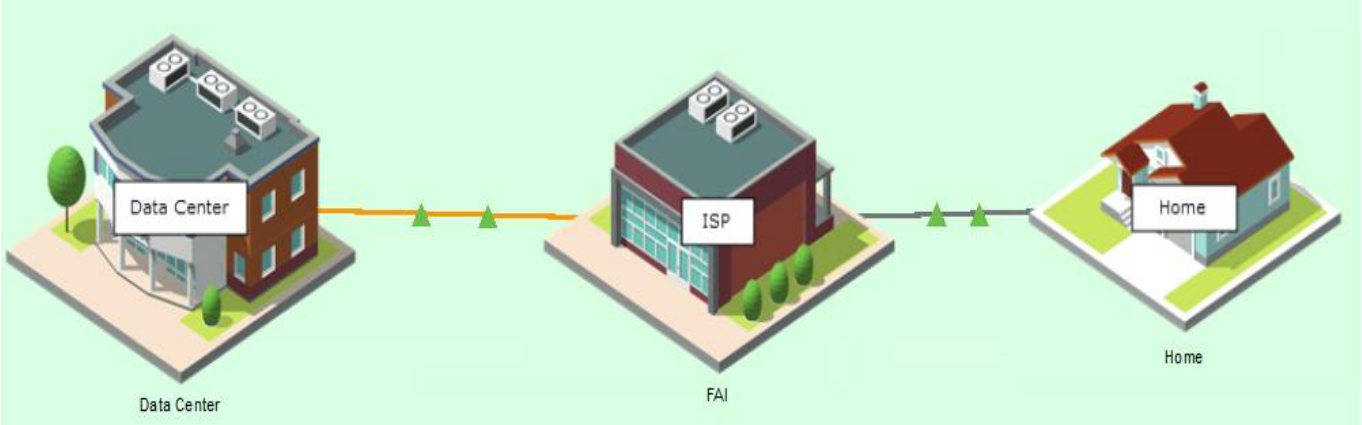
ACTIVITE 1

Configurer la sécurité (de base) des routeurs sans fil

L'objectif de cette activité est de sécurisé une installation réseau de type PAN (réseau Personnel).



Dans cette activité de Packet Tracer (PT), vous allez configurer la sécurité sans fil sur un routeur sans fil de la maison. Lors de l'installation, le routeur a été partiellement configuré, mais présente des problèmes de sécurité qui doivent être résolus. Vous renforcerez également le routeur pour limiter les attaques potentielles.

Configuration des paramètres de sécurité de base pour un routeur sans fil

Les paramètres initiaux d'un routeur sans fil domestique peuvent constituer un risque pour la sécurité. Par exemple, si les hackers connaissent votre adresse IP publique, ils peuvent rechercher sur Internet les informations d'identification par défaut (identifiant et Mot de passe) de votre routeur et y accéder à distance. Dans cette section, vous allez modifier le mot de passe du routeur et désactiver la connexion à distance.

Paramètres par défaut du routeur :

@IP routeur : **192.168.0.1**
Identifiant : **admin**
Mot de passe : **admin**

Il est important de définir un mot de passe fort ou une phrase de passe longue pour empêcher les utilisateurs non autorisés de modifier les configurations sur le routeur.

☞7 – Utilisez le fichier "***Act 1 - Défense du système et du réseau.pka***" pour la suite de l'activité.

☞8 – Cliquez sur la maison puis sur l'ordinateur fixe dans le bureau. Ouvrir le navigateur.

☞9 – Connectez-vous au routeur sans fil de la maison.

☞10 – Cliquez sur l'onglet **Administration**, puis saisissez un nouveau mot de passe : **cisconetacadrocks!**
N'oubliez-pas le point d'exclamation, faites défiler jusqu'en bas et cliquez sur **Save Settings.**

☞11 – Reconnectez-vous et vérifier que la modification est effective.

Désactivez la gestion à distance.

