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 #147
(Transcription services provided by PWOP Productions)

Richard Hicks Gets Us Secure on the ForeFront!
February 10, 2010

[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 #147, with guest Richard Hicks, recorded Monday, January 18, 2010. 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. You're listening to RunAs Radio and with me as always, my co-host, Greg Hughes.

Greg Hughes: Hey Richard, how are you doing?

Richard Campbell: I'm well, sir.

Greg Hughes: Good.

Richard Campbell: Here we are again.

Greg Hughes: Here we are once again to do a good thing.

Richard Campbell: Yeah. Remember how to do this thing.

Greg Hughes: You know where that line comes from, right?

Richard Campbell: No.

Greg Hughes: Did you ever hear the old Chickenman radio show?

Richard Campbell: I guess I didn't.

Greg Hughes: Okay, if you've heard Chickenman then send an email to info@runasradio.com, we'll take a pool here. "Here I am once again to do a good thing," he's like the super...

Richard Campbell: Chickenman.

Greg Hughes: Anyway.

Richard Campbell: All right. It's good to know that about you, Greg.

Greg Hughes: Saving the world from...

Richard Campbell: There you go.

Greg Hughes: From something.

Richard Campbell: Let us introduce our guest. Richard Hicks is a Senior Sales Engineer and Product Specialist for edge security solutions at the Security Appliance Vendors Celestix Networks. He has been working with Forefront Threat Management Gateway 2010 and its predecessors for more than 12 years. He has designed and deployed network security solutions using TMG and ISA for SMB's, military and defense organizations, and Fortune 500 companies around the world. Richard is a Microsoft Most Valuable Professional in Forefront Security and his certifications include MCP, MCSE and the MTCS, and the Microsoft Certified Information Technology Professional Enterprise Admin which is an acronym that's entirely too long. Richard lives and works in beautiful, sunny Southern California. Welcome back, Rich.

Greg Hughes: Hi, Rich.

Richard Hicks: Great. Thanks for having me on, guys. I appreciate it.

Richard Campbell: Last time you were on the show we were really focused on ISA Server but that product's gone away on us.

Richard Hicks: It has, yes. If you recall when we talked about a year ago we did talk about ISA Server and we were talking about at that time it was ISA Server 2006. We spoke about this in, I think, 2009 and of course three years for any technology product is going to be a pretty long time. It's going to be a fairly old product, but in terms of a security product of course that is an eternity as Greg will probably attest to. Obviously the threat landscape changes dramatically over time and of course the attacks become more intelligent, more directed. Of course the latest iteration of this product, it's definitely time for an upgrade and it has some new features and functionalities that I think are going to be very compelling and definitely going to improve your customers' security posture when we deploy this.

Richard Campbell: So is this just a product name change that ISA Server is now called Threat Management Gateway?

Richard Hicks: Not simply or not just a name change. Certainly the name change was important. Microsoft is trying to essentially coral all of their security offerings under the Forefront umbrella. So of course Microsoft ISA Server, which is their access solution, as well as Microsoft's Intelligent Application Gateway either as a self ETM Remote Access Solution...

Greg Hughes: Right.

Richard Hicks: Those were both kind of rolled up under the Forefront umbrella and are now of

course included in the Forefront's suite of security products.

Greg Hughes: So ISA Server has become the Threat Management Gateway?

Richard Hicks: Correct. So this is the next iteration or the next evolution of the product ISA Server. Again, referred to now as Forefront Threat Management Gateway. The good news is, of course, it's not just simply a name change. The core of the product has been improved somewhat, but the good news is that there are a number of new features and functionalities that again, can greatly enhance security and provide protection.

Greg Hughes: So let's drill into that, but before we do why don't you talk about for an IT person who has never looked at this product before, what do they need to know about Threat Management Gateway? What is it? What kind of problems can it help them solve and how do you wrap your head around it?

Richard Hicks: Well, very good. Excellent question. So Forefront Threat Management Gateway at a high level is essentially an integrated edge security gateway. So first and foremost it is an enterprise class firewall. It is capable, of course, of performing packet filtering, table packet filtering but it is also an application layer or Layer-7 firewall. Built on top of the firewall core of course are proxy services. We can perform proxy services. We can also conduct content caching services as well as VPN services, both Remote Access and site-to-site. So it's very comprehensive in that manner. The new functionalities and features in Threat Management Gateway are somewhat compelling because we, again, are building on the former ISA Server 2006 product, but included in this now are some features that really make this a true comprehensive secure web gateway. So integrated into the gateway now are antivirus and anti-malware inspection, as well as URL filtering. These are not necessarily revolutionary products themselves, but now that they're integrated in with Microsoft's product it makes them a so much more robust solution. We have an all new vulnerability-based intrusion prevention system which I'm pretty excited for. That's actually very compelling and hopefully we can talk about that in a little bit more detail. We have the ability now to actually inspect at the application layer HTTPS communication. We can terminate and inspect outbound SSL encrypted communication. Also, we have some enhanced email protection features in Threat Management Gateway that allow for a very tight and unprecedented really integration with Exchange servers. Organizations that have a Microsoft centric network will certainly benefit from this, but it also will benefit networks and organizations that have non-managed clients or third party browsers or non-Microsoft operating systems as well.

Richard Campbell: So is this literally going to be your edge device here? Internet connection comes into this or do you have something in front of it?

Richard Hicks: Really that's a design choice. It certainly is capable of performing as an edge security firewall, but the good news is that the deployed models are flexible. The networking model is actually very robust in this product. You can deploy it as an edge security device. You could deploy it as a back firewall behind an existing edge firewall. Really the design options are very many. You can pretty much install this in any manner that you can imagine.

Richard Campbell: Well, and I get to sense that it's an all in one kind of thing so then I start thinking what about load balancing or other sort of edge technologies. Maybe I'm thinking going too far here. It's not really meant for that.

Richard Hicks: Oh no, no. So it definitely has a number of roles and features. The good news is that of course it really can be deployed in all of those roles or really in the subset of them. So it has already all of these features. It's not necessary that you enable every single one, and in a lot of cases it's probably not going to be feasible to deploy it in all of these roles. In those cases you might have an independent array of Threat Management Gateway firewalls that are use for your outbound proxy. You might have another set that's used perhaps for antivirus inspection. You may have another set of firewalls that are used to deploy for email protection, those types of things. It's very scalable. There is Threat Management Gateway Enterprise Edition which allows you to build out clustered arrays of TMG Firewalls. These are arrays or essentially groups of firewalls that you can manage at a single logical unit. You can actually enable network road balancing on these firewalls and actually have a single IP address that addresses the array. In those cases you can build out clustered arrays up to eight nodes, I think, with network load balancing. It will actually support more, but what we're finding is that function is talking about eight nodes.

Richard Campbell: And I've run into that number with NLP doing web stuff as well. It's just one of those sorts of magic numbers. Now why would you want a cluster of Forefront service like that? Is it just to handle a large number of connections?

Richard Hicks: It certainly handles a large number of connections, but of course even in small environments customers are looking for high availability.

Greg Hughes: Right.

Richard Hicks: They don't want to lose internet access that's vital to their business and any business

that really relies on internet communication, at a minimum for email but certainly for collaboration and everything else. So it's always desirable to have high availability. You can create a simple two-note cluster just to have high availability.

Greg Hughes: Sure.

Richard Hicks: Also we have new features in, since we're talking about high availability, one of the new features in Threat Management Gateway is of course ISP redundancy. This is new to the product. It allows you to both balance and provide failover capabilities for ISPs.

Greg Hughes: So you can have multiple internet providers and the product will help you to make that work.

Richard Hicks: Absolutely yes. So if you have two ISPs, and it's not uncommon for even small businesses to have a couple of ISP connections...

Greg Hughes: Sure.

