

```
jetproxy.smarttravelers.com
Thu Aug 22 09:56:16 HKT 2002
+ _____ version
+ ipsec --version
Linux FreeS/WAN U1.95/K1.97
See `ipsec --copyright' for copyright information.
+ _____ proc/version
+ cat /proc/version
Linux version 2.4.18-3ipsec SMP (root@elenuial.steamballoon.com)
(gcc version 2.96 20000731 (Red Hat Linux 7.3
2.96-110)) #1 SMP Fri May 24 14:09:06 EDT 2002
+ _____ proc/net/ipsec_eroute
+ sort +3 /proc/net/ipsec_eroute
0      172.16.1.102/32  -> 160.8.0.0/16    => tun0x100
4@172.16.1.10
0      172.16.1.102/32  -> 172.16.1.10/32    => tun0x100
6@172.16.1.10
0      172.16.1.102/32  -> 180.1.1.0/24     => tun0x100
2@172.16.1.10
+ _____ proc/net/ipsec_spi
+ cat /proc/net/ipsec_spi
tun0x1005@172.16.1.102 IPIP: dir=in  src=172.16.1.10 life(c,s,h)
)=addtime(253915,0,0)
tun0x1003@172.16.1.102 IPIP: dir=in  src=172.16.1.10 life(c,s,h)
)=addtime(253915,0,0)
tun0x1001@172.16.1.102 IPIP: dir=in  src=172.16.1.10 life(c,s,h)
)=addtime(253915,0,0)
tun0x1006@172.16.1.10 IPIP: dir=out src=172.16.1.102 life(c,s,h)
)=addtime(253915,0,0)
tun0x1004@172.16.1.10 IPIP: dir=out src=172.16.1.102 life(c,s,h)
)=addtime(253915,0,0)
tun0x1002@172.16.1.10 IPIP: dir=out src=172.16.1.102 life(c,s,h)
)=addtime(253915,0,0)
esp0xec121fb@172.16.1.102 ESP_3DES_HMAC_MD5: dir=in  src=172.16
.1.10 iv_bits=64bits iv=0x6d61ecdf891fddb1
ooowin=64 alen=128 aklen=128 eklen=192 life(c,s,h)=addtime(2539
15,0,0)
esp0xec121fa@172.16.1.102 ESP_3DES_HMAC_MD5: dir=in  src=172.16
.1.10 iv_bits=64bits iv=0x660b842e5d728a1a
ooowin=64 alen=128 aklen=128 eklen=192 life(c,s,h)=addtime(2539
15,0,0)
esp0xec121f9@172.16.1.102 ESP_3DES_HMAC_MD5: dir=in  src=172.16
.1.10 iv_bits=64bits iv=0x7d3f4054776507af
ooowin=64 alen=128 aklen=128 eklen=192 life(c,s,h)=addtime(2539
15,0,0)
esp0xccf626e1@172.16.1.102 ESP_3DES_HMAC_MD5: dir=out src=172.16
.1.102 iv_bits=64bits
```

```

iv=0x9d658bb2658e6149 ooowin=64 alen=128 aklen=128 eklen=192 li
fe(c,s,h)=addtime(253915,0,0)
esp0xccf626e0@172.16.1.10 ESP_3DES_HMAC_MD5: dir=out src=172.16
.1.102 iv_bits=64bits iv=0x68928fcc3e661b39
ooowin=64 alen=128 aklen=128 eklen=192 life(c,s,h)=addtime(2539
15,0,0)
esp0xccf626df@172.16.1.10 ESP_3DES_HMAC_MD5: dir=out src=172.16
.1.102 iv_bits=64bits iv=0x97f27c956facf321
ooowin=64 alen=128 aklen=128 eklen=192 life(c,s,h)=addtime(2539
15,0,0)

```

```

+ _____ proc/net/ipsec_spigrp
+ cat /proc/net/ipsec_spigrp
tun0x1005@172.16.1.102 esp0xec121fb@172.16.1.102
tun0x1003@172.16.1.102 esp0xec121fa@172.16.1.102
tun0x1001@172.16.1.102 esp0xec121f9@172.16.1.102
tun0x1006@172.16.1.10 esp0xccf626e1@172.16.1.10
tun0x1004@172.16.1.10 esp0xccf626e0@172.16.1.10
tun0x1002@172.16.1.10 esp0xccf626df@172.16.1.10
+ _____ netstart-rn

```

```

+ netstat -nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Win
dow irtt Iface
172.16.1.10 172.16.1.10 255.255.255.255 UGH 40 0
0 ipsec0
180.1.1.0 172.16.1.10 255.255.255.0 UG 40 0
0 ipsec0
160.8.0.0 172.16.1.10 255.255.0.0 UG 40 0
0 ipsec0
172.16.0.0 0.0.0.0 255.255.0.0 U 40 0
0 eth0
172.16.0.0 0.0.0.0 255.255.0.0 U 40 0
0 ipsec0
127.0.0.0 0.0.0.0 255.0.0.0 U 40 0
0 lo
0.0.0.0 172.16.1.101 0.0.0.0 UG 40 0
0 eth0

```

```

+ _____ proc/net/ipsec_tncfg
+ cat /proc/net/ipsec_tncfg
ipsec0 -> eth0 mtu=16260(1500) -> 1500
ipsec1 -> NULL mtu=0(0) -> 0
ipsec2 -> NULL mtu=0(0) -> 0
ipsec3 -> NULL mtu=0(0) -> 0

```

```

+ _____ proc/net/pf_key
+ cat /proc/net/pf_key
sock pid socket next prev e n p sndbf Flags
Type St
f2796040 4017 f5783ce4 0 0 0 0 2 65535 00000000

