Travaux pratiques : implémentation de la sécurité VLAN

Topologie

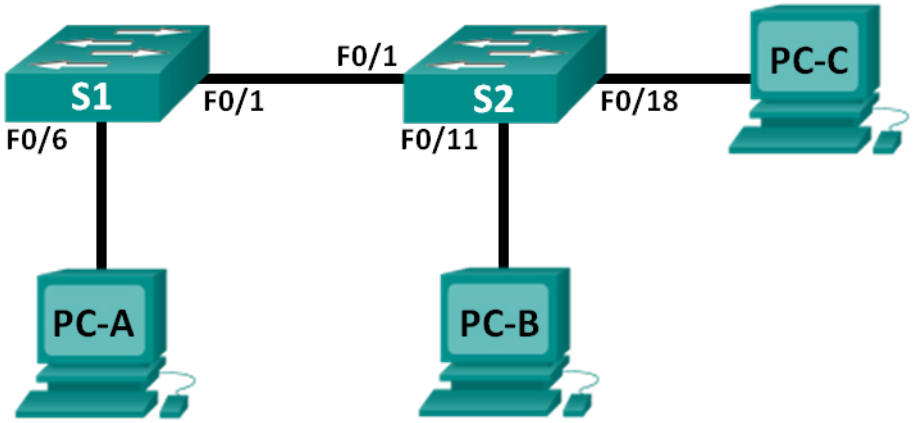

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	Carte réseau	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	Carte réseau	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	Carte réseau	172.17.99.4	255.255.255.0	172.17.99.1

Attributions de VLAN

VLAN	Nom
10	Données
99	Management&Native
999	BlackHole

Objectifs

Partie 1 : création du réseau et configuration des paramètres de périphérique de base

Partie 2 : implémentation de la sécurité VLAN sur les commutateurs

Contexte/scénario

Il est recommandé de configurer certains paramètres de sécurité de base pour les ports en mode accès et en mode trunk sur les commutateurs. Cela permet d'empêcher les attaques de VLAN ainsi que l'analyse possible du trafic réseau.

Au cours de ces travaux pratiques, vous allez configurer les périphériques réseau dans la topologie à l'aide de divers paramètres de base, vérifier la connectivité et appliquer des mesures de sécurité plus sévères sur les commutateurs. Vous allez également examiner comment les commutateurs Cisco se comportent à l'aide de diverses commandes **show**. Vous appliquerez ensuite des mesures de sécurité.

Remarque : les commutateurs utilisés dans ces travaux pratiques sont des modèles Cisco Catalyst 2960s équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques.

Remarque : assurez-vous que les commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Ressources requises

- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 3 PC (Windows 7, Vista ou XP, équipés d'un programme d'émulation du terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

Partie 1 : Création du réseau et configuration des paramètres de base du périphérique

Dans la Partie 1, vous allez configurer les paramètres de base sur les commutateurs et les PC. Reportez-vous à la table d'adressage pour connaître le nom des périphériques et obtenir des informations d'adresse.

Étape 1 : Câblez le réseau conformément à la topologie.

Étape 2 : Initialisez et redémarrez les commutateurs.

Étape 3 : Configurez les adresses IP sur PC-A, PC-B et PC-C.

Reportez-vous à la table d'adressage pour obtenir des informations sur les adresses des PC.

Étape 4 : Configurez les paramètres de base pour chaque commutateur.

a. Désactivez la recherche DNS.

b. Configurez les noms des périphériques conformément à la topologie.

c. Attribuez **class** comme mot de passe du mode d'exécution privilégié.

d. Attribuez **cisco** en tant que mots de passe de console et vty, et activez la connexion des lignes de console et vty.

e. Configurez la journalisation synchrone des lignes de console et vty.

Étape 5 : Configurez des VLAN sur chaque commutateur.

a. Créez et nommez les VLAN conformément à la table d'attribution des VLAN.

b. Configurez l'adresse IP indiquée dans la table d'adressage de VLAN 99 sur les deux commutateurs.

c. Configurez F0/6 sur S1 en tant que port d'accès et attribuez-le à VLAN 99.

d. Configurez F0/11 sur S2 en tant que port d'accès et attribuez-le à VLAN 10.

e. Configurez F0/18 sur S2 en tant que port d'accès et attribuez-le à VLAN 99.

f. Exécutez la commande **show vlan brief** afin de contrôler les attributions de VLAN et de ports.

À quel VLAN un port non attribué, tel que F0/8 sur S2, appartiendrait-il ?

Étape 6 : Configurez la sécurité de base du commutateur.

a. Configurez une bannière MOTD pour avertir les utilisateurs que tout accès non autorisé est interdit.

b. Chiffrez tous les mots de passe.

c. Désactivez tous les ports physiques non utilisés.

d. Désactivez le service Web de base en cours d'exécution.

```
S1(config)# no ip http server
S2(config)# no ip http server
```

e. Copiez la configuration en cours en tant que configuration initiale.

Étape 7 : Vérifiez la connectivité entre les périphériques ainsi que les informations VLAN.

a. À partir d'une invite de commande sur PC-A, envoyez une requête ping à l'adresse de gestion de S1. Les requêtes ping ont-elles abouti ? Pourquoi ?

b. À partir de S1, envoyez une requête ping à l'adresse de gestion de S2. Les requêtes ping ont-elles abouti ? Pourquoi ?

c. À partir d'une invite de commande sur PC-B, envoyez une requête ping aux adresses de gestion sur S1 et S2, et à l'adresse IP de PC-A et PC-C. Les requêtes ping ont-elles abouti ? Pourquoi ?

d. À partir d'une invite de commande sur PC-C, envoyez une requête ping aux adresses de gestion sur S1 et S2. Avez-vous réussi ? Pourquoi ?

