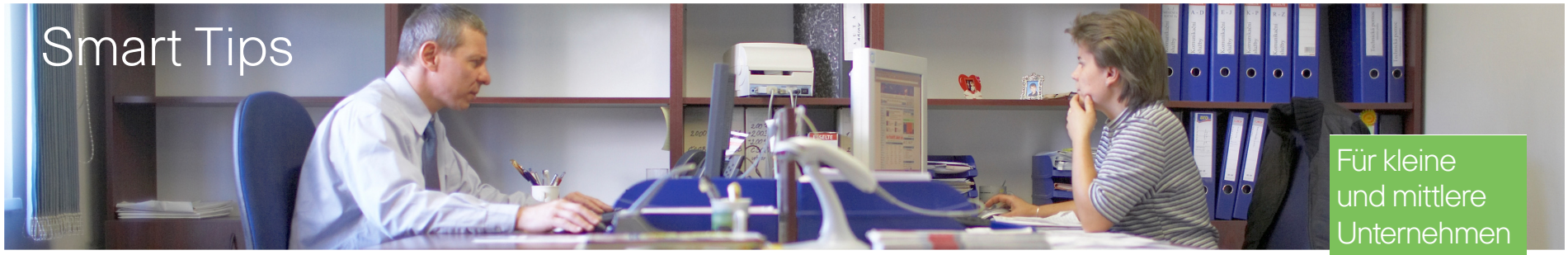


Konfiguration von PPTP VPN

Das Point-to-Point Tunneling Protocol (PPTP) ist eine Netzwerktechnologie, die VPNs (Virtual Private Networks) unterstützt. Damit kann Remote-Benutzern der sichere Zugriff auf das Unternehmensnetzwerk über das Internet ermöglicht werden. Der PPTP-VPN-Client ist für alle Microsoft Windows-Versionen, Macintosh OS X, Linux sowie sämtliche Mobilgeräte wie das iPhone geeignet.

Da die Router der Cisco Small Business RV-Serie den PPTP-Server unterstützen und die meisten Betriebssysteme über einen integrierten PPTP-VPN-Client verfügen, bietet die PPTP-VPN-Lösung eine einfache, schnelle und sichere Möglichkeit für kleine und mittlere Unternehmen, ihre Netzwerkressourcen praktisch jedem Benutzer verfügbar zu machen, der Zugang zum Internet hat. Darüber hinaus bestehen keinerlei Exportbeschränkungen hinsichtlich der Verschlüsselungstechnologien für PPTP-VPN.

PPTP ist ein Layer 2-Tunneling-Protokoll, das das IP-Paket tunnelt. Das PPTP-Protokoll wird im RFC 2637 beschrieben. PPTP arbeitet auf der Grundlage eines Client-Server-Modells mit einem Control Channel über TCP (TCP-Port 1723) und einem Generic Routing Encapsulation Tunnel (IP-Protokoll 47), der PPP-Pakete einkapselt. Obwohl neuere VPN-Technologien wie SSL VPN und IPsec VPN sicherer sind als PPTP, ist PPTP nach wie vor ein beliebtes und weit verbreitetes Netzwerkprotokoll.

Produkte

- Cisco RV110W Wireless Network Security Firewall Router (das in diesem Dokument verwendete Beispiel)
- Cisco RV120W Wireless-N Network VPN Firewall Router
- Cisco RV220W Wireless-N Network Security Firewall Router

