Contenu

Introduction

Ce document décrit comment activer le préprocesseur intégré de normalisation et vous aide à comprendre la différence et l'incidence de deux options avancées de la normalisation intégrée.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du système de puissance de feu de Cisco et renifliez.

Composants utilisés

Les informations dans ce document sont basées sur les appliances de centre et de puissance de feu de Gestion de Cisco FireSIGHT.

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.

Informations générales

Un préprocesseur intégré de normalisation normalise le trafic afin de réduire l'occasion qu'un attaquant peut éluder la détection utilisant des déploiements intégrés. La normalisation se produit juste après le paquet décodant et avant tous les autres préprocesseurs, et procède à partir des couches intérieures du paquet à l'extérieur. La normalisation intégrée ne génère pas des événements, mais elle prépare des paquets à l'usage d'autres préprocesseurs.

Quand vous appliquez une stratégie d'intrusion avec le préprocesseur intégré de normalisation activé, le périphérique de puissance de feu teste ces deux conditions afin de s'assurer que vous

utilisez un déploiement intégré :

- Pour des versions 5.4 et ultérieures, le *mode intégré* est activé dans la stratégie d'analyse de réseau (PETIT SOMME), et la *baisse quand l'en ligne* est également configuré dans la stratégie d'intrusion si la stratégie d'intrusion est placée pour relâcher le trafic. Pour des versions 5.3 et antérieures, la *baisse quand l'*option *intégrée* est activée dans la stratégie d'intrusion.

- La stratégie est appliquée avec failopen) à un positionnement intégré (ou en ligne d'interface.

Par conséquent, en plus de l'activation et de la configuration du préprocesseur intégré de normalisation, vous devez également s'assurer que ces exigences soient répondues, ou le préprocesseur ne normalisera pas le trafic :

- Votre stratégie doit être placée pour relâcher le trafic dans des déploiements intégrés.

- Vous devez s'appliquer votre stratégie à un positionnement d'en ligne.

Normalisation d'en ligne d'enable

Cette section décrit comment activer la normalisation intégrée pour des versions 5.4 et ultérieures, et également pour des versions 5.3 et antérieures.

Normalisation intégrée d'enable dans les versions 5.4 et ultérieures

La plupart des configurations de préprocesseur sont configurées dans le PETIT SOMME pour des versions 5.4 et ultérieures. Terminez-vous ces étapes afin d'activer la normalisation intégrée dans le PETIT SOMME :

1. Ouvrez une session au Web UI de votre centre de Gestion de FireSIGHT.

2. Naviguez vers les **stratégies** > le **contrôle d'accès**.

3. Cliquez sur la **stratégie d'analyse réseau** près de la zone en haut à droite de la page.

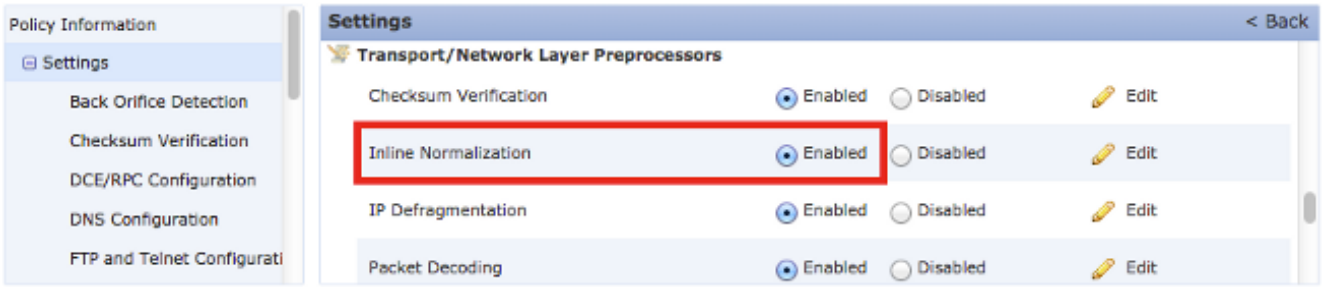
4. Sélectionnez une *stratégie d'analyse réseau* que vous voulez appliquer à votre périphérique géré.

5. Cliquez sur l'icône de *crayon* afin de commencer l'éditer, et la page de *stratégie d'éditer* paraît.

6. Cliquez sur les **configurations** du côté gauche de l'écran, et la *page Settings* paraît.

7. Localisez l'option **intégrée de normalisation** dans la région de *transport/de préprocesseur couche réseau*.

8. Sélectionnez la case d'option **activée** afin d'activer cette caractéristique :



Le PETIT SOMME avec la normalisation intégrée doit être ajouté à votre stratégie de contrôle d'accès pour que la normalisation intégrée se produise. Le PETIT SOMME peut être ajouté par l'*onglet Avancé de* stratégie de contrôle d'accès :

La stratégie de contrôle d'accès doit alors être appliquée au périphérique examinant.

