

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](#)

[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
- Appareil de sécurité adaptatif (ASA)
- protocole Syslog

Composants utilisés

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

- 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
- FMC versions 6.0.1 et ultérieures

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.

Les journaux sont utiles à la fois pour le dépannage de routine et pour la gestion des incidents. Le périphérique FTD prend en charge la journalisation locale et externe.

La journalisation locale peut vous aider à résoudre les problèmes en direct. 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.

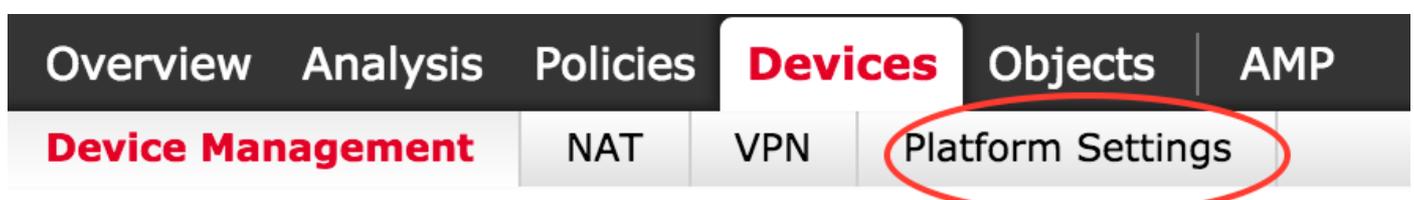
Pour la journalisation locale, l'appliance FTD prend en charge la console, l'option de mémoire tampon interne et la journalisation de session Secure Shell (SSH).

Pour la journalisation externe, l'appliance FTD prend en charge le serveur Syslog externe et le serveur de relais de messagerie.

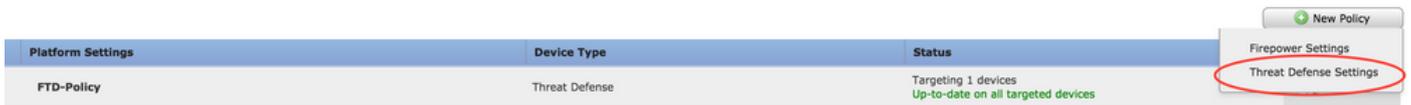
 Remarque : si un volume important de trafic traverse l'appliance, faites attention au type de journalisation/gravité/limitation de débit. Procédez ainsi afin de limiter le nombre de journaux, ce qui évite tout impact sur le pare-feu.

Configurer

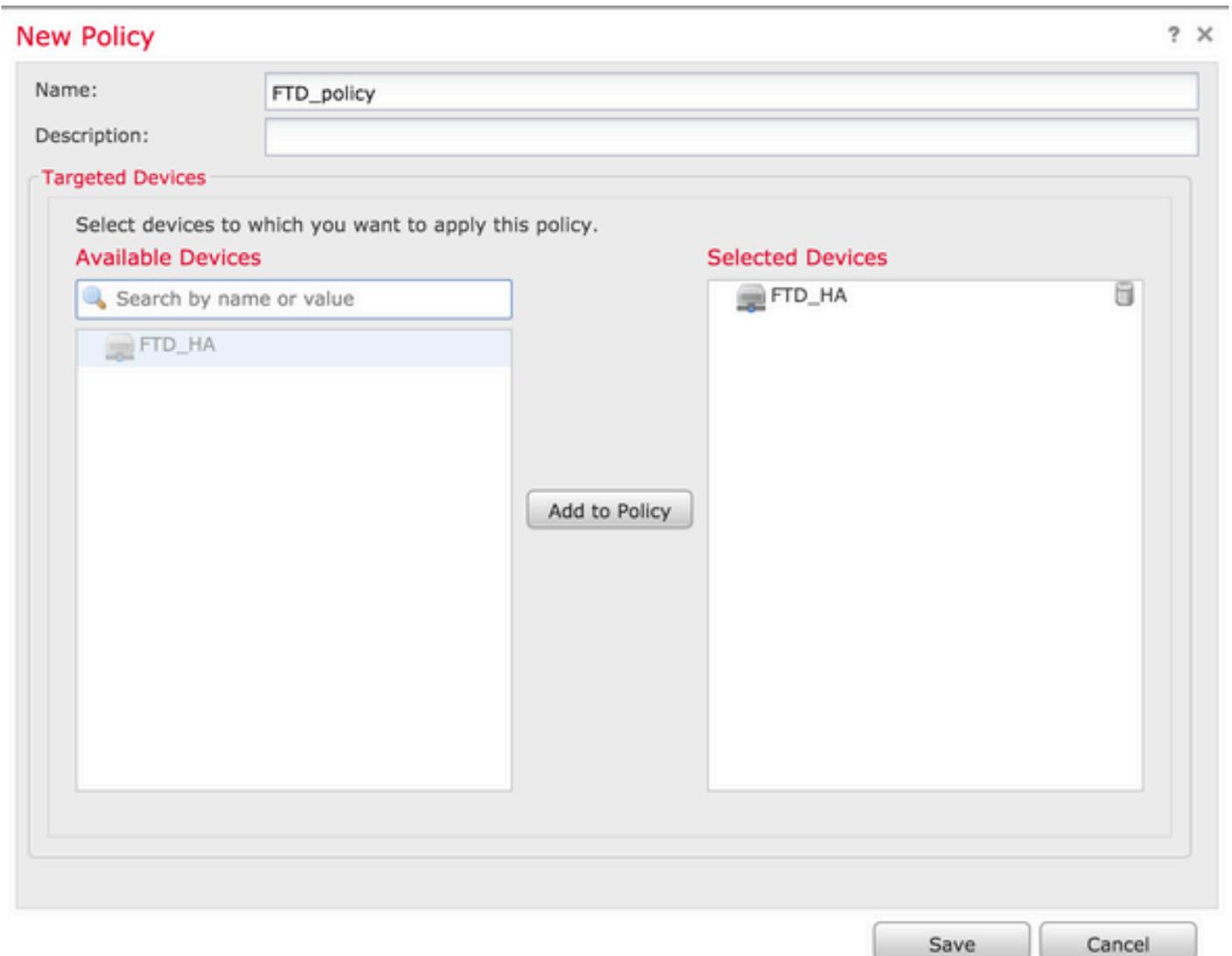
Toutes les configurations liées à la journalisation peuvent être configurées lorsque vous accédez à l' `Platform Settings` sous l'onglet `Devices` s'affiche. Choisir `Devices > Platform Settings` comme le montre cette image.



Cliquez sur l'icône représentant un crayon afin de modifier la stratégie existante ou cliquez sur **New Policy**, puis choisissez **Threat Defense Settings** afin de créer une nouvelle stratégie FTD comme illustré dans cette image.



Sélectionnez l'appliance FTD pour appliquer cette stratégie et cliquez sur **Save** comme le montre cette image.



Configuration de la configuration Syslog globale

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

Configuration de la journalisation

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

Choisir **Syslog > Logging Setup**.

Configuration de la journalisation de base

- **Enable Logging**: vérifiez la **Enable Logging** afin d'activer la journalisation. Cette option est obligatoire.
- **Enable Logging on the failover standby unit**: vérifiez la **Enable Logging on the failover standby unit** afin de configurer la journalisation sur le FTD de secours qui fait partie d'un cluster de haute disponibilité FTD.
- **Send syslogs in EMBLEM format**: vérifiez la **Send syslogs in EMBLEM format** afin d'activer le format de Syslog comme 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.
- **Send debug messages as syslogs**: vérifiez la **Send debug messages as syslogs** afin d'envoyer les journaux de débogage en tant que messages Syslog au serveur Syslog.
- **Memory size of the Internal Buffer**: 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.

Informations sur le serveur FTP (facultatif)

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

- **FTP Server Buffer Wrap**: vérifiez la **FTP Server Buffer Wrap** afin d'envoyer les données du journal de mémoire tampon au serveur FTP.
- **IP Address**: saisissez l'adresse IP du serveur FTP.
- **Username**: saisissez le nom d'utilisateur du serveur FTP.
- **Path**: saisissez le chemin d'accès au répertoire du serveur FTP.
- **Password**: saisissez le mot de passe du serveur FTP.
- **Confirm**: saisissez à nouveau le même mot de passe.

Taille de la mémoire Flash (facultatif)

Spécifiez la taille de la mémoire flash si vous souhaitez enregistrer les données du journal dans la mémoire flash une fois que la mémoire tampon interne est saturée.

- **Flash**: vérifiez la **Flash** afin d'envoyer les données du journal à la mémoire flash interne.
- **Maximum Flash to be used by Logging(KB)**: saisissez la taille maximale en Ko de mémoire flash pouvant être utilisée pour la journalisation.
- **Minimum free Space to be preserved(KB)**: saisissez la taille minimale en Ko de la mémoire flash qui doit être conservée.

Cliquer **Save** afin d'enregistrer le paramètre de la plate-forme. Sélectionnez la **Deploy**, choisissez l'appareil FTD auquel vous souhaitez appliquer les modifications, puis cliquez sur **Deploy** afin de commencer le déploiement du paramètre de la 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.

