

Come configurare il client VPN Cisco su PIX con AES

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazioni](#)

[Esempio di rete](#)

[Configurazione del PIX](#)

[Configurare il client VPN](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questa configurazione di esempio viene mostrato come configurare una connessione VPN di accesso remoto da un client VPN Cisco a un firewall PIX, utilizzando Advanced Encryption Standard (AES) per la crittografia. In questo esempio viene utilizzato Cisco Easy VPN per configurare il canale sicuro e il firewall PIX viene configurato come server Easy VPN.

Nel software Cisco Secure PIX Firewall versione 6.3 e successive, il nuovo standard di crittografia internazionale AES è supportato per proteggere le connessioni VPN da sito a sito e ad accesso remoto. Questo si aggiunge agli algoritmi di crittografia DES (Data Encryption Standard) e 3DES. Il firewall PIX supporta le dimensioni delle chiavi AES di 128, 192 e 256 bit.

Il client VPN supporta AES come algoritmo di crittografia a partire da Cisco VPN Client versione 3.6.1. Il client VPN supporta solo dimensioni della chiave di 128 bit e 256 bit.

[Prerequisiti](#)

[Requisiti](#)

In questa configurazione di esempio si presume che il PIX sia completamente operativo e configurato con i comandi necessari per gestire il traffico secondo i criteri di sicurezza dell'organizzazione.

Componenti usati

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

- Software PIX release 6.3(1)**Nota:** questa configurazione è stata testata sul software PIX versione 6.3(1) e dovrebbe funzionare su tutte le versioni successive.
- Cisco VPN Client versione 4.0.3(A)**Nota:** questa configurazione è stata testata su VPN Client versione 4.0.3(A) ma funziona sulle versioni precedenti fino alla 3.6.1 e alla versione corrente.

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

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

Premesse

Le VPN ad accesso remoto soddisfano i requisiti della forza lavoro mobile per connettersi in modo sicuro alla rete dell'organizzazione. Gli utenti mobili possono configurare una connessione protetta utilizzando il software VPN Client installato sui loro PC. Il client VPN avvia una connessione a un dispositivo del sito centrale configurato per accettare queste richieste. In questo esempio, il dispositivo del sito centrale è un firewall PIX configurato come server Easy VPN che utilizza mappe crittografiche dinamiche.

Cisco Easy VPN semplifica l'installazione delle VPN semplificando la configurazione e la gestione delle VPN. È costituito da Cisco Easy VPN Server e Cisco Easy VPN Remote. È necessaria una configurazione minima sul telecomando Easy VPN. Easy VPN Remote avvia una connessione. Se l'autenticazione ha esito positivo, Easy VPN Server esegue il push della configurazione VPN. Per ulteriori informazioni su come configurare un firewall PIX come server Easy VPN, vedere [Gestione dell'accesso remoto VPN](#).

Le mappe crittografiche dinamiche vengono utilizzate per la configurazione di IPsec quando alcuni parametri richiesti per configurare la VPN non possono essere predeterminati, come nel caso degli utenti mobili che ottengono indirizzi IP assegnati in modo dinamico. La mappa crittografica dinamica funge da modello e i parametri mancanti vengono determinati durante la negoziazione IPsec. Ulteriori informazioni sulle mappe crittografiche dinamiche sono disponibili in [Mappe crittografiche dinamiche](#).

