VPN unter Linux - ein Praxisbeispiel

Michi Zaugg - michi@digicomp.ch

24. Juni 2005

DIGICOMP
academy

Inhaltsverzeichnis

[0] Titelbild von http://www.freeswan.org

Zusammenfassung

Dieses Referat handelt von der Digicomp Academy, welche vom Framerelay der Swisscom auf VPN unter Linux mit einem normalen ISP migrierte. Es soll einerseits die Kosten und Nutzenaspekte darlegen andererseits eine kurze Einführung in VPN unter Linux geben.
Es werden Gründe erläutert, wieso das alte Framerelay ersetzt werden musste, welche andere Lösungen in Frage kamen und welche schliesslich verwendet wurden. In theoretischer und praktischer Hinsicht werden Kennzahlen wie Kosten und Bandbreiten dargestellt, auftretende Probleme aufgeführt, die notwendige Netzstruktur erklärt und die Implementation von VPN unter Linux vorgestellt.

1 Einleitung

1.1 Ausgangslage

Framerelay diente einige Jahre als Lösung für die Anbindung der Zenter an den Hauptstandort der Digicomp in Zürich. Das WAN war infolgedessen sternförmig mit Zürich als zentralem Knoten angeordnet (siehe Bild 1 unten). Ebenfalls wurde die Internetanbindung in Zürich realisiert, was hiess, dass sich die Filialen via Zürich aufs Internet begaben. Primär waren es drei Gründe, die den Ausschlag gaben, langsam aber sicher eine Ablösung dieser WAN Anbindung ins Auge zu fassen:

- Ausfallsicherheit
- Kosten
- Performance

Immer höhere Datenmengen wurden via Internet transferiert, die Webseiten und auch andere Webapplikationen wurden umfangreicher, so dass die bestehenden Bandbreiten nicht mehr ausreichten. Die Kosten, diesen Anforderungen gerecht zu werden, waren jedoch zu hoch.
Da die Kosten für Breitband Internet Anbindungen wie SDSL und ADSL stetig abnahmen, lag es nahe, eine solche Lösung gegenüber dem bestehenden Framerelay abzuwägen.
Neben Kostensenkung und höheren Bandbreiten musste natürlich die neue Lösung auch eine möglichst hohe Verfügbarkeit aufweisen.
Das Problem eines Wechsels von der Swisscom zu einem *normalen* ISP stellt sich vorallem darin, dass der Ansprechspartner nicht mehr zugleich auch der Provider der letzten Meile ist. Infolgedessen muss entweder die höhere Antwortszeit bei Leitungsproblemen, welche zwischen neuem Provider und der Swisscom auftritt, in Kauf genommen werden, oder eine Backuplösung bestehen, um die Downtime zu überbrücken.

1.2 Lösungssuche

Die Digicomp hat verschiedene Lösungen in Betracht gezogen, welche hier kurz erläutert werden.

1. Framerelay Upgrade auf höhere Bandbreiten
   Die einfachste Lösung, da keine neue Hard- oder Software gebraucht wird, um die Filialenanbindungen zu gewährleisten. Unter der Voraussetzung, dass die neue Lösung auch kosteneffektiver sein soll, ist dies nicht diskutabel (Tab 1 unten). Hinzu kommt, dass Framerelay in absehbarer Zeit durch IPSS ersetzt wird.

2. IPSS
   Die Bandbreitenproblematik könnte durch das Folgeprodukt von Framerelay, IPSS, gelöst werden. Ein grosses Plus dieses Angebotes besteht darin, Bandbreiten Upgrades quasi über Nacht anfordern zu können (dynamische Gestaltung der Bandbreiten). Preislich befindet sich IPSS etwa auf dem gleichen Niveau wie Framerelay. Negativ ins Gewicht fällt, dass die Administration der Router nicht mehr selbst administriert, sondern zwingend von der Swisscom verwaltet werden.

3. ADSL
   Die Kosten sind sehr tief (je nach Abo schon ab 50 CHF, Business Abos ab etwa 150-200 CHF). Der Nachteil liegt in der asynchronen Bandbreite und der Ausfallsicherheit. Bekanntlich unterliegt das ADSL Netz gewissen Schwankungen.

4. Cable
   Analog ADSL. Zusätzlich mit dem Nachteil behaftet, dass nicht in der ganzen Schweiz der gleiche Provider verwendet werden kann.

5. SDSL zu einem ISP via Leased Lines
   Ist in der Vergangenheit gleich teuer oder gar teurer als Framerelay gewesen. Da die Preise aber stark gesunken sind, sind nicht kommerzielle Abos (wenn keine Weiterverkäufe stattfinden) fast im Bereich von Business ADSL.

1.3 Kosten und Bandbreiten

Tabelle 1

Anbindung	**Bandbreite**	**Kosten (CHF)** [1]
Framerelay	128 kbit/s [2]	800
Framerelay	256 kbit/s [2]	1000
ADSL Business	600 kbit/s	300 [3]
ADSL Business	1200/600 kbit/s	400 [3]
SDSL via Leased Line	1024 kbit/s	350 [4]

1.4 Entscheidung zur Implementation

Instabilitäten und nicht Vereinheitlichung mit einem schweizweiten Provider liessen ADSL und Cable Lösungen eher in den Hintergrund geraten. Wir haben uns entschlossen einen Zürcher Internetprovider zu nehmen, welcher an mehr als der Hälfte der Standorte SDSL via Leased Lines anbieten konnte (d.h. lokal einen POP[5] besitzt). Die restlichen Standorte wurden mit einer Business ADSL Line mit ISDN Fallback ausgestattet, um dort den Schwankungen im ADSL Netz ausweichen zu können. SDSL Linien können gemäss Verfügbarkeitsstatistiken als ausfallsicher betrachtet werden.
Mit dieser Lösung wurden die Kosten um rund das Dreifache gesenkt (von etwa 13'000 CHF / Monat auf rund 4'000 CHF / Monat) und dabei die Bandbreiten um das 4- bis 8-fache erweitert.

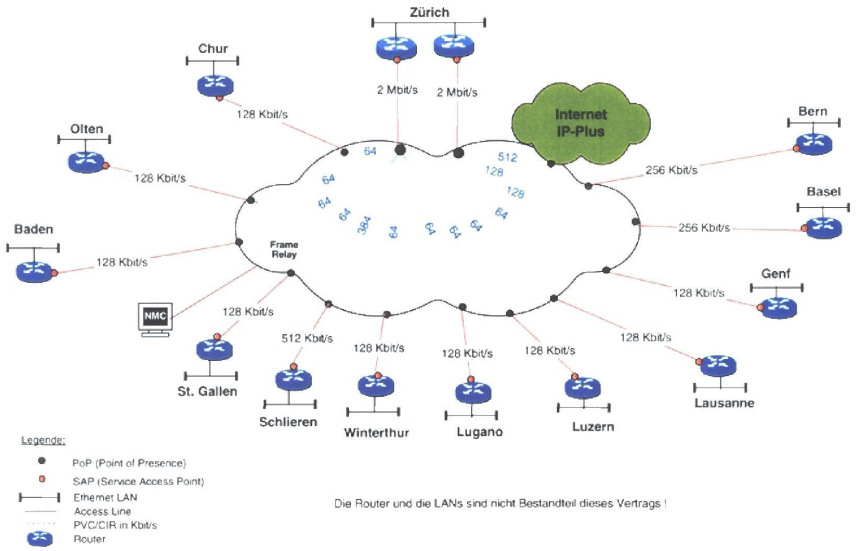
[1] Die Kosten sind ungefähre Angaben, welche die Preise von 2003 wiederspiegeln
[2] Framerelay wurde jeweils mit einem Access und einem CIR Wert verkauft (garantiert und maximal)
[3] Inklusive der Telefonlinie und ISDN Fallback
[4] Inklusive Kosten der Mietleitung (ungefähr 40 CHF/km)
[5] Point Of Presence

2 Netzwerkstruktur

2.1 Framerelay von Swisscom

2.1.1 Alter Stand

Grafik 1



Damaliges Layout des Framerelay Netzes (die angegebenen Bandbreiten sind die Access und nicht CIR Bandbreiten).

2.1.2 Vor und Nachteile

Der grosse Vorteil des Swisscom Framerelays bestand darin, dass die Swisscom Ansprechspartner für die Linien selbst (Kupfer), für die WAN Anbindung und die Internetanbindung (IP-Plus) war. Ein anderer Vorteil lag in der verwendeten Infrastruktur: Die Filialenanbindung wurde jeweils durch einen Cisco Router bewerkstelligt, was die Konfiguration und Wartung vereinfachte. Beispielsweise erfolgte die Trennung von zwei internen Netzen mittels *Access Lists* auf dem Router. Der interne Datenverkehr musste als Folge der Framerelay Technologie nicht explizit abgesichert werden.
Klare Nachteile stellten, wie schon erwähnt, die tiefen Bandbreiten und hohen Kosten dar. Weiter belastete der Internetverkehr der Aussenstellen das interne Netzwerk, was durch das sternförmige Layout gegeben war. Die Konsequenz daraus war, dass das Zentrum Zürich jeweils die aufsummierte Bandbreite der Zenter zur Verfügung stellen musste.

2.2 IPSEC via Internet

Um äquivalent zu Framerelay den internen Datenverkehr gewährleisten zu können, ist eine VPN Lösung unumgänglich. Zusätzlich erschwerend kommt hinzu,

dass jeweils zwei interne Netze pro Aussenstelle bestehen und diese entsprechend voneinander abgesichert werden müssen.
Folgende VPN Lösungen standen zur Diskussion

- Hardware Lösung
- Kommerzielle Software Firewall (z.B. Checkpoint)
- OpenSource Produkte

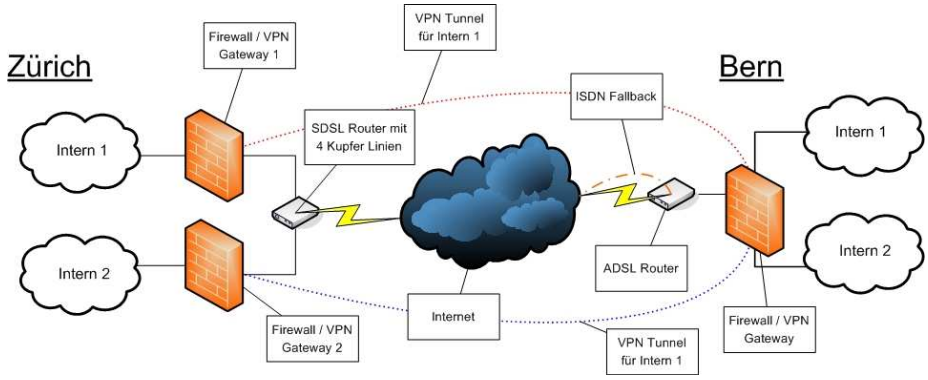
Die erste und zweite Lösung sind wiederum mit Kosten verbunden: Diese beginnen bei etwa tausend Franken für einen VPNRouter pro Aussenstelle bis einigen Zehntausend Franken für Checkpoint Software oder eine Highlevel Hardware Lösung. Da die Anforderungen relativ hoch liegen (Ausfallsicherheit bzw. Fallback-Lösung, mehrere physikalische Netze, Ausbaufähigkeit etc.), würden diese Hardware oder kommerzielle Software Lösungen teuer werden.
Die OpenSource Variante kann mit Hardware, welche noch vorhanden ist, realisiert werden, und Kosten fallen nur in der Implementation (Arbeitszeit) an. In der Regel muss mit einem Tag gerechnet werden, um eine Firewall aufzusetzen und entsprechend in Betrieb zu nehmen.
Mit zusätzlichen Diensten wie transparenter Proxy wird die Performance erhöht. IDS Tools wie Snort erkennen Attacken und stellen einen Teil des Loggings bereit. Ein Software-Raid wirkt sich positiv auf die Verfügbarkeit aus, welches komfortabel und einfach eingericht wird. Spezialitäten wie Bandbreiten-Limitierungen auf Netz, Host und Dienstebene sind ebenfalls realisiert worden. Dazu kommen die allgemeinen Eigenschaften, die eine Lösung unter OpenSource Software, im speziellen Linux, befürworten: die Stabilität, Sicherheit und Flexibilität.

