FICHE SOLUTION

Sécuriser les accès pour le travail à distance à grande échelle

Résumé

Les entreprises peuvent être confrontées à divers scénarios d'urgence potentiels : maladies, inondations, ouragans ou encore pannes de courant. La mise en œuvre d'un plan de continuité des activités est essentielle pour qu'une entreprise puisse rester opérationnelle, même en contexte de crise.

Dans certaines situations, les entreprises se retrouvent dans l'incapacité de poursuivre leurs opérations sur le lieu de travail. Il faut alors pouvoir compter sur le travail à distance tout en préservant l'aspect « sécurité ».

Fortinet offre une solution intégrée destinée à soutenir le télétravail. Les firewalls FortiGate nouvelle génération (NGFW) intègrent la prise en charge des réseaux privés virtuels (VPN) IPsec, pour que les travailleurs à distance puissent se connecter en toute sécurité au réseau de leur entreprise. Avec la protection des postes de travail fournie par FortiClient et grâce à l'authentification multifactorielle (MFA) assurée par FortiAuthenticator, les entreprises peuvent assurer leurs missions á distance et en toute sécurité, pour maintenir leurs activités.

Permettre le travail à distance, de manière sécurisée, est un aspect-clé des plans de continuité et de reprise en cas de sinistre. Une panne de courant, une maladie ou une inondation peut empêcher les employés de se rendre sur leur lieu de travail.

Dans de tels scénarios, une entreprise doit pouvoir assurer une connectivité distante sécurisée au réseau. Les 400 000 clients Fortinet disposent déjà de ce type de capacités. Les Firewalls NGFW de FortiGate assurent une prise en charge intégrée des VPN IPsec et fournissent une connectivité sécurisée aux employés travaillant hors-locaux.

Le travail à distance réduit le temps non-productif des employés de 27% en moyenne.[1]

Les employés à distance travaillent en moyenne 16,8 jours de plus par an que les employés se rendant au bureau.[2]

85% des employés affirment qu'ils atteignent une productivité maximale lorsqu'ils travaillent à distance.[3]

Autoriser le travail à distance permet d'accroître la fidélisation des employés dans 95 % des entreprises.[4]

Sécuriser le travail des équipes travaillant à distance, avec NGFW FortiGate

Les VPN IPsec et SSL intégrés dans chaque NGFW FortiGate offrent un modèle de déploiement extrêmement flexible. Les travailleurs à distance peuvent soit profiter d'une expérience sans client, soit accéder à des fonctionnalités supplémentaires grâce à un client puissant intégré à la solution de sécurité des postes de travail FortiClient. Les utilisateurs avancés et les super utilisateurs peuvent déployer un FortiAP ou un FortiGate NGFW pour bénéficier de fonctionnalités supplémentaires.

Les solutions Fortinet sont conçues pour offrir un maximum de simplicité, depuis l'achat initial jusqu'à la fin du cycle de vie. Les points d'accès sans fil NGFW FortiGate et FortiAP comprennent une fonctionnalité de déploiement sans contact. Les appliances déployées sur des sites distants peuvent également être pré-configurées avant livraison, pour une installation automatique sur place, afin d'assurer ainsi la continuité des activités et le bon déploiement du télétravail.

La structure de sécurité Fortinet s'appuie sur un système d'exploitation Fortinet classique et sur un environnement API ouvert, pour créer une architecture de sécurité large, intégrée et automatisée. Grâce à la structure de sécurité Fortinet, tous les appareils informatiques d'une entreprise, y compris ceux déployés à distance pour le télétravail, peuvent être surveillés et gérés à partir d'un seul et unique panneau de contrôle. À partir de la plateforme de gestion centralisée FortiGate NGFW ou FortiManager déployée on-site, l'équipe de sécurité peut obtenir une visibilité totale sur tous les appareils connectés, quelle que soit le type de déploiement.
En cas d'événement perturbant les opérations commerciales normales, une entreprise doit être capable de passer rapidement à un effectif de 100% en télétravail. Le tableau 1 indique le nombre d'utilisateurs simultanés de VPN que chaque modèle de FortiGate NGFW peut prendre en charge.

