F5 Friday: Join Robin &ldquo;IT&rdquo; Hood and Take Back Control of Your Applications

Lori MacVittie, 2011-28-01

Mobile users. cloud computing . End-runs around IT security by developers. The trend has always existed, it’s just speeding up now. IT needs to take back control – and fast. But first IT needs the tools with which to do that…

Let’s ignore the horrible acting by Kevin Costner in “Robin Hood: Prince of Thieves” (I personally prefer Russell Crowe in the 2010 version but that’s me and unfortunately they cover two different periods of Robin Hood’s legendary life so we’re stuck with the lesser version) and let’s just focus on a couple key lines/concepts that are relevant to the topic at hand.

Robin Hood is trying to convince his not-so-merry band of men to fight back against the Sheriff of Nottingham. One of the men complains: “Yeah, but what about our kids? The sheriff has taken all they've got too.” Robin Hood’s response, in typical heroic-tale style is: “Then, by God, we'll take it back!”

THE NEXT USER THAT TRIES TO ACCESS AN APPLICATION FROM AN IPAD ON MY NETWORK IS GOING TO LEARN THE HARD WAY WHAT “ACTIVE POLICY ENFORCEMENT” REALLY MEANS…

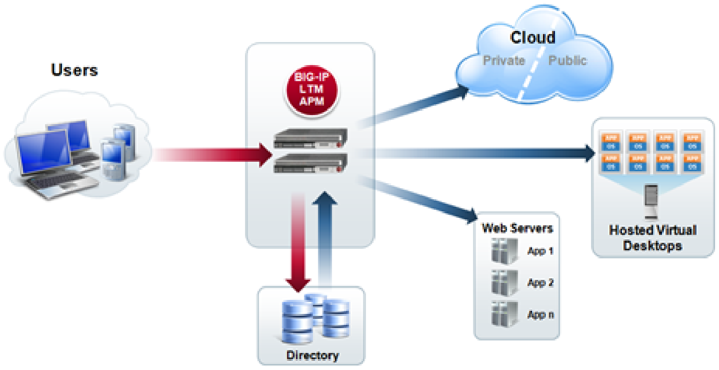
While business and mobile users and developers haven’t quite taken “all IT has got” in terms of control, they have taken more than a fair share. And that’s dangerous, because a business *user* is not *the business* and thus their demands and desires do not always march lock-step in line with business needs or requirements. They may demand, for example, that you ensure they can access applications from their iPad but “the business” might not be willing to introduce that just yet – or for all applications. Auditors – as far as I’m aware – don’t accept “users are really careful” as meeting a compliance or other regulatory requirement. Perhaps accessing the intranet is okay, but the application through which millions of dollars worth of transactions flow – well, they can’t justify the potential risk of that data ending up on a mobile device that could be next week’s “Show and Tell” gadget at the local grade school.

“The business” is not its users, and it often has some stringent security and access policies which its users would rather simply ignore. The problem is users may not be aware of such a policy and even if they are, they may be wont to believe it “doesn’t apply to them.” And because their iPad is personal – it’s not managed or governed by IT – and using WiFi, you may be aware that their use is increasing but from a technological standpoint you can’t do much about it. You’ve lost control because your security policy enforcement is focused on things like networks and application types, not devices and locations and even specific users.

LUCKILY THIS is NOT MEDIEVAL ENGLAND

Sure, you may feel like getting medieval on your users, but really that’s not an acceptable response. Seriously. It’s not.

What you need is a technological solution that can provide the means by which you can actively enforce access policies and which allows you to dynamically adjust those policies as new technology emerges and is brought into the organization and that may circumvent – intentionally or otherwise – the core security policies the business needs to enforce. That’s why it was very exciting when earlier this week we announced the availability of BIG-IP Access Policy Manager for LTM VE (LAB or PRODUCTION LTM VE only).



BIG-IP Access Policy Manager (APM) is able to control access to applications and resources not just based on identity but also on other variables associated with context. That's variables like device type, state of the endpoint, location, and even network and data-center based conditions and status. By leveraging context, APM can provide a dynamic, flexible active policy enforcement method that better aligns technology use with business goals and needs – especially those related to application access.

BIG-IP APM integrates with existing methods of authentication, and allows rich policy for authorization based on user, endpoint inspection and more. And yes, our endpoint inspection and secure remote access solutions support iOS devices.

Organizations can allow only secured devices, or restrict access to a specific set of applications from others; the choice is up to the implementer because regardless of network, or device, APM puts IT ***back in control*** of application access.

While there are lots of folks familiar with the core BIG-IP platform and our flagship load balancing and availability solution, Local Traffic Manager (LTM), many aren't as familiar with APM or aren't (understandably) comfortable with testing out a new solution by deploying it on a production-level, critical infrastructure component like LTM. The availability of APM as a module for LTM in a virtual form-factor offers an easier means of evaluating APM or simply using it to pre-configure and test desired access policies before moving them into production. My cohort Peter Silva, has written a bit more in depth on the newest virtual member of the BIG-IP family and how to leverage its capabilities to "Simplify VMware View Deployments". Be sure to check it out.

So go ahead, test it out. Join the modern version of Robin Hood's merry band of IT and take back control of your applications.

Happy Securing Access!

- Simplify VMware View Deployments
- F5 Accelerates VMware View Deployments with BIG-IP Access Policy Manager on a Virtual Platform
- BIG-IP Local Traffic Manager Virtual Edition
- BIG-IP Access Policy Manager
- Application Delivery and Load Balancing for VMware View Desktop Infrastructure
- Deploying F5 Application Ready Solutions with VMware View 4.5
- Optimizing VMware View VDI Deployments
- Global Distributed Service in the Cloud with F5 and VMware
- F5/VMWare Solutions
- Security Compliance
- BIG-IP LTM VE

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