Technote 13 – Firewalls and Data Transfer

The AcquiSuite and AcquiLite (DAS) upload data using a standard HTTP web browser transaction to a database enabled webserver. From the perspective of a firewall, this transaction looks identical to any web browser activity to an off-site website.

Webserver uploads

The AcquiSuite or AcquiLite will open a TCP connection to the remote website/database server on port 80 as an outbound connection. Data transferred over the TCP connection is a standard HTTP/POST transaction. The target website address and URL are user configurable on the AcquiSuite or AcquiLite.

If the AcquiSuite or AcquiLite is required to upload data to the BMO or other online website through a firewall, the firewall must allow outbound HTTP requests from the DAS to the external webserver on port 80. The requests use both HTTP get/post methods, and observe standard HTTP protocol.

To prevent the system from attempting to upload data to a webserver, you can disable the data upload feature. To do this, use the AcquiSuite or AcquiLite web page configuration. Select the "Log File Data" section from the left side menu. Pick "Setup/upload" option. In the right side panel, locate the field "Target address to upload data". Remove the URL from this field. i.e. the target address field should be blank.

The default port is TCP port 80, however the installer may configure the URL with a specific target port number. This will allow the AcquiSuite or AcquiLite to make an outbound http connection to a webserver on a non-standard port.

In addition, the AcquiSuite or AcquiLite may use an HTTP proxy server. To enable this, set the HTTP server and port features in the networking setup configuration page of the AcquiSuite or AcquiLite. The proxy must use a transparent method of HTTP proxy service and may not require any proprietary drivers be used on the AcquiSuite or AcquiLite side of the connection.

obvius
3300 NW 211th Terrace, Hillsboro, OR 97124
Ph: +1-503-601-2099 Fax: +1-503-601-6878

Time server: The default time server feature default is "time.obvius.com". The DAS will make an attempt to contact the time server on each data upload cycle. To prevent this, change the time server setting to a local NTP or Rdate server, or disable the feature by making the field blank. To do this, use the AcquiSuite or AcquiLite web page configuration. Select the "System" section from the left side menu. Pick the "Date and time" option. On the right side panel, locate the field "Time Server". Change the address of the time server to a local server or leave the field blank. Disabling the TimeServer is not recommended. NTP uses UDP port 123. Rdate uses TCP port 37. For systems behind a firewall, it is usually easiest to configure the system to use a local NTP time server and not route this traffic through the firewall. Note: the AcquiLite only supports NTP protocol.

DNS server: The default primary DNS server is set to “70.99.203.62” or “67.51.237.194”. The default secondary DNS server on AcquiSuite devices is set to Google at “8.8.8.8”. Change either or both of these to a local DNS server. To do this, use the AcquiSuite or AcquiLite web page configuration. Select the "Networking" section from the left side menu. Pick the "Setup" option. On the right side panel, locate the field "DNS Server". Change the address of the DNS server to a local server. DNS uses udp port 53

Firmware updates: In the AcquiSuite web page configuration. Select the "System" section from the left side menu. Pick the "Firmware Version" option. In the right side panel, the current firmware version number will be listed. At the bottom of the page, a button titled "Check for upgrades" will be present. Clicking on this will cause the AcquiSuite to connect to the buildingmanageronline.com website (port 80). The firmware will be downloaded using a standard HTTP browser based transaction, the same way as log data is uploaded to an offsite webserver. To prevent this, don't click the “check for upgrades” button. HTTP firmware update uses TCP port 80 outbound. Note, the AcquiLite does not support firmware upgrades over ethernet.

Modbus TCP: The AcquiSuite can make outbound connections to remote Modbus/TCP devices to query data. (in addition to serving as a Modbus/TCP gateway for inbound requests.) To prevent outbound requests, do not configure any remote devices in the Modbus device list.

SNMP Traps: The AcquiSuite can be configured to send outbound SNMP traps. If this option is enabled, it will send packets to the trap host on UDP port 161

FTP uploads: The AcquiSuite with firmware v2.10.1011 or later can be configured to upload log files to an FTP server. When configured for this type of upload the AcquiSuite will make outbound connections to the remote server on TCP port 21. The AcquiSuite can use passive mode transfers which should allow uploads through a generic NAT router/firewall device such as as DSL router.

Open Ports:

The AcquiSuite has several ports open for inbound connections. These are detailed below.

AcquiSuite – open ports		
TCP 80	www	Web browser interface for configuration menus
TCP 21	FTP	Download log or config file data from the DAS. Also allows firmware updates to be installed in systems that do not have open access to the internet. This feature may be disabled in the Network/Setup configuration page.
TCP 23	telnet	Command prompt access for remote debugging. This feature may be disabled in the Network/Setup page.
TCP 502	Modbus	The Modbus/TCP port may be enabled to allow remote systems the ability to query devices on the RS485 line. Access to this port can be restricted in the Modbus/Setup configuration page.
UDP 68	DHCP	When DHCP is enabled, this port is open to receive addressing information from the DHCP server.

The AcquiLite A7801 system has a limited number of ports open for inbound connections.

AcquiLite – open ports		
TCP 80	www	Web browser interface for configuration menus