



Exemple de configuration de PIX/ASA 7.x et versions ultérieures avec Syslog

Contenu

- Introduction
- Conditions préalables
- Conditions requises
- Composants utilisés
- Conventions
- Configuration Syslog de base**
- Configuration Syslog de base avec ASDM
- Envoi de messages Syslog par un VPN à un serveur Syslog
- Configuration Syslog avancée**
- Utilisation de la liste de messages
- Utilisation de la catégorie de message
- Conservation des occurrences d'ACE d'ACL
- Capture des messages Syslog du trafic VPN**
- Vérifiez
- Dépannez
- %ASA-3-201008 : Disallowing new connections
- Solution
- Informations connexes**

Introduction

Cet exemple de configuration explique comment configurer le dispositif de sécurité PIX/ASA 7.x avec Syslog.

PIX 7.0 a introduit des techniques de filtrage très granulaires pour n'autoriser la présentation que de certains messages Syslog spécifiés. La section Configuration Syslog de base de ce document explique une configuration Syslog traditionnelle. La section Configuration Syslog avancée de ce document montre les nouvelles fonctionnalités Syslog de la version 7.0.

Consultez le document Guide des messages du journal système de l'appliance de sécurité Cisco, version 7.x pour obtenir le guide complet de messages du journal système.

Consultez le document Configuration de PIX Syslog pour obtenir plus d'informations sur la façon de configurer Syslog dans le logiciel Cisco Secure PIX version 4.0.x.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- PIX 515E avec le logiciel PIX, version 7.0
- Cisco Adaptive Security Device Manager (ASDM) version 5.01

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Remarque: Référez-vous à ASA 8,2 : Configurez le Syslog utilisant le pour en savoir plus ASDM pour les détails semblables de configuration utilisant la version 6.2 et ultérieures ASDM.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration Syslog de base

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Utilisez ces commandes pour activer la journalisation, afficher les journaux et afficher les paramètres de configuration.

- **logging enable** : active la transmission des messages Syslog à tous les emplacements de sortie.
- **no logging enable** - désactive la journalisation à tous les emplacements de sortie.
- **show logging** : liste le contenu de la mémoire tampon Syslog et la configuration de la journalisation actuelle.

PIX peut envoyer des messages Syslog vers diverses destinations. Utilisez les commandes de ces sections afin de préciser l'emplacement auquel les messages doivent être envoyés :

Tampon interne

```
logging buffered severity_level
```

Aucun matériel ou logiciel externe n'est requis quand vous stockez les messages Syslog dans le tampon interne PIX. Utilisez **show logging** pour afficher les messages Syslog enregistrés.

Serveur de message Syslog

```
logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]

logging trap severity_level

logging facility number
```

Un serveur qui exécute une application Syslog est requis afin d'envoyer des messages Syslog à un hôte externe. PIX envoie les messages Syslog sur le port UDP 514 par défaut.

Adresse email

```
logging mail severity_level

logging recipient-address email_address

logging from-address email_address

smtp-server ip_address
```

Un serveur SMTP est requis quand vous envoyez les messages Syslog dans les messages électroniques. Une configuration adéquate sur le serveur SMTP est nécessaire afin de garantir que vous pouvez relayer avec succès des messages électroniques de PIX vers le client de messagerie électronique spécifié.

Console

```
logging console severity_level
```

La journalisation de la console permet aux messages Syslog de s'afficher sur la console PIX (TTY) à mesure qu'ils se produisent. Utilisez cette commande quand vous déboguez des problèmes ou en cas de charge minimale sur le réseau. N'utilisez pas cette commande quand le réseau est occupé, car cela peut réduire les performances.

Session Telnet/SSH

```
logging monitor severity_level

terminal monitor
```

La journalisation du moniteur permet aux messages Syslog de s'afficher à mesure qu'ils se produisent quand vous accédez à la console PIX avec Telnet ou SSH.

ASDM

```
logging asdm severity_level
```

ASDM a également une mémoire tampon qui peut être utilisée pour enregistrer les messages Syslog. Utilisez la commande **show logging asdm** afin d'afficher le contenu de la mémoire tampon Syslog d'ASDM.

Station de gestion SNMP

```
logging history severity_level

snmp-server host [if_name] ip_addr

snmp-server location text

snmp-server contact text

snmp-server community key

snmp-server enable traps
```

Les utilisateurs ont besoin d'un environnement SNMP (Simple Network Management Protocol) fonctionnel existant afin d'envoyer des messages Syslog en utilisant le protocole SNMP.

Consultez le document [Commandes](#) pour définir et gérer les destinations de sortie pour obtenir une référence complète sur les commandes que vous pouvez utiliser pour définir et gérer les destinations de sortie

Consultez le document [Messages listés par niveau de gravité](#) pour obtenir les messages listés par niveau de gravité.

Exemple 1

Cette sortie montre un exemple de configuration pour la journalisation dans la console avec le niveau de gravité de débogage.

```
logging enable

logging buffered debugging
```

