IPcop v1.4

VPN auf BLUE mit X.509 Zertifikat

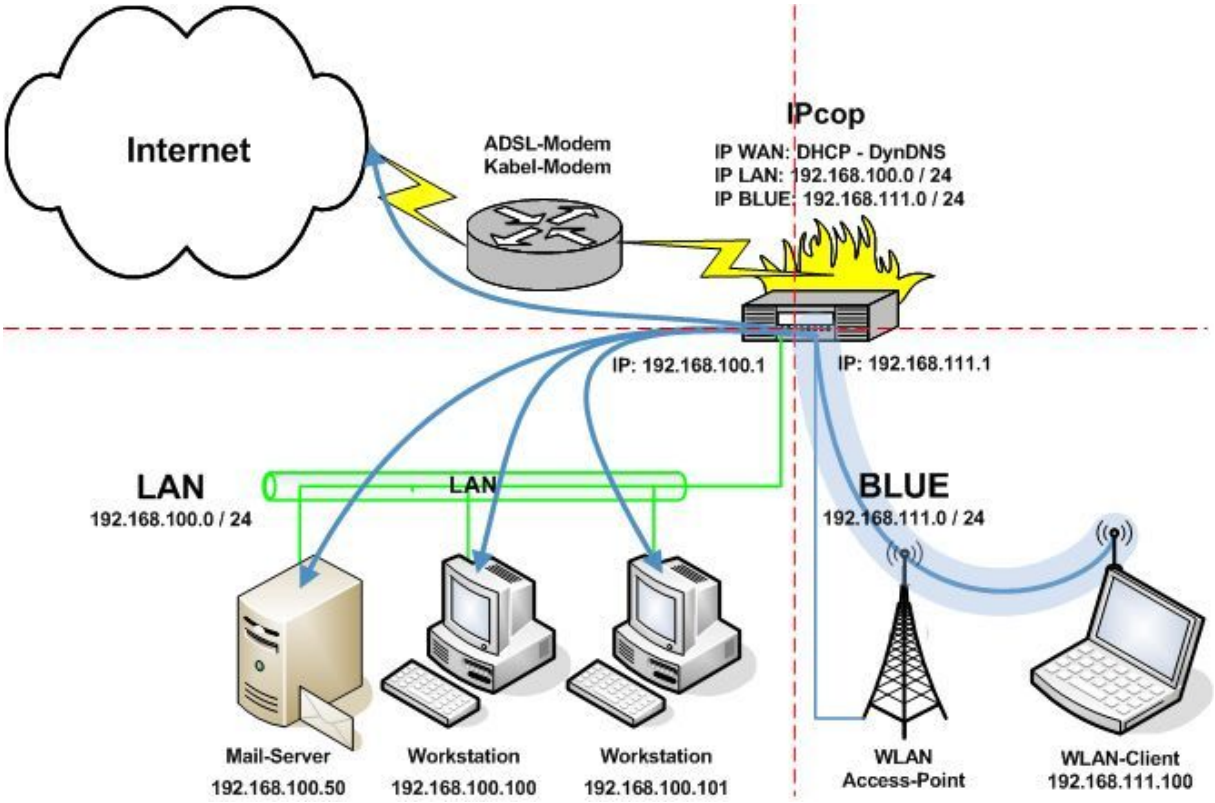
Grundsätzliches

Dieses Tutorial setzt eine Grundkonfiguration wie in dem Tutorial zum Basissetup des IPcop voraus. Die IP-Adressen müssen gegebenenfalls an die lokalen Vorgaben angepasst werden.
Zudem sollte der IPcop entsprechend dem Tutorial „VPN auf BLUE mit PSK“ erfolgreich eingerichtet worden sein.

Vorbereitung

1. Grundkonfiguration des IPcop nach einem der folgenden Tutorials:
   http://www.gutzeit.ch/ipcop/pdf/gr_konf_adsl_dyn.pdf
   http://www.gutzeit.ch/ipcop/pdf/gr_konf_adsl_fix.pdf
   http://www.gutzeit.ch/ipcop/pdf/gr_konf_kabel_dyn_fix.pdf
2. Blaue Netzwerkkarte installiert und konfiguriert
3. Vorstellung, wie das Netzwerk aussehen soll
4. Tutorial „VPN auf BLUE mit PSK“ erfolgreich durchgearbeitet

Beispiel eines Netzwerks



Vorwort

Dieses Tutorial baut auf den Informationen aus dem Tutorial „VPN auf BLUE mit PSK“ auf und setzt einen IPcop voraus, der nach dem o. g. Tutorial erfolgreich aufgesetzt wurde. Ich werde daher die dort erläuterten Begriffe hier als bekannt voraussetzen. Selbstverständlich werden neue Begriffe und Konzepte in diesem Tutorial in gewohnter Manier erklärt.

Wichtige Begriffe in Verbindung mit Zertifikaten:

- X.509 ist ein Standard für digitale Zertifikate. Ein digitales Zertifikat kann man sich als digitalen Personalausweis für einen Server/PC/User vorstellen. Ein Zertifikat garantiert, dass es sich bei dem Besitzer um die Person/Maschine handelt, die sie vorgibt zu sein. Zertifikate werden von CAs, s. u. ausgestellt und signiert. X.509 setzt ein streng hierarchisches System von vertrauenswürdigen CAs voraus.
- CA (Certification Authority) Zertifizierungsstelle, erstellt auf Anfrage Zertifikate und bürgt für ihre Korrektheit, indem sie das Zertifikat signiert. Dazu muss sichergestellt werden, dass das Zertifikat ausschliesslich von der Person/Maschine verwendet werden kann, für die es ausgestellt wurde. Je nach Sicherheitsbedürfnis werden mehr oder weniger sichere Verfahren zur Authentifizierung verwendet (eMail, Post-Ident, persönlicher Antrag/Abholung mit Ausweiskontrolle,…).

- Root-CA (Stammzertifizierungsstelle) ist die wichtigste CA in einer Zertifizierungshierarchie. Alle von untergeordneten CAs ausgestellten Zertifikate werden mit der Signatur der Root-CA versehen (signiert). Eine Root-CA entspricht in dem Beispiel mit dem Personalausweis dem Einwohnermeldeamt und der Bundesdruckerei, deren Stempel und Erzeugnisse allgemein und weltweit als vertrauenswürdig anerkannt sind. Durch das Vertrauen in diese Instanzen ist es möglich, mit einem Personalausweis ein fremdes Land zu bereisen und sich dort am Zoll zu authentifizieren. Wenn das Vertrauen in eine Root-CA verloren geht, indem z. B. der private Schlüssel zum Signieren weiterer Zertifikate in falsche Hände gerät, werden damit automatisch alle ausgestellten Zertifikate der Root-CA und ebenso alle ausgestellten Zertifikate aller untergeordneten CAs kompromittiert und damit wertlos. Windows wird von Haus aus mit einer Vielzahl als vertrauenswürdig eingestuften Root-Zertifikaten ausgeliefert. Bekannte kommerzielle Root-CAs werden z. B. von Verisign, oder Thawte betrieben. Der IPcop kann als private Root-CA verwendet werden.
- PKI (Public Key Infrastruktur) bezeichnet ein System, das es ermöglicht, digitale Zertifikate auszustellen, zu verteilen, zu überprüfen und bei Bedarf zurückzuziehen, bzw. als ungültig zu markieren. Dazu werden mindestens folgende Komponenten benötigt:
  - CA, welche die Zertifikate erstellt. IPcop kann als CA fungieren.
  - Registration Authority, bei der Anträge gestellt werden können und welche diese Anträge überprüft. Der IPcop Administrator übernimmt diese Funktion.
  - CRL (Certificat Revocation List) eine Sperrliste, mit der Zertifikate als abgelaufen oder ungültig erklärt werden können. Kann auf dem IPcop gepflegt werden.
  - Verzeichnisdienst, ein durchsuchbares Verzeichnis, für ausgestellte Zertifikate, meist ein LDAP-Server. Auf dem IPcop nicht implementiert.
  - Validierungsdienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht. Auf dem IPcop nicht implementiert.

