Autenticación auth-proxy entrante con el IPSec y la configuración de cliente VPN con el NAT y el Firewall Cisco IOS

Contenido

Introducción

Esta configuración de muestra permite que un cliente VPN acceda un servidor en otra red a través de un túnel IPsec, después de que la autenticación de usuario tenga éxito.

Una PC en 99.99.99.5 presenta el explorador Web para acceder al contenido del servidor en 10.13.1.98. Puesto que configuran al cliente VPN en el PC para pasar con la punto final 99.99.99.1 del túnel conseguir a la red 10.13.1.x, se construye el túnel IPsec y el PC consigue el pool de los de la dirección IP llamado “ourpool” (puesto que usted está haciendo la configuración del modo). El 3640 Router pide la 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: Presentaron al **comando ip auth-proxy** en el Software Release 12.0.5.T de Cisco IOS®.

prerrequisitos

Requisitos

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
- Cisco 3640 Router (c3640-jo3s56i-mz.121-2.3.T)
- Cliente Cisco Secure VPN 1.0 (mostrado como 2.0.7 en la ayuda para IRE cliente > sobre el menú) o Cliente Cisco Secure VPN 1.1 (mostrado como 2.1.12 en la ayuda para IRE cliente > sobre el menú)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

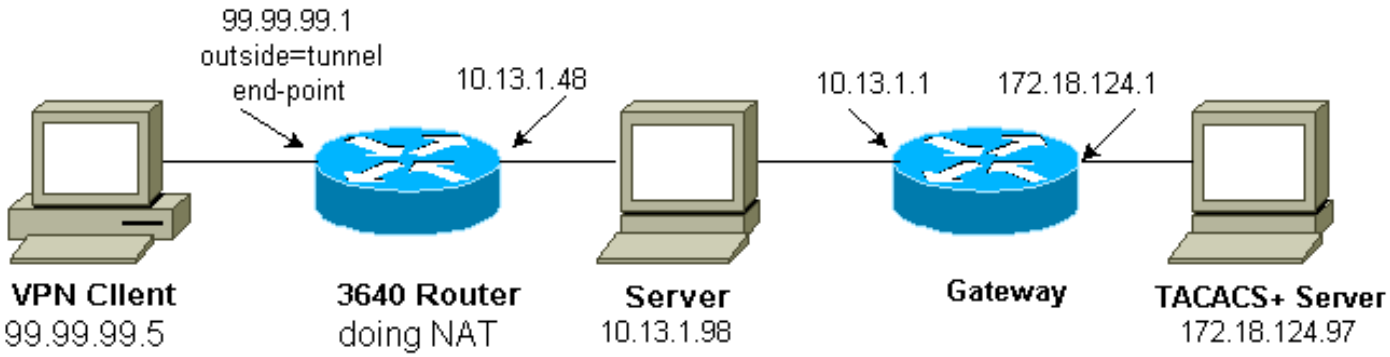
Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) 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.

Troubleshooting

Refiera al Proxy de autenticación del troubleshooting para la información de Troubleshooting.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Información Relacionada

- Cliente de Cisco VPN
- IPSec Negotiation/IKE Protocols
- Soporte técnico del Firewall Cisco IOS
- Soporte Técnico y Documentación - Cisco Systems