Configurer la défense pare-feu sécurisée pour envoyer des événements d'intrusion à un serveur Syslog à l'aide de FDM

Table des matières

Problème

L'objectif est de configurer le dispositif Secure Firewall Threat Defense (FTD) pour qu'il envoie des événements d'intrusion à un serveur Syslog via Cisco Secure Firewall Device Manager (FDM).

Environnement

FTD version 7.7.10, géré par FDM. Cette procédure s'applique également aux autres versions.

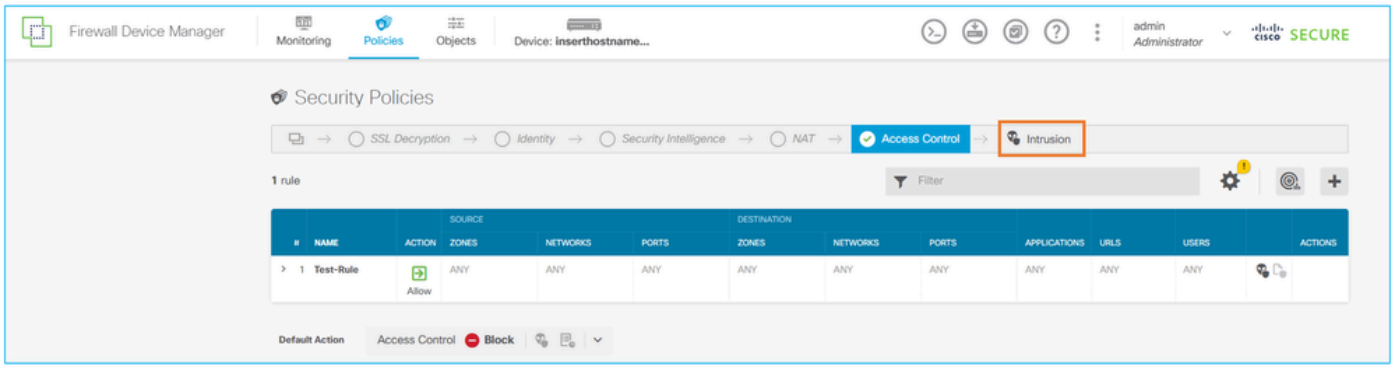
Résolution

Suivez les étapes pour configurer le FTD pour envoyer des événements d'intrusion à un serveur syslog via FDM.

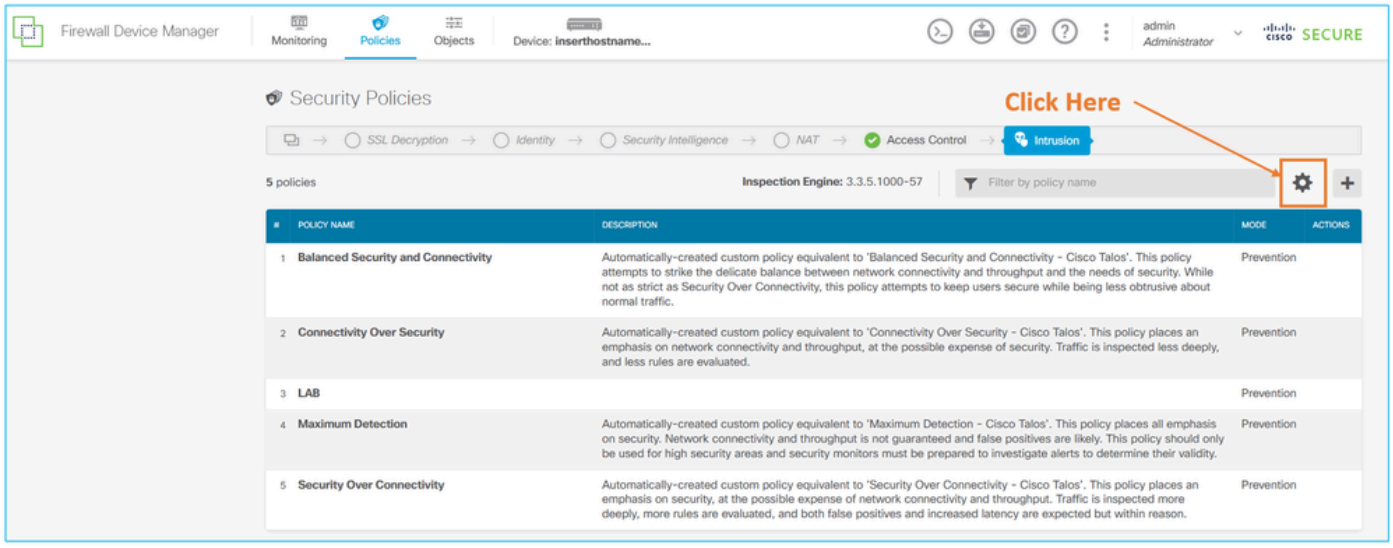
Étape 1. Dans l'interface utilisateur graphique de FDM, accédez à l'onglet Policies.



