TechRepublic
Real World. Real Time. Real IT.
August 31, 2006

SolutionBase: RADIUS deployment scenarios

by **Brien Posey**

User Service (RADIUS) has been around for what seems like forever, RADIUS has long been the authentication mechanism of choice for Internet Service Providers. Even so, RADIUS is capable of so much more than just being a gatekeeper for ISPs. In this article, I want to discuss some of the lesser known uses for RADIUS. As I do, I also I also want to show you some ways that RADIUS can be integrated into larger networks.

Before I begin

Before I get started, there are a couple of things that I want to get out of the way. First of all, as you probably know, there are a lot of different types of RADIUS servers, as well as a lot of different ways of configuring a RADIUS server to provide authentication to remote users. For the purposes of this article, all of my examples will assume that the RADIUS server is a Windows 2003 Server running Internet Authentication Service (IAS). IAS is Microsoft's version of RADIUS. I am also assuming that the RADIUS servers in my examples later on are using Windows Server 2003 domain controllers as their source of user account information.

The other thing that I want to mention is that in some of the examples that I will give later on, I have "dumbed down" some networking concepts in order to be able to focus primarily on RADIUS. For example, later on I will be talking a lot about using wireless networks. In the real world, it is common for wireless networks to be setup similarly to a VPN. However, I am going to simplify my discussions of wireless networks so that I can stay focused on RADIUS rather than getting hung up on the details of wireless security.

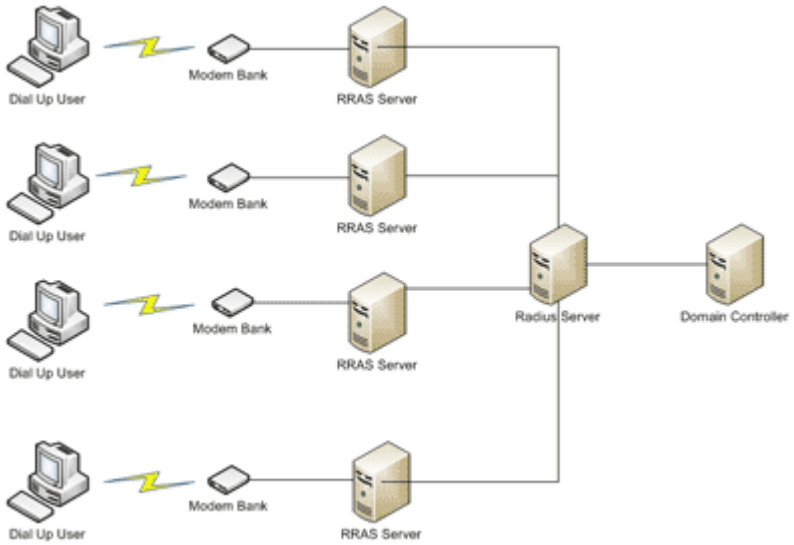
Internet service providers

As I mentioned earlier, RADIUS has been around for a long time, but Internet Service Providers were the ones that really made RADIUS famous. That being the case, I want to start out by examining a RADIUS deployment that might be used by an ISP. I know that I said that I wanted to talk about some of the less common types of RADIUS deployments,

but looking at an ISP style deployment allows me to start out simple with something that I can build on later on.

If you look at Figure A, you will see a diagram that shows four dial up users connecting to a remote network. As you can see in the figure, each dial up user is dialing into a modem bank that is connected to a Routing and Remote Access (RRAS) server. In this example, the RRAS servers are acting as network access servers for the remote users. However, the RRAS servers are not able to authenticate the user's connections on their own. Instead, the RRAS servers forward the remote access requests to the RADIUS server using the RADIUS protocol.

Figure A



This diagram shows how RADIUS might be used in a typical ISP environment.

The RADIUS server receives the request for authentication and initiates communications with a domain controller. The domain controller contains the user account, just as it would if the user were logging into a workstation that was physically connected to the network.

After the user is authenticated, remote access policies that are defined on the RADIUS server are applied to the user's connection. Assuming that the policies authorize the remote connection, then the RADIUS server tells the RRAS server to allow the connection.

Those of you who are new to RADIUS might be wondering why RADIUS is even necessary in this scenario. After all, the RADIUS server is acting as an intermediary between the RRAS server and the domain controller, so why doesn't the RRAS server just go directly to the domain controller for authentication? There are several reasons why the RRAS server doesn't talk directly to the domain controller, but the most important has to do with security.

