strongSwan - Feature #2111

Use iptables-save in test scenarios

09.09.2016 16:30 - Noel Kuntze

Status:	Closed	**Start date:**	09.09.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	testing		
Target version:	5.5.1		
Resolution:	Fixed		

Description

The output of iptables -L that is shown in the test scenarios is not helpful when figuring out how the test scenarios work, as iptables -L only shows the filter table
and the output of it is not deserializable into an iptables rule set. The output iptables-save has those two nice properties.

iptables-save by default shows all tables and can be used to load the rules into the kernel by using the iptables-restore tool.
Those two tools are included in the xtables-multi binary, which all distributions ship. It is implemented as a symlink.

Associated revisions

Revision fa36699b - 12.09.2016 16:15 - Tobias Brunner

testing: List `nat` and `mangle` tables in addition to the `filter` table

This is useful in scenarios that e.g. use NAT and/or marks.

References #2111.

Revision ac67aeb1 - 12.09.2016 16:15 - Tobias Brunner

testing: Add output of iptables-save

This might be helpful to get the complete picture of the installed
rules. `-c` is currently not used as the counters that are added in
front of every rule make the output quite hard to read and the counters
are already provided in the accompanying `iptables -v -L` output.

Fixes #2111.

History

#1 - 09.09.2016 17:14 - Tobias Brunner

- Tracker changed from Issue to Feature

- Category set to testing

- Status changed from New to Feedback

Yes, this is a known issue. Some tests explicitly list rules from other tables in console.log but not all do so.

The problem with iptables-save -c is that its output is just not as readable as that of iptables -v -L. If a scenario fails a quick glance at the stats in the current output often gives you some hints where to look further.

So perhaps we could streamline the output of the other tables, for instance, just add the nat and mangle tables after the filter table in the current file:

ikev2/nat-rw-mark/sun.iptables with nat and mangle tablesikev2/nat-rw-mark/sun.iptables with nat and mangle tables

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2  1616 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:500
    4  3896 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:4500
  120 26096 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
    4  2150 ACCEPT     tcp  --  eth0   *       192.168.0.150        0.0.0.0/0           tcp spt:80

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    84 ACCEPT     all  --  eth0   *       10.1.0.0/25          10.2.0.0/16         policy match dir in p
```

```
ol ipsec reqid 2 proto 50
    1    84 ACCEPT     all  --  *      eth0    10.2.0.0/16          10.1.0.0/25          policy match dir out
pol ipsec reqid 2 proto 50
    1    84 ACCEPT     all  --  eth0   *       10.1.0.0/25          10.2.0.0/16          policy match dir in p
ol ipsec reqid 1 proto 50
    1    84 ACCEPT     all  --  *      eth0    10.2.0.0/16          10.1.0.0/25          policy match dir out
pol ipsec reqid 1 proto 50

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2  1274 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0            udp spt:500
    4  3624 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0            udp spt:4500
  155 48548 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
    6   391 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            192.168.0.150        tcp dpt:80

=== nat table ===
Chain PREROUTING (policy ACCEPT 6 packets, 5352 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 4 packets, 5184 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1 packets, 60 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 1 packets, 60 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    84 SNAT       all  --  *      eth1    0.0.0.0/0            0.0.0.0/0            mark match 0xa to:10.
3.0.10
    1    84 SNAT       all  --  *      eth1    0.0.0.0/0            0.0.0.0/0            mark match 0x14 to:10
.3.0.20

=== mangle table ===
Chain PREROUTING (policy ACCEPT 95 packets, 18524 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    84 MARK       all  --  *      *       0.0.0.0/0            10.3.0.10            MARK set 0xa
    1    84 MARK       all  --  *      *       0.0.0.0/0            10.3.0.20            MARK set 0x14
    1   164 MARK       udp  --  *      *       192.168.0.1          0.0.0.0/0            udp spt:4510 MARK set
 0xa
    1   164 MARK       udp  --  *      *       192.168.0.1          0.0.0.0/0            udp spt:4520 MARK set
 0x14

Chain INPUT (policy ACCEPT 91 packets, 18188 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 4 packets, 336 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 121 packets, 48624 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 125 packets, 48960 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

ikev2/net2net-cert/moon.iptables where these tables are emptyikev2/net2net-cert/moon.iptables where these tables are empty

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1   156 ACCEPT     esp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     ah   --  eth0   *       0.0.0.0/0            0.0.0.0/0
    2  2177 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0            udp spt:500 dpt:500
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0            udp spt:4500 dpt:4500
   93 19020 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    4  2150 ACCEPT     tcp  --  eth0   *       192.168.0.150        0.0.0.0/0            tcp spt:80

