The GSW Business Tunnel Example Guide

GSW Business Tunnel
Example Guide

These examples are to help guide you through the configuration of your GSW Business Tunnel for many different scenarios.

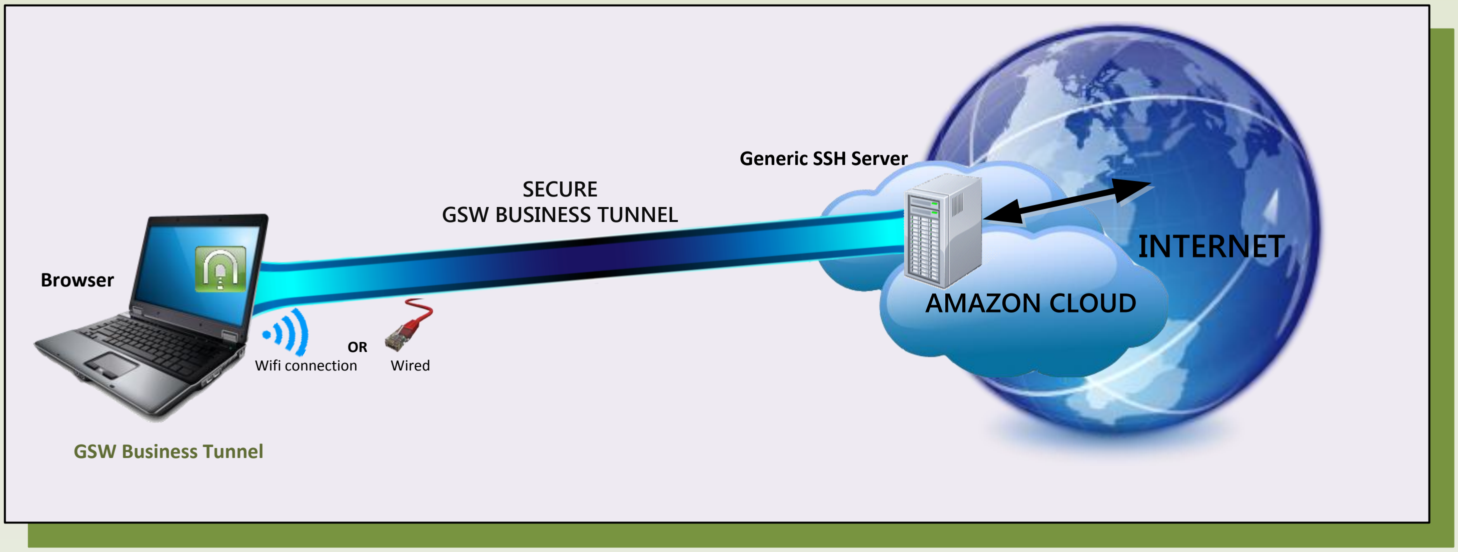
The GSW Business Tunnel can do local, dynamic or remote port forwarding. The examples are categorized by their type of port forwarding. Local port forwarding examples begin with L and then are numbered sequentially. Remote and Dynamic examples follow the same pattern.

Table of Contents

GSW
Business Tunnel

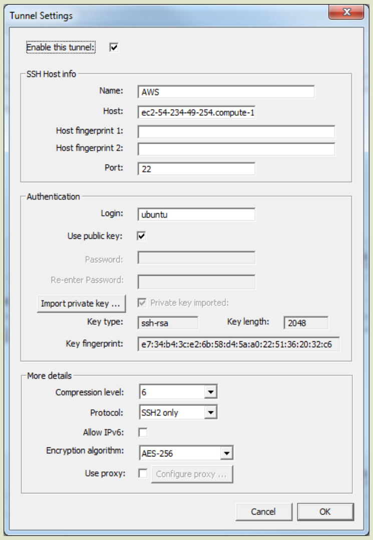
Example D01

Browse Internet Securely by Tunneling through a Generic SSH Server on Amazon Cloud



CASE: *Securely Browse the Internet by Tunneling through a Generic SSH Server on Amazon Cloud*
You can securely browse the Internet using the GSW Business Tunnel by using a generic SSH Server on the Amazon Cloud.

