SuomiNet - Network Rules

590 Beth Bartel December 29, 2009 SuomiNet 1879

Note - content is provided for historical continuity and may be out of date. The UNAVCO SuomiNet pages are not actively maintained, and up-to-date SuomiNet information should be obtained from UCAR's COSMIC program at: www.cosmic.ucar.edu/suominet.html

SuomiNet sites must be on a network. Time synchronization using the NTP protocol is required. Sites 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 participants' SuomiNet computers.

For LDM to run properly behind a firewall, the firewall must allow port 388 to be open for TCP packets. See Network Security and Set-up.

Ssh access from subnets *.cosmic.ucar.edu and unavco.org must be allowed on the cpu. (Suominet cpu's are configured at UNAVCO to allow ssh only from these subnets via the hosts.allow files.)

Port 22 must be allowed. When the suominet cpu is installed behind a firewall the firewall must allow Port 22.

On Linux systems Portmap can use tcpd to allow only specific connections. See the man pages for more details.

You should implement portmap in the tcpd "host.allow" file (host.deny should already deny any connection that is not explicitly allowed).

From the LINUX man page: man portmap

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 (22) 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, 22, 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 22 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 22 (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 22 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.