Встроенный режим отслеживания сеанса TCP на IPS

Содержание

Введение

Этот документ описывает Встроенную Характеристику отслеживания Сеанса TCP устройства Системы предотвращения вторжений (IPS).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- IPS устройства серии 4200 настроен со встроенными интерфейсами.
- Знание протокола TCP и трафиков.

Используемые компоненты

Информация в данном документе основана на следующих положениях:

- IPS 4270 с выпуском ПО 7.1 (7)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

В определенных встроенных сценариях развертывания IPS пакеты от потока TCP могут быть замечены дважды механизмом Нормализатора, который приводит к отбрасываниям из-за неподходящего потокового отслеживания. Эта ситуация, как правило, замечается, когда трафик маршрутизируется через множественные виртуальные локальные сети (VLAN) или интерфейсные пары, которые проверены одиночным действительным датчиком. Когда трафик или для направления получен от других VLAN или для интерфейсов, эта проблема далее осложнена необходимостью, чтобы позволить асимметричному трафику объединяться для надлежащего потокового отслеживания.

Схема сети

Проблема

В этой топологии сети клиент на внутренней сети инициирует соединение HTTP к серверу на внешней сети. Оба сегмента сети разделены межсетевым экраном Устройства адаптивной защиты (ASA). В этом дизайне одиночное устройство IPS настроено для подключений обоим внутренние и внешние VLAN с двумя наборами встроенных интерфейсных пар. Когда клиент инициирует сеанс к серверу, SYN TCP (синхронизируются), пакет берет этот путь (исходящий поток) через IPS и ASA:

Клиент> IPS G3/0> *vs0* > IPS G3/1> ASA G0/0> ASA G0/1> IPS G3/2> *vs0* > IPS G3/3> Сервер

После исходящего потока SYN TCP, передаваемый клиентом, замечен **vs0** действительным датчиком, поскольку пакет пересекает пару внутреннего интерфейса к Внутреннему интерфейсу ASA и снова когда пакет пересекает пару внешнего интерфейса к Web-серверу. В симметричном сценарии та же ситуация происходит в адресе возврата с ACK SYN (положительное подтверждение) и последующие пакеты от Web-сервера. Когда IPS пытается объединить потоки в одиночный TCP - подключение, копии каждого пакета в соединении наблюдаются, который приводит к запутанному Нормализатору и отброшенным пакетам. Чтобы подтвердить, встречается ли IPS с этой ситуацией, выходные данные **статистики показа virt** команда показывают большое число 1330 подписей Нормализатора TCP, которые срабатывают, а также большое число модифицированных и отклоненных пакетов и соединений.

Решение

Опция **Inline TCP Session Tracking Mode** может использоваться для преодоления ситуаций, таких как это. Существует три возможных режима, которые могут быть настроены:

1. **Действительный Датчик (Настройка по умолчанию)** - Контролирует в асимметричной ситуации с развертываниями, где клиентские пакеты замечены на одной встроенной паре, в то время как пакеты сервера замечены на второй интерфейсной паре. Две интерфейсных пары должны быть проверены вместе для наблюдения обеих сторон соединения.
2. **Интерфейс и VLAN** - Это - обходной путь к примеру топологии, показанному в этом документе, в котором две или больше встроенных интерфейсных пары назначены на тот же действительный датчик. С этой включенной опцией TCP - подключение может пересечь несколько пар, которые позволяют Нормализатору отслеживать сеансы TCP независимо для каждой встроенной пары.
3. **VLAN Только** - Это - очень редкая комбинация первых двух опций и используется, вы контролируете сочетание множества несимметричные схемы. **VLAN 1** на левой интерфейсной паре имеет клиентские пакеты и должен быть объединен с **VLAN 1** на правильной интерфейсной паре, которая имеет пакеты сервера. В этом случае трафик объединен через всех интерфейсных пар, но отдельный VLAN. Например, VLAN 1 пакет через все интерфейсы размещена вместе; пакеты VLAN 2 от всех интерфейсов размещены вместе, но VLAN 1 и пакеты VLAN 2 никогда не размещаются вместе для отслеживания сеанса TCP.

Для вышеупомянутого примера топологии существует два способа, которыми может быть решена проблема:

Решение 1

Переместите каждую встроенную интерфейсную пару в ее собственный действительный датчик. Например, одна пара на **vs0** и одна пара на **vs1**. Когда существует меньше чем четыре встроенных пары (из-за предела платформы четырех действительных датчиков), этот метод обычно рекомендуется. Нормализатор рассматривает двойные потоки как два отдельных подключения.

Решение 2

Настройте встроенный Режим отслеживания Сеанса TCP для **Взаимодействия через интерфейс и VLAN**. Этот метод рекомендуется, когда существует больше чем четыре встроенных пары, в этом случае, вы вынуждены разместить множественных встроенных пар в одиночный действительный датчик. Нормализатор рассматривает пакеты на других встроенных парах как абсолютно другие соединения в том же действительном датчике.

Настройка

Вот конфигурация для разделения действительного датчика на встроенную интерфейсную

пару:

```
IPS4510-01# conf t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Inside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# virtual-sensor vs1

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Outside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

IPS4510-01(config)# exit
```

Вот конфигурация для интерфейса и VLAN:

```
IPS4510-01# config t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# inline-tcp-session interface-and-vlan

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

Apply Changes?[yes]: yes

Warning: Change of TCP session tracking mode will not take effect until restart.

IPS4510-01(config)# exit

IPS4510-01# reset
```

Проверка

- Используйте **статистику показа virt | b команда statistics этапа Нормализатора TCP** и анализ для **Отброшенного**, **Двойного**, **Запрещенного**, или **Пакеты SendAck Передаваемая** ненулевая статистика в Нормализаторе TCP.
- Используйте **статистику показа virt | b** команда **количества SigEvent На подпись** и рассмотрите на 1330 подписи, которые запустили в сочетании с TCP статистику Normalier от предыдущей команды.

Дополнительные сведения

- [Руководство конфигурации интерфейса командой строки датчика системы предотвращения вторжений Cisco (IPS) для IPS 7.0 - встроенный режим отслеживания]

сеанса TCP
- Руководство по конфигурации Cisco Intrusion Prevention System Manager Express для IPS 7.1 - встроенный режим отслеживания сеанса TCP
- Cisco Systems – техническая поддержка и документация