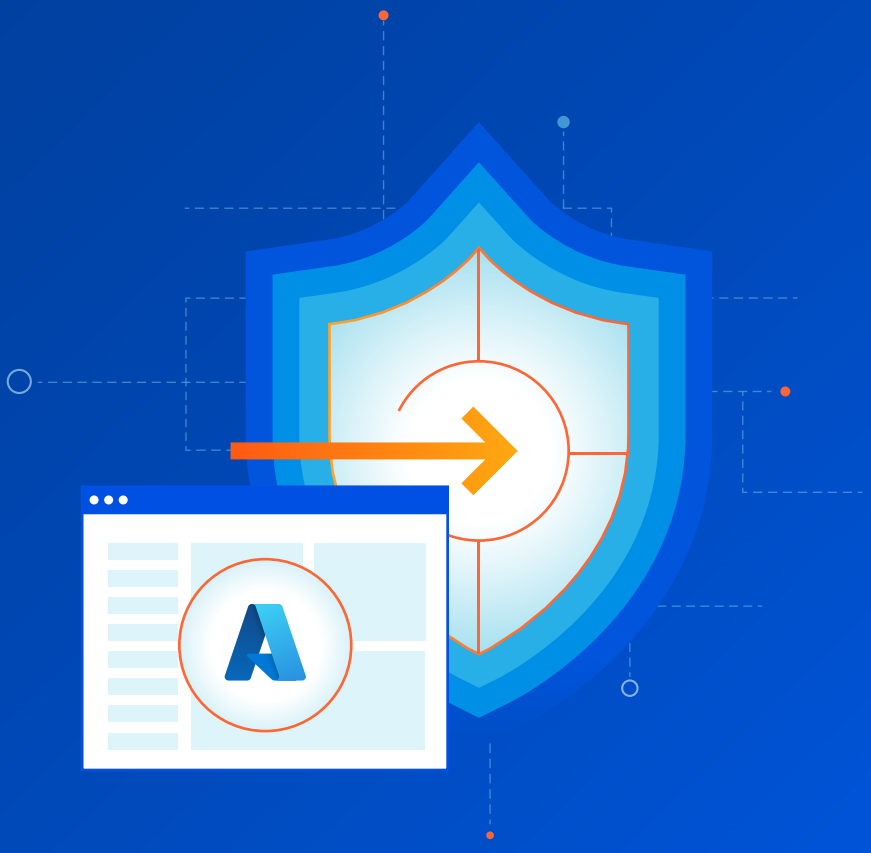
CLOUDFLARE + Microsoft

REFERENCE ARCHITECTURE

Zero Trust Application Access with Cloudflare & Microsoft Azure



Content

About Cloudflare Reference Architectures Guides

Who is this guide for?

The Overview portion of this guide is suitable for all audiences. It will provide a brief refresher on the platform features and integrations being covered. A summary of the design will follow along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind. It will include detailed information on the recommendations and the architecture process. For configuration steps, we will link to the appropriate Cloudflare Doc site articles or configuration steps on integration partner sites.

Acronyms used in this guide

Acronym	Definition
IdP	Identity Provider
MFA	Multi-factor authentication
RDP	Remote desktop software
SDP	Software-defined Perimeter
SMB	Server Message Block refers to modern dialects of the Common Internet File System (CIFS) protocol.
SSO	Single sign-on
TCP	Transmission Control Protocol
UPD	User Datagram Protocol
VPN	Virtual Private Network
ZTNA	Zero Trust Network Access
AAD	Azure Active Directory

Introduction

Cloudflare Zero Trust

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Zero Trust is a holistic approach to network security that incorporates several different principles and technologies and Zero Trust Network Access (ZTNA) is a major technology associated with Zero Trust architecture. From a high-level perspective, Zero Trust demands that users 'never trust, and always verify' network requests, as well as implement micro-segmentation for as much of their organization as possible. Finally, Zero Trust enables users to take rich analytics from these first two principal changes and use them to intelligently respond to threats in real time.

More simply put—traditional IT network security trusts anyone and anything inside the network. A Zero Trust architecture trusts no one and nothing. Traditional IT network security is based on the castle-and-moat concept. In castle-and-moat security, it is hard to obtain access from outside the network, but everyone inside the network is trusted by default. The problem with this approach is that once an attacker gains access to the network, they have free rein over everything inside. It should require security checks for every user accessing every resource. As a result, all companies, especially those whose use of Azure's broad cloud portfolio is increasing, are adopting Zero Trust architectures as an essential part of their cloud and SaaS journey.

Cloudflare Access

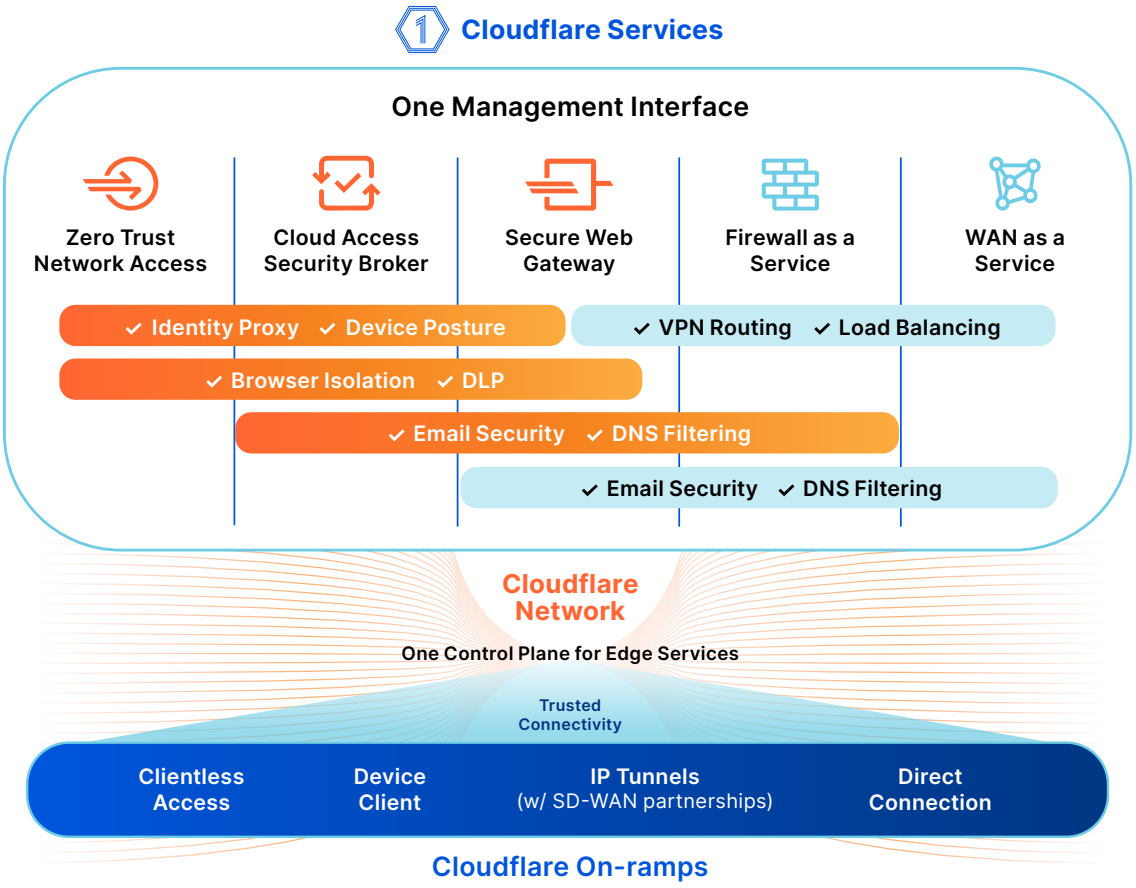
Zero Trust Network Access (ZTNA) enables organizations to implement Zero Trust security. ZTNA is similar to the software-defined perimeter (SDP) approach to controlling access. In ZTNA, like in SDP, connected devices are not aware of any resources (applications, servers, etc.) on the network other than what they are connected to.

