Contenu

Introduction

Ce document adresse la condition requise pour activer la caractéristique d'Interception TCP de Cisco sur des Routeurs de Cisco IOS/IOS-XE. L'Interception TCP est exigée pour protéger des serveurs de TCP contre des attaques par inondation SYN de TCP, un type d'attaque par déni de service.

Problème

Nous ne pouvons pas configurer ? Interception TCP d'IP ? sur des Routeurs ISR G1/G2/G3 et ASR1k. Sont ci-dessous les logs concernant la même chose :

1. **Pour des Routeurs ISR G1 :**

```
Ver de Router#show

Logiciel de Cisco IOS, logiciel 2800 (C2800NM-IPBASEK9-M), version
15.1(4)M12a, LOGICIEL de VERSION (fc1)

La disponibilité de routeur est de 14 minutes

Le système est revenu à la ROM par la recharge à UTC Tue de 07:45:56
le 1er novembre 2016

Le fichier d'image de système est "flash:c2800nm-ipbasek9-mz.151-
4.M12a(1).bpo

Dernier type de recharge : Recharge normale

<omitted>

Cisco 2811 (révision 1.0) avec les octets 512000K/12288K de la
mémoire.

ID FHK1404F3U8 de panneau de processeur

2 interfaces FastEthernet

1 port canalisé E1/PRI

La configuration de DRAM est 64 bits au loin avec la parité activée.

octets 239K de mémoire non-volatile de configuration.
```

```
octets 250368K d'ATA CompactFlash (lecture/écriture)

Données de licence :

Permis UDI :

-------------------------------------------------

SN de Device# PID

-------------------------------------------------

*0 CISCO2811 FHK1404F3U8

Le registre de configuration est 0x2102

Configuration t de Router#

Sélectionnez les commandes de configuration, une par la ligne.
Extrémité avec CNTL/Z.

TCP de Router(config)#ip ?

 le RST-compte configurent le compte de commande de puissance RST

 l'async-mobilité configurent l'async-mobilité

 taille de bloc de TCP de bloc-taille

 notification d'encombrement explicite d'enable d'ecn

    taille maximum de segment d'initiale de TCP de mss

 découverte de MTU de chemin d'enable de chemin-mtu-détection sur de
nouvelles connexions TCP

 file d'attente maximum de queuemax des paquets TCP sortants

 tcp selective-ack de l'enable sélectif-ACK

 set time de synwait-temps d'attendre sur de nouvelles connexions TCP

 option de tcp timestamp d'enable d'horodateur

 taille de la fenêtre de TCP de taille de la fenêtre
```

2. Pour des Routeurs d'ISR G2 :

```
Ver de Router#show

Logiciel de Cisco IOS, logiciel C1900 (C1900-UNIVERSALK9-M), version
15.4(3)M4, LOGICIEL de VERSION (fc1)
```

<omitted>

La disponibilité de routeur est de 1 minute

Le système est revenu à la ROM par la recharge à UTC Lun de 10:28:40 le 31 octobre 2016

Le fichier d'image de système est "flash:c1900-universalk9-mz.SPA.154-3.M4.bpo

Dernier type de recharge : Recharge normale

Dernière raison de recharge : Commande de recharge

<omitted>

Cisco CISCO1941/K9 (révision 1.0) avec les octets 2543552K/77824K de la mémoire.

ID FHK141571QW de panneau de processeur

4 interfaces FastEthernet

<omitted>

Données de licence de module de technologie pour Module:'c1900

Technologie-module de Technologie-module de technologie

Prochaine réinitialisation de type en cours

---

ipbase ipbasek9 ipbasek9 permanent

Sécurité securityk9 RightToUse securityk9

données aucun aucun aucun

NtwkEss aucun aucun aucun

Le registre de configuration est 0x2102

Configuration t de Router#

Sélectionnez les commandes de configuration, une par la ligne. Extrémité avec CNTL/Z.

TCP de Router(config)#ip ?

```
le RST-compte configurent le compte de commande de puissance RST

l'async-mobilité configurent l'async-mobilité

taille de bloc de TCP de bloc-taille

notification d'encombrement explicite d'enable d'ecn

la keepalive configurent des paramètres de keepalive de TCP

taille maximum de segment d'initiale de TCP de mss

découverte de MTU de chemin d'enable de chemin-mtu-détection sur de
nouvelles connexions TCP

file d'attente maximum de queuemax des paquets TCP sortants

tcp selective-ack de l'enable sélectif-ACK

set time de synwait-temps d'attendre sur de nouvelles connexions TCP

option de tcp timestamp d'enable d'horodateur

taille de la fenêtre de TCP de taille de la fenêtre
```

3. **Pour des Routeurs ISR G3 :**

```
Ver de Router#sh

Logiciel Cisco IOS XE version 2, version 03.15.02.S - Version
standard de support

Logiciel de Cisco IOS, logiciel ISR (X86_64_LINUX_IOSD-UNIVERSALK9-
M), version 15.5(2)S2, LOGICIEL de VERSION (fc1)

Soutien technique : http://www.cisco.com/techsupport

Copyright © 1986-2015 par Cisco Systems, Inc.

Fri compilé 16-Oct-15 18:00 par le mcpre

<omitted>

La disponibilité de routeur est de 7 minutes

La disponibilité pour ce processeur de contrôle est de 8 minutes

Système retourné à la ROM par la recharge

Le fichier d'image de système est "bootflash:isr4300-
universalk9.03.15.02.S.155-2.S2-std.SPA.bpo

Dernière raison de recharge : Commande de recharge
```

<omitted>

Données de licence de module de technologie :

Technologie-module de Technologie-module de technologie

Prochaine réinitialisation de type en cours

---

appx aucun aucun aucun

uc uck9 uck9 permanent

Sécurité securityk9 EvalRightToUse securityk9

ipbase ipbasek9 ipbasek9 permanent

processeur de Cisco ISR4331/K9 (1RU) avec les octets 1665776K/6147K de la mémoire.

ID FDO2012A0AT de panneau de processeur

3 interfaces de Gigabit Ethernet

octets 32768K de mémoire non-volatile de configuration.

octets 4194304K de mémoire physique.

octets 3223551K de mémoire flash au bootflash :.

Le registre de configuration est 0x2102

Configuration t de Router#

Sélectionnez les commandes de configuration, une par la ligne. Extrémité avec CNTL/Z.

TCP de Router(config)#ip ?

le RST-compte configurent le compte de commande de puissance RST

l'async-mobilité configurent l'async-mobilité

taille de bloc de TCP de bloc-taille

notification d'encombrement explicite d'enable d'ecn

la keepalive configurent des paramètres de keepalive de TCP

taille maximum de segment d'initiale de TCP de mss

découverte de MTU de chemin d'enable de chemin-mtu-détection sur de nouvelles connexions TCP

file d'attente maximum de queuemax des paquets TCP sortants

tcp selective-ack de l'enable sélectif-ACK

set time de synwait-temps d'attendre sur de nouvelles connexions TCP

option de tcp timestamp d'enable d'horodateur

taille de la fenêtre de TCP de taille de la fenêtre

4. **Pour des Routeurs ASR1k :**

Version de Routeur#show

Logiciel Cisco IOS XE version 2, version 03.16.01a.S - Version étendue de support

Logiciel de Cisco IOS, logiciel ASR1000 (X86_64_LINUX_IOSD-UNIVERSAL-M), version 15.5(3)S1a, LOGICIEL de VERSION (fc1)

Soutien technique : http://www.cisco.com/techsupport

Copyright © 1986-2015 par Cisco Systems, Inc.

Compilé épousez 04-Nov-15 13:57 par le mcpre

<omitted>

La disponibilité de routeur est de 1 minute

La disponibilité pour ce processeur de contrôle est de 2 minutes

Système retourné à la ROM par la recharge

Le fichier d'image de système est "bootflash:asr1001x-universal.03.16.01a.S.155-3.S1a-ext.SPA.bpo

Dernière raison de recharge : PowerOn

Permis de niveau : ipbase

Type de licence : Permanent

Prochain niveau de permis de recharge : ipbase

processeur de Cisco ASR1001-X (1NG) (révision 1NG) avec les octets 3753592K/6147K de la mémoire.

ID FXS1925Q33T de panneau de processeur

```
6 interfaces de Gigabit Ethernet

2 Dix interfaces de Gigabit Ethernet

octets 32768K de mémoire non-volatile de configuration.

octets 8388608K de mémoire physique.

les octets 6684671K d'eUSB flashent au bootflash :.

Le registre de configuration est 0x2102

ASR-HUB-01#config t

Sélectionnez les commandes de configuration, une par la ligne.
Extrémité avec CNTL/Z.

ASR-HUB-01(config)#li

TCP ASR-HUB-01(config)#ip ?

 le RST-compte configurent le compte de commande de puissance RST

 l'async-mobilité configurent l'async-mobilité

 taille de bloc de TCP de bloc-taille

 notification d'encombrement explicite d'enable d'ecn

 la keepalive configurent des paramètres de keepalive de TCP

 taille maximum de segment d'initiale de TCP de mss

 découverte de MTU de chemin d'enable de chemin-mtu-détection sur de
nouvelles connexions TCP

 file d'attente maximum de queuemax des paquets TCP sortants

 tcp selective-ack de l'enable sélectif-ACK

 set time de synwait-temps d'attendre sur de nouvelles connexions TCP

 option de tcp timestamp d'enable d'horodateur

 taille de la fenêtre de TCP de taille de la fenêtre
```

Solution

Pour activer l'Interception TCP de caractéristique, nous aurions besoin :

- Minimum d'ensemble de caractéristiques d'**entbase** sur les Routeurs ISR G1
- **Appxk9/ Datak9** sur le routeur de gammes ISRG2 et G3

- Permis minimum d'**advipservices** sur le routeur de la gamme ASR1k.

Une fois que nous activons le permis prié sur la plate-forme, nous pourrons configurer la même chose :

```
TCP de Router(config)#ip ?

 le RST-compte configurent le compte de commande de puissance RST

 l'async-mobilité configurent l'async-mobilité

 taille de bloc de TCP de bloc-taille

 notification d'encombrement explicite d'enable d'ecn

 intercepter de TCP d'enable d'interception

 la keepalive configurent des paramètres de keepalive de TCP

 taille maximum de segment d'initiale de TCP de mss

 découverte de MTU de chemin d'enable de chemin-mtu-détection sur de
nouvelles connexions TCP

 file d'attente maximum de queuemax des paquets TCP sortants

 tcp selective-ack de l'enable sélectif-ACK

 set time de synwait-temps d'attendre sur de nouvelles connexions TCP

 option de tcp timestamp d'enable d'horodateur

 taille de la fenêtre de TCP de taille de la fenêtre
```

Références

http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfdenl.html