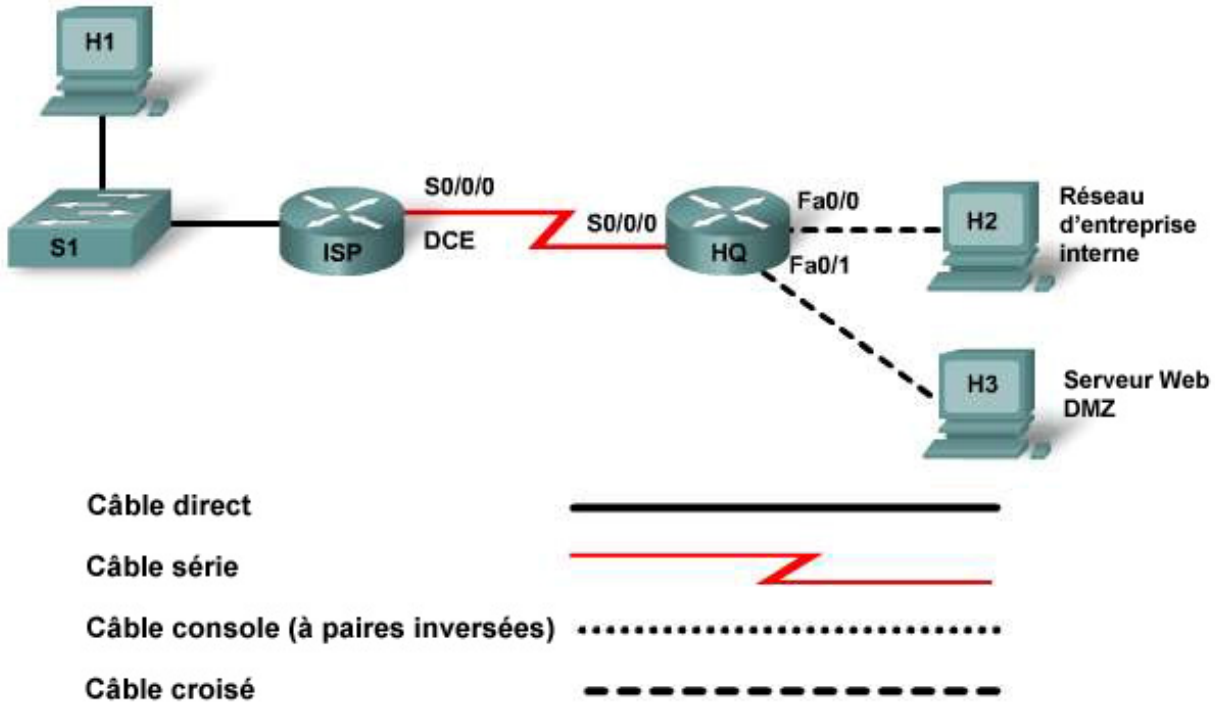
Travaux pratiques 9.5.2 : Dépannage de la configuration et du placement des listes de contrôle d'accès



Périphérique	Nom d'hôte	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut	Mot de passe actif	Mot de passe actif, vty et de console
Router 1	ISP	**Fa0/0**	172.19.2.1	255.255.255.0	N/D	class	cisco
		S0/0/0	172.16.1.1	255.255.255.252	N/D		
Router 2	HQ	**Fa0/0**	172.18.2.1	255.255.255.0	N/D	class	cisco
		Fa0/1	172.17.0.1	255.255.0.0	N/D		
		S0/0/0	172.16.1.2	255.255.255.252	N/D		
Host 1	H1	**Carte réseau**	172.19.2.2	255.255.255.0	172.19.2.1		
Host 2	H2	**Carte réseau**	172.18.2.2	255.255.255.0	172.18.2.1		
Web server (Discovery Server)	H3	**Carte réseau**	172.17.1.1	255.255.0.0	172.17.0.1		

Objectifs

- Charger les routeurs avec des préconfigurations
- Détecter les communications défectueuses
- Réunir des informations sur les listes de contrôle d'accès incorrectement configurées
- Analyser les informations pour déterminer pourquoi la communication n'est pas possible
- Proposer des solutions pour résoudre les erreurs sur le réseau
- Mettre en place des solutions pour résoudre les erreurs de réseau

