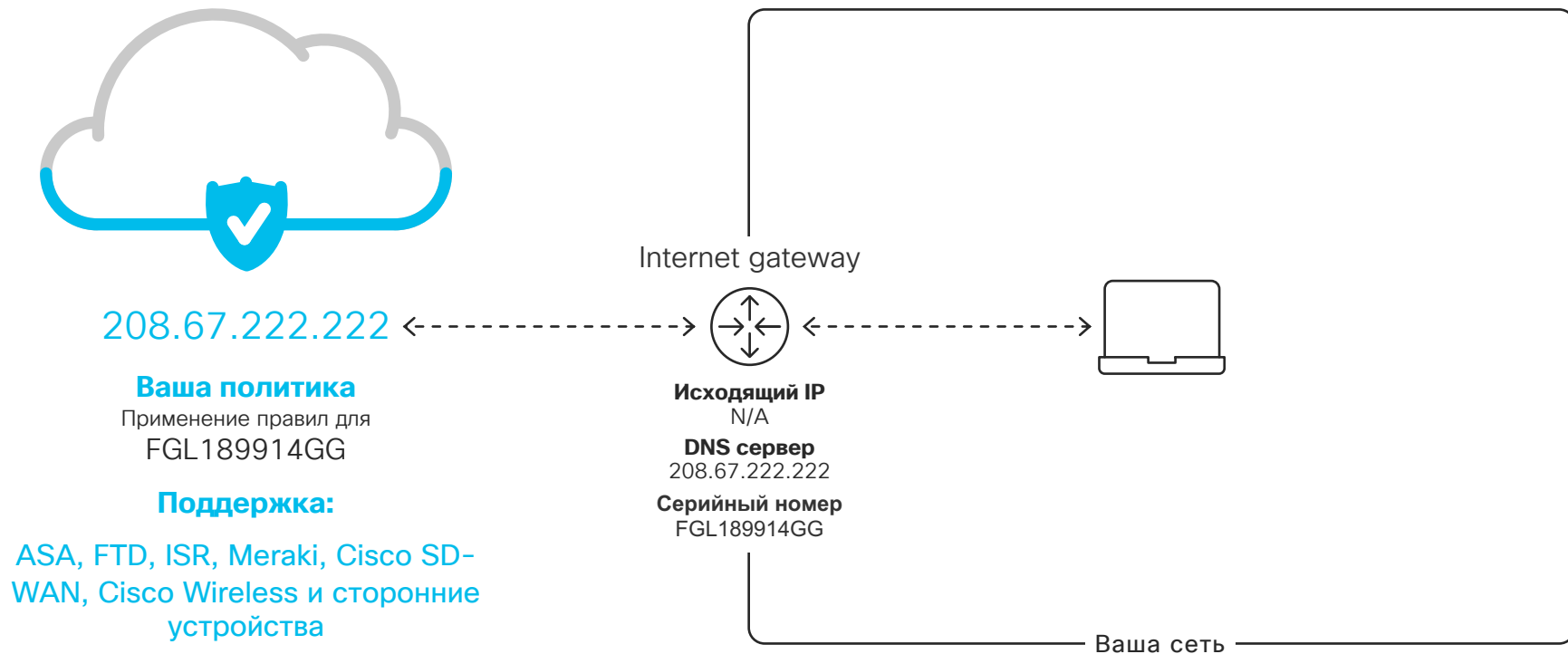


Варианты развертывания

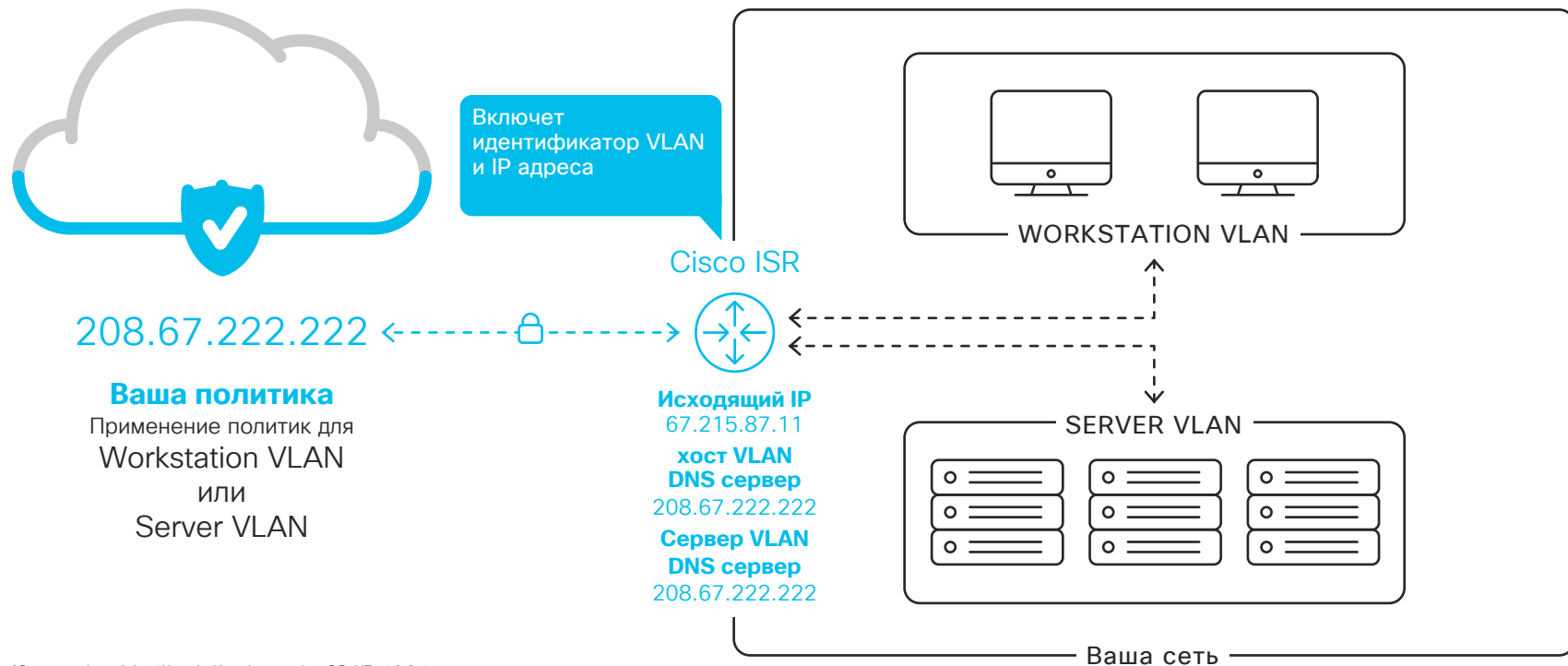
