What's the relationship between security and SDN deployment?

Jim Metzler

A couple of years ago the discussion of SDN focused primarily on the fact that SDN separated the network control function from the network forwarding function and that separation of functions might require the introduction of new protocols such as OpenFlow. More recently there has been a lot of discussion about the value of an overlay SDN model vs. an underlay SDN model and the role of specialized hardware in either model. All of these discussions are important and they all are focused on key architectural characteristics of SDN.

In my experience architectural discussions begin very early in the adoption cycle of a new technology or architecture. When we get closer to a technology or architecture crossing the chasm and being broadly adopted, we begin to see more of a discussion of operational considerations. The discussion of the operational impact of SDN is happening now as many organizations that are evaluating or trialing SDN are trying to answer a critical question: Does SDN make providing security easier or does it introduce a host of new security challenges?

The 2015 Guide to SDN and NFV[1] contains recent market research that shows that 35% of network organizations believe that SDN will enable them to implement more effective security functionality. One example of how SDN can enhance security is that security services can be implemented based on using OpenFlow-based access switches to filter packets as they enter the network. Another example is that role based access can be implemented by deploying a role-based resource allocation application that leverages the control information and capability of the SDN controller. Other security related use cases include leveraging the control information and capability of the SDN controller to provide DDoS protection.

However, *The 2015 Guide to SDN and NFV* also contains market research that shows that 12% of network organizations believe that concerns about possible security vulnerabilities is a significant inhibitor to SDN deployment. Some of the security challenges related to SDN are described *in SDN Security Considerations in the Data Center*[2]. As pointed out in that document:

- The centralized controller emerges as a potential single point of attack and failure that must be protected from threats.
- The southbound interface between the controller and underlying networking devices is vulnerable to threats that could degrade the availability, performance, and integrity of the network.
- The underlying network infrastructure must be capable of enduring occasional periods where the SDN controller is unavailable, yet ensure that any new flows will be synchronized once the devices resume communications with the controller.

[1] http://www.ashtonmetzler.com/

[2] https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf

Other security-related considerations include that IT organizations should:

- Implement measures to deal with possible control flow saturation attacks; i.e., controller DDOS attacks;
- Harden the SDN controller's operating system to ensure availability of the controller function;
- Implement effective authentication and authorization procedures that govern operator access to the controller.

I started this blog with a question: Does SDN make providing security easier or does it introduce a host of new security challenges? The answer to that question is yes - SDN has the potential to make providing security easier and at the same time, it has the potential to introduce new security challenges.