

Autenticación de proxy de autenticación entrante con configuración de cliente VPN e IPsec con NAT y firewall Cisco IOS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

[Introducción](#)

Esta configuración de muestra permite a un Cliente VPN acceder a un servidor de otra red a través de un túnel IPsec, luego de lograda la autenticación del usuario.

Una PC en 99.99.99.5 presenta el explorador Web para acceder al contenido del servidor en 10.13.1.98. Dado que el VPN Client en el PC está configurado para atravesar el punto final del túnel 99.99.99.1 para llegar a la red 10.13.1.x, el túnel IPsec está construido y el PC obtiene la dirección IP del conjunto denominada "ourpool" (ya que está realizando la configuración de modo). El router 3640 solicita autenticación. Luego de que el usuario ingresa un nombre de usuario y una contraseña (almacenados en el servidor TACACS+ en 172.18.124.97), la lista de acceso transmitida desde el servidor es agregada a la lista de acceso 117.

Nota: El comando `ip auth-proxy` se introdujo en la versión 12.0.5.T del software del IOS® de Cisco.

[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.

- Versión 12.0.7.T de software del IOS de Cisco
- Router Cisco 3640 (c3640-jo3s56i-mz.121-2.3.T)
- Cisco Secure VPN Client 1.0 (mostrado como 2.0.7 en el menú Ayuda del cliente IRE > Acerca del) o Cisco Secure VPN Client 1.1 (mostrado como 2.1.12 en el menú Ayuda del cliente IRE > Acerca del)

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

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

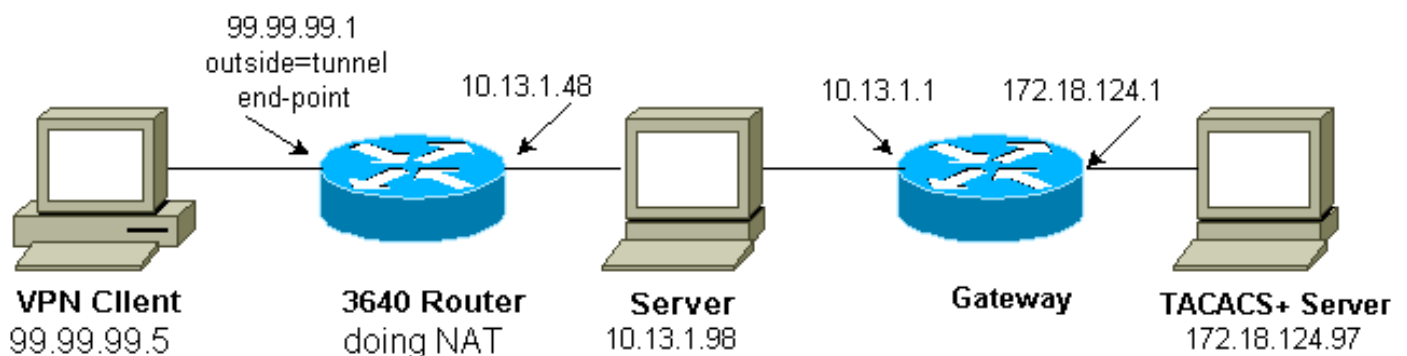
Configurar

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

Nota: Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa esta configuración:

```
Configuración del router 3640 de Cisco

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
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

```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Consulte [Resolución de Problemas de Proxy de Autenticación](#) para obtener información de troubleshooting.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos debug.

[Información Relacionada](#)

- [Cliente de Cisco VPN](#)
- [Negociación IPSec/Protocolos IKE](#)
- [Soporte Técnico del Firewall Cisco IOS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)