Activer le préprocesseur de normalisation en ligne et comprendre l'inspection avant et après accusé de réception

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Activer la normalisation en ligne
  - Activer la normalisation en ligne dans les versions 5.4 et ultérieures
  - Activer la normalisation en ligne dans les versions 5.3 et antérieures
- Activer l'inspection post-ACK et pré-ACK
  - Comprendre l'inspection post-ACK (Normalisation TCP/Normalisation TCP Payload désactivée)
  - Comprendre l'inspection pré-ACK (Normaliser TCP/Normaliser la charge utile TCP activée)

Introduction

Ce document décrit comment activer le préprocesseur de normalisation en ligne et vous aide à comprendre la différence et l'impact de deux options avancées de normalisation en ligne.

Conditions préalables

Exigences

Cisco vous recommande de connaître le système Cisco Firepower et Snort.

Composants utilisés

Les informations contenues dans ce document sont basées sur les appliances Cisco FireSIGHT Management Center et Firepower.

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Un préprocesseur de normalisation en ligne normalise le trafic afin de minimiser les risques qu'un

pirate puisse échapper à la détection à l'aide de déploiements en ligne. La normalisation se produit immédiatement après le décodage du paquet et avant tout autre préprocesseur, et se poursuit à partir des couches internes du paquet vers l'extérieur. La normalisation en ligne ne génère pas d'événements, mais elle prépare les paquets pour une utilisation par d'autres préprocesseurs.

Lorsque vous appliquez une stratégie d'intrusion avec le préprocesseur de normalisation en ligne activé, le périphérique Firepower teste ces deux conditions afin de s'assurer que vous utilisez un déploiement en ligne :

- Pour les versions 5.4 et ultérieures, le mode Inline est activé dans la stratégie d'analyse de réseau (NAP), et la stratégie Drop when Inline est également configurée dans la stratégie d'intrusion si la stratégie d'intrusion est configurée pour abandonner le trafic. Pour les versions 5.3 et antérieures, l'option Drop when Inline est activée dans la stratégie d'intrusion.

- La stratégie est appliquée à un ensemble d'interfaces en ligne (ou en ligne avec failopen).

Par conséquent, en plus de l'activation et de la configuration du préprocesseur de normalisation en ligne, vous devez également vous assurer que ces conditions sont remplies, sinon le préprocesseur ne normalisera pas le trafic :

- Votre stratégie doit être configurée pour supprimer le trafic dans les déploiements en ligne.

- Vous devez appliquer votre stratégie à un jeu en ligne.

Activer la normalisation en ligne

Cette section décrit comment activer la normalisation en ligne pour les versions 5.4 et ultérieures, ainsi que pour les versions 5.3 et antérieures.

Activer la normalisation en ligne dans les versions 5.4 et ultérieures

La plupart des paramètres du préprocesseur sont configurés dans le NAP pour les versions 5.4 et ultérieures. Complétez ces étapes afin d'activer la normalisation en ligne dans le NAP :

1. Connectez-vous à l'interface utilisateur Web de votre FireSIGHT Management Center.

2. Accédez à Policies > Access Control.

3. Cliquez sur Network Analysis Policy près de la zone supérieure droite de la page.

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

5. Cliquez sur l'icône crayon afin de commencer la modification, et la page Modifier la stratégie s'affiche.

6. Cliquez sur Settings sur le côté gauche de l'écran, et la page Settings s'affiche.

7. Localisez l'option Inline Normalization dans la zone Transport/Network Layer Preprocessor.

8. Sélectionnez la case d'option Enabled afin d'activer cette fonctionnalité :



Le NAP avec la normalisation en ligne doit être ajouté à votre stratégie de contrôle d'accès pour que la normalisation en ligne se produise. Le NAP peut être ajouté via l'onglet Avancé de la stratégie de contrôle d'accès :



La stratégie de contrôle d'accès doit ensuite être appliquée au périphérique d'inspection.

> Remarque : Pour la version 5.4 ou ultérieure, vous pouvez activer la normalisation en ligne pour certains trafics et la désactiver pour d'autres. Si vous voulez l'activer pour un trafic spécifique, ajoutez une règle d'analyse de réseau et définissez les critères et la politique de trafic sur celui qui a la normalisation en ligne activée. Si vous souhaitez l'activer globalement, définissez la stratégie d'analyse de réseau par défaut sur celle pour laquelle la normalisation en ligne est activée.

