



RUNAS RADIO



<http://www.runasradio.com>



RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Text Transcript of Show #013
(Transcription services provided by [PWOP Productions](#))



Jeff Sigman Gives Us Network Access Protection!
July 4, 2007



Jeff Sigman Gives Us Network Access Protection! July 4, 2007

[Music]

Carl Franklin: From runasradio.com, you're listening to RunAs Radio, the weekly Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing show #13, with guest Jeff Sigman, recorded Thursday, June 7, 2007, at TechEd 2007 in Orlando, Florida. RunAs Radio is produced each week by PWOP Productions, offering professional media and podcasting services online at pwop.com.

Richard Campbell: Hi there. You're listening to RunAs Radio and this is your host, Richard Campbell, and with me Greg Hughes.

Greg Hughes: Hey Richard. How are you doing?

Richard Campbell: I'm really well and having a good time. We're coming in to summer.

Greg Hughes: Yeah.

Richard Campbell: And we now have reached the end of our TechEd shows.

Greg Hughes: Yeah. This is the last of the shows that we picked up and recorded on the floor at TechEd.

Richard Campbell: Right, in Orlando. We meant to get four and just couldn't seem to squeeze that fourth one out.

Greg Hughes: Well, logistically, that's a fast-paced show with an awful lot of content and really, really busy people.

Richard Campbell: Yeah. It's funny how you really couldn't plan a lot of that stuff in advanced. Most everything we had that worked out at TechEd we did on the floor right then and there.

Greg Hughes: Absolutely. It was on the fly. I know that I spent a lot of time on my feet. Boy, I'll tell you, a couple of days there, it as painful by the time I was done running around and really talking to people and trying to find those really great nuggets of information that I thought we would talk about it and you thought would make a great show.

Richard Campbell: I agree. Always a challenge to find the right guy and the important bit of information you need to know about these technologies because I can't explain everything in half an hour. I got to get to the key things.

Greg Hughes: Right, and there are a lot of great things, but really trying to focus on what is it for an IT pro, somebody working in or running an IT department or maybe the one-person IT department, what are those things that they can take away. We've talked about IIS7. We talked about CardSpace and our final topic out of TechEd is one that I think is really, really interesting both from an IT and a security standpoint and it's something that isn't quite rocket science to do, but with Windows Server 2008, the new Network Access Protection Capabilities are really, really cool.

Richard Campbell: You're right. It's not that complicated, but it really took a lot of bits hanging together to make it all work. The new client operating system and the new features in the server operating system, it's just sort of a coalescing of these things. I think you've got an insight into this early on too. We saw this over two years ago, Microsoft was saying, "This is what we want to do." At the time, I thought, "I don't know how you're gonna make it happen," but it's really exciting to see it here.

Greg Hughes: When Microsoft was first thinking about and starting to do some of the betas that ended up being Windows Server 2003 R2, there's sort of a light version of Network Access Protection. With Windows Server 2008, which is available in beta 3, so people can download this and try it out, the new Network Access Protection just has some terrific stuff, but you know what? We don't need to explain that.

Richard Campbell: No.

Greg Hughes: Because it was explained to us. So, why don't we get to that?

Richard Campbell: Yeah. Let's go to Jeff.

Richard Campbell: Well, here we are, sitting in the fishbowl again recording another RunAs Radio at the Virtual TechEd booth around the back in the editing studio. I'm here with Greg.

Greg Hughes: How are you doing, Richard?



Jeff Sigman Gives Us Network Access Protection!
July 4, 2007

Richard Campbell: And we're sitting with Jeff Sigman. Hi, Jeff. Nice to meet you.

Jeff Sigman: Nice to meet you, Richard.

Richard Campbell: And you're working on technology I've been fascinated by awhile, which is Network Access Protection.

Jeff Sigman: It is an exciting new area of Server 2008. It's one of the key features that the product is adding to our suite of components within Windows. I'm really excited to be on the team.

Richard Campbell: Let's start at the beginning.

Jeff Sigman: All right. I'll rewind three years ago and I'm on the Windows Dev team. We're trying to look at how do we give the IT pro the ability to create policy around who can come on the network and once they're on the network, are they healthy or not, what does that healthy concept mean, and then what do we do with them once we determined they're not healthy?

Richard Campbell: This strikes me as the laptop problem, right?

Jeff Sigman: Yes.

Richard Campbell: I take my laptop from work, I take it home.

Jeff Sigman: You go get Blaster. Thanks for doing that.

Richard Campbell: Yeah.

Jeff Sigman: And you bring it back.

Richard Campbell: Yeah. I let my kid play on it or something along those lines. You don't know what happens in the home network and then I bring it back to the office.

Jeff Sigman: Exactly.

Richard Campbell: Should I really have the same privileges I had when I left? Or at least you got to have some judgment as to what's going to happen.

