strongSwan - Feature #3134

Android client - allow configuring local identity with EAP (username/password)

05.08.2019 10:44 - Karel Hendrych

Status:	Closed	**Start date:**	05.08.2019
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	android		
Target version:	5.8.2		
Resolution:	Fixed		

Description

Hello, please consider adding an option to configure local identity (DN, user-FQDN, DNS-FQDN) on Android client for EAP (username/password) VPN types. Currently the identity for IKEv2 EAP (username/password) appears to be user-FQDN (email) with value set to configured username.

The use-case is support of IKEv2 implementations (like Juniper SRX) which permit match on common IKE ID suffix (for example @domain user FQDN part) to map remote peers to profiles with AAA and IP pools.

Thanks!

Associated revisions

Revision 698a18e7 - 15.10.2019 17:05 - Tobias Brunner

android: Allow configuration of client identity for all authentication types

This replaces the drop-down box to select certificate identities with a text field (in the advanced settings) with auto-completion for SANs contained in the certificate.

The field is always shown and allows using an IKE identity different from the username for EAP authentication (e.g. to configure a more complete identity to select a specific config on the server).

Fixes #3134.

History

#1 - 12.08.2019 14:36 - Tobias Brunner

- Status changed from New to Feedback

> Currently the identity for IKEv2 EAP (username/password) appears to be user-FQDN (email) with value set to configured username.

The IKE identity is simply set to the configured EAP username/identity, the format doesn't matter but is mapped to an identity type accordingly (see IdentityParsing). Many clients do that (others use the physical IP address as IKE identity if EAP is used).

> The use-case is support of IKEv2 implementations (like Juniper SRX) which permit match on common IKE ID suffix (for example @domain user FQDN part) to map remote peers to profiles with AAA and IP pools.

Can you give an example?

#2 - 12.08.2019 16:25 - Karel Hendrych

Hello, for example

user1@pass IKE-ID making the IKEv2 headend to use RADIUS backend 10.0.0.10 doing EAP-MSCHAPv2, IP pool would be 192.168.0.0/24
user1@mfa RADIUS backend 10.0.0.11 with one time password authentication, IP pool 192.168.1.0/24

Possibly different admission within network based on selected AAA, driven by supplied IKE-ID.

Then also it's handy for multi-tenancy if we have the same usernames using different AAA:

user1@domain1
user1@domain2

We can do this on strongSwan (Linux for example) by defining leftid and eap_identity.

#3 - 15.08.2019 10:36 - Tobias Brunner

> user1@pass IKE-ID making the IKEv2 headend to use RADIUS backend 10.0.0.10 doing EAP-MSCHAPv2, IP pool would be 192.168.0.0/24
> user1@mfa RADIUS backend 10.0.0.11 with one time password authentication, IP pool 192.168.1.0/24

So the EAP username would be user1 and the domain part would solely be used to select the connection?

> Then also it's handy for multi-tenancy if we have the same usernames using different AAA:
>
> user1@domain1
> user1@domain2

I guess the EAP identity/username would be the same in that scenario, though. No?

#4 - 19.08.2019 22:39 - Karel Hendrych

Tobias Brunner wrote:

> > user1@pass IKE-ID making the IKEv2 headend to use RADIUS backend 10.0.0.10 doing EAP-MSCHAPv2, IP pool would be 192.168.0.0/24
> > user1@mfa RADIUS backend 10.0.0.11 with one time password authentication, IP pool 192.168.1.0/24
>
> So the EAP username would be user1 and the domain part would solely be used to select the connection?

Correct, user1 would be username and @pass/@mfa domain like part would specify backed settings. Similarly also common domain part from DNS FQDN and DN can be used on Juniper SRX. However I consider user FQDN as most suitable for roadwarrior profiles.

> > Then also it's handy for multi-tenancy if we have the same usernames using different AAA:
> >
> > user1@domain1
> > user1@domain2
>
> I guess the EAP identity/username would be the same in that scenario, though. No?

Not necessarily some of the backends may not like user FQDN as usernames. And decoupling EAP identity from IKE ID would also permit to have multiple choices for the backend settings (user1@domain1-pass, user1@domain1-mfa ...)

Thanks!

#5 - 08.10.2019 16:31 - Tobias Brunner

- Assignee set to Tobias Brunner

- Target version set to 5.8.2

- Resolution set to Fixed

I finally had time to look into this. The app now makes the client's IKE identity configurable for any authentication type. The drop-down field that was previously used to select client identities from certificates is replaced with a text field in the advanced settings, which provides auto-completion for SANs in case of certificate authentication. Client identities can now also be imported from profile files if EAP authentication is used.

I've released a beta version of the app that includes these changes (the code can be found in the *android-updates* branch), see here for information regarding beta testing.

#6 - 15.10.2019 17:33 - Tobias Brunner

- Status changed from Feedback to Closed

#7 - 16.10.2019 10:39 - Karel Hendrych

Hi, initially described use-case with explicitly configured user FQDN IKE-ID works great. Thanks loads!

Karel