Hauptmerkmale

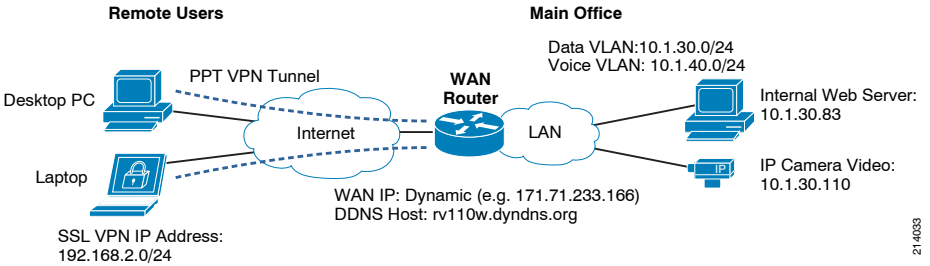
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) – Der getunnelte PPP-Datenverkehr kann mit PAP, CHAP, Microsoft CHAP v1/v2 oder EAP authentifiziert werden. Im Cisco Small Business Router der RV-Serie wird MS-CHAPv2 für die PPP-Authentifizierung verwendet. MS-CHAPv2 ist eine gegenseitige Authentifizierung mit einem unidirektional verschlüsselten Kennwort.
- Microsoft Point-to-Point Encryption (MPPE) – MPPE ist eine von Microsoft für die Verschlüsselung des PPP-Payloads entwickelte Technologie. Diese PPP-Verbindungen können über eine Einwahlleitung oder einen VPN-Tunnel hergestellt werden. MPPE ist eine Unterfunktion von Microsoft Point-to-Point Compress (MPPC). MPPE verwendet den RC4-Algorithmus mit 40-Bit- oder 128-Bit-Schlüsseln. Alle Schlüssel werden aus dem Klartext-Authentifizierungskennwort des Benutzers abgeleitet. MPPE erfordert MS-CHAPv1/v2 oder EAP. Die Cisco Router der RV-Serie unterstützen die MPPE 128-Bit-Verschlüsselung als erweiterte Option.

Netzwerkdiagramm

Abbildung 1 zeigt eine Beispielimplementierung für ein PPTP-VPN mit einem Cisco Small Business-Router der Serie RV110W. Mobile Benutzer stellen über einen sicheren PPTP VPN-Tunnel mit einem PPTP VPN-Router eine Verbindung her und können dann auf interne Server und Netzwerkressourcen zugreifen. Diese sind in der Regel durch eine Firewall, die auf dem Cisco WAN-Router ausgeführt wird, vor öffentlichen Zugriffen geschützt.

Der Cisco WAN-Router stellt darüber hinaus Routing-Funktionen zwischen unterschiedlichen VLANs zur Verfügung, darunter das Daten-VLAN (30), das Sprach-VLAN (40) und das Verwaltungs-VLAN (60). Im vorliegenden Beispiel umfasst das Daten-VLAN einen internen Webserver (10.1.30.100) und eine IP-Videokamera (10.1.30.110).

Abbildung 1 PPTP VPN mit einem Cisco Small Business Router der Serie RV220



Konfiguration eines PPTP VPN-Servers auf einem Cisco Small Business Router der Serie RV110W

Checkliste für die Vorkonfiguration

Weitere Informationen zum Abschluss der Erstkonfiguration des Routers der Serie RV10W finden Sie im RV110W Administratorhandbuch.

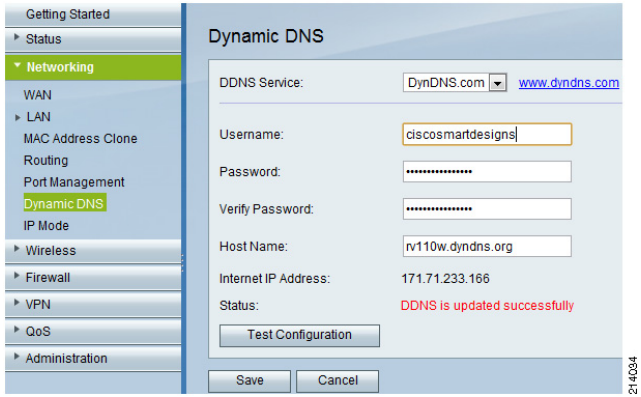
1. Stellen Sie sicher, dass der WAN-Router über eine aktive Internetverbindung verfügt. Die Network Address Translation (NAT) und eine Firewall sollten aktiviert sein.
2. Stellen Sie sicher, dass die LAN-Verbindung zwischen Router, Switch und den lokalen IP-Geräten besteht. Die Daten-, Sprach- und Verwaltungs-VLANs auf dem RV-Router und den Switches müssen ordnungsgemäß konfiguriert sein. Die VLAN-weiten Routing- und Trunking-Funktionen für die einzelnen VLANs müssen funktionsfähig sein. Außerdem muss der DHCP-Service für jedes VLAN funktionsfähig sein.
3. Stellen Sie sicher, dass die internen PCs, Server und anderen IP-Geräte mit dem LAN-Switch oder den Switch-Ports des RV-Routers verbunden sind. Vergewissern Sie sich, dass die PCs und Server miteinander kommunizieren und auf das öffentliche Internet zugreifen können.

