Package vpn

Claas Hilbrecht *email: babel (+at+) fli4l dot de*
das fli4l-Team

16. November 2005

Inhaltsverzeichnis

1 Dokumentation des Paketes cipe

1.1 CIPE - Konfiguration

fli4l nutzt die CIPE Version 1.6.0 ohne weitere Patches und Anpassungen für fli4l.

In der aktuellen CIPE Version treten zwei Probleme auf, deren Ursache nicht genau geklärt werden konnten. Bei einigen kurzen Tests funktionierten aber die CIPE Tunnel wie gewohnt.

- Das Logging via syslog funktioniert nicht korrekt. An die syslog Meldungen wird immer Datenmüll angehängt. Das sieht dann z.B. so aus:

  ```
  Sep 2 21:48:36 fli4l 7:22 ciped-cb[27580]: CIPE daemon vers 1.6.0 (c) Olaf Titz 1996
  ```

- Wenn CIPE zusammen mit OpenVPN benutzt wird, kommt es zu folgender Meldung: „kernel: cipcb: Ouch: cipe_netdev_event() wrong struct“. Diese Meldung tritt immer dann auf, wenn ein virtuelles Netzwerkdevice beim Kernel an- oder abgemeldet wird.

Das CIPE Paket ermöglicht das Verbinden zweier fli4l-Router und deren Netzwerke über einen Tunnel. Beide Partner dürfen dabei dynamische IP-Adressen benutzen.

Detailinformationen und wichtige Hinweise finden Sie auf folgender Website: http://sites.inka.de/sites/big

Es ist unbedingt notwendig den fli4l Paketfilter so anzupassen, dass die Ports, auf denen CIPE Verbindungsanfragen der CIPE Gegenstellen entgegen nimmt, geöffnet werden. Dazu muss entsprechend der Einstellungen von CIPE_x_LOCAL_PORT eine Paketfilterregel in die INPUT_LIST_x eingetragen werden. Ausserdem müssen in die FORWARD_LIST_x Regeln eingeführt werden, damit das Routen über die CIPE Tunnel erlaubt wird.

OPT_CIPE Default: OPT_CIPE='no'

Mit 'yes' wird das CIPE Paket aktiviert. Die Einstellung 'no' deaktiviert das CIPE Paket komplett.

CIPE_WATCH Default: CIPE_WATCH='yes'

Es kommt ab und zu vor, dass ein CIPE Tunnel einfach hängenbleibt. Mit CIPE_WATCH wird ein Überwachungsprozess gestartet, der alle paar Sekunden alle CIPE Tunnel, die die Prüfung CIPE_x_CHECK mit 'yes' aktiviert haben, überprüft. Stellt der Überwachungsprozess fest, dass ein CIPE Tunnel hängt, versucht er diesen CIPE Tunnel neu zu starten. In seltenen Fällen bleibt dabei auch der

Überwachungsprozess hängen. Dann hilft nur ein Neustart des fli4l-Routers. Im Normalfall sollte CIPE_WATCH immer aktiviert werden.

CIPE_START Default: CIPE_START='ip-up'

Die CIPE Tunnel werden entweder bei der Einwahl mit ip-up gestartet oder direkt zur Bootzeit. Die 'ip-up' Methode ist bei Einwahlroutern am sinnvollsten anzuwenden. Wenn aber der fli4l-Router hin einem anderem Router hängt muss hier die Auswahl 'boot' eingetragen werden, sonst werden die Tunnel aufgrund der fehlenden Einwahl nie gestartet.

CIPE_WATCH_OUTPUT Default: CIPE_WATCH_OUTPUT='/dev/tty5'

Der Überwachungsprozess gibt damit aktuelle Statusinformationen auf dem angegeben Terminal aus. Im Normalfall sollte das eine Konsole auf dem fli4l-Router sein. Wollen sie die Statusmeldungen komplett unterdrücken, tragen Sie CIPE_WATCH_OUTPUT='/dev/null' ein.

CIPE_N Default: CIPE_N='0'

Die Anzahl der aktiven CIPE Verbindungen in der Konfigurationsdatei.

CIPE_x_NAME Default: CIPE_x_NAME=''

Der Name der CIPE Verbindung. Dieser Name kann beliebig gewählt werden. Dieser Name wird bei der Statusausgabe von CIPE_WATCH ausgegeben. Damit lassen sich die verschiedenen CIPE Tunnel leicht auseinanderhalten.

