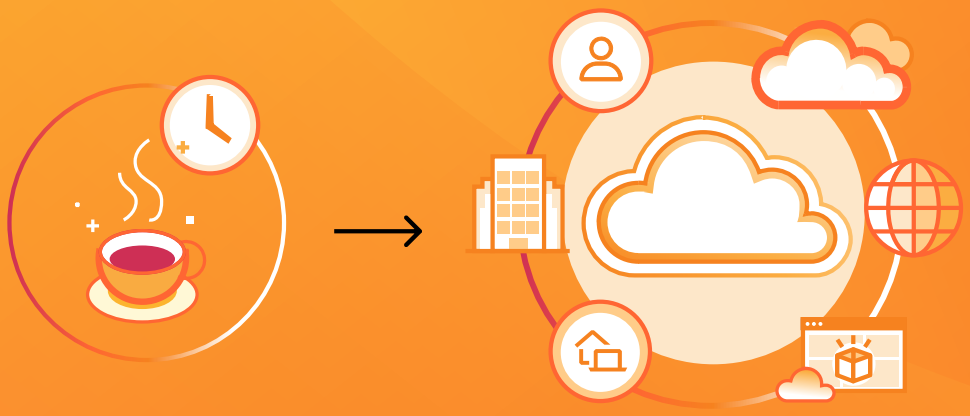
CLOUDFLARE

WHITEPAPER

Coffee shop networking with Cloudflare

A modern architecture for simplified connectivity and security



Content

3 Executive summary

4 A time for change in network architecture

5 The emergence of coffee shop networking

6 Key steps for coffee shop networking

7 Step 1: Establish user access with zero trust

8 Step 2: Enable network access

8 Step 3: Address cloud and web

9 Step 4: Achieve coffee shop networking through infrastructure reduction

10 Realizing the benefits of coffee shop networking

11 Appendix: Connecting to Cloudflare

Executive summary

Networking teams are increasingly pursuing designs that are more flexible, agile, and less capital-intensive. Organizations are borrowing concepts popularized from users working from their local coffee shop: when you grab a latte, sit down, and turn on your laptop, you're joining a public, untrusted network; yet, with the right tools, you can also work with the same applications that you use at the office.

The model for working from the coffee shop is well understood by users, who want the same simple, intuitive experience while at the office. However, to transition from the traditional enterprise private network to one that's more like the coffee shop, organizations need to develop a blueprint that helps them identify the key objectives toward simplicity that make the future state achievable. This paper outlines how to adopt coffee shop networking with Cloudflare.

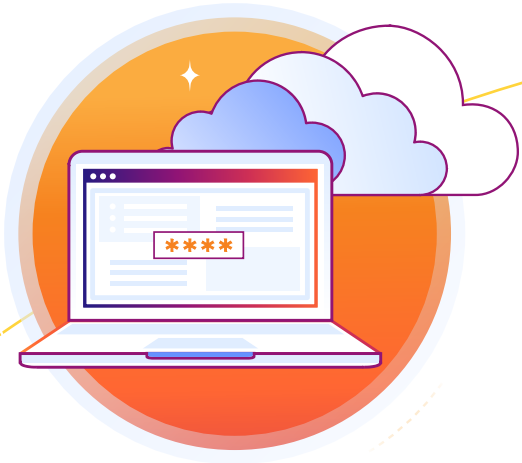
A time for change in network architecture

The traditional enterprise network uses several high-level concepts that are rapidly becoming obsolete.

Castle-and-moat security: Enterprises typically create a trusted private network that connects their offices, applications, and users within a metaphorical castle, separated from the untrusted Internet by a firewall that acts as a moat. To gain access to the trusted network, users authenticate at different network layers, using layer 2 network access controls (NAC) to identify devices, layers 3 and 4 controls to authenticate users and manage ports, and a mix of firewall controls spanning L3–L7 to enforce authorizations. To separate different resources, networks use virtual LANs (VLANs) and presume that anyone or anything that successfully authenticates has a broad level of autonomy to access resources at the same trust level. However, these network layer controls are subject to abuse, which has driven organizations to consider how to implement zero trust for more granular control over which entity can access a given resource.