En plus d'inclure le chiffrement des données en transit via un VPN, les solutions Fortinet offrent d'autres fonctionnalités pouvant aider à sécuriser le travail des équipes à distance. Ces fonctionnalités sont les suivantes :

- **Authentification multifactorielle.** FortiToken et FortiAuthenticator permettent une authentification à double facteurs pour les employés travaillant à distance.
- **Prévention des perte de données (DLP).** FortiGate et FortiWiFi fournissent cette fonctionnalité aux travailleurs à distance. Elle est notamment essentielle aux cadres nécessitant un accès fréquent aux données sensibles de l'entreprise.
- **Protection avancée contre les cyber menaces.** FortiSandbox offre une analyse des logiciels malveillants et des autres contenus suspects en sandboxing, avant qu'ils ne vous atteignent.
- **Connectivité sans fil.** Les FortiAP offrent un accès sans fil sécurisé pour les sites de travail à distance, avec une intégration et une configuration complètes.
- **Téléphonie.** FortiFone est une solution de téléphonie sécurisée IP (VoIP), dont le trafic est sécurisé, géré et contrôlé par un FortiGate NGFW. FortiFone est disponible en client logiciel et en plusieurs options hardware.

Modèle	Utilisateurs simultanés VPN SSL	Utilisateurs simultanés IPsec VPN	Gestion des FortiAP (mode tunnel)
100E	500	10 000	32
100F	500	16 000	64
300E	5 000	50 000	256
500E	10 000	50 000	256
600E	10 000	50 000	512
1100E	10 000	100 000	2,048
2000E	30 000	100 000	2,048
Modèles supérieurs	30 000	100 000	2,048
*3300E prend en charge 1 024 points d'accès Mode Tunnel			

Tableau 1 : Nombre de connexions VPN simultanées prises en charge par plusieurs modèles FortiGate NGFW.

Cas d'utilisation des produits Fortinet pour le travail à distance

Tous les employés d'une entreprise n'ont pas besoin du même niveau d'accès aux ressources lorsqu'ils travaillent à distance. Fortinet offre des solutions de télétravail sur mesure pour chaque collaborateur :

1. **Télétravailleur standard.** Le télétravailleur standard n'a besoin que d'un accès au courrier électronique, à internet, aux téléconférences, à un partage limité de fichiers et à des outils propres à ses missions (finances, RH, etc.).
   Cela inclut l'accès à des applications SaaS (Software-as-a-Service) via le cloud (ex : Microsoft Office 365) ainsi qu'une connexion sécurisée au réseau de l'entreprise.
   Les télétravailleurs standards peuvent se connecter à l'entreprise via le logiciel client VPN intégré FortiClient et s'identifier avec FortiToken, via l'authentification multifactorielle. Les utilisateurs avancés et les super utilisateurs ont uniquement accès à ce profil standard lorsqu'ils se connectent depuis un lieu différent de leur site de travail distant.

