VPN-Laborübung Vertiefung mit Netgear VPN-Gateway

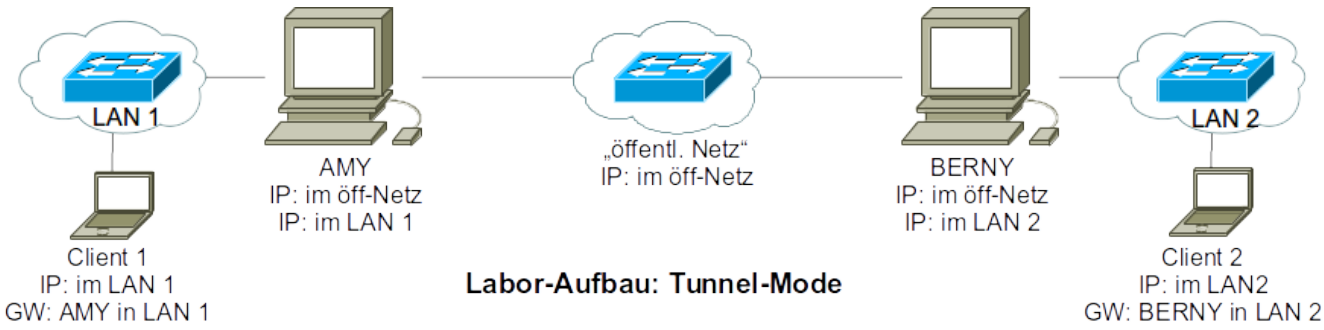
Einleitung und Übersicht

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.