Contexte / Préparation

Une petite entreprise de fabrication veut faire connaître ses produits sur Internet. Ses besoins immédiats consistent donc à promouvoir ses produits auprès des clients potentiels au moyen de présentations, de rapports et de témoignages sur les produits. Comme elle a besoin d'une infrastructure sécurisée qui répond à ses besoins internes et externes, vous avez mis en place une architecture sécurisée à deux niveaux composée d'une zone réseau interne à l'entreprise et d'une zone démilitarisée (DMZ). La zone réseau d'entreprise hébergera les serveurs privés et les clients internes. La zone DMZ accueillera un seul serveur externe fournissant des services Web. Étant donné que la société peut gérer uniquement le routeur de son siège social (HQ) et non celui de son fournisseur de services Internet (ISP), toutes les listes de contrôle d'accès doivent être appliquées au routeur du siège social.

- **La liste d'accès 101 est mise en place pour limiter le trafic sortant de la zone du réseau d'entreprise** qui héberge les serveurs privés et les clients internes. Aucun autre réseau ne doit être en mesure d'y accéder. Pour protéger le réseau, vous devez commencer par indiquer le type de trafic autorisé à en sortir. Cela peut paraître étrange, mais il faut savoir que la plupart des pirates sont des employés de l'entreprise.
- **La liste d'accès 102 est mise en place pour limiter le trafic entrant dans le réseau de l'entreprise.** Le trafic entrant dans le réseau d'entreprise provient d'Internet (ISP) ou de la zone DMZ. Seul le trafic provenant du réseau d'entreprise est autorisé à entrer dans ce réseau. Pour faciliter l'administration et le dépannage du réseau, vous devez également autoriser le trafic ICMP vers le réseau. Les hôtes internes pourront ainsi recevoir des messages ICMP. À ce stade, aucun autre type de trafic vers le réseau d'entreprise n'est autorisé.
- **La liste d'accès 111 est mise en place pour contrôler le trafic sortant du réseau DMZ.** Le réseau DMZ accueillera un seul serveur externe fournissant des services Web. Les autres services (courriel, FTP et DNS) seront mis en œuvre ultérieurement. Le trafic sortant du réseau est spécifié ici.
- **La liste d'accès 112 est mise en place pour contrôler le trafic entrant dans le réseau DMZ.** Le trafic entrant dans le réseau DMZ, qui doit être autorisé à entrer, provient d'Internet (ISP) ou du réseau d'entreprise pour des demandes de services Web. N'autorisez que les utilisateurs ICMP de l'entreprise à accéder au réseau DMZ. Aucun autre trafic n'est autorisé à entrer dans le réseau DMZ.
- **La liste d'accès 121 est mise en place pour empêcher les mystifications (spoofing).** Les réseaux font de plus en plus l'objet d'attaques par des utilisateurs externes. Les pirates essaient de pénétrer dans les réseaux et de les rendre incapables de répondre à des demandes légitimes (attaques de type déni de service - DoS). La liste d'accès doit empêcher les utilisateurs externes d'usurper des adresses internes en spécifiant trois types d'adresse IP que les pirates essaient de trouver. Il s'agit d'adresses privées internes valides telles que 172.18.2.0, d'adresses de bouclage telles que 127.0.0.0 et d'adresses de multidiffusion (ex. 224.x.x.x-239.x.x.x).

Installez un réseau similaire à celui du schéma de topologie. Tout routeur doté d'une interface telle que celle indiquée dans le schéma ci-dessus peut être utilisé. Exemple : les routeurs de la gamme 800, 1600, 1700, 1800, 2500, 2600, 2800 ou toute combinaison de ces routeurs sont utilisables.

Les informations présentées dans ces travaux pratiques s'appliquent au routeur 1841. Il est possible d'utiliser d'autres routeurs ; cependant la syntaxe des commandes peut varier. Les interfaces peuvent être différentes en fonction du modèle de routeur. Par exemple, sur certains routeurs, Serial 0 peut être Serial 0/0 ou Serial 0/0/0 et Ethernet 0 peut être FastEthernet 0/0. Le commutateur Cisco Catalyst 2960 est fourni préconfiguré : il ne nécessite que l'affectation d'informations de sécurité de base avant la connexion à un réseau.

