# Ejemplo de Configuración de VPN de LAN a LAN Dinámica entre Routers de Cisco IOS Usando CA de IOS en el Hub

### Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configurar Diagrama de la red Configuraciones Verificación Troubleshoot La autenticación de certificado falla para un túnel L2L. Información Relacionada

# **Introducción**

Este documento proporciona una configuración de ejemplo para Dynamic LAN to LAN VPN entre routers Cisco IOS<sup>®</sup> que utilizan certificados digitales mientras utilizan la función IOS Certificate Authority (CA). Este documento muestra cómo configurar el servidor de CA de IOS y cómo configurar un Cisco IOS Router para obtener un certificado de identidad mediante inscripción automática.

### **Prerequisites**

### **Requirements**

No hay requisitos específicos para este documento.

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco 2851 que ejecuta la versión 12.4(6) T del software del IOS de Cisco
- Router Cisco 871 que ejecuta la versión 12.3(14)YT1 del software del IOS de Cisco

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### **Convenciones**

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

# <u>Configurar</u>

En esta sección encontrará la información para configurar las funciones descritas en este documento.

<u>Nota:</u> Utilice la herramienta <u>Command Lookup</u> (sólo para clientes <u>registrados</u>) para obtener más información sobre los comandos utilizados en esta sección.

#### Diagrama de la red

En este documento, se utiliza esta configuración de red:



### **Configuraciones**

En este documento, se utilizan estas configuraciones:

- Configuración del servidor de la CA del IOS en el router
- Autenticar e Inscribirse en un Servidor de CA de IOS
- <u>Configuración del hub</u>
- <u>Configuración de Spoke</u>

Configuración del servidor de la CA del IOS en el router

Complete estos pasos para configurar el servidor de la CA del IOS en el router:

- Ejecute el comando crypto pki server para ingresar los parámetros para la configuración del servidor de la CA del IOS.En este caso, la etiqueta que se da a la configuración del servidor de la CA del IOS es cisco. La etiqueta puede ser lo que quieras. HubIOSCA(config)#crypto pki server cisco
- 2. Ejecute el subcomando nombre-emisor para definir la información del certificado.En este caso, el nombre común (CN), la localidad (L), el estado (ST) y el código de país (C) se definen como se muestra aquí: HubIOSCA(cs-server)#issuer-name CN=iosca.cisco.com L=RTP ST=NC C=US
- 3. Ejecute el comando **Grant**.En este caso, el servidor IOS otorga automáticamente un certificado al cliente.

HubIOSCA(cs-server)#grant auto

4. Ejecute el comando **no shut** para habilitar el servidor IOS CA. HubIOSCA(cs-server)#no shut

Después de ingresar este comando, se le pedirá que introduzca una frase de paso para proteger la clave privada. Algunos parámetros del servidor no se pueden cambiar después de la generación de certificados de CA. Introduzca una frase de paso para proteger la clave privada o **Return** para salir.

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.

#### Autenticar e Inscribirse en un Servidor de CA de IOS

El servidor de certificados también tiene un punto de confianza generado automáticamente con el mismo nombre. El punto de confianza almacena el certificado del servidor de certificados. Después de que el router detecta que se está utilizando un punto de confianza para almacenar el certificado del servidor de certificados, el punto de confianza se bloquea para que no pueda modificarse.

1. Antes de configurar el servidor de certificados, puede ejecutar el comando crypto pki trustpoint para crear y configurar manualmente este punto de confianza. Esto le permite especificar un par de llaves RSA alternativo (usando el comando rsakeypair). Nota: El punto de confianza generado automáticamente y el certificado del servidor de certificados no están disponibles para la identidad del dispositivo del servidor de certificados. Por lo tanto, cualquier interfaz de línea de comandos (CLI), como el comando ip http secure-trustpoint, que se utiliza para especificar el punto de confianza de CA para obtener certificados y autenticar el certificado de conexión del cliente, debe apuntar a un punto de confianza adicional configurado en el dispositivo del servidor de certificados.Si el servidor es un servidor de certificado autofirmado. El certificado de CA asociado tiene estas extensiones de uso de claves:Firma digitalFirma del certificadoFirma de la lista de revocación de certificados (CRL)En este caso, el router HubIOSCA está inscrito con un certificado usando un punto de confianza diferente para poder establecer un túnel VPN con el router spoke. Defina un punto de confianza, como se muestra aquí (iosca es el nombre dado a este nuevo punto de

confianza):

