Configurez la connexion sur Cisco FTD à l'aide de Cisco FMC

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Configuration de la configuration Syslog globale
    - Configuration de la journalisation
    - Configuration de la journalisation de base
    - Paramètres de journalisation VPN
    - Informations sur le serveur FTP (facultatif)
    - Taille de la mémoire Flash (facultatif)
    - Listes d'événements
    - Syslog de limitation de débit
    - Paramètres Syslog
  - Configurer la journalisation locale
  - Configuration de la journalisation externe
    - Serveur Syslog distant
    - Configuration du courrier électronique pour la journalisation
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit la configuration de la journalisation de Firepower Threat Defense (FTD) sur le Firepower Management Center (FMC)

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Technologie FirePOWER
- Appliance de sécurité adaptable (ASA)
- protocole Syslog

Composants utilisés

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

- FMC versions 6.0.1 et ultérieures.
- Image de défense contre les menaces ASA Firepower pour ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) qui exécute le logiciel version 6.0.1 et ultérieure.
- Image de défense contre les menaces ASA Firepower pour ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) qui exécute les versions 6.0.1 et ultérieures du logiciel.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les journaux système FTD fournissent des informations permettant de surveiller et de dépanner le périphérique FTD. Ces journaux sont utiles à la fois pour le dépannage de routine et pour la gestion des incidents. L'appliance FTD prend en charge la journalisation locale et externe.

La journalisation locale peut aider à résoudre les problèmes en direct, tandis que la journalisation externe est une méthode de collecte des journaux de l'appliance FTD vers un serveur Syslog externe. La journalisation sur un serveur central facilite l'agrégation des journaux et des alertes. La journalisation externe peut aider à la corrélation des journaux et à la gestion des incidents.

Pour la journalisation locale, l'appliance FTD prend en charge la console, les options de mémoire tampon interne et la journalisation de session Secure Shell (SSH). Pour la journalisation externe, l'appliance FTD prend en charge le serveur Syslog externe et le serveur de relais de messagerie.

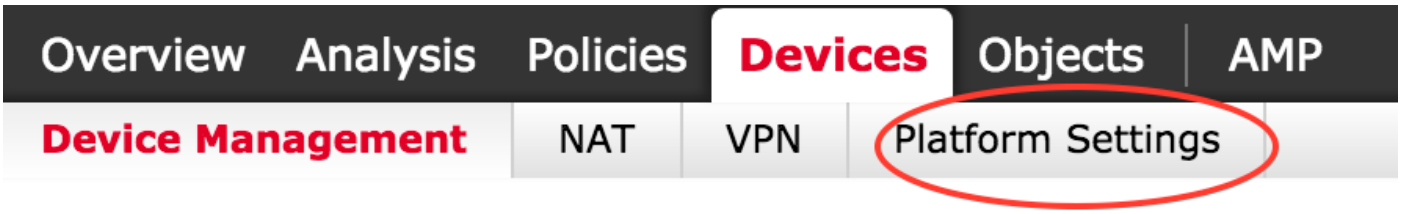
Remarque : Si un volume important de trafic traverse l'appliance, faites attention au type de journalisation/gravité/limitation du débit. Procédez ainsi afin de limiter le nombre de journaux,

---

ce qui évite tout impact sur le pare-feu.

Configurer

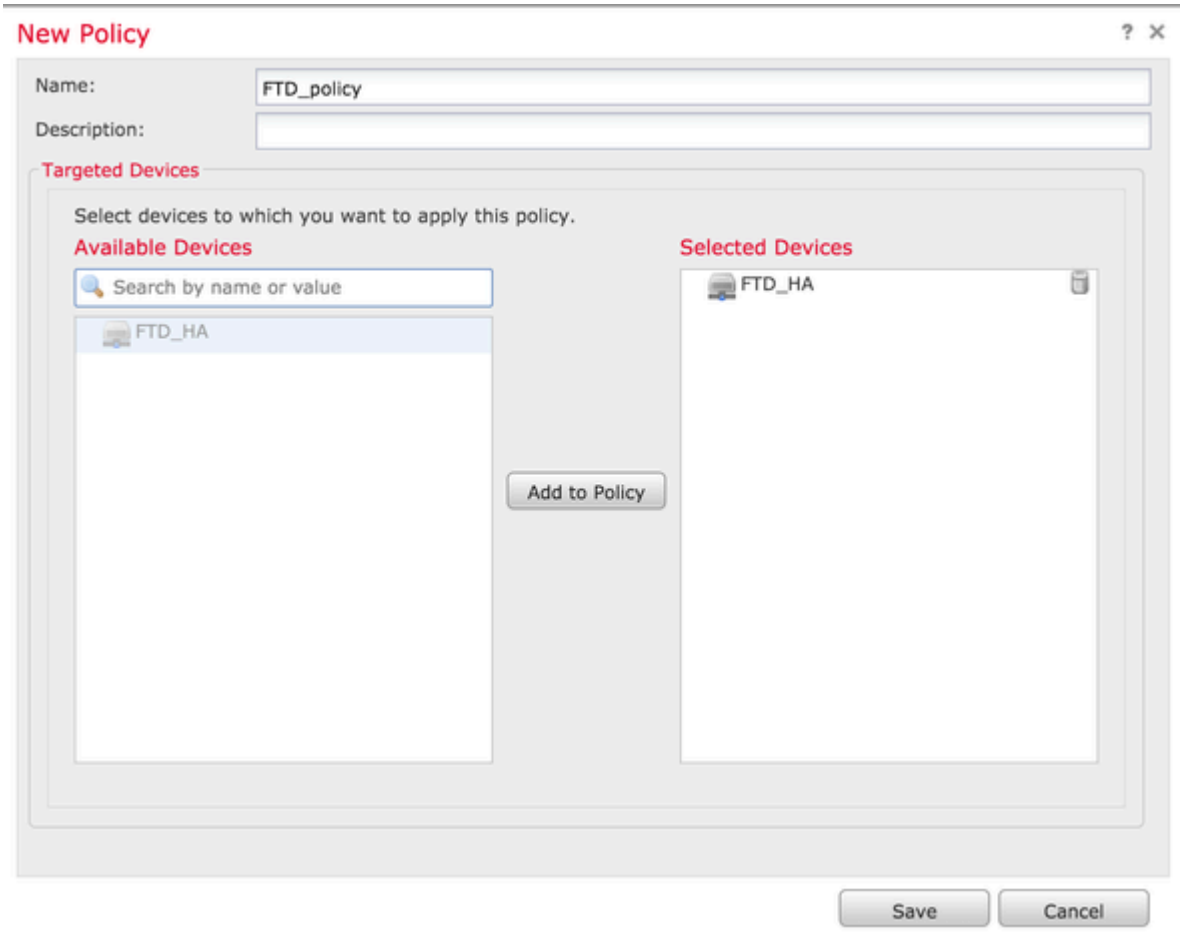
1. Toutes les configurations liées à la journalisation peuvent être configurées lorsque vous accédez à l'onglet Platform Settings sous l'onglet Devices. Choisissez Devices > Platform Settings comme illustré dans cette image :



2. Cliquez sur l'icône représentant un crayon pour modifier la stratégie existante ou cliquez sur Nouvelle stratégie, puis choisissez Paramètres de défense contre les menaces pour créer une nouvelle stratégie FTD :



3. Choisissez l'appareil FTD pour appliquer la stratégie et cliquez sur Enregistrer :



Configuration de la configuration Syslog globale

Certaines configurations s'appliquent à la fois à la journalisation locale et à la journalisation externe. Cette section détaille les paramètres obligatoires et facultatifs qui peuvent être configurés pour Syslog.

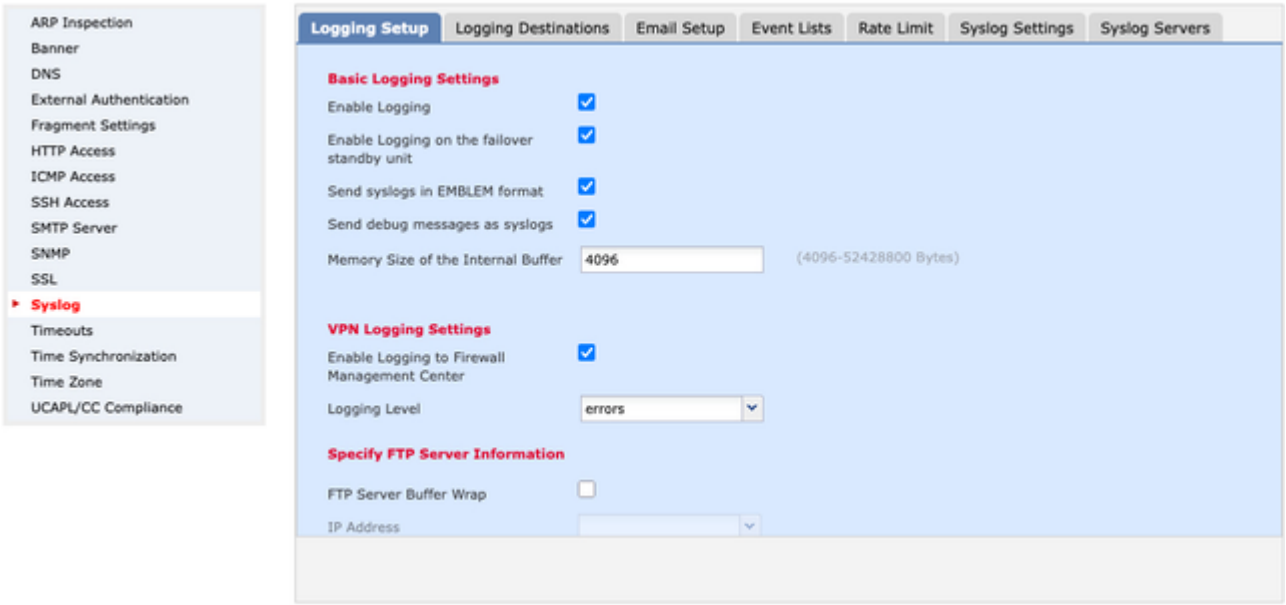
Configuration de la journalisation

1. Les options de configuration de la journalisation s'appliquent à la journalisation locale et externe. Pour configurer la configuration de la journalisation, choisissez Devices > Platform Settings.

2. Sélectionnez **Syslog** > **Logging Setup**.

Configuration de la journalisation de base

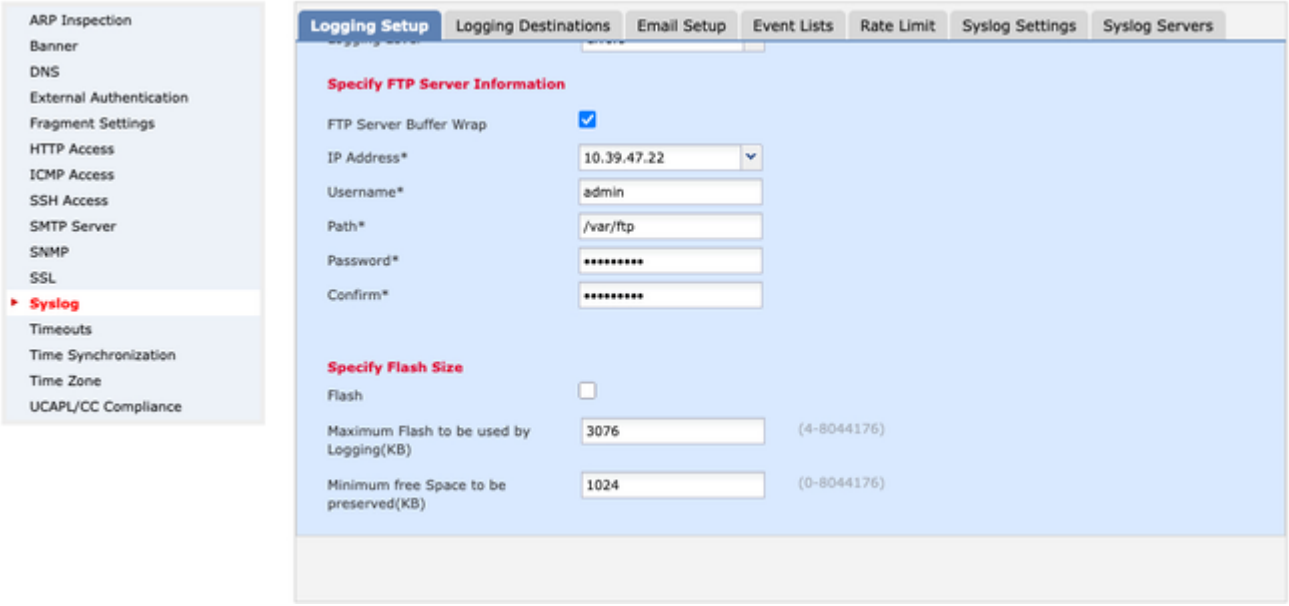
- Activer la journalisation : Cochez la case Enable Logging pour activer la journalisation (cette option est obligatoire.)
- Activer la journalisation sur l'unité de secours de basculement : Cochez la case Enable Logging on the failover standby unit pour configurer la journalisation sur le FTD de secours, qui fait partie du cluster FTD High-Availability (HA).
- Envoyer les Syslogs au format EMBLEM : Cochez la case Send syslog in EMBLEM format pour activer le format Syslog as EMBLEM pour chaque destination. Le format EMBLEM est principalement utilisé pour l'analyseur Syslog CiscoWorks Resource Manager Essentials (RME). Ce format correspond au format Syslog du logiciel Cisco IOS produit par les routeurs et les commutateurs. Il est disponible uniquement pour les serveurs Syslog UDP.
- Envoyer des messages de débogage en tant que Syslogs : Cochez la case Send debug messages as syslogs pour envoyer les journaux de débogage en tant que messages Syslog au serveur Syslog.
- Taille de la mémoire tampon interne : Saisissez la taille de la mémoire tampon interne dans laquelle FTD peut enregistrer les données du journal. Les données du journal sont tournées si leur limite de mémoire tampon est atteinte.



Paramètres de journalisation VPN

Vous pouvez activer la journalisation pour le dépannage VPN des syslogs pour les périphériques FTD. Tous les syslogs VPN apparaissent avec un niveau de gravité par défaut d'erreurs ou un niveau de gravité plus élevé (sauf s'ils ont été modifiés). Vous pouvez gérer la journalisation VPN via les paramètres de la plate-forme FTD et les niveaux de gravité des messages peuvent être ajustés en modifiant les paramètres de journalisation VPN pour les périphériques ciblés. Le fait de définir le niveau de journalisation VPN au niveau 4 et plus (avertissements, notifications, informations ou débogage) peut surcharger le FMC.

Remarque : Lorsque vous configurez un périphérique avec un VPN de site à site ou d'accès à distance, il active automatiquement l'envoi des syslogs VPN au FMC par défaut.



Informations sur le serveur FTP (facultatif)

Spécifiez les détails du serveur FTP si vous souhaitez envoyer des données de journal à un serveur FTP avant qu'il ne remplace la mémoire tampon interne.

- Enveloppe de la mémoire tampon du serveur FTP : Cochez la case FTP Server Buffer Wrap pour envoyer les données du journal de mémoire tampon au serveur FTP.
- Adresse IP: Saisissez l'adresse IP du serveur FTP.
- username (nom d'utilisateur) : Saisissez le nom d'utilisateur du serveur FTP.
- Chemin : Saisissez le chemin d'accès au répertoire du serveur FTP.
- Mot de passe : Saisissez le mot de passe du serveur FTP.
- Confirmer : Saisissez à nouveau le même mot de passe.

Taille de la mémoire Flash (facultatif)

Spécifiez la taille de la mémoire Flash pour enregistrer les données du journal dans la mémoire Flash une fois que la mémoire tampon interne est saturée.

- flash: Cochez la case Flash pour envoyer des données de journal à la mémoire Flash

interne.
- Flash maximal à utiliser par la journalisation (Ko) : Saisissez la taille maximale en Ko de mémoire flash à utiliser pour la journalisation.
- Espace libre minimal à conserver (Ko) : Saisissez la taille minimale en Ko de la mémoire flash à conserver.

Cliquez sur Save pour enregistrer le paramètre de plate-forme. Choisissez l'option Déployer, puis sélectionnez l'appliance FTD où vous souhaitez appliquer les modifications. Cliquez sur Déployer pour démarrer le déploiement du paramètre de plate-forme.

Listes d'événements

L'option Configurer les listes d'événements vous permet de créer/modifier une liste d'événements et de spécifier les données de journal à inclure dans le filtre de liste d'événements. Les listes d'événements peuvent être utilisées lorsque vous configurez les filtres de journalisation sous Destinations de journalisation.

Le système offre deux options pour utiliser la fonctionnalité des listes d'événements personnalisées.

