

# mGuard | VPN KickStart

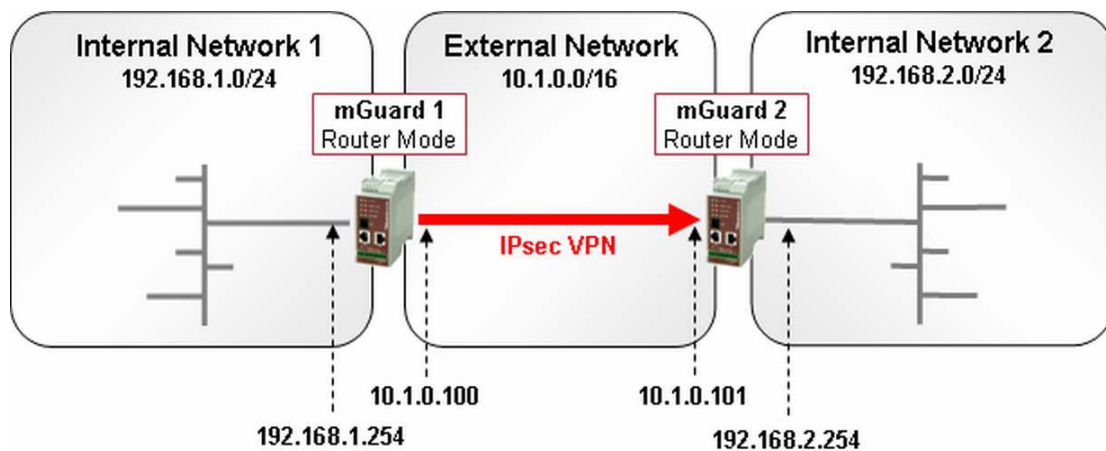
## Eine Schritt-für-Schritt Anleitung für das sichere Verbinden zweier Netzwerke durch ein mGuard basierendes IPsec-VPN

### Der VPN-Aufbau

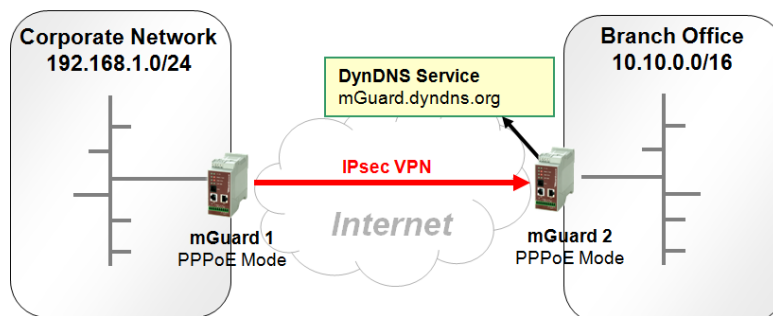
- Zwischen dem Firmennetz (erreichbar unter der IP-Adresse 192.168.x.0/24) und dem Zweigstellennetz (Remote-Netz erreichbar unter der IP-Adresse 192.168.y.0/24) soll ein sicheres IPsec VPN mit Hilfe von zwei mGuard Geräten aufgebaut werden.
- Die VPN-Verbindung soll dabei immer initiiert und aufgebaut werden, sobald die jeweilige Gegenstelle (mGuard) erreichbar ist.
- Beide mGuards werden im Router-Modus betrieben.
- Eine statische Namensauflösung auch bei dynamischen IP-Adressen der beiden mGuards wird z.B. durch den DynDNS Service ermöglicht.

### Die VPN-Randbedingungen

- Zwei mGuards mit aktueller Firmware (empfohlen: Version 7.2 oder höher)
- Valide IP-Verbindung zwischen beiden mGuards (Internet, WAN, LAN, ...)
- Gültige X.509 Zertifikate
- Festlegung Ihrer internen und externen IP-Adressen für beide mGuards (mGuard1, mGuard2)



- Optional: Festlegung der Host-Namen für mGuard1 und mGuard2 via DynDNS: mGuard1.dyndns.org, mGuard2.dyndns.org



- **Hinweis:** Zwischen den VPN-mGuards müssen die UDP-Ports 500 und 4500 geöffnet sein

