

使用IPsec的身份驗證入站和使用NAT和Cisco IOS防火牆的VPN客戶端配置

目錄

- [簡介](#)
- [必要條件](#)
- [需求](#)
- [採用元件](#)
- [慣例](#)
- [設定](#)
- [網路圖表](#)
- [組態](#)
- [驗證](#)
- [疑難排解](#)
- [相關資訊](#)

簡介

此示例配置允許VPN客戶端在使用者身份驗證成功後通過IPsec隧道訪問另一網路上的伺服器。

99.99.99.5的PC會啟動Web瀏覽器來訪問位於10.13.1.98的伺服器上的內容。因為PC上的VPN客戶端配置為通過隧道端點99.99.1到達10.13.1.x網路，所以會構建IPsec隧道，並且PC會從名為「ourpool」的池獲取IP地址（因為您正在進行模式配置）。3640路由器請求身份驗證。使用者輸入使用者名稱和密碼後（儲存在172.18.124.97處的TACACS+伺服器上），從伺服器向下傳遞的存取清單會新增到存取清單117中。

注意： ip auth-proxy指令是在Cisco IOS®軟體版本12.0.5中匯入，

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本12.0.7.T
- Cisco 3640路由器(c3640-jo3s56i-mz.121-2.3.T)
- Cisco Secure VPN Client 1.0（在IRE客戶端「幫助」>「關於」選單中顯示2.0.7）或Cisco

Secure VPN Client 1.1 (在IRE客戶端「幫助」>「關於」選單中顯示2.1.12)
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

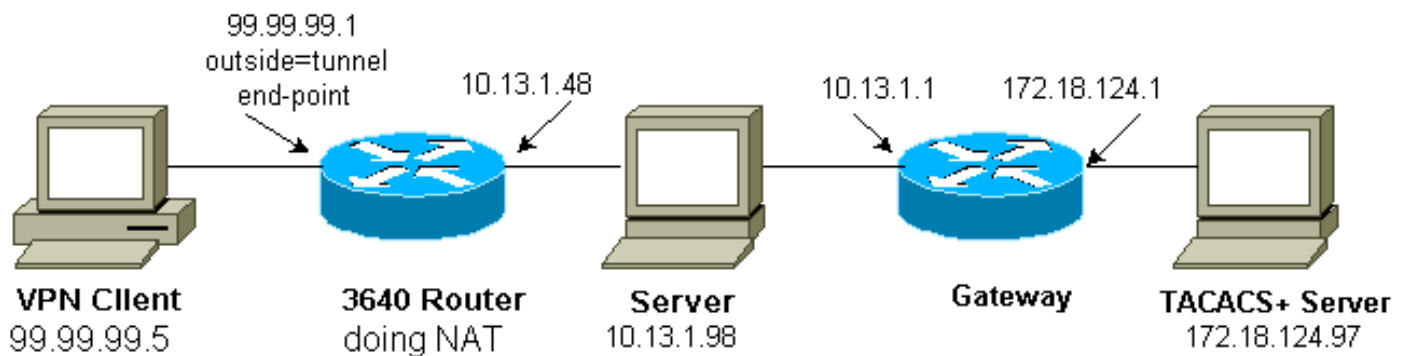
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

思科3640路由器配置

```
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
aaa new-model
aaa authentication login default group tacacs+ none
aaa authorization exec default group tacacs+ none
aaa authorization auth-proxy default group tacacs+
enable secret 5 $1$cSvL$F6VxA7kBFAGHvhBbRlNS20
enable password ww
!
ip subnet-zero
!
ip inspect name myfw cuseeme timeout 3600
```

```
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw vdolive
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco1234 address 0.0.0.0 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test client configuration address initiate
crypto map test client configuration address respond
crypto map test 5 ipsec-isakmp dynamic dyna
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.13.1.48 255.255.255.0
ip nat inside
ip inspect myfw in
ip route-cache policy
no ip mroute-cache
ip policy route-map nonat
no mop enabled
!
interface TokenRing0/0
no ip address
shutdown
ring-speed 16
!
interface Ethernet2/0
ip address 99.99.99.1 255.255.255.0
ip access-group 117 in
ip nat outside
ip auth-proxy list_a
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map test
!
interface TokenRing2/0
no ip address
shutdown
```

```
ring-speed 16
!
ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 99.99.99.50 99.99.99.60 netmask
255.255.255.0
ip nat inside source route-map rmap pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.20
ip route 172.18.124.0 255.255.255.0 10.13.1.1
no ip http server
!
access-list 110 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any
access-list 117 permit esp any any
access-list 117 permit udp any any eq isakmp
access-list 120 permit ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map rmap permit 10
match ip address 110
!
route-map nonat permit 10
match ip address 120
set ip next-hop 1.1.1.2
!
route-map nonat permit 20
!
tacacs-server host 172.18.124.97
tacacs-server key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
!
end
```

[驗證](#)

目前沒有適用於此組態的驗證程序。

[疑難排解](#)

如需疑難排解資訊，請參閱[驗證代理疑難排解](#)。

附註：使用 `debug` 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

[相關資訊](#)

- [Cisco VPN使用者端](#)
- [IPSec 協商/IKE 通訊協定](#)
- [Cisco IOS防火牆技術支援](#)
- [技術支援與文件 - Cisco Systems](#)