Laptop- GSW Business Tunnel Settings


Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: AWS
Host: ec2-54-234-49-254.compute-1
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: ubuntu
Use public key: ☑
Password:
Re-enter Password:
Import private key ... ☑ Private key imported:
Key type: ssh-rsa Key length: 2048
Key fingerprint: e7:34:b4:3c:e2:6b:58:d4:5a:a0:22:51:36:20:32:c6

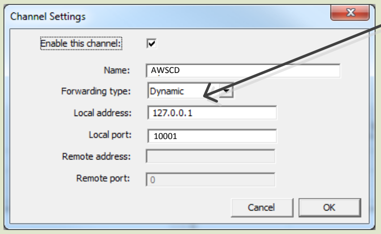
More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: ☐
Encryption algorithm: AES-256
Use proxy: ☐ Configure proxy ...

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. This is provided when you set up your Amazon Cloud.

2. Set Authentication Requirements. This is the logon ID and the private key provided when you set up the Amazon Cloud.

Laptop- GSW Business Channel Settings

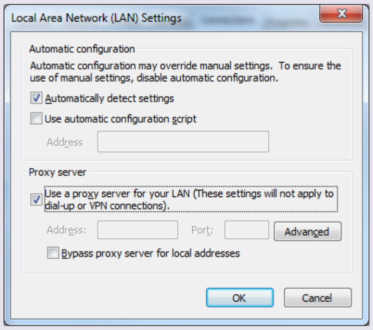

Channel Settings

Enable this channel: ☑
Name: AWSCD
Forwarding type: Dynamic
Local address: 127.0.0.1
Local port: 10001
Remote address:
Remote port: 0

1. Select Dynamic Forwarding.
2. Use the loopback address
3. Choose an available port for the local port.

Laptop- Browser Configuration

IE -> TOOLS -> Internet Options -> Connections -> LAN settings

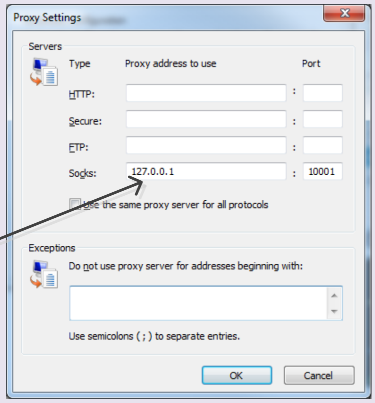

Local Area Network (LAN) Settings

Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
☑ Automatically detect settings
☐ Use automatic configuration script
Address

Proxy server
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: Port: Advanced
☐ Bypass proxy server for local addresses

1. Enable Proxy Server

2. Click on Advanced
Opens Proxy Settings.


Proxy Settings

Servers
Type Proxy address to use Port
HTTP: :
Secure: :
FTP: :
Socks: 127.0.0.1 : 10001
☐ Use the same proxy server for all protocols

Exceptions
Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

3. Configure Proxy Address and Port Number
The channel configuration for the local address and local port is used in the browser configuration. These must match. (See arrow)

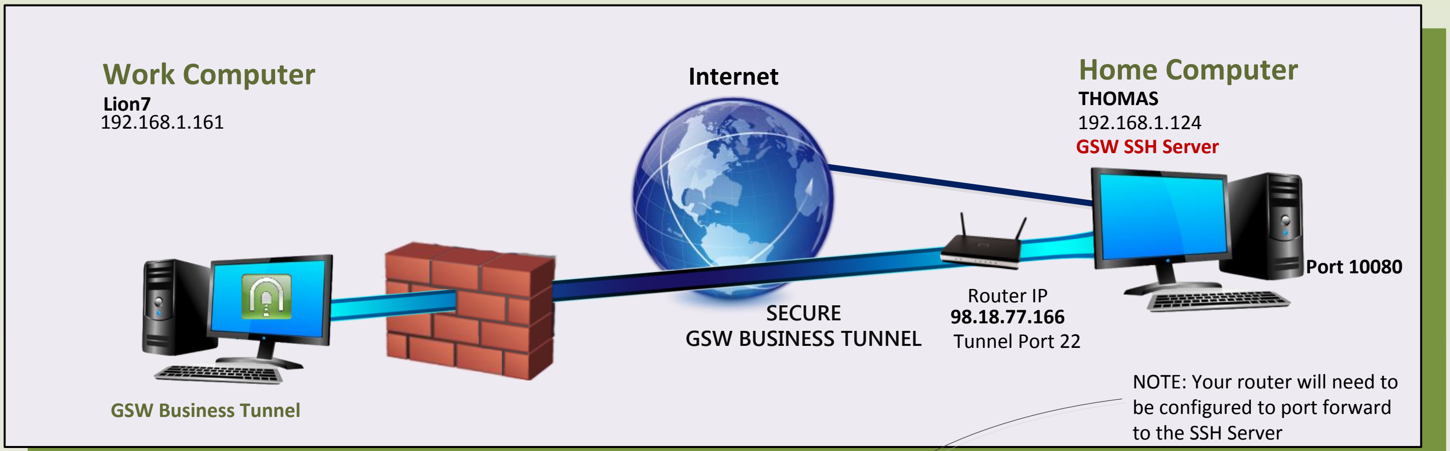
4. Click OK, OK, Apply
Your browser is now configured to use the Tunnel.
In some instances it applies to new browsers opened.