Cloudflare Access provides secure access to Azure hosted applications and on-premise applications. Also, it acts as an on-ramp to the world's fastest network to Azure and the rest of the Internet. Users connect from their devices or offices via Cloudflare's network in over 250 cities around the world. You can use Cloudflare Zero Trust on that global network to ensure that every request to every resource is evaluated for security, including user identity. We are excited to bring this secure global network on-ramp to Azure hosted applications and on-premise applications.

Also, performance is one of our key advantages in addition to security. Cloudflare serves over 32 million HTTP requests per second, on average, for the millions of customers who secure their applications on our network. When those applications do not run on our network, we can rely on our own global private backbone and our connectivity with over 10,000 networks globally to connect the user.

We are excited to bring this global security and performance perimeter network as our Cloudflare Zero Trust product for your Azure hosted applications and on-premises applications. Cloudflare Access determines if a user should be allowed access to an application or not. It uses our global network to check every request or connection for identity, device posture, location, multifactor method, and many more attributes to do so. Access also logs every request and connection — providing administrators with high-visibility. The upshot of all of this: it enables customers to deprecate their legacy VPNs.

Instead of a VPN, users connect to corporate resources through a client or a web browser. As requests are routed and accelerated through Cloudflare's edge, they are evaluated against Zero Trust rules incorporating signals from your identity providers, devices, and other context. Where RDP software, SMB file viewers, and other thick client programs used to require a VPN for private network connectivity, organizations can now privately route any TCP and UPD traffic through Cloudflare's network where that traffic is accelerated, verified, and filtered in a single pass for optimal performance and security.

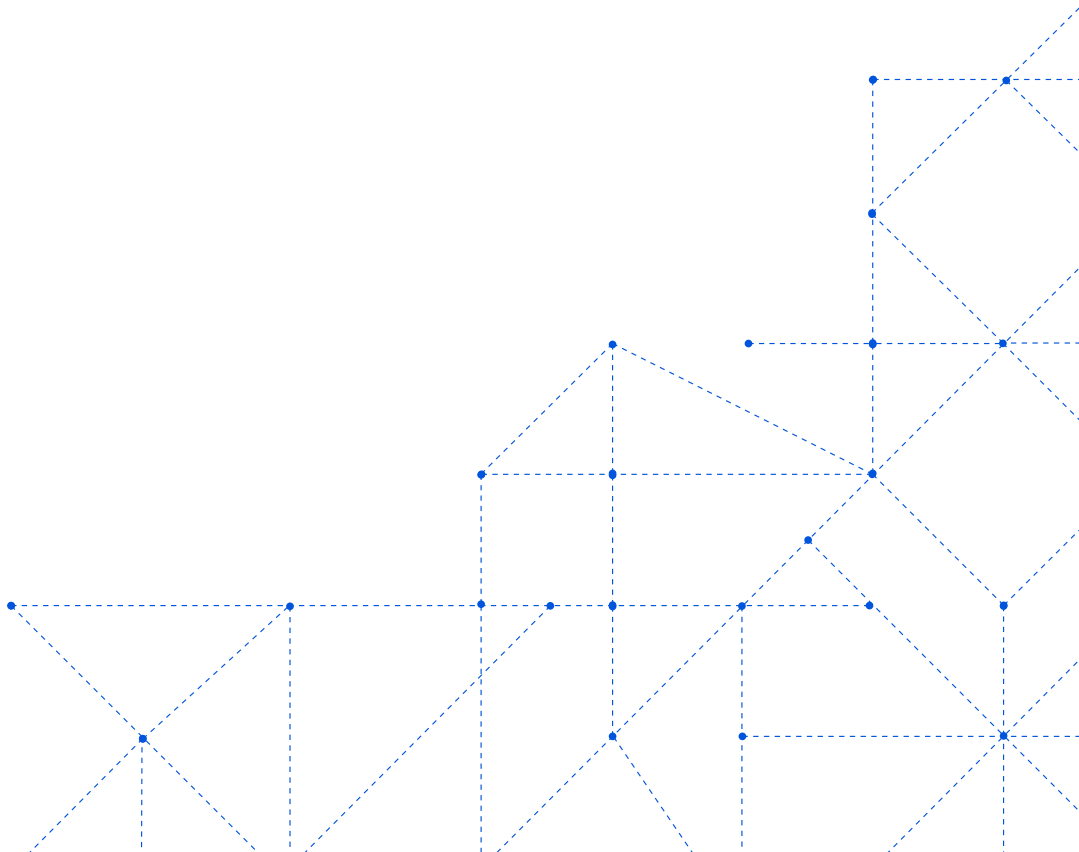


Wondering about Cloudflare Access & Zero Trust?

- Read more about Cloudflare access:
  Zero Trust Network Access with Private Routing
- Need to share a quick overview of Cloudflare access and Microsoft Azure?
  Please visit our blog: Cloudflare partners with Microsoft to protect joint customers with a Global Zero Trust Network
- You can find additional information, demo videos, case studies, analyst reports at:
  Cloudflare Access | Zero Trust Application Access
- Interested in learning more about zero trust?
  Cloudflare Zero Trust | Secure Your Applications & Networks
- Learn more about Cloudflare's partnership with Microsoft:
  Microsoft - Tech Partners | Cloudflare

Microsoft Entra

Microsoft Entra is a new product family that encompasses all of Microsoft's identity and access capabilities. The Entra family includes Microsoft Azure Active Directory (Azure AD), as well as two new product categories: Cloud Infrastructure Entitlement Management (CIEM) and decentralized identity. The products in the Entra family will help provide secure access to everything for everyone, by providing identity and access management, cloud infrastructure entitlement management, and identity verification.

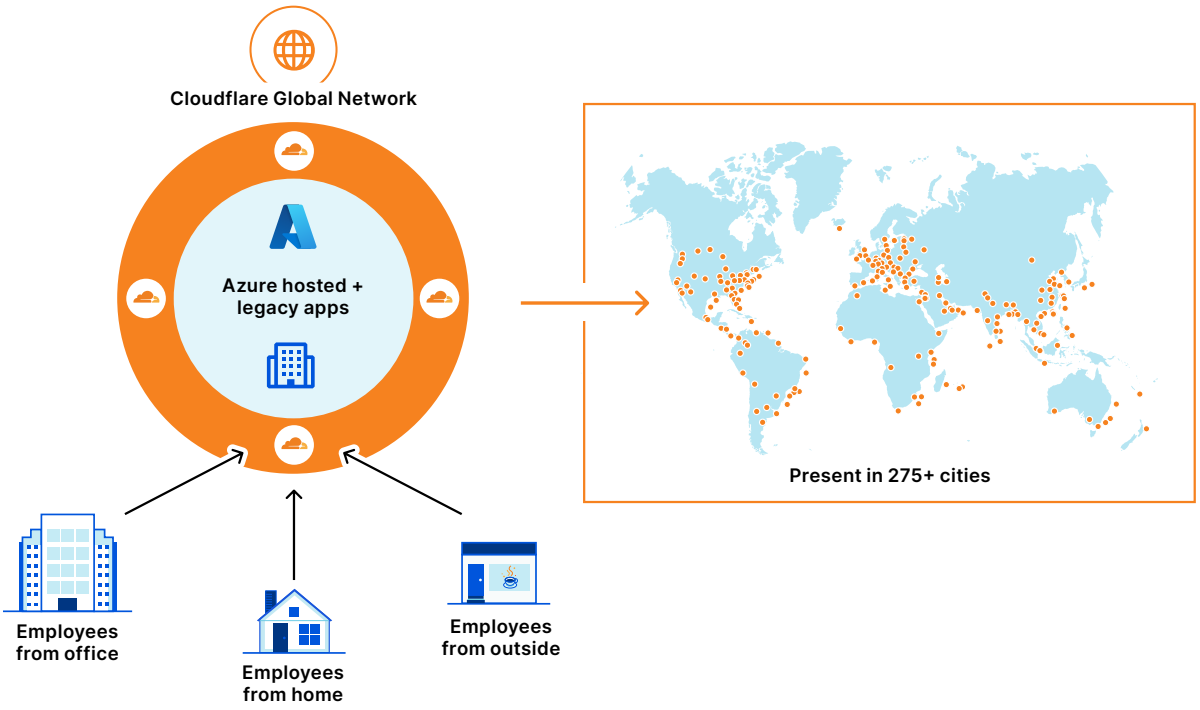


Solution Overview

Cloudflare Zero Trust Network Access + Azure Active Directory

Joint customers benefit from integrations below with Azure Active Directory by:

1. Centralized identity and access management via Azure Active Directory which provides single sign-on, multi factor authentication, and conditional access.
2. Policy oriented access to specific applications using Cloudflare Access—a VPN replacement service.
3. An additional layer of security for internal applications by connecting them to Cloudflare global network and not having to open them up to the whole Internet.



Cloudflare is joining Azure Active Directory secure hybrid access program, which enables customers to centrally manage access for their on-prem legacy applications using single sign-on (SSO) authentication. Secure hybrid access also supports pre-built integrations from key partners to help simplify and secure end user access. Cloudflare Access' integration with Azure AD also protects Azure applications. With this integration, customers can now easily use Cloudflare Access as an additional layer of security in front of their Azure-hosted and on-prem applications.

Azure AD's authentication engine integrates with Cloudflare's edge and access control for a fast, straightforward, and seamless user experience that doesn't compromise security. As a result, by combining Azure AD's single sign-on with Cloudflare's Zero Trust Network Access (ZTNA) solution, IT departments can confidently make internal resources available to a remote and mobile workforce without the headaches of a VPN.

Cloudflare's Zero Trust solution Cloudflare Access provides a modern approach to authentication for internally managed applications. When corporate applications on Azure or on-premise are protected with Cloudflare Access, they look and feel like SaaS applications, and employees can log in to them with a simple and consistent flow. Cloudflare Access acts as a unified reverse proxy to enforce access control by making sure every request is authenticated, authorized, and encrypted.

Identity

Cloudflare Access integrates out of the box with all the major identity providers, including Azure Active Directory, allowing use of the policies and users you already created to provide conditional access to your web applications. For example, you can use Cloudflare Access to ensure that only company employees and no contractors can get to your internal kanban board, or you can lock down the SAP finance application hosted on Azure or on-premise.

In addition, if there are applications that require only certain IDPs (e.g. having a social media login on a public-facing website, but only Azure AD for an in-house server), Cloudflare can implement the usage of said IDPs a la carte based on the needs of the organization.

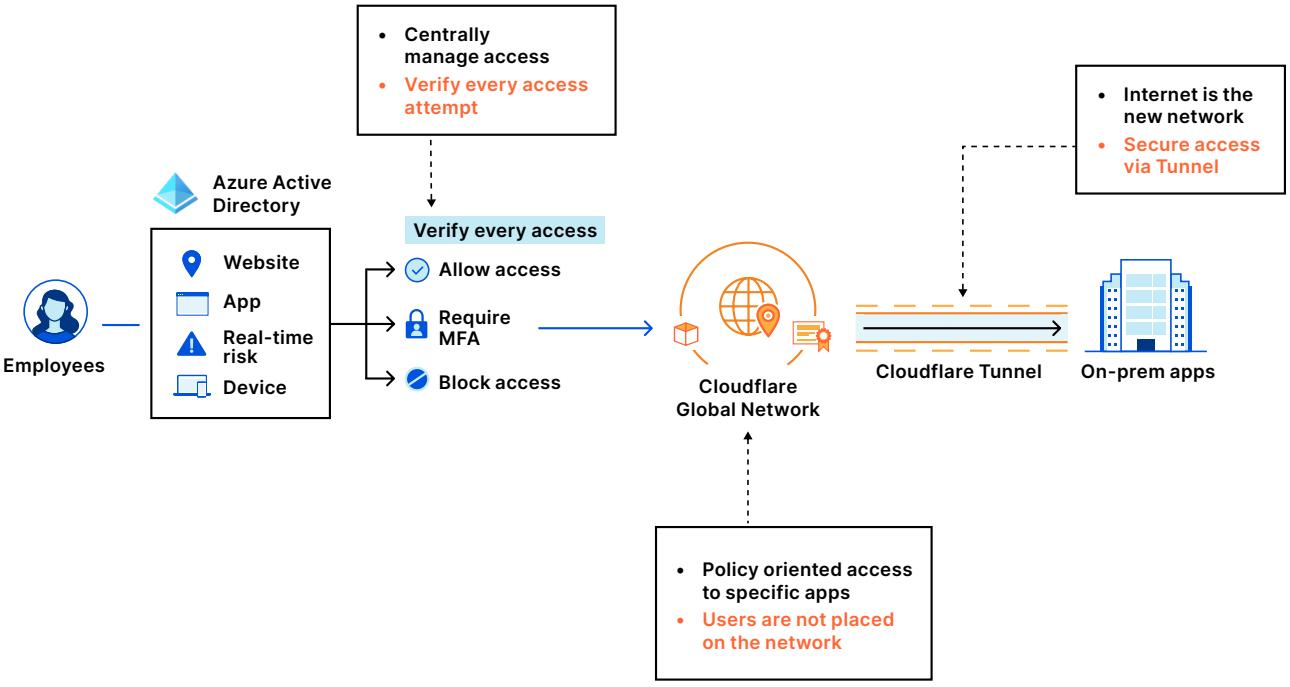
Devices

You can use TLS with Client Authentication and limit connections only to devices with a unique client certificate. Cloudflare will ensure the connecting device has a valid client certificate signed by the corporate CA, and authenticate user credentials to grant access to an internal application.

Additional security

Want to use Cloudflare Access in front of an internal application but don't want to open up that application to the whole Internet? For additional security, you can combine Access with Cloudflare Tunnel. Cloudflare Tunnel will connect from your Azure environment directly to Cloudflare's network, so there is no publicly accessible IP.

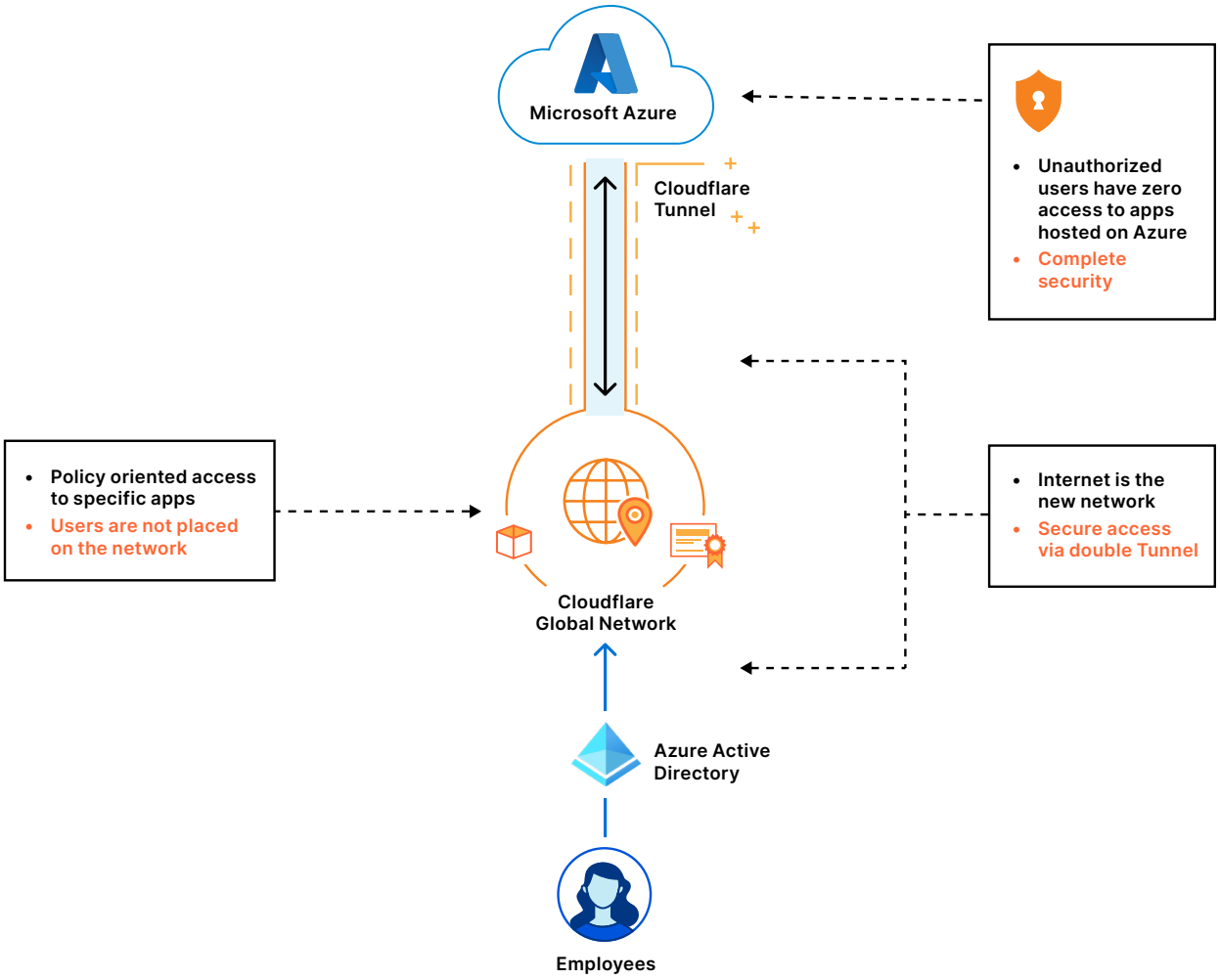
Azure AD secure hybrid access enables customers to centrally manage access to their legacy on-premise applications using SSO authentication without incremental development. Starting today, joint customers can easily use Cloudflare Access solution as an additional layer of security with built-in performance, in front of their legacy applications.



