

# Configuring IPsec Between a Catalyst 4224 Access Gateway Switch and a Cisco IOS Router

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Exemplo de depurações](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento ilustra a configuração de exemplo do IPsec entre um Switch do gateway de acesso Cisco Catalyst 4224 e um roteador Cisco que execute o software de Cisco IOS®. A criptografia é feita entre o VLAN1 do gateway de acesso (onde o crypto map é aplicado) e a relação do FastEthernet0/1 do roteador.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

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

- Cisco IOS Software Release 12.(1)14
- Software 12.2(2)YC1 IO c4224

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](#).

## 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 seguinte configuração de rede:



## Configurações

Este documento utiliza as seguintes configurações:

- [Interruptor do gateway de acesso do Catalyst 4224](#)
- [Cisco IOS Router](#)

### Interruptor do gateway de acesso do Catalyst 4224

```
 triana#show version
Cisco Internetwork Operating System Software
IOS (tm) c4224 Software (c4224-IK903SX3-M), Version
12.2(2)YC1,
EARLY DEPLOYMENT RELEASE SOFTWARE (fc2)

26 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
2 Channelized E1/PRI port(s)
1 Virtual Private Network (VPN) Module(s)
!--- Access gateway has onboard encryption service
adapter. 8 Voice FXS interface(s) 256K bytes of non-
volatile configuration memory. 31744K bytes of processor
board System flash (Read/Write) Configuration register
is 0x2102 triana#show run
Building configuration...

Current configuration : 5111 bytes
!
! Last configuration change at 13:56:01 UTC Wed May 29
2002
```

```
! NVRAM config last updated at 13:56:03 UTC Wed May 29
2002
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname triana
!
no logging buffered
enable password ww
!
memory-size iomem 25
!--- Create the VLANS as required. vlan 1
  name default
vlan 3
  name VLAN0003
!--- Create the VLANS as required. vlan 2
  name data
vlan 999
  name VLAN0999
!
ip subnet-zero
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
isdn switch-type primary-net5
voicecard mode toll-by-pass
!
!
!
!
!
!
!
!
!
ccm-manager mgcp
!
!--- Define Phase 1 policy. crypto isakmp policy 10
  authentication pre-share
crypto isakmp key yoursecretkey address 209.165.201.6
!
!
!--- Define Phase 2 policy. crypto ipsec transform-set
basic esp-des esp-md5-hmac
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
!--- Define Phase 2 policy (continued). !--- Define the
encryption peer and crypto map parameters. crypto map
mymap 10 ipsec-isakmp
  set peer 209.165.201.6
  set transform-set basic
  match address cryptoacl
!
!
no spanning-tree optimize bpdu transmission
no spanning-tree vlan 1
no spanning-tree vlan 2
no spanning-tree vlan 3
!
```

```
controller E1 2/0
!
controller E1 2/1
!
translation-rule 1
  Rule 0 ^... 1
!
translation-rule 2
  Rule 0 ^10.. 0
  Rule 1 ^11.. 1
  Rule 2 ^12.. 2
  Rule 3 ^13.. 3
  Rule 4 ^14.. 4
  Rule 5 ^15.. 5
  Rule 6 ^16.. 6
  Rule 7 ^17.. 7
  Rule 8 ^18.. 8
  Rule 9 ^19.. 9
!
translation-rule 6
  Rule 0 ^112. 119
!
translation-rule 7
  Rule 0 ^1212 1196
!
translation-rule 3
  Rule 0 ^. 0
!
translation-rule 9
  Rule 0 ^. 9
!
translation-rule 99
  Rule 0 ^90.. 0
  Rule 1 ^91.. 1
  Rule 2 ^92.. 2
  Rule 3 ^93.. 3
  Rule 4 ^94.. 4
  Rule 5 ^95.. 5
  Rule 6 ^96.. 6
  Rule 7 ^97.. 7
  Rule 8 ^98.. 8
  Rule 9 ^99.. 9
!
translation-rule 999
  Rule 0 ^2186 1196
!
translation-rule 1122
  Rule 0 ^1122 528001
  Rule 1 ^1121 519352
!
translation-rule 20
  Rule 0 ^000 500
!
!
!
interface Loopback0
  no ip address
!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface Serial1/0
```

```
no ip address
no fair-queue
!
interface Serial1/1
no ip address
!
interface FastEthernet5/0
no ip address
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
switchport voice vlan 3
spanning-tree portfast
!
!--- For the lab setup, a host is connected on this
port. interface FastEthernet5/2
no ip address
duplex auto
speed auto
!--- Place the port in VLAN 2. switchport access vlan 2
spanning-tree portfast
!
interface FastEthernet5/3
no ip address
shutdown
duplex auto
speed auto
switchport access vlan 999
spanning-tree portfast
!
interface FastEthernet5/4
no ip address
duplex auto
speed auto
switchport access vlan 2
switchport voice vlan 3
spanning-tree portfast
!
interface FastEthernet5/5
no ip address
duplex auto
speed auto
!
interface FastEthernet5/6
no ip address
duplex auto
speed auto
!
interface FastEthernet5/7
no ip address
duplex auto
speed auto
!
interface FastEthernet5/8
no ip address
duplex auto
speed auto
!
interface FastEthernet5/9
```

```
no ip address
duplex auto
speed auto
!
interface FastEthernet5/10
no ip address
duplex auto
speed auto
switchport trunk allowed vlan 1-3
switchport mode trunk
!--- By default, the port belongs to VLAN 1. interface
FastEthernet5/11
no ip address
duplex auto
speed auto
!
interface FastEthernet5/12
no ip address
duplex auto
speed auto
!
interface FastEthernet5/13
no ip address
duplex auto
speed auto
!
interface FastEthernet5/14
no ip address
duplex auto
speed auto
!
interface FastEthernet5/15
no ip address
duplex auto
speed auto
!
interface FastEthernet5/16
no ip address
duplex auto
speed auto
!
interface FastEthernet5/17
no ip address
duplex auto
speed auto
!
interface FastEthernet5/18
no ip address
duplex auto
speed auto
!
interface FastEthernet5/19
no ip address
duplex auto
speed auto
!
interface FastEthernet5/20
no ip address
duplex auto
speed auto
!
interface FastEthernet5/21
no ip address
duplex auto
```

```
speed auto
!
interface FastEthernet5/22
no ip address
duplex auto
speed auto
!
interface FastEthernet5/23
no ip address
duplex auto
speed auto
!
interface FastEthernet5/24
no ip address
duplex auto
speed auto
!
!--- Define an IP address and apply crypto map to enable
!--- IPSec processing on this interface. interface Vlan
1
ip address 209.165.201.5 255.255.255.224
crypto map mymap
!
!--- Define an IP address for VLAN 2. interface Vlan 2
ip address 192.168.10.1 255.255.255.0
!
ip classless
ip route 10.48.66.0 255.255.254.0 209.165.201.6
no ip http server
!
!
ip access-list extended cryptoacl
remark This is crypto ACL
permit ip 192.168.10.0 0.0.0.255 10.48.66.0 0.0.1.255
call rsvp-sync
!
voice-port 4/0
output attenuation 0
!
voice-port 4/1
output attenuation 0
!
voice-port 4/2
output attenuation 0
!
voice-port 4/3
output attenuation 0
!
voice-port 4/4
output attenuation 0
!
voice-port 4/5
output attenuation 0
!
voice-port 4/6
output attenuation 0
!
voice-port 4/7
output attenuation 0
!
mgcp
no mgcp timer receive-rtcp
!
mgcp profile default
```

```
!  
dial-peer cor custom  
!  
!  
!  
dial-peer voice 1 voip  
!  
dial-peer voice 2 pots  
  shutdown  
!  
!  
line con 0  
  exec-timeout 0 0  
  length 0  
line vty 0 4  
  password ww  
  login  
!  
end  
  
 triana#
```

