



<http://www.runasradio.com>



Richard
Campbell

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.



Greg
Hughes

Text Transcript of Show #130
(Transcription services provided by [PWOP Productions](#))



Dana Epp Provides DirectAccess!
October 14, 2009



[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #130, with guest Dana Epp, recorded Friday, September 18, 2009. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com. You can follow the boys on Twitter at twitter.com/runasradio.

Richard Campbell: Thank you, Brandon. This is Richard Campbell. With me as always, my co-host Greg Hughes.

Greg Hughes: That would be me. How are you?

Richard Campbell: I'm well, sir, and ready to do another RunAs.

Greg Hughes: Yeah. Hey everybody, good to talk to you again.

Richard Campbell: Yeah, glad to be here. We're always having fun and the technology just keeps rolling on. I brought back our good friend, Dana Epp.

Greg Hughes: Hey, Dana.

Dana Epp: Hey, how is it going guys?

Richard Campbell: Our most recorded guest as of this moment I think is you.

Dana Epp: Oh, really? Now I feel privileged.

Richard Campbell: Fourth or fifth show, man. It's something. In a 120, that's a lot of shows.

Greg Hughes: Welcome our co-host, Dana Epp.

Richard Campbell: Two more and you get the plaque, I think.

Dana Epp: Oh, excellent. Just give me the beer, that would be enough.

Richard Campbell: You're all about the beer.

Dana Epp: There you go.

Richard Campbell: I saw you a few weeks ago and we were chatting about technology as we are wont to do and you said something along the lines of DirectAccess changes everything.

Dana Epp: It does.

Richard Campbell: It's a whole new world and this is a combination of Windows 7.0 and 2008 R2.

Dana Epp: Yeah.

Greg Hughes: So what is it?

Richard Campbell: Yeah. You better start at the beginning.

Dana Epp: So what is it? Let me turn the table for a second. Let me ask you one question. You guys obviously do a lot of moving around the world, you need to get access to data resources at the office. I do that now.

Greg Hughes: Yup.

Richard Campbell: My life is one crappy VPN connection after another.

Greg Hughes: Yeah, mine too.

Dana Epp: There you go. User initiated VPN. So you got the issue that sometimes, especially you Richard, at a lot of places, you go overseas, I'm pretty sure that sometimes those VPNs don't work very well because the hotels don't support all the different protocols and in many cases you might have to use SSL VPN. You know, it's ugly.

Richard Campbell: It is.

Dana Epp: More importantly, you're moving a lot around the world and I'm sure your IT team must just hate your PC.

Richard Campbell: Yeah. Mostly because I'm the IT team and I hate myself.

Dana Epp: There you go. Well, so here's the reality. User initiated VPN has one problem and that is that those machines that are out in the field simply aren't under a protection scope that can be managed and maintained inside the office very well. Even with things like NAP enforcement which can allow you to quarantine and control. If you've been on the road for three months and your system haven't had the right patches in place and you try to connect back to the network and you've got a NAP enforcement policy in place and now you've got to push down 100, 300 megs of patches before you can get access to that file you were trying to get in the first place, you can be very upset.

Greg Hughes: Yeah.



Dana Epp: Because you've got to sit there and wait an hour, welcome the cost of VPN until you remediate and reboot your system just so you can reconnect just to get that file.

Richard Campbell: Yup.

