

Fedora: RE: can ping but not browse

RE: can ping but not browse

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2005-03/5931.html>

From: Ravi Prasad (ravi4edu_at_yahoo.com)

Date: 03/28/05

Date: Sun, 27 Mar 2005 18:55:32 -0800 (PST)

To: bedouglas@earthlink.net, For users of Fedora Core releases <fedora-list@redhat.com>

Hi Bruce,

Have a look at the SuSEfirewall2 file of the gateway SuSe machine. On my internal PC running Fedora I have stopped the firewall.

Regds..

```
//-----SuSEfirewall2-----START-----
# Copyright (c) 2000-2002 SuSE GmbH Nuernberg,
Germany. All rights reserved.
#
# Author: Marc Heuse <marc@suse.de>, 2002
# Please contact me directly if you find bugs.
#
# If you have problems getting this tool configures,
please read this file
# carefully and take also a look into
# -> /usr/share/doc/packages/SuSEfirewall2/EXAMPLES !
# -> /usr/share/doc/packages/SuSEfirewall2/FAQ !
# ->
/usr/share/doc/packages/SuSEfirewall2/SuSEfirewall2.conf.EXAMPLE
!
#
# /etc/sysconfig/SuSEfirewall2
#
# for use with /sbin/SuSEfirewall2 version 3.1 which
is for 2.4 kernels!
#
#
-----
#
# PLEASE NOTE THE FOLLOWING:
#
# Just by configuring these settings and using the
SuSEfirewall2 you are
# not secure per se! There is *not* such a thing you
install and hence you
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
# are safed from all (security) hazards.
#
# To ensure your security, you need also:
#
# * Secure all services you are offering to
untrusted networks (internet)
# You can do this by using software which has been
designed with
# security in mind (like postfix, apop3d, ssh),
setting these up without
# misconfiguration and praying, that they have got
really no holes.
# SuSEcompartment can help in most circumstances
to reduce the risk.
# * Do not run untrusted software. (philosophical
question, can you trust
# SuSE or any other software distributor?)
# * Harden your server(s) with the harden_suse
package/script
# * Recompile your kernel with the openwall–linux
kernel patch
# (former secure–linux patch, from Solar Designer)
www.openwall.com
# * Check the security of your server(s) regularly
# * If you are using this server as a
firewall/bastion host to the internet
# for an internal network, try to run proxy
services for everything and
# disable routing on this machine.
# * If you run DNS on the firewall: disable
untrusted zone transfers and
# either don't allow access to it from the
internet or run it split–brained.
#
# Good luck!
#
# Yours,
# SuSE Security Team
#
#
-----
#
# Configuration HELP:
#
# If you have got any problems configuring this file,
take a look at
# /usr/share/doc/packages/SuSEfirewall2/EXAMPLES for
an example.
#
#
# All types have to set enable SuSEfirewall2 in the
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
runlevel editor
#
# If you are a end-user who is NOT connected to two
networks (read: you have
# got a single user system and are using a dialup to
the internet) you just
# have to configure (all other settings are OK): 2)
and maybe 9).
#
# If this server is a firewall, which should act like
a proxy (no direct
# routing between both networks), or you are an
end-user connected to the
# internet and to an internal network, you have to
setup your proxys and
# reconfigure (all other settings are OK): 2), 3), 9)
and maybe 7), 11), 14)
#
# If this server is a firewall, and should do
routing/masquerading between
# the untrusted and the trusted network, you have to
reconfigure (all other
# settings are OK): 2), 3), 5), 6), 9), and maybe 7),
10), 11), 12), 13),
# 14), 20)
#
# If you want to run a DMZ in either of the above
three standard setups, you
# just have to configure *additionally* 4), 9), 12),
13), 17), 19).
#
# If you know what you are doing, you may also change
8), 11), 15), 16)
# and the expert options 19), 20), 21), 22) and 23) at
the far end, but you
# should NOT.
#
# If you use diald or ISDN autodialing, you might want
to set 17).
#
# To get programs like traceroutes to your firewall to
work is a bit tricky,
# you have to set the following options to "yes" : 11
(UDP only), 18 and 19.
#
# Please note that if you use service names, that they
exist in /etc/services.
# There is no service "dns", it's called "domain";
email is called "smtp" etc.
#
# *Any* routing between interfaces except masquerading
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
requires to set FW_ROUTE
# to "yes" and use FW_FORWARD or
FW_ALLOW_CLASS_ROUTING !
#
# If you just want to do masquerading without
filtering, ignore this script
# and run this line (exchange "ipp0" "ppp0" if you
use a modem, not isdn):
# iptables -A POSTROUTING -t nat -j MASQUERADE -o
ipp0
# echo 1 > /proc/sys/net/ipv4/ip_forward
# and additionally the following lines to get at least
a minimum of security:
# iptables -A INPUT -j DROP -m state --state
NEW,INVALID -i ipp0
# iptables -A FORWARD -j DROP -m state --state
NEW,INVALID -i ipp0
#
```

```
## Path: Network/Firewall/SuSEfirewall2
## Description: SuSEfirewall2 configuration
## Type: yesno
## Default: no
## ServiceRestart: SuSEfirewall2_setup
#
# 1.)
# Should the Firewall run in quickmode?
#
# "Quickmode" means that only the interfaces pointing
to external networks
# are secured, and no other. all interfaces not in the
list of FW_DEV_EXT
# are allowed full network access! Additionally,
masquerading is
# automatically activated for FW_MASQ_DEV devices. and
last but not least:
# all incoming connection via external interfaces are
REJECTED.
# You will only need to configure 2.) and FW_MASQ_DEV
in 6.)
# Optionally, you may add entries to section 9a.)
#
# Choice: "yes" or "no", if not set defaults to "no"
#
FW_QUICKMODE="no"
```

```
## Type: string
# 2.)
# Which is the interface that points to the
internet/untrusted networks?
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
#
# Enter all the network devices here which are
untrusted.
#
# Choice: any number of devices, seperated by a space
# e.g. "eth0", "ipp0 ipp1 eth0:1"
#
FW_DEV_EXT="eth1"

## Type: string
#
# 3.)
# Which is the interface that points to the internal
network?
#
# Enter all the network devices here which are
trusted.
# If you are not connected to a trusted network (e.g.
you have just a
# dialup) leave this empty.
#
# Choice: leave empty or any number of devices,
seperated by a space
# e.g. "tr0", "eth0 eth1 eth1:1" or ""
#
FW_DEV_INT="eth0"

## Type: string
#
# 4.)
# Which is the interface that points to the dmz or
dialup network?
#
# Enter all the network devices here which point to
the dmz/dialups.
# A "dmz" is a special, seperated network, which is
only connected to the
# firewall, and should be reachable from the internet
to provide services,
# e.g. WWW, Mail, etc. and hence are at risk from
attacks.
# See /usr/share/doc/packages/SuSEfirewall2/EXAMPLES
for an example.
#
# Special note: You have to configure FW_FORWARD to
define the services
# which should be available to the internet and set
FW_ROUTE to yes.
#
# Choice: leave empty or any number of devices,
seperated by a space
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
# e.g. "tr0", "eth0 eth1 eth1:1" or ""
#
FW_DEV_DMZ=""

## Type: yesno
## Default: no
#
# 5.)
# Should routing between the internet, dmz and
internal network be activated?
# REQUIRES: FW_DEV_INT or FW_DEV_DMZ
#
# You need only set this to yes, if you either want to
masquerade internal
# machines or allow access to the dmz (or internal
machines, but this is not
# a good idea). This option supersedes IP_FORWARD from
# /etc/sysconfig/network/options
#
# Setting this option one alone doesn't do anything.
Either activate
# masquerading with FW_MASQUERADE below if you want
to masquerade your
# internal network to the internet, or configure
FW_FORWARD to define
# what is allowed to be forwarded!
#
# Choice: "yes" or "no", if not set defaults to "no"
#
FW_ROUTE="yes"

## Type: yesno
## Default: no
#
# 6.)
# Do you want to masquerade internal networks to the
outside?
# REQUIRES: FW_DEV_INT or FW_DEV_DMZ, FW_ROUTE
#
# "Masquerading" means that all your internal machines
which use services on
# the internet seem to come from your firewall.
# Please note that it is more secure to communicate
via proxies to the
# internet than masquerading. This option is required
for FW_MASQ_NETS and
# FW_FORWARD_MASQ.
#
# Choice: "yes" or "no", if not set defaults to "no"
#
FW_MASQUERADE="yes"
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
## Type: string
#
# You must also define on which interface(s) to
masquerade on. This is
# normally your external device(s) to the internet.
# Most users can leave the default below.
#
# e.g. "ipp0" or "$FW_DEV_EXT"
FW_MASQ_DEV="$FW_DEV_EXT"

## Type: string
#
# Which internal computers/networks are allowed to
access the internet
# directly (not via proxys on the firewall)?
# Only these networks will be allowed access and will
be masqueraded!
#
# Choice: leave empty or any number of hosts/networks
seperated by a space.
# Every host/network may get a list of allowed
services, otherwise everything
# is allowed. A target network, protocol and service
is appended by a comma to
# the host/network. e.g. "10.0.0.0/8" allows the whole
10.0.0.0 network with
# unrestricted access. "10.0.1.0/24,0/0,tcp,80
10.0.1.0/24,0/0tcp,21" allows
# the 10.0.1.0 network to use www/ftp to the internet.
# "10.0.1.0/24,tcp,1024:65535 10.0.2.0/24" is OK too.
# Set this variable to "0/0" to allow unrestricted
access to the internet.
#
FW_MASQ_NETS="0/0"

## Type: yesno
## Default: yes
#
# 7.)
# Do you want to protect the firewall from the
internal network?
# REQUIRES: FW_DEV_INT
#
# If you set this to "yes", internal machines may only
access services on
# the machine you explicitly allow. They will be also
affected from the
# FW_AUTOPROTECT_SERVICES option.
# If you set this to "no", any user can connect (and
attack) any service on
# the firewall.
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
#
# Choice: "yes" or "no", if not set defaults to "yes"
#
# "yes" is a good choice
FW_PROTECT_FROM_INTERNAL="no"

## Type: yesno
## Default: yes
#
# 8.)
# Do you want to autoprotect all running network
services on the firewall?
#
# If set to "yes", all network access to services TCP
and UDP on this machine
# will be prevented (except to those which you
explicitly allow, see below:
# FW_SERVICES_{EXT,DMZ,INT}_{TCP,UDP})
#
# Choice: "yes" or "no", if not set defaults to "yes"
#
FW_AUTOPROTECT_SERVICES="yes"

## Type: string
#
# 9.)
# Which services ON THE FIREWALL should be accessible
from either the internet
# (or other untrusted networks), the dmz or internal
(trusted networks)?
# (see no.13 & 14 if you want to route traffic through
the firewall) XXX
#
# Enter all ports or known portnames below, seperated
by a space.
# TCP services (e.g. SMTP, WWW) must be set in
FW_SERVICES_*_TCP, and
# UDP services (e.g. syslog) must be set in
FW_SERVICES_*_UDP.
# e.g. if a webserver on the firewall should be
accessible from the internet:
# FW_SERVICES_EXT_TCP="www"
# e.g. if the firewall should receive syslog messages
from the dmz:
# FW_SERVICES_DMZ_UDP="syslog"
# For IP protocols (like GRE for PPTP, or OSPF for
routing) you need to set
# FW_SERVICES_*_IP with the protocol name or number
(see /etc/protocols)
#
# Choice: leave empty or any number of ports, known
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
portnames (from
# /etc/services) and port ranges seperated by a space.
Port ranges are
# written like this: allow port 1 to 10 -> "1:10"
# e.g. "", "smtp", "123 514", "3200:3299", "ftp 22
telnet 512:514"
# For FW_SERVICES_*_IP enter the protocol name (like
"igmp") or number ("2")
#
# Common: smtp domain
FW_SERVICES_EXT_TCP="imap imaps pop3 pop3s rsync smtp
ssh"

## Type: string
# Common: domain
FW_SERVICES_EXT_UDP=""
# Common: domain

## Type: string
# For VPN/Routing which END at the firewall!!
FW_SERVICES_EXT_IP=""

## Type: string
#
# Common: smtp domain
FW_SERVICES_DMZ_TCP=""

## Type: string
# Common: domain
FW_SERVICES_DMZ_UDP=""

## Type: string
# For VPN/Routing which END at the firewall!!
FW_SERVICES_DMZ_IP=""

## Type: string
#
# Common: ssh smtp domain
FW_SERVICES_INT_TCP=""

## Type: string
# Common: domain syslog
FW_SERVICES_INT_UDP=""

# For VPN/Routing which END at the firewall!!
FW_SERVICES_INT_IP=""

## Type: string
# 9a.)
# External services in QUICKMODE.
# This is only used for QUICKMODE (see 1.)!
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
# (The settings here are similar to section 9.)
# Which services ON THE FIREWALL should be accessible
from either the
# internet (or other untrusted networks), i.e. the
external interface(s)
# $FW_DEV_EXT
#
# Enter all ports or known portnames below, seperated
by a space.
# TCP services (e.g. SMTP, WWW) must be set in
FW_SERVICES_QUICK_TCP, and
# UDP services (e.g. syslog) must be set in
FW_SERVICES_QUICK_UDP.
# e.g. if a secure shell daemon on the firewall should
be accessible from
# the internet:
# FW_SERVICES_QUICK_TCP="ssh"
# e.g. if the firewall should receive isakmp (IPsec)
internet:
# FW_SERVICES_QUICK_UDP="isakmp"
# For IP protocols (like IPsec) you need to set
# FW_SERVICES_QUICK_IP="50"
#
# Choice: leave empty or any number of ports, known
portnames (from
# /etc/services) and port ranges seperated by a space.
Port ranges are
# written like this: allow port 1 to 10 -> "1:10"
# e.g. "", "smtp", "123 514", "3200:3299", "ftp 22
telnet 512:514"
# For FW_SERVICES_*_IP enter the protocol name (like
"igmp") or number ("2")
#
# QUICKMODE: TCP services open to external networks
(InterNet)
# (Common: ssh smtp)
FW_SERVICES_QUICK_TCP=""

## Type: string
# QUICKMODE: UDP services open to external networks
(InterNet)
# (Common: isakmp)
FW_SERVICES_QUICK_UDP=""

## Type: string
# QUICKMODE: IP protocols unconditionally open to
external networks (InterNet)
# (For VPN firewall that is VPN gateway: 50)
FW_SERVICES_QUICK_IP=""
```

Fedora: RE: can ping but not browse

```
## Type: string
#
# 10.)
# Which services should be accessible from trusted
hosts/nets?
#
# Define trusted hosts/networks (doesnt matter if they
are internal or
# external) and the TCP and/or UDP services they are
allowed to use.
# Please note that a trusted host/net is *not* allowed
to ping the firewall
# until you set it to allow also icmp!
#
# Choice: leave FW_TRUSTED_NETS empty or any number of
computers and/or
# networks, seperated by a space. e.g. "172.20.1.1
172.20.0.0/16"
# Optional, enter a protocol after a comma, e.g.
"1.1.1.1,icmp"
# Optional, enter a port after a protocol, e.g.
"2.2.2.2,tcp,22"
#
FW_TRUSTED_NETS=""
```

```
## Type: string
#
# 11.)
# How is access allowed to high (unpriviledged [above
1023]) ports?
#
# You may either allow everyone from anyport access to
your highports ("yes"),
# disallow anyone ("no"), anyone who comes from a
defined port (portnumber or
# known portname) [note that this is easy to
circumvent!], or just your
# defined nameservers ("DNS").
# Note that you can't use rpc requests (e.g. rpcinfo,
showmount) as root
# from a firewall using this script (well, you can if
you include range
# 600:1023 in FW_SERVICES_EXT_UDP ...).
# Please note that with v2.1 "yes" is not mandatory
for active FTP from
# the firewall anymore.
#
# Choice: "yes", "no", "DNS", portnumber or known
portname,
# if not set defaults to "no"
#
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
# Common: "ftp-data", better is "yes" to be sure that
everything else works :-(
FW_ALLOW_INCOMING_HIGHPORTS_TCP="no"

## Type: string
# Common: "DNS" or "domain ntp", better is "yes" to be
sure ...
FW_ALLOW_INCOMING_HIGHPORTS_UDP="DNS"

## Type: yesno
## Default: yes
#
# 12.)
# Are you running some of the services below?
# They need special attention – otherwise they won't
work!
#
# Set services you are running to "yes", all others to
"no",
# if not set defaults to "no"
# If you want to offer the below services to your DMZ
as well,
# (and not just internally), set the switches below to
"dmz",
# if you even want to offer to the world as well, set
to "ext"
# instead of "yes" (NOT RECOMMENDED FOR SECURITY
REASONS!)
#
FW_SERVICE_AUTODETECT="yes"
# Autodetect the services below when starting

## Type: yesno
## Default: no
# If you are running bind/named set to yes. Remember
that you have to open
# port 53 (or "domain") as udp/tcp to allow incoming
queries.
# Also FW_ALLOW_INCOMING_HIGHPORTS_UDP needs to be
"yes"
FW_SERVICE_DNS="no"

## Type: yesno
## Default: no
# if you use dhclient to get an ip address you have to
set this to "yes" !
FW_SERVICE_DHCLIENT="no"

## Type: yesno
## Default: no
# set to "yes" if this server is a DHCP server
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
FW_SERVICE_DHCPD="no"
```

```
## Type: yesno
```

```
## Default: no
```

```
# set to "yes" if this server is running squid. You  
still have to open the
```

```
# tcp port 3128 to allow remote access to the squid  
proxy service.
```

```
FW_SERVICE_SQUID="no"
```

```
## Type: yesno
```

```
## Default: no
```

```
# set to "yes" if this server is running a samba  
server. You still have to
```

```
# open the tcp port 139 to allow remote access to  
SAMBA.
```

```
FW_SERVICE_SAMBA="no"
```

```
## Type: string
```

```
#
```

```
# 13.)
```

```
# Which services accessed from the internet should be  
allowed to the
```

```
# dmz (or internal network – if it is not  
masqueraded)?
```

```
# REQUIRES: FW_ROUTE
```

```
#
```

```
# With this option you may allow access to e.g. your  
mailserver. The
```

```
# machines must have valid, non-private, IP addresses  
which were assigned to
```

```
# you by your ISP. This opens a direct link to your  
network, so only use
```

```
# this option for access to your dmz!!!!
```

```
#
```

```
# Choice: leave empty (good choice!) or use the  
following explained syntax
```

```
# of forwarding rules, seperated each by a space.
```

```
# A forwarding rule consists of 1) source IP/net and  
2) destination IP
```

```
# seperated by a comma. e.g. "1.1.1.1,2.2.2.2  
3.3.3.3/16,4.4.4.4/24"
```

```
# Optional is a protocol, seperated by a comma, e.g.  
"5.5.5.5,6.6.6.6,igmp"
```

```
# Optional is a port after the protocol with a comma,  
e.g. "0/0,0/0,udp,514"
```

```
#
```

```
FW_FORWARD=""
```

```
# Beware to use this!
```

Fedora: RE: can ping but not browse

```
## Type: string
#
# 14.)
# Which services accessed from the internet should be
allowed to masqueraded
# servers (on the internal network or dmz)?
# REQUIRES: FW_ROUTE
#
# With this option you may allow access to e.g. your
mailserver. The
# machines must be in a masqueraded segment and may
not have public IP addresses!
# Hint: if FW_DEV_MASQ is set to the external
interface you have to set
# FW_FORWARD from internal to DMZ for the service as
well to allow access
# from internal!
#
# Please note that this should *not* be used for
security reasons! You are
# opening a hole to your precious internal network. If
e.g. the webserver there
# is compromised – your full internal network is
compromised!!
#
# Choice: leave empty (good choice!) or use the
following explained syntax
# of forward masquerade rules, seperated each by a
space.
# A forward masquerade rule consists of 1) source
IP/net, 2) the IP to which
# the requests will be forwarded to (in the dmz/intern
net), 3) a protocol
# (tcp/udp only!) and 4) destination port, seperated
by a comma (","), e.g.
# "4.0.0.0/8,1.1.1.1,tcp,80"
#
# Optional is a port after the destination port, to
redirect the request to
# a different destination port on the destination IP,
e.g.
# "4.0.0.0/8,1.1.1.1,tcp,80,81"
#
# Optional is an target IP address on which should the
masquerading be decided.
# You have to set the optional port option to use
this.
#
# Example:
# 200.200.200.0/24,10.0.0.10,tcp,80,81,202.202.202.202
# The class C network 200.200.200.0/24 trying to
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
access 202.202.202.202 port
# 80 will be forwarded to the internal server
10.0.0.10 on port 81.
# Example:
# 200.200.200.0/24,10.0.0.10,tcp,80
# The class C network 200.200.200.0/24 trying to
access anything which goes
# through this firewall ill be forwarded to the
internal server 10.0.0.10 on
# port 80
#
FW_FORWARD_MASQ=""

# Beware to use this!

## Type: string
#
# 15.)
# Which accesses to services should be redirected to a
localport on the
# firewall machine?
#
# This can be used to force all internal users to surf
via your squid proxy,
# or transparently redirect incoming webtraffic to a
secure webserver.
#
# Choice: leave empty or use the following explained
syntax of redirecting
# rules, seperated by a space.
# A redirecting rule consists of 1) source IP/net, 2)
destination IP/net,
# 3) protocol (tcp or udp) 3) original destination
port and 4) local port to
# redirect the traffic to, seperated by a colon. e.g.:
# "10.0.0.0/8,0/0,tcp,80,3128
0/0,172.20.1.1,tcp,80,8080"
# Please note that as 2) destination, you may add '!'
in front of the IP/net
# to specify everything EXCEPT this IP/net.
#
FW_REDIRECT=""

## Type: yesno
## Default: yes
#
# 16.)
# Which logging level should be enforced?
# You can define to log packets which were accepted or
denied.
# You can also the set log level, the critical stuff
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
or everything.
# Note that logging *_ALL is only for debugging
purpose ...
#
# Choice: "yes" or "no", if not set FW_LOG_*_CRIT
defaults to "yes", and
# FW_LOG_*_ALL defaults to "no"
#
FW_LOG_DROP_CRIT="yes"

## Type: yesno
## Default: no
#
FW_LOG_DROP_ALL="no"

## Type: yesno
## Default: yes
#
FW_LOG_ACCEPT_CRIT="yes"

## Type: yesno
## Default: no
#
FW_LOG_ACCEPT_ALL="no"

## Type: string
#
# only change/activate this if you know what you are
doing!
FW_LOG="--log-level warning --log-tcp-options
--log-ip-option --log-prefix SuSE-FW"

## Type: yesno
## Default: yes
#
# 17.)
# Do you want to enable additional kernel TCP/IP
security features?
# If set to yes, some obscure kernel options are set.
# (icmp_ignore_bogus_error_responses,
icmp_echoreply_rate,
# icmp_destunreach_rate, icmp_paramprob_rate,
icmp_timeexceed_rate,
# ip_local_port_range, log_martians, mc_forwarding,
mc_forwarding,
# rp_filter, routing flush)
# Tip: Set this to "no" until you have verified that
you have got a
# configuration which works for you. Then set this to
"yes" and keep it
# if everything still works. (It should!) ;-)
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
#
# Choice: "yes" or "no", if not set defaults to "yes"
#
FW_KERNEL_SECURITY="yes"

## Type: yesno
## Default: no
#
# 18.)
# Keep the routing set on, if the firewall rules are
unloaded?
# REQUIRES: FW_ROUTE
#
# If you are using diald, or automatic dialing via
ISDN, if packets need
# to be sent to the internet, you need to turn this
on. The script will then
# not turn off routing and masquerading when stopped.
# You *might* also need this if you have got a DMZ.
# Please note that this is *insecure*! If you unload
the rules, but are still
# connected, you might your internal network open to
attacks!
# The better solution is to remove
"/sbin/SuSEfirewall2 stop" or
# "/sbin/init.d/firewall stop" from the ip-down
script!
#
#
# Choices "yes" or "no", if not set defaults to "no"
#
FW_STOP_KEEP_ROUTING_STATE="no"

## Type: yesno
## Default: yes
#
# 19.)
# Allow (or don't) ICMP echo pings on either the
firewall or the dmz from
# the internet? The internet option is for allowing
the DMZ and the internal
# network to ping the internet.
# REQUIRES: FW_ROUTE for FW_ALLOW_PING_DMZ and
FW_ALLOW_PING_EXT
#
# Choice: "yes" or "no", defaults to "no" if not set
#
FW_ALLOW_PING_FW="yes"

## Type: yesno
## Default: no
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
#
FW_ALLOW_PING_DMZ="no"

## Type: yesno
## Default: no
#
FW_ALLOW_PING_EXT="no"

##
# END of /etc/sysconfig/SuSEfirewall2
##

#
#
# -----#
#
#
# EXPERT OPTIONS – all others please don't change
these! #
#
# -----#
#
#

## Type: yesno
## Default: yes
#
# 20.)
# Allow (or don't) ICMP time-to-live-exceeded to be
send from your firewall.
# This is used for traceroutes to your firewall (or
traceroute like tools).
#
# Please note that the unix traceroute only works if
you say "yes" to
# FW_ALLOW_INCOMING_HIGHPORTS_UDP, and windows
traceroutes only if you say
# additionally "yes" to FW_ALLOW_PING_FW
#
# Choice: "yes" or "no", if not set defaults to "no"
#
FW_ALLOW_FW_TRACEROUTE="no"

## Type: yesno
## Default: yes
#
# 21.)
# Allow ICMP sourcequench from your ISP?
#
# If set to yes, the firewall will notice when
```

