NAT および Cisco IOS Firewall を使った、IPSec および VPN クライアントの設定に関する Auth-proxy 認証着信

内容

概要

次の設定例を使用すると、ユーザ認証が成功した後、VPN Client は IPSec トンネル経由で別のネットワーク上のサーバにアクセスできます。

99.99.99.5のPCがWebブラウザを起動し、10.13.1.98のサーバ上のコンテンツにアクセスします。PCのVPN Clientはトンネルのエンドポイント99.99.99.1を経由して10.13.1.xネットワークにアクセスするように設定されているため、IPsecトンネルが構築され、「pool」と呼呼呼されます。3640 ルータが認証を要求します。ユーザが（172.18.124.97 の TACACS+ サーバに格納されている）ユーザ名とパスワードを入力した後、サーバから渡されるアクセス リストは、アクセス リスト 117 に追加されます。

注：ip auth-proxyコマンドは、Cisco IOS®ソフトウェアリリース12.0.5.Tで導入されました。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 12.0.7.T
- Cisco 3640 ルータ（c3640-jo3s56i-mz.121-2.3.T）
- Cisco Secure VPN Client 1.0([IRE client Help] > [About]メニューで2.0.7と表示)またはCisco Secure VPN Client 1.1([IRE client Help] > [About]メニューで2.1.12と表示)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

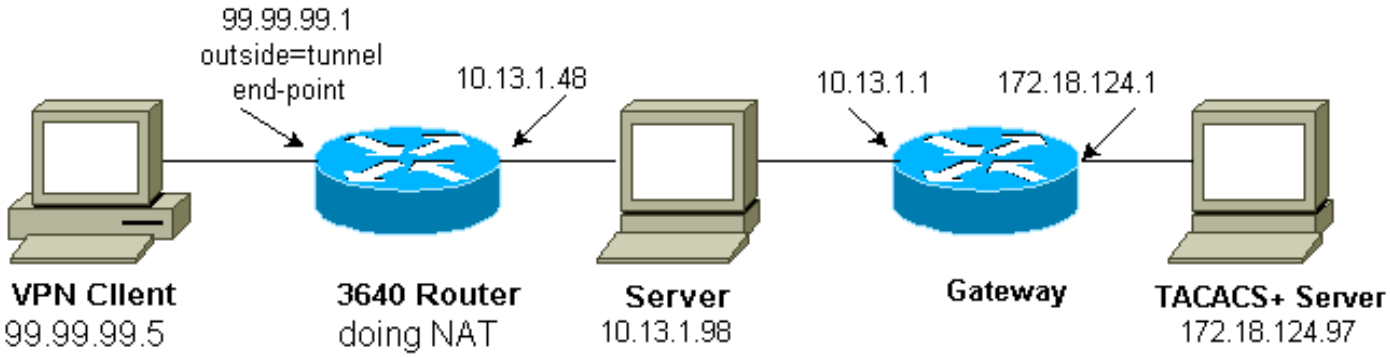
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の設定を使用しています。

Cisco 3640 ルータの設定

```
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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

トラブルシューティングの情報は、『認証プロキシのトラブルシューティング』を参照してください。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

関連情報

- Cisco VPN Client
- IPSec ネゴシエーション/IKE プロトコル
- Cisco IOS Firewallテクニカルサポート
- テクニカル サポートとドキュメント – Cisco Systems