This is a key feature for administrators. Because quite a number of servers share same public IPs behind firewalls and NATs, e.g. AWS, Azure, Cloud stack. And this will be a friendly way for Radius servers to deliver Coa/Dae messages correctly. "nas_ip = x.x.x.x" can be introduced like "nas_identifier".

---

**History**

- #1 - 16.01.2017 16:17 - Tobias Brunner
  - Category changed from charon to libcharon
  - Status changed from New to Feedback

Because quite a number of servers share same public IPs behind firewalls and NATs, e.g. AWS, Azure, Cloud stack. And this will be a friendly way for Radius servers to deliver Coa/Dae messages correctly.

Do I understand you correctly in that you want to be able to configure a static NAS-IP-Address and/or NAS-IPv6-Address attribute instead of defaulting to the actual local IP of the VPN connection?

- #2 - 16.01.2017 17:01 - Yick Xie
  
  Tobias Brunner wrote:

  > Because quite a number of servers share same public IPs behind firewalls and NATs, e.g. AWS, Azure, Cloud stack. And this will be a friendly way for Radius servers to deliver Coa/Dae messages correctly.

  Do I understand you correctly in that you want to be able to configure a static NAS-IP-Address and/or NAS-IPv6-Address attribute instead of defaulting to the actual local IP of the VPN connection?

  Yes, exactly.

- #3 - 17.01.2017 15:59 - Tobias Brunner

  Because quite a number of servers share same public IPs behind firewalls and NATs, e.g. AWS, Azure, Cloud stack. And this will be a friendly way for Radius servers to deliver Coa/Dae messages correctly.

  Do I understand you correctly in that you want to be able to configure a static NAS-IP-Address and/or NAS-IPv6-Address attribute instead of defaulting to the actual local IP of the VPN connection?

  Yes, exactly.

Is that common? According to RFC 2865 NAS-IP-Address "SHOULD be unique to the NAS within the scope of the RADIUS server”. So using the same IP for multiple NAS is technically not RFC compliant.

Also, how does setting this IP explicitly relate to "And this will be a friendly way for Radius servers to deliver Coa/Dae messages correctly." exactly? Could you describe the actual use case?
Tobias Brunner wrote:

Because quite a number of servers share same public IPs behind firewalls and NATs, e.g. AWS, Azure, Cloud stack. And this will be a friendly way for Radius servers to deliver Coa/Dae messages correctly.

Do I understand you correctly in that you want to be able to configure a static NAS-IP-Address and/or NAS-IPv6-Address attribute instead of defaulting to the actual local IP of the VPN connection?

Yes, exactly.

Is that common? According to RFC 2865 NAS-IP-Address “SHOULD be unique to the NAS within the scope of the RADIUS server”. So using the same IP for multiple NAS is technically not RFC compliant.

Also, how does setting this IP explicitly relate to “And this will be a friendly way for Radius servers to deliver Coa/Dae messages correctly.” exactly? Could you describe the actual use case?

This issue is quite prevalent, such configurations would override the private IP as only needed. I will elaborate here:

A VM instance IP is 172.0.0.1, but the public IP can be 8.8.8.8. In radius messages, the NAS-IP would be reported as 172.0.0.1, but this is actually non-sense or useless information for admins. In this case, if the radius server has to deliver Coa/Dae messages, there would be no way to know the public IP of this NAS, unless certain changes of default rules.

As for RFC, if the NAS-IP is correctly configured, this public IP should be and will be unique. And Radcli, a radius component of OCSERV introduced this feature 1 year ago. This option has helped me a lot and is harmless to the project as commented out by default.

This issue is quite prevalent, such configurations would override the private IP as only needed. I will elaborate here:

A VM instance IP is 172.0.0.1, but the public IP can be 8.8.8.8. In radius messages, the NAS-IP would be reported as 172.0.0.1, but this is actually non-sense or useless information for admins. In this case, if the radius server has to deliver Coa/Dae messages, there would be no way to know the public IP of this NAS, unless certain changes of default rules.

Strangely, RFC 5176 does not explicitly specify to which IP the Disconnect/CoA should be sent (only the port). I'd assume the RADIUS server should send it to the IP from which it received the original Access-Request (or Accounting-Request) message (to support proxying), but I guess there are some that (incorrectly?) use NAS-IP-Address, even though that poses the problem you describe with NATs. What RADIUS server do you use?

My service is based on FreeRADIUS. It is much easier to use NAS-IP-Address for most servers. And this is also helpful to deploy Huntgroups policy. Such cases do not involve proxying, then I think it could be wise to handle it on the NAS side.