Subject: IDL licenses thru a tunnel?
Posted by Anthony J. Ferro on Tue, 11 Mar 2003 21:41:03 GMT
View Forum Message <> Reply to Message

I'm trying to figure out a way to provide access to my IDL license server for our folks outside of our building's firewall (other buildings/classrooms on campus, home, other institutions, etc). I don't want to poke a generic hole in our firewall because of a) the security risk of another hole, and b) I don't really want to provide IDL to everyone on the internet (sorry). What I've been trying is to set up an ssh tunnel using something like:

ssh -f -N -L 1700:localhost:1700 username@idlserver

This _almost_ works. There is some communication going on between the client and the server, but the license request fails. I can tell that some communication occurs because the error message includes the name of the server (the client license file has "localhost").

Has anyone implemented something like this? I may have to try for a full VPN solution if this simple tunnel doesn't work.

- Tony Ferro

| Anthony Ferro tferro@as.arizona.edu |
| Steward Observatory, NICMOS Project |
| University of Arizona Phone: (520) 621-8683 |
| 933 N. Cherry Ave. FAX: (520) 621-1891 |
| Tucson, AZ 85721-0065 http://merlin.as.arizona.edu/~tferro/ |

Subject: Re: IDL licenses thru a tunnel?
Posted by Craig Markwardt on Thu, 13 Mar 2003 19:02:53 GMT
View Forum Message <> Reply to Message

"Anthony J. Ferro" <tferro@as.arizona.edu> writes:

> I'm trying to figure out a way to provide access to my IDL license
> server for our folks outside of our building's firewall (other
> buildings/classrooms on campus, home, other institutions, etc).
> I don't want to poke a generic hole in our firewall because of
> a) the security risk of another hole, and b) I don't really want
> to provide IDL to everyone on the internet (sorry). What I've
> been trying is to set up an ssh tunnel using something like:
>

> ssh -f -N -L 1700:localhost:1700 username@idlserver
>
> This _almost_ works. There is some communication going on
> between the client and the server, but the license request
> fails. I can tell that some communication occurs because the
> error message includes the name of the server (the client
> license file has "localhost").

That's a pretty neat idea, and it works for me! Of course, on the
client, you need to set the license server:

setenv LM_LICENSE_FILE 1700@localhost

Craig

--
---------- ----------
Craig B. Markwardt, Ph.D. EMAIL: craigmnet@cow.physics.wisc.edu
Astrophysics, IDL, Finance, Derivatives | Remove "net" for better response
---------- ----------

Subject: Re: IDL licenses thru a tunnel?
Posted by Anthony J. Ferro on Fri, 14 Mar 2003 16:41:18 GMT
View Forum Message <> Reply to Message

Craig Markwardt wrote:
> "Anthony J. Ferro" <tferro@as.arizona.edu> writes:
>
>
>> I'm trying to figure out a way to provide access to my IDL license
>> server for our folks outside of our building's firewall (other
>> buildings/classrooms on campus, home, other institutions, etc).
>> I don't want to poke a generic hole in our firewall because of
>> a) the security risk of another hole, and b) I don't really want
>> to provide IDL to everyone on the internet (sorry). What I've
>> been trying is to set up an ssh tunnel using something like:
>>
>> ssh -f -N -L 1700:localhost:1700 username@idlserver
>>
>> This _almost_ works. There is some communication going on
>> between the client and the server, but the license request
>> fails. I can tell that some communication occurs because the
>> error message includes the name of the server (the client
>> license file has "localhost").
>
>
> That's a pretty neat idea, and it works for me! Of course, on the

> client, you need to set the license server:
>
> setenv LM_LICENSE_FILE 1700@localhost
>
> Craig
>

Hmmm, I hadn't tried that, but it doesn't work for
me either. The problem seems to be that my server returns
it's own name (eg. idlserver) instead of "localhost" and
things fail at that point. Maybe if I get creative with
my "/etc/hosts" file.....

- Tony Ferro

Subject: Re: IDL licenses thru a tunnel?
Posted by Karl Schultz on Fri, 14 Mar 2003 19:48:15 GMT
View Forum Message <> Reply to Message

"Anthony J. Ferro" <tferro@as.arizona.edu> wrote in message
news:b4t0nenqi1@oasis.ccit.arizona.edu...
> Hmmm, I hadn't tried that, but it doesn't work for
> me either. The problem seems to be that my server returns
> it's own name (eg. idlserver) instead of "localhost" and
> things fail at that point. Maybe if I get creative with
> my "/etc/hosts" file.....
>
> - Tony Ferro
>

I'm not an expert on this, but my /etc/hosts file starts out with:

Do not remove the following line, or various programs
that require network functionality will fail.
127.0.0.1 localhost.localdomain localhost

Subject: Re: IDL licenses thru a tunnel?
Posted by Randall Skelton on Fri, 14 Mar 2003 21:59:38 GMT
View Forum Message <> Reply to Message

I do this all the time from home and sometimes resort to this when
travelling to meetings abroad.

Step 1:
^^^^^^^

```
ssh -f -N -L 1700:idl_license_server.domain:1700 username@myserver.domain
ssh -f -N -L 4100:idl_license_server.domain:4100 username@myserver.domain
```

The 'idl_license_server.domain' can either be the fully qualified hostname and domain of your IDL flexlm license manager or the ip address. This is given in your standard network license.dat file:

```
  SERVER idl_license_server.domain 0#50##ae6#cf 1700
         ^^^^^^^^^^^^^^^^^^^^^^^^^                ^^^^
```

Note that not everyone keeps the default 1700 port so be sure to check this.

The latter part, 'username@myserver.domain' is a server which you have shell, i.e. ssh, access to which is capable of connecting to the IDL license server. In this way, you do not actually need login access to a machine which runs your license manager; rather, you can tunnel through any machine that is capable of contacting the license server (i.e. any machine in your department that you can run IDL from).

The second port I tunnel seems to be required for the information being passed back from the IDL license server. I basically sniffed packets while in my office to and learned that IDL was routing packets back on 4100 and not 1700. I have no idea how standard this is but it is definitely required for my setup.

Step 2:
^^^^^^^

Change your license.dat file to point to localhost rather than your usual license server.

i.e.
```
  SERVER idl_license_server.domain 0#50##ae6#cf 1700
becomes
  SERVER localhost 0#50##ae6#cf 1700
```

Alternatively, instead of 'localhost'you could use your bonified machine hostname or 127.0.0.1. You should not need to mangle your /etc/hosts file as 'localhost' and 127.0.0.1 are very standard lookup names that resolve to your local machine.

In principle, Craig's solution should also work (and wouldn't require mangling the license.dat file) but for some reason this doesn't work for me... I can remember being rather frustrated by this after reading the flexlm docs. In my case things are slightly more complex as I have 2 separate instances of flexlm managers running on my laptop for other

packages and I already have the LM_LICENSE_FILE variable set.

My final modification was to the /usr/local/rsi/bin/idl script itself. In this case I simply test if the ssh tunnels exist prior to actually starting IDL. If they don't I create the tunnels before starting IDL.

Cheers,
Randall

On 13 Mar 2003, Craig Markwardt wrote:

> "Anthony J. Ferro" <tferro@as.arizona.edu> writes:
>
>> I'm trying to figure out a way to provide access to my IDL license
>> server for our folks outside of our building's firewall (other
>> buildings/classrooms on campus, home, other institutions, etc).
>> I don't want to poke a generic hole in our firewall because of
>> a) the security risk of another hole, and b) I don't really want
>> to provide IDL to everyone on the internet (sorry). What I've
>> been trying is to set up an ssh tunnel using something like:
>>
>> ssh -f -N -L 1700:localhost:1700 username@idlserver
>>
>> This _almost_ works. There is some communication going on
>> between the client and the server, but the license request
>> fails. I can tell that some communication occurs because the
>> error message includes the name of the server (the client
>> license file has "localhost").
>
> That's a pretty neat idea, and it works for me! Of course, on the
> client, you need to set the license server:
>
> setenv LM_LICENSE_FILE 1700@localhost
>
> Craig
>
> --
> ---------- ----------
> Craig B. Markwardt, Ph.D. EMAIL: craigmnet@cow.physics.wisc.edu
> Astrophysics, IDL, Finance, Derivatives | Remove "net" for better response
> ---------- ----------
>

Subject: Re: IDL licenses thru a tunnel?
Posted by Craig Markwardt on Tue, 18 Mar 2003 02:49:41 GMT
View Forum Message <> Reply to Message

Randall Skelton <rhskelto@atm.ox.ac.uk> writes:
> The second port I tunnel seems to be required for the information being
> passed back from the IDL license server. I basically sniffed packets
> while in my office to and learned that IDL was routing packets back on
> 4100 and not 1700. I have no idea how standard this is but it is
> definitely required for my setup.

I am following up on this, since I suddenly do have a need to tunnel
to a license server from a remote location.

I found out that it most definitely was *not* working for me, the way
I said it was. I was experimenting on a local machine that was within
the firewall, and that was not a good enough test.