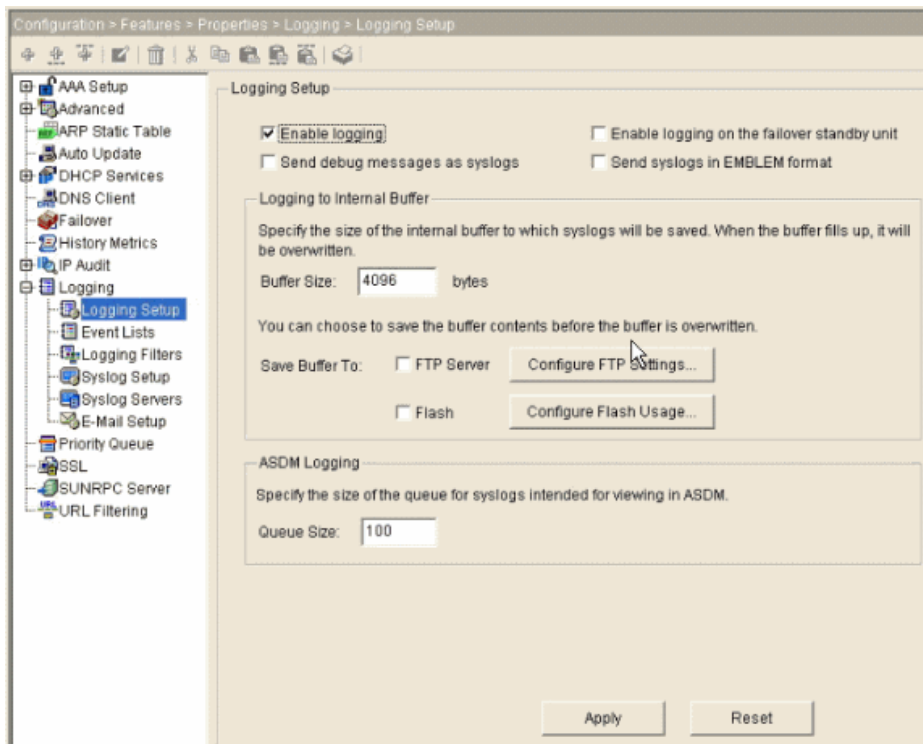
Voici un exemple de sortie.

```
%PIX|ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

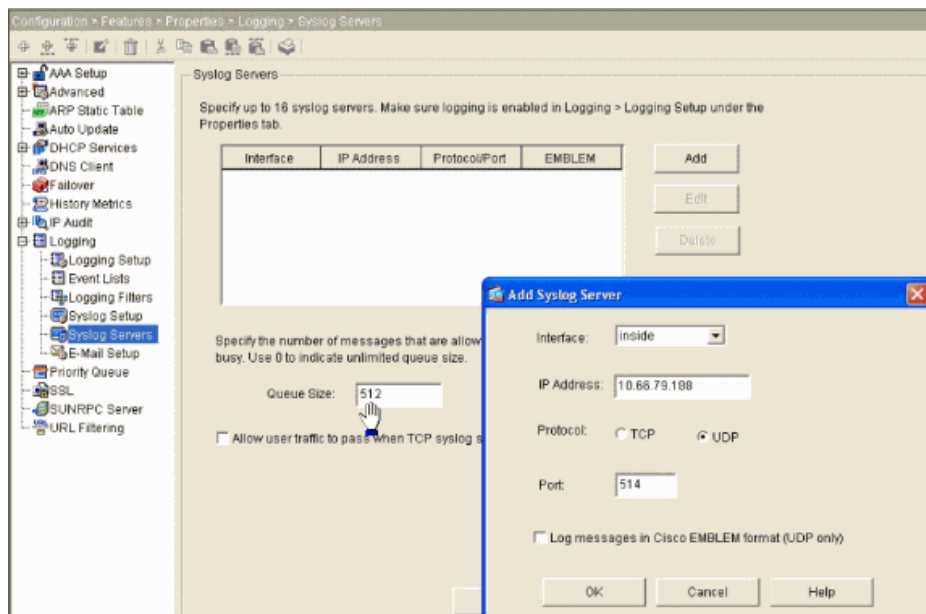
Configuration Syslog de base avec ASDM

Cette procédure explique la configuration ASDM pour toutes les destinations Syslog disponibles suivies de la configuration pour l'exemple 1.

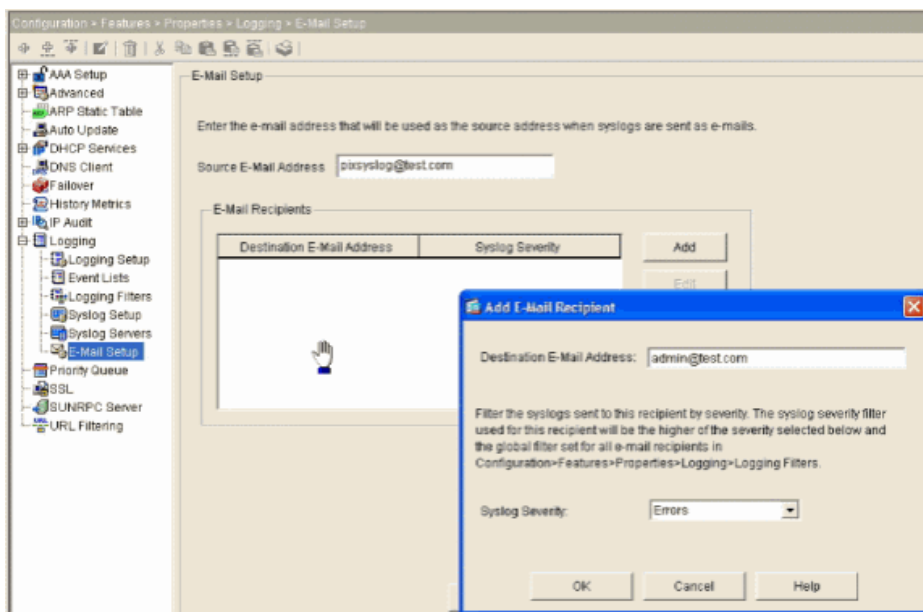
1. Accédez à la fenêtre d'accueil d'ASDM.
2. Choisissez **Configuration > Features > Properties > Logging > Logging Setup**.
3. Cochez **Enable logging in** pour activer les messages Syslog.



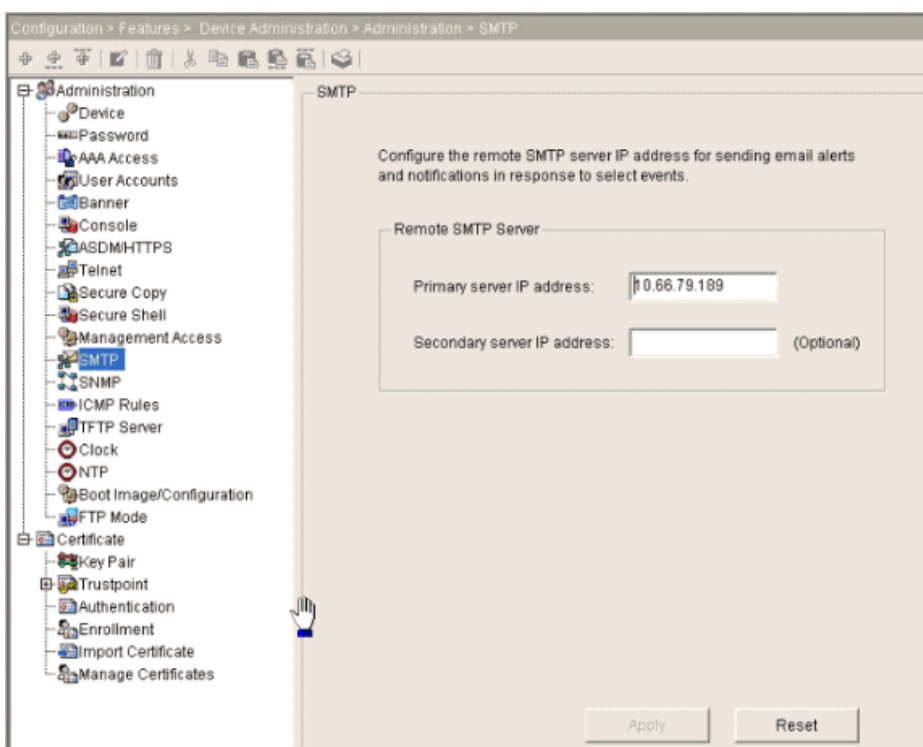
4. Choisissez **Syslog Servers** dans Logging et cliquez sur **Add** afin d'ajouter un serveur syslog.
5. Saisissez les détails du serveur syslog dans la zone Add Syslog Server (Ajouter un serveur Syslog) et choisissez **OK** lorsque vous avez terminé.



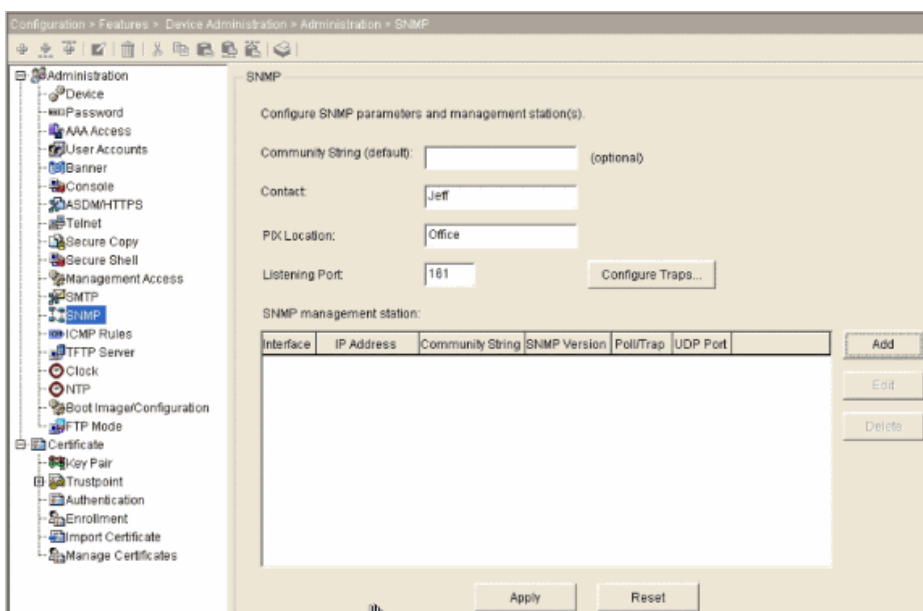
6. Choisissez **E-Mail Setup** dans Logging pour envoyer des messages Syslog aux messages électroniques.
7. Précisez l'adresse électronique source dans la zone de l'adresse électronique source et choisissez **Add** afin de configurer l'adresse électronique de destination des destinataires des messages électroniques et le niveau de gravité du message. Cliquez sur **OK** quand vous avez terminé.



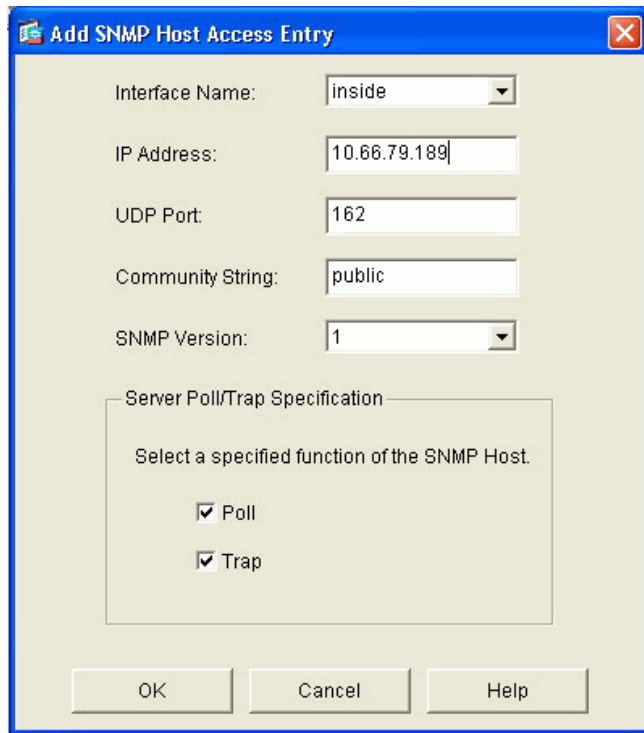
8. Choisissez **Device Administration**, puis **SMTP** et saisissez l'adresse IP du serveur afin de préciser l'adresse IP du serveur SMTP.