Activer la normalisation en ligne dans les versions 5.3 et antérieures

Complétez ces étapes afin d'activer la normalisation en ligne dans une politique d'intrusion :

1. Connectez-vous à l'interface utilisateur Web de votre FireSIGHT Management Center.

2. Accédez à Politiques > Intrusion > Politiques d'intrusion.

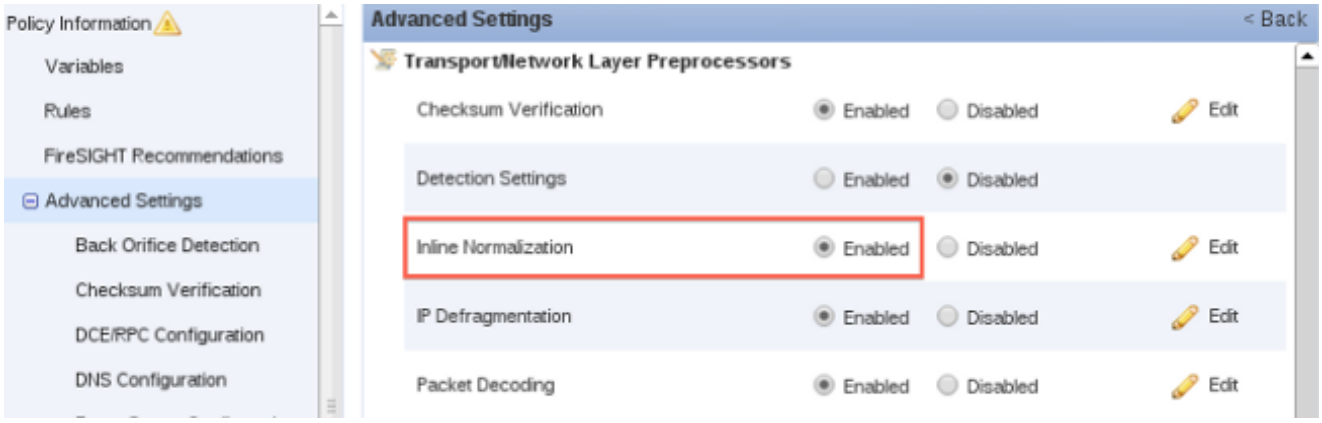
3. Sélectionnez une stratégie d'intrusion que vous souhaitez appliquer à votre périphérique géré.

4. Cliquez sur l'icône crayon afin de commencer la modification, et la page Modifier la stratégie s'affiche.

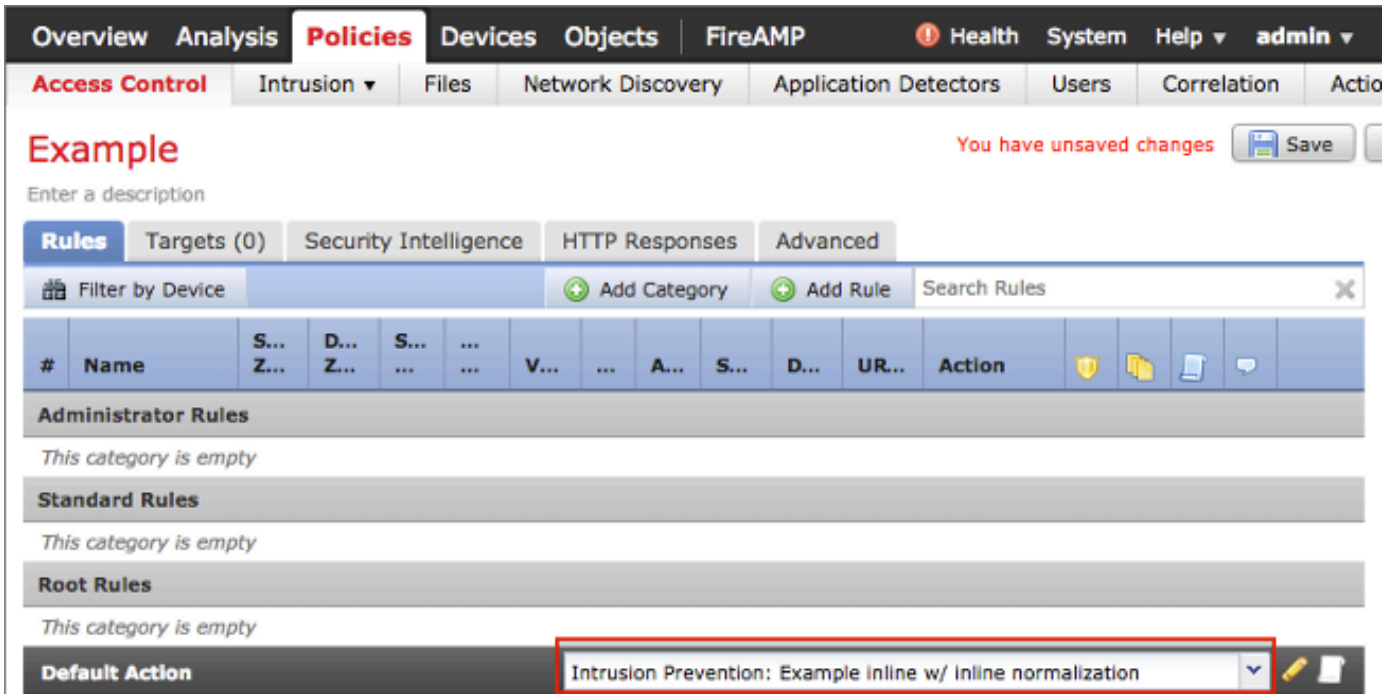
5. Cliquez sur Advanced Settings, et la page Advanced Settings s'affiche.

