Howto für opt_cipe

Daniel Proetel (daniel.proetel@totalis.de)

23. November 2001

1 Changelog

Erstellt am 17.08.2001 von dp
Geändert:

- 14.09.2001 von dp Erweiterung
- 17.09.2001 von dp Anpassungen im Howto, Berücksitigung von nur Windows Anwendern.
- 05.10.2001 von dp Bugfixes
- 14.11.2001 von dp Erweiterung
- 21.11.2001 von dp Tabelle des Beispiels nach Thomas Huber

2 Grundsätzliches

Cipe diehnt dazu , zwischen 2 Rechnern eine verschlüsselte Verbindung aufzubauen. Dadurch, daß Cipe ein eigenes Device generiert,lassen sich über diese Verbindung ganze Netze routen.Cipe tunnelt IP Pakete über eine UDP Verbindung, wobei die Daten mit einem 128 bit Schlüssel verschlüsselt werden.Das Cipe Paket funktioniert unter 1.6.2 und auch unter 2.0.1. Zur Erklärung der Funktionalität muss man sich 3 Netze vorstelle:

- Internes Netz: Das Netz und die IP's aus Sicht der Clients
- CIPE Netz: Ein Netz zwischen 2-... CIpe Rechnern
- INternet: DIe Sicht der IP's aus dem INternet, der Teil, der über das offene Internet stattfindet.

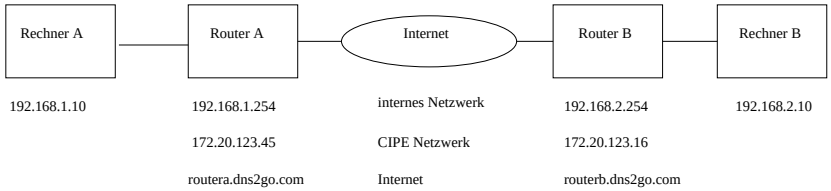

Abbildung 1: Beispiel

3 Beispiel

Router A und B verfügen über 2 Netzwerkkarten. Wird nun Cipe gestartet verfügt der Router über ein zusätzliches Interface. Da Cipe ein neues Interface generiert, wird hierfür ein eigenes Subnetz benötigt.

Hier ein Beispielhafter AUszug aus config.txt:

Router a:

OPT_CIPE='yes' #VPN with Cipe

CIPE_N='1' #Number of cipe-devices

CIPE_PTPADDR_1='172.20.123.16' #the peer's IP-Adress Die IP-Adresse des Partners im CIPE Subnetz

CIPE_IPADDR_1='172.20.123.45' #our CIPE device IP Meine IP im Cipe Subnetz

CIPE_PEER_1='134.102.20.20:4445' #The peer UDP Adress with Port DIe Offizielle IP des Partners, icl. Port.

CIPE_ME_1='0.0.0.0:4444' #My Adress with Port. Could be 0.0.0.0 with dyn. IP Meine IP , incl. Port. Wenn dyn. IP genutzt werden, kann kier bei der IP auch 0.0.0.0 stehen.

CIPE_KEY_1='xxxxxxxxxxxxxxxxxxxx' #The key, generated with ps aux|md5sum Oder auch mit MD5SUM.EXE

CIPE_CTTL_1='64'

CIPE_ROUTE_N='1' #additional route

CIPE_NETWORK_1='192.168.2.0'

CIPE_NETMASK_1='255.255.255.0'

CIPE_GW_1='172.20.123.16' # Network/GW

Router b:

OPT_CIPE='yes' #VPN with Cipe

CIPE_N='1' #Number of cipe-devices

CIPE_PTPADDR_1='172.20.123.45' #the peer's IP-Adress

CIPE_IPADDR_1='172.20.123.16' #our CIPE device IP

CIPE_PEER_1='0.0.0.0:4444' #The peer UDP Adress with Port

CIPE_ME_1='134.102.20.20:4445' #My Adress with Port. Could be 0.0.0.0 with dyn. IP

CIPE_KEY_1='xxxxxxxxxxxxxxxxxxxx' #The key, generated with ps aux|md5sum

CIPE_CTTL_1='64'