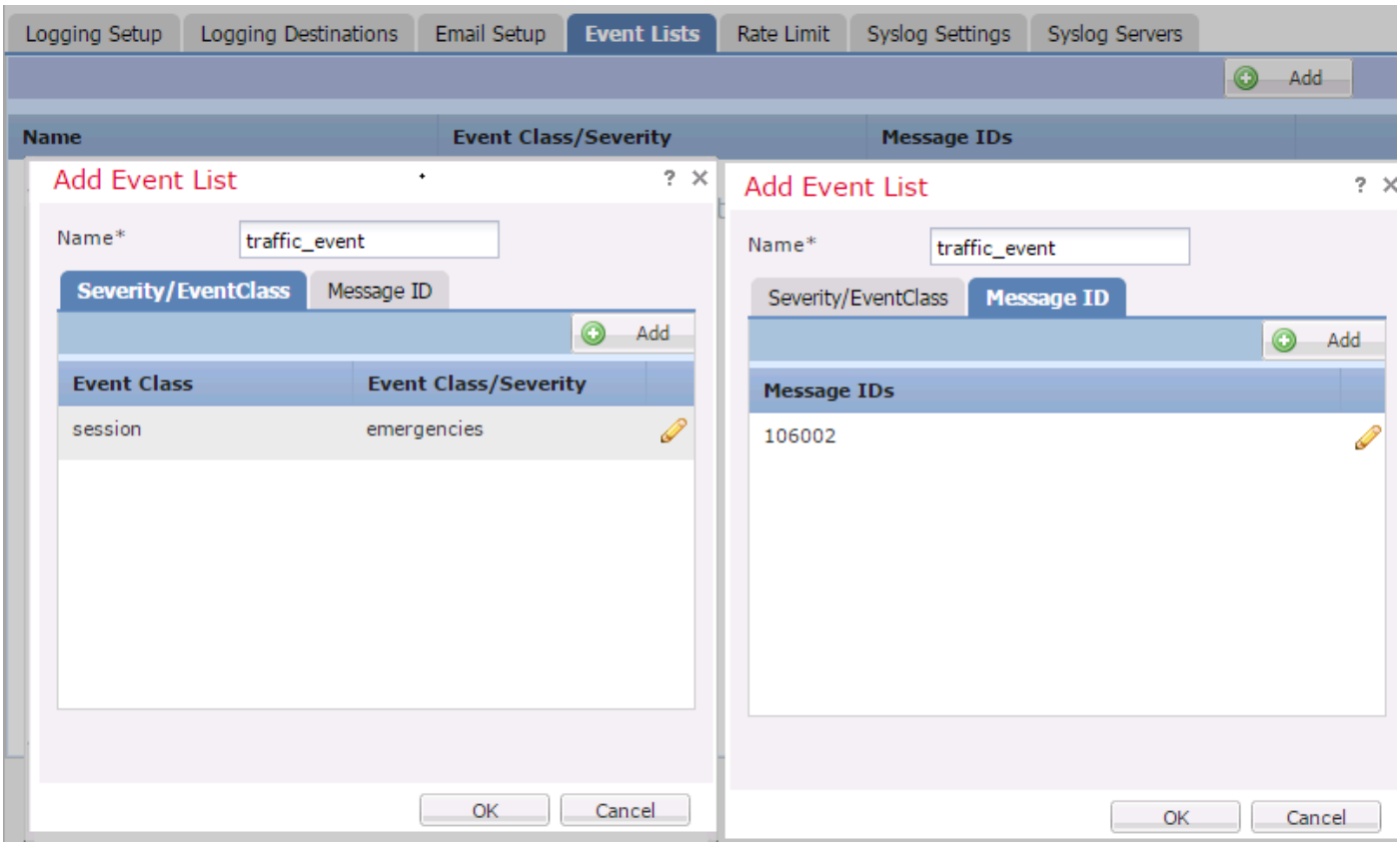
- Classe et gravité
- ID du message

---

1. Pour configurer des listes d'événements personnalisées, choisissez Device > Platform Setting > Threat Defense Policy > Syslog > Event List et cliquez sur Add. Voici les options disponibles :

- Name : Entrez le nom de la liste d'événements.
- Gravité/Classe d'événement : Dans la section Severity/Event Class, cliquez sur Add.
- Classe d'événement : Choisissez la classe d'événement dans la liste déroulante pour le type de données de journal souhaité. Une classe d'événements définit un ensemble de règles Syslog qui représentent les mêmes fonctionnalités. Par exemple, il existe une classe Event pour la session qui inclut tous les Syslogs qui se rapportent à cette session.

- Gravité Syslog : Sélectionnez le niveau de gravité dans la liste déroulante pour la classe d'événement sélectionnée. La gravité peut être comprise entre 0 (urgence) et 7 (débogage).
- ID du message : Si vous êtes intéressé par des données de journal spécifiques liées à un ID de message, cliquez sur Add pour placer un filtre basé sur l'ID de message.
- ID de message : Spécifiez l'ID de message sous forme de format individuel/plage.



---

2. Cliquez sur OK pour enregistrer la configuration.

---

3. Cliquez sur Enregistrer pour enregistrer le paramètre de plate-forme. Choisissez de déployer, sélectionnez l'appliance FTD où vous souhaitez appliquer les modifications. Cliquez sur Déployer pour démarrer le déploiement du paramètre de plate-forme.

Syslog de limitation de débit

L'option Rate limit définit le nombre de messages pouvant être envoyés à toutes les destinations configurées et définit la gravité du message auquel vous souhaitez attribuer des limites de débit.

---

1. Pour configurer les limites de débit pour les Syslog, choisissez Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit. Vous avez deux options pour spécifier la limite de débit :

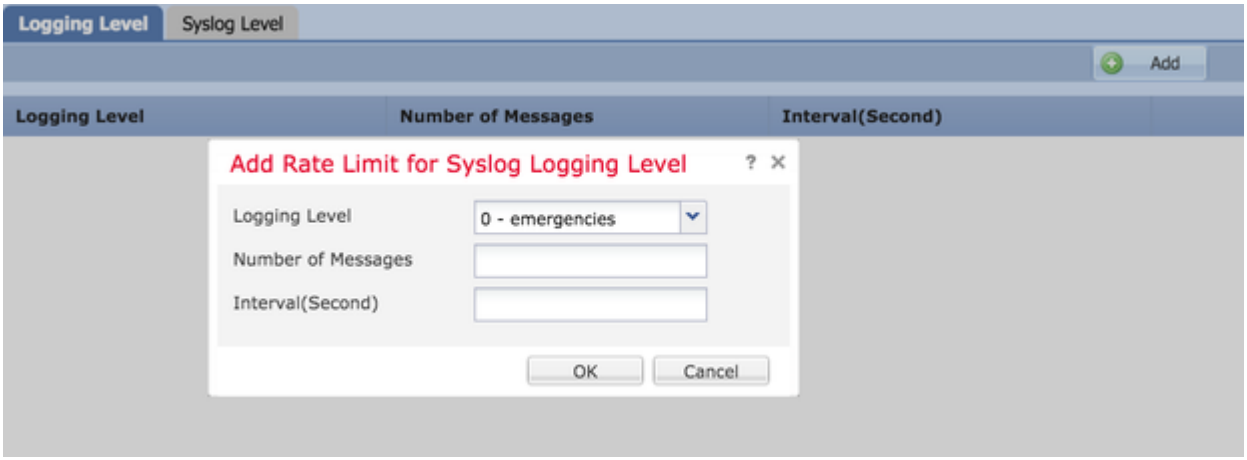
- Niveau de journalisation
- Niveaux Syslog

---

2. Pour activer la limite de débit basée sur le niveau de journalisation, choisissez Logging Level et cliquez sur Add.

- Niveau de journalisation : Dans la liste déroulante Logging Level, choisissez le niveau de journalisation que vous souhaitez ajouter à la limitation de débit.
- Nombre de messages : Saisissez le nombre maximal de messages Syslog à recevoir au cours de l'intervalle spécifié.
- Intervalle (seconde) : En fonction du paramètre Nombre de messages configuré précédemment, entrez l'intervalle de temps avec un ensemble fixe de messages Syslog à recevoir.

Le taux de Syslog est le nombre de messages/intervalles.



---

3. Cliquez sur OK pour enregistrer la configuration du niveau de journalisation.

---

4. Pour activer la limite de débit basée sur le niveau Syslog, choisissez Syslog Level et cliquez sur Add.

- ID Syslog : Les ID Syslog sont utilisés pour identifier de manière unique les messages Syslog. Dans la liste déroulante ID Syslog, sélectionnez l'ID Syslog.
- Nombre de messages : Saisissez le nombre maximal de messages syslog à recevoir au cours de l'intervalle spécifié.
- Intervalle (seconde) : En fonction du paramètre Nombre de messages configuré précédemment, entrez l'intervalle de temps avec un ensemble fixe de messages Syslog à recevoir.

Le taux de Syslog est le nombre de messages/intervalle.



---

5. Cliquez ok pour enregistrer la configuration du niveau Syslog.

---

6. Cliquez sur Enregistrer pour enregistrer le paramètre de plate-forme. Choisissez de déployer, puis sélectionnez l'appliance FTD où vous souhaitez appliquer les modifications. Cliquez sur Déployer pour démarrer le déploiement du paramètre de plate-forme.