Les routeurs sans fil domestiques sont généralement livrés avec la configuration à distance activée. Cela permet aux techniciens de votre opérateur d'accéder à votre périphérique pour vous aider à configurer votre réseau domestique ou à résoudre les problèmes. Cependant, cela peut constituer un risque pour la sécurité, car un port doit être ouvert en écoute pour que le technicien puisse se connecter au routeur. Il est souvent possible de modifier le port et d'autoriser uniquement l'accès HTTPS, mais cela n'offre aucune mesure de sécurité réelle, car un hacker pourrait détecter les ports ouverts et lancer une attaque par mot de passe contre le routeur. Si la gestion à distance est vraiment nécessaire, il serait beaucoup plus sûr de mettre en place une solution VPN (pas traitée dans notre cas). Par conséquent, vous désactiverez la gestion à distance.

☞12 – Sous l'onglet **Administration**, cherchez la gestion à distance (**Remote Management)** et désactivé-la.

☞13 – Sauvegardez la configuration.

Remarque
Cette modification entrainera la réinitialisation du routeur domestique sans fil. Pour accélérer la simulation, cliquez plusieurs fois sur l'icône "**Fast Forward Time"** en bas à gauche.
Revenez sur l'ordinateur fixe du bureau et vérifier que son adresse IP est correcte (sinon, basculer entre DHCP et Static jusqu'à obtenir une adresse correcte).

☞14 – Cliquez sur **Web Browser**. Accédez à **192.168.0.1** et ré-authentifiez-vous (si on vous le demande) en vue de la prochaine étape de l'activité.

Configurer la sécurité du réseau du routeur sans fil

À l'heure actuelle, toute personne disposant d'un périphérique sans fil à portée du Home Wireless Router (routeur sans fil domestique) peut se connecter facilement et éventuellement accéder à des périphériques sur le réseau. Pour éviter cela, dans cette section, vous allez sécuriser les réseaux sans fil afin que seuls les périphériques avec la configuration correcte puissent se connecter aux réseaux.

Remarque
Masquer le SSID d'un réseau WI-FI ne correspond pas à une mesure de sécurité car on dispose d'outils simple pour détecter le trafic Wifi et en déduire le SSID. En fait, la désactivation de la diffusion du SSID peut potentiellement faire du réseau une cible plus importante pour les attaques, car l'administrateur tente de le masquer.

☞15 – Activez la diffusion du SSID : validez le "SSID Broadcast" dans l'onglet "Wireless".

☞16 – Pour chacun des trois réseaux, remplacez le nom du SSID (défaut) par **HomeNet**.

Remarque
La mesure de sécurité la plus importante en dehors de la modification du mot de passe du routeur est peut-être le chiffrement du trafic entre le routeur et les clients sans fil. Sans chiffrement, un hacker peut utiliser des outils (souvent gratuits) pour intercepter facilement les communications. Cela peut entraîner d'autres attaques à mesure que l'hacker acquiert des informations sur vous et vos réseaux.

☞17 – Dans l'onglet **Wireless**, cliquez sur **Wireless Security**. Pour chacun des trois réseaux, configurez les éléments suivants :

SSID : **HomeNet**
Mode de sécurité : **WPA2 Personnel**
Chiffrement : **AES**
Phrase secrète : **ciscorocks**

Remarque
Le WPA2 Personnel (noté aussi WPA2-PSK) est plus simple à configurer, car il ne nécessite pas de serveur d'authentification centralisé. La configuration se fait généralement en entrant une "passphrase" sur les appareils clients.
WPA Entreprise : l'authentification des utilisateurs se fait par un serveur d'authentification centralisé. Chaque utilisateur possède son identifiant et son mot de passe.

Génial !
Ce routeur permet de configurer deux réseaux sans fil indépendants. Cela peut être utile lorsque vous souhaitez séparer le trafic invité du trafic sur vos autres réseaux. Vous garderez le réseau " **HomeNet"** pour vous et vous configurerez le deuxième réseau pour vos invités (SSID : " **GuestNet**").

En général, le WIFI invité est configuré pour accéder seulement à Internet, l'accès au réseau local (Camera IP, NAS, imprimante, autre ordinateur, …) est bloqué.

