Ekinops U-ZTNA

Modernisez vos accès distants

Juin 2026

Les organisations font face à de multiples défis

Pas seulement ceux liés à la sécurité mais aussi les défis liés à la connectivité

Connectivité

Connecter des utilisateurs où qu'ils se trouvent aux applications dont ils ont besoin, à partir de réseaux hybrides.

Gouvernance et Responsabilité

Les organisations doivent gérer des actifs exposés,une surface d'attaque importante, des vulnérabilités, mais aussi la conformité aux réglementations, les engagements avec les fournisseurs d'accès et de cloud, et enfin avec les contraintes de souveraineté.

Complexité

Les départements informatiques ont empilé de multiples solutions (VPN, Bastion, reverse proxy, etc.) qu'il est aujourd'hui couteux et complexe d'administrer.

Le besoin d'un « ZTNA universel »

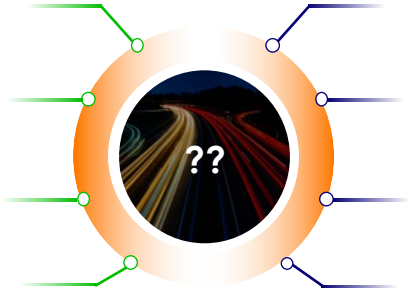
Gouvernance et sécurisation des nouveaux usages

Employés, clients, partenaires, objets, agents IA… Partout !

- Mobilité
- Siège social
- Bureaux
- Campus, usines, etc.

CHALLENGES

Comment pouvons-nous lier facilement ces deux mondes tout en garantissant une sécurité absolue de l'accès aux ressources ?



Applications, données, documents, processus… Partout !

- Internet
- Cloud privé
- Cloud public
- Centre de données

Solutions Traditionnelles

Les conséquences du passé

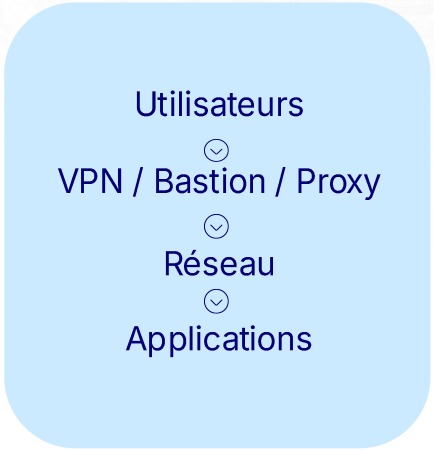
Empilement de Solutions

- En 20 ans, des solutions qui se cumulent
- VPN → Pour les employés
- Bastions → Pour les admins
- Reverse proxy → Pour certaines applications
- Solutions multi-vendeurs, séparées

Problèmes

- Vulnérabilités de sécurité
- Surface d'attaque large
- Mouvements latéraux possibles
- Applications exposées
- Problèmes opérationnels
- Trop d'outils
- Complexité
- Mauvaise expérience utilisateur

Architectures traditionnelles



Les architectures d'accès actuelles sont basées sur le réseau, alors que le monde est devenu applicatif

Le « ZTNA Universel »

Une nouvelle façon de gérer les accès aux ressources

Un principe simple

Gérer l'accès aux applications, pas au réseau

Utilisateurs

⌄

Universal ZTNA Gateway

⌄

Applications

Problèmes

Le système vérifie en permanence :

- L'identité
- Le device
- Le contexte
- La politique de sécurité

Et permet d'accéder à toutes les applications

- Web
- Client-server, SSH / RDP
- Datacenter, cloud

« Universel » ? :

parce qu'**un seul modèle d'accès** sécurisé est utilisé **pour toutes les applications** (applications web, applications client-serveur, SSH/RDP, Clouds, Datacenters,...)
et ce **quelque soit l'emplacement de l'utilisateur** (depuis le réseau local ou en mobilité)

Pourquoi le modèle ZTNA est devenu crucial

Zoom sur le contexte du cyberespace

Problématique de surface d'attaque

Quand un utilisateur se connecte :

- il **reçoit une IP interne**
- il est **dans le réseau**
- il peut **voir beaucoup plus que nécessaire**

Conséquences de la compromission

L'attaquant peut:

- Scanner le réseau
- Rebondir entre serveurs
- Atteindre des systèmes critiques

C'est ce qu'on appelle le **mouvement latéral**, présent dans presque toutes les attaques modernes.

