strongSwan - Issue #3405

Feature anti-replay for unicast and multicast SA supported by src/libipsec

09.04.2020 09:38 - Jean-Luc Jordan

Status:	Closed		
Priority:	Low		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.8.1	**Resolution:**	No change required

Description

Hi,

In my strongswan configuration, the plug-in kernel-libipsec is used.
So the own strongswan src/libipsec is embedded.

Does that library src/libipsec support the feature anti-replay for unicast and multicast SA please ?

By extracting the sections 2.2 and 2.3 of the RFC 4303,
the anti-replay could be managed if the SPI is different for each sender.
For SA multicast, there is an order to match SA in the SAD:
1- SPI, Destination, Source
2- SPI, Destination
3- SPI
Is it supported by src/libipsec please ?

Thanks in advance for your answer,
Kind Regards,
Jean-Luc J

History

#1 - 09.04.2020 10:27 - Tobias Brunner

- Status changed from New to Feedback

> Does that library src/libipsec support the feature anti-replay for unicast and multicast SA please ?

It doesn't support multicast SAs, but anti-replay protection for unicast SAs is implemented.

#2 - 10.04.2020 08:20 - Jean-Luc Jordan

Hi Tobias,
Thanks for your answer.
I am surprised by the fact that "src/libipsec doesn't support multicast SAs".
In the issue #3384,
for the following question you have answered YES
extract
" - In IPsec-v2, an SA (Security Association) is uniquely identified
by a combination of the SPI (Security Parameters Index),
protocol (ESP or AH) and the destination address. In IPsec-v3,
a unicast SA is uniquely identified by the SPI and, optionally,
by the protocol; **a multicast SA is identified by a combination
of the SPI and the destination address and, optionally, the
source address**. [YES/NO/PARTIAL]

Yes. "
That is why I though that src/libipsec supports multicast SAs.

Kind Regards,
Jean-Luc J

#3 - 14.04.2020 11:24 - Tobias Brunner

> That is why I though that src/libipsec supports multicast SAs.

I only answered that in regards to identifying the unicast SAs.

#4 - 14.04.2020 11:49 - Jean-Luc Jordan

Hi Tobias,

Just to be sure to summarize,
if the kernel-libipsec strongswan plugin is used then multicast SA is not supported.
If it is not enabled (then the kernel Linux ipsec is used) then multicast SA is supported.
Is it correct please ?

Thanks in advance for your help,
Kind Regards,
Jean-Luc J

#5 - 14.04.2020 12:01 - Tobias Brunner

> If it is not enabled (then the kernel Linux ipsec is used) then multicast SA is supported.

Maybe, I don't know exactly to what degree the kernel supports multicast SAs. strongSwan doesn't support negotiating multicast SAs anyway.

#6 - 14.04.2020 12:16 - Jean-Luc Jordan

Thanks.

Is it possible with strongSwan to create "static" multicast SAs please?
I understand now that negotiating multicast SAs is not possible with strongSwan.
But in the strongswan config file, is there a meaning to specify in conn part "no keyexchange"
to specify to not use ike ?

Kind Regards,
Jean-Luc J

#7 - 14.04.2020 14:23 - Tobias Brunner

strongSwan does not support any static configuration.

#8 - 16.04.2020 08:24 - Jean-Luc Jordan

Thanks Tobias.
Now I have understood.
If I need to create static SA, I need another meaning to do that.
By example using the "ip xfrm" commands (netlink xfrm framework).
The better way is that the 2 meanings to create statical and negotiating (dynamical) SA share the same SAD and the same SPD.
If I use "ip xfrm" commands to create statical SA, it will use the SAD of the kernel.
If I use strongswan including the plug-in kernel-libipsec,
where is located the SAD (in the kernel or in the user-land) please ?

Thanks in advance for your help,
Kind Regards,
Jean-Luc J

#9 - 16.04.2020 11:07 - Tobias Brunner

As long as you don't install duplicate policies, it should work fine if you manually install some SAs/policies even if strongSwan also uses the SAD/SPD in the kernel.

> If I use strongswan including the plug-in kernel-libipsec,
> where is located the SAD (in the kernel or in the user-land) please ?

Depends on the order of loaded plugins implementing the kernel_ipsec_t interface, in particular, *kernel-netlink* and *kernel-libipsec* (the one loaded first is used to access SAs/policies).

#10 - 16.04.2020 13:57 - Jean-Luc Jordan

My strongswan is configured as below with the plug-in:

sudo ./configure --prefix=/usr/local --sysconfdir=/etc/strongswan --disable-dependency-tracking --enable-kernel-libipsec --enable-forecast

Once compiled and started, in the log, the list of plug-in is the following one:
loaded plugins: charon aes des rc2 sha2 sha1 md5 mgf1 random nonce x5
09 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem fips-prf gmp
curve25519 xcbc cmac hmac attr kernel-libipsec kernel-netlink resolve socket-default forecast
stroke vici updown xauth-generic counters
The file strongwan.conf is
charon {
load_modular = yes
multiple_authentication = no
plugins {
include strongswan.d/charon/*.conf
}
}
The directory strongswan.d/charon contains the following files:
/etc/strongswan/strongswan.d/charon$ ls
aes.conf fips-prf.conf nonce.conf random.conf stroke.conf
attr.conf forecast.conf pem.conf rc2.conf updown.conf
cmac.conf gmp.conf pgp.conf resolve.conf vici.conf
constraints.conf hmac.conf pkcs12.conf revocation.conf x509.conf
counters.conf kernel-libipsec.conf pkcs1.conf sha1.conf xauth-generic.conf
curve25519.conf kernel-netlink.conf pkcs7.conf sha2.conf xcbc.conf
des.conf md5.conf pkcs8.conf socket-default.conf
dnskey.conf mgf1.conf pubkey.conf sshkey.conf

When 2 SA are up and when I execute the command "ip xfrm state", it displays nothing.
That means I thing that the SAD used is not the one of the kernel.
So it should be the wrong order for the plug-in kernel-libipsec and kernel-netlink.
How to change the order of the plug-in to have first kernel-netlink and after kernel-libipsec ?

Thanks in advance for your answer.
Kind Regards,
Jean-Luc

#11 - 16.04.2020 15:18 - Tobias Brunner

> How to change the order of the plug-in to have first kernel-netlink and after kernel-libipsec ?

Just don't load the *kernel-libipsec* plugin at all, or change its priority (see PluginLoad).

#12 - 25.09.2020 11:03 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required