9. Choisissez **SNMP** afin de préciser l'adresse de la station de gestion SNMP et les propriétés.



10. Choisissez **Add** afin d'ajouter une station de gestion SNMP. Saisissez les détails de l'hôte SNMP et cliquez sur **OK**.



The dialog box titled "Add SNMP Host Access Entry" contains the following fields and options:

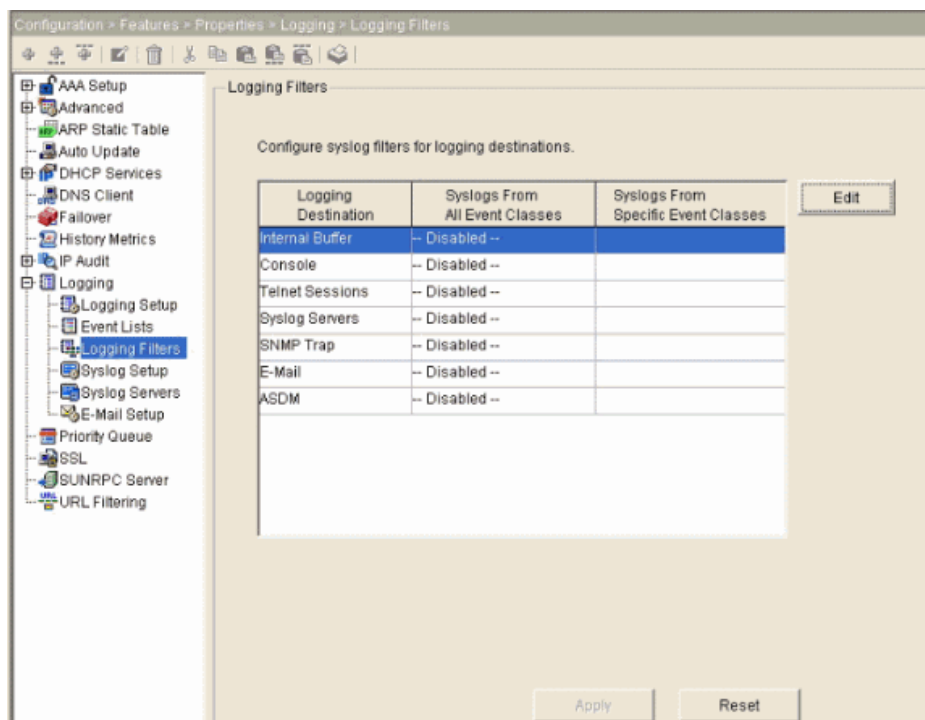
- Interface Name: inside
- IP Address: 10.66.79.189
- UDP Port: 162
- Community String: public
- SNMP Version: 1
- Server Poll/Trap Specification section with the text "Select a specified function of the SNMP Host." and two checked checkboxes: ☒ Poll and ☒ Trap.
- Buttons: OK, Cancel, Help.

11. Cliquez sur **Properties** sous Configuration et choisissez **Logging Filters** dans Logging pour sélectionner la destination des messages syslog.

12. Choisissez la destination de journalisation souhaitée et cliquez sur **Edit**.

Pour cette procédure, la commande **logging buffered debugging** de l'exemple 1 est utilisée.

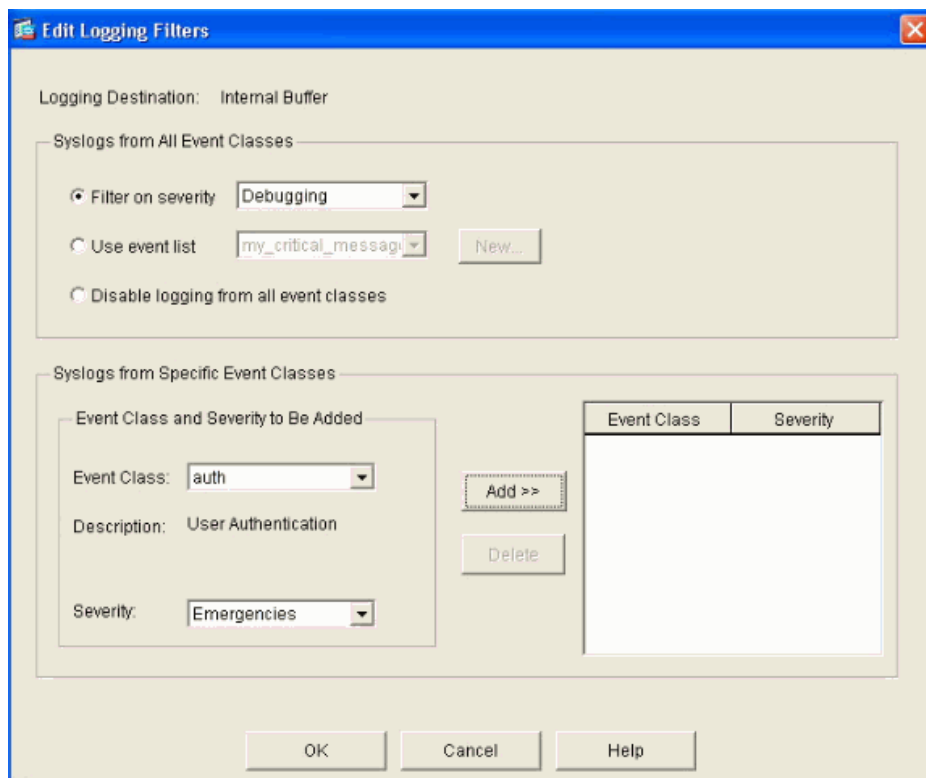
13. Choisissez **Internal Buffer** et cliquez sur **Edit**.



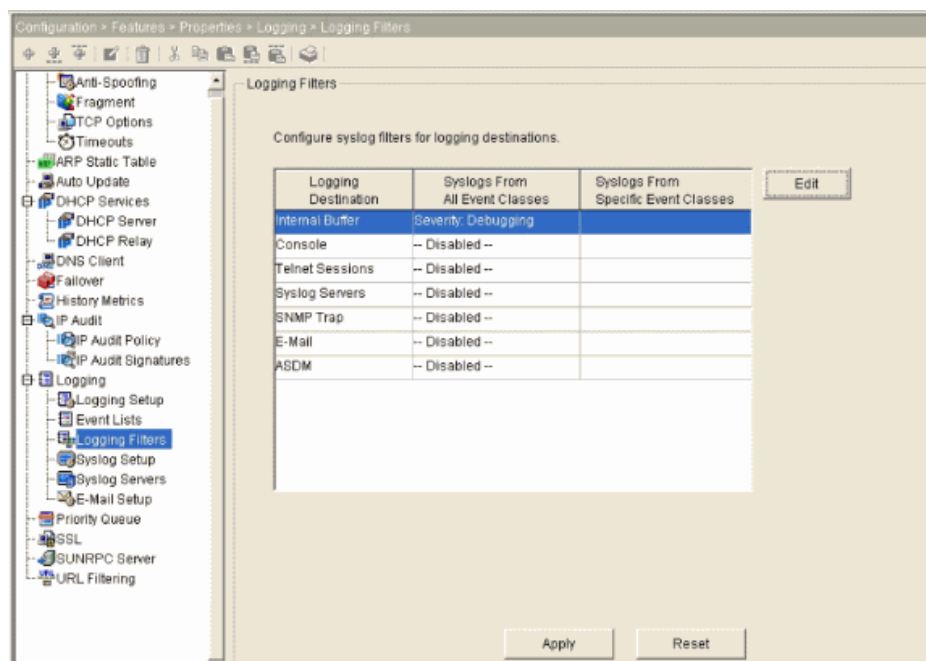
The "Logging Filters" window shows a table for configuring syslog filters. The table has three columns: "Logging Destination", "Syslogs From All Event Classes", and "Syslogs From Specific Event Classes". The "Internal Buffer" row is highlighted. An "Edit" button is located to the right of the table.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
Internal Buffer	-- Disabled --	
Console	-- Disabled --	
Telnet Sessions	-- Disabled --	
