RTDS NETWORK CONNECTION

1. INTRODUCTION

This document specifies three types of network connections for the RTDS simulator.

The following topics are discussed.

1. Stand-alone local area network (LAN) setup
2. Main network setup
3. Remote access

At the end of the document the TCP and UDP ports information related to RTDS are also mentioned.

2. STAND ALONE

- RTDS simulator and host computers are all connected together via Ethernet switches.
- Host computers manually configure their IP addresses to be in the same range as the RTDS simulator so that communication is possible. A diagram is shown in Figure 1, which shows this configuration.

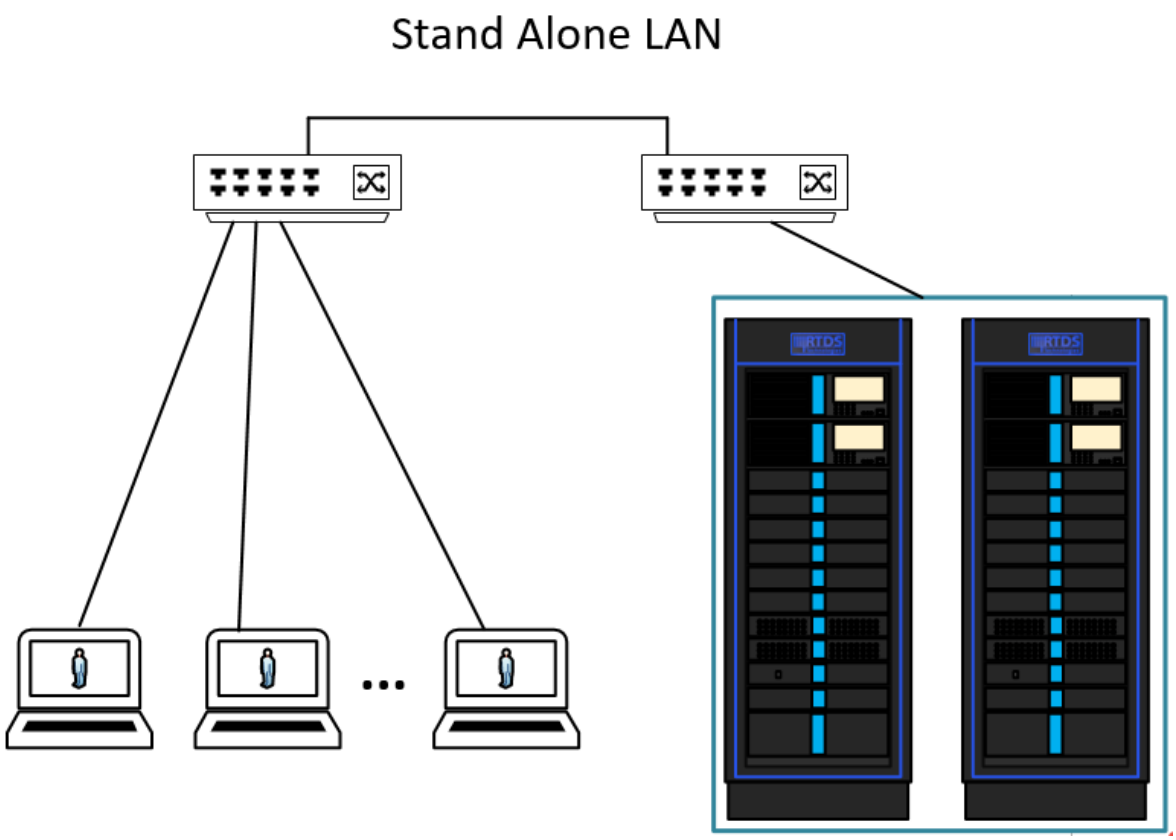

Figure 1 : Standalone LAN Connection Diagram

3. MAIN NETWORK SETUP WITH VPN

- The standalone configuration can be used as the base and then build up to connect to the main network.
- RTDS simulators are configured using static IP addresses provided by the user's IT department.
- With the RTDS simulator reconfigured with the new IP addresses provided by IT department, the RTDS simulator can now be connected to the main network. This will allow anyone connected to this network to access the RTDS simulator and run simulations.
- It also allows for other users in physically distant locations to run simulations if they are able to VPN/remote desktop. VPN network sould be setup to connect to the main network through a firewall for safety of the main network. Typically (but not always) the VPN and firewall are one device.

The connection is shown in Figure 2.