  Da diese Infrastruktur nicht vollständig auf dem IPcop abgebildet werden kann, sind etwas mehr Handgriffe nötig um mit dem IPcop als Root-CA arbeiten zu können, als wenn man eine kommerzielle CA verwenden würde. Dem stehen jedoch Einsparungen von vielen US$ pro Jahr und pro PC gegenüber. Ebenso ist es möglich, eine bestehende PKI-Infrastruktur, wie sie z. B. Windows 2000/2003 Server zur Verfügung stellt, zu nutzen.
- öffentlicher Schlüssel, wird zum Verschlüsseln einer Nachricht verwendet und kann für jedermann frei zugänglich gemacht werden (Verzeichnisdienst).
- privater Schlüssel, darf unter keinen Umständen in fremde Hände fallen, da er sonst wertlos wäre. Wird zum Entschlüsseln einer Nachricht verwendet, die mit dem öffentlichen Schlüssel chiffriert wurde. Ausserdem können Nachrichten mit diesem Schlüssel signiert werden, um die Herkunft eindeutig kenntlich zu machen und um einer Veränderung des Inhalts vorzubeugen.

Das Ziel

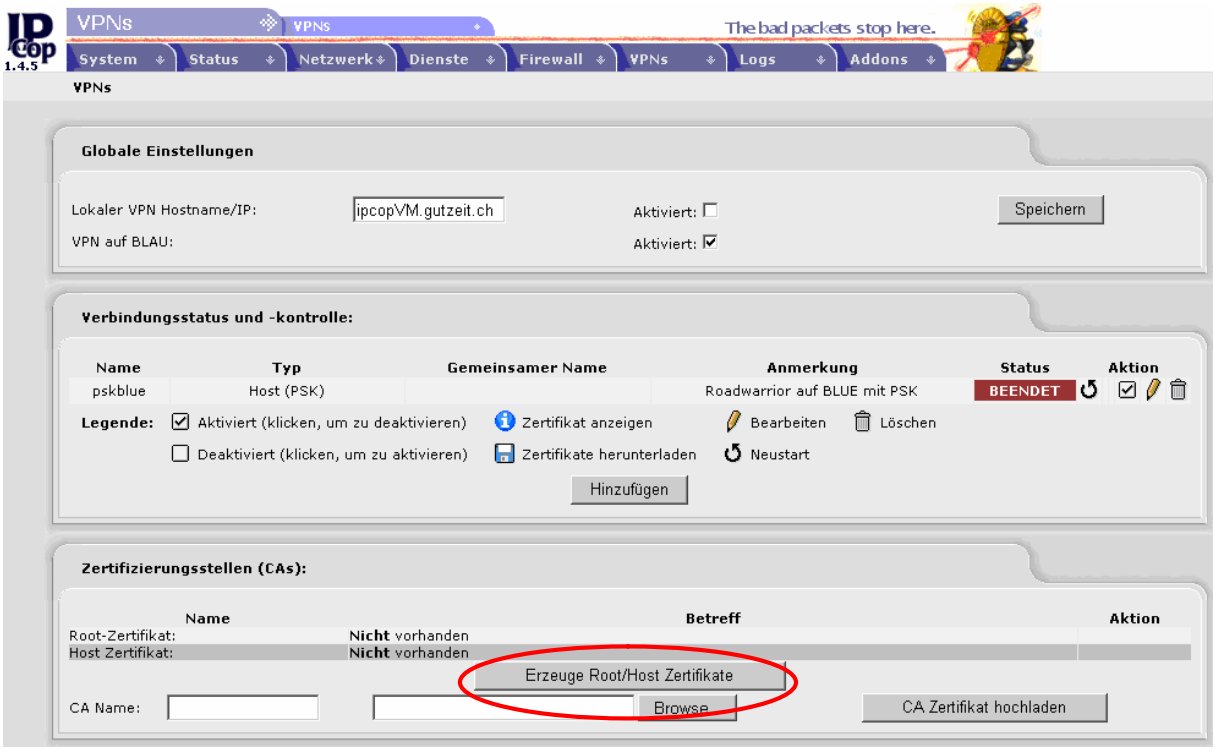
Das Ziel hat sich im Vergleich zum VPN mit PSK nicht verändert.

Neu soll die Authentifikation zwischen IPcop und WLAN-Client jedoch über Zertifikate erfolgen.

VPN mit X.509 Zertifikaten

Die Konfiguration

Übersicht



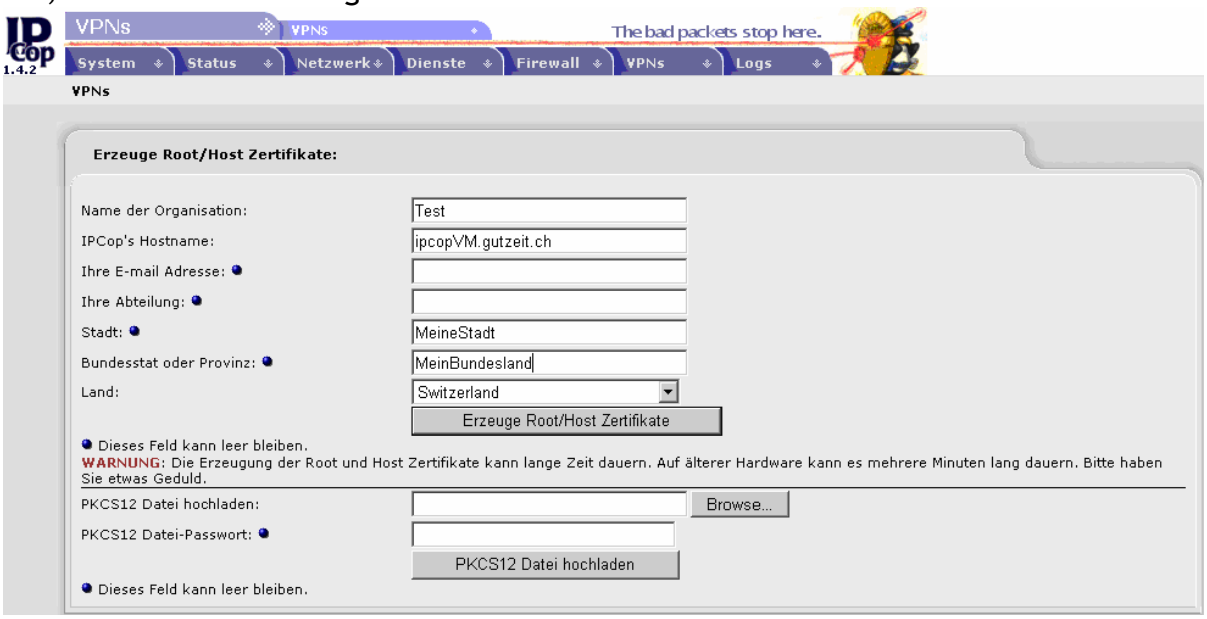
Erklärungen zu den einzelnen Optionen wurden im Tutorial VPN mit PSK gegeben. Ich werde sie hier also nicht wiederholen.

Wichtig und neu ist hier nur die Erstellung eines Root- und eines Host-Zertifikates, wodurch der IPcop zu unserer privaten Root-CA wird.

Ein beherzter Klick auf „Erzeuge Root/Host Zertifikate“ startet diesen Prozess.