## **Der mGuard VPN-Konfigurationsprozess**

1. X.509 Zertifikate und Schlüssel für die sichere, gegenseitige Authentifizierung der beiden mGuards erzeugen
2. Die passenden privaten und öffentlichen X.509 Zertifikate und Schlüssel in den jeweils passenden mGuard importieren
3. Einen sicheren IPsec VPN-Tunnel konfigurieren
4. VPN-Konfiguration testen

## 1. Schritt | mGuard Zertifikate erzeugen

Die für eine sichere Authentifizierung benötigten Zertifikate können mit dem Programm XCA oder mit Hilfe des [mGuard Certificate Generator](#) einfach und schnell erzeugt werden. Bitte beachten Sie, dass der Generator ausschließlich selbst-signierte Zertifikate ausstellen kann. Dies bedeutet, dass diese Zertifikate nicht durch eine offizielle CA beglaubigt wurden und deshalb nur für Testzwecke eingesetzt werden sollten.

Abbildung 1: mGuard Certificate Generator (mit unterschiedlichen Oberflächen)

Erzeugen Sie für jeden mGuard, der einen VPN-Tunnel terminiert, ein eindeutiges Zertifikat:

- Klicken Sie auf Abbildung 1
- Geben Sie für den ersten mGuard im Feld 'CommonName' einen eindeutigen Namen ein. In unserem Beispiel: 'mGuard\_1'
- Vergeben Sie im Feld 'Password' ein sicheres Passwort
- Klicken Sie auf den Button 'generate certificates'; Ihre Zertifikate für den ersten mGuard werden erzeugt und werden Ihnen als gepackte Datei unmittelbar zum Download angeboten. Speichern Sie die Zip-Datei (Beispiel: x509-certificate-mGuard\_1.zip) mit den (privaten und öffentlichen) Schlüsseln und den Zertifikaten (Beispiel: mGuard\_1-private-key-and-cert.p12, mGuard\_1-public-cert.pem) auf Ihrem mGuard-Konfigurationsrechner
- Entpacken Sie diese Zip-Datei für die weiteren Konfigurationsschritte
  
- Geben Sie für den zweiten mGuard im Feld 'CommonName' einen eindeutigen Namen ein. In unserem Beispiel: 'mGuard\_2'
- Vergeben Sie im Feld 'Password' ein sicheres Passwort
- Klicken Sie auf den Button 'generate certificates'; Ihre Zertifikate für den ersten mGuard werden erzeugt und werden Ihnen als gepackte Datei unmittelbar zum Download angeboten. Speichern Sie die Zip-Datei (Beispiel: x509-certificate-mGuard\_2.zip) mit den (privaten und öffentlichen) Schlüsseln und Zertifikaten (Beispiel: mGuard\_2-private-key-and-cert.p12, mGuard\_2-public-cert.pem) auf Ihrem mGuard-Konfigurationsrechner
- Entpacken Sie diese Zip-Datei und speichern Sie die entpackten Dateien für die weiteren Konfigurationsschritte auf Ihrem Konfigurationsrechner:

Name	Typ	Größe
x509-certificate-mGuard_1	ZIP-komprimierter Ordner	3 KB
x509-certificate-mGuard_2	ZIP-komprimierter Ordner	3 KB

Abbildung 2: mGuard Zertifikate für 'mGuard1' und 'mGuard2' in gepacktem Zustand

Name	Typ	Komprimierte Größe	Kennwortgeschützt	Größe	Verhältnis
mGuard_1-private-key-and-cert	Privater Informationsaustausch	2 KB	Nein	2 KB	1%
mGuard_1-public-cert	Privacy Enhanced Mail	1 KB	Nein	1 KB	33%

Abbildung 3: privater Schlüssel und öffentliches und privates Zertifikat für 'mGuard1' in entpacktem Zustand

## 2. Schritt | Schlüssel und Zertifikate importieren

- Melden Sie sich mit Hilfe eines Browsers am 'mGuard1' als Administrator an. Wie Sie Ihren mGuard erreichen, entnehmen Sie bitte der mGuard Packungsbeilage bzw. dem Benutzerhandbuch. Beispiel: <https://192.168.1.1> für einen mGuard, der im Router-Modus konfiguriert wurde, <https://1.1.1.1> für einen mGuard, der im Stealth-Modus vorliegt.

Abbildung 4: mGuard Anmeldemaske

- Default Admin-Login: admin
- Default Admin-Passwort: mGuard
- Konfigurieren Sie den mGuard als Router  
 Netzwerk > Interfaces > Allgemein > Netzwerk-Modus > Router  
 und vergeben sie eine externe – und interne IP Adresse
- Klicken Sie auf „Übernehmen“

- Passen Sie ggfs. den IP Adressbereich Ihres PC an die neue interne IP Adresse des mGuards an.
- Rufen Sie den mGuard-Menüpunkt 'Authentifizierung > Zertifikate > Maschinenzertifikate' auf
- Fügen Sie eine neue Zeile für ein neues 'Maschinenzertifikat' hinzu (Abbildung 5)



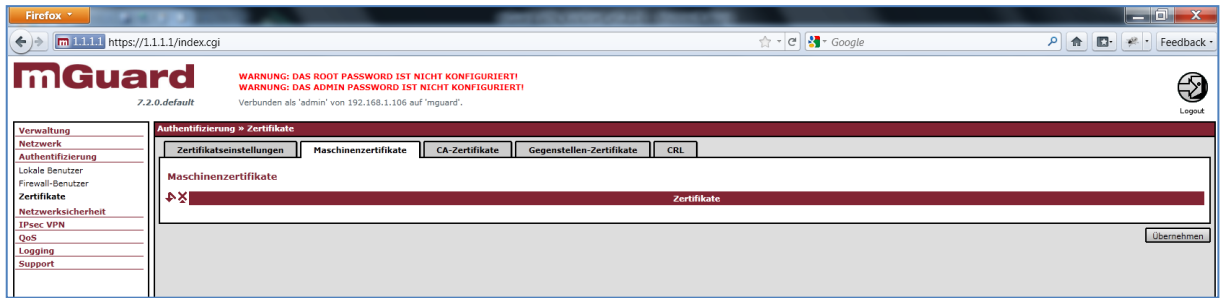


Abbildung 5: mGuard Menüeinstellungen für die Zertifikatsverwaltung

- Klicken Sie in dem Feld 'PKCS#12 hochladen' den Button 'Durchsuchen' (Abbildung 6)

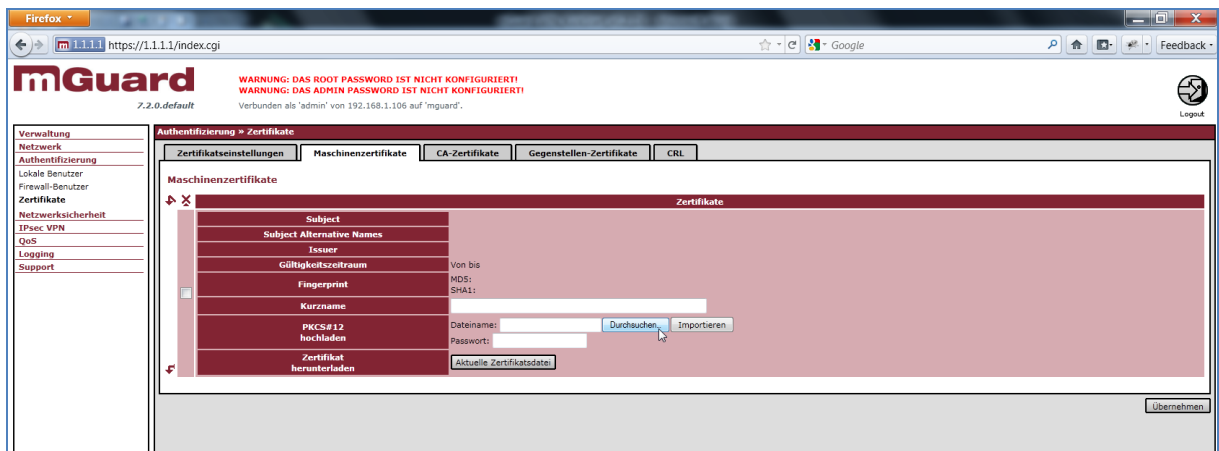


Abbildung 6: mGuard Menü-Tab für den Zertifikatsimport

- Wählen Sie die zuvor auf Ihrem Konfigurationsrechner entpackte und abgespeicherte Datei 'mGuard\_1-private-key-and-cert.p12' aus
- Tragen Sie in dem Feld 'Passwort' das beim Erzeugen der Zertifikate angegebenen Passwort ein
- Das Feld 'Kurzname' muss mit einer eindeutigen Bezeichnung ausgefüllt werden; wenn Sie hier keinen expliziten Kurznamen angeben, so wird der 'CommonName' (CN) des Zertifikats beim importieren eingetragen (Beispiel: 'mGuard\_1')
- Klicken Sie den Button 'Importieren'; der private Schlüssel und das Zertifikat für den 'mGuard1' werden importiert

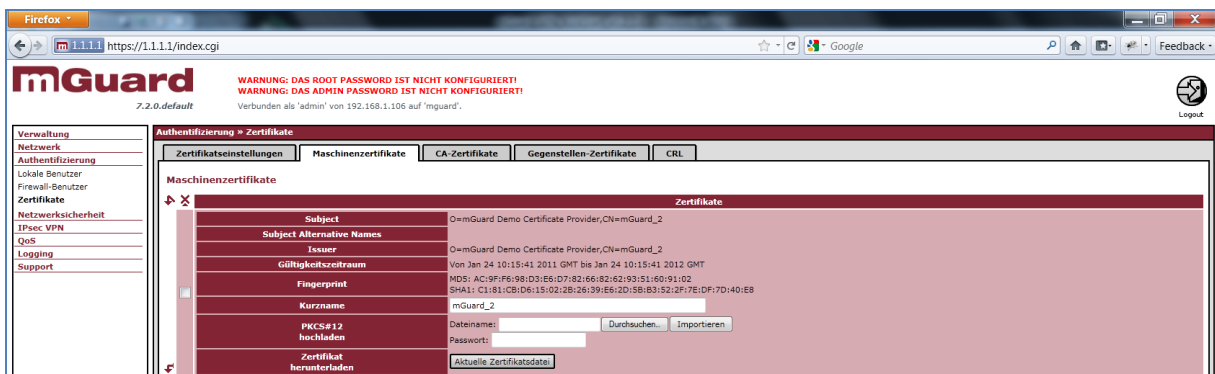


Abbildung 7: importiertes Zertifikat für 'mGuard2'

- Klicken Sie den Button „Übernehmen“

- Führen Sie das Importieren der Zertifikate äquivalent für den 'mGuard2' durch, indem Sie sich an dem 'mGuard2' als Administrator anmelden und hier ebenfalls den privaten Schlüssel und das Zertifikat für den 'mGuard2' (Beispiel: 'mGuard\_2-private-key-and-cert.p12') importieren, das auf Ihrem Konfigurationsrechner abgespeichert wurde (Abbildung 7)

