

Configuración de claves previamente compartidas, comodín y de configuración de modo, no NAT, del router

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

En esta configuración de muestra, configuran a un router para la configuración de modo (consiga una dirección IP del pool), comodín, las claves previamente compartidas (toda la parte de los PC cliente una clave común), sin el Network Address Translation (NAT). Usuario fuera del sitio puede ingresar la red y tener un IP Address interno asignado del pool. Para los usuarios, aparece que están dentro de la red. Los dispositivos dentro de la red se configuran con las rutas al pool del O.N.U-routable 10.2.1.x.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software 12.0.7T de Cisco IOS® o más adelante
- Hardware que soporta esta revisión del software
- CiscoSecure VPN cliente 1.0/1.0.A o 1.1 (mostrado como 2.0.7/E o 2.1.12, vaya

respectivamente al **Help (Ayuda) > About (Acerca de)** a marcar)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

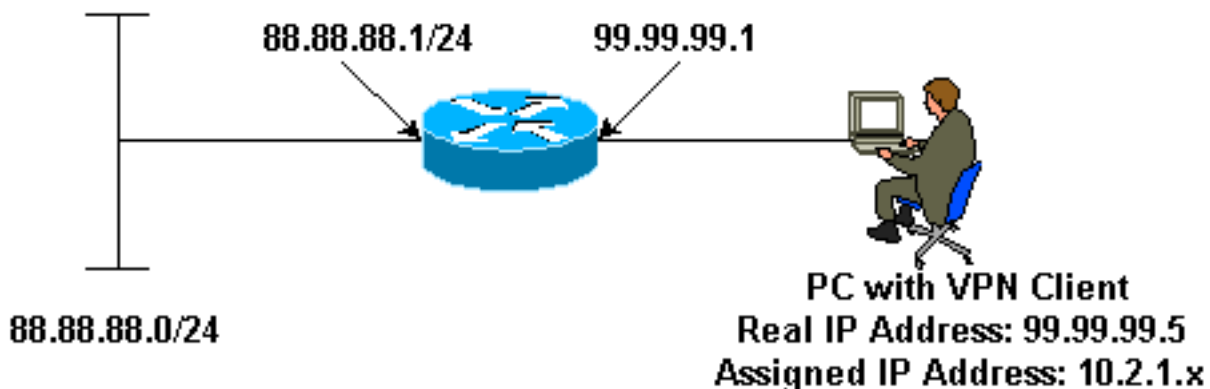
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Cliente VPN
- Router

Cliente 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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **active del show crypto engine connections** — Muestra los paquetes encriptados y desencriptados.
- **show crypto ipsec sa** - Muestra las asociaciones de seguridad de la fase 2.
- **show crypto isakmp sa** — Muestra las asociaciones de seguridad de la fase 1.

Estos debugs deben ejecutarse en ambos routers IPsec (pares). La verificación de las asociaciones de seguridad se debe realizar en ambos pares

- **depuración crypto ipsec** — Muestra los IPsec Negotiations de la Fase 2.
- **isakmp del debug crypto** — Muestra negociaciones ISAKMP de la fase 1.
- **debug crypto engine** — muestra el tráfico codificado.
- **clear crypto isakmp** — Borra las asociaciones de seguridad relacionadas con la fase 1.
- **borre el sa crypto** — Borra las asociaciones de seguridad relacionadas con la fase 2.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Soporte de productos del VPN 3000 series concentrators](#)
- [Soporte de productos del Cliente Cisco VPN 3000](#)
- [Soporte de tecnología del IPsec \(IP Security Protocol\)](#)
- [Soporte Técnico - Cisco Systems](#)