IPS 5.x e versioni successive: esempio di configurazione di NTP su IPS

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per sincronizzare l'orologio Cisco Secure Intrusion Prevention System (IPS) con un server di riferimento orario della rete utilizzando il protocollo NTP (Network Time Protocol). Il router Cisco è configurato come server NTP e il sensore IPS è configurato per utilizzare il server NTP (router Cisco) come origine ora.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Il server NTP deve essere raggiungibile dal sensore Cisco IPS prima di avviare questa configurazione NTP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 4200 IPS Device con software versione 7.0 e successive
- Cisco IPS Manager Express (IME) versione 7.0.1 e successive

Nota: mentre l'IME può essere utilizzato per monitorare i dispositivi sensore che eseguono Cisco IPS 5.0 e versioni successive, alcune delle nuove funzionalità e caratteristiche fornite con l'IME sono supportate solo sui sensori che eseguono Cisco IPS 6.1 o versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Cisco serie 4200 IPS Device con software versione 6.0 e precedenti
- Cisco IPS Manager Express (IME) versione 6.1.1

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Configurazione di un router Cisco come server NTP

Il sensore richiede una connessione autenticata con un server NTP se intende utilizzare il server NTP come sorgente di tempo. Il sensore supporta solo l'algoritmo hash MD5 per la crittografia delle chiavi. Per attivare un router Cisco come server NTP e usare l'orologio interno come origine ora, attenersi alla procedura seguente.

Completare la procedura seguente per configurare un router Cisco come server NTP:

1. Accedere al router.
2. Accedere alla modalità di configurazione.

```
<#root>

router#

configure terminal
```

3. Creare l'ID e il valore della chiave.

```
<#root>

router(config)#

ntp authentication-key key_ID md5 key_value
```

L'ID della chiave può essere un numero compreso tra 1 e 65535. Il valore della chiave è testo (numerico o carattere). Viene crittografato in seguito. Ad esempio:

```
<#root>

router(config)#

ntp authentication-key 12345 md5 123
```

Nota: il sensore supporta solo i tasti MD5. Le chiavi potrebbero essere già presenti sul router. Utilizzare il comando show running configuration per verificare la presenza di altre chiavi. È possibile utilizzare tali valori per la chiave attendibile nel passaggio 4.

4. Designare la chiave appena creata al passaggio 3 come chiave attendibile (o utilizzare una chiave esistente).

```
<#root>

router(config)#

ntp trusted-key key_ID
```

L'ID della chiave attendibile corrisponde all'ID della chiave indicato al passaggio 3. Ad esempio:

```
<#root>

router(config)#

ntp trusted-key 12345
```

5. Specificare l'interfaccia del router con cui il sensore comunicherà.

```
<#root>

router(config)#

ntp source interface_name
```

Ad esempio:

```
<#root>
router(config)#
ntp source FastEthernet 1/0
```

6. Specificare il numero dello strato principale NTP da assegnare al sensore, come mostrato di seguito:

```
<#root>
router(config)#
ntp master stratum_number
```

Ad esempio:

```
<#root>
router(config)#
ntp master 6
```

Nota: il numero dello strato principale NTP identifica la posizione relativa del server nella gerarchia NTP. È possibile scegliere un numero compreso tra 1 e 15. Per il sensore non è importante quale numero scegliere.

Configurazione del sensore per l'utilizzo di una sorgente ora NTP

Completare la procedura descritta in questa sezione per configurare il sensore in modo che utilizzi la sorgente di tempo NTP (nell'esempio riportato, il router Cisco è la sorgente di tempo NTP).

Il sensore richiede una sorgente di tempo coerente. Si consiglia di utilizzare un server NTP. Per configurare il sensore in modo che utilizzi il server NTP come sorgente ora, attenersi alla procedura descritta di seguito. È possibile utilizzare NTP autenticato o non autenticato.

Nota: per il protocollo NTP autenticato, è necessario ottenere dal server NTP l'indirizzo IP del server NTP, l'ID della chiave del server NTP e il valore della chiave.

Completare questa procedura per configurare il sensore in modo che utilizzi un server NTP come origine del tempo:

1. Accedere alla CLI utilizzando un account con privilegi di amministratore.
2. Immettere la modalità di configurazione come mostrato di seguito:

```
<#root>
sensor#
configure terminal
```

3. Accedere alla modalità host del servizio.

```
sensor(config)# service host
```

4. L'NTP può essere configurato come NTP autenticato e non autenticato.

   Per configurare un NTP non autenticato, completare la procedura seguente:

   a. Accedere alla modalità di configurazione NTP.

```
<#root>
sensor(config-hos)#
ntp-option enabled-ntp-unauthenticated
```

   b. Specificare l'indirizzo IP del server NTP.

```
<#root>
sensor(config-hos-ena)#
ntp-server ip_address
```

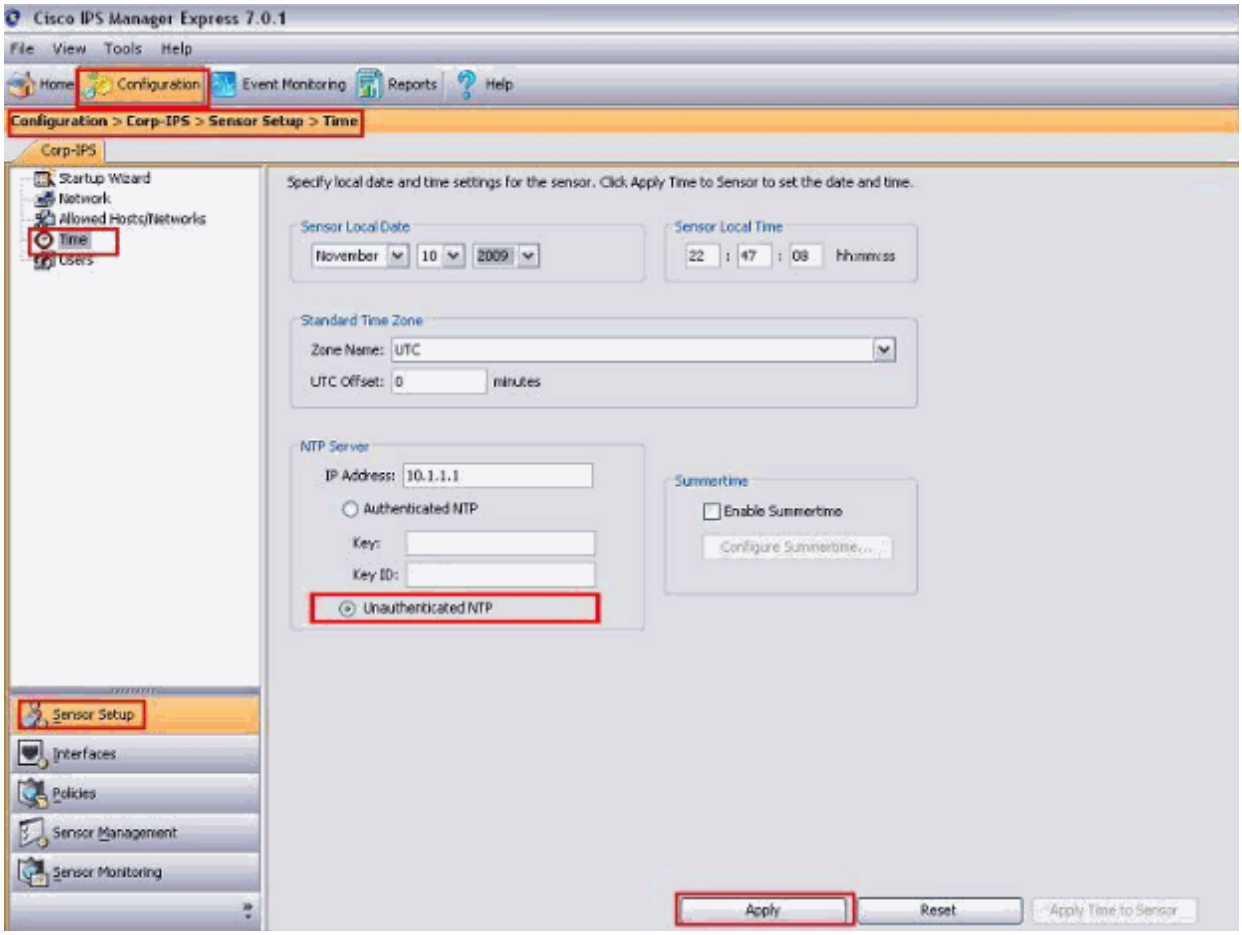
   Nell'esempio, l'indirizzo IP del server NTP è 10.1.1.1.

```
<#root>
sensor(config-hos-ena)#
ntp-server 10.1.1.1
```

Questa è la procedura per configurare il protocollo NTP non autenticato utilizzando Cisco IPS Manager Express:

a. Scegliete Configurazione > IPS aziendale > Impostazione sensore > Tempo. Quindi, fare clic sul pulsante di opzione accanto a NTP non autenticato dopo aver fornito l'indirizzo IP del server NTP come mostrato nella schermata.

b. Fare clic su Apply (Applica).



La configurazione NTP non autenticato è stata completata.

Completare questa procedura per configurare Authenticated NTP:

a. Accedere alla modalità di configurazione NTP.

<#root>

```
sensor(config-hos)#
```

ntp-option enable

b. Specificare l'indirizzo IP e l'ID della chiave del server NTP. L'ID della chiave è un numero compreso tra 1 e 65535. Questo è l'ID chiave già impostato sul server NTP.

<#root>

```
sensor(config-hos-ena)#
ntp-servers ip_address key-id key_ID
```

Nell'esempio, l'indirizzo IP del server NTP è 10.1.1.1.

<#root>

```
sensor(config-hos-ena)#
ntp-server 10.1.1.1 key-id 12345
```

c. Specificare il valore della chiave per il server NTP.

<#root>

```
sensor(config-hos-ena)#
ntp-keys key_ID md5-key key_value
```

Il valore della chiave è testo (numerico o carattere). Questo è il valore chiave già impostato sul server NTP. Ad esempio:

<#root>

```
sensor(config-hos-ena)#
ntp-keys 12345 md5-key 123
```

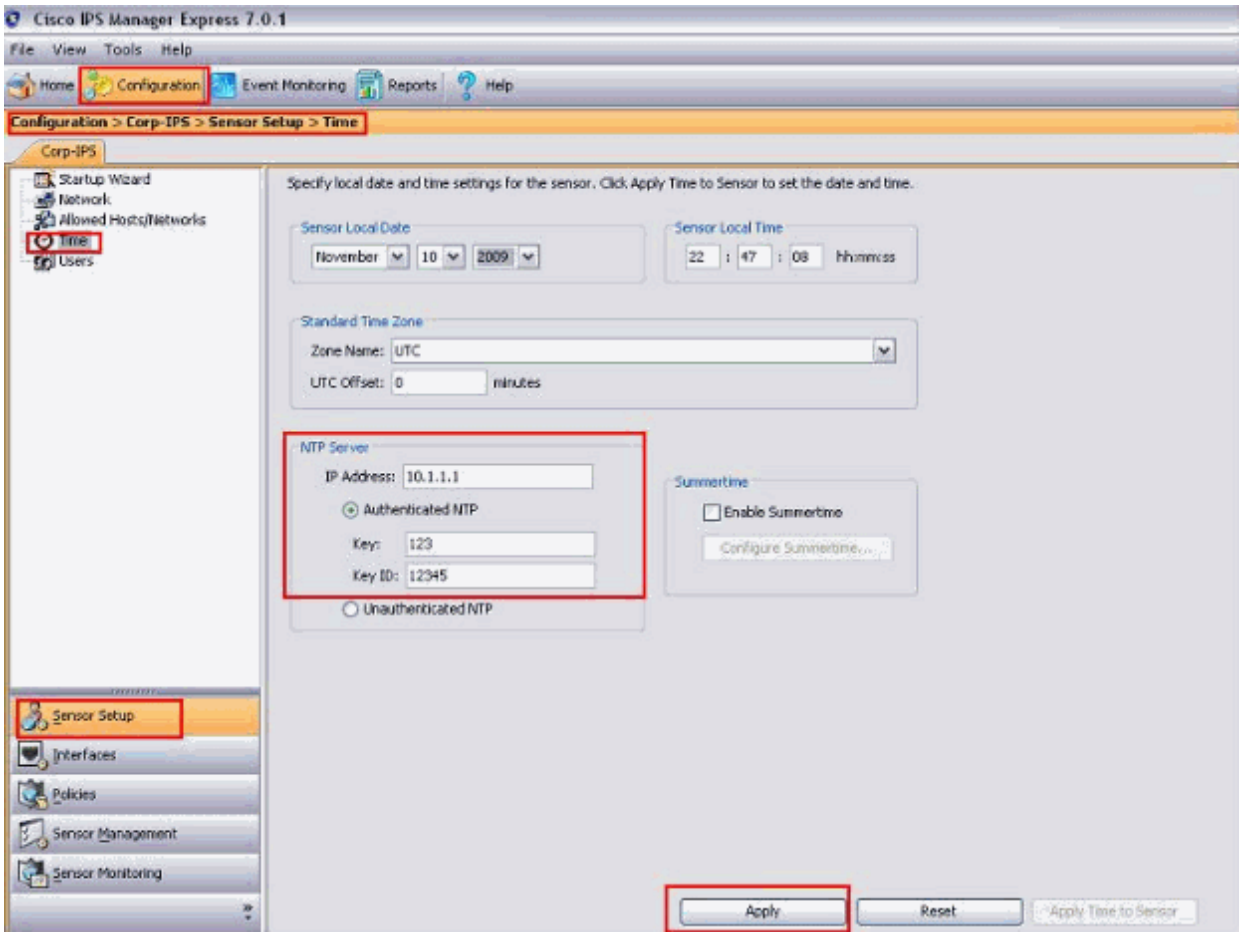
Questa è la procedura per configurare il protocollo NTP autenticato utilizzando Cisco IPS Manager Express:

a. Scegliete Configurazione > IPS aziendale > Impostazione sensore > Tempo. Quindi, fare clic sul pulsante di opzione accanto a Authenticated NTP dopo aver fornito l'indirizzo IP del server NTP come mostrato nella schermata.

b. Specificare la chiave e l'ID della chiave che devono corrispondere a quelli indicati nel server NTP.

In questo esempio Key è 123 e Key ID è 12345.

c. Fare clic su Apply (Applica).



La configurazione NTP autenticato è stata completata.

5. Uscire dalla modalità di configurazione NTP.

```
sensor(config-hos-ena)# exit

sensor(config-hos)# exit

Apply Changes:?[yes]
```

6. Premere Invio per applicare le modifiche o immettere no per annullarle.

   L'attività di configurazione è stata completata.

Verifica

In questa sezione viene spiegato come verificare che la configurazione funzioni correttamente.

Verificare le impostazioni Autenticato NTP. In questo modo, viene verificato che la configurazione Autenticato NTP venga eseguita correttamente.

<#root>

```
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)#
```

Per visualizzare il contenuto della configurazione contenuta nella modalità secondaria corrente, usare il comando show settings in qualsiasi modalità di comando del servizio. In questo modo si verifica che la configurazione NTP non autenticata venga eseguita correttamente.

<#root>

```
sensor(config-hos-ena)#
show settings


enabled-ntp-unauthenticated
   ------------------------------------------
      ntp-server: 10.1.1.1
   ------------------------------------------
```

```
sensor(config-hos-ena)#
```

Per visualizzare l'orologio di sistema, usare il comando show clock in modalità di esecuzione, come mostrato. L'esempio mostra NTP configurato e sincronizzato:

<#root>

```
sensor#
show clock detail


11:45:02 CST Tues Jul 20 2011

Time source is NTP


sensor#
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Pagina di supporto di Cisco Intrusion Prevention System
- Pagina di supporto di Cisco IPS Manager Express
- Protocollo NTP (Network Time Protocol)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).