

# Configurazione di IPSec da IOS a IOS con crittografia AES

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene fornita una configurazione di esempio per un tunnel IPSec da IOS a IOS con crittografia AES (Advanced Encryption Standard).

## Prerequisiti

### Requisiti

Il supporto della crittografia AES è stato introdotto in Cisco IOS® versione 12.2(13)T.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS Software Release 12.3(10)
- Cisco 1721 router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

## Configurazioni

Nel documento vengono usate le configurazioni mostrate di seguito.

- [Router 1721-A](#)
- [Router 1721-B](#)

### Router 1721-A

```
<#root>
R-1721-A#
show run
Building configuration...

Current configuration : 1706 bytes
!
! Last configuration change at 00:46:32 UTC Fri Sep 10 2004
! NVRAM config last updated at 00:45:48 UTC Fri Sep 10 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-1721-A
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
```

```
ip cef
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!

!--- Define Internet Key Exchange (IKE) policy.

crypto isakmp policy 10

!--- Specify the 256-bit AES as the !--- encryption algorithm within an IKE policy.

encr aes 256

!--- Specify that pre-shared key authentication is used.

authentication pre-share

!--- Specify the shared secret.

crypto isakmp key cisco123 address 10.48.66.146
!
!

!--- Define the IPSec transform set.

crypto ipsec transform-set aasset esp-aes 256 esp-sha-hmac

!

!--- Define crypto map entry name "aesmap" that will use !--- IKE to establish the security association.

crypto map aesmap 10 ipsec-isakmp

!--- Specify remote IPSec peer.

set peer 10.48.66.146

!--- Specify which transform sets !--- are allowed for this crypto map entry.
```

```
set transform-set aeset
```

*!--- Name the access list that determines which traffic !--- should be protected by IPsec.*

```
match address acl_vpn
```

```
!  
!  
!
```

```
interface ATM0  
no ip address  
shutdown  
no atm ilmi-keepalive  
dsl equipment-type CPE  
dsl operating-mode GSHDSL symmetric annex A  
dsl linerate AUTO
```

```
!
```

```
interface Ethernet0  
ip address 192.168.100.1 255.255.255.0  
ip nat inside  
half-duplex
```

```
!
```

```
interface FastEthernet0  
ip address 10.48.66.147 255.255.254.0  
ip nat outside  
speed auto
```

*!--- Apply crypto map to the interface.*

```
crypto map aesmap
```

```
!
```

```
ip nat inside source list acl_nat interface FastEthernet0 overload  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.48.66.1
```

```
ip route 192.168.200.0 255.255.255.0 FastEthernet0
```

```
no ip http server  
no ip http secure-server
```

```
!
```

```
ip access-list extended acl_nat
```

*!--- Exclude protected traffic from being NAT'ed.*

```
deny ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

```
permit ip 192.168.100.0 0.0.0.255 any
```

*!--- Access list that defines traffic protected by IPsec.*

```
ip access-list extended acl_vpn
  permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
!
end

R-1721-A#
```

## Router 1721-B

```
<#root>
R-1721-B#
show run
Building configuration...

Current configuration : 1492 bytes
!
! Last configuration change at 14:11:41 UTC Wed Sep 8 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-1721-B
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
```

*!--- Define IKE policy.*

```
crypto isakmp policy 10
```

*!--- Specify the 256-bit AES as the !--- encryption algorithm within an IKE policy.*

```
encr aes 256
```

*!--- Specify that pre-shared key authentication is used.*

```
authentication pre-share
```

*!--- Specify the shared secret.*

```
crypto isakmp key cisco123 address 10.48.66.147
```

```
!  
!
```

*!--- Define the IPSec transform set.*

```
crypto ipsec transform-set aasset esp-aes 256 esp-sha-hmac
```

```
!
```

*!--- Define crypto map entry name "aesmap" that uses !--- IKE to establish the SA.*

```
crypto map aesmap 10 ipsec-isakmp
```

*!--- Specify remote IPSec peer.*

```
set peer 10.48.66.147
```

*!--- Specify which transform sets !--- are allowed for this crypto map entry.*

```
set transform-set aasset
```

*!--- Name the access list that determines which traffic !--- should be protected by IPSec.*

```
match address acl_vpn
```

```
!  
!
```

```

!
interface Ethernet0
 ip address 192.168.200.1 255.255.255.0
 ip nat inside
 half-duplex
!
interface FastEthernet0
 ip address 10.48.66.146 255.255.254.0
 ip nat outside
 speed auto

!--- Apply crypto map to the interface.

crypto map aesmap

!
ip nat inside source list acl_nat interface FastEthernet0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.48.66.1

ip route 192.168.100.0 255.255.255.0 FastEthernet0

no ip http server
no ip http secure-server
!
ip access-list extended acl_nat

!--- Exclude protected traffic from being NAT'ed.

deny ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255

permit ip 192.168.200.0 0.0.0.255 any

!--- Access list that defines traffic protected by IPSec.

ip access-list extended acl_vpn
 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255

!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end

R-1721-B#

```

## Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi show sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando show.

- show crypto isakmp sa: visualizza lo stato dell'associazione di protezione Internet Security Association and Key Management Protocol (ISAKMP).

