UFNet2 – Guidelines

Scope

UFNet2 is the name of the next-generation, single network infrastructure for the University of Florida. With modern technology is a possible to provide a single, common, robust, high-performance network infrastructure that can meet all performance and security requirements the institution has to meet, while at the same time provide the flexibility and agility to respond quickly to needs of the education and research communities. Thus UFNet2 is an enabler to bring UF to the Top 10.

The technical foundation of UFNet2 is Multi-Protocol Label Switching (MPLS) coupled with Virtual Routing and Forwarding (VRF) which provide for Layer 3 Virtual Private Networks (L3VPN). As of August 2014 the backbone of the UF network, including the Academic Health Center (AHC) has fully deployed these technologies. Furthermore, most building networks on campus already support these technologies, which can be enabled with minor changes. By deploying multiple L3VPNs across a single common network architecture, a collection of computer systems, data, and users which play a common role and have compatible needs, security posture and access requirements, may be collected into a virtual network environment, no matter their location on campus, which is tailored to fit those needs. See the accompanying "UFNet2 Architectural Whitepaper" for more information.

Terminology

UFNet2 provides the ability to assign any port to the virtual network environment that best meets the needs and work requirements of the computer system and faculty, student, researcher, or staff member using that system. The older technology required such assignments to be made at the building or campus-area level, which forced people into networks, with associated policies and security requirements that are not matched to their work and often impose severe inefficiencies into their workflows.

Network Environments

The following virtual network environments are envisioned, each with their additional policies, guidelines, standards, change management, and governance structure.

1. Academic network environment (Academic-NE): This is essentially the network environment that exists in the majority of campus buildings, like Turlington, chemistry, geology, libraries, engineering, etc. with the policy of open access for education and research.
2. Health network environment (Health-NE): this is essentially the network in Shands hospital buildings and most buildings with health and life science education and research. The presence of protected health information (PHI) on many systems in these buildings has led to the need to secure the entire building complex.
3. ScienceDMZ: The Campus Research Network (CRN) is a 200 gigabit core network on physically separate fiber connecting the data centers with high-performance and bigdata systems in them. The ScienceDMZ network environment in UFNet2 is able to extend the ScienceDMZ policies and

standards to any port, but at lower speeds. This is ideal for smaller labs or instruments which require heavy HPC or direct external access to other research networks at high speed.

4. Administrative/Enterprise network environment (Administrative-NE): This network environment that will be developed with appropriate policies and standards to support the enterprise operations of running the University. Most administrative staff who deal with financial and human resource information (i.e. "the business of the university") will be connected to this network which will be more secure than the Academic environment.
5. Residential network environment (Residence-NE): This environment is geared toward on-campus student housing. It will provide a very similar experience to the one currently provided by the UF Department of Housing and Residence Education.
6. External network environment (External-NE): Visitors and "long term guests" to the University will be placed in this environment. It provides for a highly reliable and redundant guest network experience, but places these users outside of the traditional security boundary and gives them a posture which is substantially similar to any external user reaching UF via the Internet. The UF Visitor wireless network and the Innovation Hub are examples of tenants in this environment.
7. Industrial control systems network environment (Industrial-NE): Modern buildings have numerous control systems that are connected to the network, such as energy monitoring and environmental control, access control systems, security camera systems, building signage systems, etc. These systems can be safely placed on a separate network environment to avoid interference with the educational, research, and administrative activities of the University.

Of the previously listed environments, only the Academic-NE, Health-NE, and ScienceDMZ have been deployed. Others are currently in the development stage.

Network environment owner

Each network environment is operated by some organization that will take primary responsibility for its operation, maintenance and user support. The network environment owner cooperate and coordinate to provide service to the UF community in a way as specified in the accompanying "UFNet2 Network Policy" document.

1. UFIT Network Services is the owner of the academic, Science DMZ, administrative, residential, external, and industrial control system network environments.
2. UFHeatlth IT is the owner of the health network environment.

Helpdesk and support

The helpdesk organizations associated with the different owner are aware of the full scope of the UFNet2 network environment and will assist customers to get any issues and requests taken care of by the correct service and network environment owner, no matter which helpdesk organization is contacted by the customer.

Guidelines

Each network environment will have its own policies and standards, but the policies in this document specify a minimum that must be included in all of them. It is vital that each environment have a clear

policy which outlines acceptable use, as the primary reason for the architecture itself is to provide a technical means by which systems, users, and especially data, may be covered by a single policy no matter their physical location.

