Eingehende Auth-Proxy-Authentifizierung mit IPsec- und VPN-Client-Konfiguration mit NAT und Cisco IOS-Firewall

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Konfigurieren
Netzwerkdiagramm
Konfigurationen
Überprüfen
Fehlerbehebung
Zugehörige Informationen

Einführung

Mit dieser Beispielkonfiguration kann ein VPN-Client nach erfolgreicher Benutzerauthentifizierung über einen IPsec-Tunnel auf einen Server in einem anderen Netzwerk zugreifen.

Ein PC mit der Nummer 99.99.99.5 ruft den Webbrowser auf, um unter 10.13.1.98 auf Inhalte des Servers zuzugreifen. Da der VPN-Client auf dem PC so konfiguriert ist, dass er den Tunnel-Endpunkt 99.99.99.1 durchläuft, um zum 10.13.1.x-Netzwerk zu gelangen, wird der IPsec-Tunnel erstellt, und der PC erhält die IP-Adresse aus dem Pool "ourpool" (da Sie die Modus-Konfiguration durchführen). Der Router 3640 fordert eine Authentifizierung an. Nachdem der Benutzer einen Benutzernamen und ein Kennwort eingegeben hat (auf dem TACACS+-Server unter 172.18.124.97 gespeichert), wird die vom Server übergebene Zugriffsliste der Zugriffsliste 117 hinzugefügt.

Hinweis: Der Befehl **ip auth-proxy** wurde in Cisco IOS® Softwareversion 12.0.5.T eingeführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Softwareversion 12.0.7.T
- Cisco 3640-Router (c3640-jo3s56i-mz.121-2.3.T)
- Cisco Secure VPN Client 1.0 (im Menü IRE Client Help > About (Hilfe des IRE-Clients > Info) als 2.0.7 angezeigt) oder Cisco Secure VPN Client 1.1 (im Menü IRE Client Help (Hilfe des IRE-Clients > Info) als 2.1.12 angezeigt)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

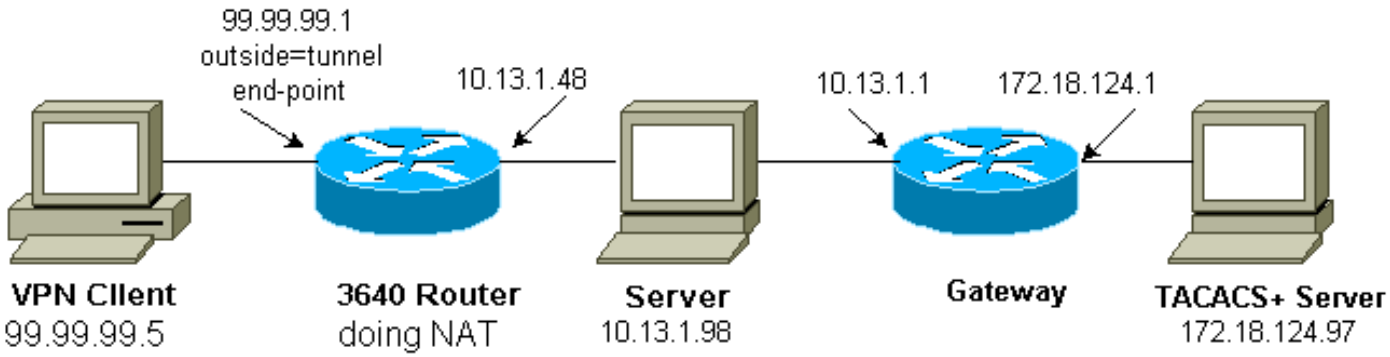
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument wird diese Konfiguration verwendet:

Konfiguration des Cisco 3640 Routers

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Informationen zur Fehlerbehebung finden Sie unter Troubleshooting Authentication Proxy (Authentifizierungsproxy).

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Zugehörige Informationen

- Cisco VPN-Client
- IPSec-Aushandlung/IKE-Protokolle
- Technischer Support für Cisco IOS Firewall
- Technischer Support und Dokumentation - Cisco Systems