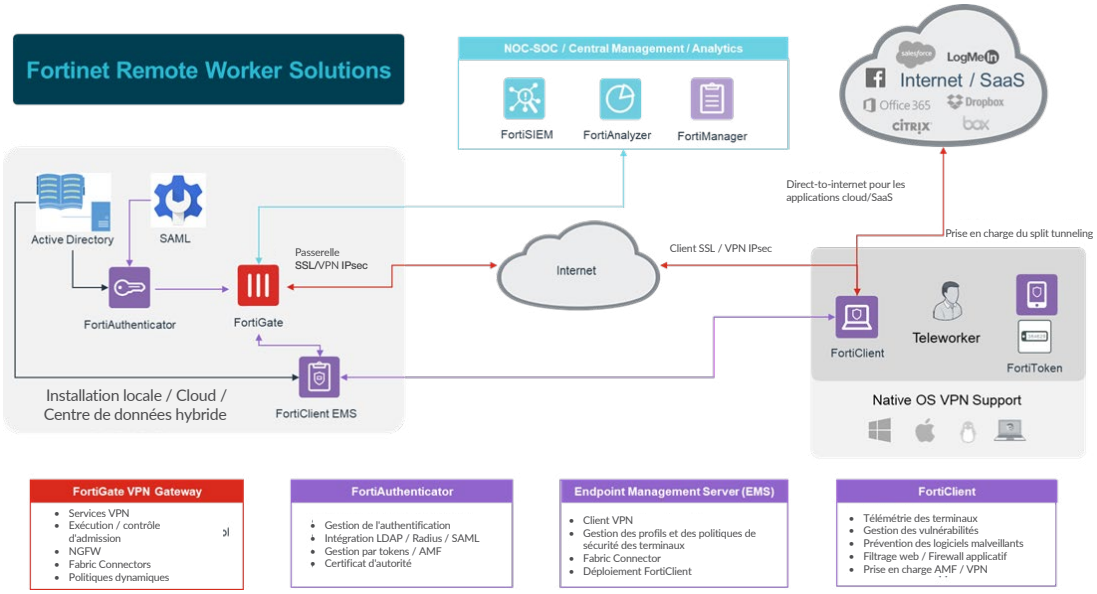

Schéma 1 : Déploiement théorique de la solution Fortinet pour un télétravailleur standard.

2. **Utilisateur avancé.** Les utilisateurs avancés sont des employés ayant besoin d'un niveau d'accès plus élevé aux ressources de l'entreprise lorsqu'ils travaillent à distance. Certains doivent, par exemple, pouvoir travailler sur plusieurs environnements informatiques en parallèle. Ces professionnels peuvent être administrateurs système, techniciens d'assistance informatique ou personnel d'urgence. Le déploiement d'un point d'accès FortiAP sur leur site de travail alternatif fournit le niveau d'accès et de sécurité dont ces utilisateurs avancés ont besoin. Ils disposent ainsi d'une connectivité sans fil sécurisée avec un tunnel sécurisé vers le réseau de l'entreprise. Les FortiAP peuvent être déployés avec un provisionnement sans contact (ZTP) et sont gérés depuis les locaux par les NGFW FortiGate. Si un téléphone professionnel doit être déployé, il suffit de le connecter au FortiAP pour assurer une connectivité au bureau principal.

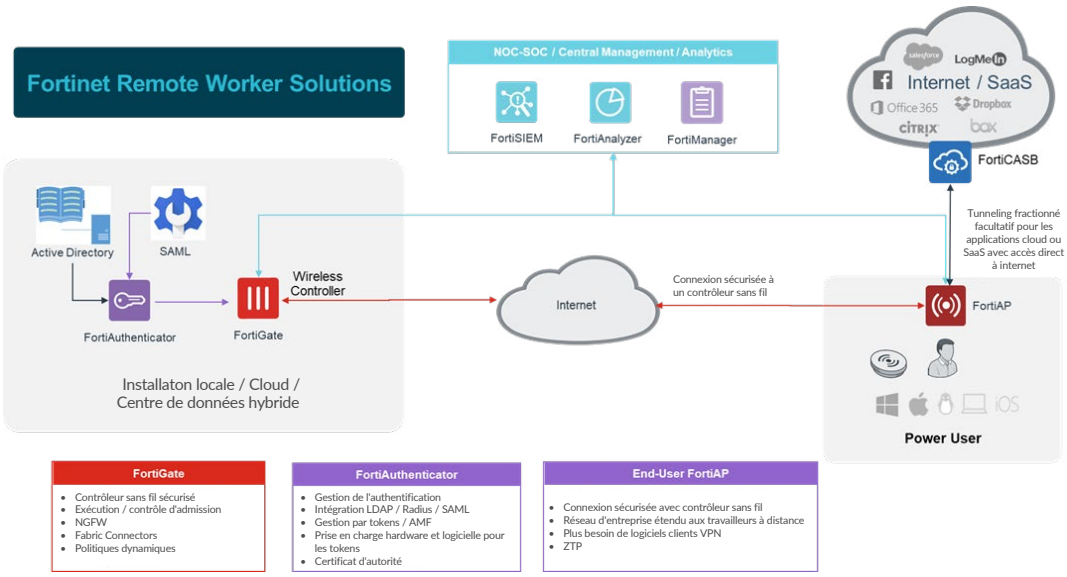

Schéma 2 : Déploiement théorique de la solution Fortinet pour l'utilisateur de puissance avancé.

