Exercice PT 5.6.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

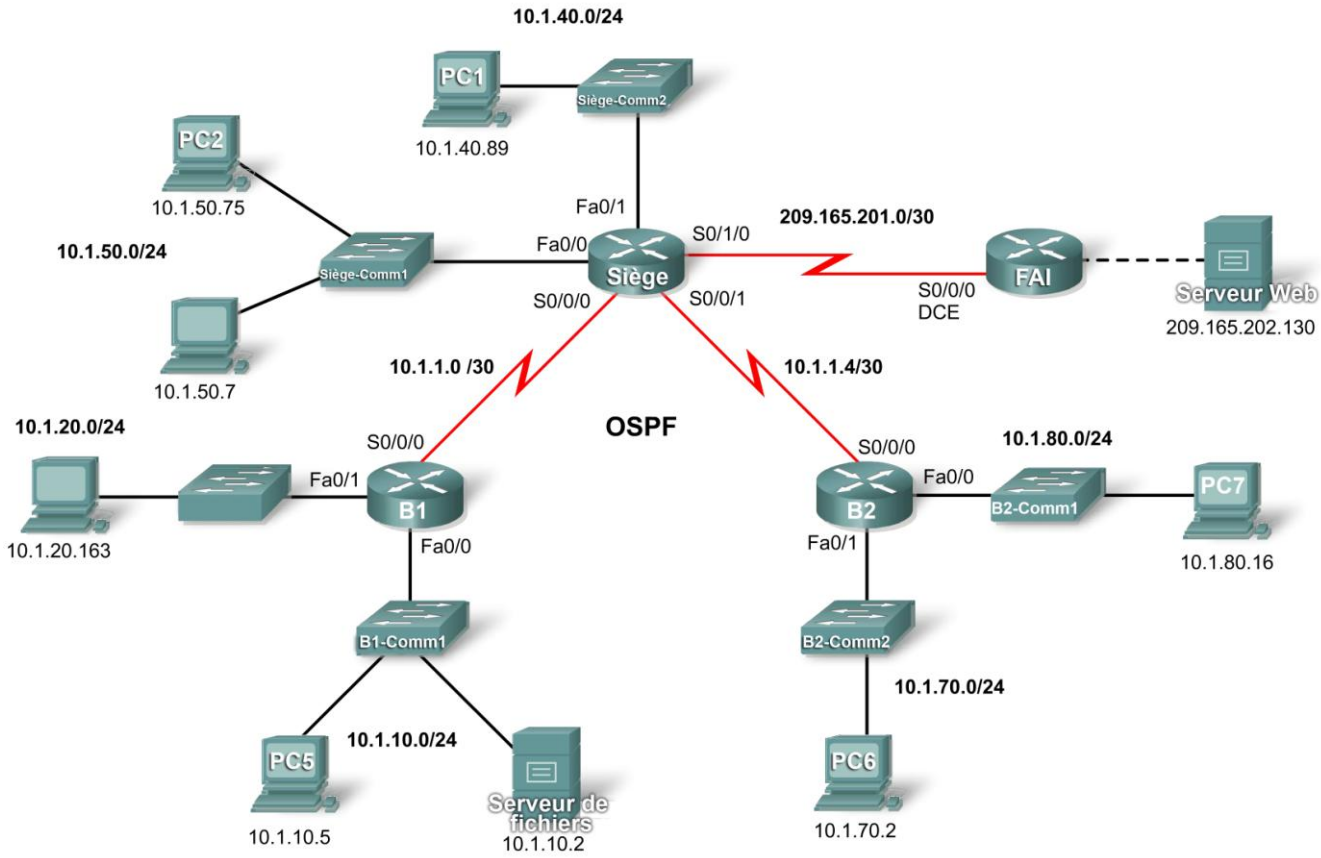

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
SIÈGE	S0/0/0	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	S0/0/0	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	S0/0/0	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
FAI	S0/0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Serveur Web	Carte réseau	209.165.202.130	255.255.255.252

Objectifs pédagogiques

- Configurer le protocole PPP avec l'authentification CHAP
- Configurer le routage par défaut
- Configurer le routage OSPF
- Mettre en œuvre et vérifier plusieurs stratégies de sécurité de listes de contrôle d'accès

Présentation

Au cours de cet exercice, vous allez faire preuve de votre capacité à configurer des listes de contrôle d'accès qui appliquent cinq stratégies de sécurité. Vous allez également configurer le protocole PPP et le routage OSPF. L'adressage IP des périphériques est déjà configuré. Le mot de passe d'exécution utilisateur est **cisco** et le mot de passe d'exécution privilégié est **class**.

Tâche 1 : configuration du protocole PPP avec l'authentification CHAP

Étape 1. Configuration de la liaison entre SIÈGE et B1 pour utiliser l'encapsulation PPP avec l'authentification CHAP

Le mot de passe pour l'authentification CHAP est **cisco123.**

Étape 2. Configuration de la liaison entre SIÈGE et B2 pour utiliser l'encapsulation PPP avec l'authentification CHAP

Le mot de passe pour l'authentification CHAP est **cisco123.**

Étape 3. Vérification du rétablissement de la connectivité entre les routeurs

SIÈGE doit être en mesure d'envoyer une requête ping à B1 et à B2. Quelques minutes peuvent être nécessaires pour que les interfaces se rétablissent. Pour accélérer le processus, vous pouvez alterner entre les modes Realtime (temps réel) et Simulation. Une autre solution permettant de contourner ce comportement de Packet Tracer consiste à utiliser les commandes **shutdown** et **no shutdown** sur les interfaces.