Syslog Servers	-- Disabled --	
SNMP Trap	-- Disabled --	
E-Mail	-- Disabled --	
ASDM	-- Disabled --	

14. Choisissez **Filter on severity** et choisissez **Debugging** dans le menu déroulant. Cliquez sur **OK** quand vous avez terminé.



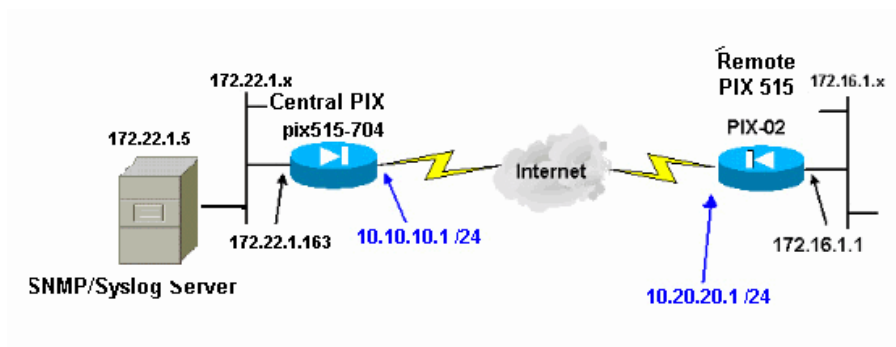
15. Cliquez sur **Apply** après être revenu à la fenêtre des filtres de journalisation.



Envoi de messages Syslog par un VPN à un serveur Syslog

Dans la conception simple de VPN site à site ou la conception plus compliquée en étoile, les gens veulent parfois contrôler tous les pare-feux PIX avec le serveur SNMP (Protocole de gestion de réseau simple) et le serveur syslog situés dans un site central.

Afin de configurer la configuration de VPN IPSec site à site, consultez le document PIX/ASA 7.x : tunnel VPN PIX à PIX simple avec l'exemple de configuration ASDM. Indépendamment de la configuration VPN, vous devez configurer le SNMP et le trafic intéressant pour le serveur syslog dans le site central et le site local.



Configuration centrale de PIX

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two PIXes.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the PIX 515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote PIX.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514
logging on
logging trap debugging
logging history debugging

!--- Define logging host information.

logging facility 16
logging host inside 172.22.1.5

!--- Define the SNMP configuration.

snmp-server host inside 172.22.1.5
snmp-server community test
snmp-server enable traps
```

Configuration distante de PIX

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two PIXes.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind PIX 515.

access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this PIX outside
!--- interface to the SYSLOG server.

access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514
```



```
!--- Define syslog server.

logging facility 23
logging host outside 172.22.1.5

!--- Define SNMP server.

snmp-server host outside 172.22.1.5
snmp-server community test
snmp-server enable traps
```

Consultez le document Surveillance du pare-feu Cisco Secure PIX en utilisant le protocole SNMP et Syslog par le tunnel VPN pour obtenir plus d'informations sur la façon de configurer PIX 6.x.

Configuration Syslog avancée

PIX 7.0 fournit plusieurs mécanismes qui vous permettent de configurer et de gérer les messages syslog dans des groupes. Ces mécanismes incluent le niveau de gravité du message, la catégorie du message, l'ID du message ou une liste de messages personnalisée que vous créez. Avec l'utilisation de ces mécanismes, vous pouvez saisir une commande unique qui s'applique à de petits ou grands groupes de messages. Quand vous configurez Syslog de cette façon, vous pouvez capturer les messages du groupe de message spécifié, non plus tous messages de la même gravité.

Utilisation de la liste de messages

Utilisez la liste de messages afin d'inclure seulement les messages syslog intéressés par le niveau de gravité et l'ID dans un groupe, puis associez cette liste de messages à la destination souhaitée.

Réalisez ces étapes afin de configurer une liste de messages.

1. Saisissez la commande **logging list message_list / level severity_level [class message_class]** afin de créer une liste de messages qui inclut des messages avec un niveau de gravité ou une liste de messages spécifiés.
2. Saisissez la commande **logging list message_list message syslog_id-syslog_id2** afin d'ajouter des messages supplémentaires à la liste de messages que vous venez de créer.
3. Saisissez la commande **logging destination message_list** afin de préciser la destination de la liste de messages créée.

Exemple 2

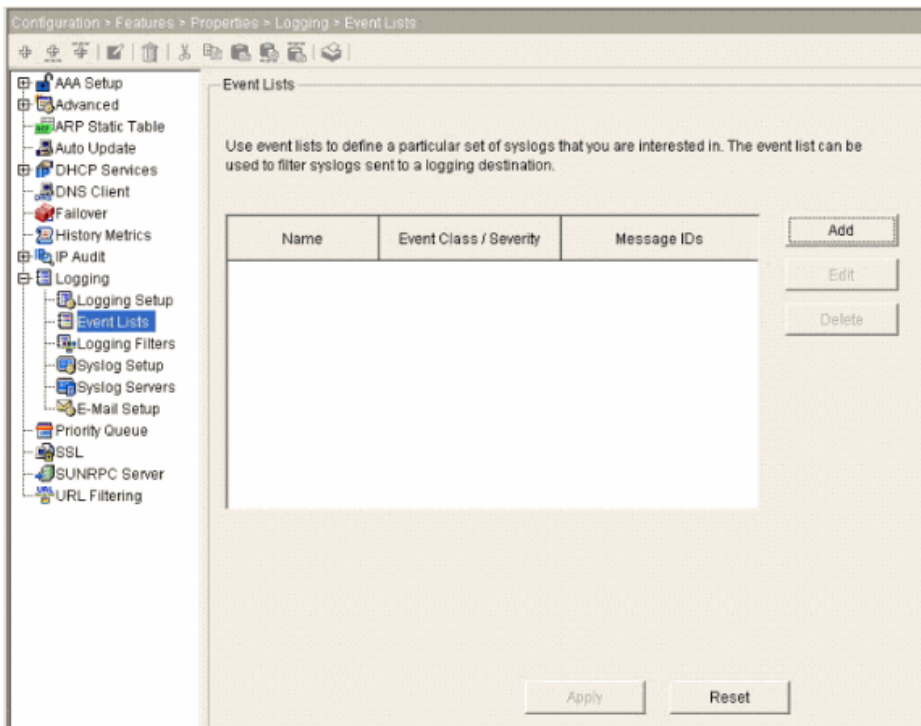
Lancez ces commandes afin de créer une liste de messages, qui inclut tous les messages de gravité 2 (critiques) avec les messages 611101 à 611323, et les envoyer également à la console :

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

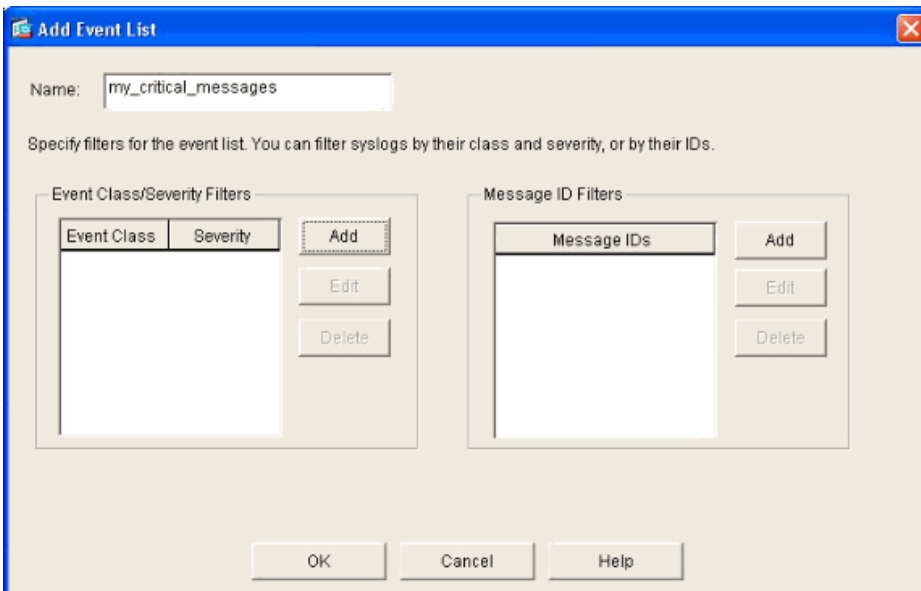
Configuration ASDM

Cette procédure montre une configuration ASDM pour l'exemple 2 avec l'utilisation de la liste de messages.

1. Choisissez **Event Lists** sous Logging et cliquez sur **Add** afin de créer une liste de messages.

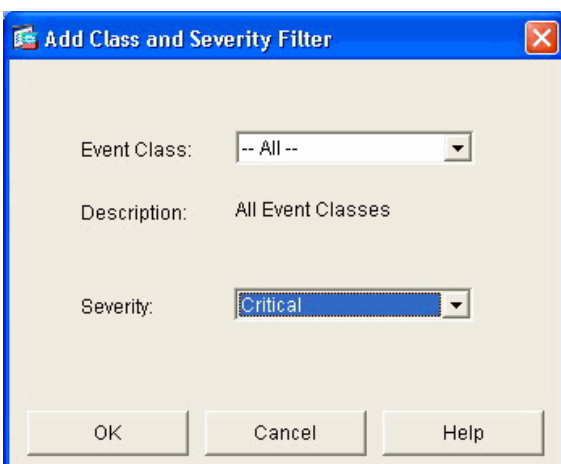


2. Saisissez le nom de la liste de messages dans la zone du nom. Dans cet exemple, **my_critical_messages** est utilisé. Cliquez sur **Add** sous Event Class/Severity Filters.



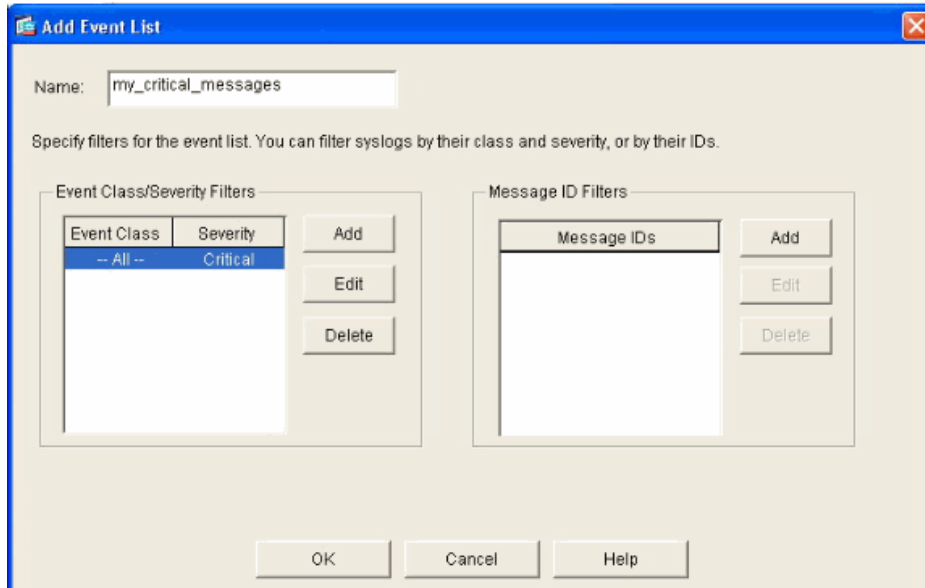
3. Choisissez la catégorie d'événement et la gravité dans les menus déroulants.

