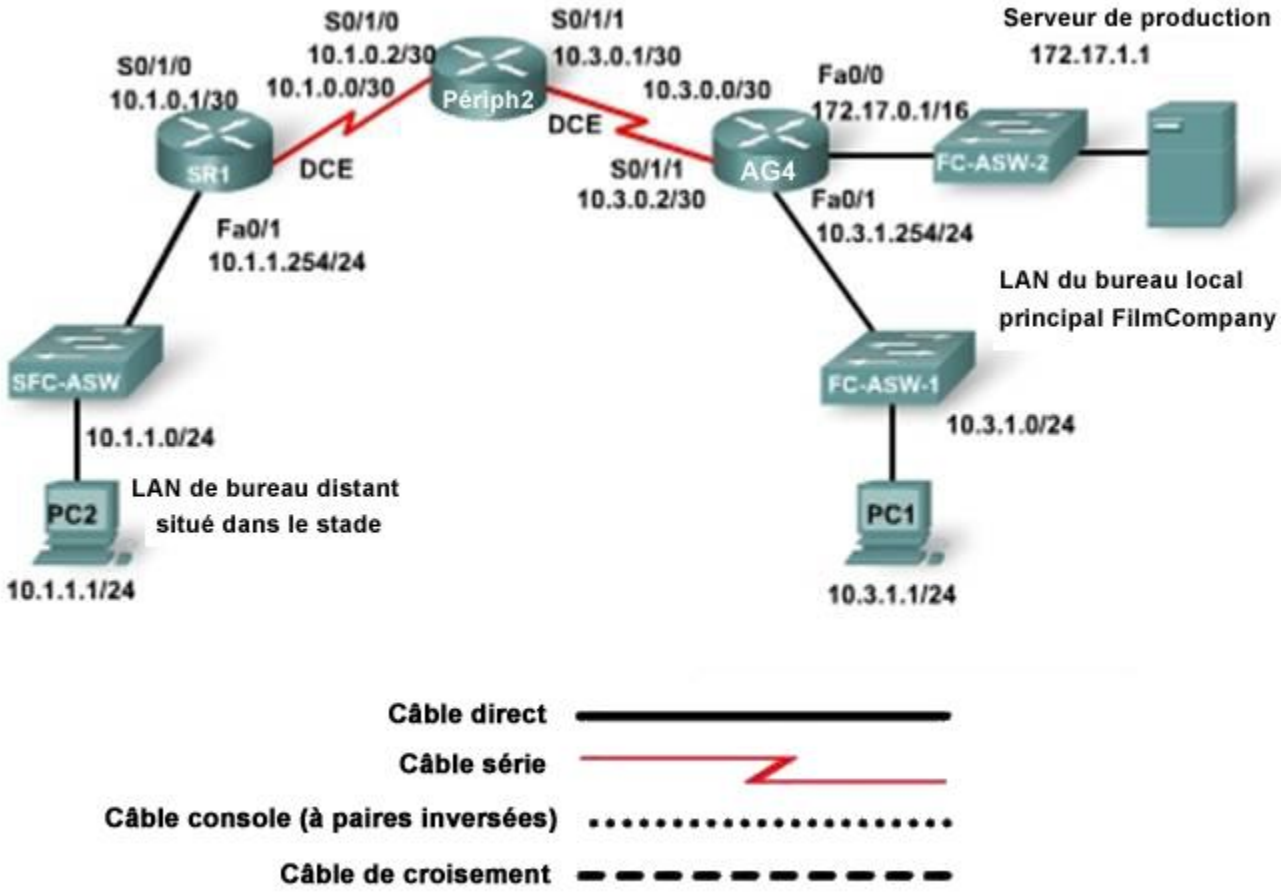
Travaux pratiques 5.5.3 Développement de listes de contrôle d'accès dans le cadre de la mise en œuvre d'un jeu de règles de pare-feu