Randall is right, you need to add another port to be forwarded, but
for me it was not 4100, it was 32769. I am not sure if this is
random, or if it is built into the license server. [but neither 4100
nor 32769 seems random.] This second port appears to be a another
layer of the licensing transaction that is required to let you run
IDL.

> Change your license.dat file to point to localhost rather than your usual
> license server.
>
> i.e.
> SERVER idl_license_server.domain 0#50##ae6#cf 1700
> becomes
> SERVER localhost 0#50##ae6#cf 1700

This still did not work for me. The reason is that at the second
layer of the transaction, the license file at the *server* is
consulted, not the local license file. So if the server is named
foobar.domain, it would have a license server file like:

SERVER foobar.domain XXXXXXXXXXXXX 1700

The license server somehow reports the foobar.domain hostname back to
the IDL client, and unfortunately you are then in a world of hurt.
The local machine tries to connect to foobar.domain:32769 (in my
case), which is also blocked by the firewall.

The solution was indeed to mangle with the hosts table, and after that
things seemed to work alright.

Summary:
* port redirect 1700

* port redirect 4100 or 32769 or whatever, use netstat to find out
* setenv LM_LICENSE_FILE 1700@localhost (allows first level transaction)
* mangle "/etc/hosts" so that *server* license.dat server name is
  aliased to 127.0.0.1 (allows second level transaction)

Now, wasn't that easy? How wonderfully useful IDL licensing is...
Harumphhh.

Craig

--
---------- ----------
Craig B. Markwardt, Ph.D. EMAIL: craigmnet@cow.physics.wisc.edu
Astrophysics, IDL, Finance, Derivatives | Remove "net" for better response
---------- ----------

Subject: Re: IDL licenses thru a tunnel?
Posted by h_chapman on Tue, 18 Mar 2003 05:35:13 GMT
View Forum Message <> Reply to Message

Randall Skelton <rhskelto@atm.ox.ac.uk> wrote in message
news:<Pine.LNX.4.33.0303142129250.11949-100000@moriarty.atm.ox.ac.uk>...

> Step 1:
> ^^^^^^^
>
> ssh -f -N -L 1700:idl_license_server.domain:1700 username@myserver.domain
> ssh -f -N -L 4100:idl_license_server.domain:4100 username@myserver.domain
>
>
> The second port I tunnel seems to be required for the information being
> passed back from the IDL license server. I basically sniffed packets
> while in my office to and learned that IDL was routing packets back on
> 4100 and not 1700. I have no idea how standard this is but it is
> definitely required for my setup.
>

To shed some light on the need for the second port, I found the answer
on globetrotter's faq:
http://www.globetrotter.com/flexlm/enduser_faq.htm#firewall

Apparently, the first port is for the license server proper, and the
second port is for the particular license daemon, in this case
idl_lmgr (terminology is now "vendor" in globetrotter's manuals, but
the idl license file retains "daemon"). Usually the license server
will negotiate a port for the daemon to do business on, but you can
force each daemon to be on a port you specify by adding at PORT=59000

(for example) at the end of the "DAEMON idl_lmgrd ..." line in the
license.dat.

DAEMON idl_lmgrd /usr/local/rsi/idl_5.6/bin PORT=59000

The next step is to open port 59000 (in addition to 1700) in your
firewall (if you have a firewall running on the license server), or
specify this when you tunnel. You can choose other ports for other
deamons (other licenses) in the license.dat.

> Step 2:
> ^^^^^^^
>
> Change your license.dat file to point to localhost rather than your usual
> license server.
>
> i.e.
> SERVER idl_license_server.domain 0#50##ae6#cf 1700
> becomes
> SERVER localhost 0#50##ae6#cf 1700
>
> Alternatively, instead of 'localhost'you could use your bonified machine
> hostname or 127.0.0.1. You should not need to mangle your /etc/hosts file
> as 'localhost' and 127.0.0.1 are very standard lookup names that resolve
> to your local machine.
>

Another interesting thing I learned from the globetrotter site is that
if you set the SERVER port to 27000 instead of idl's usual 1700, then
you only need @hostname instead of 1700@hostname for your
LM_LICENSE_FILE. 27000 is the default. So one of many ways of
tunnelling (this works for me) is:

export LM_LICENSE_FILE=@localhost
ssh -f -NL 27000:localhost:1700 myserver.com
ssh -f -NL 59000:localhost:59000 myserver.com
idl

type everything as written, except for myserver.com, which is the
remote machine running the license server.

Henry.

