strongSwan - Issue #3041

fail2ban or equivalent

30.04.2019 11:20 - smina would

Status:	Feedback		
Priority:	Low		
Assignee:			
Category:			
Affected version:	5.7.2	**Resolution:**	

Description

Hello,
is it possible to use fail2ban or equivalent to reject failed authentication IP ?
Thanks

Related issues:

Related to Feature #1506: Enhance DoS protection to deny users that failed Au...	**Feedback**	**11.06.2016**

History

#1 - 30.04.2019 11:24 - Tobias Brunner

- Tracker changed from Feature to Issue

- Status changed from New to Feedback

- Start date deleted (30.04.2019)

- Affected version set to 5.7.2

> is it possible to use fail2ban or equivalent to reject failed authentication IP ?

I'm sure you could use fail2ban or a similar tool e.g. with the ext-auth plugin or iptables to achieve that. Using RADIUS probably also allows such things. Writing a custom plugin would also be an option.

#2 - 30.04.2019 11:38 - smina would

I will try to create a fail2ban rule. I will also look at the LoggerConfiguration documentation.

Thank you Tobias

#3 - 02.05.2019 15:12 - smina would

I did it with fail2ban. For the time being, only EAP-MS-CHAPv2 failed authentication are operate.

If anybody needs it :

Firstly (optional) : create a log file for strongswan (/var/log/charon.log)
in strongswan.conf add :

```
        filelog {
                /var/log/charon.log {
            time_format = %c
                        append = no
                        default = 1
            job = -1
                        flush_line = yes
                }
                stderr {
                        ike = 2
                        knl = 3
                }
        }
```

When a failed EAP-MS-CHAPv2 authentication occured, the log file contain :

```
Thu May  2 14:59:19 2019 06[NET] received packet: from 172.18.222.246[57470] to 192.168.244.107[4500] (144 byt
es)
Thu May  2 14:59:19 2019 06[ENC] parsed IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Thu May  2 14:59:19 2019 06[IKE] EAP-MS-CHAPv2 verification failed, retry (1)
```

secondly : in fail2ban create a filter and a jail :

Filter :

```
[Init]
maxlines=3

[Definition]
failregex= [0-9]+\[NET\] received packet: from <HOST>\[[0-9]+\] to \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\[[0-9]+\
] \(\S+ \S+\)\n [0-9]{2}\[ENC] parsed IKE_AUTH request 3 \[ EAP/RES/MSCHAPV2 \]\n [0-9]{2}\[IKE] EAP-MS-CHAPv2
 verification failed
```

the regex can certainly be improved...

Jail :

```
[ipsec-auth]
enabled = true
port = 500,4500
protocol  = udp
filter = ipsec-auth
logpath = /var/log/charon.log
maxretry = 3
bantime = 86400
findtime = 3600
```

If you don't create a specific logfile for strongswan, logpath must be equal to /var/log/syslog

#4 - 02.05.2019 16:31 - Tobias Brunner

> Filter :
> [...]
> the regex can certainly be improved...

One problem is that these are not necessarily next to each other if multiple clients connect concurrently or the daemon does other stuff at the same time.

#5 - 03.05.2019 17:27 - smina would

> One problem is that these are not necessarily next to each other if multiple clients connect concurrently or the daemon does other stuff at the same time.

Yes, it's true. if some failed authentications escapes fail2ban it's embarrassing but not dramatic. The opposite hypothesis, a successful authentication identified by fail2ban as failed is unlikely (it would be necessary to authenticate 3 times, at the same time as a failed authentication).

with RADIUS, the problem would not arise, but it is not reasonable to mount a RADIUS server only for fail2ban.

is it possible to have a log containing the status of the authentication and the IP of origin on a single line with strongSwan (I don't think... I ask anyway)?

#6 - 03.05.2019 17:47 - Tobias Brunner

> is it possible to have a log containing the status of the authentication and the IP of origin on a single line with strongSwan (I don't think... I ask anyway)?

No, currently not. You'd have to add your own (e.g. via a small plugin). Or you could use the error-notify plugin, which notifies listeners about things like a failed authentication (the client's IP and port is included in the message).

#7 - 06.05.2019 09:07 - smina would

error-notify, I didn't know. I'll see what I can do with it. Thank you.

#8 - 21.05.2019 10:35 - Tobias Brunner

- Related to Feature #1506: Enhance DoS protection to deny users that failed Authentication added