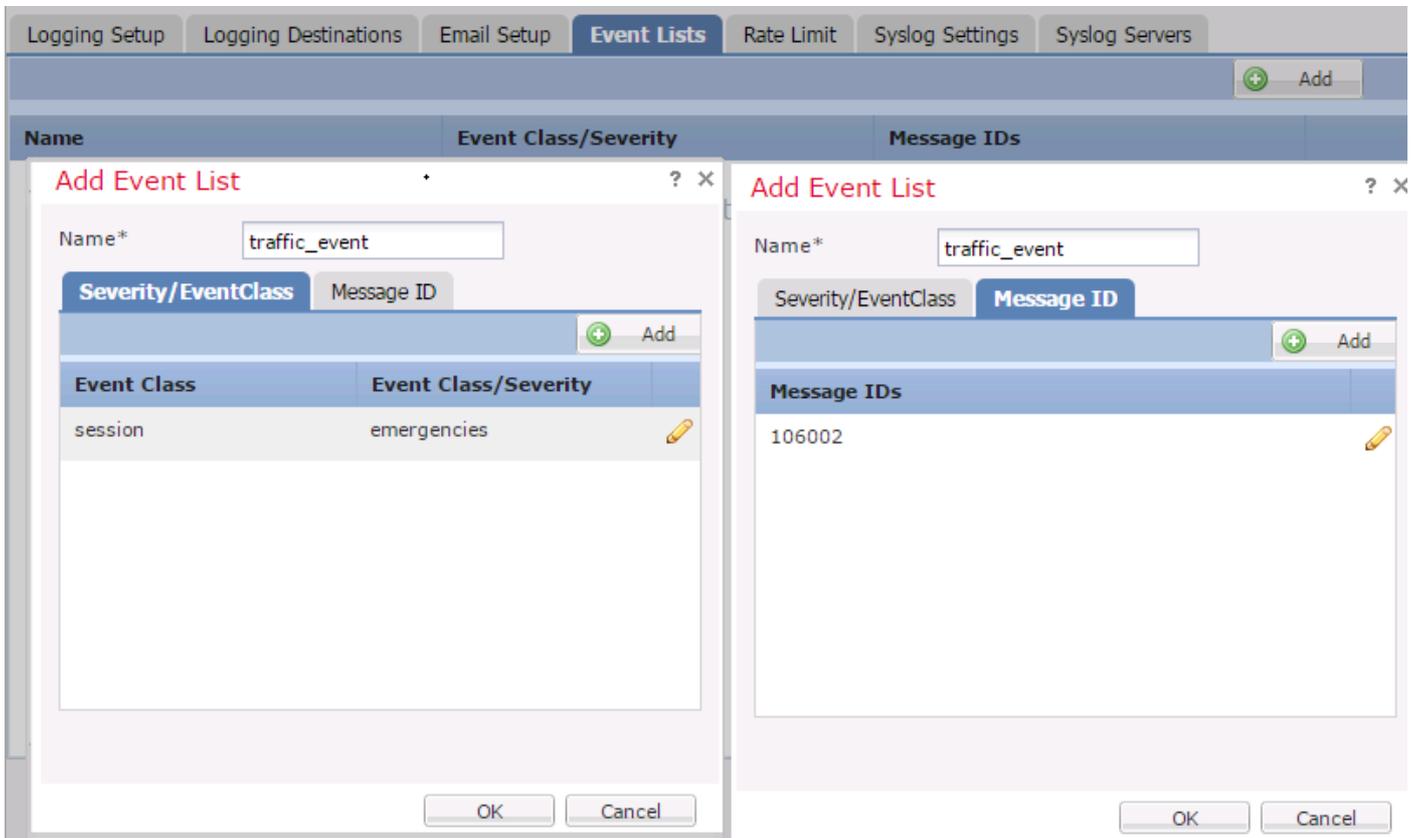
- Classe et gravité
- ID du message

Afin de 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:** saisissez le nom de la liste d'événements.
- **Severity/Event Class:** dans la section Severity/Event Class, cliquez sur **Add**.
- **Event Class:** 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 la session.

- Syslog Severity: choisissez le niveau de gravité dans la liste déroulante pour la classe d'événement choisie. La gravité peut être comprise entre 0 (urgence) et 7 (débogage).
- Message ID: si vous êtes intéressé par des données de journal spécifiques associées à un ID de message, cliquez sur Add afin de mettre un filtre basé sur l'ID du message.
- Message IDs: spécifiez l'ID de message au format individuel/ plage.



Cliquer **OK** afin d'enregistrer la configuration.

Cliquer **save** afin d'enregistrer le paramètre de la plate-forme. Choisir de **Deploy**, choisissez l'appareil FTD auquel vous souhaitez appliquer les modifications, puis cliquez sur **Deploy** afin de commencer le déploiement du paramètre de la 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.