CIPE_MAXERR_1='-1'
CIPE_ROUTE_N='1' #additional route Hier werden Routen für die internen Netze eingefügt, also alle Routen, die ins andere Netz führen.
CIPE_NETWORK_1='192.168.1.0'
CIPE_NETMASK_1='255.255.255.0'
CIPE_GW_1='172.20.123.45' # Network/GW
Hierbei ist zu beachten:
CIPE tunnelt IP-Daten über eine verschlüsselte UDP Verbindung, von daher muss die Firewall eine UDP Verbindung zulassen und zwar auf die in PEER und ME angegebenen Adressen/Ports. Die Ports können gleich lauten, das macht allerdings nur Sinn, wenn man nur eine Verbindung zwischen 2 Netzen aufbaut. Sollen allerdings viele Rechner mit einer Zentrale verbunden werden, so macht es Sinn bei den Clients einen festen Port zu Wählen und beim Server müssen die Ports natürlich unterschiedlich sein.Der Key muss bei einer Verbindung gleich sein, da über den Schlüssel die Verbindung verschlüsselt wird.

Nun hat Router A ein Interface cipcb0 mit der IP 172.20.123.45 und Router B cipcb0 mit 172.20.123.16. Die Route von Netz A nach B wird über CIPE_ROUTE EInträge gesetzt. Hierbei ist allerdings zu beachten,dass man evtl die Firewalleinträge anpassen muss, d.h. die UPD Ports bei PEER und ME müssen freigegeben sein. Hierzu werden die Forward-Regeln ergänzt, damit evtl. dasgesammte Subnetz von A geroutet wird.Somit wird aus Sicht von A das Netz 192.168.2.0/24 über cipcb0 geroutet. Ich habe einfach das script etc/rc.d/fwrules angepasst und dieses in der config.txt einfügen:
Routing from/to without masq.
ROUTE_NETWORK_N='1' #
ROUTE_NETWORK_SEND_1='192.168.3.0/24' #Routing von SEND_N nach DEST_N ohne Masq. Hier trägt man die internen
ROUTE_NETWORK_DEST_1='192.168.9.0/24' #Netzwerke ein.

und in der opt/etc/rc.d/fwrules einfügen unterhalb von
```
while [ "$idx" -le "$FORWARD_DENY_HOST_N" ]
do
    eval deny_host='$FORWARD_DENY_HOST_'$idx
    # reject forwarding of packets sent by host deny_host
    /sbin/ipchains -A forward -s $deny_host -j DENY
    idx=`/usr/bin/expr $idx + 1`
done
```

Diesen Text:
```
idx=1
while [ "$idx" -le "$ROUTE_NETWORK_N" ]
do
    eval send_host='$ROUTE_NETWORK_SEND_'$idx
    eval dest_host='$ROUTE_NETWORK_DEST_'$idx
    # reject forwarding of packets sent by host deny_host
```

```
    /sbin/ipchains -A forward -s $send_host -d $dest_host -j ACCEPT
    idx=‘/usr/bin/expr $idx + 1‘
done
```

Der Aufbau des Netzwerkes findet in diesem Beispiel mir von A nach B statt, da nur B auf der IP 134.102.20.20 mit dem UPD Port 4445 hört. Also die typische Konfiguration B ist ein Firmengateway und A ein Mitarbeiter mit dynamischer IP.Alternativ kann man statt IP-Adressen auch Hostname verwenden.

Das Archiv enthält schon die Struktur, die im fli4l Verzeichnis vorliegt. im src Verzeichnis liegt der Sourcecode von cipe. Nun sind in etc/ppp/ip-up nur noch folgende Zeilen zu ergänzen:

```
##########################
/sbin/insmod cipcb.o
/sbin/ciped-cb -o /etc/cipe/options-x # mit x für CIPE_N , evtl Mehrmals
/usr/local/sbin/ciperoute.sh
##########################
```

und in /etc/ppp/ip-down:

```
##############################
/usr/bin/killall -9 ciped-cb
/sbin/ifconfig cipcb* down
/sbin/rmmod cipcb
##############################
```

Der Inhalt der Datei opt/cipeopt.txt ist noch an die Datei opt.txt anzufügen.