Aktivierung des DDNS (Optional)

Wenn eine statische WAN-IP-Adresse verwendet wird oder der DDNS-Service (Dynamic Domain Name System) auf dem WAN-Router bereits konfiguriert ist, überspringen Sie diesen Schritt. Wenn die WAN-Schnittstelle eine dynamische IP-Adresse vom Service Provider erhält, kann DDNS für den Client verwendet werden, damit dieser mithilfe eines Hostnamens auf den PPTP VPN-Server zugreifen kann.

Schritt 1 Gehen Sie zu **Networking** > **Dynamic DNS**, um die DDNS-Einstellungen zu konfigurieren (siehe Abbildung 2). Weitere Einzelheiten finden Sie unter Smart Tips: Aktivieren des öffentlichen WAN-Zugriffs mit DDNS und Port Forwarding.

Abbildung 2 Topologie der Small Business Link Aggregation Group (LAG)



Konfiguration des PPTP VPN-Servers

Zu Beginn muss der PPTP-Server auf dem Cisco Router der RV-Serie aktiviert werden. Auch das Benutzerkonto muss auf dem Router erstellt werden.

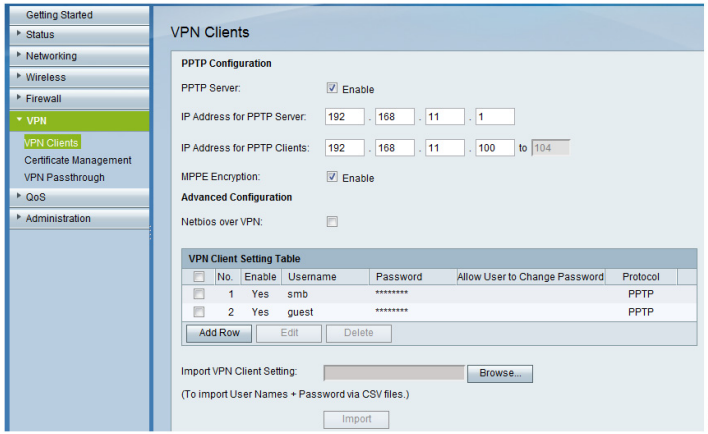
Schritt 1 Gehen Sie zu **VPN > VPN Clients**, und markieren Sie das Kontrollkästchen, um den PPTP-Server zu aktivieren (siehe Abbildung 3).

Schritt 2 Ändern Sie die IP-Adresse für den PPTP-Server und den Client. In diesem Beispiel wird 192.168.11.1 für den PPTP-Server und 192.168.11.100 für die anfängliche IP-Adresse der PPTP-Clients verwendet (Die abschließende IP-Adresse der PPTP-Clients wird automatisch ausgefüllt).

Schritt 3 Markieren Sie das Kontrollkästchen, um **MPPE Encryption (MMPE-Verschlüsselung) zu aktivieren.** Die Verschlüsselung wird nachdrücklich empfohlen.

Schritt 4 Klicken Sie auf **Add Row (Zeile hinzufügen)**, um den Namen und das Kennwort des PPTP-Client-Kontos hinzuzufügen. Markieren Sie das Aktivierungskontrollkästchen und wählen Sie unter Protocol (Protokoll) die Option **PPTP** aus.

Abbildung 3 PPTP-Konfigurationsbildschirm



Verbindung zum PPTP-Server von einem PC/Laptop mit Windows 7

Alle Windows-Betriebssysteme verfügen über einen integrierten PPTP-Client. In diesem Abschnitt finden Sie eine schrittweise Anleitung zur Verwendung des PPTP-Clients in Windows 7.

Schritt 1 Öffnen Sie auf dem Windows 7 Client-PC oder -Laptop, der mit dem Internet verbunden ist, das Netzwerk- und Freigabecenter, indem Sie auf das Taskleistensymbol für die Netzwerkverbindung (siehe Abbildung 4) klicken und **Netzwerk- und Freigabecenter öffnen** auswählen. Sie können das Netzwerk- und Freigabecenter auch über die Systemsteuerung starten.