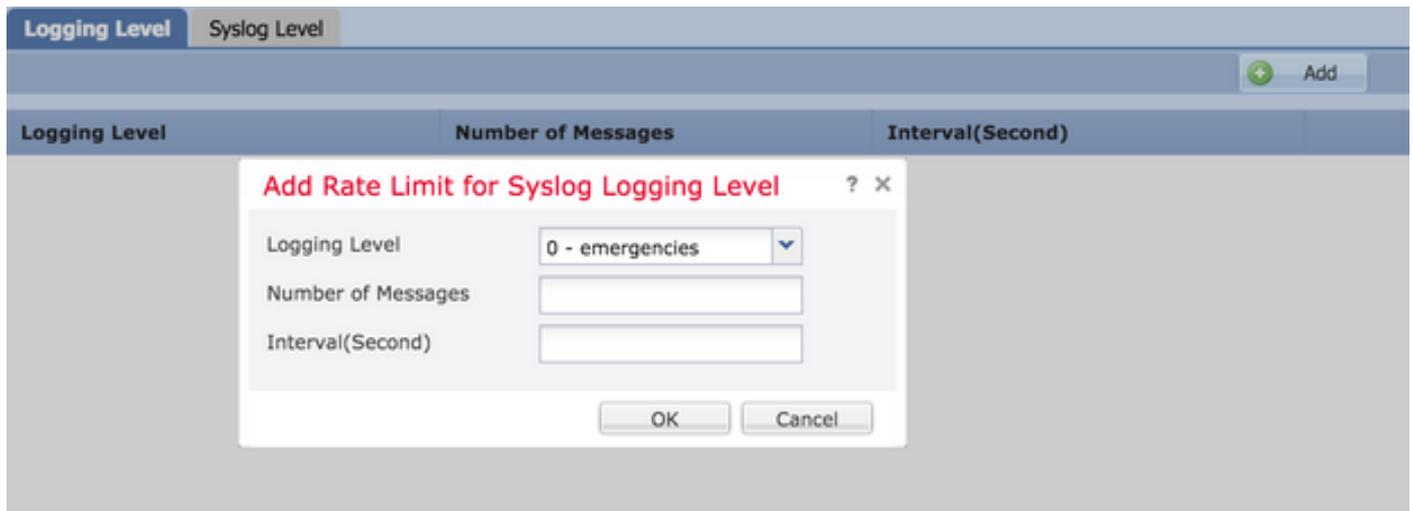
Afin de configurer des listes d'événements personnalisées, choisissez **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. Vous avez deux options selon lesquelles vous pouvez spécifier la limite de débit :

- Niveau de journalisation
- Niveaux Syslog

Afin d'activer la limite de débit basée sur le niveau de journalisation, choisissez **Logging Level** et cliquez sur **Add**.

- **Logging Level:** A partir des versions **Logging Level** , choisissez le niveau de journalisation pour lequel vous souhaitez effectuer la limitation de débit.
- **Number of Messages:** saisissez le nombre maximal de messages Syslog à recevoir au cours de l'intervalle spécifié.
- **Interval(Second):** en fonction du paramètre Nombre de messages configuré précédemment, saisissez l'intervalle de temps pendant lequel un ensemble fixe de messages Syslog peut être reçu.

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

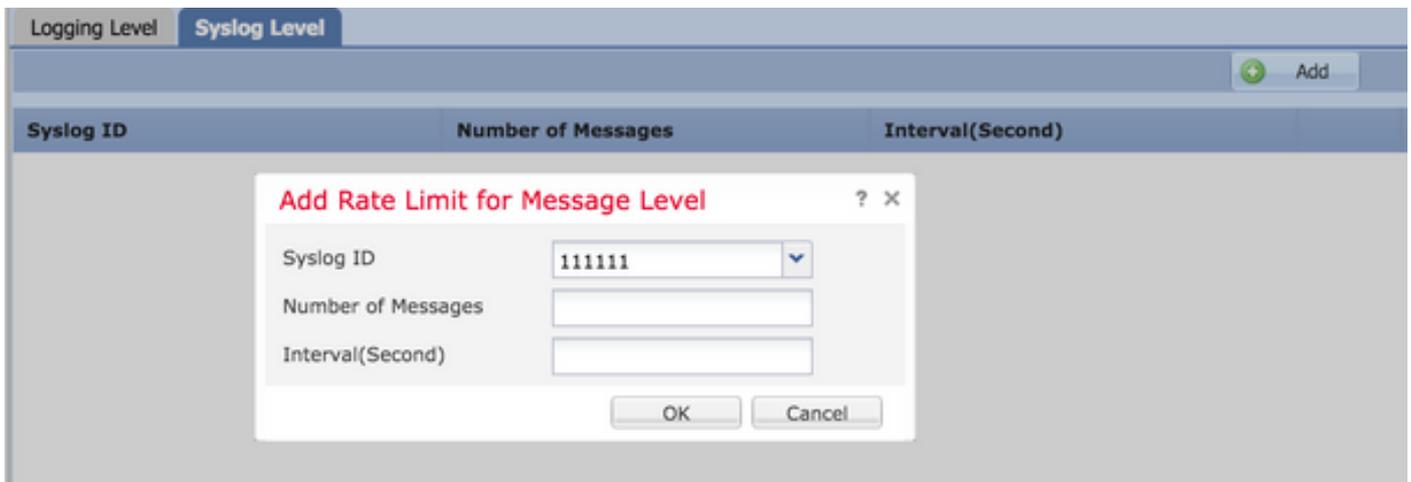


Cliquer **OK** afin d'enregistrer la configuration du niveau de journalisation.

Afin d'activer la limite de débit basée sur le niveau de journalisation, choisissez **Logging Level** et cliquez sur **Add**.

- **Syslog ID:** les ID Syslog sont utilisés pour identifier de manière unique les messages Syslog. A partir des versions **Syslog ID** dans la liste déroulante, sélectionnez l'ID Syslog.
- **Number of Messages:** saisissez le nombre maximal de messages Syslog à recevoir au cours de l'intervalle spécifié.
- **Interval(Second):** en fonction du paramètre Nombre de messages configuré précédemment, saisissez l'intervalle de temps pendant lequel un ensemble fixe de messages Syslog peut être reçu.

