
Subject: *SOLVED* How to provide access between Virtual servers

Posted by [laurent](#) on Fri, 21 Jul 2006 09:23:46 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hello All,

i have a Host H with 3 virtual server

i can access from a VPS to the internet , and with NAt rule (Via Shorewall) i can access from Internet to the 3 VPS

i want that all the 3 VPS can communicate between them.

i can't do a tcp connection from a VPS to an other , in my shorewall log in the Host, i have this error :

```
kernel: Shorewall:FORWARD:REJECT:IN=venet0 OUT=venet0 SRC=192.168.7.185
DST=192.168.7.152 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=48986 DF PROTO=TCP
SPT=47559 DPT=25 WINDOW=5840 RES=0x00 SYN URGP=0
```

some body here have the solution ?

thanks in advance

Subject: Re: How to provide access between Virtual servers

Posted by [Vasily Tarasov](#) on Fri, 21 Jul 2006 09:33:48 GMT

[View Forum Message](#) <> [Reply to Message](#)

As I understand you just set REJECT-rule for ip-forwarding from one VE to another... To be sure, please give the command on host:

```
# iptables -L -nv
```

If so, just remove this rule.

Subject: Re: How to provide access between Virtual servers

Posted by [laurent](#) on Fri, 21 Jul 2006 11:19:32 GMT

[View Forum Message](#) <> [Reply to Message](#)

Thanks for your answer

i m using a shorwall firewall

i have this in my default policy, my Host is fw

```
net      all      DROP      info
fw       all      ACCEPT
loc      all      ACCEPT
loc      venet   ACCEPT #
venet    all      ACCEPT
```

all all REJECT info

And it doesn't work.

But if i replace the last line with
all all ACCEPT
it work. but this rule is very permissive

i triyed many combination ... no good result !

Perhaps the problem is that venet0 isn't a real ethernet interface ? so we can't do this simply ...

Thanks.

Subject: Re: How to provide access between Virtual servers
Posted by [Vasily Tarasov](#) on Fri, 21 Jul 2006 11:42:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

Please try change
loc venet ACCEPT
to
all venet ACCEPT

HTH! =)

Subject: Re: How to provide access between Virtual servers
Posted by [laurent](#) on Fri, 21 Jul 2006 13:19:20 GMT
[View Forum Message](#) <> [Reply to Message](#)

Same error !

Subject: Re: How to provide access between Virtual servers
Posted by [Vasily Tarasov](#) on Fri, 21 Jul 2006 13:26:46 GMT
[View Forum Message](#) <> [Reply to Message](#)

Is it possible for you to post here the output of
iptables -L -nv
here.

Shorewall is based on iptables and I want to see exact iptables rules, that Shorewall has set.

Thanks!

Subject: Re: How to provide access between Virtual servers
Posted by [laurent](#) on Fri, 21 Jul 2006 13:45:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

attached

File Attachments

1) [iptables.txt](#), downloaded 525 times

Subject: Re: How to provide access between Virtual servers
Posted by [Vasily Tarasov](#) on Fri, 21 Jul 2006 14:15:52 GMT

[View Forum Message](#) <> [Reply to Message](#)

This is quick analysis.

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
3595	331K	eth0_fwd	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	
4006	2992K	venet0_fwd	all	--	venet0	*	0.0.0.0/0	0.0.0.0/0	
0	0	eth1_fwd	all	--	eth1	*	0.0.0.0/0	0.0.0.0/0	
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:FORWARD:REJECT:'									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

You can see the string "Shorewall:FORWARD:REJECT" - that is what in your error message, thus packets are dropped here. Therefore the packet isn't caught by the rule "venet0_fwd". Look at it:

Chain venet0_fwd (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
199	15876	dynamic	all	--	*	*	0.0.0.0/0	0.0.0.0/0	INVALID,NEW
4006	2992K	venet2all	all	--	*	eth0	0.0.0.0/0	0.0.0.0/0	
0	0	venet2all	all	--	*	eth1	0.0.0.0/0	0.0.0.0/0	

Really! out equals eth0 and eth1, but in our case, when two VEs speake, out must equals venet0 too.

