Router und VPN-Client für das öffentliche Internet auf einem Stick-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Router am zentralen Standort einrichten, um IPsec-Datenverkehr auf einem Stick auszuführen. Diese Konfiguration gilt für einen bestimmten Fall, in dem der Router ohne Aktivierung von Split-Tunneling und mobile Benutzer (Cisco VPN-Client) über den Router am zentralen Standort auf das Internet zugreifen können. Um dies zu erreichen, konfigurieren Sie die Richtlinienzuordnung im Router so, dass der gesamte VPN-Datenverkehr (Cisco VPN Client) auf eine Loopback-Schnittstelle verweist. Dadurch kann der Internetdatenverkehr als Port-Adresse übersetzt (PATed) an die Außenwelt übertragen werden.

Weitere Informationen zu einer Konfiguration auf einer PIX-Firewall finden Sie unter PIX/ASA 7.x und VPN-Client für Public Internet VPN in einem Stick Configuration Example.

Hinweis: Um Überschneidungen bei IP-Adressen im Netzwerk zu vermeiden, weisen Sie dem VPN-Client den völlig unterschiedlichen Pool von IP-Adressen zu (z. B. 10.x.x.x, 172.16.x.x, 192.168.x.x). Dieses IP-Adressierungsschema unterstützt Sie bei der Fehlerbehebung im Netzwerk.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco Router 3640 mit Cisco IOS® Softwareversion 12.4
- Cisco VPN-Client 4.8

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).

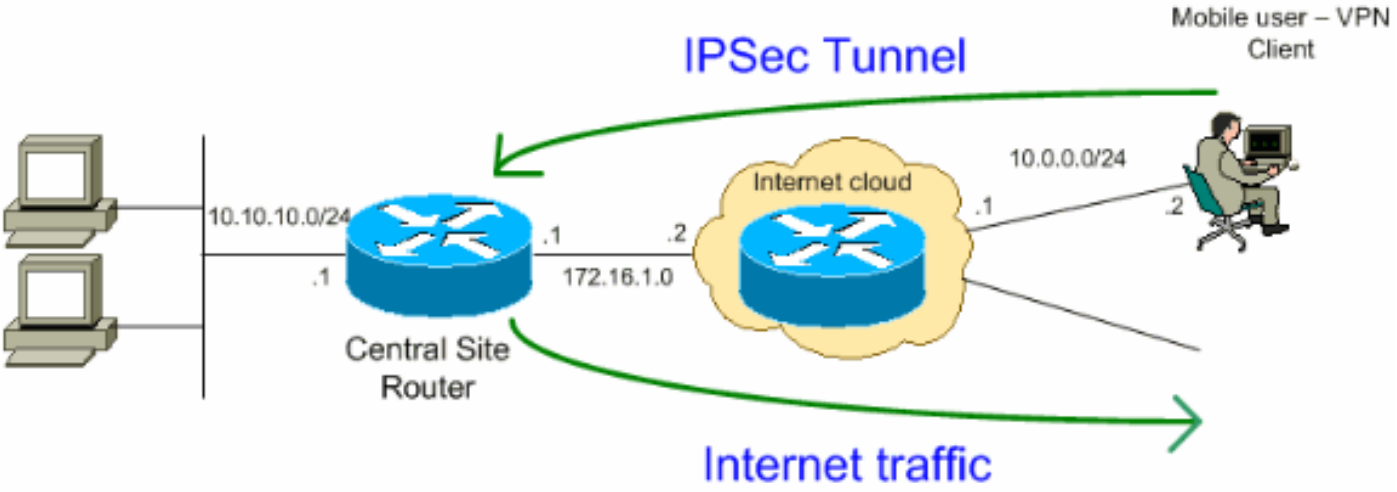
Konfigurieren

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:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet werden.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Router
- Cisco VPN-Client

Router

```
 VPN#show run
Building configuration...

Current configuration : 2170 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN
!
boot-start-marker
boot-end-marker
!
!
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
!--- In order to enable Xauth for user authentication,
!--- enable the aaa authentication commands.


aaa authentication login userauthen local

!--- In order to enable group authorization, enable !---
the aaa authorization commands.

aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!--- For local authentication of the IPsec user, !---
create the user with a password. username user password
0 cisco
!
!
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2

!--- Create a group that is used to specify the !---
WINS and DNS server addresses to the VPN Client, !---
along with the pre-shared key for authentication. crypto
isakmp client configuration group vpnclient
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
```

```
 domain cisco.com
 pool ippool
!
!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!

!--- Create a dynamic map and apply !--- the transform
set that was created earlier. crypto dynamic-map dynmap
10
 set transform-set myset
 reverse-route
!

!--- Create the actual crypto map, !--- and apply the
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
!--- Create the loopback interface for the VPN user
traffic . interface Loopback0
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
 ip nat inside

!--- Apply the crypto map on the interface. interface
FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 ip policy route-map VPN-Client
 duplex auto
 speed auto
 crypto map clientmap
!
interface Serial2/0
 no ip address
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!--- Create a pool of addresses to be !--- assigned to
the VPN Clients. ! ip local pool ippool 192.168.1.1
```

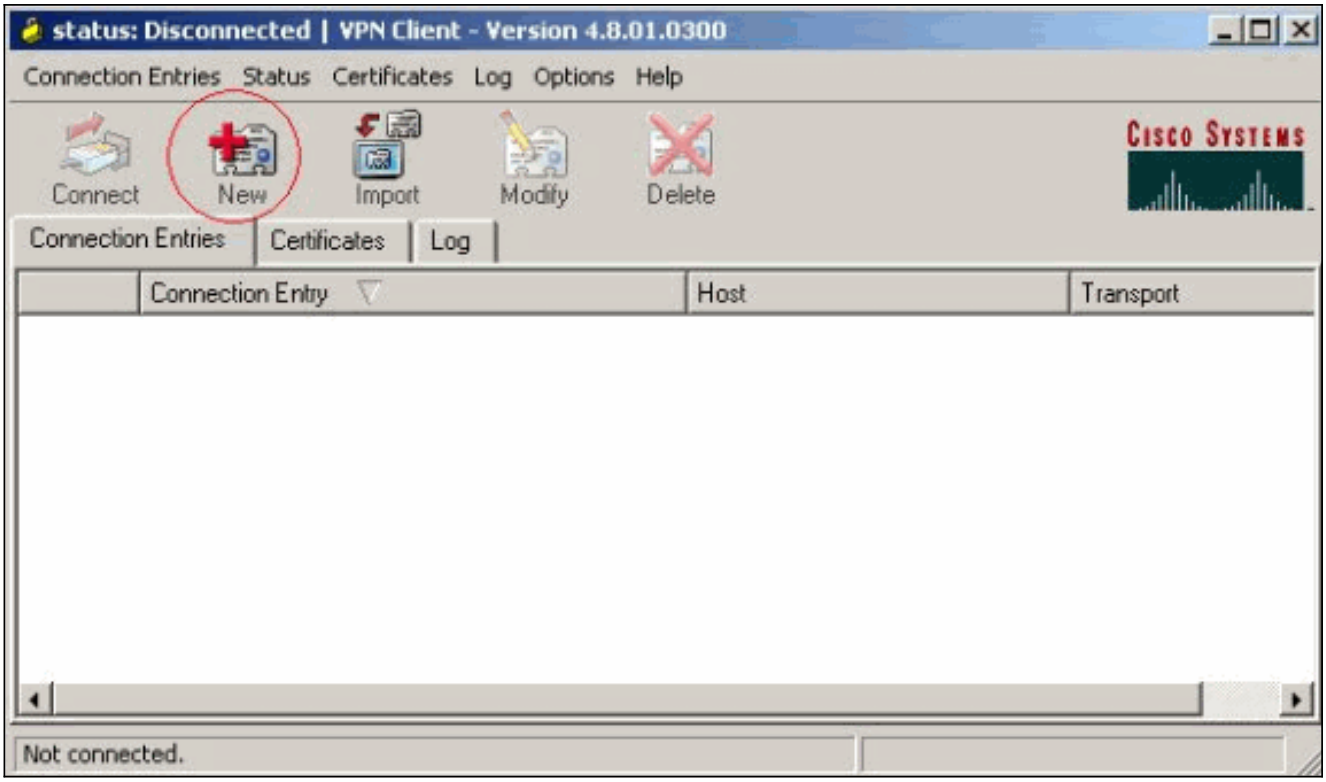
```
192.168.1.2
ip http server
no ip http secure-server
!
ip route 10.0.0.0 255.255.255.0 172.16.1.2
!--- Enables Network Address Translation (NAT) !--- of
the inside source address that matches access list 101
!--- and gets PATed with the FastEthernet IP address. ip
nat inside source list 101 interface FastEthernet1/0
overload
!
!--- The access list is used to specify which traffic is
to be translated for the !--- outside Internet. access-
list 101 permit ip any any

!--- Interesting traffic used for policy route. access-
list 144 permit ip 192.168.1.0 0.0.0.255 any
!--- Configures the route map to match the interesting
traffic (access list 144) !--- and routes the traffic to
next hop address 10.11.0.2. ! route-map VPN-Client
permit 10
 match ip address 144
 set ip next-hop 10.11.0.2
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
end
```