2.2.1 Vor und Nachteile

Die Probleme, die sich dieser VPN via ISP Lösung stellen, werden vorallem durch Dritte verursacht. Konkret bedeutet dies, dass der Provider beispielsweise bei einer physisch defekten Leitung auf die Swisscom warten muss. Die Erfahrung zeigte jedoch, dass Ausfälle beim Framerelay entsprechend Zeit gebraucht hatten, bis die Leitung oder andere Hardware ersetzt worden war.
Der klare Vorteil, abgesehen von Kosten und Bandbreiten, liegt darin, dass jede Aussenstelle über einen direkten Internetzugang verfügt und die Leitung in Zürich weniger belastet wird.

2.2.2 Beispiel für eine Aussenstelle

Bern besitzt eine ADSL Business Internetanbindung (1024/512 kbit) mit einem ISDN Fallback-fähigen Router. Die Firewall dahinter schützt zwei interne Netzwerke und erstellt zwei VPN Tunnel (gepunktete rote und blaue Linien) nach Zürich (je einen Tunnel pro internes Netz ins entsprechende Netz nach Zürich via je einen VPN Gateway).



3 IPSEC unter Linux

3.1 Geschichtliches (FreeSWAN)

In der Zeit des Wechsels von Framerelay auf die jetzige WAN Lösung war FreeSWAN noch *das* IPSEC Projekt unter Linux. Die Entwickler fanden jedoch Anfangs 2004, dass Ihr Projekt gescheitert war und gaben es auf (mehr dazu unter *http://www.freeswan.org/ending_letter.html*). Aus diesem Projekt sind einige neue gegründet worden (vgl. Abschnitt VPN Software für Linux). Auf eines dieser Projekte wurde dann auch die Digicomp migriert (OpenSWAN). Die neuen Projekte sind kompatibel zueinander, d.h. die Konfigurationsdateien können grösstenteils übernommen werden.
Das einzige, was in den neuen Projekten fehlt, ist ein virtuelles IPSEC Interface, welches bei der FreeSWAN Implementation vorhanden war. Dies war einerseits praktisch, um Statistiken auszulesen, andererseits, um die Firewall Regeln einfacher zu gestalten; mit einem kleinen Trick ist dies jedoch weiterhin möglich (siehe Abschnitt Iptables). In den neuen Projekten wird wiederum über eine solche Implementation gemunkelt: Es ist wahrscheinlich, dass bei späteren Relases ein virtuelles Interface wieder auftaucht.

3.2 VPN Software für Linux

3.2.1 StrongSWAN

http://www.strongswan.org
StrongSWAN ist aus FreeSWAN entstanden und wird durch die StronSec GmBH weiterentwickelt (Projektleiter und Entwickler ist Andreas Steffen, Hochschule für Technik Rapperswil).

3.2.2 OpenSWAN

http://www.openswan.org
Ebenfalls aus FreeSWAN entstanden, unterstützt jedoch mehr Plattformen als StrongSWAN. Das OpenSWAN Projekt wird u.a. von Astaro, Novell, SuSE und Xelerence gesponsert.

Wichtigste Features beider IPSEC Lösungen:

- Läuft unter Linux 2.4 (KLIPS) und Linux 2.6 (native IPsec) Kernels
- 3DES, AES, Serpent, Twofish oder Blowfishverschlüsselung
- Authentifizierung mit X509 Zertifikaten oder *preshared keys* möglich
- Smartcard Unterstützung
- Nat-Traversal und Virtual-IP Support

Da OpenSWAN ein grösseres Entwicklungspotential als StrongSWAN besitzt, haben wir uns für ersteres entschieden. Andreas Steffen von StrongSWAN versucht jedoch, das Projekt in Zukunft auf die Hochschule Rapperswil und Winterthur auszuweiten, was eine Vergrösserung der Projektgruppe mit sich bringt.

