Configuración del cliente IPSec - Cisco Secure VPN al Acceso de control de router central.

Contenido

Introducción

La siguiente configuración no es de uso común, sino que fue diseñada para permitir la terminación del túnel IPSec de Cisco Secure VPN Client en un router central. Cuando aparece el túnel, el PC recibe su dirección IP del conjunto de direcciones IP del router central (en nuestro ejemplo, el router se denomina "moss"), después el tráfico del conjunto puede alcanzar la red local que hay detrás de moss o se puede rutear y cifrar a la red que hay detrás del router externo (en nuestro ejemplo, el router se denomina "carter"). Además, el tráfico de la red privada 10.13.1.X a 10.1.1.X se cifra; los routers están haciendo sobrecarga de NAT.

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 12.1.5.T (c3640-io3s56i-mz.121-5.T) del Cisco IOS ® Software
- Secure VPN Client 1.1 de Cisco

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

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

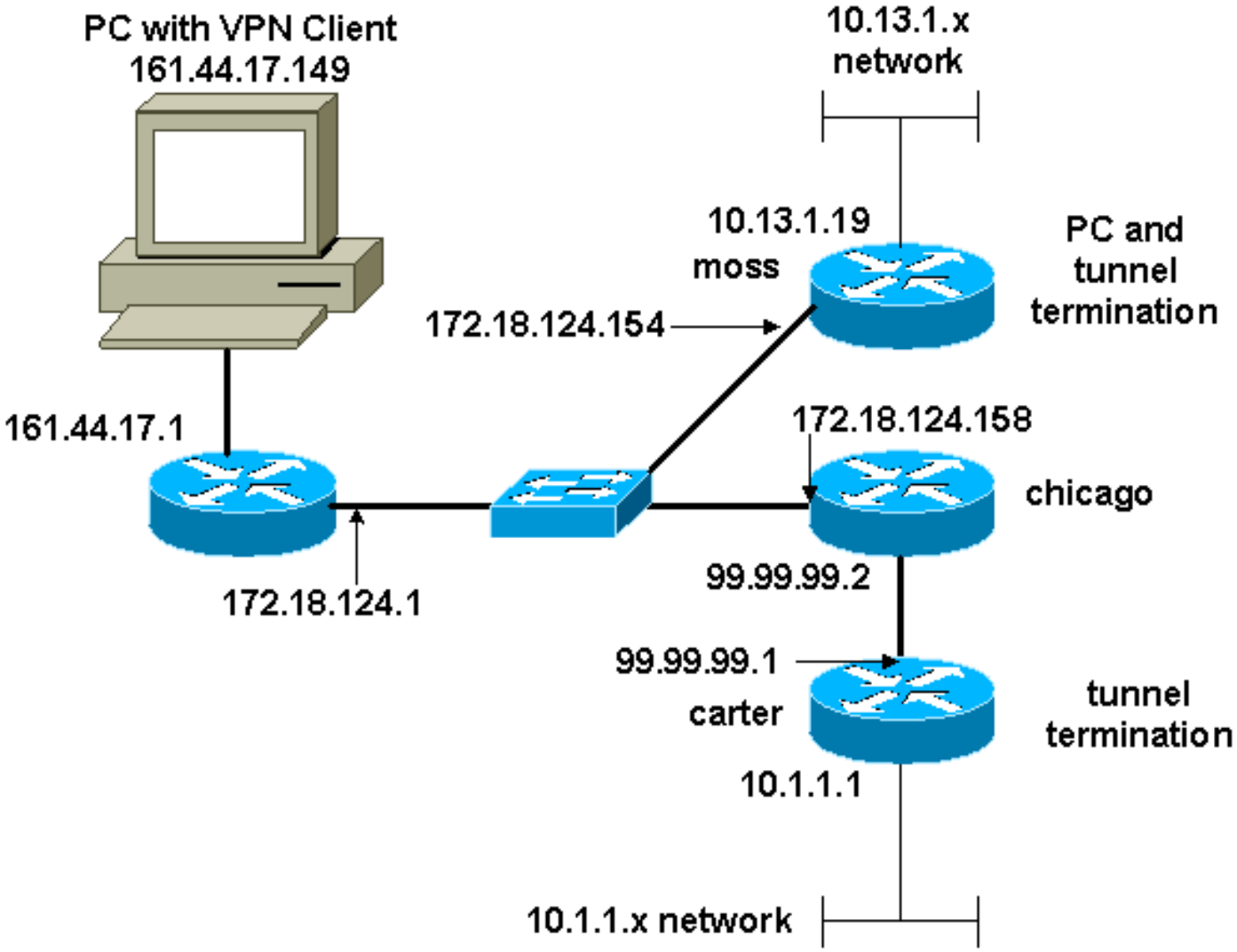
Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración moss
- Configuración carter