```
Router 1721-A

<#root>
R-1721-A#
show crypto isakmp sa

dst          src          state         conn-id slot
10.48.66.147 10.48.66.146 QM_IDLE      1      0
```

```
Router 1721-B

<#root>
R-1721-B#
show crypto isakmp sa

dst          src          state         conn-id slot
10.48.66.147 10.48.66.146 QM_IDLE      1      0
```

- show crypto ipsec sa: visualizza le statistiche sui tunnel attivi.

```
Router 1721-A

<#root>
R-1721-A#
show crypto ipsec sa

interface: FastEthernet0
  Crypto map tag: aesmap, local addr. 10.48.66.147

  protected vrf:

local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)

current_peer: 10.48.66.146:500
```



```
PERMIT, flags={origin_is_acl,}
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify 30
#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.: 10.48.66.147, remote crypto endpt.: 10.48.66.146
```

```
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 2EB0BA1A
```

```
inbound esp sas:
spi: 0xFECA28BC(4274661564)
```

```
transform: esp-256-aes esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: aesmap
sa timing: remaining key lifetime (k/sec): (4554237/2895)
IV size: 16 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x2EB0BA1A(783333914)
```

```
transform: esp-256-aes esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: aesmap
sa timing: remaining key lifetime (k/sec): (4554237/2894)
IV size: 16 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
R-1721-A#
```

## Router 1721-B

```
<#root>
```

```
R-1721-B#
```

```
show crypto ipsec sa
```

```

interface: FastEthernet0
  Crypto map tag: aesmap, local addr. 10.48.66.146

  protected vrf:

local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)

current_peer: 10.48.66.147:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 30, #pkts encrypt: 30, #pkts digest 30
  #pkts decaps: 30, #pkts decrypt: 30, #pkts verify 30
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 5, #recv errors 0

local crypto endpt.: 10.48.66.146, remote crypto endpt.: 10.48.66.147

  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
  current outbound spi: FECA28BC

  inbound esp sas:
    spi: 0x2EB0BA1A(783333914)

transform: esp-256-aes esp-sha-hmac ,

  in use settings ={Tunnel, }
  slot: 0, conn id: 2000, flow_id: 1, crypto map: aesmap
  sa timing: remaining key lifetime (k/sec): (4583188/2762)
  IV size: 16 bytes
  replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
    spi: 0xFECA28BC(4274661564)

transform: esp-256-aes esp-sha-hmac ,

  in use settings ={Tunnel, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: aesmap
  sa timing: remaining key lifetime (k/sec): (4583188/2761)
  IV size: 16 bytes
  replay detection support: Y

  outbound ah sas:

  outbound pcp sas:
R-1721-B#

```

- show crypto engine connections active: visualizza il totale di crittografia/decrittografia per

SA.

Router 1721-A						
<#root>						
R-1721-A#						
show crypto engine connections active						
ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0	10.48.66.147	set	HMAC_SHA+AES_256_C	0	0
2000	FastEthernet0	10.48.66.147	set	HMAC_SHA+AES_256_C	0	30
2001	FastEthernet0	10.48.66.147	set	HMAC_SHA+AES_256_C	30	0

Router 1721-B						
<#root>						
R-1721-B#						
show crypto engine connections active						
ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0	10.48.66.146	set	HMAC_SHA+AES_256_C	0	0
2000	FastEthernet0	10.48.66.146	set	HMAC_SHA+AES_256_C	0	30
2001	FastEthernet0	10.48.66.146	set	HMAC_SHA+AES_256_C	30	0

## Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

### Comandi per la risoluzione dei problemi

Nota: prima di usare i comandi di debug, consultare le [informazioni importanti sui comandi di debug](#).

- debug crypto ipsec: visualizza gli eventi IPsec.
- debug crypto isakmp: visualizza i messaggi sugli eventi IKE.
- debug crypto engine: visualizza le informazioni provenienti dal crypto engine.

Per ulteriori informazioni sulla risoluzione dei problemi relativi a IPsec, consultare il documento sulla [risoluzione dei problemi relativi alla protezione IP - descrizione e uso dei comandi di debug](#).

## Informazioni correlate

- [Software Cisco IOS release 12.2T - Advanced Encryption Standard \(AES\)](#)
- [Configurazione di IPsec Network Security](#)
- [Pagina di supporto per IPsec](#)
- [Supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).