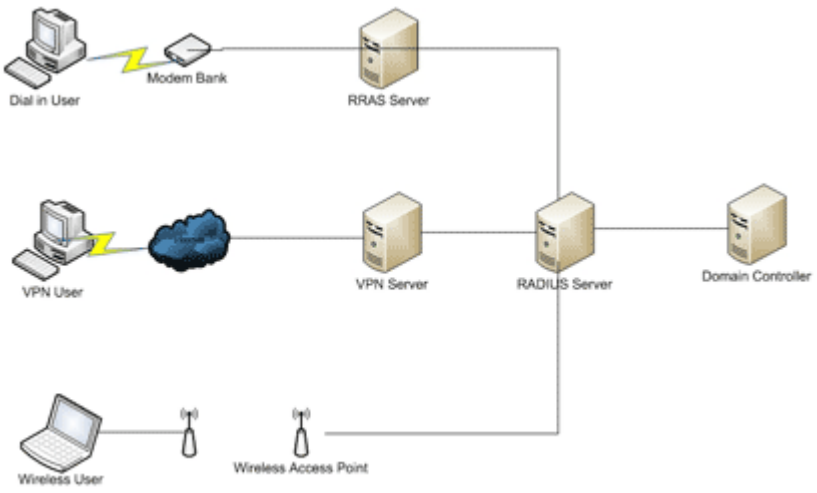
It's easy to assume that legitimate users are going to be dialing into the network, but in reality you have absolutely no idea who is dialing into the RRAS server until the user is authenticated. The person who is dialing in might be a legitimate remote user, or it could be someone evil who is out to do your network harm.

If there is a chance that someone with malicious intent could be dialing into the RRAS server, then you have to assume that there is at least some chance (albeit a small one) that the malicious user could compromise the RRAS server. If there is a slim possibility that a hacker could gain control over your RRAS server, do you really want that RRAS server to be able to directly talk to your domain controllers? Of course not. Your domain controllers contain account information for every user on your entire network. You want your domain controllers to be as far from a hacker's reach as possible. This is one of the reasons why the RRAS server does not communicate directly with a domain controller.

Corporate RADIUS deployments

Now that I have shown you how an ISP might use RADIUS, I want to show you how RADIUS might be used in a corporate environment. Larger corporations often have remote users who connect to the network in a variety of ways. If you look at Figure B, you will see that in this diagram, remote users are connecting to a corporate network via dial up, Virtual Private Network (VPN), and wireless network links.

Figure B



In a corporate environment, remote users may connect in a variety of ways.

If you look at the top row in this diagram, you will see that it is exactly the same as the ISP scenario that I discussed earlier. A user dials into a modem bank that is connected to a RRAS server. The RRAS server looks to the RADIUS server for authentication, and the RADIUS server in turn checks the user's credentials against a domain controller. Assuming that the credentials that the user entered were valid, the domain controller

validates the credentials, and then the RADIUS server looks at the remote access policy for the user and approves the connection. This approval is passed on to the RRAS server, and the remote user is allowed to access network resources.

If you look at the middle row of computers in Figure B, you can see that the same RADIUS server can also service VPN clients. In a VPN environment, the remote user tunnels through the Internet to the corporate VPN server. Before the VPN server will allow the remote user to access any network resources though, the remote user's identity must be validated. The user enters their credentials, which are then passed to the RADIUS server. The RADIUS server in turn checks the user's credentials against a domain controller. Assuming that the credentials that the user entered were valid, the domain controller validates the credentials, and then the RADIUS server looks at the remote access policy for the user and approves the connection. This approval is passed back to the VPN server, and the remote user is allowed to access network resources.

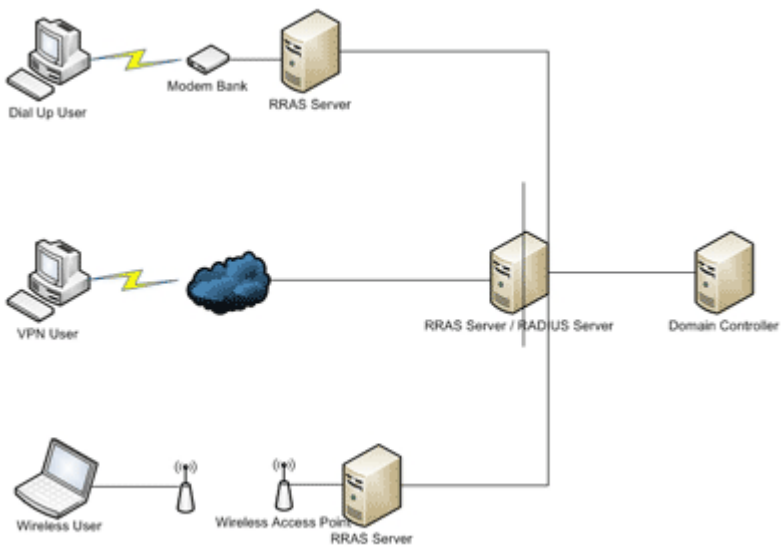
If this procedure sounds familiar, it's no coincidence. There are lots of VPN solutions on the market, but the Windows Server 2003 based VPN solution is built in to RRAS. In this particular diagram, I am using two different servers to provide access to dial in users and VPN users. I did this for both clarity, and because in larger environments, multiple servers would usually be used. In a small environment though, there is no reason why a single server could not function as both a remote access server and a VPN server.