Configuración moss

```
Version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
enable password ww
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.1 crypto
isakmp key cisco123 address 0.0.0.0 0.0.0.0 crypto
isakmp client configuration address-pool local RTP-POOL
! crypto ipsec transform-set rtpset esp-des esp-md5-hmac
! crypto dynamic-map rtp-dynamic 20 set transform-set
rtpset ! crypto map rtp client configuration address
initiate crypto map rtp client configuration address
respond !crypto map sequence for network to network
traffic crypto map rtp 1 ipsec-isakmp set peer
99.99.99.1 set transform-set rtpset match address 115 !--
-- crypto map sequence for VPN Client network traffic.
crypto map rtp 10 ipsec-isakmp dynamic rtp-dynamic !
call rsvp-sync ! interface Ethernet2/0 ip address
172.18.124.154 255.255.255.0 ip nat outside no ip route-
cache no ip mroute-cache half-duplex crypto map rtp !
interface Serial2/0 no ip address shutdown ! interface
Ethernet2/1 ip address 10.13.1.19 255.255.255.0 ip nat
inside half-duplex ! ip local pool RTP-POOL 192.168.1.1
192.168.1.254 ip nat pool ETH20 172.18.124.154
172.18.124.154 netmask 255.255.255.0 ip nat inside
source route-map nonat pool ETH20 overload ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1 ip route 10.1.1.0
255.255.255.0 172.18.124.158 ip route 99.99.99.0
255.255.255.0 172.18.124.158 no ip http server ! !---
Exclude traffic from NAT process. access-list 110 deny
ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list
110 deny ip 10.13.1.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any !---
Include traffic in encryption process. access-list 115
permit ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255 access-
list 115 permit ip 192.168.1.0 0.0.0.255 10.1.1.0
0.0.0.255 route-map nonat permit 10 match ip address 110
! dial-peer cor custom ! line con 0 transport input none
line aux 0 line vty 0 4 login ! end
```

Configuración carter

```
Current configuration : 2059 bytes
```

```
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.154 !
crypto ipsec transform-set rtpset esp-des esp-md5-hmac !
!--- crypto map sequence for network-to-network traffic.
crypto map rtp 1 ipsec-isakmp set peer 172.18.124.154
set transform-set rtpset match address 115 ! call rsvp-
sync ! interface Ethernet0/0 ip address 99.99.99.1
255.255.255.0 ip nat outside half-duplex crypto map rtp
! interface FastEthernet3/0 ip address 10.1.1.1
255.255.255.0 ip nat inside duplex auto speed 10 ! ip
nat pool ETH00 99.99.99.1 99.99.99.1 netmask
255.255.255.0 ip nat inside source route-map nonat pool
ETH00 overload ip classless ip route 0.0.0.0 0.0.0.0
99.99.99.2 no ip http server ! !--- Exclude traffic from
NAT process. access-list 110 deny ip 10.1.1.0 0.0.0.255
10.13.1.0 0.0.0.255 access-list 110 deny ip 10.1.1.0
0.0.0.255 192.168.1.0 0.0.0.255 access-list 110 permit
ip 10.1.1.0 0.0.0.255 any !--- Include traffic in
encryption process. access-list 115 permit ip 10.1.1.0
0.0.0.255 10.13.1.0 0.0.0.255 access-list 115 permit ip
10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255 route-map nonat
permit 10 match ip address 110 ! line con 0 transport
input none line aux 0 line vty 0 4 password ww login !
end
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- show crypto ipsec sa - Muestra las asociaciones de seguridad de la fase 2.
- show crypto isakmp sa — Muestra las asociaciones de seguridad de la fase 1.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

- depuración crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.
- debug crypto isakmp — muestra las negociaciones ISAKMP para la fase 1.
- debug crypto engine — muestra el tráfico codificado.
- clear crypto isakmp â€" Borra las asociaciones de seguridad relacionadas con la fase 1.
- **borre el sa crypto** — Borra las asociaciones de seguridad relacionadas con la fase 2.

Información Relacionada

- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Página de soporte para cliente Cisco VPN
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems