Basic overview of SSH Gateway service

Details

Overview

As the Internet gained popularity and functionality, several communications methods became popular at universities as the means to remotely connect to computers with Telnet being the first to reach widespread adoption. Telnet was eventually supplanted by Secure Shell (SSH) because of security and privacy concerns. For many years, TTU allowed remote SSH connections to TTUnet, the university's network. However, the Internet has become far more dangerous over the years, and organized crime now uses SSH to attack TTU computers over 100,000 times a day.

As a result of the constant attacks, Texas Tech University made a change in the way faculty and staff remotely connect to TTU systems using SSH. Beginning July 11, 2016, remote SSH access to TTU computers require an initial connection to an SSH gateway (ssh.ttu.edu) and authentication with an eRaider account. Once signed in, SSH access to TTUnet computers will be possible.

SSH connections from TTU computers to external systems will not be affected.

The SSH gateway will stop organized crime from using SSH attacks against research and educational servers.

Helpful solutions

- Connect to the SSH Gateway
- Connect to a server using the SSH Gateway
- Use the SSH Gateway for file transfers and direct connections
- How permissions work for the SSH Gateway at TTU