

# 配置路由器到路由器的 LAN 到 LAN 隧道，从一台路由器发起 IKE 积极模式

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[RouterA 调试输出](#)

[相关信息](#)

## 简介

Cisco IOS® 软件版本 12.2(8)T 引入了在主动模式下启动 Internet 密钥交换 (IKE) 的路由器功能。有关详细信息，请参阅 Bug 工具包中的 Bug ID [CSCdt30808](#) ( [仅限注册用户](#) )。以前路由器能回应主动模式的隧道协商请求，但它从未能启动过该请求。

## 先决条件

### 要求

本文档没有任何特定的前提条件。

### 使用的组件

本文档中的信息基于以下软件和硬件版本。

- 虽然接收路由器没有必要使用 Cisco IOS 12.2(8)T，但两个路由器都使用了它。

**注意：**此配置用 Cisco IOS 软件 12.2(13)T1 版进行了测试。配置的所有方面依然相同。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 背景信息

注意：新的命令行界面(CLI)命令如下：

- `crypto isakmp peer < address <x.x.x.x>/hostname <name> >`
- `set aggressive-mode client-endpoint < fqdn <name>|ipv4-address <x.x.x.x>/user-fqdn <name> >`
- `set aggressive-mode password <password>`

在下面的配置示例中，路由器 A 和路由器 B 之间有一个 LAN-to-LAN 隧道。RouterA 永远是启动路由器的隧道，并且在本例启动主动模式。虽然路由器 B 也能应用一个标准的 LAN 到 LAN 的隧道配置，但它只需一个动态加密映射就能从路由器 A 上接收隧道参数。

注意：在本例中，RouterB 不一定必须运行 Cisco IOS 软件版本 12.2(8)T 来接受路由器 A 的隧道参数。如上所述，路由器总是能接受主动模式请求，但它们从不曾能启动过该请求。

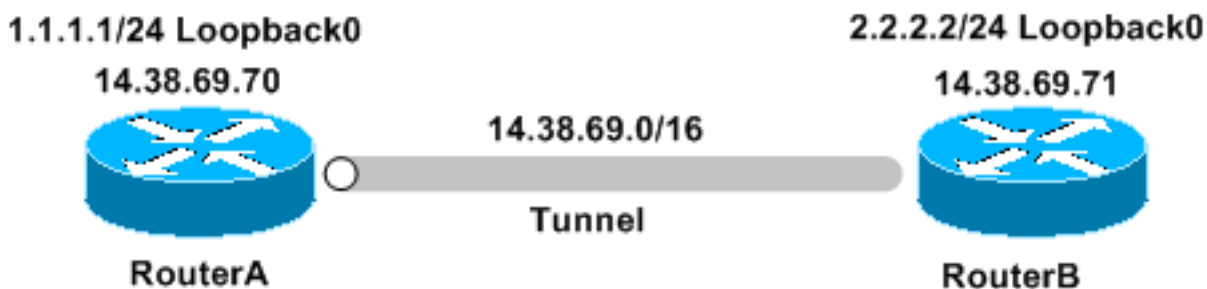
## 配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要查找本文档所用命令的其他信息，请使用 [命令查找工具](#) ( [仅限注册用户](#) )。

## 网络图

本文档使用下图所示的网络设置。



## 配置

本文档使用以下配置：

- [路由器A](#)
- [路由器B](#)

### 路由器A

```
Building configuration...
```

```
Current configuration : 1253 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto 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 classless
ip route 0.0.0.0 0.0.0.0 14.38.69.71
ip 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 0
line aux 0
line vty 0 4
  login
!
!
end
```

## 路由器B

```
Building configuration...

Current configuration : 1147 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 14.38.69.70
crypto 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 classless  
ip route 0.0.0.0 0.0.0.0 14.38.69.70  
no ip http server  
!  
!  
call rsvp-sync  
!  
!  
mgcp profile default  
!  
dial-peer cor custom  
!  
!  
line con 0  
  exec-timeout 0 0  
  speed 115200  
line aux 0  
line vty 0 4  
  login  
!  
!  
end
```

## 验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- [show crypto ipsec sa](#) - 显示第 2 阶段的安全关联。
- [show crypto isakmp sa](#) — 显示第 1 阶段安全连接。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

