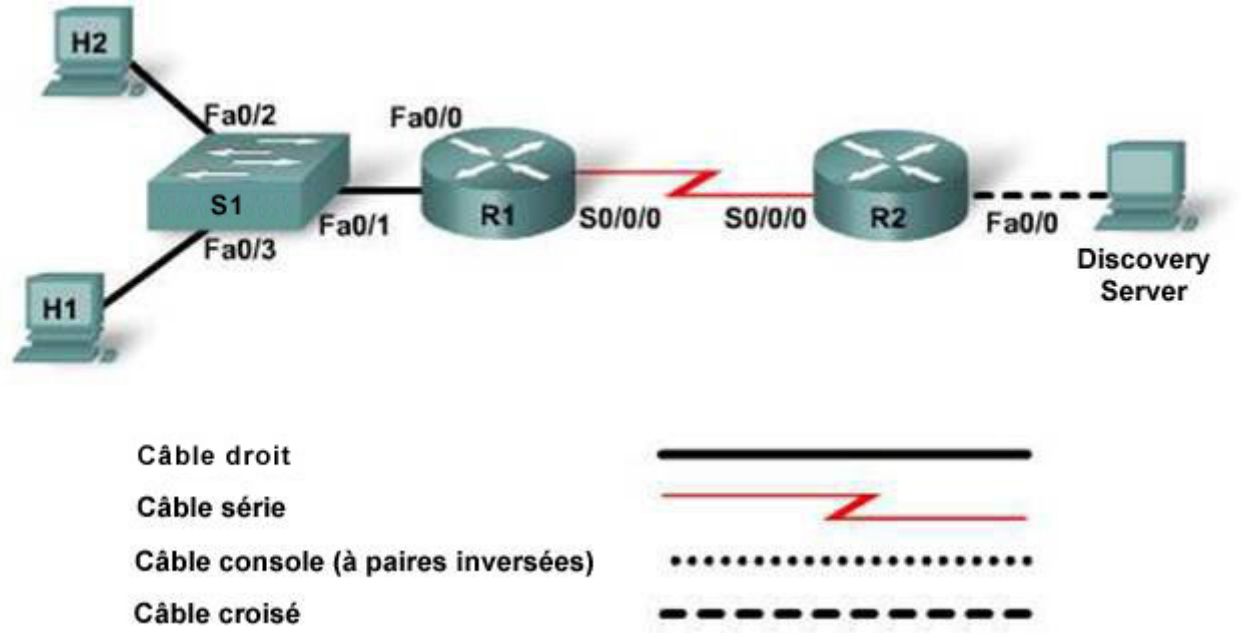
Travaux pratiques 8.5.2 : Configuration des listes de contrôle d'accès et enregistrement de l'activité dans un serveur Syslog



Périphérique	Nom d'hôte	Adresse IP Fast Ethernet 0/0	Adresse IP Serial 0/0/0	Type d'interface Serial 0/0/0	Instructions réseau	Mot de passe secret actif	Mot de passe actif, vty et de console
Routeur 1	R1	192.168.1.1/24	192.168.15.1/30	DCE	192.168.1.0 192.168.15.0	class	Cisco
Routeur 2	R2	172.17.0.1/16	192.168.15.2/30	ETTD	192.168.15.0 172.17.0.0	class	Cisco
Commutateur 1	S1					class	Cisco
Hôte 1	H1	192.168.1.5/24 Passerelle par défaut : 192.168.1.1					
Hôte 2	H2	192.168.1.6/24 Passerelle par défaut : 192.168.1.1					
Discovery Server	Server	172.17.1.1 Passerelle par défaut : 172.17.0.1					

Objectifs

- Configurer et vérifier des listes de contrôle d'accès pour contrôler le trafic
- Vérifier les listes de contrôle d'accès en utilisant un serveur syslog

Contexte / Préparation

Installez un réseau similaire à celui du schéma. Tout routeur doté d'une interface 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.

