Université Mohammed Premier Oujda
École Nationale des Sciences Appliquées
Département : Électronique, Télécommunications et Informatique
Filière : GI/GEII / Niveau : GI5/GEII5
Module : Interconnexion des réseaux

TP2 Security :

Sécurisation des ports VTY à l'aide d'une liste de contrôle d'accès IPv4 standard

Enseignant : Mohammed SABER

Année Universitaire : 2017/2018

Objectifs pédagogiques de TP :

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

Partie 1 : configuration de la topologie et initialisation des périphériques

- Configurez l'équipement pour qu'il corresponde à la topologie du réseau.
- Initialisez et redémarrez les routeurs et les commutateurs.

Partie 2 : configuration des périphériques et vérification de la connectivité

- Attribuez une adresse IP statique aux PC.
- Configurez les paramètres de base sur les routeurs.
- Vérifiez la connectivité entre les périphériques.

Partie 3 : configuration et vérification des listes de contrôle d'accès numérotées et nommées standard

- Configurez, appliquez et vérifiez une liste de contrôle d'accès standard numérotée.
- Configurez, appliquez et vérifiez une liste de contrôle d'accès nommée.

Partie 4 : modification d'une liste de contrôle d'accès standard

- Configuration et application d'une liste de contrôle d'accès aux lignes VTY.
- Vérification de l'implémentation de la liste de contrôle d'accès.
- Vérification de la liste de contrôle d'accès via Telnet et SSH.

Scénarios

l est recommandé de limiter l'accès aux interfaces d'administration de routeurs, comme la console et les lignes vty. Une liste de contrôle d'accès (ACL) peut être utilisé pour autoriser l'accès d'adresses IP spécifiques, ce qui garantit que seuls les ordinateurs d'administrateur sont autorisés à accéder via Telnet ou SSH au routeur.

Remarque : dans les sorties d'équipements Cisco, l'abréviation access-list est utilisée pour les listes de contrôle d'accès.

Au cours de ces travaux pratiques, vous allez créer et appliquer une liste de contrôle d'accès standard nommée pour limiter l'accès distant aux lignes vty du routeur.

Après avoir créé et appliqué la liste de contrôle d'accès, vous la testerez et vérifierez en accédant au routeur à partir de différentes adresses IP via Telnet ou SSH.

Ces travaux pratiques fournissent les commandes nécessaires à la création et l'application de la liste de contrôle d'accès.

Ressources requises

Ressources nécessaires :

1. Un routeur équipé des interfaces de type Ethernet ;
2. Un ordinateur Windows 7 avec un programme d'émulation de terminal (PuTTY) ;
3. Trois câbles Ethernet directs (PC-A à S1, S1 à R1, R1 à S2, S2 à PC-B) ;
4. Un câble console avec connecteur RJ-45 vers DB-9 (PC-A à R1) ;
5. Accès à l'invite de commandes des hôtes PC-A et PC-B ;
6. Accès à la configuration TCP/IP du réseau des hôtes PC-A et PC-B.
7. Deux commutateurs (Switch) ;

Consignes pour le TP

1. Suivez les instructions pour chaque étape.
2. Ne déplacez pas le matériel.
3. **N'utilisez pas les Clés USB sur les machines**.
4. A la fin de TP, SVP réorganiser votre table :
   - Éteindre toutes les machines.
   - Réorganiser les chaises à ces places avant de sortir.
   - MERCI d'avance.
5. **Chaque étudiant ne respect pas les consignes de TP sera sanctionné.**

Scénario A : Autorisant l'accès d'un PC aux lignes VTY, mais refusant toutes les autres adresses IP sources du même réseau

Étape 1 : Préparation du réseau

Atelier de TP

L'architecture de l'atelier du scénario est la suivante :

Les informations pour chaque équipement pour ces travaux pratiques sont présentées sur le tableau suivant :

Périphérique	Interface	Adresse IP	Masque réseau	Passerelle
R1	G0/1 (Type Ethernet)	192.168.10.1	255.255.255.0	N/D
PC-A	N/D	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	N/D	192.168.10.3	255.255.255.0	192.168.10.1

Étape 2 : Installation, suppression et rechargement des routeurs

Tâche 1 : Connexion des périphériques

Connectez les périphériques de réseau similaire à celui de la topologie de l'atelier.