Abbildung 4 Taskleistensymbol für eine Kabelverbindung (links) und eine kabellose Verbindung (rechts)

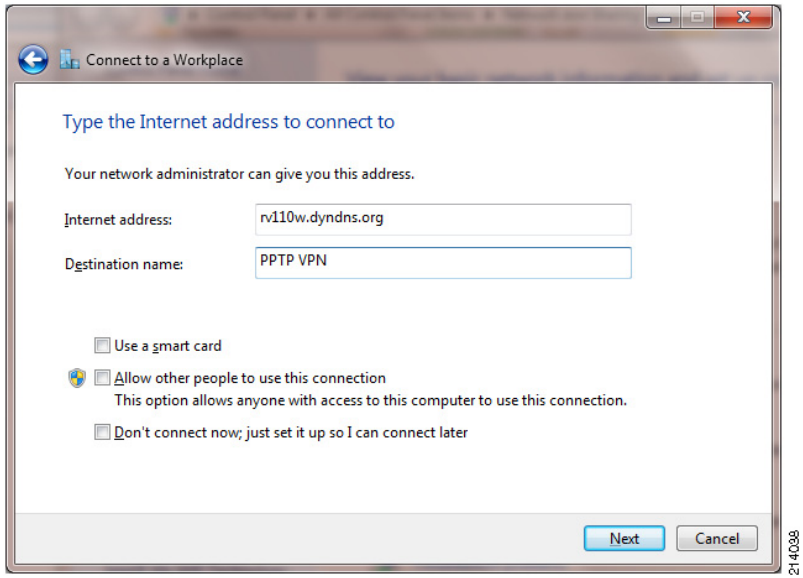
Schritt 2 Gehen Sie im Netzwerk- und Freigabecenter wie folgt vor:

a. Wählen Sie **Neue Verbindung oder neues Netzwerk einrichten**.
b. Wählen Sie im Popup-Fenster **Verbindung zum Arbeitsplatz (Richtet eine Wähl- oder VPN-Verbindung mit dem Arbeitsplatz ein.)**.
c. Klicken Sie auf **Weiter**.
d. Wählen Sie **Die Internetverbindung (VPN) verwenden**.

Schritt 3 Gehen Sie im Fenster „Verbindung zum Arbeitsplatz“ wie folgt vor:

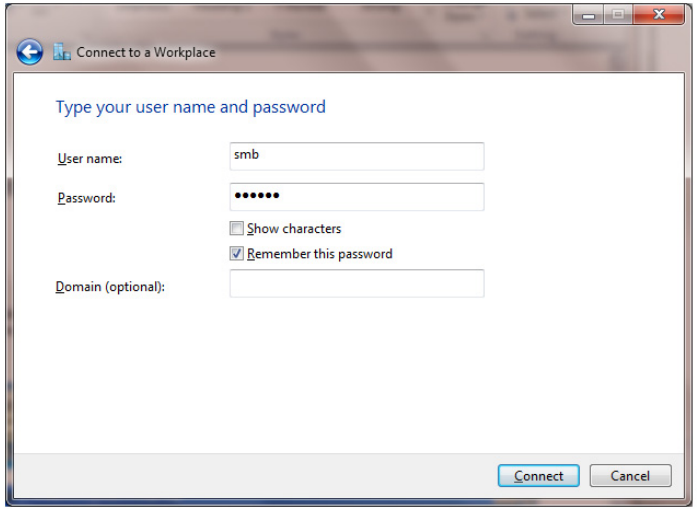
a. Geben Sie die Internetadresse oder den Hostnamen des PPTP VPN-Servers ein (siehe Abbildung 5). In diesem Beispiel wird die Internetadresse *rv110w.dyndns.org* verwendet.

Abbildung 5 Verbindung mit einem Arbeitsplatz



b. Klicken Sie auf **Weiter**.
c. Geben Sie den Benutzernamen und das Kennwort für den PPTP-Client (siehe Abbildung 6) ein, und klicken Sie auf **Verbinden**.

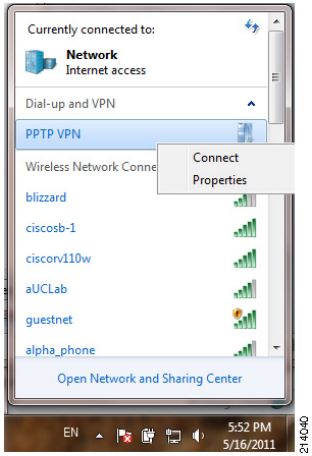
Abbildung 6 Eingabe von Benutzername und Kennwort



Schritt 4 Möglicherweise schlägt die Verbindung fehl, und die Fehlermeldung „Der lokale Computer unterstützt den angeforderten Datenverschlüsselungstyp nicht“ wird angezeigt. Ignorieren Sie diese Fehlermeldung, und klicken Sie auf **Verbindung dennoch einrichten**, um die Einrichtung abzuschließen. Nehmen Sie dann die Authentifizierungs- und Verschlüsselungseinstellungen manuell vor.

