strongSwan - Feature #835

Load-tester for Xauth

26.01.2015 16:08 - Yunkai Chen

Status:	Closed	**Start date:**	26.01.2015
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	testing		
Target version:	5.3.0		
Resolution:	Fixed		

Description

Hi All,

I want to do load test for xauth, but I don't know how to configure load tester correctly. Please help me, thanks a lot.

Here is my server's configuration:

```
conn IKEv1_Xauth_RSA
keyexchange=ikev1
leftauth=pubkey
leftcert=ios.crt
rightsourceip=172.16.0.0/20
rightauth=pubkey
rightauth2=xauth-eap
auto=add
```

My load-tester's configuration is like below.

```
plugins {
load-tester {          # enable the plugin
enable = yes           # 10000 connections, ten in parallel
version = 1
initiators = 1
iterations = 1         # use a delay of 100ms, overall time is: iterations * delay = 100s
delay = 100            # address of the gateway (releases before 5.0.2 used the "remote" keyword!)
responder = 10.0.0.174          # IKE-proposal to use
proposal = aes128-sha1-modp1024          # use faster PSK authentication instead of 1024bit RSA
initiator_auth = pubkey
issuer_cert = /etc/ipsec.d/cacerts/ca.crt
issuer_key = /etc/ipsec.d/private/ca.key
initiator_id = conn-%d-round-%d@VPN Defender.org
responder_id = "O=VPN Defender Staging, CN=vpn-stg.vpndefender.com"          # request a virtual IP using configuration payloads
request_virtual_ip = yes          # disable IKE_SA rekeying (default)
ike_rekey = 0          # enable CHILD_SA every 60s
child_rekey = 60          # do not delete the IKE_SA after it has been established (default)
delete_after_established = no          # do not shut down the daemon if all IKE_SAs established
shutdown_when_complete = no
}
}
```

If I comment rightauth2 at server side, "#rightauth2=xauth-eap", load-tester works well. If I enable rightauth2, the load-tester cannot work, even if I change the initiator_auth, "initiator_auth= pubkey|xauth", or "initiator_auth= pubkey|eap-md5". The load-tester's log is like below:

```
"Jan 26 15:01:44 24[IKE] <load-test|2> initiating Main Mode IKE_SA load-test[2] to 10.0.0.174
Jan 26 15:01:44 24[CFG] <load-test|2> configuration uses unsupported authentication
Jan 26 15:01:44 24[MGR] <load-test|2> tried to check-in and delete nonexisting IKE_SA"
```

Anyone who knows how to configure load-tester to support xauth, please help me. Really appreciated.

Associated revisions

Revision a0036708 - 27.01.2015 10:47 - Martin Willi

load-tester: Support initiating XAuth authentication

As with other configuration backends, XAuth is activated with a two round
client authentication using pubkey and xauth. In load-tester, this is configured
with initiator_auth=pubkey|xauth.

Fixes #835.

Revision 45ab5b0f - 20.02.2015 14:04 - Martin Willi

load-tester: Support initiating XAuth authentication

As with other configuration backends, XAuth is activated with a two round
client authentication using pubkey and xauth. In load-tester, this is configured
with initiator_auth=pubkey|xauth.

Fixes #835.

History

#1 - 27.01.2015 10:51 - Martin Willi

- Status changed from New to Assigned

- Assignee changed from Tobias Brunner to Martin Willi

Hi,

The load-tester plugin so far did not support initiating XAuth, as it was unaware of a xauth keyword to configure authentication.

I've tried to address that with the referenced commit. It allows you to use initiator_auth=pubkey|xauth for version=1 connections.

Regards
Martin

#2 - 28.01.2015 09:50 - Yunkai Chen

Hi Matin,

Many thanks for your help. It do works now.
However I have another problem, no matter how many initiators I configured(I have change it from 1 to 100), the connecting number cannot increase.
I monitor the SA status at server side, "watch "ipsec status|head -1"", the connecting is 5, cannot increase if I change the initiators.

```
Every 2.0s: ipsec status|head -1                                        Wed Jan 28 08:45:43 2015

Security Associations (822 up, 5 connecting):
```

I want increase connecting number to do stress test for the server. Do you have any suggestion? Please help. Thanks.

#3 - 28.01.2015 10:25 - Martin Willi

- Status changed from Assigned to Feedback

Hi,

Each initiator requires a dedicated thread. You should also have some additional threads idle to handle the actual exchange. As a rule of thumb, set the number of threads to *10 + initiators * 2* in the strongswan.conf *charon* section.

Also, you might consider adjusting the delay option of load-tester.

