Subject: [PATCH 3/4] Cleanup the error path in sk_attach_filter
Posted by Pavel Emelianov on Wed, 17 Oct 2007 09:51:11 GMT
View Forum Message <> Reply to Message

The sk_filter_uncharge is called for error handling and
for releasing the former filter, but this will have to
be done in a bit different manner, so cleanup the error
path a bit.

Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

```
diff --git a/net/core/filter.c b/net/core/filter.c
index 2be1830..54dddc9 100644
--- a/net/core/filter.c
+++ b/net/core/filter.c
@@ -398,7 +398,7 @@ int sk_chk_filter(struct sock_filter *filter, int flen)
  */
 int sk_attach_filter(struct sock_fprog *fprog, struct sock *sk)
 {
- struct sk_filter *fp;
+ struct sk_filter *fp, *old_fp;
  unsigned int fsize = sizeof(struct sock_filter) * fprog->len;
  int err;

@@ -418,19 +418,18 @@ int sk_attach_filter(struct sock_fprog *fprog, struct sock *sk)
  fp->len = fprog->len;

  err = sk_chk_filter(fp->insns, fp->len);
- if (!err) {
-  struct sk_filter *old_fp;
-
-  rcu_read_lock_bh();
-  old_fp = rcu_dereference(sk->sk_filter);
-  rcu_assign_pointer(sk->sk_filter, fp);
-  rcu_read_unlock_bh();
-  fp = old_fp;
+ if (err) {
+  sk_filter_uncharge(sk, fp);
+  return err;
  }

- if (fp)
-  sk_filter_uncharge(sk, fp);
- return err;
+ rcu_read_lock_bh();
+ old_fp = rcu_dereference(sk->sk_filter);
```

```
+ rcu_assign_pointer(sk->sk_filter, fp);
+ rcu_read_unlock_bh();
+
+ sk_filter_uncharge(sk, old_fp);
+ return 0;
 }

 int sk_detach_filter(struct sock *sk)
--
1.5.3.4
```