SuomiNet Site Network Rules Regarding Port Access

227 Beth Bartel October 30, 2008 SuomiNet 3339

SuomiNet Site network rules regarding port access.

SuomiNet sites must be on a network. That is, they must have 24/7 internet connection to allow automated data transfer via the LDM developed by UNIDATA. All the Suominet sites must comply with the LDM port requirements regardless of whether they have a firewall installed. If they cannot comply with these standards, then LDM cannot be used to transfer data. We are not allowing exceptions to LDM data transfer. We are also requiring that we be able to ssh into the SuomiNet field cpu's.

For LDM to run properly behind a firewall, item #1 is required and item #2 is optional:

1. The firewall must allow port 388 to be open for TCP packets.
2. Port 111 can be allowed and portmapper should be running.

Having port 388 allowed and reserved for LDM is required, and portmapper running and port 111 allowed is recommended, although not absolutely necessary.

For ssh to work ssh must be installed and port 23 must be allowed.

Example situation UCAR:

A firewall is installed. Most cpu's behind the firewall have port 388 blocked to the outside world, but open to UCAR subnet IP#'s. UCAR has designated "semi exposed" hosts which have port 388, the ssh port (23) port 111, the ftp port, and some other ports open. A local group system administrator designates a machine as semi exposed by setting the last part or local IP# within a range of designated #'s. The router allow ports 388, 23, etc. for these semi exposed hosts to the world at large. The local group system administrators are responsible for installing sufficient security on the semi exposed host cpu's. LDM traffic other than UCAR to UCAR is handled on one of these semi exposed hosts.

SuomiNet cpu's will have security patches installed before leaving UNAVCO, as well as the Linux OS, LDM, JSTREAM, ssh, and other functions needed to operate as SuomiNet cpu's. If SuomiNet cpu's will be behind a firewall the firewall must either allow port 388 and port 23 to all cpu's behind that firewall -or- the Suominet cpu must be in a semi exposed host category behind the firewall and the router programmed to allow ports 388, and 23 (111 recommended) to semi exposed hosts. We are recommending that SuomiNet cpu's be set up in a semi exposed configuration (only a subset of ports opened) rather than being totally outside of any local firewalls. If the local system administrator feels that additional security is necessary they can limit the outside world IP#'s allowed to use these ports at the

subnet level. A list of IP subnets that must be allowed access to the Suominet cpu ports 388 and 23 is being compiled and will be provided on request.

The IP# and name.subnet.univeristy.edu which will be assigned to the suominet cpu must be specified before the cpu is shipped from UNAVCO so that we can correctly configure LDM.

Online URL: https://kb.unavco.org/article/suominet-site-network-rules-regarding-port-access-227.html