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



Cliquer **OK** afin d'enregistrer la configuration du niveau Syslog.

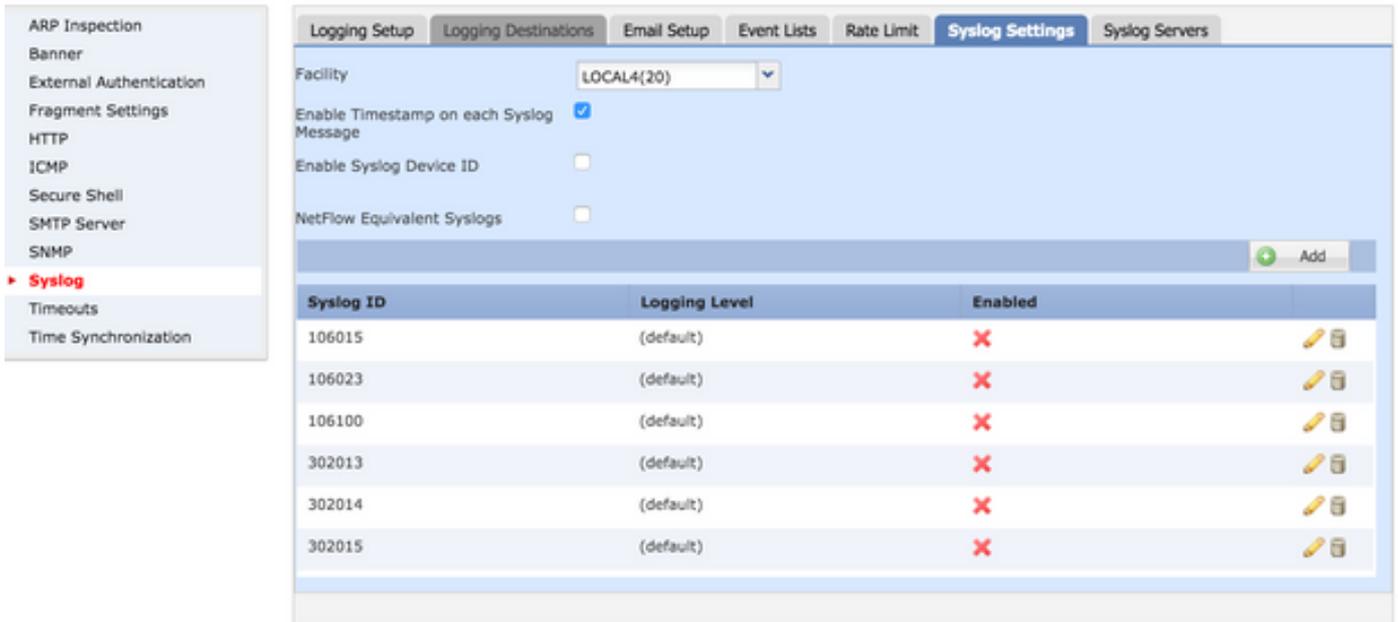
Cliquer **Save** afin d'enregistrer le paramètre de la plate-forme. Choisir de **Deploy**, choisissez l'appareil FTD auquel vous souhaitez appliquer les modifications, puis cliquez sur **Deploy** afin de commencer le déploiement du paramètre de la plate-forme.

Paramètres Syslog

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

Afin de configurer des listes d'événements personnalisées, choisissez **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings**.

- **Facility**: un code de fonction est utilisé pour spécifier le type de programme qui enregistre le message. Les messages avec des fonctionnalités différentes peuvent être traités différemment. A partir des versions **Facility** dans la liste déroulante, sélectionnez la valeur de l'installation.
- **Enable Timestamp on each Syslog Message**: vérifiez la **Enable Timestamp on each Syslog Message** afin d'inclure l'horodatage dans les messages Syslog.
- **Enable Syslog Device ID**: vérifiez la **Enable Syslog Device ID** afin d'inclure un ID de périphérique dans les messages Syslog au format non EMBLEM.
- **Netflow Equivalent Syslogs**: vérifiez la **Netflow Equivalent Syslogs** afin d'envoyer des Syslogs équivalents à NetFlow. Elle peut affecter les performances de l'appliance.
- **Add Specific Syslog ID** : pour spécifier l'ID Syslog supplémentaire, cliquez sur **Add** et précisez le **Syslog ID/ Logging Level** de l'Aide.



Cliquer **Save** afin d'enregistrer le paramètre de la plate-forme. Choisir de **Deploy**, choisissez l'appareil FTD auquel vous souhaitez appliquer les modifications, puis cliquez sur **Deploy** afin de commencer le déploiement du paramètre de la plate-forme.

Configurer la journalisation locale

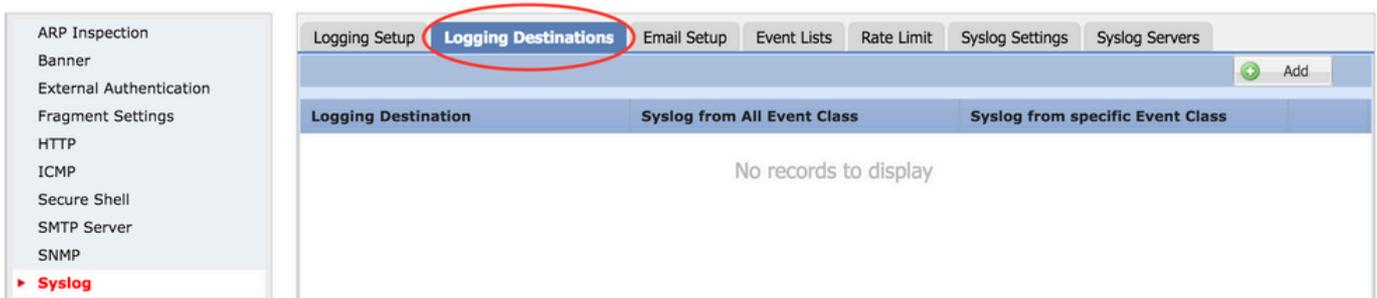
La section Logging Destination peut être utilisée afin de configurer la journalisation vers des destinations spécifiques.

Les destinations de journalisation internes disponibles sont les suivantes :

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

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

Étape 1. Choisir **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Logging Destinations**.



Étape 2. Cliquer **Add** afin d'ajouter un filtre de journalisation pour un logging destination.

Logging Destination : sélectionnez la destination de journalisation requise dans le champ **Logging Destination** liste déroulante en tant que mémoire tampon interne, console ou sessions SSH.

Classe d'événement : à partir de **Event Class** dans la liste déroulante, sélectionnez une classe Event. Comme décrit précédemment, les classes d'événements sont un ensemble de Syslog qui représentent les mêmes fonctionnalités. Les classes d'événements peuvent être sélectionnées de ces manières :

- **Filter on Severity**: les classes d'événements filtrent en fonction de la gravité des Syslogs.
- **User Event List**: les administrateurs peuvent créer des listes d'événements spécifiques (décrites précédemment) avec leurs propres classes d'événements personnalisées et les référencer dans cette section.
- **Disable Logging**: utilisez cette option afin de désactiver la journalisation pour la destination de journalisation et le niveau de journalisation choisis.

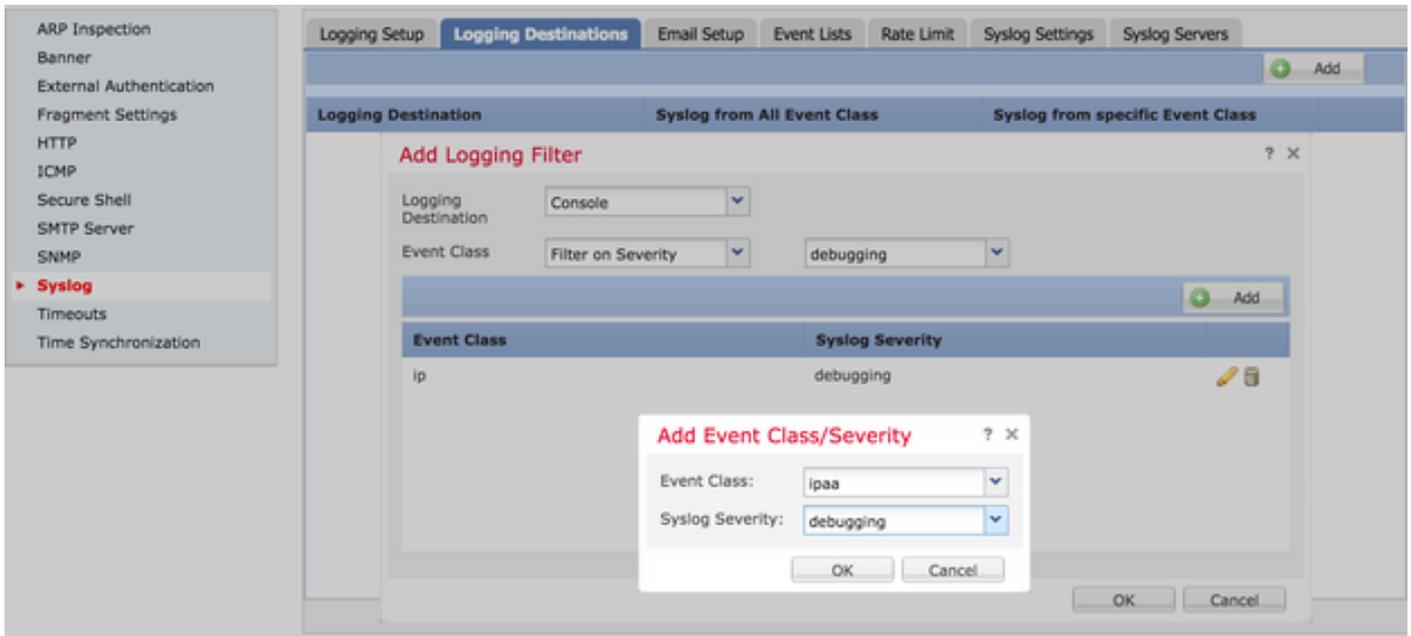
Logging Level : choisissez le niveau de journalisation dans la liste déroulante. Le niveau de journalisation est compris entre 0 (Urgences) et 7 (Débogage).

