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

Índice

Introdução

Nesta configuração de exemplo, um roteador é configurado para a configuração de modo (obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT do pool), curinga, chaves pré-compartilhada (toda a parte dos clientes PC uma chave comum), sem Network Address Translation (NAT). Um usuário externo pode incorporar a rede e ter um endereço IP interno atribuído do pool. Aos usuários, parece que estão dentro da rede. Os dispositivos dentro da rede estabelecem-se com as rotas ao pool do un-roteável 10.2.1.x.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software 12.0.7T de Cisco IOS® ou mais tarde
- Hardware que apoia esta revisão do software
- Cliente 1.0/1.0.A ou 1.1 do CiscoSecure VPN (mostrado como 2.0.7/E ou 2.1.12, respectivamente, vá ao **ajuda > sobre** verificar)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

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

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (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.

- **active do show crypto engine connections** — Mostra os pacotes criptografado e decriptografado.

- show crypto ipsec sa – Mostra as associações de segurança da fase 2.
- show crypto isakmp sa - Mostra as associações de segurança da fase 1.

Estes debugam devem ser executado em ambos os roteadores de IPSec (pares). A limpeza de associações de segurança deve ser feita em ambos os correspondentes.

- **IPsec do debug crypto** — Mostra as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Mostra o as negociações de ISAKMP de fase 1.
- **motor do debug crypto** — Mostra o tráfego que é cifrado.
- clear crypto isakmp — Limpa as associações de segurança relacionadas à fase 1.
- clear crypto sa — Limpa as associações de segurança relacionadas à fase 2.

Troubleshooting

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

Informações Relacionadas

- Sustentação do produto do VPN 3000 series concentrators
- Sustentação do produto do Cisco VPN 3000 Client
- Suporte por tecnologia do IPSEC (Protocolo de Segurança IP)
- Suporte Técnico - Cisco Systems