With the implementation of the General Computing Network (GCN), the Virtual Private Networking (VPN) options are changing. There will be two methods for remotely accessing the GCN via VPN. The new access methods are the Cisco AnyConnect VPN Client and the UNCG SSL Web Portal. Use of the AnyConnect client is reserved for UNCG imaged machines. The AnyConnect Client is supported for Windows 7 hosts, Mac OS X Intel based hosts, and 32-bit Linux (Ubuntu/RedHat) hosts that have been migrated to the GCN. At this time all other Windows, Macintosh, and Linux operating systems will be required to utilize the UNCG SSL VPN Web Portal. Any Windows operating system previous to Windows 7 is not and will not be supported for either access method. The iPad, iPhone, Android, and other mobile devices are currently not supported for either access method. All VPN resources are intended for the use of UNCG faculty, staff, and approved vendors. This VPN solution is not available for student use.

The Cisco AnyConnect SSL VPN Client is replacing the legacy Cisco VPN client currently in use. Use of this client provides you with a local IP address and allows you to operate and perform your daily duties as if you were physically connected to the UNCG GCN. Additional security features have been added with this implementation to provide additional protection for sensitive data. The new features are as follows:

- **Host Scan** – Verifies that you are connecting to the GCN with an UNCG imaged machine and that the machine meets the defined criteria to establish a secure connection to the GCN. If the AnyConnect Client is installed on a non-imaged machine or if the machine does not meet the defined criteria, the client will not be allowed to establish a connection.
- **Start Before Logon (SBL)** – Allows Windows user to establish a secure connection prior to logging into the physical machine. This option permits the native automated mapping of drives and group policy presentation.

The UNCG SSL Web Portal is the solution for users who wish to connect to UNCG resources with a non-GCN imaged machine. For this option to work correctly Active X and/or Java must be installed for Windows machines. Macintosh and Linux machines only require Java to be installed. As with the AnyConnect client your machine will be subjected to a host scan. Your machine is not required to be an UNCG imaged machine but it must meet the other defined criteria before access is granted to the web portal. The web portal allows access to personal and department drives, access to local UNCG websites, public websites, Remote Desktop, VNC, and SSH capabilities. When connected to the web portal you will not be assigned a local IP address. All connections to the web portal will be proxied through the VPN appliance.
Notes:

1. Machines connecting to UCNG must meet the following criteria:
   - Local firewall must be enabled.
   - Norton, McAfee, or AVG antivirus must be installed and updated within the previous 5 days.
2. SSL VPN users must have Active Directory credentials to logon. Users utilizing Novell credentials will be denied access. (User must be migrated to the GCN.)