在集線器上使用IOS CA的Cisco IOS路由器之間的動態LAN到LAN VPN配置示例

目錄

簡介
必要條件
需求
採用元件
慣例
設定
網路圖表
組態
驗證
疑難排解
L2L隧道的證書身份驗證失敗。
相關資訊

簡介

本檔案將提供在利用IOS憑證授權單位(CA)功能時使用數字憑證的Cisco IOS®路由器之間的動態LAN到LAN VPN的組態範例。本文演示如何配置IOS CA伺服器以及配置Cisco IOS路由器，以便通過自動註冊獲取身份證書。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行Cisco IOS軟體版本12.4(6)T的Cisco 2851路由器
- 執行Cisco IOS軟體版本12.3(14)YT1的Cisco 871路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

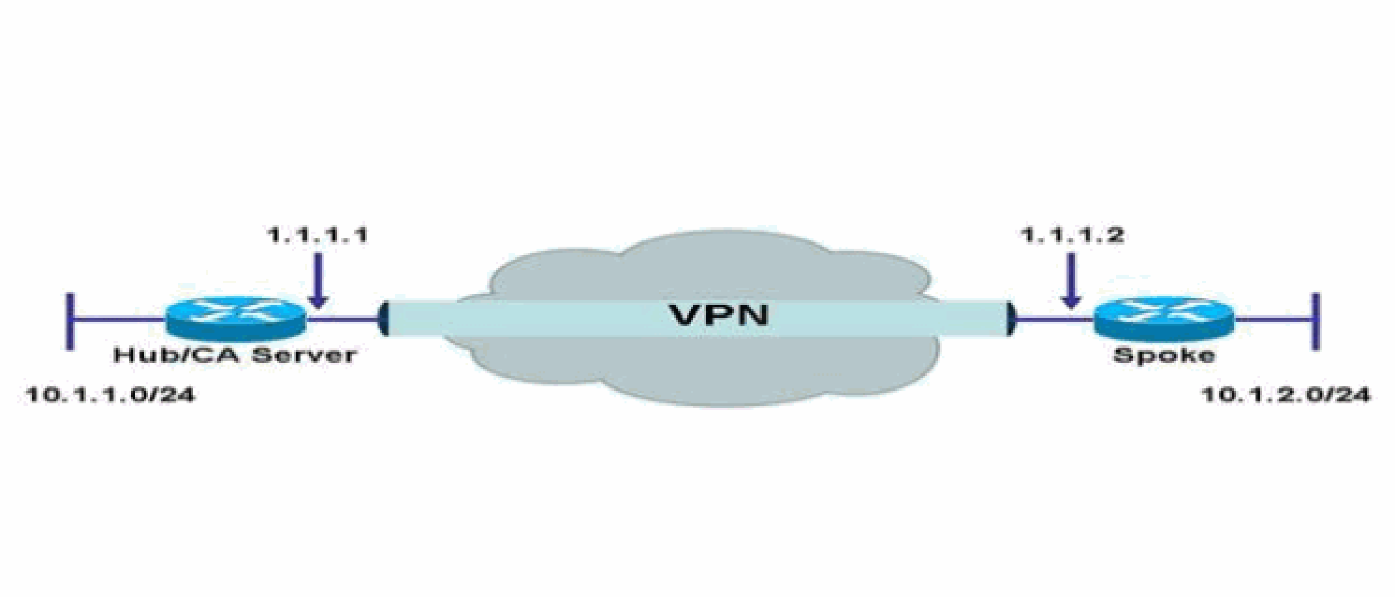
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- 在路由器上配置IOS CA伺服器
- 驗證並註冊到IOS CA伺服器
- 集線器配置
- 分支配置

在路由器上配置IOS CA伺服器

完成以下步驟，在路由器上設定IOS CA伺服器：

1. 發出**crypto pki server**命令，以便輸入IOS CA伺服器配置的引數。在這種情況下，為IOS CA伺服器配置提供的標籤為**cisco**。標籤可以是任何你想要的東西。
   ```
   HubIOSCA(config)#crypto pki server cisco
   ```

2. 發出**issuer-name**子命令以定義憑證資訊。在這種情況下，公用名(CN)、位置(L)、狀態(ST)和國家代碼(C)的定義如下所示：
   ```
   HubIOSCA(cs-server)#issuer-name CN=iosca.cisco.com L=RTP ST=NC C=US
   ```

