Two Security Approaches You Should Be Taking on Your Network

Posted At : August 14, 2019 10:55 PM | Posted By : Josh Adams
Related Categories: Router, Creative Solutions

Routers these days are very sophisticated in regards to what they can do and you should take the time to configure yours to provide robust security. While not meant to be in any way comprehensive as to everything you should be doing from a security perspective on your router, this post offers 2 security approaches you should be implementing with your devices and router(s):

1. **Use the guest network for anything that doesn't need to talk to other devices on the network.**

   Actually, if your router supports VLANs, using a VLAN for anything that doesn't need to talk to other devices on the nework is even better than using the guest network. For more information on this, **see this excellent post.**. But that post points out, most home routers do not, as of this writing, support VLANs. As such, utilizing a guest network is your best option on most home routers.

   A guest network sounds like something you would use only for your guests' devices, but this is too limited a view of a guest network; instead, you should think of your guest network as the place to put any device that doesn't need to talk to other devices on the network.

   These days there are all sorts of IoT (Internet of Things) devices that we don't access directly but rather we interact with via a cloud services. Got a smart thermostat on your network? How about a smart plug? Maybe a smart scale? Chances are that you don't directly access these devices but rather you access a cloud services to interact with these devices. Well, if that's the case, why would you want these devices to be able to talk to other devices on the network? Put them on your guest network: they'll still have access to the Internet, they just won't have access to other devices on the network. Now, you may be thinking "well, just because I don't need them to access other devices on the network doesn't mean I care if they can access other devices on the network." Well, you should care: unfortunately, devices do become compromised from time to time and if someone gets into one of yours, you don't want him/her to use that access to gain additional access to network traffic and/or devices on the network. So: guest network for anything that doesn't need to be able to talk to other devices on the network.

   And you know what would make it even better? If the guest network were on a completely separate router from your main network! If you really want to isolate the devices on your guest network as much as possible from your main network then you use 2 routers and the first (the one connected to the outside world, which most commonly would mean to your router) has the guest network on it and the second (which is connected to the WAN of the first) has your main network on it. Then even if a bad actor gains access to your guest network or to a device on it, he/she would have to gain access from the outside to your second router in order to compromise your main network.

2. **Disable access to/from the Internet for anything that doesn't need it.**

   This one goes right along with the one above: in the same way that you don't want to give access to other devices on your network to anything that doesn't need it, you don't want to give Internet access to any device that doesn't need it. Have a printer on your network? Does it need Internet access? Chances are that it does not: chances are that you only need to be able to send print jobs to it on your local network. In the last item, I pointed out that unfortunately, devices do become compromised from time to time and in that case the point was to protect everything else on the network from a device that becomes compromised; here the goal is to protect a device from becoming compromised in the first place, which is especially important considering that if you need to talk to it (in this example, send print jobs to it) then you can't put it in the guest network which means that if it does become compromised then it's that much easier for the attack to gain additional access to network traffic and/or other devices on the network. So: turn off access to/from the Internet for anything that doesn't need it.

   Okay, great! But how do you do that? Well, the mechanism will vary from router to router, but in general the approach to use is going to be to create firewall rules. You will likely need a firewall rule that blocks all access from all ports from the outside (that is, the Internet) to a device and then a second firewall rule that blocks all access from all ports from a device to the outside. And you'll need such rules for every device on your network, so it might end up being a lot of rules. However, if you follow the guidance in my post **Use a More Sophisticated IP Address Scheme on Your Network**, you can create (if your router supports it) a rule for the entire octet you use for these devices.