HubIOSCA(config)#crypto pki trustpoint iosca

2. Introduzca la URL de inscripción, como se muestra aquí: HubIOSCA(ca-trustpoint)#enrollment url http://1.1.1.1:80

En este caso, no se realiza ninguna comprobación de revocación de CRL. HubIOSCA(ca-trustpoint)**#revocation-check none** 

3. Ejecute el comando crypto ca authenticate iosca para recibir el certificado raíz. HubIOSCA(config)#crypto ca authenticate iosca

El certificado tiene estos atributos:

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. Ejecute el comando crypto ca enroll iosca para obtener el certificado de identidad.

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. Ejecute el comando **show crypto pki cert** para verificar que los certificados se hayan instalado.

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
```

**Nota:** Debido a que el servidor de la CA también es un par IPSec, el router hub necesita autenticarse e inscribirse en el servidor de la CA que está en el mismo router.

### Configuración del hub

Configuración del hub							
version 12.4							
service timestamps debug datetime msec							
service timestamps log datetime msec							
no service password-engryption							
io service password-encryption							
:							
noschame Hublosca							
DOOL-SLART-MARKER							
boot-end-marker							
logging buffered 4096 debugging							
!							
no aaa new-model							
1							
resource policy							
1							
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							
!							
<pre>! Configure a certificate map that will be used !</pre>							
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 guit grypto pki certificate chain jogga							
certificate 02 / Identity certificate received from							
the TOS CA 1 after trustpoint enrollment 30820213							
3082017C 20030201 02020102 30000609 28864886 57000101							
SUZULIC RUUSUZUL UZUZULUZ SUDDUUUS ZRUUHUUU FIUDULUL							

	3312930	27060355	04031320	696F7363	612E6369
73636F2E 63	86F6D20	4C3D5254	50205354	3D4E4320	433D5553
301E170D 30	363038	31313139	31313535	5A170D30	37303831
31313931 31	35355A	30233121	301F0609	2A864886	F70D0109
02161248 75	562494F	5343412E	63697363	6F2E636F	6D30819F
300D0609 2A	4864886	F70D0101	01050003	818D0030	81890281
8100B811 AD	3AABA8	3EC63A04	40E4B3ED	1C783C22	20C65122
6E560D22 27	731CAD5	2CC56CBD	554C69FF	4AE3EA1B	CAB25918
B249D32A A7	7861362	7E4257F3	855BD60F	FBA8D33D	15F925C5
746B9144 97	DCFFEE	4CD81070	43C9343F	92C645BC	37E0EF26
5E04394B 67	7CC536E	BFD920DE	52DC977D	830B3C60	D3CB7003
578BB681 D3	307FF4F	629F0203	010001A3	4F304D30	0B060355
1D0F0404 03	30205A0	301F0603	551D2304	18301680	14AC041C
685BDA03 4E	271B7FB	59BAE0A3	5422F759	1E301D06	03551D0E
04160414 6A	A60490F	5CC612A3	EA661102	9D645413	41F9236F
300D0609 2A	864886	F70D0101	04050003	818100BA	2DDC2D0A
5F7B4B3D 80	C8C770D	34AC1A17	EE91A89A	46FD5B9B	8550B2C5
8B8D31EC 29	D8AC3A	8F4B1A96	4C733B9D	FD98BF42	2FDFC6B1
E1D762E1 3D	04470BD	CFC73DF8	E55D7C0A	871159C5	544319B9
1DEC6563 75	5403B97	7567A81D	27F2688C	E955CED7	6E9BC90F
7D3C4C94 81	EDA619	835AF696	8E4A8BF3	C54A242D	8DB5DE59
E5B37E quit	certif	icate ca	01 ! F	loot certi	ificate
received fr	com the	IOS CA !-	after	trustpoir	lt
authenticat	<i>ion.</i> 30	82022F 30	820198 A0	030201 02	2020101
300D0609 2A	4864886	FYODOLOL	04050030	2B312930	27060355
04031320 69	96F'7363	612E6369	73636F2E	636F6D20	4C3D5254
50205354 3L	04E4320	433D5553	301E1/0D	30363038	31313139
30313534 5A	AI/UD30	39303831	30313930	3135345A	302B3129
30270603 55		20096F73	03012E03	69/3636F	2E636F6D
20403052 54	1010101	010E0002	20433D55	01000001	300D0609
2A004000 F/		62616006		22020602	0100C300
240CFD03 80		CODOCOCO		5293005	
955004F5 2A	768BD45			35575455	15253233