Périphérique	Interface	Adresse IP
SFC-ASW	VLAN 1	10.1.1.253/24
SR1	Fa0/1 S0/1/0	10.1.1.254/24 10.1.0.1/30
Périph2	S0/1/0 S0/1/1	10.1.0.2/30 10.3.0.1/30
AG4	S0/1/1 Fa0/0 Fa0/1	10.3.0.2/30 172.17.0.1/16 10.3.1.254/24
FC-ASW-2	VLAN 1	172.17.1.25/16
FC-ASW-1	VLAN 1	10.3.1.253/24
PC1	—	10.1.1.1/24
PC2	—	10.3.1.1/24
Serveur de production	—	172.17.1.1/16

Objectifs

- Interpréter une stratégie de sécurité pour définir les règles de pare-feu
- Créer des instructions de liste de contrôle d'accès pour mettre en œuvre les règles de pare-feu
- Configurer et tester les listes de contrôle d'accès

Objectifs de l'examen CCNA 640-802

Ces travaux pratiques permettent d'acquérir des compétences liées aux objectifs d'examen CCNA suivants :

- Décrire l'objet et les types de liste de contrôle d'accès
- Configurer et appliquer des listes de contrôle d'accès en fonction des exigences de filtrage du réseau (ILC/SDM)
- Configurer et appliquer des listes de contrôle d'accès afin de limiter l'accès Telnet et SSH au routeur utilisant SDM/ILC
- Vérifier et surveiller les listes de contrôle d'accès dans un environnement réseau
- Résoudre les problèmes liés aux listes de contrôle d'accès

Résultats attendus et critères de réussite

Avant de démarrer ces travaux pratiques, prenez connaissance des tâches que vous devrez effectuer. Selon vous, quel sera le résultat de l' exécution de ces tâches ?

_____

_____

_____

Quels sont les risques si vous n'utilisez pas de liste de contrôle d'accès pour sécuriser le trafic réseau ?

_____

_____

_____

Quelles méthodes permettent de limiter le flux du trafic à l'intérieur et à l'extérieur des réseaux locaux ou des réseaux étendus ?

_____

_____

_____

Contexte / Préparation

FilmCompany fournit des services à des agences, telles que celle située au stade. La sécurité et les performances ne sont pas des préoccupations majeures pour ces bureaux. Ces préoccupations obligeront le concepteur de réseau à intégrer plusieurs listes de contrôle d'accès afin de sécuriser le réseau. Les listes de contrôle d'accès doivent être mises en œuvre comme un outil simple et efficace de contrôle du trafic.

Conformément à une stratégie de sécurité de FilmCompany, créez un jeu de règles de pare-feu et mettez en œuvre des listes de contrôle d'accès étendues nommées pour appliquer le jeu de règles.

La stratégie de sécurité de FilmCompany contient une section relative à l'accès depuis des sites distants. Voici le texte de la stratégie de sécurité :

Stratégie de sécurité

Les utilisateurs qui accèdent au réseau à distance, agences comprises, nécessitent de disposer de l'accès suivant aux ressources de réseau sur site :

1. Les utilisateurs distants doivent pouvoir accéder au Serveur de production afin de visualiser leurs plannings sur le Web et entrer de nouvelles commandes.
2. Les utilisateurs distants doivent pouvoir transférer des fichiers via FTP vers/depuis le Serveur de production.
3. Les utilisateurs distants peuvent utiliser le Serveur de production pour envoyer et récupérer des courriels à l'aide des protocoles IMAP et SMTP.
4. Les utilisateurs distants ne peuvent pas accéder aux autres services disponibles sur le Serveur de production.
5. Aucun trafic n'est autorisé entre les stations de travail individuelles du bureau principal et les stations de travail de l'utilisateur distant. Tout fichier à transférer entre les deux sites doit être stocké sur le Serveur de production, puis récupéré via FTP.
6. Aucun trafic n'est autorisé entre les stations de travail du site distant et les stations de travail du site principal.
7. Aucun trafic Telnet n'est autorisé entre les stations de travail du site distant et tout autre périphérique, excepté leur commutateur local.

Étape 1 : câblage et connexion du réseau conformément au schéma de topologie

REMARQUE : si les PC utilisés dans ces travaux pratiques sont également connectés au réseau local de votre établissement ou à Internet, assurez-vous d'enregistrer les connexions de câble et les paramètres TCP/IP afin de pouvoir les rétablir à la fin des travaux pratiques.

a. Connectez les périphériques et configurez-les conformément à la topologie et à la configuration fournies.

