

Konfiguration eines Gateway-to-Gateway-VPN-Tunnels mithilfe von DynDNS auf einer Seite des Tunnels auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziele

Ein Dynamic Domain Name System (DDNS) ermöglicht den Internetzugriff auf den Server über einen Domännennamen anstelle einer IP-Adresse. DDNS behält auch IP-Adressinformationen bei, selbst wenn der Client eine dynamische IP-Zuweisung erhält, die von ständigen Änderungen durch den ISP abhängig ist. Mit dieser Konfiguration ist der Server unabhängig von der IP-Adresse immer verfügbar. Dieser Dienst kann erst verwendet werden, nachdem Sie ein Konto bei einem DDNS-Dienstanbieter eingerichtet haben.

In diesem Dokument wird erläutert, wie Sie ein Gateway-to-Gateway-VPN mit DynDNS auf der lokalen Gruppenseite und eine statische IP mit registriertem Domännennamen auf der Remote-Gruppenseite für die VPN-Router RV016, RV042, RV042G und RV082 konfigurieren.

Unterstützte Geräte

RV016
RV042
RV042G
RV082

Software-Version

4.2.2.08



Konfiguration des VPN-Tunnels

DDNS konfigurieren

Schritt 1: Besuchen Sie www.dyndns.org, und registrieren Sie einen Domännennamen.

Schritt 2: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **Setup > Dynamic DNS aus**. Die Seite *Dynamic DNS* wird geöffnet.

Schritt 3: Klicken Sie auf das Symbol **Edit** (Bearbeiten) für WAN1.

Dynamic DNS			
Interface	Status	Host Name	Configuration
WAN1	Disabled	--	
WAN2	Disabled	--	

Die Seite *Edit Dynamic DNS Setup* (DDNS-Einrichtung bearbeiten) wird geöffnet:

Dynamic DNS

Edit Dynamic DNS Setup

Interface : WAN1

Service : DynDNS.org ▼

Username :

Password :

Host Name : . .

Internet IP Address : 0.0.0.0

Status :

Schritt 4: Wählen Sie **DynDNS.org** aus der Dropdown-Liste *Service* aus.

Schritt 5: Geben Sie im Feld *Benutzername* Ihren DynDNS.org Benutzernamen ein.

Schritt 6: Geben Sie im Feld *Password* (*Kennwort*) das Kennwort für den unter DynDNS.org registrierten Benutzernamen ein.

Schritt 7. Geben Sie Ihren Hostnamen in das Feld *Hostname* ein.

Hinweis: Die beiden verbleibenden Felder auf der Seite *Edit Dynamic DNS Setup* (*DDNS-Einrichtung bearbeiten*) zeigen Informationen an und sind nicht konfigurierbar:

↗ Internet-IP-Adresse - Zeigt die IP-Adresse des Routers an. Diese Adresse wird sich ändern, da sie dynamisch ist.

↗ Status - Zeigt den Status des DDNS an. Wenn ein Fehler auftritt, stellen Sie sicher, dass Sie die DDNS-Informationen richtig eingegeben haben.

Schritt 8: Klicken Sie auf **Speichern**.

Konfiguration eines VPN-Tunnels von Standort 1 zu Standort 2

Schritt 9. Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **VPN > Gateway to Gateway** aus. Die Seite *Gateway zu Gateway* wird geöffnet:

Gateway To Gateway

Add a New Tunnel

Tunnel No. : 1

Tunnel Name :

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address :

Remote Security Group Type : Subnet

IP Address :

Subnet Mask : 255.255.255.0

IPSec Setup

Keying Mode : IKE with Preshared key

Hinweis: Bevor Sie diese Seite verlassen, klicken Sie auf **Speichern**, um die Einstellungen zu speichern, oder auf **Abbrechen**, um sie rückgängig zu machen.