Further details and best practices regarding the UFNet2 infrastructure are described in the accompanying "UFNet2 Standards" document.

1. Computers for general use by academic faculty and staff should be connected to the Academic-NE. This is the default environment at the University. Users will be placed here unless more specific policy directs them into a different environment. Although researchers often work with the computer and data systems on the ScienceDMZ, computers that are used to read email, use browser for various activities, write documents, as well as connect to Research Computing systems for software development and data management should be connect to the Academic-NE, not to the ScienceDMZ.
2. Computer systems that hold PHI on local drives or connect to network drives that hold PHI must be connected to the Heath-NE. No exceptions will be allowed.
3. Computers that are used to work on PHI remotely using a virtual desktop technology over a secure (encrypted) channel and without the ability to save data from the remote desktop server to a local drive, USB device, or locally mounted network drive can be connected to any network environment.
4. Computers used by staff members whose primary duties are financial and human resource administration should be connected to the Administrative-NE. Exception can be allowed, but a strong case must be made.
5. Computers that are used for data processing, such as collection of data from scientific instruments, of data to be stored on storage systems operated by Research Computing should be connected to the ScienceDMZ to optimize the flow of data.
6. Users which are not formally part of the University will be placed in the External NE. This often takes the form of the UF Visitor wireless network, but may also be wired as well. These users will receive non UF IP space, but are still subject to standard security analysis, and may be handled similarly to any other on-campus user by the UF Information Security Office. They are placed outside of the security boundary and their traffic must pass through the UF security policy layer before reaching other campus networks. They do not have access to private IP resources.
7. These guidelines and the choice of network environment should not be considered as mechanism to enhance network performance in and of itself. UFIT Network Services is committed to make sure that all underlying hardware systems provide optimal network bandwidth and latency within the constraints of technology and finite budgets.
8. The guidelines and choice of network environments should be used to optimize work flows, best practices, security, and governance. Multiple network environments offered by UFNet2 enable the University community to navigate conflicting issues such as the constraints imposed upon the University by laws and regulations about security and privacy with the need for openness in education and agility and innovation in research.
9. The decision and choice to move a computer user or group of computer users must take into account the context of network services provided in each network environment and which of these

services are needed by the user community. The issues are discussed in the next section of this document.

10. The organization that supports a user or group of users for their desktop needs will also provide the shared file server storage systems and support.
    a. Users who are supported by UFHealth IT and have computers in the Academic NE will be provisioned with shared file storage from servers that are connected to the Academic NE and are managed and supported by UFHealth IT.
    b. Users who have computers that are connected to the Science DMZ NE (a.k.a. Campus Research NE) will buy storage from Research Computing (HiPerGator and GatorBox).
    c. Research oriented data that is not PHI should be stored on storage systems supported by Research Computing. This storage can be accessed in all NEs.
    d. For sharing files between users and computers in different NEs, it is recommended that users use the GatorCloud OneDrive for Business service supported by UFIT. Note that it is not allowed to share ePHI this way. Users collaborating on ePHI need to work on computers that are both inside the Health NE.

Definition of relevant services

Whenever desktop and laptop computers are connected to one of the virtual Network Environments (vNE), namely Academic, Administrative, Health, Science DMZ, External, the users of these computer systems will need access to a set of services that are collectively referred to as “shared services”. Prominent examples are:

1. Shared network printers for workgroups
2. Storage servers providing network drives for collaboration and for proper storage of data

These services are designed to increase the efficiency of both the individual users of computer systems as well as of the organization. Often the services are tailored to some extent to fit the network environment. This may include preventing the shared services from being accessible from other environments. Examples:

- When computer users in offices on the same floor of a building are connected to two different network environments, it is still desirable that both computers can print to the shared network printer in the hallway.
- When users working in the same building work with different types of data, one with protected health information (PHI) data and the other not, both will need storage servers for safe keeping of their data. However, a single storage service should not hold a mixture of PHI data and non-PHI data, because that will put unnecessary restrictions on the use of the non-PHI data. Therefore IT support should provision separate storage services for staff who work with PHI data and staff who do not work with such data so that these services can be provisioned in two separate network environments, the first in the Health-NE and the second in the Academic-NE.

Users need to consult with their IT support staff about the availability and support of these services as part of planning a transition from one network environment to another.

The accompanying document “UFNet2 Standards” provides best practices and standards to assist in this process so that no functionality is lost after a computer is moved from one network environment to another.