Ressources requises :

- Un commutateur Cisco 2960 ou comparable ; vous pouvez également utiliser des câbles croisés entre les hôtes et les routeurs si le commutateur est absent.
- Un routeur doté d'une interface série et de deux interfaces Ethernet
- Un routeur doté d'une interface série et d'une interface Ethernet
- Deux PC sous Windows avec un programme d'émulation de terminal et configurés en hôtes
- Un PC sous Windows qui exécute le CD Discovery Live représentant le serveur Web
- Un câble console avec connecteurs RJ-45/DB-9 pour configurer les routeurs
- Deux câbles droits Ethernet
- Un câble série en 2 parties (ETTD/DCE)
- Deux câbles croisés
- Un CD Cisco Discovery Live (à demander au formateur)

REMARQUE : vérifiez que la mémoire des routeurs a été effacée et qu'aucune configuration de démarrage n'est présente. Les instructions d'effacement et de rechargement de la mémoire figurent à la fin du Manuel de travaux pratiques. Vous pouvez télécharger le Manuel de travaux pratiques depuis la section Tools du site Academy Connection.

REMARQUE : Routeurs SDM − Si la configuration initiale (startup-config) est effacée dans un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut lorsque le routeur est redémarré. Il est alors nécessaire de définir une configuration de base de routeur à l'aide des commandes IOS. La procédure indiquée dans ces travaux pratiques utilise des commandes IOS et ne nécessite pas l'utilisation de SDM. Si vous voulez utiliser SDM pour la configuration de base du routeur, reportez-vous aux instructions à la fin du Manuel de travaux pratiques que vous pouvez télécharger depuis la section Tools du site Academy Connection. Consultez votre formateur si besoin.

Étape 1 : connexion du matériel

a. Connectez l'interface Fa0/0 de Router 1 à l'interface Fa0/1 du commutateur à l'aide d'un câble droit.

b. Connectez un hôte au port Fa0/2 du commutateur à l'aide d'un câble droit.

c. Connectez les câbles série de Router 1 à Router 2 conformément au schéma de topologie.

d. Connectez les hôtes aux interfaces Fa0/0 et Fa0/1 de Router 2 à l'aide de câbles croisés conformément à la topologie ci-dessus.

Étape 2 : chargement de la préconfiguration dans ISP

a. Demandez à votre formateur les préconfigurations de ces travaux pratiques.

b. Connectez Host 1 au port console de Router 1 afin de charger les préconfigurations à l'aide d'un programme d'émulation de terminal.

c. Transférez la configuration de l'hôte Host 1 à Router 1 :

1) Dans le programme d'émulation de terminal de H1, sélectionnez **Transfert > Envoyer un fichier texte**.

2) Recherchez le fichier de préconfiguration et sélectionnez **Ouvrir** pour commencer le transfert de la préconfiguration dans le Routeur 1.

REMARQUE : vous pouvez également copier et coller la préconfiguration dans le routeur en utilisant le programme HyperTerminal. Sélectionnez **Édition**, puis **Coller vers l'hôte**. Avant d'utiliser la fonction **Coller**, vérifiez que vous êtes en mode de configuration.

3) Lorsque le transfert est terminé, enregistrez la configuration.

Étape 3 : chargement de la préconfiguration dans HQ

Copiez la préconfiguration dans HQ en procédant comme à l'étape 2.

Étape 4 : configuration des hôtes H1 et H2

a. Configurez les interfaces Ethernet de H1 et H2 avec les adresses IP et les passerelles par défaut provenant de la table d'adressage.

b. Testez la configuration du PC en envoyant une requête ping à la passerelle par défaut à partir de chaque PC. H1 doit pouvoir atteindre sa passerelle par défaut, mais pas H2.

Étape 5 : configuration l'hôte H3 qui est le serveur Web

a. Chargez le CD Discovery LIVE sur l'hôte H3. L'interface Ethernet du serveur est préconfigurée avec l'adresse IP et la passerelle par défaut figurant dans la table d'adressage. En cas d'utilisation d'un autre serveur Web, configurez l'adresse IP et le masque de sous-réseau correspondant aux paramètres de la table.

b. Testez la configuration du PC en envoyant une requête ping à la passerelle par défaut à partir du PC H3.