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    84 ACCEPT     all  --  eth0   *       10.2.0.0/16          10.1.0.0/16          policy match dir in p
ol ipsec reqid 1 proto 50
    1    84 ACCEPT     all  --  *      eth0    10.1.0.0/16          10.2.0.0/16          policy match dir out
pol ipsec reqid 1 proto 50

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
    1   156 ACCEPT     esp  --  *      eth0    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     ah   --  *      eth0    0.0.0.0/0            0.0.0.0/0
    2  2516 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           udp spt:500 dpt:500
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           udp spt:4500 dpt:4500
  115 35012 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
    6   391 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            192.168.0.150       tcp dpt:80

=== nat table ===
Chain PREROUTING (policy ACCEPT 8 packets, 1104 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 7 packets, 1020 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4 packets, 1124 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 5 packets, 1208 bytes)
 pkts bytes target     prot opt in     out     source               destination

=== mangle table ===
Chain PREROUTING (policy ACCEPT 164 packets, 36458 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 162 packets, 36290 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 2 packets, 168 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 183 packets, 52406 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 185 packets, 52574 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Or we could add the output of iptables-save -c in addition to the current output, or that above (optionally as separate file, but that's more work):

ikev2/nat-rw-mark/sun.iptables with iptables-save -cikev2/nat-rw-mark/sun.iptables with iptables-save -c

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2  1616 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:500
    4  3896 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:4500
  121 26092 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
    4  2150 ACCEPT     tcp  --  eth0   *       192.168.0.150        0.0.0.0/0           tcp spt:80

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    84 ACCEPT     all  --  eth0   *       10.1.0.0/25          10.2.0.0/16         policy match dir in p
ol ipsec reqid 2 proto 50
    1    84 ACCEPT     all  --  *      eth0    10.2.0.0/16          10.1.0.0/25         policy match dir out
pol ipsec reqid 2 proto 50
    1    84 ACCEPT     all  --  eth0   *       10.1.0.0/25          10.2.0.0/16         policy match dir in p
ol ipsec reqid 1 proto 50
    1    84 ACCEPT     all  --  *      eth0    10.2.0.0/16          10.1.0.0/25         policy match dir out
pol ipsec reqid 1 proto 50

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2  1274 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           udp spt:500
    4  3624 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           udp spt:4500
  154 48496 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
    6   391 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            192.168.0.150       tcp dpt:80

# Generated by iptables-save v1.4.21 on Fri Sep  9 15:00:49 2016
*raw
:PREROUTING ACCEPT [2146:474788]
:OUTPUT ACCEPT [1062:254668]
COMMIT
# Completed on Fri Sep  9 15:00:49 2016
# Generated by iptables-save v1.4.21 on Fri Sep  9 15:00:49 2016
*nat
:PREROUTING ACCEPT [6:5352]
```

