FirePOWER Management Center affiche certains événements de connexion TCP dans la mauvaise direction

Contenu

Introduction

Ce document décrit les raisons et les étapes d'atténuation pour FirePOWER Management Center (FMC) qui affichent les événements de connexion TCP dans la direction inverse, où l'adresse IP de l'initiateur est l'adresse IP du serveur de la connexion TCP et l'adresse IP du répondeur est l'adresse IP du client de la connexion TCP.

> **Note**: De tels événements ont de multiples raisons. Ce document explique la cause la plus courante de ce symptôme.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Technologie FirePOWER
- Connaissances de base de l'appliance ASA (Adaptive Security Appliance)
- Compréhension du mécanisme de synchronisation TCP (Transmission Control Protocol)

Components Used

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

- ASA Firepower Threat Defense (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) qui exécute les versions 6.0.1 et ultérieures du logiciel

- ASA Firepower Threat Defense (5512-X, 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, FP9300, FP4100) qui exécute les versions 6.0.1 et ultérieures du logiciel
- ASA avec modules Firepower (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X, 5515-X, ASA 5525-X, ASA 5545-X, ASA 555 ASA 5585-X) qui exécute les versions 6.0.0 et ultérieures du logiciel
- Firepower Management Center (FMC) version 6.0.0 et ultérieure

The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont démarré avec une configuration claire (par défaut). If your network is live, make sure that you understand the potential impact of any command.

Fond

Dans une connexion TCP, **le client** fait référence à l'adresse IP qui envoie le paquet initial. FirePOWER Management Center génère un événement de connexion lorsque le périphérique géré (capteur ou FTD) voit le paquet TCP initial d'une connexion.

Les périphériques qui suivent l'état d'une connexion TCP ont un **délai d'inactivité** défini pour s'assurer que les connexions qui ne sont pas fermées par erreur par les points de terminaison ne consomment pas la mémoire disponible pendant de longues périodes. Le délai d'inactivité par défaut des connexions TCP établies sur FirePOWER est de **trois minutes**. Une connexion TCP qui est restée inactive pendant trois minutes ou plus n'est pas suivie par le capteur IPS FirePOWER.

Le paquet suivant après le délai d'attente est traité comme un nouveau flux TCP et la décision de transfert est prise conformément à la règle qui correspond à ce paquet.Lorsque le paquet provient du serveur, l'adresse IP du serveur est enregistrée comme initiateur de ce nouveau flux. Lorsque la journalisation est activée pour la règle, un événement de connexion est généré sur FirePOWER Management Center.

> **Note**: Conformément aux stratégies configurées, la décision de transfert du paquet qui vient après le délai d'attente est différente de celle du paquet TCP initial. Si l'action par défaut configurée est « Bloquer », le paquet est abandonné.

Voici un exemple de ce symptôme :

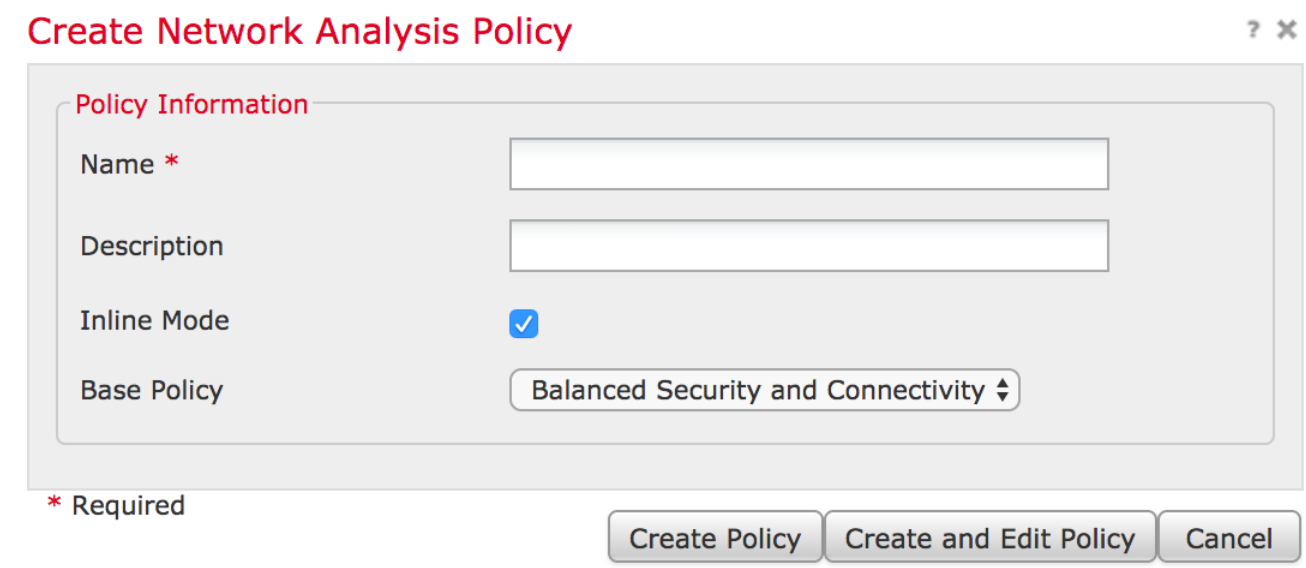
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

