**Proposé par SPIE ICS et Fortinet**

# SASE : une réponse intégrée aux défis actuels de cybersécurité

**Les organisations multisites doivent concilier la résilience de leurs réseaux avec la rationalisation des coûts opérationnels tout en sécurisant les accès et en garantissant une visibilité globale. C'est la raison pour laquelle SPIE ICS et Fortinet renforcent les connexions d'agences en suivant une méthode éprouvée. Précisions avec Alain Boucquiaux, responsable développement d'offres cybersécurité de SPIE ICS, et Julien Gourdon, ingénieur cybersécurité de Fortinet.**



De gauche à droite : **Alain Boucquiaux**, responsable développement d'offres cybersécurité de SPIE ICS, et **Julien Gourdon**, ingénieur cybersécurité de Fortinet.

Pour relever ce défi, Fortinet et son partenaire SPIE ICS recommandent une migration graduelle vers le réseau Secure SD-WAN, depuis un simple firewall d'entreprise FortiGate, complété de l'offre SASE (Secure Access Service Edge).

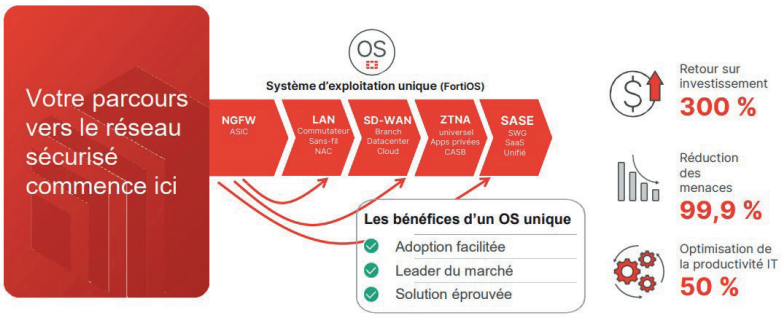
La solution Secure SD-WAN séduit un nombre croissant d'organisations distribuées et de réseaux de franchisés. Reconfigurable par logiciels[1], elle permet aux administrateurs de définir et d'appliquer des politiques sur l'ensemble du réseau en temps réel. Ce dernier s'adapte ainsi au nombre d'utilisateurs, de terminaux et d'agences à raccorder, tout en offrant une protection et une supervision unifiées.

Chaque année depuis quatre ans, le cabinet d'analyse Gartner[2] distingue Fortinet comme l'équipementier ayant la vision la plus complète et la meilleure capacité d'exécution dans le domaine du SD-WAN. Le pare-feu d'entreprise Fortinet répond aux critères de performances de sécurité les plus exigeants, sans bouleverser l'infrastructure. Comment ? Par sa modularité et ses protections contre les cybermenaces assistées par l'IA.

Pour l'intégrateur SPIE ICS, partenaire de Fortinet, « une migration graduelle vers le Secure SD-WAN remplace avantageusement des liens MPLS engourdis de solutions VPN pour accéder aux applications internes et aux services hébergés dans le cloud, en télétravail comme depuis une agence », résume Alain Boucquiaux, responsable développement d'offres cybersécurité de SPIE ICS.

## Déploiement rapide et simplifié

La méthode de migration hybride consiste à combiner des réseaux déjà en place avec une infrastructure plus sécurisée pour garantir une continuité de services tout en optimisant les ressources partagées. Les deux réseaux peuvent coexister sans perturber l'exploitation des services ni l'organisation de l'entreprise. En pratique, le déploiement du Secure SD-WAN peut suivre le rythme choisi par les responsables d'agences eux-mêmes. « Les contrôleurs de commutateurs locaux et de bornes d'accès sans fil intégrés au pare-feu FortiGate autorisent le pilotage à distance des réseaux d'agences sans exiger de licence supplémentaire. Leur supervision à distance permet de lisser les coûts de raccordement », ajoute Julien Gourdon, Systems Engineer chez Fortinet France.




