

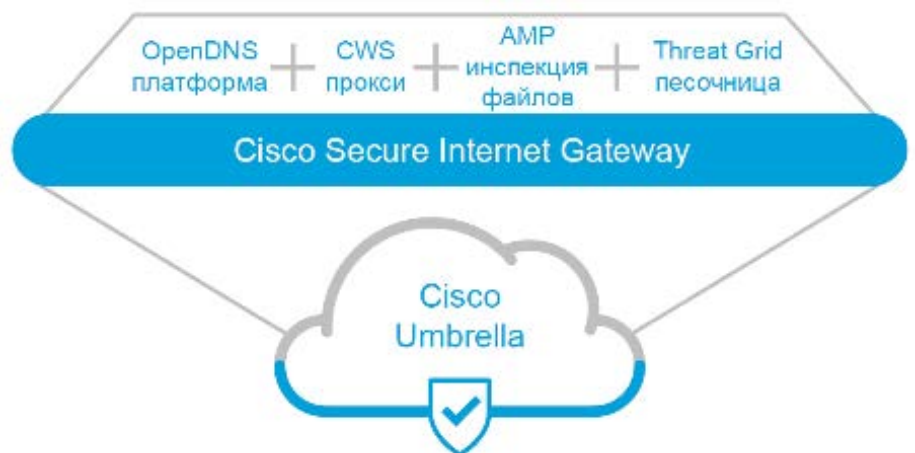
Cisco® Umbrella

Cisco Umbrella – облачный защищенный интернет-шлюз (secure internet gateway, SIG), который обеспечивает первую линию защиты от угроз в Интернете, блокируя запросы на злонамеренные адресаты (домены, IP-адреса, URL-адреса) до установления соединения.

Umbrella обеспечивает полную видимость интернет-активности всех пользователей во всех местах, на всех устройствах и блокирует угрозы до того, как они достигнут корпоративной сети или конечных точек. Будучи облачной открытой платформой, Umbrella легко интегрируется с существующим стеком безопасности и предоставляет информацию о текущих угрозах в реальном времени.

Анализируя и изучая шаблоны интернет-активности, Umbrella автоматически раскрывает инфраструктуру атакующего, поставленную для атак, и активно блокирует запросы на злонамеренные адресаты до того, как соединение будет установлено даже без добавления задержки для пользователей.

С помощью Umbrella вы можете раньше останавливать фишинг и вредоносные программы, быстрее идентифицировать уже зараженные устройства и предотвращать фильтрацию данных.