Note: Each browser has a way to enable a proxy server for the LAN.
This example shows Microsoft Internet Explorer 10 (IE 10).

GSW Business Tunnel

Example D02

Securely connect to your home computer from work and use it to browse the internet



Work Computer
Lion7
192.168.1.161

GSW Business Tunnel

Internet

SECURE
GSW BUSINESS TUNNEL

Router IP
98.18.77.166
Tunnel Port 22

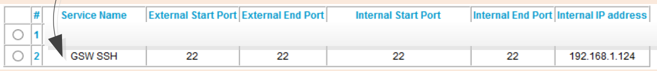
Home Computer
THOMAS
192.168.1.124
GSW SSH Server

Port 10080

NOTE: Your router will need to be configured to port forward to the SSH Server

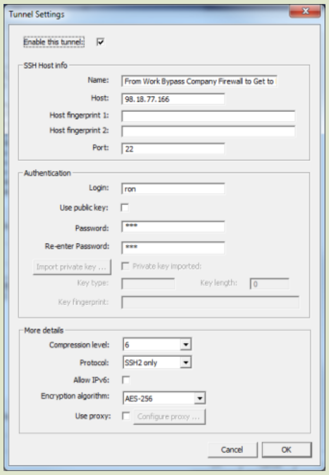
CASE: *Securely create a tunnel through a firewall to a SSH Server and Browse the Internet*
Your company firewall blocks all internet browsing. You have received permission to access certain web sites for work, but company policy will not allow the firewall to be opened up to HTTP traffic. The company firewall is open to SSH traffic. You can create a secure tunnel to a SSH server located at home (or anywhere else that you have access) and browse the internet.

NetGear N300 Router – Port Forwarding Configuration



	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○	2	GSW SSH	22	22	22	22	192.168.1.124

Lion7 – GSW Business Tunnel Configuration



Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: From Work Bypass Company Firewall to Get to
Host: 98. 18. 77. 166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: ron
Use public key: □
Password: ***
Re-enter Password: ***
Import private key ... □ Private key imported:
Key type: Key length: 0
Key fingerprint:

More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: □
Encryption algorithm: AES-256
Use proxy: □ Configure proxy ...

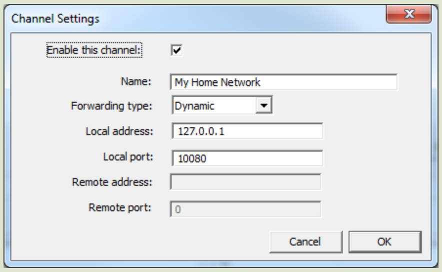
Cancel OK

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarding to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lion7 – Channel Configuration



Channel Settings

Enable this channel: ☑
Name: My Home Network
Forwarding type: Dynamic
Local address: 127.0.0.1
Local port: 10080
Remote address:
Remote port: 0

Cancel OK

1. Select Dynamic forwarding type.

2. Set the loopback address (127.0.0.1) as the local address.

3. Choose available port number to assign for local port. We selected 10080.

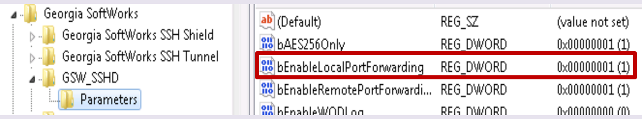
Note: Make sure that the local address and local port are the same ones used in the browser proxy configurations for SOCKS address and Port (see right)

