How To:
Do SOCKS Support with G/On
Support for special applications in G/On environments

Introduction

This document introduces SOCKS and describes the details of and how to configure Giritech's SOCKS server included with G/On 3.5.

SOCKS is an abbreviation of SOCKetS and is an Internet protocol originally developed to allow a host without network access to access resources outside via another host running the SOCKS server. Normal SOCKS servers therefore uses a large "fan-out" allowing the SOCKS clients to connect to any server on the "outside" of the SOCKS server on the Internet.

SOCKS exist in several versions with v5 (RFC 1928) being the latest and uses TCP, usually on port 1080.

To be able to use the SOCKS protocol you will need:

- A SOCKS server (such as the Giritech SOCKS server described herein)
- SOCKS aware application clients configured to use a specific SOCKS server or "Socksification" enabling an non-SOCKS aware application client to use SOCKS without requiring changes to the application client

Note that Giritech does not currently provide the SOCKS aware clients or the "socksification" tools required to enable non-SOCKS aware clients to use the SOCKS protocol!

Benefits

In general SOCKS provides simpler G/On support for some application clients.

The specific advantages of using SOCKS in your G/On environment are that it enables a simpler setup for a range of applications without requiring localhost addressing in the application clients as G/On. Obviously provided the clients are SOCKS aware! This means support for applications using relative links, e.g. some Sharepoint configurations.

Finally note that when using SOCKS with G/On, the standard SOCKS implementation with wide fan-out towards servers on the "back" of the SOCKS server is a major security issue. The Giritech SOCKS server address this issue by controlling what application servers a SOCKS client can communicate with via SOCKS. The Giritech SOCKS server controls what servers are available to which clients via an Admin controlled "whitelist" of servers similar to the server IP addresses in G/On Admin strings.

How To guide

Introduction to the SOCKS protocol in G/On environments

The standard G/On environment, without SOCKS, is shown on the figure below.
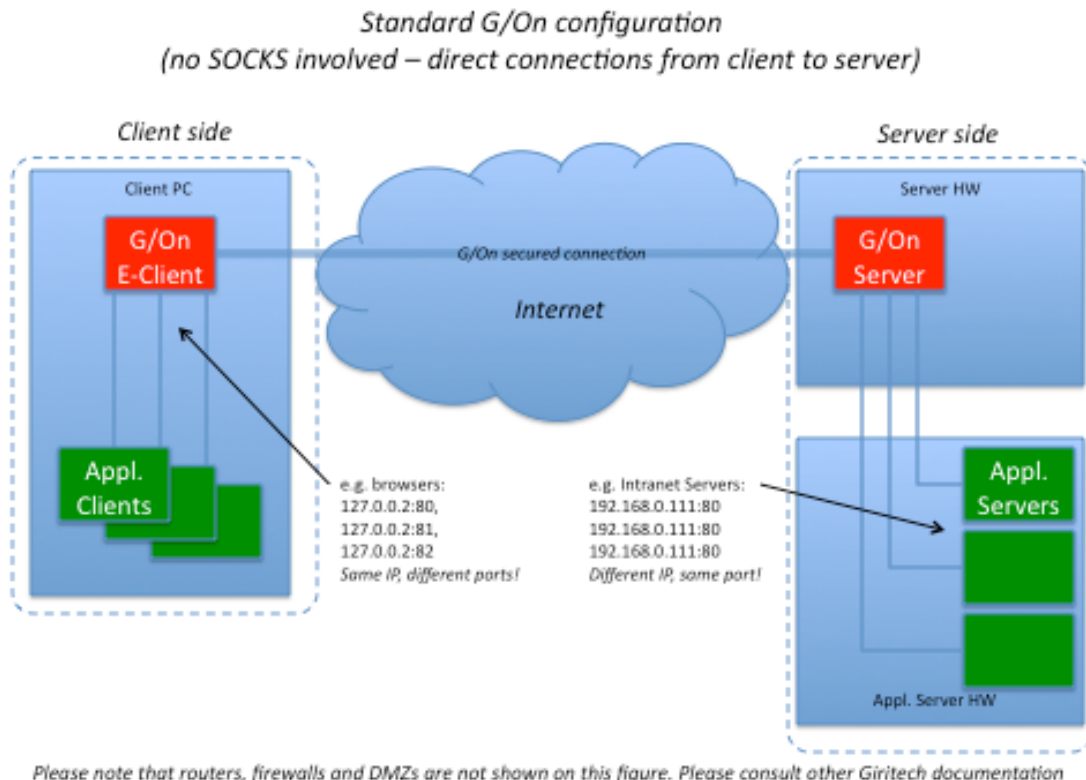
In this setup the application clients communicates with the G/On Client via the localhost on 127.0.0.2 on different ports. Same IP address, different ports. The G/On client protects the traffic and forwards it via the Internet to the G/On server where it is forwarded to the application servers on different addresses and different ports.

