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 #096
(Transcription services provided by PWOP Productions)

Richard Hicks Dig Into ISA Server!
February 11, 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 #96, with guest Richard Hicks, recorded Thursday, January 29, 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: This is Richard Campbell and you're listening to RunAs Radio. With me as always my co-host, Greg Hughes.

Greg Hughes: Hey there. Richard, how have you been?

Richard Campbell: I am doing just fine, man. I'm working on TechEd actually. They dragged me into being External Track Chair so we're picking sessions and locking down details and the first questions around Speaker Idol just came up.

Greg Hughes: Great. External Track Chair, that sounds new.

Richard Campbell: Well, I think it's a great idea. Microsoft has started getting folks on the outside, out in the world to help them plan sessions for TechEd so that, you know, they don't have so much of an insider effect. So needless to say, I pushed for good third party speakers and sort of talk about pushing on topics that are relevant today where the product teams tend to want to talk about what's coming.

Greg Hughes: Sure. Yeah, and having a good mix is always probably useful. Some stuff that I can use - nuts and bolts, hands on today, as well as looking toward what's coming in the future.

Richard Campbell: And it's a very challenging year because the Los Angeles Conference Center is not big and we went back to one week.

Greg Hughes: Right.

Richard Campbell: So just getting all the sessions in, getting room for everything has been very challenging.

Greg Hughes: Right. So dev and IT all at the same time. Yup, it will be very different but probably it will still be a lot of fun and there's always a lot of great content no matter where it's been and no matter how they've organized it. It has always been a good show.

Richard Campbell: Absolutely and I'm really looking forward to it. Of course, if you're interested in Speaker Idol, send us an email at info@runasradio.com. It looks like we will be hosting it again and we will be doing all that fun of finding new speakers for TechEd. I haven't locked the whole deal down but it looks like it's going that way so it will be good fun. Of course, send us your email, any questions about RunAs, if you want to create new shows, whatever you'd like, we're here to help.

Greg Hughes: This is sort of near and dear to my heart as the security guy. Today we get to talk about ISA Server.

Richard Campbell: Absolutely. Let me introduce our guest. Richard Hicks is a Senior Sales Engineer and Product Specialist for edge security solutions at Celestix Networks. Richard has been working with Microsoft ISA Server 2006 and its predecessors for over 12 years. Richard has designed and deployed network security solutions using ISA for SMB's, military and defense organizations, and Fortune 100 companies around the world. He is an MCSE and MCITP, and is Microsoft Certified in Proxy 2.0, ISA Server 2000, ISA Server 2004, and ISA Server 2006. He currently lives and works in beautiful, sunny Southern California, and just had to rub that in on a rainy day in Vancouver.

Greg Hughes: It's sunny in Portland, Oregon. That doesn't happen too often.

Richard Campbell: Yeah, okay. Neither one of you is helping me. Rich, you've been involved in ISA since it was Proxy Server, I mean right from the beginning then.

Richard Hicks: That is correct. I have a tremendous amount of experience. I've been doing all this for many, many years dating back to the old Proxy 2.0 product from the middle, late nine years or so.

Richard Campbell: Yeah. You know, it's funny. Microsoft, I think, struggles in the world's perception of it making a security product.

Richard Hicks: It most certainly does and that's definitely been a stigma, but Microsoft has made great strides really to kind of shed that stigma. The product is obviously a much different product than it was back in the day.

Greg Hughes: Right.

Richard Hicks: It is a full-fledged enterprise security device and is a fantastic product used to protect organizations really of any size and, of course, especially obviously adept at protecting Microsoft

resources such as SharePoint and Exchange Outlook web access, things of that nature.

Greg Hughes: Sure. If an organization is primarily deployed on the Microsoft platform, ISA Server at least always seems to be considered as one of several options, or an ISA Server appliance, or some flavor of ISA Server in figuring out how to do the perimeter security. So if I'm a Microsoft shop where I have primarily Windows platform deployed, why should I consider ISA Server and what are some of the advantages that I get with ISA Server that I may not get on other edge platforms?