Dans cet exemple, choisissez **All** et **Critical** respectivement. Cliquez sur **OK** quand vous avez terminé.



4. Cliquez sur **Add** sous les filtres d'ID de message si des messages supplémentaires sont requis.

Dans cet exemple, vous devez inclure les messages avec les ID 611101 à 611323.




The 'Add Event List' dialog box has a title bar with a close button. It contains a 'Name' field with the text 'my_critical_messages'. Below it is a descriptive text: 'Specify filters for the event list. You can filter syslogs by their class and severity, or by their IDs.' There are two main filter sections. The 'Event Class/Severity Filters' section contains a table with two columns: 'Event Class' and 'Severity'. The first row shows '-- All --' and 'Critical'. To the right of this table are 'Add', 'Edit', and 'Delete' buttons. The 'Message ID Filters' section contains a table with one column: 'Message IDs'. To its right are 'Add', 'Edit', and 'Delete' buttons. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

Event Class	Severity
-- All --	Critical

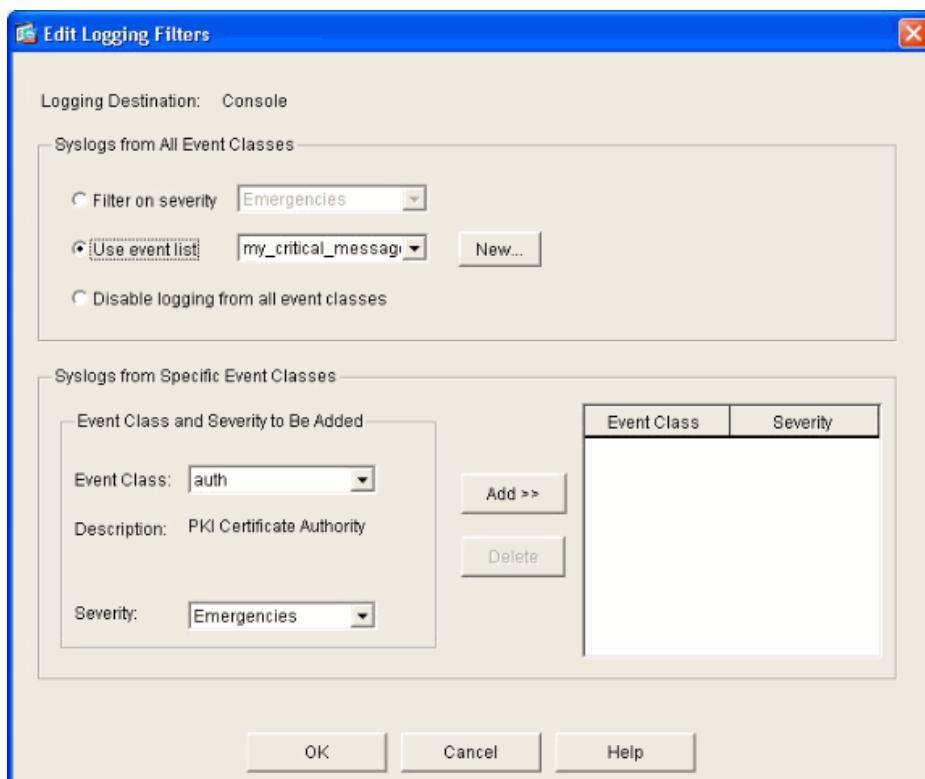
Message IDs

- Indiquez la plage d'ID dans la case des ID de message et cliquez sur **OK**.



The 'Add Syslog Message ID Filter' dialog box has a title bar with a close button. It contains the text: 'Enter the syslog message ID. Use hyphen to specify a range of syslog IDs, for example, 101001-101010.' Below this is a 'Message IDs' field containing the text '611101-611323'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

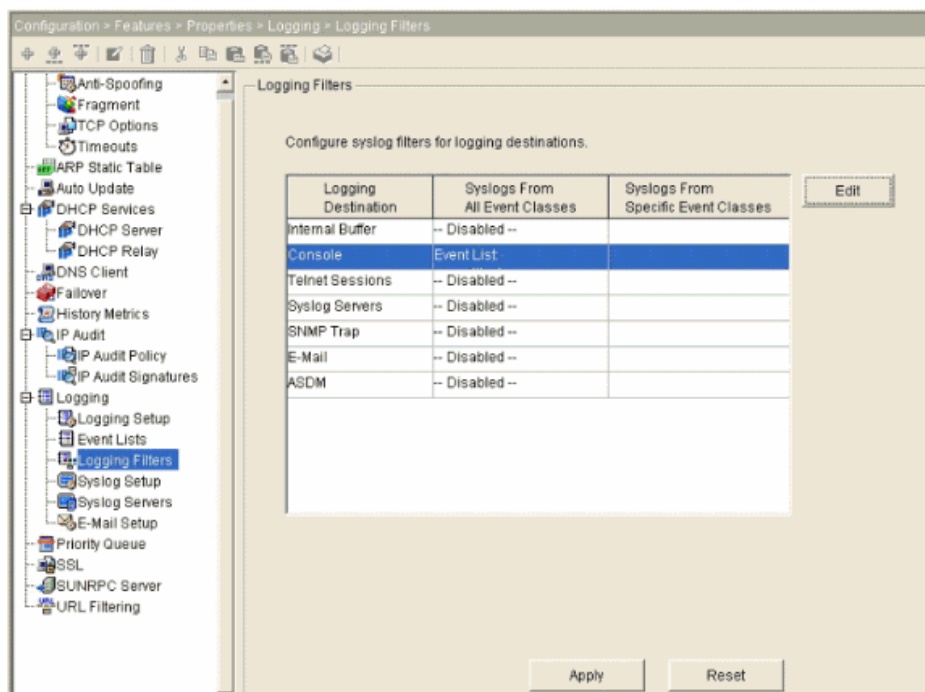
- Retournez au menu **Logging Filters** et choisissez **Console** comme destination.
- Cliquez sur **Use event list** et choisissez **my_critical_messages** dans le menu déroulant. Cliquez sur **OK** quand vous avez terminé.



The 'Edit Logging Filters' dialog box has a title bar with a close button. It contains a 'Logging Destination' field set to 'Console'. Below it is a section 'Syslogs from All Event Classes' with three radio buttons: 'Filter on severity' (selected), 'Use event list', and 'Disable logging from all event classes'. The 'Filter on severity' option has a dropdown menu set to 'Emergencies'. The 'Use event list' option has a dropdown menu set to 'my_critical_messages' and a 'New...' button. Below this is a section 'Syslogs from Specific Event Classes' with a table 'Event Class and Severity to Be Added'. The table has two columns: 'Event Class' and 'Severity'. The first row shows 'auth' and 'Emergencies'. To the right of the table are 'Add >>' and 'Delete' buttons. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Event Class	Severity
auth	Emergencies

- Cliquez sur **Apply** après être revenu à la fenêtre des filtres de journalisation.



Cela termine les configurations d'ASDM en utilisant la liste de messages comme présentée dans l'exemple 2.

Utilisation de la catégorie de message

Utilisez la catégorie de message afin d'envoyer tous les messages liés à une catégorie à l'emplacement de sortie indiqué. Quand vous précisez un seuil de niveau de gravité, vous pouvez limiter le nombre de messages envoyés à l'emplacement de sortie.