Subject: Re: How to provide access between Virtual servers
Posted by [laurent](#) on Fri, 21 Jul 2006 14:24:35 GMT

[View Forum Message](#) <> [Reply to Message](#)

Perhaps because venet0 isn't a real network's interface. it's a virtual one.
So i must do other thinks ...

Subject: Re: How to provide access between Virtual servers
Posted by [laurent](#) on Fri, 21 Jul 2006 14:44:19 GMT
[View Forum Message](#) <> [Reply to Message](#)

Ok i found
in the /etc/shorewall/interfaces i must add routeback like :
venet venet0 detect routeback

thanks

Subject: Re: *SOLVED* How to provide access between Virtual servers
Posted by [zenny](#) on Tue, 12 Dec 2006 11:44:58 GMT
[View Forum Message](#) <> [Reply to Message](#)

I have also tried to do the same and added the venet line in the /etc/shorewall/interfaces also but the shorewall just terminates with an error message that reads:

ERROR: Invalid zone (venet) in record "venet venet0 detect routeback"

Where did I go wrong? This is basically based on the 3-interface setup of shorewall. find below the output of iptables -L -nv:

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
1049	76734	eth0_in	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	
0	0	eth1_in	all	--	eth1	*	0.0.0.0/0	0.0.0.0/0	
0	0	eth2_in	all	--	eth2	*	0.0.0.0/0	0.0.0.0/0	
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:INPUT:REJECT:'									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
387	60317	eth0_fwd	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	
0	0	eth1_fwd	all	--	eth1	*	0.0.0.0/0	0.0.0.0/0	
730	313K	eth2_fwd	all	--	eth2	*	0.0.0.0/0	0.0.0.0/0	
37	1924	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
37	1924	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:FORWARD:REJECT:'									

```
37 1924 reject all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	*	lo	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	udp	--	*	eth0	0.0.0.0/0	0.0.0.0/0	udp dpts:67:68
816	214K	fw2net	all	--	*	eth0	0.0.0.0/0	0.0.0.0/0	
0	0	fw2loc	all	--	*	eth1	0.0.0.0/0	192.168.0.0/24	
0	0	fw2loc	all	--	*	eth1	0.0.0.0/0	255.255.255.255	
0	0	fw2loc	all	--	*	eth1	0.0.0.0/0	224.0.0.0/4	
404	229K	fw2dmz	all	--	*	eth2	0.0.0.0/0	0.0.0.0/0	
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix

`Shorewall:OUTPUT:REJECT:'

0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
---	---	--------	-----	----	---	---	-----------	-----------	--

Chain Drop (4 references)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	reject	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:113
50	6966	dropBcast	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 3 code 4
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 11
31	6434	dropInvalid	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport dports 135,445
2	156	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpts:137:139
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:137

dpts:1024:65535

17	944	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport dports
----	-----	------	-----	----	---	---	-----------	-----------	------------------

135,139,445

0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:1900
2	96	dropNotSyn	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:53

Chain Reject (13 references)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	reject	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:113
441	271K	dropBcast	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 3 code 4
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 11
441	271K	dropInvalid	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	reject	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport dports 135,445
0	0	reject	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpts:137:139
0	0	reject	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:137 dpts:1024:65535
0	0	reject	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport dports 135,139,445
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:1900
37	1924	dropNotSyn	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:53

Chain all2all (0 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:all2all:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain dmz2all (0 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:dmz2all:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain dmz2fw (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 8
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:dmz2fw:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain dmz2loc (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 8
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:dmz2loc:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain dmz2net (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
326	43723	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 8
404	269K	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
404	269K	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:dmz2net:REJECT:`									

404 269K reject all -- * * 0.0.0.0/0 0.0.0.0/0

Chain dropBcast (2 references)

pkts	bytes	target	prot	opt	in	out	source	destination
0	0	DROP	all	--	*	*	0.0.0.0/0	81.216.202.223
0	0	DROP	all	--	*	*	0.0.0.0/0	192.168.0.255
0	0	DROP	all	--	*	*	0.0.0.0/0	192.168.1.255
0	0	DROP	all	--	*	*	0.0.0.0/0	255.255.255.255
19	532	DROP	all	--	*	*	0.0.0.0/0	224.0.0.0/4

Chain dropInvalid (2 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
1	40	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	INVALID

Chain dropNotSyn (2 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:!0x16/0x02
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain fw2loc (3 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:fw2loc:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain fw2net (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
816	214K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:fw2net:ACCEPT:`									
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain loc2all (0 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:loc2all:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain loc2dmz (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 8
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:loc2dmz:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain loc2fw (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 8
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:loc2fw:REJECT:`									
0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain loc2net (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain logflags (5 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 4 level 6 prefix
`Shorewall:logflags:DROP:`									
0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain net2all (0 references)

pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	Drop	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:net2all:DROP:`									
:									
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state
RELATED,ESTABLISHED									
0	0	Reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	all	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 6 prefix
`Shorewall:loc2all:REJECT:`									