☞18 - Sous l'onglet Wireless, cliquez sur Guest Network (Réseau invité). Pour chacun des trois réseaux, cliquez sur **Enable Guest Profile** (Activer le profil d'invité), puis configurez les éléments suivants :

SSID : **GuestNet**
Broadcast SSID : **Enabled**
Mode de sécurité : **WPA2 Personnel**
Chiffrement : **AES**
Phrase secrète : **guestpass**

La configuration des clients sans fil.

On dispose de deux ordinateurs portables, d'une webcam, d'une sirène et d'une porte connectées :

- **Home Laptop 1** dans le salon, sera configuré sur le réseaux WiFi 1
- **Home Laptop 2** dans le bureau, sera configuré sur le réseaux WiFi 2 (invité)
- **Home_Webcam** dans le bureau, sera configuré sur le réseaux WiFi 1
- **Home_ Siren** dans le salon au-dessus de la bibliothèque, sera configuré sur le réseaux WiFi 1
- **Home Doors** sera configuré sur le réseaux WiFi 1

☞19 – Cliquez sur "Home Laptop 1" et configurez son accès WiFi. Vérifiez que l'adresse IP de l'ordinateur portable soit bien dans le réseau 192.168.0.0 / 24.

☞20 – Cliquez sur "Home Laptop 2" et configurez son accès WiFi. Vérifiez que l'adresse IP de l'ordinateur portable soit bien dans le réseau 192.168.0.0 / 24.

☞21 – Cliquez sur " **Home_Webcam** " et configurez son accès WiFi. Vérifiez que l'adresse IP soit bien dans le réseau 192.168.0.0 / 24.

☞22 – Cliquez sur " **Home_ Siren** " et configurez son accès WiFi. Vérifiez que l'adresse IP soit bien dans le réseau 192.168.0.0 / 24.

☞23 – Cliquez sur "**Home Doors** " et configurez son accès WiFi. Vérifiez que l'adresse IP soit bien dans le réseau 192.168.0.0 / 24

Vérifier les paramètres de connectivité et de sécurité

Dans cette section, vous testerez vos configurations et vos paramètres de sécurité pour vous assurer que les périphériques communiquent entre eux et qu'ils peuvent accéder à Internet.

☞24 – Cliquez sur **Home Laptop 1** et sélectionnez le navigateur**.** Accédez à **www.ptsecurity.com**.
Packet Tracer peut prendre plusieurs secondes pour converger. Vous pouvez cliquer sur **Fast Forward Time** (Avance rapide) (Alt+D) pour accélérer le processus jusqu'au chargement de la **Data Center Public Web** (page Web publique du centre de données).

☞25– Répétez cette étape pour **Home Laptop 2**.

Les réseaux Wifi **GuestNet** et **HomeNet** ne doivent normalement pas être en mesure de se connecter ou de partager des ressources. N'oubliez pas que Home Laptop 2 est configuré pour le réseau invité et ne doit normalement pas avoir accès aux périphériques du réseau domestique qui sont sur le réseau Wifi 1 (HomeNet).

☞26 – La commande ping peut vous permettre de vérifier si les réseaux Wifi communiquent. Effectuez un ping de **Home Laptop 1** vers **Home Laptop 2.**

✍ 27 – Que constatez-vous ?
Les deux ordinateurs peuvent communiquer ensemble. Cela pose un problème de confidentialité. Les hôtes sur le réseau invité ne doivent pas avoir accès aux hôtes du réseau "HomeNet".

Vous devez configurer le routeur pour empêcher les hôtes de différents réseaux de communiquer entre eux.
☞28 – Retournez dans le menu **Guest Network** du routeur (Wireless).

☞29 – Décochez l'option qui autorise les invités à se voir et à accéder au réseau local.

☞30 – À partir de **Home Laptop 1**, essayez d'envoyer une commande ping à **Home Laptop 2.**

✍ 31 – Que constatez-vous ?
Les pings devraient maintenant échouer. Cela indique que les hôtes ne sont pas autorisés à communiquer entre les deux réseaux.

✍ 32 – Est-ce que Home Laptop 2 accède toujours au site **www.ptsecurity.com ?**
Oui. C'est normal car l'accès à Internet n'est pas bloqué, c'est seulement l'accès au réseau **Home Laptop** qui est bloqué.