# Autenticazione proxy in entrata con IPsec e configurazione del client VPN con NAT e Cisco IOS Firewall

## Sommario



## Introduzione

Questa configurazione di esempio consente a un client VPN di accedere a un server in un'altra rete tramite un tunnel IPsec, dopo il completamento dell'autenticazione utente.

Un PC con indirizzo 99.99.99.5 apre il browser Web per accedere al contenuto sul server con indirizzo 10.13.1.98. Poiché il client VPN sul PC è configurato per passare attraverso l'endpoint del tunnel 99.99.99.1 per raggiungere la rete 10.13.1.x, il tunnel IPsec viene creato e il PC ottiene l'indirizzo IP dal pool denominato "ourpool" (poiché si sta eseguendo la configurazione della modalità). Il router 3640 richiede l'autenticazione. Dopo che l'utente ha immesso un nome utente e una password (memorizzati sul server TACACS+ al numero 172.18.124.97), l'elenco degli accessi passato dal server viene aggiunto all'elenco degli accessi 117.

**Nota:** il comando **ip auth-proxy** è stato introdotto nel software Cisco IOS® versione 12.0.5.T.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS release 12.0.7.T
- Router Cisco 3640 (c3640-jo3s56i-mz.121-2.3.T)
- Cisco Secure VPN Client 1.0 (visualizzato come 2.0.7 nel menu? del client IRE > Informazioni su) o Cisco Secure VPN Client 1.1 (visualizzato come 2.1.12 nel menu? del client IRE > Informazioni su)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

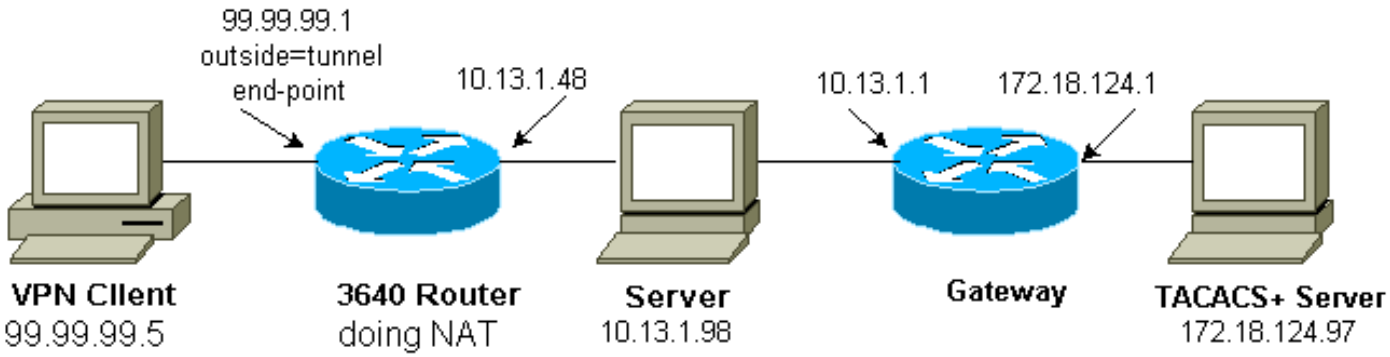
## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota: per** ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

### Esempio di rete

Nel documento viene usata questa impostazione di rete:




### Configurazioni

Nel documento viene usata questa configurazione:

| Cisco 3640 Router Configuration |
| --- |
| `Current configuration:`<br>`!`<br>`version 12.1`<br>`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
```

# Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

# Risoluzione dei problemi

Per informazioni sulla risoluzione dei problemi, fare riferimento a Risoluzione dei problemi del proxy di autenticazione.

**Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

## Informazioni correlate

- Cisco VPN Client
- Negoziazione IPSec/protocolli IKE
- Supporto tecnico Cisco IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems