
Subject: [PATCH 4/4] netns: prevent usage of flowi with not initialized fl_net in routing

Posted by [den](#) on Tue, 04 Dec 2007 09:54:35 GMT

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

Prevent usage of flowi with not initialized fl_net in routing. This is a temporary measure to simplify maintenance of the patchset.

Signed-off-by: Denis V. Lunev <den@openvz.org>

```
net/ipv4/route.c    | 1 +
net/ipv6/fib6_rules.c | 1 +
net/ipv6/ip6_fib.c  | 1 +
3 files changed, 3 insertions(+), 0 deletions(-)
```

diff --git a/net/ipv4/route.c b/net/ipv4/route.c

index 84a7f32..996fd9e 100644

--- a/net/ipv4/route.c

+++ b/net/ipv4/route.c

```
@@ -2444,6 +2444,7 @@ int ip_route_output_flow(struct rtable **rp, struct flowi *flp, struct sock
*sk,
{
    int err;
```

```
+ BUG_ON(flp->fl_net == NULL);
    if ((err = __ip_route_output_key(rp, flp)) != 0)
        return err;
```

diff --git a/net/ipv6/fib6_rules.c b/net/ipv6/fib6_rules.c

index 428c6b0..326ea69 100644

--- a/net/ipv6/fib6_rules.c

+++ b/net/ipv6/fib6_rules.c

```
@@ -38,6 +38,7 @@ struct dst_entry *fib6_rule_lookup(struct flowi *fl, int flags,
    .lookup_ptr = lookup,
};
```

```
+ BUG_ON(fl->fl_net == NULL);
    fib_rules_lookup(&fib6_rules_ops, fl, flags, &arg);
    if (arg.rule)
        fib_rule_put(arg.rule);
```

diff --git a/net/ipv6/ip6_fib.c b/net/ipv6/ip6_fib.c

index 31b60a0..706cb72 100644

--- a/net/ipv6/ip6_fib.c

+++ b/net/ipv6/ip6_fib.c

```
@@ -282,6 +282,7 @@ struct fib6_table *fib6_get_table(u32 id)
    struct dst_entry *fib6_rule_lookup(struct flowi *fl, int flags,
        pol_lookup_t lookup)
{
```

```
+ BUG_ON(fl->fl_net == NULL);
  return (struct dst_entry *) lookup(&fib6_main_tbl, fl, flags);
}
```

--

1.5.3.rc5

Subject: Re: [PATCH 4/4] netns: prevent usage of flowi with not initialized fl_net in routing

Posted by [Patrick McHardy](#) on Tue, 04 Dec 2007 14:38:38 GMT

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

Denis V. Lunev wrote:

> Prevent usage of flowi with not initialized fl_net in routing. This is
> a temporary measure to simplify maintenance of the patchset.

Please use WARN_ON, its not nice to crash peoples machines
in case you missed something.