On the client side the challenges with this default setup is that all application clients must use the localhost for G/On to be able to "catch" the traffic. Some application clients, e.g. some Sharepoint configurations, might show the wrong address in URLs or fail when using absolute addresses (links). Other clients might not be able to use other ports than the standard application port (e.g. port 3389 = RDP) and because all application clients have to use the same IP address (localhost, 127.0.0.2) it might be required that different clients uses different ports to be able to keep the traffic separate. Finally in some application clients it might not be possible at all to redirect the client to use localhost.

These are typical cases where the SOCKS protocol could help alleviate some of the disadvantages of the standard setup.

The Giritech SOCKS implementation

The Giritech SOCKS implementation consist of a Giritech SOCKS server. The server is to be installed *behind* the G/On server, between the G/On server and application servers as shown on the figure below. Seen from G/On the SOCKS server becomes the only application server to connect to. The SOCKS server delegates the connections to the final application servers.

Standard G/On configuration
(using SOCKS to "capture" traffic from application client – no G/On changes)
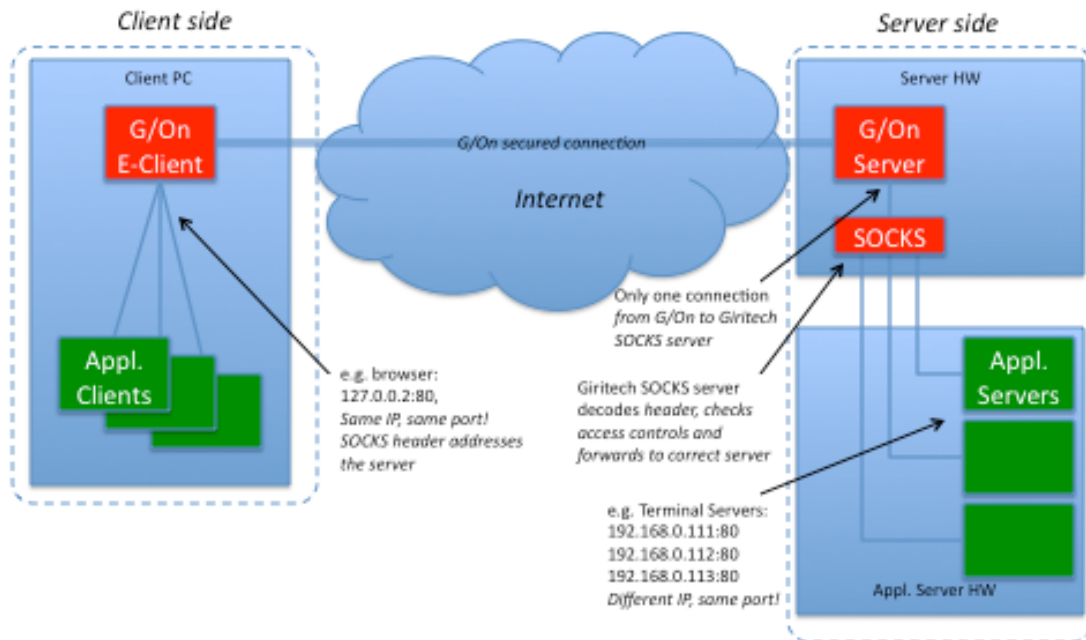
Please note that routers, firewalls and DMZs are not shown on this figure. Please consult other Giritech documentation

The Giritech SOCKS server is reached through the normal G/On localhost port forward and is designed to support SOCKS v4, v4a and v5.