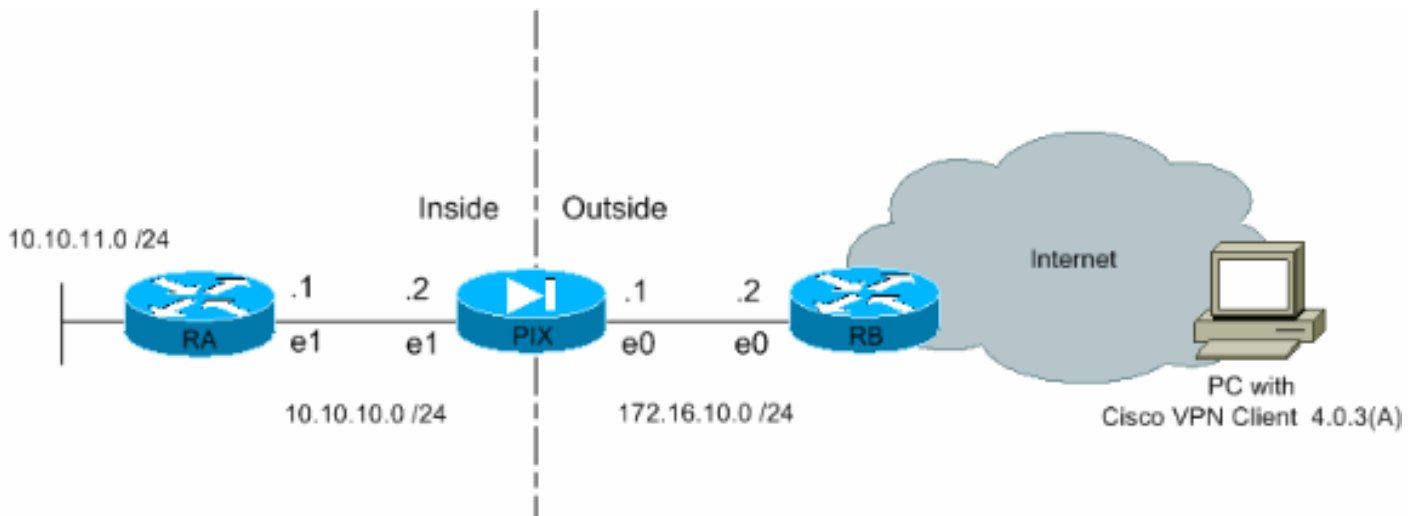
Configurazioni

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 questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione del PIX

In questo output viene mostrata la configurazione necessaria sul firewall PIX. La configurazione è solo per VPN.

PIX

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names

!--- Define the access list to enable split tunneling.
access-list 101 permit ip 10.10.10.0 255.255.255.0
10.10.8.0 255.255.255.0 access-list 101 permit ip
10.10.11.0 255.255.255.0 10.10.8.0 255.255.255.0 !---
!--- Define the access list to avoid network address !---
translation (NAT) on IPsec packets. access-list 102
permit ip 10.10.10.0 255.255.255.0 10.10.8.0
255.255.255.0 access-list 102 permit ip 10.10.11.0
```

```

255.255.255.0 10.10.8.0 255.255.255.0 pager lines 24 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 !---
Configure the IP address on the interfaces. ip address
outside 172.16.10.1 255.255.255.0 ip address inside
10.10.10.2 255.255.255.0 no ip address intf2 ip audit
info action alarm ip audit attack action alarm !---
Create a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool vpnpool1 10.10.8.1-10.10.8.254 pdm history
enable arp timeout 14400 !--- Disable NAT for IPsec
packets. nat (inside) 0 access-list 102 route outside
0.0.0.0 0.0.0.0 172.16.10.2 1 route inside 10.10.11.0
255.255.255.0 10.10.10.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h225 1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local no snmp-
server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Permit packet that came from an IPsec tunnel
to pass through without !--- checking them against the
configured conduits/access lists. sysopt connection
permit-ipsec !--- Define the transform set to be used
during IPsec !--- security association (SA) negotiation.
Specify AES as the encryption algorithm. crypto ipsec
transform-set trmset1 esp-aes-256 esp-sha-hmac !---
Create a dynamic crypto map entry !--- and add it to a
static crypto map. crypto dynamic-map map2 10 set
transform-set trmset1 crypto map map1 10 ipsec-isakmp
dynamic map2 !--- Bind the crypto map to the outside
interface. crypto map map1 interface outside !--- Enable
Internet Security Association and Key Management !---
Protocol (ISAKMP) negotiation on the interface on which
