

Содержание

[Введение](#)

[Проблема](#)

[Решение](#)

Введение

Этот документ удовлетворяет требованию для включения функции перехвата TCP Cisco на Cisco IOS/IOS-XE маршрутизаторы. Перехват TCP требуется, чтобы защищать серверы TCP от СИНХРОННЫХ АТАК TCP, типа атаки отказ в обслуживании.

Проблема

Мы неспособны настроить? IP перехват TCP? на ISR G1/G2/G3 и маршрутизаторах ASR1k. Ниже журналы относительно того же:

1. Для маршрутизаторов ISR G1:

Версия Router#show

Программное обеспечение Cisco IOS, 2800 программных обеспечений (C2800NM-IPBASEK9-M), версия 15.1 (4) M12a, РЕЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (fc1)

Период работоспособного состояния маршрутизатора составляет 14 минут

Система возвратила к ПЗУ повторной загрузкой в 7:45:56 UTC вторник 1 ноября 2016

Файл образа системы "**flash:c2800nm-ipbasek9-mz.151-4. M12a (1) .bin**"

Последний тип повторной загрузки: Обычная Повторная загрузка

<опущено>

Cisco 2811 (revision 1.0) с 512000К/12288К байтами памяти.

Идентификатор процессорной платы FHK1404F3U8

2 Интерфейса Fast Ethernet

1 С разделением каналов порт E1/PRI

Конфигурация динамического ОЗУ 64 бита шириной с включенным паритетом.

Байты 239К энергонезависимой памяти.

Байты 250368К CompactFlash ATA (Чтение-запись)

Информация лицензии:

Лицензия UDI:

SN PID Device#

* 0 CISCO2811 FHK1404F3U8

Configuration register is 0x2102

Config t Router#

!--- Введите команды конфигурации (по одной для каждой линии). В конце введите CNTL/Z.

Маршрутизатор (config) #ip tcp?

Количество RST Настраивает количество дросселя RST

асинхронная мобильность Настраивает асинхронную мобильность

TCP размера блока разделяет размер на блоки

ecn Включают Уведомление о явной перегрузке

Maximum Segment Size начальной буквы TCP mss

path-mtu-discovery Включает обнаружение MTU-маршрута на новых TCP -
подключениях

Максимальный размер очереди queueмах исходящих пакетов
TCP

выборочный-ack Включают TCP selective-ACK

synwait-разовый Set time для ожидания на новых TCP -
подключениях

метка времени Включает опцию TCP timestamp

размер окна TCP размера окна

2. Для маршрутизаторов ISR G2:

Версия Router#show

Программное обеспечение Cisco IOS, программное обеспечение C1900
(C1900-UNIVERSALK9-M), версия 15.4 (3) M4, РЕЛИЗ ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ (fc1)

<опущено>

Период работоспособного состояния маршрутизатора составляет 1 минуту

Система возвратила к ПЗУ повторной загрузкой в 10:28:40 UTC
понедельник 31 октября 2016

Файл образа системы "flash:c1900-universalk9-mz. SPA.154-3. M4.bin"

Последний тип повторной загрузки: Обычная Повторная загрузка

Последняя причина перезагрузки: Команда Повторной загрузки

<опущено>

Cisco CISC01941/K9 (revision 1.0) с 2543552К/77824К байтами памяти.

Идентификатор процессорной платы FHK141571QW

4 Интерфейса Fast Ethernet

<опущено>

Лицензионные сведения комплексной технологии для модуля:'c1900'

Комплексная технология комплексной технологии
технологии

Текущий	Тип	Следующая перезагрузка
---------	-----	------------------------

ipbase ipbasek9	Постоянный	ipbasek9
-----------------	------------	----------

безопасность securityk9 RightToUse securityk9

данные один	Ни один	Ни один	Ни
------------------------	----------------	----------------	-----------

NtwkEss	ни один	ни один	ни один
---------	---------	---------	---------

Configuration register is 0x2102

Config t Router#

!--- Введите команды конфигурации (по одной для каждой линии). В
конце введите CNTL/Z.

Маршрутизатор (config) #ip tcp?

Количество RST	Настраивает количество дросселя RST
асинхронная мобильность	Настраивает асинхронную мобильность
TCP размера блока	разделяет размер на блоки
ecn	Включают Уведомление о явной перегрузке
поддержка активности активности TCP	Настраивает Параметры поддержки
	Maximum Segment Size начальной буквы TCP mss
path-mtu-discovery	Включает обнаружение MTU-маршрута на новых TCP - подключениях
TCP	Максимальный размер очереди queueмах исходящих пакетов
выборочный-ack	Включают TCP selective-ACK
synwait-разовый подключениях	Set time для ожидания на новых TCP -
метка времени	Включает опцию TCP timestamp
	размер окна TCP размера окна

3. Для маршрутизаторов ISR G3:

Версия Router#sh

Программное обеспечение Cisco IOS XE, версия 03.15.02. S -
стандартный выпуск поддержки

Программное обеспечение Cisco IOS, программное обеспечение ISR
(X86_64_LINUX_IOSD-UNIVERSALK9-M), версия 15.5 (2) S2, РЕЛИЗ
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (fc1)

Technical support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2015 Cisco Systems, Inc.

Скомпилированный пятница 16 октября 15 18:00 mspre

<опущено>

Период работоспособного состояния маршрутизатора составляет 7 минут

Время работы без сбоев для этого управляющего процессора составляет 8 минут

System returned to ROM by reload

Файл образа системы "bootflash:isr4300-universalk9.03.15.02. S.155-2. S2-std. SPA.bin"

Последняя причина перезагрузки: Команда Повторной загрузки

<опущено>

Лицензионные сведения комплексной технологии:

Комплексная технология комплексной технологии технологии
Текущий Тип Следующая перезагрузка

аррх один	Ни один	Ни один	Ни
	uc uck9	Постоянный	uck9
	безопасность securityk9	EvalRightToUse	securityk9
	ipbase ipbasek9	Постоянный	ipbasek9

процессор ISR4331/K9 (1RU) Cisco с 1665776К/6147К байтами памяти.

Идентификатор процессорной платы FDO2012A0AT

3 Интерфейса Gigabit Ethernet

Байты 32768К энергонезависимой памяти.

Байты 4194304К физической памяти.

Байты 3223551К флэш-памяти в bootflash:.

Configuration register is 0x2102

Config t Router#

!--- Введите команды конфигурации (по одной для каждой линии). В конце введите CNTL/Z.

Маршрутизатор (config) #ip tcp?

Количество RST Настраивает количество дросселя RST

асинхронная мобильность Настраивает асинхронную мобильность

TCP размера блока разделяет размер на блоки

есп Включают Уведомление о явной перегрузке
 поддержка активности Настраивает Параметры поддержки
 активности TCP
 Maximum Segment Size начальной буквы TCP mss
 path-mtu-discovery Включает обнаружение MTU-маршрута на новых TCP -
 подключениях
 Максимальный размер очереди queueмах исходящих пакетов
 TCP
 выборочный-ack Включают TCP selective-ACK
 synwait-разовый Set time для ожидания на новых TCP -
 подключениях
 метка времени Включает опцию TCP timestamp
 размер окна TCP размера окна

4. Для маршрутизаторов ASR1k:

Версия Router#show

Программное обеспечение Cisco IOS XE, версия 03.16.01a. S -
 расширенный выпуск поддержки

Программное обеспечение Cisco IOS, программное обеспечение ASR1000
 (X86_64_LINUX_IOSD-UNIVERSAL-M), версия 15.5 (3) S1a, РЕЛИЗ
 ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (fc1)

Technical support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2015 Cisco Systems, Inc.

Скомпилированный жен& 04 ноября 15 13:57 mсpre

<опущено>

Период работоспособного состояния маршрутизатора составляет 1 минуту

Время работы без сбоев для этого управляющего процессора составляет 2
 минуты

System returned to ROM by reload

Файл образа системы "bootflash:asr1001x-universal.03.16.01a. S.155-3.
 S1a-расширение. SPA.bin"

Последняя причина перезагрузки: PowerOn

Уровень лицензии: iP Base

Тип лицензии: постоянный

Следующая лицензия повторной загрузки Уровень: iP Base

процессор ASR1001-X (1NG) Cisco (пересмотр 1 нг) с 3753592К/6147К байтами памяти.

Идентификатор процессорной платы FXS1925Q33T

6 Интерфейсов Gigabit Ethernet

2 Десять Интерфейсов Gigabit Ethernet

Байты 32768К энергонезависимой памяти.

Байты 8388608К физической памяти.

Байты 6684671К eUSB мигают в bootflash:.

Configuration register is 0x2102

ASR-HUB-01#config t

!--- Введите команды конфигурации (по одной для каждой линии). В конце введите CNTL/Z.

ASR-HUB-01 (config) #li

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

Количество RST Настраивает количество дросселя RST

асинхронная мобильность Настраивает асинхронную мобильность

TCP размера блока разделяет размер на блоки

ecn Включают Уведомление о явной перегрузке

поддержка активности Настраивает Параметры поддержки активности TCP

Maximum Segment Size начальной буквы TCP mss

path-mtu-discovery Включает обнаружение MTU-маршрута на новых TCP - подключениях

Максимальный размер очереди queueтах исходящих пакетов TCP

выборочный-ack Включают TCP selective-ACK

synwait-разовый Set time для ожидания на новых TCP -
подключениях

метка времени Включает опцию TCP timestamp

размер окна TCP размера окна

Решение

Для включения Перехвата TCP функции нам было бы нужно:

- Минимум **entbase** набора функций на маршрутизаторах ISR G1
- **Appxk9/Datak9** на ISRG2 и series маршрутизаторе G3
- Минимум **advipservices** лицензия на series маршрутизаторе ASR1k.

Как только мы включаем необходимую лицензию на платформе, мы будем в состоянии настроить то же:

Маршрутизатор (config) #ip tcp?

Количество RST Настраивает количество дросселя RST

асинхронная мобильность Настраивает асинхронную мобильность

TCP размера блока разделяет размер на блоки

esn Включают Уведомление о явной перегрузке

точка пересечения Включает прерывание TCP

поддержка активности Настраивает Параметры поддержки
активности TCP

Maximum Segment Size начальной буквы TCP mss

path-mtu-discovery Включает обнаружение MTU-маршрута на новых TCP -
подключениях

Максимальный размер очереди queueмах исходящих пакетов
TCP

выборочный-ack Включают TCP selective-ACK

synwait-разовый Set time для ожидания на новых TCP -
подключениях

метка времени Включает опцию TCP timestamp

размер окна TCP размера окна

Ссылки

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