Dana Epp: And that becomes a real problem. Now enter Microsoft. Microsoft has decided, they had seen that this type of VPN solution although great like don't get me wrong, I love VPN, I use it all the time but there's a better way to do this and that is that we need to try to find a way so that we can treat remote PCs as if they're in the LAN. If we can do that, then we have all the controls that we normally have under a group policy and Active Directory to keep it remediated up to date. Well, that's where DirectAccess comes into play because what it does, if you have Windows 7.0 Enterprise or Ultimate you can connect up to a Windows Server 2008 R2 system with DirectAccess and it treats it as an always on connection as if it's a node in the network. So what happens is that you're actually turning your entire network paradigm on the dime. And instead of treating your assets as resources that are having to be managed and maintained inside the network, we're "reparameterizing" it and saying "My network is no longer the building onion where my users and assets are." So now all of a sudden what happens is the Windows 7.0 machines are communicating with the Office at all times through an IP set connection at the machine level. So even before a user logs on, if he is connected to the internet and the machine is aware and can talk to that system as it's booting up, it can get policy from the server so it can get control and you have updates. So the system can always be patched. They can always be maintained. Policy changes that occur in any org apply to the virtual remote PCs. Here is the power and cool part of this. It means that you're always connected to the network. So resources in Outlook for those internal share point sites, those links just work. The patches that just got deployed to the LAN had been deployed to you while you're at that Starbucks. You don't even know about it. It just happens because there is a network, lower level network connection that's always being connected to the LAN and that's what DirectAccess is. It treats your remote PC like you're inside the office.

Richard Campbell: I'd like at this moment to hand you over to my security guy for crucifixion.

Dana Epp: Here's the thing. It's a balancing act. But here's the component to it. Remote users have come in through user initiated VPN or just as much of a risk, or if anything they're actually more at risk. Let me tell you why. When you're doing user initiated VPN, the attack surface is what's called Transient Risk. In other words, the risk

is no longer about the parameters I have at my main office, it's now on that remote PC. If that remote PC hasn't been patched and hasn't been up-to-date, it becomes vulnerable. So even though I might have a secure tunnel between the laptop and my office, yes, that's really strong, I have squishy ends and I'm just going to attack the remote machine and then go through a secure conduit. So what it really becomes is a secure conduit of attack.

Greg Hughes: Right.

Dana Epp: Whereas if I have it under control through DirectAccess, I can apply all the standard security policy I have in place with Active Directory which is something I won't have through user initiated VPN and more importantly because it's all driven in IPv6 and through IPsec, I can now have things like domain and server isolation so that I can say this remote PC when remote can only access these three machines. Although it is possible to do that at the firewall level for remote access normally, it is extremely difficult to do. This becomes really easy because now you can use all the benefits of IPsec across the entire net inside and outside of the network and that becomes a better way of managing security bond.

Greg Hughes: And you know what? I can't crucify all that. You're absolutely right. Dana, do you remember a couple of years ago when the big buzzword in the IT security was de-parameterization? Remember that?

Dana Epp: Yeah.

Greg Hughes: Everybody was talking about de-parameterization now. The perimeter is going away. I like the re-parameterization idea, and yeah, I can't crucify on this. This is where we need to be and where we need to go. The fact of the matter is is that we have displaced workers and workers that are working from home. I work out of the home office and I have to do a classic VPN connection in; and you're absolutely right, this is a way to make things work better and to be more secure.

Dana Epp: Yeah and what's really nice is if you take a look at the industry trend and how it works now, today, what happens is every time we need an application to work, what do we do? We have to pierce yet another port or another access or use what I call the universal firewall bypass protocol. SSL.

Richard Campbell: Port 80!

Greg Hughes: Yup, exactly. 44380.

Dana Epp: We try to do everything across there. We have no control over management and that



becomes really, really difficult. Now with DirectAccess, it's not an all or nothing game. You can still use things like IAG, the Intelligent Application Gateway, to do that SSL VPN kind of stuff in the Windows world.

Greg Hughes: Sure.

Dana Epp: And the machines that can't take advantage of DirectAccess like those XP machines and those non-Windows machines, they can still have these other solutions. But what's really nice about DirectAccess is it gives your users always an experience and that's the real component. It's really difficult to teach users to use VPN correctly. They'll get their email and they'll click on a link and just sit there, it spins forever. Oh yeah, I forgot. I've got to turn on my tunnel. This goes away. Their education is just work on it like you're in the office and they don't notice or act any differently and you get all the policy and control that's in there. What's nice is what we're doing is when we say we're re-parameterizing a network, what we're really talking about is we've got to put the security boundaries around those critical assets and we could treat local users as remote users and that's what I like. A lot of people will think that's a little anal but it's really true.