3.3 Voraussetzungen

Zitat von www.openswan.org:
Openswan is an implementation of IPsec for Linux. It supports kernels 2.0, 2.2, 2.4 and 2.6, and runs on many different platforms, including x86, x86_ 64, ia64, MIPS and ARM.
Am 2.4er oder auch 2.6er Kernel müssen ein paar Änderungen gemacht werden. Der 2.4er Kernel muss gepached werden, da er IPSEC selbst noch nicht unterstützt. Beim 2.6er Kernel ist dies dabei (native IPsec), also muss der Kernel neu konfiguriert und neu kompiliert werden.
Zusätzlich wird das Packet OpenSWAN gebraucht (oder StrongSWAN), welches die Tools für die VPN Verbindungen beinhaltet. Dies gibt es als Source-Tarball auch als Binary-Paket, z.B. RPM.

3.4 SystemVorbereitungen

Wir haben Gentoo[5] als Linux Distribution gewählt. Selbstverständlich können die folgenden Vorbereitungsschritte auch für eine andere Distribution verwendet werden. Anstelle von *emerge* sollte *rpm*, *dpkg* bzw. *apt-get* verwendet werden. Im folgenden wird ausschliesslich auf den 2.6er Kernel eingegangen. Die Installation von OpenSWAN oder StrongSWAN unter 2.4 ist auf den jeweiligen Projekt Webseiten[6] erläutert.

3.4.1 Kernel

Folgendes muss im Kernel zusätzlich aktiviert werden:

- Networking options:
  - PF_KEY sochets (NET_KEY)
  - IP: AH transformation (INET_AH)
  - IP: ESP transformation (INET_ESP)

[5] http://www.gentoo.org
[6] http://www.openswan.org bzw. http://www.strongswan.org

  - IP: IPsec user configuration interface (XFRM_USER)

- Cryptographic API:
  - HMAC support (CRYPTO_HMAC)
  - Null algorithms (CRYTO_NULL)
  - MD5 digest algorithm (CRYPT_MD5)
  - SHA1 digest algorithm (CRYPT_SHA1)
  - DES and Triple DES EDE cipher algorithms (CRYPTO_DES)
  - AES cipher algorithms (CRYPTO_AES)

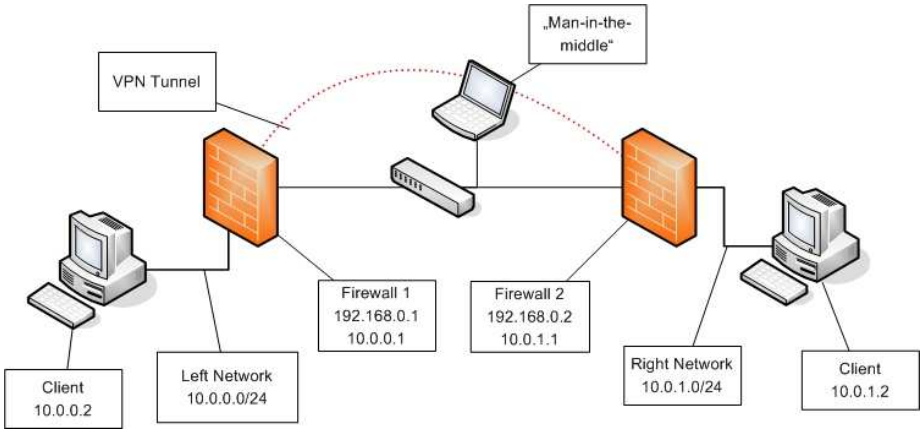
3.4.2 Softwarepakete

Unter Gentoo müssen noch zwei Pakete *gemerged* werden:

```
emerge openswan
emerge ipsec-tools
```

4 Konfiguration des Labs

Als Beispiel wird hier eine *Gateway-to-Gateway* Verbindung erstellt. Hinter den beiden Gateways befindet sich je ein Intranet. Diese sind nicht speziell durch eine Firewall Implementation abgesichert, es geht hier nur um den VPN Tunnel zwischen diesen Netzen.
Um feststellen zu können, ob diese Verbindung sicher ist, wird ein Client an den Hub zwischen den VPN Gateways angeschlossen. Dieser Client analysiert die Verbindung mit einem Sniffer (Ethereal), siehe unten.