   Le routage doit être configuré dans les liaisons de réseau étendu série afin d'établir les communications de données.

   REMARQUE : votre formateur peut remplacer le Serveur de production par un serveur équivalent dans ces travaux pratiques.

b. Configurez un accès Telnet sur chaque routeur.

c. Exécutez une requête ping entre l'Hôte 1, l'Hôte 2 et le Serveur de production afin de confirmer la connectivité du réseau.

   Dépannez la connectivité, puis établissez-la si la requête ping ou la connexion Telnet échoue.

Étape 2 : configurations de routeur de base

a. Configurez les périphériques du réseau en fonction des instructions suivantes :

- Configurez les noms d'hôte sur chaque périphérique.
- Définissez le mot de passe d'exécution privilégié **class.**
- Définissez le mot de passe **cisco** dans les connexions console.
- Définissez le mot de passe **cisco** dans les connexions vty.
- Définissez des adresses IP sur tous les périphériques.
- Activez le protocole EIGRP sur tous les routeurs et configurez chacun d'eux pour annoncer tous les réseaux connectés.
- Vérifiez la connectivité IP complète à l'aide de la commande **`ping`.**

b. Confirmez la connectivité de la couche application en établissant des connexions Telnet dans tous les routeurs.

Étape 3 : création d'un jeu de règles de pare-feu et d'instructions de liste d'accès

À partir des informations de stratégie de sécurité définies pour l'accès distant à FilmCompany, créez les règles de pare-feu qui doivent être mises en œuvre pour garantir l'application de la stratégie. Une fois la règle de pare-feu définie, créez une instruction de liste d'accès qui mettra en œuvre la règle de pare-feu. Plusieurs instructions peuvent être nécessaires pour mettre en œuvre une règle.

Voici un exemple de règle de pare-feu :

Stratégie de sécurité 1 : les utilisateurs distants doivent pouvoir accéder au Serveur de production afin de visualiser leurs plannings sur le Web et entrer de nouvelles commandes.

Règle de pare-feu : permet aux utilisateurs du réseau 10.1.1.0/24 d'accéder au Serveur de production (172.17.1.1) sur le port 80.

Instruction(s) de liste d'accès : `permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 80`

Placement de liste d'accès : trafic entrant sur le routeur SR1 Fa0/1 (n'oubliez pas que les listes de contrôle d'accès étendues doivent être placées à proximité de la source du trafic).

Pour chaque stratégie de catégorie suivante :

a. Créez une règle de pare-feu.

b. Créez une instruction de liste d'accès.

c. Déterminez le placement de la liste d'accès pour implémenter la règle de pare-feu.

Stratégie de sécurité 2 : les utilisateurs distants doivent pouvoir transférer des fichiers via FTP vers/depuis le Serveur de production.

Règle de pare-feu :

_____

_____

Instruction(s) de liste d'accès :

_____

_____

Placement de liste d'accès :

_____

_____

Stratégie de sécurité 3 : les utilisateurs distants peuvent utiliser le Serveur de production pour envoyer et récupérer des courriels à l'aide des protocoles IMAP et SMTP.

Règle de pare-feu :

_____

_____

Instruction(s) de liste d'accès :

_____

_____

Placement de liste d'accès :

_____

_____

Stratégie de sécurité 4 : les utilisateurs distants ne peuvent pas accéder aux autres services disponibles sur le Serveur de production.

Règle de pare-feu :

_____

_____

Instruction(s) de liste d'accès :

_____

_____

Placement de liste d'accès :

_____

_____

Stratégie de sécurité 5 : aucun trafic n'est autorisé entre les stations de travail individuelles du bureau principal et les stations de travail de l'utilisateur distant. Tout fichier à transférer entre les deux sites doit être stocké sur le Serveur de production, puis récupéré via FTP.

Règle de pare-feu :

_____

_____

Instruction(s) de liste d'accès :

_____

_____

Placement de liste d'accès :

_____

_____

Stratégie de sécurité 6 : aucun trafic n'est autorisé entre les stations de travail du site distant et les stations de travail du site principal.

