Windows firewall settings

This chapter indicates the possible rule settings for the Windows firewall. These can be further modified and tightened according to security needs (e.g. only allow access of specific IP addresses using the *remoteip* clause).

Enabling ICMP Ping packets (for diagnostics):

netsh advfirewall firewall add rule name="_Ping" dir=in protocol=ICMPv4 action=allow profile=any

Access of clients to D2000 Server:

netsh advfirewall firewall add rule name="_D2000 Kernel" dir=in protocol=TCP localport=3119 action=allow profile=any

Rules for D2000 SysConsole (UDP ports 3119 are also needed for the exchange of multicasts between D2000 Kernels in redundancy):

netsh advfirewall firewall add rule name="_D2000 SysConsole64" dir=in program="d:\D2000\D2000_EXE\Bin64\sysconsole.exe" action=allow profile=any

netsh advfirewall firewall add rule name="_D2000 SysConsoleTCP" dir=in protocol=TCP localport=31190-31289 action=allow profile=any

netsh advfirewall firewall add rule name="_D2000 SysConsoleTCP" dir=out protocol=TCP localport=3119,31190-31289 action=allow profile=any

netsh advfirewall firewall add rule name="_D2000 SysConsoleUDP" dir=in protocol=UDP localport=3119,31190-31289 action=allow profile=any

netsh advfirewall firewall add rule name="_D2000 SysConsoleUDP" dir=out protocol=UDP localport=3119,31190-31289 action=allow profile=any

Access to the PostgreSQL database server (for redundant application/archive servers):

netsh advfirewall firewall add rule name="_PostgreSQL" dir=in protocol=TCP localport=5432 action=allow profile=any

Access to the OpenSSH server (for the server that is used by d2u_* utilities to update clients):

netsh advfirewall firewall add rule name="_SFTP" dir=in protocol=TCP localport=22 action=allow profile=any

Other, less used settings:

Access to the EDA server (the port is adjustable with the /EDAP parameter):

netsh advfirewall firewall add rule name="_EDA" dir=in protocol=TCP localport=3121 action=allow profile=any

Access to the Oracle database and Oracle Enterprise Manager - database/archive servers on which Oracle is installed and running:

netsh advfirewall firewall add rule name="_Oracle Server" dir=in protocol=TCP localport=1521 action=allow profile=any

netsh advfirewall firewall add rule name="_Oracle WEB EM" dir=in protocol=TCP localport=1158 action=allow profile=any

Access to the Sybase database server (for the configuration/monitoring/archive database) if only one database process is running:

netsh advfirewall firewall add rule name="_Sybase Server" dir=in protocol=TCP localport=2638 action=allow profile=any

Access to the Sybase database server (for configuration/monitoring/archive database) if multiple database processes are running:

netsh advfirewall firewall add rule name="_Sybase Server" dir=in program="c:\Program Files\SQL Anywhere 12\BIN64\dbsrv12.exe" action=allow profile=any

Of course, additional rules may be necessary due to communications (e.g. access to the D2000 Gateway server, to the UDP port for the SerialOverUDP Device Redundant communication line, or access to the TCP port for server protocols). An example rule for Modbus Server protocol on a TCP/IP-TCP line (a default Modbus port 502):

netsh advfirewall firewall add rule name="_D2000 Modbus Server" dir=in protocol=TCP localport=502 action=allow profile=any