the IPsec !--- peer communicates with the PIX Firewall.
isakmp enable outside isakmp identity address !---
Define an ISAKMP policy to be used while !---
negotiating the ISAKMP SA. Specify !--- AES as the
encryption algorithm. The configurable AES !--- options
are aes, aes-192 and aes-256. !--- Note: AES 192 is not
supported by the VPN Client.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- Create a VPN group and configure the policy
attributes which are !--- downloaded to the Easy VPN
Clients. vpngroup groupmarketing address-pool vpnpool1
vpngroup groupmarketing dns-server 10.10.11.5 vpngroup
groupmarketing wins-server 10.10.11.5 vpngroup
groupmarketing default-domain org1.com vpngroup
groupmarketing split-tunnel 101 vpngroup groupmarketing
idle-time 1800 vpngroup groupmarketing password *****
telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:c064abce81996b132025e83e421ee1c3 : end

```

Nota: in questa configurazione è consigliabile non specificare aes-192 durante la configurazione del set di trasformazioni o del criterio ISAKMP. i client VPN non supportano aes-192 per la crittografia.

Nota: nelle versioni precedenti, erano richiesti i comandi di configurazione modalità IKE **isakmp client configuration address-pool** e **crypto map client-configuration address**. Tuttavia, con le versioni più recenti (3.x e successive) questi comandi non sono più necessari. È ora possibile specificare più pool di indirizzi utilizzando il comando **vpngroup address-pool**.

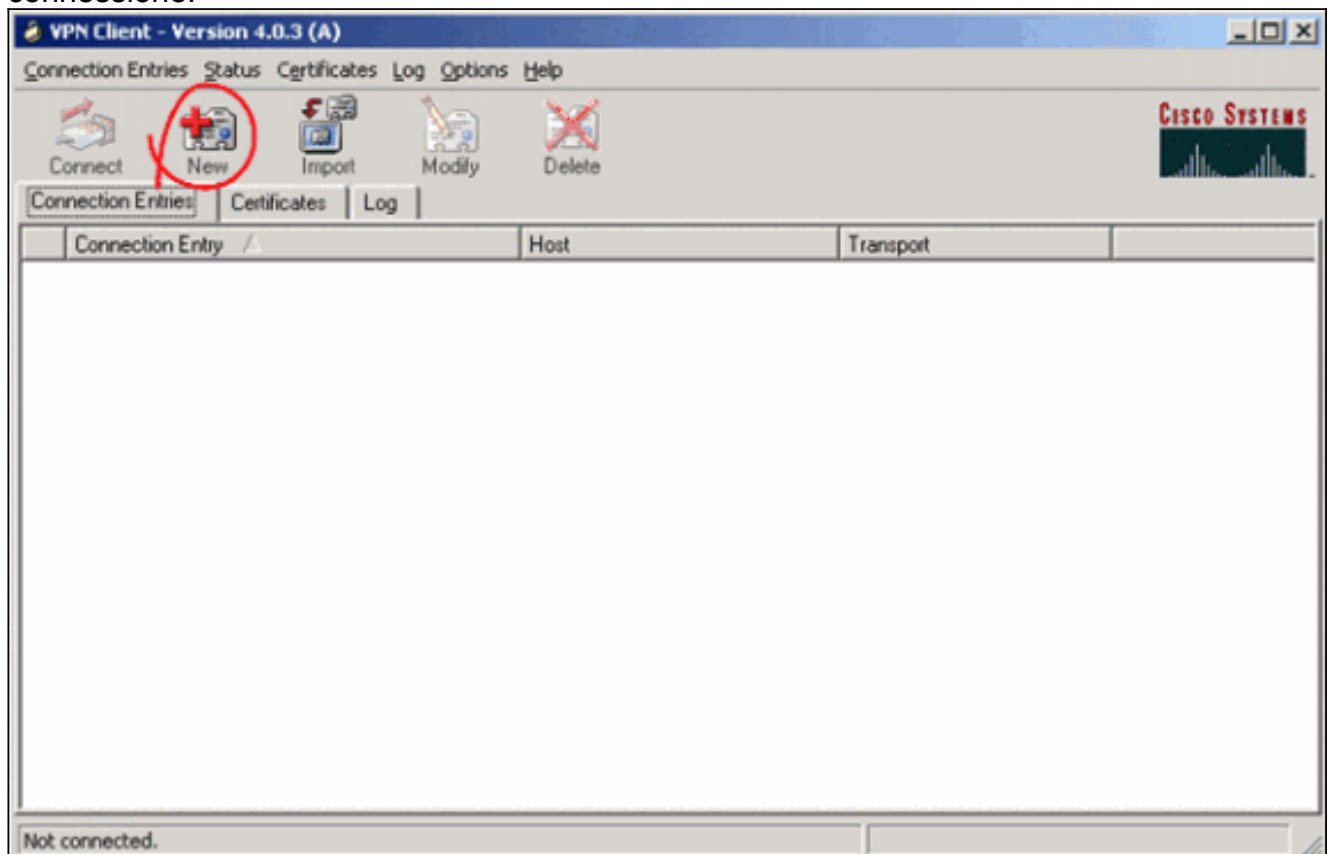
Nota: per i nomi dei gruppi VPN viene fatta distinzione tra maiuscole e minuscole. Ciò significa che l'autenticazione utente non riesce se il nome del gruppo specificato in PIX e il nome del gruppo sul client VPN sono diversi in termini di lettere maiuscole o minuscole.

Nota: ad esempio, quando si immette il nome del gruppo **GroupMarketing** in un dispositivo e **groupmarketing** in un altro dispositivo, il dispositivo non funziona.

Configurare il client VPN

Dopo aver installato il client VPN sul PC, creare una nuova connessione come mostrato nei seguenti passaggi:

1. Avviare l'applicazione VPN Client e fare clic su **Nuovo** per creare una nuova voce di connessione.



2. Nuova finestra di dialogo denominata Client VPN | Viene visualizzata la voce Crea nuova connessione VPN. Immettere le informazioni di configurazione per la nuova connessione. Nel campo Voce di connessione assegnare un nome alla nuova voce creata. Nel campo Host, digitare l'indirizzo IP dell'interfaccia pubblica del PIX. Selezionare la scheda Autenticazione e quindi digitare il nome e la password del gruppo (due volte - per la conferma). Questa operazione deve corrispondere alle informazioni immesse sul PIX utilizzando il comando **vpngroup password**. Fare clic su **Salva** per salvare le informazioni immesse. La nuova connessione è stata

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication

Name:

Password:


Confirm Password:

Certificate Authentication

Name:

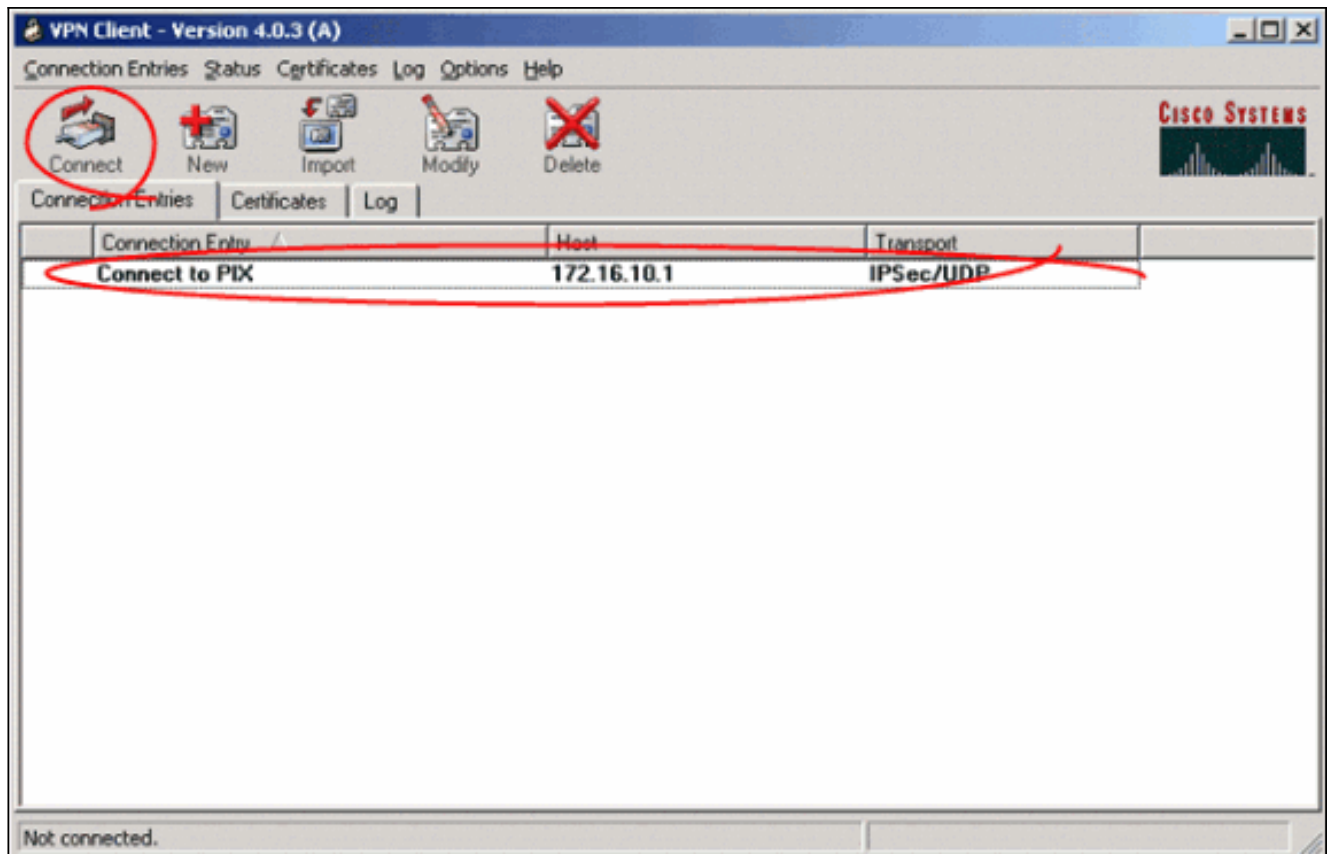
Send CA Certificate Chain