Richard Hicks: The Threat Management Gateway can handle both of those and load balance traffic between them. Very granular in terms of load balancing capability so we can decide to send – we can do almost an active passage solution where we send all of the traffic over one and in the event of an outage we roll it over to the other. We can load balance it in any fashion that we see. We can split it 50-50, 70-30 if they want, those types of things. It definitely makes for a much more available solution.

Greg Hughes: So this is stuff that we used to do at the router than in a lot of different places, because it sounds like a lot of different capabilities being sort of packaged into one big application.

Richard Hicks: Absolutely. Yes, yes.

Greg Hughes: Now, one of the things about ISA Server, if I remember correctly and tell me if I'm wrong, but as I recall you couldn't run it on a 64-bit platform. Is that right?

Richard Hicks: That's correct. So ISA Server 2006 was 32-bit. Threat Management Gateway is completely 64-bit. There are no 32-bit versions of TMG so that's great. It runs on Windows Servers 2008 and Windows Server 2008 R2, and of course we recommend Server 2008 R2 because it has the latest operating system but that's definitely a positive thing for the TMG firewall because the firewall certainly relies on the underlying operating system for its security and in this case of course Sever 2008 R2 is a fantastic platform for Threat Management Gateway.

Richard Campbell: So what's the coupling with Exchange exactly that doesn't seem obvious? Is it spam filtering?

Richard Hicks: A little bit of everything actually. So the enhanced protection that is included with Threat Management Gateway essentially in terms of the integration is the fact that we can actually install the Exchange, its transport rolled directly on the TMG firewall.

Richard Campbell: Okay.

Richard Hicks: No longer do you have to have separate Exchange edge transport device perhaps behind another firewall or something like that. We can actually install that directly on the TMG Firewall so you have a single edge security device that not only is your edge firewall but it is also your Exchange edge transport server. We can also install Forefront protection for Exchange directly on the TMG device so you can actually manage all of that with one solution and actually manage it all in TMG console. So not only the access policies for the edge firewall, but now your Exchange edge configuration as well as your spam filtering and email antivirus which is a part of Forefront protection for Exchange all installed on the same device. And of course again as we have spoken about earlier, with TMG Enterprise we have the ability to create clustered arrays and do that same thing and have high availability for our Exchange edge transport.

Richard Campbell: It's very interesting. Celestix makes an appliance approach. Of course everyone thinks of Microsoft as a software company, but you guys actually packaged this up as hardware.

Richard Hicks: That's correct. So we have a kind of term, Key Solution. So our solution is Celestix's MSA security appliances hardware version of Microsoft's Forefront Threat Management Gateway. Our appliances should be available some time in February and when that's available you'll be able to actually purchase a hardened pre-installed, pre-configured TMG appliance. What we do is we kind of package this up. We have some value added components that are in the appliance.

Greg Hughes: Right.

Richard Hicks: Really the selling point here is kind of the term Key Solution. We take the pain of installing and configuring all of the software out of it for you and take that out of the equation so that you can actually install, configure, and deploy Threat Management Gateway a lot easier and a lot more simpler than having to do it yourself.

Richard Campbell: But in the end it's just a chunk of software. You can install it on any machine you want. Is there any real special requirement to the

hardware, or is it just like two NICs is the minimum kind of thing?

Richard Hicks: Actually you can deploy it with a single network interface. Of course there are some amount of patience to what it can do with only a single network. The minimum recommended, not required, recommended of course is two network interfaces. Depending on your configuration, two network interfaces is certainly might work. In terms of hardware, of course when we talk about hardware the TMG has a lot of features and functionalities that perform a lot of application layer and inspection and it's sensitive of course to latency. So we like to be generous with the hardware on the Threat Management Gateway because any time you're doing application layer, traffic inspection, URL filtering, malware and antivirus inspection, those types of things, network inspection, those types of things again are very time sensitive and in the latency they produce a poor end-user experience so we want to be as generous as we can on the edge security device with our hardware.

Richard Campbell: When you're digging into every packet across the scene of the network, that's a lot packets.

Richard Hicks: That's correct and there are times when we're operating on streams so we actually have to essentially store some of that communication stream in order to perform inspection on it. So we're actually queuing some of that up as well so it's very important that we be generous with the hardware there.