Note:
*To be able to use the Giritech SOCKS server (or any other SOCKS server) you will need your application clients to be SOCKS aware or to be "socksified" by other means. This means that the application clients are able to (or **en-**abled to) communicate using the SOCKS protocol. This part of a SOCKS setup is not delivered by Giritech.*

Configuration of Giritech SOCKS server

As a default we recommend installing the Giritech SOCKS (GSOCKS) server on the same physical (or virtual) server as the G/On server. This allows the G/On server and the GSOCKS server to communicate via localhost and thus makes the GSOCKS server effectively un-available from other servers. There is however nothing preventing you from using a different physical or virtual server as well for running GSOCKS, just be aware that the configuration of G/On and the Giritech SOCKS server changes.

The Giritech SOCKS server is included in the G/On software package from G/On release 3.5 and onwards. You will find the Giritech SOCKS server executables and other files as a `GSOCKS.zip` *file in the* `/tools` *directory after installing the G/On server.*

First you need to unpack the files. We recommend you leave the files in a `GSOCKS` directory on the G/On server, preferably as a sub-directory under `/tools`.

Please familiarize yourself with the README document and the GSOCKS.ini file at this point in the process.

Now you need to configure the GSOCKS server according to your requirements. This process involves two steps:

1. Configuring what port the GSOCKS server should be listening on.
2. Setting up the "whitelist" of application servers to which the GSOCKS server should be able to provide access.

Finally launch the server and test it.

As an example the following outlines how to configure a GSOCKS server according the configuration shown on figure 2 above.

First create a GSOCKS.ini file, by editing the default file provided, containing:

```
LISTEN_ADDR = 127.0.0.1:1080
# The default 127.0.0.1:1080 setting restricts access to localhost
# assuming GSOCKS is on the same physical server as G/On.
# Alternatively use 0.0.0.0:1080 to make GSOCKS listen on all
# interfaces on port 1080.

[access]
# This GSOCKS setup will only allow access to the following IP
# adresses:
192.168.0.7 = *
192.168.0.8:80 = *:80
192.168.0.9 = *
```

First part of the file defines the listen-port, the second part is the "whitelist" of application servers. Note that GSOCKS does serverside resolution of DNS names so you can freely use IP addresses or server names provided your local DNS is setup correctly.

For debugging you can run GSOCKS from the commandline:

```
GSOCKS.exe --foreground
```

GSOCKS will log to GSOCKS.log (unless configured to something else) using the lowest default log-level (1). Maximum log-level is 3.

After testing, install the GSOCKS NT service:

```
GSOCKS.exe install
```

And finally start GSOCKS:
```
GSOCKS.exe start
```
Or
```
net start GSOCKS
```

To stop GSOCKS:
```
GSOCKS.exe stop
```
Or
```
net stop GSOCKS
```
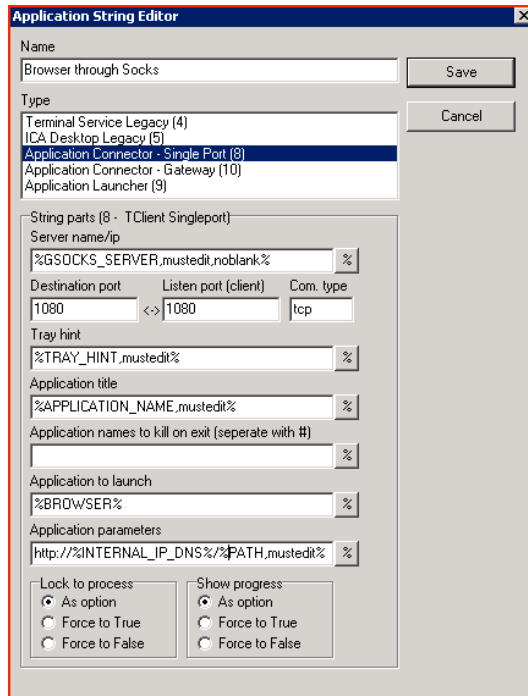
Uninstalling the GSOCKS NT service:

```
GSOCKS.exe remove
```