Remarque : il peut être nécessaire de désactiver le pare-feu du PC pour envoyer une requête ping entre les PC.

Partie 2 : Implémentation de la sécurité VLAN sur les commutateurs

Étape 1 : Configurez les ports trunk sur S1 et S2.

a. Configurez le port F0/1 de S1 en tant que port trunk.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Configurez le port F0/1 de S2 en tant que port trunk.

```
S2(config)# interface f0/1
```

```
S2(config-if)# switchport mode trunk
```

c. Vérifiez le trunking sur S1 et S2. Exécutez la commande **show interface trunk** sur les deux commutateurs.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Étape 2 : Modifiez le VLAN natif pour les ports trunk de S1 et S2.

La modification du VLAN natif pour les ports trunk à partir du VLAN 1 vers un autre VLAN est une méthode de sécurité recommandée.

a. Quel est le VLAN natif actuel pour les interfaces F0/1 de S1 et S2 ?

b. Configurez le VLAN natif sur l'interface trunk F0/1 de S1 à VLAN 99 - Management&Native.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Attendez quelques secondes. Vous devriez commencer à recevoir des messages d'erreur dans la session en mode console de S1. Que signifie le message « %CDP-4-NATIVE_VLAN_MISMATCH: » ?

d. Configurez le VLAN natif sur l'interface trunk F0/1 de S2 à VLAN 99.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Vérifiez que le VLAN natif est désormais le VLAN 99 sur les deux commutateurs. Le résultat de S1 est affiché ci-dessous.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Étape 3 : Vérifiez que le trafic peut correctement traverser la liaison trunk.

a. À partir d'une invite de commande sur PC-A, envoyez une requête ping à l'adresse de gestion de S1. Les requêtes ping ont-elles abouti ? Pourquoi ?

b. À partir de la session en mode console sur S1, envoyez une requête ping à l'adresse de gestion de S2. Les requêtes ping ont-elles abouti ? Pourquoi ?

c. À partir d'une invite de commande sur PC-B, envoyez une requête ping aux adresses de gestion sur S1 et S2, et à l'adresse IP de PC-A et PC-C. Les requêtes ping ont-elles abouti ? Pourquoi ?

d. À partir d'une invite de commande sur PC-C, envoyez une requête ping aux adresses de gestion sur S1 et S2, et à l'adresse IP de PC-A. Avez-vous réussi ? Pourquoi ?

Étape 4 : Empêchez l'utilisation du protocole DTP sur S1 et S2.

Cisco utilise un protocole propriétaire connu sous le nom de protocole DTP (Dynamic Trunking Protocol) sur ses commutateurs. Certains ports négocient automatiquement le trunking. Il est recommandé de désactiver la négociation. Vous pouvez observer ce comportement par défaut en exécutant la commande suivante :

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Résultat omis>
```

a. Désactivez la négociation sur S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Désactivez la négociation sur S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

c. Vérifiez que la négociation est désactivée en exécutant la commande **show interface f0/1 switchport** sur S1 et S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<Résultat omis>
```

Étape 5 : Sécurisez les ports d'accès sur S1 et S2.

Même si vous arrêtez les ports non utilisés sur les commutateurs, si un périphérique est connecté à l'un de ces ports et que l'interface est activée, le trunking peut avoir lieu. Par ailleurs, tous les ports par défaut sont dans VLAN 1. Il est recommandé de placer tous les ports non utilisés dans un VLAN « trou noir » (black hole). Au cours de cette étape, vous allez désactiver le trunking sur l'ensemble des ports non utilisés. Vous attribuerez également les ports non utilisés au VLAN 99. Dans le cadre de ces travaux pratiques, seuls les ports 2 à 5 seront configurés sur les deux commutateurs.

a. Exécutez la commande **show interface f0/2 switchport** sur S1. Notez le mode d'administration et l'état de la négociation de trunking.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Résultat omis>
```

b. Désactivez le trunking sur les ports d'accès de S1.

```
S1(config)# interface range f0/2 – 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Désactivez le trunking sur les ports d'accès de S2.

d. Vérifiez que le port F0/2 est configuré pour accéder à S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Résultat omis>
```

e. Vérifiez que les attributions des ports VLAN sur les deux commutateurs sont correctes. S1 est indiqué ci-dessous à titre d'exemple.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
```

```
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
Restrict VLANs allowed on trunk ports.
```

Par défaut, tous les VLAN sont autorisés à être acheminés sur des ports trunk. Pour des raisons de sécurité, il est recommandé de n'autoriser que les VLAN spécifiques souhaités à traverser des liaisons trunk sur votre réseau.

f. Faites en sorte que le port trunk F0/1 sur S1 n'autorise que les VLAN 10 et 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

g. Faites en sorte que le port trunk F0/1 sur S2 n'autorise que les VLAN 10 et 99.

h. Vérifiez les VLAN autorisés. Exécutez une commande **show interface trunk** en mode d'exécution privilégié à la fois sur S1 et S2.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

Quel est le résultat ?

Remarques générales

Quels sont, le cas échéant, les problèmes de sécurité liés à la configuration par défaut d'un commutateur Cisco ?