

SonicWALL CEO: Application awareness crucial for IT security

BY JOHN GALLANT, ERIC KNORR, NETWORK WORLD

SonicWALL® once focused on small and midsize businesses, but its introduction earlier this year of a next-generation firewall line dubbed SuperMassive E10000 Series leaves no doubt that the company is now taking aim at larger enterprises. In fact, the privately-held San Jose company's CEO, Matt Medeiros, says the enterprise market accounted for nearly half of SonicWALL's sales over the past six months. In this installment of the IDG Enterprise CEO Interview Series, Medeiros spoke recently with IDG Enterprise Chief Content Officer John Gallant and InfoWorld Editor-in-Chief Eric Knorr.

What's SonicWALL's general approach to IT security?

There is still a substantial amount of bad malware, viruses and Trojans being written by sophisticated software development teams that are invading your networks at any moment, and our primary service is stopping that from happening. Second to that, it is our fundamental belief that organizations need to enable their networks and employees to be more productive. Four years ago, there were mostly really restricted policies -- you know, don't let things happen in your network that you're not in control of. Forbid people from bringing their own devices onto the network, using their own applications at home and even tapping into the network unless they're on the LAN. We fundamentally believe very differently. We have to unleash the power of the network. We want to enable people to use any device anywhere and use any type of application that is business worthy on the network and then give you the CIO, CFO or CEO the power to mitigate how much time, where, who and what has access to that information, those applications and those business processes that are important.

Our readership deals with lots of security companies. What sets SonicWALL apart?

We provide the best firewall, which is primarily focused on malware. We also bring an integrated set of features that complement the security aspects of your network, but that enable you to maintain your network in a far more productive

way. Instead of having a discrete device, we have integrated features like gateway AV, IPS, filtering and blocking, and there are now application awareness features allowing you to look at who's utilizing your network and the way that they are utilizing their network. In addition, we've incorporated things like SSL VPN, email security/anti-spam.

Who's the SonicWALL customer? Traditionally you've been more SMB focused, but with the SuperMassive firewall featuring more than 40 Gbps of throughput you're moving way upscale.

About five years ago we made the decision to move upscale and the reason why we made that decision is because we not only were providing security for small businesses, we were also doing a lot of distributed remote branch office work primarily for corporate enterprises. They came to us and said "Look, you guys are doing a great job at the edge, at our remote branch offices and we think you have an opportunity to play here at the hub." So we developed a product road map that would suggest we could do that. I'm pleased to report that 45% of our revenue for the last six months has come from enterprises -- anything above 1,000 employees.

ANALYSIS: Is a next-gen firewall in your future?

A lot of people challenge us over "Well, how are we going to get away from our SMB roots?" But I have never seen a virus or malware that is prejudicial. Sorry, you're a small company so you get a small virus and you know what, you're the big guy so we're sending you the big heavy load. It just doesn't work that way. So from our perspective, we always had the technology. What we needed to do is recognize it was a completely different capacity level at the hub of the data center and there were certain features that were going to make a big difference in that data center environment that we didn't necessarily have to provide in an SMB environment.

Could you address your competitors in the heavyweight class as well?

The 800-pound gorilla is Cisco, Juniper, Check Point, Fortinet, those are the companies we are competing with as well.

If we're up for a bonafide RFP where they

truly aren't just shopping and trying to negotiate for the incumbent, we are doing very well. It's really all about just getting the at-bats.

That was a good segue. Your appliance approach: how are you approaching this differently than the Cisco's and the others you mentioned?

First of all, we believe in a multilayered approach, not only an appliance approach. We do provide things like an enforced AV on a client. We do provide SSL VPN, which you could argue is all about mobility and the ability to create a far more secure environment with mobile types of infrastructures.

At the appliance level for the firewall we have a very strong belief that for the near term the appliance model is the most secure way of managing the data center firewall. We can provide on an hourly basis updates and feeds to advance their signature database, to advance the performance of those products. You won't be able to get that in a virtualized world. It's not that we don't believe that the firewall will ever be virtualized. In fact, we have virtualized firewalls within our firewall. But we believe that the hardware allows us to provide a level of security that you can't get just in a software environment. Think of it no differently than a key lock on your door. There are at any point in time hundreds of thousands of knocks on the door trying to get in. Somebody's trying that key to get in. I get to change not only the software signatures that prevent them from getting in, I do far more changes on a continued basis.

The other issue is just purely network performance. People will argue with an appliance you actually induce latency. Well, the good news is Moore's Law applies to security hardware products as well, so you'll see today that we've introduced our flagship product -- the SuperMassive -- which is a multicore solution exceeding expectations on throughput and featuring full deep packet inspection.

I want to ask you about three different trends and how you're helping customers deal with them. The first one is cloud computing and it really has two angles. One is how does cloud change the security issues that customers are dealing with and how do you help them with that, and two, are you going

to be moving your capabilities into the cloud?

For the last six years we've actually been deploying our products into clouds, so many of our resellers provide Managed Security Services that use not just our firewall, but our email security, our SSL VPN and even our CDP [Continuous Data Protection]. When the company was founded all of its signature database and content management was managed in the cloud. Our customers don't see a dataset. The memory of our device, which makes our device extremely affordable, is not burdened by having to have a hard drive or having to have a substantial amount of memory to load all these signatures. We have over a million installed base users, so they've always been managed by a cloud, so we had kind of an advantage going into this cloud phenomena because we were in fact a cloud already.

Where do I think the importance of the cloud relative to security is? First of all we see far more private clouds than public clouds, especially at the enterprise. People are learning their way about what things really make sense being in the cloud and what stuff really should be resident in the physicalness of a location. In our experience with branch office kind of work, we're watching customers take this whole cloud thing already full circle. They thought they were going to do this in the cloud and now are already back to pulling the hardware utilization back into the infrastructure.

But don't you consider your Managed Service Provider customers as offering public clouds?

In some ways they are except for the fact that some of them will offer partitioned services for public and private cloud services.

For anti-spam on content filtering, what's the ratio between appliance and service customers?

About six months ago we made a decision to take anti-spam and move it onto the firewall, but it is a cloud service, so it's all done in the cloud. When I measure it from our traditional here's your email security solution to the service that we're now providing on any firewall device it's been a massive migration. That's more of an admission that people are tired of manipulating or augmenting each change. I also think that it's an admission that we probably have still a substantial excess capacity of Exchange mailboxes. One of the first things that was a consequence of the great recession was the fact that from an IT perspective you were sitting on a whole more mail capacity than you probably needed and that Exchange is not easy to deal with and it's probably easier to just watch for spam at the first device, at the perimeter. People didn't have the microprocessor capacity to do it, but we overcame that.

So you have partners that offer Managed Security Services, but do you as a company offer cloud-based services?

All of our services - content filtering, anti-spam, SSL VPN, etc. -- are really cloud-based. I think there will be extensions of this. I think you're going to hear from SonicWALL as we develop

the next generation of user portals - this whole application awareness campaign gives us great promise that there might also be different levels of cloud services that we can provide around applications and aggregation.

In terms of the second major trend -- mobility -- we're hearing more and more about how mobile clients give people freedom to use what they want to use, but at the same time there's the challenge of keeping them safe and secure. How are you helping companies deal with that?

What I'm so excited about what we're doing is it's no longer about tethering what gets done on my network. It's unleashing what gets done on my network. We fundamentally believe if we can make your employees more productive in any way shape or form there's a huge ROI for that. SonicWALL itself lets our people pretty much bring in what they want to use on the network. Now my job is to make them more secure.

In terms of security for mobility, what needs to change?

Very little has to change except for attitudes. Instead of stopping people from bringing in their iPads™ or iPhones®, Android®, Windows 7®, the new Palm OS, start opening that up and encouraging it. Now you have to decide what you want that individual and device to really have access to [around the clock].

But how does that work from a security architecture standpoint?

It is difficult because now you have to make sure that you've got this flexible model that you can really deploy, but what it really says is your threat center has got to be very good at understanding where the malware really is and where the attack premise is going to be. Second, you need to provide application awareness because there are certain applications that even though I'm letting you bring in your own device I'm not going to let you get Limewire or BitTorrent up. I'll give you a great example. We use Facebook to market our company, but I don't let our people get on Farmville. It's just notorious for malware, so we're just going to stop that aspect of it. The other thing that I think the CIO, CEO and CFO want to know is OK great, Jack has responsibility for messaging what SonicWALL is doing, but when we see Jack spending 30 hours a week on Facebook we probably have an opinion that that's not 100% SonicWALL work and we can now start to have an informed way of helping that firm be more productive. If you can help change behavior in a proactive way, you can enable a new purpose and a perspective of where IT becomes a healthier arm in the business.

Let's talk specifically about social networking. How do you help them enable the good and disable the bad?

One of the things we're really excited about with our new product introduction is this application awareness and the fact that we can get so granular at allowing, not allowing, even prescribing duration for someone. As much as I want Jack utilizing Facebook and Twitter as a means for

us to market and communicate, I certainly don't want Jack spending 30 hours a week there and if he's spending 30 hours a week, let's have an informed discussion with Jack about what is really happening. Behaviors start to change.

Getting away from this topic a little bit. You acquired a continuous data protection company a while ago. How's that part of the business doing?

We're very excited about a product that we launched at the very end of last year. It's our second generation continuous data protection backup and recovery product. It's really a small networks solution today and so we've got thousands of customers that are enjoying real-time backup. I can literally go back in and retrieve a file that I just screwed up. The user control elevates the backup and recovery process. From an IT perspective, remote branch offices hardly ever get backed up. The cost of transmission to back up was really expensive.

Do you plan on expanding that part of the business?

Yes. I think it's an area that we've now had two, three years of good success in. I think you should look at continued investment on SonicWALL's part. It's one of the reasons we are very excited about being taken private by Thoma Bravo. Look for things like virtualizing the software. Look for us to also start to add more application awareness in CDP and far more security features. I am still amazed at how many people back up the virus that brought the networks down.