3. 發出**grant**命令。在這種情況下，IOS伺服器會自動向客戶端授予證書。

   ```
   HubIOSCA(cs-server)#grant auto
   ```

4. 發出**no shut**命令以啟用IOS CA伺服器。

   ```
   HubIOSCA(cs-server)#no shut
   ```

   輸入此命令後，系統會提示您輸入密碼以保護私鑰。生成CA證書後，某些伺服器設定無法更改。輸入密碼以保護私鑰，或輸入**Return**退出。

   ```
   Password:
   Re-enter password:
    Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
    Exporting Certificate Server signing certificate and keys...
    Certificate Server enabled.
   ```

驗證並註冊到IOS CA伺服器

證書伺服器還具有一個自動生成的相同名稱的信任點。信任點儲存證書伺服器的證書。路由器檢測到信任點正用於儲存證書伺服器的證書後，信任點會鎖定，因此無法對其進行修改。

1. 在配置證書伺服器之前，可以發出**crypto pki trustpoint**命令以手動建立和設定此信任點。這允許您指定備用RSA金鑰對(使用**rsakeypair**命令)。**注意：**自動生成的信任點和證書伺服器證書對於證書伺服器裝置標識不可用。因此，用於指定CA信任點以獲取證書和驗證客戶端連線證書的任何命令列介面(CLI)(例如**ip http secure-trustpoint**命令)都必須指向在證書伺服器裝置上配置的其他信任點。如果伺服器是根證書伺服器，則它使用RSA金鑰對和多個其他屬性來生成自簽名證書。關聯的CA證書具有以下金鑰使用擴展：數位簽章證書簽名憑證撤銷清單(CRL)標籤在本例中，HubIOSCA路由器註冊了使用不同信任點的證書，以便能夠與分支路由器建立VPN隧道。定義信任點，如下所示（iosca是此新信任點的名稱）：

   ```
   HubIOSCA(config)#crypto pki trustpoint iosca
   ```

2. 輸入註冊URL，如下所示：

   ```
   HubIOSCA(ca-trustpoint)#enrollment url http://1.1.1.1:80
   ```

   在這種情況下，不會執行CRL撤銷檢查。

   ```
   HubIOSCA(ca-trustpoint)#revocation-check none
   ```

3. 發出**crypto ca authenticate iosca**命令以接收根證書。

   ```
   HubIOSCA(config)#crypto ca authenticate iosca
   ```

   憑證具有以下屬性：

   ```
   Fingerprint MD5: 441446A1 CA3C32B6 3B680204 452A00B2
         Fingerprint SHA1: 6C09E064 E4B09087 DDFFADCD 2E9C6853 1669BF39

   Do you accept this certificate? [yes/no]: yes
   Trustpoint CA certificate accepted.
   ```

4. 發出**crypto ca enroll iosca**命令以取得身分識別憑證。

   ```
   Start certificate enrollment...
    Create a challenge password. You need to verbally provide this
      password to the CA Administrator in order to revoke your certificate.
      For security reasons, your password is not saved in the configuration.
      Please make a note of it.

   Password:
   Re-enter password:
   ```

```
The subject name in the certificate includes: HubIOSCA.cisco.com
Include the router serial number in the subject name? [yes/no]: no
Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
Certificate request sent to Certificate Authority
The show crypto ca certificate iosca verbose command shows the fingerprint.
```

5. 發出**show crypto pki cert**命令，以驗證是否已安裝證書。

```
HubIOSCA#show crypto pki cert

Certificate
  Status: Available
  Certificate Serial Number: 02
  Certificate Usage: General Purpose
  Issuer:
    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
  Subject:
    Name: HubIOSCA.cisco.com
    hostname=HubIOSCA.cisco.com
  Validity Date:
    start date: 19:11:55 UTC Aug 11 2006
    end   date: 19:11:55 UTC Aug 11 2007
  Associated Trustpoints: iosca

 CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Issuer:
    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
  Subject:
    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
  Validity Date:
    start date: 19:01:54 UTC Aug 11 2006
    end   date: 19:01:54 UTC Aug 10 2009
  Associated Trustpoints: iosca cisco
```

注意：由於CA伺服器也是IPSec對等體，因此中心路由器需要驗證並註冊到位於同一路由器上的CA伺服器。

集線器配置

集線器配置

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HubIOSCA
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
!
no aaa new-model
!
resource policy
!
ip cef
!
```