Greg Hughes: No, that's true.

Dana Epp: Even inside the network, we want to rethink the security strategy. Do they really need access to those assets? Do we need to really give them full unabridged control? That's how things like slammer and all these other types of worms have been able to cause lots of problems...

Greg Hughes: Exactly.

Greg Hughes: Because they propagate across systems in ways they're not suppose to because we're just too lax in security. If we change around and say "We want to put the parameters around the assets," and then we treat local users and remote users the same, apply the same types of policy sets, we could control everything in the same way. We get a single pane of glass of view through System Center or though whatever our monitoring tools might be, how our management is all done. At the end of the day, it actually gives us less work as IT people to accomplish these goals and we allow our people to have more productivity because they literally do have real always on connectivity anywhere, anytime and that's what we need in a remote world.

Greg Hughes: If you think about it, if you want to take this to extreme, I can't advocate this yet because of, you know, the proofs and the footings so to speak. But in an IPv6 world where you could in

theory everybody could have a public internet IP, then the whole idea of a parameter could be virtual parameter and could be your more encapsulated parameter that's around the machine.

Dana Epp: Yeah.

Greg Hughes: And then the controls really are which machines can communicate with which ones, which processes can communicate, doing content inspection, being aware of the data that's being communicated or being moved or being used on a machine, there's a whole area of expertise data linkage prevention.

Dana Epp: Yeah.

Greg Hughes: But all of these things start to become aware of each other and with the technology that's out there, by sort of doing that let's take what we have and start to put it together especially with IPv6 and the security that goes along with that IPsec and others, it's not impossible anymore.

Dana Epp: Right and then the security becomes about the identity of the user and where they are. It's that question of you are who you say you are and we can authorize what you're allowed to do no matter where you are, how you are. It moves everything away from the old paradigm and allows you to say "If you need access to these types of resources, we can give them to you because we know what you're committed to do." And you can see that, there are other things. You know, I'm very passionate about Identity Management or Geneva that became ADFS, and all these other...

Greg Hughes: Right, right.

Dana Epp: They also start layering on top of each other and that's what I really like with this whole scenario.

Richard Campbell: So where does IPv6 fit into all this?

Dana Epp: So interestingly enough to make this work, especially with the IP stack layer and everything that else that's on there, IPv6 is a requirement. Now, when I say it's a requirement I'm not saying the entire org has to be running IPv6 but the endpoints do, and by default Windows 7.0 and Windows Server 2008 R2 have IPv6 in play. So we use IPv6 at the endpoints. That's how it works. And if you have a net that's using IPv6, great, it will just take advantage of it. If not, Microsoft has this fallback so that how it actually works is it will try to use native IPv6, and if that's not available it will come back to what's called 64 which is a protocol lab that will occur in it. If that doesn't work, it comes down to something



called Teredo, which you might have heard before which allows this connectivity between this and across an IPv4 network, and then if that doesn't work it then goes through the universal bypass protocol. It goes through IP-HTTPS.

Greg Hughes: Right.

Dana Epp: Now, it's not like those SSL VPN kind of solutions where you've got to go to a webpage and fill all that in. It's a very thin layer of SSL that's just basically another header. You know how you go internet frame, IP frame. You're just basically putting another layer in there and just saying...

Greg Hughes: Encapsulating.

Dana Epp: Encapsulate all the rest and so when it get to the other side we'll just bring it down and then we'll put it back across the net in IPv6. What's interesting and one thing I had to present in tech days a while back when I was presenting on this was I was showing and talking about the fact that people have this myth that you have to have IPv6 on every single machine and that's not true because if you have like a Windows Server 2003 box which might not have an IPv6 pack installed, you can use things like NAT-PT devices which are protocol translation devices that will convert an IPv6 address space into an IPv4 in a way that's an edit and so you can continue to use those systems across a DirectAccess enabled network.

