Secure Network Tunnel

Service for IBM i

CONTENT

Introduction

Green Screens VPN Service allows you to securely connect to the IBM I from outside world when IBM I is hidden behind NAT or Firewall without the need to expose IBM I itself to the Internet.

This is an alternative solution to VPN Network appliances. Service has twofold purpose:

- **Cloud Mode** - used with Green Screens Server to enable secure link with IBM I located behind NAT/Firewall.

- **Standalone Mode** - used with free VPN client to open secure tunnel. Use any standard telnet, ftp, ssh client or web browser to securely access available services running on the IBM I located behind firewall or NAT.

Service supports 2 encryption modes: token based and TLS certificate-based mode. Both methods use the same modern, fast and highly secure encryption algorithms.

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

Disclaimer

By using this program, you agree with the following:

- Program is free for use, and not chargeable when used in cloud mode.
- Standalone operational mode is limited to 15 concurrent connections, 30 minutes time limit unless licensed.
- Cloud operational mode for Green Screens Server integration is unlimited.
- 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 free version.
- If Automatic discovery is used, program will contact vpn.greenscreens.io sending digitally signed hash of dynamic serial key and defined public port to register VPN service in auto discovery cache, used by VPN clients when running auto-discovery mode.
- Upon initial start program will download default configuration and this pdf manual from www.greenscreens.io

Requirements

VPN Service program must be run inside local network where IBM I is located and properly configured to be available from the Internet so that VPN client 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
- Optionally admin password for remote management.

First start

On the first run, program will create default **config** file for standalone usage.

Files will be in the same directory where program is running.

Program will generate and save token inside config file. Share that token with VPN clients.

To change token, remove token from config file, start program to generate a new one. Program will save new token to config file. Upon every start, program will create qr.png barcode image for easier configuration through management mobile application.

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

- source – router public address and passthrough port pointing to VPN service
- target – IBM I local IP address in local network
- token – network password
- mode – “standalone” (for VPN clients)

After changing parameters, restart VPN Service.

Manual mode

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

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

- auto – set to “false” to disable discovery service
- source – router public address and passthrough port pointing to VPN service running inside internal network

After changing parameters, restart VPN Service.

Auto discovery

When enabled, program will contact **vpn.greenscreens.io** online service to detect program public IP address. IP address and port defined in config file (source attribute) will be cached on **vpn.greenscreens.io** for vpn clients to be able to retrieve data.

NOTE: VPN client will be able to retrieve the data only if it is configured with the same token.

Cloud mode

Cloud mode is used only with **Green Screens Terminal Service** running in cloud. Connection configuration from **Green Screens Terminal Service** to the VPN Service must be configured through Green Screens Terminal Service Web Admin console, Proxy settings from side bar menu.

When running in cloud mode, VPN client will not be able to connect.

Single VPN Service instance is required for every IBM I server.

Here is an example configuration for cloud mode. This is intentional for security and stability reasons. If one VPN service must be stopped or get crashed, only connections for a single IBM I server will be lost.

```
notray: true
mode: cloud
source: 35.x.x.x:52520
target: 192.168.1.192:23
token: Aj5+Ga1+bj4hJT12aiK4aD58Jmk6PGkvkts9P24kJd2oyaDsyMiS9SE1OPls=
cloud: http://demo.greenscreens.io
```

- source – incoming IP address and port (network router)
- target – IBM I IP address in internal network
- cloud - Green Screens server URL address

Also, there will be a license file named by IBM I system serial number (required) in format SYTEMSERIAL.bin.

Security

All network data between VPN Client and VPN service are encrypted with modern fast encryption algorithm: AEAD-CHACHA20-POLY1305. Data is secure if **token** used is securely distributed to the workstation operators and if operators take care about keeping passwords safe.

Network security

All incoming network packets are introspected and filtered. All packets will be redirected to the target IP, access to other resources are blocked.

Auto-discovery security

Only data sent to **vpn.greenscreens.io** service is defined public port used to access to the VPN Service. All other data are 2-layer digital signatures based on HMAC to ensure data came from our compiled programs and your defined token to prevent tampering or injecting wrong information by 3rd party. Communication is made through TLS encrypted protocol.

Below are examples of sent and received data.


```
{
 "k":"fa4bc8aae1b14877a644143de6916fbf3f44281d96115b3aeb662927fca3f279",
 "d":"f9jfHYS_3ZgtXSj_h6T9O8f5hfe-gZ28afZj34WlpmQ=",
 "s":"SaulJNCYMhRx1DhiXCeRe2So8UZnb51RH1F6fWpvL9c=",
 "v":"BWL7S8yddpF08qKLXbgGvQ==",
 "u":"1586067031",
 "p":"52520"
}

{
 "k":"fa4bc8aae1b14877a644143de6916fbf3f44281d96115b3aeb662927fca3f279",
 "d":"f9jfHYS_3ZgtXSj_h6T9O8f5hfe-gZ28afZj34WlpmQ=",
 "s":"SaulJNCYMhRx1DhiXCeRe2So8UZnb51RH1F6fWpvL9c=",
 "v":"BWL7S8yddpF08qKLXbgGvQ==",
 "u":"1586067031",
 "p":"52520",
 "ip":"127.0.0.1",
 "ts":1586067032,
 "hash":"M8HJbVLs3lduX5yg3y2zoSdLSwJyzznrs5VSh2fHV6w="
}
```


Admin security

If admin password set, it will enable remote controlling VPN service through our mobile application.

All requests are signed with HMAC internal application generated keys and defined admin password to ensure that data came from our application and owner of the password.

Currently available options are¸: get stats, enable or disable accepting client connections.

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

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

To generate certificates, use our own tool **Certgen**.
Download from: https://www.greenscreens.io/vpn-download-certgen.html.

Copy certificate files into VPN Service directory then enable TLS by setting it to 1 and optionally tlsVerify to true.

- To enable client certificate validation set **tlsVerify: true** in **config.server** file and **config.client**
- Distribute generated bin file to VPN Clients

NOTE: Settings for tls and tlsVerify must be the same on VPN Service and Client.

Certificates

When using certificates, following files are required in PEM encoded format: ca.pem, ca.key, server.pem, server.key and optionally client.pem if tlsVerify is enabled. Files must be in the same directory where VPN Service is running.

On every start application will create **bin** file for mobile application (service remote control) and for VPN Client. All listed certificate files must be available for **bin** file to be valid. How to use **bin** file with our mobile app, please refer to the mobile app manual.

NOTE: bin file will be named as defined IBM I system serial number.

Configuration file format

Config file is in YAML format where all parameters must end with column and space:
[name][column][space][value]

Example: **telnet: 23:23**

To set empty value (overriding program defaults)

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

Example2: **telnet:**

Default configuration parameters

File name is “config” without extension and must be placed in the same directory with the service program.

```
# COMMON PARAMETERS

# to enable tls,set 1 or 2 depending on operational mode
# 1 – only tls, 2 – tls and password encryption
tls: 0

# enable client certificate verification
tlsVerify: false

# auto detect public IP (serial value must not be empty)
auto: false

# listening router public IP and port
# to use public IP auto-detection,
# comment first line and uncomment second line

source: 192.168.1.3:52520
#source: :52520

#IP address of IBM i server in local company network
target: 192.168.1.100:23

# Set to true to enable system tray (windows only)
tray: false

# Set to "cloud" when used with Green Screens Server
# Set to "standalone" when used with VPN Client
mode: standalone

# Access token
#token:
```