strongSwan - Feature #383

Is it possible to get UNITY_SPLIT_INCLUDE and UNITY_LOCAL_LAN from RADIUS Access-Accept attributes?

14.08.2013 18:18 - Maxim Izergin

Status: Closed
Priority: Normal
Assignee: Tobias Brunner
Category: libcharon
Target version: 5.1.1
Resolution: Fixed

Start date: 14.08.2013
Due date: 
Estimated time: 0.00 hour

Description

I would like to move from attr-SQL to RADIUS.
It's possible to obtain IP and UNITY_BANNER from Radius Access-Accept attributes. The only things I'm missing for migration are UNITY_SPLIT_INCLUDE and UNITY_LOCAL_LAN attributes. They should be unique for each Class, so "attr" plug-in cannot be used in my case.

Does it possible to get UNITY_SPLIT_INCLUDE and UNITY_LOCAL_LAN from RADIUS Access-Accept attributes?

Thank you in advance!

Associated revisions

Revision af22622a - 11.10.2013 15:52 - Tobias Brunner
Merge branch 'radius-unity'

Adds support for Cisco Unity specific RADIUS attributes.

References #383.

History

#1 - 15.08.2013 11:22 - Tobias Brunner
- Tracker changed from Issue to Feature
- Status changed from New to Feedback

As far as I can tell from the code, forwarding other kinds of RADIUS attributes should be possible quite easily.

The question is, though, what kind of attributes those would be. For UNITY_BANNER we currently forward CVPN3000-IPSec-Banner1(15) and CVPN3000-IPSec-Banner2(36), both defined within the ALTIGA PEN (0x000c04/3076), Cisco provides a list of the defined attributes.

For UNITY_DEF_DOMAIN we could use CVPN3000-IPSec-Default-Domain(28), for UNITY_SPLITDNS_NAME there is CVPN3000-IPSec-Split-DNS-Names(29), but for UNITY_SPLIT_INCLUDE and UNITY_LOCAL_LAN there doesn't seem to be a ready to use attribute.

Well, there is CVPN3000-IPSec-Split-Tunnel-List(27) and CVPN3000-IPSec-Split-Tunneling-Policy(55) but those don't exactly correspond to the UNITY attributes. Apparently, split-tunnel-policy can take the values tunnelall(0), tunnelspecified(1), excludespecified(2). And from the Cisco docs it looks like split-tunnel-network-list takes the name of an ACL and not a list of subnets. Which seems to limit the flexibility quite a bit, that is, defining UNITY_SPLIT_INCLUDE and UNITY_LOCAL_LAN seems not possible, all addresses in the ACL are sent in either one of those ModeConfig attributes, depending on the defined policy.

I suppose we could redefine the meaning of the contents of a CVPN3000-IPSec-Split-Tunnel-List attribute to our liking (e.g. as a list of subnets, optionally with a ! before or after a subnet to send it in UNITY_LOCAL_LAN instead of UNITY_SPLIT_INCLUDE) but that wouldn't be compatible with a Cisco setup. Alternatively, we could actually implement something like ACLs (but with more flexibility), for instance:

```plaintext
charon {
  plugins {
    eap-radius {
      unity-acls {
        acl1 {
          include = <subnets>
          exclude = <subnets>
        }
        acl2 {
          include = <subnets>
        }
      }
    }
  }
}
```

19.03.2020 1/3
But that's very IKEv1/Cisco specific and might be overkill.

Of course, we could also define our own attributes in the ITA PEN (0x00902a/36906) namespace, but I don't know if that's preferable.

#2 - 15.08.2013 13:21 - Maxim Izergin

Hi Tobias,

Thank you very much for detailed answer.
Simultaneous usage of UNITY_SPLIT_INCLUDE and UNITY_LOCAL_LAN is not supported by Cisco clients, that is correct. Server should send either UNITY_SPLIT_INCLUDE or UNITY_LOCAL_LAN.

As for solution, I would prefer combination of CVPN3000-IPSec-Split-Tunnel-List attribute as a list of subnets, and CVPN3000-IPSec-Split-Tunneling-Policy as a "direction" option: 1 sends UNITY_LOCAL_LAN to the client and 2 sends UNITY_SPLIT_INCLUDE to the client.

Radius Access-Accept may look like this:

Sending Access-Accept of id 110 to 172.17.18.2 port 42221
   Class = 0x31306d626974
   CVPN3000-IPSec-Banner1 = ""
   CVPN3000-IPSec-Split-Tunnel-List = "172.20.10.0/255.255.255.240"
   CVPN3000-IPSec-Split-Tunneling-Policy = 1
   Framed-IP-Address = 10.175.63.254

Thu Aug 15 11:11:32 2013 : Info: Finished request 0.

This should be transformed into

UNITY_LOCAL_LAN = 172.20.10.0/255.255.255.240

and send to device.

Response

Sending Access-Accept of id 96 to 172.17.18.2 port 51848
   Class = 0x31306d626974
   CVPN3000-IPSec-Banner1 = ""
   CVPN3000-IPSec-Split-Tunnel-List = "172.20.10.0/255.255.255.240"
   CVPN3000-IPSec-Split-Tunneling-Policy = 2
   Framed-IP-Address = 10.175.63.254


should be transformed into

UNITY.Split.Include = 172.20.10.0/255.255.255.240

and send to device.

#3 - 16.08.2013 16:27 - Tobias Brunner

- Category set to libcharon
- Assignee set to Tobias Brunner

As for solution, I would prefer combination of CVPN3000-IPSec-Split-Tunnel-List attribute as a list of subnets, and CVPN3000-IPSec-Split-Tunneling-Policy as a "direction" option: 1 sends UNITY_LOCAL_LAN to the client and 2 sends UNITY_SPLIT_INCLUDE to the client.

That would be a possibility. I implemented this in the radius-unity branch of our repository. But I reversed the interpretation of the policy value, that is, tunnelspecified(1) sends UNITY_SPLIT_INCLUDE and excludespecified(2) sends UNITY_LOCAL_LAN. It is still a bit less flexible than e.g. the sql-attr plugin, which allows assigning both kinds of attributes to clients.

Multiple subnets can be separated with a comma (not sure if a space would be better), and are currently sent in a single configuration payload (perhaps I change that as it is not compatible with releases before 5.1.0).
Thank you very much, Tobias!
Patch is tested successfully:

```bash
# cd strongswan-5.1.0/
# wget http://wiki.strongswan.org/projects/strongswan/repository/revisions/99b6363f01496b971670c52ffbf17c7af3be36c8e8/diff/src/libcharon/plugins/eap_radius/eap_radius.c?option=diff
# mv eap_radius.c?option=diff eap_radius.patch
# patch -p1 < eap_radius.patch
# make
# make install
# ipsec start
# rm eap_radius.patch
```

Here is device log

Aug 16 18:00:24 iPhone-Maximus configd[47] <Notice>: IPSec Network Configuration started.
Aug 16 18:00:24 iPhone-Maximus configd[47] <Notice>: IPSec Phase2 starting.
Aug 16 18:00:24 iPhone-Maximus configd[47] <Notice>: IPSec Network Configuration established.
Aug 16 18:00:24 iPhone-Maximus configd[47] <Notice>: IPSec Phase1 established

I'm ready for migration from sql-atr to radius. :-)

Thank you!

Hi Tobias,

I found that INTERNAL_IP4_NETMASK is also important for me. It should be set to 255.255.255.255 in my setup, while default value is not 255.255.255.255.

Could you please support "Framed-IP-Netmask" (9) parameter from RADIUS?

Could you please support "Framed-IP-Netmask" (9) parameter from RADIUS?

I pushed another commit to that branch that adds support for this.

Thank you, Tobias!

Could you please support "Framed-IP-Netmask" (9) parameter from RADIUS?

I pushed another commit to that branch that adds support for this.

Thanks, Tobias!