Hub-and-spoke networking: From a networking point of view, organizations have traditionally used a "hub-and-spoke" model to connect branches to campus data centers via multiprotocol label switching (MPLS). These private circuits take branch traffic back through a security stack at headquarters before routing to the internal data center or egress to the Internet. However, this model has become increasingly inefficient given the rise in cloud applications.

All of these challenges are driving enterprises to simplify their networking environment, improve the user experience, and reduce operational overhead.



The emergence of coffee shop networking

The term "coffee shop networking" (CSN) was coined by Gartner to describe a modern, streamlined network architecture for the hybrid workforce. It takes inspiration from the familiar experience of connecting to the WiFi at a coffee shop, while using business applications in the cloud. In CSN, no part of the network is implicitly trusted, yet employees still work securely because access is enforced independently of the network, using identity and device context.

To make the model effective for the enterprise, IT teams could use the Internet to connect users and branch networks to the SASE services that their organizations need for security, while extending and managing secure connectivity to the cloud.

With the right implementation, the user experience for the hybrid worker is consistent from the office to the coffee shop. In order to make this possible, the organization can take steps to simplify their network topology by implementing the following foundational principles:

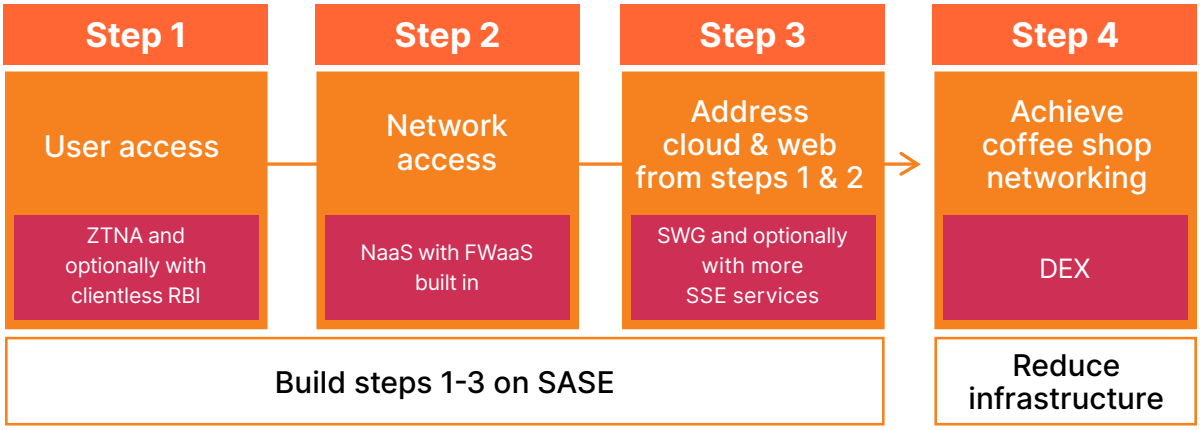
1. **Internet-first connectivity:** Use direct-to-Internet connections from branch locations in order to optimize routing for SaaS and cloud apps.
2. **Zero trust network access (ZTNA) everywhere:** Use ZTNA for access management consistently for users or non-human AI identities everywhere, whether on-prem or remote.
3. **Simplified on-prem infrastructure:** Reduce the hardware footprint at branch locations by using a cloud-managed, lightweight device, with security services delivered from the cloud.
4. **User experience monitoring:** Understand the user experience in order to maintain a high level of user satisfaction and tooling to identify and resolve problems.

These requirements are available today from Cloudflare's SASE platform. Cloudflare One delivers a unified platform that simplifies and modernizes networking and security for users and networks. It is built on a globally distributed, cloud-native architecture that runs all services on every server, ensuring high resiliency and consistent policy application.