Dans le cadre d'une migration sur une centaine de sites, le pare-feu nouvelle génération (NGFW) FortiGate est installé sur le cœur du réseau et déployé sur un échantillon d'agences. Le déploiement est ensuite industrialisé sans exiger le déplacement d'un administrateur sur les sites distants. Les configurations et les règles de sécurité de tous les sites sont consolidées via la console d'administration FortiManager.

Une fois les agences interconnectées et sécurisées, l'ensemble des utilisateurs bénéficie d'accès Internet et de partages sécurisés, où que soient hébergés les services. Face au développement du travail hybride, les utilisateurs doivent bénéficier du même niveau de sécurité où qu'ils se trouvent. La deuxième étape consiste donc à combiner l'offre FortiSASE et l'appliance FortiGate pour garantir des connexions sécurisées entre les salariés et leurs applications, quels que soient le terminal, l'emplacement et le réseau retenu.

L'approche ZTNA[3] sécurise le poste de travail et vérifie sa conformité. Les terminaux sont évalués en permanence afin de s'assurer que c'est bien le bon collaborateur qui se connecte à partir du bon « device » référencé par son entreprise.

Parmi les bénéfices perceptibles pour l'utilisateur : la qualité de service est identique partout et il gagne en agilité. L'expérience utilisateur et la productivité sont améliorées pour toutes les équipes réparties.

Parmi les bénéfices perceptibles pour l'organisation : la solution FortiAnalyzer réduit la complexité de gestion des tâches réseau et de sécurité, tout en améliorant la détection des menaces. Les équipes peuvent anticiper les incidents et cyberattaques ; elles n'agissent plus seulement en réaction.

### La migration pas-à-pas

La démarche proposée par SPIE ICS consiste à s'appuyer sur l'offre Fortinet pour étendre, pas-à-pas, la sécurité réseau du siège aux infrastructures locales des agences, à l'aide de licences associées au pare-feu FortiGate. On peut ainsi déployer ses propres règles d'accès et de filtrage de contenus jusqu'aux agences, notamment pour assurer l'égalité d'accès au réseau Internet entre les employés, conformément à la politique d'usages de l'entreprise. « L'uniformisation des règles de sécurité maintient le même niveau de sécurité, peu importe l'endroit où l'on travaille », confirme Julien Gourdon.

### Contrôle des applications critiques

Déployer les solutions SASE et ZTNA permet de sécuriser les partages de données et la collaboration en tout lieu. A ce niveau, SPIE ICS joue un rôle essentiel en garantissant que l'interconnexion et la protection de chaque agence restent cohérentes et maîtrisées. Cette intégration assure un déploiement centralisé et permet de déléguer la supervision des interconnexions à une équipe d'experts en infrastructures.

Dernier atout de l'offre SASE de Fortinet portée par SPIE ICS « le ZTNA permet de monter simplement des tunnels applicatifs ; ces canaux chiffrés autorisent l'accès aux services s'exécutant sur un cloud privé ainsi qu'aux services délivrés en mode SaaS. On conserve ainsi un contrôle de la posture des terminaux en fonction de la criticité des applications », conclut Julien Gourdon.

### Doit-on choisir entre SD-WAN et SASE ?

Non, Secure SD-WAN et SASE procurent des fonctions logicielles complémentaires pour sécuriser et optimiser les connexions d'agences réparties, tout en répondant aux enjeux de migration vers le cloud. Secure SD-WAN connecte les utilisateurs et leurs terminaux au cœur du réseau de l'organisation. L'offre SASE tient compte de l'identité et du contexte de la demande, de l'état et du comportement du terminal et de la sensibilité des données. Selon les besoins, la combinaison des deux solutions renforce l'infrastructure multisites et permet d'appliquer les mêmes règles de sécurité, partout où les collaborateurs interagissent.

**1. software-defined - 2. https://www.fortinet.com/blog/business-and-technology/fortinet-named-a-leader-in-gartner-magic-quadrant-for-Secure SD-WAN-for-fifth-year) - 3. Zero Trust Network Access**