Règle de pare-feu :

_____

_____

Instruction(s) de liste d'accès :

_____

_____

Placement de liste d'accès :

_____

_____

Stratégie de sécurité 7 : aucun trafic Telnet n'est autorisé entre les stations de travail du site distant et tout autre périphérique, excepté leur commutateur local.

Règle de pare-feu :

_____

_____

Instruction(s) de liste d'accès :

_____

_____

Placement de liste d'accès :

_____

_____

Étape 4 : création de listes de contrôle d'accès étendues

a. Passez en revue les informations de placement de liste d'accès que vous avez créées pour mettre en œuvre chaque stratégie de sécurité FilmCompany. Répertoriez les différents placements de liste d'accès notés ci-dessus.

_____

_____

_____

Selon les informations de placement, combien de listes d'accès devez-vous créer ?

Sur le routeur SR1 _____

Sur le routeur Périph2 _____

Sur le routeur AG4 _____

b. Selon les instructions de liste d'accès développées dans la tâche 3, créez chaque liste d'accès nécessaire à la mise en œuvre de stratégies de sécurité. Lorsque vous créez des listes d'accès, n'oubliez pas les principes suivants :

- Une seule liste d'accès peut être appliquée par protocole et par direction sur chaque interface.
- Les instructions de liste d'accès sont traitées dans l'ordre.

- Une fois une liste d'accès créée et appliquée dans une interface, tout le trafic qui ne correspond à aucune instruction de liste d'accès est abandonné.

c. Créez les listes d'accès dans un fichier texte ou écrivez-les ici. Évaluez chaque instruction de liste d'accès pour vous assurer qu'il filtrera le trafic comme prévu.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Pourquoi l'ordre des instructions de liste d'accès est-il si important ?

_____

_____

_____

Étape 5 : configuration et test des listes d'accès

a. Configurez les listes d'accès sur les routeurs appropriés, puis appliquez-les aux interfaces appropriées. Nommez les listes d'accès avec des noms représentatifs, tels que « RemoteOffice » ou « FilterRemote ».

Noms des listes d'accès :

_____

_____

b. Testez les listes d'accès et leur placement en effectuant les tests suivants :

1) Dans l'Hôte 1, ouvrez une fenêtre de navigateur, puis tentez de visualiser la page Web située sur le Serveur de production à l'adresse http://172.17.1.1.

Avez-vous réussi ? _____

2) Dans l'Hôte 1, ouvrez une fenêtre de navigateur, puis tentez de vous connecter au Serveur de production en saisissant ftp://172.17.1.1.

Avez-vous réussi ? _____

3) Dans l'Hôte 1, tentez d'établir une connexion Telnet avec toute adresse présente sur les routeurs ou les commutateurs.

Avez-vous réussi ? _____

4) Dans l'Hôte 1, exécutez une requête ping vers l'Hôte 2.

Avez-vous réussi ? _____

5) Dans l'Hôte 2, exécutez une requête ping vers l'Hôte 1.

Avez-vous réussi ? _____

Vos listes de contrôle d'accès ont-elles fonctionné comme prévu ? _____

Si ce n'est pas le cas, corrigez les listes de contrôle d'accès et retestez leur placement dans le réseau.

Étape 6 : documentation des configuration de routeur

Copiez et enregistrez les résultats de configuration de tous les routeurs dans un document de traitement de texte afin de visualiser leurs configurations.

Étape 7 : remarques générales

Les stratégies de conception du réseau local de FilmCompany posent de nombreux défis au concepteur. Quels ont été les plus importants défis rencontrés lors de la création d'une liste de contrôle d'accès ?

_____

_____

_____

_____

Examinez les stratégies identifiées. Ces stratégies permettent-elles d'accomplir la tâche de la même manière ?

_____

_____

Une liste de contrôle d'accès fonctionne-t-elle mieux qu'une autre ?

_____

_____

La conception de liste de contrôle d'accès choisie supportera-t-elle la croissance future et l'ajout de davantage d'hôtes sur le segment de réseau local ?

_____

_____