The Cloudflare SASE solution, Cloudflare One, includes the following key services: ZTNA (Cloudflare Access), network-as-a-service, or NaaS (Cloudflare Magic WAN), secure web gateway, or SWG (Cloudflare Gateway), firewall-as-a-service, or FWaaS (Cloudflare Magic Firewall), and digital experience monitoring (Cloudflare DEX). All of these services are managed via a single, unified interface with full API and Terraform provider support.

Key steps for coffee shop networking

The journey to simplification provides a path for organizations to unify their strategies across their security and network modernization projects.



Step 1: Establish user access with zero trust

ZTNA is a secure connectivity overlay that provides contextual enforcement of users to applications, AI agents, or infrastructure without being dependent on the security of the network itself. Organizations' initial deployments of ZTNA focused on eliminating the problematic remote access VPN, but within the context of coffee shop networking, ZTNA serves as the foundation for user access from anywhere, both remote and on-prem.

Step 2: Enable network access

For organizations with a large investment in traditional network infrastructure, the shift to an Internet-first level of connectivity can take different steps to support the mix of servers, applications, users, and endpoints. Organizations need to develop a plan to support network access for their particular scenarios using a combination of mesh networking and NaaS.

Step 3: Address cloud and web

With cloud applications requiring Internet access from all locations, organizations can shore up the inconsistent security typically seen in the enterprise. Instead of using a mix of perimeter firewalls, branch firewalls, SWGs, and so forth, apply the Internet-first connectivity principles from steps 1 and 2 to a SASE layer to deliver consistent enforcement of egress policy.

Step 4: Achieve coffee shop networking through infrastructure reduction

With the right SASE services and cloud infrastructure in place, make progress on your simplification journey by systematically reducing and eliminating appliance-based on-prem network infrastructure.

Step 1: Establish user access with zero trust

At its heart, coffee shop networking requires establishing secure communications across potentially untrustworthy, public networks.

In the past, organizations used VPNs to provide temporary network access to the on-prem data center. However, VPNs degrade the user experience, because traffic travels further the farther the user is from the VPN concentrator. Users are tempted to leave the VPN off to improve performance. When the tunnel is down, or the VPN is used in a split tunnel configuration, the user gains performance, but the organization loses visibility and the ability to consistently enforce policy.

On the security side, VPNs are also flawed. Because they invoke the castle-and-moat model, "trusted" users are provided too much access to the corporate network and the connected endpoint. The VPN gateway itself is public-facing, and subject to exploitation as well.

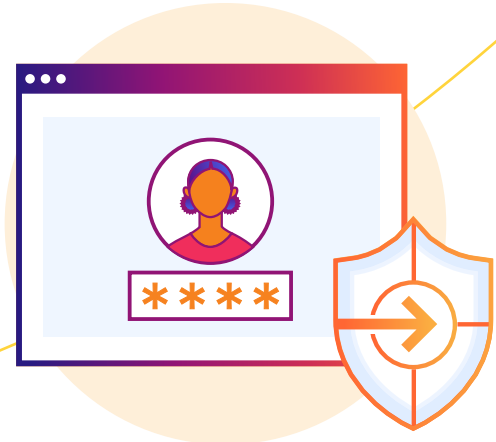
Instead of a VPN, Cloudflare's ZTNA service, Access, solves for the user experience, performance, and security by using cloud-delivered infrastructure to broker secure user access to private applications and infrastructure targets in any location. That's because with ZTNA, organizations can overcome the backhaul problem by connecting to a nearby Cloudflare data center (rather than a distant VPN concentrator) to enforce access policy to private applications in the private cloud, hybrid cloud, or public cloud.

With Access, organizations can apply contextual controls that provide users access to applications, AI agents, and infrastructure rather than connecting endpoints to the network. Unlike a VPN, with ZTNA, the endpoint isn't placed "on" the network, but rather the user is given the precise level of access needed to perform their work, and nothing more.

