

Table Of Contents

Table Of Contents .....	1
A note about MIB .....	2

[Home](#) > [Faq](#) > [FreeBSD](#)

## FreeBSD Jail Allow Ping / traceroute Commands

Posted by [Vivek Gite](#) <[vivek@nixcraft.com](mailto:vivek@nixcraft.com)>

I'm not able to ping from FreeBSD prison (jail). I'm able to resolve the names or use ftp / http for ports but ping and traceroute access is disabled. How do I allow virtualized jail application / users to perform traceroute and ping commands?

By default FreeBSD does not allows prison users / apps to create raw sockets. This is a security feature. With raw sockets one can use perl / python or tools such as nc to create raw socket and launch attacks. However, this aspects of the jail environment may be modified from the host environment using sysctl command.

security.jail.allow\_raw\_sockets MIB entry determines whether or not prison root is allowed to create raw sockets. Setting this MIB to 1 allows utilities like ping and traceroute to operate inside the prison. Type the following command:

```
# sysctl security.jail.allow_raw_sockets=1
```

Now login to jail using jexec:

```
host # jexec 1 csh
jail# ping cyberciti.biz
```

Add following line to sysctl.conf:

```
# echo 'security.jail.allow_raw_sockets=1' >> /etc/sysctl.conf
```

## A note about MIB

This is **optional configuration**. Above MIB variable affect all jails on the system. In other words, all jails will be able to use ping and traceroute command. You can deny or allow access to certain jails using host firewall such as PF. Here is a sample PF firewall:

```
# interface
int_if="em0"
ext_if="em1"

# ICMP types
icmp_types = "{ echoreq, unreachable }"

# Allowed ips for traceroute
troute_outbound_ips = "{ 10.24.55.101, 10.24.55.103, 10.24.55.111 }"

# Allowed ips for ping
ping_outbound_ips = "{ 10.24.55.103, 10.24.55.111 }"

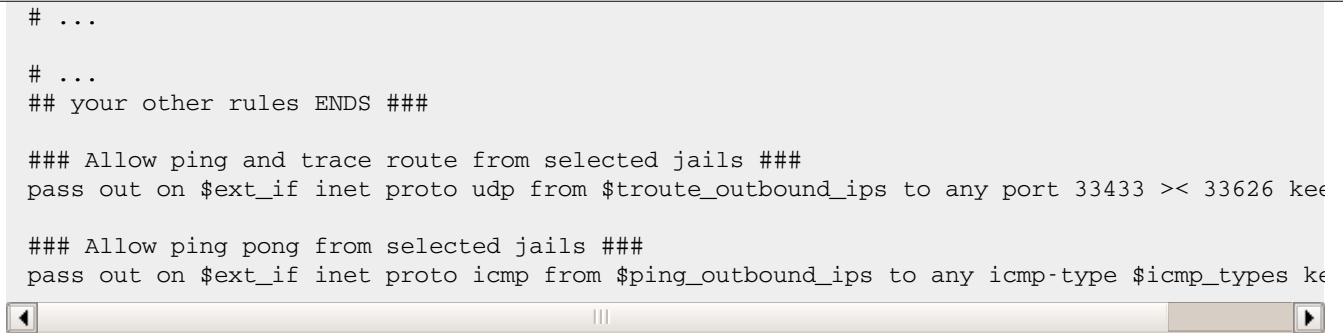
# Some defaults
set block-policy return
set loginterface $ext_if
scrub in all

# Drop ALL - drop incoming and everything else
block log all

# skip loopback and vpn interface
set skip on {lo0, $int_if}
block in quick from urpf-failed
antispoof log for $ext_if

## your other rules STARTS ###
## add your other pf rules to open port and other stuff
```

```
# ...  
  
# ...  
## your other rules ENDS ###  
  
### Allow ping and trace route from selected jails ###  
pass out on $ext_if inet proto udp from $troute_outbound_ips to any port 33433 >< 33626 keep  
  
### Allow ping pong from selected jails ###  
pass out on $ext_if inet proto icmp from $ping_outbound_ips to any icmp-type $icmp_types keep
```



4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/freebsd-jail-allow-ping-tracerouter-commands/>

URLs in this post:

[1] Image: <http://www.cyberciti.biz/faq/category/freebsd/>

---

Copyright © 2006-2010 [nixCraft](#). All rights reserved. This print / pdf version is for personal non-commercial use only. More details <http://www.cyberciti.biz/tips/copyright>.