Aufbau einer VPN-Verbindung zwischen einem IpCop-Router (1.4.8) und einem Roadwarrior bzw. zwischen zwei IpCop-Routern (1.4.8) mit PreSharedKeys

Ralf Petry, Berlin, 1.11.2005
ralf.petry@cityweb.de

Version 1.0
Versionsgeschichte:
1.11.2005 Erstellung dieser Anleitung
Geplante Erweiterungen: Einsatz von Zertifikaten, Einsatz eines linuxbasierten Roadwarriors

Vorbemerkung: Diese Anleitung entstand, nachdem ich längere Zeit benötigte, um die oben beschriebenen Szenarien um zu setzen und wurde möglich durch die intensive Hilfe der Gemeinschaft im Netz. Ich habe die Hoffnung, damit ein bisschen von dem an die Gemeinschaft zurück zu geben, was ich von ihr bekommen habe.
Unter http://ipcop.gutzeit.ch sind ausgezeichnete Tutorials erhältlich, die wissenswerte Hintergrundinformationen zum Thema IpSec bieten. Ich kann die Lektüre dringend empfehlen.
Grosser Dank und Respekt geht an Ecki, die Leute vom deutschen IpCop-Forum und die Entwickler von TauVPN.

Wichtig! Die beiden IpCops bzw. der IpCop und der Roadwarrior MÜSSEN aus unterschiedlichen Ip-Adressbereichen kommen – also bsw. steht der erste IpCop im Bereich 192.168.0.0/255.255.255.0 und der zweite IpCop oder der Roadwarrior im Bereich 192.168.23.0/255.255.255.0

In Zusammenhang mit meinem Arbeitsumfeld lag es in meinem Interesse, von meinem heimischen Arbeitsplatz auf entfernte Subnetze zu greifen zu können, um dort Fernwartungsarbeiten oder Anwenderfernbetreuung durch führen zu können.
Die entfernten Netze sind in der Regel Netze mit Windows-Clients (Windows 2000 Pro (mit SP 4) oder Windows XP Pro (mit SP 1 und SP 2)), Linux-Servern (mit Samba als Domänencontroller) und IpCop als Firewall/Router an einem DSL-Modem.
Mein heimischer Arbeitsplatz ist entweder ein Windows 2000 Pro (mit SP 4) Client oder ein Linux-Client (Kernel 2.6), jeweils hinter einer Fritz Box DSL, die im internen Heimnetz ausserdem per DHCP Adressen zu weist.

IpCop: Version 1.4.8 mit zwei Interfaces – Green und Red (Rot zeigt zum DSL Modem).

Vorarbeiten:
Roadwarrior (Host to Net)
Am entfernten Netz sind auf dem IpCop einige wenige Vorarbeiten zu leisten, ebenfalls am lokalen Windows-Client.

Net to Net
An beiden IpCop-Maschinen sind einige wenige Vorarbeiten zu leisten.

Vorarbeiten am IpCop (sowohl für Roadwarrior als auch für Net to Net Verbindungen):
Erhalten eines dynamisch auflösbaren Hostnamens über einen kostenlosen DNS-Service, unter der Voraussetzung, dass die IpCop-Maschinen bei jeder Einwahl vom Provider eine neue Ip-Adresse erhalten und nicht über eine fest-zugewiesene Ip-Adresse verfügen.

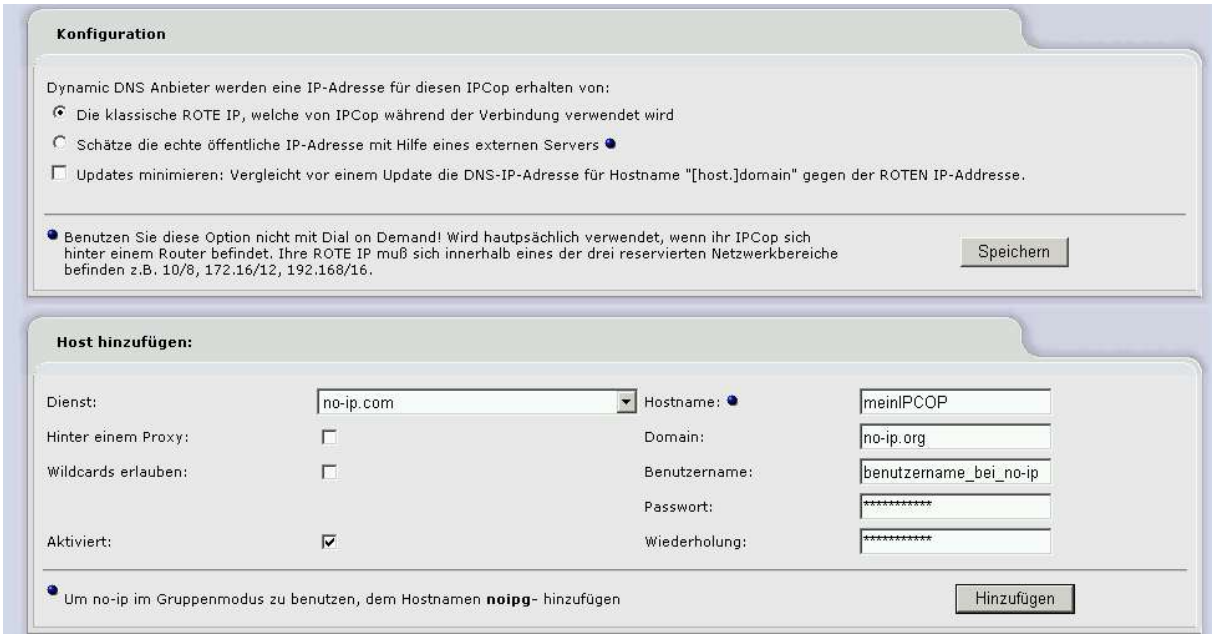
1. Aufruf der Seite www.dyndns.org oder www.no-ip.com
2. Anmeldung oder Registrierung, um seinen Host (IpCop) mit einem Hostnamen, der über das Internet auflösbar ist, zu versehen. (In der Regel reicht der kostenlose Service

der genannten Anbieter aus). (Ein möglicher Hostname wäre bsw. MeinIPCOP.no-ip.org)

Auf dem IpCop:

1. Im Administrationswebinterface auf den Reiter Dienste und dort auf Dynamischer DNS klicken

2. Entsprechend der eigenen Konfiguration ausfüllen. Wichtig sind die Felder für Benutzername und Kennwort – sie werden benötigt, damit der Update-Client der IpCop-Maschine die jeweils neu erhaltene Ip-Adresse an den Anbieter des dynamischen DNS-Dienstes melden kann.

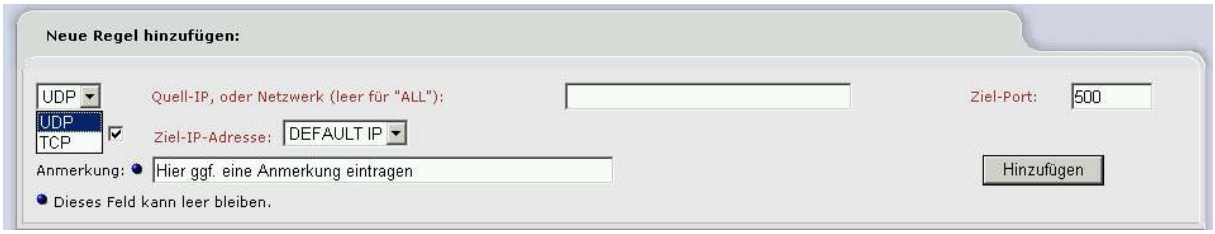


3. Auf Speichern bzw. Hinzufügen klicken. Wenn die Seite neu angezeigt wird, sollte in der Rubrik Aktuelle Hosts der relevante Eintrag stehen.