4.1 ipsec.conf

Auf jeder der beiden Gateways muss das ipsec.conf angepasst werden. Wichtig sind *conn*-Bereiche, welche entsprechend die Seiten und deren Netze hinten dran spezifizieren.

Konfiguration auf Firewall 1 (tsunami1):

```
conn tsunami1-tsunami2
        leftid=@tsunami1
        leftrsasigkey=[RSA Public Key tsunami1]
        left=192.168.0.1
        leftsubnet=10.0.0.0/24
        leftnexthop=192.168.0.2
        rightid=@tsunami2
        rightrsasigkey=[RSA Public Key tsunami2]
        right=192.168.0.2
        rightsubnet=10.0.1.0/24
        rightnexthop=192.168.0.1
        keyingtries=1
        auto=start
```

Konfiguration auf Firewall 2 (tsunami2):

```
conn tsunami1-tsunami2
        leftid=@tsunami1
        leftrsasigkey=[RSA Public Key tsunami1]
        left=192.168.0.1
        leftsubnet=10.0.0.0/24
        leftnexthop=192.168.0.2
        rightid=@tsunami2
        rightrsasigkey=[RSA Public Key tsunami2]
        right=192.168.0.2
        rightsubnet=10.0.1.0/24
        rightnexthop=192.168.0.1
        keyingtries=1
        auto=add
```

Die Konfigurationsoptionen bedeuten:

- *conn tsunami1-tsunami2* Verbindungsbeschreibung
- *leftid* Name des linken Gateways (bedeuten keine Verifikation via DNS)
- *leftrsasigkey* RSA Public Key des linken Gateways
- *left* IP des linken Gateways
- *leftsubnet* Das Subnetz hinter dem linken Gateway
- *leftnexthop* Defaultrouter des linken Gateways (hier direkt der rechte Gateway)
- rechte Seite Analog linke Seite
- *keyingtries* Wieviele Versuche unternommen werden um eine Verbindung aufzubauen
- *auto* Ob die Verbindung initiiert werden soll oder nur hinzugefügt

Der einzige Unterschied der beiden Konfigurationen, vom ipsec.conf auf tsunami1 bzw. tsunami2, liegt in der Option (*auto*). Eine Maschine gilt als *Master*, welcher auf eine inkommende Verbindung horcht (*add*), und die andere Maschine wird die Verbindung aufbauen (*start*).

4.2 ipsec.secrets

Das *ipsec.secrets* File beinhaltet die Private und Public Keys des VPN Gateways. Es gilt also diese Datei entsprechend zu schützen. Mit

```
ipsec rsasigkey 2048 > /etc/ipsec/ipsec.secrets
```

wird die Datei kreiert und in diesem Fall ein 2048 Bit Schlüssel generiert. Heute reicht ein 2048 Bit RSA Schlüssel aus, in einem Jahr sollte auf 4096 Bit gewechselt werden. Dies sollte dann wiederum für 5 Jahre ausreichen.

```
: RSA {
# RSA 2048 bits   belladona   Thu Jun 23 19:49:53 2005
# for signatures only, UNSAFE FOR ENCRYPTION
#pubkey=0sAQNFkP6YuTx+aacxHymB6e6uY6mb/+F0TljvVHRpZ ...
Modulus: 0x4590fe98b93c7e69a7311f2981e9eeae63a99bff ...
PublicExponent: 0x03
# everything after this point is secret
PrivateExponent: 0x0b982a6ec98a15119bdd853195a6fd1d ...
Prime1: 0x8a653e75dab343e795078f898afdebf197ec7d8b1 ...
Prime2: 0x80ae914dafa3a306a50383a606bae2af41950ab61 ...
Exponent1: 0x5c437ef93c77829a635a5fb10753f2a10ff2fe ...
Exponent2: 0x55c9b633ca6d1759c357ad1959d1ec74d663 ...
Coefficient: 0x687a601198761300f4d855f1963ff6 ...
}
```

Der Public Key (*pubkey*) wird auf beiden Seiten in das ipsec.conf eingetragen.

4.3 Command Line Tool *ipsec*

Die Command-Line Applikation *ipsec* dient zur Administration der VPN Verbindungen. Es können, ohne den IPSEC Dienst neu zu starten, neue Verbindungen hinzugefügt, Verbindungen runter- oder hochgefahren und Zertifikate eingelesen werden.

4.3.1 ipsec auto status

Mit

```
ipsec auto --status
```

kann der aktuelle Status ausgegeben werden. Beispielsweise:

```
000 "tsunami1-tsunami2": 10.0.0.0/24===192.168.0.1[@tsunami1]... \
192.168.0.2[@tsunami2]===10.0.1.0/24; erouted; eroute owner: #2
000 "tsunami1-tsunami2":     srcip=unset; dstip=unset
000 "tsunami1-tsunami2":   ike_life: 3600s; ipsec_life: 28800s; \
rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "tsunami1-tsunami2":   policy: RSASIG+ENCRYPT+COMPRESS+TUNNEL+\
PFS; prio: 24,24; interface: eth0;
000 "tsunami1-tsunami2":   newest ISAKMP SA: #1; newest IPsec SA: \
#2;
000 "tsunami1-tsunami2":   IKE algorithm newest: 3DES_CBC_192-MD5-\
MODP1536
```

Interessant ist hier die Zeile *tsunami1-tsunami2: 10.0.0.0/24===192.168.0.1[tsunami1]... 192.168.0.2[tsunami2]===10.0.1.0/24; erouted; eroute owner: #2*, welche uns angibt, dass ein Tunnel vom Netz 10.0.0.0/24 via Gateway 192.168.0.1 zum Netz 10.0.1.0/24 mit Gateway 192.168.0.2 existiert.

4.3.2 ipsec auto –add, –up, –down und –delete

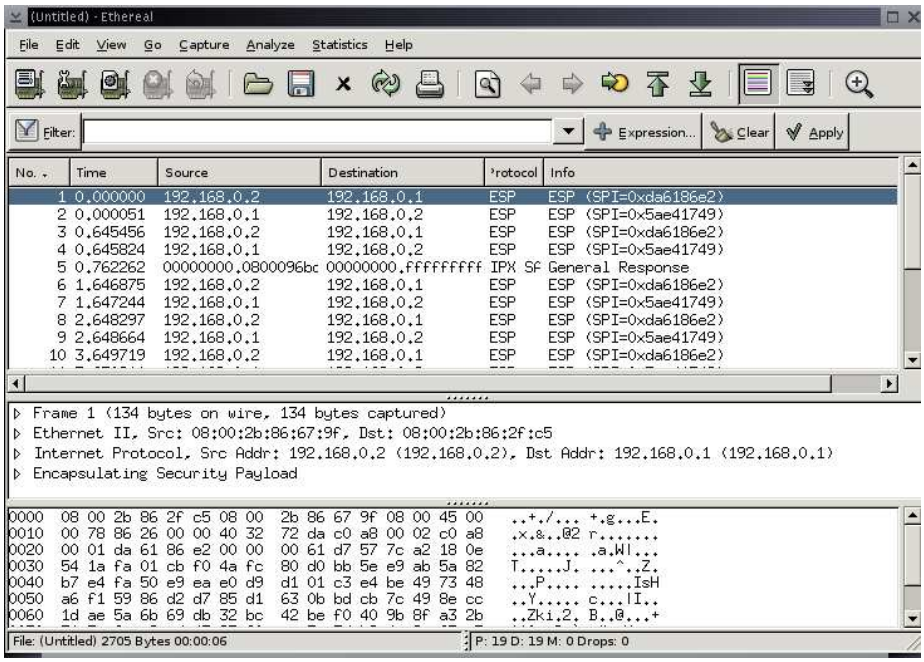
Weitere praktische Optionen für *ipsec* sind *add*, *delete*, *up* und *down*. Mit diesen kann eine (neue) IPSEC Connection hinzugefügt, heraufgefahren und entsprechend auch wieder heruntergefahren oder gelöscht werden.

```
(root@tsunami2:~)# ipsec auto --add tsunami1-tsunami2
(root@tsunami2:~)# ipsec auto --up tsunami1-tsunami2
104 "tsunami1-tsunami2" #6: STATE_MAIN_I1: initiate
003 "tsunami1-tsunami2" #6: received Vendor ID payload [Openswan \
(this version) 2.3.1  X.509-1.5.4 PLUTO_SENDS_VENDORID PLUTO_\
USES_KEYRR]
003 "tsunami1-tsunami2" #6: received Vendor ID payload [Dead Peer\
Detection]
106 "tsunami1-tsunami2" #6: STATE_MAIN_I2: sent MI2, expecting MR2
108 "tsunami1-tsunami2" #6: STATE_MAIN_I3: sent MI3, expecting MR3
004 "tsunami1-tsunami2" #6: STATE_MAIN_I4: ISAKMP SA established
117 "tsunami1-tsunami2" #7: STATE_QUICK_I1: initiate
004 "tsunami1-tsunami2" #7: STATE_QUICK_I2: sent QI2, IPsec SA \
established {ESP=>0xf743b5eb <0x88370cad xfrm=AES_0-HMAC_SHA1 \
IPCOMP=>0x000091bc <0x000086f0}
```

Erfreut ist man vorallem über die letzte Zeile: *IPsec SA established*.

4.3.3 Test des Labs

Mit dem *Man in the middle* kann getestet werden ob die Pakete effektiv die VPN Gateways verschlüsselt verlassen. Ein Tool wie *ethereal* eigenet sicher sehr gut dazu.
Auf der folgenden Abbildung kann erkennt werden, dass die Packete nur im Format *ESP* über das Netz wandern. Der Payload der Pakete ist nicht lesbar. Die versandten Pakete in dem Screen-Shot waren ICMP Echo und ICMP Reply Packete.



4.4 iptables

Wie schon oben beschrieben besitzt OpenSWAN oder StrongSWAN leider kein virtuelles ipsec Interface mehr. Mit dem Markieren der Pakete kann dies kompensiert werden. Anstatt in Iptables auf ein Interface Regeln zu definieren, kann mit *mark* auf IPSEC Packete referenziert werden.
Beispiel:

```
...
iptables -t mangle -A INPUT -p 50 -j MARK --set-mark 50
...
iptables -t nat -A POSTROUTING -o eth1 -s $intra -d $remote -m mark --mark 50 -j ACCEPT
...
```

4.5 Zusätzliche Software

Erfolgreich im Betrieb hat die Digicomp auch andere Software im Zusammenhang mit den VPN Gateways:

- CBQ - Bandbreitenlimitierung bzw. Shapping-Tool
- Snort - IDS Software
- Squid - Transparenter Proxy
- Bind - Caching Nameserver (Unterstützung für Squid)

Nähere Informationen darüber sind auf dem Internet zu finden.

5 Fazit

Die Digicomp benutzt nun diese Lösung seit genau zwei Jahren und dies mit Erfolg. Die Performance ist deutlich gestiegen und die Kosten wurden erheblich gesenkt. Die anfänglich eingesetzten Compaq Deskpro 2000 (PII, 196mb Ram, 2x 3gb IDE Disk für das Softwareraid) sind zwei Jahre durchgelaufen, ohne dass sie nur einmal Probleme verursacht haben. Selbstverständlich sind immer wieder Software-Updates gemacht worden, wenn eine Lücke bekannt oder Bugs gefixt wurden.
Schweren Herzens sind nun nach 2 Jahren Betrieb diese Maschinen ersetzt worden. Einerseits wurde vom ehemaligen RedHat auf Gentoo gewechselt und anderseits ist die Hardware auf Compaq ENSeries (PIII, 512mb Ram, 2x80 gb IDE) gewechselt worden. Primär wurde dies wegen der Inbetriebnahme einer neuen Linuxdistribution gemacht.
OpenSWAN oder ähnliche Produkte aufzusetzen, ist für einen versierten Linux Benutzer nicht schwierig. Ich hoffe, dieses Referat hat Ihnen dies präsentieren können.