3. **Super utilisateur.** Un super utilisateur est un employé nécessitant un accès avancé aux ressources confidentielles de l'entreprise, même s'il travaille depuis un autre bureau. Il traite fréquemment des informations extrêmement sensibles et confidentielles. Ces professionnels sont notamment les administrateurs possédant un accès privilégié au système, les techniciens d'assistance, les partenaires-clés du plan de continuité, le personnel d'urgence et de la direction générale.
Pour ces super utilisateurs, le site de travail alternatif doit être configuré comme un bureau alternatif. Ils ont besoin de fonctionnalités allant au-delà de celles dont disposent les utilisateurs standards et avancés. FortiAP peut être intégré à un appareil NGFW FortiGate ou FortiWiFi pour une connectivité sans fil sécurisée avec DLP intégré. FortiFone propose des versions clients logiciel ou hardware de téléphonie VoIP gérée et sécurisée via des NGFW FortiGate on-site ou via une plateforme de gestion centralisée FortiManager déployée au niveau du siège.

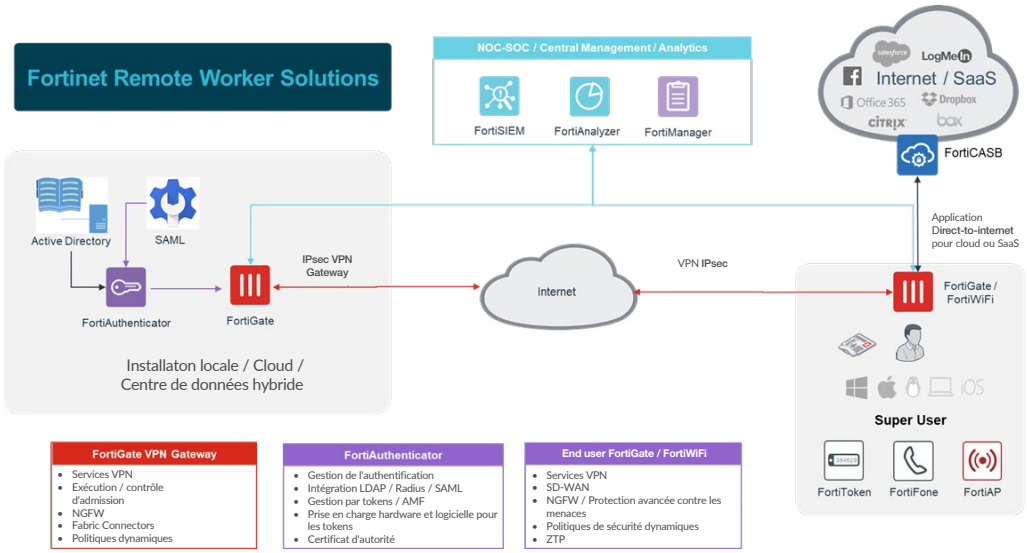

Schéma 3 : Déploiement théorique de la solution Fortinet pour le super utilisateur.

Accompagner le travail à distance

Les solutions Fortinet sont facilement déployables à distance. Les entreprises ont toutefois besoin de ressources on-site ou sur le cloud pour permettre aux télétravailleurs de travailler en toute sécurité.

De nombreuses entreprises disposent déjà de ces ressources au sein de leur architecture de sécurité existante. Un NGFW FortiGate fournit un firewall capable d'inspecter le trafic chiffré et en texte clair à l'échelle de l'entreprise, avec un impact minimal sur les performances. Toutefois, il comprend également une passerelle VPN intégrée faisant office de terminal pour les connexions chiffrées avec les télétravailleurs.

Le NGFW FortiGate s'intègre également aux infrastructures informatiques standard, notamment les services de direction d'entreprise comme Microsoft Active Directory (AD), les solutions d'authentification multi-facteurs et les solutions SSO (single sign-on). FortiAuthenticator fournit un point d'intégration unique et centralisé pour les solutions d'authentification. Il prend en charge des solutions tierces mais aussi bien entendu FortiToken, qui offre des options de tokens hardware, logiciels, e-mails et mobiles.

Dans un environnement en télétravail distribué, la visibilité et la gestion centralisée de la sécurité sont essentielles. Toutes les solutions Fortinet peuvent être intégrées à Fortinet Security Fabric. Les équipes de sécurité acquiérent ainsi visibilité et contrôle à partir d'un seul panneau de contrôle, via FortiManager. Elles peuvent aussi procéder à l'agrégation des logs et à l'analyse de la sécurité avec FortiAnalyzer. Enfin. elles peuvent détecter et répondre rapidement aux cybermenaces potentielles grâce à FortiSIEM.

