DevCentral Top5 07/31/2012

Colin Walker, 2012-31-07

Last week most of the DevCentral crew found ourselves in New York to attend the F5 Agility event wherein we got to interact with some of the many awesome users and partners in the F5 ecosystem. It was a great event, though it kept us busy. Between presentations, videos, glad handing the awesome people that were good enough to greet us at our booth, meetings and trying to keep up with a myriad of questions - we were busy enough to keep even the Evil League of Evil busy, along with their various henchmen, and there are only so many of us. Despite all of the hubbub both before and during the event, the stream of hawesome that graces the DevCentral home page day in and day out was ever vigilant. I'm back again as always to cast a spotlight on those items that struck a chord with me. And with that, here they are, my Top5 for this week:

Divert Unencrypted Traffic Through an IPS with Local Traffic Manager

http://bit.ly/M9Bral

Jason Rahm steps up to bat first with a pretty awesome article that details a wonderfully elegant and simple security solution using a couple of features one might not think of first when thinking security. The goal is pretty straight forward: Send traffic through an IPS on the way to the back end servers. The hitch in that setup is that said data must be end-to-end encrypted. This means that the BIG-IP needs to decrypt the data and re-encrypt it before sending it to the back end servers. If you're following along at home, that means the BIG-IP needs to decrypt, send to the IPS, receive the response from the IPS, re-encrypt the data, and send it to the back end. This just got a little less straight forward. Fortunately, though, Jason comes to the rescue with a tip from F5 engineer Brent Imhoff that uses route domains and a back-end data group to take the edges off of this problem. Follow along in the article, complete with diagrams, and learn how this works. I was impressed, and thought this could be quite useful for many of you out there with similar needs, so take a look for yourself and see how this magic happens.

v11.2 Features: tclsh

http://bit.ly/Okv48E

Amongst the many new features that were released in BIG-IP version 11.2, one of the ones that stuck out to me is something that most people may never know about. It has nothing to do with passing traffic or even administering the system itself. Tclsh is exactly what it sounds like, a Tcl based shell which allows you to directly enter Tcl commands for execution. This is a tool that those of us that tend to craft iRules on a regular basis have used for years to help formulate the syntax we want to deploy in our code, troubleshoot and debug, or work through the syntax of a particular command or line of code. As of v11.2 tclsh is now part of the BIG-IP release, which means you no longer have to install or manage it yourself, you can just connect to your BIG-IP and use it there from the command line. While this news may not change the life of every admin out there, it certainly hit home for me, so I figured I'd write up a little explanation of how and why one might use tclsh. Take a look and see if you learn something useful about how to make iRules development and debugging just a hair easier.

Automagic Vulnerability Scanner Integration: Cenzic Style

http://bit.ly/Njv2cK

Josh is our resident security dude on the Devcentral team. As such he's often found telling us to use 10 logins to access a system, hacking potential employee websites in the middle of their phone interview, and otherwise "improving security" for us all. We're thankful for him though, because security is a darn important topic these days, what with all of those code writing monkeys making attempts to compromise your applications and all. Along with just keeping the lights on in our security department he also happens across some darn cool stuff from time to time, and this demonstration of virtually effortless Cenzic vuln scanning via ASM is definitely one of them. For the answers to "Who is Cenzic? How do I use them? What does automatic mean?" and "What is a lemon squeezy?" you'll have to dig into the article itself. It's a good read, it's got lots of easy to follow images that darn near hold your hand through the process, and it can, in all seriousness, help add some valuable security to your deployment. If you have any interest in vuln scanning or security, check this one out, it's a good read - even if he bashes us TCL coding monkeys.

WILS: Moore's Law + Application (Un)Scalability = Virtualization

http://bit.ly/PjU0Jj

As DevCentral's most prolific blogger Lori tends to reach out and touch many, many different topics. Some of which I can follow, others sail clearly over my head. This one, however, slams straight into my brain meat and makes me sit up and take notice. This is nearly torn directly out of a conversation I've had many times with co-workers and users alike. The concept is simple: It's not possible to linearly scale applications just by adding compute power and memory. It's just… not. Lori delves into some of the how and why, and threatens us with some complex math if we don't believe her (I for one DO, so that makes it easy) and it's absolutely worth a read. Virtualization isn't just about keeping the lights on, it's about performance too. If you think that you can endlessly scale the number of threads, connections and active clients connected to a single instance of your application, well, I'd wager you're in for a rude awakening at some point. There's a reason that people tend to use many servers to host an application, and it's not just redundancy. Virtualization allows us to make better use of the ever increasing computing power available to us to host applications in a way that allows for far better scalability than just upping the power of each server. This one is an awesome read and really is food for thought as you start to plan your next app deployment or how to increase performance for those you're already managing.

SYN-Flooding Smartphones

http://bit.ly/R5aqvg

SYN-Flooding is not a new concept, and it's something that's been covered multiple times in various ways on DevCentral. This is, however, the first time I've seen anyone talking about SYN-Flooding mobile phones, however. What's more, this isn't just anyone talking about it, it's David Holmes, one of F5's sharper security minds. Did you know that some phone providers allow internet traffic all the way through to your phone? I didn't. I'm officially terrified by that statement, but I have confidence it's for a good reason. Learn more about that, why SYN-floods to smart phones might be a real thing that actually happens sometimes, and why that thing is a very bad thing indeed in this post by David. It's a good read and has links to some even more awesome content.

That wraps up this week's DC Top5. If you've got any feedback or comments never hesitate to let me know. Otherwise, I'll be back in two weeks with more DevCentral goodness for you to consume.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com