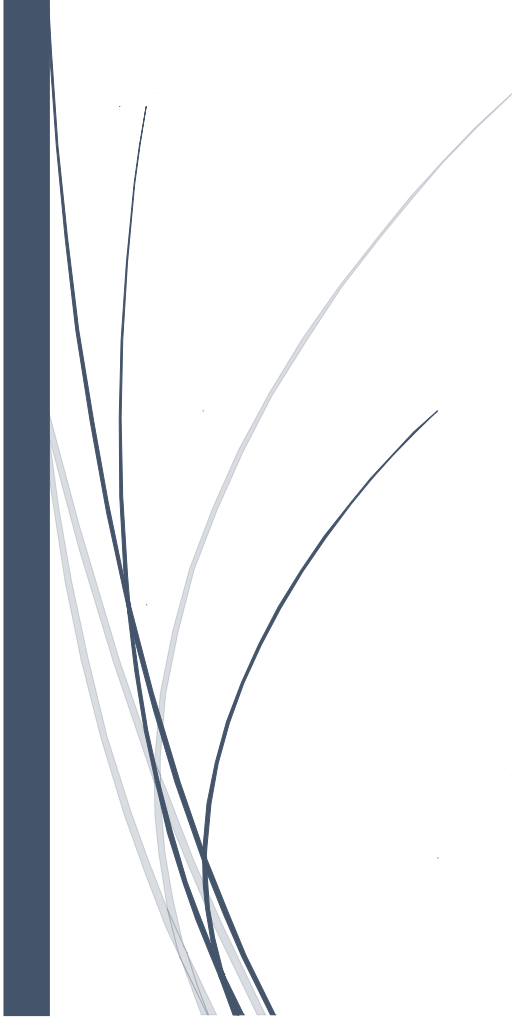
19/04/2015

# Sécurisation d'un switch Cisco

V1



Lecaudey Etienne

| Tutoriel 1.1 : Sécurisation d'un switch Cisco | | |
|---|---|---|
| Lecaudey Etienne | Version 1.0 | 19/04/2016 |

# SOMMAIRE :

## Table des matières

### Table des matières



## Objectifs :

| Tutoriel 1.1 : Sécurisation d'un switch Cisco | | |
|---|---|---|
| Lecaudey Etienne | Version 1.0 | 19/04/2016 |

L'objectif de cette procédure est de configurer et sécuriser un switch Cisco  Catalyst 2960 pour éviter toutes intrusions dans notre réseau

# *Information sur les versions*:

| | | |
|---|---|---|
| Switch Cisco | Catalyst 2960 | 192.168.1.125 |

# *Configuration des services* :

Pour commencer, nous devons donner un nom à notre switch :

```
Switch(config)#hostname SW1
```

avec cette commande, le mot de passe n'est pas crypté, nous devons alors utilisé la commande :

```
SW1(config)#enable secret 12345
```

et on crée un utilisateur local :

```
SW1(config)#username etienne password 12345
```

# Activation du Ssh :

Pour activer le Ssh nous devons donner un  nom de domaine à notre switch

```
SW1(config)#ip domain-name sio.local
```

Puis, on génère les certificats SSH :

```
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.sio.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
```

ensuite, on active le Ssh :,

```
SW1(config)#ip ssh version 2
SW1(config)#line vty 0 4
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#username etienne password 12345
```

puis on ajoute un auto-logout de session qui permettra de nous déconnecter au bout de 10 min et une déconnexion automatique en cas d'inactivité d'une durée de 5 minutes

```
SW1(config)#ip ssh version 2
SW1(config)#line vty 0 4
SW1(config-line)#exec-timeout 10 0
SW1(config-line)#line con 0
SW1(config-line)#exec-timeout 5 0
SW1(config-line)#
```

Ensuite, on ajoute une adresse IP au VLAN d'administration :

```
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.1.125 255.255.255.0
SW1(config-if)#no shutdown
```

# Désactiver les services inutiles :

- **VLAN Trunking Protocol**

le protocole VTP permet de gérer de manière centralisé les VLANS d'un réseau. Si nous n'utilisons pas ce protocole, nous le désactivons.

```
SW1(config)#vtp mode transparent
Device mode already VTP Transparent for VLANS.
```

- **Source-routing**

Le service de source-routing permet à l'émetteur d'un paquet IP de spécifier le chemin que doit prendre le paquet pour accéder à sa destination. Par mesure de sécurité, nous désactivons ce service pour éviter que ces paquets passent à travers les tables de routages

```
SW1(config)#no ip source-route
```

- **Résolution DNS**

Si la résolution DNS n'est pas configurée sur le switch, il est recommandé de désactiver les requêtes DNS

```
SW1(config)#no ip domain-lookup
```

- Service Cisco Discovery Protocol

Le service CDP (Cisco Discovery Protocol) est dangereux d'utilisation dans la mesure où il permet d'apprendre qu'il s'agit d'un matériel Cisco, de déterminer le numéro du modèle et la version de l'OS utilisé. Ces informations peuvent être utiliser pour trouver les vulnérabilités du switch, et pour préparer une attaque contre le switch.

```
SW1(config)#no cdp run
```