Étape 6 : dépannage du routeur HQ et de la liste d'accès 101

a. Commencez par dépanner le routeur HQ.

La liste d'accès 101 est mise en place pour protéger la zone interne du réseau d'entreprise qui héberge les serveurs privés et les clients internes. Aucun autre réseau ne doit être en mesure d'y accéder. Pour protéger le réseau, vous devez commencer par indiquer le type de trafic autorisé à en sortir.

b. Examinez le routeur HQ pour rechercher d'éventuelles erreurs de configuration. Commencez par afficher le résumé de la liste d'accès 101. Entrez la commande **`show access-list 101`**.

Qu'indiquent ces informations ?

_____

_____

_____

c. Vérifiez l'accessibilité en envoyant, depuis chaque système, une requête ping à tous les systèmes et à tous les routeurs. Si tous les hôtes ne reçoivent pas une requête ping, la liste d'accès présente un problème.

H2 peut-il envoyer une requête ping à sa passerelle par défaut (172.1.2.1) ? _____

H2 peut-il envoyer une requête ping au serveur Web (172.17.1.1) ? _____

H2 peut-il envoyer une requête ping à H1 (172.19.2.2) ? _____

Existe-t-il des problèmes avec la liste d'accès 101 ? _____

Dans l'affirmative, lesquels ?

_____

_____

d. Si vous constatez des erreurs, apportez les modifications nécessaires à la configuration de HQ. N'oubliez pas que vous devez supprimer et entrer à nouveau les listes d'accès si vous constatez une différence dans les commandes.

_____

_____

_____

_____

e. Exécutez la commande **`show ip interface fa0/0`**.

La liste d'accès est-elle appliquée dans le sens correct sur l'interface Fa0/0 ? _____

f. Maintenant que le réseau approprié est autorisé en entrée sur Fa 0/0, H2 doit pouvoir envoyer une requête ping à sa passerelle par défaut. Effectuez à nouveau les tests ping à partir de l'étape 6c. Si H2 ne parvient pas à envoyer de requête ping à d'autres emplacements, vous devez effectuer des opérations de dépannage supplémentaires sur les listes de contrôle d'accès.

Étape 7 : dépannage du routeur HQ et de la liste d'accès 102

a. Continuez à dépanner le routeur HQ.

La liste d'accès 102 est mise en place pour limiter le trafic entrant dans le réseau de l'entreprise (sortant sur Fa 0/0). Le trafic entrant dans le réseau d'entreprise provient d'Internet (ISP) ou de la zone DMZ. Seul le trafic provenant du réseau d'entreprise (trafic établi) est autorisé à entrer dans ce réseau. Pour faciliter l'administration et le dépannage du réseau, vous devez également autoriser les échos ICMP vers le réseau. Cela permet aux hôtes internes de recevoir des réponses provenant d'hôtes externes, mais ceux-ci ne peuvent pas envoyer de requête ping aux hôtes internes. À ce stade, aucun autre type de trafic vers le réseau d'entreprise n'est autorisé.

b. Examinez le routeur HQ pour rechercher d'éventuelles erreurs de configuration. Commencez par afficher le résumé de la liste d'accès 102. Entrez la commande **`show access-list 102`**.

Qu'indiquent ces informations ?

_____

_____

_____

_____

c. Vérifiez l'accessibilité en envoyant, depuis chaque système, une requête ping à tous les systèmes et à tous les routeurs. Si la liste d'accès fonctionne correctement, le trafic en provenance de H2 doit être autorisé. Les réponses d'écho ICMP doivent également être autorisées.

H2 peut-il envoyer une requête ping au serveur Web (172.17.1.1) ? _____

H2 peut-il envoyer une requête ping à H1 (172.19.2.2) ? _____

H1 peut-il envoyer une requête ping au serveur Web (172.17.1.1) ? _____

H1 peut-il envoyer une requête ping à H2 (172.18.2.2) ? _____

H3 peut-il envoyer une requête ping à H2 (172.18.2.2) ? _____

Existe-t-il des problèmes avec la liste d'accès 102 ? _____

Dans l'affirmative, lesquels ?