Jeff Sigman: Exactly. For me, our own Microsoft IT shop had to figure out the pre-NAP world, pre-Network Access Protection world, and their method was they end up shutting down your office. They killed the whole port in your office and you have to make a helpdesk call and you have to promise to that engineer on the phone that you'll fix whatever they found the problem. Right there, NAP, we had...

Greg Hughes: Before you plug it back into the wire.

Jeff Sigman: Exactly, and so they had flipped me on. They trust me that I'd fix it. With NAP, we knew immediately we had to be able to auto remediate we call it. That means turn the firewall back on automatically, fix Windows update, make sure he gets the critical patches, make sure his AV has the latest signatures, and then we let him back on automatically. Hopefully, he never even has to do anything manually and he never picks up the phone and calls helpdesk.

Greg Hughes: That's a lot of manual intervention though. It also doesn't really address the issue of the computers that you don't have patching control over. What if a partner or a visitor comes in with a laptop and just plugs it into your network trying to get an Internet connection?

Jeff Sigman: That's one of the great things we do. We do support. We have NAP plus 802.1X. That's switch-based, hardware-based NAP where literally you have a communication channel between the switch and Network Policy Server, which is our NAP server piece and Windows Server 2008. We will tell the switch put this guy in VLAN X or VLAN 1, 2, or 3 and the VLANs are configured such that he can only get to a limited set of resources. Let's say, you only want guest to be able to get to the Internet. We can say VLAN 3 can only get to the proxy. That's it. So, he comes in, you don't know who he is or he's unhealthy. You know who he is and he's unhealthy. You dumped him onto this VLAN. Network Policy Server tells the switch to do this. Now, you can only get to this limited number of resources.

Richard Campbell: What I like about that is it's not just a no.

Jeff Sigman: Exactly.



Jeff Sigman Gives Us Network Access Protection! July 4, 2007

Richard Campbell: It's at least something.

Jeff Sigman: All we had pre-NAP in the Microsoft world was a no. We're going to shut down your port...

Richard Campbell: And that's it.

Jeff Sigman: And you call helpdesk.

Richard Campbell: You get nothing.

Jeff Sigman: Yeah, that's it. Exactly.

Richard Campbell: It also occurs to me suddenly that we always talk about the perversion of SMTP and corruption of HTTP, but even DHCP and DNS, those protocols are just as weak in terms of security and in terms of policy as the other protocols.

Jeff Sigman: Exactly.

Richard Campbell: We just don't think of them as being part of the problem.

Jeff Sigman: Exactly.

Richard Campbell: This idea that we need to know more before I hand you an IP address. What IP address I want to hand you is going to depend on what kind of *cred* you can give me.

Jeff Sigman: Exactly. One of the common misconceptions about NAP that I wanted to make sure I got to emphasize is that some people think it's only based on DHCP. NAP is based on DHCP. That's actually not true. We support NAP802.1X, NAP IPsec, NAP Terminal Server Gateway, and NAP VPN. Those are the ones out of the box Server 2008 that we support.

Greg Hughes: So, a lot of different options for it.

Jeff Sigman: Yeah.

Greg Hughes: And relative levels of strength that you can apply now then.

Jeff Sigman: You can combine them. We find our customers, our advanced tapped customers we call them, the ones that are putting Server 2008 in

production already, they're combining. They're doing NAP, DHCP, plus IPsec or 802.1X plus IPsec.

Greg Hughes: Do IPsec, this is point-to-point IPsec tunnels?

Jeff Sigman: Actually, it's transport mode.

Greg Hughes: Okay.

Jeff Sigman: It is just no tunnels, but you have a credential on your box, a certificate. NAP, if you're healthy puts the certificate there. If you're unhealthy, it rips the certificate off. The minute that you become unhealthy, you no longer have a credential to talk to the server you're attempting to talk to.

Greg Hughes: So, I'm not creating a situation where I can't monitor my network anymore. I can still pass all the information across the network in a way that I can keep track of and monitor and sniff and do all that?

Jeff Sigman: Exactly. Well, Microsoft IT doesn't do IPsec encryption. We do authenticated header, meaning we know who you are, but we don't want to encrypt the traffic. You can still debug that. You can still sniff that in and look at it.

Greg Hughes: Sure, but from security standpoint, I think there's some real value in that. On Richard's point, I think you made a good point. We were talking earlier about DHCP and DNS and all these protocols that are made by very optimistic loving people out there that came up with a great idea.

Jeff Sigman: The idealistic world, yeah.

Greg Hughes: But didn't really look at it from a threat-modeling perspective and NAP has really come out of the need to be able to exercise a level of control that those protocols just don't allow.

Richard Campbell: And I'm thinking about doing just what you described there by assigning on VLAN and so forth. That's not actually communicating with the switch so much as controlling the DHCP server and those kinds of services, right?



Jeff Sigman Gives Us Network Access Protection! July 4, 2007

Jeff Sigman: Well, it's kind of layered. You're doing both.

Richard Campbell: Right. I'm just thinking about what gear to buy to make NAP work for me.

Jeff Sigman: Okay. The cheapest and quickest, you can set it up in five minutes, is NAP DHCP. You simply need one 2008 box that runs DHCP and Network Policy Server and, boom, you have NAP working. Then go beyond that to get an 802.1X working, you have to have a switch that supports dynamic VLAN switching with RADIUS.

Greg Hughes: Let's start with a simple NAP DHCP.

Jeff Sigman: Right, the simplest we have.

Greg Hughes: Say that three times fast.

Jeff Sigman: Okay.

Greg Hughes: What clients are going to work on that? Are there certain ones that won't work?

Jeff Sigman: Vista out of the box when it's shipped and we support XP.

Richard Campbell: Is that all additions of Vista?

Jeff Sigman: Yes.

Richard Campbell: Really? All of them? Home Editions?

Jeff Sigman: It's installed on all editions and off by default on all editions.

Richard Campbell: Wow!

Jeff Sigman: Yeah.

Richard Campbell: But you can turn it on, on any edition at all?

Jeff Sigman: Any edition can turn it on.

Richard Campbell: And there are XP editions as well or just Pro I presume?

Jeff Sigman: Well, right now we have a beta of the XP client. I can provide the blog, by the way, at the end and people can email me to get the beta if they would like it. It's going to ship in XP Service Pack 3 and when you install XP Service Pack 3, it'll be the same experience as Vista. It will be there and off.

Greg Hughes: Via group policy or similar scripting mechanisms?

Jeff Sigman: Via group policy.

Greg Hughes: We can turn that on and exercise control over that?

Jeff Sigman: 100% yes.

Richard Campbell: I'm suddenly jumping all over this for home use like if we get a Home Server Edition to support NAP, just the whole idea that when your friend comes over and uses the wireless, he can't mess up your MP3 collection.

Jeff Sigman: Or your kids.

Richard Campbell: Or your kids.

Jeff Sigman: Yeah. You have firewall auto remediation on. Your kid turns it off and we've just flipped it right back on.

Greg Hughes: Exactly.

Richard Campbell: And I flatly admit that I do apply group policy to my children.

Jeff Sigman: You do?

Richard Campbell: But the advantage of being heavily involved with Microsoft is I have all the MSDN licenses and stuff so I'm allowed to run these servers and so I have a domain at home, but that makes me crazy. It's also a serious administration headache for a home system. The idea that NAP would actually be modeled so that somebody who has a home level server, which is not going to be a huge number of customers, but it's not going to be zero either, can take advantage of "Hey, all your machines are behaving and all your friends are behaving on your network."



Jeff Sigman Gives Us Network Access Protection!
July 4, 2007

Jeff Sigman: Right.

Greg Hughes: Let's talk about what healthy means.

Jeff Sigman: Okay. Good point.

Greg Hughes: And then I'd like to maybe jump back into the different, we talked about the DHCP option and a little detail on each of those, but you've mentioned a couple of times "if your machine's not healthy."

Jeff Sigman: Right.

Greg Hughes: What are we talking about there?

Jeff Sigman: I'll define out of the box healthy.

Greg Hughes: All right.

Jeff Sigman: Meaning what you get for free or, so to speak, included with Windows. We wrap around the Windows Security Center, that is, firewall on/off, antivirus on or off, signatures up to date, those things.

Greg Hughes: Gotcha.

Jeff Sigman: You can create Policy in Server 2008 without any additional software around all of that.

Greg Hughes: Okay.

Jeff Sigman: 90% of it we can auto remediate, meaning we can just flip it back on whether you want us to or not, if the IT guy wants us to. The thing we can't do automatically is third party AV. Since we didn't write the AV product, we do not know how to turn it on or off or tweak the signature update settings. That's something where NAP is improved by third party integration with NAP. We have over 115 partners working with NAP. We have all the big players in AV and firewall working with us. To actually make a rich NAP experience for the IT guy, if he's a McAfee shop let's say, he gets McAfee's version that integrates with NAP. He installs it on the server, rolls the update out to the clients. Now, he can auto remediate even AV or their firewall product.

Greg Hughes: I see. Are there any antivirus vendors that are already integrated with NAP in their releases?

Jeff Sigman: I know of none that are shipping their software today, but the two I've personally seen are Trend Micro. They gave us a beta of it for RSA Con in San Francisco. McAfee showed their beta as well.

Greg Hughes: Oh, okay. Let's go back to the different flavors, if you will, of doing NAP.

Jeff Sigman: Okay. We call them enforcements.

Greg Hughes: There we go, different NAP enforcement levels or whatever we're going to call them. We've talked about the DHCP.

Jeff Sigman: DHCP.

Greg Hughes: I kind of get that. What are some of the other options in that network?

Jeff Sigman: I mentioned briefly about IPsec and there's a credential. It's a certificate that we remove and add to the box as you're healthy or not.

Richard Campbell: That is a clever solution!

Jeff Sigman: Yes.

Richard Campbell: Wow. I just sort of go "bing!" No software needs to understand NAP at all.

Jeff Sigman: Yeah, exactly.

Richard Campbell: All these different products.

Jeff Sigman: You mean like Outlook or something.

Richard Campbell: IE...

Jeff Sigman: Yeah.

Richard Campbell: Any of these things is dependent on certificates. You just yank the certificate.



Jeff Sigman Gives Us Network Access Protection!
July 4, 2007

Jeff Sigman: Exactly.

Richard Campbell: And all sorts of stuff are just going to go away.

Jeff Sigman: That "bing" you just had was the BillG demo we gave where Outlook is connected. The guy goes unhealthy and you'll see Outlook just disconnects.

Richard Campbell: Just disconnects.

Jeff Sigman: And then we turn the firewall back on and then Outlook just connects again. That's the ideal scene that we have.

Richard Campbell: Yeah, that's pretty cool. What a clever -- it's just one step removed from the application.

Jeff Sigman: Right, exactly.

Richard Campbell: One of the server's pieces...

Jeff Sigman: The plumbing.

Richard Campbell: That everything else is supported to.

Jeff Sigman: Exactly.

Greg Hughes: It's using the plumbing that was built in the second layer to deal with the Pollyanna protocols, if you will, that work really well, but that really weren't -- one of the reasons IPsec came around and one of the big benefits of it is you can exercise that kind of control.

Jeff Sigman: Exactly.

Greg Hughes: I think it's cool that you're using existing plumbing to do the job really well.

Jeff Sigman: We wanted to pull it off simply and we wanted to make it something you could create policies around IPsec.

Greg Hughes: Right. Without reinventing the wheel, so to speak.

Jeff Sigman: Exactly.

Greg Hughes: Yeah.

Jeff Sigman: I guess the one I haven't mentioned is RRS, Routing and Remote Access. On that one, VPN clients come in and if they go unhealthy, we leave them connected. We put a filter down on RRS and we say the guy can only get to this set of IPs. When he goes healthy, we remove that filter and he's got full flow connectivity.

Greg Hughes: Is this with Microsoft VPNs?

Jeff Sigman: Right.

Greg Hughes: Is it integrated with other third party VPNS? How does that work?

Jeff Sigman: The one we support today from Microsoft is the Routing and Remote Access in Server 2008. Just like DHCP, it is currently DHCP server inside of Server 2008. Now, two weeks ago, the TCG, the standards body around security, announced that the Statement of Health Protocol, the one we use to communicate the health of the client, has become a standard. What that means is someone could write their own third party DHCP server and do NAP, likewise, RS, SSL, VPN. People could write a server that supported our Statement of Health Protocol and it would just interop with Vista and XP, boom. That's the beauty of us becoming the standard is that now it's a published thing anybody can read. You don't have to license it. You can just interoperate.

Greg Hughes: It's free open standard for all to use.

Jeff Sigman: Exactly.

Greg Hughes: One of the things I really appreciate, Richard, about Microsoft over the last few years has been that move toward more open and accessible standards that others can use as opposed to being proprietary.

Richard Campbell: Yeah. There is far less proprietary technology these days. You're building more software around these standards and it seems like the standards are getting a chance to mature before you start tearing off on them too, so we have more chance of actually implementing against it.



Jeff Sigman Gives Us Network Access Protection!
July 4, 2007

Jeff Sigman: Exactly. The coolest thing about NAP for me is the ecosystem. Working with a third party that I typically didn't get to work with, you now have Trend Micro or whomever getting excited about NAP, building on our public API and then getting to sell more software because they integrate with NAP. It all helps move NAP forward. I love that.

Richard Campbell: When I think ecosystem, I think, "What's gonna happen to my MacBook Pros?" Are they going to be able to drop in on this?

Jeff Sigman: Yeah. Ah, I've got some hot news.

Richard Campbell: Ooh! Hit me with the hot news.

Jeff Sigman: Hot news is Avenda Systems for the Interop conference in Las Vegas wrote a NAP client on Linux in 1.5 weeks, a week-and-a-half they wrote a NAP client. They showed it at Interop Vegas and it just completely interoperated with everything, our Network Policy Server, Vista, XP, it just worked.

Greg Hughes: Again, the beauty of sharing and open standards that are simple, not only does it make it possible, it quite often makes it a lot simpler.

Richard Campbell: The big thing here is Microsoft didn't have to build it...

Jeff Sigman: Right.