Richard Campbell: I took a peek on Microsoft's website at the Forefront area and there are 9, 10 products named Forefront.

Greg Hughes: It's kind of like same office.

Richard Hicks: That's correct, yes.

Richard Campbell: It's just, oh my goodness, like how do you sort all these out. So we've really only talked about Threat Management Gateway which is one of the Forefront products.

Richard Hicks: Correct.

Richard Campbell: Some of these sound small. I mean, Forefront Protection for Exchange Server, that sounds like something that is also built in the Threat Management Gateway.

Richard Hicks: You can integrate that with Threat Management Gateway, but essentially that is Microsoft's email protection software.

Richard Campbell: Right. Are there other big ones here? I mean some of these look relatively simple pieces of software: Identity Manager, Security Console.

Greg Hughes: I can tell you Identity Manager is not simple.

Richard Campbell: Oh, I get amaze with that.

Greg Hughes: Dealing with that right now is not simple. It's quite powerful and really is a pretty cool product.

Richard Hicks: The Forefront Protection Manager suite includes a lot of different software to protect Microsoft's infrastructure so some of the big ones of course are Forefront Protection for Exchange which is the Exchange email protection software. There is Forefront Protection for SharePoint. Of course that protects our SharePoint system. Forefront Endpoint Protection which of course is our desktop and server-based antivirus.

Greg Hughes: Right.

Richard Hicks: There's -- I'm trying to think here, there's a number of different Forefront Protection suite that are used. Again, this is Microsoft security software platform. Also, Forefront Protection Manager is fairly compelling because with Forefront Protection Manager, this is formerly codenamed Sterling, with Forefront Protection Manager we can actually managed all of our endpoint protection products in the Forefront suite in a single console including integration with Threat Management Gateway. The compelling thing about Forefront Protection Manager is that it is a dynamic kind of event-driven application and since it's integrated and monitoring all of your security endpoints we can, as a security administrator, we can actually define security events and actions that might take place based on an event. So for example, let's say for instance a user comes in to his desktop, plugs in his flash drive and he has a virus infected Word document on the flash drive, Forefront Endpoint Protection will detect that and it will of course signal the Forefront Protection Manager console. At that point, the Forefront Protection Manager console recognizes that of course the user has a virus on his desktop and as the security administrator I can make a number of decisions based on that event. First thing off I may want to just prevent internet access until I have completed a scan on his workstation. So at this point Forefront Protection Manager will actually signal Threat Management Gateway and we can block his internet access and at that point I can perhaps also kick off and scan his email box so it will actually signal Forefront Protection for Exchange to go ahead and kick off his scan on his email box. There are a lot of different things that can handle this Forefront Protection Manager, a very compelling software, and if you're deploying Microsoft Forefront Protection suite

definitely something to consider and something to look into.

Richard Campbell: Somehow I have this vision of the movie Brazil. And then three guys come out of the ceiling on ropes, grab the guy, put him in a bag and disappeared down the hallway.

Richard Hicks: Exactly.

Greg Hughes: That's random.

Richard Hicks: Absolutely.

Richard Campbell: Security, darn it.

Greg Hughes: That's security.

Richard Hicks: Taken seriously. Absolutely, absolutely.

Richard Campbell: I like the idea of a common console so that right down to a bad USB key you sort of work your way back. Does NAP fit into this anywhere, Network Access Protection? Because my immediate thought when you mention NAP part was, hey, that machine is no longer safe. I'm not so worried about keeping them off the internet. I'm worried about keeping them off the servers.

Richard Hicks: Oh yes, absolutely. Threat Management Gateway integration with NAP is really confined to Remote Access VPN. So if the user comes in via the Remote Access VPN component provided by the Threat Management Gateway, we can integrate with NAP and enforce our security policies that way.

Richard Campbell: That's cool. The other product here that caught my attention was Forefront Unified Access Gateway. That sounds like a sort of superset product.

