AYI NEDJIMI Consultants

Cloudflare Zero Trust : Guide Complet Tu

29 April 2026 • Mis à jour le 29 April 2026 • 51 min de lecture

Guide complet Cloudflare Zero Trust : Cloudflare One, Tunnel, Access, Gat
d'usage, pricing et limites.

Face a l'explosion du travail hybride, a la multiplication des surfaces d'attaque et a
perimetriques traditionnelles, le modele **Zero Trust** s'est impose comme le nouvea
les acteurs qui ont democratise cette approche, **Cloudflare** occupe une place sing
de 300 points de presence, la plateforme **Cloudflare One** propose une suite integr
Browser Isolation, DLP et CASB — capable de remplacer integralement un VPN d'
sans precedent. Dans cet article de reference, nous decortiquons chaque brique d
fondements theoriques du modele ZTNA jusqu'au deploiement concret avec fichie
Terraform. Que vous soyez RSSI, architecte cloud ou ingenieur DevOps, vous trou
et exploiter une architecture **Zero Trust Network Access** basee sur Cloudflare, av
une analyse critique des limites de la solution.

Pourquoi le VPN est mort : l'avenement du Zero Trust

Pendant plus de vingt ans, le VPN (Virtual Private Network) a constitue la pierre an
d'entreprise. Le principe etait simple : etablir un tunnel chiffre entre le poste de l'u
large — souvent trop large — a l'ensemble des ressources situees derriere le pare
physiques residaient dans un datacenter unique et ou les employes travaillaient ex
hypothese fondamentale : **tout ce qui se trouve a l'interieur du perimetre est dign**

Cette hypothese s'est averee catastrophique. Les violations de donnees les plus c
Colonial Pipeline, Uber 2022 — ont toutes exploite le meme schema : un attaquant
compromission d'un fournisseur), puis se deplace lateralement a l'interieur du res
par l'architecture perimetrique. Une fois le VPN franchi, l'attaquant dispose des m
davantage s'il escalade ses droits.

Le modele **Zero Trust**, formalise par John Kindervag chez Forrester en 2010 puis d
800-207, repose sur un axiome radicalement different : **ne jamais faire confiance,**
provienne de l'interieur ou de l'exterieur du reseau — doit etre authentifiee, autori
de zone de confiance implicite.

Les piliers du Zero Trust selon le NIST et la CISA sont les suivants :

- **Verification continue de l'identite** : chaque utilisateur et chaque appareil doive
  seulement lors de la connexion initiale.
- **Principe du moindre privilege** : l'acces est accorde uniquement aux ressources
  necessaire.
- **Microsegmentation** : le reseau est decoupe en segments granulaires, empecha
  compromission d'un segment.
- **Posture de l'appareil** : l'etat de securite du terminal (OS a jour, antivirus actif, c
  d'autoriser l'acces.