

Cisco IOS®/IOS-XEルータでのTCPインターセプトの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[ISR G1ルータ用](#)

[ISR G2ルータ用](#)

[ISR G3ルータ用](#)

[ASR1kルータの場合](#)

[解決方法](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco IOS®/IOS-XEルータでCisco Transmission Control Protocol(TCP)インターセプト機能を有効にする要件について説明します。TCPインターセプトは、TCP synchronize(SYN)フラッディング攻撃 (サービス拒否攻撃の一種) からTCPサーバを保護するために必要です。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

ISR G1/G2/G3およびASR1kルータで「ip tcp intercept」を設定できません。ログは次のとおりです。

・ISR G1ルータ用

```
Router#show ver
```

```
Cisco IOS® Software, 2800 Software (C2800NM-IPBASEK9-M), Version 15.1(4)M12a, RELEASE SOFTWARE (fcl)
Router uptime is 14 minutes
System returned to ROM by reload at 07:45:56 UTC Tue Nov 1 2016
System image file is "flash:c2800nm-ipbasek9-mz.151-4.M12a(1).bin"
```

```
Last reload type: Normal Reload
```

```
<omitted>
```

```
Cisco 2811 (revision 1.0) with 512000K/12288K bytes of memory.
Processor board ID FHK1404F3U8
2 FastEthernet interfaces
1 Channelized E1/PRI port
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
250368K bytes of ATA CompactFlash (Read/Write)
```

```
License Info:
```

```
License UDI:
```

```
-----
Device#   PID                SN
-----
*0        CISCO2811          FHK1404F3U8
```

```
Configuration register is 0x2102
```

```
Router# config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#ip tcp ?
```

```
  RST-count          Configure RST throttle count
  async-mobility     Configure async-mobility
  chunk-size         TCP chunk size
  ecn                Enable Explicit Congestion Notification
  mss                TCP initial maximum segment size
  path-mtu-discovery Enable path-MTU discovery on new TCP connections
  queuemax           Maximum queue of outgoing TCP packets
  selective-ack      Enable TCP selective-ACK
  synwait-time       Set time to wait on new TCP connections
  timestamp          Enable TCP timestamp option
  window-size        TCP window size
```

• ISR G2ルータ用

Router#show ver

Cisco IOS® Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M4, RELEASE SOFTWARE (fcl)

<omitted>

Router uptime is 1 minute

System returned to ROM by reload at 10:28:40 UTC Mon Oct 31 2016

System image file is "flash:c1900-universalk9-mz.SPA.154-3.M4.bin"

Last reload type: Normal Reload

Last reload reason: Reload Command

<omitted>

Cisco CISC01941/K9 (revision 1.0) with 2543552K/77824K bytes of memory.

Processor board ID FHK141571QW

4 FastEthernet interfaces

<omitted>

Technology Package License Information for Module:'c1900'

```
-----  
Technology      Technology-package      Technology-package  
                Current          Type          Next reboot  
-----  
ipbase          ipbasek9                Permanent    ipbasek9  
security        securityk9               RightToUse   securityk9  
data            None                     None         None  
NtwkEss         None                     None         None
```

Configuration register is 0x2102

Router# config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip tcp ?

```
RST-count          Configure RST throttle count  
async-mobility     Configure async-mobility  
chunk-size         TCP chunk size  
ecn                Enable Explicit Congestion Notification  
keepalive          Configure TCP Keepalive parameters  
mss                TCP initial maximum segment size  
path-mtu-discovery Enable path-MTU discovery on new TCP connections  
queuemax           Maximum queue of outgoing TCP packets  
selective-ack      Enable TCP selective-ACK  
synwait-time       Set time to wait on new TCP connections  
timestamp          Enable TCP timestamp option  
window-size        TCP window size
```

• ISR G3ルータ用

Router#sh ver

Cisco IOS® XE Software, Version 03.15.02.S - Standard Support Release
Cisco IOS® Software, ISR Software (X86_64_LINUX_IOS® D-UNIVERSALK9-M), Version 15.5(2)S2,
RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 16-Oct-15 18:00 by mcpre