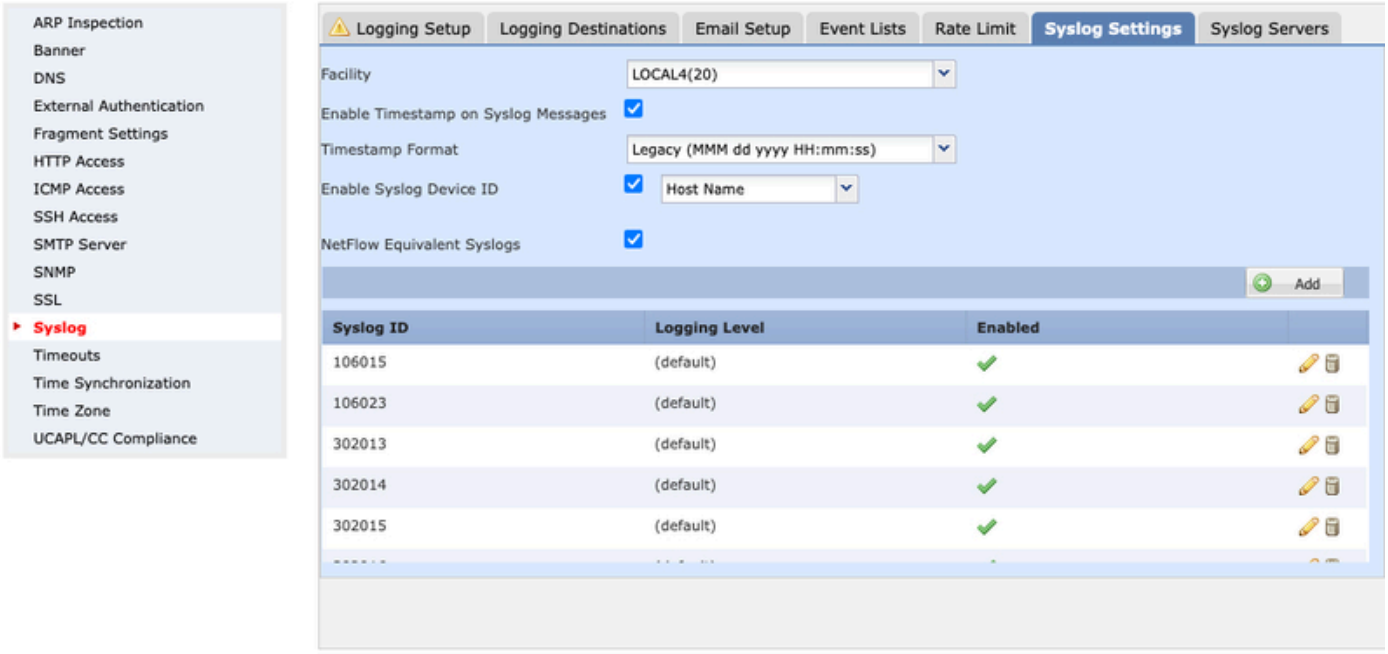
Paramètres Syslog

Les paramètres Syslog permettent de configurer les valeurs Facility à inclure dans les messages Syslog. Vous pouvez inclure l'horodatage dans les messages du journal et d'autres paramètres spécifiques au serveur Syslog.

---

1. Pour configurer des listes d'événements personnalisées, choisissez Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings.

- Installation : Un code de fonction est utilisé pour spécifier le type de programme consignant le message. Les messages avec des fonctionnalités différentes peuvent être traités différemment. Dans la liste déroulante Facility, sélectionnez la valeur Facility.
- Activer l'horodatage sur les messages Syslog : Cochez la case Enable Timestamp on Syslog Messages pour inclure l'horodatage dans les messages Syslog. Vous pouvez choisir le Format d'horodatage après avoir activé cette option.
- Activer l'ID de périphérique Syslog : Cochez la case Enable Syslog Device ID pour inclure un ID de périphérique dans les messages Syslog au format non EMBLEM.
- Syslogs équivalents Netflow : Cochez la case Syslogs équivalents NetFlow pour envoyer des syslogs équivalents NetFlow. Elle peut affecter les performances de l'appliance.
- Ajouter un ID Syslog spécifique : Pour spécifier l'ID Syslog supplémentaire, cliquez sur Add et spécifiez la case à cocher Syslog ID/ Logging Level.



---

2. Cliquez sur Enregistrer pour enregistrer le paramètre de plate-forme. Choisissez de déployer, puis sélectionnez l'appliance FTD où vous souhaitez appliquer les modifications. Cliquez sur Déployer pour démarrer le déploiement du paramètre de plate-forme.

Configurer la journalisation locale

La section Logging Destination peut être utilisée pour configurer la journalisation vers des destinations spécifiques.

Les destinations de journalisation internes disponibles sont les suivantes :

- Tampon interne : Enregistre dans le tampon de journalisation interne (tampon de journalisation).
- Console : Envoie les journaux à la console (console de journalisation).
- Sessions SSH : Enregistre les sessions Syslog vers SSH (terminal monitor).

La configuration de la journalisation locale s'effectue en trois étapes.

1. Choisissez Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.

---

2. Cliquez sur Ajouter pour ajouter un filtre de journalisation pour une destination de journalisation

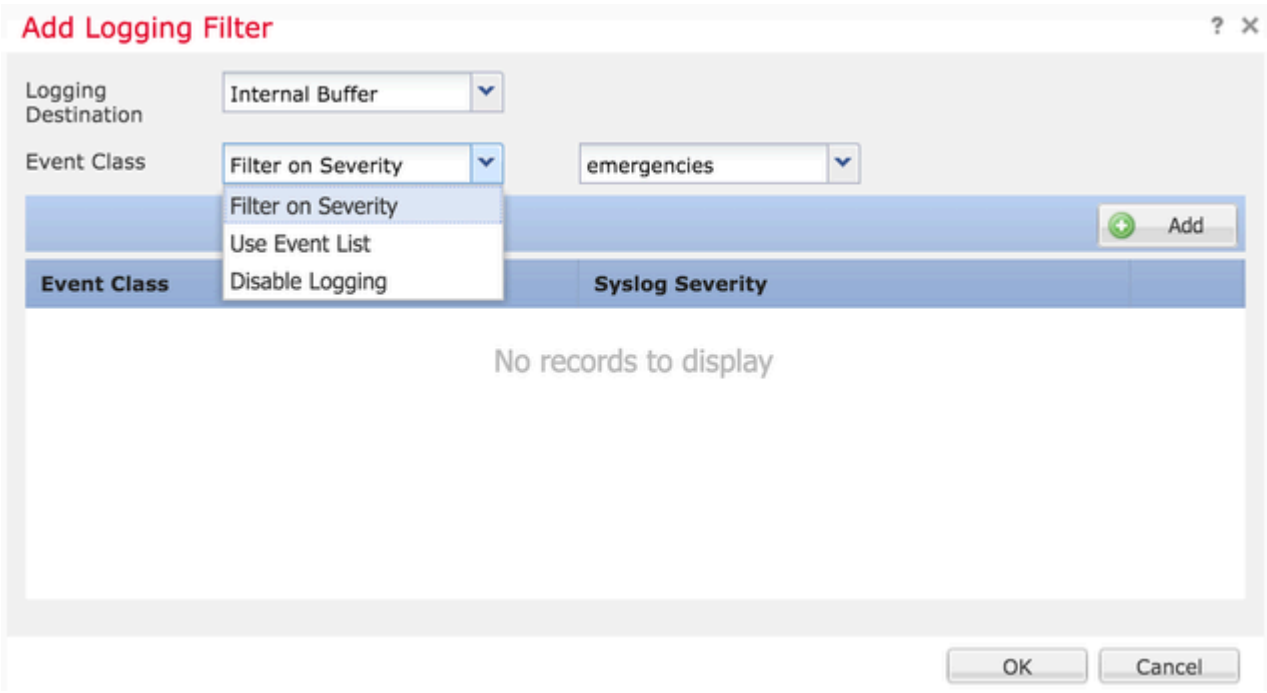
spécifique.

3. Destination de journalisation : Choisissez la destination de journalisation requise dans la liste déroulante Logging Destination comme Internal Buffer, Console ou SSH sessions.

Classe d'événement : Dans la liste déroulante Event Class, sélectionnez une classe Event. Les classes d'événements sont un ensemble de Syslog qui représentent les mêmes fonctionnalités. Les classes d'événements peuvent être sélectionnées de trois manières :

- Filtrer selon la gravité : Les classes d'événements filtrent en fonction de la gravité des Syslogs.
- Liste des événements utilisateur : Les administrateurs peuvent créer des listes d'événements spécifiques avec leurs propres classes d'événements personnalisées et les référencer dans cette section.
- Désactiver la journalisation : Utilisez cette option pour désactiver la journalisation pour la destination et le niveau de journalisation sélectionnés.

Niveau de journalisation : Sélectionnez le niveau de journalisation dans la liste déroulante. Le niveau de journalisation est compris entre 0 (Urgences) et 7 (Débogage).

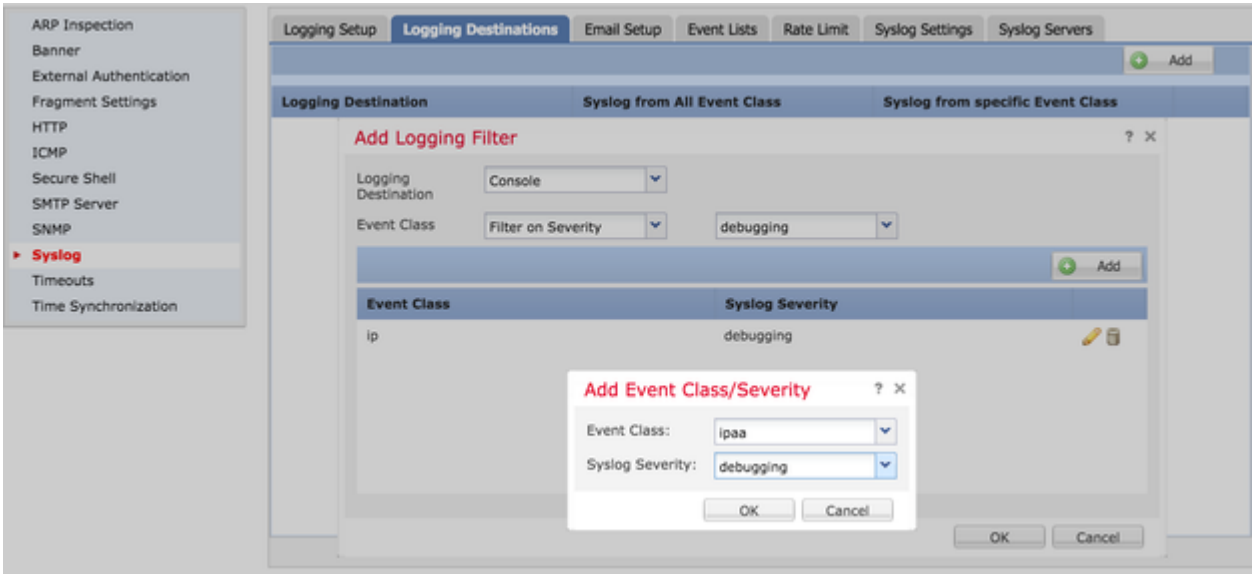


---

4. Pour ajouter une classe Event distincte à ce filtre de journalisation, cliquez sur Add.

Classe d'événement : Sélectionnez la classe d'événement dans la liste déroulante Classe d'événement.

Gravité Syslog : Sélectionnez la gravité Syslog dans la liste déroulante Gravité Syslog.



---

5. Cliquez sur OK une fois que le filtre est configuré pour ajouter le filtre pour une destination de journalisation spécifique.

---

6. Cliquez sur Enregistrer pour enregistrer le paramètre de plate-forme. Choisissez Déployer, puis l'appliance FTD sur laquelle vous souhaitez appliquer les modifications. Cliquez sur Déployer pour démarrer le déploiement du paramètre de plate-forme.

Configuration de la journalisation externe

Pour configurer la journalisation externe, choisissez Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.

FTD prend en charge ces types de journalisation externe.

- Serveur Syslog : Envoie les journaux au serveur Syslog distant.
- Déroutement SNMP : Envoie les déconnexions en tant que déroutement SNMP.
- E-mail : Envoie des journaux par e-mail avec un serveur de relais de messagerie préconfiguré.

La configuration de la journalisation externe et de la journalisation interne est identique. La sélection des destinations de journalisation détermine le type de journalisation implémenté. Il est possible de configurer des classes d'événements en fonction de listes d'événements personnalisées pour le serveur distant.

Serveur Syslog distant

Les serveurs Syslog peuvent être configurés pour analyser et stocker les journaux à distance à partir du FTD. La configuration des serveurs Syslog distants s'effectue en trois étapes.

