Différences entre les logs et les debugs sur des appliances de sécurité adaptable

Contenu

Introduction

Ce document fournit une description simple pour la fonctionnalité d'élimination des imperfections dans les appliances de sécurité adaptable (ASA) cette version 8.4 et ultérieures de passage. Cependant, certaines des caractéristiques sont disponibles seulement dans la version 9.5(2) et ultérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- ASA 5506-X avec la version de logiciel ASA 9.5(2)
- Version 7.5.2 du Cisco Adaptive Security Device Manager (ASDM)

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.

Fonctionnalité se connectante de base

Messages de débogage de traitement ASA différemment que des périphériques de Cisco IOS®. Par défaut (à moins que « se connectant le debug-suivi », qui est décrit plus tard, est utilisé), ils

sont affichés à l'écran l'un ou l'autre quand vous êtes connecté par le port de console ou par le telnet/Protocole Secure Shell (SSH), mais ils sont complètement indépendants. Quand vous utilisez la console, ils apparaissent juste après que vous sélectionnez la commande de débogage. La même action se produit également avec une session de SSH.

L'indépendance signifie que quand vous activez met au point sur le port de console et vous êtes connecté par le SSH, met au point n'apparaissent pas sur le SSH. Vous devez manuellement les activer de nouveau. En outre, si met au point sont activés sur une session de SSH qu'ils n'apparaîtront pas du tout sur l'autre session. Vous pouvez se référer à lui selon l'**élimination des imperfections de session.**

Il n'y a également aucun besoin de sélectionner la commande de **terminal monitor** sur des shows debug ASA, parce que met au point activé sur le SSH ou une session de telnet apparaissent indépendamment de cette commande. Le but de cette commande est beaucoup différent que dans des périphériques de Cisco IOS et l'exemple de configuration de Syslog ASA décrit cette caractéristique en profondeur.

Différence entre le Syslog et les messages de débogage

Met au point sont les messages spécifiés pour un certain protocole ou caractéristique des ASA. Il n'y a aucun niveau de met au point, au lieu de cela ils sont très détaillés et le niveau de détail peut être changé. Ils ne pourraient pas également avoir un horodateur, un code de message, ou un niveau d'importance. Ce dépend du détail mettent au point.

Cet exemple affiche que la différence entre met au point et les messages de Syslog en vue de la même requête ping.

C'est un exemple de sortie de débogage après que vous sélectionniez la **commande trace d'ICMP de débogage** :

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

C'est un exemple d'un message de **Syslog** en vue de la même demande d'ICMP :

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

Collectez les debugs

Le délai d'attente par défaut pour le SSH ou le telnet est de cinq minutes et la session est déconnectée après cette période de l'inactivité. Le délai d'attente par défaut pour la connexion de console est 0, ainsi il signifie que l'utilisateur est ouvert une session jusqu'aux journaux de l'utilisateur manuellement.

Malheureusement la fonctionnalité de journalisation est limitée par le délai d'attente réglé sur une méthode de gestion particulière, ainsi quand la session de SSH finit met au point également l'arrêt.

Afin de continuer à collecter met au point pendant un temps étendu, vous devez utiliser la connexion de console et alors vous pouvez les réorienter au serveur de Syslog avec la commande **se connectante de debug-suivi**. Ils seront réorientés comme message 711001 de Syslog émis au niveau d'importance 7. afin de cesser d'envoyer à ceci des messages aux logs, vous peuvent utiliser l'insertion « non » avant la commande.

```
logging debug-trace
no logging debug-trace
```

De la version 9.5.2, l'ASA te permet pour continuer à envoyer met au point comme messages de Syslog après un délai d'attente ou une déconnexion sur une connexion SSH/telnet/console. Si vous sélectionnez la commande **persistante de debug-suivi que** vous serez sélectivement clair capable met au point activé en une session d'une session différente et ils resteront actifs à l'arrière-plan. Afin de désactiver cette configuration, insérez « non » avant la commande.

```
logging debug-trace persistent
no logging debug-trace persistent
```

Par défaut, tous les messages de débogage ont une sévérité du niveau 7. afin de les filtrer des messages indésirables que vous pouvez soulever la sévérité de ce message à 3 ainsi vous collecterez seulement des messages d'erreur près de met au point. Insérez « non » afin de désactiver cette redirection.

```
logging message 711001 level 3
no logging message 711001 level 3
```

Exemple de configuration

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

Ces commandes te permettent d'envoyer des messages d'erreur et le Protocole ICMP (Internet Control Message Protocol) met au point marqué également comme erreurs au serveur de Syslog :

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

Informations connexes

- Exemple de configuration de Syslog ASA
- Support et documentation techniques - Cisco Systems