Tâche 2 : suppression des configurations existantes sur les routeurs

Il est nécessaire de commencer avec un routeur non configuré. L'utilisation d'un routeur comportant déjà une configuration peut produire des résultats imprévisibles. Les étapes suivantes permettent de préparer le routeur avant d'effectuer les travaux pratiques pour que les options de configuration précédentes ne créent pas d'interférence.

1. Passez en mode d'exécution privilégié.

2. **Effacement de la configuration :** Pour effacer la configuration, lancez la commande `erase startup-config`. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment effacer la configuration actuellement enregistrée en mémoire NVRAM, appuyez sur **Entrée**.
3. **Rechargement de la configuration :** Au retour de l'invite, lancez la commande ***reload***. Si vous êtes invité à enregistrer les modifications, répondez par **no** [**Que se passerait-il si vous répondiez yes à la question**].
4. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment recharger le routeur, appuyez sur **Entrée**. Dès que le routeur a terminé l'amorçage, choisissez de ne pas utiliser la fonction **AutoInstall**.
5. Répétez les questions 1 à 4 sur le routeur R2 ?
6. Répétez les questions 1 à 4 sur le routeur R3 ?

Étape 2 : Configuration basique des routeurs Cisco

Tâche 1 : Configuration de base de routeur

1. Configurez le nom d'hôte du routeur 1 en tant que **R1**.
2. Attribuez "**ensao**" au mot de passe de mode d'exécution privilégié sur les routeurs.
3. Attribuez "**ensao**" au mot de passe de console sur les routeurs.
4. Attribuez "**ensao**" au mot de passe vty sur les routeurs.
5. Affichez la configuration à l'aide de la commande `show running-config`.
6. Vérifier les mots de passe sont en clair sur les routeurs.
7. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**" sur les deux routeurs.

Tâche 2 : Désactivation des messages débogage non sollicités

1. Configurez les routeurs de sorte que les messages de console n'interfèrent pas avec l'entrée des commandes. Ceci est utile lorsque vous quittez le mode de configuration, car vous retournez à l'invite de commandes et l'option évite alors que des messages s'affichent dans la ligne de commande `logging synchronous` en **mode line** soit **console** soit **terminal virtuel VTY**.
2. Configurez le routeur de sorte que pas de délai d'attente, dans la ligne de commande `exec-timeout 0 0` en **mode line** soit **console** soit **terminal virtuel VTY**.
3. Désactivez la recherche DNS avec la commande `no ip domain-lookup`.
4. Sauvegardez la configuration actuelle `running-config` dans la configuration de démarrage `startup-config` sur les deux routeurs.

Tâche 3 : Configuration des interfaces de R1

1. En mode de configuration globale, configurez l'adresse IP pour l'interface de type Ethernet **G0/1** sur **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
2. Affectez la description suivante "**LAN link to S1**" pour cette interface.
3. Activez l'interface de type Ethernet.
4. Affichez la table de routage.
5. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**".

Tâche 4 : Configuration des interfaces Ethernet de PC-A et PC-B

Configurez les interfaces Ethernet de PC-A et PC-B à l'aide des adresses IP et des passerelles par défaut indiquées dans le tableau sous le diagramme de la topologie.

Tâche 5 : Vérifiez la connectivité entre les périphériques

Remarque : il est très important de vérifier si la connectivité fonctionne avant de configurer et d'appliquer des listes d'accès ! Veillez à vous assurer que votre réseau fonctionne correctement avant de commencer à filtrer le trafic.

1. A partir de **PC-A**, envoyez une requête `ping` vers **PC-B**, l' interface de type Ethernet sur **R1**. Les requêtes `ping` ont-elles abouti ?
2. A partir de **PC-B**, envoyez une requête `ping` vers **PC-A**, l' interface de type Ethernet sur **R1**. Les requêtes `ping` ont-elles abouti ?
3. A partir de **R1**, envoyez une requête `ping` vers **PC-A** et **PC-B**. Les requêtes `ping` ont-elles abouti ?

Tâche 5 : Vérifiez l'accès `Telnet` ou `SSH` avant de configurer la liste de contrôle d'accès

Remarque : il est très important de vérifier si la connectivité `Telnet` ou `SSH` fonctionne avant de configurer et d'appliquer des listes d'accès ! Veillez à vous assurer que votre réseau fonctionne correctement avant de commencer à filtrer le trafic.