Защитите устройства с помощью DNSCP



Защита с помощью партнерского устройства

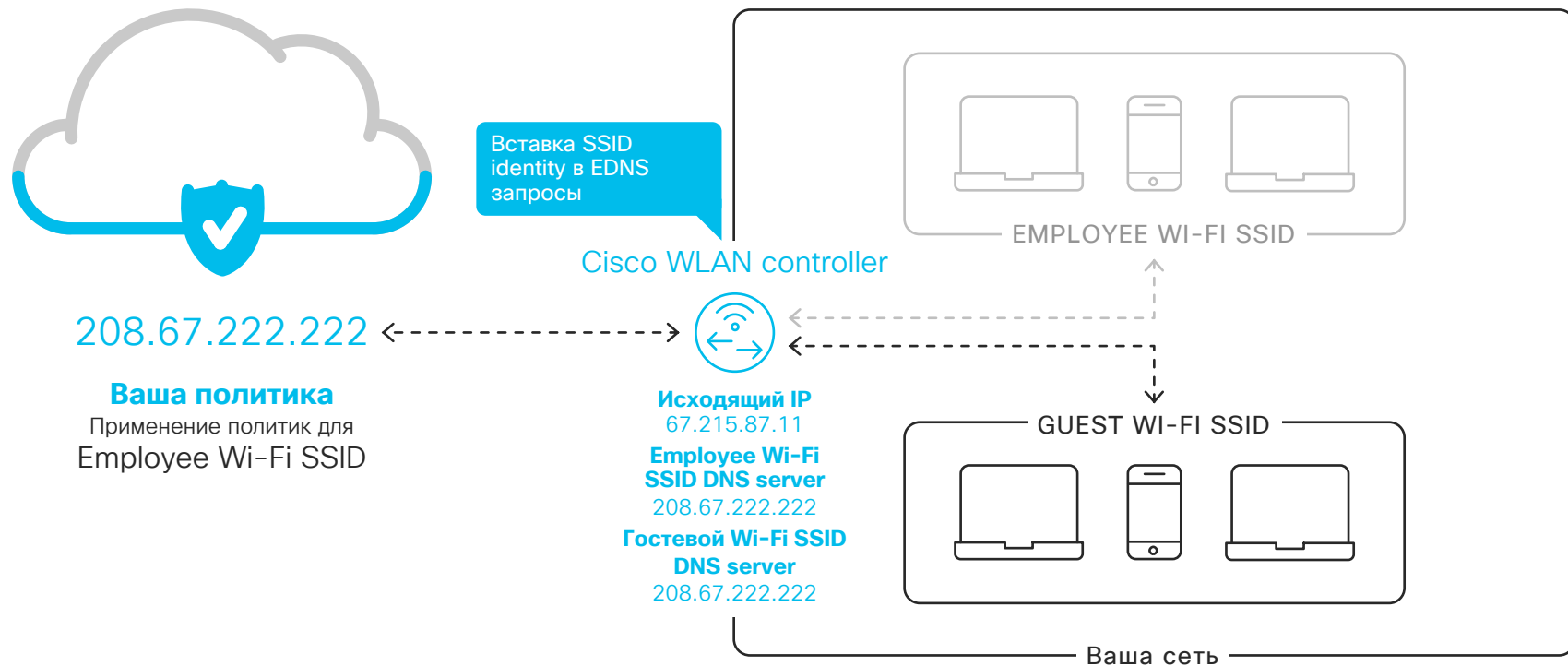


Защита устройств с Cisco ISR*



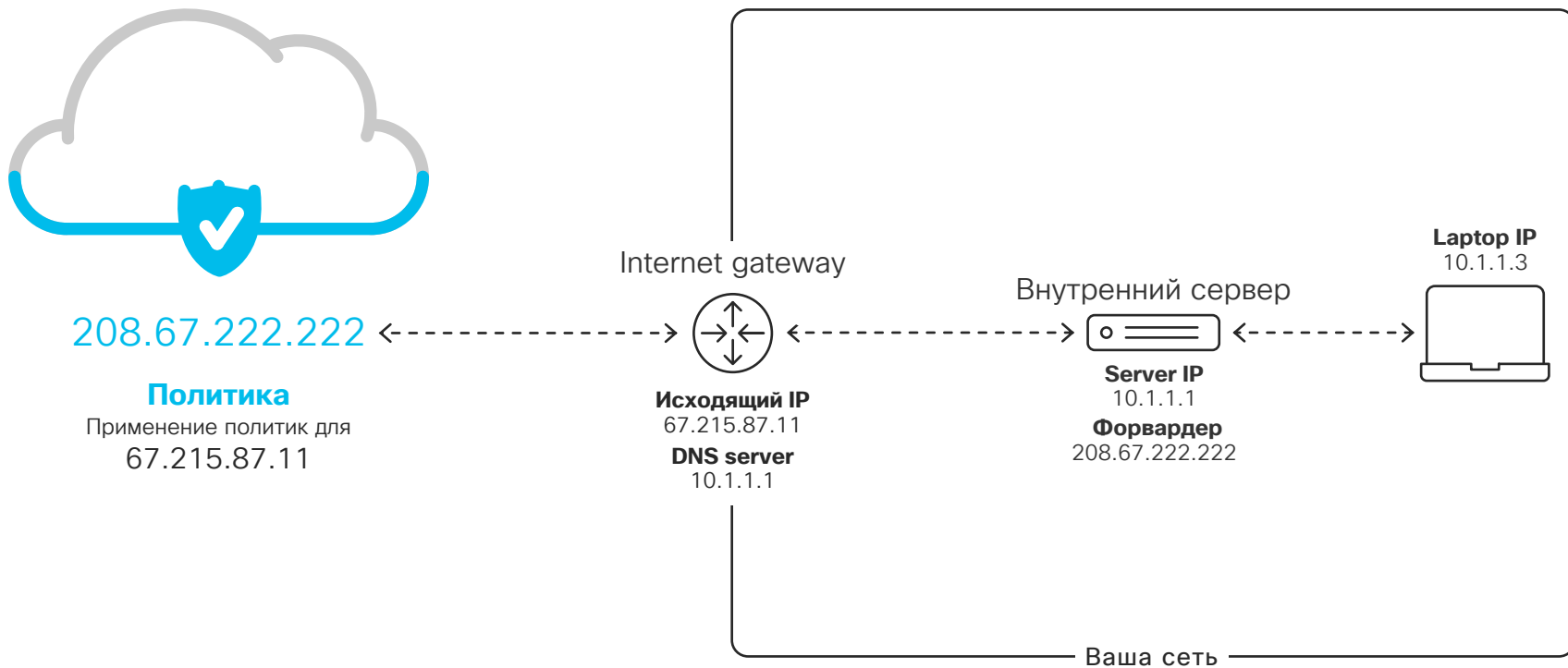
*Supported models: 1K and 4K series running OS-XE v16.6.1+

Защита wifi с Cisco WLC

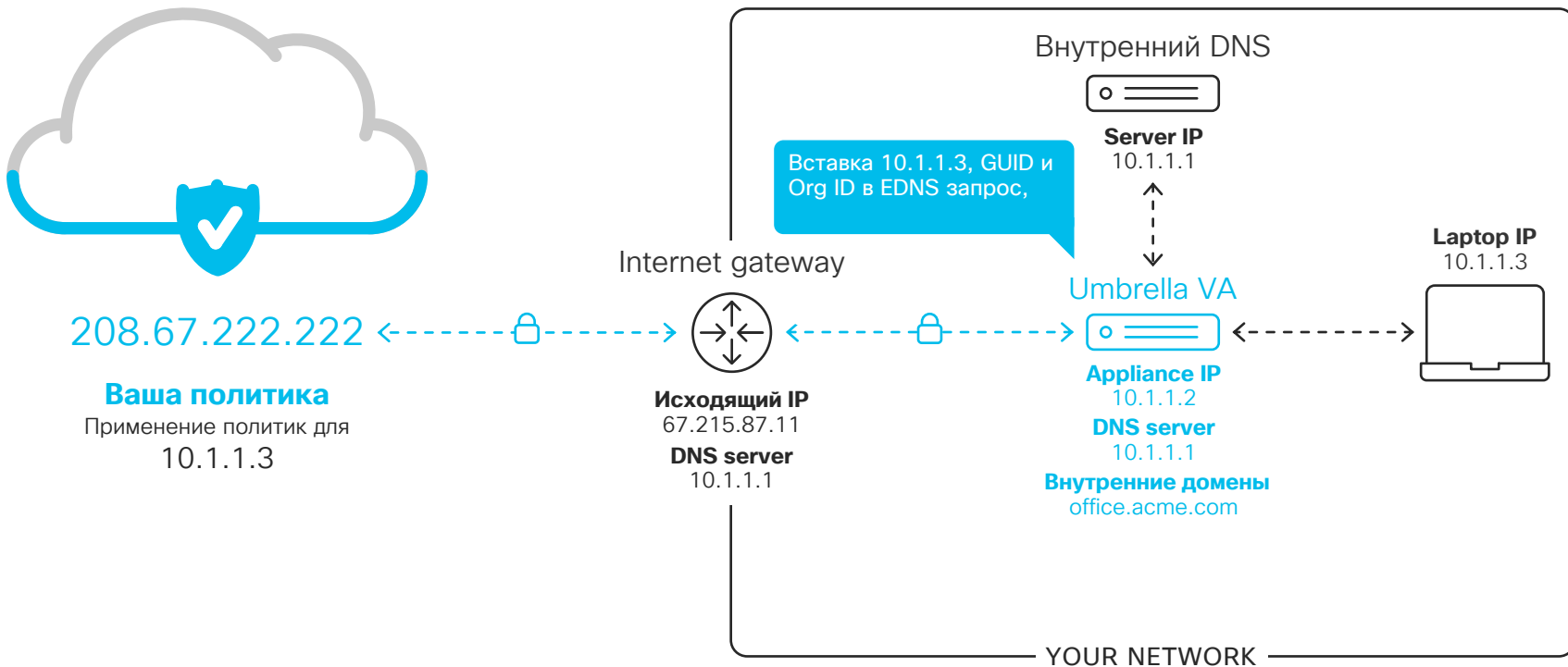


*Supported models: AireOS 8.0+ and WLC 8.4+

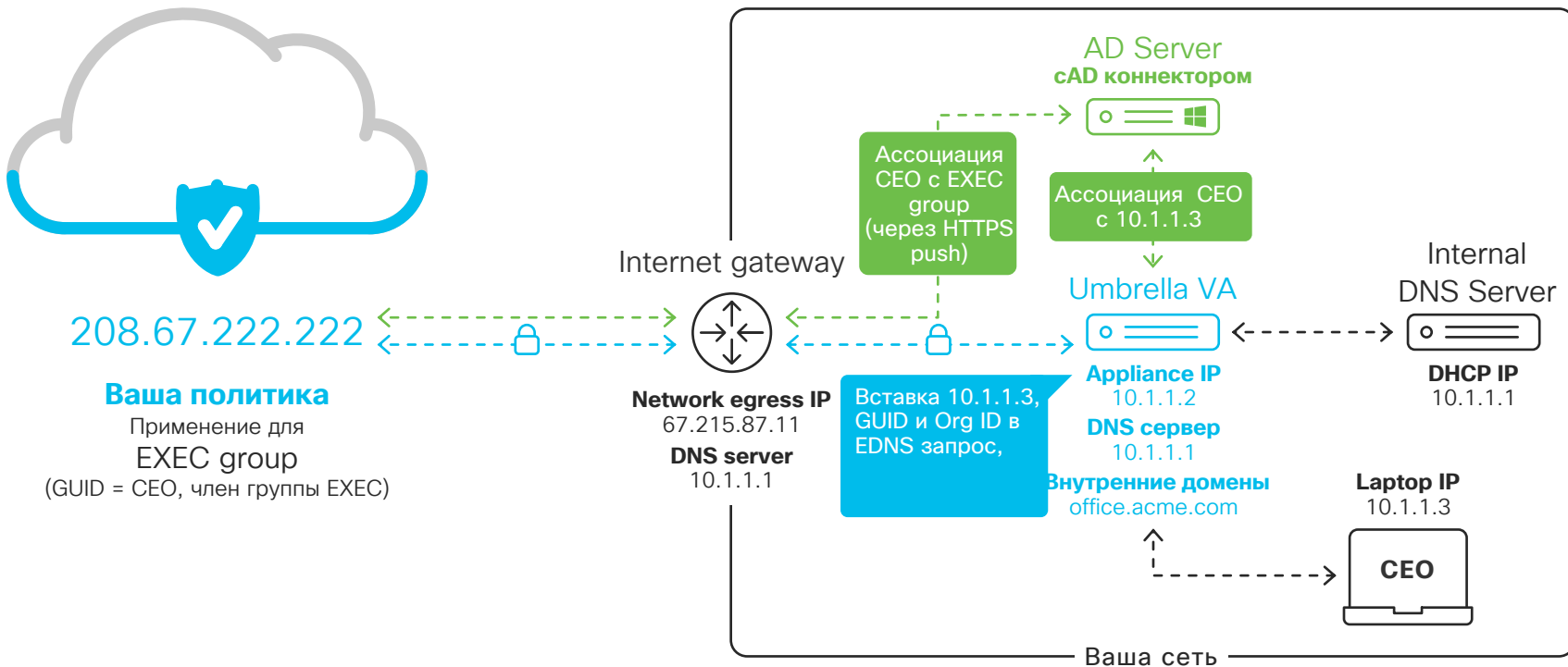
Защита сети через DNS сервер



Защита сетей с Umbrella virtual appliance



Защита пользователей AD через Connector и Umbrella virtual appliance



Самый простой продукт для запуска

- 1 Подпишитесь
- 2 Укажите ваш DNS
- 3 ВСЕ!!!