## Cisco IOS Router

```
brussels#show run  
Building configuration...  
  
Current configuration : 1538 bytes  
!  
! Last configuration change at 17:16:19 UTC Wed May 29  
2002  
! NVRAM config last updated at 13:58:44 UTC Wed May 29  
2002  
!  
version 12.1  
no service single-slot-reload-enable  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname brussels  
!  
enable secret 5 $1$/vuT$081TvZgSFJ0xq5uTFc94u.  
!  
!  
!  
!  
!  
ip subnet-zero  
no ip domain-lookup  
!  
ip cef  
ip audit notify log  
ip audit po max-events 100  
!  
!  
!--- Define Phase 1 policy. crypto isakmp policy 10  
  authentication pre-share  
crypto isakmp key yoursecretkey address 209.165.201.5  
!  
!  
!--- Define the encryption policy for this setup. crypto  
ipsec transform-set basic esp-des esp-md5-hmac  
!  
!
```



```
!--- Define a static crypto map entry for the remote PIX
!--- with mode ipsec-isakmp. !--- This indicates that
Internet Key Exchange (IKE) !--- is used to establish
the IPSec !--- security associations for protecting the
traffic !--- specified by this crypto map entry. crypto
map vpnmap 10 ipsec-isakmp
  set peer 209.165.201.5
  set transform-set basic
  match address cryptoacl
!
!
!
!
!
!
interface FastEthernet0/0
  ip address 10.48.66.34 255.255.254.0
  no ip mroute-cache
  duplex auto
  speed auto
!
interface Serial10/0
  no ip address
  shutdown
!
!--- Enable crypto processing on the interface !---
where traffic leaves the network. interface
FastEthernet0/1
  ip address 209.165.201.6 255.255.255.224
  no ip mroute-cache
  duplex auto
  speed auto
  crypto map vpnmap
!
interface Serial10/1
  no ip address
  shutdown
!
interface Group-Async1
  no ip address
  encapsulation ppp
  async mode dedicated
  ppp authentication pap
  group-range 33 40
!
ip classless
ip route 192.168.10.0 255.255.255.0 209.165.201.5
ip http server
!
!
!--- This access list defines interesting traffic for
IPSec. ip access-list extended cryptoacl
  permit ip 10.48.66.0 0.0.1.255 192.168.10.0 0.0.0.255
!
!
line con 0
  exec-timeout 0 0
  length 0
line 33 40
  modem InOut
line aux 0
line vty 0 4
  login local
!
```

```
end
```

## Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente. A verificação de operação de IPsec é feita com **comandos debug**. Um ping estendido é tentado do roteador a um host atrás do gateway de acesso.

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

- **a mostra debuga** — Indica a corrente debugam ajustes.
- **show crypto isakmp sa** — Exibe todas as associações de segurança atuais (SAs) de IKE em um peer.
- **mostre IPsec cripto sa** — Indica os ajustes usados por SA atuais.

## 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](#).

- **debug crypto ipsec** — Exibe eventos de IPsec.
- **debug crypto isakmp** - Exibe mensagens sobre eventos IKE.
- **debug crypto engine** — Exibe informações a partir do cripto mecanismo.

### Exemplo de depurações

Esta seção fornece o exemplo de debug para o gateway de acesso e o roteador.

- [Interruptor do gateway de acesso do Catalyst 4224](#)
- [Cisco IOS Router](#)

### Interruptor do gateway de acesso do Catalyst 4224

```
triana#debug crypto ipsec
Crypto IPSEC debugging is on
triana#debug crypto isakmp
Crypto ISAKMP debugging is on
triana#debug crypto engine
Crypto Engine debugging is on
triana#show debug
```

```
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
```

Crypto IPSEC debugging is on  
triana#

May 29 18:01:57.746: ISAKMP (0:0): received packet from 209.165.201.6 (N) NEW SA  
May 29 18:01:57.746: ISAKMP: local port 500, remote port 500  
May 29 18:01:57.746: ISAKMP (0:1): Input = IKE\_MSG\_FROM\_PEER, IKE\_MM\_EXCH  
Old State = IKE\_READY New State = IKE\_R\_MM1  
May 29 18:01:57.746: ISAKMP (0:1): processing SA payload. message ID = 0  
May 29 18:01:57.746: ISAKMP (0:1): found peer pre-shared key  
matching 209.165.201.6

*!--- 4224 access gateway checks the attributes for Internet Security !--- Association & Key  
Management Protocol (ISAKMP) negotiation !--- against the policy it has in its local  
configuration.* May 29 18:01:57.746: ISAKMP (0:1): Checking ISAKMP transform 1 against priority  
10 policy May 29 18:01:57.746: ISAKMP: encryption DES-CBC May 29 18:01:57.746: ISAKMP: hash SHA  
May 29 18:01:57.746: ISAKMP: default group 1 May 29 18:01:57.746: ISAKMP: auth pre-share *!---  
The received attributes are acceptable !--- against the configured set of attributes.* May 29  
18:01:57.746: ISAKMP (0:1): atts are acceptable. Next payload is 0 May 29 18:01:57.746:

CryptoEngine0: generate alg parameter May 29 18:01:57.746: CryptoEngine0:  
CRYPTO\_ISA\_DH\_CREATE(hw)(ipsec) May 29 18:01:57.898: CRYPTO\_ENGINE: Dh phase 1 status: 0 May 29  
18:01:57.898: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE Old State =  
IKE\_R\_MM1 New State = IKE\_R\_MM1 May 29 18:01:57.898: ISAKMP (0:1): SA is doing pre-shared key  
authentication using id type ID\_IPV4\_ADDR May 29 18:01:57.898: ISAKMP (0:1): sending packet to  
209.165.201.6 (R) MM\_SA\_SETUP May 29 18:01:57.898: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL,  
IKE\_PROCESS\_COMPLETE Old State = IKE\_R\_MM1 New State = IKE\_R\_MM2 May 29 18:01:58.094: ISAKMP  
(0:1): received packet from 209.165.201.6 (R) MM\_SA\_SETUP May 29 18:01:58.094: ISAKMP (0:1):  
Input = IKE\_MSG\_FROM\_PEER, IKE\_MM\_EXCH Old State = IKE\_R\_MM2 New State = IKE\_R\_MM3 May 29  
18:01:58.098: ISAKMP (0:1): processing KE payload. message ID = 0 May 29 18:01:58.098:  
CryptoEngine0: generate alg parameter May 29 18:01:58.098: CryptoEngine0:  
CRYPTO\_ISA\_DH\_SHARE\_SECRET(hw)(ipsec) May 29 18:01:58.246: ISAKMP (0:1): processing NONCE  
payload. message ID = 0 May 29 18:01:58.246: ISAKMP (0:1): found peer pre-shared key matching  
209.165.201.6 May 29 18:01:58.250: CryptoEngine0: create ISAKMP SKEYID for conn id 1 May 29  
18:01:58.250: CryptoEngine0: CRYPTO\_ISA\_SA\_CREATE(hw)(ipsec) **May 29 18:01:58.250: ISAKMP (0:1):**