Root- und Host-Zertifikat erstellen

In dieser Eingabemaske werden Informationen für die zu erstellenden Zertifikate abgefragt. Um den weiteren Ablauf nicht unnötig zu verkomplizieren, empfehle ich, nur die von mir ausgefüllten Felder zu verwenden.



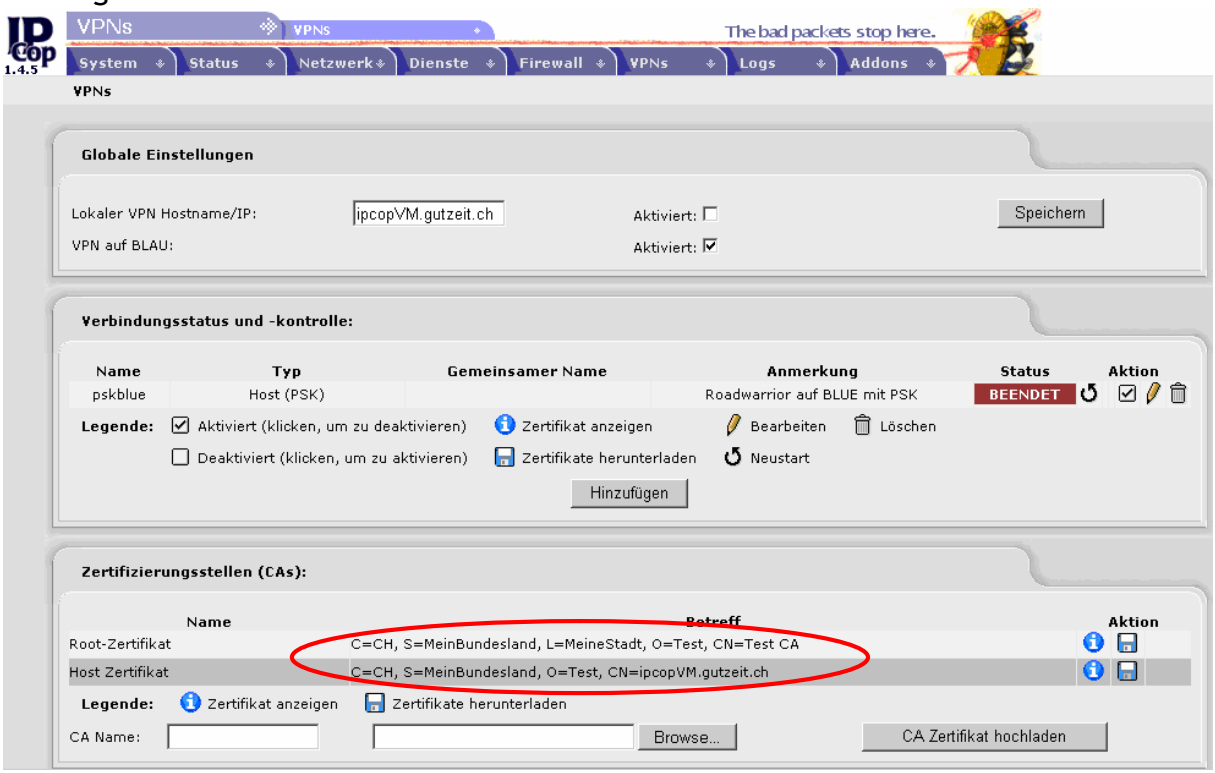
Erklärungen zu den einzelnen Optionen

Name der Organisation:	Erforderlich, bestimmt den Namen der Root CA, im obigen Beispiel heisst die Root-CA folglich „Test CA“
IPcop’s Hostname:	Erforderlich, wenn möglich einen FQDN verwenden
Ihre E-Mail Adresse:	Optional, um uns das Leben später zu erleichtern, bitte leer lassen.
Ihre Abteilung:	Optional, s. o.
Stadt:	Optional, kann ausgefüllt werden
Bundesstaat oder Provinz:	Optional, kann ausgefüllt werden
Land:	Erforderlich

Ein Klick auf „Erzeuge Root/Host Zertifikat“ bringt uns wieder zurück zum Hauptdialog.

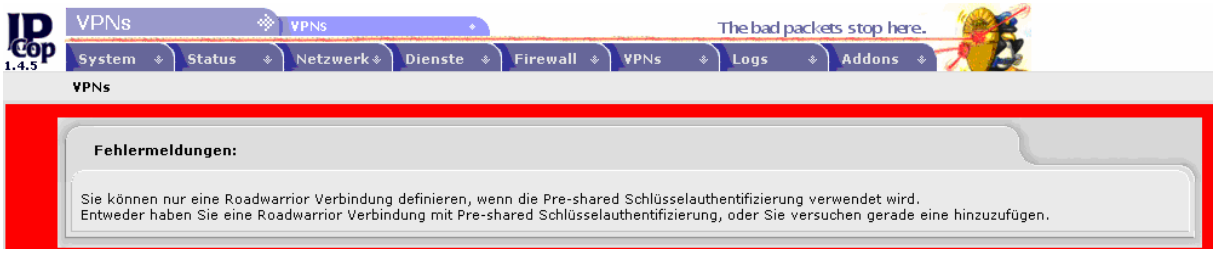
Wenn bei vorangegangenen Tests schon Zertifikate erstellt wurden, können diese z. B. mit WinSCP unter /var/ipcop/certs und /var/ipcop/ca gelöscht werden (alle Dateien in diesen Verzeichnissen müssen gelöscht werden). Ein erneuter Aufruf der Konfigurationsseite bringt dann einen „jungfräulichen“ IPcop zum Vorschein.

Das Ergebnis sollte nun in etwa so aussehen



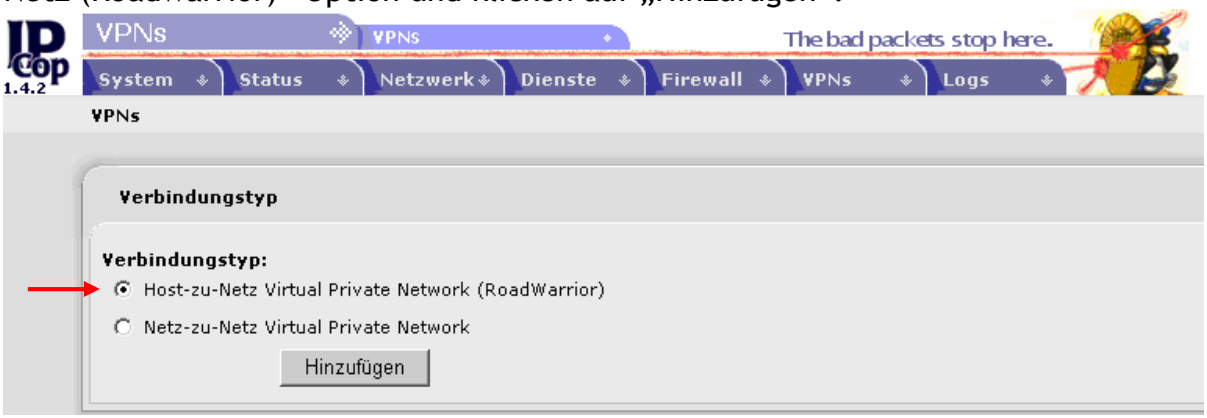
Konfiguration des IPcop

Die bestehende Verbindung mit PSK muss nun leider zuerst gelöscht werden, da IPsec nur eine einzige Verbindungskonfiguration zulässt, wenn PSK verwendet wird. Es handelt sich hierbei um eine Einschränkung von IPsec, nicht vom IPcop. In Verbindung mit Zertifikaten sind hingegen beliebig viele unterschiedliche Verbindungskonfigurationen parallel möglich. Wenn man diesen Schritt vergisst, führt das bei der Definition einer neuen Verbindung zu dieser Fehlermeldung:

