Virtual Private Networks mit IPCop hinter Routern

Vorbemerkung:

Dieses Dokument beschreibt einen Lösungsweg, wie ich mehrere VPN-Tunnel hinter einem NAT-Router erfolgreich eingerichtet habe.
Meine beiden IPCops sind Dell Optiplex GX115 mit Intel PIII (866MHz) Prozessoren, 128 MB RAM und einer 10GB Festplatte. Mittlerweile haben sich ein anderer IPCop und ein Windows Roadwarrior noch dazu gesellt.
Die Cops laufen natürlich mit der aktuellsten Softwareversion 1.4.21. Zusätzlich sind die Addons BOT, NetTraffic, Coptime und Watch-My-Tunnel installiert.

Folgendes Szenario soll dabei realisiert werden:

- Erstellung mehrerer Net-to-Net-VPNs zwischen drei IPCops.
- Jeder IPCop befindet sich hinter einem NAT-Router
- VPN-Authentifizierung mit Zertifikaten.
- Automatischer VPN Neustart nach unterbrochener Internetverbindung. (Zwangstrennung)

Inhalt:

A. Netzaufbau

Anfangs möchte ich nur die Verbindung zweier IPCops beschreiben. Die Einrichtung des dritten IPCops findet natürlich analog dazu statt.

Standort A und Standort B sind wie bereits erwähnt, identisch aufgebaut. Jeder verfügt über einen DSL Zugang mit Dynamischer IP und einem Account bei einem DynDNS-Anbieter. Der NAT-Router, in diesem Beispiel die FritzBox läuft als Router, da an ihr noch VoIP-Telefone angeschlossen sind und diese Funktion auch weiterhin erhalten bleiben soll.

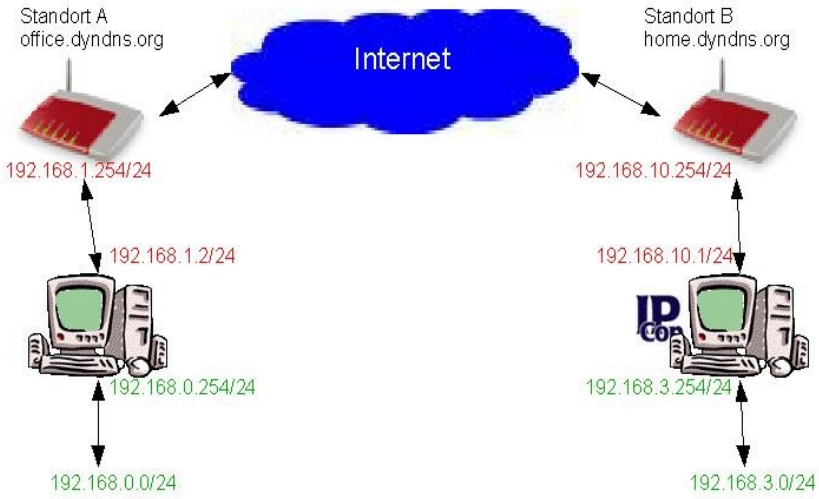

Abbildung 1: Netzabbild

Zwischen Router und IPCop befindet sich das ROTE NETZ. In diesem Beispiel habe ich ein 24er Netz gewählt. Es ist aber auch ein Netz mit einer 30er Maske möglich, da ja sowieso nur 2 Hosts in diesem Netz sind. Hinter dem IPCop befindet sich das GRÜNE NETZ. In diesem Netz sind alle vor dem bösen Internet geschützten Hosts untergebracht.

Bei den beiden Standorten ist zu beachten das nirgends die selben Subnetze eingerichtet worden sind, damit das Routing später noch funktionieren kann.

Bei der Konfiguration hatte ich beide Cops neben mir stehen und konnte so uneingeschränkt auf beide Weboberflächen zugreifen. Der eine Cop hat sich dabei ganz normal über den DSL-Router eingewählt und für den anderen hab ich eine Test-ISDN Verbindung hergestellt, ebenfalls durch Unterstützung eines NAT-Routers. Ist DynDNS schon eingerichtet, wäre es auch möglich die IPCops über die Ferne zu administrieren.

