

Mis à jour le 26/08/2026

S'inscrire

Formation Prisma Access

2 jours (14 heures)

Présentation

Prisma Access est une solution SSE cloud qui permet de sécuriser les accès distants, les applications privées et le trafic Internet avec une approche unifiée. Grâce aux mobile users, aux remote networks, aux service connections et aux mécanismes avancés de policy et de logging, vous concevez une architecture de sécurité moderne, cohérente et exploitable en production.

Notre formation Prisma Access vous permet de passer des principes de la sécurité cloud à une mise en oeuvre structurée, adaptée aux enjeux opérationnels d'une entreprise hybride.

Vous apprendrez à déployer les composants essentiels, à organiser les flux entre utilisateurs mobiles, sites distants et ressources internes, puis à piloter les règles de sécurité, l'authentification et les chemins de routage.

La formation vous guide également dans la compréhension des service connections, du GlobalProtect, des politiques de sécurité, du déchiffrement et des journaux, afin de fiabiliser les accès et d'améliorer la visibilité.

À l'issue du parcours, vous serez en mesure de configurer une architecture Prisma Access plus robuste, de mieux contrôler les accès aux ressources privées et de préparer un service exploitable dans un contexte de production.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le positionnement de Prisma Access dans une architecture de sécurité cloud.
- Mettre en place les composants clés pour les utilisateurs mobiles et les réseaux distants.

- Configurer les service connections pour relier les utilisateurs aux ressources privées.
- Définir des politiques de sécurité et des règles d'accès cohérentes.
- Exploiter les fonctions de journalisation, de visibilité et de diagnostic pour l'exploitation quotidienne.

Public visé

- Ingénieur sécurité
- Administrateur réseau
- Architecte cloud
- Analyste SOC
- Consultant cybersécurité

Pré-requis

- Connaissances de base en réseaux IP, routage et VPN.
- Pratique préalable d'un pare-feu nouvelle génération ou d'une solution de sécurité réseau.
- Compréhension des principes d'authentification, de contrôle d'accès et de segmentation.
- Expérience d'administration sur une plateforme de sécurité cloud ou d'infrastructure hybride.

Pré-requis techniques

- Un ordinateur portable récent avec suffisamment de ressources pour les manipulations de configuration.
- Une connexion Wi-Fi ou Ethernet stable pour les travaux pratiques et démonstrations.
- Un navigateur web à jour pour accéder à l'interface d'administration et aux consoles associées.
- Un micro-casque recommandé pour suivre la formation à distance dans de bonnes conditions.
- Selon le contexte, un accès à un environnement de test ou à des comptes d'administration fournis pendant la session.

Programme de notre formation Prisma Access

[Jour 1 - Matin]

Fondamentaux de la plateforme

- Positionnement de Prisma Access dans une stratégie de sécurité cloud.
- Architecture générale, composants de service et logique de déploiement.
- Différences entre accès des utilisateurs mobiles et des sites distants.
- Principes de circulation des flux entre Internet, SaaS et ressources privées.
- Lecture des prérequis d'un projet, licences, organisation et gouvernance.
- Atelier pratique : identifier les besoins d'une entreprise fictive et cartographier les usages à couvrir avec Prisma Access.

[Jour 1 - Après-midi]

Déploiement des accès utilisateurs

- Mise en oeuvre des mobile users avec GlobalProtect ou accès proxy selon le besoin.
- Paramétrage des zones, des portails et des passerelles d'accès.
- Gestion de l'authentification, des profils d'accès et des premiers contrôles de sécurité.
- Bonnes pratiques pour sécuriser le trafic Internet et les applications cloud.
- Introduction aux logs utiles pour valider le bon fonctionnement des accès.
- Atelier pratique : configurer un scénario d'accès distant pour utilisateurs mobiles et vérifier la connectivité de bout en bout.

[Jour 2 - Matin]

Connexion aux ressources privées

- Rôle des service connections dans l'accès aux ressources du siège et du datacenter.
- Principes de routage entre mobile users, remote networks et applications internes.
- Choix des sous-réseaux, des régions et des paramètres de tunnel.
- Considérations de résilience, de proximité géographique et de continuité de service.
- Organisation des politiques pour permettre les bons flux sans ouvrir inutilement le périmètre.
- Atelier pratique : construire une connexion de service et valider l'accès à une ressource privée simulée.

[Jour 2 - Après-midi]

Exploitation, sécurité et supervision

- Création et lecture des politiques de sécurité pour contrôler les flux autorisés.
- Introduction au déchiffrement et aux profils associés selon les besoins métier.
- Exploitation des journaux, de la visibilité et des indicateurs de diagnostic.
- Méthodes de validation après changement et points de contrôle en production.
- Bonnes pratiques d'exploitation pour maintenir un niveau de service stable et traçable.
- Atelier pratique : diagnostiquer un incident de connectivité et corriger la configuration à partir des logs et des règles.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs

personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.