Traditionally for on-premise applications, customers have to change their existing code or add additional layers of code to integrate Azure AD or Cloudflare Access–like capabilities. With the help of Azure Active Directory secure hybrid access, customers can integrate these capabilities seamlessly without much code change. Once integrated, customers can take advantage of the below Azure AD features and more:

1. Multi-factor authentication (MFA)
2. Single sign-on (SSO)
3. Passwordless authentication
4. Unified user access management
5. Azure AD Conditional Access and device trust

Very similarly, the Azure AD and Cloudflare Access combination can also be used to secure your Azure hosted applications. Cloudflare Access enables secure on-ramp to Azure hosted applications or on-premise applications via the below two integrations:



1. **Cloudflare Access integration with Azure AD**

   Cloudflare Access is a Zero Trust Network Access (ZTNA) solution that allows you to configure precise access policies across their applications. You can integrate Microsoft Azure Active Directory with Cloudflare Zero Trust and build rules based on user identity, group membership and Azure AD Conditional Access policies. Users will authenticate with their Azure AD credentials and connect to Cloudflare Access. Additional policy controls include Device Posture, Network, Location and more. Initializing an instance of Cloudflare Access from scratch and adding Azure AD as an IDP is a well-documented process that typically takes a few hours!

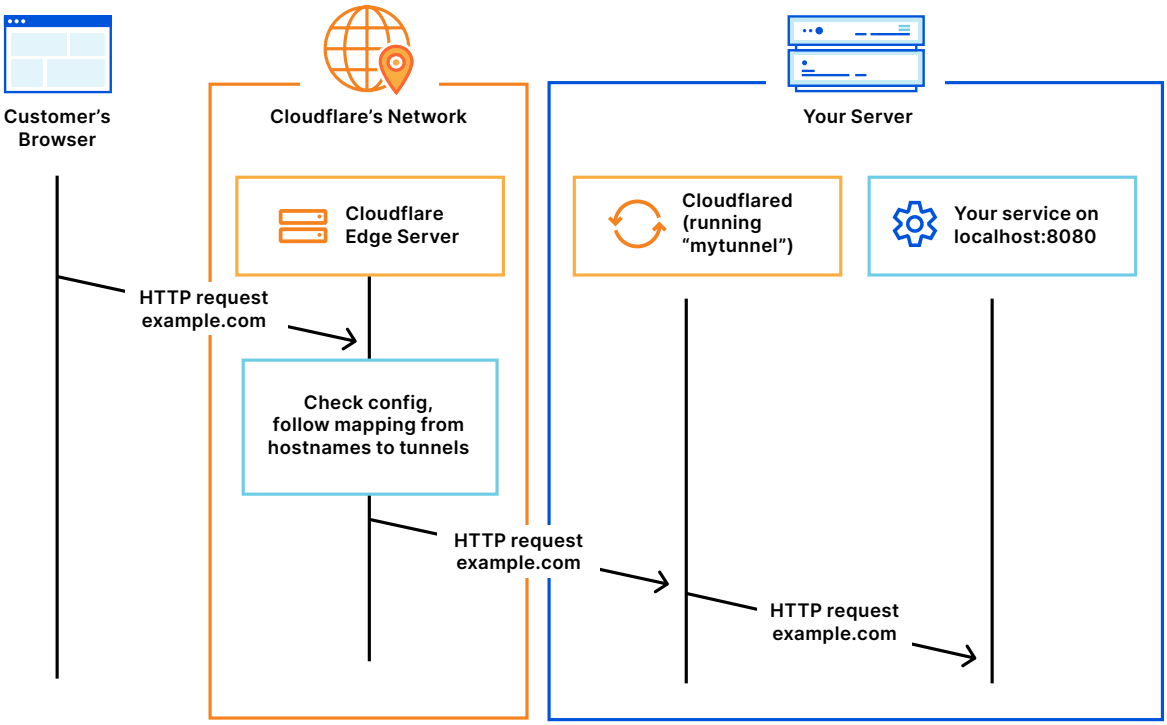
2. **Cloudflare Tunnel integration with Azure**

   Cloudflare Tunnel can expose applications running on the Microsoft Azure platform. See guide to install and configure Cloudflare Tunnel. Also, a prebuilt Cloudflare Linux image exists on the Azure marketplace. To simplify the process of connecting Azure applications to Cloudflare's network, deploy the prebuilt image to an Azure resource group. Cloudflare Tunnel is now available on Microsoft's Azure marketplace.

App Connectors

Cloudflare Tunnel provides you with a secure way to connect your resources to Cloudflare without a publicly routable IP address. With Tunnel, you do not send traffic to an external IP — instead, a lightweight daemon in your infrastructure (*cloudflared*) creates outbound-only connections to Cloudflare's edge. Cloudflare Tunnel can connect HTTP web servers, SSH servers, remote desktops, and other protocols safely to Cloudflare. This way, your origins can serve traffic through Cloudflare without being vulnerable to attacks that bypass Cloudflare

Cloudflared establishes outbound connections (*tunnels*) between your resources and the Cloudflare edge. Tunnels are persistent objects that route traffic to DNS records. Within the same tunnel, you can run as many cloudflared processes (*connectors*) as needed. These processes will establish connections to the Cloudflare edge and send traffic to the nearest Cloudflare data center.



Next steps

In the next sections, we will dive into more detail on each of these topics, providing Cloudflare best practices and recommendations for deployment. Each section will link to the appropriate Cloudflare Help documents. These documents will show you how to configure the Cloudflare service with interface walkthroughs and short overview videos.

Deployments in Azure AD

Azure AD Conditional Access

While evaluating incoming requests, Azure AD can enforce 'conditional access', which are essentially if-then statements that enforce specific user postures to permit access to a resource. For example, requiring the use of MFA to access a payroll application. Cloudflare Access is also part of Microsoft's Azure Active Directory secure hybrid access program. Customers can use this tutorial to set it up.

