[Cisco] Sécurisation

Introduction

Vous retrouverez sur cette page des procédures et des commandes qui vous aideront à sécuriser des équipements Cisco.

Sécurisation

Auto-secure

La commande suivante va exécuter tout un tas de configurations pour sécuriser le système :

```
auto secure
```

Politique de mot de passe

Vous pouvez définir une politique de mot de passe en interdisant les mots de passe inférieurs à 8 caractères par exemple :

```
security passwords min-length <MIN_LEN>
```

Politique d'authentification

Il est possible de définir une **politique de sécurité d'authentification** où l'administrateur peut choisir 3 paramètres :

1. Le nombre de tentatives autorisé avant blocage.
2. L'interval de temps du compteur de nombre de connexion.
3. Le temps de blocage.

Voici la commande :

```
login block-for <3> attemps <2> within <1>
```

Politique d'inactivité

Par défaut, une période d'inactivité de 10 minute provoquera une déconnexion automatique sur une session EXEC (privilégiée).

Vous pouvez modifier cette valeur grâce à la commande suivante :

```
exec-timeout <MINUTE> <SECOND>
```

Port protégé

Si vous souhaitez bloquer la communication entre deux ports d'un switch, vous pouvez effectuer la commande suivante sur les interfaces qui ne doivent pas communiquer pas entre elles :

```
switchport protected
```

Revision #6
Created 14 November 2023 10:39:50 by Elieroc
Updated 3 April 2025 12:26:34 by Elieroc