Fedora: RE: can ping but not browse

```
connection is choking, however
# this opens yourself to a denial of service attack.
Choose your poison.
#
# Choice: "yes" or "no", if not set defaults to "yes"
#
FW_ALLOW_FW_SOURCEQUENCH="yes"

## Type: yesno
## Default: no
#
# 22.)
# Allow/Ignore IP Broadcasts?
#
# If set to yes, the firewall will not filter
broadcasts by default.
# This is needed e.g. for Netbios/Samba, RIP, OSPF
where the broadcast
# option is used.
# If you do not want to allow them however ignore the
annoying log entries,
# set FW_IGNORE_FW_BROADCAST to yes.
#
# Choice: "yes" or "no", if not set defaults to "no"
#
FW_ALLOW_FW_BROADCAST="no"

## Type: yesno
## Default: yes
#
FW_IGNORE_FW_BROADCAST="yes"

## Type: yesno
## Default: no
#
# 23.)
# Allow same class routing per default?
# REQUIRES: FW_ROUTE
#
# Do you want to allow routing between interfaces of
the same class
# (e.g. between all internet interfaces, or all
internal network interfaces)
# be default (so without the need setting up
FW_FORWARD definitions)?
#
# Choice: "yes" or "no", if not set defaults to "no"
#
FW_ALLOW_CLASS_ROUTING="no"
```

Fedora: RE: can ping but not browse

```
## Type: string
#
# 25.)
# Do you want to load customary rules from a file?
#
# This is really an expert option. NO HELP WILL BE
GIVEN FOR THIS!
# READ THE EXAMPLE CUSTOMARY FILE AT
/etc/sysconfig/scripts/SuSEfirewall2-custom
#
#FW_CUSTOMRULES="/etc/sysconfig/scripts/SuSEfirewall2-custom"
FW_CUSTOMRULES=""
```

```
## Type: yesno
## Default: no
#
# 26.)
# Do you want to REJECT packets instead of DROPing?
#
# DROPing (which is the default) will make portscans
and attacks much
# slower, as no replies to the packets will be sent.
REJECTing means, that
# for every illegal packet, a connection reject packet
is sent to the
# sender.
#
# Choice: "yes" or "no", if not set defaults to "no"
#
FW_REJECT="no"
```

```
## Type: string
#
# 27.)
# Tuning your upstream a little bit via HTB
(Hierarchical Token Bucket)
# for more information about HTB see
http://www.lartc.org
#
# If your download collapses while you have a parallel
upload,
# this parameter might be an option for you. It
manages your
# upload stream and reserves bandwidth for special
packets like
# TCP ACK packets or interactive SSH.
# It's a list of devices and maximum bandwidth in
kbit.
# For example, the german TDSL account, provides
128kbit/s upstream
# and 768kbit/s downstream. We can only tune the
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

