Subject: *SOLVED* ip_conntrack_ftp for iptables/ftp server in VE
Posted by enpx on Wed, 26 Dec 2007 11:22:18 GMT
View Forum Message <> Reply to Message

Dec 26 21:54:06 br-gw kernel: REJECTED: IN=stc OUT= PHYSIN=stc PHYSOUT=veth101.stc MAC=00:18:51:99:01:ca:00:04:23:b3:ab:c6:08:00 SRC=192.168.12.241 DST=192.168.15.16 LEN=52 TOS=0x08 PREC=0x00 TTL=63 ID=21500 DF PROTO=TCP SPT=35387 DPT=58139 WINDOW=5840 RES=0x00 SYN URGP=0

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by khorenko on Wed, 26 Dec 2007 12:08:51 GMT
View Forum Message <> Reply to Message

--
Konstantin.

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE

2.6.18-ovz-smp-alt18, iptables-1.3.7-alt1

```
# lsmod
Module                  Size  Used by
ip_conntrack_ftp       18256  0
ipt_LOG                15872  1
simfs                  13976  5
vzethdev               23056  0
vznetdev               33672  5
vzrst                 143272  0
vzcpt                 120376  0
vzdquota               57576  5 [permanent]
vzmon                  52368  9 vzethdev,vznetdev,vzrst,vzcpt
vzdev                  12680  4 vzethdev,vznetdev,vzdquota,vzmon
af_packet              41868  0
xt_tcpudp              12160  21
iptable_nat            19332  12
ip_nat                 30352  2 vzrst,iptable_nat
iptable_mangle         13696  5
iptable_filter         13568  7
ipt_REJECT             14336  4
ip_tables              32360  3 iptable_nat,iptable_mangle,iptable_filter
bridge                 74544  0
8021q                  32768  5
dm_mod                 73936  0
ide_cd                 51616  0
rtc                    23424  0
ehci_hcd               43016  0
evdev                  19840  0
psmouse                52112  0
cdrom                  45992  1 ide_cd
uhci_hcd               34328  0
i2c_i801               17300  0
serio_raw              16516  0
pcspkr                 12032  0
i2c_core               33280  1 i2c_i801
usbcore               155944  3 ehci_hcd,uhci_hcd
tg3                   121988  0
sg                     47272  0
xt_multiport           12160  4
xt_state               11008  12
x_tables               29704  7
```

```
ipt_LOG,xt_tcpudp,iptable_nat,ipt_REJECT,ip_tables,xt_multiport,xt_state
ip_conntrack           80788  11 ip_conntrack_ftp,vzrst,vzcpt,iptable_nat,ip_nat,xt_state
nfnetlink              16456  2 ip_nat,ip_conntrack
button                 16544  0
ext3                  154000  2
jbd                    82544  1 ext3
mbcache                18824  1 ext3
raid1                  32896  2
ahci                   32004  6
libata                121120  1 ahci
sd_mod                 30976  8
scsi_mod              166320  4 sg,ahci,libata,sd_mod
ide_disk               25984  0
ide_generic             9856  0 [permanent]
generic                14596  0 [permanent]
piix                   20228  0 [permanent]
ide_core              164608  5 ide_cd,ide_disk,ide_generic,generic,piix
```

```
+ /sbin/iptables -F
+ /sbin/iptables -X
+ /sbin/iptables -t nat -F
+ /sbin/iptables -t nat -X
+ /sbin/iptables -P INPUT DROP
+ /sbin/iptables -P OUTPUT DROP
+ /sbin/iptables -P FORWARD DROP
+ /sbin/iptables -N allowed
+ /sbin/iptables -A allowed -j ACCEPT
+ /sbin/iptables -N rejected
+ /sbin/iptables -A rejected -j LOG --log-prefix 'REJECTED: '
+ /sbin/iptables -A rejected -p tcp -j REJECT --reject-with tcp-reset
+ /sbin/iptables -A rejected -j REJECT --reject-with icmp-port-unreachable
+ /sbin/iptables -A INPUT -i lo -j allowed
+ /sbin/iptables -A OUTPUT -o lo -j allowed
+ /sbin/iptables -A INPUT -p tcp -m state --state established,related -j allowed
+ /sbin/iptables -A OUTPUT -p tcp -m state --state established,related -j allowed
+ /sbin/iptables -A INPUT -p icmp -j allowed
+ /sbin/iptables -A OUTPUT -p icmp -j allowed
+ /sbin/iptables -A OUTPUT -p tcp --syn -j allowed
+ /sbin/iptables -A INPUT -p tcp --syn -i + -d 0.0.0.0/0 --dport 21 -j allowed
+ /sbin/iptables -A INPUT -p tcp --syn -i + -d 0.0.0.0/0 --dport 22 -j allowed
+ /sbin/iptables -A INPUT -j rejected
+ /sbin/iptables -A OUTPUT -j rejected
+ /sbin/iptables -A FORWARD -j rejected
```

$ lftp 192.168.15.16
lftp 192.168.15.16:~> ls

Dec 26 23:46:05 br-gw xinetd[12199]: START: ftp pid=3600 from=192.168.12.224
Dec 26 23:46:05 br-gw kernel: REJECTED: IN=stc OUT= PHYSIN=stc PHYSOUT=veth101.stc
MAC=00:18:51:99:01:ca:00:04:23:b3:ab:c6:08:00 SRC=192.168.12.224 DST=192.168.15.16
LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=56914 DF PROTO=TCP SPT=47429 DPT=64100
WINDOW=5840 RES=0x00 SYN URGP=0

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by khorenko on Fri, 28 Dec 2007 14:58:33 GMT
View Forum Message <> Reply to Message

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by enpx on Sat, 29 Dec 2007 06:20:09 GMT
View Forum Message <> Reply to Message

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by khorenko on Sat, 29 Dec 2007 12:20:50 GMT
View Forum Message <> Reply to Message

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by enpx on Sun, 30 Dec 2007 15:39:42 GMT
View Forum Message <> Reply to Message

Quote:

Quote:

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by gblond on Tue, 08 Jan 2008 11:36:35 GMT
View Forum Message <> Reply to Message

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by enpx on Wed, 09 Jan 2008 08:03:36 GMT
View Forum Message <> Reply to Message

IPTABLES="ipt_REJECT iptable_filter iptable_mangle iptable_nat ip_nat_ftp ip_conntrack_ftp"

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by gblond on Wed, 09 Jan 2008 09:01:30 GMT
View Forum Message <> Reply to Message

Subject: Re: ip_conntrack_ftp for iptables/ftp server in VE
Posted by enpx on Wed, 09 Jan 2008 09:28:24 GMT
View Forum Message <> Reply to Message