Contexte du Risque Cyber

- La fréquence et la sophistication des attaques augmentent
- Les VPN sont remplis de vulnérabilités (CVE)
- Les identifiants sont les premières infos volées et sont échangés contre des centimes sur le darknet
- L'IA générative est en plein essor (Mythos)
- 97 % des attaques ne piratent pas : elles se connectent

Exemples d'attaques majeures basées sur ces éléments : *Colonial Pipeline ransomware attack* / *GitHub and TeamPCP*
Le point commun : La confiance implicite permet à l'attaque de se propager.

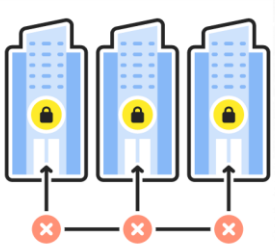
Avec le modèle ZTNA, **l'utilisateur n'entre jamais dans le réseau.**
Il permet de passer d'une logique de confiance implicite à **une logique de vérification continue**.
Le système vérifie l'identité, le device, le contexte et donne **accès uniquement** à l'application autorisée.
Le périmètre d'attaque est limité et contraint

“Sécurité réseau“ vs “Sécurité des applications“

Pourquoi les solutions héritées du passé sont toujours nécessaires mais plus suffisantes?

Les défenses de sécurité périmétriques basiques sont difficiles à franchir, mais une fois qu’un acteur malveillant a réussi à pénétrer, il peut se déplacer librement à l'intérieur du réseau

Modèle traditionnel	Modèle Zéro confiance
Accès au niveau réseau	Accès au niveau de l'application
Confiance une fois connectée	Ne jamais faire confiance, toujours vérifier
Authentification lors de la connexion	Authentification par applications
Confiance implicite	Contrôle continu
Déplacement latéral complet	Applications invisibles / Déplacement latéral limité
Conçu pour le « on-site »	Conçu pour le Cloud



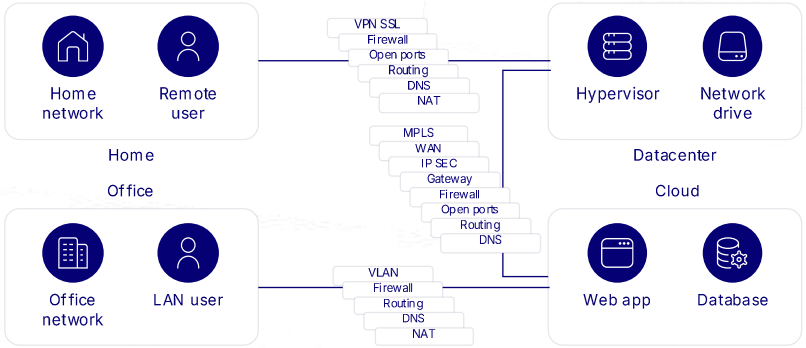
Un réseau complexe qui vérifie en continu chaque demande d'accès, assure une protection renforcée contre les menaces internes et externes

L'avenir de la sécurité ne consiste plus seulement à protéger le réseau,

mais à protéger chaque application individuellement

De la connectivité réseau à la connectivité applicative

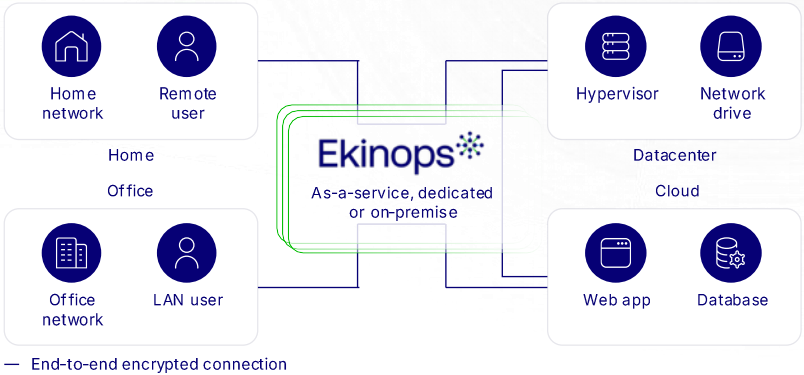
Changements de modèles et de points de vue



Modèle hérité

Des couches de solutions empilées pour interconnecter les réseaux et couvrir différents usages.

Complexe à gérer, sécuriser, mettre à niveau et utiliser



Nouveau modèle

Ekinops Universal ZTNA vise à connecter les utilisateurs de manière sécurisée et directe à leurs applications.

Une seule plateforme, un seul réseau, intégré à Ekinops SASE

Les architectures Zero Trust sont recommandées par les agences gouvernementales et les organismes de normalisations majeurs: **NIST, DoD/NSA, CISA, ENISA, ANSSI**

Ekinops U-ZTNA

En quelques mots

Ekinops U-ZTNA est une approche de cybersécurité qui vise **à sécuriser l'accès aux applications** plutôt qu'à l'ensemble du réseau.
Il repose sur **une vérification stricte et continue de chaque posture d'utilisateur et d'appareil** avant d'accorder un accès à une ressource spécifique.

