

Network Management will utilize 'best practices' for protection of the network. These best practices include:

1. Utilization of commercially available firewalls to maintain control over access to the network, including identification and defense against potential denial of service attacks and other internet based attacks.
2. Utilization of commercially available content filters to protect the network and its users from other internet threats such as spyware and spam.
3. Utilization of Internet Usage Policies on the content filters will allow for control of the internet destinations allowed to be navigated to via the network. This will prevent any use of the network to reach destinations involved in illegal or other harmful activities.
4. Utilization of integrated gateway anti-virus capabilities on the content filters will provide for an additional layer of protection from virus attacks.
5. Utilization of the content filters to manage the traffic allowed from certain applications both destined for the network and originating from devices on the network.
6. An additional layer of protection can be provided by the content filters by managing the file types allowed to be transported (download or upload) across the network.

All of these capabilities are available from the appliances provided by all major providers of content filtering devices. Additionally, these capabilities are fully configurable to ensure that the filtering and protection taking place is fully in compliance with the NOFA without compromising the ability of the network to provide the required services to its users.

Internet Service Providers may not over-subscribe port interconnection capacity beyond three hundred (300%) percent, network management practices will be applied to insure compliance..