1. A partir de **PC-A**, envoyez une requête `Telnet` ou `SSH` vers l' interface de type Ethernet sur **R1**. La requête `Telnet` ou `SSH` a-t-elle abouti ?
2. A partir de **PC-B**, envoyez une requête `Telnet` ou `SSH` vers l' interface de type Ethernet sur **R1**. La requête `Telnet` ou `SSH` a-t-elle abouti ?

Étape 3 : Configuration et application d'une liste de contrôle d'accès aux lignes VTY

Tâche 1 : Configurez une liste de contrôle d'accès standard numérotée

Les listes de contrôle d'accès standard filtrent le trafic en fonction de l'adresse IP de la source. L'une des meilleures pratiques types pour les listes de contrôle d'accès standard consiste à la configurer et l'appliquer aussi près que possible de la destination.

Configurez la liste de contrôle d'accès numérotée qui autorise l'accès de la machine **PC-A** sur **R1**.

Remarque : Puisque nous ne voulons pas autoriser l'accès à partir des autres ordinateurs, la propriété de refus implicite de la liste d'accès répond à nos besoins.

Tâche 2 : Placez une liste de contrôle d'accès standard sur le routeur

L'accès aux interfaces de Router doit être autorisé, et l'accès `Telnet` ou `SSH` doit être limité. Par conséquent, vous devez placer la liste de contrôle d'accès sur les lignes `Telnet` ou `SSH` de 0 à 4. A

partir de l'invite de configuration de Router, passez en mode de configuration de ligne pour les lignes de 0 à 4 et utilisez la commande `access-class` pour appliquer la liste de contrôle d'accès à toutes les lignes VTY.

Étape 4 : Vérification de l'implémentation de la liste de contrôle d'accès

Tâche 1 : Vérifiez la configuration de la liste de contrôle d'accès et son application aux lignes VTY

Utilisez `show access-lists` pour vérifier la configuration de la liste de contrôle d'accès. Utilisez la commande `show run` pour vérifier que la liste de contrôle d'accès a été appliquée aux lignes VTY.

Tâche 2 : Vérifiez que la liste de contrôle d'accès fonctionne convenablement

Les deux ordinateurs doivent pouvoir envoyer une requête `ping` à Router, mais seul PC-A doit être en mesure d'établir une connexion `Telnet` ou `SSH` avec cet équipement.

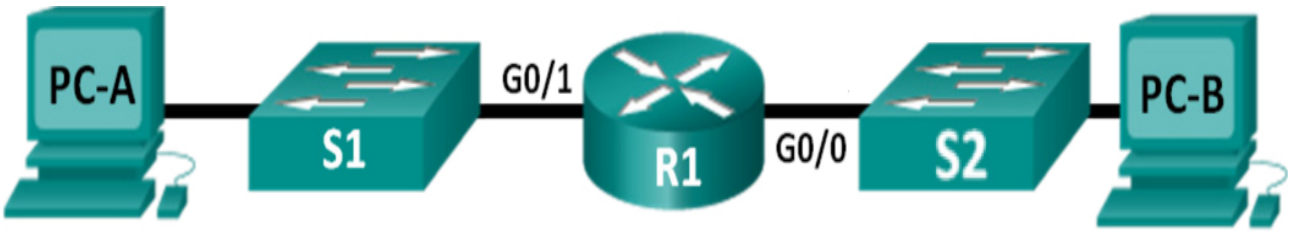
1. A partir de **PC-A**, envoyez une requête `ping` vers **PC-B**, l' interface de type Ethernet sur **R1**. Les requêtes `ping` ont-elles abouti ?
2. A partir de **PC-B**, envoyez une requête `ping` vers **PC-A**, l' interface de type Ethernet sur **R1**. Les requêtes `ping` ont-elles abouti ?
3. A partir de **PC-A**, envoyez une requête `Telnet` ou `SSH` vers l' interface de type Ethernet sur **R1**. La requête `Telnet` ou `SSH` a abouti ?
4. A partir de **PC-B**, envoyez une requête `Telnet` ou `SSH` vers l' interface de type Ethernet sur **R1**. La requête `Telnet` ou `SSH` a abouti ?

