IPS 5.x и более поздние версии: NTP на примере конфигурации IPS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Родственные продукты
Условные обозначения
!--- конфигурацию
Настройте маршрутизатор Cisco, чтобы быть Сервером NTP
Настройте датчик для Использования источника времени NTP
Проверка
Устранение неполадок
Дополнительные сведения

Введение

Этот документ предоставляет пример конфигурации для синхронизации часов Системы предотвращения вторжений (IPS) Cisco Secure с сервером сетевого времени с помощью Протокола NTP. Маршрутизатор Cisco настроен как сервер NTP, и сенсор IPS настроен для использования сервера NTP (маршрутизатор Cisco) в качестве источника времени.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Сервер NTP должен быть достижимым от датчика Cisco IPS перед началом этой конфигурации NTP.

Используемые компоненты

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

- Устройство IPS Cisco серии 4200, которое работает под управлением ПО версии 7.0 и позже

- Cisco IPS Manager Express (IME) версия 7.0.1 и позжеПримечание: В то время как IME может использоваться к устройствам контрольного датчика, которые выполняют Cisco IPS 5.0 и позже, некоторые новые характеристики и функциональность, отправленная в IME, только поддерживаются на датчиках, которые выполняют Cisco IPS 6.1 или позже.

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.

Родственные продукты

Этот документ также может использоваться со следующими версиями программного и аппаратного обеспечения:

- Устройство IPS Cisco серии 4200, которое выполняет версии программного обеспечения 6.0 и ранее
- Cisco IPS Manager Express (IME) версия 6.1.1

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

!--- конфигурацию

Настройте маршрутизатор Cisco, чтобы быть Сервером NTP

Датчик требует аутентифицируемого соединения с сервером NTP, если он переходит, используют сервер NTP в качестве источника времени. Датчик поддерживает только алгоритм хэширования MD5 для шифрования ключей. Используйте следующую процедуру для активации маршрутизатора Cisco, чтобы действовать как сервер NTP и использовать его внутренние часы в качестве источника времени.

Выполните эти шаги для устанавливания маршрутизатора Cisco для действия как сервер NTP:

1. Вход в систему маршрутизатора.
2. Введите режим конфигурации.`router#`**`configure terminal`**
3. Создайте ключевой ID и значение параметра.`router(config)#`**`ntp authentication-key key_ID md5 key_value`** Ключевой ID может быть номером между 1 и 65535. Значение параметра является текстом (числовой или символ). Это зашифровано позже. Пример:`router(config)#`**`ntp authentication-key 12345 md5 123`** Примечание: Датчик только поддерживает ключи MD5. Ключи могли бы уже существовать на маршрутизаторе. Используйте **показ рабочая** команда настройки для проверки для других ключей. Можно использовать те значения для доверяемого ключа в шаге 4.
4. Определяйте ключ, который вы просто создали в шаге 3 как доверяемый ключ (или используйте существующий ключ).`router(config)#`**`ntp trusted-key key_ID`** Доверяемый ключевой ID является тем же номером как ключевой ID в шаге 3.

Пример:`router(config)#`**`ntp trusted-key 12345`**

5. Задайте интерфейс на маршрутизаторе, с которым свяжется датчик.`router(config)#`**`ntp source interface_name`** Пример:`router(config)#`**`ntp source FastEthernet 1/0`**
6. Задайте номер страты NTP master, который будет назначен на датчик как показано здесь:`router(config)#`**`ntp master stratum_number`** Пример:`router(config)#`**`ntp master 6`**
   Примечание: Номер страты NTP master определяет относительное положение сервера в иерархии NTP. Можно выбрать номер между 1 и 15. Это не важно для датчика, какой номер вы выбираете.