Richard Campbell: And Apple didn't have to build it.

Jeff Sigman: Exactly.

Richard Campbell: Other people were motivated to write the software. They would do everything they need to do to make it happen.

Jeff Sigman: Right. We've had two companies say, "We want to write your Mac NAP client."

Richard Campbell: Nice.

Jeff Sigman: We're pumping them up. Go for it, guys. We'd love to have it.

Richard Campbell: You talked about NAP RS, which was Routing Services?

Jeff Sigman: Routing and Remote Access.

Richard Campbell: Routing and Remote Access, but you also said NAP VPN.

Jeff Sigman: Yes.

Richard Campbell: Two different things?

Jeff Sigman: No. The VPN is terminated by Routing and Remote Access. It is our VPN Server. You can call it the same thing.

Richard Campbell: Okay. What was the other one? Terminal Services?

Jeff Sigman: Terminal Server Gateway.

Richard Campbell: Terminal Server Gateway. I immediately thought this is something about terminal services.

Jeff Sigman: Right. This is a brand new feature in 2008. You'll have to pardon my lack of knowledge. I'll tell you what I know. You basically, instead of your desktop, you are *terminal servering* an app. Instead of just sharing the desktop, you have an app that appears to be running locally, but it's going through the RTP to a backend and you think you're running it. When you authenticate with that, that guy checks your client health, they integrate with NAP, and if you're not healthy it reacts to that and you won't be able to connect to that app until your client is healthy.

Greg Hughes: That's an interesting way to gate that.

Jeff Sigman: You can almost call it app-based NAP, almost.

Richard Campbell: Yeah, app-based NAP. The interesting side effect of the new terminal services ability, the ability to only share the app, is it becomes harder and harder to know you're making remote connections. Where does the app actually live and what are the consequences of you using it? NAP becomes more essential in that scenario because the



Jeff Sigman Gives Us Network Access Protection! July 4, 2007

user who may have the best intentions in the world is unaware of the threat he serves.

Jeff Sigman: Correct. I can't wait to see where that goes. I can't wait to see the adoption of that feature and see if app-based NAP becomes something that people start demanding more of.

Richard Campbell: Yeah, it's an interesting thought. In some way, it's easier to just go down to the layer 2 stuff, deal with my IPsec, make my connection go away or my ability to authenticate to go away rather than fight with anything else.

Greg Hughes: Well, to a certain extent, but if you were -- I'm sort of thinking out loud here. If I have Outlook that needs to connect to an Exchange Server from the Internet, then NAP for my client that's running Outlook that is connecting to the Exchange Server remotely over HTTPS, that might actually be something that would be really useful to make sure that my client is clean before I allow a connection.

Jeff Sigman: We're actually in talks with the Office team, we're in talks with the Windows Mobile guys because then the next thing you start thinking about is why isn't my cell phone have a NAP client on it?

Greg Hughes: Sure. Or if I have an extranet that's based on SharePoint, I want to be able to do direct SharePoint integration as opposed to just basic web UI, then maybe I can exercise some control in that area. I can see where this could be something that's really interesting as it grows over time. The term deperimeterization has become one of those catch phrases that's out there, but this is one of the types of things Network Access Protection is really key in terms of flavor of what it takes to deperimeterize and not rely on the firewall anymore, but rather to secure the endpoint, to secure where the data lives and to redefine your perimeter.

Richard Campbell: Yeah. As soon as you say reperimeterize or deperimeterize, I start thinking about those great social experiments where guys dropped USB keys in the parking lot and people consistently picked them up and plugged them in.

Jeff Sigman: Right. What happens there?

Richard Campbell: The idea that every access point into your network has the ability to evaluate its risk, to be able to be tested for that vulnerability and then mitigate the risk or at least *containerize* it.

Jeff Sigman: Exactly. Let that unknown -- the IT pros I've met at the show, in looking into the future, they want to get better control on that question mark, all these nodes out there that they feel loss of control. It's mainly unmanaged guys.

Richard Campbell: Yeah, these out of control vectors that are just easy ways to get yourself into trouble.

Greg Hughes: Okay. If I want to implement this today...

Jeff Sigman: Yes.

Greg Hughes: Say I'm an Active Directory shop. I have a Windows domain. I'm running Windows Server 2003. I want to give this a try. Help us all understand what it takes to be able to put this into place and start playing with it right now, find out what it's all about.

Jeff Sigman: Great question. My motto for the show is "Try NAP now."

Greg Hughes: Okay.

Jeff Sigman: That's great. We have five step by step guides sitting on microsoft.com/nap and it's also via the blog.

Greg Hughes: NAP, right?

Jeff Sigman: Right.

Greg Hughes: Okay.

Jeff Sigman: The thing to do is these are lab guides. How do I set up a lab at my company to show me that NAP works and what it does? You can follow these guides with beta 3, either the beta 3 you got at TechEd or beta 3, it's actually publicly downloadable on the web.