### 3. Schritt | VPN-Tunnel konfigurieren

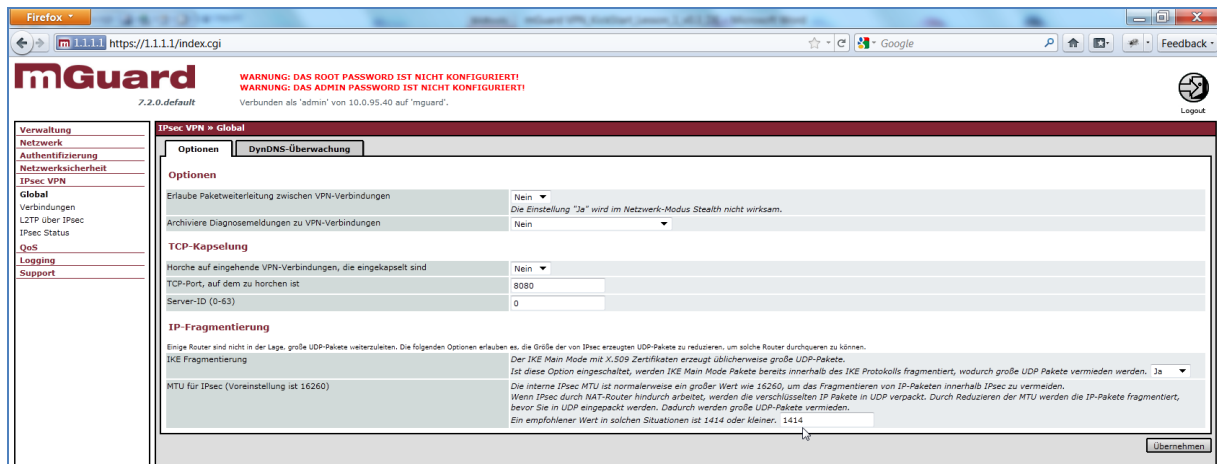


Abbildung 8: globale Einstellungen für IPsec VPN-Tunnel

- Rufen Sie den mGuard-Menüpunkt 'IPsec VPN > Global > Optionen' auf
- Überprüfen Sie, ob unter IP-Fragmentierung der Wert für 'IKE Fragmentierung' auf 'Ja' steht
- Ändern Sie unter IP-Fragmentierung den Wert für 'MTU für IPsec' auf einen Wert von 1414 oder niedriger
- **Hinweis:** Diese Einstellungen verhindern eventuelle Probleme bei Netzwerkkonfigurationen, die mit großen MTU-Werten nicht umgehen können; hierbei wird die Performance eventuell etwas geringer, dafür arbeitet das VPN zuverlässiger
- Klicken Sie auf „Übernehmen“



### VPN-Tunnel für 'mGuard1' konfigurieren

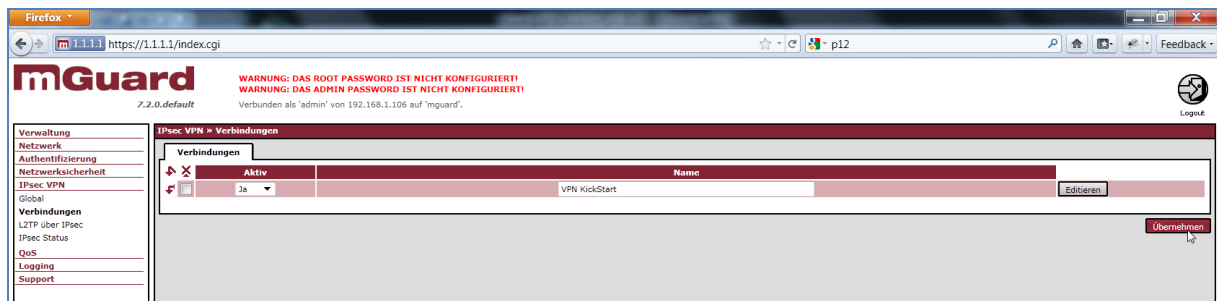


Abbildung 9: Verbindungs-Einstellungen für IPsec VPN-Tunnel

- Falls noch nicht geschehen, verbinden Sie sich mit dem zu konfigurierenden mGuard (Beispiel: 'mGuard1') und melden Sie sich mit Administrator-Rechten an
- Rufen Sie den Menüpunkt 'IPsec VPN > Verbindungen' auf
- Legen Sie eine neue VPN-Verbindung an, indem Sie auf den Pfeil ('neue Zeile einfügen') klicken
- Geben Sie dieser Verbindung einen eindeutigen Namen (Beispiel: VPN KickStart) und klicken Sie 'Übernehmen'
- Klicken Sie anschließend auf 'Editieren' (Abbildung 9)
- Tragen Sie im Reiter 'Allgemein' abweichend von den Default-Einstellungen im Feld 'Adresse des VPN-Gateways der Gegenstelle' entweder den DynDNS Namen oder die externe IP-Adresse der Gegenstelle des VPN-Tunnels ein (Beispiel: 10.1.2.254 bzw. mGuard2.dyndns.org)
- Wählen Sie hier abweichend von den Default-Einstellungen als 'Verbindungsinitiierung' den Wert 'Initiiere' aus
- Unter 'Transport- und Tunnelleinstellungen' wird die IP-Adresse der internen Ethernet-Schnittstelle des lokalen 'mGuard1' im Feld 'Lokal' eingetragen. Beispiel: 192.168.1.0/24
- Desweiteren wird die interne IP-Adresse der Remote-Gegenstelle (hier: 'mGuard2') im Feld 'Remote' eingetragen. Beispiel: 192.168.2.0/24 (Abbildung 10)
- Klicken Sie auf 'Übernehmen'



**IPsec VPN » Verbindungen » zu Maschine 2**

**Allgemein** | Authentifizierung | Firewall | IKE-Optionen

**Optionen**

Ein beschreibender Name für die VPN-Verbindung: VPN KickStart

Aktiv: Ja

Adresse des VPN-Gateways der Gegenstelle (Eine IP-Adresse, ein Hostname oder '%any' für beliebige, mehrere Gegenstellen oder Gegenstellen hinter einem NAT-Router.): 10.1.2.254

Interface, welches bei der Einstellung '%any' für das Gateway benutzt wird: Extern

Verbindungsinitiation: Initiere

Kapsle den VPN Datenverkehr in TCP ein: Nein

**Transport- und Tunneleinstellungen**

Aktiv	Typ	Lokal	Remote	Aktion
<input checked="" type="checkbox"/>	Tunnel	192.168.1.0/24	192.168.2.0/24	Mehr...

Zurück | Übernehmen

Abbildung 10: Allgemeine Verbindungs-Einstellungen für IPsec VPN-Tunnel

- Importieren Sie im Reiter 'Authentifizierung' im Feld 'Gegenstellen-Zertifikat' das öffentliche Zertifikat des 'mGuard2' (hier: 'mGuard\_2-public-cert.pem'), das auf Ihrem Konfigurationsrechner gespeichert wurde
- Wählen Sie unter „Lokales X.509-Zertifikat“ das zuvor in Schritt 2 eingetragene Maschinenzertifikat aus
- Klicken Sie auf 'Übernehmen'



Adresse: https://192.168.1.254/index.cgi

**mGuard** 7.3.1.default

WARNING: DAS ROOT PASSWORD IST NICHT KONFIGURIERT!  
WARNING: DAS ADMIN PASSWORD IST NICHT KONFIGURIERT!

Verbunden als 'admin' mit Rolle 'admin' von 192.168.1.193 auf 'mguard'.

**IPsec VPN » Verbindungen » zu mGuard2**

**Allgemein** | **Authentifizierung** | Firewall | IKE-Optionen

**Authentisierung**

Authentisierungsverfahren: X.509-Zertifikat

Lokales X.509-Zertifikat: MGUARD1

Remote CA-Zertifikat: Kein CA-Zertifikat, sondern das Gegenstellen-Zertifikat unten

Gegenstellen-Zertifikat:

Subject: CN=MGUARD2,O=PxC,L=HBG,ST=BW,C=DE

Subject Alternative Names:

Issuer: CN=WorkshopCA,O=PxC,L=HBG,ST=BW,C=DE

Gültigkeitszeitraum: Von Dec 3 11:05:18 2010 GMT bis Dec 2 11:05:18 2015 GMT

Fingerprint: MD5: B9:23:9D:AB:19:38:3C:A0:BD:B5:CF:EC:A9:57:9F:A5  
SHA1: 8B:88:7C:6B:79:F3:2A:CC:A1:19:2B:C8:55:03:24:6A:1D:F1:78:47

Dateiname (\*.pem):

Abbildung 11: Authentifizierungs-Einstellungen für IPsec VPN-Tunnel

## VPN-Tunnel für 'mGuard2' konfigurieren

- Führen Sie die o.g. Konfigurationsschritte für 'mGuard1' nun für die VPN-Gegenstelle (hier: 'mGuard2') durch:
  - Geben Sie „%any“ als Adresse des VPN-Gateways der Gegenstelle an
  - Hierbei werden unter Transport- und Tunneleinstellungen die Lokale- und Remote-IP- Adresse jeweils über Kreuz eingetragen
  - In den 'mGuard2' wird das öffentliche Zertifikat der Gegenstelle (hier: 'mGuard1') importiert
  - Die „Verbindungsinittierung“ wird auf „Warte“ eingestellt

IPsec VPN » Verbindungen » zu mGuard2

**Allgemein** | Authentifizierung | Firewall | IKE-Optionen

**Optionen**

Ein beschreibender Name für die VPN-Verbindung: zu mGuard1

Aktiv: Ja

Adresse des VPN-Gateways der Gegenstelle (Eine IP-Adresse, ein Hostname oder '%any' für beliebige, mehrere Gegenstellen oder Gegenstellen hinter einem NAT-Router.): %any

Interface, welches bei der Einstellung %any für das Gateway benutzt wird: Extern

Verbindungsinittierung: Warte

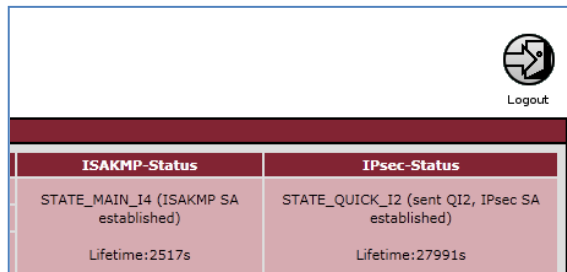
Kapseln den VPN Datenverkehr in TCP ein: Nein

**Transport- und Tunneleinstellungen**

	Aktiv	Typ	Lokal	Remote	Aktion
	Ja	Tunnel	192.168.2.0/24	192.168.1.0/24	Mehr...

