Outil de capture WebVPN sur le dispositif de sécurité adaptatif dédié de la gamme Cisco ASA 5500

Contenu

Introduction

Le dispositif de sécurité adaptatif de la gamme Cisco ASA 5500 comprend un outil de capture WebVPN qui vous permet de consigner les informations relatives aux sites Web qui ne s'affichent pas correctement sur une connexion WebVPN. Vous pouvez activer l'outil de capture à partir de l'interface de ligne de commande (CLI) de l'appliance de sécurité. Les données enregistrées par cet outil peuvent aider votre représentant du service d'assistance à la clientèle Cisco à résoudre les problèmes.

Remarque : lorsque vous activez l'outil de capture WebVPN, cela a un impact sur les performances de l'appliance de sécurité. Veillez à désactiver l'outil de capture après avoir généré les fichiers de sortie.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez aux exigences suivantes avant d'essayer cette configuration :

- Utilisez l'interface de ligne de commande (CLI) afin de configurer le dispositif de sécurité adaptatif de la gamme Cisco ASA 5500.

Components Used

Les informations de ce document sont basées sur l'appliance de sécurité adaptable de la gamme Cisco ASA 5500 qui exécute la version 7.0.

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.

Conventions

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

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Fichiers de sortie de l'outil de capture WebVPN

Lorsque l'outil de capture WebVPN est activé, l'outil de capture stocke les données de la première URL visitée dans ces fichiers :

- original.000 : contient les données échangées entre le dispositif de sécurité et le serveur Web.
- mangled.000 : contient les données échangées entre le dispositif de sécurité et le navigateur.

Pour chaque capture subséquente, l'outil de capture génère des fichiers originaux supplémentaires correspondants.<nnn> et gérés.<nnn> et incrémente les extensions de fichier. Dans cet exemple, la sortie de la commande **dir** affiche trois ensembles de fichiers à partir de trois captures d'URL :

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6           -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
3399        -rw-        4928            08:32:51 Feb 14 2005 ORIGINAL.001
3400        -rw-        6167            08:32:51 Feb 14 2005 MANGLED.001
3401        -rw-        5264            08:35:23 Feb 14 2005 ORIGINAL.002
3402        -rw-        6503            08:35:23 Feb 14 2005 MANGLED.002
hostname#
```

Activer l'outil de capture WebVPN

Remarque : Le système de fichiers Flash présente des limites lorsque plusieurs fichiers sont ouverts pour l'écriture. L'outil de capture WebVPN peut entraîner une corruption du système de fichiers lorsque plusieurs fichiers de capture sont mis à jour simultanément. Si cette défaillance

doit se produire avec l'outil de capture, contactez le centre d'assistance technique Cisco (TAC).

Afin d'activer l'outil de capture WebVPN, utilisez la commande **debug menu webvpn 67** à partir du mode d'exécution privilégié :

```
debug menu webvpn 67
```

Where:

- **cmd** est 0 ou 1. 0 désactive la capture. 1 active la capture.
- **user** est le nom d'utilisateur à associer pour la capture de données.
- **url** est le préfixe d'URL à mettre en correspondance pour la capture de données. Utilisez l'un des formats d'URL suivants :Utilisez /http pour capturer toutes les données.Utilisez /http/0/<serveur/chemin> pour capturer le trafic HTTP vers le serveur identifié par <serveur/chemin>.Utilisez /https/0/<serveur/chemin> pour capturer le trafic HTTPS vers le serveur identifié par <serveur/chemin>.

Utilisez la commande **debug menu webvpn 67 0** afin de désactiver la capture.

Dans cet exemple, l'outil de capture WebVPN est activé pour capturer le trafic HTTP de l'utilisateur2 qui visite le site Web wwwin.abcd.com/hr/people :

```
hostname#debug menu webvpn 67 1 user2 /http/0/wwwin.abcd.com/hr/people
Mangle Logging: ON
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

Dans cet exemple, l'outil de capture WebVPN est désactivé :

```
hostname#debug menu webvpn 67 0
Mangle Logging: OFF
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

Recherche et téléchargement des fichiers de sortie de l'outil de capture WebVPN

Utilisez la commande **dir** afin de localiser les fichiers de sortie de l'outil de capture WebVPN. Cet exemple montre la sortie de la commande **dir** et inclut les fichiers ORIGINAL.000 et MANGLED.000 qui ont été générés :

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6         -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
```

```
hostname#
```

Vous pouvez télécharger les fichiers de sortie de l'outil de capture WebVPN sur un autre ordinateur à l'aide de la commande **copy flash**. Dans cet exemple, les fichiers ORIGINAL.000 et MANGLED.000 sont téléchargés :

```
hostname#copy flash:/original.000 tftp://10/86.194.191/original.000
Source filename [original.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [original.000]?
!!!!!!
21601 bytes copied in 0.370 secs
hostname#copy flash:/mangled.000 tftp://10/86.194.191/mangled.000
Source filename [mangled.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [mangled.000]?
!!!!!!
23526 bytes copied in 0.380 secs
hostname#
```

Remarque : afin d'éviter toute corruption possible du système de fichiers, ne pas autoriser la suppression des fichiers originaux.<nn> et gérés.<nnn> des captures précédentes. Lorsque vous désactivez l'outil de capture, supprimez les anciens fichiers afin d'empêcher la corruption du système de fichiers.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guides de configuration des appareils de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems