Configurazione e registrazione di un router Cisco IOS su un altro router Cisco IOS configurato come server CA

Sommario

Introduzione

In questo documento viene descritto come configurare un router Cisco IOS® come server Certification Authority (CA). Viene inoltre illustrato come registrare un altro router Cisco IOS per ottenere un certificato radice e ID per l'autenticazione IPsec dal server CA.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Due router Cisco serie 2600 con software Cisco IOS versione 12.3(4)T3.

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.

Esempio di rete

Nel documento viene usata questa impostazione di rete:

Convenzioni

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

Generazione ed esportazione della coppia di chiavi RSA per il server di certificazione

Il primo passaggio consiste nella generazione della coppia di chiavi RSA utilizzata dal server CA Cisco IOS. Sul router (R1), generare le chiavi RSA come mostrato nell'output:

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

R1(config)#
*Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Nota: è necessario utilizzare lo stesso nome per la coppia di chiavi (*key-label*) che si intende utilizzare per il server dei certificati (tramite il comando **crypto pki server** ***cs-label*** **descritto in seguito).**

Esporta coppia di chiavi generata

Esportare le chiavi nella memoria RAM non volatile (NVRAM) o nel protocollo TFTP (in base alla configurazione in uso). Nell'esempio viene usata la NVRAM. In base all'implementazione, è

possibile utilizzare un server TFTP separato per memorizzare le informazioni sul certificato.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123

% Key name: cisco1
   Usage: General Purpose Key
Exporting public key...
Destination filename [cisco1.pub]?
Writing file to nvram:cisco1.pub
Exporting private key...
Destination filename [cisco1.prv]?
Writing file to nvram:cisco1.prv
R1(config)#
```

Se si utilizza un server TFTP, è possibile reimportare la coppia di chiavi generata, come mostrato in questo comando:

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

Nota: se non si desidera esportare la chiave dal server di certificati, importarla nuovamente nel server di certificati dopo averla esportata come coppia di chiavi non esportabile. In questo modo, la chiave non può più essere tolta.

Verifica coppia di chiavi generata

Usare il comando **show crypto key mypubkey rsa** per verificare la coppia di chiavi generata.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: cisco1
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
  B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
  7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
% Key pair was generated at: 09:51:54 UTC Jan 22 2004
Key name: cisco1.server
 Usage: Encryption Key
 Key is exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
  72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
  EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
  C1607433 5C7BC549 D532D18C DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

Abilitare il server HTTP sul router

Il server CA Cisco IOS supporta solo registrazioni effettuate tramite SCEP (Simple Certificate Enrollment Protocol). Di conseguenza, per rendere possibile questa operazione, il router deve eseguire il server HTTP Cisco IOS incorporato. Utilizzare il comando **ip http server** per abilitarlo:

```
R1(config)#ip http server
```

Abilitare e configurare il server CA sul router

Attenersi alla seguente procedura:

1. Èmolto importante ricordare che il server di certificazione deve utilizzare lo stesso nome della coppia di chiavi appena generata manualmente.L'etichetta corrisponde all'etichetta della coppia di chiavi generata:
   ```
   R1(config)#crypto pki server cisco1
   ```

   Dopo aver abilitato un server certificati, è possibile utilizzare i valori predefiniti preconfigurati o specificare i valori tramite CLI per la funzionalità del server certificati.
2. Il comando **database url** specifica la posizione in cui vengono scritte tutte le voci di database per il server CA. Se questo comando non viene specificato, tutte le voci del database vengono scritte in Flash.
   ```
   R1(cs-server)#database url nvram:
   ```

   Nota: se si utilizza un server TFTP, l'URL deve essere **tftp://<indirizzo_ip>/directory**.
3. Configurare il livello del database:
   ```
   R1(cs-server)#database level minimum
   ```

   Questo comando controlla il tipo di dati archiviati nel database di registrazione certificati:**Minimo**: le informazioni archiviate sono sufficienti solo per continuare a rilasciare nuovi certificati senza conflitti. Valore predefinito.**Nomi**: oltre alle informazioni fornite nel livello minimo, il numero di serie e il nome del soggetto di ciascun certificato.**Completo**: oltre alle informazioni fornite nei livelli minimo e nomi, ogni certificato rilasciato viene scritto nel database.**Nota:** la parola chiave **complete** produce una grande quantità di informazioni. Se viene emesso, è necessario specificare anche un server TFTP esterno in cui memorizzare i dati tramite il comando **url** del **database**.
4. Configurare il nome dell'autorità emittente della CA sulla stringa DN specificata. Nell'esempio, viene utilizzato il CN (nome comune) cisco1.cisco.com, L (località) della RTP e C (paese) degli USA:
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Specificare la durata, in giorni, di un certificato CA o di un certificato.I valori validi sono compresi tra *1 e 1825 giorni*. La durata predefinita del certificato CA è di tre anni e quella del certificato è di un anno. La durata massima del certificato è inferiore di *un mese* alla durata del certificato CA. Ad esempio:
   ```
   R1(cs-server)#lifetime ca-certificate 365
   R1(cs-server)#lifetime certificate 200
   ```
6. Definire la durata, in ore, del CRL utilizzato dal server dei certificati. Il valore massimo della durata è **336 ore** (due settimane). Il valore predefinito è **168 ore** (una settimana).
   ```
   R1(cs-server)#lifetime crl 24
   ```

7. Definire un CDP (Certificate-Revocation-List Distribution Point) da utilizzare nei certificati rilasciati dal server dei certificati.L'URL deve essere un URL HTTP. Ad esempio, l'indirizzo IP del nostro server era 172.18.108.26:

```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. Utilizzare il comando **no shutdown** per abilitare il server CA:
```
R1(cs-server)#no shutdown
```

Nota: eseguire questo comando solo dopo aver completato la configurazione del server di certificati.

Configurazione e registrazione del secondo router IOS (R2) nel server certificati

Attenersi alla procedura seguente.

1. Configurare un nome host e un nome di dominio e generare le chiavi RSA su R2.Per configurare il nome host del router in modo che sia R2, usare il comando **hostname**:
```
Router(config)#hostname R2
R2(config)#
```
Si noti che il nome host del router è stato modificato subito dopo l'immissione del comando **hostname**.Usare il comando **ip domain-name** per configurare il nome di dominio sul router:
```
R2(config)#ip domain-name cisco.com
```

Usare il comando **crypto key generate rsa** per generare la coppia di chiavi R2:
```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```
2. Utilizzare questi comandi in modalità di configurazione globale per dichiarare alla CA che il router deve utilizzare (in questo esempio, CA Cisco IOS) e specificare le caratteristiche della CA trustpoint:

```
crypto ca trustpoint cisco
 enrollment retry count 5
 enrollment retry period 3
 enrollment url http://14.38.99.99:80
 revocation-check none
```

Nota: il comando **crypto ca trustpoint** unifica il comando **crypto ca identity** e il comando **crypto ca trusted-root**, fornendo così funzionalità combinate in un unico comando.
3. Utilizzare il comando **crypto ca authentication cisco** (cisco è l'etichetta del punto di attendibilità) per recuperare il certificato radice dal server CA:
```
R2(config)#crypto ca authenticate cisco
```

4. Per registrare e generare, usare il comando **crypto ca enroll cisco** (cisco è l'etichetta del punto di attendibilità):
```
R2(config)#crypto ca enroll cisco
```

Dopo aver completato la registrazione al server CA Cisco IOS, visualizzare i certificati rilasciati utilizzando il comando **show crypto ca certificates**. Questo è l'output del comando. Il

comando visualizza le informazioni dettagliate sul certificato, che corrispondono ai parametri configurati nel server CA Cisco IOS:

```
R2#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 02
  Certificate Usage: General Purpose
  Issuer:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Subject:
    Name: R2.cisco.com
    hostname=R2.cisco.com
  CRL Distribution Point:
 http://172.18.108.26/cisco1cdp.cisco1.crl
Validity Date:
    start date: 15:41:11 UTC Jan 21 2004
    end   date: 15:41:11 UTC Aug 8 2004
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: cisco

CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Issuer:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Subject:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Validity Date:
    start date: 15:39:00 UTC Jan 21 2004
    end   date: 15:39:00 UTC Jan 20 2005
  Associated Trustpoints: cisco
```

5. Immettere questo comando per salvare la chiave nella memoria flash persistente:

```
hostname(config)#write memory
```

6. Per salvare la configurazione, immettere questo comando:

```
hostname#copy run start
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show crypto ca certificates**: visualizza i certificati.
- **show crypto key mypubkey rsa**: visualizza la coppia di chiavi.

```
!% Key pair was generated at: 09:28:16 EST Jan 30 2004
  !Key name: ese-ios-ca
  ! Usage: General Purpose Key
  ! Key is exportable.
```

```
! Key Data:
!  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198
!  C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060
!  E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B
!  ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE
!  9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001
!% Key pair was generated at: 09:28:17 EST Jan 30 2004
!Key name: ese-ios-ca.server
! Usage: Encryption Key
! Key is exportable.
! Key Data:
!  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5
!  0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9
!  18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2
!  3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001
```

- **crypto pki server ese-ios-ca info crl**: visualizza l'elenco di revoche di certificati (CRL).

```
! Certificate Revocation List:
!    Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
!    This Update: 09:58:27 EST Jan 30 2004
!    Next Update: 09:58:27 EST Jan 31 2004
!    Number of CRL entries: 0
!    CRL size: 300 bytes
```

- **crypto pki server ese-ios-ca info request**: visualizza le richieste di registrazione in sospeso.

```
! Enrollment Request Database:
! ReqID  State      Fingerprint                      SubjectName
! --------------------------------------------------------------------
```

- **show crypto pki server**: visualizza lo stato corrente del server PKI (public key infrastructure).

```
! Certificate Server status: enabled, configured
!    Granting mode is: manual
!    Last certificate issued serial number: 0x1
!    CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
!    CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
!    Current storage dir: nvram:
!    Database Level: Names - subject name data written as .cnm
```

- **server crypto pki *cs-label* grant { all | *id-transazione* }**: concede tutte le richieste SCEP o solo quelle specifiche.
- **crypto pki server *cs-label* rifiuto { all | *id-transazione* }**: rifiuta tutte le richieste SCEP o solo quelle specifiche.
- **crypto pki server cs-label password generate [*minutes*]** - Genera una password temporanea (OTP) per una richiesta SCEP (minuti - periodo di tempo (in minuti) durante il quale la password è valida. L'intervallo valido è compreso tra 1 e 1440 minuti. L'impostazione predefinita è 60 minuti.**Nota:** è valido un solo OTP alla volta. Se viene generato un secondo OTP, l'OTP precedente non è più valido.
- **crypto pki server *cs-label* revoke *certificate-serial-number* - Revoca un certificato in base al relativo numero di serie.**
- **crypto pki server *cs-label* richiesta *pkcs10* {url *url* | *terminal*} [pem]**: aggiunge manualmente la richiesta di registrazione dei certificati base64 o PEM PKCS10 al database di richiesta.
- **crypto pki server *cs-label* info crl**: visualizza le informazioni relative allo stato del CRL corrente.
- **crypto pki server *cs-label* info request**: visualizza tutte le richieste di registrazione dei certificati in sospeso.

Per ulteriori informazioni sulla verifica, vedere la sezione Verifica della coppia di chiavi generata di questo documento.

Risoluzione dei problemi

Per informazioni sulla risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug.

Nota: in molte situazioni è possibile risolvere i problemi quando si elimina e ridefinisce il server CA.

Informazioni correlate

- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems