Poster Abstract:

Demand-Provisioned Linux Containers for Private Network Access

System Administrators often need to have remote access to restricted networks that are separated for security reasons. The most common solution to this problem is to use a virtual private network (VPN) between the system administrator's client host to the restricted network. This solution exposes the restricted network directly to a potentially compromised client host. To avoid this direct network connection, an alternate solution is to configure an intermediate server, often called a bastion host, which serves as an explicit man-in-the-middle between untrusted and trusted networks. The bridge between networks is often established using secure shell (SSH). This solution reduces risk by implementing a central point of monitoring and ingress to the trusted network. Unfortunately, this also changes the bastion server's threat surface. Compromises to the intermediate server can result in the capture of authentication data (potentially from multiple users and for both the bastion itself or for assets on the private network) and can be a launch point for subsequent attacks.

To mitigate this risk, we have created an architecture that supports self-service provisioning of non-persistent bastion containers that are unique to each user. These containers only last for the duration of the connection, are only created after the client has authenticated with multiple factors, and perform live auditing outside the container to log user behavior in the private network. The system has four primary internal components: 1) a web-based front-end where users can request a session. 2) a controller on the compute host that manages the creation and destruction of containers, 3) the individual bastion containers, and 4) audit capabilities for both container creation and user monitoring inside of the containers.

This poster describes the system architecture and how we apply least privilege to each internal component to minimize risk. We also describe the implementation of our system, present initial results of its performance overhead, and walk through how a user would initiate a session.

This work is sponsored by the Assistant Secretary of Defense for Research & Engineering under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.