The screenshot shows the 'Add Logging Filter' dialog box. It features a title bar with the text 'Add Logging Filter' in red. Below the title bar, there are several input fields and a table. The 'Logging Destination' field is a dropdown menu with 'Internal Buffer' selected. The 'Event Class' field is a dropdown menu with 'Filter on Severity' selected, and a sub-menu is open showing three options: 'Filter on Severity', 'Use Event List', and 'Disable Logging'. To the right of the 'Event Class' field is a text field containing 'emergencies' with a dropdown arrow. A green '+ Add' button is located to the right of the text field. Below these fields is a table with two columns: 'Event Class' and 'Syslog Severity'. The table is currently empty, with the text 'No records to display' centered below it. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Étape 3. Afin d'ajouter une classe Event distincte à ce filtre de journalisation, cliquez sur **Add**.

Event Class: sélectionnez la classe d'événement dans la liste déroulante **Event Class** liste déroulante.

Syslog Severity: sélectionnez la gravité Syslog dans la liste déroulante **Syslog Severity** liste déroulante.



Cliquer **OK** une fois que le filtre est configuré pour ajouter le filtre pour une destination de journalisation spécifique.

Cliquer **save** afin d'enregistrer le paramètre de la plate-forme. Choisir **Deploy**, choisissez l'appareil FTD auquel vous souhaitez appliquer les modifications, puis cliquez sur **Deploy** afin de commencer le déploiement du paramètre de plate-forme.

Configuration de la journalisation externe

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

FTD prend en charge ces types de journalisation externe.

- Syslog Server : envoie les journaux au serveur Syslog distant.
- Interruption SNMP : envoie les déconnexions en tant qu'interruption SNMP.
- E-Mail : envoie les 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.

Étape 1. Choisir **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers**.

Étape 2. Configurez le paramètre relatif au serveur Syslog.

- Autoriser le trafic utilisateur à passer lorsque le serveur Syslog TCP est en panne : 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. Vérifiez la **Allow user traffic to pass when TCP syslog server is down** afin d'autoriser le trafic à traverser l'interface lorsque le serveur Syslog est arrêté.
- Taille de la file d'attente des 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 la valeur minimale est 1 message. Si 0 est spécifié dans cette option, la taille de la file d'attente est considérée comme illimitée.

The screenshot shows the 'Syslog Servers' configuration page. At the top, there are tabs for 'Logging Setup', 'Logging Destinations', 'Email Setup', 'Event Lists', 'Rate Limit', 'Syslog Settings', and 'Syslog Servers'. Below the tabs, there is a checkbox labeled 'Allow user traffic to pass when TCP syslog server is down' which is currently unchecked. Below this, there is a text input field for 'Message Queue Size(messages)*' with the value '512' entered. To the right of the input field, there is a note: '(0 - 8192 messages). Use 0 to indicate unlimited Queue Size'. Below the input field, there is a green '+ Add' button. Below the 'Add' button, there is a table with the following columns: 'Interface', 'IP Address', 'Protocol', 'Port', and 'EMBLEM'. The table is currently empty, and the text 'No records to display' is centered below the table.

Étape 3. Pour ajouter des serveurs Syslog distants, cliquez sur **Add**.

IP Address: À partir des versions **IP Address**, choisissez un objet réseau dans lequel les serveurs Syslog sont répertoriés. Si vous n'avez pas créé d'objet réseau, cliquez sur l'icône plus (+) afin de créer un nouvel objet.

Protocol: cliquez sur le bouton **TCP** ou **UDP** pour la communication Syslog.

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

Log Messages in Cisco EMBLEM format(UDP only): cliquez sur le bouton **Log Messages in Cisco EMBLEM format (UDP only)** afin d'activer cette option s'il est nécessaire de consigner les messages au format EMBLEM de Cisco. Ceci s'applique uniquement aux Syslog basés sur UDP.

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

Add Syslog Server

IP Address*

Protocol TCP UDP

Port (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only)

Available Zones

Selected Zones/Interfaces

outside

Cliquer **OK** et **save** afin d'enregistrer la configuration.

Cliquer **save** afin d'enregistrer le paramètre de la plate-forme. Choisir **Deploy**, choisissez l'appareil FTD auquel vous souhaitez appliquer les modifications, puis cliquez sur **Deploy** afin de commencer le déploiement du paramètre de la plate-forme.