**SKEYID state generated**

May 29 18:01:58.250: ISAKMP (0:1): processing vendor id payload  
May 29 18:01:58.250: ISAKMP (0:1): speaking to another IOS box!  
May 29 18:01:58.250: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
Old State = IKE\_R\_MM3 New State = IKE\_R\_MM3

May 29 18:01:58.250: ISAKMP (0:1): sending packet to 209.165.201.6 (R) MM\_KEY\_EXCH  
May 29 18:01:58.250: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_COMPLETE  
Old State = IKE\_R\_MM3 New State = IKE\_R\_MM4

May 29 18:01:58.490: ISAKMP (0:1): received packet from 209.165.201.6  
(R) MM\_KEY\_EXCH

May 29 18:01:58.490: CryptoEngine0: CRYPTO\_ISA\_IKE\_DECRYPT(hw)(ipsec)  
May 29 18:01:58.490: ISAKMP (0:1): Input = IKE\_MSG\_FROM\_PEER, IKE\_MM\_EXCH  
Old State = IKE\_R\_MM4 New State = IKE\_R\_MM5

May 29 18:01:58.490: ISAKMP (0:1): processing ID payload. message ID = 0  
May 29 18:01:58.490: ISAKMP (0:1): processing HASH payload. message ID = 0  
May 29 18:01:58.490: CryptoEngine0: generate hmac context for conn id 1  
May 29 18:01:58.490: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)

**May 29 18:01:58.490: ISAKMP (0:1): SA has been authenticated with 209.165.201.6**

*!--- Phase 1 authentication is successful and the SA is authenticated.* May 29 18:01:58.494:  
ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE Old State = IKE\_R\_MM5 New State =  
IKE\_R\_MM5 May 29 18:01:58.494: ISAKMP (1): ID payload next-payload : 8 type : 1 protocol : 17  
port : 500 length : 8 May 29 18:01:58.494: ISAKMP (1): Total payload length: 12 May 29  
18:01:58.494: CryptoEngine0: generate hmac context for conn id 1 May 29 18:01:58.494:  
CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec) May 29 18:01:58.494: CryptoEngine0: clear dh  
number for conn id 1 May 29 18:01:58.494: CryptoEngine0: CRYPTO\_ISA\_DH\_DELETE(hw)(ipsec) May 29  
18:01:58.494: CryptoEngine0: CRYPTO\_ISA\_IKE\_ENCRYPT(hw)(ipsec) May 29 18:01:58.494: ISAKMP  
(0:1): sending packet to 209.165.201.6 (R) QM\_IDLE May 29 18:01:58.498: ISAKMP (0:1): Input =  
IKE\_MSG\_INTERNAL, IKE\_PROCESS\_COMPLETE Old State = IKE\_R\_MM5 New State = IKE\_P1\_COMPLETE May 29  
18:01:58.518: ISAKMP (0:1): received packet from 209.165.201.6 (R) QM\_IDLE May 29 18:01:58.518:  
CryptoEngine0: CRYPTO\_ISA\_IKE\_DECRYPT(hw)(ipsec) May 29 18:01:58.518: CryptoEngine0: generate

hmac context for conn id 1 May 29 18:01:58.518: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
May 29 18:01:58.522: ISAKMP (0:1): processing HASH payload. message ID = -1809462101 May 29  
18:01:58.522: ISAKMP (0:1): processing SA payload. message ID = -1809462101 May 29 18:01:58.522:  
ISAKMP (0:1): Checking IPsec proposal 1 May 29 18:01:58.522: ISAKMP: transform 1, ESP\_DES May 29  
18:01:58.522: ISAKMP: attributes in transform: May 29 18:01:58.522: ISAKMP: encaps is 1 May 29  
18:01:58.522: ISAKMP: SA life type in seconds May 29 18:01:58.522: ISAKMP: SA life duration  
(basic) of 3600 May 29 18:01:58.522: ISAKMP: SA life type in kilobytes May 29 18:01:58.522:  
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 May 29 18:01:58.522: ISAKMP: authenticator  
is HMAC-MD5 May 29 18:01:58.522: validate proposal 0 **May 29 18:01:58.522: ISAKMP (0:1): atts are  
acceptable.**