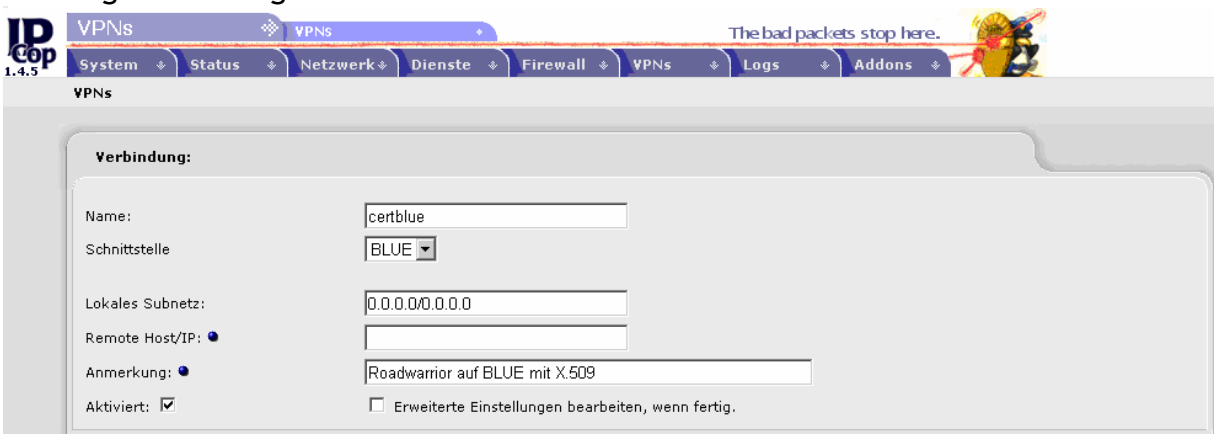


Nun geht es richtig los

Als erstes klicken wir im Abschnitt „Verbindungsstatus und -kontrolle“ s. o. auf den Button „Hinzufügen“. Im darauf erscheinenden Fenster wählen wir die „Host zu Netz (Roadwarrior)“ Option und klicken auf „Hinzufügen“.



Der folgende Dialog erscheint:



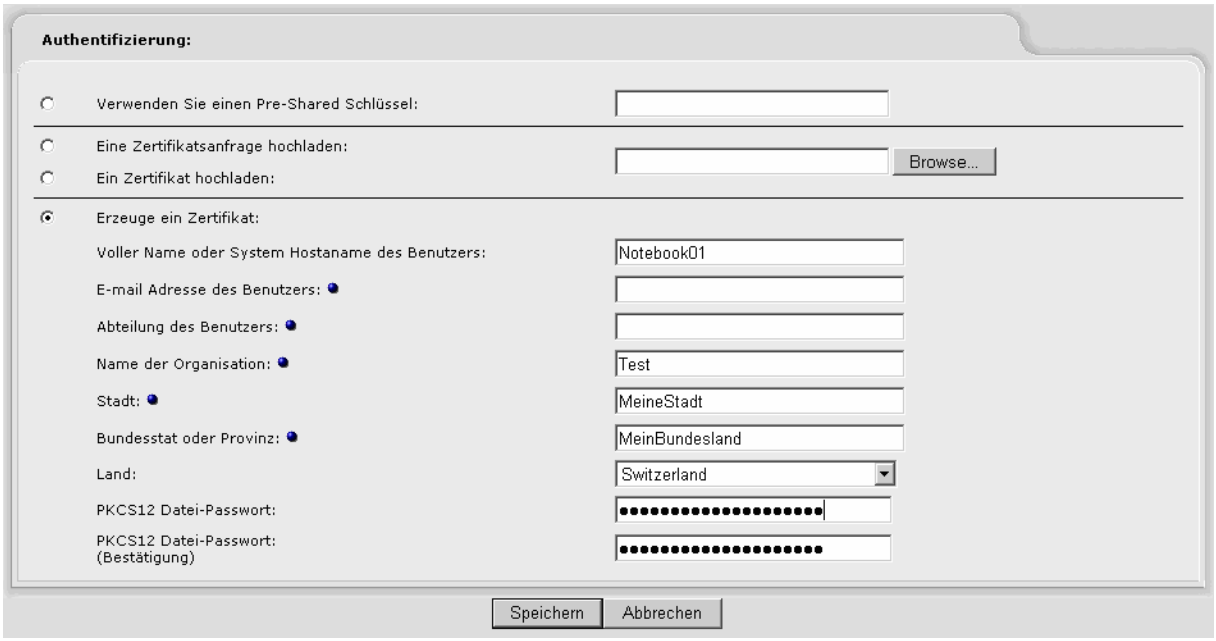
Erklärungen zu den einzelnen Optionen

Name:	Erforderlich, darf nur Buchstaben und Zahlen enthalten.
Schnittstelle:	Erforderlich, muss von RED auf BLUE gewechselt werden.
Lokales Subnetz:	Erforderlich, hier sollte entweder das grüne Subnetz, in unserem Fall 192.168.100.0/255.255.255.0, oder 0.0.0.0/0.0.0.0 stehen, je nach dem, ob man nur Verbindungen ins LAN, oder alle Verbindungen der WLAN-Clients verschlüsseln möchte. Aufgrund der weiter oben definierten Ziele, verwende ich 0.0.0.0/0.0.0.0, sprich sämtliche existierenden IPs als Ziel für unser zu erstellendes VPN. Dadurch wird der gesamte abgehende Verkehr eines VPN-Clients durch den VPN-Tunnel gezwungen und es werden keine unverschlüsselten Pakete mehr über das WLAN verschickt.

Remote Host/IP:	Optional, kann die IP oder den FQDN des VPN-Clients beinhalten, wenn diese(r) bekannt ist. Bleibt für unser Setup leer.
Anmerkung:	Optional, sollte aber unbedingt eine verständliche Beschreibung der Verbindung enthalten.
Aktiviert:	Erklärt sich wohl von selbst ;-)
Erweiterte Einstellungen:	Müssen normalerweise nicht angepasst werden.

Authentifizierung

Der zweite Teil der Seite beschäftigt sich mit den unterschiedlichen Authentifizierungsmethoden. Den Abschnitt für PSK haben wir früher schon kennen gelernt. Nun wollen wir uns mit dem Abschnitt für die Zertifikatserstellung befassen.



Erklärungen zu den einzelnen Optionen

Voller Name oder… :	Erforderlich, der Name des VPN-Clients. Entweder der FQDN, oder der NetBIOS-Name des PC.
E-Mail Adresse des… :	Optional, um uns das Leben später zu erleichtern, bitte leer lassen.
Abteilung des Benutzers:	Optional, s. o.
Name der Organisation:	Optional, ist in der Regel schon ausgefüllt.
Stadt:	Optional, ist in der Regel schon ausgefüllt.
Bundesstaat oder Provinz:	Optional, ist in der Regel schon ausgefüllt.
Land:	Erforderlich
PKCS12 Datei-Passwort:	Erforderlich, schützt das Clientzertifikat vor unbefugter Benutzung. Es ist daher wichtig, ein sehr gutes Passwort zu verwenden. Wenn das Passwort jedoch verloren geht, ist die PKCS12-Datei damit unbrauchbar. Da wir aber unsere eigene CA betreiben, können wir uns zum Glück jederzeit ein neues Zertifikat erstellen ;-)

Die Option „Eine Zertifikatsanfrage hochladen:“ erlaubt es, die CA auf dem IPcop zu verwenden, um eine vorgängig erstellte Zertifikatsanfrage eines Clients zu verarbeiten und damit ein Zertifikat zu erstellen.
Die Option „Ein Zertifikat hochladen:“ erlauben es, eine schon bestehende eigene CA (z. B. TinyCA für Linux, oder die Zertifikatsdienste von Windows 2000/2003 Server) zu verwenden. Durch das Hochladen wird hier dem IPcop das Clientzertifikat bekannt gemacht.

