

MIGRATION SSL VPN

Solutions Alternatives et Processus de Transition

Fortinet prévoit de décommissionner progressivement le VPN SSL sur les modèles FGT avec 2GB de RAM, affectant plusieurs modèles tels que FGT40F, FGT60F, FGT61F, et FGR60F.

Cette décision vise à améliorer la sécurité et la performance des solutions VPN en proposant des alternatives robustes comme le VPN IPsec, le ZTNA (Zero Trust Network Access), et FortiSASE Hybride.

TRANSITION VPN SSL VERS VPN IPSEC L'indispensable...

- **Budget** : à partir deux jours de configuration
- **Description** : Utilisation du protocole IPsec pour créer des tunnels chiffrés sur Internet
- **Avantages** : Plus sécurisé, plus performant sans changer d'architecture.
- **Prérequis** : Fortigate
- **Étapes de migration** : Configuration VPN IPSEC sur Fortigate en parallèle de l'existant, déploiement manuel de la configuration VPN IPsec sur les endpoints, tests de bon fonctionnement.

• **En option** : Centralisation, management et supervision des Forticlient avec Forticlient EMS Cloud.

- Licence par packs de 25 équipements ou à l'unité à partir de 25
- A partir 2 jours de configuration supplémentaires

...Pour aller plus loin, en termes de sécurité
avec une orientation cloud et ultra mobilité :

TRANSITION VERS ZTNA (ZERO TRUST NETWORK ACCESS)

- **Budget** : sur mesure en fonction de vos besoins
- **Description** : Solution basée sur l'identité, l'application et l'état de conformité du terminal de connexion + vérification continue
- **Avantages** : Remplace l'accès VPN SSL par un accès direct et fluide aux applications, qu'elles soient **on-premise** ou dans le cloud
- **Prérequis** : Fortigate version 7+, FortiEMS Cloud
- **Étapes de migration** : Upgrade du Fortigate, configuration FortiEMS Cloud, création des règles d'accès ZTNA

TRANSITION VERS FORTISASE (SECURE ACCESS SERVICE EDGE)

- **Budget** : sur mesure en fonction de vos besoins
- **Description** : Solution hybride combinant SD-WAN, matériel SD-branch et services de sécurité SSE pour les collaborateurs hybrides
- **Avantages** : Optimisé pour les infras multisites, centralisation des accès distants, intégration progressive ou avancée des services cloud
- **Prérequis** : Vérification de la compatibilité Fortigate avec FortiSASE
- **Étapes de migration** : Validation du besoin client, configuration initiale FortiSASE, déploiement Forticlient avec FortiSASE

ZTNA (ZERO TRUST NETWORK ACCESS)

- Le ZTNA repose sur le principe de ne faire confiance à aucun endpoint jusqu'à preuve de sa légitimité, car tous les endpoints sont considérés comme vulnérables. Peu importe où se trouve l'utilisateur, il se connecte à une gateway (FortiOS, Fortigate, FortiSASE, etc.) qui agit comme proxy pour accéder aux ressources, à condition qu'il soit authentifié et validé par les règles d'accès. Le ZTNA se base sur l'appareil et la ressource, et non sur la localisation de l'utilisateur.
- Le filtrage peut être réalisé en fonction de l'IP ou de l'adresse MAC, avec des tags indiquant si le endpoint est sur site ou à distance, permettant ainsi un filtrage différent selon la situation. L'accès est donné application par application, éliminant le besoin d'un accès large au réseau comme avec un VPN. Une session unique est créée pour chaque accès, et l'expérience utilisateur reste la même, que ce soit à l'intérieur ou à l'extérieur de l'entreprise, avec un accès transparent via la gateway.

FORTISASE (SECURE ACCESS SERVICE EDGE)

- La solution SASE de Fortinet permet un accès sécurisé au Web, au cloud et aux applications pour les collaborateurs hybrides, tout en simplifiant les opérations. Elle combine le SD-WAN (Software-Defined Wide Area Network) avec les services de sécurité SSE (Security Service Edge) FortiSASE fournis dans le cloud pour étendre la convergence de la mise en réseau et de la sécurité de la périphérie du réseau aux utilisateurs distants.
- L'idée est de proposer une solution hybride pour les clients disposant déjà d'un Fortigate. On garde le Fortigate pour gérer les accès et la sécurité sur site pour les utilisateurs, et on utilise FortiSASE avec FortiEMS et ZTNA pour gérer les accès distants. Cela permettra de pousser les clients à migrer petit à petit toute leur infrastructure vers FortiSASE. Forticloud (équivalent Fortigate) permettra de gérer les politiques d'accès et de sécurité pour la partie off net.
- Cela évite de surcharger la bande passante sur site car chaque connexion vers FortiSASE établit un tunnel, et le trafic remonte jusqu'au FortiSASE avant de redescendre sur site.

COMPARATIF DES SOLUTIONS

CARACTÉRISTIQUES	ZTNA (ZERO TRUST NETWORK ACCESS)	FORTISASE (SECURE ACCESS SERVICE EDGE)
Description	Solution basée sur l'identité, l'application et de l'état de conformité de son terminal de connexion + vérification continue	Solution hybride combinant SD-WAN et services de sécurité SSE pour les collaborateurs hybrides
Avantages	Remplace l'accès VPN SSL par un accès direct et fluide aux applications, qu'elles soient on-premise ou dans le cloud	Optimisé pour les infrastructures multisites, centralisation des accès distants, intégration progressive des services cloud
Prérequis	Fortigate version 7+ FortiClient EMS Cloud	Vérification de la compatibilité Fortigate avec FortiSASE
Etapes de migration	Upgrade du Fortigate, configuration FortiEMS Cloud, création des règles d'accès ZTNA	Validation du besoin client, configuration initiale FortiSASE, déploiement Forticlient avec FortiEMS Cloud
Résumé des coûts	Achat des licences pour Forticlient ZTNA pour FortiEMS Cloud	Coût des licences et des services FortiSASE
Résumé du temps	A définir en atelier suivant la configuration client	A définir en atelier suivant la configuration client
Impact	Transition transparente pour les utilisateurs, pas d'impact en temps réel sur la production	Transition transparente pour les utilisateurs, pas d'impact en temps réel sur la production