Richard Hicks: Well, first of all, and that's an excellent question and one that we get quite often, I'll be honest with you, the reason that you would want to deploy Microsoft ISA as far as wanting to protect internal resources, because it has some features and functionality and it has some capabilities that no other product, no other firewall product on the market today can do. That namely is the ability to perform seamless integrated or transparent authentication of user access. So a traditional firewall that you would deploy today, maybe it's a hardware-based firewall, most typically controls traffic based on source destination, protocol, and port. We can do some very instant things like that to control network access. The ISA Firewall has the capability to do those things as well. It has the capability of doing simple packet filtering like that, but it also has advance capabilities that allows us to perform user and group-based authentication as well so we can apply access rules not only to source and IP address destination, IP address protocol in port, but we have the ability to authenticate these users and also place policies and access rules based on who the user is or based on their Active Directory membership that has some very, very compelling security features that along with that. We know who's going where, we know what application their using most of the time, and also that information is recorded in a log and with the ISA Firewall as well. So very compelling reasons there to deploy the Microsoft ISA Firewall.

Greg Hughes: So it sounds like there are a couple of assumptions that somewhere I have, you mentioned Active Directory, that I have a directory and that's my user base so I supposed that could be whether it's a corporate application, or would this be something that would be useful from the standpoint of I have users on the internet that I want to be able to have them sign-up for accounts and I want to be able to control their access not only as you say based on their network type of information but also on their authentication. You were talking about authorization type of activity, right.

Richard Hicks: That's correct, authentication and authorization absolutely. So we have the ability to authenticate the users and of course, you know, we apply access policies based on those users or groups and then we have the ability to authorize that access in that manner as well if you're talking about access that is outbound access. So I'm trying to protect, for instance, my corporate internal users from going out to public websites. I can grant access based on users or groups. More often than not that's going to be groups, of course, and so that has some definite advantages to us. Also, keep in mind that with the traditional firewall I wouldn't have to grant access, again based on individual IP addresses, maybe subnets, maybe network ranges, that type of thing and the user experience get hampered because if the user is mobile and so their moving around in offices or workstations within an office, they may not in those cases have the same access that they would at their workstation as they would in another workstation, in a lab, or maybe on another floor in the building. With the Microsoft ISA product, we have the ability to perform those types of things based on your user account and your group membership. So the experience is the same for me wherever I log in and whether that be on my workstation, in a lab, in a remote office. The access policy applies to me and follows me wherever I go.

Greg Hughes: Okay, I got you.

Richard Campbell: Now, if my understanding is correct, we're primarily talking about outbound security here where it's ISA serving us the proxy to the internet for internal users versus the sort of external connectivity I need people to log in to get to my website?

Richard Hicks: Certainly the scenario that I just explained to you was for an outbound proxy, but we have the ability to leverage strong user and group-based authentication for inbound proxy as well, or reversed proxy. So in the event, for instance, I wanted to make a SharePoint site available to users, either my corporate internal users who have them would be able to reach the SharePoint site from home or from another office, or perhaps this is a SharePoint site that's used for information and collaborative purposes with another business partner or another external entity, I still have the ability to authenticate those users. I may have those users in a separate OU in my domain, I may have a separate domain in my Active Directory force for them. I can segregate that in any number of ways, but I do have the ability to enforce user and group-based access controls on reverse proxy or inbound traffic as well.

Greg Hughes: How granular can I get with that control enforcement? We're talking down to the page level. I mean, sort of helped the IT guy be educated here as to what programmatically I might be able to do.

Richard Hicks: Oh yes, absolutely. Yeah, yeah, we can get very granular with that. Obviously, based on users and groups so I can do this down to the individual user, I can do it based on your membership, but I also have the ability again to control access to exactly where it is that you go in my internal network. I can grant you access to a particular published website, and everything in that website I can actually control the access down to the user as it's getting to the folder or the individual document. I may grant you access to a particular subdirectory under a website so you can go to, you know, example.com/training and you can see everything under that, but yes, I do have the ability to actually say you can see training/hr/default.htm and that's all you can see. So we do have some granular access controls that we can place with the ISA Firewall.

Greg Hughes: Those access controls are actually done in the ISA Firewall application, is that correct?

Richard Hicks: That is correct, yes.

Greg Hughes: Great.

Richard Campbell: I'm of course an inbound guy. I'm the guy running all these servers and trying to find better ways to handle access. When you start talking about the fact that ISA understands Active Directory, I start thinking about, hey, can I offload authentication work for my web servers here.

Greg Hughes: Right. Say I have a hundred thousand users of my web application in some big community thing or what have you. Maybe I should be leveraging Active Directory instead of building a custom user account provider that's all built into SQL and that cost a lot of money to maintain.

