SECURITY NOW!

Transcript of Episode #3

NAT Router Firewalls

Description: How and why any simple NAT Router makes a terrific hardware firewall. (And what you must disable to prevent it from being bypassed!)

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-003.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-003-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 3 for September 1, 2005, NAT Routers.

So let's talk about routers, because this is something you schooled me in some time ago and convinced me that a software firewall wasn't as good - even though you're the guy who really put ZoneAlarm on the map - wasn't as good as a hardware router.

Steve Gibson: Well, yeah. I guess the point is that a software firewall, while it's running in your machine, it's victim to anything that your machine is. And we know, we know for sure that many malware now deliberately knows about software firewalls and has taken actions to shut them down. So while a software firewall is certainly a good thing to have for monitoring outbound flow from your machine, what few people recognize is that a NAT router, the same kind of NAT router that, you know, many people have for so-called "IP sharing," where they have one IP on their cable modem or their DSL, and they want to share it among many machines, that makes inherently an extremely good hardware firewall. Nothing is able to come across the router that isn't expected. Because the way it works is that the router needs to know, when packets do arrive, which machine behind the router that is in your own private network is expecting to receive it. Since they're all sharing that one IP, the router has to have some way of figuring out which one asked for it. The way it does that is it watches the packets leaving the network. It watches any machines on the LAN sending data out onto the Internet. When packets leave, it makes a note of that packet, where it's bound for, and it changes the IP on the packet to its own public IP and gives it a port so that, when data comes back from that remote server, it looks in this table, so-called "connection table," to try to find a match. When it's able to match it up, that tells it which of the machines - because you might have, you know, you could have 15 of them behind your NAT router - it tells it which of the machines originated that traffic in the outgoing direction, so that it knows how to route it in the incoming direction.

Leo: So that's what a router is doing. It's saying, the data came from X; when it comes back, I send it to X. That's called "routing."

Steve: Exactly.

Leo: How does that protect me?

Steve: Well, the way it protects you is that hackers that are scanning the 'Net, or worms that are infecting the 'Net, that are just sending out data - or remember for a while there was the Windows Messenger spam, where people were getting these pop-up Messenger dialogues all the time? All of that - worms, hackers, scanners, Messenger spam, all that - those are unsolicited packets, meaning that they're coming from some random IP and port number, and they're just scanning across your IP range of your ISP, and that traffic tries to reach your computers. Well, the beauty of having a NAT router as, like, your first line of defense, is any of that stuff coming in, the router thinks, oh, maybe this is expected, maybe it's been solicited by a computer behind the router. So it checks its table. It will not find an entry there because it's coming from, you know, any of four...

Leo: It's unsolicited, right.

Steve: Yeah, exactly. It's coming from any of other, you know, 4 billion IPs - there literally are 4 billion possible IPs - and so it ignores it. It just throws it away.

Leo: Is, I mean, is that all a firewall does?

Steve: That's really all a firewall does.

Leo: So just by the virtue of the fact that it can't route a packet it didn't expect, it's blocking everything unexpected, it's a firewall.

Steve: Yeah.

Leo: Even if it doesn't say so on the box? Even if they don't say, this is a router and firewall?

Steve: Exactly. Any NAT router is also a firewall.

Leo: Now, this raises a couple of questions. First of all, are all broadband routers NAT firewalls? Or NAT routers?

Steve: I don't think I've ever seen one that isn't.

Leo: That's how they work.

Steve: Yeah. That's essentially - that's why people buy them is they want to share one IP, one public IP among multiple machines.

Leo: So if it's able to do that, it's blocking stuff. The second thing, and this is the one that people come up with most often when I tell them, oh, no, you've got a very good firewall with your router, they say, "But it's only looking at incoming traffic. What about outbound traffic?"