La syntaxe des commandes indiquée dans les travaux pratiques peut varier. Par exemple, les interfaces peuvent être différentes en fonction du modèle de routeur. 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 :

- Deux commutateurs Cisco 2960 ou tout autre commutateur comparable
- Deux routeurs Cisco 1841 ou autres routeurs comparables, chacun doté d'une connexion série et d'une interface Ethernet
- Deux PC Windows équipés d'un programme d'émulation de terminal et configurés comme hôtes
- Un CD Discovery Live pour le serveur
- Un PC utilisable en tant que Discovery Server
- Au moins un câble console à connecteur RJ-45/DB-9 pour configurer les routeurs et le commutateur
- Trois câbles droits Ethernet
- Un câble croisé Ethernet
- Un câble série ETTD/DCE
- Le démon Kiwi Syslog (à télécharger à l'adresse www.kiwisyslog.com ou à demander à votre formateur)

REMARQUE : vérifiez que la mémoire des routeurs et du commutateur a été effacée et qu'aucune configuration de démarrage n'est présente. Les instructions d'effacement de la mémoire figurent à la fin de ces travaux pratiques.

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 de ces travaux pratiques ou consultez votre formateur si besoin.

REMARQUE : ces travaux pratiques utilisent le CD Discovery Server Live. Pour des instructions détaillées sur l'installation et la configuration du CD Discovery Server Live, consultez le manuel de travaux pratiques que vous pouvez télécharger depuis la section Tools du site Academy Connection.

Étape 1 : connexion du matériel

a. Connectez l'interface Serial 0/0/0 du routeur R1 à l'interface Serial 0/0/0 du routeur R2 à l'aide d'un câble série.

b. Connectez l'interface Fa0/0 du routeur R1 au port Fa0/1 du commutateur S 1 à l'aide d'un câble droit.

c. Connectez l'hôte H1 au port Fa0/3 du commutateur S1 à l'aide d'un câble droit.

d. Connectez l'hôte H2 au port Fa0/2 du commutateur S1 à l'aide d'un câble droit.

e. Connectez le serveur Discovery Server à l'aide d'un câble croisé à l'interface Fa0/0 du routeur R2.

Étape 2 : configuration de base du routeur R1

Étape 3 : configuration de base du routeur R2

Étape 4 : configuration de base du commutateur S1

Étape 5 : configuration des hôtes avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut corrects

a. Configurez chaque hôte avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut corrects.

1) L'hôte H1 doit être configuré avec les paramètres suivants : adresse IP/masque de sous-réseau 192.168.1.5 /24 et passerelle par défaut 192.168.1.1.

2) L'hôte H2 doit être configuré avec les paramètres suivants : adresse IP/masque de sous-réseau 192.168.1.6 /24 et passerelle par défaut 192.168.1.1.

3) Le serveur doit être configuré avec les paramètres suivants : adresse IP 172.17.1.1 et passerelle par défaut 172.17.0.1.

b. Chaque hôte doit pouvoir envoyer une requête ping aux autres hôtes. Si cette requête échoue, procédez au dépannage requis. Vérifiez soigneusement qu'une adresse IP spécifique et une passerelle par défaut ont été attribuées à la station de travail.

Étape 6 : configuration et application des listes de contrôle d'accès

Les listes de contrôle d'accès sont configurées pour contrôler les services auxquels les hôtes H1 et H2 peuvent accéder sur le serveur. La liste de contrôle d'accès créée permet l'accès Web (HTTP) et FTP de l'hôte H1 au serveur mais le refuse à l'hôte H2. Celui-ci sera autorisé à accéder au serveur par une connexion Telnet, mais ce service sera interdit à l'hôte H1. Ces listes de contrôle d'accès seront configurées et vérifiées par des commandes **show** et la journalisation. La journalisation sera activée sur les instructions des listes de contrôle d'accès.

a. Créez une liste de contrôle d'accès conforme aux conditions ci-dessus. Cette liste de contrôle d'accès s'applique à R1.

```
R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www log
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp log
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet log
```

```
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any
```