Subject: Re: IDL licenses thru a tunnel?
Posted by Craig Markwardt on Tue, 18 Mar 2003 14:53:41 GMT

h_chapman@fastmail.fm (Henry) writes:
>
> Another interesting thing I learned from the globetrotter site is that
> if you set the SERVER port to 27000 instead of idl's usual 1700, then
> you only need @hostname instead of 1700@hostname for your
> LM_LICENSE_FILE. 27000 is the default. So one of many ways of
> tunnelling (this works for me) is:
>
> export LM_LICENSE_FILE=@localhost
> ssh -f -NL 27000:localhost:1700 myserver.com
> ssh -f -NL 59000:localhost:59000 myserver.com
> idl
>
> type everything as written, except for myserver.com, which is the
> remote machine running the license server.

Hmmm, I still find that this give the same kind of server lookup error
that the original poster was reporting.

Because the *server*'s configuration file contains the name
myserver.com, and reports that back to the client, the client will
attempt to make a connection to myserver.com no matter what, and this
will be blocked by the firewall. That's why I had to fiddle with the
/etc/hosts table.

Craig
--
---------- ----------
Craig B. Markwardt, Ph.D. EMAIL: craigmnet@cow.physics.wisc.edu
Astrophysics, IDL, Finance, Derivatives | Remove "net" for better response
---------- ----------

Subject: Re: IDL licenses thru a tunnel?
Posted by R.Bauer on Tue, 18 Mar 2003 18:18:32 GMT

Craig Markwardt wrote:

>
> h_chapman@fastmail.fm (Henry) writes:
>>
>> Another interesting thing I learned from the globetrotter site is that
>> if you set the SERVER port to 27000 instead of idl's usual 1700, then
>> you only need @hostname instead of 1700@hostname for your
>> LM_LICENSE_FILE. 27000 is the default. So one of many ways of

>> tunnelling (this works for me) is:
>>
>> export LM_LICENSE_FILE=@localhost
>> ssh -f -NL 27000:localhost:1700 myserver.com
>> ssh -f -NL 59000:localhost:59000 myserver.com
>> idl
>>
>> type everything as written, except for myserver.com, which is the
>> remote machine running the license server.
>
> Hmmm, I still find that this give the same kind of server lookup error
> that the original poster was reporting.
>
> Because the *server*'s configuration file contains the name
> myserver.com, and reports that back to the client, the client will
> attempt to make a connection to myserver.com no matter what, and this
> will be blocked by the firewall. That's why I had to fiddle with the
> /etc/hosts table.
>
> Craig

just an idea did you have thougt about an alias in hosts.

Reiamr

--
Forschungszentrum Juelich
email: R.Bauer@fz-juelich.de
http://www.fz-juelich.de/icg/icg-i/
========== ======
a IDL library at ForschungsZentrum Juelich
http://www.fz-juelich.de/icg/icg-i/idl_icglib/idl_lib_intro. html

---

Subject: Re: IDL licenses thru a tunnel?
Posted by R.Bauer on Tue, 18 Mar 2003 18:23:03 GMT
View Forum Message <> Reply to Message

I should have read the previous posting Craig, it is already described to
set an alis

Reimar

Reimar Bauer wrote:

> Craig Markwardt wrote:
>
>>

>> h_chapman@fastmail.fm (Henry) writes:
>>>
>>> Another interesting thing I learned from the globetrotter site is that
>>> if you set the SERVER port to 27000 instead of idl's usual 1700, then
>>> you only need @hostname instead of 1700@hostname for your
>>> LM_LICENSE_FILE. 27000 is the default. So one of many ways of
>>> tunnelling (this works for me) is:
>>>
>>> export LM_LICENSE_FILE=@localhost
>>> ssh -f -NL 27000:localhost:1700 myserver.com
>>> ssh -f -NL 59000:localhost:59000 myserver.com
>>> idl
>>>
>>> type everything as written, except for myserver.com, which is the
>>> remote machine running the license server.
>>
>> Hmmm, I still find that this give the same kind of server lookup error
>> that the original poster was reporting.
>>
>> Because the *server*'s configuration file contains the name
>> myserver.com, and reports that back to the client, the client will
>> attempt to make a connection to myserver.com no matter what, and this
>> will be blocked by the firewall. That's why I had to fiddle with the
>> /etc/hosts table.
>>
>> Craig
>
> just an idea did you have thougt about an alias in hosts.
>
> Reiamr
>

--
Forschungszentrum Juelich
email: R.Bauer@fz-juelich.de
http://www.fz-juelich.de/icg/icg-i/
========== ======
a IDL library at ForschungsZentrum Juelich
http://www.fz-juelich.de/icg/icg-i/idl_icglib/idl_lib_intro. html

---

Subject: Re: IDL licenses thru a tunnel?
Posted by Anthony J. Ferro on Wed, 19 Mar 2003 19:17:31 GMT
View Forum Message <> Reply to Message

Hi all,

My thanks to all who helped and responded. I've now been able

to get this to work, so I thought I'd post a summary of what I did to get this to work. (Note I'm doing this all under Linux, but it should work for other systems too.)

The basic problem in my original attempt is that IDL actually requires _two_ connections to get a license. The first is to the FlexLM license manager. That's normally on port 1700 and that's what I was able to connect to originally. The second connection is to the VENDOR deamon, in this case RSI's idl_lmgrd. That normally falls to some unused default value, but it can be specified on the license server in the license file on the DAEMON line (aka the VENDOR line in the FlexLM docs). I've chosen to specify that port.

What I've now done to enable me to work from home (behind a NAT system) to connect to my work (behind a firewall) license server is....

On the server, license.foo.edu, I modified the license file so that it starts out something like this:

```
SERVER license 001122334455 1700
DAEMON idl_lmgrd /usr/local/rsi/idl_5.6/bin PORT=31700
```

On my home system, home.bar.com, I had to first modify my /etc/hosts file so that "license" is the loopback address:

```
127.0.0.1               localhost.localdomain localhost home license
```

This is required because the FlexLM license server knows who it is supposed to be (from the SERVER line). Next I have a "basic" license.dat file with:

```
SERVER localhost 001122334455 17000
USE_SERVER
```

So far, this has all been a one-time setup. Now, to run IDL locally, I first start up two ssh tunnels to my license server with a script which has:

```
ssh -f -N -L 17000:localhost:1700 license.foo.edu
ssh -f -N -L 31700:localhost:31700 license.foo.edu
```

Then I just use the "idl" command as normal. As long as those tunnels are up, everything should work. Note that I use the ports "17000" and "31700" just because they are free (high number) and might remind me why they are there.

I hope this helps anyone else trying to work out this type of
configuration.

- Tony

 -- -----------
| Anthony Ferro   tferro@as.arizona.edu |
| Steward Observatory, NICMOS Project |
| University of Arizona   Phone: (520) 621-8683 |
| 933 N. Cherry Ave.   FAX: (520) 621-1891 |
| Tucson, AZ 85721-0065   http://merlin.as.arizona.edu/~tferro/ |
 -- -----------

Subject: Re: IDL licenses thru a tunnel?
Posted by Thomas Gutzler on Thu, 20 Mar 2003 01:24:45 GMT
View Forum Message <> Reply to Message

Anthony J. Ferro wrote:
>
>   Hi all,
>
>   My thanks to all who helped and responded. I've now been able
> to get this to work, so I thought I'd post a summary of what I
> did to get this to work. (Note I'm doing this all under Linux,
> but it should work for other systems too.)

Seems to me, that the windows version is a bit more friendly. All I had
to do to get IDL running from behind a NAT is to
- set a System Variable: LM_LICENSE_FILE to 1700@localhost

- and configure my ssh-client (ssh secure shell)
  listen port: 1700
  Destination Host: IP of licenseserver
  Destination Port: 1700
  [x] Allow local Connections only
  Type: tcp
  as an outgoing connection

easy, isn't it ?

Tom

Subject: Re: IDL licenses thru a tunnel?
Posted by Anthony J. Ferro on Mon, 24 Mar 2003 16:19:11 GMT
View Forum Message <> Reply to Message

Thomas Gutzler wrote:
> Anthony J. Ferro wrote:
>
>>
>> Hi all,
>>
>> My thanks to all who helped and responded. I've now been able
>> to get this to work, so I thought I'd post a summary of what I
>> did to get this to work. (Note I'm doing this all under Linux,
>> but it should work for other systems too.)
>
>
> Seems to me, that the windows version is a bit more friendly. All I had
> to do to get IDL running from behind a NAT is to
> - set a System Variable: LM_LICENSE_FILE to 1700@localhost
>
> - and configure my ssh-client (ssh secure shell)
> listen port: 1700
> Destination Host: IP of licenseserver
> Destination Port: 1700
> [x] Allow local Connections only
> Type: tcp
> as an outgoing connection
>
> easy, isn't it ?
>
> Tom
>

That's interesting. You only had to set up one tunnel? I guess
I'll have to play with the set up some more. I was able to use
the environmental variable routine working too for the connection.
Somehow the modified license file seems like a slightly nicer
solution for me (eg. it will work when I set up a new user and
forget to add the LM_LICENSE_FILE def.).

- Tony Ferro
