

---

Subject: [PATCH 17/16] net: Disable netfilter sockopts when not in the initial network namespace

Posted by [ebiederm](#) on Sat, 08 Sep 2007 21:47:12 GMT

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

---

Until we support multiple network namespaces with netfilter only allow netfilter configuration in the initial network namespace.

Signed-off-by: Eric W. Biederman <[ebiederm@xmission.com](mailto:ebiederm@xmission.com)>

---

Ooops I overlooked this one on my first path through when gathering up this patchset.

```
net/netfilter/nf_sockopt.c | 7 +++++++  
1 files changed, 7 insertions(+), 0 deletions(-)
```

```
diff --git a/net/netfilter/nf_sockopt.c b/net/netfilter/nf_sockopt.c  
index 8b8ece7..c12ea9b 100644  
--- a/net/netfilter/nf_sockopt.c  
+++ b/net/netfilter/nf_sockopt.c  
@@ -80,6 +80,9 @@ static int nf_sockopt(struct sock *sk, int pf, int val,  
 struct nf_sockopt_ops *ops;  
 int ret;  
  
+ if (sk->sk_net != &init_net)  
+ return -ENOPROTOOPT;  
+  
+ if (mutex_lock_interruptible(&nf_sockopt_mutex) != 0)  
 return -EINTR;  
  
@@ -138,6 +141,10 @@ static int compat_nf_sockopt(struct sock *sk, int pf, int val,  
 struct nf_sockopt_ops *ops;  
 int ret;  
  
+ if (sk->sk_net != &init_net)  
+ return -ENOPROTOOPT;  
+  
+ if (mutex_lock_interruptible(&nf_sockopt_mutex) != 0)  
 return -EINTR;  
  
--  
1.5.3.rc6.17.g1911
```

---

Containers mailing list  
[Containers@lists.linux-foundation.org](mailto:Containers@lists.linux-foundation.org)