Solution

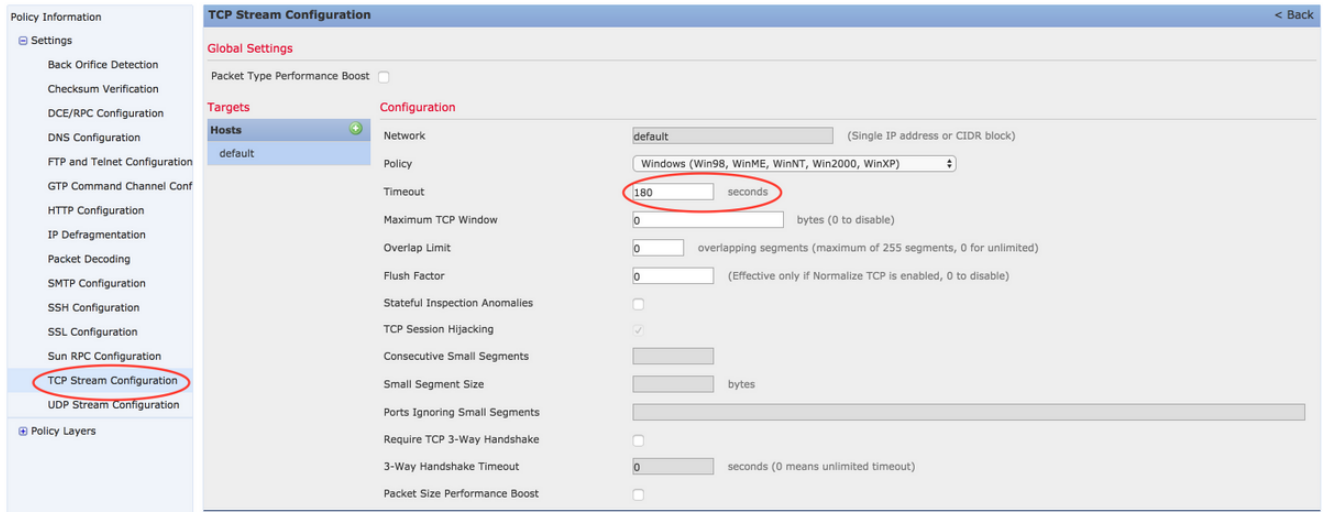
Le problème mentionné ci-dessus est atténué en augmentant le **délai** d'**attente** des connexions TCP. Pour modifier le délai d'attente,

1. Accédez à **Politiques > Contrôle d'accès > Intrusion**.
2. Accédez au coin supérieur droit et sélectionnez **Stratégie d'accès au réseau**.

3. Sélectionnez **Créer une stratégie**, choisissez un nom et cliquez sur **Créer et modifier une stratégie**. Ne modifiez pas la **stratégie de base.**

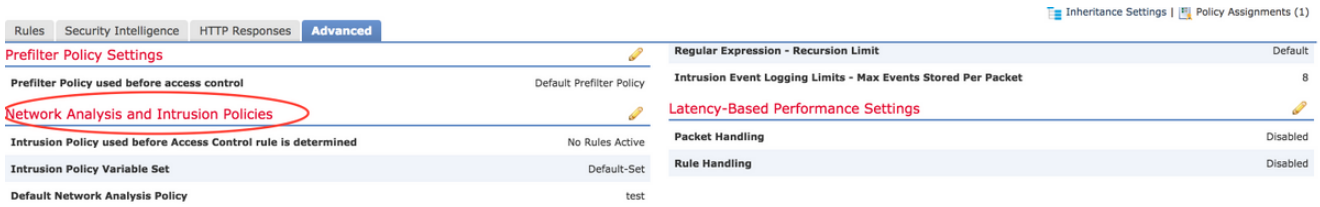


4. Développez l'option **Paramètres** et choisissez **Configuration du flux TCP**.
5. Accédez à la section de configuration et modifiez la valeur de **Timeout** selon vos besoins.



6. Accédez à **Politiques > Contrôle d'accès > Contrôle d'accès**.
7. Sélectionnez l'option **Modifier** pour modifier la stratégie appliquée au périphérique géré approprié ou créer une nouvelle stratégie.

8. Sélectionnez l'onglet **Avancé** dans la stratégie Accès.
9. Recherchez la section **Analyse du réseau et stratégies d'intrusion** et cliquez sur l'icône **Modifier**.



10. Dans le menu déroulant **Stratégie d'analyse de réseau par défaut**, sélectionnez la stratégie créée à l'étape 2.
11. Cliquez sur **OK** et **enregistrez** les modifications.
12. Cliquez sur l'option **Déployer** pour déployer les stratégies sur les périphériques gérés appropriés.

Attention : L'augmentation du délai d'attente devrait augmenter l'utilisation de la mémoire. FirePOWER doit suivre les flux qui ne sont pas fermés par les points d'extrémité pendant plus longtemps. L'augmentation réelle de l'utilisation de la mémoire est différente pour chaque réseau unique car elle dépend de la durée pendant laquelle les applications réseau maintiennent les connexions TCP inactives.

Conclusion

La valeur de référence de chaque réseau pour le délai d'inactivité des connexions TCP est différente. Cela dépend entièrement des applications utilisées. Une valeur optimale doit être établie en observant la durée pendant laquelle les applications réseau maintiennent les connexions TCP inactives. Pour les problèmes liés au module de service FirePOWER sur un Cisco ASA, lorsqu'une valeur optimale ne peut pas être déduite, le délai d'attente peut être réglé en l'augmentant en plusieurs étapes jusqu'à la valeur de délai d'attente d'ASA.

Informations connexes

- Guide de démarrage rapide de Cisco Firepower Threat Defense pour l'ASA
- Support et documentation techniques - Cisco Systems
- Guide de démarrage rapide ASA Firepower