strongSwan - Bug #421

updown script fails to install firewall rules when protected protocol is ICMP[v6]

26.09.2013 13:58 - drumfire _

Status:	Closed	**Start date:**	26.09.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:			
Target version:	5.1.1		
Affected version:	5.1.0	**Resolution:**	Fixed

Description

It looks like ip6tables is not called correctly. From syslog:

```
updown: ip6tables v1.4.20: unknown option "--dport"
updown: Try `ip6tables -h' or 'ip6tables --help' for more information.
```

In my exec log (thanks to grsecurity I could capture where this happens):

```
ip6tables -D FORWARD -o eth0 -p 58 -s ADDRESS::/56 -d ADDRESS/128 --dport 128 -m policy --pol ipsec --pro
```

Protocol 58 is ICMPv6. This does indeed not support --dport.

I am not sure in which category this fits.

Associated revisions

Revision 3ea7165a - 17.10.2013 16:59 - Tobias Brunner

Merge branch 'icmp'

Improves handling of ICMP[v6] traffic selectors that specify message type and code.

Fixes #421.

History

#1 - 15.10.2013 20:58 - drumfire _

Greetings,

My tunnels are working suboptimal and I wonder if this has anything to do with it. I don't really understand how the script works though, is this not an important issue?

Thank you

#2 - 15.10.2013 22:21 - Tobias Brunner

- Status changed from New to Assigned

- Assignee set to Tobias Brunner

- Target version set to 5.1.1

A fix for this issue is on its way (check the *icmp* branch of the Git repository).

> My tunnels are working suboptimal and I wonder if this has anything to do with it.

Whether this issue has anything to do with that probably depends on your strongSwan and firewall configuration.

> I don't really understand how the script works though, is this not an important issue?

The script is called after a CHILD_SA is established, if *leftfirewall* is set to *yes*. That option is intended in situations where the default policies of the *INPUT/OUTPUT/FORWARD* chains are set to *DROP* (or traffic is otherwise blocked). The script then installs the required firewall rules that allow traffic from/to the established tunnels.

#3 - 17.10.2013 17:05 - Tobias Brunner

- Status changed from Assigned to Closed

- Resolution set to Fixed

I merged the branch into master.

#4 - 17.10.2013 21:04 - drumfire _

Hello Tobias,

> The script is called after a CHILD_SA is established, if leftfirewall is set to yes. That option is intended in situations where the default policies of the INPUT/OUTPUT/FORWARD chains are set to DROP (or traffic is otherwise blocked). The script then installs the required firewall rules that allow traffic from/to the established tunnels.

I do have a DROP policy in those chains so yes, chances are that there are some forwarding issues. We'll see whether this is the case.

> Resolution set to Fixed

Very nice, thank you.

#5 - 01.11.2013 13:51 - Tobias Brunner

- Subject changed from Bug in IPv6 firewall script to updown script fails to install firewall rules when protected protocol is ICMP[v6]

#6 - 23.04.2014 03:02 - drumfire _

Not sure if I should create a new bug report or not, please let me know if this is preferred over reopening this one.

While I noticed that the fix works for ICMP, I discovered that it does not yet work properly when --proto esp:

```
ip6tables -I INPUT 1 -i eth0 -p 0 -s <IP-A>/128 --sport 514 -d <IP-B>/60 -m policy --pol ipsec --proto esp --r
eqid 1 --dir in -j ACCEPT
ip6tables v1.4.21: unknown option "--sport"
Try `ip6tables -h' or 'ip6tables --help' for more information.
```

As an aside: I also noticed that the iptables line contains -p 0 first, and --proto esp later. It's no cause for concern but I wanted to point it out just in case.

Cheers

#7 - 23.04.2014 09:15 - Tobias Brunner

Please open a new ticket. It looks like a different issue and it makes it easier to track.