```

3 1

```
+ _____ proc/net/pf_key-star
+ cd /proc/net
+ egrep '^ pf_key_registered pf_key_supported
pf_key_registered:satype socket pid sk
pf_key_registered: 2 f5783ce4 4017 f2796040
pf_key_registered: 3 f5783ce4 4017 f2796040
pf_key_registered: 9 f5783ce4 4017 f2796040
pf_key_registered: 10 f5783ce4 4017 f2796040
pf_key_supported:satype exttype alg_id ivlen minbits maxbits
pf_key_supported: 2 14 3 0 160 160
pf_key_supported: 2 14 2 0 128 128
pf_key_supported: 3 15 3 128 168 168
pf_key_supported: 3 14 3 0 160 160
pf_key_supported: 3 14 2 0 128 128
pf_key_supported: 9 15 4 0 128 128
pf_key_supported: 9 15 3 0 32 128
pf_key_supported: 9 15 2 0 128 32
pf_key_supported: 9 15 1 0 32 32
pf_key_supported: 10 15 2 0 1 1
+ _____ proc/sys/net/ipsec-star
+ cd /proc/sys/net/ipsec
+ egrep '^ debug_ah debug_eroute debug_esp debug_ipcomp debug_
netlink debug_pfkey debug_radij debug_rcv
debug_spi debug_tunnel debug_verbose debug_xform icmp inbound_p
olicy_check tos
debug_ah:0
debug_eroute:0
debug_esp:0
debug_ipcomp:0
debug_netlink:0
debug_pfkey:0
debug_radij:0
debug_rcv:0
debug_spi:0
debug_tunnel:0
debug_verbose:0
debug_xform:0
icmp:1
inbound_policy_check:1
tos:1
+ _____ ipsec/status
+ ipsec auto --status
000 interface ipsec0/eth0 172.16.1.102
000
000 "linux-fw1": 172.16.1.102...172.16.1.10
000 "linux-fw1": ike_life: 3600s; ipsec_life: 5400s; rekey_ma
rgin: 540s; rekey_fuzz: 100%; keyingtries: 3
```

```
000 "linux-fw1": policy: PSK+ENCRYPT+TUNNEL+DISABLEARRIVALCHE
CK; interface: eth0; erouted
000 "linux-fw1": newest ISAKMP SA: #0; newest IPsec SA: #4; e
route owner: #4
000 "linux-fw1-2": 172.16.1.102...172.16.1.10===160.8.0.0/16
000 "linux-fw1-2": ike_life: 3600s; ipsec_life: 5400s; rekey_
margin: 540s; rekey_fuzz: 100%; keyingtries: 3
000 "linux-fw1-2": policy: PSK+ENCRYPT+TUNNEL+DISABLEARRIVALC
HECK; interface: eth0; erouted
000 "linux-fw1-2": newest ISAKMP SA: #0; newest IPsec SA: #3;
eroute owner: #3
000 "linux-fw1-1": 172.16.1.102...172.16.1.10===180.1.1.0/24
000 "linux-fw1-1": ike_life: 3600s; ipsec_life: 5400s; rekey_
margin: 540s; rekey_fuzz: 100%; keyingtries: 3
000 "linux-fw1-1": policy: PSK+ENCRYPT+TUNNEL+DISABLEARRIVALC
HECK; interface: eth0; erouted
000 "linux-fw1-1": newest ISAKMP SA: #1; newest IPsec SA: #2;
eroute owner: #2
000
000 #4: "linux-fw1" STATE_QUICK_I2 (sent QI2, IPsec SA establis
hed); EVENT_SA_REPLACE in 4677s; newest IPSEC;
eroute owner
000 #4: "linux-fw1" esp.ccf626e1@172.16.1.10 esp.ec121fb@172.16
.1.102 tun.1006@172.16.1.10
tun.1005@172.16.1.102
000 #3: "linux-fw1-2" STATE_QUICK_I2 (sent QI2, IPsec SA establ
ished); EVENT_SA_REPLACE in 4819s; newest
IPSEC; eroute owner
000 #3: "linux-fw1-2" esp.ccf626e0@172.16.1.10 esp.ec121fa@172.
16.1.102 tun.1004@172.16.1.10
tun.1003@172.16.1.102
000 #2: "linux-fw1-1" STATE_QUICK_I2 (sent QI2, IPsec SA establ
ished); EVENT_SA_REPLACE in 4783s; newest
IPSEC; eroute owner
000 #2: "linux-fw1-1" esp.ccf626df@172.16.1.10 esp.ec121f9@172.
16.1.102 tun.1002@172.16.1.10
tun.1001@172.16.1.102
000 #1: "linux-fw1-1" STATE_MAIN_I4 (ISAKMP SA established); EV
ENT_SA_REPLACE in 2668s; newest ISAKMP
+ _____ ifconfig-a
+ ifconfig -a
eth0 Link encap:Ethernet HWaddr 00:E0:18:60:E5:D7
inet addr:172.16.1.102 Bcast:172.16.255.255 Mask:25
5.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:20971 errors:0 dropped:0 overruns:0 frame:
0
TX packets:14844 errors:0 dropped:0 overruns:0 carrie
```

r:0
collisions:0 txqueuelen:100
RX bytes:2152442 (2.0 Mb) TX bytes:2157566 (2.0 Mb)
Interrupt:20 Base address:0x2000

ipsec0 Link encap:Ethernet HWaddr 00:E0:18:60:E5:D7
inet addr:172.16.1.102 Mask:255.255.0.0
UP RUNNING NOARP MTU:16260 Metric:1
RX packets:4196 errors:0 dropped:0 overruns:0 frame:0
TX packets:4990 errors:0 dropped:140 overruns:0 carri

er:0
collisions:0 txqueuelen:10
RX bytes:359125 (350.7 Kb) TX bytes:776788 (758.5 Kb

