Packet Tracer - Configuration de mots de passe sécurisés et de SSH

# Table d'adressage

| Appareil | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| --- | --- | --- | --- | --- |
| RTA | G0/0 | 172.16.1.1 | 255.255.255.0 | N/A |
| PCA | Carte réseau | 172.16.1.10 | 255.255.255.0 | 172.16.1.1 |
| Commutateur1 | VLAN 1 | 172.16.1.2 | 255.255.255.0 | 172.16.1.1 |

# Scénario

L'administrateur réseau vous a demandé de préparer **RTA** et **SW1** pour le déploiement. Avant de le connecter au réseau, il faut mettre en place des mesures de sécurité.

# Des intructions

## Configurer les mesures de sécurité de base sur le routeur

Ouvrez une invite de commandes.

* + 1. Configurez l'adressage IP sur le **PCA** en fonction du tableau d'adressage.

Fermez l'invite de commandes.

Ouvrez la fenêtre de configuration.

* + 1. Console dans RTA depuis le terminal sur PCA.
    2. Configurez le nom d'hôte comme **RTA**.
    3. Configurez l'adressage IP sur **RTA** et activer l'interface.
    4. Cryptez tous les mots de passe en clair.

RTA(config)# **service password-encryption**

* + 1. Fixez la longueur minimale du mot de passe à 10.

RTA(config)# **security password min-length 10**

* + 1. Choisissez un mot de passe secret fort. **Remarque** : Choisissez un mot de passe dont vous vous souviendrez, ou vous devrez réinitialiser l'activité si vous êtes verrouillé hors de l'appareil.
    2. Désactivez la commande de recherche DNS.

RTA(config)# **no ip domain-lookup**

* + 1. Réglez le nom de domaine sur **CCNA.com**(sensible à la casse pour la notation en PT).

RTA(config)# **ip domain-name CCNA.com**

* + 1. Créez un utilisateur de votre choix avec un mot de passe fortement crypté.

RTA (config) # **nom d' *utilisateur any\_user* secret *any\_password***

* + 1. Générez des clés RSA de 1 024 bits.

**Remarque**: Dans Packet Tracer, entrez la commande crypto key generate rsa et appuyez sur Entrée pour continuer.

RTA(config)# **crypto key generate rsa**

Le nom des clés sera : **RTA.CCNA.com**

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

quelques minutes.

How many bits in the modulus [512]: **1024**

* + 1. Bloquez pendant trois minutes quiconque n'arrive pas à se connecter au bout de quatre tentatives en deux minutes.

RTA(config)# **login block-for 180 attempts 4 within 120**

* + 1. Configurez toutes les lignes VTY pour l'accès SSH et utilisez les profils d'utilisateurs locaux pour l'authentification.

RTA(config)# **line vty 0 4**

RTA(config-line)# **transport input ssh**

RTA(config-line)# **login local**

* + 1. Réglez le délai d'expiration du mode EXEC sur 6 minutes sur les lignes VTY.

RTA(config-line)# **exec-timeout 6**

* + 1. Enregistrez la configuration en mémoire NVRAM.

Fermez la fenêtre de configuration.

* + 1. Accédez à l'invite de commande sur le bureau de **PCA** pour établir une connexion SSH à **RTA** .

Ouvrez une invite de commandes.

C : \ > **ssh/ ?**

Packet Tracer PC SSH

Utilisation : **SSH -l nom d'utilisateur cible**

C : \ >

Fermez l'invite de commandes.

## Configurer la sécurité de base sur le commutateur

Configurez le commutateur **SW1** avec les mesures de sécurité correspondantes. Reportez-vous aux étapes de configuration sur le routeur si vous avez besoin d'aide supplémentaire.

* + 1. Cliquez sur **SW1** et sélectionnez l'onglet **CLI** .

Ouvrez la fenêtre de configuration.

* + 1. Configurez le nom d'hôte comme **SW1**.
    2. Configurez l'adressage IP sur le SW1 **VLAN1** et activez l'interface.
    3. Configurez l'adresse de la passerelle par défaut.
    4. Désactivez tous les ports de commutation inutilisés.

**Remarque** : Sur un commutateur, il est une bonne pratique de sécurité de désactiver les ports inutilisés. Une méthode pour le faire consiste simplement à arrêter chaque port avec la commande '**shutdown**'. Cela nécessiterait d'accéder à chaque port individuellement. Il existe une méthode de raccourci pour apporter des modifications à plusieurs ports à la fois à l'aide de la **commande** Interface range. Sur **SW1,** tous les ports sauf FastEtherNet0/1 et GigabiteThernet0/1 peuvent être fermés avec la commande suivante :

SW1(config)# **interface range F0/2-24, G0/2**

SW1 (config-if-range) # **shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

<Output omitted>

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

La commande utilisait la plage de ports de 2 à 24 pour les ports FastEthernet, puis une plage de ports unique de GigabiteThernet0/2.

* + 1. Chiffrez tous les mots de passe en clair.
    2. Choisissez un mot de passe secret fort.
    3. Désactivez la commande de recherche DNS.
    4. Réglez le nom de domaine sur **CCNA.com**(sensible à la casse pour la notation en PT).
    5. Créez un utilisateur de votre choix avec un mot de passe fortement crypté.
    6. Générez des clés RSA de 1 024 bits.
    7. Configurez toutes les lignes VTY pour l'accès SSH et utilisez les profils d'utilisateurs locaux pour l'authentification.
    8. Réglez le délai d'expiration du mode EXEC sur 6 minutes sur toutes les lignes VTY.
    9. Enregistrez la configuration en mémoire NVRAM.

Fermez la fenêtre de configuration.

Fin du document