Richard Hicks: Certainly. Yes, absolutely and that's definitely very common scenario where people will use Active Directory in that fashion to handle those types of authentication and request.

Greg Hughes: So what would you say are the top three big changes that have happened in ISA Server in the latest revision? What are the real big differentiators for those that, and I have to admit that I have been one who in the past has said, well, because of previous versions of ISA Server that I had worked with and some limitations that I run across, and granted these were a few versions ago, what are the top three things that should convince me that this is the application to look at in a Microsoft environment?

Richard Hicks: Okay, excellent questions. One of the things that have changed dramatically is really the entire architecture of the product. Beginning with ISA 2004, the product really changed entirely from previous versions. If you have any experience with the older products like ISA 2000, absolutely nothing like that. This is a full-featured enterprise fast firewall now. It has the user interface, it's much, much more intuitive than it ever was in ISA 2000. ISA 2000 was very unintuitive, but beginning in ISA 2004 and certainly carrying over to today's product of ISA 2006, the management console is essentially like any other enterprise class firewall. You have an ordered set of rules that have very intuitive policies that you can look at source destination, protocol, port, time of day, user and group information if you're applying those typed of things, and again ordered so that you can see that Rule 1, 2, 3, 4, we can see what order to process in, very much more intuitive. The ISA 2006 product has some of the strong suits of that, and some of the things that have changed dramatically are the ease of deployment for things like Outlook, Web access, and SharePoint. So publishing those sites and protecting those sites effectively can be a bit of a challenge and it's extremely daunting if you're doing it with some of the older products, but today that is all wizard driven and essentially you can go through, follow the prompts and you can be up and running and securely publishing your internal resources like Outlook Web Access and like SharePoint, very quickly and very easily by just following the prompts. So that's kind of the hallmark of Microsoft products anyway...

Greg Hughes: Sure.

Richard Hicks: It is very intuitive wizard-based interfaces like that. Also, when we talk about security, the security of the product has improved immensely over the years. We have an integrated firewall core that is unified now. We don't have some other services that were kind of ancillary to some of those core products. Some of those core services are now integrated into the firewall core. The firewall core itself is a Kernel mode firewall engine driver, again runs in Kernel mode, very high performance and very secure. Those are some enhancements over some of the earlier products that you may be familiar with. So definitely, we made some improvements in terms of security, usability. The latest product also includes things like flood mitigation and increasing detection capabilities as well. The latest product is very, very resilient when it comes under attack. It does a fantastic job of defending itself and staying online to be able to service the service request in the event there is a flood or a worm propagating through your network or, like I said, the ISA Firewall itself is under attack and in the case of perhaps a Dos attack or something to that effect.

Greg Hughes: That's great and I'd like to touch more on some of that in a minute, as well as I want to make sure that we address the appliance side of things which I know you have some specific knowledge about because that is fairly new too in recent version of the product, but before we do that, because you've mentioned the ability to "publish" or it was just a sort of reverse proxy way of preventing the end user from directly attaching, for example, to the Outlook Web Access server or the SharePoint server. Correct?

Richard Hicks: Uh-hum, yes.

Greg Hughes: And so I know we have the wizard for those couple of applications. If I have a home-grown application that I've built, can I leverage ISA Server to publish it to the outside world as well?

Richard Hicks: Oh yes, most definitely. So obviously, for very complex applications like SharePoint and Microsoft Outlook Web Access, we do have some wizard interfaces for those, but yeah, that absolutely does not prevent you from publishing any application that you wish on your internal resource. Those applications do not have to be web-based. They're not strictly limited to web-based protocols so if they're using non-web-based protocols, something other than HTTP, HTTPS, we have the ability to publish those and make those available securely to public internet resources as well.

Greg Hughes: What about maybe a more complex web applications that are multiple web server session-based types of things where session affinity is important from a user's standpoint in using maybe a custom web application. How can ISA Server -- and this really isn't just about ISA Server or the ISA Firewall. This is about sort of in general, but what do people need to think about or what are sort of the rules to live by when it comes to putting these more advanced firewalls out in front of the more complex session-based web applications?