)

ipsec1 Link encap:IPIP Tunnel HWaddr
NOARP MTU:0 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:10
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

ipsec2 Link encap:IPIP Tunnel HWaddr
NOARP MTU:0 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:10
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

ipsec3 Link encap:IPIP Tunnel HWaddr
NOARP MTU:0 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:10
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:848 errors:0 dropped:0 overruns:0 frame:0
TX packets:848 errors:0 dropped:0 overruns:0 carrier:

0

collisions:0 txqueuelen:0
RX bytes:54188 (52.9 Kb) TX bytes:54188 (52.9 Kb)

+ _____ ipsec/directory

+ ipsec --directory

/usr/local/lib/ipsec

```
+ _____ hostname/fqdn
+ hostname --fqdn
jetproxy.smarttravelers.com
+ _____ hostname/ipaddress
+ hostname --ip-address
172.16.1.102
+ _____ uptime
+ uptime
 9:56am up 2 days, 22:32, 1 user, load average: 0.18, 0.07,
0.02
+ _____ ps
+ ps alxwf
+ egrep -i 'ppid|plutolipsecklips'
 F UID PID PPID PRI NI VSZ RSS WCHAN STAT TTY
TIME COMMAND
000  0 4204 3618 16  0 2204 972 wait4 S pts/0
0:00          \_ /bin/sh /usr/sbin/ipsec barf
000  0 4205 4204 19  0 2228 1016 wait4 S pts/0
0:00          \_ /bin/sh /usr/lib/ipsec/barf
000  0 4245 4205 19  0 1480 436 pipe_w S pts/0
0:00          \_ grep -E -i ppid|plutolips
eckli
040  0 4011  1 20  0 1972 908 wait4 S pts/0
0:00 /bin/sh /usr/local/lib/ipsec/_plutorun --debug none
--uniqueids
040  0 4015 4011 20  0 1972 908 wait4 S pts/0
0:00 \_ /bin/sh /usr/local/lib/ipsec/_plutorun --debug none
--uniqu
100  0 4017 4015 15  0 1968 848 schedu S pts/0
0:00 | \_ /usr/local/lib/ipsec/pluto --nofork --debug-none
--uniq
000  0 4016 4011 18  0 1960 896 pipe_w S pts/0
0:00 \_ /bin/sh /usr/local/lib/ipsec/_plutoload --load %searc
h
--st
000  0 4012  1 16  0 1356 460 pipe_w S pts/0
0:00 logger -p daemon.error -t ipsec__plutorun
+ _____ ipsec/showdefaults
+ ipsec showdefaults
routephys=eth0
routephys=eth0
routevirt=ipsec0
routevirt=ipsec0
routeaddr=172.16.1.102
routeaddr=172.16.1.102
routenextthop=172.16.1.101
routenextthop=172.16.1.101
defaultroutephys=eth0
```

```
defaultroutevirt=ipsec0
defaultrouteaddr=172.16.1.102
defaultroutenexthop=172.16.1.101
+ _____ ipsec/conf
+ ipsec _include /etc/ipsec.conf
+ ipsec _keycensor

#< /etc/ipsec.conf 1
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

# More elaborate and more varied sample configurations can be f
ound
# in FreeS/WAN's doc/examples file, and in the HTML documentati
on.

# basic configuration
config setup
    # THIS SETTING MUST BE CORRECT or almost nothing will w
ork;
    # %defaultroute is okay for most simple cases.
    interfaces=%defaultroute
    # Debug-logging controls: "none" for (almost) none, "a
ll" for lots.
    klipsdebug=none
    plutodebug=none
    # Use auto= parameters in conn descriptions to control
startup actions.
    plutoload=%search
    plutostart=%search
    # Close down old connection when new one using same ID
shows up.
    uniqueids=yes

# defaults for subsequent connection descriptions
# (mostly to fix internal defaults which, in retrospect, were b
adly chosen)
conn %default
    keyingtries=3
#    disablearrivalcheck=no
#    authby=rsasig
#    leftrsasigkey=%dns
#    rightrsasigkey=%dns
```

```
# connection description for (experimental!) opportunistic encryption
# (requires KEY record in your DNS reverse map; see doc/opportunism.howto)
#conn me-to-anyone
#   left=%defaultroute
#   right=%opportunistic
#   keylife=1h
#   rekey=[sums to e4ac...]
#   # uncomment this next line to enable it
#   #auto=route
```

```
# sample VPN connection
#conn sample
#   # Left security gateway, subnet behind it, next hop toward right.
#   left=10.0.0.1
#   leftsubnet=172.16.0.0/24
#   leftnexthop=10.22.33.44
#   # Right security gateway, subnet behind it, next hop toward left.
#   right=10.12.12.1
#   rightsubnet=192.168.0.0/24
#   rightnexthop=10.101.102.103
#   # To authorize this connection, but not actually start it, at startup,
#   # uncomment this.
#   #auto=add
```

```
conn linux-fw1
    type=tunnel
    keyexchange=ike
    auth=esp
    pfs=no
    left=172.16.1.10
    right=172.16.1.102
    keylife=90m
    authby=secret
    auto=start
```

```
conn linux-fw1-1
    type=tunnel
    keyexchange=ike
    auth=esp
    pfs=no
```

```
left=172.16.1.10
leftsubnet=180.1.1.0/24
right=172.16.1.102
keylife=90m
authby=secret
auto=start
```

```
conn linux-fw1-2
type=tunnel
keyexchange=ike
auth=esp
pfs=no
left=172.16.1.10
leftsubnet=160.8.0.0/16
right=172.16.1.102
keylife=90m
authby=secret
auto=start
```

```
+ _____ ipsec/secrets
+ ipsec _include /etc/ipsec.secrets
+ ipsec _secretcensor
```

```
#< /etc/ipsec.secrets 1
172.16.1.102 172.16.1.10 : PSK "[sums to 0cfc.
..]"
172.16.1.10 172.16.1.102 : PSK "[sums to 0cfc.
..]"
```

```
+ _____ ipsec/ls-dir
+ ls -l /usr/lib/ipsec
total 2500
-rwxr-xr-x 1 root root 11085 May 28 00:34 _confre
ad
-rwxr-xr-x 1 root root 46413 May 28 00:34 _copyri
ght
-rwxr-xr-x 1 root root 2163 May 28 00:34 _includ
e
-rwxr-xr-x 1 root root 1472 May 28 00:34 _keycen
sor
-rwxr-xr-x 1 root root 69817 May 28 00:34 _pluto_
adns
-rwxr-xr-x 1 root root 3495 May 28 00:34 _plutol
oad
-rwxr-xr-x 1 root root 4265 May 28 00:34 _plutor
un
-rwxr-xr-x 1 root root 7294 May 28 00:34 _realse
tup
-rwxr-xr-x 1 root root 1971 May 28 00:34 _secret
censor
```

```

-rwxr-xr-x 1 root  root    6839 May 28 00:34 _startk
lips
-rwxr-xr-x 1 root  root    5014 May 28 00:34 _updown
-rwxr-xr-x 1 root  root   10912 May 28 00:34 auto
-rwxr-xr-x 1 root  root    7132 May 28 00:34 barf
-rwxr-xr-x 1 root  root  225325 May 28 00:34 eroute
-rwxr-xr-x 1 root  root   97952 May 28 00:34 ikeping
-rwxr-xr-x 1 root  root    2909 May 28 00:34 ipsec
-rw-r--r-- 1 root  root    1950 May 28 00:34 ipsec_p
r.template
-rwxr-xr-x 1 root  root  161950 May 28 00:34 klipsde
bug
-rwxr-xr-x 1 root  root    2437 May 28 00:34 look
-rwxr-xr-x 1 root  root   16157 May 28 00:34 manual
-rwxr-xr-x 1 root  root    1847 May 28 00:34 newhost
key
-rwxr-xr-x 1 root  root  139801 May 28 00:34 pf_key
-rwxr-xr-x 1 root  root  787868 May 28 00:34 pluto
-rwxr-xr-x 1 root  root   52734 May 28 00:34 ranbits
-rwxr-xr-x 1 root  root   77818 May 28 00:34 rsasigk
ey
-rwxr-xr-x 1 root  root   16653 May 28 00:34 send-pr
lrwxrwxrwx 1 root  root      22 Jun 28 10:43 setup -
> /etc/rc.d/init.d/ipsec
-rwxr-xr-x 1 root  root    1041 May 28 00:34 showdef
aults
-rwxr-xr-x 1 root  root    3484 May 28 00:34 showhos
tkey
-rwxr-xr-x 1 root  root  246334 May 28 00:34 spi
-rwxr-xr-x 1 root  root  202066 May 28 00:34 spigrp
-rwxr-xr-x 1 root  root   71191 May 28 00:34 tncfg
-rwxr-xr-x 1 root  root   16876 May 28 00:34 uml_net
jig
-rwxr-xr-x 1 root  root  135365 May 28 00:34 whack
+ _____ ipsec/updowns
++ ls /usr/lib/ipsec
++ egrep updown
+ cat /usr/lib/ipsec/_updown
#!/bin/sh
# default updown script
# Copyright (C) 2000, 2001 D. Hugh Redelmeier, Henry Spencer
#
# This program is free software; you can redistribute it and/or
# modify it
# under the terms of the GNU General Public License as publishe
# d by the
# Free Software Foundation; either version 2 of the License, or
# (at your

```

```
# option) any later version. See <http://www.fsf.org/copyleft/
# gpl.txt>.
#
# This program is distributed in the hope that it will be usefu
# l, but
# WITHOUT ANY WARRANTY; without even the implied warranty of ME
# RCHANTABILITY
# or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Pub
# lic License
# for more details.
#
# RCSID $Id: _updown,v 1.19 2002/03/25 18:04:42 henry Exp $
```

```
# CAUTION: Installing a new version of FreeS/WAN will install
# a new
# copy of this script, wiping out any custom changes you make.
# If
# you need changes, make a copy of this under another name, and
# customize
# that, and use the (left/right)updown parameters in ipsec.conf
# to make
# FreeS/WAN use yours instead of this default one.
```

```
# check interface version
case "$PLUTO_VERSION" in
1.[0]) # Older Pluto?!? Play it safe, script may be using new
# features.
# echo "$0: obsolete interface version \" $PLUTO_VERSION',
# ">&2
# echo "$0: called by obsolete Pluto?" >&2
# exit 2
# ;;
1.*) ;;
*) echo "$0: unknown interface version \" $PLUTO_VERSION"
# ">&2
# exit 2
# ;;
esac
```

```
# check parameter(s)
case "$1:$*" in
':) # no parameters
# ;;
ipfwadm:ipfwadm) # due to (left/right)firewall; for defa
```

```

ult script only
;;
custom:*)          # custom parameters (see above CAUTION
comment)
;;
*)    echo "$0: unknown parameters \"${*}\" ">&2
      exit 2
;;
esac

# utility functions for route manipulation
# Meddling with this stuff should not be necessary and requires
# great care.
uproute() {
    doroute add
}
downroute() {
    doroute del
}
doroute() {
    parms="-net $PLUTO_PEER_CLIENT_NET netmask $PLUTO_PEER_
CLIENT_MASK"
    parms2="dev $PLUTO_INTERFACE gw $PLUTO_NEXT_HOP"
    case "$PLUTO_PEER_CLIENT_NET/$PLUTO_PEER_CLIENT_MASK" i
n
    "0.0.0.0/0.0.0.0")
        # horrible kludge for obscure routing bug with
opportunistic
        it="route $1 -net 0.0.0.0 netmask 128.0.0.0 $pa
rms2 &&
        route $1 -net 128.0.0.0 netmask 128.0.0
.0 $parms2"
        ;;
    *)    it="route $1 $parms $parms2"
        ;;
    esac
    eval $it
    st=$?
    if test $st -ne 0
    then
        # route has already given its own cryptic messa
ge
        echo "$0: \"${it}' failed" ">&2
        if test " $1 $st" = " add 7"
        then
            # another totally undocumented interfac
e -- 7 and
            # "SIOCADDRT: Network is unreachable" m

