Mode de cheminement de session TCP intégrée sur l'IPS

Contenu

Introduction

Ce document décrit la fonctionnalité de suivi intégrée de session TCP de l'appliance de Système de prévention d'intrusion (IPS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliances de gamme 4200 IPS configurées avec les interfaces intégrées.
- La connaissance du protocole TCP et de la circulation.

Composants utilisés

Les informations dans ce document sont basées en fonction :

- IPS 4270 avec la version de logiciel 7.1(7)

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Dans certains scénarios de déploiement IPS d'en ligne, des paquets d'un flot de TCP peuvent être vus deux fois par l'engine de normalisateur, qui a comme conséquence les baisses en raison du cheminement inexact de flot. Cette situation est typiquement vue quand le trafic est conduit par les plusieurs réseaux locaux virtuels (VLAN) ou les paires d'interface qui sont surveillées par un capteur virtuel simple. Cette question est encore compliquée par la nécessité pour permettre au trafic asymétrique pour fusionner pour le flot approprié dépistant quand le trafic pour l'un ou l'autre de direction est reçu de différents VLAN ou d'interfaces.

Diagramme du réseau

Problème

En cette topologie du réseau, un client sur le réseau intérieur initie une connexion HTTP au serveur sur le réseau extérieur. Les deux segments de réseau sont séparés par un Pare-feu de l'appliance de sécurité adaptable (ASA). Dans cette conception, une appliance simple IPS est configurée pour brancher sur les les deux les VLAN intérieurs et extérieurs avec deux ensembles de paires intégrées d'interface. Quand le client initie la session au serveur, le paquet de synchronisation de TCP (synchronisez) prend ce chemin (flot sortant) par l'IPS et l'ASA :

Client > IPS G3/0 > *vs0* > IPS G3/1 > ASA G0/0 > ASA G0/1 > IPS G3/2 > *vs0* > IPS G3/3 > serveur

Après le flot sortant, la synchronisation de TCP envoyée par le client est vue par le capteur **vs0** virtuel pendant que le paquet traverse les paires d'interface interne vers l'interface interne de l'ASA et de nouveau quand le paquet traverse les paires extérieures d'interface vers le web server. Dans un scénario symétrique, la même situation se produit dans le chemin de retour avec la synchronisation ACK (un accusé de réception positif) et des paquets suivants du web server. Quand les tentatives IPS de combiner les flots dans une connexion TCP simple, des doublons de chaque paquet dans la connexion sont observées, qui a comme conséquence un normalisateur confus et des paquets abandonnés. Afin de confirmer si un IPS rencontre cette situation, la sortie de la commande de **virt stat d'exposition** affiche un grand nombre de 1330 signatures de normalisateur de TCP qui se déclenchent, aussi bien qu'un grand nombre de paquets et de connexions modifiés et refusés.

Solution

L'option de **cheminement de mode de session TCP intégrée** peut être utilisée pour surmonter des situations de ce type. Il y a trois modes possibles qui peuvent être configurés :

1. **Capteur virtuel (valeur par défaut)** - Moniteurs dans une situation asymétrique de déploiement où des paquets de client sont vus sur une paire intégrée, alors que des paquets de serveur sont vus sur une deuxième paire d'interface. Les deux paires d'interface doivent être surveillées ensemble pour voir les deux côtés de la connexion.
2. **Interface et VLAN** - C'est un contournement à l'exemple de topologie affiché dans ce document, dans lequel deux paires intégrées ou plus d'interface sont assignées au même capteur virtuel. Cette option étant activé, une connexion TCP peut traverser plus d'une paire, qui permet au normalisateur pour dépister des sessions TCP indépendamment pour chaque paire intégrée.
3. **VLAN seulement** - C'est une combinaison très rare des deux premières options et t'est utilisée surveillent une combinaison de plusieurs réseaux asymétriques. **Le VLAN 1** sur les paires gauches d'interface a des paquets de client et doit être combiné avec le **VLAN 1** sur la bonne paire d'interface, qui a les paquets de serveur. Dans ce cas, le trafic est agrégé à travers toutes les paires d'interface, mais est isolé par VLAN. Par exemple, les paquets VLAN 1 à travers toutes les interfaces sont placés ensemble ; Les paquets VLAN 2 de toutes les interfaces sont placés ensemble, mais les paquets VLAN 1 et VLAN 2 ne sont ensemble jamais placés pour le cheminement de session TCP.

Pour la topologie d'exemple ci-dessus, il y a deux manières que le problème peut être résolu :

Solution 1

Entrez chaque paire intégrée d'interface dans son propre capteur virtuel. Par exemple, une paire sur **vs0** et une paire sur **vs1**. Cette méthode est généralement recommandée quand il y a moins de quatre paires intégrées (en raison de la limite de plate-forme de quatre capteurs virtuels). Le normalisateur traite les flots en double en tant que deux connexions distinctes.

Solution 2

Configurez le mode de cheminement de session TCP intégrée **pour relier et le VLAN**. Cette méthode est recommandée quand il y a plus de quatre paires intégrées, dans ce cas, vous êtes forcé pour placer de plusieurs paires intégrées dans un capteur virtuel simple. Le normalisateur traite des paquets sur différentes paires intégrées en tant que connexions complètement différentes dans le même capteur virtuel.

Configurez

Voici la configuration pour séparer le capteur virtuel par paires intégrées d'interface :

```
IPS4510-01# conf t
```

```
IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Inside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# virtual-sensor vs1

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Outside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

IPS4510-01(config)# exit
```

Voici la configuration pour l'interface et le VLAN :

```
IPS4510-01# config t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# inline-tcp-session interface-and-vlan

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

Apply Changes?[yes]: yes

Warning: Change of TCP session tracking mode will not take effect until restart.

IPS4510-01(config)# exit

IPS4510-01# reset
```

Vérifiez

- Utilisez le **virt stat d'exposition |** commande et examen de **statistiques d'étape de normalisateur de TCP b** pour **relâché**, le **doublon**, **refusé**, ou les **paquets de SendAck a envoyé des** statistiques différentes de zéro dans le normalisateur de TCP.
- Utilisez le **virt stat d'exposition |** commande et examen de **compte de SigEvent de Par-signature b** pour 1330 signatures qui se sont déclenchées en même temps que les statistiques de Normalier de TCP de la commande précédente.

Informations connexes

- Guide de configuration CLI de capteur de Système de protection contre les intrusions Cisco IPS 7.0 - mode de cheminement de session TCP intégrée
- Guide de configuration de Manager Express de Système de protection contre les intrusions Cisco IPS 7.1 - Mode de cheminement de session TCP intégrée
- Support et documentation techniques - Cisco Systems