May 29 18:01:58.522: IPSEC(validate\_proposal\_request): proposal part #1,  
*!--- After the attributes are negotiated, !--- IKE asks IPsec to validate the proposal.* (key  
eng. msg.) dest= 209.165.201.5, src= 209.165.201.6, dest\_proxy= 192.168.10.0/255.255.255.0/0/0  
(type=4), src\_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4), protocol= ESP, transform= esp-des  
esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4 *!--- spi is  
still zero because SAs have not been set.* May 29 18:01:58.522: validate proposal request 0 May  
29 18:01:58.522: ISAKMP (0:1): processing NONCE payload. message ID = -1809462101 May 29  
18:01:58.522: ISAKMP (0:1): processing ID payload. message ID = -1809462101 May 29 18:01:58.522:  
ISAKMP (1): ID\_IPV4\_ADDR\_SUBNET src 10.48.66.0/255.255.254.0 prot 0 port 0 May 29 18:01:58.522:  
ISAKMP (0:1): processing ID payload. message ID = -1809462101 May 29 18:01:58.522: ISAKMP (1):  
ID\_IPV4\_ADDR\_SUBNET dst 192.168.10.0/255.255.255.0 prot 0 port 0 May 29 18:01:58.522: ISAKMP  
(0:1): asking for 1 spis from ipsec May 29 18:01:58.522: ISAKMP (0:1): Node -1809462101, Input =  
IKE\_MSG\_FROM\_PEER, IKE\_QM\_EXCH Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE May 29  
18:01:58.526: IPSEC(key\_engine): got a queue event... May 29 18:01:58.526: IPSEC(spi\_response):  
getting spi 3384026087 for SA from 209.165.201.6 to 209.165.201.5 for prot 3 May 29  
18:01:58.526: ISAKMP: received ke message (2/1) May 29 18:01:58.774: CryptoEngine0: generate  
hmac context for conn id 1 May 29 18:01:58.774: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
May 29 18:01:58.774: CryptoEngine0: CRYPTO\_ISA\_IKE\_ENCRYPT(hw)(ipsec) May 29 18:01:58.774:  
ISAKMP (0:1): sending packet to 209.165.201.6 (R) QM\_IDLE May 29 18:01:58.774: ISAKMP (0:1):  
Node -1809462101, Input = IKE\_MSG\_FROM\_IPSEC, IKE\_SPI\_REPLY Old State = IKE\_QM\_SPI\_STARVE New  
State = IKE\_QM\_R\_QM2 May 29 18:01:58.830: ISAKMP (0:1): received packet from 209.165.201.6 (R)  
QM\_IDLE May 29 18:01:58.830: CryptoEngine0: CRYPTO\_ISA\_IKE\_DECRYPT(hw)(ipsec) May 29  
18:01:58.834: CryptoEngine0: generate hmac context for conn id 1 May 29 18:01:58.834:  
CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec) May 29 18:01:58.834: ipsec allocate flow 0 May 29  
18:01:58.834: ipsec allocate flow 0 May 29 18:01:58.834: CryptoEngine0:  
CRYPTO\_ISA\_IPSEC\_KEY\_CREATE(hw)(ipsec) May 29 18:01:58.834: CryptoEngine0:  
CRYPTO\_ISA\_IPSEC\_KEY\_CREATE(hw)(ipsec) **May 29 18:01:58.838: ISAKMP (0:1): Creating IPsec SAs**

May 29 18:01:58.838: inbound SA from 209.165.201.6 to 209.165.201.5  
(proxy 10.48.66.0 to 192.168.10.0)  
May 29 18:01:58.838: has spi 0xC9B423E7 and conn\_id 50 and flags 4  
May 29 18:01:58.838: lifetime of 3600 seconds  
May 29 18:01:58.838: lifetime of 4608000 kilobytes  
May 29 18:01:58.838: outbound SA from 209.165.201.5 to 209.165.201.6  
(proxy 192.168.10.0 to 10.48.66.0)  
May 29 18:01:58.838: has spi 561973207 and conn\_id 51 and flags 4  
May 29 18:01:58.838: lifetime of 3600 seconds  
May 29 18:01:58.838: lifetime of 4608000 kilobytes  
May 29 18:01:58.838: ISAKMP (0:1): deleting node -1809462101 error FALSE reason  
"quick mode done (await())"  
May 29 18:01:58.838: ISAKMP (0:1): Node -1809462101, Input = IKE\_MSG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_R\_QM2 New State = IKE\_QM\_PHASE2\_COMPLETE