1. Choisissez Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers.

---

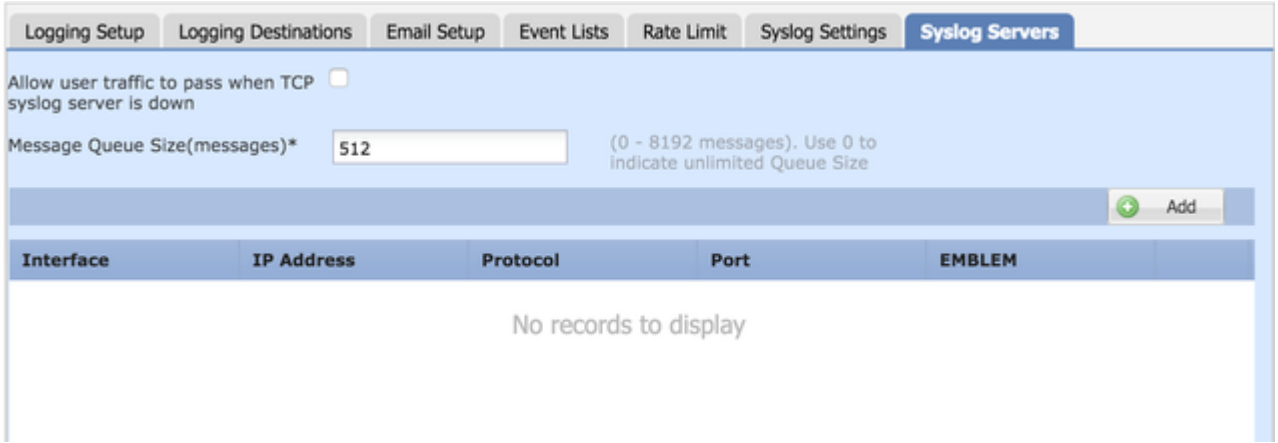
2. Configurez le paramètre relatif au serveur Syslog.

---

3. Autorisez le trafic utilisateur à passer lorsque le serveur Syslog TCP est arrêté. Si un serveur Syslog TCP a été déployé sur le réseau et qu'il n'est pas accessible, le trafic réseau via l'ASA est refusé. Cela s'applique uniquement lorsque le protocole de transport entre l'ASA et le serveur Syslog est TCP. Cochez la case Allow user traffic to pass when TCP syslog server is down pour permettre au trafic de passer par l'interface lorsque le serveur Syslog est arrêté.

---

4. Taille de la file de messages : La taille de la file d'attente des messages est le nombre de messages qui sont mis en file d'attente dans le FTD lorsque le serveur Syslog distant est occupé et n'accepte aucun message de journal. La valeur par défaut est 512 messages et le minimum est 1 message. Si 0 est spécifié dans cette option, la taille de la file d'attente est considérée comme illimitée.



---

5. Pour ajouter des serveurs Syslog distants, cliquez sur Add.

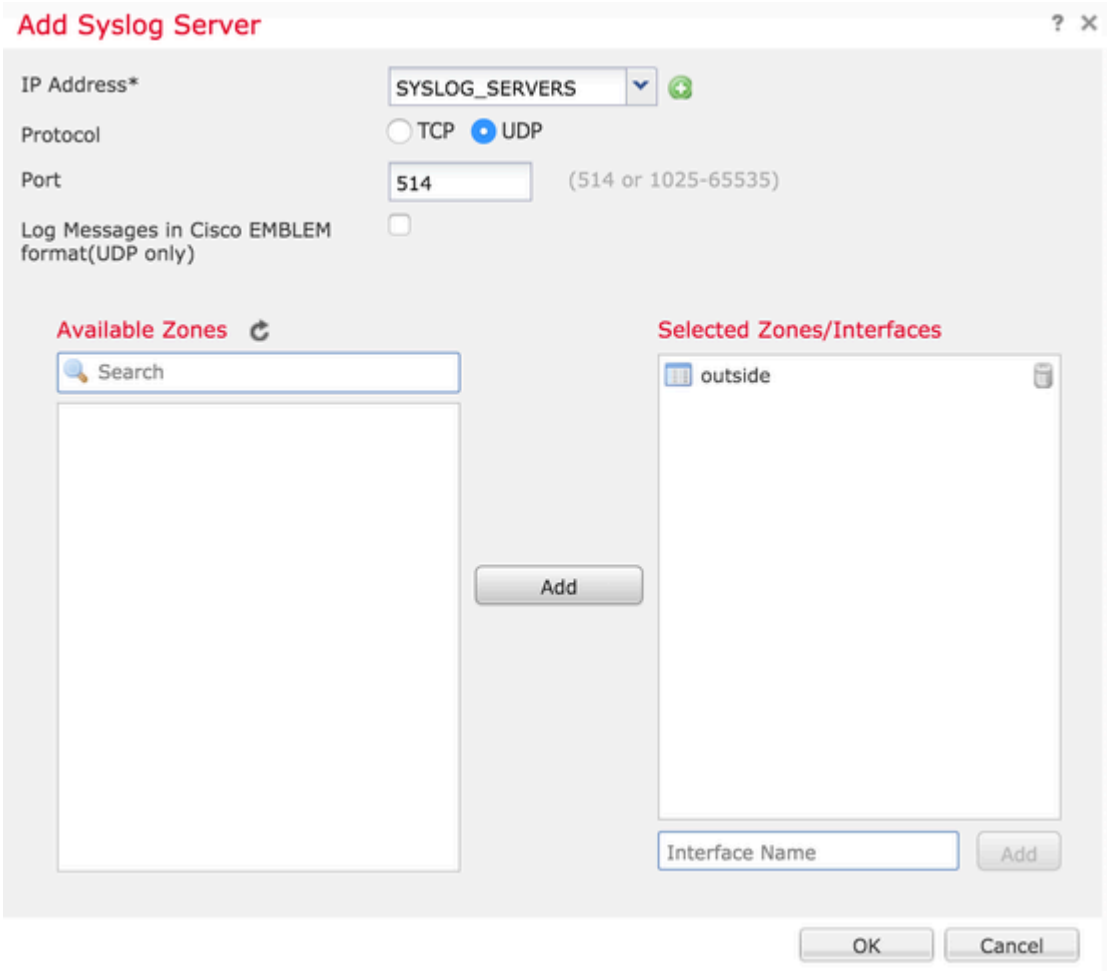
Adresse IP: Dans la liste déroulante IP Address, sélectionnez un objet réseau dont les serveurs Syslog sont répertoriés. Si vous n'avez pas créé d'objet réseau, cliquez sur l'icône plus (+) pour créer un nouvel objet.

Protocole : Cliquez sur la case d'option TCP ou UDP pour la communication Syslog.

Port : Saisissez le numéro de port du serveur Syslog. Par défaut, il est 514.