```

eans that

```

        # the gateway isn't reachable.
        echo "$0: (incorrect or missing nexthop
setting??)" >&2
        fi
    fi
    return $st
}

```

the big choice

```

case "$PLUTO_VERB:$1" in
prepare-host:*)|prepare-client:*)
    # delete possibly-existing route (preliminary to adding
a route)
    case "$PLUTO_PEER_CLIENT_NET/$PLUTO_PEER_CLIENT_MASK" in
n
    "0.0.0.0/0.0.0.0")
        # horrible kludge for obscure routing bug with
opportunistic
        it="route del -net 0.0.0.0 netmask 128.0.0.0 2>
&1 ;
        route del -net 128.0.0.0 netmask 128.0.
0.0 2>&1"
        ;;
    *)
        it="route del -net $PLUTO_PEER_CLIENT_NET \
netmask $PLUTO_PEER_CLI
ENT_MASK 2>&1"
        ;;
    esac
    oops="`eval $it`"
    status="$?"
    if test "$oops" = "" -a "$status" != "0"
    then
        oops="silent error, exit status $status"
    fi
    case "$oops" in
'SIOCDELRT: No such process'*)
        # This is what route (currently -- not document
ed!) gives
        # for "could not find such a route".
        oops=
        status=0
        ;;
    esac
    if test "$oops" != "" -o "$status" != "0"

```

```

then
    echo "$0: \'$it' failed ($oops)" >&2
fi
exit $status
;;
route-host:*|route-client:*)
    # connection to me or my client subnet being routed
    uproute
    ;;
unroute-host:*|unroute-client:*)
    # connection to me or my client subnet being unrouted
    downroute
    ;;
up-host:*)
    # connection to me coming up
    # If you are doing a custom version, firewall commands
    go here.
    ;;
down-host:*)
    # connection to me going down
    # If you are doing a custom version, firewall commands
    go here.
    ;;
up-client:*)
    # connection to my client subnet coming up
    # If you are doing a custom version, firewall commands
    go here.
    ;;
down-client:*)
    # connection to my client subnet going down
    # If you are doing a custom version, firewall commands
    go here.
    ;;
up-client:ipfwadm)
    # connection to client subnet, with (left/right)firewal
l=yes, coming up
    # This is used only by the default updown script, not b
y your custom
    # ones, so do not mess with it; see CAUTION comment up
at top.
    ipfwadm -F -i accept -b -S $PLUTO_MY_CLIENT_NET/$PLUTO_
MY_CLIENT_MASK \
        -D $PLUTO_PEER_CLIENT_NET/$PLUTO_PEER_CLIENT_MA
SK
    ;;
down-client:ipfwadm)
    # connection to client subnet, with (left/right)firewal
l=yes, going down

```

```

# This is used only by the default updown script, not b
y your custom
# ones, so do not mess with it; see CAUTION comment up
at top.
ipfwadm -F -d accept -b -S $PLUTO_MY_CLIENT_NET/$PLUTO_
MY_CLIENT_MASK \
-D $PLUTO_PEER_CLIENT_NET/$PLUTO_PEER_CLIENT_MA
SK
;;
*) echo "$0: unknown verb \"$PLUTO_VERB' or parameter \"$1
" ">&2
exit 1
;;
esac
+ _____ proc/net/dev
+ cat /proc/net/dev
Inter-l Receive
l Transmit
face lbytes packets errs drop fifo frame compressed multica
stlbytes packets errs drop fifo colls carrier compressed
lo: 54188 848 0 0 0 0 0 0
0 54188 848 0 0 0 0 0 0
ipsec0: 359125 4196 0 0 0 0 0 0
0 776788 4990 0 140 0 0 0 0
ipsec1: 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
ipsec2: 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
ipsec3: 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
eth0: 2152502 20972 0 0 0 0 0 0
0 2157566 14844 0 0 0 0 0 0
+ _____ proc/net/route
+ cat /proc/net/route
Iface Destination Gateway Flags RefCnt Use
Metric Mask MTU Window
IRTT
ipsec0 0A0110AC 0A0110AC 0007 0 0
0 FFFFFFFF 40
0 0

ipsec0 000101B4 0A0110AC 0003 0 0
0 00FFFFFF 40 0
0

ipsec0 000008A0 0A0110AC 0003 0 0
0 0000FFFF 40 0
0

