

# RE: check group membership in Connection Request Policy

---

*Source:*

<http://www.tech-archive.net/Archive/Internet/microsoft.public.internet.radius/2007-01/msg00032.html>

---

- *From:* rt-seb <[rtseb@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:rtseb@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 23 Jan 2007 04:50:00 -0800
- 

Hello Robert,

"Robert Holzwarth" wrote:

Thanks for your comments.

The access request does not contain a valid user password, so there is no way for the IAS to authenticate the request. The VPN3000 NAS verifies the digital certificate. Therefore "Authenticate request on this server" cannot be enabled, as far as I understand and as a consequence no RAS Policy is ever checked.

Ah, I see. Authentication is done at the VPN3000, but authorization should be performed at the RADIUS server (group assignment).  
So what data does the VPN3000 send to the IAS? At least a username?  
If that is the case, a custom IAS extension would be really a solution.

We already do 802.1x authentication with our Enterasys switches, MAC authentication is supported out of the box.  
Is your DLL extending RAS Policy or the CRP?

Depends.

In your case it might be this way:

- there is a CRP with "Accept users without validating credentials"
- the IAS extension would perform authorization  
(if a username is provided by the VPN3000, the extension would do an AD lookup in order to figure out the AD group membership of that user)
- there would be no need for a RAS policy

If you want you can contact me privately ([discuss\(at\)rt-solutions.de](mailto:discuss(at)rt-solutions.de)).

One thing I do not understand is how MAC authentication should be possible "out-of-the box"? This must be a local solution: there is no

RE: check group membership in Connection Request Policy

RADIUS server performing central MAC authentication, right?

Sebastian

"rt-seb" wrote:

Hello,

"Robert Holzwarth" wrote:

There is no special need for CRP, IAS simply does only apply CRPs, because IAS is not able to do authentication, since digital certificates are used on the NAS.

Note: there are two different policies: CRP and RAS.

It works like this:

- a request arrives at the IAS
- the request is matched against a CRP (based on certain rules a CRP determines whether this request has to be forwarded to another RADIUS server or if it has to be terminated at the current IAS)
- => as you want to terminate the request you have to select "Authenticate request on this server"
- finally the IAS tries to apply a RAS policy to this request
- => you need to have a RAS policy that matches to your requests (e.g. certificate based authentication coming from VPN)

If the user is member of the specific group, the access request should be accepted and a class 25 attribute "OU=some string" is returned to the NAS.

Yes, I am interested in your custom IAS extension. What functionality does it provide?

Currently, the purpose of this extension is to perform MAC authentication for clients that do not speak 802.1x (e.g. printers). This is supported by Cisco ("MAC authentication bypass") and HP for example. The extension determines if it is a MAC authentication. If so the client will be authenticated using a MAC address database (either a file or Active Directory/LDAP). If the MAC is known and valid then the extension signals this to the IAS. Optionally the extension sets attributes for a connection

RE: check group membership in Connection Request Policy

(e.g. put a device in a special VLAN).

In principle it would also be possible to modify the IAS extension to do other things, like supporting other authentication methods or sending custom strings to access devices (switches, APs, VPN gateways ...).

"rt-seb" wrote:

Hello Robert,

"Robert Holzwarth" wrote:

We would like to check group membership of webvpn users, who authenticate against a Cisco VPN3000 with digital certificates. Remote Access Policies are not applied at all, if "Accept users without validating credentials" is enabled in the Connection Request Policy, as far as I understand IAS. Is developing our own authorization extension dll the only solution?

You need to provide more information. Why do you need to use a CRP? Why not use RAS? Are the users member of a certain AD groups? What should happen after the IAS has determined group membership? However, if you select "Accept users without .." the RAS policies are indeed not applied. Btw, I've developed a custom IAS extension. Maybe this is something you are interested in. Bye!

Sebastian

RE: check group membership in Connection Request Policy