Greg Hughes: This is Window Server 2008 beta 3?



Jeff Sigman Gives Us Network Access Protection! July 4, 2007

Jeff Sigman: Exactly.

Greg Hughes: Cool T-shirts, by the way.

Jeff Sigman: Yes. You can use Vista right out of the box or you can, like I said, contact me via email and get that beta client of NAP, the NAP client for XP.

Richard Campbell: You want to share that email address now?

Jeff Sigman: Sure. It is jeff.sigman@microsoft.com.

Richard Campbell: So, you're going to get emails from folks...

Jeff Sigman: Bring it on!

Richard Campbell: They're going to be that client.

Jeff Sigman: Bring it on.

Richard Campbell: I really think it would be interesting to see more of these things being tested out in different environments.

Jeff Sigman: I'm getting a lot of positive feedback. I'm also getting constructive criticism. They'll say, "Hey, I couldn't get it working in this way." I'll do exchanges with them and find out, "Ah, there's something wrong with their switch," and we got that ironed out. I love the feedback.

Greg Hughes: This is something we've been talking about. I know that I've been wishing for it and the community's been talking about it for years. The whole concept, some of the old terminology, I think it's probably the same stuff just with new names on it, but the idea of quarantine zones and network quarantines and being able to control when somebody's coming in remotely whether or not they have the clean machines so that you can let them in. It's good to see this coming to fruition and productized and actually going out as something that's going to be a formally supported piece of commercial software as opposed to a proof of concept package that's handed out on Windows 2003 Server with a set of limited functionality.

Jeff Sigman: Right. I know what you're talking about actually.

Greg Hughes: It sounds like your team has come long, long ways...

Jeff Sigman: We have.

Greg Hughes: Relatively quickly.

Jeff Sigman: We have. We went from RQS/RQC to where I'm sitting today in three years. I'm really proud of actually what we've gotten done and I hope, I hope the world loves it. I really hope they do.

Richard Campbell: Well, I'm not ready to give up on this topic yet because there are a couple more things I want to pound on a bit.

Jeff Sigman: Okay.

Richard Campbell: VPN is just a huge issue and huge at discussions and obviously when you've got a remote guy connecting into your network as if he is there, NAP is obviously essential. You have no idea what's coming at you from that angle.

Jeff Sigman: Right.

Richard Campbell: I'm still trying to imagine how you're going to control what a guy can do without just cutting him out if he's got a non-NAP compliant machine and a VPN.

Jeff Sigman: I see. Well, the thing that we're telling people to do is the critical things to get themselves fixed up. Typically, that's either the WSS Server or however the guy gets patches through SMS. SMS actually integrates inside of NAP. SMS could go grab those patches over VPN, pull them down, and then he can declare himself healthy again.

Greg Hughes: And then drop the patches, right?

Richard Campbell: So, NAP's reaction to a non-compliant machine coming in via VPN will be to only open the services that could fix them.

Jeff Sigman: That's the best practice, yes.



Jeff Sigman Gives Us Network Access Protection!
July 4, 2007

Richard Campbell: Right. Could you actually go so far as redirect of some kind? How is a guy going to receive a notification that he's not compliant?

Jeff Sigman: You haven't seen my NAP demo.

Richard Campbell: I have not seen your NAP demo.

Jeff Sigman: Man!

Richard Campbell: You know, it's very tough to show a NAP demo on a radio show.

Jeff Sigman: It is.

Richard Campbell: You're going to have to walk me through this.

Jeff Sigman: Picture a bubble and this bubble says, "You do not meet the corporate standards," or "Your machine has been discovered to not meet corporate policy and your network access could be limited." That's the bubble. It comes up with the UI that says, "Here's exactly what's wrong and here's what you can do about it." It literally goes down to firewalls off, turn it on.

Greg Hughes: Oh okay. Right. Right.

Jeff Sigman: You can also brand it. IT shops can put their little logo. They can control the text that's on the banner. It says Microsoft IT at my company and then it has a URL, it's a fix-up help. That URL is something the IT guy pushes down to say, "Here are steps you can go through to fix yourself if we can't fix you automatically."

Greg Hughes: Another big question here, is Microsoft using this now?

Jeff Sigman: Yes, we are. Oh, can I tell the Microsoft story? This is a beautiful story.

Richard Campbell: Absolutely. I love a good dog food story.

Jeff Sigman: Okay. We're live across North America with NAP IPsec and NAP DHCP. We have around 60,000 to 80,000 nodes doing NAP. Guess

what we found? 20,000 machines across North America...

Greg Hughes: A lot of dirty machines.

Jeff Sigman: Weren't running either firewall or AV or both, 20,000.

Richard Campbell: Out of how many?

Jeff Sigman: 60,000 to 80,000.