Richard Hicks: Yes, certainly the ISA Firewall is capable of doing those things and obviously there are a lot of complexities that arise when you start deploying complex especially home built applications or the applications were built in-house. But when you talk about session affinity, the ISA Firewall really doesn't have any problems with that. Those requests, keep in mind that in a reverse proxy scenario the proxy server itself, the ISO firewall in this case, is really requesting the content from your published resources, your internal web-based application in this case, on behalf of users on the public internet and so it really appears as the client. So any session affinity that you would have for a normal user, the ISA Firewall is still going to leverage those mechanisms for you and if you have concerns over load bouncing, like I know one of the problems has been in the past that when you have a clustered array of ISA Firewalls, we do have some features of functionality that we can enable on that that allows that to load balance the ISA Firewall array and with that we do have a single affinity, a bi-directional affinity, so that the traffic coming through an ISA enterprise if it has multiple ISA Firewalls in the array, the session actually sticks with the individual firewall that originally processed its request and it stays with that ISA Firewall over the life of that session.

Greg Hughes: Then the firewall can manage the session on the other side of the connection there. Got you, makes sense. So you've just start to touch on my next follow-up question which really had to do continuity, availability, and disaster recovery type of situations which from an architecture standpoint are always very important considerations when it comes to buying and deploying firewall architecture. So for somebody who is looking at, you know, maybe needing to have a two datacenters, I mean maybe too hot or hot-warm type of situation, what's the story for ISA as far as the people that need to make that kind of deployment?

Richard Hicks: So certainly we have a lot of availability features that are a part of the Microsoft ISA enterprise version. With that, we have the capability to create clustered arrays anywhere from 2 up to 32 hosts in a single array. The arrays themselves should be located in a physical proximity to each other. So the members of an individual array should be in one datacenter, but it doesn't prevent you from having multiple and geographically dispersed arrays. So I can certainly have one array in a primary datacenter, I can have another array in another datacenter that's connected to other egress point to the internet. I can have both those. I can actually load, bounce among those if I wish. I can use them in active standby scenario if that is something that you choose, release of design decision-based on how you want to implement it, but the beauty there is that I manage the use as a single entity. I have the ability to manage access policies globally in the enterprise in a single location and actually have that be done with a single policy or a single rule set. So anytime I make changes in the enterprise, I can actually apply those via an enterprise policy and so any access rules that I create, whether they be inbound or outbound, I have the ability to apply in both locations so that you don't have any conflicts if you do have to switch over.

Greg Hughes: Sure.

Richard Campbell: All right, hardware time. So generally, the policy around ISA, if I read the docs correctly, is that it should be installed on its own hardware. Right?

Richard Hicks: Absolutely. That's correct, yes.

Richard Campbell: I mean, maybe you're bias here because you are involved with a vendor that sells this thing but it worries me to install ISA on my own hardware so I'm trying a weigh the difference between I grab my own gear and turn it into a ISA Server versus these like Celestix products, these dedicated ISA machines. What's the difference?

Richard Hicks: Certainly. So you bring up a very common scenario in net. The ISA Firewall software is relatively easy to install like a lot of other Microsoft products, but the problem is what you don't know. There are some configuration changes or there are configurations and design considerations that can be made that if are not made correctly can result, first of all, a product that may not provide all the security necessary or it may not warn well. One of the things with an appliance version of the Microsoft ISA Firewall, such as the Celestix MSA Security Appliance that we sell, is that it comes preinstalled and preconfigured. It's out of the box ready to run. You have the assurance that it's installed and configured correctly, that the underlying operating system is hardened using Microsoft industry best practices and that it's configured properly, and again, really you have that assurance knowing that we do this all the time, we do this daily, we live and breathe ISA. For a lot of our customers, they deploy ISA once and they certainly don't have a lot of ISA expertise, they may not even have a tremendous amount of information security or networking background as well. So they have that assurance that they're going to get something that has been an effective solution that is capable of protecting their network efficiently and safely.

Greg Hughes: We have to ask, you say that there are a few things that maybe might be fairly common or at least typical of that people may not realize or that they really need to pay attention to when they're configuring, so assuming that they're not using an appliance, that they are using the ISA software, installing it on their own hardware, what are the key things that we need to be thinking about?

Richard Hicks: A lot of those have to do, really center around things like network configuration, the network design and deployment, the routing infrastructure that the ISA Firewall is involved with, things having to do with authentication obviously come up, a name resolution, Active Directory configuration, there's a lot of things that can really be sticking points that if you don't have a lot of experience with this can seem pretty innocuous at first but you realize that you very quickly and easily can grant access where you didn't think you were or you can easily circumvent the access controls that are in place if it's not configured properly.

Greg Hughes: So foundational type of things is kind of what we're talking about.

Richard Hicks: Correct.