Erase User Password | Save | Cancel



creata.

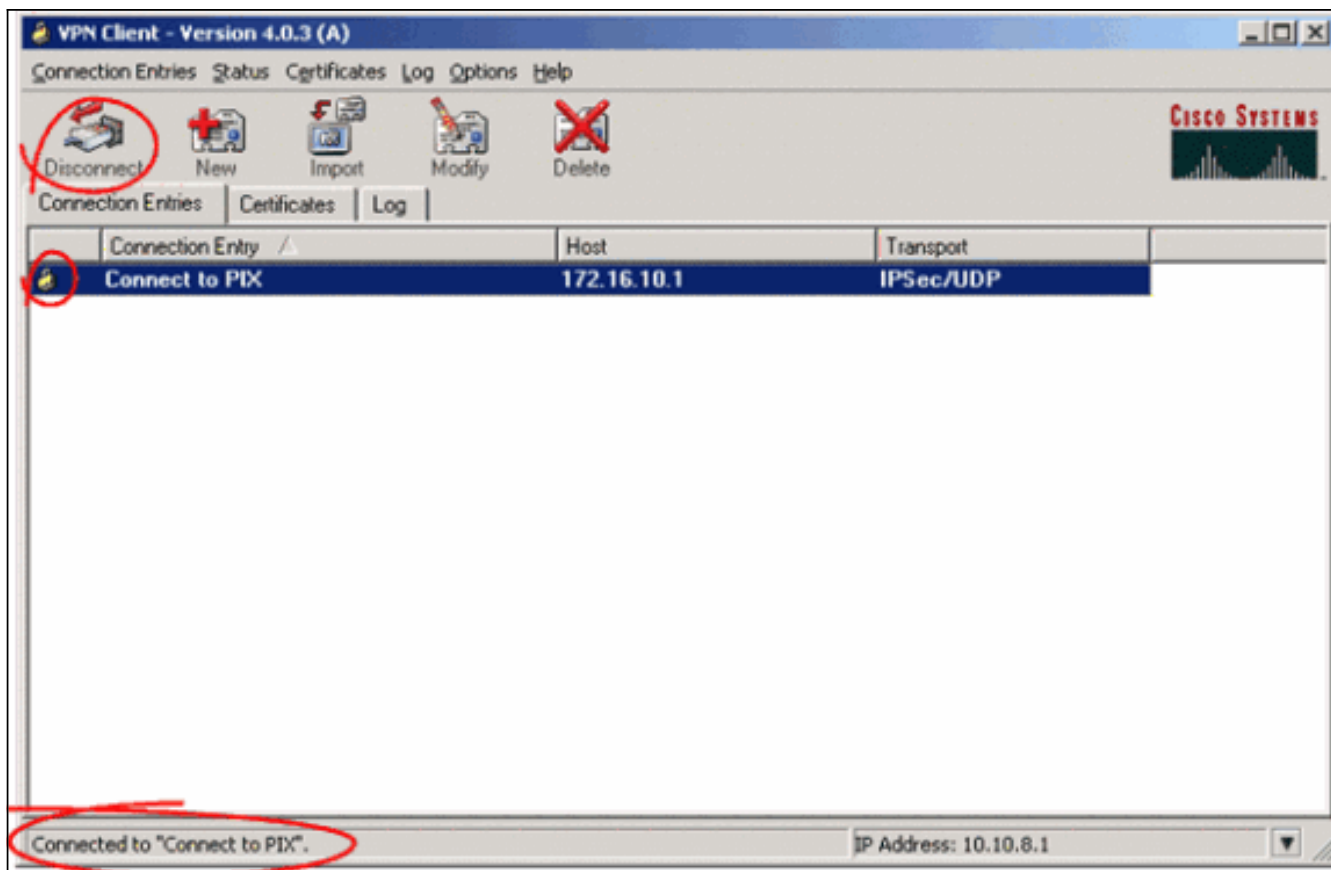
3. Per connettersi al gateway utilizzando la nuova voce di connessione, selezionare la voce di connessione facendo clic su di essa una volta e quindi fare clic sull'icona **Connetti**. Un doppio clic sulla voce di connessione produce lo stesso effetto.



Verifica

Sul client VPN, una connessione al gateway remoto stabilita correttamente è indicata dai seguenti elementi:

- Sulla voce di connessione attiva viene visualizzata un'icona gialla con un lucchetto chiuso.
- L'icona Connetti sulla barra degli strumenti (accanto alla scheda Voci di connessione) cambia in Disconnetti.
- La riga di stato alla fine della finestra mostra lo stato "Connesso a" seguito dal nome della voce di connessione.



Nota: per impostazione predefinita, una volta stabilita la connessione, il client VPN riduce a icona di blocco chiuso nella barra delle applicazioni di Windows, nell'angolo inferiore destro della barra delle applicazioni di Windows. Fare doppio clic sull'icona a forma di lucchetto chiuso per rendere nuovamente visibile la finestra del client VPN.

Sul firewall PIX, questi comandi **show** possono essere utilizzati per verificare lo stato delle connessioni stabilite.

Nota: 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 ipsec sa:** visualizza tutte le SA IPsec correnti sul PIX. Inoltre, l'output mostra l'indirizzo IP effettivo del peer remoto, l'indirizzo IP assegnato, l'indirizzo IP e l'interfaccia locali e la mappa crittografica applicata.