ZTNA solves for access from any location, not just in remote scenarios. In fact, if the user experience works well when the user is not at the office, then why not use the same measures for consistent enforcement of policy when the user is in any office? If the guest network replicated the coffee shop WiFi experience, then there would be no need to implement anything other than Internet connectivity, thus providing the opportunity for further simplification of infrastructure down the road.

Key benefits of ZTNA for user access include:

- **Consistent user experience:** Employees have the exact same login process and application or agentic AI access experience whether they are at corporate headquarters, a local coffee shop, or their home office.
- **Fast performance without backhaul:** ZTNA with Access uses the global Cloudflare network for a nearby connection no matter where the user is located.
- **Uniform security posture:** Whether on-prem or off-prem, all users experience consistent enforcement of policy. Security policies use contextual information including user identity, device identity, and device posture to enforce least-privilege access controls uniformly.
- **Reduced attack surface:** With Access, organizations do not need to expose their infrastructure to inbound traffic. Access brokers connections between the client and an outbound connection from the app or infrastructure resource over Cloudflare Tunnel.



Step 2: Enable network access

The foundation of coffee shop networking is established in step 1 by securing all user access (to private apps and the Internet) through ZTNA. In an ideal scenario, where every endpoint could run a zero trust agent, this might be sufficient.

However, physical branch, campus, and data center locations have realities that an agent-centric model alone cannot address. The goal of the second step, therefore, is to modernize the network infrastructure to handle these realities without recreating the complexity of the legacy WAN (MPLS and heavy hardware stacks).

To enable modernized network access, organizations must address three specific challenges at the branch:

1. **Non-user traffic:** Offices contain numerous devices such as printers, WiFi access points, security cameras, and other IoT/OT devices that cannot run a ZTNA agent. This "headless" traffic requires a network-level on-ramp to securely connect to internal resources or the Internet.
2. **High availability (HA):** Branch offices require resilient Internet connectivity. A mechanism is needed to manage multiple Internet links (e.g., fiber with 5G backup) and perform dynamic path selection to ensure uptime.
3. **Basic LAN management:** Even simplified networks need traffic management. For example, segmenting user traffic from IoT/OT devices is good practice, while still allowing minimal local routes on an as-needed basis.

To establish modernized network access for branches, data centers, and non-user devices (like servers or IoT), Cloudflare offers two approaches, with NaaS providing the foundation for WAN modernization.

Approach 1 — NaaS with Cloudflare Magic WAN: For organizations that need to support numerous locations across a WAN, retire MPLS, and handle traffic from both users and non-users, the primary strategy is to deploy Magic WAN.

Magic WAN provides NaaS by leveraging the Cloudflare global network as the new corporate backbone. This is enabled by a lightweight edge device: the Cloudflare Magic WAN Connector (available as an appliance or VM). Instead of using conventional MPLS, organizations extend their WAN using local Internet connections. Magic WAN provides cloud-delivered network services for performance optimization, routing, and security (FWaaS, or firewall-as-a-service). With services deployed from the cloud, the network team can significantly reduce the hardware footprint at the branch, retire legacy routers and firewalls, and centrally manage network and security services across the globe.

Approach 2 — Mesh networking with Cloudflare WARP Connector: Full branch network modernization may not be the immediate goal for your organization. In specific scenarios such as connecting isolated servers, specialized environments, or specific subnets, mesh networking offers a tactical solution.

Mesh networking provides site-to-site connectivity as an extension of zero trust, using the software-based Cloudflare WARP Connector. It can be used to facilitate zero trust connections to other WARP Connectors (for site-to-site connectivity between subnets) or end-user endpoints with the WARP client (to support use cases for server-initiated traffic). Mesh networks operate as a secure overlay, providing ways to extend connectivity without requiring changes to the underlying network itself.

With Cloudflare, you can leverage NaaS (Magic WAN) as the strategic path for WAN modernization, complemented by mesh networking for specific connectivity needs.

Step 3: Address cloud and web

The growing number of cloud and web applications have created part of the network complexity problem. As discussed, the problems occur while trying to overcome the conflicting objectives among network performance, security requirements, and the corresponding complexity.

Conventionally, the options for addressing how users and networks connect to the cloud and web include:

- **Internet breakout at the branch/split tunnel at the endpoint:** To reduce backhaul to a security appliance, organizations sometimes permit user traffic to egress directly to the Internet. These options may improve performance to the cloud and the Internet, but decrease visibility and control. The breakout traffic is no longer visible to the IT organization, thus creating a security gap.

- **SWG point products for branch/remote user endpoint traffic:** To shore up security problems for the breakout traffic, some organizations use a SWG to provide some incremental protection. However, if there is a discrepancy between the policies enforced by the SWG and the policies enforced by the perimeter firewall, this creates a new set of complexity problems.
- **More infrastructure:** To limit backhauling to a security appliance, organizations might add more firewalls. In the case of branch offices, this would mean deployment of branch firewalls or unified threat management (UTM) appliances to permit local egress. In the case of remote users, organizations may attempt to reduce performance latency by adding more VPN gateways with firewalls around the world. Both scenarios add more infrastructure to try and address the security problem, which further compounds the complexity of managing even more hardware.

Cloudflare's SASE architecture overcomes the trade-offs normally seen with traditional approaches. Instead of sending private traffic and cloud traffic in different directions, the network traffic path is consistent with Cloudflare. Whether at the branch or remote, all traffic goes to a Cloudflare data center. From the Cloudflare network, access to the cloud and Internet are protected by policies from Cloudflare's SWG, FWaaS, CASB, and DLP services.

Using Cloudflare, there are no performance or security tradeoffs, because traffic is locally processed from the Cloudflare data centers, which operate from 300+ cities around the world. Your branches do not need to deploy more infrastructure because they are leveraging the services delivered from our data centers.

Step 4: Achieve coffee shop networking through infrastructure reduction

By using Cloudflare's network as an extension of your own, a number of network architectural constructs and on-prem hardware appliances can be either minimized or eliminated. You can systematically reduce the on-prem infrastructure footprint that creates IT complexity by shifting user-to-application security and connectivity to Cloudflare, and right-sizing what remains on site.

From the "user access" perspective:

- **Eliminate VPN concentrators globally:** Access runs in the cloud and provides per-application, least-privilege access without requiring on-premises remote access VPN concentrators. Decommission legacy RA-VPNs as you complete migration of user groups and apps.
- **Monitor user experience with DEX:** Schedule lightweight HTTP and traceroute checks from WARP-enrolled devices to public apps protected by Gateway; track real-time and historical page-load, DNS, and server-response metrics in Cloudflare Dashboard; enable DEX notifications to flag connectivity or performance degradation; and trigger remote captures to collect on-device diagnostics for faster root-cause analysis.

From the "network access" perspective:

- **Downsize branch hardware footprint:** With the broader adoption of SASE, organizations can offload capabilities for network security through Cloudflare One rather than manage yet another branch firewall. With security delivered through Magic Firewall within Cloudflare One, true layer 3 firewall policies are deployed globally in the cloud within seconds, without the headaches of conventional on-prem hardware upgrades and policy changes.
- **Use cloud-delivered composable services:** This will help avoid disruptively inserting network appliances to add functionality and support new requirements. The network connection to the cloud service remains the same — only the policies affecting how the traffic is processed is changed.
- **Streamline data center firewall policies:** Reduce the attack surface by blocking all inbound traffic and eliminating allow policies for users. Access applications, Model Context Protocol (MCP) servers, and infrastructure targets through the steps taken to implement ZTNA.
- **Simplify the LAN:** With local Internet breakouts and user-to-app policy enforcements now in place, standardized LAN designs replace the need for bespoke VLANs. Precise, per-resource authorization replaces excessive network access — and the LAN stays focused on reliable connectivity and basic segmentation.

