Firewall Manager Test Cases

Semen Cirit

June 19, 2009

1. Try to open firewall manager from system settings.
2. Try to open firewall manager from Kmenu.
3. Try to stop firewall service from the start/stop button of firewall manager.
   Execute the following command:

   ```
   # service list
   ```

   Observe that iptables service gets off.
4. Try to start service from the start/stop button of firewall manager.
   Execute the following command:

   ```
   # service list
   ```

   Observe that iptables service gets on.
5. Push the configuration button and try these actions for options: Block incoming connections or Block outgoing connections.
   5.1. Adding port
   5.2. Removing port
   5.3. Taking up a port
   5.4. Taking down a port

   Note: Observe the outputs of this command for each situation.
   Execute the following command:

   ```
   # iptables --list-rules
   ```

6. Block incoming connections:
   6.1. After adding a port from firewall manager.
      6.1.1. Enable limited content serving Observe that the output of the above command contains these:

```
-A PARDUS-IN-MOD-SERVING -p tcp -m multiport --dports <addedPORT> \
    -j ACCEPT
-A PARDUS-IN-MOD-SERVING -p tcp -m multiport --dports 0:1024 \
    -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REJECT --reject-with \
    icmp-port-unreachable
-A PARDUS-IN-MOD-SERVING -p udp -m multiport --dports 0:1024 \
    -j REJECT --reject-with icmp-port-unreachable
```

6.1.2. Disable block incoming connections
Observe that the above lines are removed from the output of the below command.

6.2. Without adding a port
Observe that the output of the above command contains these:

```
-A PARDUS-IN-MOD-SERVING -p tcp -m multiport --dports 0:1024 \
    -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REJECT --reject-with \
    icmp-port-unreachable
-A PARDUS-IN-MOD-SERVING -p udp -m multiport --dports 0:1024 \
    -j REJECT --reject-with icmp-port-unreachable
```

6.3. Internet sharing

6.3.1. Enable Internet sharing (If you have two internal ethernet card or an extra external ethernet card, you can test this part, if not skip the following step.

6.3.1.1. Select different values for gate to internet and gate to home network Observe that the above command output contains these:

```
-A PARDUS-FW-MOD-SHARING -i <input> -o <output> -m state \
    --state ESTABLISHED,RELATED -j ACCEPT
-A PARDUS-FW-MOD-SHARING -i <output> -o <input> -j ACCEPT
-t nat -A PARDUS-POST-MOD-SHARING -o <input> -j MASQUERADE
```

6.3.1.2. Give same values
Observe that the above lines are removed from the output of the below command.

6.4. Block outgoing connections

6.4.1. After adding a port from firewall manager.

6.4.1.1. Enable block outgoing connections
Observe that the port is added
There should be lines like below at output of the command:

```
-A PARDUS-FW-MOD-BLOCK -p tcp -m multiport --dports <addedPORT> \
    -j DROP
-A PARDUS-OUT-MOD-BLOCK -p tcp -m multiport --dports <addedPORT> \
    -j DROP
```

6.4.1.2. Disable block outgoing connections
Observe that the above lines are removed from the output of the below command.

7. Pratical part of tests

First activate firewall on both two computers.

If the service openssh was disabled, start it from service manager.

7.1. Block incoming connections:

7.1.1. Disable block incoming connections
(If you have a static ip or your two machine is in the same network, you can test this case, if not skip it)
Try to make a remote connection from an other computer to your computer.
Execute the following command:

```
# ssh <your_computer_name>@<static_ip>
```

Observe that the connection is being accepted.

7.1.2. Try to add a well known port and enable block incoming connections. Open the related service of this port from service-manager.

7.1.2.1. Try to make a remote connection from an other computer to your computer.

```
# ssh <your_computer_name>@<static_ip>
```

Observe that the connection refused.

7.1.2.2. Try to make a remote connection using the added port from an other computer to your computer.

```
# ssh -p <port> <your_computer_name>@<static_ip>
```

Observe that the connection is accepted.

7.2. For internet sharing:
(If you have two internal ethernet card or an extra external ethernet card and an extra computer, you can test this part, if not skip it.)

7.2.1. Plug an extra external or internal ethernet card to your computer. And plug an ethernet cable between your computer and the other. (And if the other computer have an internet acces please stop it.)

7.2.2. Enable internet sharing from firewall-manager.

7.2.3. Choose the first ethernet card for gate to internet, and the second for gate to home network.
Now try to connect to connect internet over your computer and observe it.

7.3. Block outgoing connections:
(If you have a static ip or your two machine is in the same network, you can test this case, if not skip it)

7.3.1. Disable access restriction

7.3.1.1. Try to make a remote connection with using a well known port from your computer to the other remote computer. If the remote computer has a static ip you can use it for remote connection.
Execute the following command:

```
# ssh -p <port> <remote_computer_name>@<static_ip>
```

Observe that the connection accepted.

7.3.1.2. Try to add a well known port and enable block outgoing connections.
Try to make a remote connection using added port from your computer to the other computer.

```
# ssh -p <port> <remote_computer_name>@<static_ip>
```

Observe that the connection refused.