Thomas – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

X64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

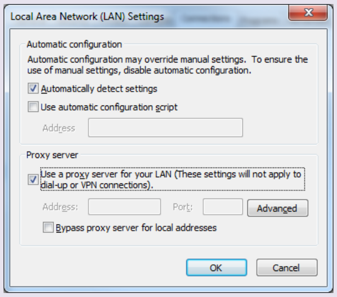
X86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



```
(Default)                    REG_SZ      (value not set)
bAES256Only                  REG_DWORD   0x00000001 (1)
bEnableLocalPortForwarding   REG_DWORD   0x00000001 (1)
bEnableRemotePortForwardi... REG_DWORD   0x00000001 (1)
bEnableWODLog                REG_DWORD   0x00000000 (0)
```

Lion7 – Browser Configuration

1. Enable Proxy Server
IE -> TOOLS -> Internet Options -> Connections -> Advanced LAN settings



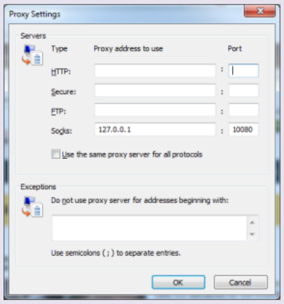
Local Area Network (LAN) Settings

Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
☑ Automatically detect settings
□ Use automatic configuration script
Address

Proxy server
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: Port: Advanced
□ Bypass proxy server for local addresses

OK Cancel

2. Configure SOCKS Address and Port



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:		
Secure:		
FTP:		
Socks:	127.0.0.1	10080

□ Use the same proxy server for all protocols

Exceptions
Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

OK Cancel

Note: Each browser has a way to enable a proxy server for the LAN.
This example shows Microsoft Internet Explorer 10 (IE 10).

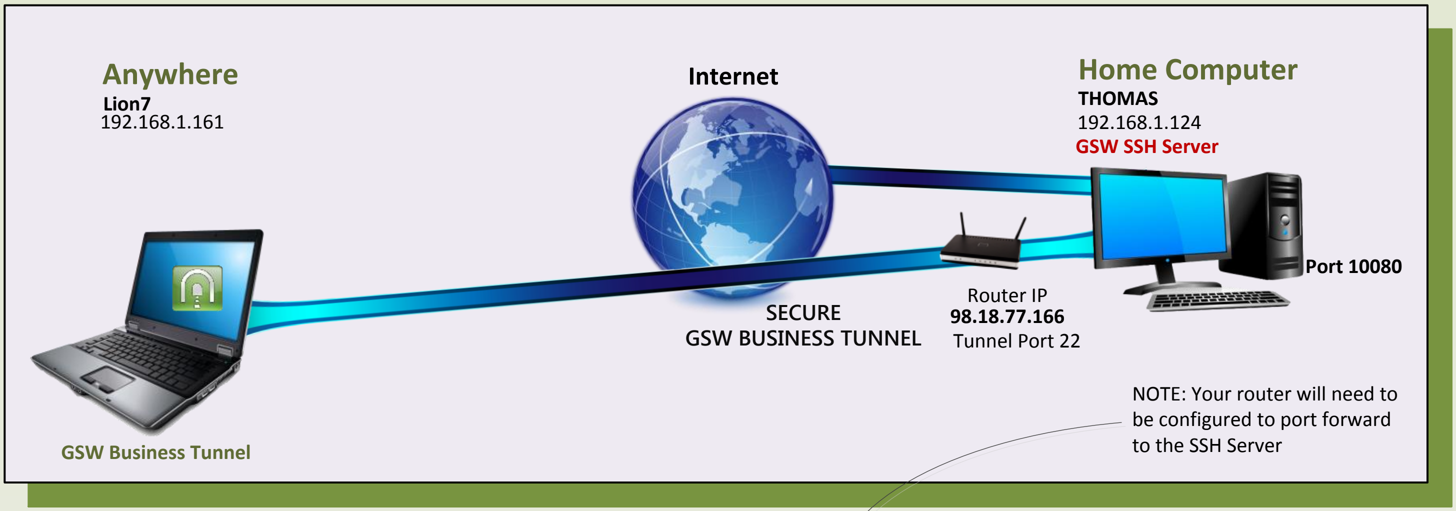
Lion7 – Browser Usage

Open Browser and enter the URL to start browsing.

GSW Business Tunnel

Example D03

Securely Connect to Your Home Computer From Anywhere Browse the Internet



Anywhere
Lion7
192.168.1.161

Internet

Home Computer
THOMAS
192.168.1.124
GSW SSH Server

Port 10080

SECURE
GSW BUSINESS TUNNEL

Router IP
98.18.77.166
Tunnel Port 22

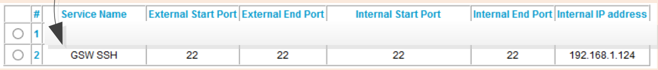
NOTE: Your router will need to be configured to port forward to the SSH Server

GSW Business Tunnel

CASE: *Connect to your Home Computer from Anywhere and Browse the Internet*
You are traveling and want to Remote Desktop to your home computer. You can do this from anywhere using the GSW Business Tunnel.

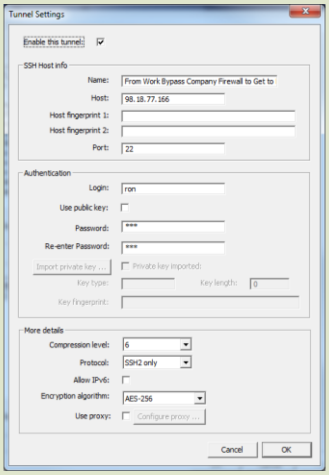
**Note: This example is the same configuration as D02.

NetGear N300 Router – Port Forwarding Configuration



	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○	2	GSW SSH	22	22	22	22	192.168.1.124

Lion7 – GSW Business Tunnel Configuration



Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: From Work Bypass Company Firewall to Get to
Host: 98. 18. 77. 166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: ron
Use public key: ☐
Password: ***
Re-enter Password: ***
Import private key ... ☐ Private key imported:
Key type: Key length: 0
Key fingerprint:

More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: ☐
Encryption algorithm: AES-256
Use proxy: ☐ Configure proxy ...

Cancel OK

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarding to the SSH Server Host, so we use the router IP Address

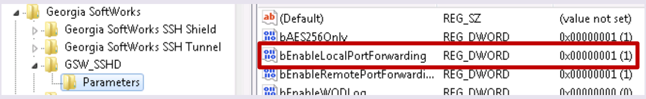
2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Thomas – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

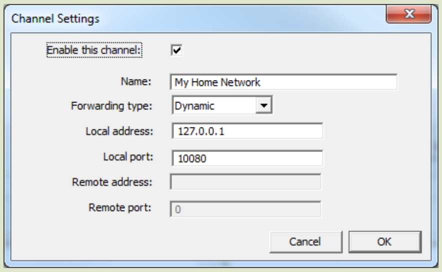
x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



```
Georgia SoftWorks                          (Default)                      REG_SZ     (value not set)
   Georgia SoftWorks SSH Shield            bAES256Only                    REG_DWORD  0x00000001 (1)
   Georgia SoftWorks SSH Tunnel            bEnableLocalPortForwarding     REG_DWORD  0x00000001 (1)
   GSW_SSHD                                bEnableRemotePortForwardi...   REG_DWORD  0x00000001 (1)
      Parameters                           bEnableWODLog                  REG_DWORD  0x00000000 (0)
```

Lion7 – Channel Configuration



Channel Settings

Enable this channel: ☑
Name: My Home Network
Forwarding type: Dynamic
Local address: 127.0.0.1
Local port: 10080
Remote address:
Remote port: 0

Cancel OK

1. Select Dynamic forwarding type.

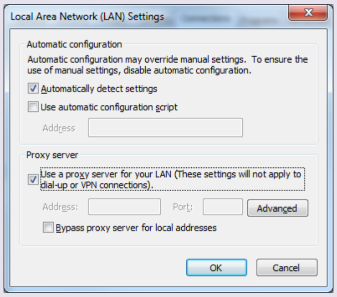
2. Set the loopback address (127.0.0.1) as the local address.

3. Choose available port number to assign for local port. We selected 10080.

Note: Make sure that the local address and local port are the same ones used in the browser proxy configurations for SOCKS address and Port (see right)

Lion7 – Browser Configuration

1. Enable Proxy Server
IE -> TOOLS -> Internet Options -> Connections -> Advanced LAN settings



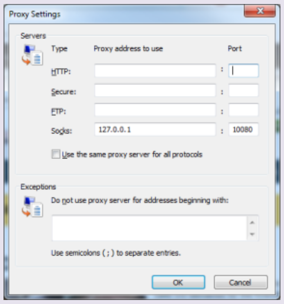
Local Area Network (LAN) Settings

Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
☑ Automatically detect settings
☐ Use automatic configuration script
Address

Proxy server
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: Port: Advanced
☐ Bypass proxy server for local addresses

OK Cancel

2. Configure SOCKS Address and Port



Proxy Settings

Servers
Type Proxy address to use Port
HTTP: :
Secure: :
FTP: :
Socks: 127.0.0.1 : 10080
☐ Use the same proxy server for all protocols

Exceptions
Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

OK Cancel

Note: Each browser has a way to enable a proxy server for the LAN.
This example shows Microsoft Internet Explorer 10 (IE 10).

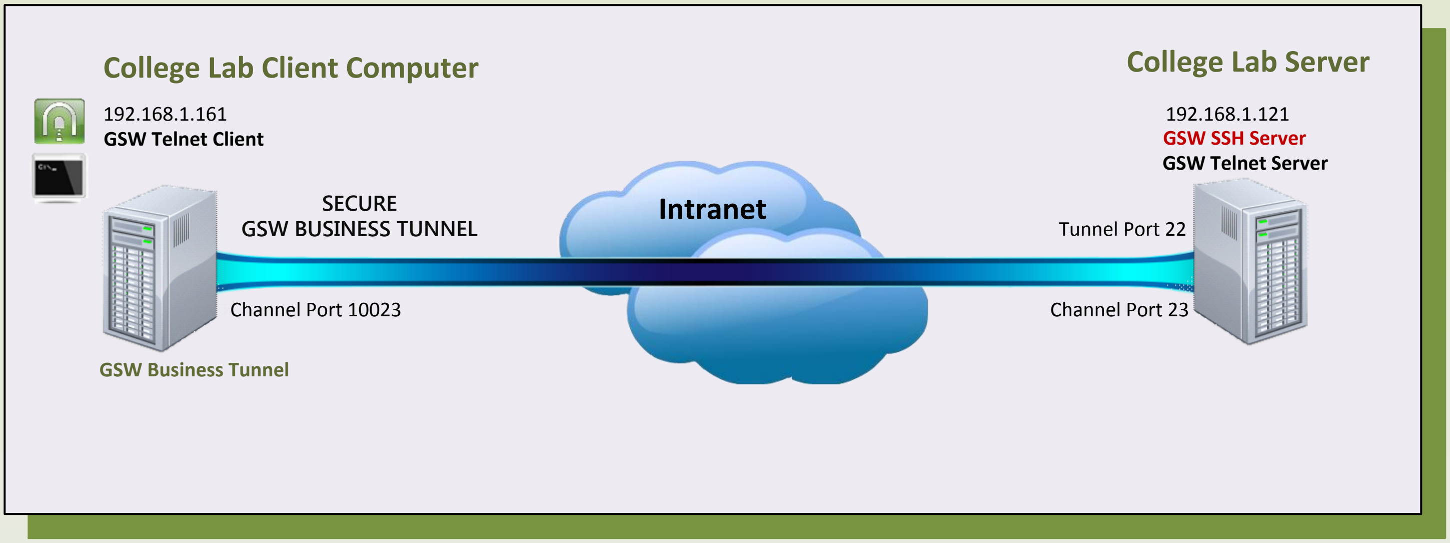
Lion7 – Browser Usage

Open Browser and enter the URL to start browsing.

GSW Business Tunnel

Example L01

Make a Telnet Connection Secure using the GSW Business Tunnel



College Lab Client Computer

192.168.1.161
GSW Telnet Client

College Lab Server

192.168.1.121
GSW SSH Server
GSW Telnet Server

SECURE
GSW BUSINESS TUNNEL

Intranet

Channel Port 10023

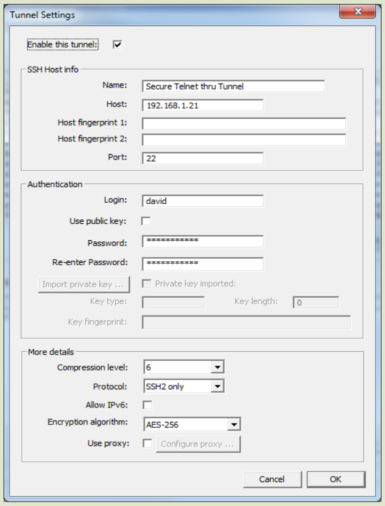
Tunnel Port 22

Channel Port 23

GSW Business Tunnel

Case:
A local technical college wants to demonstrate how you can secure telnet with an SSH Tunnel. In the technical lab they set up a telnet connection and use a network monitoring tool to observe the data. Then as shown in this example they set up the GSW Business Tunnel and then create the Telnet connection. Now when they monitor the line the data is encrypted

Lab Client Computer – GSW Business Tunnel Configuration



Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: Secure Telnet thru Tunnel
Host: 192.168.1.21
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: david
Use public key: ☐
Password: ***********
Re-enter Password: ***********
Import private key ... ☐ Private key imported:
Key type: Key length: 0
Key fingerprint:

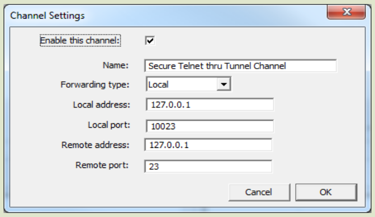
More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: ☐
Encryption algorithm: AES-256
Use proxy: ☐ Configure proxy ...

SSH Host and Authentication Settings

1. Set Address of SSH Server Host.

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lab Client Computer – Channel Configuration



Channel Settings

Enable this channel: ☑

Name: Secure Telnet thru Tunnel Channel
Forwarding type: Local
Local address: 127.0.0.1
Local port: 10023
Remote address: 127.0.0.1
Remote port: 23

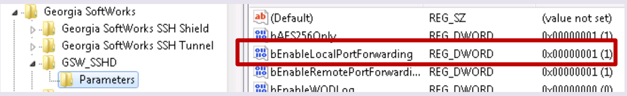
1. Select Local forwarding type.
2. Set the loopback address (127.0.0.1) as the local address.
3. Choose available port number to assign for local port. We selected 10023.
4. For the remote address, use the loopback address 127.0.0.1
5. For the remote port, use Port 23, the common Telnet Server port.

College Lab Server – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



```
Georgia SoftWorks
  Georgia SoftWorks SSH Shield
  Georgia SoftWorks SSH Tunnel
  GSW_SSHD
    Parameters
```

```
(Default)                       REG_SZ      (value not set)
bAES256Only                     REG_DWORD   0x00000001 (1)
bEnableLocalPortForwarding      REG_DWORD   0x00000001 (1)
bEnableRemotePortForwardi...    REG_DWORD   0x00000001 (1)
bEnableWODLog                   REG_DWORD   0x00000000 (0)
```

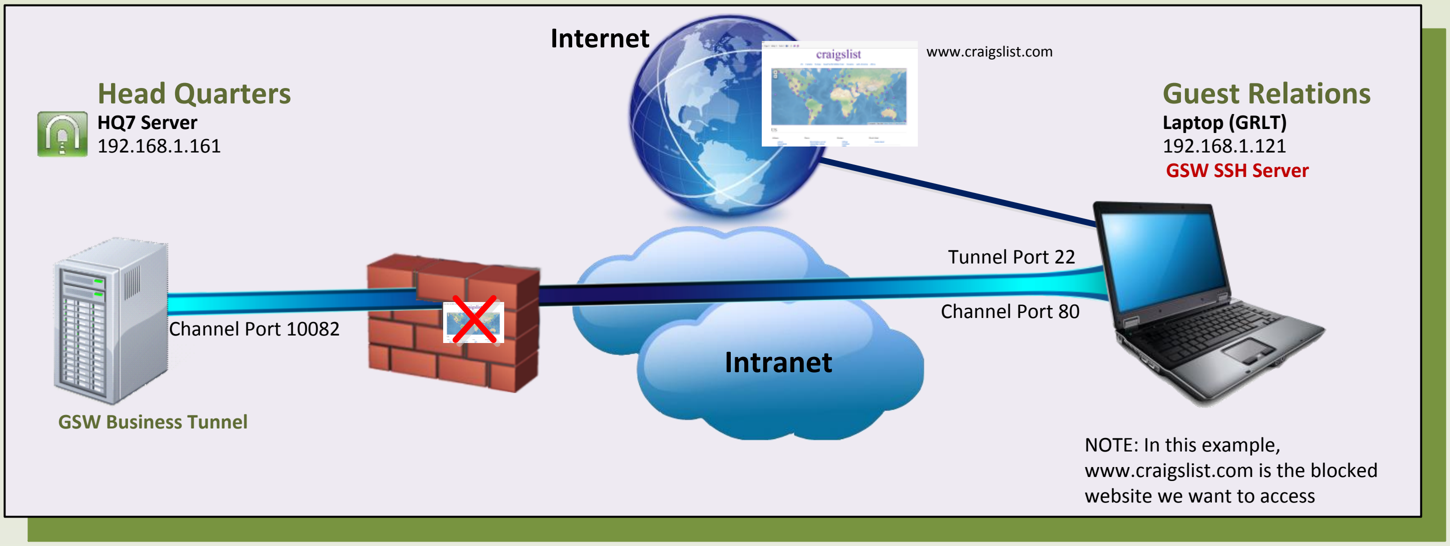
Lab Client Computer – Telnet Client Shortcut

Using the local address and port configured in the channel configuration, modify the Telnet Client Shortcut
@gs_clnt.exe -h127.0.0.1 -P10023 -udavid -phidden -d.

