Configurazione di IPSec - Cisco Secure VPN Client per il controllo dell'accesso del router centrale

Sommario

Introduzione

La configurazione seguente non viene utilizzata comunemente, ma è stata progettata per consentire la terminazione del tunnel IPSec del client VPN sicuro Cisco su un router centrale. Quando il tunnel arriva, il PC riceve il proprio indirizzo IP dal pool di indirizzi IP del router centrale (nell'esempio riportato il router è denominato "moss"), quindi il traffico del pool può raggiungere la rete locale dietro il moss o essere indirizzato e crittografato sulla rete dietro il router esterno (nell'esempio riportato il router è denominato "carter"). Inoltre, il traffico dalla rete privata da 10.13.1.X a 10.1.1.X è crittografato; i router stanno eseguendo un sovraccarico NAT.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.1.5.T (c3640-io3s56i-mz.121-5.T)

- Cisco Secure VPN Client 1.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

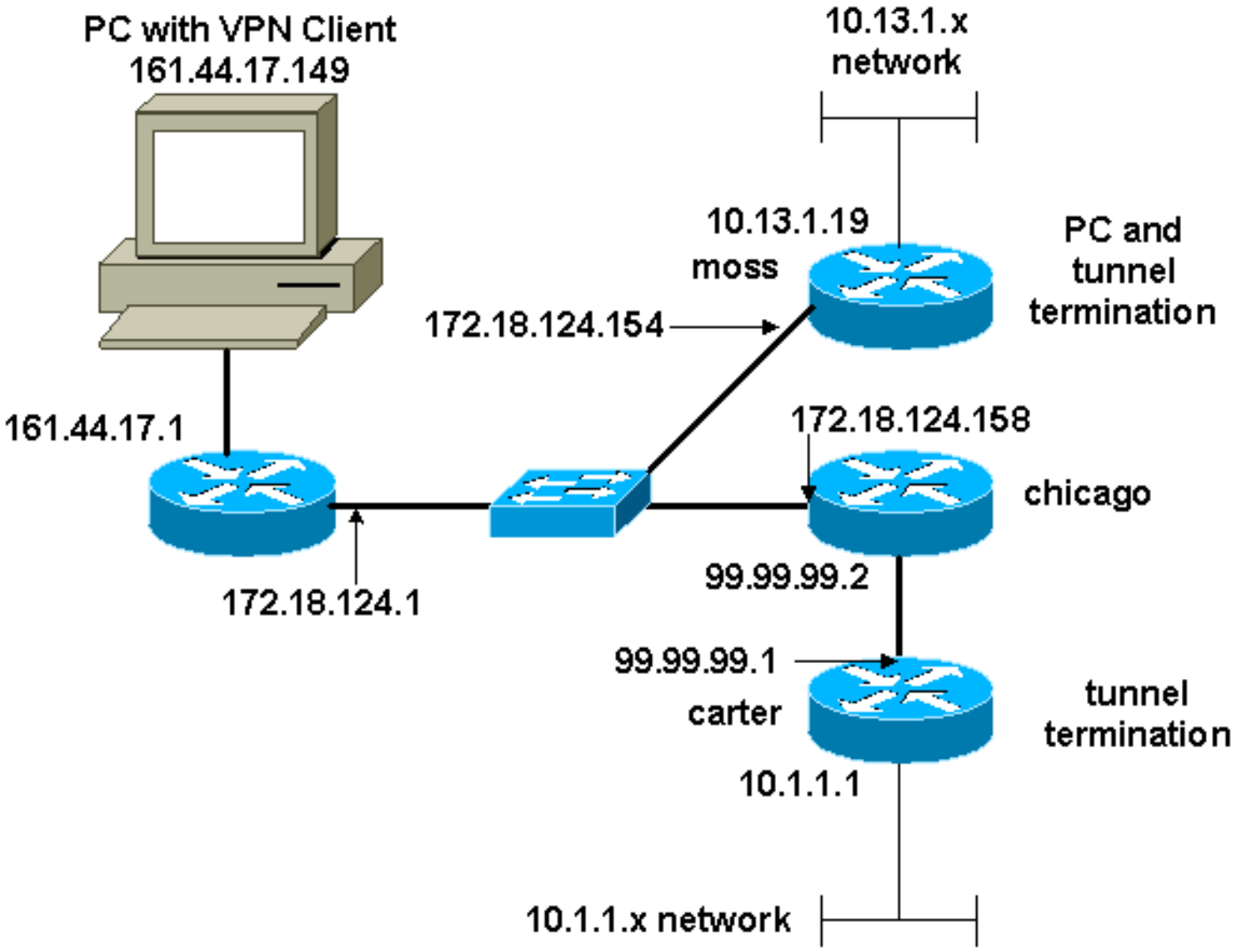
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione moss
- Configurazione del dispositivo di scorrimento

Configurazione 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
```

Configurazione del dispositivo di scorrimento

```
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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

- **debug crypto ipsec**: visualizza le negoziazioni IPSec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP della fase 1.
- **debug crypto engine**: visualizza il traffico crittografato.
- **clear crypto isakmp**: cancella le associazioni di sicurezza correlate alla fase 1.
- **clear crypto sa**: cancella le associazioni di sicurezza correlate alla fase 2.

Informazioni correlate

- Configurazione di IPSec Network Security
- Configurazione del protocollo di protezione di Internet Key Exchange
- Pagina di supporto per Cisco VPN Client
- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems