Содержание

Введение

Этот документ описывает, как настроить и verifiy Cisco TrustSec (CTS) с Выходным отражателем.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания о решении Cisco TrustSec.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутаторы Catalyst 6500 с Supervisor Engine 2T на IOS Release 15.0 (01) SY
- Генератор трафика IXIA

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.

Общие сведения

Cisco TrustSec является поддерживающей идентичность архитектурой доступа к сети, которая помогает клиентам обеспечивать безопасное сотрудничество, усиливать безопасность и удовлетворять требования соответствия. Это также предоставляет основанную инфраструктуру принудительной политики масштабируемой роли. Пакеты помечены на основе состава группы источника пакетов во входе сети. Политика,

привязанная к группе, применена, поскольку эти пакеты пересекают сеть.

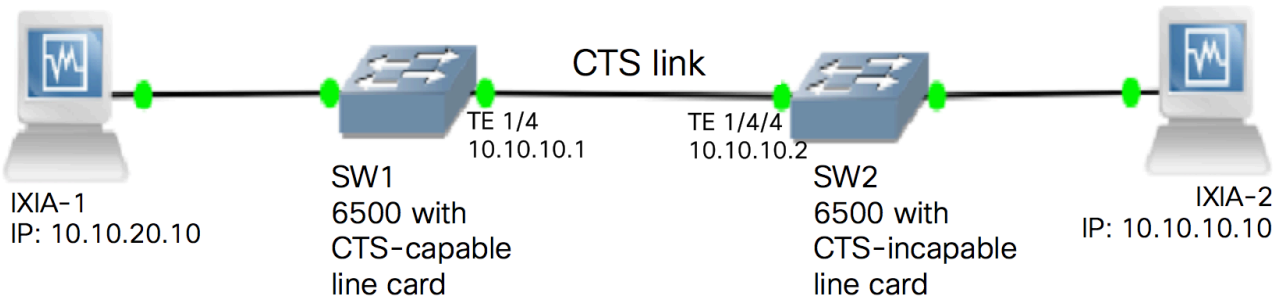
Коммутаторы серии Catalyst 6500 с Supervisor Engine 2T и линейные карты серии 6900 предоставляют завершенную поддержку программного и аппаратного обеспечения для реализации CTS. Для поддержки функциональности CTS существует специальное приложение Определенные Интегральные схемы (ASIC-схемы), используемые на новых линейных картах серии 6900. Устаревшие линейные карты не имеют этих специализированных ASIC-схем и поэтому, не поддерживайте CTS.

Отражатель Cisco TrustSec использует Порт коммутатора Catalyst Анализатор (SPAN) для отражения трафика от неспособного к CTS модуля коммутации до Supervisor Engine для присвоения тега группы безопасности (SGT) и вставки.

Выходной отражатель Cisco TrustSec внедрен на коммутаторе распределения с каналами связи Уровня 3, где неспособный к CTS модуль коммутации стоит перед коммутатором доступа. Это поддерживает Централизованные Передающие Карты (CFC) и Distributed Forwarding Card (DFC).

Настройка

Схема сети



Конфигурация SW1

Настройте CTS manual на канале связи к SW2 с этими командами:

Конфигурация SW2

Включите выходной отражатель на коммутаторе с этими командами:

> **Примечание:** Коммутатор должен быть повторно загружен для включения выходного режима отражателя.

Настройте CTS Manual на порту, связанном с SW1 с этими командами:

Настройте статический SGT на SW2 для IP - адреса источника 10.10.10.10 от IXIA.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Текущий режим CTS может быть просмотрен с этой командой:

Состояние канала CTS может быть просмотрено с этой командой:

Проверьте, что IFC-состояние ОТКРЫТО на обоих коммутаторах. Выходные данные должны быть похожими на это:

Проверка через netflow выведена

Netflow может быть настроен с этими командами:

Примените Netflow на входной интерфейс коммутатора SW1:

Проверьте, что входящими пакетами является наклеенный Коммутатор SW1 SGT.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.