

IAS 2003 for Cisco VPN Authorization (MS A.D. Group Lookup)

Source: <http://www.tech-archive.net/Archive/Internet/microsoft.public.internet.radius/2004-06/0043.html>

From: Minal (minalkc_at_rediffmail.com)

Date: 06/15/04

Date: 15 Jun 2004 08:15:39 -0700

Hi,

For one of our client, we are using Cisco VPN concentrator and Cisco VPN client for remote access VPN. The VPN concentrator authenticates using certificates. The VPN client certificate is authenticated by the VPN concentrator itself. The Cisco VPN concentrator has all root CA certs, its own identity cert and checks the CRL. Cisco VPN concentrator does this certificate authentication perfectly. This portion works fine.

We want to further do a Microsoft A.D. Group lookup to verify if the user is a member of a rollup group "Home Users".

The concentrator can do LDAP queries for Authorization but this needs the VPN concentrator schema extension. We do not want to use schema extension. We have formed a rollup group in the Microsoft A.D. for user groups permitted for VPN connectivity. We simply need a group lookup as our Authorization whether the user is present in this rollup group or not and accordingly he should be allowed or denied VPN connectivity respectively.

The concentrator can also do RADIUS queries for Authorization.

How can we use IAS 2003 to do just this job of a group lookup in the Microsoft A.D. ? Since Cisco VPN concentrator performs Authentication itself, we have configured the IAS 2003 server as an Authorization server.

Our trials attempts with IAS to do the Authorization indicate that the IAS essentially tries to do the Authentication of the VPN user. We do not want the IAS to do any Authentication. It should just do Authorization by way of a group lookup in the A.D.

The Cisco VPN concentrator can pass a common user password alongwith the authorization request. We could convert the incoming request user name to a common name created in the A.D. but then this does not

microsoft.public.internet.radius: IAS 2003 for Cisco VPN Authorization (MS A.D. Group Lookup)

provide the group lookup functionality. For some reason, the IAS does not want to give up the Authentication. We want just a group lookup.

Anyone out there done this ? All help welcome. Step-by-step instructions would be most helpful.

Thanks in advance.

Minal.