The OpenDNS Global Network Delivers a Secure Connection Every Time. Everywhere.
Network Performance

Users’ devices create multiple simultaneous connections each time we exchange data with other Internet hosts (e.g. browsing Websites). So the latency (aka. delay) to establish each connection is the most important performance metric of a cloud-delivered service’s network.

Peering Relationships Shortens the Path.

Typically one cannot drive from point A to point B via a straight line as the crow flies. Roadways connecting these points limit the shortest routes available. If each point has nearby highway on-ramps, many traffic intersections can be avoided, which shortens the path. The Internet works in much the same fashion, except that physical parameters are meaningless. Expeditious routing through the Internet’s ever-changing topology is most relevant.

And the quantity of a network’s POPs (Points of Presence) is often a less determining factor than the quantity and quality of its peering relationships. Such as those established with well-connected, first-tier ISPs at the Internet’s core. Each peer effectively offers a shortcut for traffic to flow thru the 5,000+ ISPs that make up the overall fabric of the Internet’s topology (see page 5 for a more detailed illustration).

Short Distances Do Not Necessarily Increase Speed.

Many vendors often show prospects a network map indicating the distribution and quantity of their POPs. False assumptions are often made that connection latency decreases the nearer a vendor’s POP is located to the ISP’s POP for which networks and devices connect to. Yet the shortest path between the ISP and the vendor may actually route traffic across the Pacific Ocean and back due to a lack of peers or other transit paths. Or may require excessive hops to route around such slow links, which in total, still results in a slower path between points A and B. Of course, it’s difficult to map the route speed between every endpoint and the vendor’s network. And the speed fluctuates.

Most security cloud services use traditional Unicast routing, which advertises a unique IP address for every server. Such services will deploy load-balancers at each POP so there is only one unique IP address per location. During setup, a specific location’s IP address may need to be chosen for each provisioned network or device. However, the Internet’s topology is always changing around networks and the geographic location is always changing for roaming computers or mobile devices. And often such static setups lead to slower connections via a less optimal starting point.

---

1 Beware of some vendors’ marketed numbers. Some include privately accessible POPs. Or POPs used only for data retention, management or reporting systems, but not traffic enforcement. Or some POPs only enforce one traffic protocol (e.g. SMTP), while others enforce different traffic (e.g. HTTP/S).
Always Selecting the Optimal Starting Point.

Umbrella is the only such network security service in the market that leverages Anycast routing. Anycast enables every server at every POP to advertise the same IP address globally, not per location. And without load balancers, which add latency and risk of failure. Implementing Anycast routing via the OpenDNS Global Network is complex, time consuming and costly. It requires maintaining a lot of hardware, owning a large IP address space, managing sophisticated routing policies, and developing many peering relationships to upstream ISPs. This burden is owned entirely by a team of OpenDNS engineers at our network operation center, not the customer!

Now every customer network and device, automatically or manually setup, connects to the same IP address. Regardless of variable Internet topology or geographic location. Anycast uses invisible load-balanced routing logic, not actual load-balancers, to always route traffic to the OpenDNS POP that will provide the shortest path for every connection. Customers no longer need to manage and/or host a configuration file to perform this action as with most other security cloud services.

Achieving the Lowest Connection Latency Between Any Two Points.

The OpenDNS Global Network provides 23 publicly accessible POPs distributed across 4 continents, with more planned. More importantly, these POPs are co-located with the number one, two and three most well-connected IXPs (Internet Exchange Points) on each continent. Since 2006, OpenDNS has established over 1641 peering sessions with other well-connected networks thereby shortening the path between any two endpoints Internet-wide. These relationships enable the OpenDNS Global Network to deliver secure connections via shorter paths relative to any other security cloud service’s network. And an entire hop less than the average network. While actual connection latency between router hops will vary, the total connection latency between points A and B is more likely to be the lower by leveraging the OpenDNS Global Network.