CIPE_x_REMOTE_HOST Default: CIPE_x_REMOTE_HOST=''

Entweder wird hier die DNS- oder IP-Adresse der CIPE Gegenstelle eingetragen. Die DNS-Adresse kann auch eine DynDNS-Adresse sein.

CIPE_x_REMOTE_PORT Default: CIPE_x_REMOTE_PORT=''

Der Port einer CIPE Gegenstelle.

CIPE_x_REMOTE_STATICIP Default: CIPE_x_REMOTE_STATICIP=''

Wenn die CIPE Gegenstelle über eine feste IP-Adresse verfügt, sollten sie hier 'yes' eintragen. Dabei ist es egal, ob bei CIPE_x_REMOTE_HOST eine DNS- oder IP-Adresse eingetragen wurde. Wenn die Gegenstelle eine Zugang mit dynamischer IP Adressvergabe benutzt, muss hier 'no' eingetragen werden.

CIPE_x_LOCAL_HOST Default: CIPE_x_LOCAL_HOST=''

Dieser Eintrag sollte normalerweise leer bleiben, dann horcht CIPE auf allen auf dem fli4l-Router vorhandenen IP-Adressen. Theoretisch ist es auch möglich eine DNS- oder IP-Adresse einzutragen. Bitte denken sie daran, dass eine CIPE Gegenstelle auch in der Lage sein muss mit dieser DNS- oder IP-Adresse Kontakt aufzunehmen. Das funktioniert nicht, wenn sie CIPE z. B. auf einer lokalen IP-Adresse des fli4l-Routers horchen lassen und die Gegenstelle versucht, Ihren fli4l-Router über eine Internetverbindung zu erreichen.

CIPE_x_LOCAL_PORT Default: CIPE_x_LOCAL_PORT="

CIPE horcht auf diesem Port auf eingehende Verbindungsanfragen von einer CIPE Gegenstelle.

CIPE_x_KEY Default: CIPE_x_KEY="

Mit einem 32 Zeichen langen Schlüssel, der aus den Ziffern 0–9 und den Buchstaben a–f bestehen darf, wird die CIPE Verbindung verschlüsselt. Der Schlüssel muss auf beiden CIPE Gegenstellen exakt gleich sein! Der Schlüssel muss geheim bleiben, da mit Kenntnis des Schlüssel die CIPE Verbindung abgehört werden kann, bzw. sich ein Angreifer an Ihrer CIPE Verbindung anmelden kann. Die Ausgabe von md5sum eignet sich gut als Schlüssel.

CIPE_x_CHECK Default: CIPE_x_CHECK="

Mit 'yes' wird diese CIPE Verbindung regelmäßig von einem Überwachungsprozess überprüft. Sie sollten diese Einstellung immer auf 'yes' lassen, es sei denn, es gibt Probleme mit dem Überwachungsprozess.

CIPE_x_CHECK_IP Default: CIPE_x_CHECK_IP="

Für die Prüfung ob der CIPE Tunnel verfügbar ist kann hier eine extra IP Adresse eingegeben werden. Standardmäßig wird CIPE_x_REMOTE_VPN_IP geprüft, aber bei einigen Gegenstellen mit deaktiviertem ICMP würde der Test fehlschlagen. Daher kann man in diesen Fällen eine IP angeben, die definitv erreichbar sein sollte wenn das VPN funktioniert.

CIPE_x_REMOTE_VPN_IP Default: CIPE_x_REMOTE_VPN_IP="

Die IP-Adresse der CIPE Gegenstelle. Diese IP-Adresse darf nicht in Ihrem oder dem Netz der CIPE Gegenstelle Netz vorkommen. Ausserdem sollte die IP-Adresse aus dem Bereich der frei zur Verfügung stehenden IP-Adressen kommen.

CIPE_x_LOCAL_VPN_IP Default: CIPE_x_LOCAL_VPN_IP="

Die IP-Adresse der CIPE Verbindung in Ihrem Netzwerk. Es gelten dieselben Regeln wie bei CIPE_x_REMOTE_VPN_IP.

CIPE_x_ROUTE_N Default: CIPE_x_ROUTE_N="

Die Anzahl der Routen, die über diese CIPE Verbindung geroutet werden sollen.

CIPE_x_ROUTE_x Default: CIPE_x_ROUTE_x="

Das Netzwerk, das über diese CIPE Verbindung geroutet werden soll. Hier wird das Netzwerk in der Form Netzwerk/Netmaskenbits angegeben. Also beispielsweise 192.168.145.0/24. Jeder Eintrag darf nur eine Route enthalten! Wenn sie mehr als ein Netz routen wollen, benutzen Sie einfach mehrere CIPE_x_ROUTE_x Einträge.