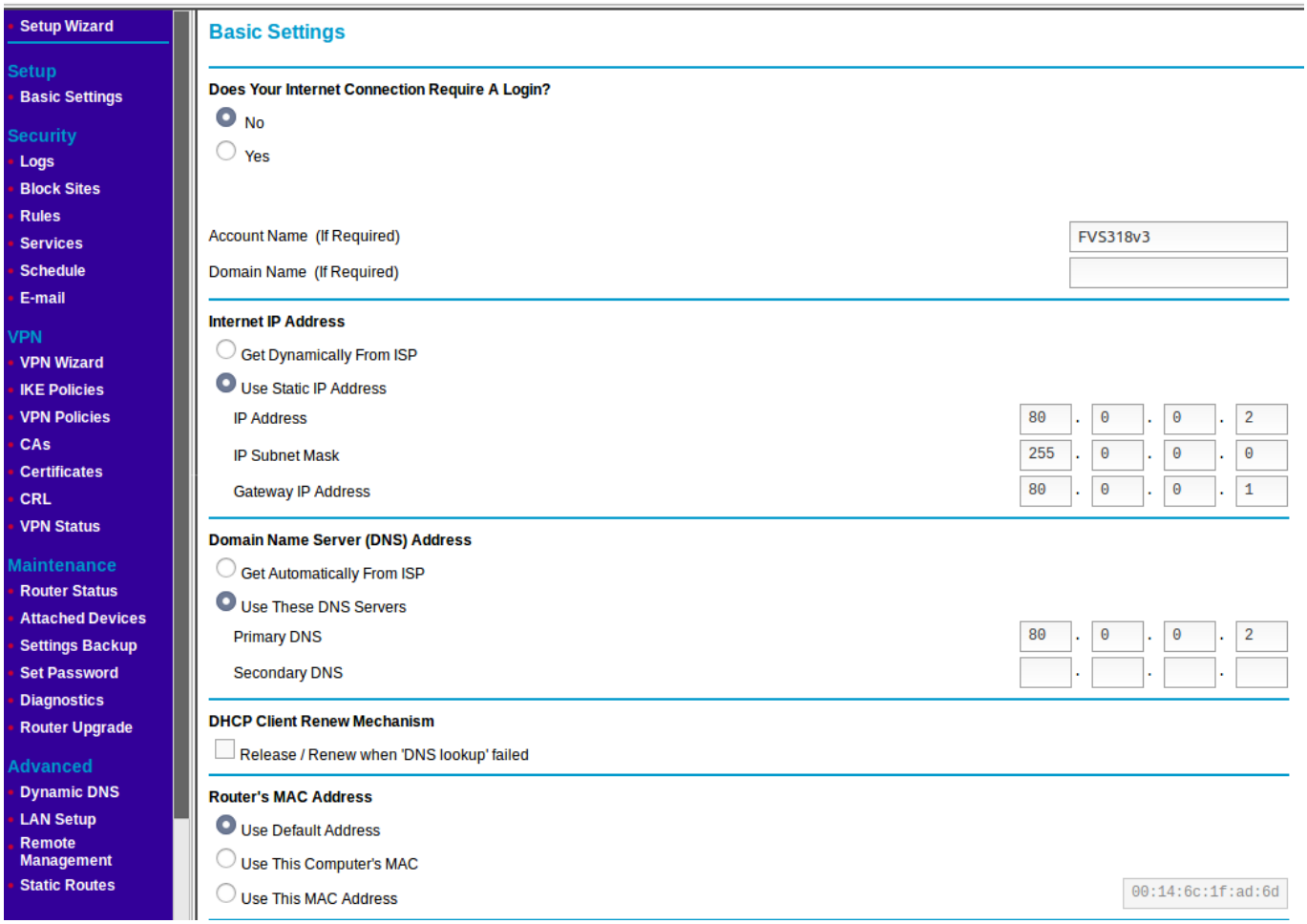


Die Verbindung soll als Tunnel mit automatischer Schlüsselaushandlung (IKE/ISAKMP) aufgebaut werden. Als VPN-Gateway wird das Netgear