«Secure Access Switches»

Une sécurité informatique étendue à l'ensemble du réseau

Grâce à la connexion directe des «Secure Access Switches» de la série D FortiSwitch avec FortiGate, l'instance centrale de sécurité informatique, Fortinet rend possible une gestion consolidée de la sécurité jusqu'au niveau switch.

Qu'il s'agisse de PME, de bureaux régionaux ou d'entreprises dotées d'une organisation décentralisée: grâce aux «Secure Access Switches» de la série D FortiSwitch, les entreprises soucieuses de leur sécurité disposent d'une famille de commutateurs performants s'intègrant parfaitement dans une infrastructure pare-feu et WLAN sécurisée existante de Fortinet, fixant ainsi un nouveau standard en termes de sécurité informatique intégrale. Le contrôle central de tous les commutateurs connectés par le dispositif «Next Generation Firewall» FortiGate constitue le cœur de la solution. L'ensemble de la gestion des commutateurs basés sur Fortinet est consolidé par le pare-feu central. Par rapport aux structures hétérogènes, cela simplifie énormément la manipulation et augmente considérablement la sécurité globale.

Une sécurité informatique de portée générale

Le concept de l'intégration directe des Secure Access Switches dans le dispositif de sécurité FortiGate (la gestion de la communication est effectuée par des tunnels basés sur le protocole CAPWAP) correspond au besoin d'accorder à différents utilisateurs et groupes d'usagers (collaborateurs internes, partenaires, invités) des accès extrêmement sécurisés à des données, des applications et/ou des services autorisés individuellement. Et ce indépendamment de l'appareil utilisé, du point et du type d'accès physique (par câble ou WLAN). Ainsi, grâce à la configuration centralisée, il est possible de définir des zones de sécurité dédiées, par exemple pour les visiteurs, valables quel que soit le type d'accès. Lorsqu'un appareil est connecté à un port FortiSwitch, les composantes d'accès sont vérifiées et l'utilisateur est authentifié. Une fois que celui-ci s'est connecté avec succès à l'aide de ses données d'accès, il peut accéder aux ressources autorisées conformément aux règles d'accès préalablement définies. Ce faisant, l'instance centrale de sécurité conserve toujours le contrôle sur les appareils et les utilisateurs et sait où et quand ils se trouvent dans le réseau.

L'incorporation optionnelle de la solution d'authentification FortiAuthenticator de Fortinet mérite une mention particulière. Elle permet une autorisation (partage des applications en fonction des droits attribués individuellement) et une authentification (vérification de l'authenticité de la personne habilitée) sécurisées des utilisateurs sur l'ensemble du réseau de l'entreprise (NAC 802.1x).

Puissant

Les «Secure Access Switches» de Fortinet sont disponibles en différentes versions. Leur taille est limitée à 1U, ils prennent en charge 8 à 48 ports et peuvent être obtenus en version POE (Power over Ethernet). Tous les modèles offrent la possibilité de former des LAN virtuels avec des règles de sécurité spécifiques au VLAN. Cette segmentation (des données) soutient la convergence de la voix, des données et du WLAN et répond aux vastes exigences de conformité concernant la «séparation des données». Important: si des données sont transmises d'un VLAN à l'autre, le routage s'effectue par l'instance de sécurité centrale FortiGate de Fortinet, ce qui apporte un maximum de sécurité. L'emploi de dispositifs FortiGate à accélération matérielle extrêmement performants en tant qu'«Internal Segmentation Firewalls» rend possible cette architecture «Secure Access Switch» intégrale.

Aperçu des caractéristiques de FortiSwitch

Fortinet révolutionne le marché de la sécurité informatique avec les «Secure Access Switches» de la série D FortiSwitch.

- «Secure Access Switches» performants avec 8 à 48 ports; disponibles aussi en version POE (Power over Ethernet)
- Intégration directe dans l'instance de sécurité centrale FortiGate de Fortinet; gestion de la sécurité consolidée sur l'ensemble du réseau
- Authentification et autorisation globales des utilisateurs avec partage des ressources en fonction des droits indiqués préalablement (NAC 802.1x) – y compris intégration sécurisée des invités
- Identification des utilisateurs et des appareils dans l'ensemble du réseau, indépendamment des composantes d'accès, du lieu et du type (LAN, WLAN, appareils mobiles etc.)
- Formation de zones VLAN et WLAN communes
- Accès protégé à des ports dédiés, en fonction des droits définis
- Prise en charge des environnements convergents (voix, données, trafic WLAN)

BOLL
IT Security Distribution

BOLL ENGINEERING SA

En Budron H15, 1052 Le Mont-sur-Lausanne
Tel 021 533 01 60 / contact@boll.ch
www.boll.ch