

# Réseau et sécurité évoluent conjointement

Une infrastructure homogène et évolutive pour le réseau et la sécurité permet de minimiser les coûts d'exploitation et de configuration, de sécuriser efficacement l'ensemble du réseau de l'entreprise contre les menaces actuelles et futures, et de préparer l'établissement à sa croissance à venir.

D'une part, des menaces qui deviennent de plus en plus ingénieuses, des virus conventionnels aux ransomwares perfides. De l'autre, l'importance croissante de la sécurité informatique dans la réussite commerciale ainsi que de nouveaux modèles de travail et d'utilisation comme le home office, les services de cloud, le travail mobile et le «bring your own device»: les exigences portant sur les performances, la disponibilité et la sécurité du réseau de l'entreprise augmentent en permanence, dans les grandes organisations comme dans les PME.

## «Connected UTM» pour une sécurité réseau complète

Pour rendre les réseaux d'entreprise encore plus sûrs et plus faciles à gérer, Fortinet propose une solution de sécurité très efficace qui s'étend de la sécurité des réseaux jusqu'à celle des terminaux en utilisant l'intégration de composants de sécurité et de réseau. En tant qu'élément central, les pare-feu UTM (Unified Threat Management) proposent des technologies comme la protection contre les intrusions, les anti-malwares, le filtrage web, la protection contre le spam et bien plus encore. Avec le «Connected UTM», les connexions Internet jusqu'aux appareils des clients, l'accès par câble et WLAN ainsi que les solutions add-on pour la sécurité des applications et de la communication sont ainsi réunis dans ce qu'on appelle une «Security Fabric».

En 2015, pour la septième année consécutive, l'entreprise d'étude de marché Gartner a placé le spécialiste de la sécurité et des réseaux Fortinet en position leader dans son «quadrant magique» pour l'Unified Threat Management. L'offre de Fortinet transforme la vision d'un «Connected UTM» et d'une «Security Fabric» en une réalité et crée une infrastructure de sécurité et de réseau homogène d'une seule traite. Des composants tels que les pare-feu FortiGate, les services UTM FortiGuard avec une intelligence locale et basée sur le cloud, la solution de sécurité pour les terminaux FortiClient, les commutateurs réseau de la série des FortiSwitch Secure Access Switch, les points d'accès sans fil de la série FortiAP ainsi que les composants WLAN basés sur l'infrastructure font partie de la solution globale.

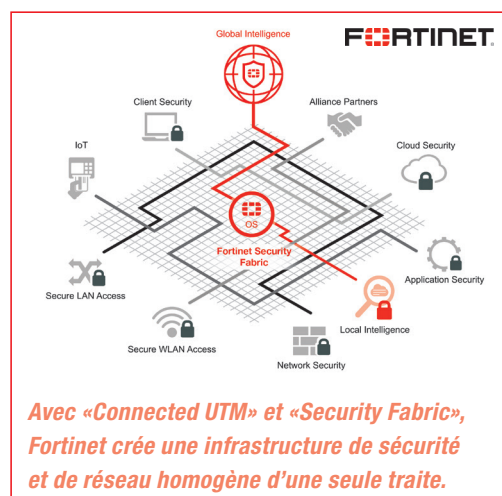
## Une infrastructure homogène auprès d'un même fournisseur

De cette façon, l'ensemble de l'infrastructure de sécurité et du réseau se laisse gérer à travers une seule et unique plate-forme de gestion pilotable de façon intuitive. La base logicielle des équipements Fortinet est formée par le système d'exploitation renforcé FortiOS. Par ailleurs, les performances du système sont garanties par les processus ASIC développés par Fortinet ainsi que par le «Parallel Path Processing», une combinaison qui assure suffisamment de performance, même dans les environnements les plus exigeants – comme par exemple les grandes organisations, les centres de calcul, les fournisseurs de services informatiques et les opérateurs de télécommunications.

Une infrastructure de sécurité et de réseau homogène provenant d'un seul fournisseur rend possible une consolidation optimale de tous les composants impliqués, facilite la gestion et aide à réduire les coûts. Elle garantit en outre une grande évolutivité, de façon à ce que l'entreprise soit prête pour sa croissance future.

## Des commutateurs pour toutes les éventualités

Au côté des pare-feu UTM, les commutateurs sont les éléments centraux de chaque réseau. La famille FortiSwitch propose des Secure Access Switches pour les entreprises de toute taille et pour toutes les exigences



avec des capacités de switching de 20 à 336 Gbit/s, 8 à 48 ports LAN, diverses configurations uplink (jusqu'à 4 x 10 GE SFP+ et 2x 40 GE QSFP+) et une prise en charge du PoE ou PoE+ (802.3 af/at) pour l'alimentation électrique des appareils connectés tels que les points d'accès, les caméras et les téléphones IP, etc.

En les combinant aux mécanismes de sécurité des pare-feu FortiGate, les commutateurs permettent des solutions sophistiquées telles que la segmentation interne et un accès LAN sécurisé par une authentification, ceci aussi bien sur le WLAN que sur le réseau câblé. A cet égard, différentes topologies sont prises en charge, depuis les connexions simples jusqu'à celles qui sont entièrement redondantes. En plus de l'intégration directe avec les pare-feu UTM en mode FortiLink, les FortiSwitches peuvent aussi être employés facultativement en mode autonome.

### «CONNECTED UTM» ET FORTISWITCHES: LES POINTS FORTS

- Sécurisation flexible et évolutive du réseau de l'entreprise
- Stoppe les attaques avant qu'elles n'infiltrerent le réseau
- Gère l'ensemble du réseau à travers une seule plate-forme
- Optimise les flux de données sur la base des priorités des applications
- Sécurise les réseaux sans fil et câblés
- Protège tous les appareils, y compris les BYOD
- Des commutateurs pour tous les environnements, des PME jusqu'aux centres de calcul des fournisseurs

**BOLL**  
IT Security Distribution

### BOLL Engineering SA

En Budron H15  
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60  
contact@boll.ch  
www.boll.ch