strongSwan - Issue #2160

support for opportunistic encryption

27.10.2016 03:26 - Noel Kuntze

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.5.1	**Resolution:**	

Description

Does strongSwan actually support opportunistic encryption after the trap-any branch was merged?
This test scenario doesn't talk about opportunistic
encryption, so I guess it enforces IPsec protection for the hosts listed in rightsubnet. Is that right?

For real opportunistic encryption, I guess charon needs to insert *pass* policies for host that don't support
OE or where auth fails. So far correct?

History

#1 - 02.11.2016 15:05 - Tobias Brunner

- Status changed from New to Feedback

> Does strongSwan actually support opportunistic encryption after the trap-any branch was merged?

No.

> This test scenario doesn't talk about opportunistic
> encryption, so I guess it enforces IPsec protection for the hosts listed in rightsubnet. Is that right?

Correct.

> For real opportunistic encryption, I guess charon needs to insert *pass* policies for host that don't support
> OE or where auth fails. So far correct?

I guess, but OE can go even further (no authentication, authentication via DNSSEC etc.). You might want to read some of the related RFCs (e.g. the old RFC 4322, or RFC 7619 that allows negotiation IKEv2 SAs without authentication).

#2 - 02.11.2016 15:21 - Noel Kuntze

Tobias Brunner wrote:

> > For real opportunistic encryption, I guess charon needs to insert *pass* policies for host that don't support
> > OE or where auth fails. So far correct?
>
> I guess, but OE can go even further (no authentication, authentication via DNSSEC etc.). You might want to read some of the related RFCs (e.g. the old RFC 4322, or RFC 7619 that allows negotiation IKEv2 SAs without authentication).

Thank you for the links. Would a patch set for OE in strongSwan be acceptable?

#3 - 06.05.2020 10:32 - Madhu Mohan Nelemane

Noel Kuntze wrote:

> Tobias Brunner wrote:
>
> > For real opportunistic encryption, I guess charon needs to insert *pass* policies for host that don't support
> > OE or where auth fails. So far correct?

> I guess, but OE can go even further (no authentication, authentication via DNSSEC etc.). You might want to read some of the related RFCs (e.g. the old RFC 4322, or RFC 7619 that allows negotiation IKEv2 SAs without authentication).

Thank you for the links. Would a patch set for OE in strongSwan be acceptable?

This seems to be an old issue. Is there any update on the support for Opportunistic IPSEC ? Is there a patch or test scenario/document to implement OE with strongswan with 5.8.x versions ?