Steve: Well, and that's a really good point. It permits outbound traffic all the time, which is why it still makes sense to have a personal firewall running on the computer. You know, people want security to be perfect. They want it to be an absolute, black or white thing. And it's just not. So the more security you have, the better. And so a hardware firewall - one of the nicest things about a NAT router is that, if you have a computer with a personal firewall, I mean, that's just directly on the Internet with no NAT router, you'll very quickly get used to seeing all these pop-up messages as your software firewall is saying, oh, no, you're being attacked, you know, I'm blocking this, I'm blocking that. Here's somebody attacking you, blah blah blah, you know. The personal firewalls running on computers tend to be very noisy because they're trying to sell you on all the benefit that they're delivering. They're saying, look at all the good I'm doing for you. This horrible stuff would have actually reached into your computer if I, the software firewall, hadn't blocked it. Well, it's just nonsense. You know, I coined the acronym "IBR" for Internet Background Radiation. It's just like static on the 'Net.

Leo: There's always - this stuff's always going to be happening.

Steve: Well, in fact, we're never going to get worm-free now. There's worms out. And it's common knowledge that, if you take an unpatched Windows machine and stick it on the Internet, within minutes it's compromised, and it's got spyware and malware crawling in it. Because the 'Net is just now crawling with this stuff, we're never going to get rid of it. It's just - it's part of the 'Net ecosystem.

Leo: So you're always going to see this background radiation.

Steve: Yes.

Leo: Unless, of course, you put on a router, and then it suddenly gets silent. Gets very quiet.

Steve: Well, that's exactly what happens. As I was going to make the point, is that, if your computer with a software firewall is right on the Internet with no other protection, then the software firewall's popping up all the time. If, however, the moment you put a router on your Internet connection, everything else still works, but your software firewalls go quiet. They're not complaining anymore. They're not popping things up because nothing is coming inbound that's going to get past the router.

Leo: So you say the software firewall protects you against outbound traffic. Why would there be any outbound traffic? Isn't that my machine? What's coming from my machine?

Steve: Well, of course, that's the benefit of a software firewall, is that malware can get into your system and use your Internet connection without your knowledge.

Leo: So if your machine already is infected, the software firewall can notify you that something's going on under your nose.

Steve: Exactly. It will...

Leo: In fact, that's how you discovered spyware.

Steve: That's exactly right. I was beta testing the very first pre-release version of ZoneAlarm, and I had something on my machine which just completely surprised me. I think it was PKZIP for Windows briefly had some adware that, I mean, it wasn't malicious spyware, it was just adware that was bundled in. And I had installed it because I was wondering how it compared to WinZip. And I thought, well, I'll give this a try. Well, it brought some advertising software along with it which, without my knowledge or permission, was using my connection and connecting to remote servers. I don't know that it was doing anything bad. I doubt that it was. But the fact that this was happening said, whoa, you know, there's a need for knowing what's going on.

Leo: So you said something interesting. You said it's not a bad idea to have both a hardware router, acting as an inbound firewall, and a software firewall to protect you from outbound traffic. Do you need both?

Steve: I think it makes sense to have both.

Leo: There is a downside to software firewalls. Now, you mentioned one, which is that bad guys can turn them off, if they're sophisticated enough.

Steve: Right.

Leo: But the other is it does add to the complexity of your system. You're running system-level software that can cause problems and takes up CPU cycles and memory.

Steve: Well, and, yes. And I'm all for not adding stuff you don't need. Which is why one of the upcoming positive features of the Windows Vista OS is they've finally added an outbound filtering capability to the XP firewall, which will be on by default, and users will begin to have this sort of functionality we've always had to add add-ons in order to get. It'll be built into the OS and just inherently more stable.

Leo: The current Windows firewall isn't as effective?

Steve: No, in fact, the current Windows firewall is very much like a little NAT router on your own system. It allows outbound traffic to flow without being fettered at all, but it does block incoming traffic. So it's sort of like having a little NAT router right there. But of course all the hackers know how to turn it off.

Leo: Right. Is it fairly easy to do?

Steve: Oh, yeah. It's quite trivial, actually, to turn it off.

Leo: Oh, that's too bad.

Steve: I mean, and that's an inherent problem with a software firewall. But I don't see that changing anytime soon because to change Windows architecture would be just a huge, a huge revamp of the OS.

Leo: So if you've got a router, no point in using the Windows firewall. It's not giving you any additional protection. But you might want to run something like ZoneAlarm, my personal favorite right now. I think you were the one who told me about it, is the Sygate personal edition, the free Sygate firewall?

