

# Глобальная сеть Cisco Umbrella

## Производительность сети

При выборе облачной платформы обеспечения безопасности важно учесть производительность сети. Пользовательские устройства создают несколько одновременных подключений при каждом переходе на веб-сайт. Поэтому задержка в создании каждого подключения – самый важный показатель производительности любого облачного сервиса.

## Отношения пикинга сокращают путь

Обычно добраться из точки А в точку В по прямой невозможно. Число возможных кратчайших маршрутов ограничено дорогами, соединяющими эти точки. Если исходный пункт и пункт назначения расположены рядом с выездами на автомагистраль, то можно выбрать маршрут с меньшим количеством транспортных развязок. Это сокращает путь. Интернет работает примерно так же. Точки обмена интернет-трафиком (IXP, Internet Exchange Point) аналогичны выездам на автомагистраль – они позволяют нескольким сетям обмениваться трафиком, сокращая общий путь.

Благодаря созданию точек присутствия (POP, Point of Presence) рядом с точками IXP сети могут устанавливать больше отношений пикинга. Самые ценные отношения пикинга устанавливаются с интернет-провайдерами первого уровня в ядре Интернета. Каждый одноранговый узел сокращает путь для передачи трафика по сети из более чем 5000 интернет-провайдеров, составляющей общую матрицу топологии Интернета.



## Сокращение расстояния не всегда увеличивает скорость

Многие поставщики демонстрируют потенциальным клиентам карту сети, где указано количество и расположение точек присутствия<sup>1</sup>. Клиенты могут ошибочно предполагать, что задержка подключения меньше, если точка присутствия поставщика физически расположена ближе к точке присутствия интернет-провайдера, через которую подключаются сети и устройства клиентов. Однако для создания кратчайшего пути между интернет-провайдером и поставщиком может потребоваться множество промежуточных узлов из-за отсутствия отношений пикинга или транзита. Это замедляет передачу трафика между точками А и В независимо от физического расстояния.

Многие облачные сервисы безопасности (такие как защищенные веб-шлюзы) используют традиционную одноадресную маршрутизацию, при которой для каждого сервера объявляется уникальный IP-адрес. Подобные сервисы развертывают балансировщики нагрузки в каждой точке присутствия, и каждому расположению назначается единственный уникальный IP-адрес. Во время настройки может потребоваться выбрать IP-адрес конкретного расположения для каждой инициализированной сети или для каждого устройства. Однако топология Интернета непостоянна, а географическое положение всегда меняется для компьютеров в роуминге или мобильных устройств. Статическая настройка часто приводит к задержкам подключений через менее оптимальную начальную точку.

### Источники данных

1 Будьте внимательны с заявлениями отдельных поставщиков. Некоторые показатели включают точки присутствия с частным доступом. Кроме того, могут быть указаны точки присутствия, используемые только для хранения данных, систем управления или отчетности, но не для контроля передачи трафика. Некоторые точки присутствия могут использовать только один протокол передачи трафика (например, SMTP), тогда как остальные точки присутствия работают по другому протоколу (например, HTTPS).

## Выбор оптимальной начальной точки

Cisco Umbrella – первый сервис сетевой безопасности на рынке, который использует Anycast-маршрутизацию. В этом случае каждый сервер в каждой точке присутствия объявляет один и тот же IP-адрес во всей глобальной сети, а не в зависимости от конкретного расположения. Следовательно, балансирующие нагрузки, увеличивающие задержку и риск отказа, становятся не нужны. Реализация Anycast-маршрутизации в глобальной сети Cisco Umbrella – непростая задача. Для этого нужно обслуживать большой парк оборудования, иметь в собственности большое пространство IP-адресов, управлять сложными политиками маршрутизации и устанавливать многочисленные отношения пирина с вышестоящими интернет-провайдерами. Эти обязанности полностью берут на себя инженеры Umbrella в нашем центре управления сетью.