Настройте датчик для Использования источника времени NTP

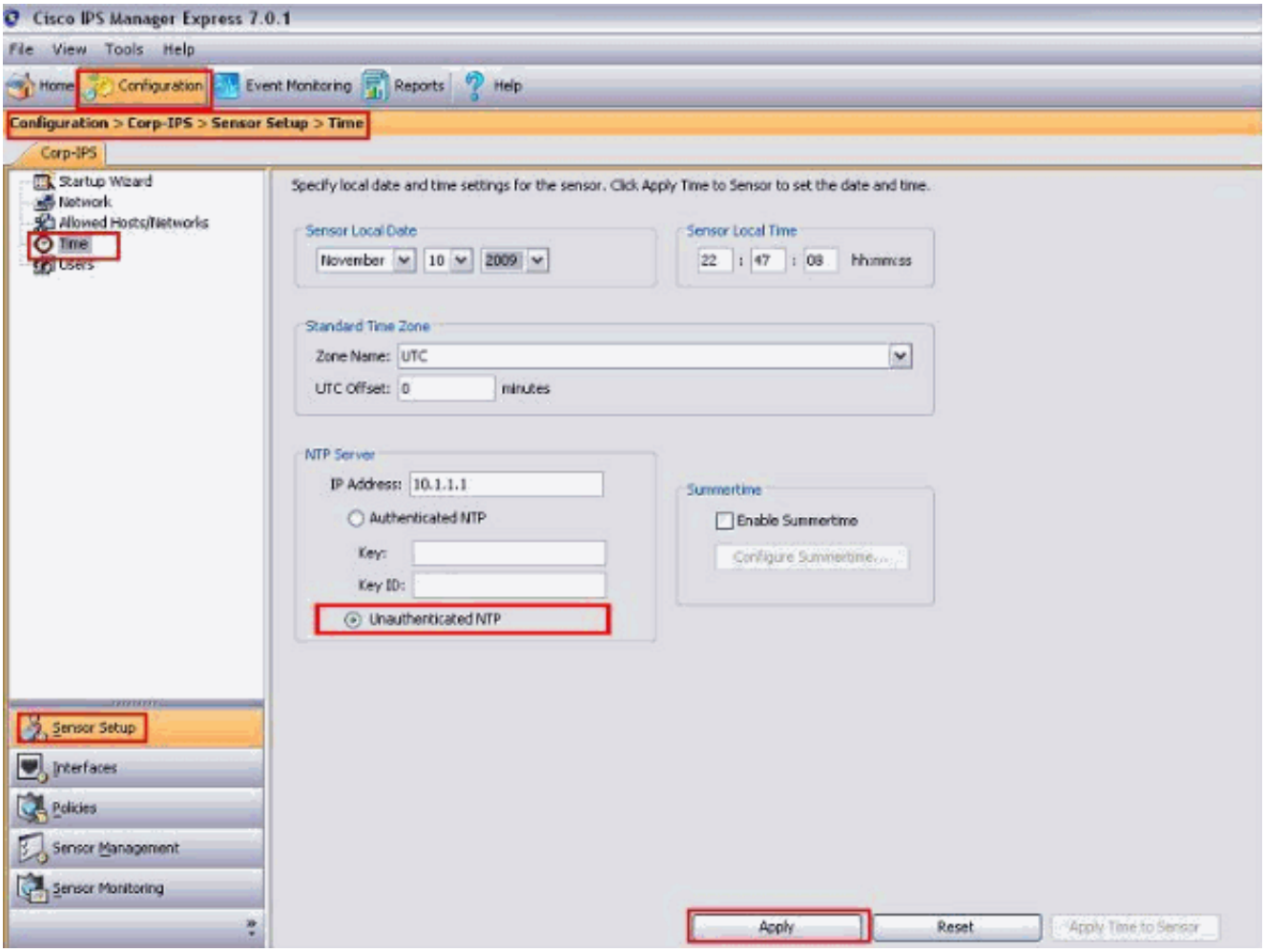
Выполните шаги в этом разделе для настройки датчика для использования источника времени NTP (маршрутизатор Cisco является источником времени NTP в данном примере).

Датчик требует последовательного источника времени. Рекомендуется использовать сервер NTP. Используйте следующую процедуру для настройки датчика для использования сервера NTP в качестве его источника времени. Можно использовать Аутентифицируемый или Не прошедший поверку подлинности NTP.