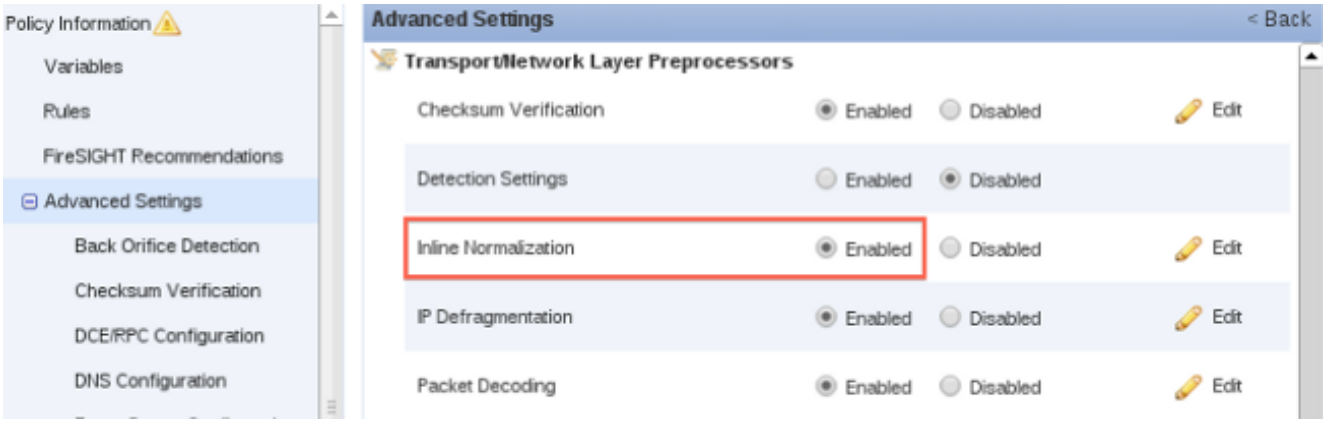
> Remarque: Pour la version 5.4 ou ultérieures, vous pouvez activer la normalisation intégrée pour certain trafic et la désactiver pour l'autre trafic. Si vous voulez l'activer pour le trafic spécifique, ajouter une *règle d'analyse réseau* et placer les critères et la stratégie du trafic à celle qui a la normalisation intégrée activée. Si vous voulez l'activer globalement, alors placez la *stratégie par défaut d'analyse réseau à* celle qui a la normalisation intégrée activée.

Normalisation intégrée d'enable dans les versions 5.3 et antérieures

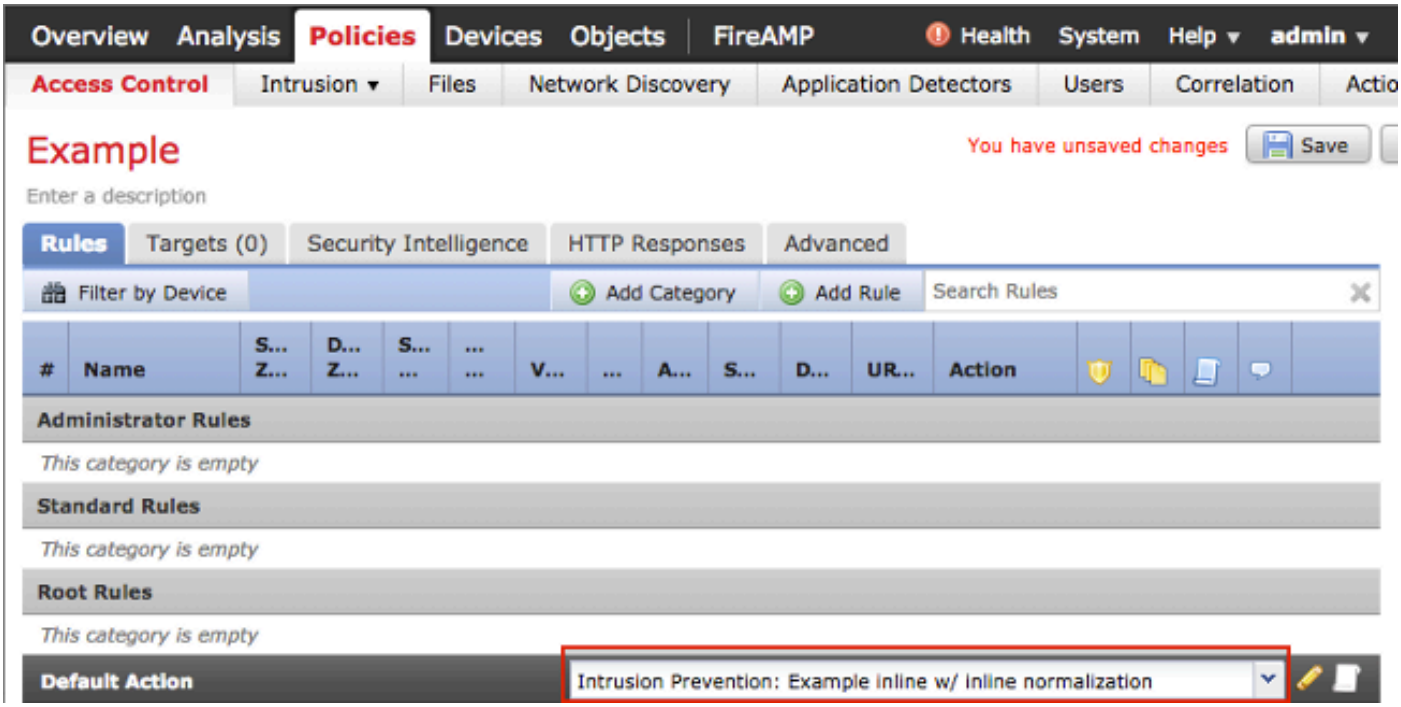
Terminez-vous ces étapes afin d'activer la normalisation intégrée dans une stratégie d'intrusion :

1. Ouvrez une session au Web UI de votre centre de Gestion de FireSIGHT.
2. Naviguez vers des **stratégies > l'intrusion > des stratégies d'intrusion**.
3. Sélectionnez une *stratégie d'intrusion* que vous voulez appliquer à votre périphérique géré.
4. Cliquez sur l'icône de *crayon* afin de commencer l'éditer, et la page de *stratégie d'éditer* paraît.
5. Cliquez sur les **paramètres avancés**, et la page de ***paramètres avancés*** paraît.
6. Localisez l'option **intégrée de normalisation** dans la région de *transport/de préprocesseur couche réseau*.

7. Sélectionnez la case d'option **activée** afin d'activer cette caractéristique :



Une fois que la stratégie d'intrusion est configurée pour la normalisation intégrée, il doit ajouter comme action par défaut dans la stratégie de contrôle d'accès :



La stratégie de contrôle d'accès doit alors être appliquée au périphérique examinant.

Vous pouvez configurer le préprocesseur intégré de normalisation afin de normaliser l'ipv4, l'IPv6, la version 4 (ICMPv4) d'Internet Control Message Protocol, l'ICMPv6, et le trafic TCP dans n'importe quelle situation. La normalisation de chaque protocole se produit automatiquement quand cette normalisation de protocole est activée.

Inspection de l'enable POST-ACK et inspection Pré-ACK

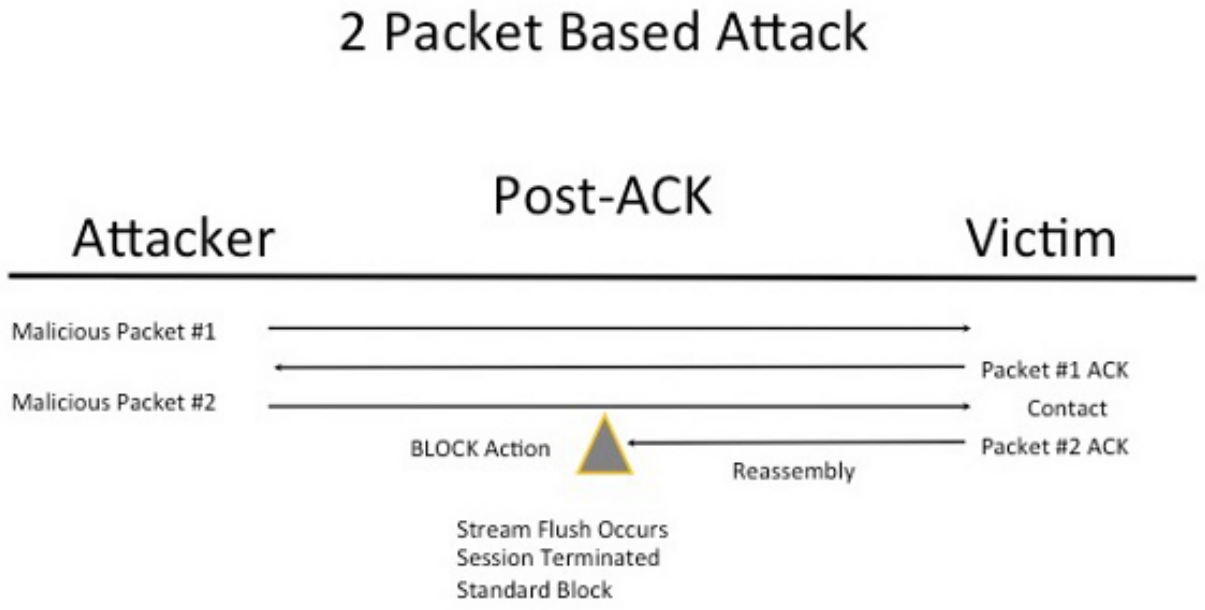
Après que vous activiez le préprocesseur intégré de normalisation, vous pouvez éditer les configurations afin d'activer l'option de *charge utile de TCP de normalisation*. Cette option dans le préprocesseur de normalisation d'en ligne commute entre deux modes différents d'inspection :

