

**SWAN SonicWALL / VPN UNITS
REMOTE ACCESS / SHARED CONTROL POSITION PAPER**

REGARDING REMOTE ACCESS VIA THE SONICWALL VPN FOR MEMBER LIBRARIES' STAFFS: The Metropolitan Library System/SWAN central site staff will not *willingly* condone, provide, or support remote access.

REGARDING SHARED CONTROL WITH THE MEMBER LIBRARIES' STAFFS OF THE FIREWALL: The Metropolitan Library System/SWAN central site staff will not *willingly* condone, provide, or support shared control.

These views are held in the best interest of the security of the shared database, of shared SWAN central site equipment, and of the member libraries and their communities.

BACKGROUND

Due to constant advances in technology, it is impossible for SWAN central site staff to prevent circumvention of the security measures provided by SonicWALL units currently installed in member libraries *UNLESS* all SonicWALL units are regulated by SWAN central site staff. It is also impossible for SWAN central site staff to monitor and regulate each member library utilizing such methods to provide its users remote access to their respective home libraries.

Moreover, SWAN cannot take measures to secure such practices that may already be in place in member libraries. The providing of remote access to any user is in no way condoned or supported, as it jeopardizes the security of all patron information maintained in the shared database.

Additionally, in cases where such measures have already been enacted to route traffic around the existing SonicWALL, SWAN central site staff is unable to provide true firewall protection to member libraries' networks, and thus cannot be responsible for local security breaches at the member library level.

Finally, according to the emerging technological scenario described in this position paper, SWAN central site staff will no longer be able to provide accurate data regarding network usage, bandwidth, or other such pertinent information to its member libraries.

Therefore, SWAN central site staff will control a single SonicWALL device located at the member library and will, upon request, provide secure VPN access from remote PC's to the member library. While SWAN central site staff will be solely responsible for monitoring and maintaining these connections, every effort will be made to work with staff members and/or authorized consultants from member libraries.

SWAN SONICWALL / VPN CERTIFICATION PAGE

By signing this certification page, the SWAN member library administrator signifies that s/he has read and understands the risks and challenges associated with shared control of the SonicWALL / virtual private network. Please complete and return this certification page **by October 1, 2006**, to the attention of the SWAN Administrative Assistant.

Library Name

Library Administrator's Signature

Date