IPcop v1.4

VPN auf BLUE mit PSK

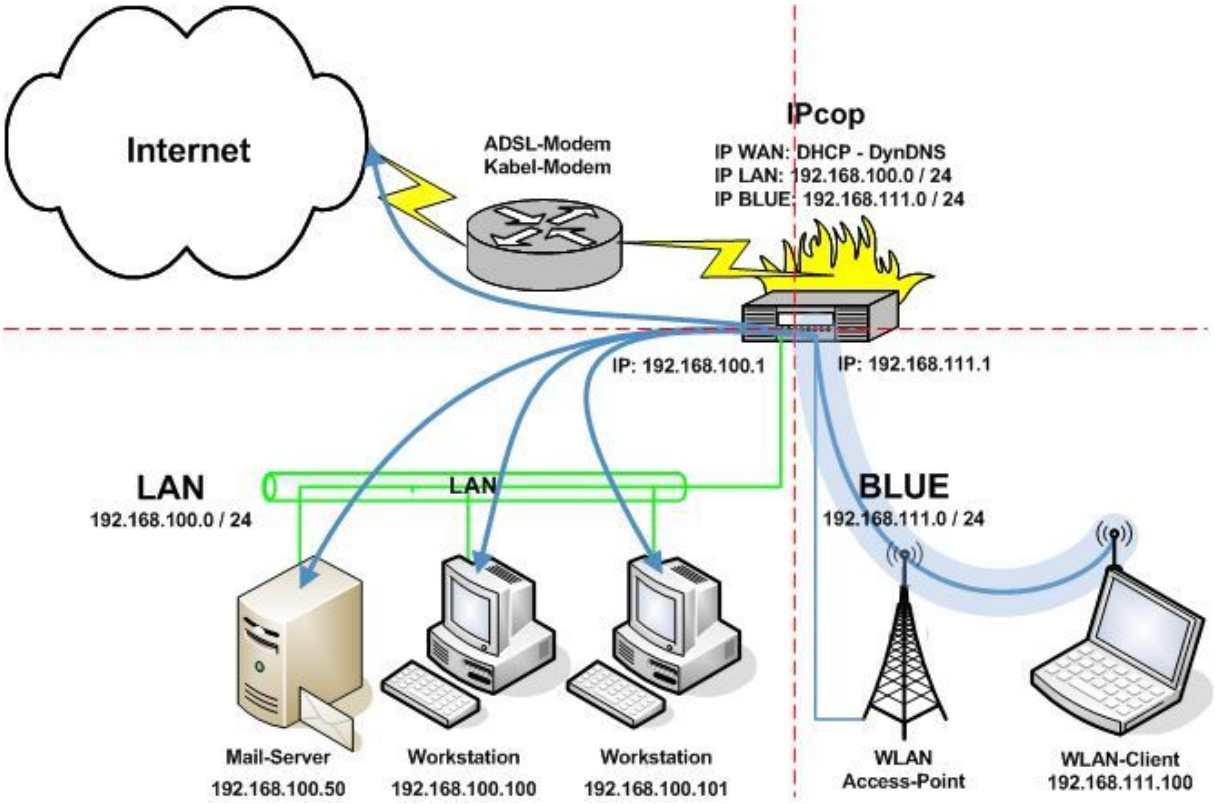
Grundsätzliches

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.
Zuerst werden die Begriffe VPN und IPsec erklärt. Anschliessend werden die Einstellungen besprochen, die nötig sind, um ein VPN mit einem WLAN-Client am blauen Interface aufzubauen.

Vorbereitung

1. Grundkonfiguration des IPcop erfolgreich durchgeführt.
2. Blaue Netzwerkkarte installiert und konfiguriert.
3. Vorstellung, wie das Netzwerk aussehen soll.

Beispiel eines Netzwerks



Was ist ein VPN?

VPN steht für Virtual Privat Network. Es ermöglicht eine sichere Übertragung von Daten über ein unsicheres Netzwerk. Dazu wird ein virtueller, verschlüsselter Tunnel zwischen zwei Partnern eingerichtet, welche dann auf einem, für andere Personen nicht abhörbaren Weg, miteinander kommunizieren können. Genau genommen müsste ein Tunnel nicht zwingend verschlüsselt werden, um VPN genannt zu werden, unverschlüsselte Verbindungen können ebenfalls als VPN bezeichnet werden. Normalerweise sind die Tunnel heutzutage aber über unterschiedliche Verschlüsselungstechniken geschützt.

Dabei kommen in der Regel 2 verschiedene Techniken zum Einsatz. Auf Microsoftseite wird seit längerer Zeit PPTP (Point to Point Tunneling Protokoll) verwendet. Aufgrund von Sicherheitslücken ist dieses Protokoll nicht mehr uneingeschränkt als sicher einzustufen. Auf dem IPcop ist PPTP daher nicht implementiert. Microsoft bietet seit Windows 2000 die Möglichkeit, IPsec zur Verschlüsselung von Tunnels zu verwenden. Dabei geht Microsoft jedoch einen anderen Weg, als die meisten anderen VPN-Implementationen. Microsoft verwendet als Tunneling-Protokoll L2TP (Layer 2 Tunneling Protokoll), welches auf Layer 2 (OSI-Referenzmodell) für den Tunnelaufbau verantwortlich zeichnet. Da L2TP keinerlei Verschlüsselung bietet, setzt Microsoft IPsec auf Layer 3 ein, um den Inhalt vor unbefugten Augen zu schützen.

Dieser Ansatz macht einen direkten, assistentengestützten Verbindungsaufbau mit dem IPcop leider unmöglich. Wie es dennoch recht einfach und fast ausschliesslich mit Bordmitteln zu schaffen ist, will dieses Tutorial zeigen.

IPsec, als zweite wichtige Technik ist ein Industriestandard, welcher plattformübergreifend (Windows, Linux, Unix, Mac,…) verfügbar ist. IPsec ermöglicht neben Vertraulichkeit (durch Verschlüsselung) und Authentizität (digitale Signatur), auch Datenintegrität (Prüfsumme, wodurch sich Änderungen feststellen lassen). Zusätzlich besteht ein Schutz gegen Replay-Attacken. Damit ist IPsec eine allseits anerkannt sichere Technik zur Verschlüsselung von IP-Traffic.

Wichtige Begriffe in Verbindung mit IPsec:

- IKE (Internet Key Exchange), sorgt für die automatische Schlüsselverwaltung von IPsec. Hierzu wird der Diffie-Hellmann Algorithmus zum sicheren Schlüsselaustausch über ein unsicheres Netzwerk verwendet. IKE kommuniziert über UDP-Port 500
- SA (Security Association), Ergebnis der Verhandlungen zwischen den VPN-Partnern. Hierin werden die Authentifizierungs- und Verschlüsselungsalgorithmen für die weitere Kommunikation festgelegt.
- AH (Autentication Header), sorgt für Integrität und Authentizität der übertragenen Pakete. Zusätzlich werden damit Replay-Attacken (Aufzeichnen und späteres Abspielen einer Datenübertragung) verhindert. AH versucht, alle Daten in einem IP-Datagramm zu schützen. Es werden nur Felder ausgeschlossen, die sich auf dem Weg sicher ändern. Im Unterschied zu ESP werden die Nutzdaten nicht verschlüsselt, sondern nur vor Veränderung geschützt.
- ESP (Encapsulated Security Payload), soll die Authentifizierung, Integrität und Vertraulichkeit von IP-Paketen sicher stellen. Im Unterschied zu AH wird der Kopf des IP-Paketes nicht mit berücksichtigt. AH und ESP können auch kombiniert verwendet werden.
- Main Mode (Phase 1), wird in der ersten Phase von IKE genutzt. Hierbei handeln der Initiator (derjenige, der die Verbindung aufnehmen will) und der Antwortende miteinander SAs aus. Diese "Verhandlung" geschieht in folgenden sechs Schritten:
    1. Initiator sendet einen oder mehrere Vorschläge mit Authentifizierungs- und Verschlüsselungsalgorithmen.
    2. Antwortender wählt einen Vorschlag aus und bestätigt diesen.
    3. Initiator sendet den öffentlichen Teil der Diffie-Hellmann-Schlüsselvereinbarung und einen zufälligen Wert (Nonce).
    4. Antwortender schickt ebenfalls den öffentlichen Teil der Diffie-Hellmann-Schlüsselvereinbarung und einen zufälligen Wert (Nonce).
    5. Initiator berechnet Signatur und sendet diese mit seiner Identität an den Antwortenden. Diese Daten werden mit einem symmetrischen Schlüssel verschlüsselt.
    6. Antwortender schickt die gleiche Daten von seiner Seite an den Initiator.

- Quick Mode (Phase 2), wird in der zweiten Phase von IKE zur Anwendung gebracht. Die gesamte Kommunikation in dieser Phase erfolgt verschlüsselt. Wie in der ersten Phase wird zunächst ein Vorschlag (Proposal) gemacht. Dieser wird zusammen mit einem Hashwert und der Nonce übertragen. Später werden die Schlüssel neu berechnet, und es gehen keinerlei Informationen aus den zuvor generierten SAs ein. Dies stellt sicher, dass niemand von den zuvor generierten Schlüsseln auf die neuen schließen kann.
- PSK (Pre Shared Key), steht für ein Passwort, welches für die Aushandlung der Sitzungsschlüssel verwendet wird. Wenn PSK verwendet wird, müssen alle Verbindungen dasselbe Passwort verwenden. Dieser Umstand macht PSK in Umgebungen mit vielen Verbindungen (Roadwarrior) anfällig. Fällt das Passwort eines Roadwarrior in falsche Hände, muss es für alle Verbindungen geändert werden.
- X.509, steht für ein digitales Zertifikat. Dieses Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle (CA, Certification Authority) signiert sein. Es ist immer an einen DN (Distinguished Name), meist den DNS-Namen, gebunden und damit eindeutig einem PC/Server zugeordnet.
- NAT-T, (NAT-Traversal) erlaubt IPsec-Verbindungen durch NAT Devices wie z. B. ADSL-Router. Dazu wird zusätzlich UDP Port 4500 benötigt. Windows PCs, mit Ausnahme von Windows XP SP2, benötigen einen Hotfix,s. http://support.microsoft.com/default.aspx?scid=kb;en-us;818043

Das Ziel

Was wollen wir erreichen?

Meine Vorstellung von einem sicheren WLAN ist die, dass jemand, der sich tatsächlich die Mühe gemacht hat, meinen WEP128 Schlüssel zu knacken (mehr gibt meine Hardware leider nicht her), nachher trotzdem weder Zugriff auf meine Daten erhält, noch in irgendeiner Weise meinen Internetzugang missbrauchen kann.

Wir haben es also mit zwei unterschiedlichen Herausforderungen zu tun.

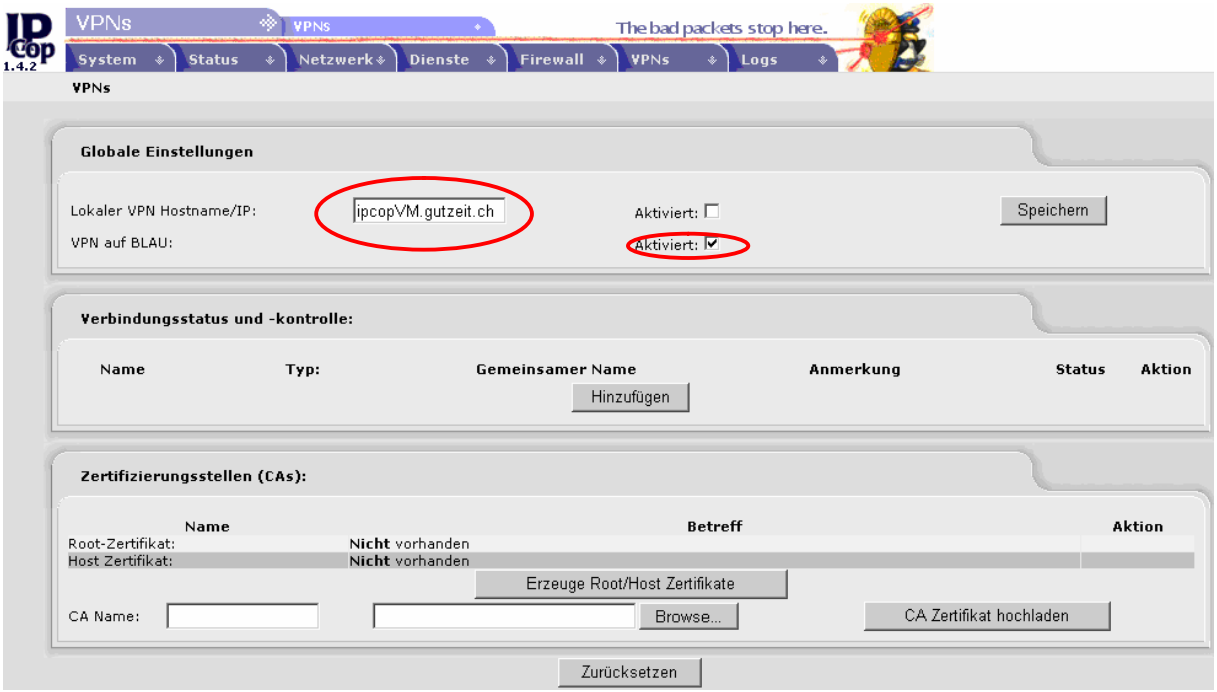
1. Datensicherheit. Dies kann durch sichere Verschlüsselung (IPsec) auf der WLAN-Strecke gewährleistet werden.

2. Schutz des Internetzugangs vor Spammern, Hackern/Crackern, oder auch nur dem „tauschwütigen Nachbarn“. Dieses Ziel lässt sich nur erreichen, wenn aller Verkehr vom WLAN aus vom IPcop geblockt wird und nur Traffic via VPN erlaubt wird.

Prinzipiell besteht bei der im Folgenden vorgestellten Konfiguration nicht einmal mehr die Nötigkeit, die Verschlüsselung für das WLAN, sei es WEP oder WPA, zu aktivieren. Alle Daten werden prinzipiell IPsec-Verschlüsselt in den Äther geschickt und ein Zugriff auf das Internet ist für einen Client ohne funktionierende VPN-Konfiguration auch nicht möglich. Trotzdem sollte auf der WLAN-Hardware immer die höchstmögliche Verschlüsselung (WEP, WPA,…) verwendet werden.

Die Konfiguration

Übersicht



Erklärungen zu den einzelnen Optionen

Lokaler VPN Hostname/IP:	Wenn FQDNs verwendet werden, sollte hier der FQDN des IPcop stehen. Dies ist vor allem bei einem VPN auf RED wichtig, wenn keine fixe IP-Adresse vorhanden ist. Dann sollte hier z. B. der DynDNS-Name stehen. Für ein VPN nur auf BLUE, reicht auch die IP-Adresse. Besser ist jedoch auch hier ein FQDN. Dieser Name kann leicht über das hosts-File auf dem IPcop in eine IP-Adresse aufgelöst werden.
VPN auf Blau:	Sollte natürlich aktiviert werden.
Hinzufügen:	Hier können später verschiedene VPN-Konfigurationen erzeugt werden.
Erzeuge Root/Host Zertifikat:	Wenn ein VPN mit X.509 Zertifikaten eingerichtet werden soll, müssen hier erst die benötigten Zertifikate erstellt werden.
CA Zertifikat hochladen:	Hier könnte ein bestehendes Root-Zertifikat auf den IPcop hochgeladen werden. Kommt in Frage, wenn man über eine eigene CA (Certification Authority) verfügt und die Zertifikate daher nicht auf dem IPcop erstellen möchte.
Speichern:	Nicht vergessen zu speichern, damit die entsprechenden Firewallregeln auf dem IPcop aktiviert werden !!!

VPN mit PSK

Als erstes werden wir jetzt ein VPN mit PSK einrichten. Diese Variante ist leicht zu implementieren und eignet sich daher besser für die ersten Schritte.

Checkliste:

Auf der Seite des IPcop werden folgende Informationen benötigt:

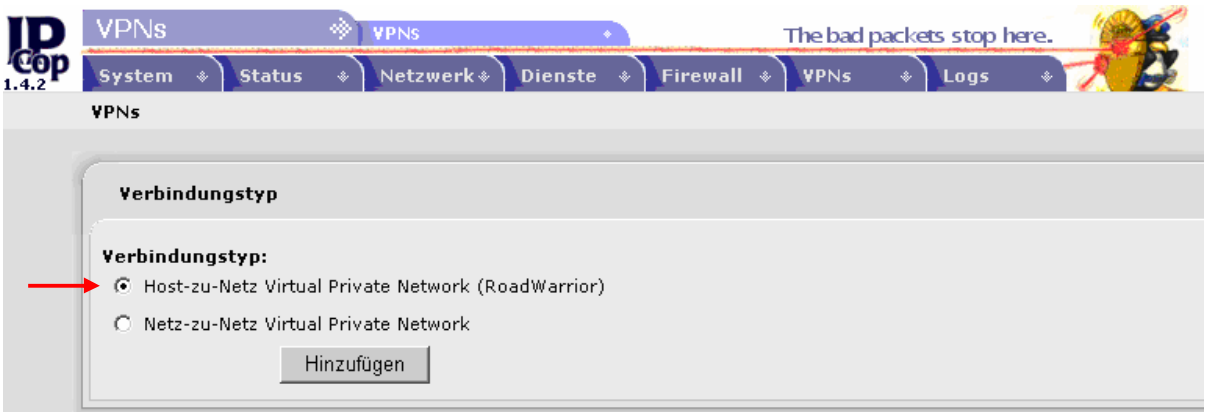
Name der Verbindung:	pskblue
Schnittstelle:	BLUE
Lokales Subnetz:	0.0.0.0/0.0.0.0, wenn jeglicher Traffic verschlüsselt werden soll. 192.168.100.0/255.255.255.0, wenn nur der Traffic nach GREEN verschlüsselt werden soll.
Passwort:	Geheimes#Passwort~

Auf der Clientseite werden folgende Informationen benötigt:

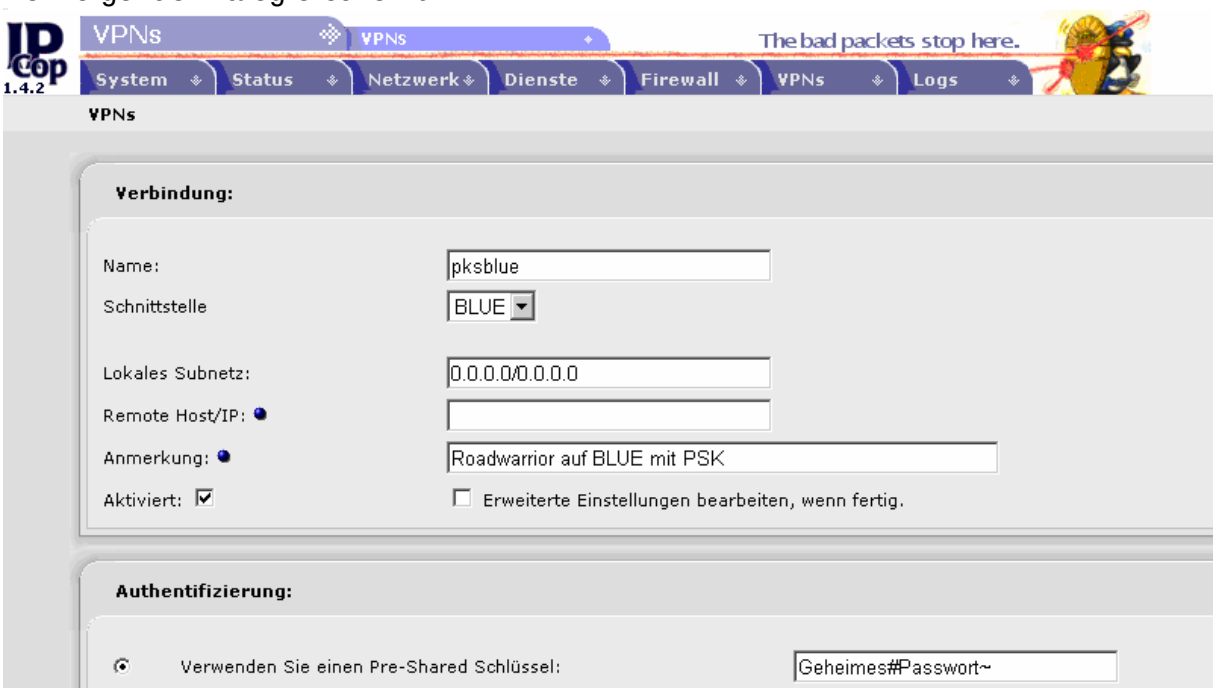
Name der Verbindung:	pskblue
left (Lokale IP):	192.168.111.1
leftsubnet:	* (* steht für 0.0.0.0/0.0.0.0)
right (Gateway):	%any (%any wird zur Laufzeit mit der aktuellen IP gefüllt)
Passwort:	Geheimes#Passwort~

Konfiguration des IPcop

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.

Nach dem Speichern der Verbindung landen wir wieder auf der Hauptseite, welche sich nun mit unserer neu erstellten Verbindung präsentiert.

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“.

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

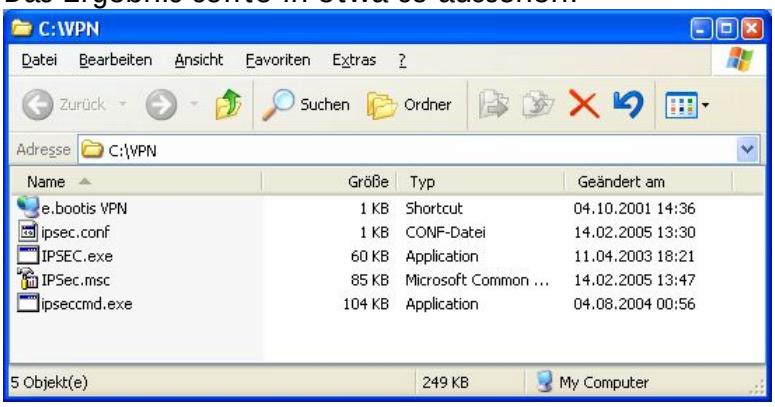
Windows XP

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.

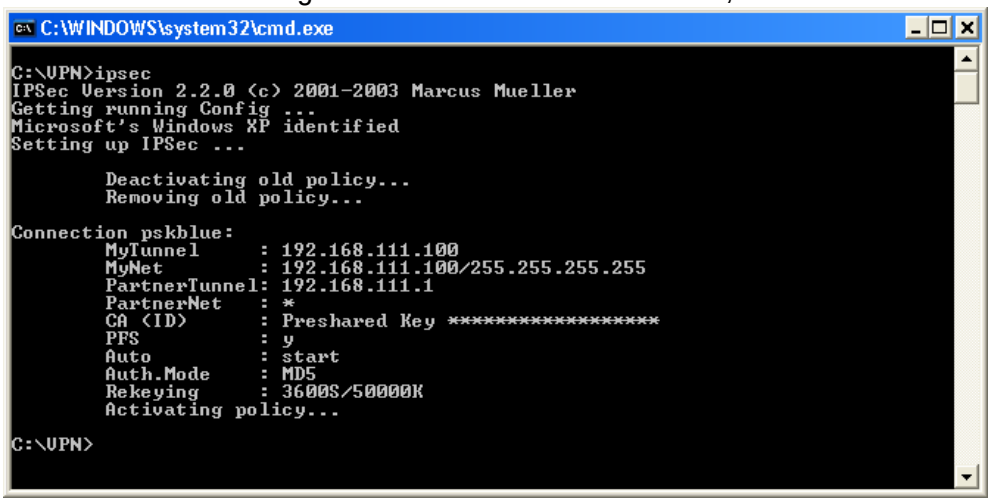


Jetzt muss nur noch die Datei „ipsec.conf“ an die lokalen Gegebenheiten angepasst werden. In unserem Beispiel müsste sie so aussehen:

```
conn pskblue
      left=192.168.111.1
      leftsubnet=*
      presharedkey=Geheimes#Passwort~
      right=%any
      network=auto
      auto=start
      pfs=yes
      authmode=MD5
```

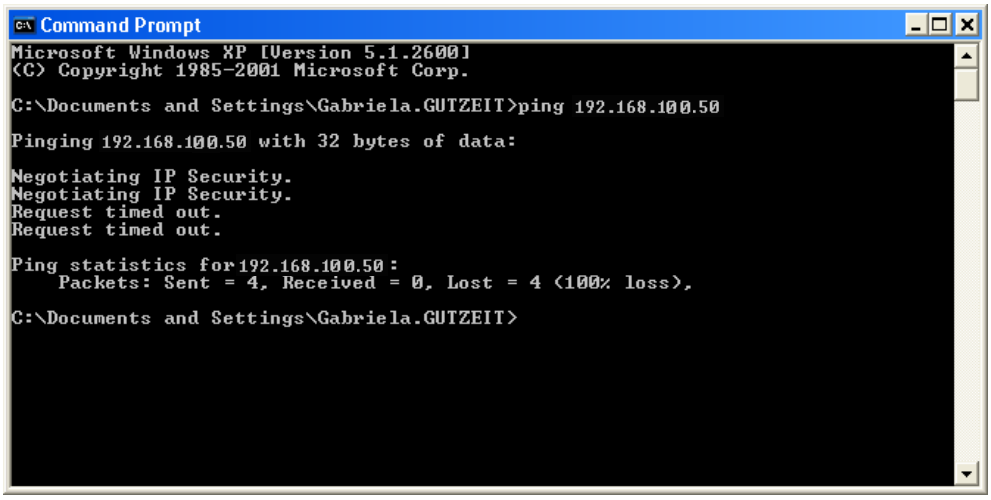
Anmerkung: Statt 192.168.111.1 kann auch der FQDN, z. B. „ipcopVM.gutzeit.ch“, verwendet werden, vorausgesetzt, der Name kann auf die BLUE-IP des IPCop aufgelöst werden.
„leftsubnet=*“ beschreibt das Subnetz 0.0.0.0/0.0.0.0, also alle verfügbaren IP-Adressen, oder das gesamte Internet.

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.

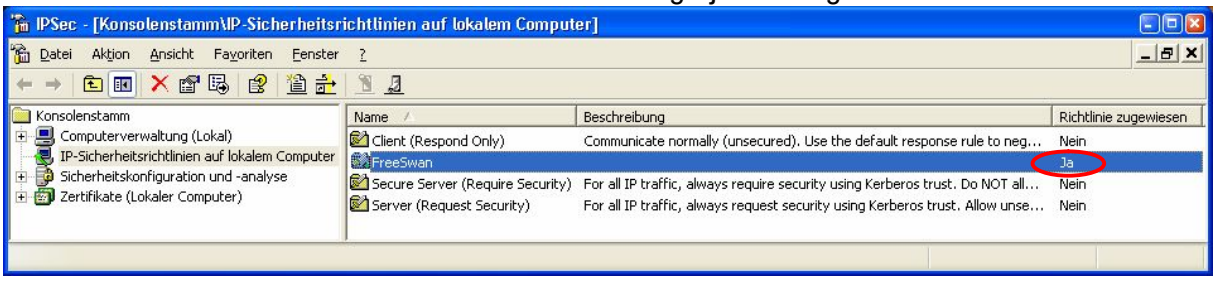
Ein Verbindungsversuch ins LAN mit „ping 192.168.100.50“ wird einige Male den Schriftzug „Sicherheit wird verhandelt“ ausspucken, bevor eine Rückantwort kommt. Dieses Verhalten ist normal.



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…

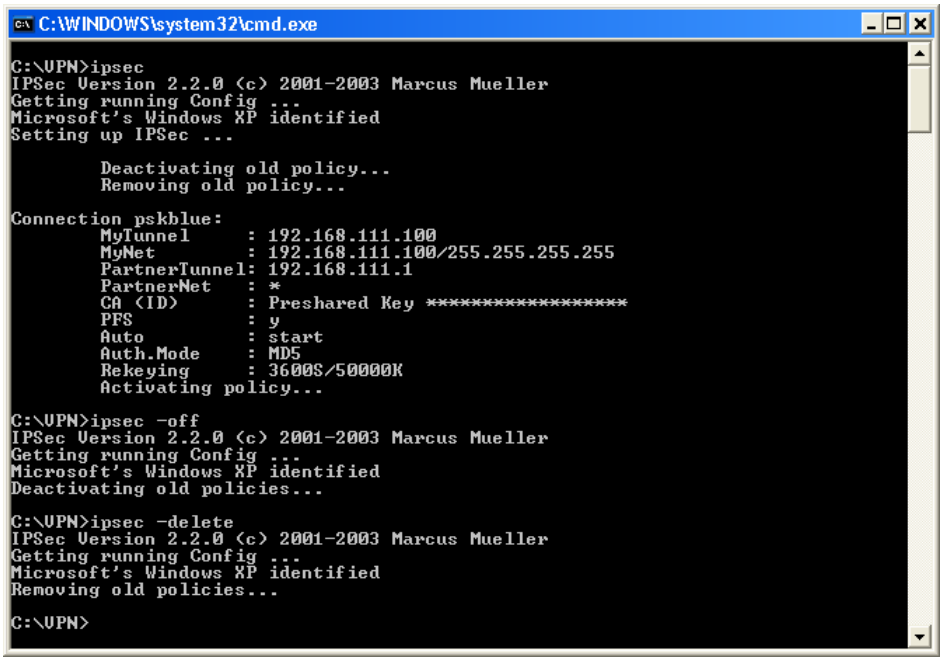
Jetzt steht das VPN und ein Blick in die Web-GUI des IPcop zeigt nach einem Refresh der Seite (erneuter Klick auf VPN im Kopf der Seite) folgendes Bild.

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

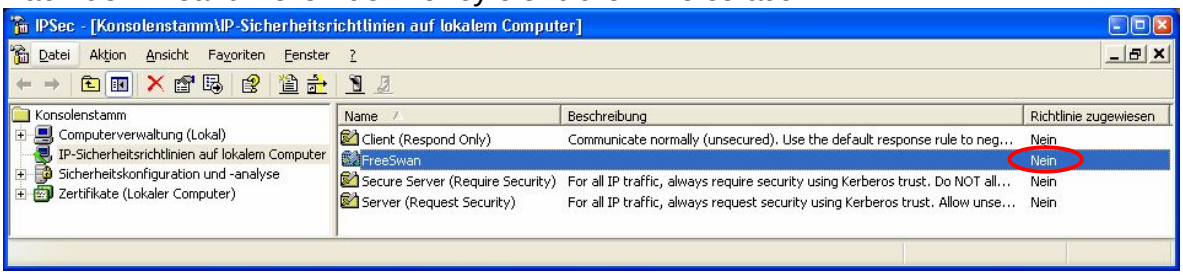


Das Markus Müller Tool hat mit den Informationen aus dem File „ipsec.conf“ eine IPsec-Konfiguration für Windows erstellt und aktiviert. Mit einem Doppelklick auf den Eintrag lassen sich nun die Details erforschen…

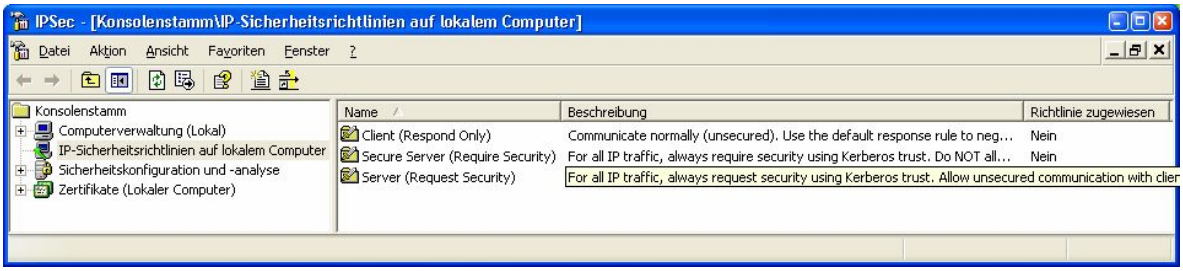
Um das VPN auf dem Client zu beenden, genügt ein „C:\VPN\ipsec.exe –off“. Um die VPN-Konfiguration endgültig aus dem Gedächtnis von Windows zu löschen, muss das Kommando „C:\VPN\ipsec.exe –delete“ eingegeben werden. Bei meinen Tests kam es gelegentlich vor, dass die Konfiguration mit „-delete“ nicht 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!!!

Mögliche Probleme:

Namensauflösung über das VPN

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 immer von Routern geblockt, so dass die Netzwerkumgebung leer bleibt. Eine Verbindung ist jedoch trotzdem möglich.

Gateway

Ein weiterer Stolperstein ist ein falsches Gateway auf dem zu erreichenden Server. Angenommen, Der IPcop wird zu Testzwecken parallel zu einem bestehenden Gateway und mit eigenem Internetzugang installiert. Wohin schickt ein Server im LAN dann die Antwortpakete? Natürlich zu seinem Defaultgateway und damit nicht zum IPcop. Das verursacht dann „seltsame" Probleme in der Art, dass zwar der VPN-Tunnel steht, aber kein Server dahinter erreichbar ist.
Die Lösung besteht nun darin, das Defaultgateway des Servers auf den IPcop zeigen zu lassen. Über statische Routen auf dem IPcop lassen sich dann auch komplexere Konfigurationen abbilden.

Beim Verbindungsaufbau

Wenn alle Schritte wie beschrieben ausgeführt werden, ist nicht mit Problemen zu rechnen. Falls der Verbindungsaufbau doch scheitern sollte, geben die Logfiles auf dem IPcop unter „Logs“ -> „System-Logdateien“ -> „IPsec“ detailliert Auskunft über die Fehlerursache. Auf der Windowsseite kann die Fehleranalyse mit Hilfe von folgendem KnowledgeBase Artikel gestartet werden.
http://support.microsoft.com/default.aspx?scid=kb;en-us;257225

Sonstige Bedenken bei Verwendung von PSK

Der Aufbau von VPN-Verbindungen mit Hilfe von PSK hat einige negative Seiteneffekte, die hier nicht unerwähnt bleiben sollten.

1. Die Sicherheit eines VPNs mit PSK steht und fällt mit dem verwendeten Passwort. Das Passwort sollte daher mit Bedacht gewählt werden. Mindestens 14 Zeichen, GROSS- und kleinschreibung, Zahlen und Sonderzeichen sollten verwendet werden.
2. Es kann nur eine einzige Verbindungskonfiguration in Verbindung mit PSK geben. Dies ist eine Einschränkung von IPsec, nicht vom IPcop. Das heisst, alle User müssen das gleiche Passwort verwenden. Wenn das Passwort eines Users kompromittiert wird, muss es bei allen Usern geändert werden.
3. Ein Parallelbetrieb von PSK und X.509 Zertifikaten ist nicht möglich. Dies ist eine Einschränkung von IPsec, nicht vom IPcop.
4. Der gleichzeitige Betrieb eines VPNs auf RED und BLUE mit PSK ist aus den o. g. Gründen nicht möglich.

Aus den o. g. Gründen sollte PSK nur eine Übergangs-/Testlösung darstellen, die baldmöglichst durch eine Lösung mit X.509 Zertifikaten ersetzt werden sollte.

Und jetzt?

- Wie stelle ich mein BLUE-VPN auf X.509 Zertifikate um?
- 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.