Configuration d'IPSec – Contrôle d'accès entre Cisco Secure VPN Client et routeur central

Contenu

Introduction

La configuration suivante n'est généralement pas utilisée, mais a été conçue pour permettre la terminaison de tunnel IPSec de Cisco Secure VPN Client sur un routeur central. Pendant que le tunnel apparaît, le PC reçoit son adresse IP du groupe d'adresses IP du routeur central (dans notre exemple, le routeur est nommé « Mousse »), puis le trafic du groupe peut atteindre le réseau local derrière « Mousse » ou être chiffré et acheminé vers le réseau derrière le routeur périphérique (dans notre exemple, le routeur est nommé « Carter »). Le trafic du réseau privé 10.13.1.X à 10.1.1.X est en outre chiffré; les routeurs effectuent une surcharge de NAT.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

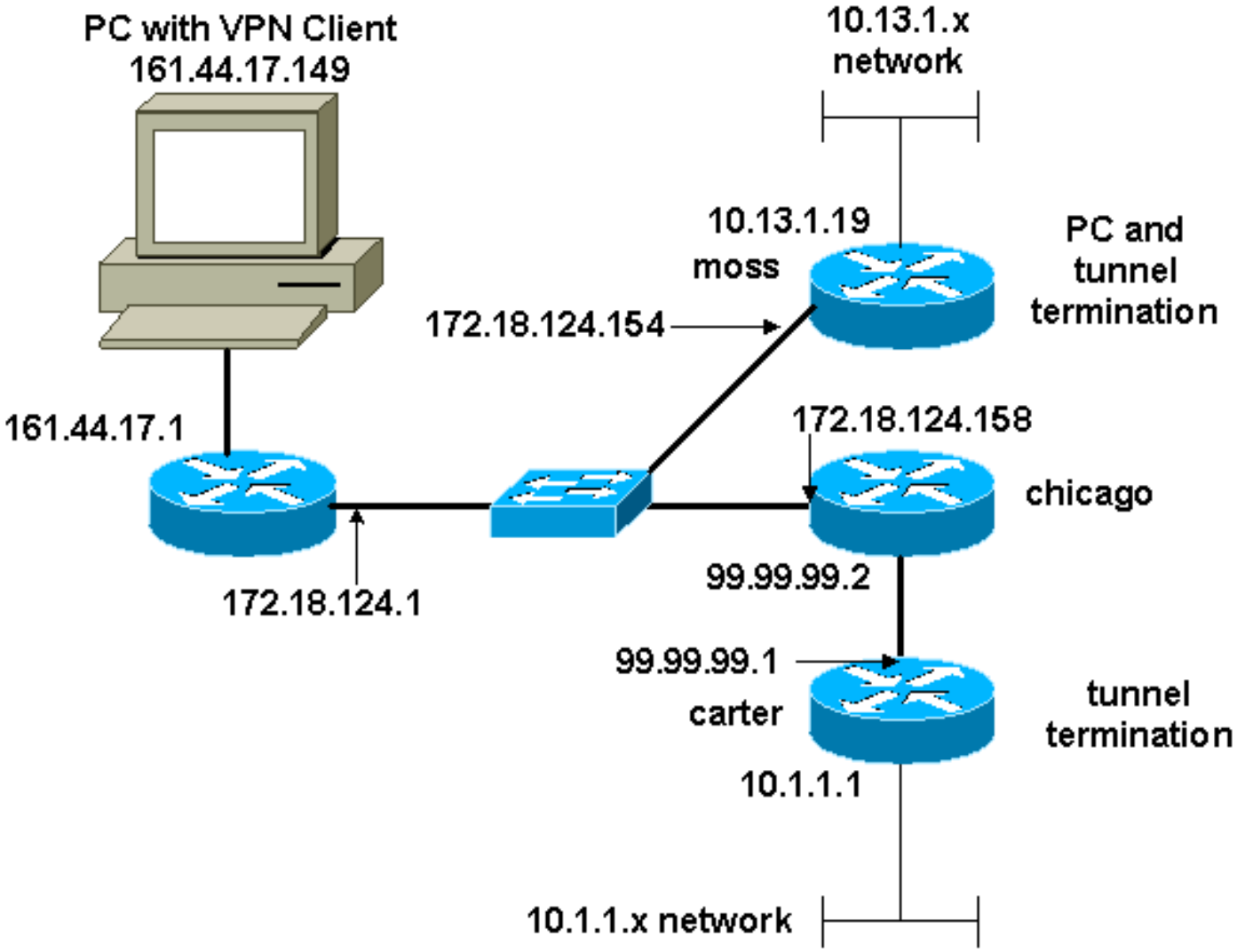
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- configuration de mousse
- configuration de Carter

configuration de mousse

```
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
```

configuration de 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
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto ipsec sa** - Montre les associations de sécurisation de phase 2.
- **show crypto isakmp sa** - Montre les associations de sécurisation de phase 1.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'émettre des commandes de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

- **debug crypto ipsec** — Affiche les négociations IPSecs de la phase 2.
- **debug crypto isakmp** — Affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Montre le trafic crypté.
- **clear crypto isakmp** — Autorise les associations de sécurité liées à la phase 1.
- **clear crypto sa** — Autorise les associations de sécurité liées à la phase 2.

Informations connexes

- Sécurité des réseaux de configuration d'IPSec
- Configurer le protocole de sécurité IKE
- Cisco VPN Client Support Page
- Page d'assistance IPsec
- Support technique - Cisco Systems