

RE: "Guest mode" in WiFi RADIUS?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-08/msg00296

- *From:* Ryan Hanisco <RyanHanisco@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 7 Aug 2007 08:00:03 -0700
-

Hi Chris,

I like to use 802.1x with PEAP to the workstations. This requires you to run a CA internally, but simplifies the setup on the workstations as it can provide a rotating key and only relies on encrypted username and password from the workstation rather than typing in a key/ shared secret.

Cisco has some step-by-step document on this as it is how they have theirs set up internally. I have also done this at a large company with dozens of sites so I can answer questions too.

—
Ryan Hanisco
MCSE, MCTS: SQL 2005, Project+
Chicago, IL

Remember: Marking helpful answers helps everyone find the info they need quickly.

"Chris Lukowski" wrote:

Is there an online guide on how to do something like this? I don't mind work on the back end as long as it's relatively simple to get guests onto our network (19 times out of 20 this will only be for access to the internet or their office VPNs) without compromising our network security. Right now we are using MAC filtering, WPA w/ TKIP-PSK, and no SSID broadcasts. So not only do we have to go into their wireless settings and add our SSID, but we also have to type in our PSK password right in front of them and THEN go to a workstation and add their MACs to the appropriate WAP. What a PITA. There has to be a better way, and I'm willing to bet that way is even more secure than what we have now.

"Ryan Hanisco" wrote:

Hi Chris,

RE: "Guest mode" in WiFi RADIUS?

Often times, companies will take a different tack on this. They will create two different VLANS, one for authenticated internal clients and another for guests. When a user authenticates to IAS/ Radius, you can hand back the VLAN as one of the responses of successful authentication and the WAP will change the VLAN on which the client communicates.

This lowers the security burden on IT staff as you're not troubleshooting every NIC driver and windows configuration out there that some one might bring in. This also allows you to build access lists and QoS policies to protect resources and bandwidth from these guests.

This works well with CISCO access points and is functional with others as these values are part of the standard RADIUS negotiation. This takes a bit more networking skill, but can lower the support burden.

Of course you can hide your SSID and use MAC authentication, but this adds only a minute or two to the hacking time if a skilled person wants to get in. SSIDs can be sniffed and MACs impersonated.

—
Ryan Hanisco
MCSE, MCTS: SQL 2005, Project+
Chicago, IL

Remember: Marking helpful answers helps everyone find the info they need quickly.

"Chris Lukowski" wrote:

Hi,

Right now we have a bunch of spread out and independent Linksys wireless access points that we're considering pointing to a central Windows Server 2003 RADIUS (or RRAS) server. One main goal we're trying to accomplish apart from the centralization of security settings is the ability to quickly allow a guest to connect to our wireless network with his laptop WITHOUT having to enter much more than our SSID. Right now we're using TKIP-PSK WPA security and in order for us to allow a sales rep to connect his/her laptop to our network we have to enter in our network key, usually with them standing right over us. We're not entirely comfortable with that, and going

RE: "Guest mode" in WiFi RADIUS?

into their wireless network settings and adding our SSID w/ network key is a pain, but I don't see any other way around it. That is unless there's a cool wireless USB device that will allow us to hardcode our SSID and other credentials to the device so that all we do is attach it to a laptop, install the drivers, and let it rip. I'm not sure that switching to RADIUS will make our lives easier in the "guest visitor" scenario, but we just need to make sure that devices not part of our Active Directory domain can authenticate using a guest password (without having the user logout of their session and signing on as a Guest).