```
logging class message_class destination | severity_level
```

Exemple 3

Saisissez cette commande afin d'envoyer tous les messages de la catégorie ca avec un niveau de gravité urgent ou supérieur vers la console.

```
logging class ca console emergencies
```

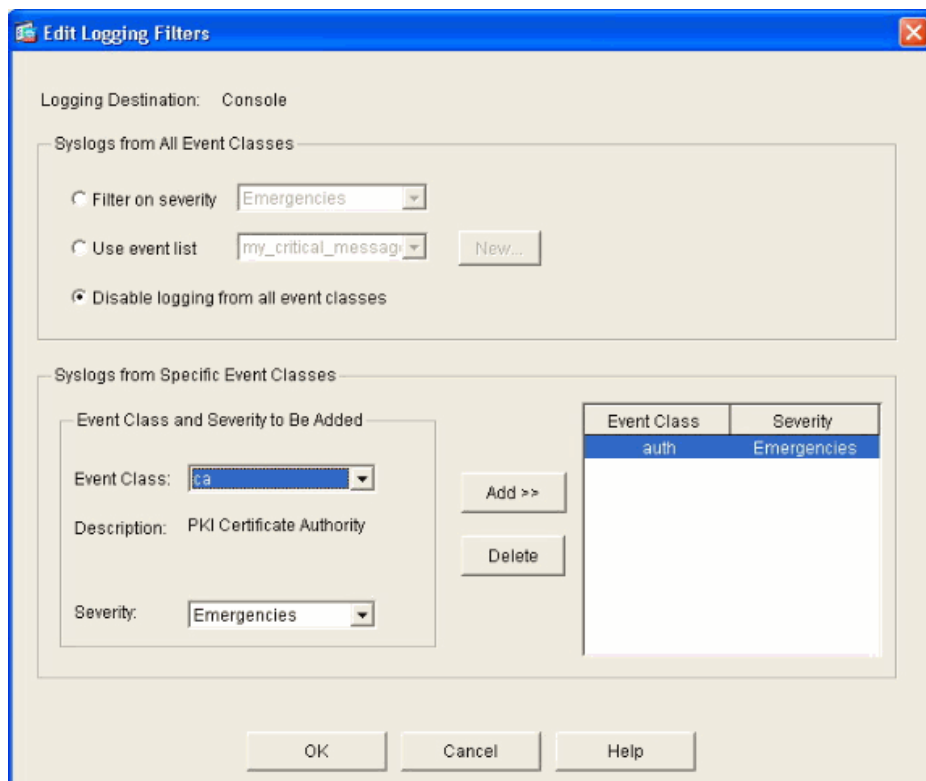
Configuration ASDM

Cette procédure montre la configuration ASDM pour l'exemple 3 avec l'utilisation de la liste de messages.

1. Choisissez le menu **Logging Filters** et choisissez **Console** comme destination.
2. Cliquez sur **Disable logging from all event classes**.
3. Sous les Syslog des catégories d'événement spécifiques, choisissez la catégorie d'événement et la gravité que vous souhaitez ajouter.

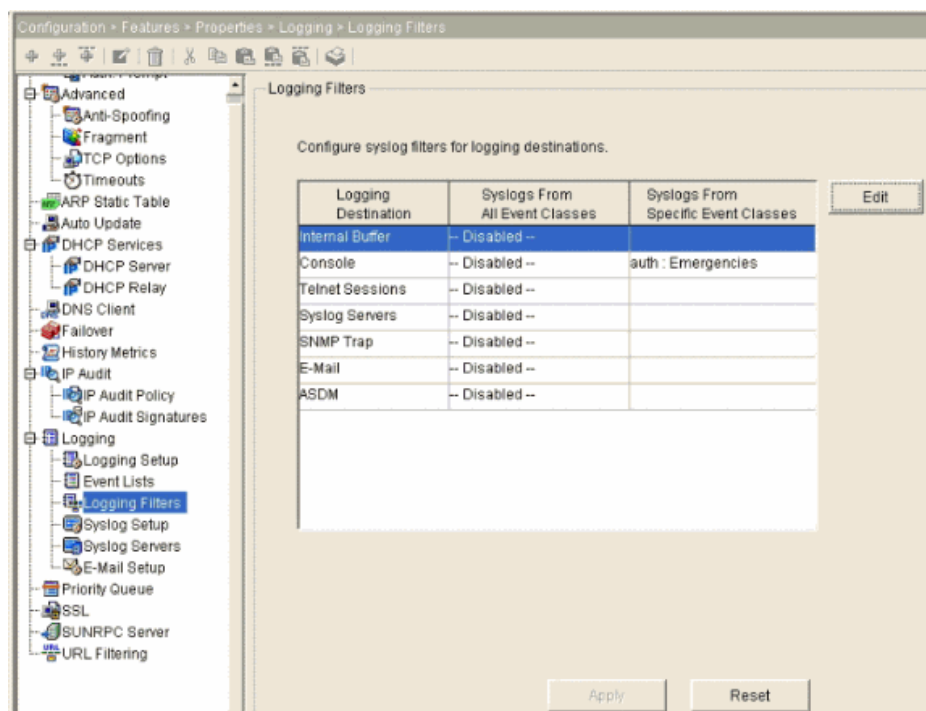
Cette procédure utilise **ca** et **Emergencies** respectivement.

4. Cliquez sur **Add** afin d'ajouter cela dans la catégorie de message et cliquez sur **OK**.



5. Cliquez sur **Apply** après être revenu à la fenêtre des filtres de journalisation.

La console collecte maintenant le message de catégorie Ca avec le niveau de gravité Emergencies comme indiqué sur la fenêtre des filtres de journalisation.



Cela termine la configuration ASDM pour l'exemple 3.

Consultez le document Messages listés par niveau de gravité pour obtenir une liste des niveaux de gravité des messages du journal.

Consignation des occurrences d'ACE d'ACL

Ajoutez l'option **log** à chaque élément de liste d'accès (ACE) que vous souhaitez afin de consigner les occurrences d'une liste d'accès. Utilisez cette syntaxe :

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

Exemple :

