GD group Firewall requests

The standard procedure to request one or more ports to be accessible from the outside or from the LAN is the following. It only applies to non-Quattor GD machines.

Local firewall (access from the CERN LAN)

The local firewall on the system must firstly be configured to enable external or LAN access to the port(s). For test machines, this can be done manually.

For production machines, the hosts are using lcg-fw, which is installed by default on GD systems. The default *lcg-fw* configuration is to only offer SSH access to the CERN LAN, but all outgoing connections are permitted.

In order to change the firewall template that has been allocated to a node, you can contact gd-security-services@cernNOSPAMPLEASE.ch by specifying what type of service your host will be providing. An updated template will be issued and automatically installed on the node (providing its runs *lcg-fw*).

If you attempt to manually change the firewall rules on a node running *lcg-fw*, the registered profile will be re-installed the next time the hourly cron job is run. If you wish to make a temporary change, you can either:

- Contact gd-security-services@cernNOSPAMPLEASE.ch to change temporarily the firewall template
- Deprecated: you can change the local rules by suspending the update of the firewall template. This can be done by issuing the following command on the node:

```
chmod -x /etc/cron.hourly/firewall.cron
```

Please consult instructions here for more information. The local firewall status of GD machines is visible at https://lcg-fw.cern.ch/public/.

Site firewall

Site firewall changes in GD are managed by different service managers:

- Yvan Calas for the PROD
- Antonio Retico for the PPS
- Louis Poncet for the TB
- Romain Wartel for non-standard requests.

In order to enable incoming access to a service on a GD host, the responsible service manager of the relevant group (PROD, PPS, TB) needs to be contacted. Alternatively, an email can be sent to gd-firewall@cernNOSPAMPLEASE.ch, and will be picked up by the relevant service manager.

These service managers are responsible to ensure that:

- The host runs the GD security tools (lcg-fw, gd-auth) and is correctly associated with a nominated contact
- The host is patched automatically
- The host runs standard services that precisely match the description of an existing Set (RB, CE, etc.)
- No unused network service is running on the host

It is also recommended that these service managers ask Computer.Security@cernNOSPAMPLEASE.ch to run a security scan against the host and seek for advice, but service managers remains responsible for enabling (or

not) incoming access to the host.

Help

Do not hesitate to contact Romain Wartel to:

- discuss in advance potential issues with a particular firewall request
- seek for help to define your firewall requirements (ex: what ports do I need to request to enable my gLite CE to be reachable from the outside?).

-- Romain Wartel - 27 Nov 2006

This topic: LCG > FirewallRequests
Topic revision: r3 - 2007-03-09 - RomainWartel