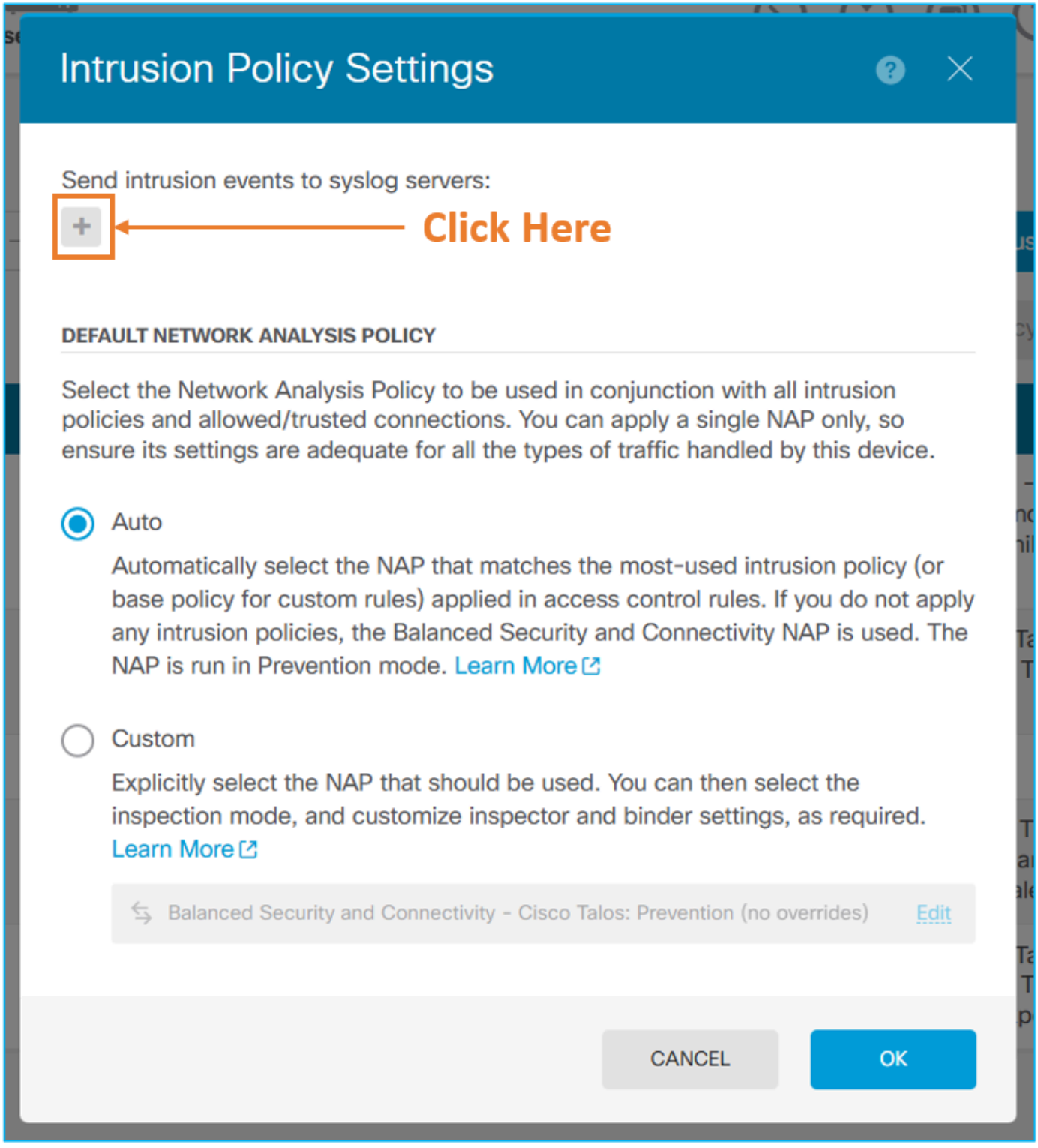
Étape 2. Cliquez sur l'onglet Intrusion.