Richard Campbell: What's interesting I think as IT folks, which is a bit of a digression, is we look for reasons to not have to think about a technology.

Dana Epp: Yeah.

Richard Campbell: Like for me, when I hear IPv6, I think "Oh, okay, my network is not up to that." So I can't think about DirectAccess. It's not just important to me. This is why I brought it up. It doesn't matter what I'm running on my network, it doesn't matter what my gateways look like or anything like that. This technology is going to find a way over the network.

Dana Epp: Yup, yup. You guys have used Vista before. Have you guys ever use that application in this called Meeting Space?

Richard Campbell: No.

Greg Hughes: Yes.

Dana Epp: No? This is a really cool application, screen sharing application that Microsoft had built right into Vista called Meeting Space, and the reason I bring it up and it seems out of tangent but

it brings back the fact that it's an application that actually runs over IPv6 and there are a lot of people that have tried it out and they spit out Meeting Space and they connect up and they're sharing screens and docks and all these kinds of stuff and like, wow, it works so great. What they didn't realize is it's using IPv6. Both of those that are running IPv6 and handled it and communicated over the net and they didn't even know it.

Richard Campbell: And so the point being IPv6 just works even if it's not necessarily doing what you think it would be doing working in the end, it does find a way to work on existing networks.

Dana Epp: That's right, yeah.

Richard Campbell: Especially in the early days of Vista, there were lots of people turning off the IPv6 stack.

Dana Epp: Well, you know what's actually funny is what they don't know they do. So I spend a lot of time in the small business world and lecture on things like Small Business Server 2008 and it was funny because a lot of people thought of the default when they deployed it that they just turn off IPv6 and you can't do that on 2008. It doesn't work very well, and all of a sudden people are saying, "Why, why? I just want to turn it off. I don't need it." I said, "You know what? There are lots of systems that do now, so play nice. Just play nice."

Richard Campbell: Right.

Dana Epp: I think that's just about education and one thing I had on tech days is more than probably three quarters of the people in that room, IPv6 was new to them, and so we have actually -- Microsoft is going to get together, we'll probably do a webinar or something like that and teach IPv6 to everybody because I think a lot of people don't understand how it works and the big gobbledy goop that they see, the big long colonized string is really just hex values that are representative of what we used to think of, you know, 192.168.1.45. It's just a lot longer because the escape is figure. There's only a certain number of IPs that could fit in the IPv4 world and they made it significantly larger in the IPv6. These people need to understand how it works and in time it will come. The nice thing is a lot of Microsoft technologies have been built on it so it will just work out-of-the-box and you don't need to know a lot about it.

Richard Campbell: I also think we've forgotten what IPv4 was like in the late '90s before CIDR really kicked in and IPs became terrifying because we were doing everything we could to scavenge them. When we go to IPv6, you're essentially going to be carrying



around on your machine a permanent identifier like there's so much capability that comes out of it naturally when we have that sort of stability with IP addresses.

Dana Epp: Yeah, for sure, for sure and that's the thing. Everything should have an IP. It's just a matter of how do you put that and what space can you put in. A lot of people don't realize that we actually run out of IP addresses back in -- what was it? '96? If every single person had an IP without net, we would have exhausted all the IP spaces already.

Richard Campbell: Yeah.

Dana Epp: So, you know, we have already had to find solutions to get around that which is the whole point of what things like NETBURN was invented for, and IPv6 is just something that's a lot better because it was designed specifically for the internet in mind especially when it relates to all the number of devices that are coming out. You know, we're not just talking PCs here. It's pretty much anything that could talk in a network. So it's those Windows Mobile devices. It's those toasters, whatever it is, at the end of the day it's going to have a device ID, an IP address basically, and you want to be able to communicate with it and that's important.

