Konfiguration von IPSec - Cisco Secure VPN Client zu Central Router Controlling Access

Inhalt

Einführung

Die folgende Konfiguration wird normalerweise nicht verwendet, wurde jedoch entwickelt, um die Terminierung von Cisco Secure VPN Client IPSec-Tunneln auf einem zentralen Router zu ermöglichen. Wenn der Tunnel hochgefahren wird, erhält der PC seine IP-Adresse vom IP-Adresspool des zentralen Routers (in unserem Beispiel wird der Router als "Moss" bezeichnet). Anschließend kann der Poolverkehr das lokale Netzwerk hinter dem Moos erreichen oder über das Netzwerk hinter dem äußeren Router weitergeleitet und verschlüsselt werden (in unserem Beispiel wird der Router als "Carter" bezeichnet). Darüber hinaus wird der Datenverkehr vom privaten Netzwerk 10.13.1.X bis 10.1.1.X verschlüsselt. die Router überladen NAT.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

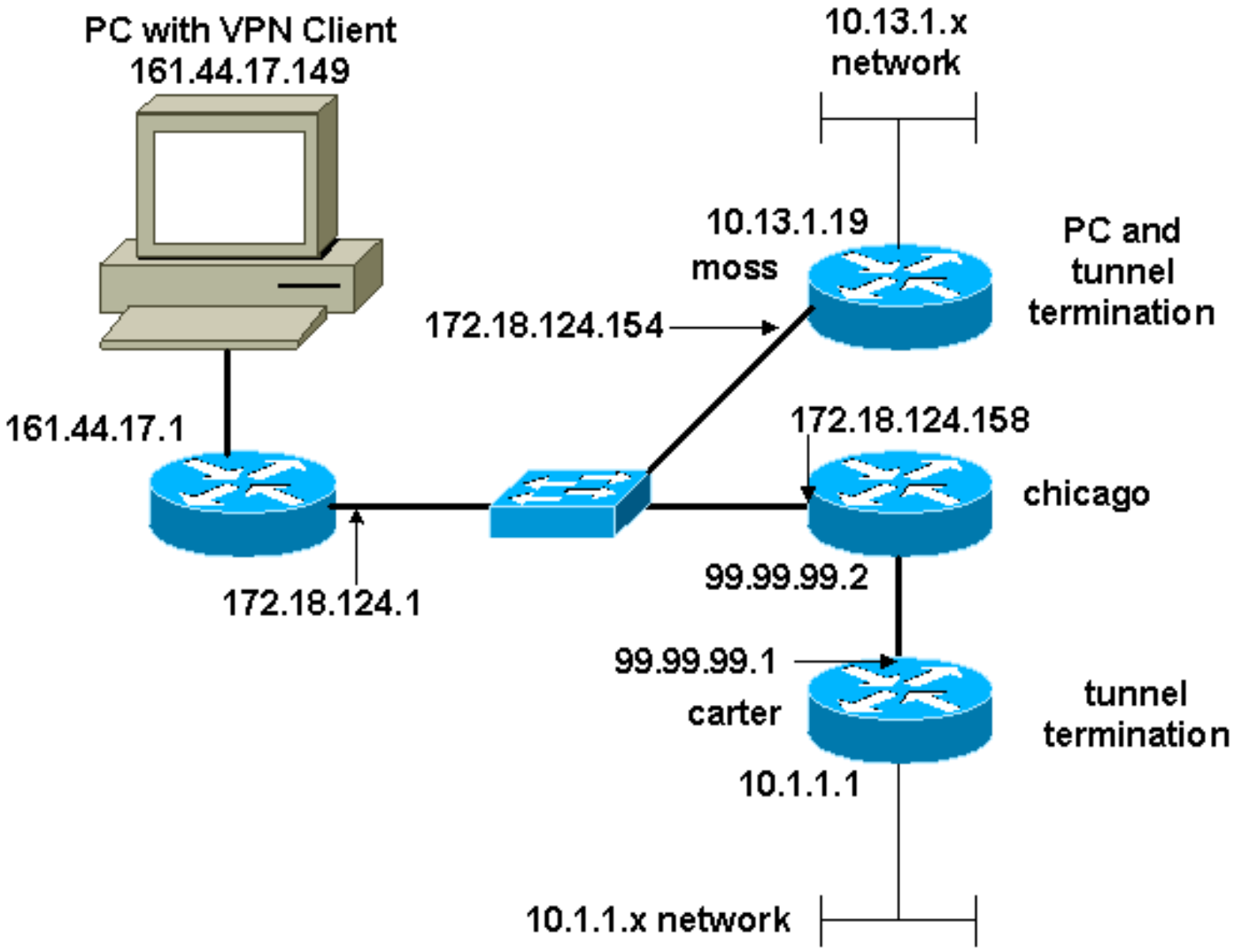
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Mooskonfiguration
- Carter-Konfiguration

Mooskonfiguration

```
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
```

Carter-Konfiguration

```
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
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1 an.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- **debug crypto ipsec** - Zeigt die IPSec-Verhandlungen von Phase 2.
- **debug crypto isakmp** - Zeigt die ISAKMP-Verhandlungen für Phase 1.
- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **clear crypto isakmp**: Löscht die Sicherheitszuordnungen für Phase 1.
- **clear crypto sa**: Löscht die Sicherheitszuordnungen für Phase 2.

Zugehörige Informationen

- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Support-Seite für Cisco VPN-Clients
- IPSec-Support-Seite
- Technischer Support - Cisco Systems