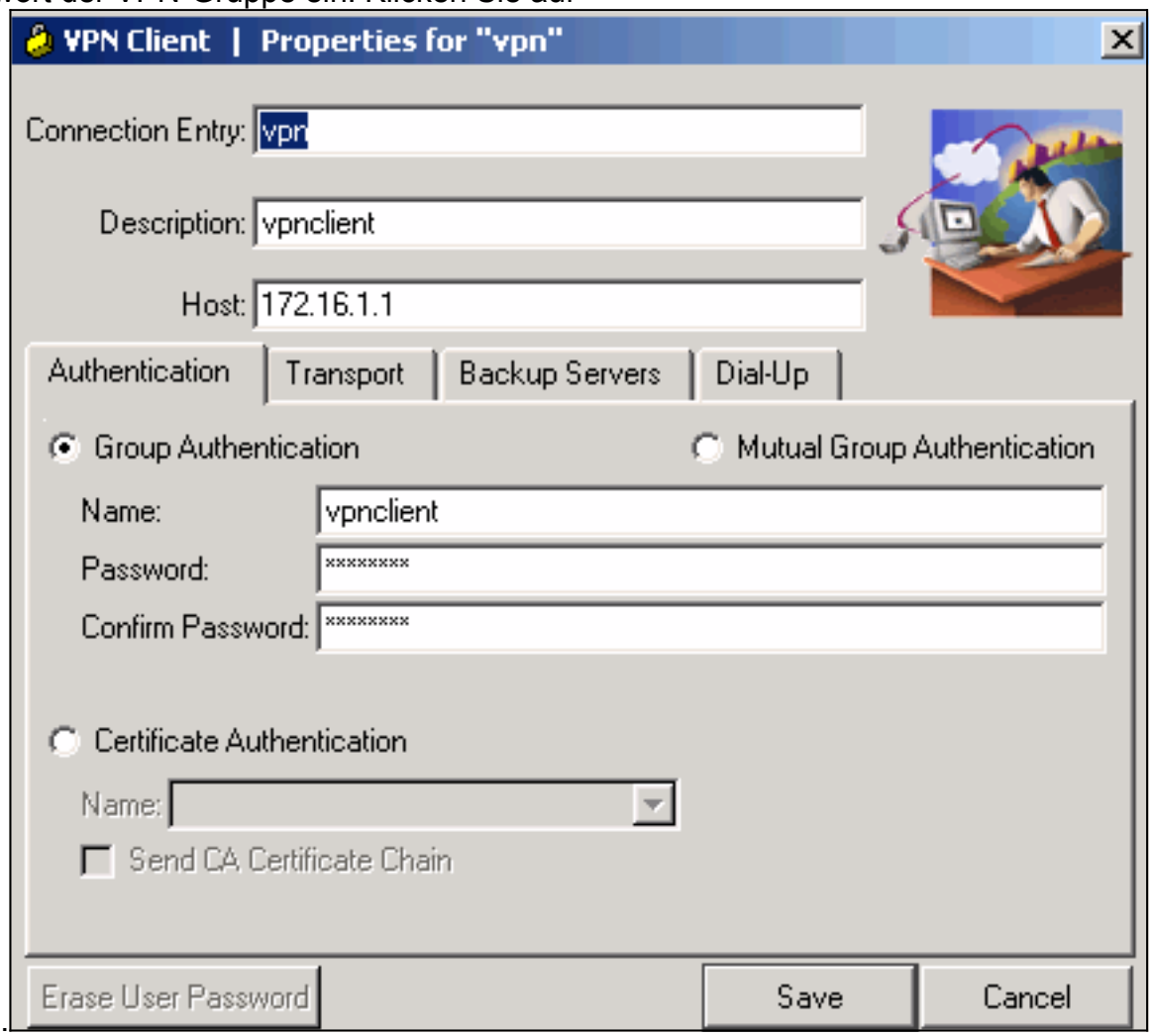
Konfiguration des VPN-Clients 4.8

Führen Sie diese Schritte aus, um den VPN-Client 4.8 zu konfigurieren.

1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > VPN Client aus**.
2. Klicken Sie auf **Neu**, um das Fenster Create New VPN Connection Entry (Neue VPN-Verbindung erstellen) zu
   öffnen.

