

# Zero Trust Network Access (ZTNA) – Principes et mise en oeuvre

2 jours (14 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

**1950 € HT** par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

## Objectifs

A l'issue de cette formation, vous serez capable de :

- Reconnaître les principes et les enjeux du modèle Zero Trust
- Identifier les différences entre VPN classiques et ZTNA
- Concevoir une architecture Zero Trust adaptée à votre entreprise
- Mettre en oeuvre une solution ZTNA open source sur Linux ou Windows
- Configurer un proxy Zero Trust avec authentification centralisée (SSO, MFA)
- Appliquer la segmentation applicative et la vérification des accès
- Intégrer des outils ZTNA avec des exigences de conformité (ISO 27001, NIS2, RGPD)
- Réaliser un déploiement ZTNA sécurisé et auditable.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

Administrateurs systèmes et réseaux, responsables sécurité IT, ingénieurs infrastructure, chefs de projet sécurité ou IT.

### Prérequis

Avoir une bonne compréhension des réseaux TCP/IP, NAT, DNS, une maîtrise de base des environnements Linux et Windows ainsi qu'une connaissance des fondamentaux de la sécurité informatique (Firewall, VPN, IAM).

# Programme

## 1 Pendant votre formation

### Zero Trust Network Access (ZTNA) – Principes et mise en oeuvre

Jour 1 – Matin

#### Introduction au Zero Trust et au ZTNA

- Origine et nécessité du Zero Trust dans un contexte de transformation numérique
- L'IT face à la mobilité et les menaces internes
- Les VPN
  - Définition et fonctionnement
  - Modèle de confiance implicite
  - Accès réseau large
- Principes du ZTNA
  - "Never trust, always verify"
  - Accès par application
  - Segmentation logique
- Présentation d'une architecture ZTNA typique
  - Les agents
  - Les brokers
  - Les connecteurs
- Aperçu des standards et cadres de référence
  - NIST SP 800-207
  - ANSSI
  - Architecture SASE

#### Exemples de travaux pratiques (à titre indicatif)

- *Déploiement de Pritunl Zero (ZTNA open source)*
  - *Installation de Pritunl Zero sur Ubuntu Server (via APT ou script fourni)*
  - *Configuration initiale de l'interface d'administration (certificats, utilisateurs)*
  - *Déclaration et publication d'une application Web interne (ex. site intranet)*
  - *Intégration d'un fournisseur d'identité (Keycloak ou Azure AD) en OIDC / SAML*
  - *Test d'accès par un utilisateur test : authentification, redirection, accès par application*
  - *Vérification du filtrage d'accès et du cloisonnement réseau*

Jour 1 – Après-midi

#### Gestion des identités et politiques d'accès ZTNA

- Les concepts-clés
  - IAM
  - IdP
  - Les groupes
  - Les rôles
  - Les attributs de contexte
- Protocoles d'authentification utilisés en ZTNA
  - SAML
  - OAuth2
  - OIDC
- Keycloak
  - Présentation
  - Création de realm
  - Les utilisateurs
  - Les clients
  - La MFA
  - Gestion des identités centralisées
  - SSO
  - Gestion de session
- Panorama de solutions ZTNA commerciales et open source : Tailscale, OpenZiti, Zscaler ZPA, Cloudflare Access...
- Posture de l'appareil
  - Vérification du terminal
  - Conformité AV
  - Le rôle du système d'exploitation
  - Le chiffrement

## Jour 2 – Matin

### Exemples de travaux pratiques (à titre indicatif)

- Mise en oeuvre d'un proxy ZTNA (Pomerium + Keycloak)
  - Installation de Pomerium via Docker Compose
  - Configuration de l'intégration OIDC avec Keycloak (client, secret, redirect URI)
  - Définition de deux routes HTTP sécurisées (applications Web internes)
  - Création de groupes d'accès dans Keycloak et mapping dans les politiques Pomerium
  - Mise en place d'une authentification MFA (optionnelle)
  - Test d'accès depuis navigateur, validation des règles (accès autorisé / refusé)

## Jour 2 – Après-midi

### Sécurité défensive, conformité et micro-segmentation

- Mapping ZTNA basé sur les normes
  - Contrôles d'accès : ISO 27001
  - Minimisation : RGPD
  - Réduction de surface d'attaque : NIS2
- Application du principe du moindre privilège et cloisonnement des flux
- Micro-segmentation : isoler les ressources selon les groupes métier / application / sensibilité
- Supervision et journalisation des accès (logs d'accès, détection d'anomalies)

#### *Exemples de travaux pratiques (à titre indicatif)*

- *Découpage d'une architecture type selon les principes de conformité, de minimisation, de réduction de la surface d'exposition et de micro-segmentation*
- *Ajout d'une deuxième application dans Pomerium ou Pritunl Zero*
- *Attribution de groupes d'accès distincts*
- *Test de la présentation conditionnelle des applications*

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

### Accessibilité aux personnes en situation de handicap

## Sessions

### À distance

Du 15 octobre 2026 au 16 octobre 2026

Du 2 février 2027 au 3 février 2027

### Aix-en-Provence

Du 15 octobre 2026 au 16 octobre 2026

### Angers

Du 15 octobre 2026 au 16 octobre 2026

### Blois

Du 15 octobre 2026 au 16 octobre 2026

### Bordeaux

Du 15 octobre 2026 au 16 octobre 2026

### Bourges

Du 15 octobre 2026 au 16 octobre 2026

**Chartres**

Du 15 octobre 2026 au 16 octobre 2026

**Chateauroux**

Du 15 octobre 2026 au 16 octobre 2026

**Dijon**

Du 15 octobre 2026 au 16 octobre 2026

**Grenoble**

Du 15 octobre 2026 au 16 octobre 2026

**Le Havre**

Du 15 octobre 2026 au 16 octobre 2026

**Le Mans**

Du 15 octobre 2026 au 16 octobre 2026

**Lille**

Du 15 octobre 2026 au 16 octobre 2026

**Lyon**

Du 15 octobre 2026 au 16 octobre 2026

Du 15 octobre 2026 au 16 octobre 2026

**Metz**

Du 15 octobre 2026 au 16 octobre 2026

**Montpellier**

Du 15 octobre 2026 au 16 octobre 2026

**Mulhouse**

Du 15 octobre 2026 au 16 octobre 2026

**Nancy**

Du 15 octobre 2026 au 16 octobre 2026

**Nantes**

Du 15 octobre 2026 au 16 octobre 2026

**Nice**

Du 15 octobre 2026 au 16 octobre 2026

**Niort**

Du 15 octobre 2026 au 16 octobre 2026

**Orléans**

Du 15 octobre 2026 au 16 octobre 2026

**Paris La Défense**

Du 15 octobre 2026 au 16 octobre 2026

Du 23 février 2027 au 24 février 2027

**Poitiers**

Du 15 octobre 2026 au 16 octobre 2026

**Reims**

Du 15 octobre 2026 au 16 octobre 2026

**Rennes**

Du 15 octobre 2026 au 16 octobre 2026

**Strasbourg**

Du 15 octobre 2026 au 16 octobre 2026

**Toulouse**

Du 15 octobre 2026 au 16 octobre 2026

**Tours**

Du 15 octobre 2026 au 16 octobre 2026