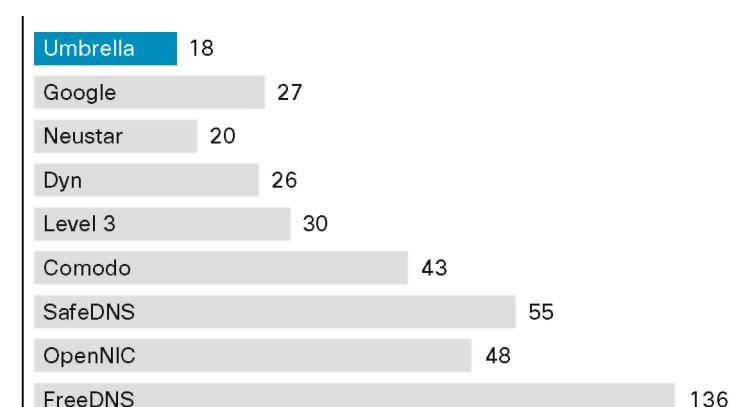
При Anycast-маршрутизации каждая сеть и все устройства наших клиентов подключаются к одному и тому же IP-адресу, независимо от изменений топологии Интернета или географического положения. Anycast-адресация использует скрытый алгоритм маршрутизации с балансировкой нагрузки, а не реальные балансирующие. В результате трафик всегда направляется на ту точку присутствия Umbrella, которая обеспечит кратчайший путь для каждого подключения. В отличие от большинства облачных сервисов обеспечения безопасности, Umbrella не требует от пользователей хранить файл конфигурации и (или) управлять им для маршрутизации трафика.

## Обеспечение минимальной задержки подключения между любыми двумя точками

Наша глобальная сеть насчитывает 25 общедоступных точек присутствия (по состоянию на ноябрь 2016 г.), распределенных по пяти континентам, и в будущем планируется увеличить это число. Самое главное, наши точки присутствия расположены совместно с точками IXP, занимающими первое, второе и третье места по количеству связей на каждом континенте. Разместив наши центры обработки данных в этих основных точках IXP, мы установили более 2000 пириговых сеансов с другими сетями, сократив путь между любыми двумя точками в Интернете.

Благодаря этим отношениям пирина глобальная сеть Umbrella может поддерживать надежные подключения с более короткими маршрутами, чем любая другая сеть облачного сервиса обеспечения безопасности<sup>2</sup>. Традиционно подключения Umbrella на целый транзитный участок короче, чем у среднестатистической сети. Результаты недавно проведенной независимой сравнительной оценки производительности Umbrella см. в этой [гостевой публикации блога](#), созданной аналитиком Microsoft. (Примечание. Веб-сервис OpenDNS был приобретен компанией Cisco в августе 2015 года.) Хотя фактическая задержка для каждого транзитного участка будет различаться, Umbrella зачастую может уменьшить совокупную задержку подключений для пользователей.

## Скорость обработки DNS-запросов



Среднее время отклика в Северной Америке (мс)

Источники данных  
2 Источник: Hurricane Electric Internet Services [<http://bgp.he.net/>].  
Маршрутизаторы BGP объявляют пути между сетями с помощью номеров автономных систем (AS, Autonomous System). Американский регистратор интернет-номеров (American Registry for Internet Numbers, ARIN) присвоил глобальной сети Cisco Umbrella номер AS36692. Для сравнения использовались показатели, заявленные для каждого номера AS конкурента. Среднее значение было рассчитано для конкурентов, использующих несколько номеров AS.

## Отказоустойчивость сети

Найти надежную и доступную сеть, поддерживающую каждое подключение, – задача первостепенной важности для наших заказчиков. Любое нарушение доступа к Интернету приводит к ущербу из-за упущеной выгоды. Многие поставщики заявляют об отказоустойчивости своих сетей на уровне 99,999%. Однако в подробных условиях часто указано, что это не тот уровень, который поставщик обеспечивает на протяжении всего срока обслуживания. На самом деле поставщик обязуется вернуть часть стоимости услуги, если данный уровень не будет достигнут.

## Высокие стандарты ведения деятельности и полная прозрачность

Глобальная сеть Cisco Umbrella сохраняет стопроцентную отказоустойчивость с момента запуска в 2006 г. Umbrella строится на доверии со стороны более 85 млн активных интернет-пользователей, которые ежедневно используют наши службы рекурсивных DNS-серверов для подключения к сети.

Мы убеждены, что это доверие более ценно, чем условие возмещения затрат, прописанное в соглашении об уровне обслуживания клиента. Ниже приведен снимок экрана с текущим состоянием нашей сети и свернутым перечнем различных операционных сообщений и уведомлений за 30 дней. Эта информация опубликована на веб-странице <http://cs.co/umbrellasystems>.

