Best Practices: Network Border Protection

featuring Rachel Kartch as Interviewed by Suzanne Miller

Suzanne Miller: Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University's Software Engineering Institute. The SEI is a federally funded research and development center operated by Carnegie Mellon University and sponsored by the U.S. Department of Defense and. Today's podcast is available on the SEI website at sei.cmu.edu/podcasts.

My name is Suzanne Miller. I am a principal researcher here at the SEI. Today I am very pleased to introduce you to our guest, Rachel Kartch. She is the technical manager for situational awareness in the SEI's CERT Division. Today, we are here to talk about network border protection, part of our Best Practices Series.

Before we get into that, I wanted to ask you a little bit about how you came to be here. What is it about the SEI that brought you into this work, and what is it that you hope to accomplish with it?

Rachel Kartch: Well, thanks, glad to be here. Prior to coming to the SEI, I worked in private industry as a network engineer for close to 15 years. I came to the SEI in part because I saw a way to help make a difference for our sponsors using a lot of the things that I learned from actually doing the job in private industry and finding ways to help use what I learned to help other people do things better.

Suzanne: OK. So you are basically very much in tune with our major mission of transitioning better practices into the software engineering, and in your case, the information security community. That is always good.

So network border protection, our topic today, is about our borders around our organization's data, which is one of the valuable things that each organization tries to protect. Let us talk about what is it about network border protection that is problematic, and what kinds of things are we researching at the SEI to help deal with the issues in protecting your network borders?

Rachel: Sure. Network border protection—that is just one piece of what has to be a multi-faceted and multi-layered approach to security. I think way back in the day, back when I was a network engineer, a lot of times people had this idea that all you really needed was a good firewall. You needed this one device, and you would keep all the bad stuff out and keep all the good stuff in. Obviously, we all know that that is not the truth. We all know that you need to have lots of different security tools. You need to have lots of different approaches. In some cases, you need special policies. You need a lot of different tools in your tool bag to maintain security for your entire organization.

Network border protection is just one of those tools. Even so, it is a little more complicated than just saying, *Protect the border*. Because most organizations that we work with, and most of the organizations that I worked at, prior to coming to the SEI, actually have multiple layers to the border. So that is what creates the challenge. Because frankly, in my experience, I find that there’s often errors of either doing too much or doing too little at different places in the border.

It seems like an important topic for us to cover because it is a critical part of anybody’s defense. Like I said, it is not the only thing, but it is critical. So we wanted to just address some of the best practices.

Suzanne: It is like putting a lock on the door. If you have a lock on the door, you have to decide who to give keys to, and that is part of that decision of who gets into what pieces. But if you do not have a lock on the door, then anybody can get in. And so you really do not want to go there, either. That is the first thing, I think, is we do not want everybody getting in.

What are some of the things that you have learned in terms of working in this area that are helpful to people that are trying to make decisions about how much, how far? The contrast between usability and security is one that immediately comes up in this when you start talking about policies. So how do we help people to make those kinds of determinations?

Rachel: Well, for every organization it is ultimately going to be different. Every organization has to assess their own needs based on what it is they are actually trying to do, what their business is, what their users need. There are always going to be, let us say, opportunities for people to decide for themselves.

One of the things that we like to share with people, though, is at a very broad level here is a way to approach the problem. When we are talking about network border protection, typically most of our larger organizations will have a router at the Internet like something at the Internet border. Then, on the inside, just beyond that router they will have a firewall.

So we talk to people about what is the best general approach to securing the border at the Internet router, and then what do you do on the firewall. Then within those best practices, there is opportunity for people to assess their own needs and to make specific decisions that are relevant to their situation.

Suzanne: So, take for example, organizations that are engaged in collaborations with other organizations. Everybody's got a firewall, an internet, and we have to figure out how to allow—I have heard tunneling used—how do we let them through the tunnel and keep other people out? So this is one of the decision areas that people have to pay attention to. Because if those people that I like cannot get through the tunnel, we cannot work together.