U-ZTNA

Pour les organisations qui cherchent à renforcer leur résilience face à **des menaces de plus en plus automatisées**, le **modèle ZTNA** devient **un levier de protection central** et non pas un simple complément technique

Les principaux **bénéfices** d'Ekinops U-ZTNA sont :

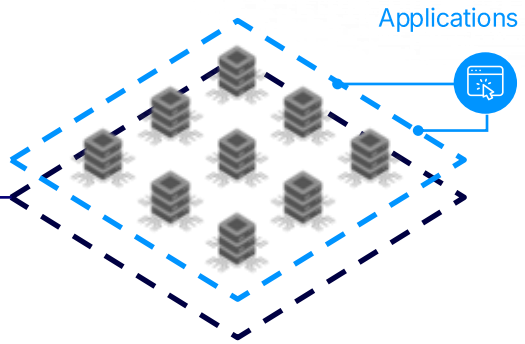
- Limitations et contrôles pour renforcer la sécurité des accès
- Protection des environnements hybrides et distants
- Réduction significative de la surface d'attaque
- Simplification de la conformité réglementaire
- Amélioration de l'expérience utilisateur pour les administrateurs de sécurité et les utilisateurs finaux

Ekinops U-ZTNA contrôle tous les accès

UTILISATEURS
GROUPES D'UTILISATEURS

- **Validation de l'utilisateur**
- **Authentification forte** — *MFA, Passwordless*
- **Contrôle de la posture de l'appareil** — *OS, environnement, antivirus, EDR...*
- **Accès *Moindre Privilège***
- **Activation du contrôle contextuel permanent**
- **Accès aux applications**

