strongSwan - Feature #3423

Specify which certificates to send with send_certreq?

23.04.2020 09:53 - Glen Huang

Status:	Closed	**Start date:**	23.04.2020
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:			
Resolution:	Won't fix		

Description

When authenticate with certificates in a StrongSwan responder, I have CA certificates that are meant to authenticate initiators and sent to initiators to authenticate responder itself. Enabling send_certreq sends all CA certificates regardless how they are meant to be used.

Is it possible to specify that StrongSwan should only send certificates specified in remote.cacerts, or mark any CA certificate not to be sent in certreq?

History

#1 - 23.04.2020 11:58 - Tobias Brunner

- Status changed from New to Feedback

Note that no CA certificates are actually sent, only SHA-1 hashes.

> Is it possible to specify that StrongSwan should only send certificates specified in remote.cacerts

That's theoretically already the case. However, when a responder has to send certificate requests (in the IKE_SA_INIT response) it does not yet have a peer config (which is selected based on the identities). So it can't use that option. Initiators on the other hand will only use configured CA certificates.

> mark any CA certificate not to be sent in certreq?

Currently not.

#2 - 23.04.2020 12:14 - Glen Huang

Thanks for the quick reply.

I didn't realize config was not yet matched when an initiator tried connect.

However, does that mean that if I have multiple connections, each with their own remote.cacerts, a initiator connecting to any connection is going to receive combined remote.cacerts sha1 values in all connections, since charon at that point doesn't know which connection should be selected?

#3 - 23.04.2020 13:34 - Tobias Brunner

> However, does that mean that if I have multiple connections, each with their own remote.cacerts, a initiator connecting to any connection is going to receive combined remote.cacerts sha1 values in all connections, since charon at that point doesn't know which connection should be selected?

Again, for a responder, *remote.cacert* is completely irrelevant as it's not available when required. So a responder will send hashes for all trusted CA certificates that are loaded when generating the IKE_SA_INIT response.

#4 - 25.09.2020 11:40 - Tobias Brunner

- Category set to libcharon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Won't fix