

IPSec de roteador a roteador (chaves RSA) no túnel GRE com exemplo da configuração RIP

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Procedimento de Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece uma configuração de exemplo para roteadores com chaves RSA. Ambos os roteadores são configurados para chaves RSA e túnel de IPSec/Generic Routing Encapsulation (GRE) com Routing Information Protocol (RIP).

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador Cisco que executa o Software Release 12.2 de Cisco IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- [Configuração de criptografia para o roteador 101](#)
- [Roteador 101](#)
- [Configuração de criptografia para o roteador 102](#)
- [Roteador 102](#)

Configuração de criptografia para o roteador 101

```
101(config)#crypto isakmp enable
101(config)#crypto isakmp identity hostname
101(config)#crypto isakmp policy 1
101(config-isakmp)#authentication rsa-encr
101(config)#access-list 101 permit gre host 20.1.1.1
host 20.1.1.2
101(config)#crypto ipsec transform-set test esp-des esp-
sha-hmac
101(cfg-crypto-trans)#mode transport
101(config)#crypto map test 10 ip
101(config)#crypto map test 10 ipsec-is
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
101(config-crypto-map)#set transform-set test
101(config-crypto-map)#match address 101
101(config-crypto-map)#set peer 20.1.1.2
```

```
101(config-crypto-map)#  
  
101(config)#access-list 101 permit gre host 20.1.1.1  
host 20.1.1.2  
  
101(config)#interface Tunnel0  
101(config-if)#crypto map test  
  
101(config)#interface ethernet 1/0  
101(config-if)#crypto map test
```

Roteador 101

```
101(config)#crypto isakmp enable  
101(config)#crypto isakmp identity hostname  
101(config)#crypto isakmp policy 1  
101(config-isakmp)#authentication rsa-encr  
101(config)#access-list 101 permit gre host 20.1.1.1  
host 20.1.1.2  
101(config)#crypto ipsec transform-set test esp-des esp-  
sha-hmac  
101(cfg-crypto-trans)#mode transport  
101(config)#crypto map test 10 ip  
101(config)#crypto map test 10 ipsec-is  
% NOTE: This new crypto map will remain disabled until a  
peer  
and a valid access list have been configured.  
101(config-crypto-map)#set transform-set test  
101(config-crypto-map)#match address 101  
101(config-crypto-map)#set peer 20.1.1.2  
101(config-crypto-map)#  
  
101(config)#access-list 101 permit gre host 20.1.1.1  
host 20.1.1.2  
  
101(config)#interface Tunnel0  
101(config-if)#crypto map test  
  
101(config)#interface ethernet 1/0  
101(config-if)#crypto map test
```

Configuração de criptografia para o roteador 102

```
102(config)#crypto isakmp enable  
102(config)#crypto isakmp identity hostname  
102(config)#crypto isakmp policy 1  
102(config-isakmp)#authentication rsa-encr  
102(config)#access-list 101 permit gre host 20.1.1.2  
host 20.1.1.1  
102(config)#crypto ipsec transform-set test esp-des esp-  
sha-hmac  
102(cfg-crypto-trans)#mode transport  
102(config)#crypto map test 10 ip  
102(config)#crypto map test 10 ipsec-is  
% NOTE: This new crypto map will remain disabled until a  
peer  
and a valid access list have been configured.  
102(config-crypto-map)#set transform-set test  
102(config-crypto-map)#match address 101  
102(config-crypto-map)#set peer 20.1.1.1  
102(config-crypto-map)#
```

```
102(config)#interface Tunnel0
102(config-if)#crypto map test

102(config)#interface ethernet 1/0
102(config-if)#crypto map test
```

Roteador 102

```
102#write terminal
Building configuration...

Current configuration : 1484 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 102
!
!
clock timezone PST -8
ip subnet-zero
ip domain name cisco.com
ip host 101.cisco.com 20.1.1.1
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
 authentication rsa-encr
crypto isakmp identity hostname
crypto isakmp keepalive 20 5
!
!
crypto ipsec transform-set test esp-des esp-sha-hmac
 mode transport
!
crypto map test 10 ipsec-isakmp
 set peer 20.1.1.1
 set transform-set test
 match address 101
!
!
crypto key pubkey-chain rsa
 named-key 101.cisco.com
 address 20.1.1.1
 key-string
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241
00A7D24F E6E15787
 5EE1434A A76A3DC1 ADE96A4D C6B4D0F3 A7DDAD10 446EF83A
89D1115F 0C517118
 ECAF418E F4C84823 2A017B97 F85690EF EBCF3414 AB3E81F6
A5020301 0001
 quit
!
!
!
interface Loopback1
 ip address 172.16.1.1 255.255.255.0
!
```

```
interface Tunnel0
 ip address 10.10.10.2 255.255.255.252
 ip mtu 1420
 tunnel source Ethernet0/0
 tunnel destination 20.1.1.1
 crypto map test
!
interface Ethernet0/0
 ip address 20.1.1.2 255.255.255.0
 crypto map test
!
interface Ethernet1/0
 no ip address
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface Ethernet0/0
 network 10.0.0.0
 network 172.16.0.0
!
ip classless
no ip http server
!
!
access-list 101 permit gre host 20.1.1.2 host 20.1.1.1
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
102#
```

[Verificar](#)

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **mostre o detalhe cripto isakmp sa** — Indica todas as associações de segurança atuais do Internet Key Exchange (IKE) (SA) em um par.
- **mostre IPsec cripto sa** — Indica os ajustes usados por SA atuais.
- **active do show crypto engine connections** — Indica um sumário da informação de configuração para as crypto-engines.
- **show ip route** - Exibe o estado atual da tabela de roteamento.

Saída do comando do roteador 101

101#show crypto isakmp sa detail

*Dec 28 21:15:19.371: ISAKMP (0:14): purging node 543282640

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

Conn id	Local	Remote	Encr	Hash	Auth	DH	Lifetime	Capabilities
14	20.1.1.1	20.1.1.2	des	sha	rsig	1	23:59:06	D

101#show crypto ipsec sa

interface: Ethernet1/0

Crypto map tag: test, local addr. 20.1.1.1

local ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)

current_peer: 20.1.1.2:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 20.1.1.1, remote crypto endpt.: 20.1.1.2

path mtu 1420, media mtu 1420

current outbound spi: 7FB7A347

inbound esp sas:

spi: 0x7221D7D2(1914820562)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: test

sa timing: remaining key lifetime (k/sec): (4468975/3586)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x7FB7A347(2142741319)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2001, flow_id: 2, crypto map: test

sa timing: remaining key lifetime (k/sec): (4468975/3586)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

interface: Tunnel0
  Crypto map tag: test, local addr. 20.1.1.1

local ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)
current_peer: 20.1.1.2:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 20.1.1.1, remote crypto endpt.: 20.1.1.2
path mtu 1420, media mtu 1420
current outbound spi: 7FB7A347

inbound esp sas:
  spi: 0x7221D7D2(1914820562)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Transport, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4468975/3585)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x7FB7A347(2142741319)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Transport, }
    slot: 0, conn id: 2001, flow_id: 2, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4468975/3584)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

101#**show crypto engine connections active**

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
14	Ethernet1/0	20.1.1.1	set	HMAC_SHA+DES_56_CB	0	0
2000	Ethernet1/0	20.1.1.1	set	HMAC_SHA+DES_56_CB	0	6
2001	Ethernet1/0	20.1.1.1	set	HMAC_SHA+DES_56_CB	5	0

101#**show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

```

Gateway of last resort is not set

```
    20.0.0.0/24 is subnetted, 1 subnets
C       20.1.1.0 is directly connected, Ethernet1/0
R       172.16.0.0/16 [120/1] via 10.10.10.2, 00:00:08, Tunnel0
    10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Tunnel0
C       192.168.1.0/24 is directly connected, Loopback1
101#
```

[Saída do comando do roteador 102](#)

102#show crypto isakmp sa detail

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
```

Conn id	Local	Remote	Encr	Hash	Auth	DH	Lifetime	Capabilities
15	20.1.1.2	20.1.1.1	des	sha	rsig	1	23:58:44	D

102#show crypto ipsec sa

interface: Ethernet0/0

Crypto map tag: test, local addr. 20.1.1.2

```
local ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)
current_peer: 20.1.1.1:500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 20.1.1.2, remote crypto endpt.: 20.1.1.1
path mtu 1420, media mtu 1420
current outbound spi: 92F52EF2
```

inbound esp sas:

```
spi: 0x1D25013E(488964414)
  transform: esp-des esp-sha-hmac ,
  in use settings = {Transport, }
  slot: 0, conn id: 2000, flow_id: 1, crypto map: test
  sa timing: remaining key lifetime (k/sec): (4596388/3494)
  IV size: 8 bytes
  replay detection support: Y
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x92F52EF2(2465541874)
  transform: esp-des esp-sha-hmac ,
  in use settings = {Transport, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: test
  sa timing: remaining key lifetime (k/sec): (4596388/3494)
```


IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

interface: Tunnel0

Crypto map tag: test, local addr. 20.1.1.2

local ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)

current_peer: 20.1.1.1:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 20.1.1.2, remote crypto endpt.: 20.1.1.1

path mtu 1420, media mtu 1420

current outbound spi: 92F52EF2

inbound esp sas:

spi: 0x1D25013E(488964414)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: test

sa timing: remaining key lifetime (k/sec): (4596388/3493)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x92F52EF2(2465541874)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2001, flow_id: 2, crypto map: test

sa timing: remaining key lifetime (k/sec): (4596388/3493)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

102#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
15	Ethernet0/0	20.1.1.2	set	HMAC_SHA+DES_56_CB	0	0
2000	Ethernet0/0	20.1.1.2	set	HMAC_SHA+DES_56_CB	0	3
2001	Ethernet0/0	20.1.1.2	set	HMAC_SHA+DES_56_CB	4	0

102#

102#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```
20.0.0.0/24 is subnetted, 1 subnets
C    20.1.1.0 is directly connected, Ethernet0/0
172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.0 is directly connected, Loopback1
10.0.0.0/30 is subnetted, 1 subnets
C    10.10.10.0 is directly connected, Tunnel0
R    192.168.1.0/24 [120/1] via 10.10.10.1, 00:00:08, Tunnel0
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. Para obter informações adicionais sobre do Troubleshooting, veja por favor o [Troubleshooting de Segurança IP - Compreendendo e usando comandos debug](#).

Procedimento de Troubleshooting

Siga estas instruções para resolver problemas da sua configuração.

1. Gerencia as chaves RSA no roteador 101.

```
101#show crypto key mypubkey rsa
101#
101#
101#conf t
101(config)#ip domain-name cisco.com
101(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for signing and
                  encryption
  usage-keys    Generate separate RSA key pairs for signing and encryption
```

```
101(config)#crypto key generate rsa
The name for the keys will be: 101.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]
```

```
101#show crypto key mypubkey rsa
% Key pair was generated at: 12:02:08 PST Dec 28 2002
Key name: 101.cisco.com
Usage: General Purpose Key
Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A7D24F E6E15787
  5EE1434A A76A3DC1 ADE96A4D C6B4D0F3 A7DDAD10 446EF83A 89D1115F 0C517118
  ECAF418E F4C84823 2A017B97 F85690EF EBCF3414 AB3E81F6 A5020301 0001
% Key pair was generated at: 12:02:12 PST Dec 28 2002
Key name: 101.cisco.com.server
Usage: Encryption Key
Key Data:
```

```
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B2092A 86483641
EB09900B BA0CD88A BE915C5E 05C1496B 70093D8B BC277A88 0E256BBE 4DB7EF92
8FE93C61 710309A3 451DAB72 93F35CD0 1CAD15AC B904B2B4 73B7A9F5 65A79E66
8D145427 F06DD89C 862B88BB 4C671508 AB3443BB 6270388C A7020301 0001
```

101#

2. Gerencia as chaves RSA no roteador 102.

```
102#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
102(config)#ip domain-name cisco.com
```

```
102(config)#crypto key gen rsa
```

```
The name for the keys will be: 102.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]
```

```
102#show crypto key mypubkey rsa
```

```
% Key pair was generated at: 12:03:45 PST Dec 28 2002
```

```
Key name: 102.cisco.com
```

```
Usage: General Purpose Key
```

```
Key Data:
```

```
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DB4FEB EF0C0D3D
72FC5BD3 29C8E94B 726161BC F1AF337C E5F2D11D FBFC2245 95EA2AB7 9D09156C
08A5A7CD 36E43D94 F1E3C978 37A79379 384D2A72 CE575E91 3F020301 0001
```

```
% Key pair was generated at: 12:03:48 PST Dec 28 2002
```

```
Key name: 102.cisco.com.server
```

```
Usage: Encryption Key
```

```
Key Data:
```

```
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00BFD36E A1642BFC
77C88F89 8A260840 213E122E E1AF1E24 AF39B984 DACA06BC C303AD77 95BB6B6C
89CC6D13 B16CC4E3 45C101E4 61A13924 5559891A AB59B40D 826A5066 231B48D6
AEB2B367 94F6C492 016F8778 74B368A2 BFD1424D 79C63C94 5F020301 0001
```

102#

3. Resolva o hostname.

```
102(config)#ip host 101.cisco.com 20.1.1.1
```

4. Troque as chaves de uso geral no roteador 101.

```
101(config)#crypto key pubkey-chain rsa
```

```
101(config-pubkey-chain)#named-key 102.cisco.com
```

```
% Named public key resolved to ip address: 20.1.1.2
```

```
101(config-pubkey-key)#key-string ?
```

```
Enter a public key as a hexadecimal number ....
```

```
101(config-pubkey)#$6F70D 01010105 00034B00 30480241 00DB4FEB EF0C0D3D
```

```
101(config-pubkey)#$26161BC F1AF337C E5F2D11D FBFC2245 95EA2AB7 9D09156C
```

```
101(config-pubkey)#$1E3C978 37A79379 384D2A72 CE575E91 3F020301 0001
```

```
101(config-pubkey)#quit
```

```
101(config-pubkey-key)#exit
```

5. Troque as chaves de uso geral no roteador 102.

```
102(config)#crypto key pubkey-chain rsa
```

```
102(config-pubkey-chain)#named-key 101.cisco.com
```

```
% Named public key resolved to ip address: 20.1.1.1
```

```
102(config-pubkey-key)#key-string
```

```
Enter a public key as a hexadecimal number ....
```

```
102(config-pubkey)#$6F70D 01010105 00034B00 30480241 00A7D24F E6E15787
```

```
102(config-pubkey)#$DE96A4D C6B4D0F3 A7DDAD10 446EF83A 89D1115F 0C517118
```

```
102(config-pubkey)#$A017B97 F85690EF EBCF3414 AB3E81F6 A5020301 0001
102(config-pubkey)#quit
102(config-pubkey-key)#exit
102(config-pubkey-chain)#exit
102(config)#exit
```

Comandos para Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Note: [Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.](#)

O roteador 101 debuga:

```
102(config)#crypto key pubkey-chain rsa
102(config-pubkey-chain)#named-key 101.cisco.com
% Named public key resolved to ip address: 20.1.1.1
102(config-pubkey-key)#key-string
Enter a public key as a hexadecimal number ....

102(config-pubkey)#$6F70D 01010105 00034B00 30480241 00A7D24F E6E15787
102(config-pubkey)#$DE96A4D C6B4D0F3 A7DDAD10 446EF83A 89D1115F 0C517118
102(config-pubkey)#$A017B97 F85690EF EBCF3414 AB3E81F6 A5020301 0001
102(config-pubkey)#quit
102(config-pubkey-key)#exit
102(config-pubkey-chain)#exit
102(config)#exit
```

O roteador 102 debuga:

```
102(config)#crypto key pubkey-chain rsa
102(config-pubkey-chain)#named-key 101.cisco.com
% Named public key resolved to ip address: 20.1.1.1
102(config-pubkey-key)#key-string
Enter a public key as a hexadecimal number ....

102(config-pubkey)#$6F70D 01010105 00034B00 30480241 00A7D24F E6E15787
102(config-pubkey)#$DE96A4D C6B4D0F3 A7DDAD10 446EF83A 89D1115F 0C517118
102(config-pubkey)#$A017B97 F85690EF EBCF3414 AB3E81F6 A5020301 0001
102(config-pubkey)#quit
102(config-pubkey-key)#exit
102(config-pubkey-chain)#exit
102(config)#exit
```

Informações Relacionadas

- [Página de suporte do IPSec](#)
- [Suporte Técnico - Cisco Systems](#)