配置 IPSec - 从 Cisco Secure VPN 客户端到控制访问的中心路由器

目录

简介

以下配置不是常用配置，该配置用于允许在中央路由器上使用 Cisco 安全 VPN 客户端 IPSec 隧道终端。在隧道启动后，PC 将从中央路由器的 IP 地址池（在我们的示例中，该路由器名为“moss”）接收其 IP 地址，然后池数据流会到达 moss 后的本地网络或被路由到边远路由器（在我们的示例，该路由器名为“carter”）后的网络并进行加密。此外，专有网络 10.13.1.X 与 10.1.1.X 之间的流量也将被加密；路由器正在执行 NAT 过载。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS软件版本12.1.5.T (c3640-io3s56i-mz.121-5.T)
- Cisco 安全 VPN 客户端 1.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

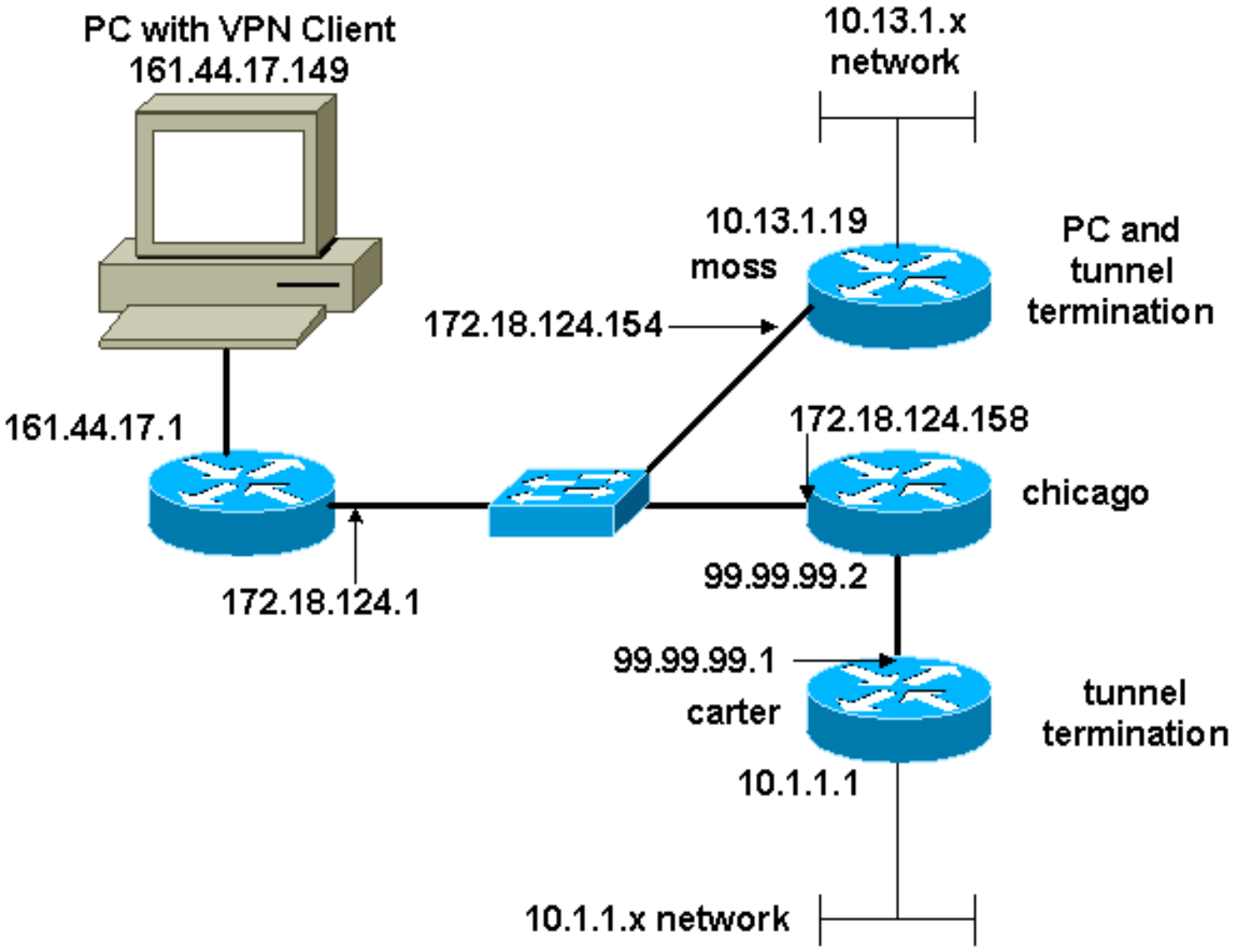
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- 青苔配置
- 卡特配置

青苔配置

```
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
```

卡特配置

```
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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto ipsec sa** — 显示第 2 阶段安全连接。
- **show crypto isakmp sa** - 显示第 1 阶段的安全关联。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。
- **debug crypto engine** - 显示已加密的数据流。
- **clear crypto isakmp** - 清除与第 1 阶段相关的安全关联。
- **clear crypto sa** - 清除与第 2 阶段相关的安全关联。

相关信息

- **配置 IPSec 网络安全**
- **配置 Internet 密钥交换安全协议**
- Cisco VPN 客户端支持页
- IPSec 支持页面
- 技术支持 - Cisco Systems