

# Un WiFi puissant au Musée national suisse

Au Musée national suisse de Zurich, des expositions très intéressantes parsemées de stations interactives modernes attendent les visiteurs, le tout grâce au WiFi, basé sur des pare-feu et des points d'accès signés Fortinet, qui couvre tout le site.

Avec l'ouverture du nouveau bâtiment, très impressionnant, en août 2016, le Musée national suisse de Zurich est entré dans une nouvelle ère. «Nous ne voulons cependant pas proposer une belle coquille vide, mais permettre de faire l'expérience d'un musée à la pointe de ce qui existe en technique d'exposition», déclare René Vogel, directeur du service informatique du musée. L'un des prérequis pour y parvenir: un WiFi couvrant toute la surface. D'une part pour les applications internes telles que la connexion au réseau des scanners de ticket mobiles et, d'autre part, pour les visiteurs.

Ceux-ci profitent d'un E-Guide sous la forme d'une appli de smartphone ou de tablette. On la charge via un SSID spécial, qui ne demande aucune inscription compliquée. Ceux qui souhaitent utiliser le réseau au-delà de l'E-Guide, par exemple pour surfer sur Internet, devront s'enregistrer et s'authentifier par SMS. D'après René Vogel, l'offre est demandée: «Les cinq premiers mois, nous avons comptabilisé près de 5500 utilisateurs authentifiés». Les touristes sans abonnement au réseau local apprécient particulièrement cet accès gratuit à Internet.

Certains secteurs du Musée national suisse avaient déjà été équipés d'un WiFi, mais celui-ci ne fonctionnait pas parfaitement et il n'était pas possible de l'étendre comme on l'aurait souhaité. Pour la couverture du site dans son intégralité, une nouvelle solution était dès lors nécessaire. «Nos exigences étaient claires: il nous fallait plus de SSID, nous voulions subdiviser le réseau à l'aide de VLAN de manière logique en différents

segments et nous souhaitons un réseau sans fil puissant, qui servirait à différents services», relate le directeur informatique en soulignant qu'une solution intégrant de nouveaux contrôleurs WiFi séparés et hors de prix n'entrait pas en ligne de compte.

## Une solution intégrée

Le prestataire informatique BeeLine Networks GmbH a su convaincre par une solution à portée de main: le pare-feu Fortigate en place a été remplacé par le modèle 600D, plus puissant. L'auto-enregistrement et l'authentification par SMS des visiteurs, de même que l'enregistrement des accès sont pris en charge par un FortiAuthenticator 200D. Il s'agit d'un système intégré: le pare-feu sécurise les réseaux câblés et sans fil en les consolidant et, en même temps, la configuration et l'administration du WiFi se font directement sur le pare-feu. Les points d'accès s'intègrent automatiquement au système. Le gérant de BeeLine, Martin Hess, résume ainsi l'avantage principal: «Nous n'avons pas été obligés de scanner et d'intégrer à la main chaque point d'accès séparément». Pour couvrir l'ensemble du site 74 points d'accès de type FortiAP 221C sont utilisés et quatre FortiAP 224D pour l'extérieur. 26 autres points d'accès servent par ailleurs de réserve en prévision de besoins ultérieurs et pour les expositions spéciales. Avec le WiFi intégré basé sur FortiGate, paramétrer un VLAN sécurisé avec accès VPN permettant une télémaintenance pour certaines stations est un jeu d'enfant. Or, jusqu'à présent, il fallait bien souvent disposer de connexions DSL et de câbles.



## Un partenaire de poids

René Vogel est satisfait du nouveau WiFi et voit la collaboration avec BeeLine Networks et BOLL d'un très bon œil: «BeeLine, cela fait un moment que nous les connaissons. La coopération fonctionne très bien, même si parfois, nous avons des demandes assez compliquées et des délais courts». Un entretien très ouvert a par ailleurs eu lieu avec BOLL lors de la phase d'évaluation: «Nous avons pu nous familiariser avec la solution et poser toutes les questions qui nous sont venues à l'esprit. Ça nous a beaucoup aidé dans notre prise de décision».

## WiFi FortiGate Integrated: les points forts

- Wireless Networking puissant et flexible
- Configuration intégrée et administration de tous les points d'accès
- Fonctions de sécurité du pare-feu de nouvelle génération compris pour le trafic WiFi

- Point d'accès Rogue Detection & Suppression
- Aucuns frais d'équipement ou de licence pour les contrôleurs WiFi séparés
- Combinaison avec FortiAuthenticator permettant un portail d'auto-enregistrement pour utilisateurs invités
- En choisissant le modèle de pare-feu FortiGate, possibilité de graduer en de petits environnements jusqu'à de très grands, comprenant des milliers de points d'accès
- Vaste sélection de points d'accès pour une utilisation à l'intérieur et à l'extérieur

**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