strongSwan - Feature #1506

Enhance DoS protection to deny users that failed Authentication

11.06.2016 10:50 - Danny Kulchinsky

Status:	Feedback	**Start date:**	11.06.2016
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:			
Target version:			
Resolution:			

Description

In our implementation, we are seeing many cases of ineligible users attempting connection and failing authentication. Since we don't control the user base (Mobile devices that are pre-configured to attempt to establish a connection).

The reason for failing authentication is related to user eligibility in Radius backend systems (also not controlled by us). Although it fails authentication, the device will keep trying to connect regardless.

We are looking for an efficient way to "block" these connection attempts, one idea would be an enhancement to the DoS protection framework to deny "Source IP + Port" for any new IKE_SA_INIT request for a deny period (seconds/minutes/hours) in case it failed Authentication (using same identity and source ip+port) X times within a defined period.

Although this doesn't fall directly into DoS category - it still provides an additional layer of protection from overloading the security gateway with known to fail connection attempts.

Related issues:

Related to Issue #3041: fail2ban or equivalent	**Feedback**

History

#1 - 13.06.2016 09:26 - Tobias Brunner

- Status changed from New to Feedback

You could easily write a plugin that does this. You currently can't reject IKE_SA_INIT message as early as the receiver does in its DoS processing but you can avoid the DH overhead and authentication delay via RADIUS by rejecting the message quite early via the *message* hook.

#2 - 17.06.2016 12:22 - Danny Kulchinsky

Tobias Brunner wrote:

> You could easily write a plugin that does this. You currently can't reject IKE_SA_INIT message as early as the receiver does in its DoS processing but you can avoid the DH overhead and authentication delay via RADIUS by rejecting the message quite early via the *message* hook.

Not sure I understand, if the Reject is provided by the RADIUS it means that IKE Phase 1 (DH) was already completed, isn't it ? perhaps I'm missing something, could you elaborate some more ?

#3 - 17.06.2016 12:26 - Tobias Brunner

> Not sure I understand, if the Reject is provided by the RADIUS it means that IKE Phase 1 (DH) was already completed, isn't it ? perhaps I'm missing something, could you elaborate some more ?

Why should the Reject be provided by RADIUS?

#4 - 17.06.2016 12:37 - Danny Kulchinsky

Tobias Brunner wrote:

> > Not sure I understand, if the Reject is provided by the RADIUS it means that IKE Phase 1 (DH) was already completed, isn't it ? perhaps I'm missing something, could you elaborate some more ?

> Why should the Reject be provided by RADIUS?

Ok I just re-read your previous reply, I misunderstood - sorry.

Would you consider adding this enhancement to the Roadmap ?

#5 - 17.06.2016 14:31 - Tobias Brunner

> Would you consider adding this enhancement to the Roadmap ?

Maybe, but this has currently no priority, sorry.

#6 - 21.05.2019 10:35 - Tobias Brunner

- Related to Issue #3041: fail2ban or equivalent added