Greg Hughes: You know, we did a great show. I think it's one of my favorite shows. I have several favorite shows but one of them was with Sean Siler from Microsoft who is, at least at that time, was the Program Manager for IPv6 there at Microsoft and it was like around show #50 or so. The IPv6 world is just really important for IT people to know about. That's one that's worth going back and looking for I think. I know I've gone back and listened to it a couple of times over the last -- has it been more than a year since we talk to Sean?

Richard Campbell: Yeah, more than a year and I keep looking for more IPv6 shows because I do think it's an important topic. There are not a lot of people that conversant on it yet.

Greg Hughes: It might be good to have Sean back on and have him talk about that and as a sidebar for people that may not be aware. Remember the first I'm a PC commercial that came out, and there was like the PC guy that looks like the PC guy from the Apple commercial?

Richard Campbell: Yeah.

Greg Hughes: Remember that? That's Sean.

Richard Campbell: Really?

Dana Epp: Really? I didn't know that.

Greg Hughes: Yeah. I remember I saw that, looking at that commercial and I'm like "That guy looks familiar." I mean, the IPv6, there's a lot of learning to do, isn't there Dana, when it comes to IPv6?

Dana Epp: Oh yeah.

Greg Hughes: It's not like IPv4.

Dana Epp: No, no, there's a lot in it.

Greg Hughes: It's more complex.

Dana Epp: What's interesting is there are lots of identifiers and things inside to understand what kind of system is this and how does it all work together.

Greg Hughes: Right.

Dana Epp: And you can take a look and if you understand the string there's a lot of interesting information inside it that you need to understand in setting it up and configuring it. There are a couple of other technologies. IPsec together with IPv6 is a very strong combination.

Greg Hughes: Right.

Dana Epp: Understanding it and knowing it just really make you a better rounded IT Pro that could take advantage of what you probably already have in your infrastructure and you don't even know it.

Greg Hughes: I mean, I could spend a weekend reading books and kind of get my head around IPv4. IPv6, maybe I'm just getting older but I really think IPv6 is substantially more complex. It really does take some time and some learning to understand it in its entirety.

Dana Epp: Yeah. I can't deny that, yeah. It's definitely not, you know, it's not like reading.

Richard Campbell: Remember when we first tried to learn CIDR, the whole masking thing and going down to single two or three IPs, like that was not easy to learn either.

Dana Epp: No, no. Remember when the day you move from token-ring to internet and you had to deal with IP, everyone was pretty dumb

Richard Campbell: Yeah.

Dana Epp: Now we're coming to the next level of that and it's going to keep going. But the good thing is and I think there are a lot more people



out there to help each other and add value like when Sean did his session on this there was also an interesting conversation that happened on there but you then go pass that, you could see since then there's been a lot of conversations from everything from edge, (you know, the videocast) to lots of the stuff being documented on how to do it and back then I think it just became -- because the number of IT Pros that exist now needs to use this stuff are significantly increasing, there are a lot of people with experience that can help us to understand how to really take advantage and use this stuff. I don't think it's about sitting in a physical class to learn how to do IPv6. I think a lot of it is understand what our systems are now, how do we enable the IPv6 now, how can we see that in our current work? And so things like, you know, I do crumbled Meeting Space but it's really a good indicator, hey, I can spin up two applications and two different machines that have an IPv6 back in place and that's just going to talk.

Richard Campbell: Yeah, it just works.

Dana Epp: Now how the heck did that happen?

Richard Campbell: Yeah.

Dana Epp: How did that happen? Did you set up an IPv6 network? Do you have a special CP Server that's automatically issuing different IP schemas for that IPv6? How come it just worked?

Greg Hughes: Yeah.

Dana Epp: Do an IPCONFIG and take a look at the ugliness that you see there when you've got IPv6 in play. Learn what that means, and that's going to accomplish this some other time.

Greg Hughes: Yeah. My home office rather does IPv6 and IPv4 both and there have been times when I've spent and I've start digging around. It's really pretty fascinating and there's a lot of really good cool stuff that comes along with IPv6.