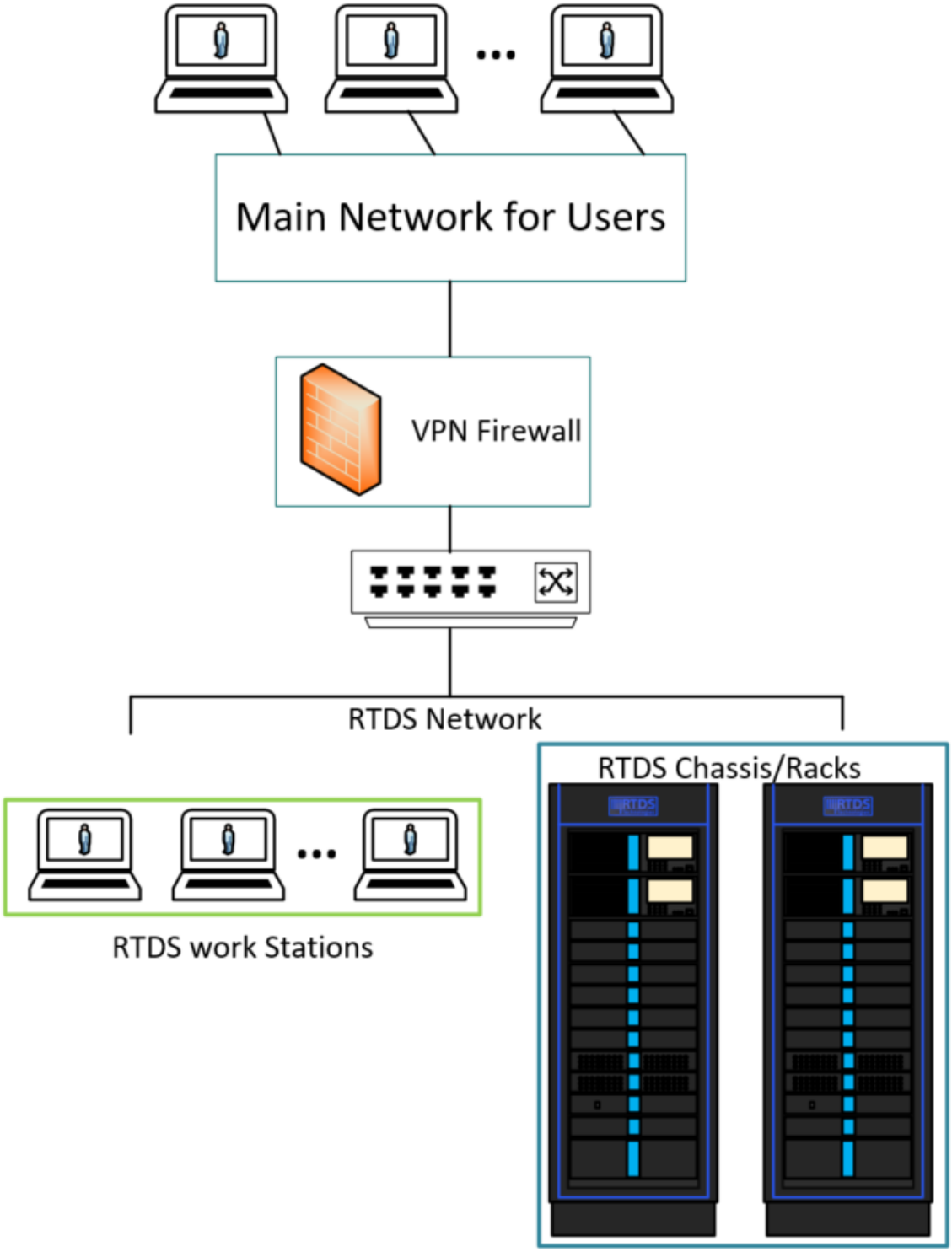

Figure 2 : Main Network Setup with VPN

3.1. ADVANTAGES OF VPN NETWORK

• Anyone with a VPN client can keep their RTDS cases and data local to their PC.

• Does not require as much physical infrastructure because there's no need for a local workstation or jump server.

• If you use an open source VPN solution, such as OpenVPN, it can be fairly inexpensive to deploy.

3.2. DISADVANTAGES OF VPN NETWORK

• Because of the way VPNs are usually implemented, the connected PC is usually connected to an adjacent routable network, rather than being connected directly to the RTDS network. This means that these workstations will normally not be able to see non-routable protocols such as IEC 61850 GOOSE or IEC 61850 SV. These protocols are often used by the GTNET card, and it's useful to be able to see them using Wireshark on a PC. However, because of the way routed VPNs work, this is not possible.

• VPNs effectively extend your security perimeter out to the PCs. So the PCs also need to be secured.

4. SETUP USING JUMP SERVER FOR REMOTE ACCESS

- RTDS simulatos are configured using static IP addresses provided by the user's IT department.
- With the RTDS simulators reconfigured with the new IP addresses provided by IT department, the RTDS simulator can now be connected to a jump server work station.
- This way RTDS simulator is not connected to the main network and is only accessible through the jump work station. Users from the main network connect to the RTDS simulator through a firewall jump server.

The connection is shown in Figure 3.