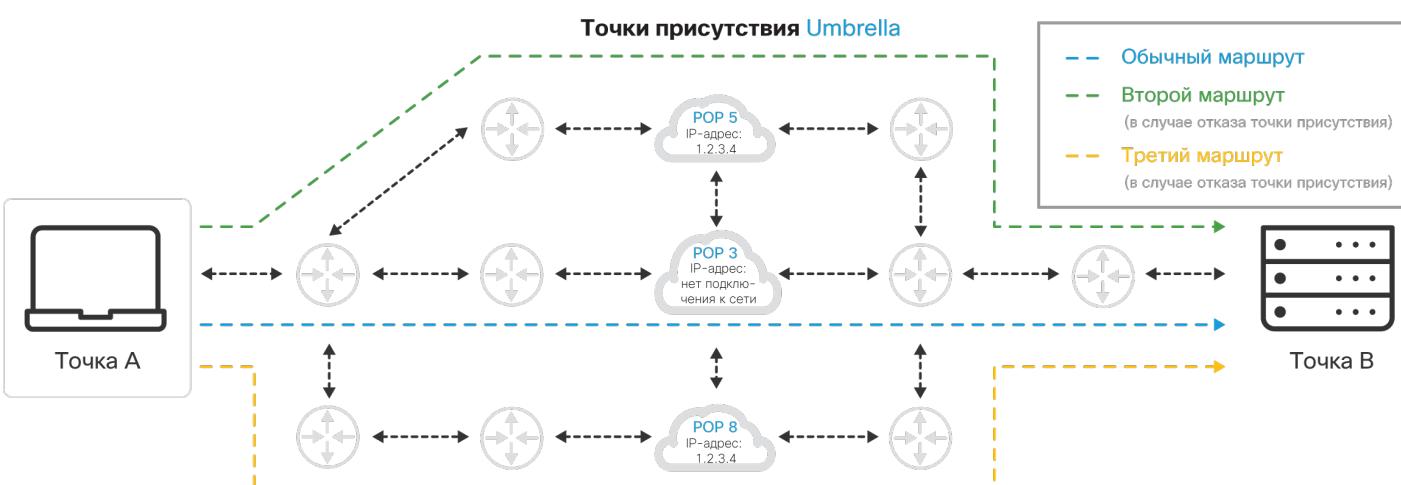
### За последние 30 дней

Дата	Система OpenDNS	Расположения																						Число DNS-запросов в день		
		AMS	ASH	BER	CDG	CHI	CPH	DFW	FRA	HKG	JNB	LAX	LON	MIA	NYC	OTP	PAO	PRG	SEA	SIN	SYD	WRW	YYZ	YVR	NRT	
19 октября 2016 г.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	89,284,186,745	
18 октября 2016 г.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	90,064,501,674
17 октября 2016 г.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	94,254,270,801
16 октября 2016 г.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	71,240,319,481
		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	74,980,772,526
		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	89,351,757,939

## Надежное подключение к сети

Вместо устаревших методов циклического обслуживания или физических балансировщиков нагрузки при Anycast-адресации используется алгоритм маршрутизации с балансировкой нагрузки. Если сервер или вся точка присутствия переходит в автономный режим из-за технического обслуживания, стихийного бедствия, отказа или атаки (см. POP 3 в примере ниже), они прекращают объявлять свой общий IP-адрес. После этого все вышестоящие сетевые устройства уровня 3 (например, маршрутизаторы BGP) прозрачно перенаправляют новые подключения на следующий оптимальный сервер или точку присутствия. В приведенном ниже примере следующей оптимальной точкой присутствия будет POP 5 из-за меньшего количества транзитных участков и более низкой стоимости канала.

Вам не нужно перенаправлять трафик или менять настройки межсетевого экрана, если Umbrella потребуется внести временные или постоянные изменения в свою глобальную сеть из-за технического обслуживания, смены расположения или DDoS-атаки (распределенная атака типа «отказ в обслуживании»). Глобальная сеть Umbrella также сохраняет пропускную способность, которая на порядок превышает нашу ежедневную пиковую нагрузку. Даже в худшем случае, если несколько точек присутствия Umbrella выйдут из строя, ни один клиент не потеряет доступа к сети.



## Топология Интернета

Интернет часто называют «сетью сетей», поскольку он включает более 5000 сетей интернет-провайдеров, тесно связанных друг с другом.

