Dr.Backup™
online backup service

Adjusting Firewall and Security Settings to Support Online Backup

If you operate your network in an enhanced security mode -- **or otherwise actively restrict any outbound network connections to the Internet** – then adjustments to your security software or firewall may be required.

This technical note will summarize how the Dr.Backup service interacts with the Internet. We provide specific technical guidance you or your technology consultant will need in order to tailor your environment to support our online backup service.

The following program files (listed in their default location on a 64-bit device) must be permitted to fully communicate over the Internet:

C:\Program Files (x86)\Remote Backup\rbclient.exe
C:\Program Files (x86)\Remote Backup\rbbackupprogress.exe
C:\Program Files (x86)\Remote Backup\rbtransfer.exe

Communication with our Internet-based storage servers is through a security-enhanced version of the PASV FTP protocol. All connections are initiated from the client software running on your machine. On schedule, backup data is "pushed" from your machine to our servers. Our servers NEVER self-initiate a network session to "pull" data.

Our software connects using port 21 to a random node on a storage cluster server. That connection serves as the "control port" for the duration of the backup session. Using this control port, the backup software negotiates use of data ports where the encrypted backup payload will be transferred (or retrieved in the case of a RESTORE operation.)

Storage Server Cluster Name: rbs.drbackup.net
IP Address Range: 66.241.7.1 – 66.241.7.30
TCP Control Port: 21 (or Alternate TCP Control Port: 211)
TCP Data Ports: 20000 – 60000
Triggers may be required on your firewall if Stateful Package Inspection (SPI) is implemented.

Theory of Operation: Dr.Backup software connects to rbs.drbackup.net, using TCP port 21 to initiate a session. The node connected to can be anywhere in the IP range specified. Once application security has been verified, the actual backup begins. A secure PASV FTP protocol is used to assign/de-assign data port numbers -- one for each individual encrypted file in the payload. After all file transfers have completed and backup summary information is updated, open data and control ports are closed and the backup process ends.

Dr.Backup technicians can assist you in testing that adjustments/changes made to your local security environment properly support the Dr.Backup software. For support we ask you to connect to our screen sharing tool which uses the TCP Address: **72.66.21.11** **Port: 8008**