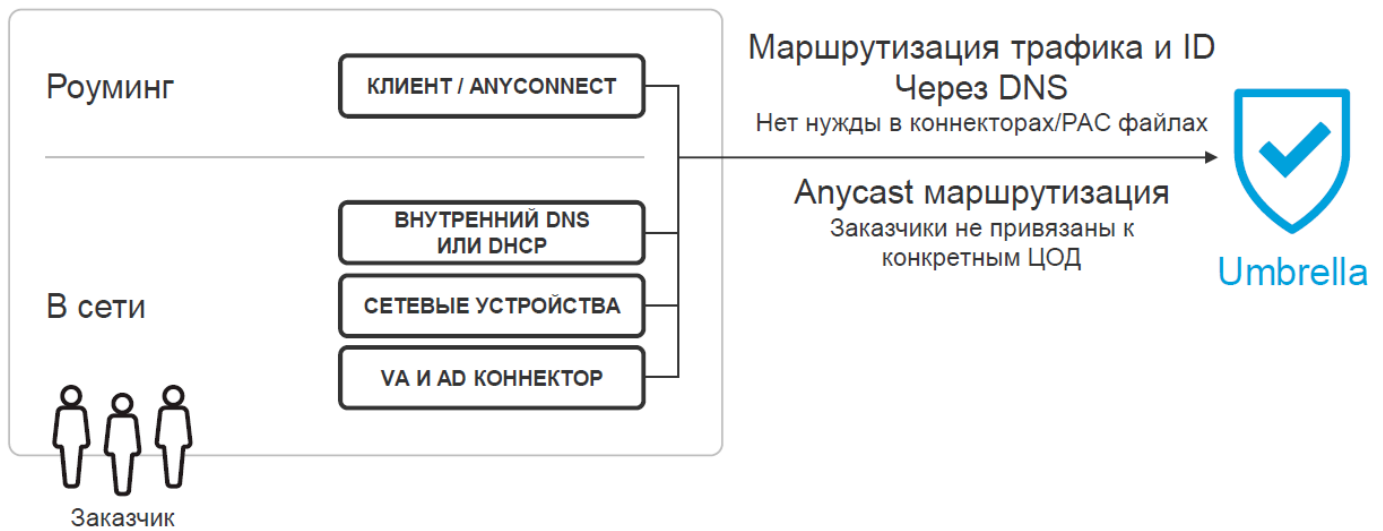


Шлюз SIG защищает доступ в Интернет повсюду, даже если пользователи не прибегают к VPN. SIG действует как контрольно-пропускной пункт в Интернет, обеспечивая первую линию контроля и защиты независимо от того, где пользователи находятся и к чему хотят подключиться.

Cisco Umbrella создан как облачная платформа информационной безопасности, рубеж защиты пользователей, как в корпоративной сети, так и за ее пределами. Umbrella преграждает путь действующим и возникающим угрозам по всем

портам и протоколам, блокирует доступ к опасным доменам, адресам (URL и IP) и файлам - до установки соединения или загрузки файла. Система безопасности Umbrella не требует сложных эксплуатационных манипуляций. Все процедуры выполняются в облаке и нет аппаратного обеспечения, которое требуется монтировать, программного - чтобы его обновлять.

Вы можете приобрести сервис Cisco Umbrella у компании Winncom Technologies, которая более 8 лет имеет статус Cisco Gold Partner.



Общекорпоративное развертывание в течение нескольких минут

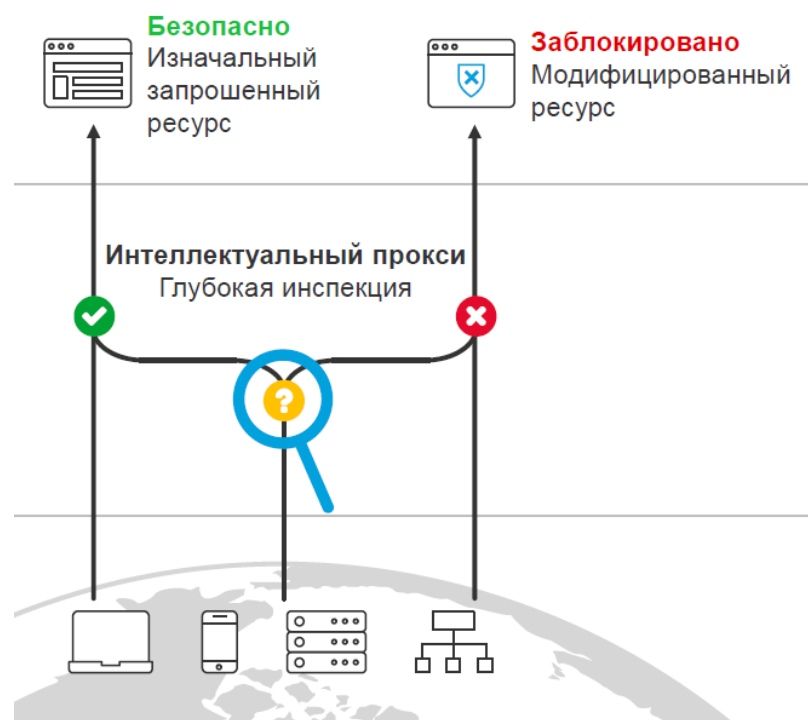
Организация-заказчик может организовать защиту своих ресурсов за несколько минут, используя при этом ресурсы Cisco, включая клиенты AnyConnect, интегрированные сервисные маршрутизаторы Integrated Services Router 4K и контроллеры беспроводных LAN, чтобы направить интернет-трафик (как в корпоративной сети, так и вне ее) на шлюз Umbrella.

Кроме того, с помощью приложения Cisco Security Connector вы можете использовать расширение Umbrella для защиты контролируемых устройств на ОС iOS 11.

Интеллектуальное предотвращение атак до их начала

В течение дня Umbrella решает более 100 млрд интернет-запросов и коррелирует эти актуальные данные с 11 млрд архивных событий. Затем проводится анализ для выявления характерных особенностей и

аномалий, а также создаются модели для автоматического раскрытия инфраструктуры злоумышленника, подготавливаемой к следующей атаке.



