

Re: IAS as RADIUS

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2006-09/msg00150.html>

- *From:* "the" <shirtrippa@xxxxxxxxxxxx>
 - *Date:* Thu, 7 Sep 2006 15:45:38 -0600
-

"Phillip Windell" <@.> wrote in message
news:%23cDBtIs0GHA.1568@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"the" <shirtrippa@xxxxxxxxxxxx> wrote in message
news:eGABZxr0GHA.4044@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Let's define access as having access to any resource. web, network, anything. if they are unauthorized, i want it to be like they're not even plugged into to that ethernet port.

Ok, but that doesn't clarify it. They can be plugged into the port, even get an IP#, even use a valid user account, and **still** not be able to use printers, file shares, or have web access.

Ideally, i'd like a group that once granted access is only allowed out of port 80(and maybe 443, or mail ports if they need it). this way they cant wreak havok on our network, but they'd be able to browse and read mail as needed.

That's easy. Create accounts for them, or just one special account for all of them to use. Let's call the account "Vendors" (or whatever you want). Then create a new Globab Group for them, let's call it "Temp Vendors" (or whatever you want). Add the account Vendors to the group "Temp Vendors". Set the Temp Vendors group as the Primary Group for that account. Now remove the account from the "Domain Users" group.

If i understood how to do that, i would. i can find no where in IAS to create any kind of object, all i can get it to do is pull from AD. some of these computers arent even on our domain, so i need a RADIUS server that doesn't rely on pulling users from our domain. What im assuming is that i can create a user on the server running IAS somewhere that it pulls from, but the server it will be on, sint an AD server. If you can clear that up

Re: IAS as RADIUS

for me, that'd be excellent.

There....now you have an account and a group which have permission to absolutely nothing....except for things the "Everyone Group" has access to, but that was always your responsibility to limit access to the Everyone Group long before this issue ever came along.

Mail Access depends on where the mail server is at. If it is on the Internet then the Firewall or Proxy controls that as well. If it is on the LAN then they already don't have access to it because they have no mailbox. no mailbox=no mail server access.

Internet Access is just simply done at the Firewall or Proxy Device.

Good high-end proxy servers like ISA Server allow/deny based on user accounts, so that of easily solved,...you don't give their account access to anything,...which is already the default anyway,...problem solved.

But lesser nat-based firewall only restrict by Source IP, Protocol, and Dest IP.

So you have to choose one option:

1. stop using DHCP
2. control where in the building they are able to connect in,...make those wall jacks a particular subnet that the Nat Device can allow/deny
3. use one of the expensive quarantine solutions the other guys have been trying to describe to you.

Let's not get too complicated too fast, regardless what i must do to get them too the inet, it'd be great to be able to allow just a handful of ports/protocols/services available across the entire network, as to restrict access from everything else. this way theyd have the needed functionality, while limiting access on our internal network. that way if they have a virus, it;d be harder for it to propogate throughout our network.

But i need to get a system in place to restrict access all together before i can get fancy and try to give them limited access.

No that is not true. It doesn't work like that. There is no one "system" that will do that. There many many many forms and methods of access control for different things and they all have to be coordinated together into a full security system. You either do it and do it right, or you don't. That is why the people who can do this, and do it correctly make the \$\$\$\$ (or at least they should).

Re: IAS as RADIUS

what i mean by that "...having a system in place to restrict access..." is having a crude, rudimentary setup in my lab that has the basic functionality of what im trying to accomplish. whether it be a xp/2950 switch/IAS system that im picturing so far, or something else, before i try to get granular, i just want something in my lab to work with. were there simply a system that worked id not have a job :D then i'd be sleeping at your house. and if it ever comes to that, just know that im a fan of ice cream :P

From Neteng:

There is nothing to configure for the supplicant, it's all configured on your switches. Once dot1x is setup and working, you can deploy Cisco NAC and that controls network access and resources. Google for dot1x and you'll find more than enough to read. Were implementing dot1x with Cisco ACS on the backend. I know your looking at IAS and that should work too.

<http://www.tek-tips.com/viewthread.cfm?qid=1239274&page=7>

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_example09186a00800947

Excellent, i'll do some reading and pry your brain some more if i get stopped some more.