# Auth−proxy Authentication Inbound with IPsec and VPN Client Configuration with NAT and Cisco IOS Firewall

### Document ID: 14295

## Contents



## Introduction

This sample configuration allows a VPN Client to access a server on another network through an IPsec tunnel, after the user authentication succeeds.

A PC at 99.99.99.5 brings up the web browser to access content on the server at 10.13.1.98. Since the VPN Client on the PC is configured to go through tunnel end−point 99.99.99.1 to get to the 10.13.1.x network, the IPsec tunnel is built and the PC gets the IP address out of the pool called "ourpool" (since you are doing mode−configuration). The 3640 router requests authentication. After the user enters a username and password (stored on the TACACS+ server at 172.18.124.97), the access list passed down from the server gets added to access list 117.

**Note:** The **ip auth−proxy** command was introduced in Cisco IOS® Software Release 12.0.5.T.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.0.7.T
- Cisco 3640 router (c3640−jo3s56i−mz.121−2.3.T)
- Cisco Secure VPN Client 1.0 (shown as 2.0.7 in the IRE client Help > About menu) or Cisco Secure VPN Client 1.1 (shown as 2.1.12 in the IRE client Help > About menu)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

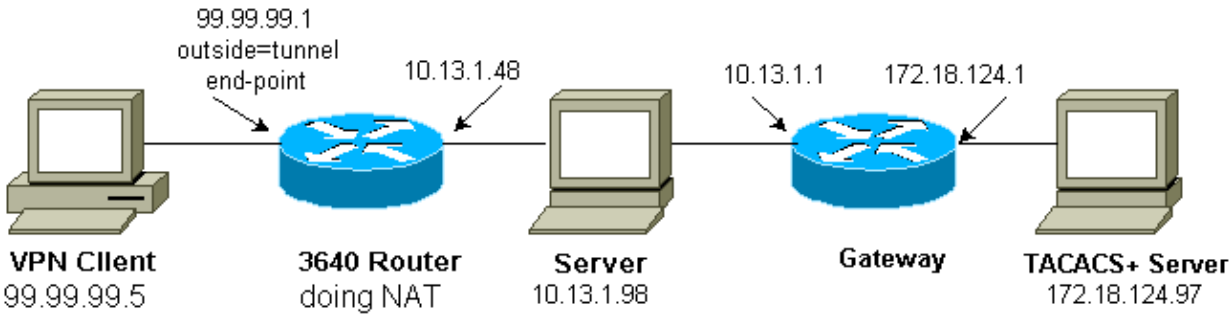
# Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:




## Configurations

This document uses this configuration:

**Cisco 3640 Router Configuration**

```
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
```

# Verify

There is currently no verification procedure available for this configuration.

# Troubleshoot

Refer to Troubleshooting Authentication Proxy for troubleshooting information.

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

# Related Information

- **Cisco VPN Client**
- **IPSec Negotiation/IKE Protocols**
- **Cisco IOS Firewall Technical Support**
- **Technical Support & Documentation − Cisco Systems**



Updated: Aug 15, 2006 Document ID: 14295