

Cloudflare and Equinix Network Interconnection

Increased Performance and Security at Lower Cost Than Using Public Transit Providers

Introduction

Enterprises today are rapidly responding to the opportunities and challenges presented by hybrid- and multi-cloud architectures. The organizations successfully making this transition are implementing a digital edge strategy that places strategic control points closer to users, clouds and networks. However, evolving enterprise architecture toward this digital edge requires maintaining effective security and privacy safeguards at the front ends of both their internet and internal worlds. These organizations also need to own the security of their applications and data and maintain company and government compliance regulations.

To deliver security and privacy safeguards, enterprises need to replicate similar controls that have previously existed onsite or in an enterprise's private domain, but do so in a cloud-oriented environment. A new set of security guardrails and the emerging "zero-trust" model are required to protect enterprises as this transformation takes place.

Challenges

Traditional IT architectures have consolidated infrastructure and localized services and traffic around centralized "cores." However, the hybrid-cloud shift has effectively turned enterprise architectures upside down, where those centralized cores can no longer protect a growing number of enterprise environments. This is demonstrated in a number of different ways.

Challenging enforcement of security policies across all data centers and appliances: Converting a higher level of visibility into relevant action requires the enforcement of ubiquitous security policies across all enterprise domains, including on-premises capabilities. While security policy creation can be centralized, policy enforcement across the corporate network oftentimes requires updating individual appliances.

As more SaaS applications and cloud workload usage moves to the edge, policy enforcement needs to benefit from the same highly-scalable solutions as policy creation.


Moving data to the edge requires more stringent security and access controls: Additionally, the center of data gravity is moving. Enterprises are now placing data at the edge in order to reduce latency and keep it closer to users and applications. In addition to ensuring proper management and distribution of this data, data security and privacy must also be considered. Network architects need to design solutions that protect data from potential exposure and ensure proper access controls to that data. Implementing proper access controls to data at the edge ensures access by only authorized users and systems.


Lack of end-to-end monitoring across applications: Today's applications are distributed combinations of automated components from multiple sources or vendors – deployed centrally in a regional colocation data center, a cloud service infrastructure and/or across a multi-cloud environment. Today's centralized IT infrastructures and siloed business processes lack the end-to-end visibility required to effectively and efficiently monitor all of the complex interactions across distributed applications and services.




Solution

To meet these needs imposed by a shift to hybrid-cloud architectures, enterprises need to respond with a cloud-oriented approach at all levels of the architecture that replicates or improves on previous security postures.

 Cloudflare's global cloud platform accomplishes this by delivering a broad range of services with integrated, purpose-built network and security solutions that provide companies with visibility of all traffic across their entire network infrastructure. Cloudflare enables organizations to balance workloads across public and private cloud deployments, and can enforce consistent security policies across multiple environments - all while avoiding cloud vendor lock-in.

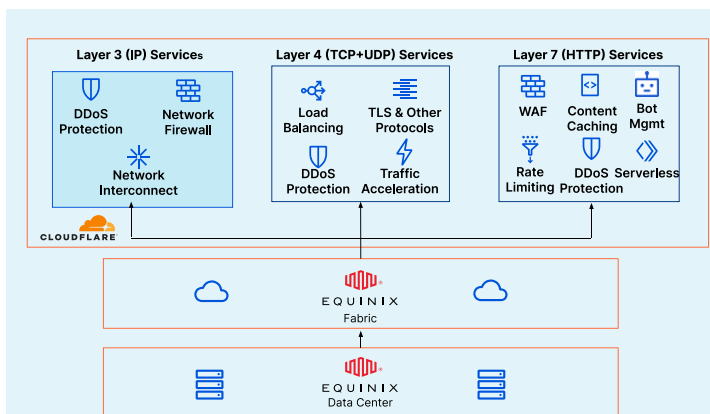
 Cloudflare One is a network-as-a-service solution for enterprises that securely connects your remote users, offices, and data centers to each other and the resources that they need. Cloudflare's enterprise offering replaces the patchwork of appliances and WAN technologies with a single network, providing security, performance and control through one user interface.

 This solution consists of several components such as Cloudflare's WARP Gateway Clients for desktop and mobile, Access for SaaS solution, a browser isolation product, and Cloudflare's network firewall. This works in conjunction with Cloudflare's Magic Transit solution, which enables enterprises to secure their networks from IP-layer (i.e., DDoS) attacks.

Interconnecting to Cloudflare One and Magic Transit with Equinix Fabric

Cloudflare is partnering with Equinix to assist customers in gaining easier access to Cloudflare's globally distributed network, via Cloudflare's Network Interconnect (CNI) program. As part of CNI, Equinix Fabric™ allows mutual customers to interconnect directly and privately to Cloudflare -- even when an organization is not physically located in the same data center as Cloudflare. The customer can order a port and a virtual connection on a dashboard, and Equinix's interconnection fabric will establish the connection to Cloudflare's network.

Since many customers are already connected to these fabrics for their connections to traditional cloud service providers, it is a very convenient method to establish private connectivity with Cloudflare.



This Cloudflare and Equinix combination is a great way to boost performance and for many existing solutions. By utilizing this joint solution wherever a customer's origin infrastructure is located, **customers can get increased performance and security at lower cost than using public transit providers.**

For additional information or to learn more, please contact your Equinix or Cloudflare Account Manager.

Technical Specifications

Equinix Fabric Ports: 1 Gbps or 10 Gbps ports available

Connection Speeds: Right-size connection speeds as demands shift and spin up/down in real time

Connection Options: Layer 2

Availability: 99.999% (dual ports) / 99.9% (single port)

Availability

The Cloudflare / Equinix CNI offering is currently available in these markets:

- Seven virtual interconnection markets: In the Americas: Ashburn, VA; Dallas; New York/Newark; San Jose/Silicon Valley. Also available in London, Singapore and Tokyo.
- Over 30 physical interconnections across the Americas, Asia and Europe. For full list see: <https://www.cloudflare.com/network-interconnect-partnerships/>

For additional information, please contact your Equinix or Cloudflare Account Manager or email interconnection@cloudflare.com.