Steve: I like Sygate. I like - actually my favorite two are the Kerio or the Tiny personal firewall.

Leo: Tiny's very good, yeah.

Steve: And of course Sygate just got purchased by Symantec.

Leo: Right.

Steve: So it's going to be gone here before long.

Leo: It won't be free anymore, yeah.

Steve: Don't know if you can still get it.

Leo: Right. So Tiny or Kerio. Is it K-e...

Steve: K-e-r-i-o.

Leo: ...r-i-o, all right. So those are two. And they're free?

Steve: Yes, they have free, and then they have commercial editions. But the free ones work just fine.

Leo: I have to admit, I don't run an outbound firewall. I just trust that my NAT router is protecting me. And I guess, if you're pretty sure you're not infected by spyware or malware of some kind, that's probably okay.

Steve: Actually, Leo, I don't either.

Leo: Oh. You make me feel better because I don't want that additional complexity and...

Steve: But, see, I also don't have antivirus or anti-spyware of any kind.

Leo: But you're very careful about what you do.

Steve: I'm, yeah, the term would be "anal." I mean, I am so careful. Nothing could make me open a file attachment in email. I mean, just nothing.

Leo: No.

Steve: I also do something which is uncommon, which is to surf with IE. I still use Internet Explorer, but it's locked down so that it won't run any scripting or do anything unless I explicitly permit it on a per-site basis.

Leo: We have the instructions that you gave me some time ago for doing that on my radio show website. I will put a link to that in the show notes so that people can - it involves trusted zones and protecting yourself that way. And it's kind of a pain in the butt, to be honest with you, Steve, I mean...

Steve: I know. I know.

Leo: That's the nature of security.

Steve: It really is. There isn't a way to be out there exposed on the Internet and be safe. So you've just got to keep your guard up.

Leo: So we've talked a little bit about, just to recap, the fact that a router makes a very good inbound firewall. If you want further protection, a software firewall will protect you against outbound traffic. There is an exception, though. Routers, in order to do some things on the Internet, you have to poke a hole in the router.

Steve: Correct.

Leo: Does that compromise your security?

Steve: Well, it potentially does. And, in fact, it's the one caveat and the caution that I try to always remind people about. And that's this thing called Universal Plug and Play. This was a standard that Microsoft created which first appeared in XP. And of course it had all kinds of problems and exploits. In fact, it's why I created by UnPlug n' Pray freeware, to shut this off on the XP side. But that's different than shutting it off on the router side. What Unplug and Play - I'm sorry. What Universal Plug and Play, which is what it's called on the router, does is it allows any computer behind the router to ask for holes to be opened up so that this unsolicited traffic that we are talking about the router being so good about blocking, to allow the unsolicited traffic to actually pass through the router, even though it's not a conversation or a connection that has been initiated from behind the router. So it is a hole that traffic is allowed to come through, and then routed to a specific machine. This is important for, in some cases, for peer-to-peer file sharing, but mostly for things like Instant Messaging clients, where you want to be able to be part of a peer-to-peer network. You want to be able to receive incoming messages into your network. The problem, of course, is that Instant Messaging is replete with all kinds of malicious software, you know, malware, spyware, viruses, there's all kinds of problems and security problems with Instant Messaging that users need to be aware of. So contemporary routers have - they all have something called Universal Plug and Play. If you don't know you need it, turn it off.

Leo: This is essentially what it's doing, is automatically port-forwarding.

Steve: Well, it's automating the configuration of the router. But there's no security associated with it. You don't get a pop-up; you get no notice whatsoever. And, in fact, even if you look at the user interface, you know, how you're able to go to a sort of a virtual website and web pages the router creates, you can look at that, and it doesn't even show you what port-forwarding has been configured by the software behind your back.

Leo: It may be turned on without your knowledge, without warning. And there's no way of knowing what was turned on.

Steve: Correct. And...

Leo: If I turn off UPnP in my router settings, does it turn off all the forwarding that's been done?

Steve: I would turn it off, and then I would restart or reset the router so that it's going to come up fresh and clean.