Richard Campbell: Yeah, I really think it is the difference between ISA and the OS you're putting it on, that sort of default configuration in an operating system is not tuned to be a network compliance type of product.

Richard Hicks: Correct, correct.

Richard Campbell: That there's got to be some tweaking to get that right and there's also you see a lot of stuff in an OS that is on by default that you don't need if you're just going to make it do ISA Server.

Richard Hicks: Absolutely and one of the things with this Celestix MSA Security Appliance is that, again, you get all of that out of the box, it's all been done for you. We've removed any unnecessary services and applications when we've hardened it, again using Microsoft industry best practices, so that you have the assurances that it's done right, that you haven't disabled something that is necessary for the ISA Firewall software to run, but everything that is not is definitely has been hardened and locked down for you.

Greg Hughes: So what is ISA appliance? Is it effectively just a trimmed down Windows 2003 server running the ISA software with a lot of custom configuration done?

Richard Hicks: Correct. Yes, absolutely. So in the case of the MSA Security Appliance from Celestix, it is a purpose built security appliance system. It's not a white box, so it's not a server that we just stick our nameplate on and send it to you.

Greg Hughes: Sure.

Richard Hicks: The Celestix MSA Security Appliance is designed from the ground up to be a nice firewall. So you get a couple of benefits from that. First of all is that our boxes are very lean and mean. So they weren't designed like a general purpose or industry's standard server. They were designed to be a security appliance. They're much smaller, they're much leaner, they have the reduced footprint that really results in things like reduced power consumption, reduction in heat output, increases in overall time between failures. Those types of things definitely manage just to deploy ISA on an appliance.

Greg Hughes: One of the terms that we hear over and over again over the past several years when we're talking about firewalls, you know, as doing security consulting I hear the term all the time, and people don't always know exactly what it means or what the product's capabilities are, but the term is Layer 7 or the application layer firewall. Maybe you can explain what that means and then relate that to ISA Server as far as how it fits into the equation of PCI requirements, for example, that require layer 7 or application layer firewall.

Richard Hicks: Absolutely. So yes, absolutely the ISA Firewall is capable of performing deep application layer inspection, layer 7 traffic inspection, and I will give you a perfect example of that. So for instance, on a traditional firewall we would open up TCP Port 80 to allow outbound or inbound web traffic. On the ISA Firewall, we can do the same thing but where the ISA Firewall excels, again with this layer 7 application layer inspection capabilities is not only do we open up TCP Port 80, but we also inspect the communication that goes on over TCP Port 80. A perfect example of that is that the ISA Firewall and its default configuration allow only valid RFC compliant HTTP traffic over TCP Port 80. If you attempt to perform any other type of communication over TCP Port 80, the ISA Firewall will block it. So for instance, let's say on the public internet I configure a terminal server and I configure it to listen on Port 80 so that from inside my internal network I can just use Port 80 with my RTP client, get to my remote server and then I can do whatever I wanted to do in that manner. A traditional firewall actually allows that traffic because it matches the parameters source destination protocol and it works. The ISA Firewall would match all that as well but as soon as I try to establish a communication that was using something other than valid HTTP, the ISA Firewall would actually reject that. So it has additional intelligence there to protect our communication. Also, it gives us the ability to very granularly control the types of HTTP communication that goes on. So for instance, I can open up TCP Port 80 to the public internet, but I can also write an access rule that says if when you make this request your user agent string is eDonkey or Kazaa, block that communication.

Greg Hughes: Sure.

Richard Hicks: So I can block effectively peer-to-peer communication that attempts to traverse an already open TCP Port on my ISA Firewall and I have the ability to control things, for instance, like I can block executable content, I can unblock FTP uploads, I can make certain that only certain SMTP verbs are allowed through my ISA Firewall, things of that nature.

Richard Campbell: You know, I've realized something looking at the sort of spectrum of ISA, it's always been built on the one network stack that ISA 2000 and 2006 has been the Windows 2000 network stack which of course morphs into the 2003 one but it's still essentially the same stack. We haven't seen a version of ISA on the new network stack that came in Vista and Server 2008.

Richard Hicks: No, but that is coming and I'm glad you bring that up because the next iteration of this software is referred to as Threat Management Gateway. That will be available for Windows Server 2008. It will run only on 64 bits server 2008 and I'm actually very, very excited about that product because, you're right, it's going to run on the next generation TCP/IP stack which is obviously much more robust and much high performing and also with the advance Windows Filtering Platform the Threat Management Gateway developers are going to have much more granular access packets in that PCP or in that communication stream. I think it's going to be a tremendous product. Also, the Treat Management Gateway is going to have some advance features like Malware Inspection, there's going to be some advance features with being able to inspect for viruses and worms and things at the gateway that's built into the product so it's going to be great.

Richard Campbell: I also get to imagine that a new network stack product is going to be IPv6 savvy.

Richard Hicks: I'm certain it will have IPv6 capabilities, yes, absolutely.

Richard Campbell: Up until now, ISA has been a 32-bit only product and an IPv4 product really.

Richard Hicks: Correct. Yes, that's correct.

Richard Campbell: They changed the name. It's a different product, they made a big jump here.

Richard Hicks: I believe so, yes. It's definitely going to be much enhanced in terms of a performance certainly because it's going to be running on a 64-bit operating system. So we will have the ability to certainly tile a lot more users on there because we've broken free of some of the memory constraints of the 32-bit operating system, and again as you have mentioned earlier, the fact that it's going to built on the next generation TCP/IP stack is definitely going to be fantastic.

Richard Campbell: My experience with the new stack has been that it's not focused as much on performance as the old stack was so it's going to be interesting to see how well it actually performs, but yeah, new products coming in and I say it's getting a little longer too this 2009.

Richard Hicks: It's been around for a little bit while but it is very stable and very well performing and still very secure.

Greg Hughes: So what's the timing on the new product? Do we know it yet? Is it coming really soon now or is it one of those, you know, we've seen it, it's being worked on but it's still a little way out.

Richard Hicks: I think it's still a little bit way out. I can't speak officially obviously on Microsoft's behalf, but I know that the first beta has been out for awhile. I know that the second beta is forthcoming soon and so I would expect that Microsoft will run with that second beta for a period of time so I'm going to guess probably late two or three, maybe early q-4th by my best estimate.

Greg Hughes: So if I have a need right now, then the current product is something I can look at to try to meet those needs, but maybe in the future I might want to make a move to something like that, a new product.

Richard Hicks: Absolutely. There would certainly be upgrade perhaps and the good news is that if you purchase a Celestix MSA Security Appliance today and you have a valid support contract, you are eligible for upgrades so your investment is not wasted there. If you deploy ISA Server 2006 today, you certainly would not be throwing any money away in the event that the Threat Management Gateway comes out later this year.

Greg Hughes: One last question about the appliance, whether it's the appliance or the software I install myself, what about reporting? I mean, stuff that works really well and does a great job of blocking things and stateful inspection and keeping the bad guys out and letting the good guys get to just the things they are supposed to get to is great. One of the weaknesses in the past of a lot of different firewall and security systems has been my ability to do non-affiliation or to report and validate that's doing what it's supposed to do.

Richard Hicks: Sure. So what's reporting in the ISA Firewall, the reporting features are not terribly full-featured. The reporting in the product is not, in my personal opinion, is not that great. The good news about it is this. There are a multitude of third party vendors that actually sells fantastic reporting tools that integrate with the ISA Firewall and so although the base features in the product are adequate maybe for some people, if you need enhanced reporting features there are certainly a number of excellent third party products that do a much better job of advanced reporting and things of that nature. So that's generally been my recommendation. Take a look at the product, the based product for yourself. If the reporting, if the report on those things of that nature are not up to spec or don't meet your requirements, if you're not limited there, you can leverage third parties and get some wonderful reporting and advance features like that.

Greg Hughes: Great, and your company's appliance, is that something where -- any enhancements you've made or do you have the same abilities to leverage the same third parties, or how does that work for you guys?

Richard Hicks: No. So we don't include any enhancements with logging and reporting in our appliance, but the good thing is that our appliance, as you know, they're locked down but we don't lock you out. You can certainly install third party components because that's one of the features of the ISA Firewall, it's highly extensible. There is a tremendous third party ecosystem for advanced and enhanced products for the ISA Firewall, a lot of those, and one of those being logging and reporting and so yes, if you purchase an appliance you are certainly welcome to install third party utilities like that to enhance the base features.

Greg Hughes: Great. A lot of information today.

Richard Hicks: Very good.

Richard Campbell: Richard, thanks so much for coming on the show.

Greg Hughes: Yeah, we appreciate it.

Richard Hicks: Thanks for having me. It's been tremendous pleasure.

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