

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Saída de depuração do RouterA](#)

[Informações Relacionadas](#)

[Introdução](#)

O Cisco IOS® Software Release 12.2(8)T introduz a funcionalidade do roteador para iniciar o Internet Key Exchange (IKE) no modo agressivo. Para mais informação veja o Bug ID [CSCdt30808 \(clientes registrados somente\)](#) no Bug Toolkit. Antes, o roteador podia responder a um pedido da negociação do túnel no modo agressivo, mas nunca conseguiu iniciá-lo.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- O Cisco IOS 12.2(8)T foi usado em ambos os roteadores, embora não fosse necessário o ter no roteador de recepção.

Nota: Esta configuração foi testada com Cisco IOS Software Release 12.2(13)T1. Todos os aspectos da configuração permanecem os mesmos.

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 você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

[Convenções](#)

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

[Informações de Apoio](#)

Nota: Os comandos novos do comando line interface(cli) são como segue:

- par cripto < endereço <x.x.x.x > do isakmp / <name> do hostname >
- ajuste o <name> do cliente-valor-limite < FQDN do modo assertivo | ipv4-address <x.x.x.x > / <name> USER-FQDN >
- ajuste o <password> da senha do modo assertivo

No exemplo de configuração abaixo, RouterA e RouterB têm um túnel LAN para LAN entre si. O RouterA sempre será o túnel que inicia o roteador, e ele foi configurado neste exemplo para iniciar em modo agressivo. O Roteador B simplesmente tem um mapa de criptografia dinâmico para aceitar os parâmetros de túnel a partir do Roteador A, embora ele também possa ter tido uma configuração de túnel de LAN para LAN aplicada.

Nota: Neste exemplo, o roteadorB não tem que ser Cisco IOS Software Release 12.2(8)T running para aceitar os parâmetros do túnel do roteadorA. Como mencionado acima, os roteadores que sempre aceitaram uma solicitação de modo assertivo simplesmente nunca conseguiram iniciá-lo.

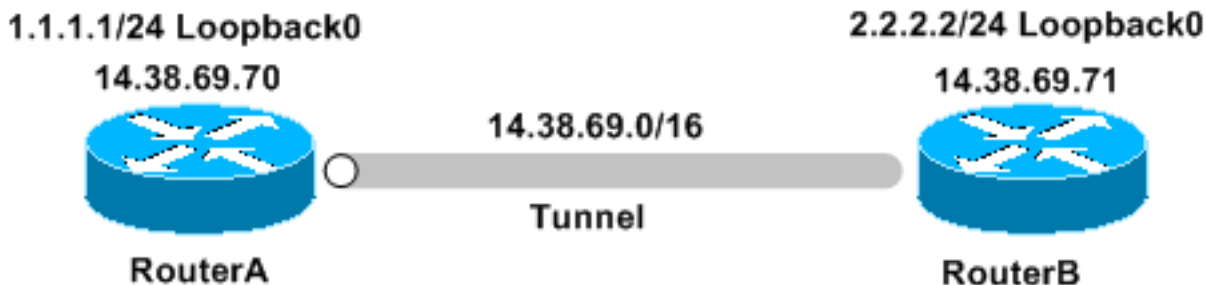
[Configurar](#)

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

Nota: 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 instalação de rede mostrada no diagrama abaixo.



[Configurações](#)

Este documento utiliza as seguintes configurações:

- [RoteadorA](#)

- [RoteadorB](#)