```
pixfirewall(config)#access-list 101 line 1 extended permit icmp any any log
```

Quand l'option **log** est précisée, elle génère le message syslog 106100 pour l'ACE auquel elle est appliquée. Le message syslog 106100 est généré pour chaque flux ACE d'autorisation ou de refus correspondant qui passe par le pare-feu PIX. Le flux de la première correspondance est mis en cache. Les correspondances ultérieures incrémentent le nombre d'occurrences affiché dans la commande **show access-list**.

Unable to connect to remote host: , Connection timed out pour l'ACE, et les nouveaux messages 106100 sont générés à la fin de l'intervalle défini par des secondes d'intervalle si le nombre d'occurrences pour le flux n'est pas égal à zéro. Le comportement de journalisation de liste d'accès par défaut, qui est le **mot-clé de journal** non spécifié, est que si un paquet est refusé, alors le message 106023 est généré, et si le paquet est autorisé, alors aucun message syslog n'est généré.

Un niveau Syslog facultatif (0 - 7) peut être indiqué pour les messages syslog générés (106100). Si aucun niveau n'est précisé, le niveau par défaut est 6 (informatif) pour un nouvel ACE. Si l'ACE existe déjà, alors son niveau de journal existant reste inchangé. Si l'option **log disable** est spécifiée, la journalisation de la liste d'accès est complètement désactivée. Aucun message syslog, notamment le message 106023, n'est généré. L'option par défaut **log** restaure le comportement de journalisation de liste d'accès par défaut.

Réalisez ces étapes afin de permettre au message syslog 106100 de s'afficher dans la sortie de la console :

1. Lancez la commande **logging enable** afin d'activer la transmission des messages du journal système vers tous les emplacements de sortie. Vous devez définir un emplacement de sortie de journalisation afin d'afficher tout journal.
2. Lancez la commande **logging message <message_number> level <severity_level>** afin de définir le niveau de gravité d'un message du journal système spécifique.

Dans cet exemple, lancez la commande **logging message 106100** pour activer le message 106100.

3. Lancez la commande **logging console message_list | severity_level** afin de permettre aux messages du journal système de s'afficher sur la console d'appliance de sécurité (TTY) à mesure qu'ils se produisent. Réglez le severity_level entre 1 et 7, ou utilisez le nom du niveau. Vous pouvez également préciser quels messages sont envoyés avec la variable message_list.
4. Lancez la commande **show logging message** afin d'afficher une liste de messages du journal système qui ont été modifiés par rapport à la configuration par défaut, qui sont les messages auxquels a été attribué un niveau de gravité différent et les messages qui ont été désactivés.

Voici un exemple de sortie de la commande **show logging message** :

```
pixfirewall#show logging message 106100
syslog 106100: default-level informational (enabled)
pixfirewall# %PIX-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Capture des messages Syslog du trafic VPN

Utilisez la commande **logging list** afin de capturer le Syslog pour les messages de VPN IPSec de LAN à LAN et d'accès à distance seulement. Cet exemple capture tous les messages du journal système de la catégorie VPN (IKE et IPsec) avec le niveau de débogage ou supérieur.

Exemple :

```
hostname(config)#logging enable
hostname(config)#logging timestamp
hostname(config)#logging list my-list level debugging class vpn
hostname(config)#logging trap my-list
hostname(config)#logging host inside 192.168.1.1
```

Remarque: La commande **logging list** est prise en charge sur la version 7.2(1) et ultérieure.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

1. Si vous ne recevez pas les messages 304001 Syslog, assurez-vous que la commande **inspect http** est activée sur l'ASA.
2. Si vous souhaitez refuser l'envoi d'un message syslog spécifique au serveur syslog, vous devez utiliser la commande indiquée.

```
hostname(config)#no logging message <syslog_id>
```

Consultez ce document sur la commande **logging message** pour obtenir plus d'informations.

%ASA-3-201008 : Disallowing new connections

Le message d'erreur %ASA-3-201008: Disallowing new connections . s'affiche quand l'ASA n'arrive pas à contacter le serveur syslog et qu'aucune nouvelle connexion n'est autorisée.

Solution

Ce message apparaît quand vous avez activé les messages du journal système de TCP et le serveur syslog ne peut pas être atteint, ou quand vous utilisez le serveur syslog Cisco ASA (PFSS) et que le disque du système Windows NT est plein. Procédez comme suit pour résoudre ce message d'erreur :

- Désactivez les messages du journal système de TCP s'ils sont activés.
- Si vous utilisez PFSS, libérez de l'espace sur le système Windows NT où PFSS réside.
- En outre, assurez-vous que le serveur syslog est disponible et que vous pouvez exécuter une commande ping sur l'hôte depuis la console Cisco ASA.
- Redémarrez la journalisation de messages système de TCP pour autoriser le trafic.

Si le serveur syslog devient indisponible et si la journalisation de TCP est configurée, utilisez la commande **logging permit-hostdown** ou passez à la journalisation UDP.

Informations connexes

- **Références des commandes du pare-feu Cisco Secure PIX**
- **Demandes de commentaires (RFC)** [🔗](#)
- **Exemples et notes techniques de configuration**

© 1992-2010 Cisco Systems Inc. Tous droits réservés.

Date du fichier PDF généré: 30 juillet 2013

http://www.cisco.com/cisco/web/support/CA/fr/109/1096/1096240_pix70-syslog.html