Scénario B : Configuration et vérification des restrictions VTY

Étape 1 : Préparation du réseau

Atelier de TP

L'architecture de l'atelier du scénario est la suivante :



Les informations pour chaque équipement pour ces travaux pratiques sont présentées sur le tableau suivant :

Périphérique	Interface	Adresse IP	Masque réseau	Passerelle
R1	G0/0 (Type Ethernet)	192.168.1.1	255.255.255.0	N/D
	G0/1 (Type Ethernet)	192.168.2.1	255.255.255.0	N/D
PC-A	N/D	192.168.2.2	255.255.255.0	192.168.2.1
PC-B	N/D	192.168.1.2	255.255.255.0	192.168.1.1

Étape 2 : Configuration basique des routeurs Cisco

Tâche 1 : Configuration de base de routeur

Même Configuration que le scénario A, concernant les tâches (1 et 2) de l'étape 2.

Tâche 2 : Configuration des interfaces de R1

1. En mode de configuration globale, configurez l'adresse IP pour l'interface de type Ethernet **G0/0** sur **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
2. Affectez la description suivante "**LAN link to S2**" pour cette interface.
3. Activez l'interface de type Ethernet.
4. En mode de configuration globale, configurez l'adresse IP pour l'interface de type Ethernet **G0/1** sur **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
5. Affectez la description suivante "**LAN link to S1**" pour cette interface.
6. Activez l'interface de type Ethernet.
7. Affichez la table de routage.
8. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**".

Tâche 3 : Configuration des interfaces Ethernet de PC-A et PC-B

Configurez les interfaces Ethernet de PC-A et PC-B à l'aide des adresses IP et des passerelles par défaut indiquées dans le tableau sous le diagramme de la topologie.

Tâche 5 : Vérifiez la connectivité entre les périphériques

Remarque : il est très important de vérifier si la connectivité fonctionne avant de configurer et d'appliquer des listes d'accès ! Veillez à vous assurer que votre réseau fonctionne correctement avant de commencer à filtrer le trafic.

1. A partir de **PC-A**, envoyez une requête `ping` vers **PC-B** et les interfaces de type Ethernet sur **R1**. Les requêtes `ping` ont-elles abouti ?
2. A partir de **PC-B**, envoyez une requête `ping` vers **PC-A** et les interfaces de type Ethernet sur **R1**. Les requêtes `ping` ont-elles abouti ?
3. A partir de **R1**, envoyez une requête `ping` vers **PC-A** et **PC-B**. Les requêtes `ping` ont-elles abouti ?

Tâche 5 : Vérifiez l'accès `Telnet` ou `SSH` avant de configurer la liste de contrôle d'accès

1. A partir de **PC-A**, envoyez une requête `Telnet` ou `SSH` vers l' interface de type Ethernet sur **R1**. La requête `Telnet` ou `SSH` a-t-elle abouti ?
2. A partir de **PC-B**, envoyez une requête `Telnet` ou `SSH` vers l' interface de type Ethernet sur **R1**. La requête `Telnet` ou `SSH` a-t-elle abouti ?

Étape 3 : Configuration et application de la liste de contrôle d'accès sur R1

Vous allez configurer une liste de contrôle d'accès standard nommée et l'appliquer aux lignes de terminal virtuel de routeur pour restreindre les accès à distance au routeur.

Tâche 1 : Configurez une liste de contrôle d'accès standard nommée

Créez une liste de contrôle d'accès standard nommée s'appeler **ADMIN-VTY** conformément à la stratégie suivante : Créez une entrée de contrôle d'accès d'autorisation (**permit**) pour le PC-A administrateur à l'adresse **192.168.2.2**, ainsi qu'une entrée de contrôle d'accès d'autorisation (**permit**) supplémentaire pour autoriser les autres adresses IP administratives réservées entre **192.168.2.4** et **192.168.2.7**.

Remarquez que la première entrée de contrôle d'accès **permit** autorise un hôte unique. En utilisant le mot clé **host**, l'instruction d'entrée de contrôle d'accès **permit 192.168.2.2 0.0.0.0** aurait pu être utilisée à la place. La deuxième entrée de contrôle d'accès **permit** autorise les hôtes **192.168.2.4** à **192.168.2.7**, en utilisant le **masque générique 0.0.0.3**, qui est l'inverse d'un masque de sous-réseau **255.255.255.252**.

Tâche 2 : Placez une liste de contrôle d'accès standard nommée sur le routeur

Maintenant que l'entrée de contrôle d'accès nommée est créée, appliquez-la en entrée aux lignes vty.

Tâche 3 : Vérification de la liste de contrôle d'accès standard nommée

L'utilisation de diverses commandes `show` peut vous aider à vérifier la syntaxe et l'emplacement de vos listes de contrôle d'accès sur votre routeur.