Dana Epp: Oh yeah, for sure. And for those who have environments that are just not going to work and they need some areas and maybe they use certain network segments to work IPv6, like I said there's the NET-PT devices specifically that allow you to route through there. It used to be these devices were really expensive, but now Sysco IOS actually has NAT-PT built into it. I think it's version 12.2. I think it's about where it was. So that means those low-end Sysco handed devices that are like 200 bucks, they completely support IPv6 and with the PT so if you've got some of those devices that just aren't going to speak IPv6 anytime soon like those Windows 2000 boxes, well fine, put it over on the other side of it

and you'll continue and that PT stuff will take care of it, route all the run for you.

Richard Campbell: So how much do I really need to know about IPv6 to make DirectAccess work?

Dana Epp: Well, you've got to have a little bit of knowledge because you've got to need to know how to use things like ISATAP and have things configured in both ends. But here's the great thing. By default, on installation of Windows 7.0 and Windows Server 2008 R2, IPv6 is already set up and in play for you.

Richard Campbell: So in theory, it should just work. You don't have to know anything.

Dana Epp: Yeah. Well, you're going to need to have a little bit of knowledge. There are a couple of things you have to do to set up like ISATAP-ping DNS records and stuff like that so that it can do proper reverse look-up.

Richard Campbell: So what's an ISATAP?

Dana Epp: ISATAP is one of those big acronyms. You know, it's the Intra-Site Automatic Tunnel Addressing Protocol which basically will take an IPv6 address and allow it to run across an IPv4 network. So by default, that's how you're going to be able to talk on your standard IPv4 network and have Windows 7 device talk to Windows Server 2008 device or to Vista utilizers that are going to communicate to, you know, talk IPv6.

Richard Campbell: Cool.

Greg Hughes: So in Device Manager, when I see that ISATAP adapter, that's what that is. That is that bridging device. Okay, got you.

Dana Epp: It requires that you have to have an IPv4 net as well because it's a dual stack. Great, it sits there, it does okay.

Greg Hughes: Sure.

Dana Epp: I've got an IPv6 address, I've got to go to an IPv6 address but I have an IPv4 network there, how am I going to make that happen? ISATAP is design to do that, power the IPv6 across the IPv4.

Richard Campbell: Cool. And I also obviously need 2008 R2 on the server-side of this.

Dana Epp: For the DA component, that is definitely an R2 component.

Richard Campbell: Right.



Dana Epp: But the rest of the net like your significant authority and your DNS and all that kind of stuff, that's when you run a Server 2008.

Greg Hughes: So if I'm an IT shop person and I want to give this a try just to try to learn about it, install it, and see how I might be able to use it in my environment, what do I need to do? What should I plan for here?

Dana Epp: You know, in my opinion, Microsoft has a really good hands-on lab and what I would suggest is I'm a big fan of testing in a virtualized environment; you can spin up three machines. You're going to spin up a Windows Server 2008 domain controller which is going to have DNS on there with the certificate authority. Then what you're going to do is spin up a Windows Server 2008 R2 that's going to have DirectAccess on it and then you're going to spin up a Windows 7 Enterprise or Ultimate VM, and then what you're going to be able to do is you'd have all those domains joined together, you've got the DirectAccess box and you type tunix and basically you're going to have one, it's going to be allowed to be in your external net, you can play around a little bit and then at the end of the day you're going to set up a security group inside of the domain that you're going to assign that computer to, you're going to assign that security group to DirectAccess, make a couple of changes in the DNS. This is all in a really simple hands-on lab, very easy to test, and then you're going to disconnect it from the domain and you're going to put it on the outside of the interface and then you're going to see a DA connection just happen. Of course, that's if you follow the directions and do it right. But that's the way to do it as you can take a look in there, and then once you're confident that it makes sense to you it is easy to roll that out. A lot of times a lot of the infrastructures are already in play, and in these organizations we have taken advantage of it. You just need to snap in that R2 box and of course deploy Windows 7.0 Enterprise more often and that will give you the ability to make that happen.

Richard Campbell: Do I have to have the Win 7.0 box inside the network to set this up, or can I do the whole thing remote?

Dana Epp: The initial provisioning has to be done -- well, there has to be a net because you can always do network provisioning over a VPN. So you could actually have a machine that's not even domain-joined, you've got to have a VPN in to domain-join it, allow it to do a force, a GP update force to get the policies, to get it deployed out to you for the DA side of it and so the system becomes DA aware, and then as soon as you disconnect from the

VPN DA will spin up and be able to take advantage of what needs to be done.

Richard Campbell: Let me tell you, I would not miss the VPN client. I find that Microsoft VPN client obnoxious like it pops over the top of editing when it loses a connection and then it's getting into the whole, oh, I'm running 64-bit OS and Sysco for some reason just doesn't make a 64-bit VPN Client.

Dana Epp: Yeah, yeah. What I like with DA is just, you know, at bottom right corner on Windows 7 it just tells you connect it to the network with internet. There are some who are just going to say, you know, it's beginning to tell you it's connected to DirectAccess to the network.

Richard Campbell: Right.

Dana Epp: You will act and feel as if you're in the network. It will just be a little slower depending on where you are.

Greg Hughes: I got one question. I mean, I know my current VPN Client of use is Check Point, VPN Client to it, to a check point concentrator. But I'm using RSA Tokens usually if I'm remote to access a particular network. So is there a DirectAccess story for doing multifactor authentication?

Dana Epp: Yeah. So by default, built within the DirectAccess, it has complete two-factor authentication support with Smart Card so if you've got the ability to have Smart Card configurations, it will work on there. If that's not available what I recommend -- and of course our own company there's two-factor authentication solutions -- is to run a credential provider on Windows 7.0 machine itself and add the two-factor authentication to the Windows log-on because what you're doing is enforcing the identity at the log-in level of the machine and then allowing the normal network to control everything else based on their identity for, you know, through the IPsec layer of things.

Greg Hughes: Right. I guess I'm thinking I like to do the fingerprint thing or something, a card or some kind for the machine but I'd also like to have something that prevents me from accessing anything outside of the machine.

Dana Epp: We're definitely working with Microsoft on a solution for that because obviously we have invested reason to do so, but as it stands right now their integration for multifactor authentications are Smart Card technology.

Richard Campbell: Well, and of course Microsoft uses Smart Card so it makes sense.



Dana Epp: Yeah and that's why. They dogfooded DirectAccess themselves in their own org and they have a lot of remote workers that need to get access to Redmond's corp LAN.

Richard Campbell: Yeah.

Dana Epp: And they went through all the pains of, you know, 53000 user network and I think it's larger than that. I don't know what they had to do with the number nodes they need to get on the DA but I know pretty much every Microsoft employee I talked to, every blue badge has got eyes on the DA net now and just loving it and they've got a larger net to deal with than a lot of people and interestingly enough it worka and that's good.

Greg Hughes: It's very cool.

Richard Campbell: I guess one of the concerns I would have then is stolen laptops just dropping straight into the network.

Dana Epp: Well, you know, at the end of the day there's complimentary security technologies that are in play here like stolen laptops are still to be protected by things like BitLocker and there should be a TPM in there and they should be encrypting the drive and making sure that the data cannot be touched. The thing with DirectAccess is you can tie NAP enforcement help-check rules in there. Actually it does by default. It's just a matter of is it an enforcement rule, etc? Is it just a monitoring rule set?

Richard Campbell: Right.

Dana Epp: So you still have all the controls of Network Access Protection to be able to say is this machine in health, and more importantly is not only have we build the check and validate that it's got the right health to take it. We're also going to be able to be assured that they got all the other policy in play which is not something you normally get with the VPN connection because it's a hit and miss thing. Will policy gets deployed when that time comes up in time to allow enforcement? Where this happens, with a separate IPsec tunnel at the machine level using machine certificates, that all pointing you need a certificate authority board that you can have some machine level understanding that is the machine I think it is and I can deploy policy to it.