```
no ip domain lookup
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!
! crypto pki server cisco
 issuer-name CN=iosca.cisco.com L=RTP ST=NC C=US
 grant auto
! crypto pki trustpoint cisco
 revocation-check crl
 rsakeypair cisco
!
! crypto pki trustpoint iosca
 enrollment url http://1.1.1.1:80
 revocation-check none
!
!--- Configure a certificate map that will be used !---
in the ISAKMP profile. crypto pki certificate map
certmap 1 issuer-name co cisco.com ! crypto pki
certificate chain cisco certificate ca 01 !--- Root
certificate created when the IOS CA Server !--- is
enabled. 3082022F 30820198 A0030201 02020101 300D0609
2A864886 F70D0101 04050030 2B312930 27060355 04031320
696F7363 612E6369 73636F2E 636F6D20 4C3D5254 …… 0B1DAECA
FE7388B8 D2B1EFF9 B1269F90 C418BCD1 C45A1B64 99C1A400
99897C7D 9720A789 A374E8D1 E117CEE5 CD90F678 98ECFD46
7DF3C029 58B85899 74D34A52 B489A610 8DED6FA7 7012D13B
1B822EB9 7F65BA quit crypto pki certificate chain iosca
certificate 02 !--- Identity certificate received from
the IOS CA !--- after trustpoint enrollment. 30820213
3082017C A0030201 02020102 300D0609 2A864886 F70D0101
04050030 2B312930 27060355 04031320 696F7363 612E6369
73636F2E 636F6D20 4C3D5254 50205354 3D4E4320 433D5553
301E170D 30363038 31313139 31313535 5A170D30 37303831
31313931 3135355A 30233121 301F0609 2A864886 F70D0109
02161248 7562494F 5343412E 63697363 6F2E636F 6D30819F
300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B811 AD3AABA8 3EC63A04 40E4B3ED 1C783C22 20C65122
6E560D22 2731CAD5 2CC56CBD 554C69FF 4AE3EA1B CAB25918
B249D32A A7861362 7E4257F3 855BD60F FBA8D33D 15F925C5
746B9144 97DCFFEE 4CD81070 43C9343F 92C645BC 37E0EF26
5E04394B 67CC536E BFD920DE 52DC977D 830B3C60 D3CB7003
578BB681 D307FF4F 629F0203 010001A3 4F304D30 0B060355
1D0F0404 030205A0 301F0603 551D2304 18301680 14AC041C
685BDA03 4E71B7FB 59BAE0A3 5422F759 1E301D06 03551D0E
04160414 6A60490F 5CC612A3 EA661102 9D645413 41F9236F
300D0609 2A864886 F70D0101 04050003 818100BA 2DDC2D0A
5F7B4B3D 8C8C770D 34AC1A17 EE91A89A 46FD5B9B 8550B2C5
8B8D31EC 29D8AC3A 8F4B1A96 4C733B9D FD98BF42 2FDFC6B1
E1D762E1 3D4470BD CFC73DF8 E55D7C0A 871159C5 544319B9
1DEC6563 75403B97 7567A81D 27F2688C E955CED7 6E9BC90F
7D3C4C94 81EDA619 835AF696 8E4A8BF3 C54A242D 8DB5DE59
E5B37E quit certificate ca 01 !--- Root certificate
received from the IOS CA !--- after trustpoint
authentication. 3082022F 30820198 A0030201 02020101
300D0609 2A864886 F70D0101 04050030 2B312930 27060355
04031320 696F7363 612E6369 73636F2E 636F6D20 4C3D5254
50205354 3D4E4320 433D5553 301E170D 30363038 31313139
30313534 5A170D30 39303831 30313930 3135345A 302B3129
30270603 55040313 20696F73 63612E63 6973636F 2E636F6D
204C3D52 54502053 543D4E43 20433D55 5330819F 300D0609
2A864886 F70D0101 01050003 818D0030 81890281 8100C368
246CFD63 86BA2F7C 626160C6 37EDC62F 3293B6B3 A006ED81
```