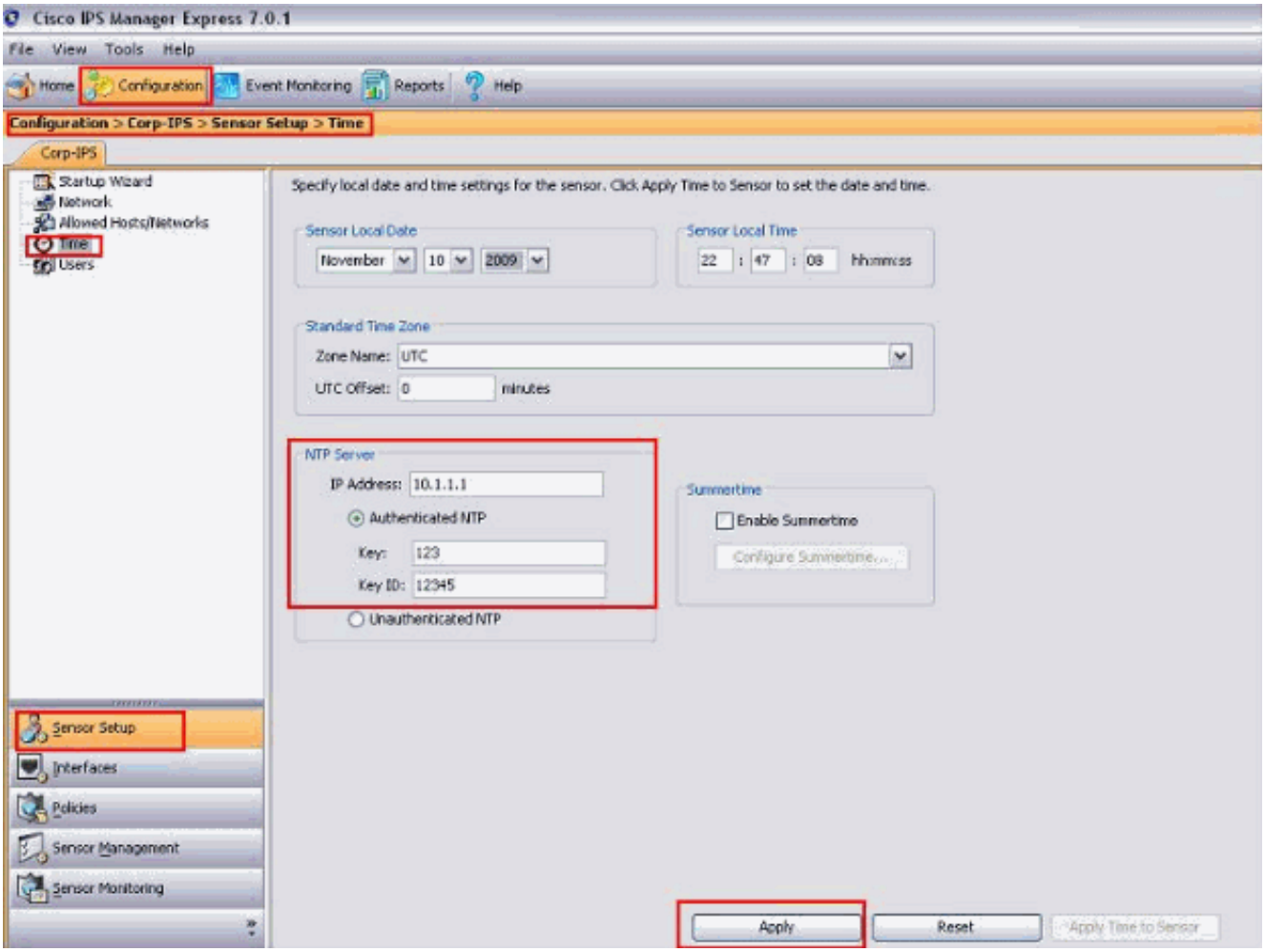
Примечание: Для Аутентифицируемого NTP необходимо получить IP-адрес сервера NTP, ID ключа сервера NTP и значение параметра от сервера NTP.

Выполните эти шаги для настройки датчика для использования сервера NTP в качестве его источника времени:

1. Войдите к CLI с помощью учетной записи с администраторскими привилегиями.
2. Введите режим конфигурации как показано здесь:`sensor#`**`configure terminal`**
3. Перейдите в сервисный режим хоста.`sensor(config)# service host`
4. NTP может быть настроен как Аутентифицируемый и Не прошедший поверку подлинности NTP.Выполните эти шаги для настройки Не прошедшего поверку подлинности NTP:Перейдите в режим конфигурации NTP.`sensor(config-hos)#`**`ntp-option enabled-ntp-unauthenticated`** Задайте IP-адрес сервера NTP.`sensor(config-hos-ena)#`**`ntp-server ip_address`** В данном примере IP-адрес сервера NTP 10.1.1.1.`sensor(config-hos-ena)#`**`ntp-server 10.1.1.1`** Это - процедура для настройки Не прошедшего поверку подлинности NTP с помощью Cisco IPS Manager Express:Выберите **Configuration> Corp-IPS> Sensor Setup> Time**. Затем нажмите кнопку с зависимой фиксацией рядом с **Не прошедшим поверку подлинности NTP** после обеспечения IP-адреса сервера NTP как показано в снимке экрана.**Щелкните "Применить".**



Это завершает Не прошедшую поверку подлинности конфигурацию NTP.Выполните эти шаги для настройки Аутентифицируемого NTP:Перейдите в режим конфигурации NTP.`sensor(config-hos)#`**`ntp-option enable`** Задайте IP-адрес сервера NTP и ключевой ID. Ключевой ID является номером между 1 и 65535. Это - ключевой ID, который вы уже устанавливаете на сервере NTP.`sensor(config-hos-ena)#`**`ntp-servers ip_address key-id key_ID`** В данном примере IP-адрес сервера NTP 10.1.1.1.`sensor(config-hos-ena)#`**`ntp-server 10.1.1.1 key-id 12345`** Задайте сервер NTP значения параметра.`sensor(config-hos-ena)#`**`ntp-keys key_ID md5-key key_value`** Значение параметра является текстом (числовой или символ). Это - значение параметра, которое вы уже устанавливаете на сервере NTP. Пример:`sensor(config-hos-ena)#`**`ntp-keys 12345 md5-key 123`** Это - процедура для настройки Аутентифицируемого NTP с помощью Cisco IPS Manager Express:Выберите **Configuration> Corp-IPS> Sensor Setup> Time**. Затем нажмите кнопку с зависимой фиксацией рядом с **Аутентифицируемым NTP** после обеспечения IP-адреса сервера NTP как показано в снимке экрана.Предоставьте ключ и ключевой ID, который должен совпасть с упомянутый в сервере NTP.В данном примере Ключ равняется 123, и Ключевой ID 12345.**Щелкните "Применить".**



Это завершает Аутентифицируемую конфигурацию NTP.

5. Выходной режим конфигурации NTP.`sensor(config-hos-ena)# exit`

   ```
   sensor(config-hos)# exit

   Apply Changes:?[yes]
   ```

6. Нажмите **Enter**, чтобы применить изменения или войти **не** для отмены от них.Это завершает задачу конфигурации.

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Проверьте Аутентифицируемые параметры настройки NTP. Это удостоверяется, что Аутентифицируемая конфигурация NTP сделана правильно.

```
sensor(config-hos-ena)#show settings enabled ----------------------------------------------
ntp-keys (min: 1, max: 1, current: 1) ---------------------------------------------- key-id:
12345 ---------------------------------------------- md5-key: 123 ----------------------------
---------------- ---------------------------------------------- ntp-servers (min: 1, max: 1,
current: 1) ---------------------------------------------- ip-address: 10.1.1.1 key-id: 12345 -
------------------------------------------- ----------------------------------------------
sensor(config-hos-ena)#
```

Для отображения содержания конфигурации, содержавшейся в текущем подрежиме, используйте команду параметров настройки показа в любом сервисном командном режиме. Это проверяет, что Не прошедшая поверку подлинности конфигурация NTP сделана правильно.

```
sensor(config-hos-ena)#show settings enabled-ntp-unauthenticated ------------------------------
--------------- ntp-server: 10.1.1.1 ------------------------------------------
sensor(config-hos-ena)#
```

Для отображения системных часов используйте команду show clock в Режиме EXEC как показано. Данный пример показывает NTP, настроенный и синхронизируемый:

```
sensor#show clock detail 11:45:02 CST Tues Jul 20 2011 Time source is NTP sensor#
```

Устранение неполадок

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

Дополнительные сведения

- Страница технической поддержки системы предотвращения вторжений Cisco (IPS)
- Страница технической поддержки Cisco IPS Manager Express
- Network Time Protocol (NTP)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация