Configurando Modo de Roteador-config, Caractere Geral, Chaves Pré-compartilhadas, sem NAT

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

Nesta configuração de exemplo, um roteador é configurado para a configuração do modo (obtenha um endereço IP do pool), curinga, chaves pré-compartilhadas (todos os clientes de PC compartilham uma chave comum), sem Network Address Translation (NAT). Um usuário externo pode entrar na rede e ter um endereço IP interno atribuído do pool. Aos usuários, parece que estão dentro da rede. Os dispositivos dentro da rede são configurados com rotas para o pool 10.2.1.x não roteável.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco IOS® 12.0.7T ou posterior
- Hardware que suporta esta revisão de software
- CiscoSecure VPN Client 1.0/1.0.A ou 1.1 (mostrado como 2.0.7/E ou 2.1.12, respectivamente, vá para **Help > About** (**Ajuda > Sobre** 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.

Conventions

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

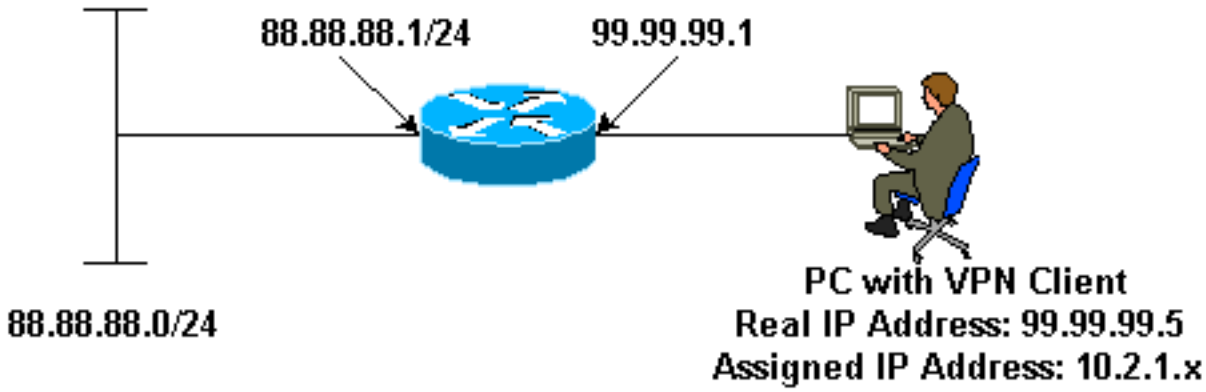
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Cliente de VPN
- Router

Cliente de 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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto engine connections ative** — Mostra os pacotes criptografados e descriptografados.
- **show crypto ipsec sa** — Mostra as associações de segurança da fase 2.
- **show crypto isakmp sa** — Mostra as associações de segurança da fase 1.

Essas depurações devem ser executadas em ambos os roteadores IPSec (peers). A limpeza de associações de segurança deve ser feita em ambos os correspondentes.

- **debug crypto ipsec** — Mostra as negociações de IPSec da fase 2.
- **debug crypto isakmp** — Mostra as negociações ISAKMP da fase 1.
- **debug crypto engine** — Mostra o tráfego que está criptografado.
- **clear crypto isakmp — Limpa as associações de segurança relacionadas à fase 1.**
- **clear crypto sa — Limpa as associações de segurança relacionadas à fase 2.**

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte ao produto VPN 3000 Series Concentrators
- Suporte ao produto cliente Cisco VPN 3000
- Suporte à tecnologia IPSec (IP Security Protocol)
- Suporte Técnico - Cisco Systems