# Packet Tracer – Pare-feu de serveurs et ACL de routeurs

## Table d'adressage

| Appareil | Adresse IP privée | Adresse IP publique | Masque de sous-réseau | Site |
|---|---|---|---|---|
| Serveur web | S/O | 209.165.201.10 | 255.255.255.0 | Internet |

## Objectifs

**Partie 1 : Se connecter au serveur web**

**Partie 2 : Bloquer les sessions HTTP non chiffrées**

**Partie 3 : Accéder au pare-feu sur le serveur de messagerie**

## Contexte

Au cours de cette activité, vous accéderez en tant qu'utilisateur sur le site de Metropolis et vous vous connecterez à un serveur web distant avec HTTP et HTTPS. L'adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez un terminal client sur le site de Metropolis pour tester la connectivité à un serveur web distant, puis sécuriserez le site de Metropolis en interdisant aux sessions web non chiffrées de se connecter au monde extérieur.

# Partie 1 : Se connecter au serveur web

## Étape 1 : Accédez au serveur web du siège sur l'ordinateur de Sally avec HTTP.

a. Cliquez sur le site du **siège social de la Metropolis Bank**, puis sur l'ordinateur de **Sally**.

b. Cliquez sur l'onglet **Poste de travail**, puis sur **Navigateur web**.

c. Saisissez l'URL **http://www.cisco.corp**, puis cliquez sur **Go**.

d. Cliquez sur le lien **Page de connexion**.

Pourquoi est-il risqué d'envoyer des informations via ce site ?

## Étape 2 : Accédez au serveur web du siège social sur le PC de Sally avec HTTPS.

a. Accédez au **Navigateur web** sur l'ordinateur de Sally.

b. Saisissez l'URL **https://www.cisco.corp**, puis cliquez sur Go.

c. Cliquez sur le lien **Page de connexion**.

Pourquoi est-il moins risqué d'envoyer des informations via ce site ?

d. Fermez l'ordinateur de **Sally**.

# Partie 2 : Bloquer les sessions HTTP non chiffrées

## Étape 1 : Configurez le routeur HQ_Router.

a. Sur le site du **siège social de la Metropolis Bank**, cliquez sur le routeur **HQ_Router**.

b. Cliquez sur l'onglet **CLI**, puis appuyez sur **Entrée**.

c. Utilisez le mot de passe **cisco** pour vous connecter au routeur.

d. Utilisez la commande **enable**, puis **configure terminal** pour accéder au mode de configuration globale.

Pour éviter la circulation de trafic HTTP non chiffré via le routeur du siège, les administrateurs réseau peuvent créer et déployer des listes de contrôle d'accès (ACL).

Les commandes suivantes ne relèvent pas du cadre de cette formation, mais sont utilisées pour montrer qu'il est possible de bloquer le trafic non chiffré via le routeur HQ_Router.

e. Depuis le mode de configuration globale **HQ_Router**(config)# copiez la configuration access-list suivante, puis collez-la sur le routeur **HQ_Router**.

```
!
access-list 101 deny tcp any any eq 80
access-list 101 permit ip any any
!
int gig0/0
ip access-group 101 in
!
end
```

f. Fermez le routeur **HQ_Router**.

## Étape 2 : Accédez au serveur web du siège sur l'ordinateur de Sally avec HTTP.

a. Sur le site du **siège social de la Metropolis Bank**, cliquez sur l'ordinateur de **Sally**.

b. Cliquez sur l'onglet **Poste de travail**, puis sur **Navigateur web**.

c. Saisissez l'URL **http://www.cisco.corp**, puis cliquez sur **Go**.

L'ordinateur de **Sally** est-il en mesure d'accéder au serveur web du siège social avec HTTP ?

## Étape 3 : Accédez au serveur web du siège social sur le PC de Sally avec HTTPS.

a. Accédez au **Navigateur web** sur l'ordinateur de Sally.

b. Saisissez l'URL **https://www.cisco.corp**, puis cliquez sur Go.

L'ordinateur de Sally est-il capable d'accéder au serveur web du siège en utilisant le protocole HTTP ?

c. Fermez l'ordinateur de **Sally**.

# Partie 3 : Accéder au pare-feu sur le serveur de messagerie

a. Sur le site du **siège social de la Metropolis Bank**, cliquez sur le serveur **de messagerie**.

b. Cliquez sur l'onglet **Bureau**, puis sur **Pare-feu**. Aucune règle de pare-feu n'est mise en œuvre.

Pour éviter l'envoi ou la réception de trafic autre que des e-mails depuis le serveur de messagerie, les administrateurs réseau peuvent créer des règles de pare-feu directement sur le serveur, ou, comme évoqué précédemment, utiliser des listes de contrôle d'accès (ACL) sur un terminal réseau tel qu'un routeur.

## Suggestion de barème de notation

| Section d'exercice | Emplacement de la question | Nombre maximum de points | Points obtenus |
|---|---|---|---|
| Partie 1 : Se connecter au serveur web | Étape 1 | 15 | |
| | Étape 2 | 15 | |
| Partie 2 : Bloquer les sessions HTTP non chiffrées | Étape 2 | 15 | |
| | Étape 3 | 15 | |
| | **Questions** | **60** | |
| | **Score relatif à Packet Tracer** | **40** | |
| | **Score total** | **100** | |