---

2 The OpenDNS Global Network consists of (10) ten POPs across the Americas; (10) ten POPs across Europe, Middle East and Africa; and (3) three POPs across Asia-Pacific. Please request the locations from a technical support rep to help determine the expected average route speeds to your networks.

3 Source: Hurricane Electric Internet Services (http://bgp.he.net/). BGP routers announce paths between networks using Autonomous System (AS) numbers. The OpenDNS Global Network is assigned AS36692 by ARIN (American Registry for Internet Numbers). The metrics reported for each competitor’s AS number was used for comparison. Mean value was calculated for competitor’s using multiple AS numbers.

4 Competitor C’s networks are not assigned a routable AS number. The AS numbers of the ISP networks hosting competitor C’s POPs are used instead.

5 Source: Cymru (http://www.cymru.com/BGP/avg_aspath_len.html). One way to determine the interconnectedness of the Internet is to look at the average path length between any AS.

---

OpenDNS

The OpenDNS Global Network Delivers a Secure Connection Every Time. Everywhere
Network Uptime

The availability and reliability to establish and maintain every secure connection is paramount. Any impact to business-critical Internet access translates to opportunity costs. Vendors’ marketing often claims “99.999%” network uptime. Fine print regularly reveals that this is not a metric the vendor delivers over the entire life of the service. Just that the vendor will reimburse a percent of the service cost if it fails to meet this metric. Will their reimbursement cover the lost opportunity?

Operational Excellence with Complete Transparency

Umbrella is built on a foundation of trust that OpenDNS has established for over 50 million active Internet users relying on recursive DNS services for network connectivity. The OpenDNS Global Network has maintained 100% uptime since it launched in 2006. OpenDNS believes that is more valuable than just a promise (aka. service level agreement) to reimburse customers. Below is a snapshot of the current status and rolling 30-day window of various operational messages and notices that is published online at http://208.69.38.170/.

Connect with Confidence

Rather than crude round-robin methods or physical load balancers, Anycast uses load-balanced routing logic, which is invisible to individual servers or entire PoPs. If a server or entire PoP (#3 in the example below) is taken offline for maintenance, disasters, failures or attacks, it ceases to advertise its shared IP address. Then all upstream layer-3 network devices (e.g. BGP routers) will transparently route new connections to the next best server or POP (#5 in the example below due to a lower link cost). The traditional burden is completely removed from the customer if OpenDNS needs to make a temporary or permanent change to its global network. Such as periodic service maintenance, major location shifts, or extended failovers due to on-going DDoS (Distributed Denial of Service) attacks. Also, the OpenDNS Global Network strives to maintain double the global network capacity as the daily peak usage. Even in a worse case situation taking several entire OpenDNS POPs offline would not cause any customers to lose network connectivity.
Internet’s Topology

The Internet is often referred to as a “Network of Networks”, as it consists of over 5,000 ISPs interconnected with one another in a sparsely meshed fabric.

The Core

The core of the Internet’s topology is created using peering agreements at IXPs (Internet Exchange Points), which allow first-tier ISPs or other service providers like OpenDNS to exchange traffic bound for one another’s customers. Greater quantity and quality of peers at a IXP, equals fewer routing hops and link latency encountered between customers’ networks or devices and the OpenDNS Global Network. And between the OpenDNS Global Network and content or name servers.

The Edge

Millions of business networks and billions of home networks are connected via transit agreements for direct Internet access from each ISP’s PoP. Transit agreements are also used to connect OpenDNS to first-tier ISPs and first-tier ISPs to smaller ISPs, commonly at the Internet’s edges. Many regional second- or third-tier ISPs that business or home networks receive access from have no peering agreements at IXPs or geographic dispersion making their network connectivity susceptible to greater latency or outages, respectfully.
Umbrella is brought to you by OpenDNS.

Trusted by millions around the world.

The easiest way to prevent malware and phishing attacks, contain botnets, and make your Internet faster and more reliable.