250F228E 95	000D45 50Δ34D4	1620C98C	20FFB14B		4612F6EC
58457D98 AF	39BD937	B29691F9	FDBCBF21	860323FF	10121010 1A1C9D7B
39A41C4B 13	310203	010001A3	63306130	0F060355	1D130101
FF040530 03	30101FF	300E0603	551D0F01	01FF0404	03020186
301F0603 55	51D2304	18301680	14AC041C	685BDA03	4E71B7FB
59BAE0A3 54	122F759	1E301D06	03551D0E	04160414	AC041C68
5BDA034E 71	B7FB59	BAE0A354	22F7591E	300D0609	2A864886
F70D0101 04	1050003	81810099	256FCF71	084766ED	BDE8F6D8
F158BDF0 D1	875B0A	57A3FBB8	DD8EF9AD	E5BB3E95	3A65893B
B11DBE9A 6E	593701	0B1DAECA	FE7388B8	D2B1EFF9	B1269F90
C418BCD1 C4	15A1B64	99C1A400	99897C7D	9720A789	A374E8D1
E117CEE5 CD	090F678	98ECFD46	7DF3C029	58B85899	74D34A52
B489A610 8D	DED6FA7	7012D13B	1B822EB9	7F65BA qu	it !
B489A610 8D <i>Configure 1</i>	DED6FA7 I <i>PSEC ph</i>	7012D13B ase 1 par	1B822EB9 <i>cameters</i> .	7F65BA qu crypto is	it ! sakmp policy
B489A610 8D <i>Configure 1</i> 10 hash md5	DED6FA7 I <i>PSEC ph</i> 5 ! !	7012D13B ase 1 par Configur	1B822EB9 rameters. re ISAKMP	7F65BA qu crypto is profile f	ait ! sakmp policy for the
B489A610 8E <i>Configure 1</i> 10 hash md5 <i>dynamic !</i>	DED6FA7 [ <i>PSEC_ph</i> 5 ! ! LAN t	7012D13B ase 1 par Configur o LAN tur	1B822EB9 rameters. re ISAKMP nnel. cryp	7F65BA qu crypto is profile f pto isakmp	ait ! sakmp policy for the p profile
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t	DED6FA7 [ <i>PSEC ph</i> 5 ! ! <i>LAN t</i> crust-po	7012D13B ase 1 par Configur o LAN tur int iosca	1B822EB9 rameters. re ISAKMP nnel. cryp match ce	7F65BA qu crypto is profile f oto isakmp ertificate	ait ! sakmp policy for the p profile a certmap !
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse	DED6FA7 IPSEC ph 5 ! ! LAN t crust-po ec trans	7012D13B ase 1 par Configur o LAN tur int iosca form-set	1B822EB9 cameters. ce ISAKMP mel. cryp match ce strong ah	7F65BA qu crypto is profile i oto isakmp ertificate -md5-hmac	ait ! sakmp policy for the p profile e certmap ! c esp-des !
B489A610 8D Configure 1 10 hash md5 dynamic ! 121vpn ca t crypto ipse ! Config	DED6FA7 <i>IPSEC ph</i> <i>LAN t</i> <i>LAN t</i> <i>LAN t</i> <i>LAN t</i> <i>LAN t</i> <i>LAN t</i>	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp	1B822EB9 rameters. re ISAKMP mel. cryp match ce strong ah oto map. c	7F65BA qu crypto is profile i eto isakmy ertificate -md5-hmac erypto dyr	ait ! sakmp policy for the p profile e certmap ! c esp-des ! namic-map
B489A610 8E Configure 1 10 hash md5 dynamic ! 121vpn ca t crypto ipse ! Config dynmap 10 s	DEDGFA7 <i>IPSEC ph</i> 5 ! ! LAN t crust-po ec trans gure dyn set tran	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set	1B822EB9 rameters. re ISAKMP mel. cryp match ce strong ah oto map. co strong s	7F65BA qu crypto is profile i oto isakmy ertificate md5-hmac erypto dyr set isakmy	ait ! sakmp policy for the profile certmap ! cesp-des ! namic-map p-profile
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn !	DEDGFA7 <i>IPSEC ph</i> 5 ! ! LAN t crust-po ec trans gure dyn set tran - Config	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set ure crypt	1B822EB9 ameters. The ISAKMP amel. crypt a match ce strong am bto map. co strong s co map tha	7F65BA qu crypto is profile i oto isakmp ertificate -md5-hmac erypto dyr set isakmp at will be	<pre>it ! sakmp policy for the p profile c certmap ! c esp-des ! namic-map p-profile c applied on</pre>
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn ! ! the ph	DEDGFA7 <i>IPSEC ph</i> 5 ! ! LAN t crust-po ec trans gure dyn set tran - Config mysical	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set ure crypt interface	1B822EB9 ameters. re ISAKMP mel. cryp match ce strong an oto map. co strong s co map that e. crypto	7F65BA qu crypto is profile i eto isakmp ertificate rmd5-hmac erypto dyr et isakmp it will be map mymap	<pre>it ! sakmp policy for the p profile c certmap ! sesp-des ! namic-map p-profile e applied on p 10 ipsec-</pre>