B. Vorarbeiten

1.IPCop

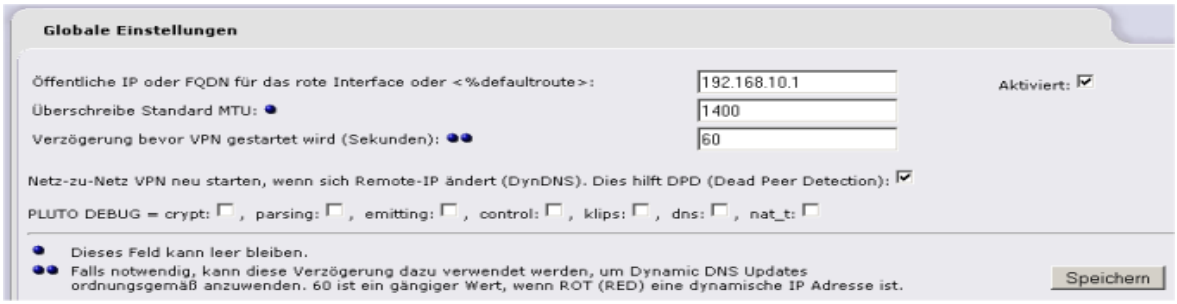

Abbildung 2: Globale Einstellungen der Verbindung

Wir beginnen mit einer jungfräulichen VPN-Einstellung, d.h. Keine Zertifikate und sonstigen Einstellungen sind bis jetzt getätigt. Bei den Globalen Einstellungen müsst ihr die RED-IP des IPCops angeben. Mit der MTU hatte mit dem Wert 1400 gute Ergebnisse. Wobei man durchaus noch mit verschiedenen Werten experimentieren könnte. Die Verzögerung hab ich auf 60 Sekunden eingestellt damit der Router noch genügend Zeit hat, die IP bei einem DynDNS-Anbieter zu aktualisieren. Die Dead-Peer-Detection sollte natürlich aktiviert werden. Dann einen Haken bei Aktivieren und abschließend auf Speichern klicken.

Zertifikate:

Als nächstes müssen die CA- und Host-Zertifikate erstellt werden. Der Hostname wird automatisch ausgefüllt und müsste die ROTE IP des IPCops beinhalten. Dem Zertifikat geben wir einen eindeutigen Namen, der bei mir nur aus Kleinbuchstaben und keinen Sonderzeichen besteht. Die optionalen Felder hab ich freigelassen. Das CA-Zertifikat und das Host-Zertifikat hab ich nun auf dem lokalen Rechner gespeichert und hab jedem einen eindeutigen Namen zugeordnet.

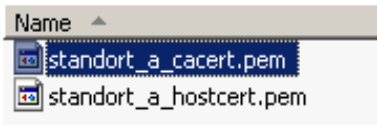

Abbildung 3: Eindeutige Bezeichnung erleichert das Arbeiten ungemein

Nachdem alle Zertifikate auf allen Cops erstellt wurden, müssen die jeweiligen CA's auf den Gegenstellen-Cops importiert werden um dem IPCop die CA der Gegenseite bekannt zu machen. Das ganze sollte jetzt so wie auf dem Bild aussehen. Abbildung 4 ist ein Screenshot von den Zertifizierungsstellen. Das Root-Zertifikat ist die eigene CA, darunter das eigene Host-Zertifikat. In der dritten Zeile das neu importierte CA-Zertifikat der Gegenstelle. Für weitere Cops müssen dementsprechend die jeweiligen CA's importiert werden.

Abbildung 4: So sieht die erfolgreiche Importierung des Zertifikats aus. In der dritten Zeile finden wir nun das Root-(CA)-Zertifikat des IPCops der Gegenseite.

Verbindung:

Nun zur Verbindungskonfiguration. Als nächstes erstellen wir eine neue Netz-zu-Netz Verbindung. Für den Namen der Verbindung hab ich auch **nur Kleinbuchstaben** und **keine Sonderzeichen** verwendet. Die Host IP-Adresse und das lokale Grüne Subnetz wurde auch schon ausgefüllt. Nun nur noch für die Remoteseite den Host, das Subnetz und die ID eintragen.

Abbildung 5: Erstellung eines Netz-zu-Netz-VPNs

Abbildung 6: IP- und Hosteinstellungen des neuen VPNs

Bei Authentifizierung wählen wir „*Ein Zertifikat hochladen*" und wählen das entsprechende **Host-Zertifikat des Remote-IPCops**.