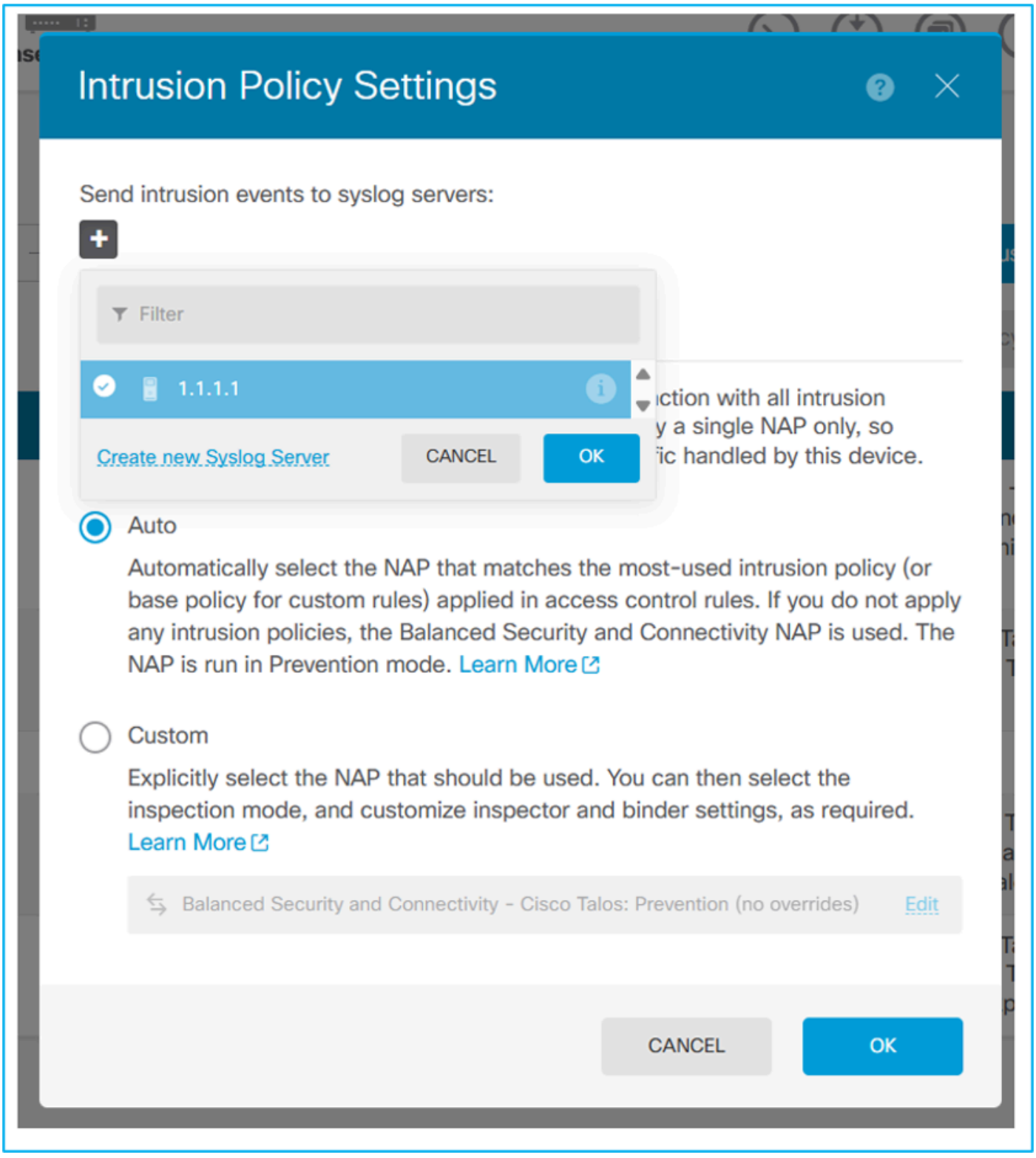
Étape 3. Cliquez sur le bouton Paramètres.



Étape 4. Dans la section Send Intrusion Events to Syslog Servers, cliquez sur le bouton plus (+).



Étape 5. Sélectionnez l'objet serveur Syslog, puis cliquez sur OK.



Étape 6: Déployez les modifications de configuration sur le pare-feu.

Motif

Pour configurer l'envoi des événements d'intrusion à un serveur Syslog, sélectionnez le serveur Syslog dans les paramètres de stratégie d'intrusion.

Autres informations utiles

Guide de configuration de Cisco Secure Firewall Device Manager

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.