Schritt 10. Geben Sie im Feld *Tunnel Name* (*Tunnelname*) einen Namen für den VPN-Tunnel zwischen Standort 1 und Standort 2 ein.

Gateway To Gateway

Add a New Tunnel

Tunnel No. : 1

Tunnel Name :

Interface : WAN1

Enable :

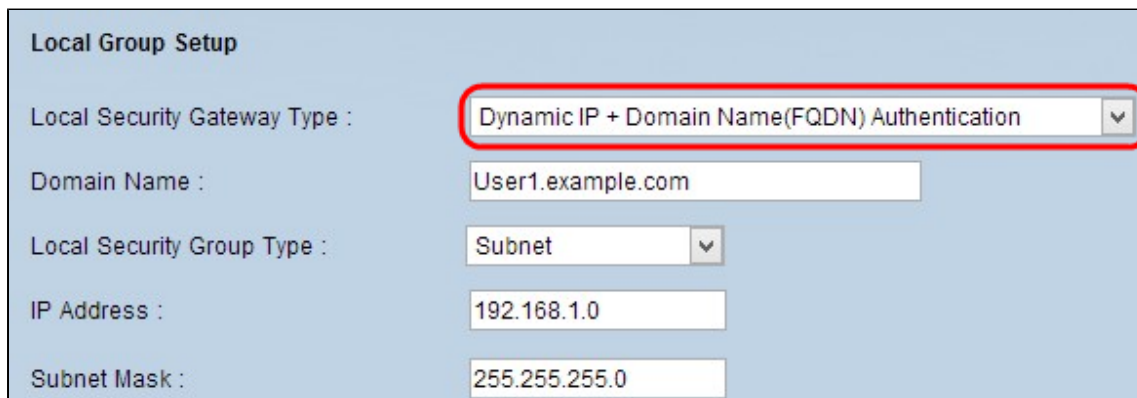
Hinweis: Der Tunnelname dient lediglich als Referenz und muss nicht mit dem Namen übereinstimmen, der am anderen Ende des VPN-Tunnels verwendet wird.

Schritt 11. Wählen Sie den WAN-Port aus der Dropdown-Liste *Interface* (*Schnittstelle*) aus, der für

diesen Tunnel verwendet werden soll.

Schritt 12: Aktivieren Sie **Enable**, um den VPN-Tunnel zu aktivieren. Das Kontrollkästchen wird deaktiviert, sobald der VPN-Tunnel erstellt wurde.

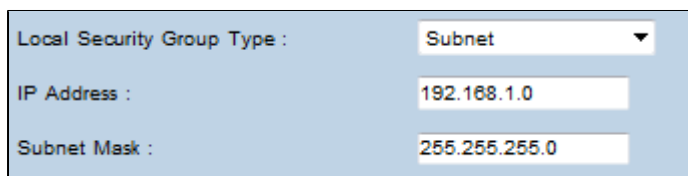
Schritt 13: Wählen Sie im Bereich *Local Group Setup (Lokale Gruppeneinrichtung)* in der Dropdown-Liste *Local Security Gateway Type (Lokaler Sicherheits-Gateway-Typ)* die Option **Dynamic IP + Domain Name (FQDN) Authentication (Dynamische IP + Domänenname (FQDN)-Authentifizierung)** aus.



Local Group Setup	
Local Security Gateway Type :	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name :	User1.example.com
Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Schritt 14: Geben Sie im Feld **Domain Name (Domänenname)** den registrierten DynDNS-Domännennamen ein.

Schritt 15: Wählen Sie **Subnet** aus der Dropdown-Liste *Local Security Group Type (Lokaler Sicherheitsgruppentyp)* aus. Der Typ der lokalen Sicherheitsgruppe definiert, welche LAN-Ressourcen den VPN-Tunnel verwenden können.

