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

## Contenido



## Introducción

En esta configuración de ejemplo, se configura un router para la configuración de modo (obtenga una dirección IP del conjunto), comodín y claves previamente compartidas (todos los clientes de PC comparten una clave común), sin traducción de direcciones de red (NAT). Un usuario externo puede ingresar a la red y tener una dirección IP interna asignada desde el grupo. Para los usuarios, aparece que están dentro de la red. Los dispositivos dentro de la red se configuran con rutas al conjunto 10.2.1.x no enrutable.

## Prerequisites

### Requirements

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.

- Cisco IOS® Software 12.0.7T o posterior
- Hardware compatible con esta revisión de software
- CiscoSecure VPN Client 1.0/1.0.A o 1.1 (mostrado como 2.0.7/E o 2.1.12, respectivamente,

vaya a **Ayuda > Acerca** de verificar)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

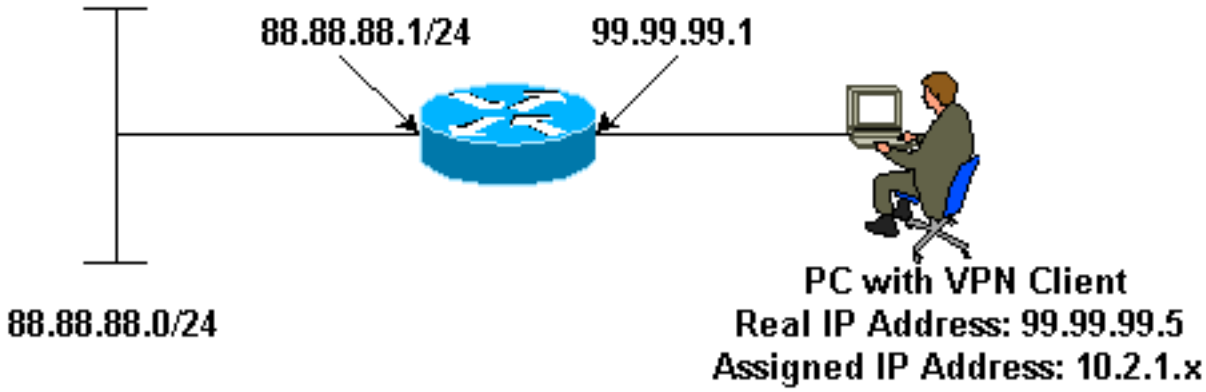
# Configurar

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

**Nota:** Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo 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.

- **show crypto engine connections active**: muestra los paquetes cifrados y descifrados.
- **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.**

Estas depuraciones deben ejecutarse en ambos routers IPSec (peers). La verificación de las asociaciones de seguridad se debe realizar en ambos pares

- **depuración crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.**
- **debug crypto isakmp** : muestra las negociaciones ISAKMP de la fase 1.
- **debug crypto engine — muestra el tráfico codificado.**
- **clear crypto isakmp â€" Borra las asociaciones de seguridad relacionadas con la fase 1.**
- **clear crypto sa** : borra las asociaciones de seguridad relacionadas con la fase 2.

# Troubleshoot

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

# Información Relacionada

- Soporte de Productos de Concentradores de la Serie VPN 3000
- Soporte del producto Cisco VPN 3000 Client
- Compatibilidad con tecnología IPSec (IP Security Protocol)
- Soporte Técnico - Cisco Systems