

# Architecture for Next Generation VPN Service

Technology Architecture Group

March 21, 2008

[www.oit.duke.edu/tag](http://www.oit.duke.edu/tag)

Following last year's deployment of a new core data network, OIT's Network Services department has been working hard to similarly enhance other systems, including the VPN service. While the service has performed admirably over the last 5 years, it is provisioned by a single box that must be manually reset if its network connection drops for any reason. As well, users find the service difficult to use in some hotels, airports, and other WiFi locations, due to common blocking of the VPN traffic.

For these reasons, it was time to plan for the future.

## ***Virtual Private Networking (VPN)***

VPN systems create an encrypted tunnel between computers located at home or on the road back to Duke's network. This prevents others from eavesdropping on your network activity at public WiFi hotspots, for example.

A significant new feature is the ability to enable access to virtual networks on the new core data network, shown to the right.

Each campus user can belong to one or more groups authorized to access a particular virtual network. Using LDAP and Shibboleth, users are authenticated and granted access to the appropriate networks. The "Link, don't duplicate" principle underlies this design. Interestingly, as Shibboleth handles user authentication, the VPN system never handles the NetID password.

The prototype system is now being tested by several IT administrators at Duke to evaluate it for broader deployment.

***"Create robust, secure systems" is a well-represented principle in the new VPN system design. If one box fails, the other continues operating seamlessly.***

The Architectural Principles were a significant influence on the design of the prototype next-generation VPN service. The prototype has no single point of failure, it recovers gracefully from anomalies, and provides a way to connect even when significant traffic blocking is in place. It does so by tunneling traffic using HTTPS, a popular protocol for securely accessing web sites. The service uses a thin client to avoid requiring repeated system reboots upon client installation.