_____

_____

d. Si vous constatez des erreurs, apportez les modifications nécessaires à la configuration de HQ. N'oubliez pas de supprimer complètement la liste d'accès avant de la corriger. Les commandes doivent figurer en ordre séquentiel logique.

_____

_____

_____

_____

_____

_____

_____

_____

e. Ouvrez un navigateur Web (ex. Windows Explorer, Netscape Navigator ou Firefox) sur chaque hôte et entrez l'adresse du serveur Web dans la zone d'adresse. Vérifiez que H2 a accès au serveur Web.

f. Exécutez la commande **`show ip interface fa0/0`**.

La liste d'accès est-elle appliquée dans le sens correct sur l'interface ? _____

g. À ce stade, les listes de contrôle d'accès appliquées à l'interface FastEthernet 0/0 sur HQ doivent autoriser tout le trafic nécessaire depuis et vers le réseau d'entreprise. Comme cela n'est pas le cas, nous devons effectuer des opérations de dépannage supplémentaires.

Étape 8 : dépannage du routeur HQ et de la liste d'accès 111

a. Continuez à dépanner le routeur HQ.

La liste d'accès 111 est mise en place pour protéger le réseau DMZ. Le réseau DMZ accueillera un seul serveur externe fournissant des services Web. Les autres services (courriel, FTP et DNS) seront mis en œuvre ultérieurement. Le routeur HQ autorise l'entrée sur le réseau DMZ des services Web destinés au serveur Web. Seuls les utilisateurs de l'entreprise recevront l'autorisation d'accès ICMP dans le réseau DMZ. Aucun autre trafic n'est autorisé à entrer dans le réseau DMZ.

b. Examinez le routeur HQ pour rechercher d'éventuelles erreurs de configuration. Commencez par afficher le résumé de la liste d'accès 111. Entrez la commande **`show access-list 111`**.

Qu'indiquent ces informations ?

_____

_____

_____

_____

c. Vérifiez l'accessibilité en envoyant, depuis chaque système, une requête ping à tous les systèmes et à tous les routeurs. H1 ne doit pas pouvoir envoyer de requête ping à H2 si la liste d'accès est correcte.

H2 peut-il envoyer une requête ping au serveur Web ? _____

H1 peut-il envoyer une requête ping au serveur Web ? _____

H3 peut-il envoyer une requête ping à H2 (172.18.2.2) ? _____

Existe-t-il des problèmes avec la liste d'accès 111 ? _____

Dans l'affirmative, lesquels ?

_____

_____

_____

_____

d. Si vous constatez des erreurs, apportez les modifications nécessaires à la configuration de HQ.

_____

_____

_____

_____

e. Exécutez la commande **`show ip interface fastethernet0/1`**.

La liste d'accès est-elle appliquée dans le sens correct sur l'interface ? _____

f. Utilisez la commande **ping** pour tester la connectivité. Les tests ping doivent révéler que H3 peut envoyer une requête ping à sa passerelle par défaut et à la passerelle par défaut de H2. H3 peut aussi envoyer une requête ping à H1. H3 ne peut toujours pas envoyer de requête ping à H2, mais ce comportement est conforme à la liste de contrôle d'accès 102. Si les tests ping ne produisent pas les résultats attendus, passez au dépannage de la liste d'accès suivante.

Étape 9 : dépannage du routeur HQ et de la liste d'accès 112

a. Continuez à dépanner le routeur HQ.

La liste d'accès 112 est mise en place pour protéger le réseau DMZ. Le trafic entrant dans le réseau DMZ, qui doit être autorisé à entrer, provient d'Internet (ISP) ou du réseau d'entreprise pour des demandes de services Web. N'autorisez que les utilisateurs ICMP de l'entreprise à accéder au réseau DMZ. Aucun autre trafic n'est autorisé à entrer dans le réseau DMZ.

b. Examinez le routeur HQ pour rechercher d'éventuelles erreurs de configuration. Commencez par afficher le résumé de la liste d'accès 112. Entrez la commande **`show access-list 112`**.

Qu'indiquent ces informations ?

_____

_____

_____

_____

c. Vérifiez l'accessibilité en envoyant, depuis chaque système, une requête ping à tous les systèmes et à tous les routeurs. Si la liste d'accès est correcte, H1 ne doit pas pouvoir envoyer de requête ping au serveur Web ou à H2.

H2 peut-il envoyer une requête ping au serveur Web ? _____

H1 peut-il envoyer une requête ping au serveur Web ? _____

H1 peut-il ouvrir une page Web sur H3 ? _____

H2 peut-il ouvrir une page Web sur H3 ? _____

Existe-t-il des problèmes avec la liste d'accès 112 ? _____

Dans l'affirmative, lesquels ?

_____

_____

d. Si vous constatez des erreurs, apportez les modifications nécessaires à la configuration de HQ.

_____

_____

_____

_____

e. Ouvrez un navigateur Web (ex. Windows Explorer, Netscape Navigator ou Firefox) et entrez l'adresse du serveur Web dans la zone d'adresse. Vérifiez que H1 et H2 ont accès au serveur Web.

H1 peut-il afficher la page Web sur le serveur Web ? _____

H2 peut-il afficher la page Web sur le serveur Web ? _____

H1 peut-il envoyer une requête ping à tous les emplacements ? _____

H2 peut-il envoyer une requête ping à tous les emplacements ? _____

f. Exécutez la commande **`show ip interface fastethernet0/1`**.

La liste d'accès est-elle appliquée dans le sens correct sur l'interface ? _____

g. Si les services du navigateur Web ne fonctionnent pas comme ils le devraient, effectuez le dépannage nécessaire.

Étape 10 : dépannage du routeur HQ et de la liste d'accès 121

a. Continuez à dépanner le routeur HQ.

La liste d'accès 121 est mise en place pour empêcher les mystifications (spoofing). Les réseaux font de plus en plus l'objet d'attaques par des utilisateurs externes. Les pirates essaient de pénétrer dans les réseaux et de les rendre incapables de répondre à des demandes légitimes (attaques de type déni de service - DoS). La liste d'accès doit empêcher les utilisateurs externes d'usurper des adresses internes en spécifiant trois types d'adresse IP que les pirates essaient de trouver : il s'agit d'adresses privées internes valides telles que 172.19.2.0, d'adresses de bouclage telles que 127.0.0.0 et d'adresses de multidiffusion (ex. 224.x.x.x-239.x.x.x).

b. Examinez le routeur HQ pour rechercher d'éventuelles erreurs de configuration. Commencez par afficher le résumé de la liste d'accès 121. Entrez la commande **`show access-list 121`**.

Qu'indiquent ces informations ?

_____

_____

_____

_____

c. Vérifiez l'accessibilité en envoyant, depuis chaque système, une requête ping à tous les systèmes et à tous les routeurs. Si la liste d'accès est correcte, seul H2 doit pouvoir envoyer des requêtes ping au serveur Web.

H2 peut-il envoyer une requête ping au serveur Web ? _____

H2 peut-il envoyer une requête ping à H1 ? _____

H1 peut-il envoyer une requête ping au serveur Web ? _____

H1 peut-il envoyer une requête ping à H2 ? _____

Existe-t-il des problèmes avec la liste d'accès 121 ? _____

Dans l'affirmative, lesquels ?

_____

_____

_____

_____

d. Exécutez la commande **`show ip interface serial0/0/0`**.

La liste d'accès est-elle appliquée dans le sens correct sur l'interface ? _____

e. Si vous constatez des erreurs, apportez les modifications nécessaires à la configuration de HQ.

_____

_____

_____

f. Ouvrez un navigateur Web (ex. Windows Explorer, Netscape Navigator ou Firefox) sur chaque hôte et entrez l'adresse du serveur Web dans la zone d'adresse. Vérifiez que H1 et H2 ont toujours accès au serveur Web.

H1 peut-il afficher la page Web sur le serveur Web ? _____

H2 peut-il afficher la page Web sur le serveur Web ? _____

Étape 11 : remarques générales

Les préconfigurations fournies pour ces travaux pratiques comportaient plusieurs erreurs de configuration. Utilisez l'espace ci-dessous pour décrire brièvement les erreurs que vous avez identifiées.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____