Richard Campbell: So, 60,000 to 80,000 machines, a third.

Jeff Sigman: Who were not running AV or firewall.

Richard Campbell: Wow!

Jeff Sigman: One or the other or both.

Richard Campbell: You know what's interesting? As a guy who has been to dozens of Microsoft offices, I've never been able to get connectivity most of the time because the network has always been so locked down.

Jeff Sigman: Oh yeah.

Richard Campbell: I think an interesting side effect of having a product resource like NAP is that it's going to enable you to raise that barrier.

Jeff Sigman: Exactly.

Richard Campbell: More of your third party folks, your vendors and your visitors are going to be, "Please give me an IP address so I can get out. I don't want the rest of your network. I just want to get out."

Jeff Sigman: Exactly. Listen to this. Our IT shop thought of something that we never did in the product team. I'm one of the guys who wrote it. Here's something we never thought of. They turned it on in reporting mode only we call it so their policies never enforced anything across those 60,000 to 80,000...

Greg Hughes: You're just reporting your status? That's something that's NAP...



Jeff Sigman Gives Us Network Access Protection! July 4, 2007

Jeff Sigman: They locked it to SQL. That's it.

Greg Hughes: Something else NAP gives you, it's more than just enforcing the network policy, it also gives you a real world view in I would imagine close to real time...

Jeff Sigman: It is.

Greg Hughes: Of what your network actually looks like so you can actually have an idea of what the hell is the status of all of your machines.

Jeff Sigman: We didn't even have a concept of reporting mode. This guy said, "Oh, let's not enforce. Let's just report."

Richard Campbell: Yeah. I don't want to annoy anybody. I want to find out how bad the situation actually is.

Jeff Sigman: Then they built this graph out of SQL and it shows these 20,000 machines and then they go, "Okay, how the heck are we going to do this without talking to these people?" Then they turned NAP into we call it deferred enforcement. I call it probation. Basically what that is, is you put a date on the server that says, "We will quarantine you," or "We will restrict your access on this date," and they just set it ahead a year. We saw compliance. We saw unhealthy machines go from 20 to 10 in a week. Just by putting that bubble in their face, we fixed 10,000 machines over North America and then a month later, we're down to 1% or around 500 machines are not compliant.

Greg Hughes: All the power of having somebody know that you know.

Jeff Sigman: Exactly.

Richard Campbell: We know you've been misbehaving.

Jeff Sigman: Yeah. A year later, we have less than 500 machines non-healthy and we fixed our network without enforcing anybody.

Greg Hughes: And those machines that are non-healthy, you can exercise the level of control over them as necessary.

Jeff Sigman: Right. We know their Mac address. We know their IP. Sometimes we even know their name, their username. Guess what? They started calling helpdesk. This is where I'm going to mention a bug, which typically you don't do, but I think it's amusing. It turns out these 500 machines hit a WMI bug. If you know Security Center publishes into WMI states of various things. These machines had hit a WMI corruption and they could not tell that the firewall or AV was on or off, so they called helpdesk and helpdesk figures out that you can reset the repository of WMI. Now, these guys all go healthy, so we go down to zero.

Richard Campbell: The 500 were actually all...

Jeff Sigman: A bug.

Richard Campbell: All corrupted WMI.

Jeff Sigman: Exactly.

Richard Campbell: And so getting that corruption fixed up, got them reported properly, and hopefully goes away.

Jeff Sigman: Exactly. Then you start debating, "Do we ever want to turn enforcement on?" You have to debate whether you want to go there and I think each company will make that...

Greg Hughes: It's a risk versus business decision.

Jeff Sigman: Right.

Greg Hughes: It's all about risk management, as we say, not risk abatement. We can mitigate it and we can manage it, but it's not about turning everything off. The whole idea is to enable the business to be able to do their jobs.

Jeff Sigman: Exactly. Continue making money your business...

Greg Hughes: Right. Some pretty exciting stuff.



Jeff Sigman Gives Us Network Access Protection!

July 4, 2007

Jeff Sigman: Can you tell I'm enthusiastic about it?

Richard Campbell: You seem to like it. In my relationship with Microsoft, I had an opportunity to see earlier incarnations of this. I thought, "Wow. This is gonna be impressive when it comes along the lines." It's nice to see it actually showing up with the 2008 edition.

Jeff Sigman: I appreciate you saying that.

Richard Campbell: It hasn't been that far.

Jeff Sigman: No.

Richard Campbell: I'm thinking about how I would retrofit into my existing network with this. I can imagine setting up a virtual PC machine and just going one step at a time.

Greg Hughes: Let's dive really quick before we're out of time here into the 802.1X requirements.

Jeff Sigman: It's one of my favorite ones.

Greg Hughes: Why don't you talk about how that works, why 802.1X is chosen and used, and what it takes to be able to implement that?