Rachel: Absolutely. The key part of that is knowing all of those requirements. That is frequently very challenging, especially if you are dealing with an organization that has grown over time, maybe an organization where there was a merger or an acquisition. So different business units have now come together. Maybe the requirements in what was going on were not very thoroughly documented to begin with, and so now you are in a situation where people can say, *Well, I know we have got some business partners that we need to allow through the firewall, but we do not have the list of all the IP addresses. We do not have a list of all the users*. That can become very challenging because you know that you have this need. You have to allow certain things through, but you do not necessarily have clearly documented, *What were all the things that we needed to allow through*.

Frequently, people are very sensitive to the risk of stopping business, the risk of accidentally shutting down a connection that needs to be kept open. In particular, if you look at certain industries, for instance, financial, if you accidentally terminate a connection that a trader was using to do something that was very time-sensitive, there is a huge business problem there. And people are very worried about that risk.

Unfortunately, what we sometimes see result is that people say, *Well, I can't risk accidentally shutting down something that was supposed to be kept open*. So they err on the other side of letting too much stuff through. That is why one of the key things that any organization should do when they are looking at their policy for network border filtering is understanding what is supposed to be allowed through? That can sometimes be a project in and of itself, doing the research, working with all the business groups, working with all the user groups, understanding everything that is supposed to be permitted, and at some point making the decision about whether to say, *OK, we now have to go ahead and close down some of these holes because we have not found anybody who can admit to ownership of allowing this connection through*.

That is potentially a risk, and every organization needs to reach a point where they can say, *All right, we have done all the research we can. We now accept the risk. We need to close some of these holes for our security*.

Suzanne: For organizations that are kind of in that position of, *I am not sure if these openings, these tunnels are allowed*, is there an intermediate way of …I am thinking of strategies like having all the traffic from those ports going into a quarantine area, so that I can monitor, *Is there actual activity going on before I let them back into the fold, as it were?* Or *yes, once a quarter somebody needs to actually access that*. Are there things like that that people can do?

Rachel: Yes. Definitely something that people can do would be to monitor. So say maybe you look at your firewall rules, and you see a bunch of rules that are in there that are permitting certain things and you are kind of like, *I do not know if that is supposed to be there*. You can set up a schedule or a system where you say, *We are going to monitor for three months, and we are going to see if any traffic hits these rules over a period of three months*. When you are devising something like that, you need to make sure that you are keeping your business rhythms in mind so that you know maybe there is something that only gets processed once a quarter. You have to make sure that you make that window long enough that you are capturing things that may only happen occasionally but are very business-critical when they do happen.

So definitely set up a monitoring schedule. See if anything is actually successfully hitting the rule. Then sometimes it will be a matter of detective work after that where you can say, *Well, we saw this IP address talk to this IP address. Let's go see if we can hunt down the system owner and figure out who these people are and just ask them directly. What is this thing*?

Suzanne: Sure. Yes, and I think there is a lot of businesses that have different cadences for different kinds of activity. There is a lot of financial activity that happens on a quarterly basis, but you have also got things like, *We go to this trade show every February*. *There may be things related to getting ready for that trade show that we work with partners on, that we only see them in February, things like that.*

So the message is, you want to be careful, but you also need to think about your own stakeholders, your business rhythm, and understand where there might be things that do not happen all the time but still have an impact on your business if they are missing. So that is challenging.

Rachel: Yes, it is. When you think about it, everything we do in security is ultimately about trade-offs. There is almost always some sort of trade-off between, we will say usability and security. There is always something that makes it a little more challenging for someone to get their job done, but it is being done for the sake of security.

It is the same thing when you talk about locking down the network perimeter, locking down the firewall. There is that risk that you are going to accidentally maybe keep somebody from being able to do their job, but you are doing that because of the risk that you see with this gaping hole in the firewall that nobody is able to explain. That is why one of the best practices that I discuss in my blog post is about labeling everything. In particular, most firewalls these days give you the ability to put in a note or a label on a rule. Future network administrators and future firewall administrators will thank you if you go ahead and you put a note in, every time you create a new rule to say, *This is what this is for. This is the business unit that requested this. This is the reason it is here.* So that at the very least five years from now when somebody is looking at it and they see, *Oh, that rule was put in there to support something that has not happened since 2013; that business is no longer here. We can go ahead and we can close that hole in the firewall*.

Suzanne: Or, *We have reorganized, and that part of our business is actually not something we do anymore. So we do not need to interact with people in that area*. How frequent is it, in your opinion, that those kinds of holes are the entry point?

You have got to go looking for the holes if you are a malware kind of enthusiast. Are those kinds of holes in the firewall, are they a large part of how malware and ransomware and all these other attacks happen? Or, is this a relatively small part of how organizations get targeted? Do you have any information on that? Is there any data on that?

Rachel: I do not have any data on that, so that is not a question I can answer authoritatively. I do know that we see, for instance, things like ransomware, malware. There are a number of different vectors through which that comes in, a lot of it anecdotally. I would say a lot of people believe it happens frequently because of user activity.

So somebody click on something in an email is a frequent problem. Somebody took a USB drive and put it in their laptop, and they should not have done that, and there was a file on that USB drive that infected their laptop. I cannot say whether holes in the firewall account for a significant portion of that kind of activity.

I do know that it has been claimed that certain recent events happened or at least spread as a result of certain ports that were left open on people's network perimeters, but I cannot really say anything authoritatively about that.

Suzanne: From my viewpoint as somebody who works in an organization that I know is trying to collaborate, I can see the proliferation of open ports being something that would provide somebody that has a nice random number generator with entertainment on a Saturday night. It is not out of the realm of possibility that these are ways that people get into your organization.

Rachel: Exactly. People out there are scanning all the time. Anybody who is looking at the logs, if they are logging on this kind of thing, if they are looking at logs on their Internet router. If they are logging on the access list. If they are looking at the logs on their firewall, anybody on the Internet is going to see that people are scanning all the time.

So any port that is open, that somebody can identify as open is a possible target. We have seen at organizations where they had a port that it was deliberately opened because they had a business partner who needed to be able to access something, but it was not left open only to the business partner's IP addresses. They just left it wide open because in some cases they might not know all of the IP addresses that need to connect. I mean, I have seen this in prior jobs. We see this kind of thing a lot. That gets abused. People find an open port, and you should not underestimate the ability of people to identify all sorts of ways to abuse those open ports.

So best practice is, if there is something that you need to allow to be open to the outside and it is not something really basic, like port 80 for your website, you need to lock it down to the known external parties that need to be able to get in. There are very few ports that you should allow open to your network…

Suzanne: To the world.

Rachel: …to the world that are not, like, the really basic, like, port 80, port 443 for your website, port 53 if you are running a DNS server. Only allow those ports open to those specific servers. There is very little other stuff that the whole world should be able to get into your network and do.

Suzanne: So labeling is a best practice. I am also hearing logging and not just logging but looking at your logs and reviewing those. How often would you recommend people to be reviewing for their Internet router when they are trying, especially at the beginning when they are trying to figure out what do I really have?

Rachel: That is a very difficult question to answer because, of course, a lot of people think that the problem we have in security these days is not a lack of data; it is too much data. So, show me the organization that has enough staff on hand that not only can they log on everything, but then they can sit and review those logs every day. Realistically, that is not going to happen.

So there should also be a process of—and again, this is sort of a project people have to go through—identifying what are the most important things. What are the things that you care about the most? Prioritizing those things. Make sure that you are logging on those things; and then having a process. Whether it is a human reviewing them, and, again, it is not very realistic to say, *We can assign lots of staff to just sit and pore through the logs*, but at least to have maybe those events that are considered critical flagged in the logs. Also if you have some security tools that can parse those logs, have an alert on…get a security tool that will parse the logs and alert on the things that are of the most importance to you. But, critical to that process is going through the internal examination to decide what your priorities are. That is something that a lot of people skip, or they are not sure how to do it.

Suzanne: Well, it is not a security thing, right? That is a business stakeholder thing. On the list of things that business stakeholders have to do, that probably does not make the top three when you are in a typical business that is trying to run for a profit. So I think part of this education process on border protection is this is critical to your business. If you want to make sure that you are not leaving openings into your Internet borders, your firewall, the people on the business side have got to take some time to help the people in security to understand what is a priority? Otherwise, it is going to be the opinion of a technical engineer, not a business person. And sometimes they may coincide, but not necessarily. You cannot count on that.

Rachel: Ideally you need both. Because you need the business side to be able to say, *What are the things we care about the most*? *What are the events that we care about the most? What are the systems we care about the most*?

On the technical side, first of all, you need people who can understand, *Well, what would that look like in the logs? If something were to happen, how would we know it?* But, at the same time, sometimes people are very worried about things in logs that they should not spend a lot of time on.

So I talked about scanning before. If somebody scans and you just see on your Internet router, your external-facing interface, somebody did a port scan. They were looking for open ports. How much do you care about that? We know that that happens all the time. There is a good chance that you do not want to send somebody to review the logs every time there's a port scan because they would be doing a lot of reviewing logs just to say, *Oh, look, somebody port scanned us*. Maybe there's a reason out there why somebody would care about that, but a lot of people consider that to be noise. And so you would not necessarily want to get too reactive every time there is a port scan.

But maybe you notice that there is one particular IP address out there that seems to be persistently trying to scan you and is trying different kinds of scans, and has just spent two weeks attempting every possible scan known to man and has followed it up with some brute force attempts. *They all failed but oh, we can see that there is one IP address that really seems to be trying something. Maybe then we care about it.*

Suzanne: It could be anything from a competitor looking for industrial espionage to someone with more malicious intentions. But you are not going to know that. But yes, *Which ones do I triage to actually go after?* is going to be one of the challenges of this.

I think you are going to be busy for a while because network border protection…I can think of machine-learning kinds of applications, all kinds of things that in the future could help with this. But I think the message that this is both a business and a security issue, and that you need to understand, *What do you have and what do you need to leave open?* is really the key to protecting your border for your Internet and for your firewall. Those are things that we want to make sure our listeners take home today.

Any other take-homes that you want to make sure people pay attention to when they are dealing with this kind of issue?

Rachel: I think I would probably reiterate, *label everything you do*. The biggest problem I have seen when I have been looking at networks in particular in past jobs is coming into a new place and nobody understands why something was done. So labeling everything is really important.

The other thing that I would urge people—especially if you are in the process of setting up a new service, and people are not sure. *Well, what do we need to permit through? OK, let us just permit all ports for now, and we will lock it down later*. That later usually doesn't happen. People—often in the name of trying to get something done—will have a really, really wide hole in the firewall. *Just allow everything through, and we will figure it out later.*

But once they have achieved what they need with the system, nobody sticks around to say, *OK, now we have to do all the extra work and figure out exactly which ports this is using and lock it down*. So I see a lot of security holes that were left by people just trying to get a job done and not going back and doing the cleanup later. So yes, go back and do that cleanup.

Suzanne: So, either do the lockdown process initially, so that you are safe from the get-go, or plan for the cleanup, and do not let that planned-for time get away from you. Because we all know how easy it is to let that get away from you.

Rachel: Yes. Ideally do the lockdown initially. But I know what reality is like, and I know that often there are deadlines to meet, and nobody is able to figure it out beforehand. But it has to be built into whatever project you are doing. *Hey, this project is not considered completed until we have locked down the firewall appropriately*.

Suzanne: Good advice, Rachel. I thank you. And I thank you for joining us today and expanding our ideas in terms of what some of the best practices are in network border protection.

For our listeners, this is not the only podcast on best practices in network security. We have several others that are being recorded and have been recorded. Those are going to be available through links in the transcript for this, as well as on the website. We invite you to look at some of those other podcasts as they become available. Also [I want to] reiterate that this is going to be available at our internal SEI website at www.sei.cmu.edu/podcasts.

Also, there is a blog post that Rachel has authored on this. If you go to our insights.sei.cmu.edu site for our blogs, look under the authors and look for Rachel under Kartch, K-A-R-T-C-H. That is probably the easiest way to find that blog post. So thank you for doing that for us as well.

This podcast is also available on the SEI YouTube channel and also on the Carnegie Mellon's iTunes U site. We invite to you find it in any of those places that are convenient to you. As always, if you have any other questions for us, please do not hesitate to contact us at info@sei.cmu.edu. Thank you, Rachel. And thank you all for watching.