```
upstream.
#
# Example:
# If you want to tune a 128kbit/s upstream DSL device
like german TDSL set
# the following values:
# FW_HTB_TUNE_DEV="ppp0,125"
# where ppp0 is your pppoe device and 125 stands for
125kbit/s upstream
#
# you might wonder why 125kbit/s and not 128kbit/s.
Well practically you'll
# get a better performance if you keep the value a few
percent under your
# real maximum upload bandwidth, to prevent the DSL
modem from queuing traffic in
# it's own buffers because queing is done by us now.
# So for a 256kbit upstream
# FW_HTB_TUNE_DEV="ppp0,250"
# might be a better value than "ppp0,256". There is no
perfect value for a
# special kind of modem. The perfect value depends on
what kind of traffic you
# have on your line but 5% under your maximum upstream
might be a good start.
# Everthing else is special fine tuning.
# If you want to know more about the technical
background,
#
http://tldp.org/HOWTO/ADSL-Bandwidth-Management-HOWTO/
# is a good start
#
FW_HTB_TUNE_DEV=""
```

```
//-----SuSEfirewall2-----END-----
```

--- bruce <bedouglas@earthlink.net> wrote:

```
> ravi...
>
> i know it's basic, but check the firewall/security
> for port 80/8080
> whichever you;re using for your http connection. do
> this on both machines...
>
> let us know the results...
>
>
>
> -----Original Message-----
> From: fedora-list-bounces@redhat.com
```

RE: can ping but not browse

Fedora: RE: can ping but not browse

> [mailto:fedora-list-bounces@redhat.com]On Behalf Of
> Ravi Prasad
> Sent: Sunday, March 27, 2005 5:59 PM
> To: fedora-list@redhat.com
> Subject: can ping but not browse
>
>
>
> Hi all..
> I am using FedoreCore2 on my DELL PC in a
> LAN(IP:
> 192.168.100.10).A SuSe9 machine(IP: 192.168.100.1)
> on
> the same LAN is connected to internet via DSL and it
> is configured with IP masquerading. I have made this
> Suse machine as default gateway. My machine is dual
> boot with WinXP and FedoraCore2. Everything works
> fine
> in WinXP. But in Fedora I am only able to ping the
> outside addresses but not able to browse them. Some
> points which can help to figure out the problem:
>
> 1. Ping works fine. I can ping to every internal LAN
> machine and outside adresses like google.com and
> kernel.org.
> 2. Every other machine on LAN can ping my computer.
> 3. In browser when I type a domain name it finishes
> DNS lookup and starts HTTP transaction but then
> infinetly waits saying "Waiting for reply".
> 4. I installed and started the httpd daemon on my
> computer and tried to browse my machine by another
> machine on LAN. Then also that machine waits
> infinitely saying "Waiting for reply".
> 5. I started httpd on another machine on LAN and
> tried
> to browse from my system but the same behavior,
> "waiting for reply".
> 6. I looked on net and the links were pointing to
> DNS
> problem. So i tried on the browser by directly
> giving
> the IP address(like 216.239.57.99 for google.com)
> and
> not the domain name. But still same behavior,
> "waiting
> for reply".
>
>
> I stopped my computers firewall and tried but still
> the same behavior.
>

RE: can ping but not browse

Fedora: RE: can ping but not browse

> *Can anyone help to figure out the problem.*
>
> *Regds..*
>
>
>
> _____
> *Do You Yahoo!?*
> *Tired of spam? Yahoo! Mail has the best spam*
> *protection around*
> <http://mail.yahoo.com>
>
> --
> *fedora-list mailing list*
> *fedora-list@redhat.com*
> *To unsubscribe:*
> <http://www.redhat.com/mailman/listinfo/fedora-list>
>
> --
> *fedora-list mailing list*
> *fedora-list@redhat.com*
> *To unsubscribe:*
> <http://www.redhat.com/mailman/listinfo/fedora-list>
>

Do You Yahoo!?
Tired of spam? Yahoo! Mail has the best spam protection around
<http://mail.yahoo.com>

--
fedora-list mailing list
fedora-list@redhat.com
To unsubscribe: <http://www.redhat.com/mailman/listinfo/fedora-list>