Jeff Sigman: Okay.

Greg Hughes: In fact, it might even be useful for some people who are listening for you to explain what the heck 802.1X is in the first place.

Jeff Sigman: Okay, great. 802.1X is all about user and machine authentication at the physical connecting device, so that's your wireless access point, what most people think of as a hub or a switch.

Greg Hughes: A switch, right.

Jeff Sigman: It's user and machine auth at that point when you plug in or when you connect to wireless. It's all about going back to the 80 or the user account database and saying, "Can this person actually get an IP on my network?"

Greg Hughes: Right.

Jeff Sigman: The guest scenario there is if we don't know who they are, we put them somewhere. Either that or we just drop them completely.

Greg Hughes: Right. Or VLAN them off to the guest network or however you want to do that.

Jeff Sigman: Right. VLAN is virtual LAN in that this is a concept of think of an IP area within a switch in its memory itself where you can segment those things off. That's how I'd try to think about it.

Greg Hughes: So, you only route to that one particular virtual LAN, if you will?

Jeff Sigman: Exactly.

Greg Hughes: And all of the other VLANs on the switch are inaccessible.

Jeff Sigman: Right, and then you add health on top of that. So, the guy has authenticated to the switch port, you add health on top. If he's not healthy, you can actually tell the switch move to VLAN unhealthy and then he'll only have access to machines you've allowed routable through that VLAN.

Greg Hughes: Gotcha.

Richard Campbell: I can think of a weaker solution, but not requiring the gear for that, which would just be using NAP DHCP to assign different subnets based on pass-fail, whatever levels you want to go.

Jeff Sigman: Yeah. Through NAP DHCP, you can push down routes. The guy loses his default gateway in NAP DHCP and you can push routes down so he can only get to WSS or the Internet proxy or whatever you want to... Exactly.

Richard Campbell: Right. You could filter him down and limit him. If you're really clever, you'd be pushing him to a gateway that's rewriting all his IPs so he's being sent to the same place saying, "You're not compliant. Here's how you get fixed." No, I'm not letting you out until you get yourself fixed.

Jeff Sigman: Yeah, like the hotel scenario where they grab your browser.



Jeff Sigman Gives Us Network Access Protection! July 4, 2007

Richard Campbell: Absolutely. That's what's exactly I was thinking is that I would have all that capability relatively easily. These switches aren't extraordinarily expensive. We're talking about a basic layer 3 managed switch as 802.1X supports.

Jeff Sigman: Dell has a \$400 one I found on their website. All it has to support is dynamic VLAN switching via RADIUS. That literally is a bullet item when you go and buy a switch. Cisco's had it on their switches for 10 years and I think within the last three or four, all the major vendors have it. We had a rack at Interop Vegas with 12 switches in it and we just showed the customers I can plug in any one of these guys, extreme networks, Aruba Networks...

Greg Hughes: HP, all of the above.

Jeff Sigman: Yeah, HP ProCurve. I plugged in to all of the networks.

Greg Hughes: That's pretty terrific. For some large organizations where the switches are maybe a little bit older, it is possible to need a retrofit?

Jeff Sigman: Right.

Greg Hughes: All modern switches do include 802.1X.

Jeff Sigman: Yes. That's been my experience.

Richard Campbell: Yeah. I can't disagree with you there. Odds are there's quite a few that just haven't configured it or haven't needed it before.

Jeff Sigman: Right.

Richard Campbell: This is a whole other way to take advantage of it. The big thing with the whole VLAN-ing of this is that now the traffic is completely isolated, someone with bad intent is going to have a tough time circumventing it.

Jeff Sigman: Exactly.

Richard Campbell: If somebody is just messing up.

Jeff Sigman: Yeah. I have a webcast of how you set up from zero to infinity at Windows Server

2008 with 802.1X on the blog. If you don't mind if I mention that.

Richard Campbell: Absolutely. Please do.

Jeff Sigman: It's blogs.technet.com/nap.

Richard Campbell: NAP for Network Access Protection.

Jeff Sigman: Access Protection, exactly.

Richard Campbell: Jeff, really been fun to talk to you.

Jeff Sigman: Awesome!

Richard Campbell: Exciting, exciting product. Nice to see something brand new coming out...

Jeff Sigman: Yes. Yes.

Richard Campbell: That's going to shake things up and make our lives a little easier at the same time.

Jeff Sigman: And, my opinion, one of the key reasons to go to 2008.

Greg Hughes: Absolutely.

Jeff Sigman: Of course, I'm on the team so I have that opinion.

Richard Campbell: You are bought. There is no two ways about it.

Jeff Sigman: Slightly.

Richard Campbell: But I appreciate the enthusiasm. It's been really fun to talk to you.

Jeff Sigman: Yes.

Richard Campbell: And we'll talk to you next week on RunAs Radio.