Secure Network Tunnel

Client for IBM i

© Green Screens Ltd., 2016 - 2020.

CONTENT

Introduction

Green Screens VPN Client allows you to securely connect to the IBM I located in different network when hidden behind NAT or Firewall without the need to expose IBM I to the Internet.

Available services are: SOCK5, TELNET, FTP, SSH, HTTP, HTTPS and DDM.

Client programs can be downloaded from:
https://www.greenscreens.io/vpn-download-client.html

Disclaimer

By using this program, you agree with the following:

- Program is free for use, and not chargeable.
- MS Windows version is digitally signed to prevent 3rd party malware injection
- At www.greenscreens.io one can find file hashes to verify file integrity
- Product does not save or record user data or activity.
- Use on your own risk. Green Screens Ltd. will not take any responsibility for damage.
- Green Screens Ltd. does not provide any technical support for this product.
- If Automatic discovery is used, program will contact vpn.greenscreens.io sending digitally signed hash of dynamic serial key to receive public IP address of remote VPN service.
- Upon initial start program will download default configuration (text file) and this pdf manual from www.greenscreens.io

Requirements

VPN Tunnel Service must be run inside local network where IBM I is located and properly configured to be available from the Internet so that this program can connect to.

- Supported OS: MS Windows 32/64bit, Linux 32/64bit, MacOS 32/64bit.
- Public IP address and mapped port for the router behind which VPN Service is running
- IBM I local IP address
- Access token - password for network encryption

First start

On the first run, program will download default **config** file from www.greenscreens.io

Files will be in the same directory where program is running. Config is set to auto-discovery.

Open **config** file with text editor and change following.

- target – router public address and passthrough port pointing to VPN service
- token – network password defined in VPN service

After changing parameters, restart VPN Client. Then use your favorite telnet client and connect to 127.0.0.1:23

Manual mode

In a case auto-discovery is not available or for security concerns, change configuration to manual mode by disabling auto-discovery.

Open **config** file with text editor and change following.

- auto – set to “false” to disable discovery service
- target – set to the Public IP address and port of your remote VPN service (x.x.x.x:52520)

After changing parameters, restart VPN Client

Connecting to the IBM i

Connection can be established directly or through SOCK5 protocol.

NOTE: Green Screens Server support SOCK5 and use it as a default mechanism.

If SOCK5 is used, software clients must support proxy SOCK5. In such a case, IBM i IP address will be local IP or remote network such as 192.168.x.x or 10.x.x.x network range. And SOCK5 IP address will be 127.0.0.1.

When software client does not support SOCK5, direct connection is the only possibility. To connect to the IBM I, use “localhost” or 127.0.0.1. Software such as telnet clients will now connect to the locally running VPN client.

VPN client takes care of encrypting and redirecting all the data to the remote VPN Service running inside your company network close to the IBM i.

SSL/TLS security

Version 2.0 supports strong password based and certificate-based TLS network encryption. Level of TLS encryption depends on strength of the certificate keys. The bigger the key, the better protection but also slower.

It is possible to mix password based and TLS based encryption to get multiple layers of networked encryption, however this is not recommended due to performance issues if many parallel connections are used.

NOTE: Shared password connections (fastest), highly secure if password is kept secret. Also, this is the easiest way to setup a VPN tunnel.

- To use only shared password encrypted connections – set **tls: 0** in **config.client** file.
- To use TLS only encrypted connections – set **tls: 1** in **config.client** file.
- To use TLS and shared password encrypted connections – **set tls: 2** in **config.client** file.

NOTE: The same type of security settings must be set on VPN Client and VPN server.

Certificates

When using certificates, **bin** file used by VPN Service must be used here also to enable TLS. Files must be in the same directory where VPN Client is running. Bin file is named by the IBM I serial number used.

Configuration file format

Config file is in YAML format where all parameters are in the following format:
[name][column][space][value]

Example: **telnet: 23:23**

To set empty value (overriding program defaults)

Example1: **telnet: #23:23**

Example2: **telnet:**

Standard services

There are 6 standard services supported: SOCK5, TELNET, FTP, SSH, HTTP, HTTPS

Services are configured with default ports and their mappings to the ports on the remote side.

Format is:
protocol: in_port:out:port

Format example:
telnet: 23:23

NOTE: Program will start network services listening on ports defined inside config file. It might happen that some other programs are already using some of the ports. In that case, port remapping is required.

For an example, if local port 23 is already used, change configuration to connect to port 2300:

telnet: 2300:23

Now, local telnet client will connect to 127.0.0.1:2300

DDM Services

DDM services are part of IBM I, used by System I navigator, JT400, and Client Access, ACS etc.

NOTE: DDM service use multiple ports and main setup port 449 which request for other port mappings from IBM I server. As dynamic port assignment is not available, ports must be set manually to match the ports defined on IBM I system. Config file is already preconfigured with standard ports.

If DDM services are note used, set **ddm: off** (default is on)

If DDM SSL is used, set **ssl: on** (default is off)

Default configuration parameters

auto: true

tray: true

token:
target: 127.0.0.1:52520

ssl: off
ddm: on

sock: 1080
telnet: 23:23
ftp: #21:21
ssh: #22:22
http: #80:80
https: #443:443

as-svrmap: 449

as-drda: 446
as-central: 8470
as-database: 8471
as-dataq: 8472
as-file: 8473
as-netprt: 8474
as-rmtcmd: 8475
as-signon: 8476

as-drda-ssl: 448
as-central-ssl: 9470
as-database-ssl: 9471
as-dataq-ssl: 9472
as-file-ssl: 9473
as-netprt-ssl: 9474
as-rmtcmd-ssl: 9475
as-signon-ssl: 9476

© 2016 Green Screens Ltd. All Rights Reserved.