Différences entre les journaux et les débogages sur les appareils de sécurité adaptatifs

Contenu

Introduction

Ce document fournit une description simple de la fonctionnalité de débogage dans les appliances de sécurité adaptatives (ASA) qui exécutent les versions 8.4 et ultérieures. Cependant, certaines fonctionnalités ne sont disponibles que dans les versions 9.5(2) et ultérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Fonctionnalité de journalisation de base

Les ASA gèrent les messages de débogage différemment des périphériques Cisco IOS®. Par défaut (à moins que « logging debug-trace », décrit plus loin, ne soit utilisé), ils sont affichés à l'écran soit lorsque vous êtes connecté via le port de console, soit via telnet/Secure Shell (SSH), mais ils sont complètement indépendants. Lorsque vous utilisez la console, elles apparaissent

immédiatement après que vous avez entré la commande debug. La même action se produit également avec une session SSH.

L'indépendance signifie que lorsque vous activez les débogages sur le port de console et que vous êtes connecté via SSH, les débogages n'apparaissent pas sur SSH. Vous devez les réactiver manuellement. En outre, si les débogages sont activés sur une session SSH, ils n'apparaîtront pas du tout sur l'autre session. Vous pouvez y faire référence en tant que **débogage par session.**

Il n'est pas nécessaire d'entrer la commande **terminal monitor** sur un ASA afin d'afficher les débogages, car les débogages activés sur SSH ou une session telnet apparaissent indépendamment de cette commande. L'objectif de cette commande est très différent de celui des périphériques Cisco IOS et de l'exemple de configuration Syslog ASA décrit cette fonctionnalité en détail.

Différence entre les messages Syslog et Debug

Les débogages sont des messages spécifiés pour un protocole ou une fonctionnalité spécifique des ASA. Il n'y a pas de niveau de débogages, ils sont plutôt très détaillés et le niveau de détail peut être changé. Ils peuvent également ne pas avoir d'horodatage, de code de message ou de niveau de gravité. Cela dépend du débogage particulier.

Cet exemple montre la différence entre les débogages et les messages syslog en ce qui concerne la même requête ping.

Voici un exemple de sortie de débogage après avoir entré la commande **debug icmp trace** :

```
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
```

Voici un exemple de message **syslog** relatif à la même requête 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
```

Collecter les débogages

Le délai d'attente par défaut pour SSH ou telnet est de cinq minutes et la session est déconnectée après cette période d'inactivité. Le délai d'attente par défaut pour la connexion console est 0, ce qui signifie que l'utilisateur est connecté jusqu'à ce que l'utilisateur se déconnecte manuellement.

Malheureusement, la fonctionnalité de journalisation est limitée par le délai défini sur une méthode de gestion particulière, donc lorsque la session SSH termine les débogages s'arrêtent également.

Afin de continuer à collecter les débogages pendant une longue période, vous devez utiliser la connexion console, puis vous pouvez les rediriger vers le serveur syslog avec la commande **logging debug-trace**. Ils seront redirigés en tant que message syslog 711001 émis au niveau de gravité 7. Afin d'arrêter d'envoyer ces messages aux journaux, vous pouvez utiliser insert « no »

avant la commande.

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

Àpartir de la version 9.5.2, l'ASA vous permet de continuer à envoyer des débogages en tant que messages syslog après un délai d'attente ou de vous déconnecter sur une connexion SSH/telnet/console. Si vous entrez la commande **debug-trace persistent**, vous pourrez effacer sélectivement les débogages activés dans une session à partir d'une session différente et ils resteront actifs en arrière-plan. Afin de désactiver cette fonction, insérez « no » avant la commande.

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

Par défaut, tous les messages de débogage ont une gravité de niveau 7. Afin de les filtrer des messages indésirables, vous pouvez augmenter la gravité de ce message à 3 afin que vous ne collectionniez que les messages d'erreur en regard des débogages. 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 vous permettent d'envoyer des messages d'erreur et des débogages ICMP (Internet Control Message Protocol) marqués également comme des erreurs au serveur 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 ASA Syslog
- Support et documentation techniques - Cisco Systems