```
:INPUT ACCEPT [4:5184]
:OUTPUT ACCEPT [1:60]
:POSTROUTING ACCEPT [1:60]
[1:84] -A POSTROUTING -o eth1 -m mark --mark 0xa -j SNAT --to-source 10.3.0.10
[1:84] -A POSTROUTING -o eth1 -m mark --mark 0x14 -j SNAT --to-source 10.3.0.20
COMMIT
# Completed on Fri Sep  9 15:00:49 2016
# Generated by iptables-save v1.4.21 on Fri Sep  9 15:00:49 2016
*mangle
:PREROUTING ACCEPT [95:18468]
:INPUT ACCEPT [91:18132]
:FORWARD ACCEPT [4:336]
:OUTPUT ACCEPT [119:47624]
:POSTROUTING ACCEPT [123:47960]
[1:84] -A PREROUTING -d 10.3.0.10/32 -j MARK --set-xmark 0xa/0xffffffff
[1:84] -A PREROUTING -d 10.3.0.20/32 -j MARK --set-xmark 0x14/0xffffffff
[1:164] -A PREROUTING -s 192.168.0.1/32 -p udp -m udp --sport 4510 -j MARK --set-xmark 0xa/0xffffffff
[1:164] -A PREROUTING -s 192.168.0.1/32 -p udp -m udp --sport 4520 -j MARK --set-xmark 0x14/0xffffffff
COMMIT
# Completed on Fri Sep  9 15:00:49 2016
# Generated by iptables-save v1.4.21 on Fri Sep  9 15:00:49 2016
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
[2:1616] -A INPUT -i eth0 -p udp -m udp --dport 500 -j ACCEPT
[4:3896] -A INPUT -i eth0 -p udp -m udp --dport 4500 -j ACCEPT
[122:26144] -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
[4:2150] -A INPUT -s 192.168.0.150/32 -i eth0 -p tcp -m tcp --sport 80 -j ACCEPT
[1:84] -A FORWARD -s 10.1.0.0/25 -d 10.2.0.0/16 -i eth0 -m policy --dir in --pol ipsec --reqid 2 --proto esp -
j ACCEPT
[1:84] -A FORWARD -s 10.2.0.0/16 -d 10.1.0.0/25 -o eth0 -m policy --dir out --pol ipsec --reqid 2 --proto esp
-j ACCEPT
[1:84] -A FORWARD -s 10.1.0.0/25 -d 10.2.0.0/16 -i eth0 -m policy --dir in --pol ipsec --reqid 1 --proto esp -
j ACCEPT
[1:84] -A FORWARD -s 10.2.0.0/16 -d 10.1.0.0/25 -o eth0 -m policy --dir out --pol ipsec --reqid 1 --proto esp
-j ACCEPT
[2:1274] -A OUTPUT -o eth0 -p udp -m udp --sport 500 -j ACCEPT
[4:3624] -A OUTPUT -o eth0 -p udp -m udp --sport 4500 -j ACCEPT
[156:50440] -A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT
[6:391] -A OUTPUT -d 192.168.0.150/32 -o eth0 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Fri Sep  9 15:00:49 2016
```

ikev2/nat-rw-mark/sun.iptables with iptables-saveikev2/nat-rw-mark/sun.iptables with iptables-save

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2  1616 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:500
    4  3896 ACCEPT     udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:4500
  120 26040 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
    4  2150 ACCEPT     tcp  --  eth0   *       192.168.0.150        0.0.0.0/0           tcp spt:80

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    84 ACCEPT     all  --  eth0   *       10.1.0.0/25          10.2.0.0/16         policy match dir in p
ol ipsec reqid 2 proto 50
    1    84 ACCEPT     all  --  *      eth0    10.2.0.0/16          10.1.0.0/25         policy match dir out
pol ipsec reqid 2 proto 50
    1    84 ACCEPT     all  --  eth0   *       10.1.0.0/25          10.2.0.0/16         policy match dir in p
ol ipsec reqid 1 proto 50
    1    84 ACCEPT     all  --  *      eth0    10.2.0.0/16          10.1.0.0/25         policy match dir out
pol ipsec reqid 1 proto 50

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2  1274 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           udp spt:500
    4  3624 ACCEPT     udp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           udp spt:4500
  154 48496 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
    6   391 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            192.168.0.150       tcp dpt:80

# Generated by iptables-save v1.4.21 on Fri Sep  9 15:03:19 2016
*raw
:PREROUTING ACCEPT [2496:590517]
```

```
:OUTPUT ACCEPT [1459:359528]
COMMIT
# Completed on Fri Sep  9 15:03:19 2016
# Generated by iptables-save v1.4.21 on Fri Sep  9 15:03:19 2016
*nat
:PREROUTING ACCEPT [6:5352]
:INPUT ACCEPT [4:5184]
:OUTPUT ACCEPT [1:60]
:POSTROUTING ACCEPT [1:60]
-A POSTROUTING -o eth1 -m mark --mark 0xa -j SNAT --to-source 10.3.0.10
-A POSTROUTING -o eth1 -m mark --mark 0x14 -j SNAT --to-source 10.3.0.20
COMMIT
# Completed on Fri Sep  9 15:03:19 2016
# Generated by iptables-save v1.4.21 on Fri Sep  9 15:03:19 2016
*mangle
:PREROUTING ACCEPT [94:18416]
:INPUT ACCEPT [90:18080]
:FORWARD ACCEPT [4:336]
:OUTPUT ACCEPT [119:47624]
:POSTROUTING ACCEPT [123:47960]
-A PREROUTING -d 10.3.0.10/32 -j MARK --set-xmark 0xa/0xffffffff
-A PREROUTING -d 10.3.0.20/32 -j MARK --set-xmark 0x14/0xffffffff
-A PREROUTING -s 192.168.0.1/32 -p udp -m udp --sport 4510 -j MARK --set-xmark 0xa/0xffffffff
-A PREROUTING -s 192.168.0.1/32 -p udp -m udp --sport 4520 -j MARK --set-xmark 0x14/0xffffffff
COMMIT
# Completed on Fri Sep  9 15:03:19 2016
# Generated by iptables-save v1.4.21 on Fri Sep  9 15:03:19 2016
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i eth0 -p udp -m udp --dport 500 -j ACCEPT
-A INPUT -i eth0 -p udp -m udp --dport 4500 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.168.0.150/32 -i eth0 -p tcp -m tcp --sport 80 -j ACCEPT
-A FORWARD -s 10.1.0.0/25 -d 10.2.0.0/16 -i eth0 -m policy --dir in --pol ipsec --reqid 2 --proto esp -j ACCEP
T
-A FORWARD -s 10.2.0.0/16 -d 10.1.0.0/25 -o eth0 -m policy --dir out --pol ipsec --reqid 2 --proto esp -j ACCE
PT
-A FORWARD -s 10.1.0.0/25 -d 10.2.0.0/16 -i eth0 -m policy --dir in --pol ipsec --reqid 1 --proto esp -j ACCEP
T
-A FORWARD -s 10.2.0.0/16 -d 10.1.0.0/25 -o eth0 -m policy --dir out --pol ipsec --reqid 1 --proto esp -j ACCE
PT
-A OUTPUT -o eth0 -p udp -m udp --sport 500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -m udp --sport 4500 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT
-A OUTPUT -d 192.168.0.150/32 -o eth0 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Fri Sep  9 15:03:19 2016
```

I think I prefer the first option. The output of iptables-save could perhaps be added as a separate file later.

#2 - 09.09.2016 17:39 - Noel Kuntze

I'm pretty sure there's a rather big opposition to just having iptables-save output in the scenarios.
As I like readable output as well, I'd like to actually see both: Supply iptables -v -L for all the tables, as well as iptables-save.
The latter for people so they can actually read the rules and the first for people that (for some reason) like iptables -L -v better.

I see that it is more work. If it's not easily solvable (just running a script over all the scenario files to add the tables is not enough?),
I'd vote for complete output of iptables-save -c.

#3 - 09.09.2016 18:14 - Tobias Brunner

> The latter for people so they can actually read the rules

One problem with that is that people might just blindly copy-n-paste the stuff (as they always seem to be doing), as it is e.g. hard to tell which rules are added manually (and required to be added) and which e.g. automatically by the updown script or a plugin.

> I see that it is more work. If it's not easily solvable (just running a script over all the scenario files to add the tables is not enough?),

It's just in a single script that generates that stuff. Anyway, I pushed a couple of patches to the *2111-testing-iptables* branch (currently does not use -c, so the rules are properly aligned and more readable).

#4 - 09.09.2016 18:21 - Noel Kuntze

> One problem with that is that people might just blindly copy-n-paste the stuff (as they always seem to be doing), as it is e.g. hard to tell which rules are added manually (and required to be added) and which e.g. automatically by the updown script or a plugin.

One could use the comment module to add comments to the rules that are added by the updown script or the plugin. And for the rules in the examples, the same can be done.
Like this: -m comment --comment "This is a comment."

> It's just in a single script that generates that stuff. Anyway, I pushed a couple of patches to the 2111-testing-iptables branch (currently does not use -c, so the rules are properly aligned and more readable).

That's pretty neat, thanks!

#5 - 09.09.2016 19:26 - Tobias Brunner

> One could use the comment module to add comments to the rules that are added by the updown script or the plugin. And for the rules in the examples, the same can be done.
> Like this: -m comment --comment "This is a comment."

Yeah, thought about that too. But I don't think it's a good idea to have a dependency on that module for plugins or the default updown script (while it is probably enabled on common distro kernels it is still an optional module).

#6 - 09.09.2016 21:45 - Noel Kuntze

Tobias Brunner wrote:

> > One could use the comment module to add comments to the rules that are added by the updown script or the plugin. And for the rules in the examples, the same can be done.
> > Like this: -m comment --comment "This is a comment."
>
> Yeah, thought about that too. But I don't think it's a good idea to have a dependency on that module for plugins or the default updown script (while it is probably enabled on common distro kernels it is still an optional module).

Understandable. Adding shell code into the updown script to detect if the comment module is supported would not be excusable, as it's considered a legacy.

#7 - 12.09.2016 18:02 - Tobias Brunner

- Assignee set to Tobias Brunner

- Target version set to 5.5.1

- Resolution set to Fixed

#8 - 22.09.2016 13:44 - Tobias Brunner

- Status changed from Feedback to Closed