There is another aspect of infrastructure reduction that's possible as well: use SASE to consolidate operations for both ZTNA and NaaS from the same platform. Since SASE provides a converged architecture for security and networking from the same infrastructure, ongoing management is easier. This approach is known as single-vendor SASE, which is available through Cloudflare One.

Realizing the benefits of coffee shop networking

This paper discusses the path toward coffee shop networking using Cloudflare. With the proper plan, organizations can take advantage of a number of benefits through this approach compared to their traditional connectivity:

- **Lower total cost of ownership (TCO):** By reducing the number of security subscription services on firewalls, lowering capital expenditures on hardware appliances and administrative overhead, and using Internet connectivity instead of private MPLS circuits, organizations can dramatically reduce their TCO for networking.
- **Simplicity:** Reducing hardware with coffee shop networking eliminates the expense of maintaining a large footprint at remote locations such as branch offices, while reducing complexity and the need for dedicated on-site IT staff.
- **Agility:** The cloud-native approach of coffee shop networking allows for rapid deployment of new sites, and instantaneous updates to network and security policies.
- **Scalability:** The architecture is designed to grow with the business, enabling IT to manage a highly distributed network at a massive scale — with minimal operational overhead.
- **Consistency:** Every user, regardless of their physical location, benefits from a uniform end-user experience and a single security posture.
- **Cost optimization:** The light network edge approach to networking reduces capital expenses, without having to acquire and depreciate hardware.

These are but a few ways that the coffee shop networking model can help your organization. To learn more, contact your Cloudflare team to start planning your simplification journey.

Appendix: Connecting to Cloudflare

Cloudflare offers a number of ways to connect users, devices, applications, and sites to a Cloudflare data center. The following options are available:

User and device connectivity

Cloudflare supports both agent-based and agentless methods for users and devices to connect to our platform.

- **Software agent (WARP client):** The unified software agent, called WARP, securely on-ramps user traffic on managed endpoints to the Cloudflare platform. It is supported on various operating systems, including Windows, macOS, Android OS, iOS, and Linux.
- **Agentless access:** Cloudflare provides agentless options, which organizations can use with bring your own device (BYOD) or third-party contractor endpoints.
- In addition, organizations can use Cloudflare services using **other integration methods,** such as proxy auto-configuration (PAC) files or OS/browser-level DNS configurations.

Network, application, and server connectivity

For connecting physical locations, data centers, and cloud environments, Cloudflare offers several methods:

- **Cloudflare Tunnel**
  - **cloudflared:** Lightweight daemon connects private hosts to Cloudflare without requiring public-facing IP addresses or inbound firewall allow policies. This connector can be deployed on any compute environment, including VMs, bare metal servers, or containers.
  - **Cloudflare WARP Connector:** An agent that enables server-initiated / bidirectional traffic, mesh networking, and site-to-site connectivity. It acts as a router that establishes a connection between a private subnet and a Cloudflare data center.
- **Cloudflare Magic WAN tunnels (IPsec/GRE):** Customers can connect their networks using standard IPsec or GRE tunnels to the cloud-native Magic WAN service. This supports compatibility with existing third-party network devices and SD-WAN vendors.
- **Cloudflare Magic WAN Connector appliance:** A plug-and-play, fully cloud-managed device available as a physical appliance or a VM. It enables zero-touch connectivity from customer branches to a Cloudflare data center via IPsec WAN tunnels.
- **Cloudflare Network Interconnect (CNI):** For better security and performance than the public Internet, CNI offers direct circuit-based interconnects to the Cloudflare network. CNI supports direct physical connections as well as virtual connections over a mutual partner.

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

REV:BDES-8471.2025NOV18