### 故障排除命令

**注意：** 在发出 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。
- **debug crypto engine** - 显示已加密的数据流。

### RouterA 调试输出

```
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= 0x400C
00:08:26: ISAKMP: received ke message (1/1)
00:08:26: ISAKMP: local port 500, remote port 500
00:08:26: 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       : 8
00:08:26: ISAKMP (1): Total payload length: 12
00:08:26: ISAKMP (0:1): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_AM
Old State = IKE_READY New State = IKE_I_AM1

00:08:26: ISAKMP (0:1): beginning Aggressive Mode exchange
00:08:26: 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 1
00:08:36: ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH
00:08:36: ISAKMP (0:1): sending packet to 14.38.69.71 (I) AG_INIT_EXCH
00:08:37: ISAKMP (0:1): received packet from 14.38.69.71 (I) AG_INIT_EXCH
00:08:37: ISAKMP (0:1): processing SA payload. message ID = 0
00:08:37: ISAKMP (0:1): SA using tunnel password as pre-shared key.
00:08:37: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
00:08:37: ISAKMP: encryption DES-CBC
00:08:37: ISAKMP: hash MD5
00:08:37: ISAKMP: default group 1
00:08:37: ISAKMP: auth pre-share
00:08:37: ISAKMP: life type in seconds
00:08:37: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:08:37: ISAKMP (0:1): atts are acceptable. Next payload is 0
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): vendor ID is Unity
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): vendor ID is DPD
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): speaking to another IOS box!
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): processing KE payload. message ID = 0
00:08:37: ISAKMP (0:1): processing ID payload. message ID = 0
00:08:37: ISAKMP (0:1): processing NONCE payload. message ID = 0
00:08:37: ISAKMP (0:1): SA using tunnel password as pre-shared key.
00:08:37: ISAKMP (0:1): SKEYID state generated
00:08:37: ISAKMP (0:1): processing HASH payload. message ID = 0
00:08:37: ISAKMP (0:1): SA has been authenticated with 14.38.69.71
00:08:37: ISAKMP (0:1): IKE_DPD is enabled, initializing timers
00:08:37: ISAKMP: Locking DPD struct 0x82702444
  from crypto_ikmp_dpd_ike_init, count 1
00:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old 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 message  
00:08:37: ISAKMP: received ke message (6/1)  
00:08:37: ISAKMP: received KEYENG\_IKMP\_MORE\_SAS message  
00:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM\_IDLE  
00:08:37: ISAKMP (0:1): purging node -1844394438  
00:08:37: 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 = 133381228  
00:08:37: ISAKMP (0:1): processing NOTIFY RESPONDER\_LIFETIME protocol 1  
spi 0, message ID = 133381228, sa = 82701CDC  
00:08:37: ISAKMP (0:1): processing responder lifetime  
00:08:37: ISAKMP (0:1): deleting node 133381228 error  
FALSE reason "informational (in) state 1"  
00:08:37: ISAKMP (0:1): Input = IKE\_MESG\_FROM\_PEER, IKE\_INFO\_NOTIFY  
Old 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 14.38.69.71  
00:08:38: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -1119238561  
00:08:38: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM\_IDLE  
00:08:38: ISAKMP (0:1): Node -1119238561, Input = IKE\_MESG\_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 = -1119238561  
00:08:38: ISAKMP (0:1): processing SA payload. message ID = -1119238561  
00:08:38: ISAKMP (0:1): Checking IPSec proposal 1  
00:08:38: ISAKMP: transform 1, ESP\_3DES  
00:08:38: ISAKMP: attributes in transform:  
00:08:38: ISAKMP: encaps is 1  
00:08:38: ISAKMP: SA life type in seconds  
00:08:38: ISAKMP: SA life duration (basic) of 3600  
00:08:38: ISAKMP: SA life type in kilobytes  
00:08:38: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0  
00:08:38: ISAKMP: authenticator is HMAC-MD5  
00:08:38: 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= 0x4

00:08:38: ISAKMP (0:1): processing NONCE payload. message ID = -1119238561  
00:08:38: ISAKMP (0:1): processing ID payload. message ID = -1119238561  
00:08:38: ISAKMP (0:1): processing ID payload. message ID = -1119238561  
00:08:38: ISAKMP (0:1): Creating IPSec SAs  
00:08:38: 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 4  
00:08:38: lifetime of 3600 seconds  
00:08:38: lifetime of 4608000 kilobytes  
00:08:38: 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 C  
00:08:38: lifetime of 3600 seconds  
00:08:38: lifetime of 4608000 kilobytes  
00:08:38: 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\_MESG\_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= 0x4
00:08:38: 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= 0xC
00:08:38: 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= 2000
00:08:38: 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= 2001
00:08:38: ISAKMP: received ke message (7/1)
00:08:38: ISAKMP: DPD received kei with flags 0x10
00:08:38: ISAKMP: Locking DPD struct 0x82702444 from
crypto_ikmp_dpd_handle_kei_mess, count 2
```

## [相关信息](#)

- [IPSec 支持页面](#)
- [技术支持 - Cisco Systems](#)