Le centre de Gestion de puissance de feu affiche quelques événements de connexion TCP dans la mauvaise direction

Contenu

Introduction

Ce document décrit les raisons et les étapes de réduction pour la Gestion Center(FMC) de puissance de feu affichant des événements de connexion TCP dans la direction inverse où l'IP de demandeur est l'IP du serveur de la connexion TCP et le responder que l'IP est l'IP du client de la connexion TCP.

> Remarque: Il y a de plusieurs raisons pour l'occurrence de tels événements. Ceci documente explique la plupart de cause classique de ce symptôme.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Technologie de puissance de feu
- Connaissance de base de l'appliance de sécurité adaptable (ASA)
- Compréhension de mécanisme de synchronisation de Transmission Control Protocol(TCP)

Composants utilisés

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

- La défense contre des menaces de puissance de feu ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) cette exécute la version de logiciel 6.0.1 et plus tard

- La défense contre des menaces de puissance de feu ASA (5512-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X,FP9300,FP4100) cette exécute la version de logiciel 6.0.1 et plus tard
- L'ASA avec les modules de puissance de feu (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) ces exécute les versions de logiciel 6.0.0 et plus tard
- Version 6.0.0 et ultérieures du centre de Gestion de puissance de feu (FMC)

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 commencé par une configuration (par défaut) claire. Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Fond

Dans une connexion TCP, le **client** se réfère à l'IP qui envoie le paquet initial. Le centre de Gestion de puissance de feu génère un événement de connexion quand le périphérique géré (capteur ou FTD) voit le paquet TCP initial d'une connexion.

Les périphériques qui dépistent l'état d'une connexion TCP ont un **délai d'attente de veille** défini pour s'assurer que les connexions qui ne sont pas incorrectement fermées par des points finaux ne consomment pas la mémoire disponible pendant des longues périodes de temps. Le délai d'attente de veille par défaut pour les connexions TCP établies sur la puissance de feu est de **trois minutes**. Une connexion TCP qui est restée de veille pendant trois minutes ou plus, n'est pas dépistée par le capteur IPS de puissance de feu.

Le paquet suivant après que le délai d'attente soit traité comme nouvel écoulement de TCP et décision d'expédition est pris selon la règle qu'apparie ce paquet. Quand le paquet est du serveur, l'IP du serveur est enregistré comme demandeur de ce nouvel écoulement. Quand se connecter est activé pour la règle, un événement de connexion est généré au centre de Gestion de puissance de feu.

> Remarque: Selon des stratégies configurées, la décision d'expédition pour le paquet qui est livré après que le délai d'attente soit différent de la décision pour le paquet TCP initial. Si l'action par défaut configurée est « bloc », le paquet est lâché.

Un exemple de ce symptôme est selon le tir d'écran ci-dessous :

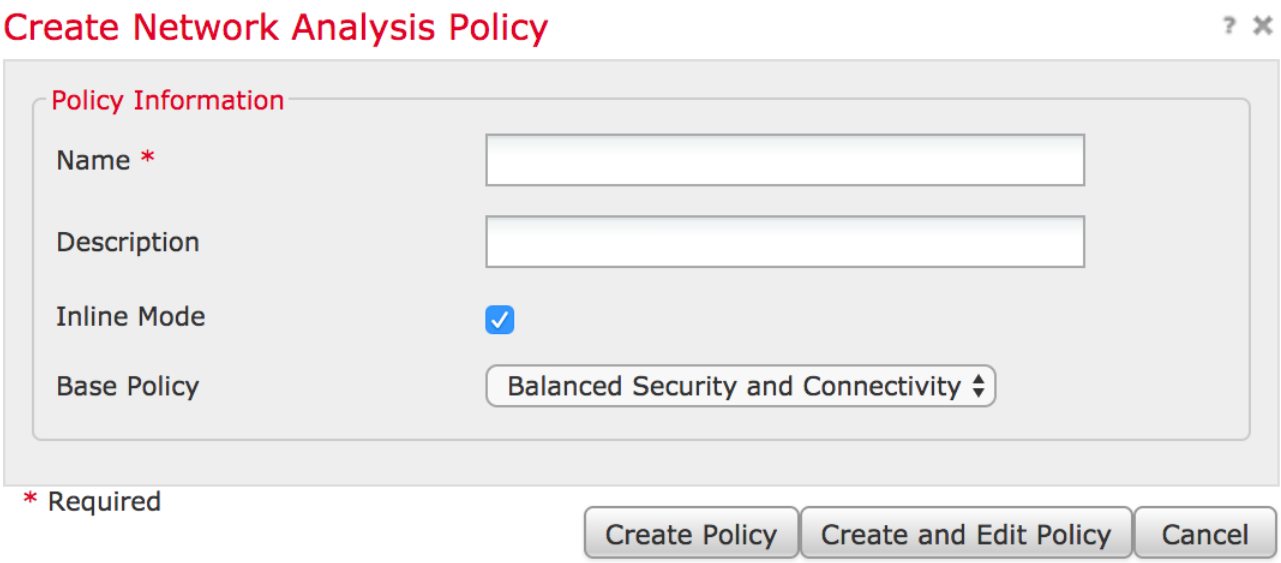
	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
	2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
	2017-05-12 17:39:13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