Mit „Speichern“ wird das Zertifikat erstellt und wir gelangen wieder zurück auf die Hauptseite, wo wir nun folgendes zu sehen bekommen:

Ein Klick auf das Stiftsymbol ermöglicht spätere Anpassungen der Konfiguration. Dass der Status auf „Beendet“ steht, ist zu erwarten und momentan OK. Erst wenn eine Clientverbindung besteht, ändert sich der Status auf „Offen“. Auf der Statusseite dagegen erscheint in der Diensteübersicht bei VPN nun der Status „Läuft“.

Das erstellte Zertifikat „certblue.p12“ muss nun durch einen Klick auf das Diskettensymbol vom IPcop heruntergeladen werden und mit einem geeigneten Mittel (Diskette, USB-Stick,…) auf den Ziel-PC transferiert werden. Diese Datei beinhaltet, neben dem Clientzertifikat, auch das Root-Zertifikat des IPcop.

Damit ist die Konfiguration auf dem IPcop abgeschlossen.

Konfiguration des Clients

Als erstes besorgen wir uns alle nötigen Tools um IPsec auf einer Windows 2000/2003/XP-Maschine komfortabel einrichten zu können. NT 4.0 kann mit Bordmitteln kein IPsec und ist daher auf (kommerzielle) IPsec-Software von Drittherstellern angewiesen.

Windows 2000

Windows 2000 muss mindestens SP2 installiert haben, SP4 ist empfohlen!
http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp
Ausserdem benötigen wir für Windows 2000 die Datei „IPsecpol.exe“ Version 1.22 oder höher. Diese Datei ist Bestandteil des W2k Ressource Kit und hier zu finden.
http://agent.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp

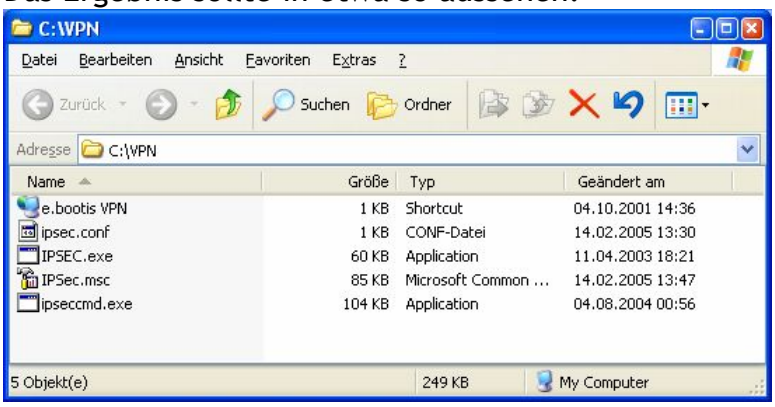
Windows XP

Bei Windows XP müssen zuerst die Windows XP Support Tools installiert werden. Diese befinden sich auf der Installations-CD im Ordner \SUPPORT\TOOLS. Es ist

wichtig die Vollinstallation auszuwählen, damit die Datei „IPseccmd.exe“ den Weg auf die Festplatte findet. Ist Windows XP SP2 im Einsatz, empfiehlt es sich, statt dessen die aktuellen Support Tools hier herunter zu laden und zu installieren.
http://support.microsoft.com/default.aspx?scid=kb;en-us;838079

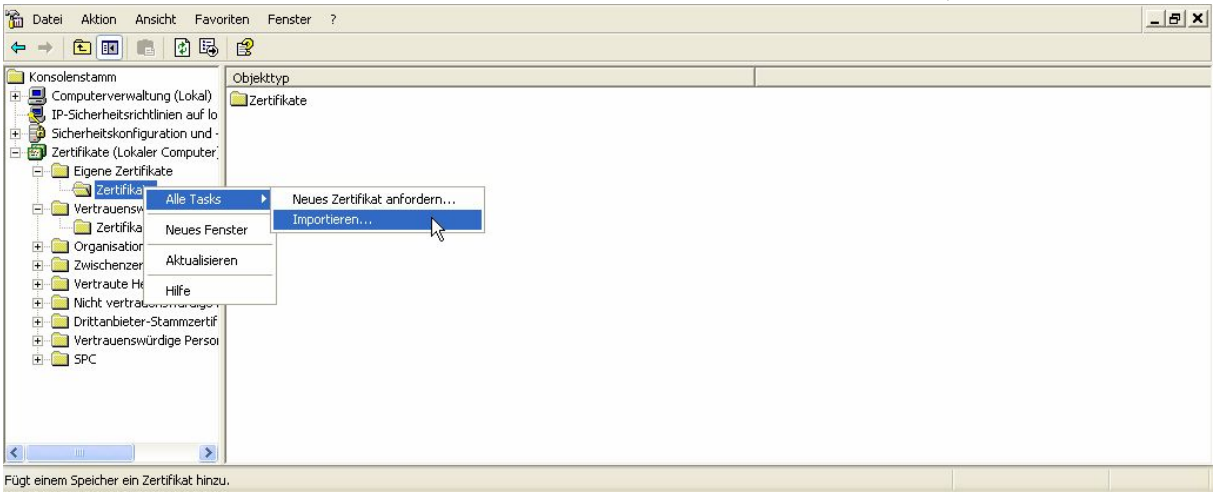
Als letztes benötigen wir noch das IPsec-Tool von Markus Müller.
http://vpn.ebootis.de/package.zip

Wir erstellen als erstes einen Ordner C:\VPN und entpacken die Datei „package.zip“ dort hinein. Anschliessend muss bei Windows 2000 noch die Datei „IPsecpol.exe“ in diesen Ordner installiert werden. Unter Windows XP kann die Datei „IPseccmd.exe“ (normalerweise zu finden unter C:\Programme\Support Tools\ipseccmd.exe) einfach in diesen Ordner kopiert werden.
Das Ergebnis sollte in etwa so aussehen.



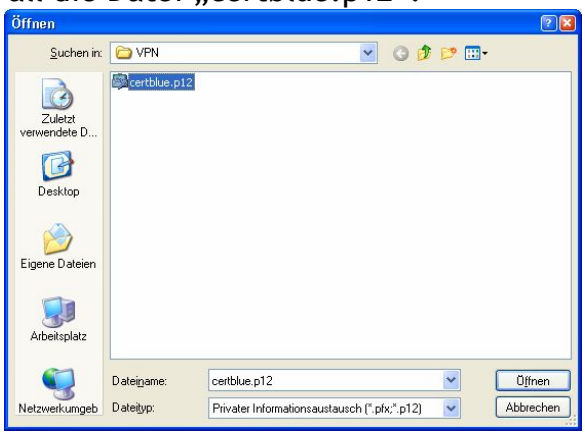
Nach diesen Vorbereitungsarbeiten geht es jetzt ans Eingemachte.

Zertifikat-Import auf dem Client
Damit sich der Windows-Client erfolgreich beim IPcop authentifizieren kann, muss das vorhin auf dem IPcop exportierte Zertifikat „certblue.p12“ auf dem Client installiert werden. Dazu öffnen wir die Datei „C:\VPN\IPSec.msc“, s. Screenshot.

