

# Autorização de autenticação proxy de entrada com configuração do IPsec e de cliente VPN com NAT e Cisco IOS Firewall

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Esta configuração de exemplo permite que um cliente VPN alcance um server em uma outra rede através de um túnel de IPsec, depois que a autenticação de usuário sucede.

Um PC em 99.99.99.5 ativa o navegador da Web para acessar o conteúdo no servidor em 10.13.1.98. Desde que o cliente VPN no PC é configurado para atravessar o valor-limite 99.99.99.1 do túnel obter à rede 10.13.1.x, o túnel de IPsec é construído e o PC obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT fora do pool chamado “ourpool” (desde que você está fazendo a configuração de modo). O 3640 Router pede a autenticação. Depois que o usuário digitar o nome de usuário e a senha (armazenados no servidor TACACS+ em 172.18.124.97), a lista de acesso passada do servidor é adicionada à lista de acesso 117.

**Nota:** O comando `ip auth-proxy` foi introduzido no Software Release 12.0.5.T de Cisco IOS®.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

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

- Cisco IOS Software Release 12.0.7.T
- Cisco 3640 Router (c3640-jo3s56i-mz.121-2.3.T)
- Cisco Secure VPN Client 1.0 (mostrado como 2.0.7 na ajuda de cliente de IRE > sobre o menu) ou Cisco Secure VPN Client 1.1 (mostrado como 2.1.12 na ajuda de cliente de IRE > sobre o menu)

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

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

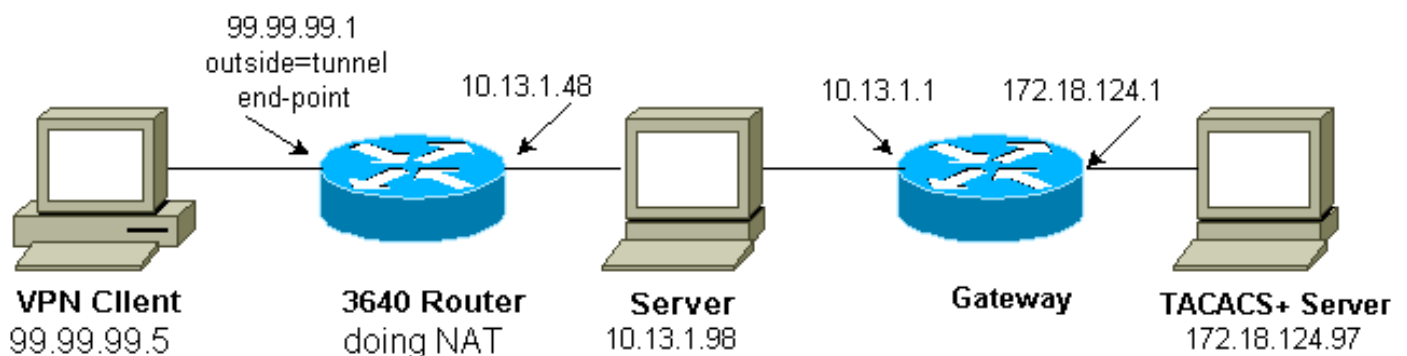
## Configurar

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

**Nota:** Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



## Configurações

Este documento utiliza esta configuração:

| Configuração do Roteador Cisco 3640  |
|--|
| Current configuration:<br>!<br>version 12.1<br>service timestamps debug uptime<br>service timestamps log uptime<br>no service password-encryption<br>! |

```
hostname carter
!
aaa new-model aaa authentication login default group
tacacs+ none aaa authorization exec default group
tacacs+ none aaa authorization auth-proxy default group
tacacs+ enable secret 5 $1$cSvL$F6VxA7kBFAGHvhBbRlNS20
enable password ww ! ip subnet-zero ! ip inspect name
myfw cuseeme timeout 3600 ip inspect name myfw ftp
timeout 3600 ip inspect name myfw http timeout 3600 ip
inspect name myfw rcmd timeout 3600 ip inspect name myfw
realaudio timeout 3600 ip inspect name myfw smtp timeout
3600 ip inspect name myfw sqlnet timeout 3600 ip inspect
name myfw streamworks timeout 3600 ip inspect name myfw
tftp timeout 30 ip inspect name myfw udp timeout 15 ip
inspect name myfw tcp timeout 3600 ip inspect name myfw
vdolive ip auth-proxy auth-proxy-banner ip auth-proxy
auth-cache-time 10 ip auth-proxy name list_a http ip
audit notify log ip audit po max-events 100 cns event-
service server ! crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco1234
address 0.0.0.0 0.0.0.0 crypto isakmp client
configuration address-pool local ourpool ! crypto ipsec
transform-set mypolicy esp-des esp-md5-hmac ! crypto
dynamic-map dyna 10 set transform-set mypolicy ! crypto
map test client configuration address initiate crypto
map test client configuration address respond crypto map
test 5 ipsec-isakmp dynamic dyna ! interface Loopback0
ip address 1.1.1.1 255.255.255.0 ! interface Ethernet0/0
ip address 10.13.1.48 255.255.255.0 ip nat inside ip
inspect myfw in ip route-cache policy no ip mroute-cache
ip policy route-map nonat no mop enabled ! interface
TokenRing0/0 no ip address shutdown ring-speed 16 !
interface Ethernet2/0 ip address 99.99.99.1
255.255.255.0 ip access-group 117 in ip nat outside ip
auth-proxy list_a no ip route-cache no ip mroute-cache
no mop enabled crypto map test ! interface TokenRing2/0
no ip address shutdown ring-speed 16 ! ip local pool
ourpool 10.2.1.1 10.2.1.254 ip nat pool outsidepool
99.99.99.50 99.99.99.60 netmask 255.255.255.0 ip nat
inside source route-map rmap pool outsidepool ip
classless ip route 0.0.0.0 0.0.0.0 99.99.99.20 ip route
172.18.124.0 255.255.255.0 10.13.1.1 no ip http server !
access-list 110 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255 access-list 110 permit ip 10.13.1.0 0.0.0.255
any access-list 117 permit esp any any access-list 117
permit udp any any eq isakmp access-list 120 permit ip
10.13.1.0 0.0.0.255 10.2.1.0 0.0.0.255 dialer-list 1
protocol ip permit dialer-list 1 protocol ipx permit
route-map rmap permit 10 match ip address 110 ! route-
map nonat permit 10 match ip address 120 set ip next-hop
1.1.1.2 ! route-map nonat permit 20 ! tacacs-server host
172.18.124.97 tacacs-server key cisco ! line con 0
transport input none line aux 0 line vty 0 4 password ww
! end
```

## [Verificar](#)

No momento, não há procedimento de verificação disponível para esta configuração.

## [Troubleshooting](#)

Refira [pesquisando defeitos o Proxy de autenticação](#) para a informação de Troubleshooting.

**Nota:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

## Informações Relacionadas

- [Cisco VPN Client](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Suporte técnico do Cisco IOS Firewall](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)