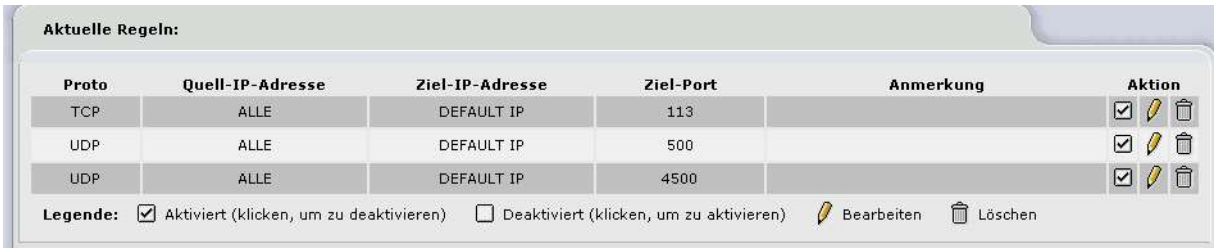
Im nächsten Schritt müssen auf dem IpCop (bei einer Net to Net Verbindung auf beiden Cops) die eingehenden Ports freigegeben werden:

1. Dazu den Registerreiter Firewall und dort Externer Zugang anklicken

2. Unter dem Punkt Neue Regel hinzufügen zuerst das Protokoll auswählen (UDP) und anschliessend im Feld Ziel-Port die Portnummer 500 eintragen



3. Auf Hinzufügen klicken, um diese Regel hinzu zu fügen.
4. Den gleichen Vorgang für den UDP-Port 4500 wiederholen
5. Anschliessend sollte die Webseite folgendes anzeigen (Beispiel)



Bei einem VPN-Net-to-Net Szenario zwischen zwei IpCops müssen die zuvor erwähnten Schritte auf beiden Seiten durchgeführt werden.

Jetzt könnte man mit der Einrichtung der VPN-Informationen auf der IpCop-Seite weitermachen. Dazu aber später, zuerst die Vorarbeiten auf der Windows-Client Seite.

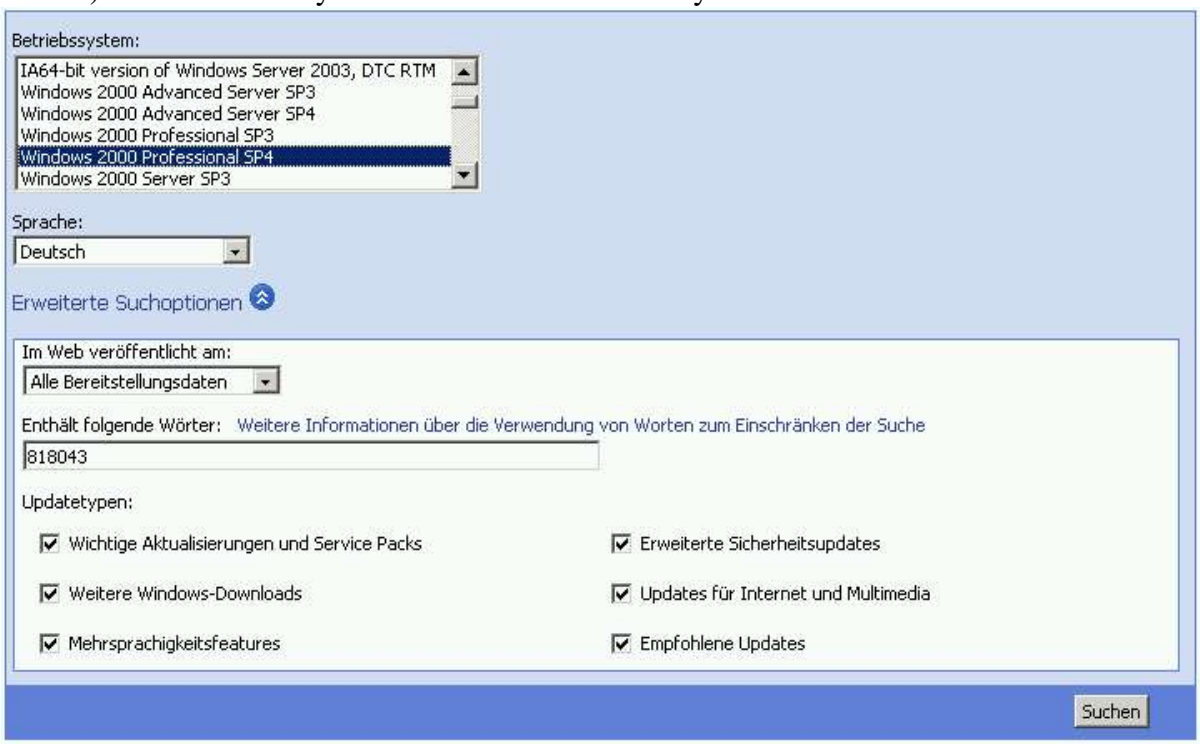
Ich habe mit den Ipsec-tools von Markus Müller meine ersten Versuche gestartet und bin grandios gescheitert (na ja, nicht ganz so grandios, aber trotzdem). Entweder hat noch irgendetwas gefehlt oder ich hatte eine Fehlkonfiguration – am Ende habe ich mich für den kostenlos erhältlichen TAUVpn Client entschieden (dazu später noch mehr). Der Client ist erhältlich unter http://sourceforge.net/projects/ivpn .

Windows 2000 Clients sollten mindestens SP 2 installiert haben – SP 4 ist noch besser (ein verantwortungsbewusster Administrator hat das sicherlich längst getan).
Windows 2000 Service Pack 4:
http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp
Windows 2000 benötigt darüber hinaus noch eine Datei zum Erstellen der IpSec-Policy:
http://agent.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp
(oder im Windows 2000 Resource Kit – wichtig ist die Version 1.22 oder höher und: in das Verzeichnis C:\Programme\Resource Kit\ installieren)

Windows XP SP 1 benötigt die Support Tools, die auf der Installations-CD im Verzeichnis support\tools liegen. Bitte mit Administratorrechten und als vollständige Version installieren.

Windows XP SP 2 benötigt ebenfalls die mit Administratorrechten und als vollständige Version zu installierenden Support Tools. Hier sollte aber nicht auf die Installations-CD zurück gegriffen werden, sondern auf die von Microsoft bereit gestellten aktuellsten Versionen:
http://support.microsoft.com/default.aspx?scid=kb;en-us;838079

Darüber hinaus benötigen alle Windows 2000 Clients bis Windows XP SP 1 einen IpSec-NAT Patch: (siehe auch http://support.microsoft.com/default.aspx?scid=kb;en-us;818043).
Zu diesem Zweck folgende Webseite aufrufen:
http://v4.windowsupdate.microsoft.com/catalog
Dort auf den Link für die Suche nach Updates für die Microsoft Betriebssystem suchen und in der darauf erscheinenden Webseite die erweiterten Suchoptionen öffnen. Im Feld „Enthält folgende Wörter“ die Ziffern des o.g. Artikels aus der Knowledgebase eingeben (also 818043). Unter Betriebssystem das relevante Betriebssystem auswählen.



Achtung! Windows XP Pro SP 1 Nutzer – in der Liste NICHT Windows XP Pro SP 1 sondern Windows XP SP 1 wählen.

Mir ist es passiert, dass unter der Angabe Windows XP Professional SP1 kein Update gefunden wurde... .

Auf Suchen klicken...
Das Update installieren und den Rechner neu starten.

Wenn alles getan ist ... (erst mal kein Schultheiss, sondern...), den TauVPN-Client herunterladen und installieren.
Dazu http://sourceforge.net/projects/ivpn öffnen. Ich habe mich dazu entschieden, nicht die aktuellste Beta-Version zu benutzen, sondern die letzte stabile Version – in meinem Fall die 0.35. Um diese zu erhalten, weiter unten auf der Seite auf den Link für „View all project Files“ (oder http://sourceforge.net/project/showfiles.php?group_id=81232) klicken und anschliessend die letzte stabile Version auswählen, herunterladen und installieren.

TauVPN-0.35 [show only this release]			2005-06-06 13:34
Download TauVPN-0.35-setup.zip	645337	1530 i386	.exe (32-bit Windows)
Download TauVPN-0.35-source.zip	329995	95 i386	Source .zip
Download TauVPN_how-to_0.35.pdf	229340	1257 Platform-Independent	pdf

Ich habe mir gleich noch die Anleitung mit heruntergeladen – auf 10 Seiten steht alles drauf, was man so braucht, um TauVPN zum Laufen zu bringen.

Jetzt beginnt die eigentliche Einrichtung der VPN-Verbindung

IpCop-Seite:
Auf den Registerreiter VPN und dort auf den Eintrag VPN klicken.

Im Bereich Globale Einstellungen im Feld Lokaler VPN Hostname ... den Namen eintragen, unter dem der IpCop bei dem Anbieter für den dynamischen DNS registriert ist (siehe auch weiter oben). Auf Aktiviert und anschliessend auf Speichern klicken.

Anschliessend im Bereich Verbindungsstatus und –kontrolle auf die Schaltfläche Hinzufügen klicken... es erscheint (die Seite, die alles entscheidet) (na ja, nicht ganz):

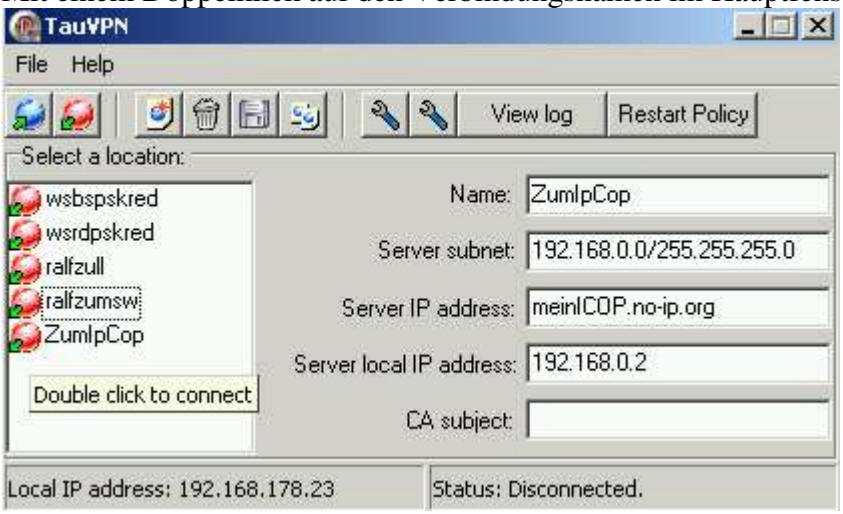
Hier muss der Verbindungstyp festgelegt werden: für’s erste bauen wir die RoadWarrior Verbindung auf: also auswählen und auf Hinzufügen klicken.
Anschliessend kann man die entsprechenden Eintragungen vornehmen. Im Feld Name kommt ein beliebiger Name für die Verbindung rein, ohne Leerzeichen etc.. Die Schnittstelle zeigt auf RED, das lokale Subnetz bezieht sich auf das Subnetz, dem der IpCop vorsteht. Remote Host/IP kann leer bleiben, unter Anmerkung habe ich eingetragen, wofür diese Verbindung

gut sein soll und im Feld Pre-Shared Schlüssel steht mein wahnsinnig geheimes Passwort drin.
Anschliessend auf Speichern klicken – woraufhin man zur VPN-Übersichtsseite zurückkehrt, wo mittlerweile die Verbindung aufgeführt wird (allerdings im Status Beendet).

An dieser Stelle sind wir für die IpCop-Seite fertig und wenden uns der Windows-Client Seite zu.
Alle Vorarbeiten sind erledigt (hoffentlich) und TauVPN ist installiert.
TauVPN wird aufgerufen, um eine entsprechende Verbindung einzutragen (siehe auch Anleitung für TauVPN).

Die dritte Schaltfläche von links () erlaubt das Anlegen einer neuen Verbindung.

Die Eintragungen in den Feldern sprechen eigentlich für sich – der Verbindungsname ist frei wählbar, Preshared key ist auszuwählen und im Feld Preshared key einzutragen (muss dem Passwort entsprechen, das bei der Konfiguration der VPN-Verbindung auf dem IpCop benutzt wurde). Das Server subnet entspricht dem Subnetz, das hinter dem IpCop liegt, die Server IP ist die dynamische Adresse und die Server local IP entspricht der IP-Adresse, die die grüne Netzwerkschnittstelle des IpCop erhalten hat.
Auf OK klicken.
In den Global Settings, erreichbar aus dem Hauptfenster (der linke der beiden Schraubenschlüssel), unter dem Registerreiter Advanced, sind noch das Oakley-log zu aktivieren (das aber erst nach einem Rechnerneustart tatsächlich protokolliert wird – siehe auch Anleitung für TauVPN).
Mit einem Doppelklick auf den Verbindungsnamen im Hauptfenster



wird die VPN-Verbindung aufgebaut. Wenn alles klappt, kommt folgende Meldung aus dem Systemschacht (Hier leicht abgewandelt, da der Screenshot auf eine andere Verbindung verweist):

Glückwunsch.
Fertig.
Rumspringen, freuen, Bier aufmachen, Nachbarn holen, Stolz wie Bolle sein.

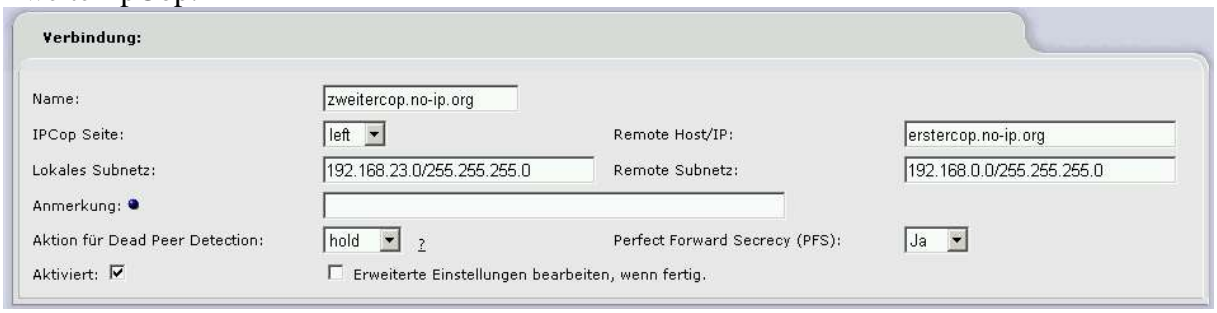
Oder...

Sich an der Net to Net Verbindung probieren...

An Vorarbeiten ist auf beiden IpCops das gleiche zu leisten: Anmelden eines dynamisch auflösbaren Namens, Einrichtung des Updateclients (Dienste, dynamischer DNS), Portfreigabe (Firewall, Externer Zugang), darauf achten, dass beide IpCops einem jeweils unterschiedlichen Netz angehören.
Anschliessend unter VPN, VPN weiter arbeiten:
In den Globalen Einstellungen den jeweiligen Hostnamen eintragen (der selbstverständlich für jeden der beiden IpCop anders lauten muss!!!), ggf. auf Aktiviert und anschliessend auf Speichern klicken.

Im Bereich Verbindungsstatus und –kontrolle auf Hinzufügen klicken und anschliessend beim Verbindungstyp Netz zu Netz auswählen und auf Hinzufügen klicken.
Was im ersten Cop eingetragen wird, wird beim zweiten gewissermassen spiegelbildlich gemacht:
Erster IpCop:

Zweiter IpCop:



die Bezeichnung left (bei IpCop Seite) bedeutet übrigens immer lokal und right immer entfernt (remote).

Jeweils Speichern und fertig ist der Lack. Das Schöne an der Net to Net Verbindung ist die Tatsache, dass ich mit den Clients hinter den Routern in die anderen Netze komme, ohne irgendwelche Programme installiert haben zu müssen (zu haben müssen?), das im Moment noch weniger Schöne ist die für mich noch offene Frage, wie ich den Verbindungsauf- bzw. abbau steuern kann – aber das kommt auch noch.

Viel Erfolg beim Nachbauen.