- **Service HTTP :**

Le service http est utilisé pour administrer le routeur en http. Ce protocole est non sécurisé notamment pour la transmission des mots de passe en clair sur le réseau, il est donc recommandé de le désactiver.

```
SW1(config)#no ip http server
```

- **Service finger**

Le service finger est utilisé pour découvrir quels utilisateurs sont enregistrés dans un dispositif du réseau. Il est donc recommandé de le désactiver.

```
SW1(config)#no service finger
```

- **Services small-servers**

Les services « small-server » (echo, daytime…) doivent être désactivés s'ils ne sont pas utilisés.

```
SW1(config)#no service tcp-small-servers
SW1(config)#no service udp-small-servers
```

# Activer les services de sécurité :

- **Service password encryption**

Le service password-encryption devra être activé. Il chiffre certains mots de passe avec un algorithme dit de type 7 à savoir l'algorithme de Vigenère, considéré comme (très) faible. Il n'a d'utilité que pour protéger visuellement certaines informations de la configuration des regards indiscrets. Il n'est pas possible de changer d'algorithme à l'heure actuelle, il s'agit d'une limitation de CISCO.

```
SW1(config)#service password-encryption
```

- **Service tcp-keepalives-in**

L'activation de ce service peut réduire les effets d'une attaque DoS. Les sessions orphelines seront terminées pour ne pas consommer de ressources système.

```
SW1(config)#service tcp-keepalive-in
```

- **Service scheduler**

Une fois ce service activé, les processus plantés ou bloqués seront tués.

```
SW1(config)#scheduler max-task-time 5000
```

- **Désactivation des interfaces non utilisées**

```
SW1(config)#interface range fastEthernet 0/1-24
SW1(config-if-range)#shutdown
```

- **Anti-DHCP snooping :**

```
SW1(config)#ip dhcp snooping
```

pour activer les trames dhcp sur un port du switch nous utilisons les commandes suivantes :

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#ip dhcp snoo
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#ip dhcp snooping limit rate 100
```

# Port-security:

**Sécurisation manuel :**

Pour sécuriser des ports avec port-security, nous devons utiliser les commandes suivantes :

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address 74d4.358f.f6f5
```


**Nous devons entrer l'adresse mac manuellement pour sécuriser ce port.**

**Sécurisation automatique :**

```
SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address sticky
```

ici, le premier ordinateur à se brancher sur le port aura son adresse MAC réservé sur ce port.

**Configuration la réaction lors de la violation de sécurité :**

**3 méthodes :**

- shutdown :Elle désactive l'interface lorsque qu'il y a violation. Pour la réactive, nous devons désactiver le port manuellement et le réactiver manuellement (shutdown – no shutdown)
- protect : Les trames ayant des adresses MAC de sources inconnues sont bloquées, les autres sont autorisées
- restrict : Alerte SNMP envoyée et le compteur de violation est incrémenté

pour activer ces réactions, nous devons utilisées les commandes suivantes :

```
SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security violation nom_methode
```

On peut aussi augmenter le nombre d'adresse mac par port avec la commande :

```
SW1(config-if)#switchport port-security maximum x
```

X étant le nombre d'adresse max accepté sur le port.

## Voir les ports sécurisés :

show port-security :

voir de manière globale les ports sécurisés

```
SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Fa0/1              1            1                  0         Shutdown
      Fa0/3              1            0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

show port-security address :

Voir de manière détaillé les adresses mac de chaque port :

```
SW1#show port-security address
          Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                       Ports   Remaining Age
                                                                (mins)
----    -----------       ----                       -----   -------------
   1    74d4.358f.f6f5    SecureConfigured           Fa0/1         -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

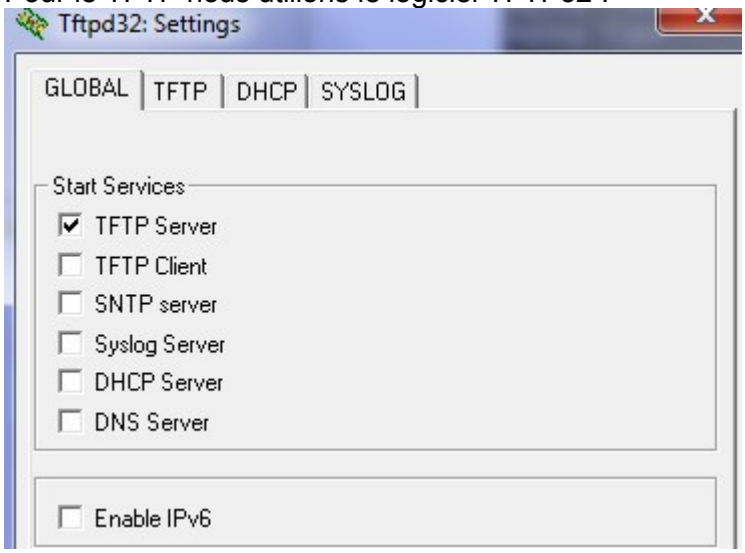
show port-security interface Fastethernet 0/1 :