RoteadorA

```
Building configuration...Current configuration : 1253
bytes!version 12.2service timestamps debug uptime
service timestamps log uptime
no service password-
encryption!hostname RouterA!memory-size iomem 10ip
subnet-zero!!!!crypto isakmp policy 1 hash md5
authentication pre-sharecrypto isakmp keepalive 30
5!crypto isakmp peer address 14.38.69.71 set aggressive-
mode password cisco123 set aggressive-mode client-
endpoint ipv4-address 14.38.69.70 !!crypto ipsec
transform-set myset esp-3des esp-md5-hmac !crypto map
mymap 1 ipsec-isakmp set peer 14.38.69.71 set
transform-set myset match address 100!!!
interface Loopback0 ip address 1.1.1.1
255.255.255.0!interface Ethernet0/0 ip address
14.38.69.70 255.255.0.0 half-duplex crypto map
mymap!interface BRI0/0 no ip address shutdown!interface
Ethernet0/1 no ip address shutdown half-duplex!ip
classlessip route 0.0.0.0 0.0.0.0 14.38.69.71ip http
server!
!access-list 100 permit ip 1.1.1.0
0.0.0.255 2.2.2.0 0.0.0.255!call rsvp-sync!!mgcp profile
default!dial-peer cor custom!!line con 0 exec-timeout 0
0line aux 0line vty 0 4 login!!end
```

RoteadorB

```
Building configuration...Current configuration : 1147
bytes!version 12.2service timestamps debug uptime
service timestamps log uptime
no service password-
encryption!hostname RouterB!!ip subnet-zero!!!!crypto
isakmp policy 1 hash md5 authentication pre-sharecrypto
isakmp key cisco123 address 14.38.69.70crypto isakmp
keepalive 30 5!!crypto ipsec transform-set myset esp-
3des esp-md5-hmac !crypto dynamic-map mymap 10 set
transform-set myset !!crypto map mainmap 1 ipsec-isakmp
dynamic mymap !!!interface Loopback0 ip address 2.2.2.2
255.255.255.0!
interface FastEthernet0/0 ip
address 14.38.69.71 255.255.0.0 duplex auto speed auto
crypto map mainmap!interface Serial0/0 no ip address
shutdown no fair-queue!interface FastEthernet0/1 no ip
address shutdown duplex auto speed auto!ip classlessip
route 0.0.0.0 0.0.0.0 14.38.69.70no ip http server!
!call rsvp-sync!!mgcp profile default!dial-peer cor
custom!!line con 0 exec-timeout 0 0 speed 115200line aux
0line vty 0 4 login!!end
```

[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 IPsec cripto sa?** Mostra à fase 2 associações de segurança.
- **mostre isakmp cripto sa?** Mostra as associações de segurança da fase 1

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Nota: Antes de emitir comandos debug, consulte [Informações importantes sobre comandos debug](#).

- **IPsec do debug crypto?** Mostra as negociações de IPSEC de fase 2.
- **isakmp do debug crypto?** Mostra as negociações de ISAKMP de fase 1.
- **motor do debug crypto?** Mostra o tráfego que é cifrado.

