Assembling a C2SIM Sandbox

Component Architecture

Major components of C2SIM Sandbox environment as hosted at GMU are described below.

Virtual Private Network (VPN)

This could involve a combination of hardware and software. It is possible to have the sandbox environment entirely virtualized if the C2 and simulation software being used support it. Some of the software components in the GMU hosted sandbox environment could not be easily virtualized, so some parts are running on bare metal hardware. This means our environment required a physical router and network switch. The VPN clients tend to be either SSL/TLS based or IPSec based. In your configuration, you may want to consider the capability to assign persistent IP addresses to individual users.

Open source VPN software options:

- OpenVPN (SSL/TLS) (used in the GMU C2SIM sandbox)
- Openswan (IPSec)
- Softether (SSL/TLS or IPSec)

There are also commercial VPN appliances that could support this capability (list is just a few examples):

- Cisco VPN routers that support the Cisco AnyConnect
- Dell SonicWall appliances with SonicWall NetExtender (or pure IPsec)
- Barracuda VPN products

Authentication

It may be useful to use an authentication system such as LDAP, Active Directory, etc. In order to manage individual accounts and user groups. The VPN products above can use a variety of authentication methods. Depending on the level of security needed, you can even assign individual certificates to end users, or enable a 2 factor authentication scheme.

The C2SIM Sandbox at GMU currently uses a custom database backend for managing user and group information.

C2SIM Server

The C2SIM services currently run in a VMWare virtual machine running in a VMWare vSphere hypervisor. You could also run it on bare metal or in another virtualization environment such as KVM or Xen. It will need to be assigned an IP address within your private network.

Remote Access Service

If you wish to allow remote users to login and remotely interact directly with certain applications, such as C2 or simulation systems, a remote access service can be used. The two most common are virtual network computing (VNC) and remote desktop protocol (RDP). RDP is natively supported by MS Windows.

Some open source VNC products (these work with Windows and Linux):

- TightVNC (used in GMU C2SIM Sandbox)
- RealVNC
- TigerVNC

The GMU C2SIM Sandbox also uses Apache Guacamole as a web based HTML5 compliant remote desktop gateway. This allows client less access to systems within our sandbox using a web browser.

Security Considerations

If allowing external users remote access to systems, you should consider security considerations in their ability to modify the software and configurations of the systems. The systems should be locked down sufficiently to prevent users from permanently modifying anything. Group policy settings and use of limited user accounts are one way to accomplish this. In a virtual environment, you can use snapshot capability to regularly revert the system to a baseline config. Alternatively, there are products like Faronic's DeepFreeze that you can use to restore the system to specific configuration at reboot and undo any changes.