- Accusé de réception de courrier (POST-ACK)

- Pré accusé de réception (Pré-ACK)

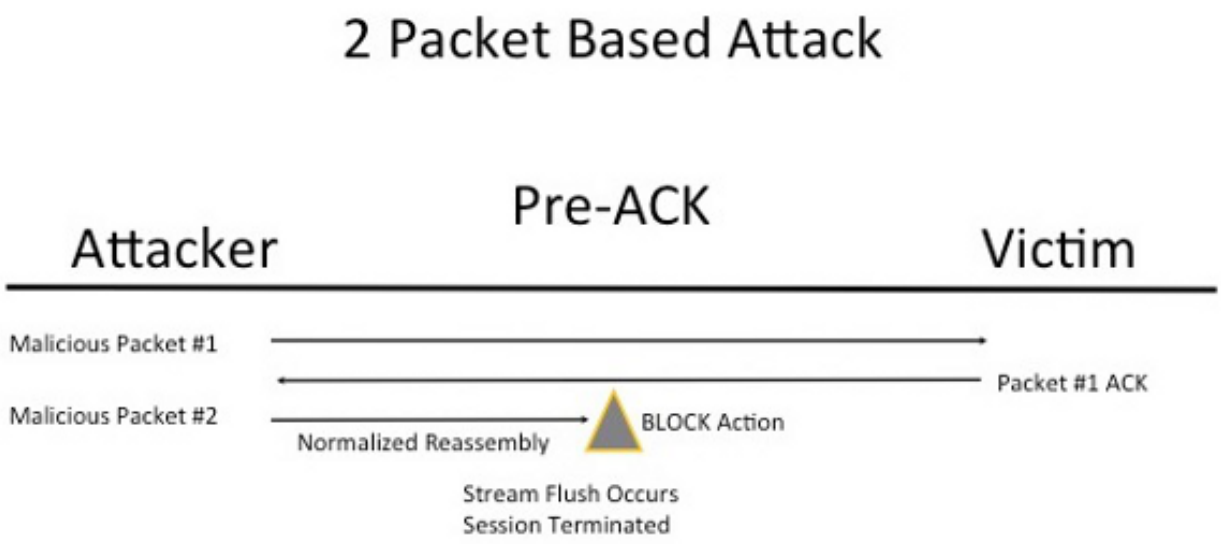
Comprenez l'inspection POST-ACK (normalisez la charge utile de TCP TCP/Normalize désactivée)

Dans l'inspection POST-ACK, le réassemblage de flux de paquets, l'annulation (main hors fonction au reste du procédé d'inspection), et la détection reniflent dedans se produit après que l'accusé de réception (ACK) de la victime pour le paquet qui se termine l'attaque soit reçu par le Système de prévention d'intrusion (IPS). Avant que l'annulation de flot se produise, le paquet offensant a déjà atteint la victime. Par conséquent, l'alerte/baisse se produit après que le paquet offensant ait atteint la victime. Cette action se produit quand l'ACK de la victime pour le paquet offensant atteint l'IPS.



Comprenez l'inspection Pré-ACK (normalisez la charge utile de TCP TCP/Normalize activée)

Cette caractéristique normalise le trafic juste après le paquet décodant et avant que tout autre reniflent la fonction est traitée afin de réduire des efforts d'évasion de TCP. Ceci s'assure que les paquets atteignant l'IPS sont identiques comme ceux qui sont passés en fonction à la victime. Reniflez les baisses le trafic sur le paquet qui se termine l'attaque avant que l'attaque atteigne sa victime.



Quand vous activez *normalisez le TCP*, le trafic qui apparie ces conditions est également abandonné :

- Copies retransmises des paquets précédemment relâchés
- Trafiquez que des tentatives de continuer une session précédemment relâchée
- Trafiquez qu'apparie l'un de ces règles de préprocesseur de flot de TCP :

  129:1129:3129:4129:6129:8129:11129:14 à 129:19

  Remarque: Afin d'activer les alertes pour le TCP coulez les règles qui sont abandonnées par le préprocesseur de normalisation, vous doit activer la caractéristique d'*anomalies d'inspection avec état* dans la configuration de flot de TCP.