

Re: Securing Cisco devices using MS IAS (RADIUS) server

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2005-02/0121.html>

From: Johnny (*Johnny_at_discussions.microsoft.com*)

Date: 01/28/05

Date: Thu, 27 Jan 2005 16:17:02 -0800

Thanks for the reply, Ryan

Here is how I have the IAS configured:

1. Open up the MMC for the IAS service and connect to the server.
2. Select Clients from the containers in the left pane. Right-click on the Clients Container and select New | Client. Assign the client a descriptive name (in my case I used 'CiscoRouter') and select RADIUS as the protocol.
3. Enter the IP Address of the RADIUS client (Cisco device) and the shared secret that will be used to authenticate the RADIUS client (Cisco Device) to the IAS server.

Then to the Policy:

4. Right-click on the Remote Access Policies container in the left pane of the MMC and select New Remote Access Policy. I entered a descriptive name here.
5. Select Add to add a condition for authorization and select from the available options. Generally, you will use Windows Groups for AD based rules. (I did use Windows Groups)
6. Click add to add a group and select the group from AD you want to use for authorization. In this case I created a group and added a few accounts to it in the AD.
7. Select Grant for the permission.
8. Click the "Edit Profile" button and Select the Authentication tab and enable PAP authentication. I disabled CHAP, MS-CHAP and MS-CHAP v2.
9. On the Advanced tab select add to add a vendors specific option
10. Click on "add" to add an attribute and make the following selections.
11. Select Configure Attribute and enter the following in the Attribute Value Box: "Shell:priv-lvl=15"
12. Add a Second attribute of the name "Service Type" and value "login"

Create another rule for "user-mode" access to the Cisco device

13. Repeat steps 8 " 13 this time naming the rule to reflect the lower level

microsoft.public.win2000.networking: Re: Securing Cisco devices using MS IAS (RADIUS) server

of access that will be granted.

14. You will now see the rule you created in the MMC. It is important to remember that the rules will be applied in order. Once the RADIUS (IAS) server finds a match it will stop processing the remaining rules. THE ORDER IS IMPORTANT.

So basically I have 2 rules.

I can take screenshots of my configuration tomorrow morning (I'm away from the lab environment at the moment)... but the above was the process I followed. I'm not entirely sure how it is configured at the moment since I made changes to it when it wasn't working.

I followed the implimentation that was described in this document:

http://www.giac.org/practical/GCWN/Damon_Martin.pdf

Again, thanks for taking a look at this!

-Johnny

"Ryan Hanisco" wrote:

> *Johnny,*
>
> *Give us a bit more if an idea of how you set up the IAS service...*
>
> *Did you configure each router as a RADIUS client? You will need to do this*
> *for them to be able to Authenticate. From there you need to make a rule*
> *that resolves the username against the AD group that you want to permit to*
> *logon.*
>
> *As an aside, think about the security of passing domain account logon info*
> *to the radius server... Make sure you are in a management VLAN to handle*
> *this and control it with an ACL.*
>
> --
> *Ryan Hanisco*
> *MCSE, MCDBA*
> *Flagship Integration Services*
>
> *"Johnny" <Johnny@discussions.microsoft.com> wrote in message*
> *news:2880E281-6C4E-4684-95CF-D20E017E7D65@microsoft.com...*
> *Hi,*
> >
> *I'm trying to get the MS IAS service that is bundled with Windows Server*
> *2000 to act as a radius for Cisco routers on our network. The idea being*
> *that users who are authorized to log into the routers can do so with their*
> *AD*
> *accounts. This was successfully done and documented here:*
> >

Re: Securing Cisco devices using MS IAS (RADIUS) server

microsoft.public.win2000.networking: Re: Securing Cisco devices using MS IAS (RADIUS) server

> > http://www.giac.org/practical/GCWN/Damon_Martin.pdf
> >
> > *I have setup a test lab but am unable to get this to work in my lab
> > environment. I have put a sniffer on the switch (using port mirroring of
> > course) and noticed that the RADIUS request is coming from my test router
> to
> > the IAS server then the IAS server seems to never respond back. Also the
> IAS
> > logs do not show any activity. I have checked to make sure port numbers
> are
> > correct on the router, etc. But I really don't think my Cisco router is
> > configured incorrectly (I've checked all documentation from Cisco
> regarding
> the AAA commands and RADIUS commands).*
> >
> > *Has anyone ever tried to do this and if so, can they offer any advice,
> > assistance?*
> >
> > *Much thanks!*
> >
> > *-Johnny*
> >
>
>
>