May 29 18:01:58.838: IPSEC(key\_engine): got a queue event...  
May 29 18:01:58.838: IPSEC(initialize\_sas): ,  
(key eng. msg.) dest= 209.165.201.5, src= 209.165.201.6,  
dest\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),  
src\_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4),  
protocol= ESP, transform= esp-des esp-md5-hmac ,  
lifedur= 3600s and 4608000kb,  
spi= 0xC9B423E7(3384026087), conn\_id= 50, keysize= 0, flags= 0x4  
*!--- IPsec SAs are now initialized and encrypted !--- communication can now take place.* May 29  
18:01:58.838: IPSEC(initialize\_sas): , (key eng. msg.) src= 209.165.201.5, dest= 209.165.201.6,  
src\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), dest\_proxy= 10.48.66.0/255.255.254.0/0/0

```
(type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi=
0x217F07D7(561973207), conn_id= 51, keysize= 0, flags= 0x4 !--- IPsec SAs are now initialized
and encrypted !--- communication can now take place. May 29 18:01:58.838: IPSEC(create_sa): sa
created, (sa) sa_dest= 209.165.201.5, sa_prot= 50, sa_spi= 0xC9B423E7(3384026087), sa_trans=
esp-des esp-md5-hmac , sa_conn_id= 50 May 29 18:01:58.838: IPSEC(create_sa): sa created, (sa)
sa_dest= 209.165.201.6, sa_prot= 50, sa_spi= 0x217F07D7(561973207), sa_trans= esp-des esp-md5-
hmac , sa_conn_id= 51 !--- Observe that two IPsec SAs are created. !--- Recollect that IPsec SAs
are bidirectional. triana# triana# triana# triana#show crypto isakmp sa
```

```
dst          src          state          conn-id  slot
209.165.201.5  209.165.201.6  QM_IDLE          &n bsp;  1      0
```

```
triana#show crypto ipsec sa
```

```
interface: Vlan 1
```

```
  Crypto map tag: mymap, local addr. 209.165.201.5
```

```
local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.48.66.0/255.255.254.0/0/0)
```

```
current_peer: 209.165.201.6
```

```
  PERMIT, flags={origin_is_acl,}
```

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

```
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

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

```
  #send errors 0, #recv errors 0
```

```
local crypto endpt.: 209.165.201.5, remote crypto endpt.: 209.165.201.6
```

```
path mtu 1500, media mtu 1500
```

```
current outbound spi: 217F07D7
```

```
inbound esp sas:
```

```
  spi: 0xC9B423E7(3384026087)
```

```
  transform: esp-des esp-md5-hmac ,
```

```
  in use settings = {Tunnel, }
```

```
  slot: 0, conn id: 50, flow_id: 1, crypto map: mymap
```

```
  sa timing: remaining key lifetime (k/sec): (4607998/3536)
```

```
  IV size: 8 bytes
```

```
  replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
  spi: 0x217F07D7(561973207)
```

```
  transform: esp-des esp-md5-hmac ,
```

```
  in use settings = {Tunnel, }
```

```
  slot: 0, conn id: 51, flow_id: 2, crypto map: mymap
```

```
  sa timing: remaining key lifetime (k/sec): (4607999/3536)
```

```
  IV size: 8 bytes
```

```
  replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
triana#
```

```
Cisco IOS Router
```

```
brussels#show debug
```

```
Cryptographic Subsystem:
```

```
  Crypto ISAKMP debugging is on
```

```

Crypto Engine debugging is on
Crypto IPSEC debugging is on
brussels#p
Protocol [ip]:
Target IP address: 192.168.10.5
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: fastethernet0/0
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.5, timeout is 2 seconds:

May 29 18:01:54.285: IPSEC(sa_request): ,
  (key eng. msg.) src= 209.165.201.6, dest= 209.165.201.5,
  src_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4),
  dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0x217F07D7(561973207), conn_id= 0, keysize= 0, flags= 0x4004
May 29 18:01:54.285: ISAKMP: received ke message (1/1)
May 29 18:01:54.285: ISAKMP: local port 500, remote port 500
May 29 18:01:54.289: ISAKMP (0:1): beginning Main Mode exchange
May 29 18:01:54.289: ISAKMP (1): sending packet to 209.165.201.5 (I) MM_NO_STATE
May 29 18:01:54.461: ISAKMP (1): received packet from 209.165.201.5 (I) MM_NO_STATE
May 29 18:01:54.461: ISAKMP (0:1): processing SA payload. message ID = 0
May 29 18:01:54.461: ISAKMP (0:1): Checking ISAKMP transform 1
  against priority 10 policy
May 29 18:01:54.465: ISAKMP:      encryption DES-CBC
May 29 18:01:54.465: ISAKMP:      hash SHA
May 29 18:01:54.465: ISAKMP:      default group 1
May 29 18:01:54.465: ISAKMP:      auth pre-share
May 29 18:01:54.465: ISAKMP (0:1): atts are acceptable. Next payload is 0
May 29 18:01:54.465: CryptoEngine0: generate alg parameter
May 29 18:01:54.637: CRYPTO_ENGINE: Dh phase 1 status: 0
May 29 18:01:54.637: CRYPTO_ENGINE: Dh phase 1 status: 0
May 29 18:01:54.637: ISAKMP (0:1): SA is doing pre-shared key authentication
May 29 18:01:54.637: ISAKMP (1): SA is doing pre-shared key authentication using
  id type ID_IPV4_ADDR
May 29 18:01:54.641: ISAKMP (1): sending packet to 209.165.201.5 (I) MM_SA_SETUP
May 29 18:01:54.805: ISAKMP (1): received packet from 209.165.201.5 (I) MM_SA_SETUP
May 29 18:01:54.805: ISAKMP (0:1): processing KE payload. message ID = 0
May 29 18:01:54.805: CryptoEngine0: generate alg parameter
May 29 18:01:55.021: ISAKMP (0:1): processing NONCE payload. messa!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/21/24 ms
brussels#ge ID = 0
May 29 18:01:55.021: CryptoEngine0: create ISAKMP SKEYID for conn id 1
May 29 18:01:55.025: ISAKMP (0:1): SKEYID state generated
May 29 18:01:55.029: ISAKMP (0:1): processing vendor id payload
May 29 18:01:55.029: ISAKMP (0:1): speaking to another IOS box!
May 29 18:01:55.029: ISAKMP (1): ID payload
  next-payload : 8
  type          : 1
  protocol      : 17
  port          : 500
  length        : 8
May 29 18:01:55.029: ISAKMP (1): Total payload length: 12
May 29 18:01:55.029: CryptoEngine0: generate hmac context for conn id 1

```