```
9038D4F3 2A20577D C8D88BEF FD5E427A 5D5B3471 E4D3EDF9
9EBC51C7 1768BD45 7D2E90B0 059F72AE 35F7E4E5 15AE3233
A50F2A8E 950A34D4 1620C98C 20FFB14B DF446F5E 4612F6EC
5B457D9B AB9BD937 B29691F9 FDBCBF21 860323FF 1A1C9D7B
39A41C4B 13310203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
301F0603 551D2304 18301680 14AC041C 685BDA03 4E71B7FB
59BAE0A3 5422F759 1E301D06 03551D0E 04160414 AC041C68
5BDA034E 71B7FB59 BAE0A354 22F7591E 300D0609 2A864886
F70D0101 04050003 81810099 256FCF71 084766ED BDE8F6D8
F158BDF0 D1875B0A 57A3FBB8 DD8EF9AD E5BB3E95 3A65893B
B11DBE9A 6E593701 0B1DAECA FE7388B8 D2B1EFF9 B1269F90
C418BCD1 C45A1B64 99C1A400 99897C7D 9720A789 A374E8D1
E117CEE5 CD90F678 98ECFD46 7DF3C029 58B85899 74D34A52
B489A610 8DED6FA7 7012D13B 1B822EB9 7F65BA quit !---
Configure IPSEC phase 1 parameters. crypto isakmp policy
10 hash md5 ! !--- Configure ISAKMP profile for the
dynamic !--- LAN to LAN tunnel. crypto isakmp profile
l2lvpn ca trust-point iosca match certificate certmap !
crypto ipsec transform-set strong ah-md5-hmac esp-des !
!--- Configure dynamic crypto map. crypto dynamic-map
dynmap 10 set transform-set strong set isakmp-profile
l2lvpn !--- Configure crypto map that will be applied on
!--- the physical interface. crypto map mymap 10 ipsec-
isakmp dynamic dynmap ! interface GigabitEthernet0/0 ip
address 14.1.21.199 255.255.252.0 duplex auto speed auto
no keepalive !--- Apply crypto map to the physical
interface. interface GigabitEthernet0/1 ip address
1.1.1.1 255.255.255.0 duplex auto speed auto crypto map
mymap ! interface FastEthernet0/2/0 ! interface
FastEthernet0/2/1 ! interface FastEthernet0/2/2 !
interface FastEthernet0/2/3 ! interface Vlan1 ip address
10.1.1.254 255.255.255.0 ! ip route 0.0.0.0 0.0.0.0
GigabitEthernet0/1 ! ip http server no ip http secure-
server ! control-plane ! line con 0 line aux 0 line vty
0 4 login ! scheduler allocate 20000 1000 ! webvpn
context Default_context ssl authenticate verify all ! no
inservice ! End
```

分支配置

分支配置

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spoke
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!
ip subnet-zero
ip cef
!
```

```
no ip dhcp use vrf connected
!
ip domain name cisco.com
no ip ips deny-action ips-interface
!--- Configure a trustpoint that this router will use !-
-- to authenticate and enroll to the IOS CA Server.
crypto pki trustpoint iosca enrollment url
http://1.1.1.1:80 revocation-check none ! !--- Configure
a certificate map that will be !--- used in the ISAKMP
profile. crypto pki certificate map certmap 1 issuer-
name co cisco.com ! crypto pki certificate chain iosca
certificate 03 30820210 30820179 A0030201 02020103
300D0609 2A864886 F70D0101 04050030 2B312930 27060355
04031320 696F7363 612E6369 73636F2E 636F6D20 4C3D5254
50205354 3D4E4320 433D5553 301E170D 30363038 31313139
31373137 5A170D30 37303831 31313931 3731375A 3020311E
301C0609 2A864886 F70D0109 02160F53 706F6B65 2E636973
636F2E63 6F6D3081 9F300D06 092A8648 86F70D01 01010500
03818D00 30818902 818100A3 98320490 640B33E8 85E3920C
D0BF30F0 038BCFFF 64F1AD1A 7AA1DC92 9D4C160B 905B7FED
F468AC3C 32B5F09B 38DC714E 8ADB227F 7E779259 CC54EDA1
D3CFDDCC 3EB707E3 E5C44059 2097773C 80011AD3 C65CA3BB
82656432 0A305CF4 13D6E3E2 918377EC 0299C91A 87D99287
B44CBDB8 A482F138 5FC365FD 0853D869 A9260302 03010001
A34F304D 300B0603 551D0F04 04030205 A0301F06 03551D23
04183016 8014AC04 1C685BDA 034E71B7 FB59BAE0 A35422F7
591E301D 0603551D 0E041604 14F4DCD0 90A2DB61 7C70F86B
496D3213 592F94D3 9D300D06 092A8648 86F70D01 01040500
03818100 300D3A37 94A561E1 CB38C49F BBB0D19B C2AE09E4
7DFA4ABC 53B53DBB CBE39BCB 903262C9 06AEBE90 2DEE15EE
F343D93A 77D94A24 4BC1EC72 28CE386B B2D9A124 64031AD5
0C8DC97F 76792024 702C849E 13B8CF21 A303FF5B C41EF2B7
77B31117 ED514324 EF8242B7 548E36A6 391540C9 2D913570
6D103F49 DE0CC14C 49C404FF quit certificate ca 01
3082022F 30820198 A0030201 02020101 300D0609 2A864886
F70D0101 04050030 2B312930 27060355 04031320 696F7363
612E6369 73636F2E 636F6D20 4C3D5254 50205354 3D4E4320
433D5553 301E170D 30363038 31313139 30313534 5A170D30
39303831 30313930 3135345A 302B3129 30270603 55040313
20696F73 63612E63 6973636F 2E636F6D 204C3D52 54502053
543D4E43 20433D55 5330819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C368 246CFD63 86BA2F7C
626160C6 37EDC62F 3293B6B3 A006ED81 9038D4F3 2A20577D
C8D88BEF FD5E427A 5D5B3471 E4D3EDF9 9EBC51C7 1768BD45
7D2E90B0 059F72AE 35F7E4E5 15AE3233 A50F2A8E 950A34D4
1620C98C 20FFB14B DF446F5E 4612F6EC 5B457D9B AB9BD937
B29691F9 FDBCBF21 860323FF 1A1C9D7B 39A41C4B 13310203
010001A3 63306130 0F060355 1D130101 FF040530 030101FF
300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304
18301680 14AC041C 685BDA03 4E71B7FB 59BAE0A3 5422F759
1E301D06 03551D0E 04160414 AC041C68 5BDA034E 71B7FB59
BAE0A354 22F7591E 300D0609 2A864886 F70D0101 04050003
81810099 256FCF71 084766ED BDE8F6D8 F158BDF0 D1875B0A
57A3FBB8 DD8EF9AD E5BB3E95 3A65893B B11DBE9A 6E593701
0B1DAECA FE7388B8 D2B1EFF9 B1269F90 C418BCD1 C45A1B64
99C1A400 99897C7D 9720A789 A374E8D1 E117CEE5 CD90F678
98ECFD46 7DF3C029 58B85899 74D34A52 B489A610 8DED6FA7
7012D13B 1B822EB9 7F65BA quit username cisco password 0
ww !--- Configure IPSEC phase 1 parameters. crypto
isakmp policy 10 hash md5 !--- Configure ISAKMP profile
for the !--- LAN 2 LAN tunnel. crypto isakmp profile
l2lvpn ca trust-point iosca match certificate certmap !
crypto ipsec transform-set strong ah-md5-hmac esp-des !-
-- Configure crypto map that will pull !--- the ISAKMP
```

```
profile created. crypto map mymap 10 ipsec-isakmp set
peer 1.1.1.1 set transform-set strong set isakmp-profile
l2lvpn match address 100 ! interface FastEthernet0 !
interface FastEthernet1 ! interface FastEthernet2 !
interface FastEthernet3 !--- Apply LAN to LAN crypto map
on the !--- physical interface. interface FastEthernet4
ip address 1.1.1.2 255.255.255.0 no ip proxy-arp ip
route-cache flow duplex auto speed auto crypto map mymap
! interface Dot11Radio0 no ip address shutdown speed
basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0
18.0 24.0 36.0 48.0 54.0 station-role root ! interface
Vlan1 ip address 10.1.2.254 255.255.255.0 ! ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet4 ! no ip http
server no ip http secure-server ! access-list 100 permit
ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 ! control-plane
! line con 0 no modem enable line aux 0 line vty 0 4
login ! scheduler max-task-time 5000 end
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

L2L隧道的證書身份驗證失敗。

有時，當您使用有效的CA證書進行ISAKMP身份驗證時，IPsec協商可能會失敗。VPN通道交涉使用預先共用金鑰，因為預先共用金鑰真的是個小封包。如果憑證驗證需要透過傳送整個憑證，就會產生大型封包進行分段。分段可防止憑證在裝置之間正確驗證。

降低MTU並交換為全雙工以解決此問題。將MTU值設定為無需分段的大小：

```
Router(config)#interface type [slot_#/]port_#
Router(config-if)#ip mtu MTU_size_in_bytes
```

相關資訊

- [技術支援與文件 - Cisco Systems]