```
0 0 reject all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain loc2dmz (1 references)

```
pkts bytes target prot opt in out source destination state
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 8
0 0 Reject all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 LOG all -- * * 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 6 prefix
`Shorewall:loc2dmz:REJECT:`
0 0 reject all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain loc2fw (1 references)

```
pkts bytes target prot opt in out source destination state
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 8
0 0 Reject all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 LOG all -- * * 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 6 prefix
`Shorewall:loc2fw:REJECT:`
0 0 reject all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain loc2net (1 references)

```
pkts bytes target prot opt in out source destination state
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain logflags (5 references)

```
pkts bytes target prot opt in out source destination state
0 0 LOG all -- * * 0.0.0.0/0 0.0.0.0/0 LOG flags 4 level 6 prefix
`Shorewall:logflags:DROP:`
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain net2all (0 references)

```
pkts bytes target prot opt in out source destination state
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
0 0 Drop all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 LOG all -- * * 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 6 prefix
`Shorewall:net2all:DROP:`
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain net2dmz (1 references)

```
pkts bytes target prot opt in out source destination state
349 58343 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state
```

RELATED,ESTABLISHED

```
0 0 ACCEPT udp -- * * 0.0.0.0/0 192.168.1.250 udp dpts:5060:5088
0 0 ACCEPT udp -- * * 0.0.0.0/0 192.168.1.250 udp dpts:8000:20000
0 0 ACCEPT udp -- * * 0.0.0.0/0 192.168.1.250 udp dpt:3478
1 50 ACCEPT udp -- * * 0.0.0.0/0 192.168.1.250 udp dpt:4569
0 0 ACCEPT tcp -- * * 0.0.0.0/0 192.168.1.250 tcp dpt:25
0 0 ACCEPT tcp -- * * 0.0.0.0/0 192.168.1.250 tcp dpt:110
0 0 ACCEPT tcp -- * * 0.0.0.0/0 192.168.1.250 tcp dpt:80
0 0 ACCEPT tcp -- * * 0.0.0.0/0 192.168.1.250 tcp dpt:81
0 0 ACCEPT tcp -- * * 0.0.0.0/0 192.168.1.250 tcp dpt:22
0 0 ACCEPT tcp -- * * 0.0.0.0/0 192.168.1.204 tcp dpts:80:81
0 0 Drop all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 LOG all -- * * 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 6 prefix
`Shorewall:net2dmz:DROP:`
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain net2fw (1 references)

```
pkts bytes target prot opt in out source
```

Shall be obliged for help to overcome the problem.

Subject: Re: *SOLVED* How to provide access between Virtual servers
Posted by [jbond007](#) on Tue, 12 Dec 2006 14:10:57 GMT

[View Forum Message](#) <> [Reply to Message](#)

the best way is Use easy Gui form webmin !
firewall is very easy !

then check the files cat /etc/syconfig/iptables

Subject: Re: *SOLVED* How to provide access between Virtual servers
Posted by [zenny](#) on Wed, 13 Dec 2006 05:57:31 GMT

[View Forum Message](#) <> [Reply to Message](#)

Let me clear my situation to explain why webmin is not the way to go. I tried yum install webmin in the hostnode, but reported that there is no such maches.

I am using 3-interface home network with eth0 (internet), eth1 (local) and eth2 (dmz). The host node of the machine serves as firewall and also a gateway to the local and dmz (connected to voip server by a crossove cable). Now the problem whatever I change in the shorewall configurations as stated above and other changes, my voipserver connected to eth2 could not access the termination server as well as the VEs are not accessible.

Does anyone has any clue with the existing stuff?