```

```
eth0 000010AC 00000000 0001 0 0
0 0000FFFF 40 0 0
```

```
ipsec0 000010AC 00000000 0001 0 0
0 0000FFFF 40 0 0
```

```
lo 0000007F 00000000 0001 0 0
0 000000FF 40 0 0
```

```
eth0 00000000 650110AC 0003 0 0
0 00000000 40 0 0
```

```
+ _____ proc/sys/net/ipv4/ip_forward
+ cat /proc/sys/net/ipv4/ip_forward
0
+ _____ proc/sys/net/ipv4/conf/star-rp_filter
er
+ cd /proc/sys/net/ipv4/conf
+ egrep '^ all/rp_filter default/rp_filter eth0/rp_filter ipsec0/rp_filter lo/rp_filter
all/rp_filter:0
default/rp_filter:0
eth0/rp_filter:0
ipsec0/rp_filter:0
lo/rp_filter:0
+ _____ uname-a
+ uname -a
Linux jetproxy.smarttravelers.com 2.4.18-3ipsecsmp #1 SMP Fri M
ay 24 14:09:06 EDT 2002 i686 unknown
+ _____ redhat-release
+ test -r /etc/redhat-release
+ cat /etc/redhat-release
Red Hat Linux release 7.3 (Valhalla)
+ _____ proc/net/ipsec_version
+ cat /proc/net/ipsec_version
FreeS/WAN version: 1.97
+ _____ iptables/list
+ iptables -L -v -n
Chain INPUT (policy ACCEPT 223 packets, 9762 bytes)
pkts bytes target prot opt in out source
destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

pkts bytes target prot opt in out source
destination

Chain OUTPUT (policy ACCEPT 149 packets, 10531 bytes)

pkts bytes target prot opt in out source
destination

+ _____ ipchains/list

+ ipchains -L -v -n

ipchains: Incompatible with this kernel

+ _____ ipfwadm/forward

+ ipfwadm -F -l -n -e

Generic IP Firewall Chains not in this kernel

+ _____ ipfwadm/input

+ ipfwadm -I -l -n -e

Generic IP Firewall Chains not in this kernel

+ _____ ipfwadm/output

+ ipfwadm -O -l -n -e

Generic IP Firewall Chains not in this kernel

+ _____ iptables/nat

+ iptables -t nat -L -v -n

Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)

pkts bytes target prot opt in out source
destination

Chain POSTROUTING (policy ACCEPT 3 packets, 349 bytes)

pkts bytes target prot opt in out source
destination

Chain OUTPUT (policy ACCEPT 3 packets, 349 bytes)

pkts bytes target prot opt in out source
destination

+ _____ ipchains/masq

+ ipchains -M -L -v -n

ipchains: cannot open file `/proc/net/ip_masquerade'

+ _____ ipfwadm/masq

+ ipfwadm -M -l -n -e

Generic IP Firewall Chains not in this kernel

+ _____ iptables/mangle

+ iptables -t mangle -L -v -n

Chain PREROUTING (policy ACCEPT 223 packets, 9762 bytes)

pkts bytes target prot opt in out source
destination

Chain INPUT (policy ACCEPT 223 packets, 9762 bytes)

pkts bytes target prot opt in out source
destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 149 packets, 10531 bytes)

pkts bytes target prot opt in out source destination

Chain POSTROUTING (policy ACCEPT 149 packets, 10531 bytes)

pkts bytes target prot opt in out source destination

+ _____ proc/modules

+ cat /proc/modules

```

iptables_mangle      3104  0 (autoclean) (unused)
iptables_nat         21876  0 (autoclean) (unused)
ip_contrack          22732  1 (autoclean) [iptables_nat]
iptables_filter      2720  0 (autoclean) (unused)
ip_tables            14592  5 [iptables_mangle iptables_nat ip
table_filter]
ide-cd                30336  0 (autoclean)
cdrom                 32608  0 (autoclean) [ide-cd]
soundcore             7172  0 (autoclean)
iscsi                 94632  0 (unused)
autofs                12676  0 (autoclean) (unused)
eepro100              20752  1
usb-ohci              21568  0 (unused)
usbcore               76768  1 [usb-ohci]
ext3                  70752  2
jbd                   53632  2 [ext3]
sym53c8xx             63236  3
sd_mod                12896  6
scsi_mod              112272  3 [iscsi sym53c8xx sd_mod]

```

+ _____ proc/meminfo

+ cat /proc/meminfo

total: used: free: shared: buffers: cached:

Mem: 923131904 574210048 348921856 0 122089472 212791296

Swap: 1879040000 0 1879040000

MemTotal: 901496 kB

MemFree: 340744 kB

MemShared: 0 kB

Buffers: 119228 kB

Cached: 207804 kB

SwapCached: 0 kB

Active: 347512 kB

Inact_dirty: 8060 kB

Inact_clean: 19648 kB

Inact_target: 75044 kB

HighTotal: 0 kB

```
HighFree:      0 kB
LowTotal:     901496 kB
LowFree:      340744 kB
SwapTotal:    1835000 kB
SwapFree:     1835000 kB
Committed_AS: 85680 kB
+ _____ dev/ipsec-ls
+ ls -l '/dev/ipsec*'
ls: /dev/ipsec*: No such file or directory
+ _____ proc/net/ipsec-ls
+ ls -l /proc/net/ipsec_eroute /proc/net/ipsec_klipsdebug /proc
/net/ipsec_spi /proc/net/ipsec_spigrp /proc/net/ipsec_tncfg
/proc/net/ipsec_version
-r--r--r--  1 root  root      0 Aug 22 09:56 /proc/n
et/ipsec_eroute
-r--r--r--  1 root  root      0 Aug 22 09:56 /proc/n
et/ipsec_klipsdebug
-r--r--r--  1 root  root      0 Aug 22 09:56 /proc/n
et/ipsec_spi
-r--r--r--  1 root  root      0 Aug 22 09:56 /proc/n
et/ipsec_spigrp
-r--r--r--  1 root  root      0 Aug 22 09:56 /proc/n
et/ipsec_tncfg
-r--r--r--  1 root  root      0 Aug 22 09:56 /proc/n
et/ipsec_version
+ _____ usr/src/linux/.config
+ test -f /usr/src/linux/.config
+ egrep 'IPINETLINK' /usr/src/linux/.config
# CONFIG_MWINCHIP6 is not set
# CONFIG_MWINCHIP2 is not set
# CONFIG_MWINCHIP3D is not set
CONFIG_SYSVIPC=y
CONFIG_MD_MULTIPATH=m
CONFIG_NETLINK=y
CONFIG_RTNETLINK=y
CONFIG_NETLINK_DEV=y
CONFIG_IP_MULTICAST=y
CONFIG_IP_ADVANCED_ROUTER=y
CONFIG_RTNETLINK=y
CONFIG_NETLINK=y
CONFIG_IP_MULTIPLE_TABLES=y
CONFIG_IP_ROUTE_FWMARK=y
CONFIG_IP_ROUTE_NAT=y
CONFIG_IP_ROUTE_MULTIPATH=y
CONFIG_IP_ROUTE_TOS=y
CONFIG_IP_ROUTE_VERBOSE=y
CONFIG_IP_ROUTE_LARGE_TABLES=y
# CONFIG_IP_PNP is not set
```

