Backup and Remote access for SnBCorp

Remco Hobo

March 2, 2005

1 Introduction

Since SnBCorp was first founded over two year ago, the need for a more flexible network environment has steadily grown. At the moment resources can only be accessed from inside the company and not remote. Also, since the data stored at SnBCorp has grown quite a lot over the past year, it is paramount a new backup solution is found. At the moment the stored data can not be guaranteed. For these reasons, this report is written.

2 The company

At this moment SnBCorp‘s main product is delivering automation solutions for various companies. Because of this, a lot of reports are written for customers. These rapports are one of the main products of the corporation and are quite valuable. SnBCorp currently employes forty three persons, of which thirty are production employees, ten are administrative and three have various duties.

At the moment, 30 GB of data is stored the servers. 10GB is stored on the mail server, and 20 is stored on the file server. All mail data is quite valuable, but the data on the file server is critical, loss of this data can make the company go bankrupt.

The company has forty workstations, all running Debian with an KDE graphical environment. There are two Windows 2000 servers, 'mail' and 'data'. The network consists of three switches, which are operating in a spanning tree. The mail and data server both have a raid-5 setup and can both store 50 GB of data. There is no backup system in place at the moment. Fifteen employees have laptops, of which ten have linux installed on them and five use Windows XP. The company has an 8Mbit internet connection, which is connected to the Linux firewall which also houses the company‘s website.

3 The needs

The main concern at the moment is the data. The need for a secure and relyable backup solution is mission-critical. Another point of attention is the need for remote access to the company. As SnBCorp spreads its wings across national borders, the need arises for remote access to data stored at the company. Also, employees would like to get access to their workstations via the use of SSH. In general the following requirements have to be met:

- A backup solution has to be found for all mail and data files;
- A secure and reliable VPN solution has to be found;
- A way for remote employees to get an SSH connection to their workstations has to be found.

4 The backup procedure

For the daily backups, an external DLT streamer has to be purchased. With it‘s SCSI interface it can be connected to the data server. With the use of the program 'backup exec' daily backups can be scheduled. All data from the D: partition on the 'data' server, containing all user files and global data files is backuped as well as the D: partition of the 'mail' server. Also, the company‘s website is backuped with the job. The system states of both servers aren't backuped since this data isn't mission critical and one server can be easily restored with the use of the ready-made ghost images. Every night, a full backup is made of the 30GB that is used. For this, a total of 20 tape is needed.

Every first workingday of the month, a tape, named after the current month will be inserted. For all workingdays, tapes corresponding with the name of the weekday have to be inserted, with exception of Thursday. For this day, four tapes called Thursday 1, Thursday 2, Thursday 3 and Thursday 4 are available. On the first Thursday of the month, Thursday 1 has to be inserted. On the second Thursday of the month, Thursday 2 has to be inserted and so on.

The accountant is in charge of changing tapes every workingday. He also has to take the Thursday tapes and the monthly tapes home and has to make sure the tapes are stored safely at his house.

5 VPN

Three different VPN solutions have been thought of and tested. The first is IPSec using Freeswan[1] and X509 certificates. The Second is L2TP by Microsoft and the third is PPTP[4].

After comparing these three systems, the Freeswan implementation has been chosen, this has a couple of reasons:

- Freeswan is an open standard;
- Freeswan is less expensive, even though setting it up is more time-consuming then L2TP;
- L2TP will not work on the linux laptops;
- PPTP isn't secure enough.
- Freeswan runs on linux and therefore has less security issues. This is very important as the VPN server has to operate safely when connected directly to the internet.

- It can run on the Linux firewall so no extra hardware has to be purchased.

To make use of the X509 certificates, SuperFreeswan[3] has to be used.

6 SSH

SSH connectivity to workstations can easily be achieved in various ways. SSH V2 in it‘s self is reasonably secure, however, if a security weakness exists on one of the workstations, enabling direct SSH connectivity may be risky. Therefore, it is our opinion the SSH traffic has to be routed through the VPN server. This means remote employees have to first make an VPN connection to the office and thereafter connect directly to their workstation using SSH. Setting up SSH connectivity is quite easily since all workstations have a linux operating system. For the SSH servers, openSSH[2] will be used, as it is a proven program. Also, when the KDE environment has to be used remotely, a VNC server can be set up on each workstation to accommodate these needs.

7 Conclusion

As this report sets out, all new demands that have been outed by the organization can be met. The first step however is to get the backup system implemented as it is company-critical. This will take approximately twenty manhours to set-up. After that, the VPN solution can be set-up. Setting this up will take about 80 manhours, after which, instructing employees will take twenty manhours.
Setting up SSH will take about ten manhours, and instructing employees five.

References

[1] Freeswan website http://freeswan.org

[2] OpenSSH website http://openssh.org

[3] Freeswan with X509 certificates http://www.freeswan.ca/code/super-freeswan/

[4] The PPTP site http://pptpclient.sourceforge.net/