GENESIS64 – Communication through a Firewall, DMZ or Cloud

APPLICATION NOTE

October 2015

Description: Guide to setting up communication through a Firewall, DMZ or the Cloud.
General Requirement: Basic knowledge of GENESIS64, networking/firewall knowledge.

Introduction

Many times there is a firewall that an outside client must bypass to access data located on an internal server. This document will describe how to achieve this by using a machine, hereby called the **Edge Server,** situated in the Cloud, Web Server in DMZ, or between Firewalls.

An Edge Server is a GENESIS64 server that forwards client requests to another GENESIS64 Server. The GENESIS64 Server running on the internal network then handles everything and sends the responses back to the client via the Edge Server.

The advantage of this approach is that no new ports need to be opened in your firewalls, because all communication could be via HTTP (port 80).

> **NOTE:** Other ports or different communication channels such as HTTPS or NET.TCP can be set up if desired.

We will assume that you have following setup (see network diagram shown in Figure 1):

- **Edge Server** with an external IP address (193.85.188.171).
- **Internal GENESIS64 Server** (GENESIS64 Application or Server) inside your intranet with an internal name/IP address (172.16.0.241).
- **Firewall** (Firewall) between Edge and Internal Server. Traffic goes through the firewall, but it is not necessary to open a new port unless you want to use a different port or communication channel.
- **Client PC** (WebHMI Client)

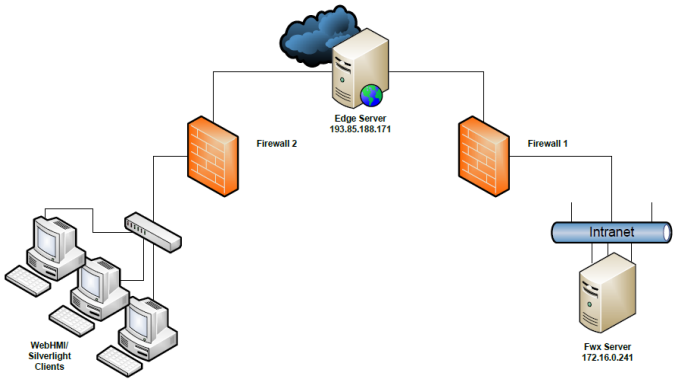

Figure 1 - Network diagram for Edge Solution

Setting up the Edge Server

1. **Start Workbench** by clicking on Start → All Programs → ICONICS → Workbench.
2. Click on **Tools → Platform Services**.
3. Change the Server Role to **Forwarding** as shown in Figure 2.
4. Click on the **Advanced tab** and type in the name or IP address of your internal GENESIS64 Server machine (the internal PC with GENESIS64, shown as 172.16.0.241 on Figure 1).

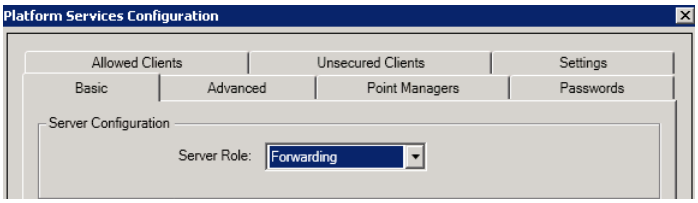

Figure 2 - Adding the forwarded server on the Edge Server

5. Click **OK** to save the changes.
6. Restart **ICONICS FrameWorX** via the Services Control Panel.

Setting up the internal GENESIS64 Server

For security reasons it must be the internal GENESIS64 server which initiates the connection to the Edge server.

1. Start **Workbench**.
2. Click on **Tools → Platform Services.**
3. Click on the **Advanced** tab.
4. Check the box for "Enable Reporting to Server(s) in Azure or DMZ".
5. Type the name or IP address of your Edge server into the list of Server URLs.