Remarque : il est possible que les interfaces se désactivent de façon aléatoire pendant l'exercice à cause d'un bogue de Packet Tracer. En principe, l'interface se rétablit seule après quelques secondes d'attente.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 29 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration du routage par défaut

Étape 1. Configuration du routage par défaut de SIÈGE vers FAI

Configurez une route par défaut sur SIÈGE en utilisant l'argument *exit interface* pour envoyer tout le trafic par défaut vers FAI.

Étape 2. Test de la connectivité au serveur Web

SIÈGE doit être en mesure d'envoyer une requête ping au serveur Web à l'adresse 209.165.202.130 tant que la requête ping provient de l'interface Serial0/1/0.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 32 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration du routage OSPF

Étape 1. Configuration d'OSPF sur SIÈGE

- Configurez OSPF à l'aide de l'ID de processus 1.
- Annoncez tous les sous-réseaux à l'exception du réseau 209.165.201.0.
- Transmettez les informations de route par défaut aux voisins OSPF.
- Désactivez les mises à jour d'OSPF vers FAI et vers les réseaux locaux de SIÈGE.

Étape 2. Configuration d'OSPF sur B1 et B2

- Configurez OSPF à l'aide de l'ID de processus 1.
- Sur chaque routeur, configurez les sous-réseaux adéquats.
- Désactivez les mises à jour d'OSPF vers les réseaux locaux.

Étape 3. Test de la connectivité dans l'ensemble du réseau

Le réseau doit maintenant avoir une connectivité totale de bout en bout. Chaque périphérique doit être en mesure d'envoyer une requête ping à tout autre périphérique, y compris au serveur Web à l'adresse 209.165.202.130.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 76 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : mise en œuvre de plusieurs stratégies de sécurité de listes de contrôle d'accès

Étape 1. Mise en œuvre de la stratégie de sécurité numéro 1

Empêchez le réseau 10.1.10.0 d'accéder au réseau 10.1.40.0. Tout autre accès à 10.1.40.0 est autorisé. Configurez la liste de contrôle d'accès sur SIÈGE en utilisant la liste de contrôle d'accès numéro 10.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 2. Vérification de la mise en œuvre de la stratégie de sécurité numéro 1

Une requête ping de PC5 à PC1 doit échouer.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 80 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 4. Mise en œuvre de la stratégie de sécurité numéro 2

L'hôte 10.1.10.5 n'est pas autorisé à accéder à l'hôte 10.1.50.7. Tous les autres hôtes sont autorisés à accéder à 10.1.50.7. Configurez la liste de contrôle d'accès sur B1 en utilisant la liste de contrôle d'accès numéro 115.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 5. Vérification de la mise en œuvre de la stratégie de sécurité numéro 2

Une requête ping de PC5 à PC3 doit échouer.

Étape 6. Vérification des résultats

Votre taux de réalisation doit être de 85 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 7. Mise en œuvre de la stratégie de sécurité numéro 3

Les hôtes 10.1.50.1 à 10.1.50.63 ne disposent pas d'un accès Web au serveur Intranet à l'adresse 10.1.80.16. Tout autre accès est autorisé. Configurez la liste de contrôle d'accès sur le routeur adéquat en utilisant la liste de contrôle d'accès numéro 101.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- Sur quel routeur configurer la liste de contrôle d'accès ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 8. Vérification de la mise en œuvre de la stratégie de sécurité numéro 3

Pour tester cette stratégie, cliquez sur PC3, puis sur l'onglet **Desktop,** puis sur **Web Browser**. Pour l'URL, saisissez l'adresse IP du serveur Intranet, 10.1.80.16, puis appuyez sur **Entrée**. Après quelques secondes, vous devez recevoir un message de dépassement de délai d'attente de la requête. PC2 et tout autre PC du réseau doivent être en mesure d'accéder au serveur Intranet.

Étape 9. Vérification des résultats

Votre taux de réalisation doit être de 90 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 10. Mise en œuvre de la stratégie de sécurité numéro 4

Utilisez le nom **NO_FTP** pour configurer une liste de contrôle d'accès nommée qui empêche le réseau 10.1.70.0/24 d'accéder aux services FTP (port 21) du serveur de fichiers à l'adresse 10.1.10.2. Tout autre accès doit être autorisé.

Remarque : les noms sont sensibles à la casse.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- Sur quel routeur configurer la liste de contrôle d'accès ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 11. Vérification des résultats

Packet Tracer ne prenant pas en charge le test de l'accès FTP, vous ne pourrez pas vérifier cette stratégie. Cependant, votre taux de réalisation doit être de 95 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 12. Mise en œuvre de la stratégie de sécurité numéro 5

FAI représentant la connectivité à Internet, configurez une liste de contrôle d'accès nommée appelée **FIREWALL** dans l'ordre suivant :

1. Autorisez uniquement les réponses ping entrantes en provenance du FAI et de toute source au-delà du FAI.
2. Autorisez uniquement les sessions TCP établies à partir du FAI et de toute source au-delà du FAI.
3. Bloquez explicitement tout autre accès entrant à partir du FAI et de toute source au-delà du FAI.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- Sur quel routeur configurer la liste de contrôle d'accès ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 13. Vérification de la mise en œuvre de la stratégie de sécurité numéro 5

Pour tester cette stratégie, tout PC doit être en mesure d'envoyer une requête ping à FAI ou au serveur Web. Cependant, ni FAI ni le serveur Web ne doivent pouvoir envoyer de requête ping à SIÈGE ou à tout autre périphérique au-delà de la liste de contrôle d'accès **FIREWALL.**

Étape 14. Vérification des résultats

Votre taux de réalisation doit être de 100%. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.