Configurazione della configurazione della modalità router, del carattere jolly e delle chiavi già condivise, nessun NAT

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Configurazione
Esempio di rete
Configurazioni
Verifica
Risoluzione dei problemi
Informazioni correlate

Introduzione

In questa configurazione di esempio, viene configurato un router per la configurazione della modalità (ottenere un indirizzo IP dal pool), chiavi precondivise con caratteri jolly (tutti i client PC condividono una chiave comune), senza NAT (Network Address Translation). Un utente fuori sede può accedere alla rete e avere un indirizzo IP interno assegnato dal pool. Gli utenti sembrano essere all'interno della rete. I dispositivi all'interno della rete sono configurati con percorsi al pool 10.2.1.x non instradabile.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Software Cisco IOS® versione 12.0.7T o successive
- Hardware che supporta questa revisione software
- Cisco Secure VPN Client 1.0/1.0.A o 1.1 (visualizzati rispettivamente come 2.0.7/E o 2.1.12,

andare a **Guida > Informazioni** su da controllare)

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.

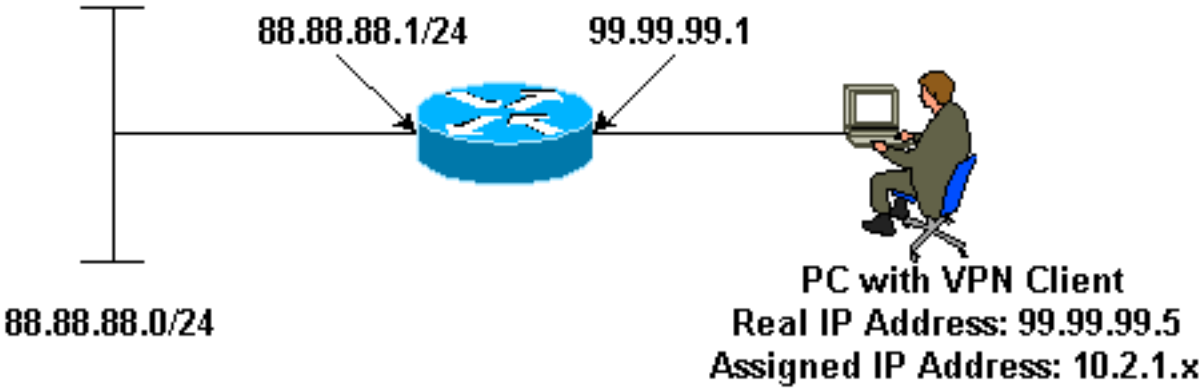
Configurazione

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

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Client VPN
- Router

Client VPN

```
Network Security policy:

1- Myconn
        My Identity = ip address
                Connection security: Secure
                Remote Party Identity and addressing
                        ID Type: IP subnet
                        88.88.88.0
```

```
                        Port all Protocol all

                Connect using secure tunnel
                        ID Type: IP address
                        99.99.99.1
                        Pre-shared key = cisco123

        Authentication (Phase 1)
        Proposal 1
                Authentication method: pre-shared 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
```

Router

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
enable password ww
!
username cisco password 0 cisco
!
clock timezone EST -5
ip subnet-zero
cns event-service server
!

crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
 set transform-set trans1
crypto map intmap client configuration address initiate
```

```
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Ethernet0

 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache

 crypto map intmap
!
interface Ethernet1
 ip address 88.88.88.1 255.255.255.0
 no ip directed-broadcast
!

ip local pool ourpool 10.2.1.1 10.2.1.254
ip classless
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

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 engine connections active**: visualizza i pacchetti crittografati e decrittografati.
- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1.

I debug devono essere in esecuzione su entrambi i router IPSec (peer). La cancellazione delle associazioni di protezione deve essere eseguita su entrambi i peer.

- **debug crypto ipsec**: visualizza le negoziazioni IPSec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP della fase 1.
- **debug crypto engine**: visualizza il traffico crittografato.
- **clear crypto isakmp**: cancella le associazioni di sicurezza correlate alla fase 1.
- **clear crypto sa**: cancella le associazioni di sicurezza correlate alla fase 2.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Supporto dei concentratori VPN serie 3000
- Supporto dei prodotti Cisco VPN 3000 Client
- Supporto della tecnologia IPSec (IP Security Protocol)
- Supporto tecnico – Cisco Systems