Talk about another product line: the next-gen firewall. What is it?

We've always been a UTM (unified threat management) player so we understand what a UTM device is - it is a firewall. It is a gateway solution. It is an intrusion prevention, intrusion detection device. We stack on top of that content filtering, anti-spam, SSL VPN, so there's a few features that we've incorporated on top of that UTM device that others don't include in their definition of UTM, so that's the core of what UTM is today. Now when you add on top of that the ability to do application awareness and control as well as visualization, now you're at the next-generation firewall. The ability to see what's going on in your network, to visualize it and then prescribe specific ways to improve security, network productivity and employee productivity, that's the next-generation firewall.

Talk about how that market is developing. There's a sense that next-gen firewall market is still down in the low gear.

I don't think so at all. First of all, there are over 22 million first generation firewalls out there. Those firewalls, if you just look at our installed base, the average life cycle is three to five years, so there's a huge upgrade opportunity that's going to happen just because people will buy the logic that this application awareness addition is a very important part of the next way for IT departments to be far more in line with the business objectives of a company. They can be seen as a business provider, not a business

limiter, and that's going to be a calling for CIOs to want to replace their existing firewalls. The second thing is you don't necessarily have to disconnect. We would argue don't disconnect your gen one firewall. Keep it in the same position it is in and let it just be a bump in the wire until you can start to roll out these new features and policies.

Is there anything specific that you have had to do for highly virtualized environments?

We do definitely see more virtualized environments for SSL VPN, for email security in the traditional sense and certainly see it also in some aspects of virtualizing the security feeds and signatures in the database. We are also working on virtualizing firewalls within a firewall device.

I was looking at research your folks put out about the amount of malware activity in the past year. Does it get to a point where we can't keep up with it the way we're dealing with it today?

You could go do the math and suggest there's no way anybody's going to keep up with that type of growth rate. But we are keeping up -- we're ahead of it. Our technology is so different than anybody else's, Reassembly-Free Deep Packet Inspection™. The fact that we're looking at every packet, the fact that there's no proxy involved, the fact that we can look at any file size, any protocol, really gives us the advantage. Now, on the other hand, the math would tell you that if we start to see a substantial multiplication of malware we're all going to have trouble. The answer unfortunately is that you start to do more blocking. The answer is we've got to get better at IP reputation and that's where we're investing a substantial amount of our time and why we always believe that building that into the email security business may not necessarily be about email itself and spam elimination. But what we felt was the reputation of that spam provided us

with a direct link to potential malware creation and we've proven that to be true. We think there's also more to be done around you and I from an authentication standpoint. I'm really excited about some of the stuff that we're seeing relative to two-factor authentication. By way of example, my iPhone has a camera. It also has a specific IP address. It also has my password. It also has a cell number. There's a lot of really good data that if we correlated this properly it would work. The camera, the benefit of it, is I can get a retina scan, so if all this data is lined up right and you have a retina scan it's probably me sending that email.

What are your development priorities for 2011?

We want to perfect application awareness. We think that there is a tremendous amount of network and employee productivity that can be gained. There's so many new applications that are going to be important and possibly much more leading edge than your ERP or CRM applications today.

All environments are different. Can you make a generalization about the right approach to application awareness?

You've got to take a good look at what's going on in your network and take the time to understand what's happening. Don't get into the behavior of "a-ha" when you turn on application intelligence and just block, block, block. The most important thing is to get the data pool right, get the business structure right. Why is it that this person is doing this and what are they doing it for? Get into a healthy conversation about that -- and we have done that -- and I can tell you that our people are working longer and harder. You might look at the data pool and see that 20% of the time people are doing things that I would not constitute as work but guess what: they're working 12 hours, 14 hours a day. If business leaders approach application aware-

ness the right way, they're going to be heroes, not goats.

My last question has to do with acquisitions because that's something that really defines the security industry. There's a tremendous amount of activity there, so what's your strategy in terms of building or buying innovation, and also, is SonicWALL a target?

Acquisitions have happened in the security industry because of integration. People want to integrate features. We're a great example of it. When we bought MailFrontier we bought it for the spam feeds and IP reputation database. When we bought Aventail we bought SSL VPN technology. We believe fundamentally this mobile environment is going to explode. We needed to provide remote access connection securely. We integrated it under our firewall. CDP we're going to take the other way. We think that with data at rest there's a huge opportunity for us to take some of the features that we have in our firewall and pull it in that environment and make data at rest a better and a more productive environment.

SonicWALL has done five acquisitions since I have been here, so we've been kind of a serial acquiring company. I think it's going to continue for technology in search of a channel for us. We're going to continue to look at things. Relative to SonicWALL, people might say "Hey maybe they're off the market because they've gone private." First and foremost we are an independent company. We didn't get acquired by Cisco or HP or Dell or IBM or Check Point or McAfee. Is there potential for SonicWALL to become part of an acquisition for a major company? Over time I certainly would think that would be an opportunity for somebody to look at. If you read our proxy on the transaction of going private there wasn't only one person knocking at the door.



SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com