#### 4. Schritt | VPN testen

- Schließen Sie die beiden konfigurierten mGuards in den entsprechenden Netzumgebungen an
- Optional: Sorgen Sie für eine valide Verbindung in das Internet (UDP-Ports 500 und 4500 geöffnet)
- Melden Sie sich auf einem der beiden mGuards an
- Rufen Sie den Menüpunkt 'IPsec VPN > IPsec Status' auf
- Prüfen Sie, ob die beiden mGuards (hier: 'mGuard1', 'mGuard2') untereinander eine VPN-Verbindung aufbauen
- Hierbei müssen in den Spalten 'ISAKMP-Status' und 'IPsec Status' die Verbindungen mit den Stati 'ISAKMP SA established' und 'IPsec SA established' angezeigt werden

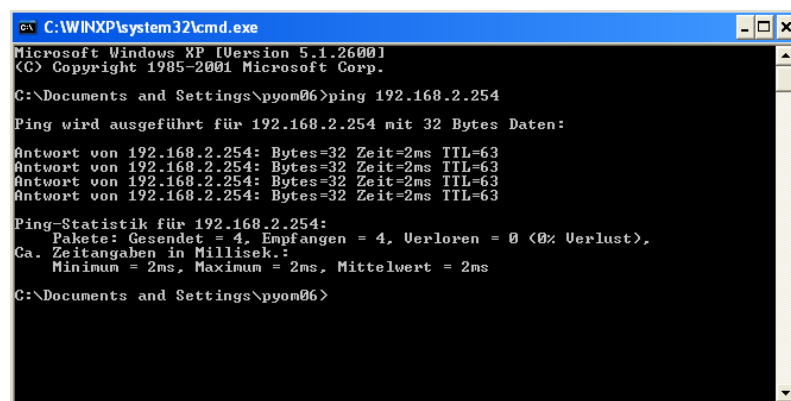


The screenshot shows a web interface with a 'Logout' button and a table with two columns: 'ISAKMP-Status' and 'IPsec-Status'. The 'ISAKMP-Status' column shows 'STATE\_MAIN\_I4 (ISAKMP SA established)' with a lifetime of 2517s. The 'IPsec-Status' column shows 'STATE\_QUICK\_I2 (sent QI2, IPsec SA established)' with a lifetime of 27991s.

ISAKMP-Status	IPsec-Status
STATE_MAIN_I4 (ISAKMP SA established) Lifetime:2517s	STATE_QUICK_I2 (sent QI2, IPsec SA established) Lifetime:27991s

Abbildung 13: IPsec VPN-Statusanzeige

- Überprüfen Sie die sichere VPN-Verbindung, indem Sie entweder die jeweilige VPN-Gegenstelle anpingen (mit mGuard firmware v7.3.1 und 7.4 nicht bei jeder Konfiguration möglich) oder aber den Zugriff auf die Gegenstelle (WebServer, Steuerung, Rechner, etc.) im Remote-Netz testen:



```
C:\WINXP\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\pyon06>ping 192.168.2.254
Ping wird ausgeführt für 192.168.2.254 mit 32 Bytes Daten:
Antwort von 192.168.2.254: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.2.254: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.2.254: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.2.254: Bytes=32 Zeit=2ms TTL=63
Ping-Statistik für 192.168.2.254:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 2ms, Maximum = 2ms, Mittelwert = 2ms
C:\Documents and Settings\pyon06>
```

Abbildung 14: Anpingen der IP-Adresse 192.168.2.254 im Remote-Netz via IPsec VPN-Tunnel

**Gratulation! Sie haben ein sicheres IPsec-VPN mit mGuards erfolgreich aufgebaut.**