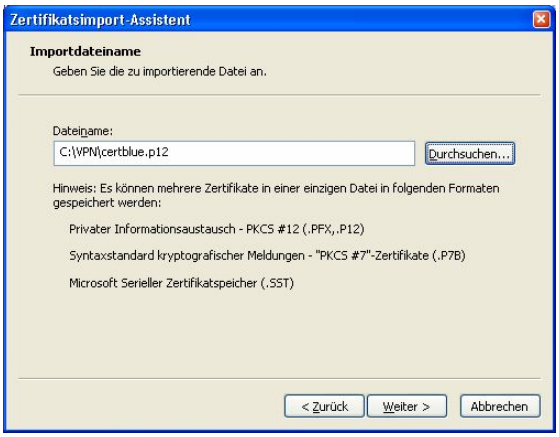


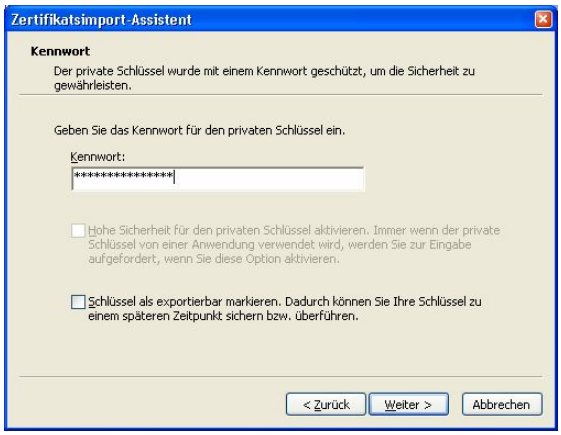
Ein Rechtsklick auf einen Zertifikat-Ordner ermöglicht den Start des Importassistenten.

Mit „Weiter“ gelangt man zu einem Dialog, mit dem man das zu importierende Zertifikat auswählen kann. In unserem Fall die Datei „certblue.p12“.

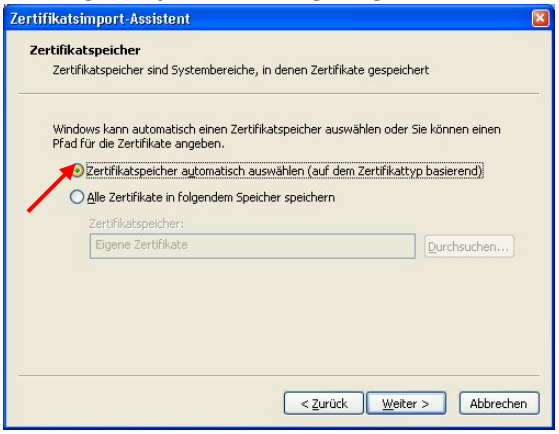


Um das Zertifikat zu importieren, wird das Passwort benötigt, welches bei der Erstellung des Zertifikats verwendet wurde.



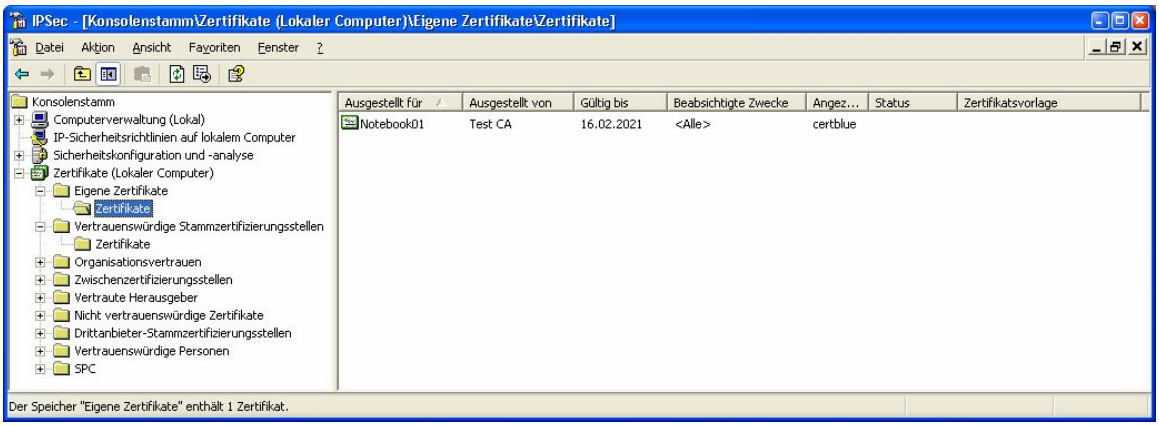


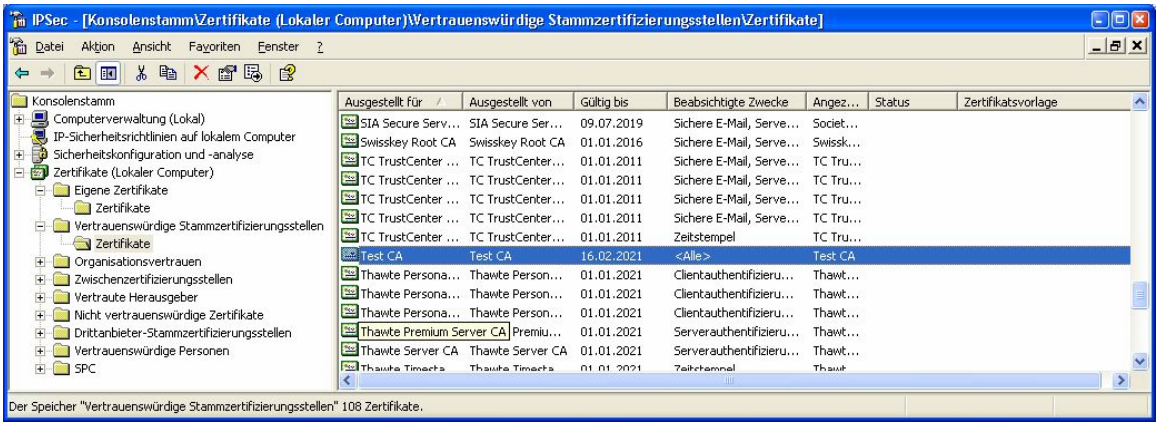
Die Option „Zertifikatspeicher automatisch wählen“ muss manuell aktiviert werden. Dadurch wird sowohl das Clientzertifikat, als auch das Rootzertifikat im richtigen Speicher abgelegt.



Nach einem Klick auf „Fertigstellen“, sollte folgender Dialog erscheinen:

Um den Erfolg des Importvorgangs selbst zu überprüfen, können wir nun in der Zertifikatsverwaltung nachschauen, ob die Zertifikate eingetragen sind. Bei meinen Tests war es gelegentlich nötig, die „IPSec.msc“ zu beenden und neu zu starten, damit die importierten Zertifikate angezeigt wurden. Das Ergebnis sollte so aussehen:





Beide Zertifikate müssen vorhanden sein, damit der Verbindungsaufbau später klappt.

!!! Der Import des Zertifikates mittels Doppelklick, das heisst, ohne das oben beschriebene Prozedere, genügt/funktioniert nicht !!!

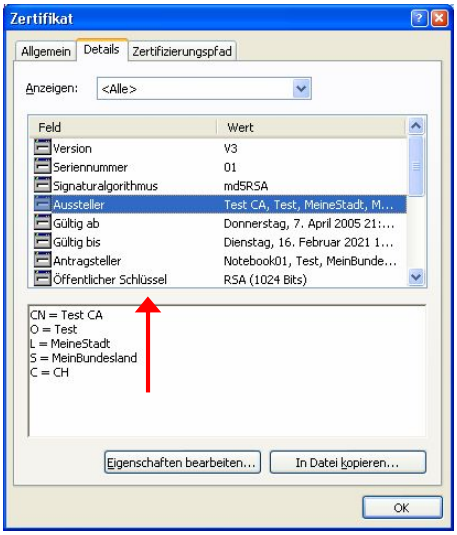
Der Grund hierfür ist, dass es sowohl Zertifikatsspeicher für jeden User, als auch einen Zertifikatsspeicher für die Maschine gibt. Bei einem Doppelklick wird das Zertifikat immer im Speicher des Users abgelegt. In der „IPSec.msc“ dagegen ist die Zertifikatsverwaltung für die Maschine (Lokaler Computer) geöffnet. Nur wenn die Zertifikate für den Computer gespeichert werden funktioniert später das VPN.

Jetzt muss nur noch die Datei „ipsec.conf“ an die lokalen Gegebenheiten angepasst werden. In unserem Beispiel müsste sie so aussehen:

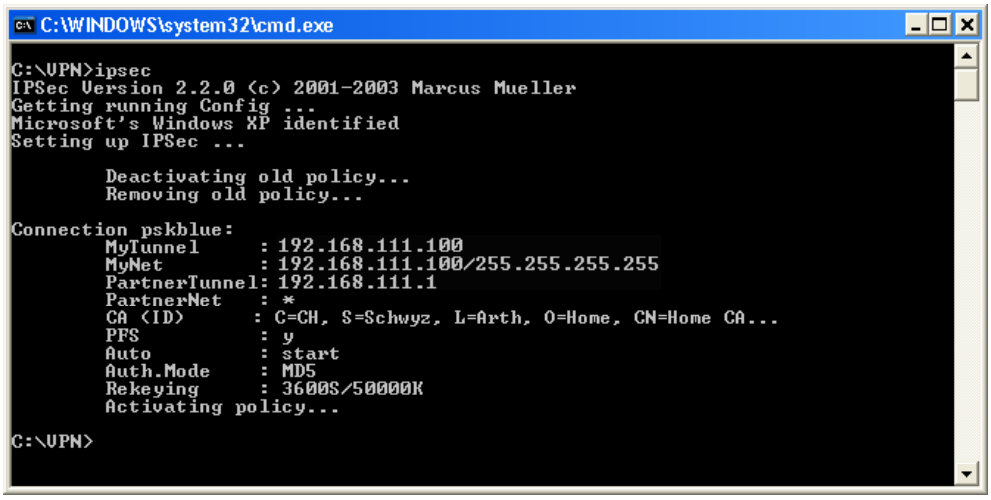
```
conn certblue
      left=192.168.111.1
      leftsubnet=*
      leftca="C=CH, S=MeinBundesland, L=MeineStadt, O=Test, CN=Test CA"
      right=%any
      network=auto
      auto=start
      pfs=yes
      authmode=MD5
```

Anmerkung: Statt 192.168.111.1 kann auch der FQDN, z. B. „ipcopVM.gutzeit.ch“, verwendet werden, vorausgesetzt, der Name kann aufgelöst werden. „leftsubnet=*“ beschreibt das Subnetz 0.0.0.0/0.0.0.0, also alle verfügbaren IP-Adressen, oder das gesamte Internet.

Die korrekten Einträge für „leftca=…“ findet man, wenn man in der IPSec.msc auf eines der importierte Zertifikat doppelklickt und unter „Details“ -> „Aussteller“ die Einträge im unteren Feld ausliest, s. Screenshot. Die Reihenfolge der zu übernehmenden Einträge ist von unten nach oben.

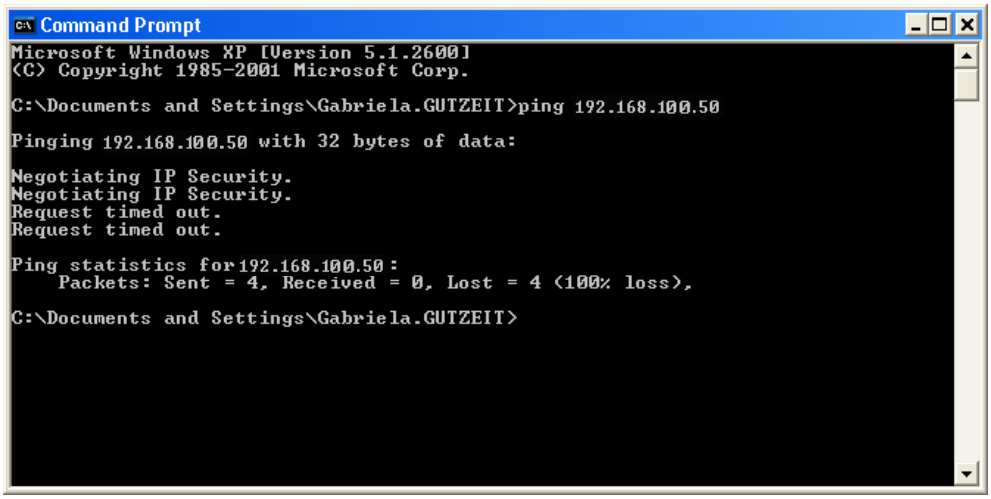


Nun kann auf einer Kommandozeile testweise C:\VPN\ipsec.exe aufgerufen werden. Es scrollen dann einige Linien über den Bildschirm, welch in etwa so aussehen:



Werden hier stattdessen Fehlermeldungen ausgegeben, hilft es meist, die Datei „ipsec.conf“ aus einer leeren *.txt Datei neu zu erstellen, sprich die wenigen Zeilen einfach abzutippen.

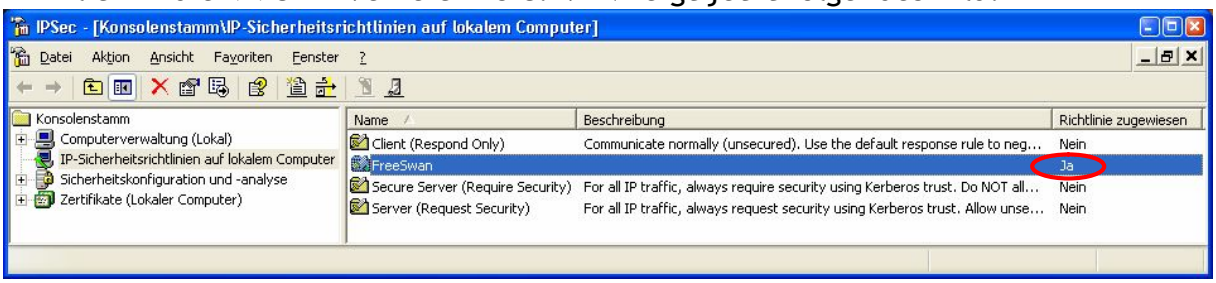
Ein Verbindungsversuch ins LAN mit „ping 192.168.100.50“ wird einige Male den Schriftzug „Sicherheit wird verhandelt“ ausspucken, bevor eine Rückantwort kommt. Dieses Verhalten ist normal.



Bei Verwendung von Windows XP SP2 erscheint, wie oben ersichtlich, ein Timeout statt der erwünschten Rückantwort des Servers im LAN. Dieses Verhalten ist der Personal Firewall von Windows XP zuzuschreiben. Wenn die PF deaktiviert ist, geht auch der Ping durch den Tunnel. Seltsamerweise genügte es bei meinen Versuchen gelegentlich, die Firewallkonfigurationsseite mehrfach ohne Änderungen aufzurufen während ein „ping -t 192.168.1“ lief. Plötzlich kamen die Antworten dann durch… Das explizite Erlauben von ICMP in der XP-Firewallkonfiguration funktionierte dagegen nicht.

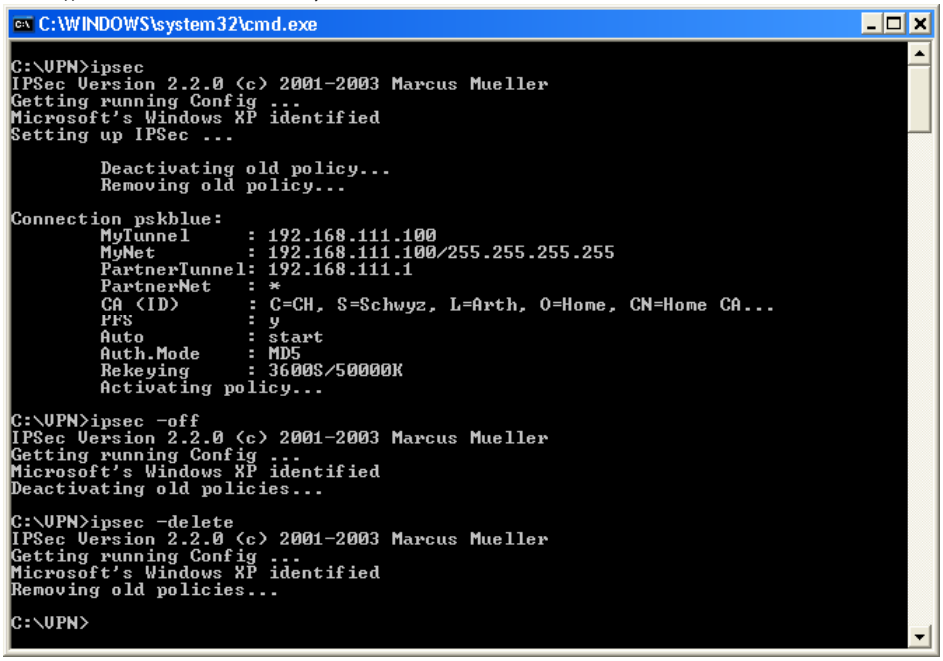
Jetzt steht das VPN und ein Blick in die Web-GUI des IPcop zeigt nach einem Refresh der Seite (erneuter Klick auf VPN im Kopf der Seite) folgendes Bild.

Ein Blick in die MMC im Verzeichnis C:\VPN zeigt jetzt folgendes Bild:

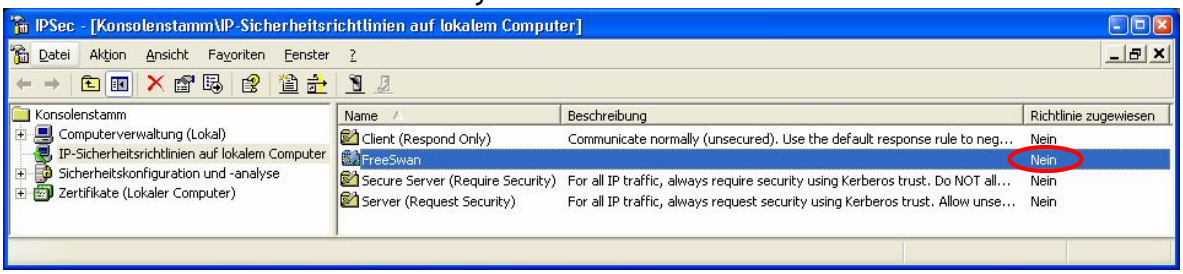


Das Markus Müller Tool hat mit den Informationen aus dem File „ipsec.conf“ eine IPsec-Konfiguration für Windows erstellt und aktiviert. Mit einem Doppelklick auf den Eintrag lassen sich nun die Details erforschen…

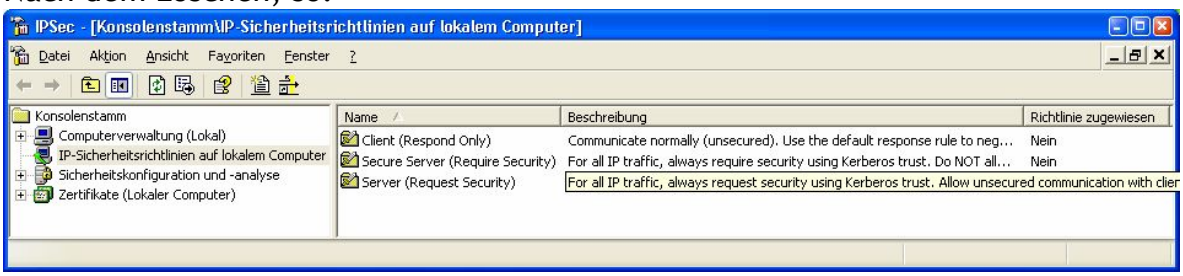
Um das VPN auf dem Client zu beenden, genügt ein „C:\VPN\ipsec.exe -off“. Um die VPN-Konfiguration endgültig aus dem Gedächtnis von Windows zu löschen, muss das Kommando „C:\VPN\ipsec.exe -delete“ eingegeben werden. Bei meinen Tests kam es gelegentlich vor, dass die Konfiguration mit „-delete“ nicht sauber gelöscht wurde. Wenn ich die Konfiguration dagegen zuerst mit „-off“ deaktivierte und dann mit „-delete“ löschte, funktionierte es immer.



Nach dem Deaktivieren der Policy sieht die MMC so aus:



Nach dem Löschen, so:



Solange ein VPN-Client immer via WLAN auf das Internet und das LAN zugreift, muss die IPsec-Policy nie deaktiviert, bzw. gelöscht werden. Die Konfiguration übersteht sogar einen Reboot ohne Probleme. Solange diese Policy jedoch aktiviert ist, versucht der Client immer ein VPN aufzubauen und verweigert **jegliche** unverschlüsselte Kommunikation!!!

Der VPN-Tunnel steht jetzt zwar, von einer brauchbaren Verbindung kann man so aber noch nicht ganz sprechen. Bisher ist eine Verbindung ins LAN nur über IP-Adressen möglich, was zwar funktioniert, aber doch recht unkomfortabel ist. Um diesem Missstand abzuhelfen, müssen wir nun noch die Namensauflösung einrichten.

Als Erstes sollte der DHCP-Server für BLUE so konfiguriert werden, dass als DNS-Server 192.168.111.1 (BLUE IPcop) verteilt wird.

Der zweite Schritt ist die Konfiguration des „hosts“-File auf dem IPcop. Seit der Version 1.4 lässt sich das zum Glück bequem via Web-GUI erledigen. Unter „Dienste“ -> „Hosts bearbeiten“ sollten alle Server/PCs mit der dazugehörigen IP erfasst werden. Damit Clients via DHCP immer die gleiche IP-Adresse erhalten, können Reservierungen eingerichtet werden, s. mein DHCP-Tutorial.

Wenn für WLAN-Clients bisher ein Eintrag unter „Firewall“ -> „Zugriff auf Blau“ eingerichtet war, kann dieser Eintrag nun entfernt werden, da der Client jetzt via VPN auf das Internet zugreifen kann , vorausgesetzt, das Remote-Subnetz wurde mit 0.0.0.0/0.0.0.0 definiert.

Weiter Möglichkeiten der Namensauflösung sind WINS-Server und/oder DNS-Server im LAN. Diese Konfiguration kann dann natürlich auch via DHCP verteilt werden.

Jetzt sollte es möglich sein, via „net use x: \\Servername\Sharename“ auf der Kommandozeile ein Netzlaufwerk zu mappen. Ebenso sollte es jetzt möglich sein, im Explorer entweder über die Adresszeile, oder über „Extras“ -> „Netzlaufwerk verbinden“ auf Shares im LAN zuzugreifen.

Wichtig: In der Netzwerkumgebung werden ohne WINS-Server keine weiteren Server/PCs auftauchen. Das ist normal, da die Netzwerkumgebung über NetBIOS Broadcasts „gefüllt“ wird. Broadcasts werden jedoch in der Regel von Routern geblockt, so dass die Netzwerkumgebung leer bleibt. Eine Verbindung ist jedoch trotzdem möglich.

Und jetzt?

- Wie geht das mit dem VPN auf RED für einen/mehrere Roadwarrior?
- Wie richte ich ein Netz zu Netz VPN ein?
- Ich habe Fragen zu anderen Themen.

Also weiter geht’s mit dem nächsten Tutorial.