VPN Technology at Tri-C

This document outlines the purpose, benefits and security changes in the VPN technology at Tri-C.

The SSL VPN System
OSSC has implemented the Cisco Adaptive Security Appliance with the new SSL VPN feature. This provides a central location for initiating multiple levels of access, with robust security. For most levels of access, this will make using VPN easier, and for all levels, more secure. Because the new VPN uses only TCP port 443, it can connect in more places, and is less likely to encounter problems once connected. The starting point is https://remoteuser.tri-c.edu.

By default, the SSL VPN is essentially a proxy for your connectivity to Tri-C’s internal resources. It will securely tunnel an internal web service like Xtender to your client outside the network. It also presents a web-based tool for access file shares, including an automatic link to your H: drive. The Application Helper will automatically allow some local application on the client to tunnel to an internal resource, such as the Remote Desktop or Application Xtender clients. The traditional full VPN tunnel may also be established, if all the security requirements are met.

Security Additions
On top of the SSL encryption used by the new VPN solution, the Cisco Secure Desktop client installs to ensure a more secure VPN session. For web-based session, the CSD cleans the client browser cache to help mitigate sensitive information being stored locally. In order to establish a full VPN tunnel, the CSD performs a security evaluation. The primary requirement for a full VPN tunnel is that the client needs to be a Tri-C Managed Computer (see definitions below). Other requirements should only result in a failed tunnel if a system is broken or misconfigured.

Applications operational in web-only mode (examples, not a full list)
- File shares
- H: drive
- Remote Desktop (Application Access must be started)
- SalesLogix
- SSH/Telnet (through Java applications in the left menu)
- If you want to add an application to this list, please send the request to helpdesk@tri-c.edu, indicating the new VPN solution
Applications which need a full tunnel

- Applications requiring access to a mapped network drive (O: for example)
  - Using an Archive or Personal Folder on your H: drive with Outlook (note, Microsoft does not support using PSTs over a network: http://support.microsoft.com/kb/297019)
- Microsoft Outlook

Definitions

VPN: Virtual Private Networking

OSSC: Office of Safe and Secure Computing

Proxy: A server that passes a request for information to another server on your behalf. In this case, the server is tunneling your request to the internal network and handling the response.

Employee: A college employee with college-managed equipment.

Managed Computer: A college-owned computer with a standard college image and configuration, joined to the domain. Contact Desktop Support for more information. Apple computers may require an extra configuration step from Desktop Support to support a full tunnel.

Revision History

1.2.0 7/21/2010  Peter Anderson  Network Security Analyst