The bottom row of the diagram shown in Figure B shows a wireless user authenticating through a RADIUS server. In this particular diagram, the wireless access point is acting as a wireless gateway and is connected directly to the RADIUS server. It is not uncommon though for a wireless access point to be connected to a VPN server and for wireless clients to be treated as VPN clients.

Performing double duty

The next thing that I want to show you is that it is possible for a Windows Server 2003 based RADIUS server to be schizophrenic. If you look at Figure C, you will see that the RADIUS server in the diagram is simultaneously functioning as both a RADIUS server and as a RRAS server (in this case an RRAS based VPN server).

Figure C



It is possible for a Windows Server 2003 based RADIUS server to also act as a RRAS server.

Unfortunately, this diagram is probably not as clear as it should be. When I created the diagram, I wanted to show that the RADIUS server contained two different NICs, but I could not find any icons that looked like network cards. Instead, I drew a vertical line down the middle of the server to show that the server is split into two sections.

In this particular deployment, the RADIUS server is multihomed. The RRAS service is bound to one NIC, and RADIUS is bound to another NIC. In this way, the server is acting similarly to a router.

In this particular diagram, the RRAS portion of the server is servicing VPN clients, but it could really be performing any remote access duty. In this case though, the remote users tunnel through the Internet and establish a remote connection to the RRAS / VPN server. As was the case before, the user's identity needs to be authenticated before the VPN server will give the remote user access to any network resources. The VPN server hands the authentication responsibility off to the RADIUS server, which happens to be running on the same box.

You will notice in the diagram that RADIUS is bound to a separate network interface than RRAS. This prevents a domain controller from being directly accessible over the Internet. Instead, the RADIUS server contacts the domain controller over its own interface and validates the user's credentials. After the credentials have been validated and the user's remote access policy is confirmed, the VPN server is informed, and the remote user is given access to network resources.

There is one more thing that I want to show you about this diagram before I move on. Notice that the dial-up and wireless interfaces are both connected to their own RRAS

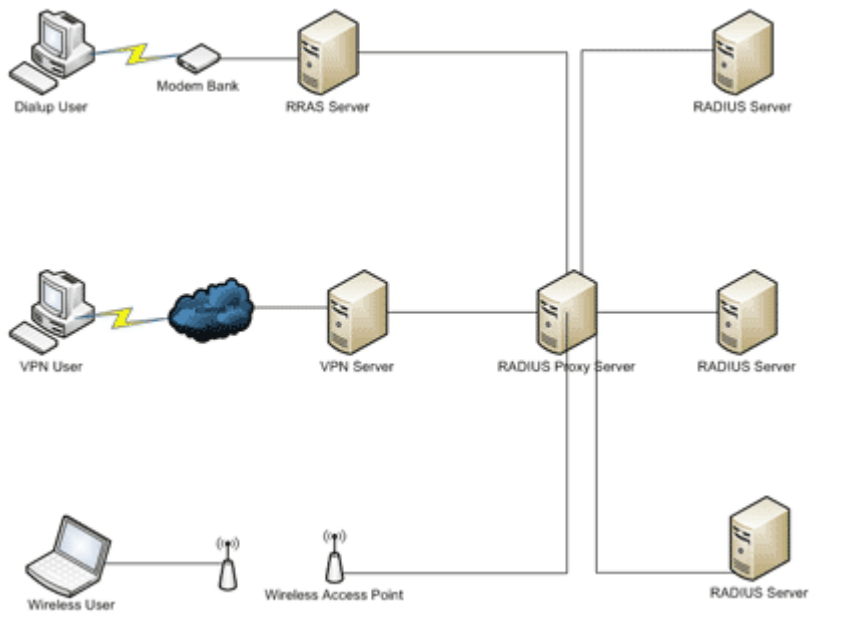
servers. These RRAS servers are multihomed, and one of the interfaces connects to the same network as the RADIUS server. They are not connected to the same interface as the RRAS portion of the RADIUS server.

A RADIUS proxy

In the last three diagrams that I have shown you, the organization has had remote users connecting through dial-up, VPN, and wireless links. In real life, if a company has that many remote users, then there is a good chance that the RADIUS server could become overloaded, and have trouble processing all of the authentication requests in a timely manner.

If you look at Figure D, you will see that the various remote access servers are now connecting to a RADIUS proxy rather than directly to a RADIUS server. The RADIUS proxy's job is to provide RADIUS load balancing services. As authentication requests come in to the RADIUS proxy, the requests are evenly distributed to the back end RADIUS servers for processing. This prevents any one individual RADIUS server from becoming a bottleneck due to an excessive workload.

Figure D



A RADIUS proxy can distribute the authentication workload.

The domain controllers are not shown in this diagram, but most networks include multiple domain controllers. In this type of deployment, the multiple RADIUS servers would be able to check user's credentials against multiple domain controllers. Again, this

would prevent a single network component (with the possible exception of the RADIUS proxy itself) from becoming a bottleneck.