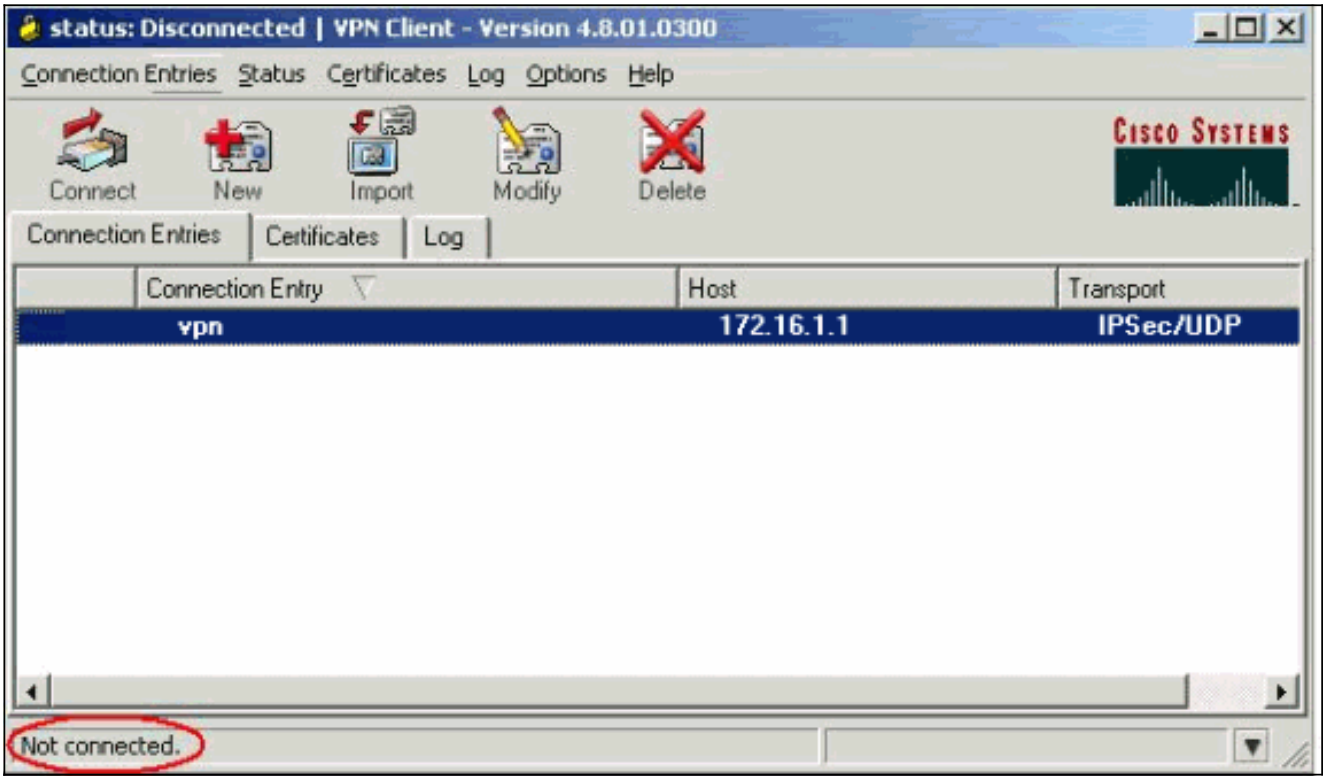


3. Geben Sie den Namen des Connection Entry zusammen mit einer Beschreibung ein, geben Sie die externe IP-Adresse des Routers im Host-Feld ein, und geben Sie den Namen und das Kennwort der VPN-Gruppe ein. Klicken Sie auf **Speichern**.

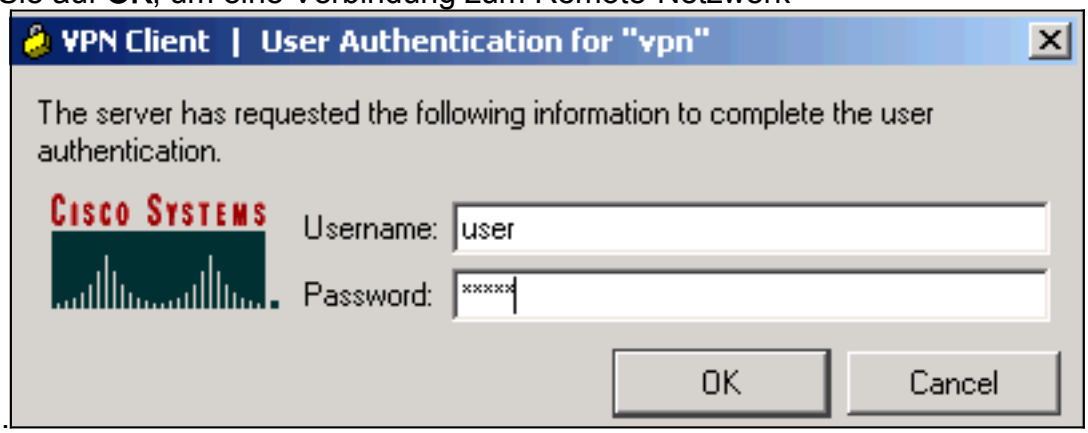


4. Klicken Sie auf die Verbindung, die Sie verwenden möchten, und klicken Sie im Hauptfenster des VPN-Clients auf

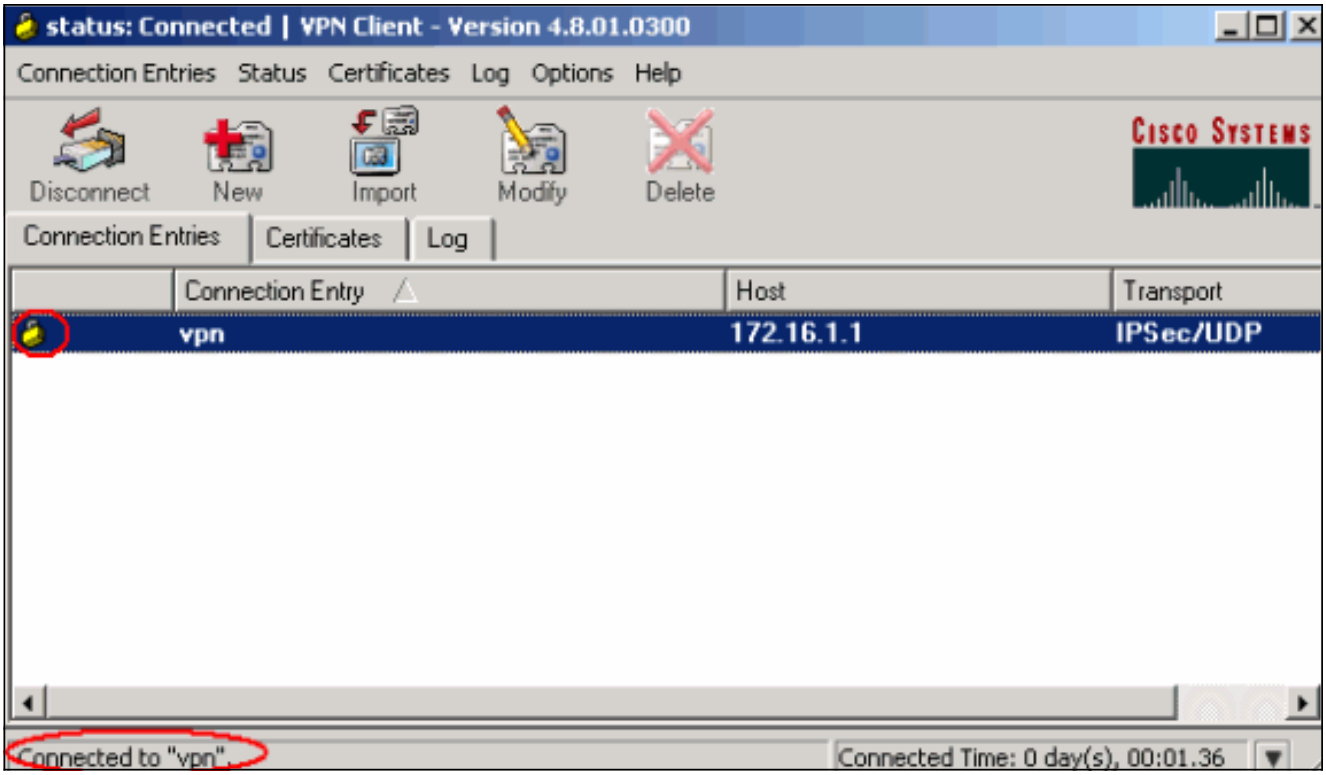
Verbinden.



