

Quasi Homework #1

Senior Design Dec1713

Members:

Tim Lindquist, Steven Warren, Terver Ubwa, Gregory Steenhagen, Ian Harris, Khoi Cao

Hardware Firewall

Background

The Bluemix application our group chose to research was Hardware Firewall. This service provides an essential layer of security to a hardware system. It prevents unwanted traffic from hitting servers and allows for server resources to be dedicated for their intended purpose. IBM offers Hardware Firewalls as a add-on feature for all servers on the SoftLayer public network. The SoftLayer Hardware Firewalls work by being built on enterprise grade hardware applications and is split into three different customer versions: Shared Firewall, Dedicated Firewall, and Fortigate Security Appliance. Each version has it pros and cons and it's up to the customer to choose which service will best meet their needs. Hardware security is a prominent threat in today's world. Many cyber threats are constantly bombarding hardware and software systems. By having safety measures in place such as this Bluemix application, consumers could potentially avoid major leaks or injections of sensitive data from their product.

Relevance to our project

Our project requires data transmission through a 3G module to a web application. The web app we would be using for the project would require some amount of protection from hackers and other unauthorised persons who might want to gain access. Also considering the fact that our project can be modified to perform functions other than collection of data for farmers, the security of the web app which would be used becomes even more relevant. SoftLayer's Hardware Firewall which provide security for customers and has a reputation for providing uninterrupted services and since our nodes would have a sleep and wake time, this eliminates the issue of having to change the engineering design structure of the project. Apart from the earlier mentioned advantages, there is also the option of choosing between shared firewall, dedicated firewalls and the fortigate security. This gives us more options to choose from in order to meet our need.

Implementation

Our team would implement this service by attaching the Bluemix Firewall to our hardware nodes that are out in the field. This feature will assist in keeping the system locked down and secure. We have already taken precautions within our team to prevent hackers or unwanted traffic from retrieving our access to the system by using Iowa State's servers. Given that we made our entire system through Bluemix and not Iowa State, we would need a security platform such as the Firewall through IBM's Bluemix.

Another aspect of security for our project is we would need to prevent intruders from accessing our server through our hardware nodes. This is where Bluemix's Hardware Firewall

would come into play. It would ensure that a hacker or unwanted traffic could not get to our server directly. The Hardware Firewall would also allow us to keep unwanted traffic from entering through our hardware in the field (nodes). This is likely where we have the least amount of security so having a system that is capable of keeping the information in our nodes to the server in a secure fashion would be most beneficial.

When looking at the features that Bluemix is offering, our team needed to ensure the specs of the tool would work with our application. The throughput that the server is expecting from the node's side is going to be minimal, possibly a few hundred bytes a day while the spec allows up to 2000 Mb per second. Also the option of utilizing a gui for setting up the firewall is beneficial because over 60% of our team is focused more in hardware rather than software.

Pros

As is the case for any pre-built application, there are pros and cons associated with using SoftLayer's Hardware firewall. One pro that comes from using this service, would be the extreme customization provided by SoftLayer. Up to 79 different rules can be configured for the primary IP address associated with the server. With such a high level of customization available, we would be able to configure the firewall to best serve us. By defining the format of the data that is sent to our server, we could save the server from ever having to parse that data.

Another positive effect that would come from using this application, is that it can be added on to our project at a later date. Instead of requiring us to setup the firewall during development stages, and having to fight with it throughout the entire development process, we would be able to focus on implementing the communication protocol of our project first, and focus on securing it later.

Cons

There are definitely positives for using a pre-built firewall solution, but Bluemix's option has some downsides in the context of our project. The firewall is a physical device, meaning it must be attached to the local network of the server. While the plug-and-play nature of the device is convenient, it provides some challenges for our project that leaves us with two options. First, we would need to host our web application through one of Bluemix's other services. Second, we could likely buy a physical device, but that begs the question is it worth it? Another potential downside is that if the device goes down, all servers behind the firewall are exposed. By running the firewall on the server itself (which is relatively easy on Linux, like we are already using) all services go down, which almost seems preferred to having an exposed server. Between the cost and the availability of what we already have, Bluemix's firewall service seems to be a little overkill unless we were already using other services they offer.

Conclusion

Internet of Things (IoT) is growing faster than ever before; it still has to cope with the common challenge of the cyber world: security threats. BlueMix, the Hardware Firewall appears to be one of the most popular security solution for IoT system. With the advantage of the versatility and

universality, BlueMix can support to a wide range of customers, from small individual projects to large-scale business ones. For our current application, the cost of services and supplies is, however a barrier for us to access to this technology. This makes BlueMix not a practical solution for now. It still be a great solution for the future plan as our sensor web can be scaled up with additional functions and data.