Leo: Oh, interesting. Because it may, in fact, retain some of those port-forwarding settings. Now, frequently people will do port-forwarding intentionally. If I want to use BitTorrent or MSN Messenger, I will, in order to use it, I will have to do some port-forwarding. I will have to open up some holes in my router. But at least I'm doing that explicitly.

Steve: Well, and, in fact, yes. When you and I were using Skype for these conferences before, I had to deliberately open a port through my router so that a friend - actually, it wasn't you that I had a problem with. It was someone else who had a VPN router that wasn't peer-to-peer friendly. And so I had to open my side up so that Skype was able to hook us up directly, and we were able to get a good connection.

Leo: Oh, interesting, okay. So there are times when you do do this. But at least you've done it explicitly. You know it's being done, and it's not some malware that's doing it, it's you.

Steve: Well, that's exactly the problem, is that malware will start becoming - and as far as I know, there isn't any yet, but we might as well be ahead of the curve this time. Malware will start issuing UPnP commands to reach out to people's routers, as routers become more popular, in order to open holes back into the malware, so that, for example, traditional trojans are able to operate. Because a trojan that would normally be functional will be blocked by a router. No one will be able to call in to the trojan as they used to.

Leo: Well, so I'm going to now extend our list of things that you should do. So we said you should have a router. You might want to have a software firewall, as well. You should, on this router, you should turn off Universal Plug and Play.

Steve: And then restart the router.

Leo: Restart the router. And one more thing I'll add, which I know you would add, but is that you should change the password on the router because all of them have default passwords which are well known.

Steve: Well, and that's the other thing, too, is that some routers have an option for WAN management, that is, W-A-N, stands for Wide Area Network; as opposed to LAN, which is the Local Area Network. In other words, some routers allow you to have administrative access from the Internet side.

Leo: Oh, boy.

Steve: Unless you really know that you need that, you'd absolutely want to turn that off. So if you, as you're browsing through your router configuration, you see WAN Management is enabled, absolutely turn that off.

Leo: And it's often enabled by default, it seems.

Steve: It is, and it's just crazy.

Leo: I think that what happens is a manufacturer wants as few support calls as possible. So they really configure these to be as loose and open as possible because they don't want people to call and say, well, I can't do this.

Steve: Right.

Leo: But of course you don't want to be able to do that unless you have a specific need. There's one other thing that people often do and have problems with routers, and that is run a server, particularly game servers, but there are other kinds of servers, a web server, that you might want to run. And routers are going to get in the way of those, as well, aren't they.

Steve: Well, that brings up a really interesting issue because that's the so-called "DMZ," the Demilitarized Zone, as it's called on routers. And the idea is that you can designate one of your machines to be the machine that unsolicited traffic goes to on purpose. Or, as we've said, you could just forward specific ports. For example, you were just saying, you know, people might want to run a game server. The problem with that is, and it's a serious security issue, is that the router is essentially making that machine part of your LAN. That is, you're allowing unsolicited traffic and trusting this traffic to come into your LAN, aimed at a specific machine. But once it gets there, if something were malicious that got into that machine you deliberately opened, that machine has access to all the other computers in your network. It's on your LAN.

So one trick that I have never seen anywhere is you can actually use two NAT routers. You're able to put NAT routers in series. So that, for example, you'd have an external NAT router and an internal NAT router. And you might want to put this link on the show notes. It's www.grc.com/nat/nat.htm. I've put together a page where I've drawn some diagrams to make this a little more clear and explained it carefully because it's a very cool idea. The idea is that you could put your game server on the external NAT, on the NAT that's connected to the Internet. And then, rather than putting the rest of your computers on the same NAT router, put them on their own NAT router and then hook that second NAT router to the first one, essentially in series.

Leo: So the first one's passing all traffic through. But the second one's blocking traffic from those computers you want to keep off the DMZ.

Steve: Well, and it's also - so no longer is your game server on your LAN. Essentially...

Leo: It's separated, as well.

Steve: It's sort of on, like, WAN 2. It's sort of on a separate network. And again, you're able to access the game server because you're going upstream. You're going through the NAT outbound, which is where the game server is, on the outside of your second NAT; but it can't get to you. So if something were to compromise it, you are safe. Another cool application would be, if you wanted to mess with wireless, but you were still, you know, you had, like, first-generation wireless technology with WEP security - which is actually an oxymoron - as opposed to the WPA security, which is really good security, what you could do is you could have your wireless router on the Internet, and then have a standard non-wireless router which runs your main network, your wired network, and you plug your second router into the wireless router. The beauty of that is that no wireless traffic is then able to reach into your network because that second NAT router blocks everything trying to come into it.

Leo: So conceptually these both are the same idea, which is that anything that's at risk is isolated from the rest of your network by this second router, which provides a barrier against these at-risk routers or computers.

Steve: Right. In fact, you can sort of think of a NAT router sort of like a one-way valve. Data can flow out of it without any trouble. But unsolicited data is unable to flow back in. It's sort of like a backflow valve. It won't let the data come in the other direction. And you can chain them. You can put them in series and come up with, you know, interesting network topologies to really increase the overall security of your system. Say, for example, you were a family, and you had a bunch of teenagers, all with their own computers.

Leo: Isolate them.

Steve: Well, no. No, actually - well, essentially. So, and then you've got Mom and Dad's adult computer, where the banking and the stock portfolio and all that stuff is. You just - you connect it to the family router through its own NAT router, giving it its own little one-way valve. It's able, you know, the adult computer, Mom and Dad's computer could still get out to the Internet. But nothing that infects the kids' computers and their LAN has an opportunity to come back in to you.

Leo: That's a really useful metaphor for how a router works. It's a one-way valve. Outgoing traffic's allowed, but unknown incoming traffic is always blocked.

Steve: Yup.

Leo: And then, if you conceptually understand that, then I think it makes sense - this more advanced description of DMZs and so forth makes a little bit more sense.

Steve: Yeah, it's very cool.

Leo: Steve, great stuff. And I will this time put together a list of links on the show notes which are available at thisweekintech.com. A reminder to folks who subscribe to all of our podcasts - This Week in Tech, Security Now!, Radio Leo, the Laporte Report, and the KFI podcast - that we've moved them off FeedBurner and onto their own RSS feeds, so that - you probably won't have to do anything. Most RSS software is going to be smart enough. FeedBurner has an automatic redirect. The feed software that you use will, in all likelihood, see that redirect and change the URL for you. If it doesn't, just so you know, the new feed for this podcast is leo.am/podcasts/sn, for Security Now!.

And of course we're still hosted - and gratefully hosted - by AOL's Podcast Channel on AOL Radio at aolmusic.com. Without them, there'd be no way we could do these podcasts pro bono. But they absorb the costs of the immense amount of bandwidth; we don't have to. Thank you, AOL.

And thank you, Steve, for another great description. I think routers are one of the most important tools in the security arsenal. And I think everybody should have one. If you have a broadband connection, get a router. I feel bad for people with dialup because, I mean, there's the WiFlyer, and there's some dialup routers, but they're very expensive.

Steve: Well, and the only advantage, really, is they're not on the 'Net 24/7.

Leo: Right.

Steve: So they're only connected briefly. And of course routers have come down so that they're below 50 bucks now.

Leo: Yeah.

Steve: It's a great little security appliance.

Leo: Even if you only have one computer connected to a DSL or cable modem, a router is pretty much a must-have.

Steve: Right.

Leo: Oh, and another nice feature of Security Now!, Steve Gibson has decided to foot the bill for transcripts. So does that mean we'll have full text of each podcast, Steve?

Steve: Each podcast, about 24 hours after it goes public, will have both a text and a ready-to-print PDF file that are very small, and it allows people just to get them in text if they want to.

Leo: Wow, that's really great. I mean, it underscores that this is really a pro bono effort on your part to just get the word out about security. And that's one thing you've done all along with GRC.com. So the web page is GRC.com/securitynow?

Steve: .htm.

Leo: .htm. Thank you, Steve Gibson. We'll see you at GRC.com and back here again next Thursday for Security Now!.