Schritt 5 Klicken Sie wie in Schritt 1 auf das Taskleistensymbol für die Netzwerkverbindungen. Die neu erstellte PPTP-Verbindung (in diesem Beispiel mit der Bezeichnung PPTP VPN) wird in den Kategorien Einwahl und VPN angezeigt. Klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften** (siehe Abbildung 7).

Abbildung 7 Derzeit verbunden mit



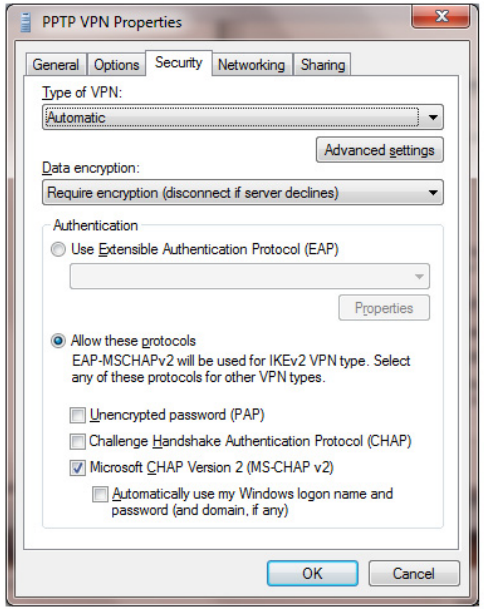
Schritt 6 Gehen Sie im Fenster „Eigenschaften“ wie folgt vor:

a. Wählen Sie die Registerkarte **Sicherheit** (siehe Abbildung 8).

b. Entfernen Sie die Markierung bei **Challenge Handshake Authentication-Protokoll (CHAP)**, lassen Sie **Microsoft CHAP, Version 2 (MS-CHAPv2)** markiert, und achten Sie darauf, dass für die Datenverschlüsselung **Erforderlich (Verbindung trennen, falls Server dies ablehnt)** eingestellt ist.

c. Klicken Sie auf **OK**, um den Vorgang abzuschließen.

Abbildung 8 PPTP VPNJ-Eigenschaften

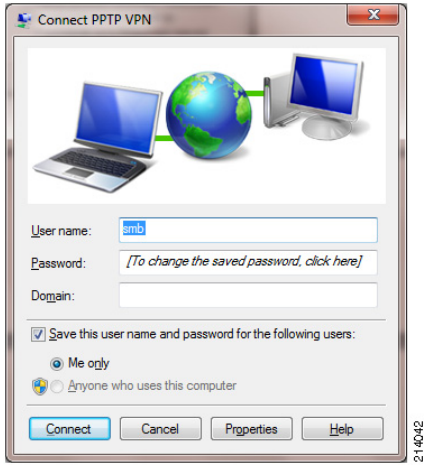


Schritt 7 Klicken Sie wie in Schritt 1 auf das Taskleistensymbol für die Netzwerkverbindungen, und gehen Sie wie folgt vor:

a. Klicken Sie auf die PPTP-Verbindung (in diesem Beispiel als PPTP VPN bezeichnet).

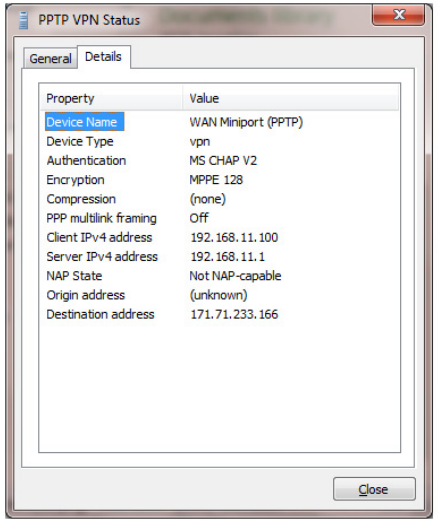
b. Klicken Sie mit der linken Maustaste, und wählen Sie **Verbinden**. Das Anmeldefenster wird angezeigt (siehe Abbildung 9). Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie auf die Schaltfläche **Verbinden**. Die Verbindung sollte erfolgreich hergestellt werden.