Cloudflare Access + Azure AD

For on-premise legacy applications, we are excited to announce that Cloudflare is an Azure Active Directory secure hybrid access partner. Cloudflare Access can integrate with Azure AD's Conditional Access rules to require that users connect to certain applications from managed devices. To enable it, you must integrate Azure AD with Cloudflare Access as a cloud app that requires managed device connections. You can use Cloudflare Access' per-app IdP feature to segment which Access applications require Azure AD with managed devices and which only require Azure AD.

Azure AD Configuration

When you integrate Cloudflare Access with Azure AD, Azure AD treats Cloudflare as a single cloud application, even if you have multiple applications secured with Cloudflare Access. To introduce device posture requirements, Cloudflare Access can reuse that same integration.

If you want to allow users to reach certain applications with only Azure AD logins, and no device requirement, you will need to maintain two distinct integrations. One integration with Cloudflare will require device management and the other will only require Azure AD logins.

You can configure which applications secured by Cloudflare Access use which integration in the steps below.

1. Follow the instructions to integrate Cloudflare Access as a cloud app with Azure AD.
2. Repeat this step a second time if you want to maintain an integration that does not require Azure AD device management. We recommend giving each a distinct name that will be used in the steps below.
3. Next, create a new Conditional Access policy in Azure AD. In that policy, you can require that users connect from Managed, Hybrid, or compliant devices. Apply that policy to the integration with Cloudflare Access.
4. Apply that policy to the integration with Cloudflare Access.

Cloudflare Access Configuration

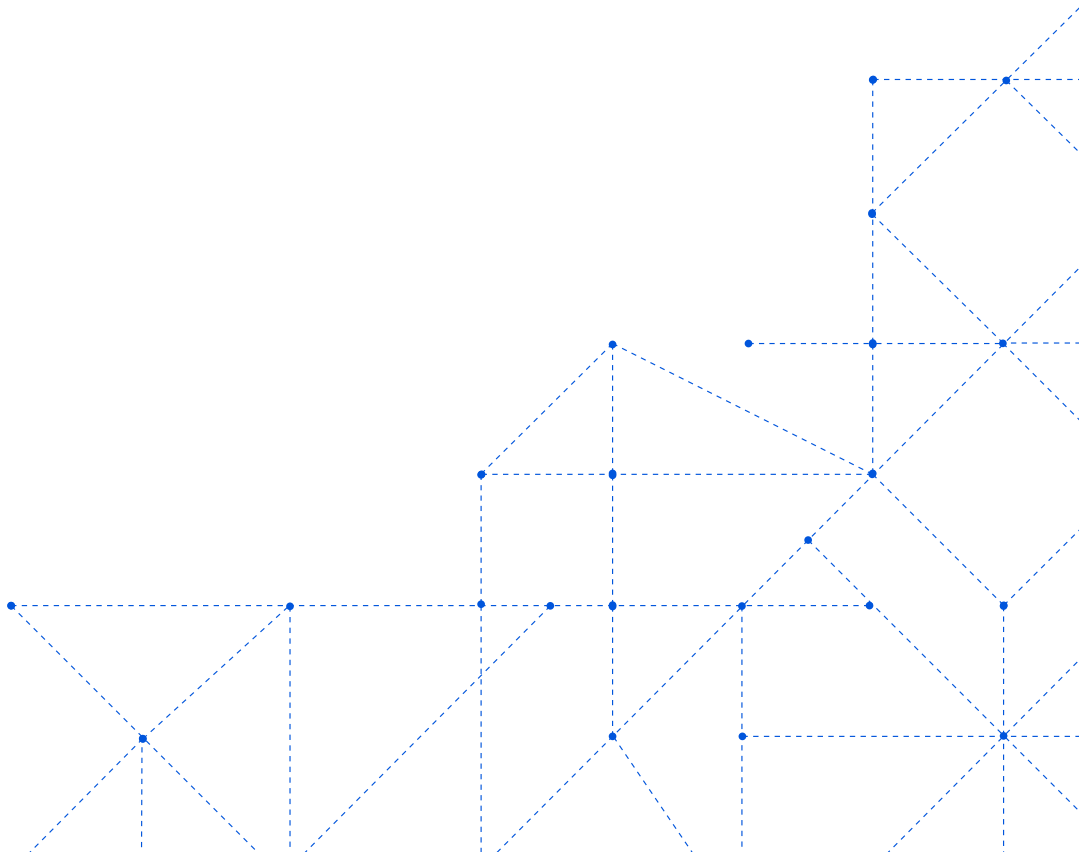
In the Cloudflare for Zero Trust dashboard, you can configure which applications require connections from a managed device and which do not.

1. Navigate to an application that requires managed device connections.
2. Open the Authentication tab.
3. Toggle the Azure AD integration that requires managed device usage.

Walkthrough: Connect to ZTNA with Azure AD credentials

You can integrate Microsoft Azure AD (Active Directory) with Cloudflare Zero Trust and build rules based on user identity and group membership. Users will authenticate with their Azure AD credentials and connect to Zero Trust.

- Set up Azure AD as an identity provider
- Use Azure AD groups
- Example API Configuration



Deployments in Microsoft Azure

Implementing Cloudflare App Connector in Azure

Cloudflare Tunnel is available as a Virtual Machine in the Azure Marketplace. When deployed, the Cloudflare Tunnel software can handle 1000 tunnels (app connectors), 1000 IP routes (if the user exposes private IP space via the app connector) and 25 replicas (load-balancers) per account. Though it varies based on hardware, the expected throughput of Cloudflare Tunnel should be 500 mbps

The following deployments are available for Cloudflare Tunnel:

1. Ubuntu 20.04 VM
2. CentOS 7.2 VM
3. Windows 10 VM running Cloudflared Tunnel natively
4. Windows 10 image running Cloudflare Tunnel inside a nested HyperV

Azure offers many types of VM sizes, and most of them are suitable for production use with Cloudflare tunnel - the tunnel daemon, cloudflared, was designed to run on hardware as simple as a Raspberry Pi.

However, depending on the image used, the minimum requirements for a system running the app connector are as follows:

1. Microsoft Azure's smallest VM Sizes (like the B1s) can run Cloudflare Tunnel.
   - 1 vCPU, 1GB RAM, 2 Data Disks, 320 Max IOPs
2. Both the Ubuntu 20.04 and CentOS 7.2 images were provisioned on size DS1_v2
   - 1vCPU, 3.5GB RAM, 4 Data Disks, 3200 Max IOPs
3. The native and nested Windows 10 deployments were provisioned on size DS2_v3
   - 2vCPU, 8GB RAM, 4 Data Disks, 3200 Max IOPs

***Note** - while these images were provisioned using these parameters, these VM sizes can be modified as needed during setup*

Deploying App Connectors via Azure Marketplace VMs

Instances of Cloudflare Tunnel can be downloaded from the Azure Marketplace and deployed directly to any existing resource group. These templates are VMs with cloudflare tunnel pre-installed on the device, but not yet authenticated to a specific Cloudflare Zero Trust account. If you are unable to install Cloudflare Tunnel directly on the origin server, Cloudflare recommends using marketplace images to ensure the connectors launch consistently each time.

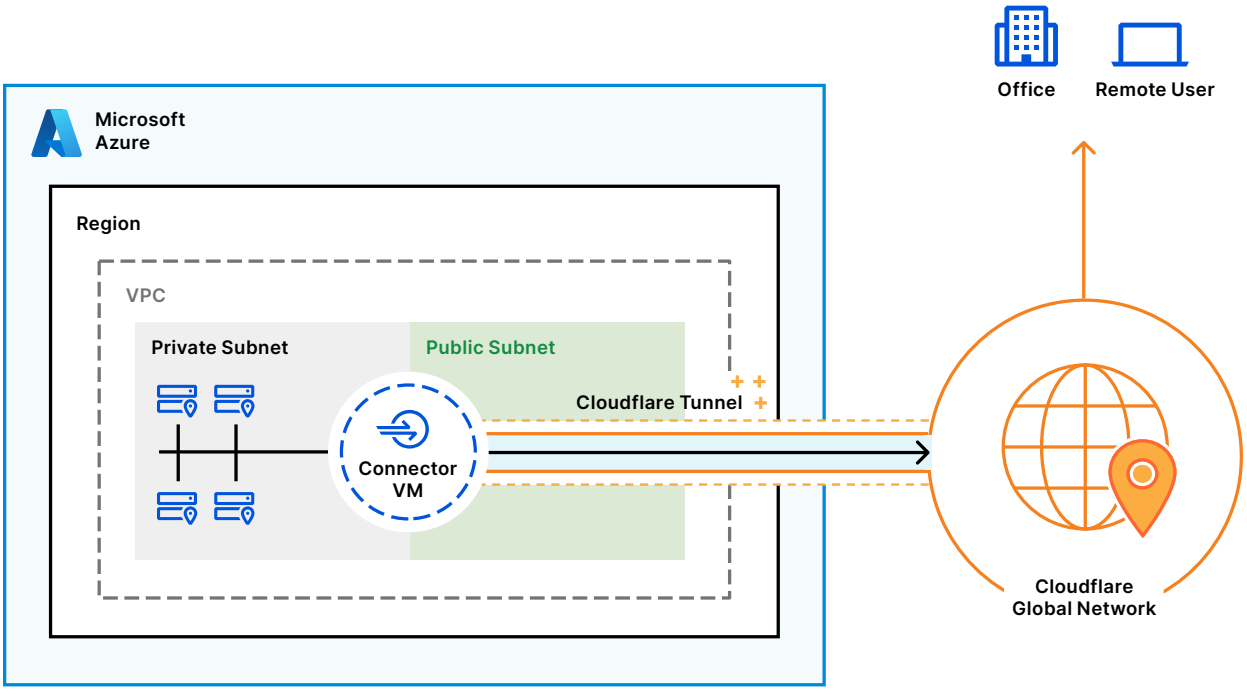
Once the image is created and the tunnel authorized to your cloudflare account, you'll then need to create a configuration file specifying where your origin servers are located and which services/ports need to be proxied.

Learn more about tunnel configuration here.

App Connector placement in Azure

App Connectors deployed via Azure VMs should be located as close to your applications as possible to avoid additional latency. This can mean deploying Cloudflare Tunnel on the origin server itself, or deploying the app connector in a connection broker VM.

In this model, you'll deploy Cloudflare Tunnel as a separate VM instance in the same VPC. The app connector exists in the same subnet as the applications they service.



Multiple App Connector VMs can service the same group of origin servers for load-balancing purposes. These additional connectors are referred to as replicas. When considering where your App Connectors need to be placed and grouped, it's important to remember that Cloudflare will automatically choose the appropriate data center to route or failover through based on the location of the app connector, and no additional configuration is required on the user's end beyond setting up the connector and any replicas.

App Connector connectivity to Cloudflare

Cloudflare Tunnel provides access to the services running on the target origin servers via their connection to Cloudflare's global edge network.

Internally, Cloudflare Tunnel enables your users to reach your internal applications that are using RFC 1918 IP addresses (also known as Private IP ranges). Cloudflare Tunnel will carry client-to-server TCP and UDP traffic between users and applications. These connections are brokered by the app connector, and when a connection is established bi-directional communication within the session can occur as well.

In order to function properly, connectors need to be able to reach Cloudflare's edge – you will need to verify the following:

1. Your app connector can reach the internet
2. Your app connector must not have security policies that block it from accessing Cloudflare's edge network or 1.1.1.1 (important if you need to restrict outbound access to your VM)

Cloudflare Tunnel will only make outbound connections, so having one or multiple app connectors behind a NAT gateway will not impact your service given the firewall rules are configured properly.

Even though your users may move geographically, Cloudflare will automatically route them through the nearest PoP without the need for user intervention. Cloudflare Tunnel maintenance is handled automatically by Cloudflare. Updates occur quietly and can do so while the tunnel is active, causing no disruption to the proxied service.

Cloudflare tunnel can run on Mac OS, Windows, Debian + Redhat Linux distributions and as a standalone Docker image. As long as your host meets the minimum OS requirements, you do not need to perform active maintenance on the VM.

For more information on App Connector connectivity requirements, please visit here.

Load-Balancing and Replicas

When you first run it, Cloudflare Tunnel establishes four outbound-only connections between the origin server and the Cloudflare network. These four connections are made to four different servers spread across at least two distinct data centers. This model ensures high availability and mitigates the risk of individual connection failures. This means in event a single connection, server, or data center goes offline, your resources will remain available.

