使用集线器上的 IOS CA 在 Cisco IOS 路由器之间实现动态 LAN 到 LAN VPN 的配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[网络图](#)
[配置](#)
[验证](#)
[故障排除](#)
[L2L隧道的证书身份验证失败。](#)
[相关信息](#)

简介

本文档提供了在使用IOS证书颁发机构(CA)功能时使用数字证书的Cisco IOS®路由器之间动态LAN到LAN VPN的示例配置。本文档演示如何在配置 Cisco IOS 路由器以及如何配置 IOS CA 服务器以便通过自动注册获得身份证书。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 Cisco IOS 软件版本 12.4(6) T 的 Cisco 2851 路由器
- 运行 Cisco IOS 软件版本 12.3(14)YT1 的 Cisco 871 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

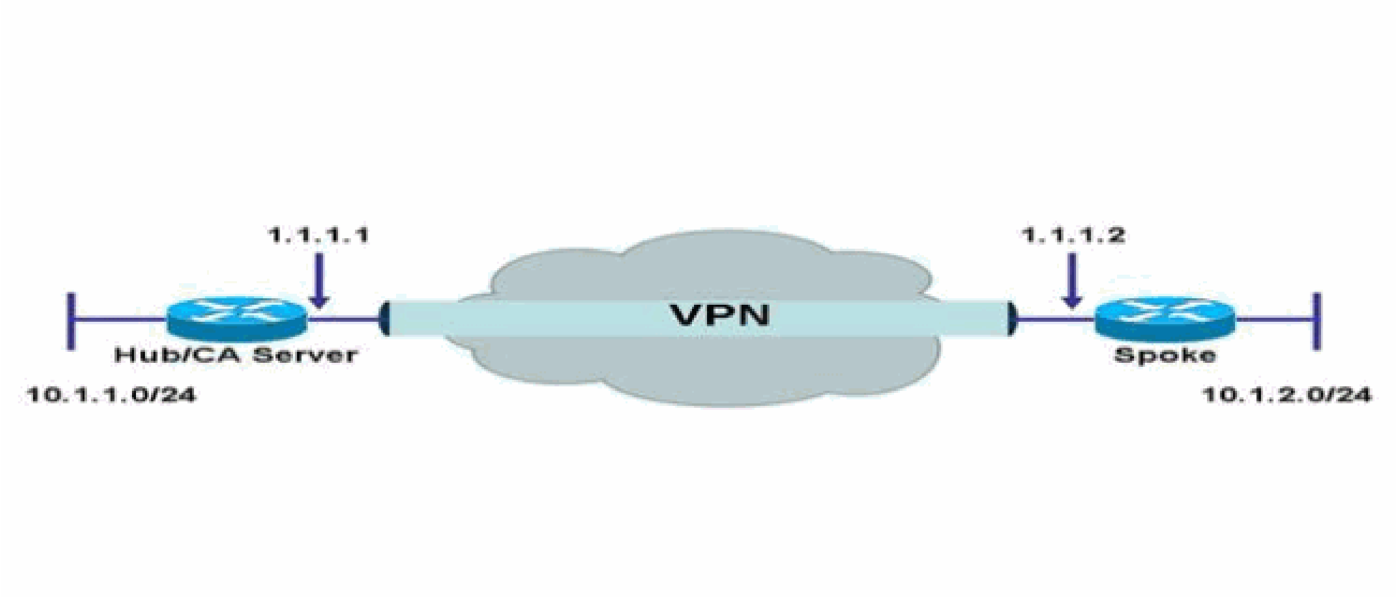
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- 在路由器上配置 IOS CA 服务器
- 身份验证并注册到 IOS CA 服务器
- 中心配置
- 分支配置

在路由器上配置 IOS CA 服务器

要在路由器上配置 IOS CA 服务器，请完成以下步骤：

1. 发出 **crypto pki server 命令以便输入 IOS CA 服务器配置的参数。**在本例中，赋予 IOS CA 服务器配置的标签是 **cisco**。该标签可以是您喜欢的任何名称。
   ```
   HubIOSCA(config)#crypto pki server cisco
   ```
2. 发出 **issuer-name 子命令以便定义证书信息。**在本例中，公用名称(CN)、位置(L)、状态(ST)和国家/地区代码(C)定义如下：
   ```
   HubIOSCA(cs-server)#issuer-name CN=iosca.cisco.com L=RTP ST=NC C=US
   ```

3. 发出 **grant 命令。**在本例中，IOS 服务器自动向客户端授予证书。

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

4. 发出 **no shut 命令以便启用 IOS CA 服务器。**

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

   在您输入此命令后，系统提示您输入密码短语以保护私有密钥。在生成 CA 证书以后，有些服务器设置无法进行更改。输入密码短语以保护私有密钥，或输入 **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.
   ```

身份验证并注册到 IOS CA 服务器

证书服务器也有一个自动生成的同名信任点。该信任点存储证书服务器的证书。当路由器检测到正在使用某个信任点存储证书服务器的证书之后，该信任点将会锁定，无法对其进行修改。

1. 在您配置证书服务器之前，您可以发出 **crypto pki trustpoint 命令以便手工创建和设置此信任点。**这样，您就可以指定一个备用 RSA 密钥对（使用 **rsakeypair 命令）。注意：**自动生成的信任点和证书服务器证书对于证书服务器设备标识不可用。因此，用于指定CA信任点以获取证书和验证客户端连接证书的任何命令行界面(CLI)(如**ip http secure-trustpoint**命令)都必须指向证书服务器设备上配置的附加信任点。如果服务器是根证书服务器，则它使用 RSA 密钥对和几个其他属性生成自签名证书。相关的 CA 证书具有以下密钥扩展用途：数字签名证书签名证书撤销列表(CRL)签名在本例中，HubIOSCA 路由器使用其他信任点凭借证书进行登记以便能与分支路由器建立 VPN 隧道。按照下面所示定义一个信任点（iosca 是为这个新信任点指定的名称）：

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

2. 输入注册 URL，如下所示：

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

   在本例中，未进行 CRL 撤销检查。

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

3. 发出 **crypto ca authenticate iosca 命令以便接收根证书。**

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

   该证书具有以下属性：

   ```
   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. 发出 **crypto ca enroll iosca 命令以便获取身份证书。**

   ```
   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. 发出 **show crypto pki cert** 命令以便验证已安装了证书。

```
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：由于CA服务器也是IPSec对等体，因此中心路由器需要对位于同一路由器上的CA服务器进行身份验证并注册到该服务器。

中心配置

中心配置

```
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
```

验证

当前没有可用于此配置的验证过程。

故障排除

L2L隧道的证书身份验证失败。

有时，当您使用有效的CA证书进行ISAKMP身份验证时，IPsec协商可能会失败。VPN隧道协商与预共享密钥配合使用，因为预共享密钥确实是小数据包。如果证书身份验证需要通过发送整个证书，这会创建大数据包，这些数据包会被分段。分段会阻止证书在设备之间正确进行身份验证。

降低MTU并切换为全双工以解决此问题。将MTU值设置为无需分段的大小：

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

相关信息

- 技术支持和文档 - Cisco Systems