Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Réflecteur d'ENVERGURE](#)
[Capture du trafic FWSM sur le fond de panier de commutateur](#)
Étape 1 : Déterminez le Port canalisé utilisé par FWSM
Étape 2 : Définissez les interfaces de source et de destination
Étape 3 : Vérifiez la session de surveillance
Informations connexes

Introduction

Ce document décrit comment surveiller le trafic envoyé à et reçu d'un Module de services de Pare-feu (FWSM). Sur la plate-forme de Routeurs de gamme 7600 de Cisco Catalyst 6500/Cisco, il y a deux sessions de Fonction Switched Port Analyzer (SPAN) qui peuvent être utilisées pour réorienter le trafic à une destination port pour des activités telles que des saisies ou des transmissions à d'autres périphériques de Sécurité physique (tels qu'une intrusion Detection System). Des sessions d'ENVERGURE sont également connues comme sessions de surveillance.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Sécurité des réseaux
- Connaissance des captures de données (renifleurs)

Composants utilisés

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

- Commutateurs de gamme Cisco Catalyst 6500/7600
- Engine 720 de superviseur de gamme 7600 de Cisco Catalyst 6500/Cisco
- Cisco FWSM

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.

Réflecteur d'ENVERGURE

Quelques modules de service, tels que le FWSM, utilisent une de leurs deux sessions de surveillance pour tous les modules de service afin de communiquer avec les ASIC sur le superviseur. Cette artère de communications active le trafic de multidiffusion, aussi bien que tout autre trafic qui exige l'engine centrale de réécriture, à commuter egressing le FWSM ou d'autres modules de service. Ce type de session est connu comme réflecteur d'ENVERGURE et est activé par défaut. Le réflecteur d'ENVERGURE est exigé si les utilisations de commutateur distribuaient l'EtherChannel (de croix-module) ; un EtherChannel distribué existe quand un Port canalisé a les plusieurs interfaces qui sont empaquetées et qui croisent de plusieurs linecards.

Remarque: Le module de service d'appliance de sécurité adaptable (ASA-SM) n'exige pas le réflecteur d'ENVERGURE, ainsi vous peut désactiver le réflecteur si autre module de service ne l'exige pas.

La deuxième session peut être utilisée pour d'autres sessions de surveillance, telles que le reniflement de paquet.

Utilisez le **show monitor session toute la** commande afin de voir le statut des sessions de surveillance ; recherchez la session de module de service comme type.

Capture du trafic FWSM sur le fond de panier de commutateur

Utilisez une session de surveillance afin de répartir le trafic au lequel est envoyé et reçu du FWSM sur les interfaces internes du fond de panier. Dans cet exemple, la session 1 est installée pour renifler le trafic à et du FWSM.

Étape 1 : Déterminez le Port canalisé utilisé par FWSM

Le FWSM utilise généralement un nombre de Port canalisé interne numéro 270 ou plus élevé. Employez la commande **récapitulative de show etherchannel** afin de déterminer quel port est en service.

Dans cet exemple, l'ID de Port canalisé 272 est assigné pour le FWSM dans l'emplacement 3. Le FWSM se connecte au fond de panier de commutateur par l'intermédiaire de six ports de 1 Go, qui sont empaquetés dans un EtherChannel interne.

Étape 2 : Définissez les interfaces de source et de destination

Employez les **1 commandes d'interface de destination d'interface** et de **session de surveillance 1 de source de la session de surveillance** afin de définir la source et les interfaces de destination pour les sessions de surveillance. Dans cet exemple, l'interface de source est le Port canalisé 272 (comme identifié dans l'étape 1), et l'interface de destination est le gigabit 5/48 de port où un périphérique physique de renifleur sera connecté.

Étape 3 : Vérifiez la session de surveillance

Employez la commande du **show monitor session 1** afin de vérifier la session de surveillance.

La sortie prouve que le Port canalisé 272 (Po272) est la source d'envergure et qu'il surveillera tout le trafic envoyé à et reçu du FWSM dans l'emplacement 3.

Remarque: Si vous répartissez l'EtherChannel de Go du six ports 1, vous pouvez dépasser le débit de paquets (ou le débit en entrée de renifleur) de l'interface de destination. S'il y a plus de trafic sur le Port canalisé FWSM qu'est physiquement possible sur une 1 interface d'Ethernets de Go (le débit de transmission de la destination port Gi5/48), l'interface de destination peut ne pas pouvoir sortir tous les paquets au renifleur.

Informations connexes

- Version 12.2SXF de Catalyst 6500 et guide de configuration du logiciel de reconstructions : SPAN local, Remote SPAN (RSPAN), et RSPAN encapsulé
- Support et documentation techniques - Cisco Systems