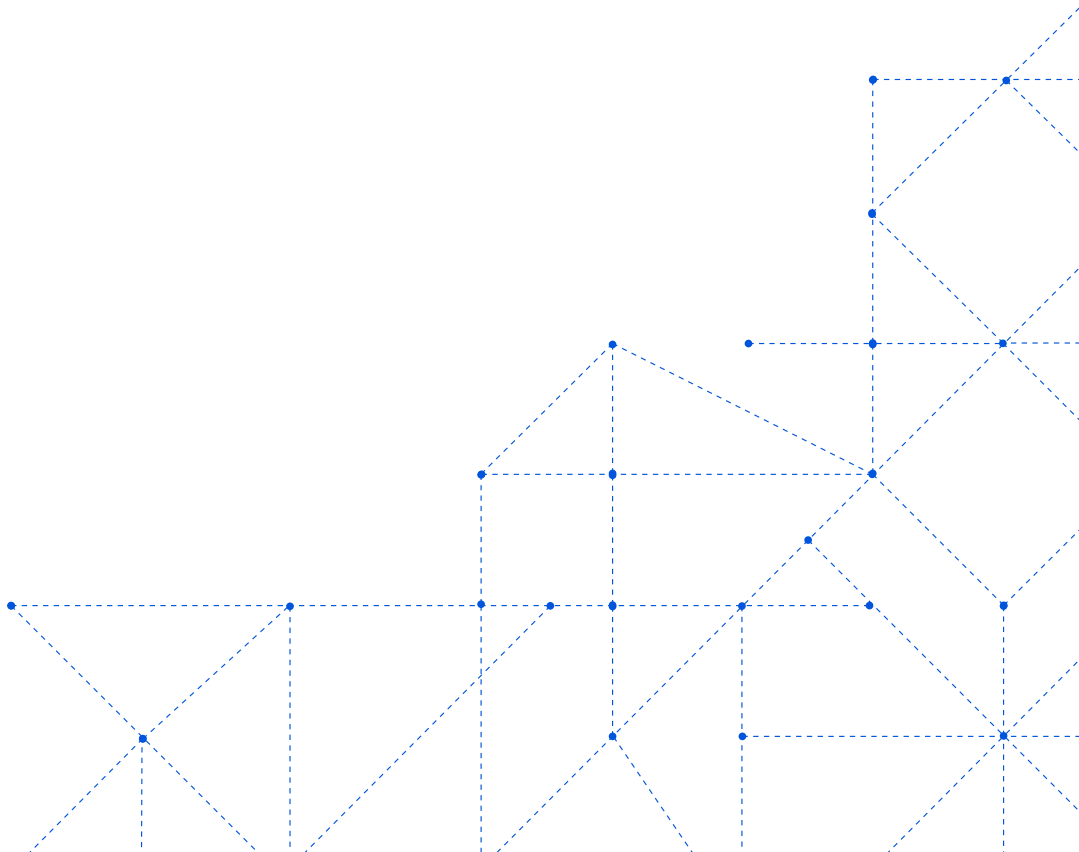
Cloudflare Load Balancing allows users to proactively steer traffic away from unhealthy origins and intelligently distribute the traffic load based on a multitude of steering algorithms. This process ensures that errors are not served to end users and empowers businesses to tightly couple overall business objectives to their traffic behavior.

To learn more about load balancing, please visit here.

Cloudflare Tunnel also allows users to deploy additional instances of our connector, cloudflared, for availability and failover scenarios. We refer to these unique instances as replicas. Each replica establishes four new connections which serve as additional points of ingress to your origin, should you need them. Each of the replicas will point to the same tunnel. This ensures that your network remains up in the event a single host running cloudflared goes down.

By design, replicas do not offer any level of traffic steering (random, hash, or round-robin). Instead, when a request arrives to Cloudflare, the network will pick any connection available to the origin. If a connection fails, we will retry others, but there is no guarantee about which connection is chosen.

To learn more about deploying replicas, please visit here.



Creating & Evolving Cloudflare Access Policy

Integrating Cloudflare Access and Azure AD

Cloudflare Zero Trust allows you to integrate Azure AD with Cloudflare Access. Your team can simultaneously use multiple providers, reducing friction when working with partners or contractors.

Adding an identity provider as a login method requires configuration both on the Zero Trust dashboard and with the identity provider itself. Consult our IdP-specific documentation to learn more about what you need to set up.

Cloudflare Zero Trust supports social identity providers that do not require administrator accounts, open source providers, and corporate providers. Cloudflare also supports using signed AuthN requests with SAML providers.

Configuration help

You will need to configure both Cloudflare and your IdP to work together.
You can find detailed instructions here.

Access Policy decision criteria and framework

Cloudflare Access determines who can reach your application by applying the Access policies you configure. An Access policy consists of an **Action** as well as rules which determine the scope of the action. To build a rule, you need to choose a **Rule type**, **Selector**, and a **Value** for the selector.

In addition to determining which users are authorized to various applications, these access rules determine what device postures are considered compliant when evaluating inbound requests. For example, you can require users to access the application from a specific geographic location or IP, or enforce the usage of a device client or presence of a specific application on their device such as an EPP.

Access Policies are created using Cloudflare's universal policy builder, which allows users to stack criteria, create exceptions and enforce requirements, and supports the use of regular expressions.

You will find out details about actions, rule types, selectors here.

Legacy Active Directory servers

If users have self-hosted AD servers that they will continue to use as organization-wide IDPs, cloudflare does allow them to onboard the windows server as an Application and onboard it as a source of truth for other applications. In this scenario, users will need to install Cloudflare Tunnel on the origin server itself, and they will need an additional IDP in place first to allow proper authentication to the service.

Users can also control L4 access to the windows server via Cloudflare Zero Trust network rules, if onboarding it via tunnel is for any reason not an option.

Once Access to the AD server has been established, you can onboard it to Cloudflare Zero trust as an IDP.

Azure AD B2C

Microsoft provides users an additional variant of Azure AD, known as Azure AD B2C (Business to Customer) - while built on the same technology as AAD, B2C allows businesses to build customer-facing applications and allow anyone to sign into those applications without having restrictions on the user account.

With this, consumers can use their preferred social media, enterprise, or local identities to get SSO access to applications and APIs. This kind of implementation would be ideal for anyone who wants to authenticate large volumes of end users to their web/mobile applications without creating restrictions in the process that harm the end user experience.

In the context of Cloudflare ZT + Azure AD, implementing a B2C identity provider would also be easily manageable in the per-app IDP implementation (the ability to pick and choose which IDPs can authenticate users to certain applications).

About Cloudflare

Cloudflare, Inc. is on a mission to help build a better Internet. Cloudflare's platform protects and accelerates any Internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network, which gets smarter with every request. As a result, your end customers see significant improvement in performance and a decrease in spam and other attacks.

By partnering with Cloudflare, together we help your customers consume your IP solution simply and cost efficiently, all while being protected and optimized by Cloudflare.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3879.2022OCT18