

Re: IAS as RADIUS

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2006-09/msg00147.html>

- *From:* "the" <shirtrippa@xxxxxxxxxxxxx>
 - *Date:* Thu, 7 Sep 2006 14:31:48 -0600
-

"Phillip Windell" <@.> wrote in message
news:ebvtIir0GHA.1288@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

First, IAS is RADIUS. IAS is just MS's name for their deployment of it.
Second, RADIUS is not the solution for anything that I have read here yet.
RADIUS still requires Domain Accounts to be on the domain,...which you
already said you don't want to pull users from. If you create local
accounts on a particular server (like maybe the ISA Server) then RADIUS is
not used for that.

Let's go back to the beginning.

Define "access".
Access to what? Access from what? Access to where?
Is access simply getting an IP# from DHCP?
Is access retrieving a resource on the LAN?
Is access opening a web page on the Net?
What is not considered "access"? (that may sound silly but it is not).

We can not figure out a way to stop something if we don't know what it is
we are trying to stop.

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. 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. 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.

From Neteng:
The "supplciant" is a piece of software on the client PC. Windows XP is the

Re: IAS as RADIUS

only MS OS that comes with a 802.1x supplicant (but a poor one). 802.1x was developed to prevent unauthorized PC's from being placed on the network. Note I said PC's, not users. Do you want to prevent non-corporate PC's from being on the network and/or unauthorized people from getting on the network?

MAC ACL's would be horrible to manage so I would try and stay away from that.

Ah ok, i get you on the supplicant thing now. I dont anticipate anyone trying to plug into our network with a pre-XP machine, however if i have to configure 802.1x on each PC trying to plug into our network that could be as much of a management nightmare as MAC filtering.

Preventing unauthroized PC's from being placed on the network is exactly what im going for, i'd much rather these outside users use one of our workstations, but i think you and i both know that isn't going to happen. i'm compltely open to idea's, if you have any links that will get me going that'd would be much appreciated.

.