Greg Hughes: Sure and if you revoke that certificate, then obviously that is no longer valid.

Dana Epp: When setting up, your certificate authority has to have a revocation list available so that you can for obvious reasons -- they usually revoked these machines if they need to. Well, I think it's really cool. Because you've got a machine

level connection, you can do some interesting things like wipe the PC even before a person log on. If someone plugs it into a network and it has called home, you can say, hey, you know what? We don't trust that machine anymore, wipe it, and it will get wiped.

Richard Campbell: Interesting.

Greg Hughes: Cool.

Dana Epp: Pretty cool.

Greg Hughes: What does DirectAccess management look like?

Dana Epp: You treat it differently. Once you configure the group that the person is in there and you've done an initial set, that's kind of cool. The DirectAccess has this really nice Wizard. It's a four-step Wizard of set up the security groups that you need to apply it to, set up how the DA is suppose to work with resources with the domain controller and what the certificate authority is, what are the SSL sorts that are going to be used in play, and then you basically set up the application servers and then finally, as part of that Wizard, it would ask you would you like to create some IPsec rules and do things like server and domain installation.

Greg Hughes: Yeah.

Dana Epp: Yeah, those components do it to give you the ability to control breakdown of the individual machine level if you have to. Once that is done though the rest of it it just, because it's treated and in it's view post as a PC on the net you're current management modern tools -- and System Center is a perfect example for this, it just comes under management so you got to see it the way you want it. It's going to work. That means that there is no separate management that you have to do on the DA side of things. But interestingly enough, with Windows 7.0, one thing Microsoft did do is one problem IT Pros have all the time with VPN is how come it's not working. Is it because there's the hotel is blocking the firewall port? Is it because the configuration is wrong? Is the user entering a passwords wrong? Well, with Windows 7.0, outside of just DA, if you actually right click on the network icon in the tray in the bottom right, there's an option there that allows you that says "troubleshoot your problems," and it will automatically do things and check to see the health of your network connectivity. But if you actually click on there, I have a different problem after it does its normal scan. This is an entire section which is dedicated to DirectAccess so then what it does is it does a complete dump of everything that's going on in the net. So you get the IPCONFIG in the system configuration, all that stuff,



and it also gives you basically a network dump of what's going on which you can then load into things like Netmon which is another free tool that Microsoft provides for network monitoring and you can load that right out there in a post analysis point of view so that you can figure out why the user is not able to get connected up and that's very useful from a diagnostics point of view.

Richard Campbell: Sounds great.

Dana Epp: Yeah.

Richard Campbell: Dana, we're just about out of time here. Any final words?

Dana Epp: DirectAccess is going to change the world. It will allow anywhere, everywhere access and I'm really looking forward to seeing the world move to Windows 7.0 to take advantage of it.

Greg Hughes: You know, there are not many statements that take that broad of a scope that I would tend to agree with but this is one that could potentially really, truly change the way that business is done with computers. I kind of tend to agree.

Richard Campbell: Wow, both security guys on the same side. I don't understand this. I'm confused.

Greg Hughes: If you can do it well and do it right and it enables business, then I mean there are not a whole lot of things in the computer world that are no-brainers but there are a few and so as long as this all comes true and as long as it works out the way that it is intended to, it could be a gain.

Dana Epp: Remote productivity the way it's meant to be allow people to get access to the resources as they need it when they need it, you know, the secure scope that we can control and manage to reduce risk, to accept the level of business owners and as IT professionals. What more can you ask for?

Greg Hughes: So you it could be a game changer for sure.

Richard Campbell: It's all about the love. Dana, thanks so much for coming on the show.

Dana Epp: You're welcome. Thanks for inviting me.

Greg Hughes: Talk to you later, Dana.

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