Window Coverings and Security

Don MacVittie, 2011-05-04

Note: While talking about this post with Lori during a break, it occurred to me that you might be thinking I meant "MS Windows". Not this time, but that gives me another blog idea… And I'll sneak in the windows –> Windows simile somewhere, no doubt.

Did you ever ponder the history of simple things like windows? Really? They evolved from open spaces to highly complex triple-paned, UV resistant, crank operated monstrosities. And yet they serve basically the same purpose today that they did when they were just openings in a wall. Early windows were for ventilation and were only really practical in warm locales. Then shutters came along, which solved the warm/cold problem and kept rain off the bare wood or dirt floors, but weren't very air tight. So to resolve that problem, a variety of materials from greased paper to animal hides were used to cover the holes while letting light in. This progression was not chronologically linear, it happened in fits and starts, with some parts of the world and social classes having glass windows long before the majority of people could afford it. When melted sand turned out to be relatively see-through though, the end was inevitable. Glass was placed into windows so the weather stayed mostly out while the sun came in. The ability to open windows helped to "air out" a residence or business on nice warm days, and closing them avoided excessive heat loss on cold days. At some point, screens came along that kept bugs and leaves out when they were open. Then artificial glass and double-paned windows came along, and now there are triple paned windows that you can buy with blinds built into the frame, that you can open fully, flip down, and clean the outside of without getting a ladder and taking a huge chunk of your day. Where are windows headed next? I don't know.

This development of seemingly unrelated things –screens and artificial glass and crankable windows – came about because people were trying to improve their environment. And that, when it comes down to it, is why we see advancement in any number of fields. In IT security, we have Web Application Firewalls to keep application-targeting attacks out, while we have SSL to keep connections secure, and we have firewalls to keep generic attacks out, while deploying anti-virus to catch anything that makes it through.

And that's kind of like the development of windows, screens, awnings or curtains… All layers built up through experience to tackle the problem of letting the good (sunshine) in, while keeping the bad (weather, dust, cold) out. Curtains even provide an adjustable filter for sunlight to come through. Open them to get more light in, close them to get less… Because there is a case where too much of a good thing can be bad. Particularly if your seat at the dining room table is facing the window and the window is facing directly east or west.

We're at a point in the evolution of corporate security where we need to deploy these various technologies together to do much the same with our public network that windows do with the outside. Filter out the bad in its various forms and allow the good in. Even have the ability to crank down on the good so we can avoid getting too much of a good thing.

Utilizing an access solution to allow your employees access to the systems they require from anywhere or any device enables the business to do their job, while protecting against any old hacker hopping into your systems – it's like a screen that allows the fresh air in, but filters out the pests. Utilizing a solution that can protect publicly facing applications from cross site scripting and SQL injection attacks is also high on the list of requirements – or should be. Even if you have policies to force your developers into checking for such attacks in all of their code, you still have purchased apps that might need exposing, or a developer might put in an emergency fix to a bug that wasn't adequately security tested. It's just a good idea to have this functionality in the network. That doesn't even touch upon certification and audit reasons for running one, and they are perhaps the biggest drivers.

Since I mentioned compliance, a tool that offers reporting is like when the sun shining in the window makes things too warm. You know when you need to shut the curtains – or tighten your security policy, as the case may be.

XML firewalls are handy when you're using XML as a communications method and want to make certain that a hacker didn't mock up anything from an SQL Injection attack hidden in XML to an "XML bomb" type attack, and when combined with access solutions and web application firewalls, they're another piece of our overall window(s) covering. If you're a company whose web presence is of utmost importance, or one where a sizeable or important part of your business is conducted through your Internet connection, then DoS/DDoS protection is just plain and simply a good idea. Indeed, if your site isn't available, it doesn't matter why, so DDoS protection should be on the mandatory checklist.

SSL encryption is a fact of life in the modern world, and another one of those pieces of the overall window(s) covering that allows you to communicate with your valid users but shut out the invalid or unwanted ones. If you have employees accessing internal systems, or customers making purchases on your website, SSL encryption is pretty much mandatory. If you don't have either of those use cases, there are still plenty of good reasons to keep a secure connection with your users, and it is worth considering, if you have access to the technology and the infrastructure to handle it.

Of course, it is even cooler if you can do all of the above and more on a single high-performance platform designed for application delivery and security. Indeed, a single infrastructure point that could handle these various tasks would be very akin to a window with all of the bells and whistles. It would keep out the bad, let in the good, and through the use of policies (think of them as curtains) allow you to filter the good so that you are not letting too much in. That platform would be F5 BIG-IP LTM, ASM, and APM. Maybe with some EDGE Gateways thrown in there if you have remote offices. All in one place, all on a single bit of purpose-built high-performance Application Delivery Network hardware. It is indeed worth considering.

In this day and age, the external environment of the Internet is hostile, make certain you have all of the bits of security/window infrastructure necessary to keep your organization from being the next corporation to have to send data breach notifications out. Not all press is good press, and that's one we'd all like to avoid. Review your policies, review your infrastructure, make sure you're getting the most from your security architecture, and go home at the end of the day knowing you're protecting corporate assets AND enabling business users. Because in the end, that's all part of IT's job.

Just remember to go back and look it over again next year if you are one of the many companies who doesn't have dedicated security staff watching this stuff.

It's an ugly Internet out there, you and your organization be careful…

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