Une sécurité parfaitement intégrée avec les solutions Fortinet

L'infrastructure Fortinet Security Fabric permet une intégration parfaite des collaborateurs travaillant à distance. Toutes les solutions Fortinet sont connectées via Fortinet Security Fabric, pour offrir une visibilité optimale et permettre une configuration et une surveillance à partir d'un seul panneau de contrôle. Grâce aux Fabric Connectors, à un environnement API ouvert, au soutien de la communauté DevOps et à un vaste écosystème, Security Fabric permet l'intégration de plus de 250 solutions tierces.

Cette intégration est essentielle : en effet, une entreprise peut - dans certains contextes - être amenée à brutalement passer au travail à distance. La visibilité et la gestion de l'architecture de sécurité via une unique interface permet de veiller à ce que le passage au télétravail ne mette pas en péril la cybersécurité de l'organisation.

Les solutions suivantes font partie de Fortinet Security Fabric et accompagnent le télétravail sécurisé de vos équipes :

- **FortiClient**. FortiClient renforce la sécurité des terminaux en offrant visibilité, contrôle et défense proactive. FortiClient permet de découvrir, surveiller et évaluer les risques affectant les terminaux, en temps réel.
- **FortiGate.** Les NGFW FortiGate utilisent des processeurs de cybersécurité spécialement conçus pour offrir une protection de haut-niveau, une visibilité de bout en bout, un contrôle centralisé et une inspection performante du trafic en clair ou chiffré.
- **FortiWiFi.** Les passerelles sans fil FortiWiFi associent les avantages de sécurité des NGFW FortiGate à un point d'accès sans fil. Elles offrent ainsi une solution intégrée « réseau et sécurité » pour les télétravailleurs.
- **FortiFone.** FortiFone fournit des communications vocales unifiées grâce à une connectivité VoIP sécurisée et gérée via les NGFW de FortiGate. L'interface client logiciel de FortiFone permet aux utilisateurs de passer ou de recevoir des appels, d'accéder à la messagerie vocale, de consulter l'historique des appels et d'accéder au répertoire de l'entreprise, directement depuis un appareil mobile. Plusieurs options hardware sont disponibles.
- **FortiToken.** FortiToken confirme l'identité des utilisateurs en ajoutant un deuxième facteur au processus d'authentification par le biais de jetons (tokens) physiques ou mobiles, à partir d'applications.
- **FortiAuthenticator.** FortiAuthenticator fournit des services d'authentification centralisés : services SSO, gestion des certificats ou encore gestion des invités.
- **FortiAP.** FortiAP fournit un accès sans fil sécurisé aux entreprises distribuées et aux travailleurs à distance. FortiAP peut être facilement géré depuis un NGFW FortiGate ou via le cloud.
- **FortiManager.** FortiManager permet le contrôle et la gestion des politiques de sécurité à travers l'ensemble de l'entreprise, pour une meilleure compréhension des cybermenaces, à partir du trafic réseau. FortiManager comprend des fonctionnalités permettant de contenir les attaques avancées. Évolutif, cet outil permet de gérer jusqu'à 10 000 appareils Fortinet.

- **FortiAnalyzer.** FortiAnalyzer fournit des outils analytiques de cybersécurité et de gestion des logs pour améliorer la détection des menaces et la prévention des intrusions informatiques.
- **FortiSandbox.** Les solutions de sandboxing Fortinet associent détections avancées, mesures automatisées, données exploitables et déploiements flexibles pour stopper les attaques ciblées et la fuite de données. FortiSandbox est disponible en service cloud et est inclus dans la plupart des abonnements FortiGuard.

Une base solide pour assurer la continuité des activités

Les entreprises doivent pouvoir assurer la continuité de leur activité, même en cas de crise. Pour y parvenir, elles doivent donner à leurs employés les moyens de recourir au télétravail, à tout moment. Mais même à distance, le personnel doit travailler en toute sécurité. Les solutions Fortinet sont facilement déployables et configurables. Elles permettent d'assurer la sécurité, la visibilité et le contrôle total de la cybersécurité, quel que soit l'environnement de déploiement.

1 « The Benefits of Working From Home » Airtasker, 9 septembre 2019.

2 Ibid.

3 Abdullahi Muhammed, « Here's Why Remote Workers Are More Productive Than In-House Teams, » Forbes, 21 mai 2019.

4 Ibid.

12 mars 2020 10:11

618770-0-0-EN