Solution

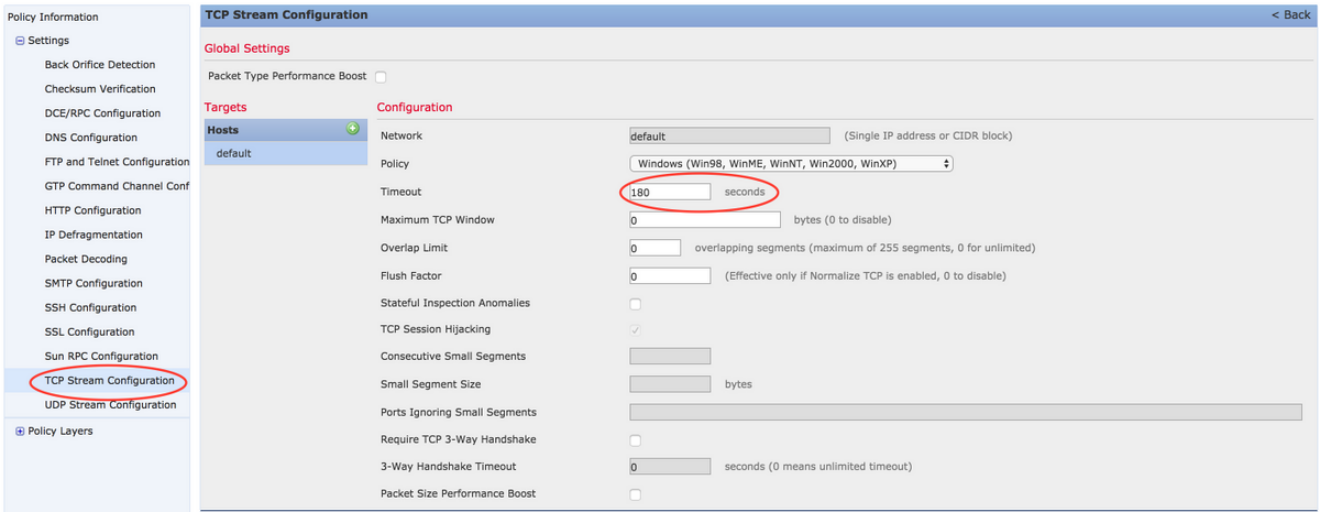
Le problème mentionné ci-dessus est atténué en augmentant le **délai d'attente des** connexions TCP. Dans la modification de commande le délai d'attente,

1. Naviguez vers les **stratégies > le contrôle d'accès > l'intrusion**.
2. Naviguez vers le coin haut droit et sélectionnez la **stratégie d'accès au réseau**.

3. Choisi **créez la stratégie**, choisissez un nom et cliquez sur en fonction **Create et éditez la stratégie**. Ne modifiez pas la **stratégie de base.**

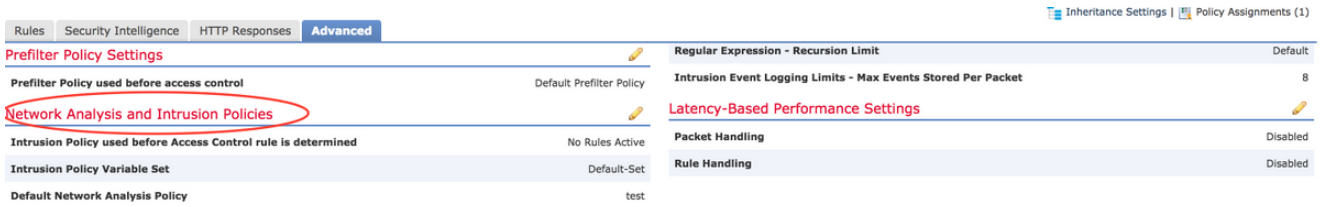


4. Développez l'option de **configurations** et choisissez la **configuration de flot de TCP**.
5. Naviguez vers la section de configuration et changez la valeur du **délai d'attente** comme désirée.



6. Naviguez vers les **stratégies > le contrôle d'accès > le contrôle d'accès**.
7. Sélectionnez l'option **éditent** pour éditer la la stratégie appliquée au périphérique géré approprié ou pour créer une nouvelle stratégie.

8. Sélectionnez l'**onglet Avancé** dans la stratégie d'Access.
9. Localisez l'**analyse réseau et la** section de **stratégies d'intrusion** et cliquez sur en fonction l'icône **Edit**.



10. Du menu déroulant de la **stratégie par défaut d'analyse réseau**, choisissez la stratégie créée dans l'étape 2.
11. Cliquez sur OK et **sauvegardez les** modifications.
12. Cliquez sur en fonction l'option **Deploy** de déployer maintient l'ordre aux périphériques manged appropriés.

Attention : On s'attend à ce que le délai d'attente croissant entraîne une utilisation de mémoire plus élevée, puissance de feu doit dépister les écoulements qui ne sont pas clôturés par des points finaux pendant un plus long temps. L'augmentation réelle de l'utilisation de mémoire est différente pour chaque seul réseau car elle dépend de combien de temps les applications réseau gardent l'inactif de connexions TCP.

Conclusion

Le benchmark de chaque réseau pour le délai d'attente de veille des connexions TCP sont différent. Il dépend complètement des applications qui sont en service. Une valeur optimale doit être établie en observant combien de temps les applications réseau gardent l'inactif de connexions TCP. Pour les questions qui concernent le module de service de puissance de feu sur Cisco ASA, quand une valeur optimale ne peut pas être déduite, le délai d'attente peut être accordé en l'augmentant intensifie dedans à la valeur du dépassement de durée de l'ASA.

Informations connexes

- Guide de démarrage rapide de défense contre des menaces de puissance de feu de Cisco pour l'ASA
- Support et documentation techniques - Cisco Systems
- Guide de démarrage rapide de puissance de feu ASA