#4 - 29.01.2015 08:35 - Yunkai Chen

Hi Matin,

It seems not work in my environment. I want increase connecting number to test VPN server's handling ability. It is the second number of "Security Associations (13 up, 5 connecting)"

I have change the threads and initiators, but connecting number still around 5.
there are several case I tested.
1. threads=210, initiator=100
ipsec load-tester initiate 1000 10
2. threads=30, initiator=10
ipsec load-tester initiate 1000 10
3. threads=30, initiator=10
ipsec load-tester initiate 1000 2

On all above case, connecting cannot exceed 5.

```
Every 2.0s: ipsec status|head -1                                    Thu Jan 29 07:20:15 2015

Security Associations (13 up, 5 connecting):
```

Here is my configuration of load-tester.

```
charon {
install_routes = yes
load_modular = yes
plugins {
include strongswan.d/charon/*.conf
}
include strongswan.d/charon-logging.conf
reuse_ikesa = no
threads = 30
plugins {
load-tester {      # enable the plugin
enable = yes       # 10000 connections, ten in parallel
version = 1
initiators = 10
iterations = 1       # use a delay of 100ms, overall time is: iterations * delay = 100s
delay = 10       # address of the gateway (releases before 5.0.2 used the "remote" keyword!)
responder = 10.0.0.174       # IKE-proposal to use
proposal = aes128-sha1-modp1024       # use faster PSK authentication instead of 1024bit RSA
initiator_auth = pubkey|xauth
issuer_cert = /etc/ipsec.d/cacerts/ca.crt
issuer_key = /etc/ipsec.d/private/ca.key
initiator_id = conn-%d-round-%d@VPN Defender.org
responder_id = "O=VPN Defender Staging, CN=vpn-stg.vpndefender.com"       # request a virtual IP using configuration payloads
request_virtual_ip = yes       # disable IKE_SA rekeying (default)
ike_rekey = 0       # enable CHILD_SA every 60s
child_rekey = 60       # do not delete the IKE_SA after it has been established (default)
delete_after_established = yes       # do not shut down the daemon if all IKE_SAs established
shutdown_when_complete = no
}
}
}
```

#5 - 29.01.2015 09:05 - Martin Willi

Hi,

Have you disabled the Denial of Service protection on the responder?

By default, charon limits the overall number of half-open IKE_SAs allowed, to limit the impact of DoS attacks. If more than 10 IKE_SAs are connecting, but not yet established, charon starts requesting COOKIEs. Additionally, a single peer is allowed to have a maximum of 5 half-open connections only.

To disable DoS protection completely, set the dos_protection option to no. The COOKIE and single peer thresholds can be individually configured using cookie_threshold and block_threshold options. Refer to strongswan.conf for a description of these options.

Regards
Martin

#6 - 13.02.2015 08:59 - Yunkai Chen

Hi Martin,

Really sorry for the long delay, I was busy in other things before days.

I have tried the configuration you provide, but it seems not work. The connecting number is still very low.

On both client and server side, I add below configurations in strongswan.conf

```
dos_protection=no
block_threshold=1000
```

When I run command "ipsec load-tester initiate 1000 20", there will be retransmission occurs, and the connecting slows down. And I feel there is no 10 threads works concurrently, when I configure 10 threads in strongswan.conf.

```
dos_protection=no
block_threshold=1000
threads = 64
plugins {
load-tester {      # enable the plugin
enable = yes       # 10000 connections, ten in parallel
version = 1
initiators = 10
iterations = 1          # use a delay of 100ms, overall time is: iterations * delay = 100s
delay = 10
......
}
}
ipsec load-tester initiate 1000 20
.+.+.+..++.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+..++.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+..++.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+..+..+++.+.+.+.+.+..+.++.+.+.+.+.+.+.+.+*..+.++..+
+.+.+..++.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.***.*+.+.++.+.+.+.+.+.+..+.+.++.+.+..+.++.+.+.+.+.+.+.+.+.+.+.+.
+.+.+.+******...++.+
```

#7 - 20.02.2015 14:11 - Martin Willi

- Tracker changed from Issue to Feature

- Status changed from Feedback to Closed

- Priority changed from High to Normal

- Target version set to 5.3.0

- Resolution set to Fixed

Fix merged to master.

> I have tried the configuration you provide, but it seems not work. The connecting number is still very low.
> ipsec load-tester initiate 1000 20

For that load issue, please try using a shorter delay, multiple simultaneous initiate commands, and monitor what your threads are doing in ipsec statusall. If that doesn't help, please open a separate ticket for that issue.

Regards
Martin

#8 - 25.02.2015 02:32 - Yunkai Chen

Thanks. I will have a try.