VPN-Gateway eingesetzt. Als Clients werden zwei normale PCs verwendet.

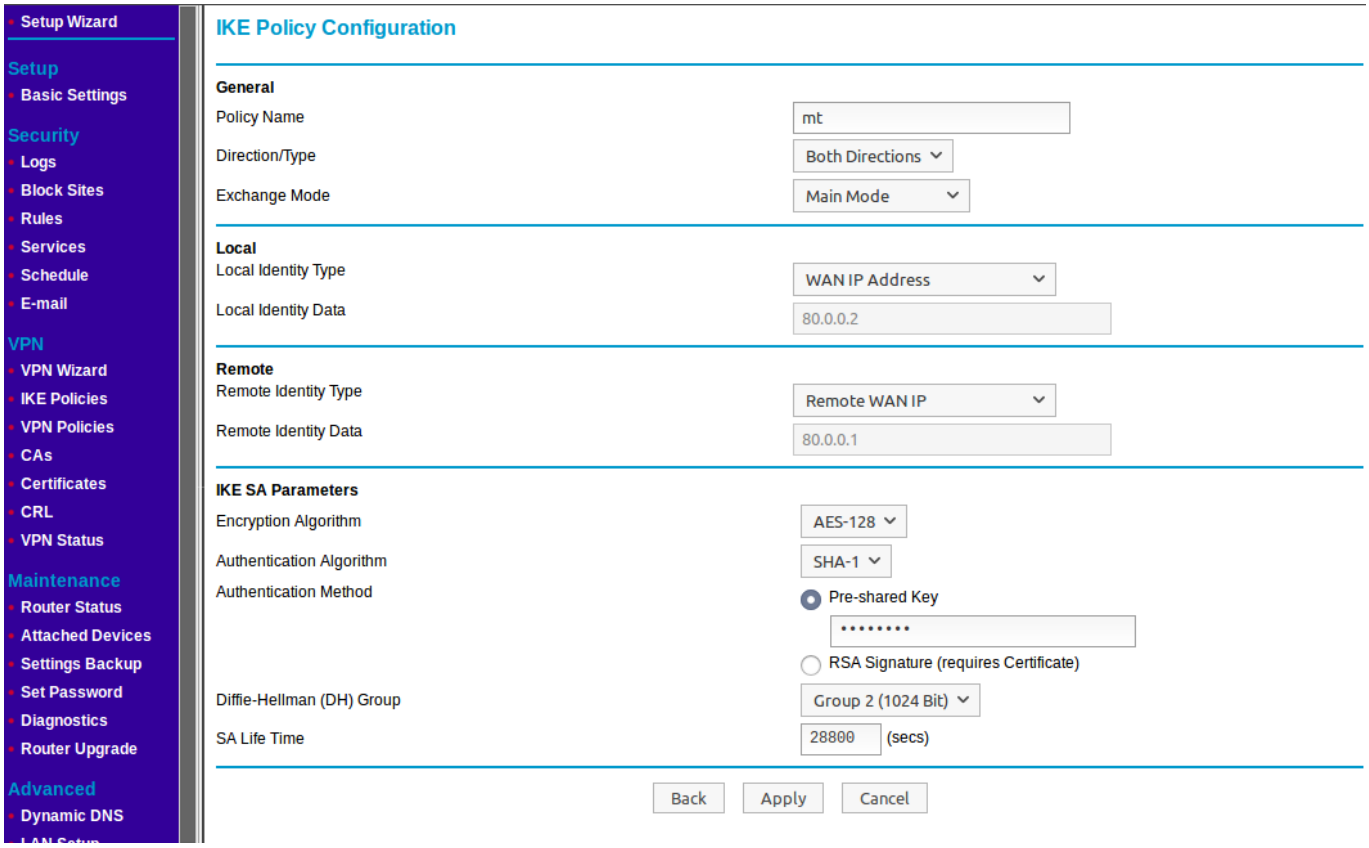
Die folgende Tabelle zeigt ein mögliches Adressschema für den Laboraufbau:

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

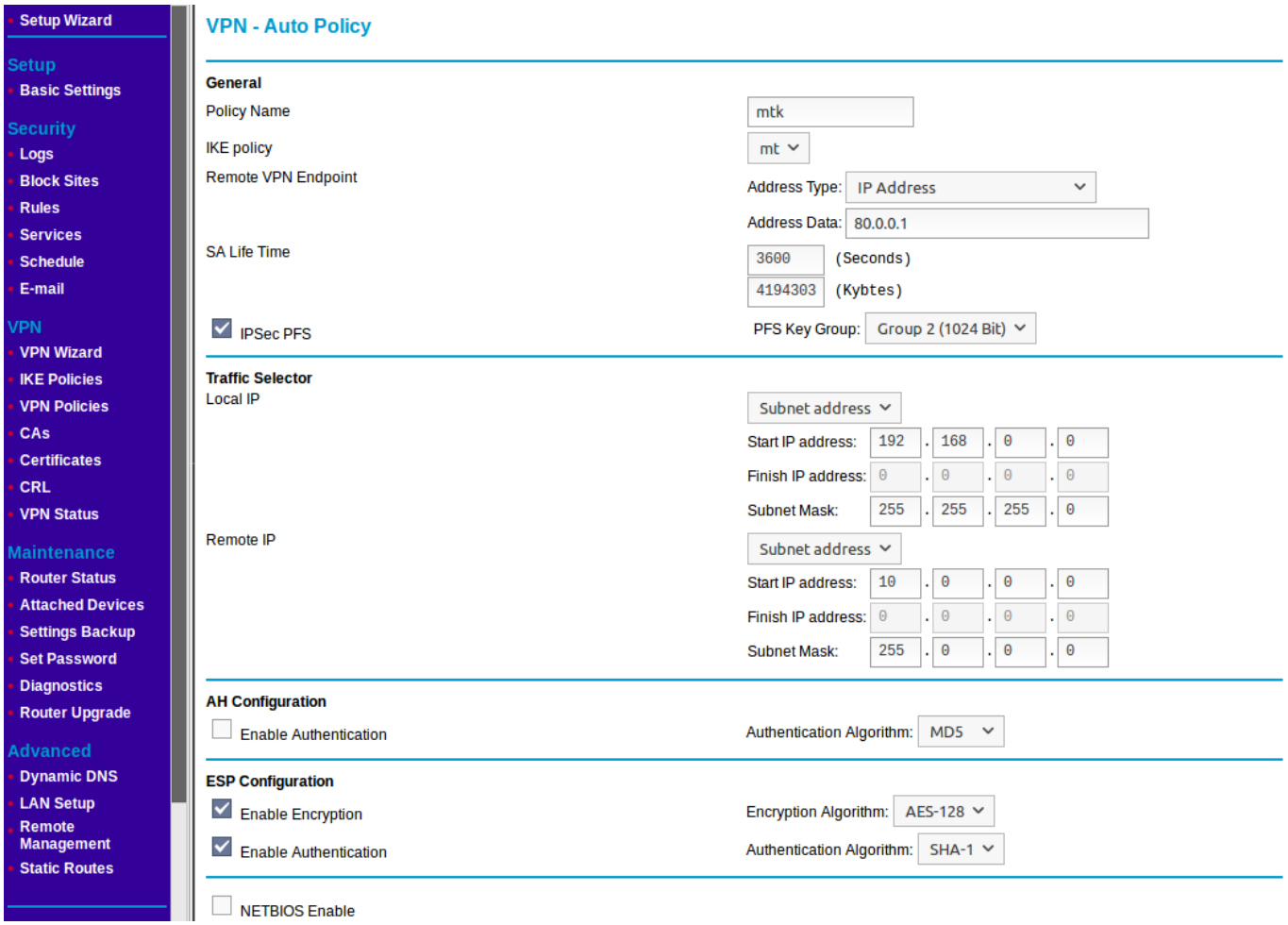


IKE-Konfiguration