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn ! ! the ph isakmp dyna	DEDGFA7 IPSEC ph 5 ! ! LAN t crust-po ec trans gure dyn set tran - Config hysical amic dyn	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set ure crypt interface map ! int	1B822EB9 rameters. re ISAKMP mel. crypt match ce strong ah oto map. co strong s co map that e. crypto erface Gi	7F65BA qu crypto is profile i eto isakmy ertificate -md5-hmac erypto dyr et isakmy at will be map mymap gabitEthe	<pre>it ! sakmp policy for the profile certmap ! cesp-des ! namic-map p-profile capplied on p 10 ipsec- ernet0/0 ip</pre>
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn ! ! the ph isakmp dyna address 14.	DEDGFA7 <i>IPSEC ph</i> <i>i !</i> <i>LAN t</i> crust-po ec trans <i>gure dyn</i> set tran <i>- Config</i> <i>hysical</i> amic dyn <i>1.21.19</i>	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set ure crypt interface map ! int 9 255.255	1B822EB9 mameters. re ISAKMP mel. crypt match ce strong ah oto map. co strong s co map that e. crypto match ce strong s co map that e. crypto strong s strong strong s strong strong	7F65BA qu crypto is profile i eto isakmp ertificate -md5-hmac erypto dyr set isakmp at will be map mymap gabitEthe plex auto	<pre>hit ! sakmp policy for the profile c certmap ! c esp-des ! hamic-map p-profile c applied on p 10 ipsec- ernet0/0 ip p speed auto raiged</pre>
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn ! ! the ph isakmp dyna address 14. no keepaliv	DEDGFA7 IPSEC ph 5 ! ! LAN t crust-po cc trans gure dyn set tran - Config hysical amic dyn 1.21.19 re !	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic crypt sform-set ure crypt interface map ! int 9 255.255 Apply cry	1B822EB9 ameters. re ISAKMP mel. crypt match ce strong ah oto map. cc strong s co map that e. crypto cerface Gi 5.252.0 du pto map t	7F65BA qu crypto is profile i oto isakmy ertificate 	<pre>it ! sakmp policy for the profile certmap ! cesp-des ! namic-map p-profile e applied on p 10 ipsec- ernet0/0 ip p speed auto vsical ddreag</pre>
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn ! ! the ph isakmp dyna address 14. no keepaliv interface.	DEDGFA7 IPSEC ph S ! ! LAN t crust-po ec trans gure dyn set tran - Config mysical amic dyn 1.21.19 re ! interfa	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set ure crypt interface map ! int 9 255.255 Apply cry ce Gigabi	1B822EB9 ameters. re ISAKMP mel. crypt match ce strong ah to map. cc strong s co map that e. crypto erface Gi 5.252.0 du pto map t tEthernet	7F65BA qu crypto is profile i oto isakmp ertificate -md5-hmac erypto dyr set isakmp at will be map mymap gabitEthe plex auto to the phy 0/1 ip ac	<pre>hit ! sakmp policy for the profile certmap ! cesp-des ! hamic-map p-profile capplied on pol0 ipsec- ernet0/0 ip pospeed auto vsical ddress cerveto man</pre>
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn ! ! the ph isakmp dyna address 14. no keepaliv interface. 1.1.1.1 255	DEDGFA7 IPSEC ph 5 ! ! LAN t crust-po ec trans gure dyn set tran - Config hysical amic dyn 1.21.19 ye ! interfa 5.255.25 erface	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set ure crypt interface map ! int 9 255.255 Apply cry ce Gigabi 5.0 duple	1B822EB9 ameters. re ISAKMP amel. cryp a match ce strong am ato map. co strong s co map that c. crypto c. crypto c. crypto c. crypto c. crypto d. crypto d. crypto c. crypto c. crypto d. crypto c. crypt	7F65BA qu crypto is profile i eto isakmp ertificate a-md5-hmac rypto dyr et isakmp at will be map mymap gabitEthe plex auto co the phy 0/1 ip ac peed auto	<pre>it ! sakmp policy for the p profile c certmap ! c esp-des ! namic-map p-profile e applied on p 10 ipsec- ernet0/0 ip p speed auto vsical ddress crypto map ace</pre>
B489A610 8E Configure 1 10 hash md5 dynamic ! 12lvpn ca t crypto ipse ! Config dynmap 10 s 12lvpn ! ! the ph isakmp dyna address 14. no keepaliv interface. 1.1.1.1 255 mymap ! int FastEtherne	DEDGFA7 IPSEC ph 5 ! ! LAN t crust-po ec trans gure dyn set tran - Config hysical amic dyn 1.21.19 ye ! interfa 5.255.25 cerface at 0/2/1	7012D13B ase 1 par Configur o LAN tur int iosca form-set amic cryp sform-set ure crypt interface map ! int 9 255.255 Apply cry ce Gigabi 5.0 duple FastEther	1B822EB9 mameters. re ISAKMP mel. crypt match ce strong ah oto map. cc strong s co map that e. crypto merface Gi 0.252.0 du mpto map t tEthernet ex auto sp met0/2/0 ce FastFt	7F65BA qu crypto is profile i eto isakmy ertificate -md5-hmac erypto dyr et isakmy at will be map mymap gabitEthe plex auto 0/1 ip ac eed auto	<pre>hit ! sakmp policy for the profile c certmap ! c esp-des ! hamic-map p-profile c applied on p 10 ipsec- ernet0/0 ip p speed auto vsical ddress crypto map ace 2/2 !</pre>

10.1.1.254 255.255.255.0 ! ip route 0.0.0.0 0.0.0 GigabitEthernet0/1 ! ip http server no ip http secureserver ! 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

#### Configuración de Spoke

Configuración de Spoke								
version 1	2.3							
no servic	e pad							
service t	imestamps	s debuq da	atetime ma	sec				
service timestamps log datetime msec								
no servic	e passwoi	d-encrypt	cion					
hostname	Spoke							
!	-							
boot-star	t-marker							
boot-end-	marker							
!								
no aaa ne	w-model							
!								
resource	policy							
!								
ip subnet	-zero							
ip cef								
!								
no ip dha	p use vrf	connecte	ed					
!								
ip domain	name cis	sco.com						
no ip ips	deny-act	ion ips-i	interface					
! Conf	Eigure a t	trustpoint	t that the	is router	will use !-			
to aut	henticate	e and enro	oll to the	e IOS CA :	Server.			
crypto pk	i trustpo	oint iosca	a enrollme	ent url				
http://1.	1.1.1:80	revocatio	on-check r	none ! !	Configure			
a certifi	cate map	that will	l be !	used in a	the ISAKMP			
profile.	crypto pł	i certifi	icate map	certmap 2	l issuer-			
name co c	isco.com	! crypto	pki certi	ificate cl	nain iosca			
certifica	ite 03 308	320210 308	320179 A00	030201 020	020103			
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
OB1DAECA 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
121vpn 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
```

# **Verificación**

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

### **Troubleshoot**

### La autenticación de certificado falla para un túnel L2L.

A veces, la negociación IPSec puede fallar cuando utiliza un certificado CA válido para la

autenticación ISAKMP. La negociación del túnel VPN funciona con claves previamente compartidas porque las claves previamente compartidas son realmente paquetes pequeños. Si la autenticación del certificado necesita enviar el certificado completo a través, esto crea grandes paquetes que se fragmentan. La fragmentación evita que el certificado se autentique correctamente entre los dispositivos.

Baje la MTU y cambie a dúplex completo para resolver este problema. Configure el valor de MTU en un tamaño que no deba fragmentarse:

Router(config)#interface type [slot\_#/]port\_#
Router(config-if)#ip mtu MTU\_size\_in\_bytes

# Información Relacionada

Soporte Técnico y Documentación - Cisco Systems