```
CONFIG_NET_IPIP=y
CONFIG_NET_IPGRE=m
CONFIG_NET_IPGRE_BROADCAST=y
CONFIG_IP_MROUTE=y
CONFIG_IP_PIMSM_V1=y
CONFIG_IP_PIMSM_V2=y
# IP: Netfilter Configuration
CONFIG_IP_NF_CONNTRACK=m
CONFIG_IP_NF_FTP=m
CONFIG_IP_NF_IRC=m
CONFIG_IP_NF_QUEUE=m
CONFIG_IP_NF_IPTABLES=m
CONFIG_IP_NF_MATCH_LIMIT=m
CONFIG_IP_NF_MATCH_MAC=m
CONFIG_IP_NF_MATCH_MARK=m
CONFIG_IP_NF_MATCH_MULTIPORT=m
CONFIG_IP_NF_MATCH_TOS=m
CONFIG_IP_NF_MATCH_TCPMSS=m
CONFIG_IP_NF_MATCH_STATE=m
CONFIG_IP_NF_MATCH_UNCLEAN=m
CONFIG_IP_NF_MATCH_OWNER=m
CONFIG_IP_NF_FILTER=m
CONFIG_IP_NF_TARGET_REJECT=m
CONFIG_IP_NF_TARGET_MIRROR=m
CONFIG_IP_NF_NAT=m
CONFIG_IP_NF_NAT_NEEDED=y
CONFIG_IP_NF_TARGET_MASQUERADE=m
CONFIG_IP_NF_TARGET_REDIRECT=m
CONFIG_IP_NF_NAT_IRC=m
CONFIG_IP_NF_NAT_FTP=m
CONFIG_IP_NF_MANGLE=m
CONFIG_IP_NF_TARGET_TOS=m
CONFIG_IP_NF_TARGET_MARK=m
CONFIG_IP_NF_TARGET_LOG=m
CONFIG_IP_NF_TARGET_TCPMSS=m
CONFIG_IP_NF_COMPAT_IPCHAINS=m
CONFIG_IP_NF_NAT_NEEDED=y
CONFIG_IP_NF_COMPAT_IPFWADM=m
CONFIG_IP_NF_NAT_NEEDED=y
# IP: Virtual Server Configuration
CONFIG_IP_VS=m
# CONFIG_IP_VS_DEBUG is not set
CONFIG_IP_VS_TAB_BITS=16
CONFIG_IP_VS_RR=m
CONFIG_IP_VS_WRR=m
CONFIG_IP_VS_LC=m
CONFIG_IP_VS_WLC=m
CONFIG_IP_VS_LBLC=m
```

```
CONFIG_IP_VS_LBLCR=m
CONFIG_IP_VS_DH=m
CONFIG_IP_VS_SH=m
CONFIG_IP_VS_FTP=m
CONFIG_IPV6=m
# IPv6: Netfilter Configuration
CONFIG_IP6_NF_IPTABLES=m
CONFIG_IP6_NF_MATCH_LIMIT=m
CONFIG_IP6_NF_MATCH_MARK=m
CONFIG_IP6_NF_FILTER=m
CONFIG_IP6_NF_MANGLE=m
CONFIG_IP6_NF_TARGET_MARK=m
CONFIG_ATM_CLIP=y
# CONFIG_ATM_CLIP_NO_ICMP is not set
CONFIG_IPX=m
# CONFIG_IPX_INTERN is not set
CONFIG_NETLINK=y
CONFIG_RTNETLINK=y
CONFIG_IPSEC=y
CONFIG_IPSEC_IPIP=y
CONFIG_IPSEC_AH=y
CONFIG_IPSEC_AUTH_HMAC_MD5=y
CONFIG_IPSEC_AUTH_HMAC_SHA1=y
CONFIG_IPSEC_ESP=y
CONFIG_IPSEC_ENC_3DES=y
CONFIG_IPSEC_IPCOMP=y
CONFIG_IPSEC_DEBUG=y
# CONFIG_IDEDMA_PCI_WIP is not set
# CONFIG_IDE_CHIPSETS is not set
CONFIG_SCSI_IPS=m
# CONFIG_SCSI_IZIP_EPP16 is not set
# CONFIG_SCSI_IZIP_SLOW_CTR is not set
CONFIG_IPDDP=m
CONFIG_IPDDP_ENCAP=y
CONFIG_IPDDP_DECAP=y
CONFIG_TULIP=m
# CONFIG_TULIP_MWI is not set
CONFIG_TULIP_MMIO=m
# CONFIG_HIPPI is not set
CONFIG_PLIP=m
CONFIG_SLIP=m
CONFIG_SLIP_COMPRESSED=y
CONFIG_SLIP_SMART=y
CONFIG_SLIP_MODE_SLIP6=y
CONFIG_CIPSE=m
CONFIG_STRIP=m
CONFIG_IPHASE5526=m
CONFIG_WANPIPE_CHDLC=y
```

```
CONFIG_WANPIPE_FR=y
CONFIG_WANPIPE_X25=y
CONFIG_WANPIPE_PPP=y
CONFIG_WANPIPE_MULTPPP=y
CONFIG_PCMCIA_XIRTULIP=m
CONFIG_SERIAL_MULTIPORT=y
CONFIG_I2C_PHILIPSPAR=m
CONFIG_INPUT_GRIP=m
+ _____ etc/syslog.conf
+ cat /etc/syslog.conf
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/co
nsole

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;cron.none
/var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/lo
g/secure

# Log all the mail messages in one place.
mail.* /var/lo
g/maillog

# Log cron stuff
cron.* /var/lo
g/cron

# Everybody gets emergency messages
*.emerg *

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/lo
g/spooler

# Save boot messages also to boot.log
local7.* /var/lo
g/boot.log

#
# INN
#
news.=crit /var/log/news
```

```
/news.crit
news.=err                /var/log/news
/news.err
news.notice              /var/log/news
/news.notice
+ _____ lib/modules-ls
+ ls -ltr /lib/modules
total 20
drwxr-xr-x  4 root  root    4096 Jun 27 09:51 2.4.7-1
Ocustom
drwxr-xr-x  4 root  root    4096 Jun 28 09:52 2.4.18-
3smp
drwxr-xr-x  4 root  root    4096 Jun 28 09:53 2.4.18-
3
drwxr-xr-x  4 root  root    4096 Jun 28 10:21 2.4.18-
3debug
drwxr-xr-x  4 root  root    4096 Jun 28 10:38 2.4.18-
3ipsecsmp
+ _____ proc/ksyms-netif_rx
+ egrep netif_rx /proc/ksyms
c01dcee0 netif_rx_Rsmp_7f5f3ded
+ _____ lib/modules-netif_rx
+ modulegoo kernel/net/ipv4/ipip.o netif_rx
+ set +x
2.4.18-3:      U netif_rx_R35fec680
2.4.18-3debug:    U netif_rx_R35fec680
2.4.18-3ipsecsmp:  U netif_rx_Rsmp_7f5f3ded
2.4.18-3smp:     U netif_rx_Rsmp_7f5f3ded
2.4.7-10custom:
+ _____ kern.debug
+ test -f /var/log/kern.debug
+ _____ klog
+ sed -n '75,$p' /var/log/messages
+ egrep -i 'ipsecklips|pluto'
+ cat
Aug 22 09:55:35 jetproxy ipsec_setup: Starting FreeS/WAN IPsec
U1.95/K1.97...
Aug 22 09:55:35 jetproxy ipsec_setup: KLIPS debug `none'
Aug 22 09:55:35 jetproxy ipsec_setup: KLIPS ipsec0 on eth0 172.
16.1.102/255.255.0.0 broadcast 172.16.255.255
Aug 22 09:55:35 jetproxy ipsec_setup: ...FreeS/WAN IPsec starte
d
Aug 22 09:55:36 jetproxy ipsec__plutorun: 104 "linux-fw1-1" #1:
STATE_MAIN_I1: initiate
Aug 22 09:55:36 jetproxy ipsec__plutorun: 106 "linux-fw1-1" #1:
STATE_MAIN_I2: sent MI2, expecting MR2
Aug 22 09:55:36 jetproxy ipsec__plutorun: 108 "linux-fw1-1" #1:
STATE_MAIN_I3: sent MI3, expecting MR3
```

```
Aug 22 09:55:36 jetproxy ipsec__plutorun: 004 "linux-fw1-1" #1:
STATE_MAIN_I4: ISAKMP SA established
Aug 22 09:55:36 jetproxy ipsec__plutorun: 112 "linux-fw1-1" #2:
STATE_QUICK_I1: initiate
Aug 22 09:55:36 jetproxy ipsec__plutorun: 004 "linux-fw1-1" #2:
STATE_QUICK_I2: sent QI2, IPsec SA established
Aug 22 09:55:36 jetproxy ipsec__plutorun: 112 "linux-fw1-2" #3:
STATE_QUICK_I1: initiate
Aug 22 09:55:36 jetproxy ipsec__plutorun: 004 "linux-fw1-2" #3:
STATE_QUICK_I2: sent QI2, IPsec SA established
Aug 22 09:55:36 jetproxy ipsec__plutorun: 112 "linux-fw1" #4: S
TATE_QUICK_I1: initiate
Aug 22 09:55:36 jetproxy ipsec__plutorun: 004 "linux-fw1" #4: S
TATE_QUICK_I2: sent QI2, IPsec SA established
+ _____ plog
+ sed -n '1030,$p' /var/log/secure
+ egrep -i pluto
+ cat
Aug 22 09:55:35 jetproxy ipsec__plutorun: Starting Pluto subsys
tem...
Aug 22 09:55:35 jetproxy Pluto[4017]: Starting Pluto (FreeS/WAN
Version 1.95)
Aug 22 09:55:36 jetproxy Pluto[4017]: added connection descript
ion "linux-fw1-1"
Aug 22 09:55:36 jetproxy Pluto[4017]: added connection descript
ion "linux-fw1-2"
Aug 22 09:55:36 jetproxy Pluto[4017]: added connection descript
ion "linux-fw1"
Aug 22 09:55:36 jetproxy Pluto[4017]: listening for IKE message
s
Aug 22 09:55:36 jetproxy Pluto[4017]: adding interface ipsec0/e
th0 172.16.1.102
Aug 22 09:55:36 jetproxy Pluto[4017]: loading secrets from "/et
c/ipsec.secrets"
Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1-1" #1: initiat
ing Main Mode
Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1-1" #1: ISAKMP
SA established
Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1-1" #2: initiat
ing Quick Mode
PSK+ENCRYPT+TUNNEL+DISABLEARRIVALCHECK
Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1-1" #2: sent QI
2, IPsec SA established
Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1-2" #3: initiat
ing Quick Mode
PSK+ENCRYPT+TUNNEL+DISABLEARRIVALCHECK
Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1-2" #3: sent QI
2, IPsec SA established
```

Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1" #4: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+DISABLEARRIVALCHECK
Aug 22 09:55:36 jetproxy Pluto[4017]: "linux-fw1" #4: sent QI2,
IPsec SA established
+ _____ date
+ date
Thu Aug 22 09:56:16 HKT 2002