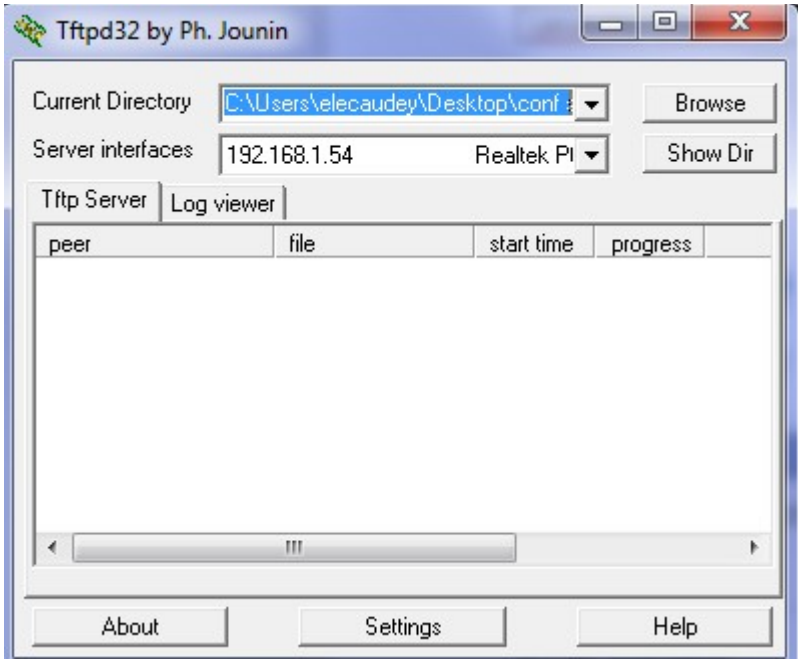
voir de manière détaille la sécurité sur un port spécifique :

```
SW1#show port-security interface fastethernet 0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

# TFTP :

Pour le TFTP nous utilions le logiciel TFTP32 :

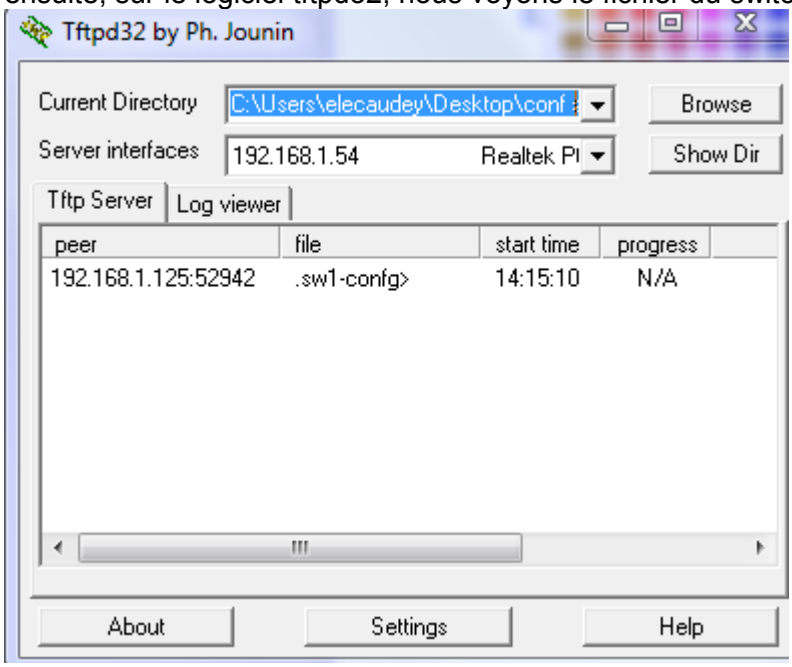


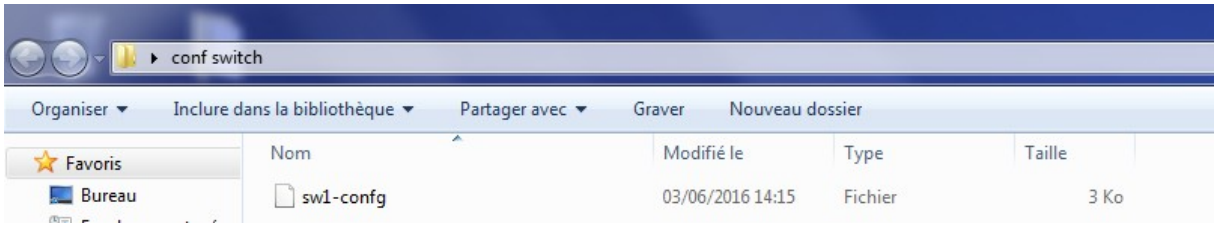




puis sur le switch, on entre la commande suivantes :

```
SW1#copy start tftp
Address or name of remote host []? 192.168.1.54
```

ensuite, sur le logiciel tftpd32, nous voyons le fichier du switch :




*Fichier de configuration du switch dans le même dossier que cette procédure*