Configuration avec NAT et Cisco IOS Firewall de l'authentification des utilisateurs entrants par proxy d'authentification, avec IPsec et VPN Client

Contenu

Introduction

Cet exemple de configuration permet à un client VPN d'accéder à un serveur sur un autre réseau via un tunnel IPsec, une fois l'authentification de l'utilisateur réussie.

Un PC à l'adresse 99.99.99.5 active le navigateur Web pour accéder au contenu sur le serveur à l'adresse 10.13.1.98. Puisque le client VPN sur le PC est configuré pour passer par le point d'extrémité 99.99.99.1 du tunnel pour accéder au réseau 10.13.1.x, le tunnel IPsec est construit et le PC obtient l'adresse IP du pool appelé « ourpool » (puisque vous faites la configuration en mode). Le routeur 3640 demande l'authentification. Une fois que l'utilisateur a entré un nom d'utilisateur et un mot de passe (stockés sur le serveur TACACS+ à l'adresse 172.18.124.97), la liste d'accès transmise depuis le serveur est ajoutée à la liste d'accès 117.

Remarque : La commande **ip auth-proxy** a été introduite dans le logiciel Cisco IOS® Version 12.0.5.T.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS Version 12.0.7.T
- Routeur Cisco 3640 (c3640-jo3s56i-mz.121-2.3.T)
- Cisco Secure VPN Client 1.0 (voir 2.0.7 dans le menu Aide du client IRE > À propos) ou Cisco Secure VPN Client 1.1 (voir 2.1.12 dans le menu Aide du client IRE > À propos)

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

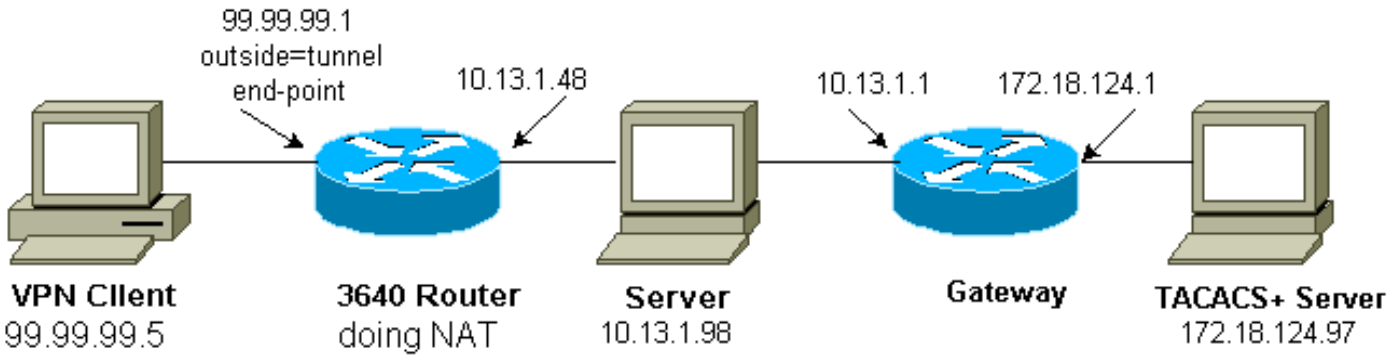
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise la configuration suivante :

Configuration du routeur Cisco 3640

`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
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Référez-vous à Dépannage du proxy d'authentification pour des informations de dépannage.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Informations connexes

- Client VPN Cisco
- Négociation IPSec/Protocoles IKE
- Assistance technique Cisco IOS Firewall
- Support et documentation techniques - Cisco Systems