Réseaux informatiques

Les besoins en réseau informatique d'un bureau ou d'un complexe sont très spécifiques aux budgets, à la taille, à la capacité et aux besoins opérationnels globaux de l'organisme. Les organismes devraient envisager d'engager du personnel spécialisé dans les technologies de l'information et les réseaux pour aider à la mise en place de réseaux de bureau et de sous-bureau.

Mise en place du réseau de bureau/complexe

Dans la plupart des sites sur le terrain, il y aura à l'avenir tout un mélange de plusieurs équipements de réseau de bureau. Il s'agit notamment des éléments suivants :

Connexion à un FAI externe - La connexion à un fournisseur d'accès à Internet (FAI) externe peut se faire sous la forme de l'internet par satellite, d'une ligne téléphonique ou d'un autre type de connexion dédiée à un réseau établie par le FAI.

Modem - Les modems reçoivent les signaux provenant des FAI et les traduisent en signaux exploitables par les réseaux domestiques ou de bureau. Les modems contiennent également des informations spécifiques à l'utilisateur qui sont utilisées pour localiser, suivre et surveiller le trafic à des fins de sécurité et de facturation. Sans modem, tout équipement de réseau domestique ou de bureau serait incapable de réellement communiquer avec des réseaux extérieurs.

Routeur - Un routeur est un dispositif qui divise et gère le trafic internet, permettant à plusieurs appareils informatiques d'avoir leurs propres adresses IP et MAC uniques, ainsi que de communiquer avec Internet et entre eux en même temps sur un réseau. Les routeurs possèdent une variété de configurations et de fonctions. Certains peuvent surveiller et contrôler le trafic sur le réseau local, et d'autres ont une capacité Wi-Fi. Le type de routeur utilisé dépend des besoins opérationnels.

Pare-feu - Un pare-feu est un dispositif qui surveille et filtre spécifiquement le contenu internet provenant de réseaux extérieurs. Les pare-feu sont pratiques pour empêcher les logiciels malveillants, les intrusions occasionnelles dans les réseaux, ou même pour bloquer les contenus non autorisés par la politique informatique de chaque organisation. Dans les réseaux simplifiés, les pare-feu sont souvent regroupés avec les modems ou les routeurs, mais les réseaux perfectionnés peuvent disposer de pare-feu autonomes ayant des protocoles différents pour les divers utilisateurs des services.

Commutateur - Un commutateur de réseau est comme une forme avancée de routeur : il contrôle et distribue l'internet entre plusieurs appareils en réseau, mais les commutateurs sont capables de surveiller et de contrôler en détail chaque appareil. Les commutateurs sont également utilisés pour filtrer, bloquer et sécuriser les réseaux internes, à l'instar des pare-feu qui protègent contre les menaces externes.

Serveur - Les serveurs sont définis comme des ordinateurs entièrement consacrés au stockage et au partage de fichiers au sein d'un réseau. Les serveurs peuvent être aussi simples que des ordinateurs de bureau ordinaires ou aussi complexes que de grands dispositifs informatiques spécialisés présentant des exigences d'installation particulières. Ces dernières années, de nombreux organismes se sont mis à utiliser des serveurs « hors site » qui hébergent et gèrent des fichiers et des données à partir d'emplacements extérieurs aux bureaux, parfois dans un autre pays. Les serveurs hors site sont des solutions tout à fait acceptables, mais si les utilisateurs du serveur n'ont pas une connexion constante à l'internet, un serveur local peut

être préférable.

1 FAI externe

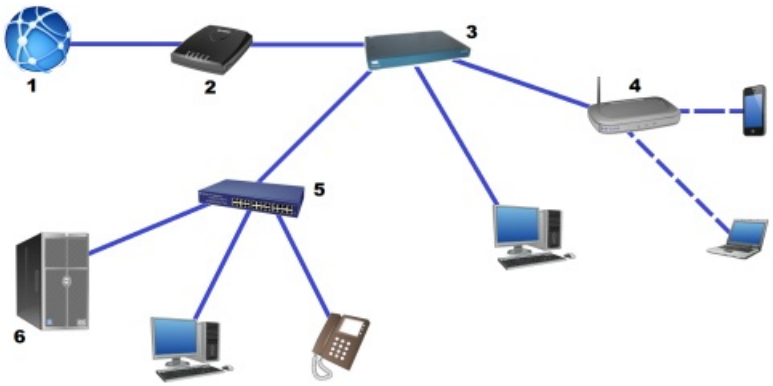
2 Modem

3 Routeur/pare-feu

4 Routeur Wi-Fi

5 Commutateur de réseau

6 Serveur



Sécurité opérationnelle

Les exigences de sécurité opérationnelle de chacun des réseaux locaux doivent suivre des règles de base.

Contrôle d'accès - Seules les personnes autorisées doivent avoir accès aux réseaux et aux appareils informatiques. Tous les ordinateurs doivent être protégés par un mot de passe, et les routeurs Wi-Fi doivent également nécessiter des identifiants de connexion. Certains réseaux autorisent l'accès temporaire d'invités, mais les besoins en matière de paramètres spéciaux varient en fonction de l'environnement opérationnel.

Logiciels malveillants - Tous les appareils informatiques des réseaux doivent être équipés d'une forme de logiciel antivirus et les systèmes d'exploitation doivent être à jour en permanence. Les organismes doivent envisager d'installer des pare-feu et/ou des commutateurs possédant des paramètres gérés afin de réduire également les tentatives d'intrusion ou la transmission de logiciels malveillants.

Politique informatique - Les organismes doivent élaborer des politiques informatiques internes et les communiquer à tous les collaborateurs et utilisateurs du réseau. Les politiques informatiques doivent comprendre des réglementations sur ce qui est considéré comme un comportement acceptable, les règles d'utilisation des différents types de matériel, et établir des directives en cas de non-respect.