Vérifiez une liste de contrôle d'accès numérotée. (**Utilisation** : `show access-lists`).

Étape 4 : Vérification de la liste de contrôle d'accès via `Telnet` ou `SSH`

Tâche 1 : Test de la liste de contrôle d'accès aux lignes VTY à partir les différents réseaux

1. A partir de **PC-A**, envoyez une requête `ping` vers les interfaces de type Ethernet sur **R1**. ont-elles abouti ?
2. A partir de **PC-B**, envoyez une requête `ping` vers les interfaces de type Ethernet sur **R1**. ont-elles abouti ?
3. A partir de **PC-A**, envoyez une requête `Telnet` ou `SSH` vers les interfaces de type Ethernet sur **R1**. Les requêtes `Telnet` ou `SSH` ont-elles abouti ?
4. Dans le cas oui, Tapez `exit` à l'invite de commande et appuyez sur Entrée pour quitter la session `Telnet` ou `SSH`.
5. A partir de **PC-B**, envoyez une requête `Telnet` ou `SSH` vers les interfaces de type Ethernet sur **R1**. Les requêtes `Telnet` ou `SSH` ont-elles abouti ?
6. Dans le cas oui, Tapez `exit` à l'invite de commande et appuyez sur Entrée pour quitter la session `Telnet` ou `SSH`.

Tâche 2 : Test de la liste de contrôle d'accès aux lignes VTY à partir le même réseau

1. Modifiez votre adresse IP de la machine **PC-A** pour vérifier si la liste de contrôle d'accès nommée bloque les adresses IP non autorisées. Remplacez l'adresse IPv4 par **192.168.2.100** sur **PC-A**.
2. A partir de **PC-A**, envoyez une requête `ping` vers les interfaces de type Ethernet sur **R1**. ont-elles abouti ?
3. Essayez à nouveau d'établir une connexion `Telnet` ou `SSH` sur **R1**. La session `Telnet` ou `SSH` a-t-elle abouti ? Quel message a-t-il été reçu ?
4. Modifiez l'adresse IP sur **PC-A** pour vérifier si la liste de contrôle d'accès nommée autorise un hôte dont l'adresse IP figure dans la plage **192.168.2.4 - 192.168.2.7** à établir une connexion `Telnet` ou `SSH` avec le routeur. Après avoir modifié l'adresse IP sur PC-A, ouvrez une invite de commande Windows et essayez d'établir une connexion `Telnet` ou `SSH` avec le routeur **R1**.
5. A partir de **PC-A**, envoyez une requête `ping` vers les interfaces de type Ethernet sur **R1**. ont-elles abouti ?
6. La session `Telnet` ou `SSH` a-t-elle abouti ?
7. A partir du mode d'exécution privilégié sur **R1**, tapez la commande `show ip access-lists` et appuyez sur Entrée. Dans le résultat de la commande, notez que Cisco IOS affecte automatiquement les numéros de ligne aux entrées de contrôle d'accès (ACE) de la liste de contrôle d'accès (ACL) par incréments de 10 et indique le nombre de fois que chaque entrée de contrôle d'accès d'autorisation (**permit**) a été correctement associée (entre parenthèses).
8. A votre avis, pourquoi est-ce qu'il y a deux correspondances pour chaque entrée de contrôle d'accès **permit** alors qu'une seule connexion a été lancée à partir de chaque adresse IP ?

Étape 5 : Suppression des configurations sur les routeurs

Il est nécessaire de commencer avec un routeur non configuré. L'utilisation d'un routeur comportant déjà une configuration peut produire des résultats imprévisibles. Les étapes suivantes permettent de préparer le routeur avant d'effectuer les travaux pratiques pour que les options de configuration précédentes ne créent pas d'interférence.

1. Passez en mode d'exécution privilégié.
2. **Effacement de la configuration :** Pour effacer la configuration, lancez la commande ***erase startup-config***. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment effacer la configuration actuellement enregistrée en mémoire NVRAM, appuyez sur **Entrée**.
3. **Rechargement de la configuration :** Au retour de l'invite, lancez la commande ***reload***. Si vous êtes invité à enregistrer les modifications, répondez par **no** [**Que se passerait-il si vous répondiez yes à la question**].
4. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment recharger le routeur, appuyez sur **Entrée**. Dès que le routeur a terminé l'amorçage, choisissez de ne pas utiliser la fonction **AutoInstall**.