### Ядро

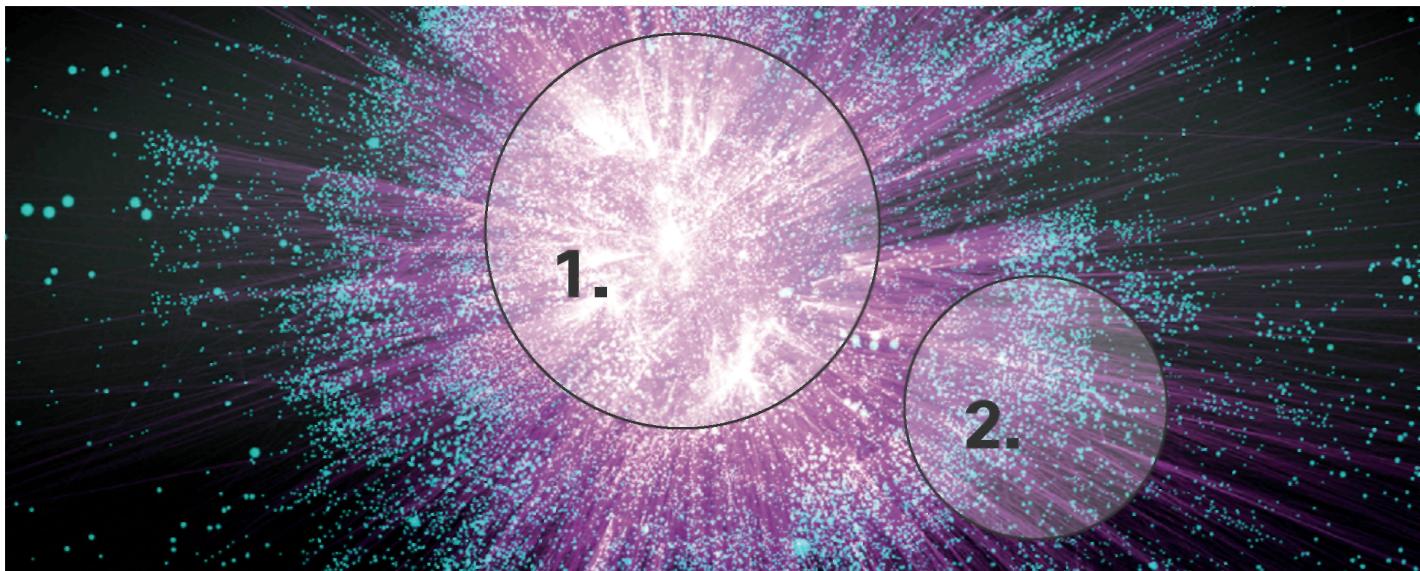
Ядро в топологии Интернета создается с помощью соглашений о пикинге в точках IXP, которые позволяют интернет-провайдерам первого уровня или другим поставщикам услуг типа Umbrella обмениваться трафиком, предназначенным для их клиентов. Чем больше количество и выше качество одноранговых узлов в точке IXP, тем меньше транзитных участков на маршруте и ниже задержка связи между сетями или устройствами клиентов и глобальной сетью Umbrella. Отношения пикинга также ускоряют подключения между нашей сетью и серверами контента или имен.

### Периметр

Миллионы бизнес-сетей и миллиарды домашних сетей используют соглашения о транзите для прямого доступа к Интернету из каждой точки присутствия интернет-провайдера. Соглашения о транзите также служат для подключения Umbrella к сетям интернет-провайдеров первого уровня и для подключения этих интернет-провайдеров к сетям более мелких поставщиков, обычно находящихся на интернет-периметре. Многие региональные интернет-провайдеры предоставляют бизнес-сетям и домашним сетям доступ к Интернету. Зачастую эти интернет-провайдеры второго или третьего уровней не имеют соглашений о пикинге в точках IXP или географически рассредоточены. В результате их сетевые подключения становятся подвержены большим задержкам или отказам соответственно.

### Визуализация топологии Интернета

На этом рисунке показаны связи (фиолетовые линии) между всеми автономными системами (голубые точки) в Интернете.



### 1. Ядро

Яркие белые участки в центре рисунка отражают высокую плотность подключений между точками IXP в ядре Интернета. Точки присутствия Umbrella расположены совместно с этими главными точками IXP в пикинговых узлах по всему миру.

### 2. Периметр

Кольцо голубых точек, окружающее ядро, представляет периметр Интернета, состоящий из более мелких региональных сетей.



Cisco Umbrella