Abbildung 9 Anmeldung für die PPTP VPN-Verbindung



c. Wenn die PPTP VPN-Verbindung hergestellt ist, klicken Sie mit der rechten Maustaste auf die PPTP-Verbindung, und wählen Sie **Status**. Wählen Sie im Status-Fenster (siehe Abbildung 10) die Registerkarte **Details**. Der Bildschirm zeigt die korrekte Verschlüsselungs- und Authentifizierungsart sowie die zugewiesene Client-IP-Adresse an. In diesem Beispiel verwendet der PPTP-Client MS CHAPv2 für die Authentifizierung, MPPE 128 für die Verschlüsselung und 192.168.11.100 als Client-IP-Adresse.

Abbildung 10 PPTP-VPN Status – Details



Verbindung zum PPTP-Server mit Mac OS 10.5

Schritt 1 Wählen Sie **Apple-Menü > Systemeinstellungen > Netzwerk**, und klicken Sie auf die Schaltfläche **+**, um eine neue Netzwerkverbindung hinzuzufügen.

Schritt 2 Gehen Sie im Fenster „Netzwerk“ wie folgt vor:

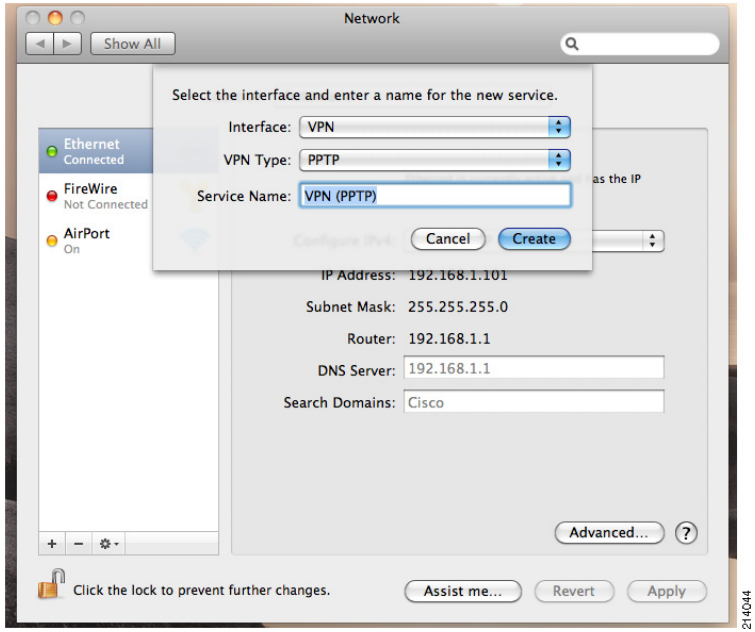
a. Wählen Sie als Anschluss **VPN**.

b. Wählen Sie als VPN-Typ **PPTP**.

c. Geben Sie als Dienstnamen einen beliebigen Namen ein (in diesem Beispiel VPN PPTP).

d. Klicken Sie zum Fortfahren auf die Schaltfläche **Erstellen**.

Abbildung 11 Netzwerkverbindung



Schritt 3 Gehen Sie im nächsten Fenster (siehe Abbildung 12) wie folgt vor:

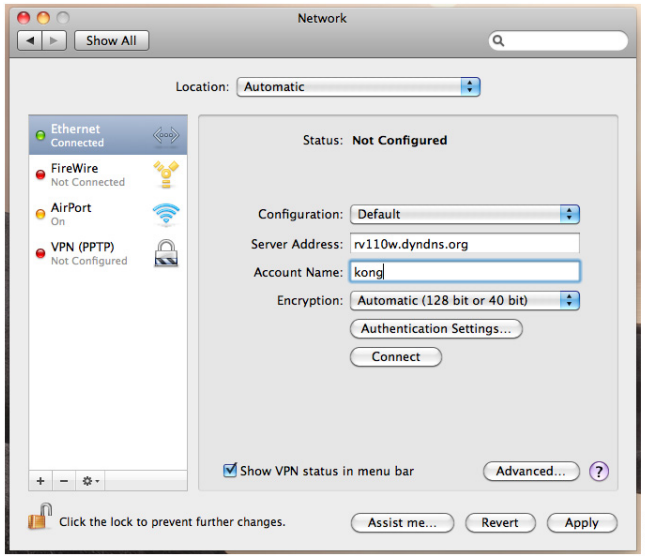
a. Geben Sie als Serveradresse die IP-Adresse oder den Hostnamen ein. In diesem Beispiel ist dies rv110w.dyndns.org.

b. Geben Sie als Account-Namen den PPTP VPN-Client-Benutzernamen ein.

c. Lassen Sie die anderen Standardeinstellungen unverändert; achten Sie darauf, dass die Verschlüsselung **Automatisch (128 Bit oder 40 Bit)** lautet und dass **VPN-Status in der Menüzeile anzeigen** ausgewählt ist.