b. Appliquez la liste de contrôle d'accès à l'interface FastEthernet 0/0 de R1 dans le sens entrant.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 110 in
```

c. Sur l'hôte H1, ouvrez un navigateur Web et essayez de vous connecter aux services Web et FTP du serveur. Dans la zone d'adresse du navigateur Web, entrez **http://172.17.1.1**.

La connexion Web de l'hôte H1 a-t-elle abouti ? _____

d. Dans la zone d'adresse du navigateur Web, entrez **ftp://172.17.1.1**.

La connexion FTP de l'hôte H1 a-t-elle abouti ? _____

e. Essayez de vous connecter aux services Web et FTP du serveur à partir de l'hôte H2.

Pouvez-vous vous connecter à partir de l'hôte H2 ? _____

f. Essayez d'établir une connexion Telnet au serveur à partir des hôtes H1 et H2.

La connexion Telnet à partir de l'hôte H1 a-t-elle abouti ? _____

La connexion Telnet à partir de l'hôte H2 a-t-elle abouti ? _____

Lorsque vous essayez d'établir ces connexions, des messages sur la console R1 indiquent les lignes `access-list` correspondant aux divers types de paquets transmis.

Étape 7 : configuration du service syslog sur l'hôte H2

L'option de journalisation dans une ligne `access-list` fournit des informations utiles ; elle présente cependant des inconvénients :

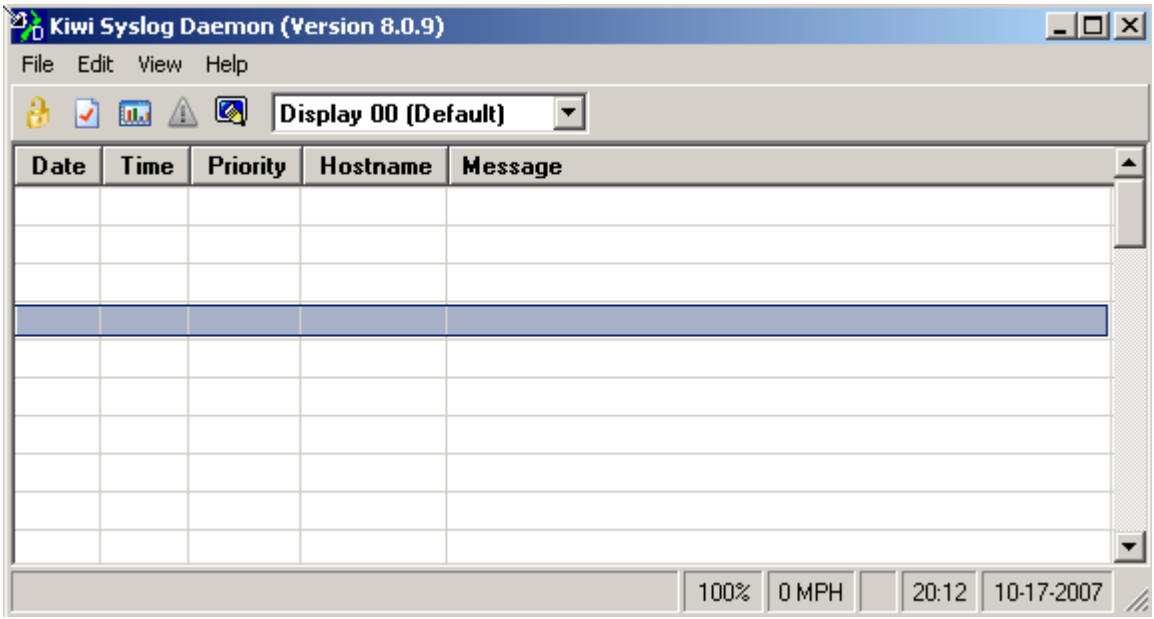
- Elle peut consommer des ressources importantes sur le routeur.
- Elle exige également qu'une connexion console avec le routeur soit active en permanence, faute de quoi les messages ne sont pas disponibles.

Une solution qui remédie à ces deux inconvénients est d'enregistrer les messages sur un serveur syslog. Cela réduit la charge sur le routeur et offre une destination pour les messages. De plus, des outils de gestion permettent d'analyser la sortie syslog pour faciliter la détection des problèmes.

Installez le démon Kiwi Syslog sur l'hôte H2. Le cas échéant, demandez de l'aide à votre formateur.

REMARQUE : de nombreux serveurs syslog sont disponibles sur le marché ou en version libre « open source ». Dans ces travaux pratiques, nous utilisons le serveur syslog Kiwi que vous pouvez télécharger à l'adresse www.kiwisyslog.com.

Lorsque le serveur syslog est en cours d'exécution sur le serveur, l'écran ressemble à celui-ci :



Le service syslog doit être configuré sur le routeur. Cela nécessite de configurer correctement la date et l'heure et d'activer le service d'horodatage sur le routeur, ainsi que de configurer le routeur pour l'envoi de messages de console au serveur syslog.

Étape 8 : configuration du routeur de façon à utiliser correctement le service syslog

L'affichage de la date et de l'heure correctes dans les messages syslog est essentiel lorsque vous utilisez syslog pour surveiller un réseau. Si vous ne connaissez pas la date et l'heure correctes d'un message, il est parfois impossible de déterminer l'événement réseau qui a produit le message.

a. Configurez la date et l'heure sur le routeur. Remplacez les heures, les minutes, les secondes, le mois, le jour et l'année par les valeurs correctes.

```
R1#clock set 15:22:00 may 17 2007
```

b. Configurez le fuseau horaire sur le routeur. Remplacez le nom de la zone et le décalage horaire par les valeurs correspondant à votre zone géographique.

```
R1(config)#clock timezone cdt -5
```

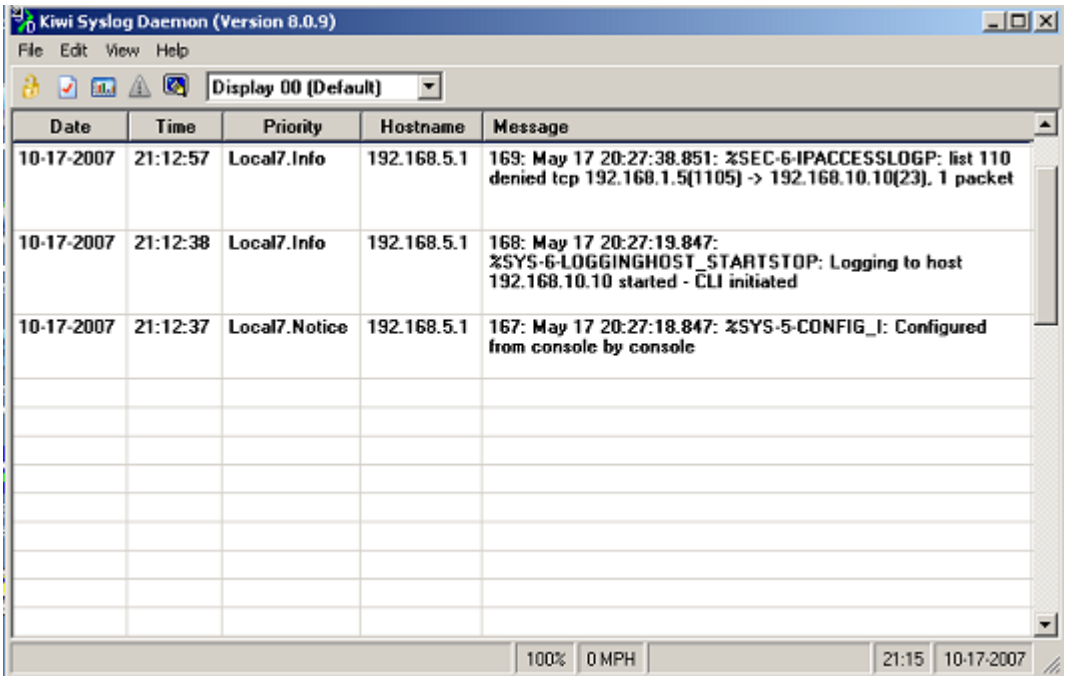
c. Activez le service d'horodatage sur le routeur.

```
R1(config)#service timestamps
```

d. Configurez le service syslog sur le routeur pour envoyer des messages syslog au serveur syslog.

```
R1(config)#logging 192.168.1.6
```

e. Essayez d'établir une connexion Telnet à partir de l'hôte H1 au serveur. Affichez ensuite l'écran syslog sur le serveur. Il doit ressembler à l'exemple ci-dessous :



f. Étant donné que la journalisation est activée à tous les niveaux, tous les messages de console sont affichés dans la sortie syslog, y compris les messages de configuration. Pour contrôler l'affichage des messages, configurez le niveau de journalisation pour produire un message.

REMARQUE : la date et l'heure s'affichent à la fois dans le message système et comme une fonction du serveur syslog Kiwi.

g. Dans la configuration actuelle, les messages syslog s'affichent dans le serveur syslog et sur la console. Lorsque le serveur syslog les affiche, il est possible de désactiver la journalisation sur le routeur R1.

```
R1(config)#no logging console
```

h. Essayez diverses connexions Telnet, Web et FTP au serveur à partir des deux hôtes et observez les résultats sur le serveur syslog. Outre l'affichage des messages lors des tentatives de connexion, observez les autres messages en provenance des hôtes H1 et H2 (p.ex. des messages de diffusion NetBIOS - port UDP 138).

Étape 9 : remarques générales

a. Indiquez les avantages de l'utilisation d'un serveur syslog à la place de la journalisation sur une console.

_____

_____

Quel facteur détermine le nombre maximal de messages enregistrés sur le serveur syslog ?

_____