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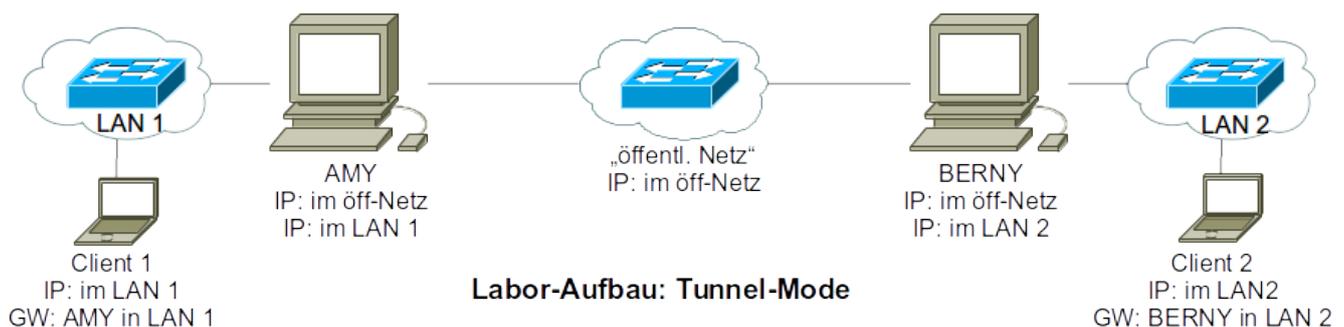
Die Verbindung soll als Tunnel mit automatischer Schlüsselaushandlung (IKE/ISAKMP) aufgebaut werden. Als VPN-Gateway wird das Netgear VPN-Gateway eingesetzt. Als Clients werden zwei normale PCs verwendet.

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) `FVS318v3`

Domain Name (If Required)

Internet IP Address

- ○ Get Dynamically From ISP
- ⦿ Use Static IP Address

IP Address `80` . `0` . `0` . `2`

IP Subnet Mask `255` . `0` . `0` . `0`

Gateway IP Address `80` . `0` . `0` . `1`

Domain Name Server (DNS) Address

- ○ Get Automatically From ISP
- ⦿ Use These DNS Servers

Primary DNS `80` . `0` . `0` . `2`

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 `00:14:6c:1f:ad:6d`

IKE-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

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
	••••••••
	◯ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
SA Life Time	28800 (secs)

[Back] [Apply] [Cancel]

Policy-Konfiguration

Site-to-Site mit dedizierten LANs:

- 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	mtk
IKE policy	mt

Remote VPN Endpoint   Address Type: IP Address

Address Data: 80.0.0.1

SA Life Time   3600 (Seconds)

4194303 (Kybtes)

☑ IPSec PFS   PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP   Subnet address

Start IP address:	192	168	0	0
Finish IP address:	0	0	0	0
Subnet Mask:	255	255	255	0

Remote IP   Subnet address

Start IP address:	10	0	0	0
Finish IP address:	0	0	0	0
Subnet Mask:	255	0	0	0

AH Configuration

☐ Enable Authentication   Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption   Encryption Algorithm: AES-128

☑ Enable Authentication   Authentication Algorithm: SHA-1

☐ 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	mtpolicy
IKE policy	mt

Remote VPN Endpoint
Address Type: IP Address
Address Data: 80.0.0.1

SA Life Time: 3600 (Seconds)
4194303 (Kybtes)

☑ IPSec PFS   PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Remote IP: Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

☐ Enable Authentication   Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption   Encryption Algorithm: AES-256
☑ Enable Authentication   Authentication Algorithm: SHA-1

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	☑	mtk	Auto	192.168.0.0 / 255.255.255.0	10.0.0.0 / 255.0.0.0	Disabled	ESP

Edit   Move   Delete

Apply   Cancel

Add Auto Policy   Add Manual Policy

Status-Abfrage

[1)]

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