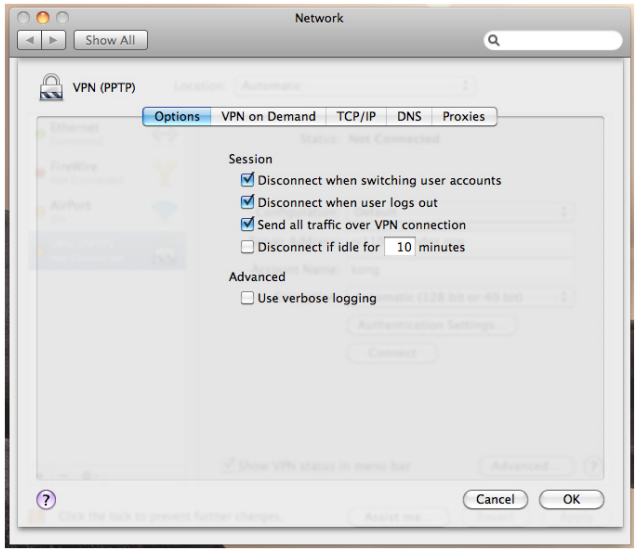
d. Klicken Sie auf **Anwenden**.

Abbildung 12 Netzwerkkonfiguration



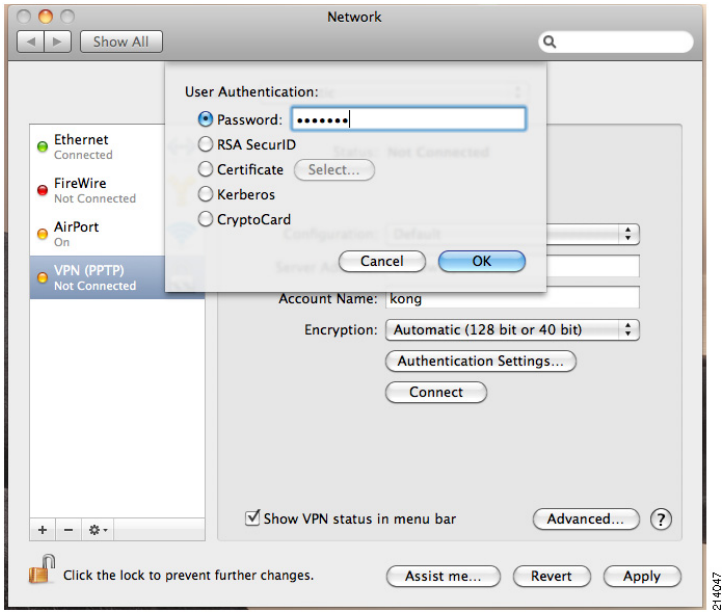
Schritt 4 Klicken Sie auf **Weitere Optionen**, und markieren Sie im Tab **Optionen Gesamten Verkehr über VPN senden** (siehe Abbildung 13). Klicken Sie auf **OK**.

Abbildung 13 Netzwerkoptionen



Schritt 5 (Optional) Wenn Sie möchten, dass Mac OS Ihr Kennwort speichert, klicken Sie auf die Schaltfläche **Authentifizierungseinstellungen**, und geben Sie das Kennwort ein (siehe Abbildung 14).

Abbildung 14 Authentifizierungseinstellungen



Sie haben ihre PPTP VPN-Verbindung erfolgreich eingerichtet. Klicken Sie auf **Verbinden**, um die Verbindung zum PPTP VPN-Server herzustellen.

Überwachen der PPTP VPN-Verbindungen auf dem Server

Als Administrator können Sie unter **Status** > **VPN-Status** den Status aller aktiven PPTP VPN-Clients überwachen (siehe Abbildung 15). Zu den Statusinformationen gehören der Name des Benutzers, die PPTP Client-IP-Adresse, Status, Start- und Endzeit, Dauer sowie das Protokoll. Der Administrator kann auch jede Verbindung mit der Schaltfläche „Verbindung trennen“ unterbrechen.

Abbildung 15 VPN-Status