The Center for Cyber Defenders

Expanding Computer Security Knowledge

Operational Access Assurance

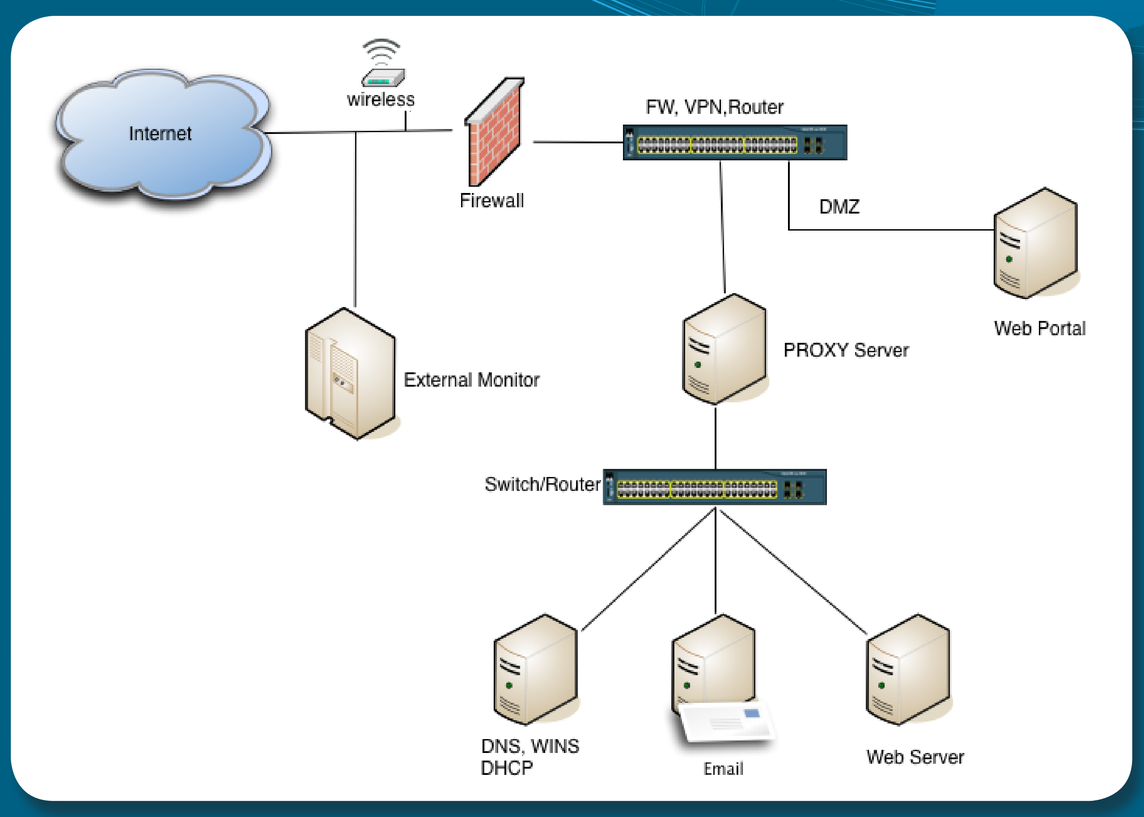
Kaitlyn Gurule, New Mexico Institute of Mining and Technology
Matt Kagie, Cornell University

Project Mentors: Mathew Anderson, Bryan Ingram, Elliott Quarles, and Eric Santillanes, 9533

SAND2012-7282P

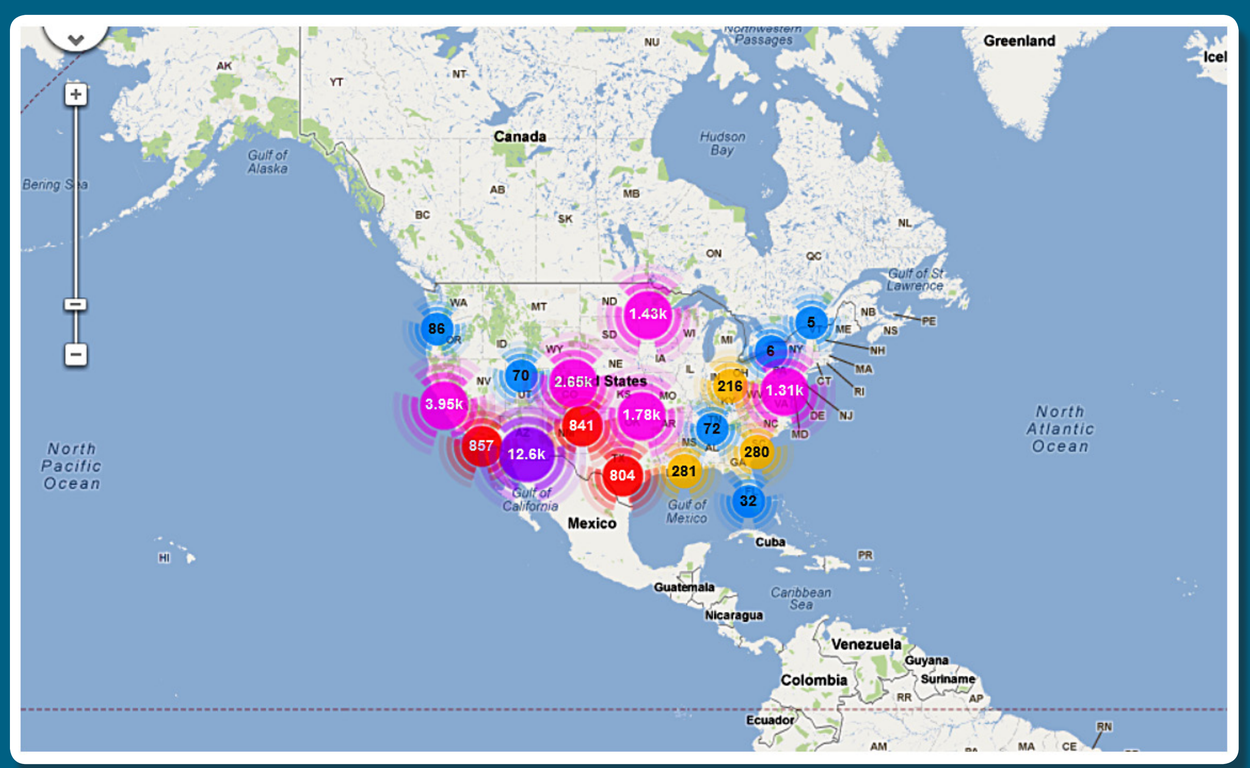
Problem Statement:

In addition to normal, everyday use, Sandia National Laboratory's Internet accessible web servers undergo a myriad of malicious scans from external sources. The issue is that those scans can be done at such a slow interval that when they are compared with millions of other legitimate accesses they blend in with benign traffic. We need to determine whether a given access is suspicious.



Objective and Approach:

The objective of this project is to enhance cyber security by analyzing who is attempting to connect to Sandia's network. Splunk, a data aggregation tool, gives us the ability to correlate data from multiple web servers. We used indicators, such as geographic location, IP address owner, number of different servers accessed, URL path, and time, to determine if an access is believed to be suspicious. If an event is flagged as suspicious, it will be reported on an event-driven dashboard and emailed to support personnel.



Results:

After completing the Splunk server installation, data was collected via Splunk forwarding agents installed on production web servers. As the project is still in progress, it is hoped that network traffic data will be scanned for suspicious activity on hourly intervals. The reporting done here allows administrators more freedom to focus on other aspects of cyber security, rather than focusing so much time analyzing traffic. It enhances the ability to determine if anything must be done to maintain the security and availability of the system.

Impact and Benefits:

The reporting and analysis, done by Splunk gives us the ability to determine unauthorized attempts to access Sandia's Internal Network to obtain information. In addition, it allows more freedom for network administrators to spend their time on other issues rather than focusing on analyzing the network traffic.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2012-XXXXP.