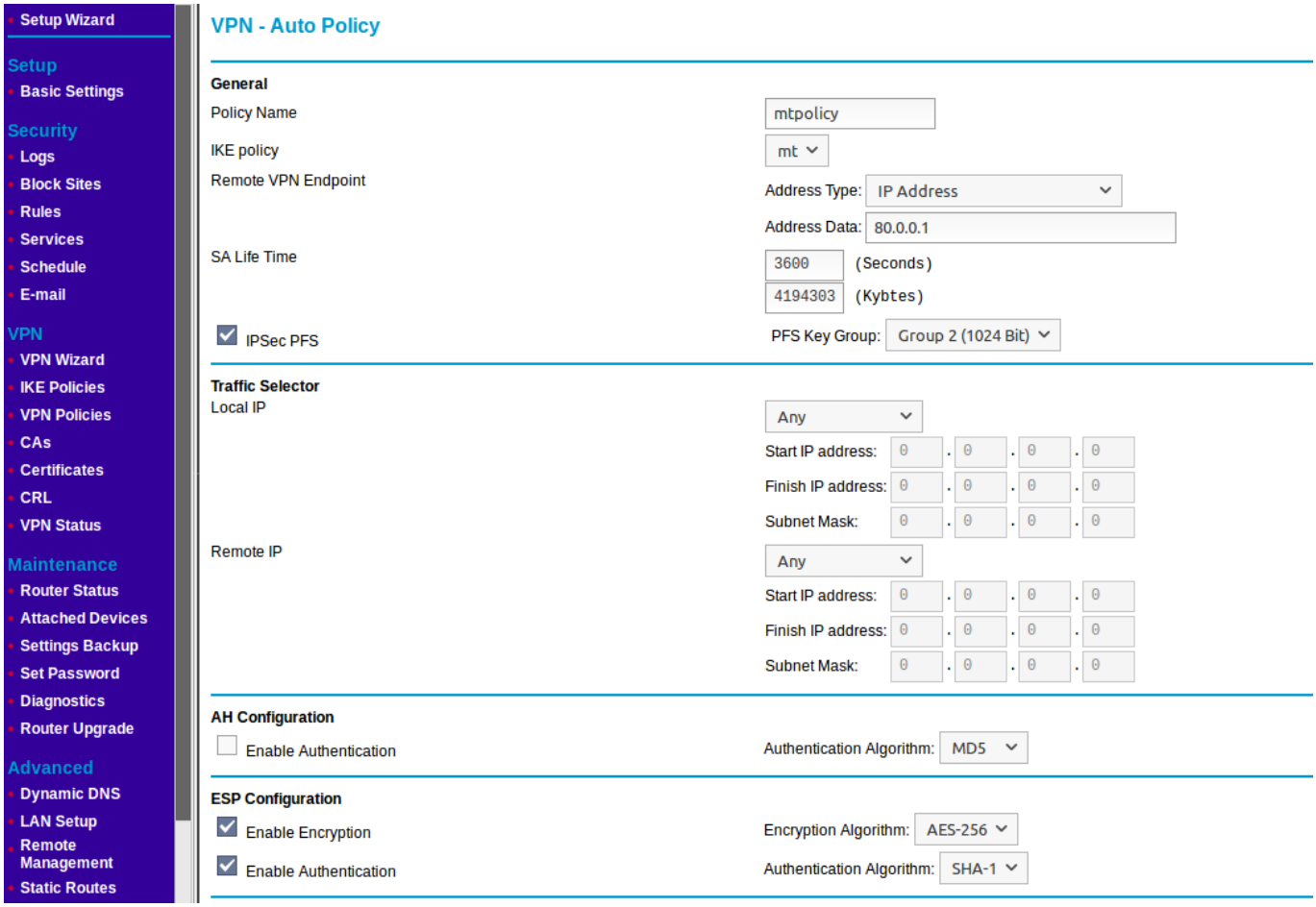


Policy-Konfiguration

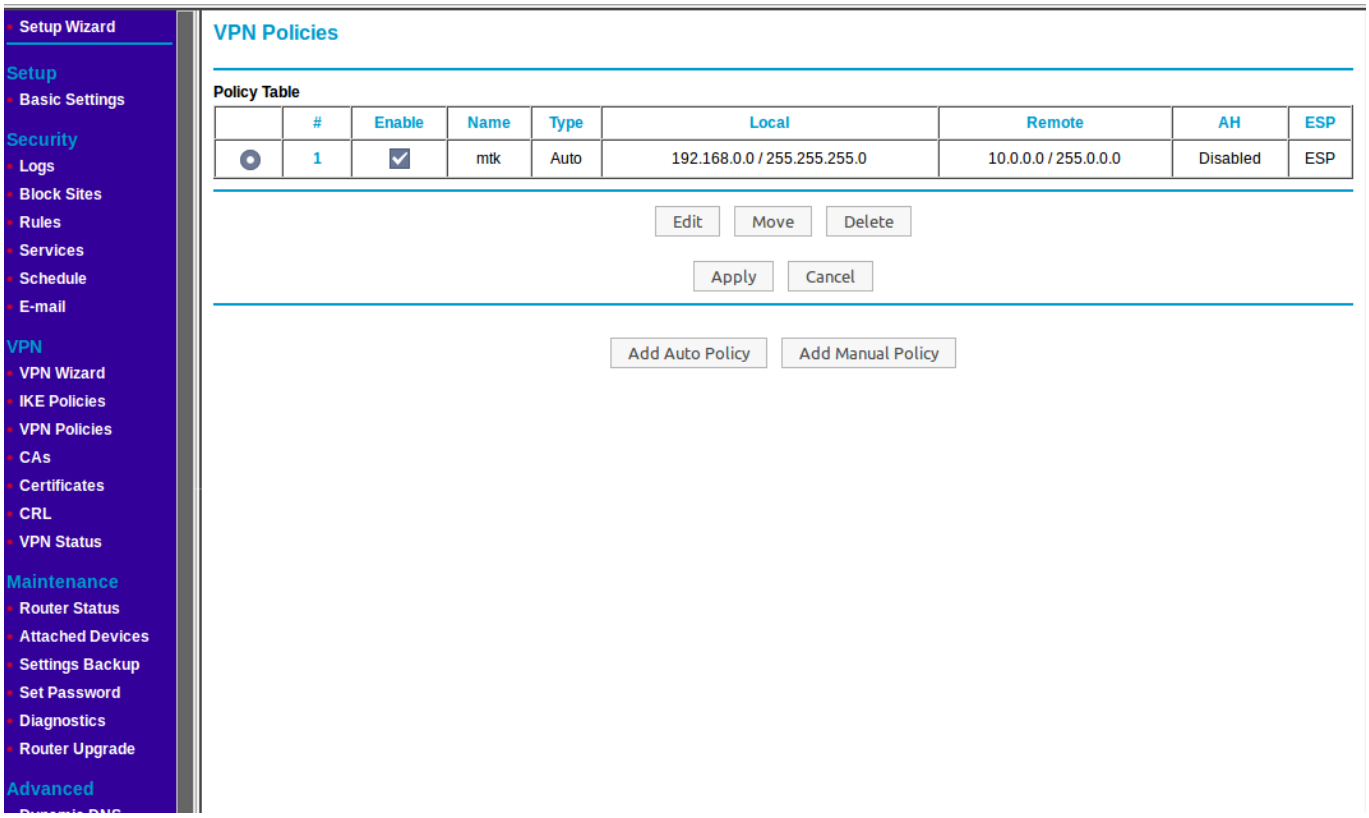
Site-to-Site mit dedizierten LANs:



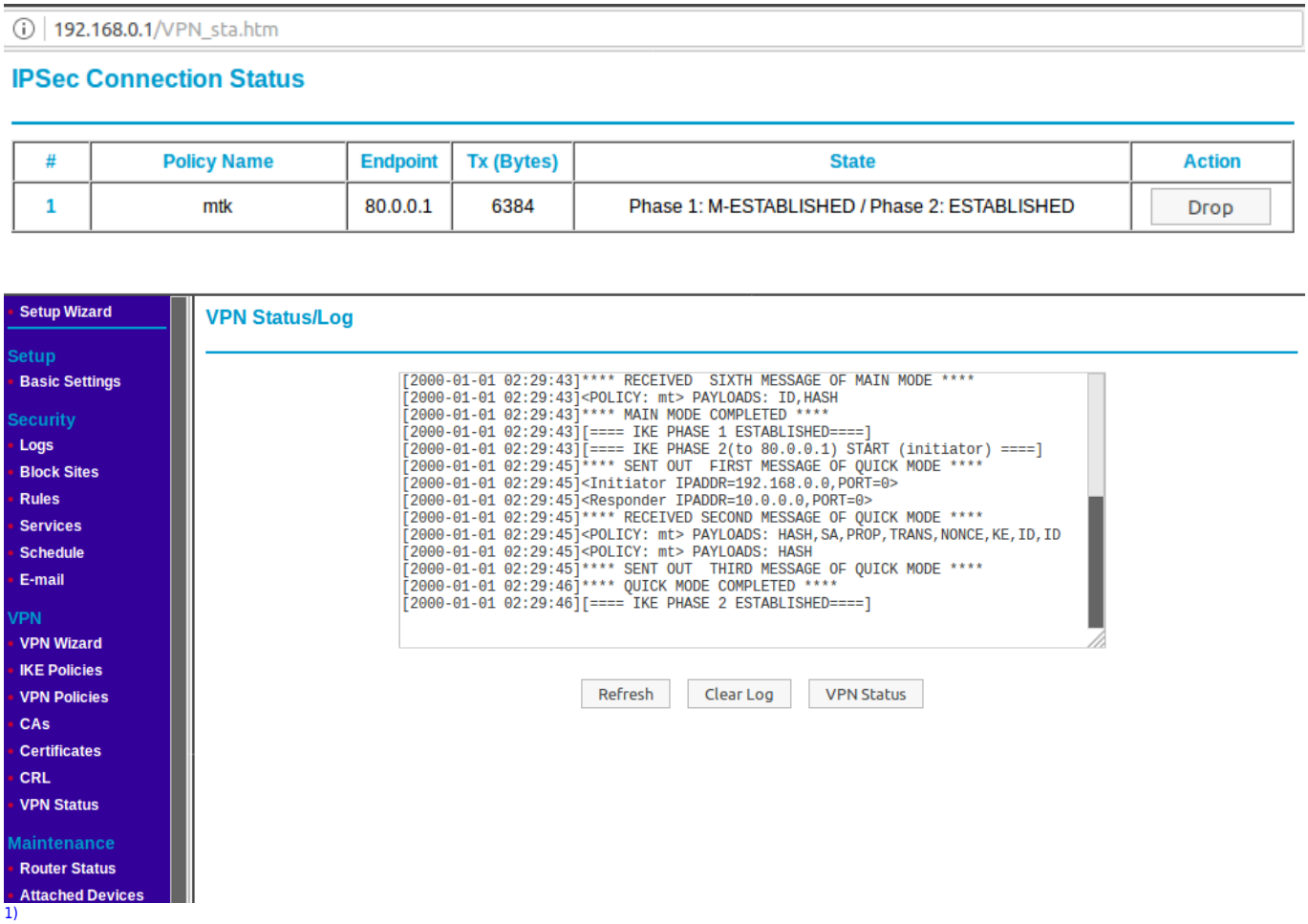
Site-to-Site mit beliebigen LANs (ungetestet):



Übersicht über die Policies:



Status-Abfrage



1)

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