6. Localisez l'option Inline Normalization dans la zone Transport/Network Layer Preprocessor.

7. Sélectionnez la case d'option Enabled afin d'activer cette fonctionnalité :



Une fois la stratégie d'intrusion configurée pour la normalisation en ligne, elle doit être ajoutée comme action par défaut dans la stratégie de contrôle d'accès :



La stratégie de contrôle d'accès doit ensuite être appliquée au périphérique d'inspection.

Vous pouvez configurer le préprocesseur de normalisation en ligne afin de normaliser le trafic IPv4, IPv6, ICMPv4 (Internet Control Message Protocol Version 4), ICMPv6 et TCP dans n'importe

quelle combinaison. La normalisation de chaque protocole se produit automatiquement lorsque cette normalisation de protocole est activée.

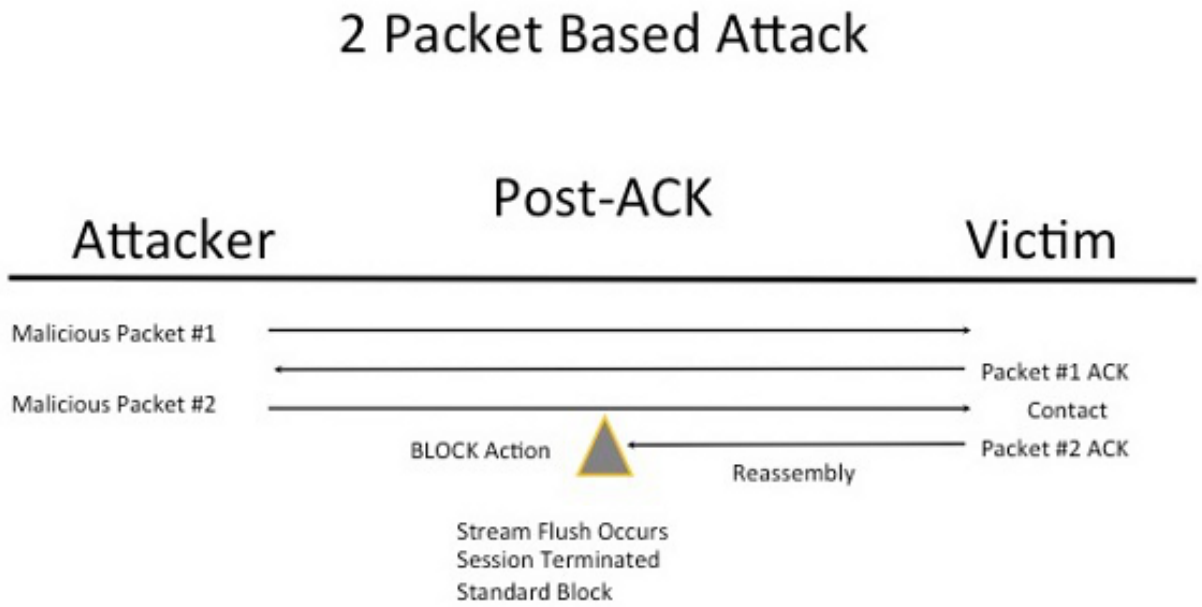
Activer l'inspection post-ACK et pré-ACK