U-ZTNA



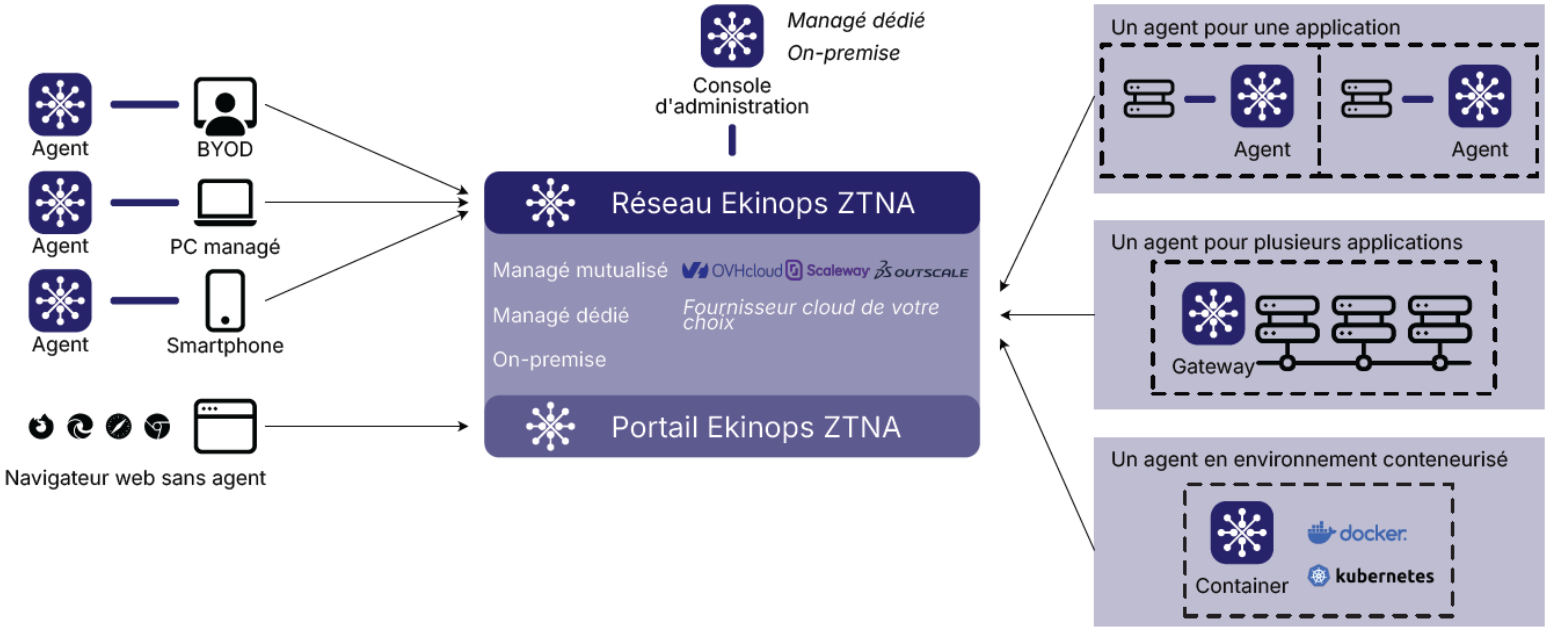
Réseau Ekinops ZTNA

Avantages Majeurs

- Indépendance de tout opérateur tiers
- Chiffrement de bout en bout natif (*True* ZTNA)
- Invisibilité des infrastructures IT et des applications
- Tolérance aux fautes et aux compromissions

Ekinops Universal ZTNA

Architecture avec ou sans agent, « as-a-service » mutualisé ou dédié, on-premise ou hybride



LE RÉSEAU DISPARAÎT DU MODÈLE D'ACCÈS → FOCUS SUR LES APPLICATIONS

Ekinops U-ZTNA

Caractéristiques Principales

- Nombre illimité d'applications
- Trafic illimité
- Multi-OS : Windows, Mac OS, Linux, iOS, Android
- Modes de déploiement Agent et Agentless
- Portail web d'administration avec accès sécurisé
- Indépendant de tout fournisseur Cloud
- Micro-segmentation
- Chiffrement de bout en bout
- Journaux de connexion et administratifs
- Authentification sans mot de passe
- Intégrations avec les fournisseurs d'identité (IdPs)
- Vérification de la posture des appareils (antivirus, verrouillage d'écran et pare-feu)
- Sensibilisation au contexte (validation des conditions d'accès, y compris sur les conditions géographiques))
- Capacités de redirection et d'exportation de journaux
- MFA OTP (mot de passe unique dédié et personnalisable)
- Haute disponibilité (active/passive)
- Sensibilisation aux changements en temps réel
- Gestion des Bastions avec enregistrements de sessions
- Routage cryptographique (basé sur des paires de clés)

U-ZTNA

DISPONIBLE EN SAAS, ON-PREMISE ET HYBRIDE
TARIFICATIONS SELON ABONNEMENTS ANNUELS PAR UTILISATEURS

ZTNA “Classique”

Le problème

BEAUCOUP DE SOLUTIONS ZTNA SONT PARTIELLES

Limites Fréquentes:

- Sécurisent seulement les applications web
- Nécessitent un agent lourd
- Accès non uniformes
- Séparation des solutions cloud/on-prem

Les entreprises finissent avec:

- VPN
- ZTNA
- Bastion
- Reverse proxy
- Architectures complexes
- Des accès fragmentés…

La plupart des solutions ZTNA ne couvrent qu’une partie des problèmes

Pourquoi choisir Ekinops U-ZTNA?

Différenciateur clé sur d'autres vendeurs de solutions du marché

Implémentation	"Invisibilité" des points d'accès	Indépendance aux infrastructures
Broker tiers	✓	✗
Passerelle exposée	✗	✓

Les deux approches ont des avantages et des inconvénients :

- ***Invisibilité des points d'entrée*** **:** mais dépendance à l'infrastructure avec risques d'indisponibilité et d'éventuels accès aux services de l'entreprises en cas de compromission…
- ***Indépendance opérationnelle*** **:** mais passerelle exposée à des points d'entrée visibles

Le différentiateur majeur d'Ekinops U-ZTNA est de combiner le meilleur des 2 approches :

- **Invisibilité des points d'entrée Internet :** moins de surface d'attaque
- **Indépendance vis-à-vis d'un tiers de confiance :** réduction des coûts et résilience accrue

Ekinops ZTNA	✓	✓

La proposition de valeur d'Ekinops U-ZTNA

Authentique approche *Zero Trust*

Sécurité renforcée

- Plus de réseau exposé
- Plus de « lateral movement »
- Principe « **least privilege** »

Simplification des Opérations

Le ZTNA peut remplacer :

- VPN
- Bastions
- Reverse proxy
- Accès partenaires séparés

Meilleure expérience utilisateurs

- Accès direct aux applications
- Passwordless / SSO
- Pas de tunnel global
- Performance améliorée
- Transparence totale en cas d'audit