Saída de depuração do RouterA

```
00:08:26: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 14.38.69.70, remote=
14.38.69.71, local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4), remote_proxy=
2.2.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 4608000kb, spi= 0x4B68058A(1265108362), conn_id= 0, keysize= 0, flags=
0x400C00:08:26: ISAKMP: received ke message (1/1)00:08:26: ISAKMP: local port 500, remote port
50000:08:26: ISAKMP (0:1): SA has tunnel attributes set.00:08:26: ISAKMP (0:1): SA is doing
unknown authentication!00:08:26: ISAKMP (1): ID payload next-payload : 13 type
: 1 protocol : 17 port : 500 length : 800:08:26: ISAKMP
(1): Total payload length: 1200:08:26: ISAKMP (0:1): Input = IKE_MSG_FROM_IPSEC,
IKE_SA_REQ_AMold State = IKE_READY New State = IKE_I_AM1 00:08:26: ISAKMP (0:1): beginning
Aggressive Mode exchange00:08:26: ISAKMP (0:1): sending packet to 14.38.69.71 (I)
AG_INIT_EXCH...Success rate is 0 percent (0/5)vpn-2611a1#00:08:36: ISAKMP (0:1):
retransmitting phase 1 AG_INIT_EXCH...00:08:36: ISAKMP (0:1): incrementing error counter on sa:
retransmit phase 100:08:36: ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH00:08:36: ISAKMP
(0:1): sending packet to 14.38.69.71 (I) AG_INIT_EXCH00:08:37: ISAKMP (0:1): received packet
from 14.38.69.71 (I) AG_INIT_EXCH00:08:37: ISAKMP (0:1): processing SA payload. message ID =
000:08:37: ISAKMP (0:1): SA using tunnel password as pre-shared key.00:08:37: ISAKMP (0:1):
Checking ISAKMP transform 1 against priority 1 policy00:08:37: ISAKMP: encryption DES-
CBC00:08:37: ISAKMP: hash MD500:08:37: ISAKMP: default group 100:08:37: ISAKMP:
auth pre-share00:08:37: ISAKMP: life type in seconds00:08:37: ISAKMP: life duration
(VPI) of 0x0 0x1 0x51 0x80 00:08:37: ISAKMP (0:1): atts are acceptable. Next payload is
000:08:37: ISAKMP (0:1): processing vendor id payload00:08:37: ISAKMP (0:1): vendor ID is
Unity00:08:37: ISAKMP (0:1): processing vendor id payload00:08:37: ISAKMP (0:1): vendor ID is
DPD00:08:37: ISAKMP (0:1): processing vendor id payload00:08:37: ISAKMP (0:1): speaking to
another IOS box!00:08:37: ISAKMP (0:1): processing vendor id payload00:08:37: ISAKMP (0:1):
processing KE payload. message ID = 000:08:37: ISAKMP (0:1): processing ID payload. message ID =
000:08:37: ISAKMP (0:1): processing NONCE payload. message ID = 000:08:37: ISAKMP (0:1): SA
using tunnel password as pre-shared key.00:08:37: ISAKMP (0:1): SKEYID state generated00:08:37:
ISAKMP (0:1): processing HASH payload. message ID = 000:08:37: ISAKMP (0:1): SA has been
authenticated with 14.38.69.7100:08:37: ISAKMP (0:1): IKE_DPD is enabled, initializing
timers00:08:37: ISAKMP: Locking DPD struct 0x82702444 from crypto_ikmp_dpd_ike_init, count
100:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE 00:08:37: ISAKMP (0:1):
Input = IKE_MSG_FROM_PEER, IKE_AM_EXCHold State = IKE_I_AM1 New State = IKE_P1_COMPLETE
00:08:37: IPSEC(key_engine): got a queue event...00:08:37: IPsec: Key engine got
KEYENG_IKMP_MORE_SAS message00:08:37: ISAKMP: received ke message (6/1)00:08:37: ISAKMP:
received KEYENG_IKMP_MORE_SAS message00:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I)
QM_IDLE 00:08:37: ISAKMP (0:1): purging node -184439443800:08:37: ISAKMP (0:1): Sending
initial contact.00:08:37: ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): processing HASH payload. message ID = 13338122800:08:37: ISAKMP (0:1):
processing NOTIFY RESPONDER_LIFETIME protocol 1 spi 0, message ID = 133381228, sa =
82701CDC00:08:37: ISAKMP (0:1): processing responder lifetime00:08:37: ISAKMP (0:1): deleting
node 133381228 error FALSE reason "informational (in) state 1"00:08:37: ISAKMP (0:1): Input =
```

```
IKE_MSG_FROM_PEER, IKE_INFO_NOTIFYOld State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
00:08:38: ISAKMP: quick mode timer expired.00:08:38: ISAKMP (0:1): src 14.38.69.70 dst
14.38.69.7100:08:38: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -111923856100:08:38:
ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE 00:08:38: ISAKMP (0:1): Node -
1119238561, Input = IKE_MSG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State =
IKE_QM_I_QM1 00:08:38: ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE 00:08:38:
ISAKMP (0:1): processing HASH payload. message ID = -111923856100:08:38: ISAKMP (0:1):
processing SA payload. message ID = -111923856100:08:38: ISAKMP (0:1): Checking IPsec proposal
100:08:38: ISAKMP: transform 1, ESP_3DES00:08:38: ISAKMP: attributes in transform:00:08:38:
ISAKMP: encaps is 100:08:38: ISAKMP: SA life type in seconds00:08:38: ISAKMP: SA
life duration (basic) of 360000:08:38: ISAKMP: SA life type in kilobytes00:08:38: ISAKMP:
SA life duration (VPI) of 0x0 0x46 0x50 0x0 00:08:38: ISAKMP: authenticator is HMAC-
MD500:08:38: ISAKMP (0:1): atts are acceptable.00:08:38: IPSEC(validate_proposal_request):
proposal part #1, (key eng. msg.) INBOUND local= 14.38.69.70, remote= 14.38.69.71,
local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4), remote_proxy= 2.2.2.0/255.255.255.0/0/0
(type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi=
0x0(0), conn_id= 0, keysize= 0, flags= 0x400:08:38: ISAKMP (0:1): processing NONCE payload.
message ID = -111923856100:08:38: ISAKMP (0:1): processing ID payload. message ID = -
111923856100:08:38: ISAKMP (0:1): processing ID payload. message ID = -111923856100:08:38:
ISAKMP (0:1): Creating IPsec SAs00:08:38: inbound SA from 14.38.69.71 to 14.38.69.70
(proxy 2.2.2.0 to 1.1.1.0)00:08:38: has spi 0x4B68058A and conn_id 2000 and flags
400:08:38: lifetime of 3600 seconds00:08:38: lifetime of 4608000
kilobytes00:08:38: outbound SA from 14.38.69.70 to 14.38.69.71 (proxy 1.1.1.0 to
2.2.2.0)00:08:38: has spi 1503230765 and conn_id 2001 and flags C00:08:38:
lifetime of 3600 seconds00:08:38: lifetime of 4608000 kilobytes00:08:38: ISAKMP (0:1):
sending packet to 14.38.69.71 (I) QM_IDLE 00:08:38: ISAKMP (0:1): deleting node -1119238561
error FALSE reason ""00:08:38: ISAKMP (0:1): Node -1119238561, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 00:08:38:
IPSEC(key_engine): got a queue event...00:08:38: IPSEC(initialize_sas): , (key eng. msg.)
INBOUND local= 14.38.69.70, remote= 14.38.69.71, local_proxy= 1.1.1.0/255.255.255.0/0/0
(type=4), remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform=
esp-3des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0x4B68058A(1265108362),
conn_id= 2000, keysize= 0, flags= 0x400:08:38: IPSEC(initialize_sas): , (key eng. msg.)
OUTBOUND local= 14.38.69.70, remote= 14.38.69.71, local_proxy= 1.1.1.0/255.255.255.0/0/0
(type=4), remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform=
esp-3des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0x59997B2D(1503230765),
conn_id= 2001, keysize= 0, flags= 0xC00:08:38: IPSEC(create_sa): sa created, (sa) sa_dest=
14.38.69.70, sa_prot= 50, sa_spi= 0x4B68058A(1265108362), sa_trans= esp-3des esp-md5-
hmac , sa_conn_id= 200000:08:38: IPSEC(create_sa): sa created, (sa) sa_dest= 14.38.69.71,
sa_prot= 50, sa_spi= 0x59997B2D(1503230765), sa_trans= esp-3des esp-md5-hmac ,
sa_conn_id= 200100:08:38: ISAKMP: received ke message (7/1)00:08:38: ISAKMP: DPD received kei
with flags 0x1000:08:38: ISAKMP: Locking DPD struct 0x82702444 from
crypto_ikmp_dpd_handle_kei_mess, count 2
```

[Informações Relacionadas](#)

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