Ein Beispiel soll die Konfiguration verdeutlichen: Peter und Maria ihre Netzwerke mit ihren fli4l-Routern über das Internet miteinander verbinden. Peter benutzt als privates

Netz 192.168.145.0/24 und hat den Namen 'peter.eisfair.net' als DynDNS Adresse registiert. Bei Maria sieht es ähnlich aus, nur benutzt sie das Netzwerk 10.23.17.0/24 und als DynDNS Adresse 'maria.eisfair.net'. Computer aus den privaten Netzerken von Maria und Peter, sollen uneingeschränkt aufeinander zugreifen können.

Die cipe.txt Konfigurationsdatei der beiden sieht bei einer direkten Gegenüberstellung wie folgt aus:

CIPE Option	Peter	Maria
OPT_CIPE=	'yes'	'yes'
CIPE_WATCH=	'yes'	'yes'
CIPE_WATCH_OUTPUT=	'/dev/tty5'	'/dev/tty5'
CIPE_N=	'1'	'1'
CIPE_1_NAME=	'to_maria'	'to_peter'
CIPE_1_REMOTE_HOST=	'maria.eisfair.net'	'peter.eisfair.net'
CIPE_1_REMOTE_PORT=	'10000'	'10001'
CIPE_1_REMOTE_STATICIP=	'no'	'no'
CIPE_1_LOCAL_HOST=	''	''
CIPE_1_LOCAL_PORT=	'10001'	' 10000'
CIPE_1_KEY=	'12345678901234567890123456789012'	'12345678901234567890123456789012'
CIPE_1_CHECK=	'yes'	'yes'
CIPE_1_REMOTE_VPN_IP=	'192.168.200.231'	'192.168.200.193'
CIPE_1_LOCAL_VPN_IP=	'192.168.200.193'	'192.168.200.231'
CIPE_1_ROUTE_N=	'1'	'1'
CIPE_1_ROUTE_1=	'10.23.17.0/24'	192.168.145.0/24

Man sieht in dem Beispiel sehr gut, dass die meisten Einstellungen nur getauscht werden müssen. Wenn beispielsweise bei einem fli4l-Router der Eintrag CIPE_x_LOCAL_PORT auf 1234 und der Eintrag CIPE_x_REMOTE_PORT auf 5678 gesetzt wird, müssen bei der Gegenstelle genau diese Einstellungen getauscht werden. Das gleiche gilt für CIPE_x_REMOTE_VPN_IP und CIPE_x_LOCAL_VPN_IP. Passen die Einstellungen nicht zusammen, kann kein VPN Tunnel aufgebaut werden.

Jetzt müssen noch die jeweiligen Paketfilter angepasst werden. Das wird in der base.txt gemacht. In diesem Beispiel findet nur die neue Paketfilterkonfiguration des fli4l 2.1.x Berücksichtigung. Für die Konfiguration des Paketfilters des fli4l 2.0.x, schauen Sie bitte in die Dokumentation des CIPE Paketes dieser Version. Hier sind wieder die jeweiligen Einträge gegenübergestellt.

Paketfiltereinstellung	Peter	Maria
INPUT_LIST_x	'10001 ACCEPT'	'10000 ACCEPT'
INPUT_LIST_x	'10.23.17.0/24 ACCEPT'	'192.168.145.0/24 ACCEPT'
FORWARD_LIST_x	'192.168.145.0/24 10.23.17.0/24 ACCEPT BIDIRECTIONAL'	'10.23.17.0/24 192.168.145.0/24 ACCEP
POSTROUTING_LIST_x	'10.23.17.0/24 192.168.145.0/24 ACCEPT BIDIRECTIONAL'	'192.168.145.0/24 10.23.17.0/24 ACCEP

Mit diesen Einstellungen können die Benutzer auf das jeweilige andere Netzwerk zugreifen. Wenn die Einträge in der FORWARD_LIST *vor* dem Eintrag FORWARD_LIST_1='tmpl:samba DROP' stehen, dann ist ein uneingeschränkter Zugriff auf das jeweils andere Netzwerk (also auch auf Windows Freigaben) möglich.

Wichtig ist es, dass die Einträge in der POSTROUTING_LIST *vor* dem MASQUERADE Eintrag stehen.

A Anhang zum Paket cipe

Index