```
Pixfirewall#show crypto ipsec sa
```

```
interface: outside
```

```
  Crypto map tag: map1, local addr. 172.16.10.1
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.10.8.1/255.255.255.255/0/0)
```

```
current_peer: 172.16.12.3:500
```

```
dynamic allocated peer ip: 10.10.8.1
```

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

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

```
#pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25
```

```
#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.: 172.16.10.1, remote crypto endpt.: 172.16.12.3
```

```
path mtu 1500, ipsec overhead 64, media mtu 1500
```



```
current outbound spi: cbabd0ce
```

```
inbound esp sas:
```

```
spi: 0x4d8a971d(1300928285)
transform: esp-aes-256 esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: map1
sa timing: remaining key lifetime (k/sec): (4607996/28685)
IV size: 16 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0xcbabd0ce(3417034958)
transform: esp-aes-256 esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: map1
sa timing: remaining key lifetime (k/sec): (4608000/28676)
IV size: 16 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

- **show crypto isakmp sa**: visualizza lo stato della SA ISAKMP creata tra peer.

```
Pixfirewall#show crypto isakmp sa
```

```
Total      : 1
```

```
Embryonic  : 0
```

dst	src	state	pending	created
172.16.10.1	172.16.12.3	QM_IDLE	0	1

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Questi comandi di debug possono aiutare a risolvere i problemi relativi alla configurazione della VPN.

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

- **debug crypto isakmp**: visualizza l'associazione di sicurezza ISAKMP generata e gli attributi IPsec negoziati. Durante la negoziazione della SA ISAKMP, il PIX può probabilmente ignorare diverse proposte come "non accettabili" prima di accettarne una. Una volta concordata l'associazione di protezione ISAKMP, gli attributi IPsec vengono negoziati. Anche in questo caso, è possibile che diverse proposte vengano rifiutate prima di accettarne una, come mostrato nell'output del comando **debug**.

```
crypto_isakmp_process_block:src:172.16.12.3, dest:172.16.10.1 spt:500 dpt:500
OAK_AG exchange
```

```
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share (init)
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP: keylength of 256
!--- Proposal is rejected since extended auth is not configured. ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share (init)
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP: keylength of 256
!--- Proposal is rejected since MD5 is not specified as the hash algorithm. ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP: keylength of 256
!--- This proposal is accepted since it matches ISAKMP policy 10. ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
!--- Output is suppressed. OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3348522173

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: key length is 256
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
!--- This proposal is not accepted since transform-set !--- trmset1 does not use MD5. ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: key length is 256
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
!--- This proposal is accepted since it matches !--- transform-set trmset1. ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 3
!--- Output is suppressed.
```

- **debug crypto ipsec:** visualizza le informazioni sulle negoziazioni delle associazioni di protezione IPsec.

```

IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with      172.16.12.3
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
  dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
  src_proxy= 10.10.8.1/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfb0cb69(263244649) for SA
  from      172.16.12.3 to      172.16.10.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
  dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
  src_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0xfb0cb69(263244649), conn_id= 2, keysize= 256, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.10.1, dest= 172.16.12.3,
  src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
  dest_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0xda6c054a(3664512330), conn_id= 1, keysize= 256, flags= 0x4

```

Con le configurazioni mostrate in questo documento, il client VPN è in grado di connettersi correttamente al sito centrale PIX utilizzando AES. Si è talvolta osservato che, sebbene il tunnel VPN sia stato stabilito correttamente, gli utenti non sono in grado di eseguire attività comuni, ad esempio eseguire il ping delle risorse di rete, accedere al dominio o esplorare le risorse di rete. Per ulteriori informazioni sulla risoluzione di questi problemi, vedere [Risoluzione dei problemi di Risorse di rete Microsoft dopo aver stabilito un tunnel VPN con il client VPN Cisco](#).

[Informazioni correlate](#)

- [Advanced Encryption Standard \(AES\)](#)
- [Introduzione alla crittografia IP Security \(IPSec\)](#)
- [Risoluzione dei problemi di sicurezza IP - Informazioni e uso dei comandi di debug](#)
- [Pagina di supporto per la negoziazione IPsec/i protocolli IKE](#)
- [Pagina di supporto PIX](#)
- [Pagina di supporto per Cisco VPN Client](#)
- [Informazioni di riferimento sui comandi PIX](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)