Охват вредоносных сайтов и файлов

Шлюз Umbrella получает данные для идентификации и предотвращения угроз, используя средства Cisco Security. В их составе:

- модели машинного обучения, позволяющие выявить известные и появляющиеся угрозы, блокировать подключения к вредоносным сайтам на уровнях DNS и IP;
- интеллектуальные средства Cisco Talos для блокирования вредоносных URL на уровне HTTP/S;
- технология Cisco Advanced Malware Protection (AMP) для обнаружения вредоносных файлов и блокирования их в облаке.

Повсеместная визуализация и защита

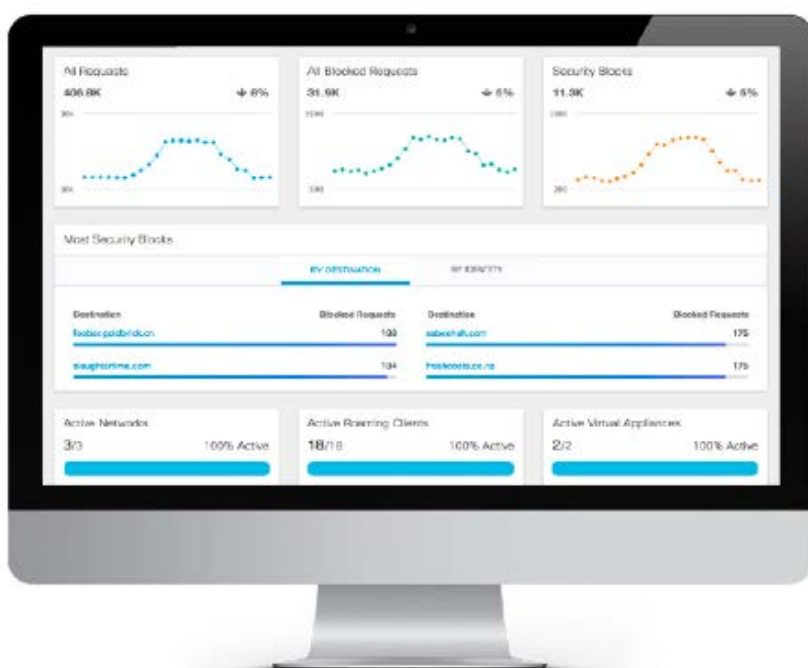
Umbrella обеспечивает визуализацию, необходимую для защиты интернет-доступа по всем устройствам в сети, всем офисным площадкам и всем пользователям в роуминге. Сочетание Umbrella и технологии Cisco Cloudlock Cloud Access Security Broker поможет организациям определить, какие используются приложения, и применить политики, блокирующие опасные или некорректные приложения.

Обнаружение и контроль для приложений SaaS

Umbrella в сочетании с технологией Cloudlock позволяет организациям обнаруживать и контролировать конфиденциальные данные в приложениях SaaS как на сети, так и вне ее.

Надежная и быстрая связь как залог качества обслуживания.

При использовании Umbrella заказчикам не придется жаловаться на снижение скорости или разрыв соединений. Umbrella использует маршрутизацию Anycast — каждый ЦОД объявляет тот же IP-адрес, и поэтому запросы прозрачно пересылаются на свободный и предлагающий максимальную скорость, при этом автоматическое аварийное переключение обеспечивает 100% работоспособность.



Сравнение основных тарифных планов

	Wireless LAN	Professional	Insight	Platform
	Для гостевого доступа Wi-Fi*	Для малого бизнеса	Для средних компаний	Для интеграции с корпоративными системами
Лицензирование				
По количеству устройств	ДА			
По количеству пользователей		ДА	ДА	ДА
Покрытие				
On-network (любое устройство)	Только LAN	ДА	ДА	ДА
Off-network (ноутбуки)		ДА	ДА	ДА
Детальность политик и отчетности				
По сети и хосту	Только сеть	ДА	ДА	ДА
По подсети и пользователю			ДА	ДА
Глубина фильтрации и покрытия				
DNS Layer (домены + IP-адреса)	ДА	ДА	ДА	ДА
IPv4 Layer (IP-адреса без DNS)			ДА	ДА
Proxy (security + IWF URL)	ДА		ДА	ДА
Интеграция на основе API				ДА
Видимость и интеллект угроз				
Базовые логи и отчеты	ДА	ДА	ДА	ДА
Расширенная отчетность			ДА	ДА
Управление логирование чезер S3			ДА	ДА
Консоль для расследования атак				ДА

Примечание: * Работает со специфическими решениями Cisco и интеграцией.

Дополнительная информация:

<https://umbrella.cisco.com/>