Ekinops U-ZTNA

Principaux Bénéfices

Renforcement de la Cybersécurité

- Visibilité accrue sur les activités par utilisateur
- Assure un contrôle efficace de qui a accede à quoi et quand
- S'applique aux utilisateurs sur site ainsi qu'aux utilisateurs à distance, y compris les nomades et les travailleurs à domicile
- Améliore la gestion des appareils personnels pour accéder aux données professionnelles (BYOD)
- Suppression de toutes les dépendances à l'infrastructure réseau.
- Sécurise l'accès aux environnements multi-cloud sans mot de passe avec une granularité Utilisateur

Augmentation de la sécurité applicative

- Chiffrement de bout en bout (AES 256)
- Haute Disponibilité (actif/passif)
- Accès Moindre Privilège
- Standardisation des niveaux d'accès et de sécurité des échanges sur l'ensemble du SI

Souplesse d'intégration

- Compatibilité avec l'existant
- Intégration simple et rapide
- Aucune inspection de traffic: les données privées restent privées

Facilite la conformité réglementaire

- Contrôles d'accès standardisés, alignés avec les exigences réglementaires (RGPD, NIS2)
- Traçabilité claire et exploitable des accès aux applications et aux données (NIS2, DORA)
- Référentiel centralisé des applications : utile pour les audits.
- Justifications simplifiées des mesures de sécurité mises en place.

Ekinops U-ZTNA

Sécurise tous les accès distants, quelque soit la source, et sur tous les appareils




Authentique *Zero Trust*

- Vérifications permanentes de postures utilisateurs et appareils
- Indépendance aux fournisseurs tiers
- IT sous-jacente rendue invisible
- Chiffrement de bout-en-bout (AES 256)
- Authentification forte sans mot de passe
- Accès Moindre Privilège

Universel

- Un seul mode d'accès sécurisé pour toutes les applications, quelle que soit la localisation de l'utilisateur
- S'applique à tous les protocoles (web, SSH, RDP, DB, protocoles propriétaires et personnalisés…)
- Disponible en version *Agentless*
- Solution de Bastion incluse
- S'applique à tous les postes travail, tous les mobiles et tous les OS

Sécurité & Conformité

- Entreprise européenne : la seule solution ZTNA native (non héritée des solutions traditionnelles)
- Contribue à votre conformité RGPD, NIS2, DORA : Auditabilité complète
- Résilience aux compromissions
- Conçue pour les boucliers de protection d'aujourd'hui et de demain

Simplicité & Efficacité

- 80% de réduction des risques d'intrusion
- Peut fonctionner sur site, dans un cloud privé, SaaS ou hybride
- Facilité d'integration
- Transparence pour les utilisateurs finaux
- 5 fois moins de temps d'installation et de configuration que les solutions traditionnelles

Le “Zero Trust” … et la confiance numérique?

Pas de “Zero Trust” sans souveraineté

Pourquoi une solution Européenne ?

Souveraineté
- Contrôle des données
- Juridiction européenne

Confiance
- Pas de dépendance stratégique
- Alignement réglementaire

Proximité
- Support local
- Compréhension des exigences européennes

Principes Fondamentaux

Never trust, always verify
- accès **par application**
- basé sur **l’identité**
- contrôlé par **politiques dynamiques**

Bénéfices :
- aucune exposition réseau
- applications invisibles
- accès minimal

Qui contrôle réellement l’accès à vos applications critiques ?

Ekinops est la seule plateforme Universal ZTNA et SASE conçue et opérée en Europe, offrant sécurité Zero Trust native et souveraineté numérique.

Universal ZTNA

AES-256
Chiffrement de bout en bout

Journaux d'accès détaillés

5 000 +
Protocoles pris en charge

Ekinops

As-a-service*, dédié ou *on-premise

OVHcloud
Scaleway
OUTSCALE

Modes as-a-service et dédié hébergé sur du cloud souverain

Accès réseau Zero Trust

Accès aux applications et services simple et sécurisé

Passwordless
Authentification forte par certificat et authentification multifacteur

Présence mondiale
Avec plus de 25 points de présence répartis sur le globe et activables sur demande

Surface d'attaque invisible

Vérification de la conformité utilisateur et appareil

Antivirus · Pare-feu · OS · Mises à jour · Screenlock · Processus · Localisation · Horaires

Microsoft Entra ID · okta · SafeNet Trusted Access from THALES

Connexion aux fournisseurs d'identités tiers

Windows · Windows Server · chromeOS · Android · macOS · iOS · iPadOS · Ubuntu · debian · CentOS · Red Hat

Haute disponibilité
Connecteur et passerelle configurable en actif-passif

99.99%
de disponibilité sur l'année écoulée

UNIVERSAL ZTNA ASSURE **CONNECTIVITÉ** ET **CYBERSÉCURITÉ**

Ekinops

MERCI

www.ekinops.com