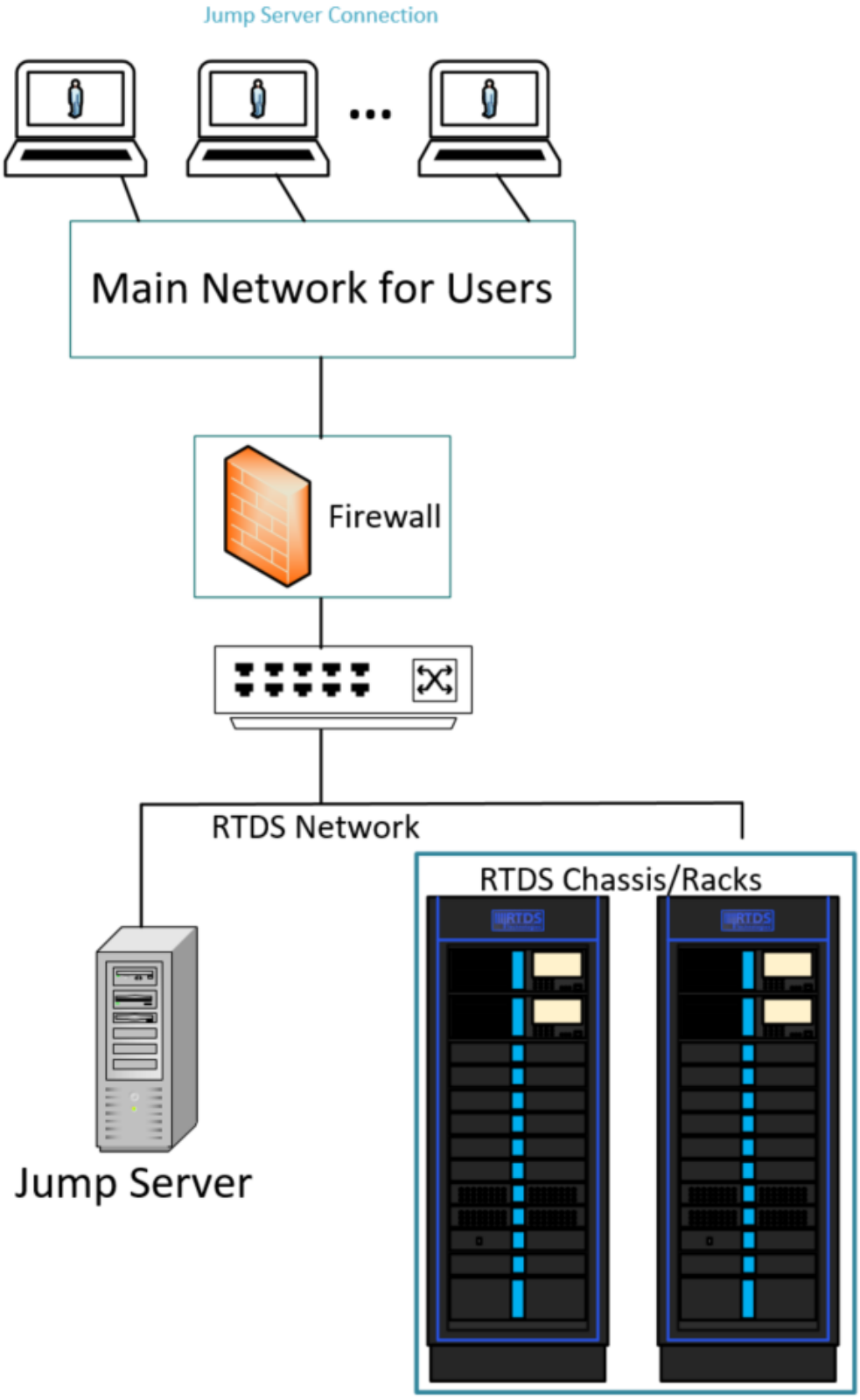

Figure 3 : Jump Server Connection

4.1. ADVANTAGES OF JUMP SERVER NETWORK

- A Jump server is a PC or Windows Server that is directly connected to the RTDS network. And because of this, it should be able to see non-routable protocols such as IEC 61850 GOOSE and SV (as explained above) using Wireshark.
- RTDS cases and data are stored on the jump server; this can simplify backups and security.

4.2. DISADVANTAGES OF JUMP SERVER NETWORK

- This solution is not as scalable as a VPN solution.
- User may want to use a Windows Server operating system with Windows Terminal Server installed, with enough licenses to accommodate all the users. And the Windows server will have to have enough physical resources to support those users. All these add to infrastructure costs.

5. TCP – UDP PORTS

TCP Ports Used By RSCAD:

4068,4069,4070,4071 (Required To Download/Run Cases)

TCP Ports Used By Local Computer:

23 (To Telnet to a rack, or other hardware)

There are also various TCP ports that are user controlled such as:

502 (If Using Modbus Script Functionality on the Default Port)

--- (Any Port Specified in the Listen on Port Runtime Script Command)

--- (Any Port Specified by the PMU Component in Draft)

UDP Ports:

2,4455,4456,53693 (Required To Download/Run Cases)

The *SOURCE* TCP and UDP port numbers are randomly allocated by your PC

(this is typical of most TCP/IP client software).

However there are times when RTDS racks need to send asynchronous commands back to the RSCAD clients which can cause issues when the traffic goes through a NAT firewall. For this reason using a NAT firewall between RSCAD clients and the RTDS racks is not recommended. Using simple TCP/IP routing between RSCAD clients and RTDS racks works fine