Consigner les messages au format Cisco EMBLEM (UDP uniquement) : Cochez la case Log Messages in Cisco EMBLEM format (UDP seulement) pour activer cette option. S'il est nécessaire de consigner les messages au format EMBLEM de Cisco (applicable uniquement pour le Syslog basé sur UDP).

Zones disponibles : Entrez les zones de sécurité sur lesquelles le serveur Syslog est accessible et déplacez-le vers la colonne Selected Zones/Interfaces.



---

6. Cliquez sur OK et sur Save pour enregistrer la configuration.

---

7. Cliquez sur Enregistrer pour enregistrer le paramètre de plate-forme. Choisissez Déployer et sélectionnez l'appliance FTD où vous souhaitez appliquer les modifications. Cliquez sur Déployer pour démarrer le déploiement du paramètre de plate-forme.

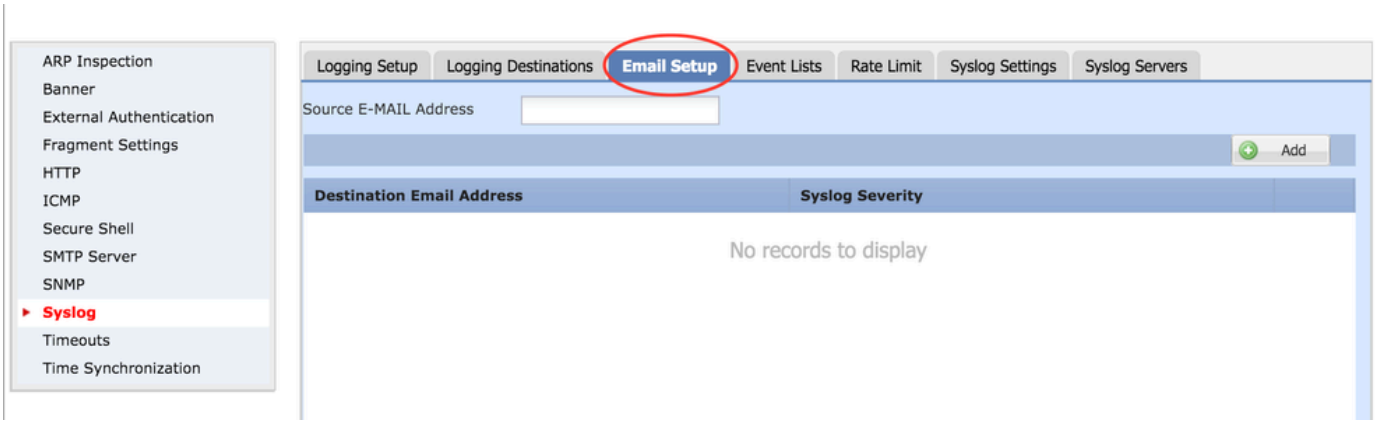
Configuration du courrier électronique pour la journalisation

FTD vous permet d'envoyer le Syslog à une adresse e-mail spécifique. Le courrier électronique ne peut être utilisé comme destination de journalisation que si un serveur de relais de messagerie a déjà été configuré.

La configuration des paramètres de messagerie pour les Syslogs s'effectue en deux étapes.

1. Choisissez Device > Platform Setting > Threat Defense Policy > Syslog > Email Setup.

Adresse e-mail source : Saisissez l'adresse e-mail source qui apparaît sur tous les e-mails envoyés à partir du FTD et contenant les Syslogs.

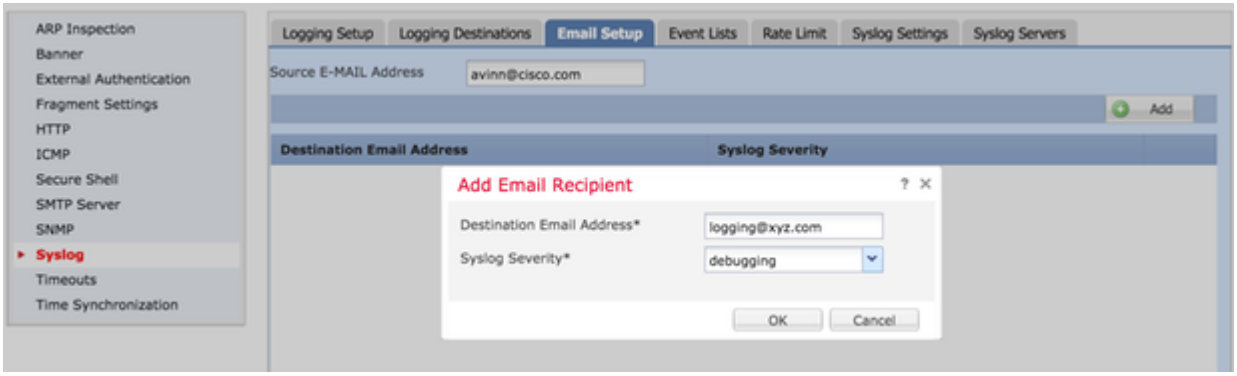


---

2. Pour configurer l'adresse e-mail de destination et la gravité Syslog, cliquez sur Add.

Adresse e-mail de destination : Saisissez l'adresse e-mail de destination à laquelle les messages Syslog sont envoyés.

Gravité Syslog : Sélectionnez la gravité Syslog dans la liste déroulante Gravité Syslog.



---

3. Cliquez sur OK pour enregistrer la configuration.

---

4. Cliquez sur Enregistrer pour enregistrer le paramètre de plate-forme. Choisissez Déployer, puis sélectionnez l'appliance FTD où vous souhaitez appliquer les modifications. Cliquez sur Déployer pour démarrer le déploiement du paramètre de plate-forme.

Vérifier

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vérifiez la configuration Syslog FTD dans l'interface de ligne de commande FTD. Connectez-vous à l'interface de gestion du FTD et exécutez la commande system support diagnostic-cli pour accéder à la console dans l'interface de ligne de commande de diagnostic.

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
```

```
logging flash-maximum-allocation 3076
logging permit-hostdown
```

Assurez-vous que le serveur Syslog est accessible à partir du FTD. Connectez-vous à l'interface de gestion FTD via SSH et vérifiez la connectivité avec la commande ping.

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

Vous pouvez effectuer une capture de paquets pour vérifier la connectivité entre le FTD et le serveur Syslog. Connectez-vous à l'interface de gestion FTD via SSH et exécutez la commande system support diagnostic-cli. Pour les commandes de capture de paquets, référez-vous à Exemple de configuration de capture de paquets ASA avec CLI et ASDM.

Assurez-vous que le déploiement de la stratégie est correctement appliqué.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.