

带IPSec 的认证代理验证入站，以及带NAT和Cisco IOS防火墙的VPN客户端配置

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

在用户认证成功后，此配置示例允许VPN客户端通过IPSec隧道访问在另一网络的一个服务器。

地址在99.99.99.5的PC启动网络浏览器访问内容在地址10.13.1.98的服务器。因为PC的VPN客户端配置通过隧道终点99.99.99.1达到10.13.1.x网络，IPSec隧道被构建，并且PC使IP地址脱离池呼叫“ourpool”（因为您执行模式配置）。3640路由器请求验证。在用户输入用户名和密码（存储在TACACS+服务器在172.18.124.97）后，从服务器通过的下来访问列表添加到访问列表117。

注意： ip auth-proxy指令在Cisco IOS软件版本12.0.5.T被引入

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12.0.7.T
- Cisco 3640路由器(c3640-jo3s56i-mz.121-2.3.T)
- 思科安全VPN客户端1.0 (显示作为2.0.7在IRE客户端帮助> About菜单)或思科安全VPN客户端1.1 (显示作为2.1.12在IRE客户端帮助> About菜单)

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](#)。

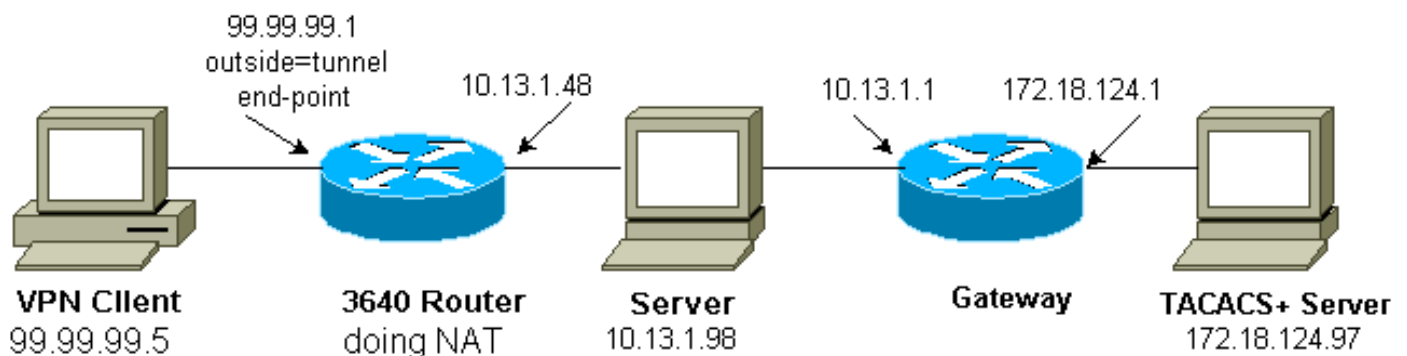
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用 [命令查找工具](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

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：

```
Cisco 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 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
```

验证

当前没有可用于此配置的验证过程。

故障排除

关于故障排除信息参考[故障排除认证代理](#)。

注意： 使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

相关信息

- [Cisco VPN 客户端](#)
- [IPsec 协商/IKE 协议](#)
- [Cisco IOS 防火墙技术支持](#)
- [技术支持和文档 - Cisco Systems](#)