Travaux pratiques 4.6.2 : configuration avancée de la sécurité

Diagramme de topologie

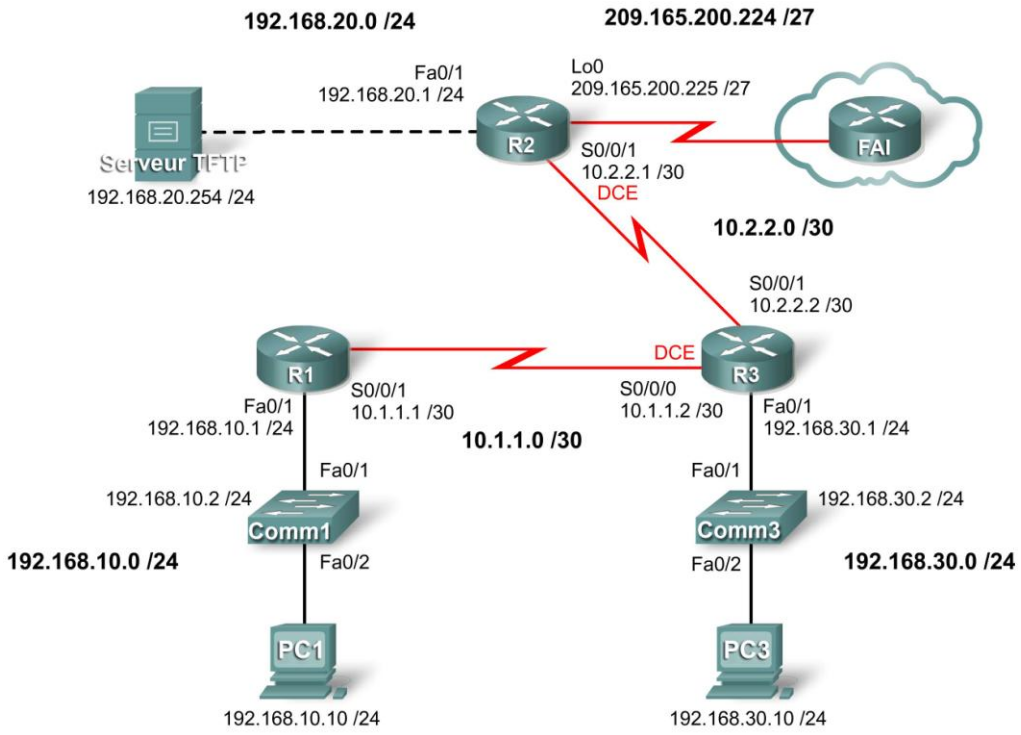

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/1	192.168.10.1	255.255.255.0	N/D
	S0/0/1	10.1.1.1	255.255.255.252	N/D
R2	Fa0/1	192.168.20.1	255.255.255.0	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	N/D
R3	Fa0/1	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
Comm1	VLAN10	192.168.10.2	255.255.255.0	N/D
Comm3	VLAN30	192.168.30.2	255.255.255.0	N/D
PC1	Carte réseau	192.168.10.10	255.255.255.0	192.168.10.1
PC3	Carte réseau	192.168.30.10	255.255.255.0	192.168.30.1
Serveur TFTP	Carte réseau	192.168.20.254	255.255.255.0	192.168.20.1

Objectifs pédagogiques

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

- Câbler un réseau conformément au diagramme de topologie
- Supprimer la configuration de démarrage et recharger un routeur pour revenir aux paramètres par défaut
- Exécuter les tâches de configuration de base d'un routeur
- Configurer et activer des interfaces
- Configurer la sécurité de base des ports
- Désactiver les services et interfaces Cisco inutilisés
- Protéger les réseaux d'entreprise contre des principales attaques externes et internes
- Comprendre et gérer les fichiers de configuration Cisco IOS ainsi que le système de fichiers Cisco
- Configurer et utiliser Cisco SDM (Security Device Manager) pour définir la sécurité de base d'un routeur

Scénario

Au cours de ces travaux pratiques, vous apprendrez à configurer la sécurité au moyen du réseau indiqué dans le diagramme de topologie. Si vous rencontrez des difficultés, reportez-vous aux travaux pratiques sur la sécurité de base. Essayez cependant de travailler en parfaite autonomie. Dans le cadre de cet exercice, n'activez pas la protection par mot de passe et évitez de vous connecter aux lignes de console, afin d'éviter toute déconnexion accidentelle. Vous devez toutefois sécuriser la ligne de console par d'autres moyens. Dans ces travaux pratiques, le mot de passe à utiliser est **ciscoccna**.

Tâche 1 : préparation du réseau

Étape 1 : câblage d'un réseau similaire à celui du diagramme de topologie

Étape 2 : suppression des configurations existantes sur les routeurs

Tâche 2 : exécution des configurations de routeur de base

Étape 1 : configuration des routeurs

Configurez les routeurs R1, R2 et R3 conformément aux instructions suivantes :

- Configurez le nom d'hôte du routeur conformément au diagramme de topologie.
- Désactivez la recherche DNS.
- Configurez une bannière de message du jour.
- Configurez les adresses IP sur les interfaces des routeurs R1, R2 et R3.
- Activez le protocole RIPv2 sur tous les routeurs de tous les réseaux.
- Créez une interface de bouclage sur R2 afin de simuler une connexion Internet.
- Créez des réseaux locaux virtuels sur les commutateurs Comm1 et Comm3, puis configurez les interfaces à intégrer aux réseaux locaux virtuels.
- Configurez le routeur R3 afin d'assurer une connectivité sécurisée SDM.
- Installez SDM sur PC3 ou R3, si ce n'est déjà fait.

Étape 2 : configuration des interfaces Ethernet

Configurez les interfaces Ethernet de PC1, PC3 et du serveur TFTP à l'aide des adresses IP et des passerelles par défaut figurant dans la table d'adressage fournie au début de ces travaux pratiques.

Étape 3 : test de la configuration du PC via l'envoi d'une requête ping à la passerelle par défaut de chaque PC et du serveur TFPT

Tâche 3 : sécurisation de l'accès aux routeurs

Étape 1 : configuration d'une authentification AAA et de mots de passe sécurisés à l'aide d'une base de données locale

Créez un mot de passe sécurisé pour l'accès au routeur. Créez le nom d'utilisateur **ccna**, à stocker localement sur le routeur. Configurez le routeur de manière à utiliser la base de données d'authentification locale. Dans ces travaux pratiques, pensez à utiliser le mot de passe **ciscoccna**.

Étape 2 : sécurisation de la console et des lignes vty

Configurez la console, ainsi que les lignes vty, de manière à refuser l'accès aux utilisateurs saisissant un mot de passe et un nom d'utilisateur incorrects, et ce à deux reprises en l'espace de 2 minutes. Bloquez toute tentative de connexion supplémentaire pendant 5 minutes.

Étape 3 : vérification du refus des tentatives de connexion, une fois le nombre maximal de tentatives autorisé atteint

Tâche 4 : sécurisation de l'accès au réseau

Étape 1 : sécurisation du protocole de routage RIP

N'envoyez pas de mises à jour RIP aux routeurs non tributaires du réseau (tous les routeurs non mentionnés dans ce scénario). Authentifiez les mises à jour RIP et cryptez-les.

Étape 2 : vérification du fonctionnement du routage RIP

Tâche 5 : consignation des activités via le protocole SNMP (Simple Network Management Protocol)

Étape 1 : configuration de la connexion SNMP au serveur syslog via l'adresse 192.168.10.250 sur tous les périphériques

Étape 2 : consignation de tous les messages avec un niveau de gravité 4 sur le serveur syslog

Tâche 6 : désactivation des services réseau Cisco inutilisés

Étape 1 : désactivation des interfaces inutilisées de tous les périphériques

Étape 2 : désactivation des services globaux inutilisés sur R1

Étape 3 : désactivation des services d'interface inutilisés sur R1

Étape 4 : utilisation de la fonction AutoSecure pour sécuriser R2

Dans ces travaux pratiques, pensez à utiliser le mot de passe **ciscoccna**.

Tâche 7 : gestion de Cisco IOS et des fichiers de configuration

Étape 1 : identification de l'emplacement du fichier running-config dans la mémoire du routeur

Étape 2 : transfert du fichier running-config de R1 vers R2 via le serveur TFTP

Étape 3 : interruption et restauration de R1 via ROMmon

Copiez, puis collez, les commandes suivantes sur R1. Restaurez R1 ensuite, via ROMmon.

```
line vty 0 4
 exec-timeout 0 20
line console 0
 exec-timeout 0 20
end
copy run start
exit
```

Étape 4 : depuis R2, restauration de la configuration enregistrée dans R1, via le serveur TFTP

Étape 5 : suppression de la configuration enregistrée depuis R2

Tâche 8 : sécurisation de R2 via SDM

Étape 1 : connexion à R2 via PC1

Étape 2 : accès à la fonction d'audit de sécurité

Étape 3 : exécution d'un audit de sécurité

Étape 4 : définition des paramètres à appliquer au routeur

Étape 5 : validation de la configuration du routeur

Tâche 9 : documentation des configurations des routeurs

Exécutez la commande **show run** sur chaque routeur et capturez les configurations.

Tâche 10 : remise en état

Supprimez les configurations et rechargez les routeurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage souhaité et restaurez les paramètres TCP/IP pour les PC hôtes habituellement connectés aux autres réseaux (réseaux locaux de votre site ou Internet).