```

May 29 18:01:55.033: ISAKMP (1): sending packet to 209.165.201.5 (I) MM_KEY_EXCH
May 29 18:01:55.049: ISAKMP (1): received packet from 209.165.201.5 (I) MM_KEY_EXCH
May 29 18:01:55.053: ISAKMP (0:1): processing ID payload. message ID = 0
May 29 18:01:55.053: ISAKMP (0:1): processing HASH payload. message ID = 0
May 29 18:01:55.053: CryptoEngine0: generate hmac context for conn id 1
May 29 18:01:55.057: ISAKMP (0:1): SA has been authenticated with 209.165.201.5
!--- Phase 1 is completed and Phase 2 starts now. May 29 18:01:55.057: ISAKMP (0:1): beginning
Quick Mode exchange, M-ID of -1809462101 May 29 18:01:55.061: CryptoEngine0: generate hmac
context for conn id 1 May 29 18:01:55.065: ISAKMP (1): sending packet to 209.165.201.5 (I)
QM_IDLE May 29 18:01:55.065: CryptoEngine0: clear dh number for conn id 1 May 29 18:01:55.337:
ISAKMP (1): received packet from 209.165.201.5 (I) QM_IDLE May 29 18:01:55.341: CryptoEngine0:
generate hmac context for conn id 1 May 29 18:01:55.345: ISAKMP (0:1): processing SA payload.
message ID = -1809462101 May 29 18:01:55.345: ISAKMP (0:1): Checking IPsec proposal 1 May 29
18:01:55.345: ISAKMP: transform 1, ESP_DES May 29 18:01:55.345: ISAKMP: attributes in transform:
May 29 18:01:55.345: ISAKMP: encaps is 1 May 29 18:01:55.345: ISAKMP: SA life type in seconds
May 29 18:01:55.345: ISAKMP: SA life duration (basic) of 3600 May 29 18:01:55.345: ISAKMP: SA
life type in kilobytes May 29 18:01:55.345: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
May 29 18:01:55.349: ISAKMP: authenticator is HMAC-MD5 May 29 18:01:55.349: validate proposal 0
May 29 18:01:55.349: ISAKMP (0:1): atts are acceptable.
May 29 18:01:55.349: IPSEC(validate_proposal_request): proposal part #1,
!--- After negotiating the attributes, IKE asks IPsec to !--- validate the proposal. (key eng.
msg.) dest= 209.165.201.5, src= 209.165.201.6, dest_proxy= 192.168.10.0/255.255.255.0/0/0
(type=4), src_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4), protocol= ESP, transform= esp-des
esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 !--- spi is
still zero because SAs have not been set. May 29 18:01:55.353: validate proposal request 0 May
29 18:01:55.357: ISAKMP (0:1): processing NONCE payload. message ID = -1809462101 May 29
18:01:55.357: ISAKMP (0:1): processing ID payload. message ID = -1809462101 May 29 18:01:55.357:
ISAKMP (0:1): processing ID payload. message ID = -1809462101 May 29 18:01:55.357:
CryptoEngine0: generate hmac context for conn id 1 May 29 18:01:55.361: ipsec allocate flow 0
May 29 18:01:55.361: ipsec allocate flow 0 May 29 18:01:55.369: ISAKMP (0:1): Creating IPsec SAs
May 29 18:01:55.369: inbound SA from 209.165.201.5 to 209.165.201.6
(proxy 192.168.10.0 to 10.48.66.0)
May 29 18:01:55.369: has spi 561973207 and conn_id 2000 and flags 4
May 29 18:01:55.373: lifetime of 3600 seconds
May 29 18:01:55.373: lifetime of 4608000 kilobytes
May 29 18:01:55.373: outbound SA from 209.165.201.6 to 209.165.201.5
(proxy 10.48.66.0 to 192.168.10.0)
May 29 18:01:55.373: has spi -910941209 and conn_id 2001 and flags 4
May 29 18:01:55.373: lifetime of 3600 seconds
May 29 18:01:55.373: lifetime of 4608000 kilobytes
May 29 18:01:55.377: ISAKMP (1): sending packet to 209.165.201.5 (I) QM_IDLE
May 29 18:01:55.377: ISAKMP (0:1): deleting node -1809462101 error FALSE reason ""
May 29 18:01:55.381: IPSEC(key_engine): got a queue event...
May 29 18:01:55.381: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 209.165.201.6, src= 209.165.201.5,
dest_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4),
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x217F07D7(561973207), conn_id= 2000, keysize= 0, flags= 0x4
!--- IPsec SAs are now initialized and encrypted !--- communication can now take place. May 29
18:01:55.381: IPSEC(initialize_sas): , (key eng. msg.) src= 209.165.201.6, dest= 209.165.201.5,
src_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4), dest_proxy= 192.168.10.0/255.255.255.0/0/0
(type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi=
0xC9B423E7(3384026087), conn_id= 2001, keysize= 0, flags= 0x4 !--- IPsec SAs are now initialized
and encrypted !--- communication can now take place. May 29 18:01:55.385: IPSEC(create_sa): sa
created, (sa) sa_dest= 209.165.201.6, sa_prot= 50, sa_spi= 0x217F07D7(561973207), sa_trans= esp-
des esp-md5-hmac , sa_conn_id= 2000 May 29 18:01:55.385: IPSEC(create_sa): sa created, (sa)
sa_dest= 209.165.201.5, sa_prot= 50, sa_spi= 0xC9B423E7(3384026087), sa_trans= esp-des esp-md5-
hmac , sa_conn_id= 2001 !--- Observe that two IPsec SAs are created. !--- Recollect that IPsec
SAs are bidirectional. brussels# brussels#show crypto isakmp sa
dst src state conn-id slot
209.165.201.5 209.165.201.6 QM_IDLE 1 0

```

```
brussels#show crypto ipsec sa
```

```
interface: FastEthernet0/1
```

```
  Crypto map tag: vpnmap, local addr. 209.165.201.6
```

```
local ident (addr/mask/prot/port): (10.48.66.0/255.255.254.0/0/0)
```

```
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
```

```
current_peer: 209.165.201.5
```

```
  PERMIT, flags={origin_is_acl,}
```

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

```
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

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

```
  #send errors 1, #recv errors 0
```

```
local crypto endpt.: 209.165.201.6, remote crypto endpt.: 209.165.201.5
```

```
path mtu 1500, media mtu 1500
```

```
current outbound spi: C9B423E7
```

```
inbound esp sas:
```

```
  spi: 0x217F07D7(561973207)
```

```
  transform: esp-des esp-md5-hmac ,
```

```
  in use settings = {Tunnel, }
```

```
  slot: 0, conn id: 2000, flow_id: 1, crypto map: vpnmap
```

```
  sa timing: remaining key lifetime (k/sec): (4607998/3560)
```

```
  IV size: 8 bytes
```

```
  replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
  spi: 0xC9B423E7(3384026087)
```

```
  transform: esp-des esp-md5-hmac ,
```

```
  in use settings = {Tunnel, }
```

```
  slot: 0, conn id: 2001, flow_id: 2, crypto map: vpnmap
```

```
  sa timing: remaining key lifetime (k/sec): (4607999/3560)
```

```
  IV size: 8 bytes
```

```
  replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
brussels#
```

## [Informações Relacionadas](#)

- [Página de suporte do IPSec](#)
- [Uma introdução ao IPsec](#)
- [Suporte Técnico - Cisco Systems](#)