Configurazione di IPSec - Chiavi precondivise con caratteri jolly con Cisco Secure VPN Client e configurazione in modalità non condivisa

Sommario

Introduzione

In questa configurazione di esempio viene illustrato un router configurato per chiavi già condivise con caratteri jolly: tutti i client PC condividono una chiave comune. Un utente remoto accede alla rete mantenendo il proprio indirizzo IP; i dati tra il PC di un utente remoto e il router sono crittografati.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Software Cisco IOS® versione 12.2.8.T1
- Cisco Secure VPN Client versione 1.0 o 1.1 - Fine del ciclo di vita
- Router Cisco con immagine DES o 3DES

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.

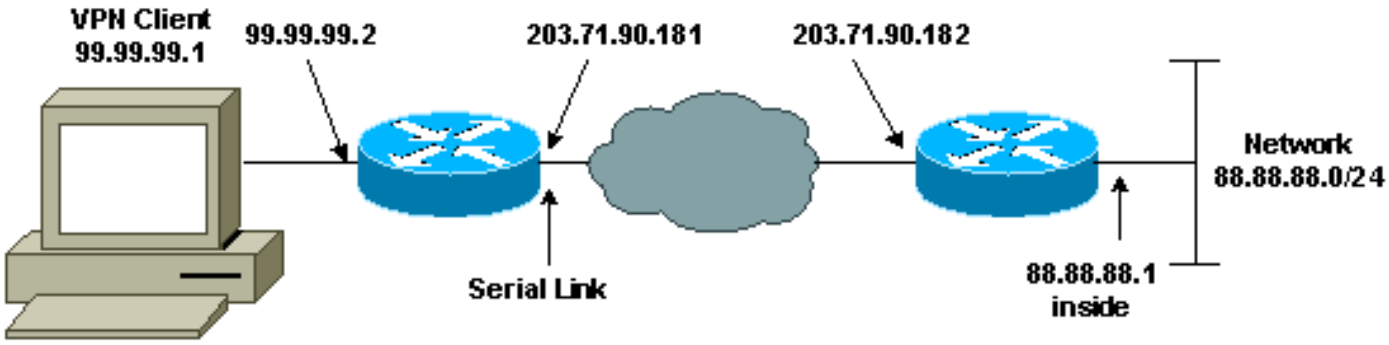
Configurazione

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).

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazioni

Questo documento utilizza le configurazioni mostrate di seguito.

- Configurazione router
- Configurazione client VPN

Configurazione router

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
```

```
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

Configurazione client VPN

```
Network Security policy:


1- Myconn
    My Identity
         Connection security: Secure
         Remote Party Identity and addressing
         ID Type: IP subnet
         88.88.88.0
         255.255.255.0
         Port all Protocol all


    Connect using secure tunnel
         ID Type: IP address
```

```
          203.71.90.182


    Authentication (Phase 1)
    Proposal 1

        Authentication method: Preshared key
        Encryp Alg: DES
        Hash Alg: MD5
        SA life:  Unspecified
        Key Group: DH 1

    Key exchange (Phase 2)
    Proposal 1
        Encapsulation ESP
        Encrypt Alg: DES
        Hash Alg: MD5
        Encap: tunnel
        SA life: Unspecified
        no AH

2- Other Connections
       Connection security: Non-secure
       Local Network Interface
         Name: Any
         IP Addr: Any
         Port: All
```

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 le associazioni di sicurezza della fase 1.
- **show crypto ipsec sa**: visualizza le associazioni di sicurezza e le informazioni sul proxy, l'incapsulamento, la crittografia, la decapsulamento e la decrittografia della fase 1.
- **show crypto engine connections active**: visualizza le connessioni correnti e le informazioni relative ai pacchetti crittografati e decrittografati.

Risoluzione dei problemi

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

Comandi per la risoluzione dei problemi

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

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Nota: è necessario cancellare le associazioni di protezione su entrambi i peer. Eseguire i comandi del router in modalità di non abilitazione.

Nota: è necessario eseguire questi debug su entrambi i peer IPSec.

- **debug crypto isakmp**: visualizza gli errori durante la fase 1.
- **debug crypto ipsec**: visualizza gli errori durante la fase 2.
- **debug crypto engine**: visualizza le informazioni provenienti dal crypto engine.
- **clear crypto isakmp**: cancella le associazioni di sicurezza della fase 1.
- **clear crypto sa**: cancella le associazioni di sicurezza della fase 2.

Informazioni correlate

- Pagina di supporto per IPSec
- Pagine di supporto client VPN 3000
- Supporto tecnico – Cisco Systems