Implémenter les paramètres de plate-forme pour le dépannage VPN

Table des matières

Introduction

Ce document décrit comment organiser et identifier facilement les journaux de débogage VPN à l'aide de Secure Firewall Management Center et de Secure Firewall Threat Defense.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protection pare-feu contre les menaces (FTD)
- Centre de gestion du pare-feu sécurisé (FMC)

- Compréhension de base de la navigation dans l'interface utilisateur graphique FMC et l'interface de ligne de commande FTD
- Affectation de stratégie existante pour les paramètres de plateforme

Composants utilisés

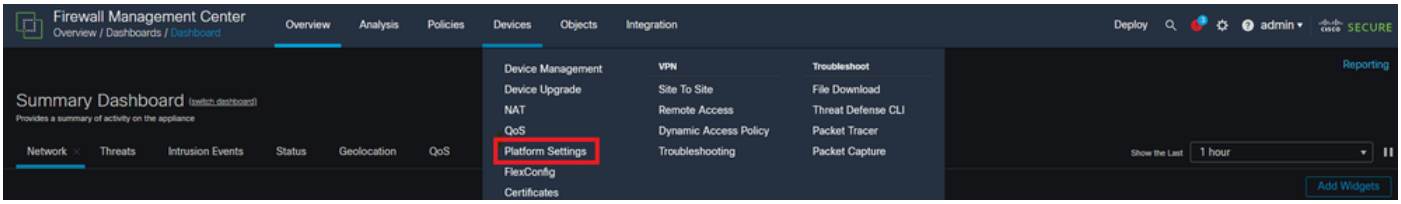
Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles suivantes :

- Firewall Management Center version 7.3
- Protection pare-feu version 7.3

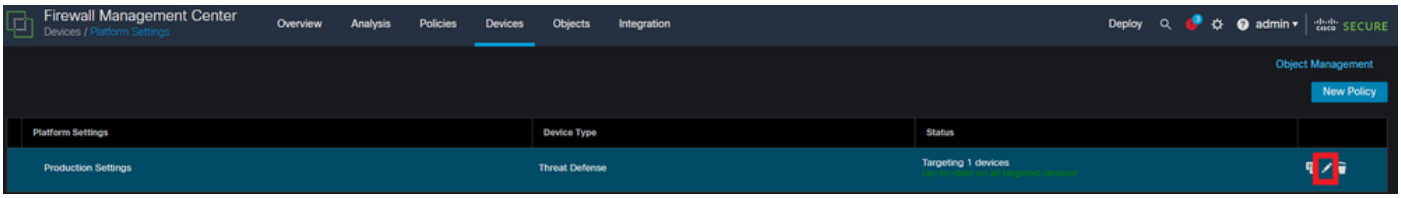
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Centre de gestion des pare-feu

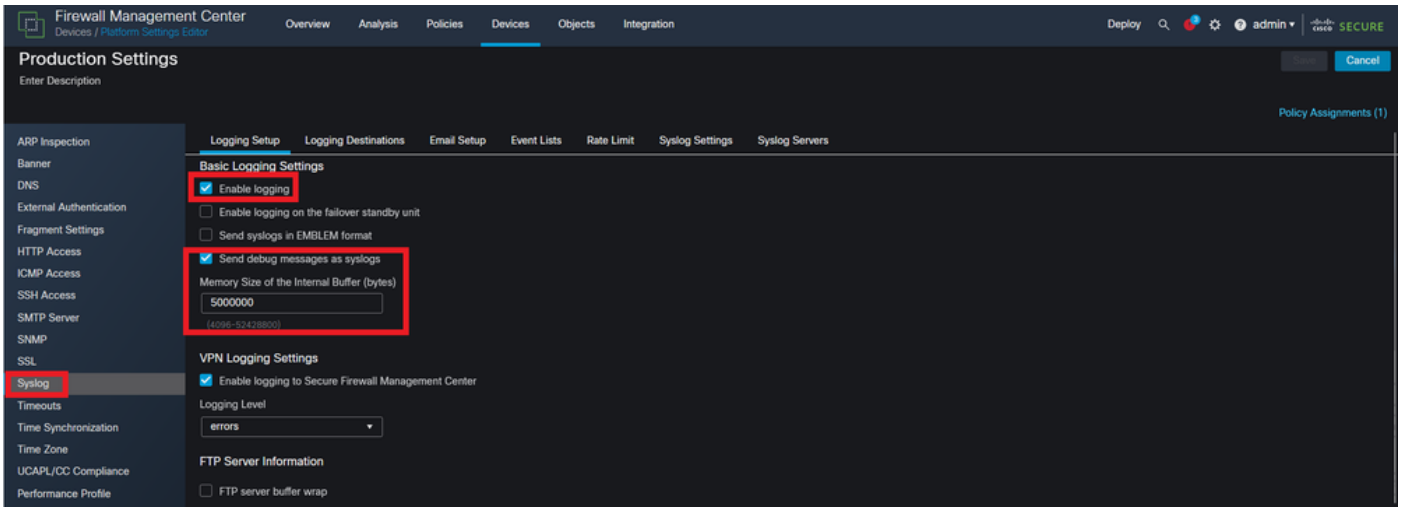
Accédez à Devices > Platform Settings.



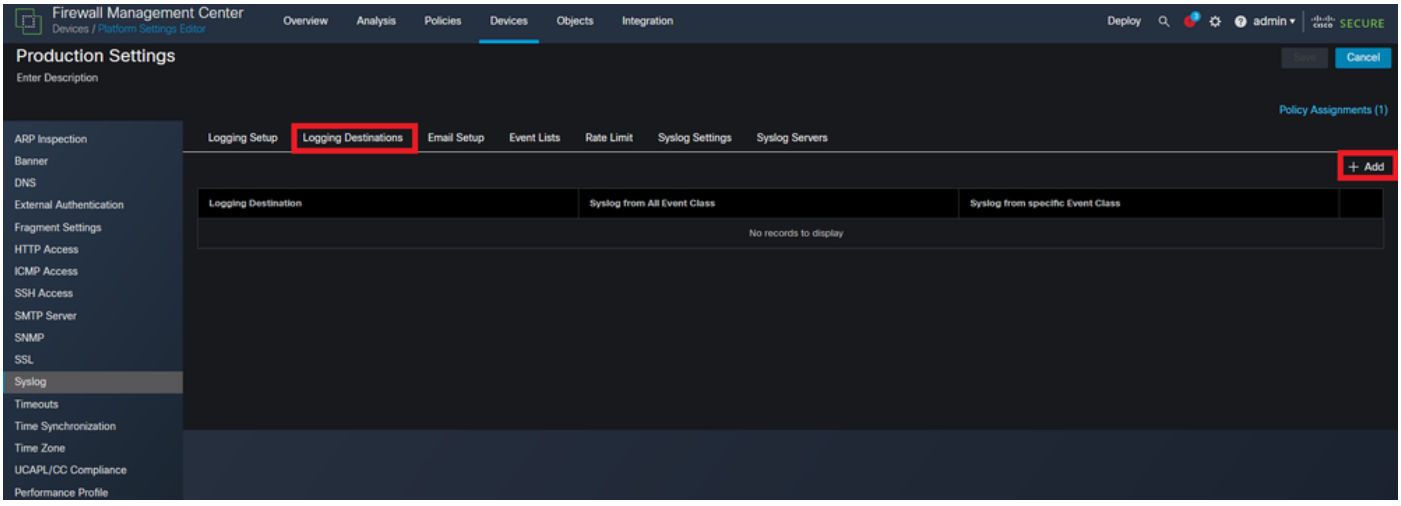
Cliquez sur l' **pencil**icône située entre copy et supprimer icon.



Accédez à Syslogdans la colonne de gauche des options et vérifiez que **Enable Logging**, et **Send debug messages as syslog** sont activés. Assurez-vous également que le Memory Size of the Internal Buffer est défini avec une valeur appropriée pour le dépannage.

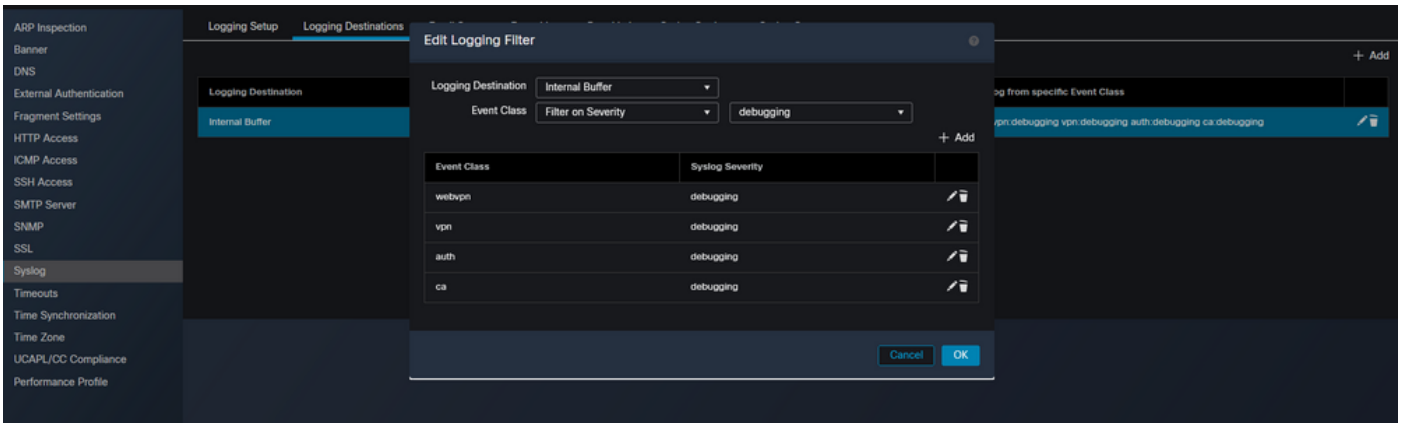


Cliquez **Logging Destinations** sur, puis sur **+Add**.



Dans cette section, la destination de journalisation est une préférence de l'administrateur et **Internal**

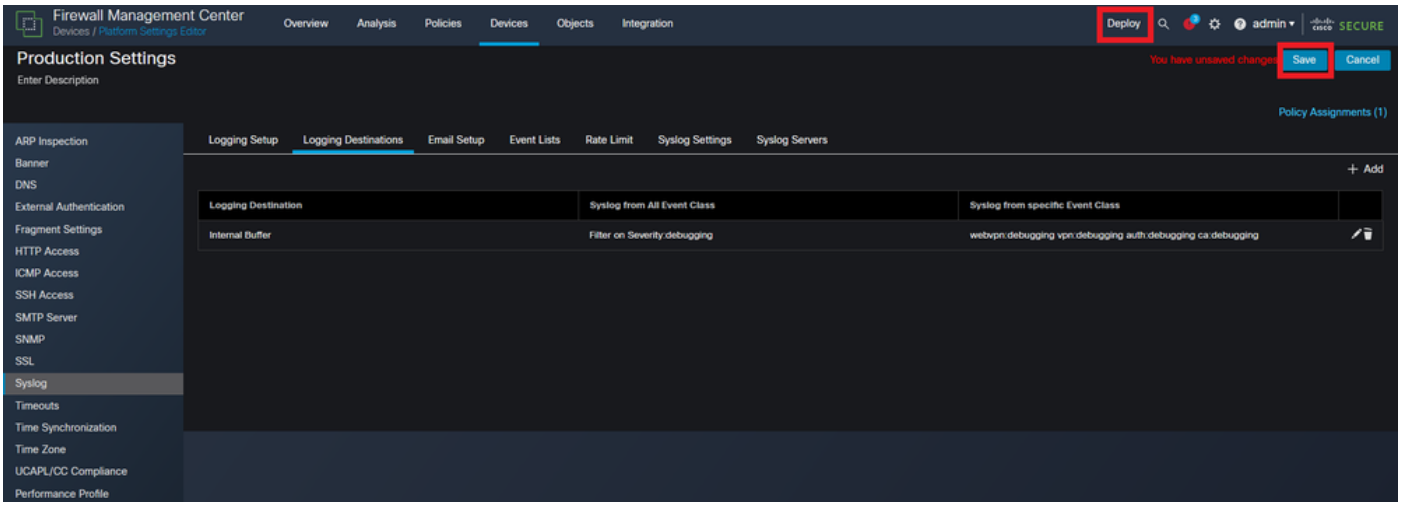
Buffer est utilisée. Remplacez **Event Class** par **Filter on Severity and debugging**. Une fois cette opération terminée, cliquez sur +Add et choisissez webvpn, vpn, auth, et catous avec la gravité Syslog debugging. Cette étape permet à l'administrateur de filtrer ces sorties de débogage vers un message syslog spécifique de 711001. Ces sorties peuvent être modifiées en fonction du type de dépannage. Cependant, ceux choisis dans cet exemple couvrent les problèmes de site à site, d'accès à distance et de VPN AAA les plus courants.



Créez des classes d'événements et des filtres pour les débogages.

Avertissement : Le niveau de journalisation de la mémoire tampon passe alors au débogage et consigne les événements de débogage pour les classes spécifiées dans la mémoire tampon interne. Il est recommandé d'utiliser cette méthode de journalisation à des fins de dépannage, et non pour une utilisation à long terme.

Choose Save en haut à droite, puis Deployla configuration change.



Protection pare-feu

Accédez à l'interface de ligne de commande FTD et exécutez la commandeshow logging setting. Les paramètres indiqués ici reflètent les modifications apportées au FMC. Assurez-vous que la journalisation debug-trace est activée et que la journalisation de la mémoire tampon correspond

aux classes et au niveau de journalisation spécifiés.

```
FTD72# show logging setting
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled (persistent)
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, class auth vpn webvpn ca, 362685 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC_logging: list MANAGER_VPN_EVENT_LIST, class auth vpn webvpn ca, 27 messages logged
```

Affichez les paramètres de journalisation dans l'interface de ligne de commande FTD.

Enfin, appliquez un débogage afin de vous assurer que les journaux sont redirigés vers syslog:711001. Dans cet exemple, `debug webvpn anyconnect 255` est appliqué. Cela déclenche une notification de journalisation debug-trace, indiquant à l'administrateur que ces débogages sont redirigés. Afin d'afficher ces débogages, émettez la commande `show log | in 711001`. Cet ID Syslog ne contient désormais que les débogages VPN appropriés tels qu'appliqués par l'administrateur. Les journaux existants peuvent être effacés avec une mémoire tampon de journalisation claire.

```
FTD72# debug webvpn anyconnect 255
INFO: 'logging debug-trace' is enabled. All debug messages are currently being redirected to syslog:711001 and will not appear in any monitor session
INFO: debug webvpn anyconnect enabled at level 255.
FTD72# show log | in 711001
```

Affiche tous les débogages VPN en cours de redirection vers syslog 711001.

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.