Setting up G/On to support Giritech SOCKS

The last steps required to enable the Giritech SOCKS server is setting up the G/On server. This requires only a few changes to match what was configured in the GSOCKS.ini file.
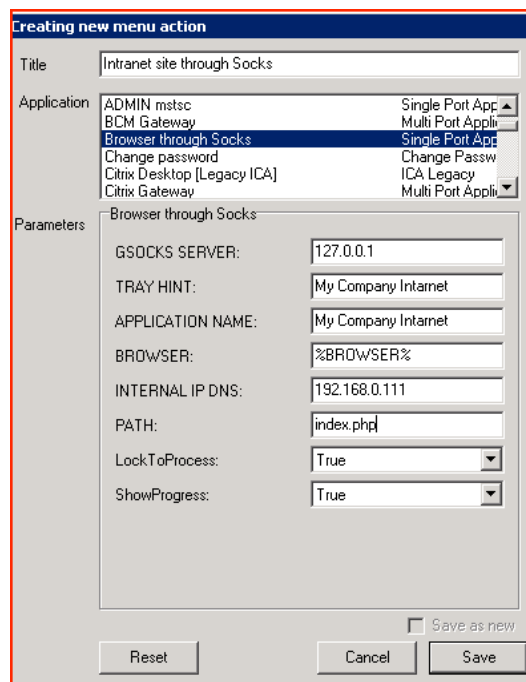
The following typical example shows how to configure a G/On server to use the GSOCKS server for remote browser access to an intranet on the inside of the LAN.

First you need to change or create an application string the can use the SOCKS server for browser access ("Browser through Socks"):

Note how this string is configured to use port 1080 (the SOCKS port) and allows you to enter what SOCKS server you want to use in case you have more than one in your G/On installation.

Secondly you need to enter the parameters to the string to create a "menu action":

In this instantiation you direct the local client (the browser) to communicate via localhost as usual for G/On installations and tells it to access the intranet on the internal IP address 192.168.0.111 looking for "index.php".

The %BROWSER% parameter launches the default Internet browser on the client PC. To make the menu action you created work, the browser must be SOCKS enabled or "socksified" as shown here below.

Please note that this example is for an Internet Explorer statically configured to use proxy.
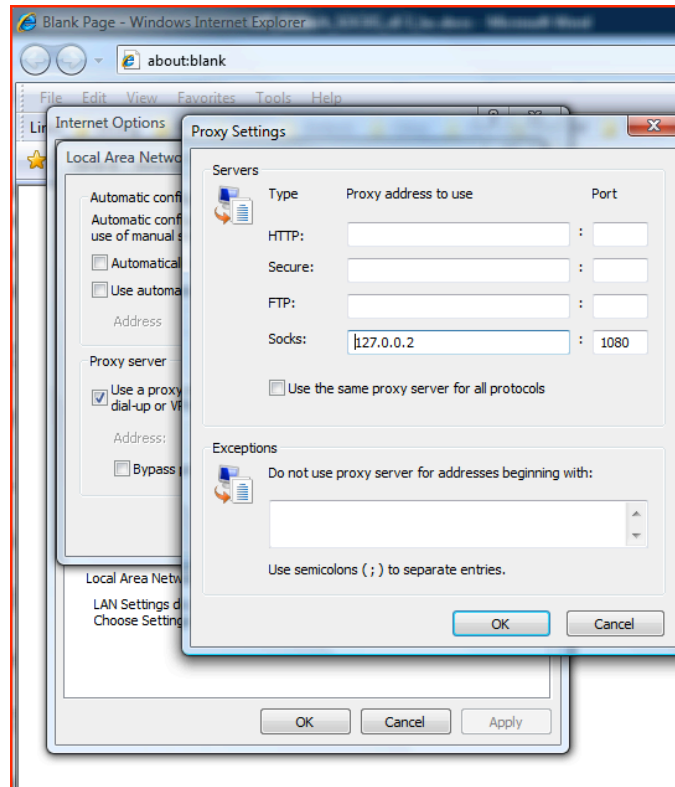
These settings have nothing to do with G/On but direct the SOCKS implementation in the Internet Explorer browser to use the SOCKS server at 127.0.0.2, port 1080. Remember how we configured the G/On installation to forward traffic from this IP:port to the G/On server where it will be forwarded to the Giritech SOCKS server?

This should complete the setup of Giritech SOCKS and enable G/On to use it.

More information

For more information on how to configure the Giritech SOCKS server or help to decide whether your application clients support SOCKS please contact Giritech Support: support@giritech.com