Richard Hicks: Essentially yes. So Forefront Unified Access Gateway is the latest revision of the Microsoft Intelligent Application Gateway or IAG software. This is Microsoft's Remote Access offering. This is essentially an SSL VPN but it certainly does much more than that. Unified Access Gateway is essentially a Remote Access solution. As we've talked about with Threat Management Gateway, it's an integrated edge security gateway that offers a number of different roles. Essentially Unified Access Gateway takes one of those roles, the Remote Access role, and kind of super charges that. UAG is the remote access solution of choice for Microsoft products. It is an SSL VPN, but it's certainly much more than that. With the Unified Access Gateway, we have the ability to create application portals. We have the ability to -- it's highly extensible and highly customizable so we can really do a lot of different things with Unified Access Gateway. Right now the most compelling reason of course to deploy Unified Access Gateway is that you're considering a Direct Access solution. I know sometime last year you guys had Dana Epp on. He was talking about Direct Access.

Greg Hughes: Right.

Richard Campbell: Right. Direct Access is like the replacement for VPN access...

Richard Hicks: Yes. It really is the future of Remote Access.

Richard Campbell: Right.

Richard Hicks: It is instant access, always on access for the enterprise, and the nice part of that, well, of course Direct Access as Dana had mentioned is really built into Windows infrastructure.

Greg Hughes: Right.

Richard Hicks: UAG essentially adds significant value to an existing or to your post Direct Access solution. With UAG of course we have the ability to provide high availability to a Direct Access solution which is not available or very difficult to implement without UAG. Also, UAG has some new IPv6 transition technologies that essentially make it so that when you deploy UAG with Direct Access you do not need to have native IPV6 running anywhere in your Microsoft environment. It only really needs to be running on the UAG gateway and we can transition and we could make applications available that are native IPv4 available through Direct Access which is something that you cannot do without UAG.

Richard Campbell: Yeah. Dana mentioned that you have to have the IPv6 stack running on the Win 7.0 client machine as well as on the R2 server.

Greg Hughes: Right. To take advantage of that.

Richard Campbell: So UAG eliminates that requirement?

Richard Hicks: It eliminates that requirement from your backend application. So I can have a native application server on the backend running IPv4 and not having an IPv6 stack on it.

Richard Campbell: Okay.

Richard Hicks: So the Windows 2000 box or a Windows 2003 box without IPv6 running on it. With UAG and with some of the transition technologies like DNS64 and NAT64, we have the ability to actually extend those over Direct Access without having native IPv6 running on the backend server. That's not available with the Vanilla Direct Access

implementation that's available in standard Windows products outside of UAG.

Greg Hughes: Is that sort of like a publishing model? They're publishing it out to an IPv6 network...?

Richard Hicks: Yup.

Greg Hughes: As kind of a proxy?

Richard Hicks: Correct, reverse proxy essentially. Yes.

Greg Hughes: Got you.

Richard Campbell: So it sounds to me, you know, Direct Access comes with R2 and is sort of the plain Jane version. If you want to spend a little money on it, and it sounds like a good idea to do so, you buy Forefront UAG and you take Direct Access up a notch.

Richard Hicks: Absolutely. You take it up a notch in terms of it's certainly easier to deploy because of the transition technologies that are included in UAG and also provides for high availability like I cannot imagine anyone wanting to deploy a solution like Direct Access without some basic high availability and UAG provides it.

Greg Hughes: So I guess I'm curious. If you take UAG next to TMG (our EIEIO world here,)

[Laughter]

so if you take those two things next to each other there's some redundancy between the products. But when you use them together, do they integrate directly together? Is it a tight integration or are you deploying a second product in UAG that sort of trumps the other product but they're separate from each other, or is there something a little bit in between where they have a touch point but they're not necessarily tightly integrated?

Richard Hicks: Well, that's a great question and one certainly that we get quite often. So what I like to say is that these two products are very complimentary. They do have some overlap in their capabilities. So again with Threat Management Gateway, it really is an access solution. Threat Management Gateway always is really about protecting our corporate users when they're accessing internet. So it's really an outbound access solution. However, it does have some remote access capabilities. So in other words it does support client-based VPN. It does support site-to-site VPN as well. Now with Unified Access Gateway, essentially this is a premium remote access solution. If you have limited or very simple remote access requirements, Threat Management Gateway may meet those requirements. However, if you're going to want to have more detailed and more granular endpoint protection -- excuse me, more detailed and more granular endpoint inspection, then UAG is your choice. If you want Direct Access and want high availability for Direct Access, then UAG is your choice. But there maybe times when you actually deploy both. Like there maybe times when you have an environment where you're trying to protect your inside users accessing the internet and we want the capabilities of Integrated Gateway Antivirus, we want the URLs filtering, we want to be able to inspect outbound SSL encrypt to traffic so that we can protect our internal users when they're going out to the internet, UAG does not do that. UAG is purely a Remote Access solution today and so UAG is really about allowing access into our network securely.

Greg Hughes: So I guess when I think about these products we talk about a common management interface. What does that really mean from a day to day standpoint? I mean the cost of managing these things really or these products, a lot of the times -- for this class of products, not just the Forefront stuff but just security and a lot of IT infrastructure products in general, isn't so much in the upfront cost, the acquisition and the deployment. It's in the use of it overtime. Is there a capability in the Forefront suite for common policy across products if you use the unified or centralized management interface? Are there are some things that I can get extra by deploying it that way that make me more efficient?

Richard Hicks: Absolutely. So at a low level if we're talking simply about Threat Management Gateway, absolutely. So we have the ability to manage any number of firewalls at a single manager console, and depending on your configuration you can actually manage them with a single firewall policy with Unified Access Gateway. Unified Access Gateway now has support for clustered arrays and you get the same capabilities. I can manage a group of UAG, Remote Access Servers with a common policy. Now, from a higher level if you're looking at this from a Forefront security suite view you can manage those from a single point using Forefront Protection Manager and in that case what you have is a single management console that has the ability to configure and interact with all of the Forefront Protection suite products. So yes, you do have a single management console. You don't have multiple products that you have to manage with multiple different consoles and learn a number of different types of user interfaces. You have a common user interface and of course with Microsoft, Microsoft products are very typically easy to install, easy to configure, easy to deploy, easy to maintain, and easy to manage. Their user interfaces are usually very intuitive and you have a common looking field across all of the Forefront Protection products like that. So yeah.

Greg Hughes: I guess my question even a little more specifically is, and I'm asking this in the blind, I don't know the answer to it, but when think about managing multiple applications at a single console, one of the things that helps me to be consistent is if I can write one set of policies, security policies if you will, which will then be pushed out to and consumed by all the different applications that are out there. So in other words if I have some inbound access management in one product and a little bit in the other product that I can write one policy that then can be leverage across all those applications that might consume that portion of my security policy, that's kind of where I was going. Is that there today? Is it something that might be there in the future?

Richard Hicks: To some extent, yes, and again that will be done with Forefront Protection Manager. Now, with Forefront Manager I don't think that you can actually write like firewall policies with that and Remote Access policies, but certainly you can enforce a general security policy across a broad suite of Forefront section endpoints. But today it doesn't have the ability, at least to my knowledge, to actually install and configure access policies on the firewall, configure Remote Access policies on the UAG system and so forth, but we're probably getting there at some point but we're not quite there today.

Greg Hughes: Okay, fair enough.

Richard Campbell: Guys, we're just about out of time. Richard, any final words?

Richard Hicks: No, not really. You know, as I've said before the Threat Management Gateway, is an excellent product has a lot of new features and functionalities. I encourage you to go out to their website and take a look at that, and of course I have to throw in a plug for the people who pay my pay check and that is Celestix Network. If you're looking to deploy this quickly and easily, I would certainly encourage you to look at the hardware client version of Threat Management Gateway. We have those coming out in the next month or so -- so it should be good.

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

Greg Hughes: Thanks, Richard.

Richard Hicks: Thanks. It was great.

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