Configuration du courrier électronique pour la journalisation

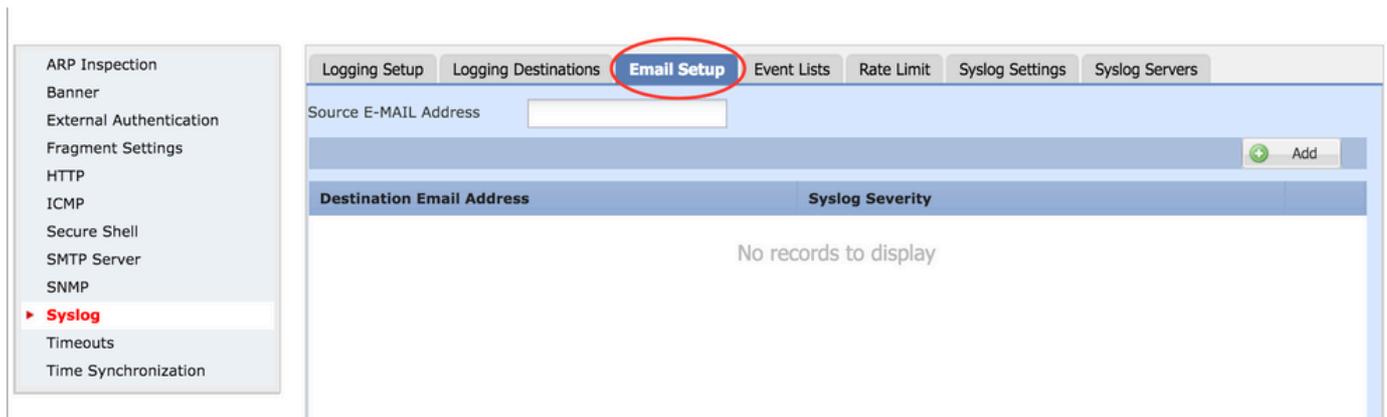
FTD vous permet d'envoyer le Syslog à une adresse e-mail spécifique. Le courrier électronique ne peut être utilisé comme destination de journalisation que si un serveur de relais de messagerie a déjà été configuré.

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

Étape 1. Choisir **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Email Setup**.

Source E-MAIL Address: saisissez l'adresse e-mail source qui apparaît sur tous les e-mails envoyés à

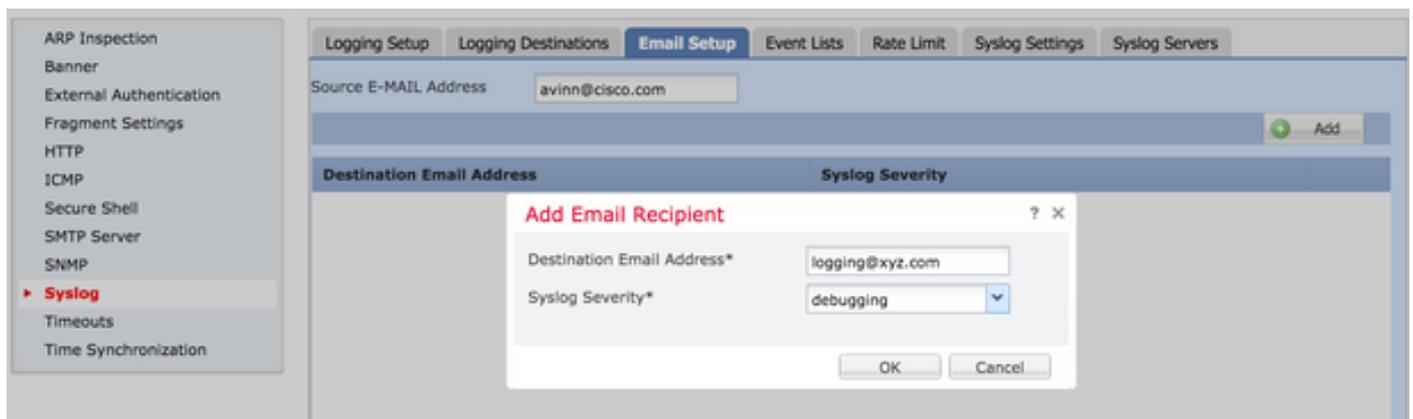
partir du FTD qui contiennent les Syslogs.



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

Destination Email Address: saisissez l'adresse e-mail de destination à laquelle les messages Syslog sont envoyés.

Syslog Severity: sélectionnez la gravité Syslog dans la liste déroulante Syslog Severity liste déroulante.



Cliquer **OK** afin d'enregistrer la configuration.

Cliquer **save** afin d'enregistrer le paramètre de la plate-forme. Choisir **Deploy**, choisissez l'appareil FTD auquel vous souhaitez appliquer les modifications, puis cliquez sur **Deploy** afin de commencer le déploiement du paramètre de la 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, puis saisissez le `system support diagnostic-cli` afin

d'accéder à 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 le `ping erasecat4000_flash:`.

```
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 afin de vérifier la connectivité entre le FTD et le serveur Syslog. Connectez-vous à l'interface de gestion FTD via SSH et entrez 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

- [Guide de démarrage rapide de Cisco Firepower Threat Defense pour ASA](#)
- [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.