Abbildung 7: "Ein Zertifikat hochladen" und das Host-Zertifikat der Gegenstelle auswählen. Wird die Konfiguration gespeichert, so wird auch das Zertifikat hochgeladen.

Ein Klick auf den Speichern-Button beendet die Konfiguration der Verbindung. Danach wird man auf die VPN-Übersichtsseite weitergeleitet. Jetzt loggen wir uns mit Putty oder WinSCP bzw. dem dementsprechenden Linuxtools (fish:// usw.) auf dem IPCop ein und beginnen mit der Bearbeitung der Konfigurationsdateien.

a) ipsec.conf

Die Konfigurationsdatei /var/ipcop/vpn/ipsec.conf muss nach der Bearbeitung folgendermaßen aussehen:

```
config setup
        interfaces="%defaultroute "
        klipsdebug="none"
        plutodebug="none"
        plutoload=%search
        plutostart=%search
        virtual_private=%v4:192.168.0.0/16,%v4:!192.168.3.0/255.255.255.0
        uniqueids=no
        nat_traversal=no                        # NAT-T ausschalten
        overridemtu=1500                        # Muss nicht angepasst werden

conn %default
        keyingtries=0
        disablearrivalcheck=no

conn namederverbindung #RED
        left=192.168.10.1
        leftnexthop=%defaultroute
        leftsubnet=192.168.3.0/255.255.255.0
        right=office.dyndns.org
        rightsubnet=192.168.0.0/255.255.255.0
        rightnexthop=%defaultroute
        leftcert=/var/ipcop/certs/hostcert.pem
        rightcert=/var/ipcop/certs/namederverbindungcert.pem
        leftid="@home.dyndns.org"
        rightid="192.168.1.2"
        ike=aes128-sha-modp1536,aes128-sha-modp1024,aes128-md5-modp1536,aes128-md5-
modp1024,3des-sha-modp1536,3des-sha-modp1024,3des-md5-modp1536,3des-md5-modp1024
        esp=aes128-sha1,aes128-md5,3des-sha1,3des-md5
        ikelifetime=1h
        keylife=4h
        dpddelay=30
        dpdtimeout=120
        dpdaction=restart
        pfs=yes
        authby=rsasig
        leftrsasigkey=%cert
        rightrsasigkey=%cert
        auto=start
```

Wichtig: Im Abschnitt config setup muss nat_traversal=no eingetragen werden, da sonst im Logfile „Both are NATed“ auftaucht. Ipsec erwartet dann die Pakete auf Port 4500/UDP.

b) ipsec.secrets

Die ipsec.secrets muss noch von Hand bearbeitet werden. Die Einträge für `left` und `right` werden aus der `ipsec.conf` übernommen.

```
192.168.10.1 office.dyndns.org : RSA /var/ipcop/certs/hostkey.pem
192.168.10.1 munich.dyndns.org : RSA /var/ipcop/certs/hostkey.pem
```

In diversen HowTos wird darauf hingewiesen, das unbedingt ein Leerzeichen nach dem Doppelpunkt stehen muss. Will man mehrere VPNs realisieren, fügt man weitere Zeilen bestehend left, right und dem Pfad zur hostkey.pem hinzu.
Wichtig ist nun, das nach jeder Bearbeitung der Verbindung bzw. ein Klick auf Neustart der Verbindung die Konfigurationsdateien neu geschrieben werden und Änderungen verloren sind.

B. Vorarbeiten

2.NAT-Router

Nun zu den Vorbereitungen am Router, was in meinem Fall jeweils eine FritzBox ist.

Im folgenden werden die benötigten Portweiterleitungen eingerichtet. Dazu gibt es mehrere Möglichkeiten. Entweder man gibt die ROTE IP des IPCops als „**Exposed Host**" an. Dadurch werden alle Ports für die keine spezielle Regel erstellt wurde an den IPCop weitergeleitet. In der Weboberfläche finden wir nun folgenden Hinweis:

Achtung: Die Firewall Ihrer FRITZ!Box ist deaktiviert.
Der als "Exposed Host" angegebene Computer ist ungeschützt im Internet sichtbar und erreichbar. Ausgenommen sind Portfreigaben zu anderen Computern in der Liste der Portfreigaben, welche nur an diese weiter geleitet werden.

Dieser Hinweis sollte uns ja nicht wirklich stören, da der IPCop ja eine Firewall mitbringt.
Die zweite Möglichkeit besteht darin, nur die benötigten Ports an den IPCop weiterzuleiten.

Source Port	Protocol	Destination IP	Destination Port
500	UDP	IPCop RedIP	500
N/A	ESP	IPCop RedIP	N/A

Liste der Portfreigaben

Aktiv	Bezeichnung	Protokoll	Port	an IP-Adresse	an Port		
☑	VPN1	UDP	500	192.168.10.1	500		
☑	VPN3	ESP		192.168.10.1			

Abbildung 8: Die Übersicht aller eingerichteten Portfreigaben sollte nun so aussehen.

Zu beachten ist dabei, das Port 4500 UDP nicht zum IPCop weitergeleitet wurde, da Port 4500 nur gebraucht wird, wenn NAT-Traversal aktiviert ist und ESP-Pakete in UDP-Paketen verschickt werden. Da wir aber eine Portweiterleitung eingerichtet haben, entfällt für diese Regeln das NAT. Zum Abschluss müssen noch unsere geforderten ESP-Pakete an den IPCop weitergeleitet werden.

C. Abschluss

Zum Abschluss der Einrichtungsarbeiten muss das IPSec-Modul noch neu gestartet werden. Da die Weboberfläche bei jeder „Berührung" die Konfigurationsdateien neu schreibt, loggen wir uns per SSH auf beiden IPCops ein und starten mit dem Befehl ipsecctrl S das Modul ipsec neu.

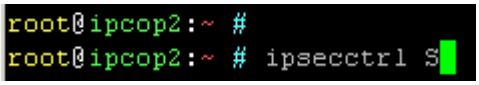

Abbildung 9: ipsecctrl S bewirkt einen Neustart des VPN-Moduls.

Eine Kontrolle in der Weboberfläche des IPCops sollte nach einiger Zeit das gewünschte Ergebnis zum Vorschein bringen.

Abbildung 10: Steht der Tunnel wird das „BEENDET" durch das „OFFEN" Symbol ersetzt.

Pings und der Zugriff auf Windowsfreigaben usw. dürften nun von einem Client im grünen Netz ins andere grüne Netz problemlos möglich sein. Sollte etwas nicht funktionieren, so sind zuerst die Firewalleinstellungen in BOT zu kontrollieren ggf. BOT kurz deaktivieren. Im Zuge der neuen BOT-Version sind weitere (IPSEC-RED) Interfaces eingerichtet worden, womit der Verkehr auf dem ipsec-Interface genauer definiert werden kann.

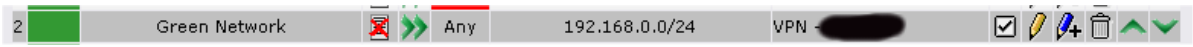

Abbildung 11: Freigabe in BOT für das VPN. Auf der Gegenseite natürlich auch.

Die VPN's die ich nach dieser Anleitung eingerichtet habe laufen schon über mehrere Tage durch DPD, vpn-watch bzw. watch-my-tunnel über mehrere Zwangstrennungen bzw. unterbrochene Internetverbindungen problemlos hinweg.
Im Log sind nur folgende „Fehlermeldungen" zu finden, wobei IP für die öffentliche IP der Gegenstelle steht.

```
packet from    IP    :500: Informational Exchange is for an unknown (expired? ) SA
```

Das passiert immer kurz bevor eine neue IKE-Verhandlung abläuft und ist meiner Meinung nach als „normal" anzusehen ist, da kurz danach

`ISAKMP SA established` bzw. `sent QI2, IPsec SA established`
im Log auftaucht.

Viel Spaß beim nachbauen ;-)

PS:
Bei Fragen oder Verbesserungsvorschläge wendet euch doch an www.ipcop-forum.de, dort gibt es gute Links ohne die es mir auch nicht möglich gewesen wäre ein VPN einzurichten. Ich möchte mich hiermit auch ganz herzlich bei allen denen bedanken, die durch ihre Antworten im Forum bzw. HowTos und FAQs auf anderen Homepages die funktionierende Einrichtung mehrerer VPNs möglich gemacht haben.