Après avoir activé le préprocesseur de normalisation en ligne, vous pouvez modifier les paramètres afin d'activer l'option Normalize TCP Payload. Cette option du préprocesseur de normalisation en ligne permet de passer d'un mode d'inspection à l'autre :

- Post-accusé de réception (Post-ACK)
- Pré-accusé de réception (Pre-ACK)

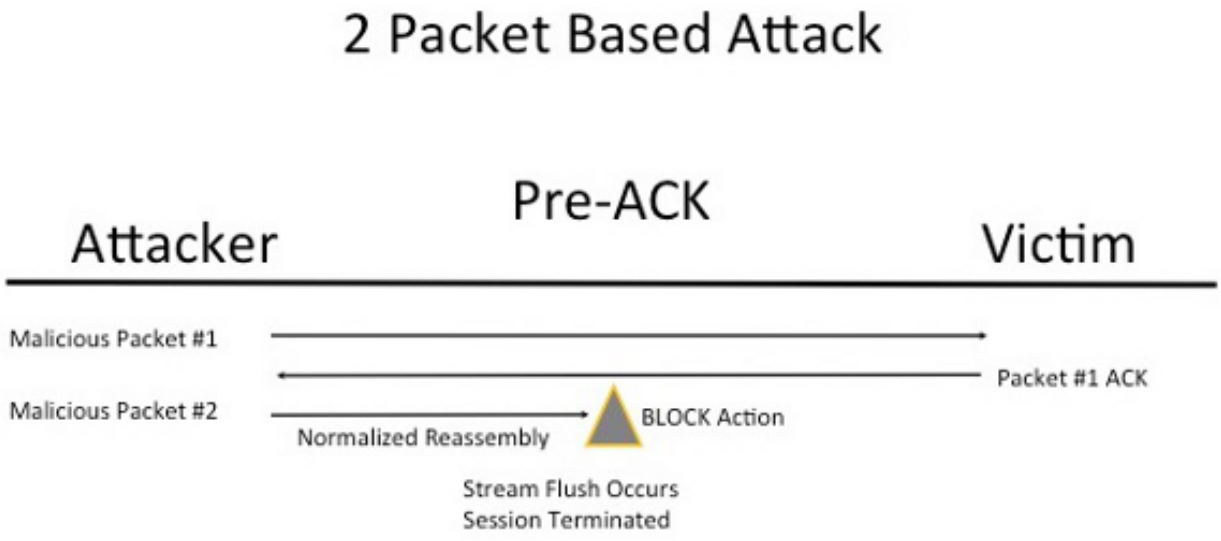
Comprendre l'inspection post-ACK (Normalisation TCP/Normalisation TCP Payload désactivée)

Dans l'inspection post-ACK, le réassemblage du flux de paquets, le vidage (transfert au reste du processus d'inspection) et la détection dans Snort se produisent après la réception par le système de prévention des intrusions (IPS) de l'accusé de réception (ACK) de la victime du paquet qui a terminé l'attaque. Avant que le flux ne soit vidé, le paquet incriminé a déjà atteint la victime. Par conséquent, l'alerte/abandon se produit une fois que le paquet incriminé a atteint la victime. Cette action se produit lorsque le message ACK de la victime pour le paquet incriminé atteint le système IPS.



Comprendre l'inspection pré-ACK (Normaliser TCP/Normaliser la charge utile TCP activée)

Cette fonctionnalité normalise le trafic immédiatement après le décodage des paquets et avant le traitement de toute autre fonction Snort afin de minimiser les efforts d'évasion TCP. Cela permet de s'assurer que les paquets atteignant l'IPS sont les mêmes que ceux qui sont transmis à la victime. Snort abandonne le trafic sur le paquet qui termine l'attaque avant que l'attaque n'atteigne sa victime.



Lorsque vous activez Normalize TCP, le trafic qui correspond à ces conditions est également abandonné :

- Copies retransmises de paquets précédemment abandonnés
- Trafic qui tente de poursuivre une session précédemment abandonnée
- Trafic correspondant à l'une des règles de préprocesseur de flux TCP suivantes :
  - 129:1
  - 129:3
  - 129:4
  - 129:6
  - 129:8
  - 129:11
  - 129:14 à 129:19

Remarque : Afin d'activer les alertes pour les règles de flux TCP qui sont abandonnées par le préprocesseur de normalisation, vous devez activer la fonctionnalité Anomalies d'inspection avec état dans la configuration de flux TCP.

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.

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.