

University Technology Services

NOTICE: Improved Secure Access from off-campus to McMaster server systems

With the advent of the [VPN service](#), UTS is able to offer a better option for managing the majority of systems (those not designed for general public access) from off-campus. The general [campus firewall](#) protects systems on campus from unsolicited traffic initiated from outside networks (i.e. a system on-campus can request interaction with systems elsewhere, but remains 'invisible' behind the firewall to systems probing from outside).

Until now, system administrators or small groups accessing a shared campus system from off-campus networks have been forced to request *server access* status, an exemption from the campus firewall rules, which left the McMaster machine exposed to outside access (and unfortunately, also to attack). The VPN service allows the machine to be protected by the campus firewall, but enables McMaster community members to access it and carry out any interaction with no restriction, as if located on-campus. Following authentication to identify the community member, the secure tunnel through which the traffic flows is encrypted and hence protected from 'sniffing' during the session.

This method of access not only enhances security for the group using the server, but also for the community as a whole, because servers are the most vulnerable points in the McMaster campus network. Systems not protected by firewalls are potential targets for hackers, computer worms and viruses propagated by computer worms. Once one server becomes infected or compromised, it is often used to launch attacks on other computers connected to the internal (campus) network, bypassing campus firewall protection.

For these reasons (see also [Secure Connections from External Sources](#)), we are no longer accepting server access forms as a method of gaining outside access for administrative or shared system purposes to machines on campus. For this type of access, the VPN service provides a much better secure alternative, and reduces exposure of University systems to unauthorized use and exposure of confidential or personal information to outside attack. Of course, the remote system you use to access the campus network requires protection against viruses, since with the VPN it effectively becomes an on-campus system.

For information and instructions, see: <http://www.mcmaster.ca/uts/network/vpn/>

Only those server systems that provide services to the Internet public at large (e.g. public web servers), should be placed in the Campus Server Access list (the list which exempts systems from the general campus firewall protection rules which otherwise apply). Such public server systems require very careful system administration in order to protect them from the frequent forms of attack that are prevalent. A few pointers on system administration can be found in the [Server System Security](#) pages, and you should consider placing firewall protection directly in front of the server which implements security rules specific to your service needs. If it is necessary for your computer to provide services to the Internet public at large, please complete a Request for Server Access form: <http://www.mcmaster.ca/uts/help/serveraccessform.pdf>