<omitted>

Router uptime is 7 minutes
Uptime for this control processor is 8 minutes
System returned to ROM by reload
System image file is "bootflash:isr4300-universalk9.03.15.02.S.155-2.S2-std.SPA.bin"
Last reload reason: Reload Command

<omitted>

Technology Package License Information:

```
-----  
Technology      Technology-package      Technology-package  
                Current      Type                Next reboot  
-----  
appx            None                None                None  
uc              uck9                Permanent           uck9  
security        securityk9          EvalRightToUse     securityk9  
ipbase          ipbasek9            Permanent           ipbasek9  
-----
```

cisco ISR4331/K9 (1RU) processor with 1665776K/6147K bytes of memory.
Processor board ID FDO2012A0AT
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.

Configuration register is 0x2102

Router# config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip tcp ?

```
RST-count          Configure RST throttle count  
async-mobility     Configure async-mobility  
chunk-size         TCP chunk size  
ecn                Enable Explicit Congestion Notification  
keepalive          Configure TCP Keepalive parameters  
mss                TCP initial maximum segment size  
path-mtu-discovery Enable path-MTU discovery on new TCP connections  
queuemax           Maximum queue of outgoing TCP packets  
selective-ack      Enable TCP selective-ACK  
synwait-time       Set time to wait on new TCP connections  
timestamp          Enable TCP timestamp option  
window-size        TCP window size
```

• ASR1kルータの場合

```
Router#show version

Cisco IOS® XE Software, Version 03.16.01a.S - Extended Support Release
Cisco IOS® Software, ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSAL-M), Version 15.5(3)S1a,
RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Nov-15 13:57 by mcpre
```

<omitted>

```
Router uptime is 1 minute
Uptime for this control processor is 2 minutes
System returned to ROM by reload
System image file is "bootflash:asr1001x-universal.03.16.01a.S.155-3.S1a-ext.SPA.bin"
Last reload reason: PowerOn
```

```
License Level: ipbase
License Type: Permanent
Next reload license Level: ipbase
```

```
cisco ASR1001-X (1NG) processor (revision 1NG) with 3753592K/6147K bytes of memory.
Processor board ID FXS1925Q33T
6 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
6684671K bytes of eUSB flash at bootflash:
```

```
Configuration register is 0x2102
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#ip tcp ?
RST-count          Configure RST throttle count
async-mobility     Configure async-mobility
chunk-size         TCP chunk size
ecn                Enable Explicit Congestion Notification
keepalive          Configure TCP Keepalive parameters
mss                TCP initial maximum segment size
path-mtu-discovery Enable path-MTU discovery on new TCP connections
queuemax           Maximum queue of outgoing TCP packets
selective-ack      Enable TCP selective-ACK
synwait-time       Set time to wait on new TCP connections
timestamp          Enable TCP timestamp option
window-size        TCP window size
```

解決方法

TCPインターセプト機能を有効にするには、次が必要です。

- ISR G1ルータのentbaseフィーチャセットの最小
- ISRG2およびG3シリーズルータ上のAppxk9/Datak9
- ASR1kシリーズルータのアドビサービスライセンスの最小要件

プラットフォームで必要なライセンスを有効にすると、次のように設定できます。

```
Router(config)#ip tcp ?
RST-count          Configure RST throttle count
async-mobility     Configure async-mobility
```

chunk-size	TCP chunk size
ecn	Enable Explicit Congestion Notification
intercept	Enable TCP intercepting
keepalive	Configure TCP Keepalive parameters
mss	TCP initial maximum segment size
path-mtu-discovery	Enable path-MTU discovery on new TCP connections
queuemax	Maximum queue of outgoing TCP packets
selective-ack	Enable TCP selective-ACK
synwait-time	Set time to wait on new TCP connections
timestamp	Enable TCP timestamp option
window-size	TCP window size

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfdenl.html
- [テクニカル サポートとドキュメント – Cisco Systems](#)