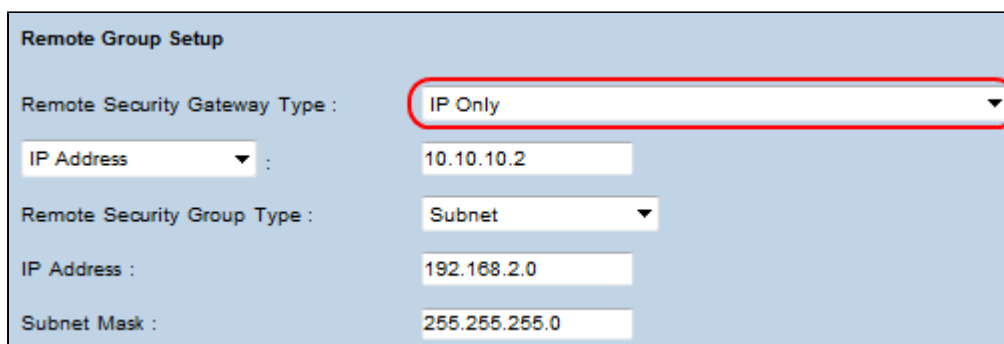


Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Schritt 16: Geben Sie die IP-Adresse in das Feld *IP-Adresse* ein.

Schritt 17: Geben Sie die Subnetzmaske in das Feld *Subnetzmaske* ein.

Schritt 18: Wählen Sie im Bereich "*Remote Group Setup*" (*Remote-Gruppen-Setup*) in der Dropdown-Liste *Remote Security Gateway Type (Typ des Remote-Sicherheits-Gateways)* die Option **IP Only (Nur IP)** aus.



Remote Group Setup	
Remote Security Gateway Type :	IP Only
IP Address :	10.10.10.2
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

Schritt 19: Wählen Sie **IP by DNS Resolved (IP durch DNS aufgelöst)** aus der nächsten Dropdown-

Liste aus, um ein Gerät anzugeben.

Remote Security Gateway Type :	IP Only
IP Address :	10.10.10.2
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

Schritt 20: Nachdem Sie **IP by DNS Resolved (IP durch DNS aufgelöst)** aus der Dropdown-Liste ausgewählt haben, geben Sie den registrierten Domännennamen des Routers in das Feld daneben ein.

Remote Security Gateway Type :	IP Only
IP by DNS Resolved :	Example.com
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

Schritt 21: Wählen Sie **Subnet** aus der Dropdown-Liste *Remote Security Group Type (Remote-Sicherheitsgruppentyp)* aus. Der Typ der Remote-Sicherheitsgruppe gibt an, welche Ressourcen im Remote-LAN auf den VPN-Tunnel zugreifen können.

Schritt 22: Geben Sie die IP-Adresse des Subnetzwerks in das Feld *IP-Adresse* ein.

Schritt 23: Geben Sie die Subnetzmaske in das Feld *Subnetzmaske* ein.

Schritt 24: Suchen Sie im Bereich *IP Sec Setup (IP-Sicherheit)* das Feld *Preshared Key (Vorinstallierter Schlüssel)*, und geben Sie einen Preshared Key ein, der zur Authentifizierung des entfernten IKE-Peers verwendet werden soll. Es können bis zu 30 Zeichen und Hexadezimalwerte eingegeben werden. An beiden Enden des VPN-Tunnels muss derselbe vorinstallierte Schlüssel verwendet werden. Für die übrigen Felder im Bereich **IPSec Setup** können Standardwerte verwendet werden.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key : **ciscosupport**

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

Save Cancel

Schritt 25: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Hinweis: Konfigurieren Sie den anderen Router mit den Schritten 9 bis 25. Gehen Sie dazu wie folgt vor, und schalten Sie die Konfiguration für die *lokale Gruppeneinrichtung* und die *Remote-Gruppeneinrichtung* um. Die Konfiguration des ersten Routers im Bereich für die *lokale Gruppeneinrichtung* entspricht der Konfiguration des zweiten Routers im Bereich für die *Remote-Gruppeneinrichtung*.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.