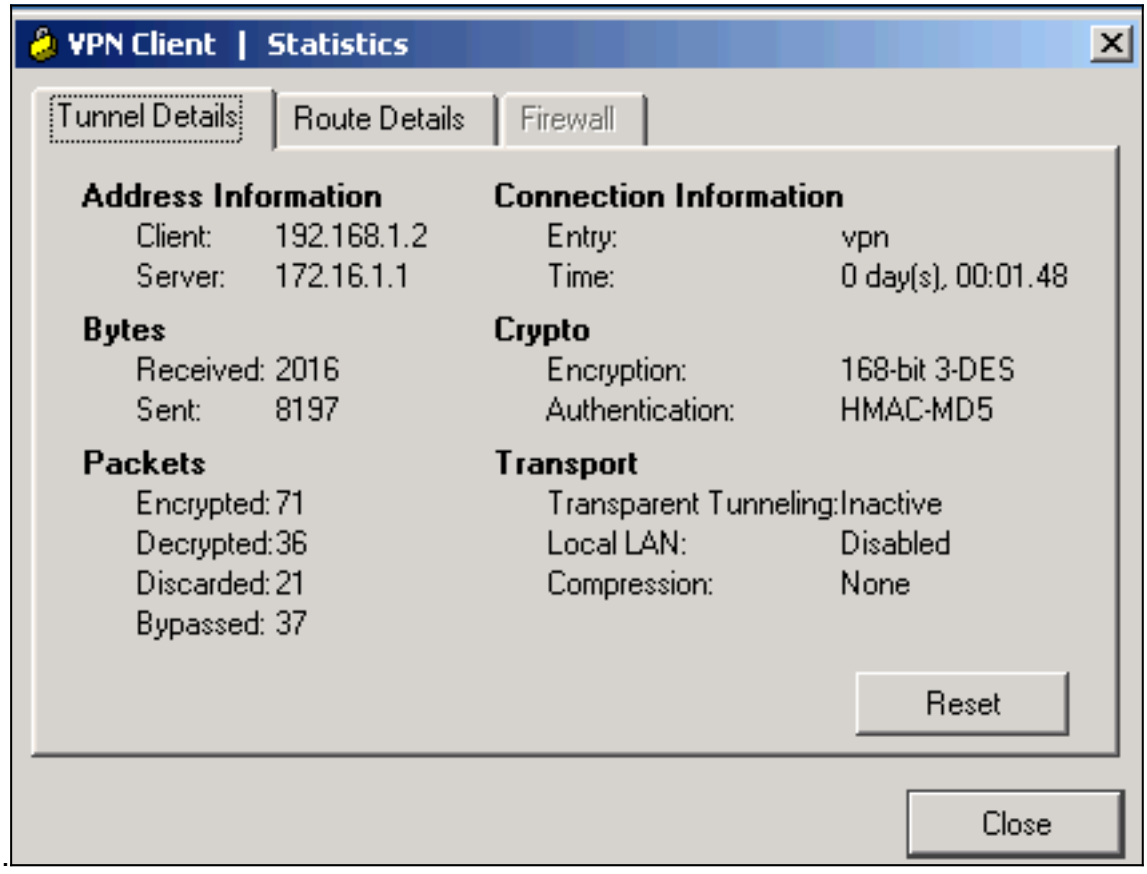
5. Geben Sie bei Aufforderung die Informationen zu Benutzername und Kennwort für Xauth ein, und klicken Sie auf **OK**, um eine Verbindung zum Remote-Netzwerk herzustellen.



6. Der VPN-Client wird mit dem Router in der Zentrale verbunden.



7. Wählen Sie **Status > Statistics (Status > Statistik)**, um die Tunnelstatistiken des VPN-Clients zu überprüfen.



Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle.

Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE Security Associations (SAs) in einem Peer an.

```
VPN#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: clientmap, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={}
    #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270
    #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0xEF7C20EA(4017889514)

     inbound esp sas:
      spi: 0x17E0CBEC(400608236)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: clientmap
        sa timing: remaining key lifetime (k/sec): (4530341/3288)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xEF7C20EA(4017889514)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: clientmap
        sa timing: remaining key lifetime (k/sec): (4530354/3287)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto ipsec sa**: Zeigt die von aktuellen SAs verwendeten Einstellungen.

```
VPN#show crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.1      10.0.0.2        QM_IDLE              15    0 ACTIVE
```

Fehlerbehebung

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

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

- **debug crypto ipsec**: Zeigt die IPsec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen von Phase 1 an.

Zugehörige Informationen

- IPsec-Aushandlung/IKE-Protokolle
- Cisco VPN Client - Produktsupport
- Cisco Router - Produktsupport
- Technischer Support und Dokumentation - Cisco Systems