Das Subnetz 172.20.123.x wird für Cipe genutzt, da somit bei uns eine Einfügung in das Firewallkonzept möglich war.

4 fil4l 2.0.1

Hier gestaltet sich die Konfiguration einfacher.

Beispiel für 2.0.1 mit dynamischer IP:

```
OPT_CIPE='yes'                  #VPN with Cipe
CIPE_N='1'                      #Number of cipe-devices
CIPE_PTPADDR_1='172.20.123.16'  #the peer's IP-Adress Die IP-Adresse des Partners im CIPE Subnetz
CIPE_IPADDR_1='172.20.123.45'   #our CIPE device IP Meine IP im Cipe Subnetz
CIPE_PEER_1='test.dyndns.org:4445'      #The peer UDP Adress with Port DIe Offizielle IP des Partners, icl. Port.
CIPE_ME_1='test1.dyndns.org:4444'               #My Adress with Port. Could be 0.0.0.0 with dyn. IP Meine IP , incl. Port. Wenn dyn. IP genutzt werden, kann kier bei der IP auch 0.0.0.0 stehen.
CIPE_KEY_1='xxxxxxxxxxxxxxxxxxxxx'      #The key, generated with ps aux|md5sum Oder auch mit MD5SUM.EXE
```

CIPE_CTTL_1='64'
CIPE_ROUTE_N='1' #additional route
CIPE_NETWORK_1='192.168.2.0'
CIPE_NETMASK_1='255.255.255.0'
CIPE_GW_1='172.20.123.16' # Network/GW

Hier wird ein Tunnel von test.dyndns.org nach test1.dyndns.org aufgebaut.

CIPE_PTPADDR beschreibt die IP Adresse des Tunnelendstückes (andere Seite). Hier also die TUnneladresse des Routers B.

CIPE_IPADDR beschreibt meine (ROuter A) Adresse des Tunnelendstückes.

CIPE_PEER ist die Adresse des Partners, die offizielle Adresse

CIPE_ME ist meine officzelle Adresse.

CIPE_KEY der für die Kommunikation verwendete Schlüssel. Er muss bei beiden Partnern gleich sein.

CIPE_NETWORK ist das Netz auf der Seite von Router B.

CIPE_GW ist die IP Adresse des Routers B , da dieser der Gateway ins Netz 192.168.2.0 ist.

5 Hinweise zu dynamischen IPs

Es ist möglich beide Seiten mit dynamischen IP zu realisieren. Hierzu muss jede Seite per Nameservice auflösbar sein. Cipe erkennt einen Wechsel der IP .

6 Prüfen der Installation

Es gibt ein paar einfach Möglichkeiten die Installation zu prüfen.

Am besten führt man am Router einen Ping auf die Cipe-IP des anderen Routers aus. Wenn hier eine Antwort erfolgt, ist die Cipeverbindung io. Kommt keine Antwort, so sollte man vor allem den Schlüssel und die IP's in der config.txt prüfen.

Läuft der direkte ping, kann man nun das Netz auf der anderen Seite anpingen. (hier zB. bei router A ein ping auf die 192.168.2.1), ist auch dieses OK, so kann man diesen Versuch von einem beliebigen Rechner im Netz A machen.

7 Windows

Unter Windows kann man den 128 Bit Schlüssel mit md5sum.exe erzeugen. (http://www.edv.agrar.tu-muenchen.de/~syring/win32/UnxUtils.html)

CIPE für Windows findet man unter
http://cipe-win32.sourceforge.net/

8 Troubleshooting

Typische Fehlerquellen:

- Bei ROuter A muss der UDP Port CIPE_PEER_N mit der Angabe bei router B CIPE_ME_N übereinstimmen.
- Die Clinetnetze müssen bei Routing without Masq eingetragen werden!!!!!

9 Changelog für opt_cipe

23.11.2001 EInfügen von ping in ip-up, für dyndns Verbindungen.