

VPN-Laborübung Vertiefung mit Netgear VPN-Gateway

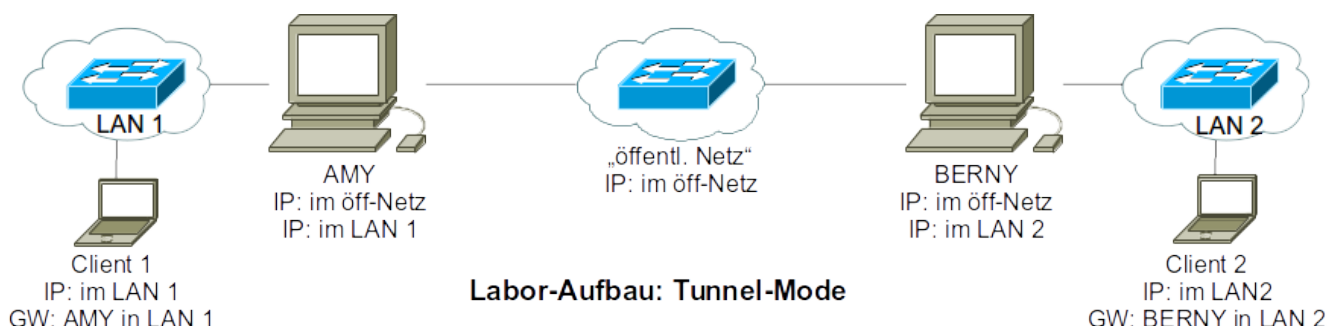
Einleitung und Übersicht

Als Anwendung soll ein Site-to-Site VPN aufgebaut werden. Hierzu werden folgende Elemente benötigt:

- zwei Netgear als VPN-Gateways auf jeweils einem Labor-PC installiert werden (public/private networks)
- zwei Labor-PCs als Clients (private networks), die als LAN-Clients konfiguriert werden.
- ein-zwei Switch ggf. ein Hub zum Mitschneiden der VPN-Verbindung ¹⁾

Insgesamt werden also 4 Labor-PCs und 1-2 Switche benötigt.

Das folgende Bild zeigt den prinzipiellen Aufbau.



Die Verbindung soll als Tunnel mit automatischer Schlüsselaushandlung (IKE/ISAKMP) aufgebaut werden. Als VPN-Gateway wird das Netgear VPN-Gateway eingesetzt. Als Clients werden zwei normale PCs verwendet.

Die folgende Tabelle zeigt ein mögliches Adressschema für den Laboraufbau:

Netzelement/Bereich	Parameter	Wert	Bedeutung
locale-privat	IP-Netz	10.0.0.0/8	privates LAN auf Amy-Seite (MikroTik)
remote-privat	IP-Netz	192.168.0.0/8	privates LAN auf Berny-Seite (Netgear)
public	IP-Netz	80.0.0.0/8	öffentliches Netz für die Verbindung der VPN-Gateways
public-Amy	IP-Adresse	80.0.0.1/8	öffentliche IP-Adresse von Amy (MikroTik)
locale-privat-Amy	IP-Adresse	10.0.0.1/8	private IP-Adresse von Amy (dient als Gateway für LAN) (MikroTik)
public-Berny	IP-Adresse	80.0.0.2/8	öffentliche IP-Adresse von Berny (Netgear)
remote-private-Berny	IP-Adresse	192.168.0.1/8	private IP-Adresse von Amy (dient als Gateway für LAN)

Basis-Konfiguration

- Setup Wizard
- Setup
 - Basic Settings
- Security
 - Logs
 - Block Sites
 - Rules
 - Services
 - Schedule
 - E-mail
- VPN
 - VPN Wizard
 - IKE Policies
 - VPN Policies
 - CAs
 - Certificates
 - CRL
 - VPN Status
- Maintenance
 - Router Status
 - Attached Devices
 - Settings Backup
 - Set Password
 - Diagnostics
 - Router Upgrade
- Advanced
 - Dynamic DNS
 - LAN Setup
 - Remote Management
 - Static Routes

Basic Settings

Does Your Internet Connection Require A Login?

No
 Yes

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

Get Dynamically From ISP
 Use Static IP Address

IP Address . . .

IP Subnet Mask . . .

Gateway IP Address . . .

Domain Name Server (DNS) Address

Get Automatically From ISP
 Use These DNS Servers

Primary DNS . . .

Secondary DNS . . .

DHCP Client Renew Mechanism

Release / Renew when 'DNS lookup' failed

Router's MAC Address

Use Default Address
 Use This Computer's MAC
 Use This MAC Address

IKE-Konfiguration

IKE Policy Configuration

General

Policy Name: mt

Direction/Type: Both Directions

Exchange Mode: Main Mode

Local

Local Identity Type: WAN IP Address

Local Identity Data: 80.0.0.2

Remote

Remote Identity Type: Remote WAN IP

Remote Identity Data: 80.0.0.1

IKE SA Parameters

Encryption Algorithm: AES-128

Authentication Algorithm: SHA-1

Authentication Method: Pre-shared Key

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

SA Life Time: 28800 (secs)

Buttons: Back, Apply, Cancel

Policy-Konfiguration

Site-to-Site mit dedizierten LANs:

VPN - Auto Policy

General

Policy Name:

IKE policy:

Remote VPN Endpoint

Address Type:

Address Data:

SA Life Time

(Seconds)

(Kytbes)

IPsec PFS

PFS Key Group:

Traffic Selector

Local IP

Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

Remote IP

Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

AH Configuration

Enable Authentication

Authentication Algorithm:

ESP Configuration

Enable Encryption

Encryption Algorithm:

Enable Authentication

Authentication Algorithm:

NETBIOS Enable

Site-to-Site mit beliebigen LANs (ungetestet):

- Setup Wizard
- Setup**
- Basic Settings
- Security**
- Logs
- Block Sites
- Rules
- Services
- Schedule
- E-mail
- VPN**
- VPN Wizard
- IKE Policies
- VPN Policies
- CAs
- Certificates
- CRL
- VPN Status
- Maintenance**
- Router Status
- Attached Devices
- Settings Backup
- Set Password
- Diagnostics
- Router Upgrade
- Advanced**
- Dynamic DNS
- LAN Setup
- Remote Management
- Static Routes

VPN - Auto Policy

General

Policy Name:

IKE policy:

Remote VPN Endpoint

Address Type:

Address Data:

SA Life Time

(Seconds)

(Kytbes)

IPsec PFS

PFS Key Group:

Traffic Selector

Local IP

Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

Remote IP

Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

AH Configuration

Enable Authentication

Authentication Algorithm:

ESP Configuration

Enable Encryption

Encryption Algorithm:

Enable Authentication

Authentication Algorithm:

Übersicht über die Policies:

- Setup Wizard
- Setup**
- Basic Settings
- Security**
- Logs
- Block Sites
- Rules
- Services
- Schedule
- E-mail
- VPN**
- VPN Wizard
- IKE Policies
- VPN Policies
- CAs
- Certificates
- CRL
- VPN Status
- Maintenance**
- Router Status
- Attached Devices
- Settings Backup
- Set Password
- Diagnostics
- Router Upgrade
- Advanced**
- Dynamic DNS

VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP
⊞	1	<input checked="" type="checkbox"/>	mtk	Auto	192.168.0.0 / 255.255.255.0	10.0.0.0 / 255.0.0.0	Disabled	ESP

Status-Abfrage

192.168.0.1/VPN_sta.htm

IPSec Connection Status

#	Policy Name	Endpoint	Tx (Bytes)	State	Action
1	mtk	80.0.0.1	6384	Phase 1: M-ESTABLISHED / Phase 2: ESTABLISHED	<input type="button" value="Drop"/>

- Setup Wizard
- Setup
 - Basic Settings
- Security
 - Logs
 - Block Sites
 - Rules
 - Services
 - Schedule
 - E-mail
- VPN
 - VPN Wizard
 - IKE Policies
 - VPN Policies
 - CAs
 - Certificates
 - CRL
 - VPN Status
- Maintenance
 - Router Status
 - Attached Devices

VPN Status/Log

```
[2000-01-01 02:29:43]**** RECEIVED SIXTH MESSAGE OF MAIN MODE ****
[2000-01-01 02:29:43]<POLICY: mt> PAYLOADS: ID,HASH
[2000-01-01 02:29:43]**** MAIN MODE COMPLETED ****
[2000-01-01 02:29:43][==== IKE PHASE 1 ESTABLISHED====]
[2000-01-01 02:29:43][==== IKE PHASE 2(to 80.0.0.1) START (initiator) ====]
[2000-01-01 02:29:45]**** SENT OUT FIRST MESSAGE OF QUICK MODE ****
[2000-01-01 02:29:45]<Initiator IPADDR=192.168.0.0,PORT=0>
[2000-01-01 02:29:45]<Responder IPADDR=10.0.0.0,PORT=0>
[2000-01-01 02:29:45]**** RECEIVED SECOND MESSAGE OF QUICK MODE ****
[2000-01-01 02:29:45]<POLICY: mt> PAYLOADS: HASH,SA,PROP,TRANS,NONCE,KE,ID,ID
[2000-01-01 02:29:45]<POLICY: mt> PAYLOADS: HASH
[2000-01-01 02:29:45]**** SENT OUT THIRD MESSAGE OF QUICK MODE ****
[2000-01-01 02:29:46]**** QUICK MODE COMPLETED ****
[2000-01-01 02:29:46][==== IKE PHASE 2 ESTABLISHED====]
```

Es können theoretisch alle Verbindungen über einen Switch geführt werden, da bis auf die VPN-Verbindung keine logische Kommunikation möglich ist

From:
<http://www.kopfload.de/> - **kopfload - Lad Dein Hirn auf!**

Permanent link:
http://www.kopfload.de/doku.php?id=lager:oeff_netze:vpn_vertiefung_netgear&rev=1510601331

Last update: **2025/11/19 16:13**