NOTE: For improved communication speed, NET.TCP communication channel could be used between the Edge server and the internal GENESIS64 server. In order to do that, you have to specify the protocol and port in the name of the Edge server such as "net.tcp://EdgeServer:8778/NetTcp" instead of stating "EdgeServer" when following step 5.

6. Click **OK** to save the changes. You should see your Edge server in the list as shown in Figure 3.

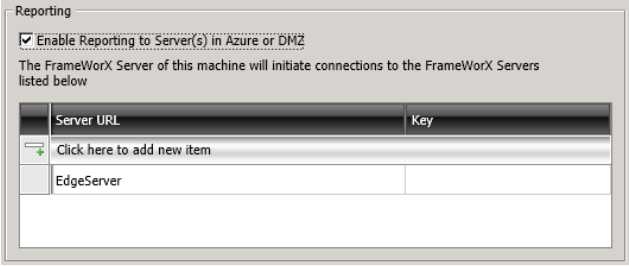

Figure 3 - Enabling Reporting to Edge Servers(s)

7. Restart **ICONICS FrameWorX** via the Services Control Panel.

Setting Up the Clients

1. Start **Workbench** on the Edge server
2. Click on **Tools → FrameWorX Server.**
3. Change the server node to your Edge Server name or IP address and select the HTTP protocol (port 80) as shown in Figure 4 unless you want the clients to use a different channel or port.

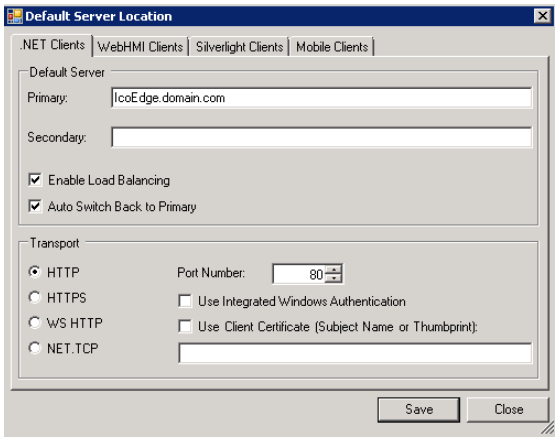

Figure 4 - Settings for .NET Clients

NOTE: .NET Clients tab influences only local .NET clients such as Workbench Classic or GraphWorX64. It has no effect on remote .NET clients because they read the settings from their respective local configuration files. If you have such clients, modify their Default Server Location settings to use the Edge Server.

4. Click Save to apply the changes.

NOTE: The HTTP protocol is slower than NET.TCP. For more details about protocols and ports used by ICONICS products, see the Knowledge Base article KB-2820.

5. Click on the **WEBHMI Clients** tab and make sure that the settings match the .NET Clients settings.
6. Click **Save** to apply the changes.
7. Repeat step 5-6 for **Silverlight Clients**. Note that the HTTP protocol is already set as default, because Silverlight clients run best over this protocol.

Reading Data via Edge

You can now connect .NET, WebHMI, and Silverlight Clients to the Edge server. To test this, follow these steps:

1. On the client(s), create new a GraphWorX64 display with some data points from your internal GENESIS64 Server. Save it and publish it to your web server (most likely your Edge server is also your web server).
2. Open your client and connect to the display you just published. You will see the OPC points and controls with data coming from your internal GENESIS64 server through the Edge server.

Licensing and Security

There is no specific license required for Edge server. All the requests for license from clients are forwarded.

Security context cannot be forwarded in the current version due to requests aggregation. To deploy ICONICS security on the Edge server, you have to synchronize the security configuration on the Edge server with the security configuration on the internal GENESIS64 server.

GENESIS64 through DMZ or the Cloud

Configuring an Edge server to work through DMZ or the Cloud is similar to the steps above. For more details on how to configure GENESIS64 in the Cloud (e.g. Microsoft Azure) refer to Cloud documentation and application notes.

Copyright 2015 ICONICS, Inc.