GSW
Business Tunnel

Example L02

Securely Access Blocked Website from Headquarters via Computer on Company Intranet



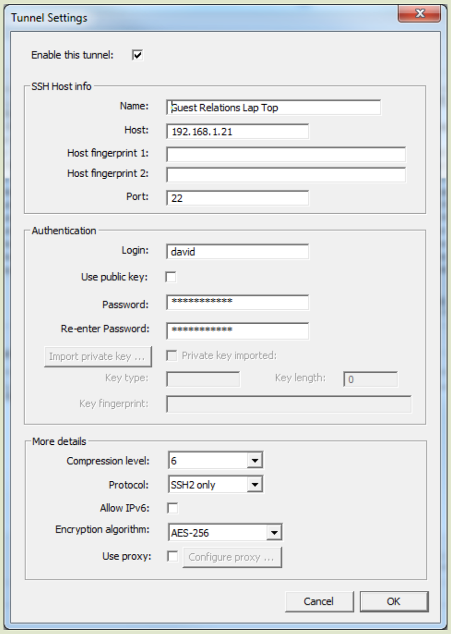
NOTE: In this example, www.craigslist.com is the blocked website we want to access

Case:

Access to www.craigslist.com is blocked by the company proxy filter in Headquarters. However, the company has some older office furniture for sale on craigslist. The facilities manager wants to view the ad. He knows that the training laptop on the company intranet in the guest relations building has access to the internet and is running the GSW SSH Server.

The HQ7 (running the GSW Business Tunnel) creates a tunnel to the Guest Relations Laptop (GRLT) which is running the GSW SSH Server and has access to www.craigslist.com

HQ7 – GSW Business Tunnel Configuration


Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: Guest Relations Lap Top
Host: 192.168.1.21
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: david
Use public key: □
Password: ************
Re-enter Password: ************
□ Private key imported:
Key type:
Key length: 0
Key fingerprint:

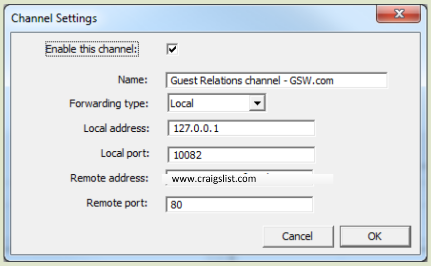
More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: □
Encryption algorithm: AES-256
Use proxy: □

SSH Host and Authentication Settings

1. Set Address of SSH Server Host.

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

HQ7 – Channel Configuration


Channel Settings

Enable this channel: ☑
Name: Guest Relations channel - GSW.com
Forwarding type: Local
Local address: 127.0.0.1
Local port: 10082
Remote address: www.craigslist.com
Remote port: 80

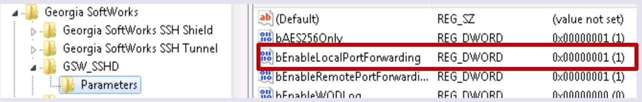
1. Select Local forwarding type.
2. Set the loopback address (127.0.0.1) as the local address.
3. Choose available port number to assign for local port. We selected 10082.
4. Fill in the host address of the blocked website as the remote address.
5. Use 80 for the Remote Port

GRLT – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters


```
Georgia SoftWorks
    Georgia SoftWorks SSH Shield
    Georgia SoftWorks SSH Tunnel
    GSW_SSHD
        Parameters
```

(Default)	REG_SZ	(value not set)
bAES256Only	REG_DWORD	0x00000001 (1)
bEnableLocalPortForwarding	REG_DWORD	0x00000001 (1)
bEnableRemotePortForwardi...	REG_DWORD	0x00000001 (1)
bEnableWODLog	REG_DWORD	0x00000000 (0)

HQ7 – Browser Configuration

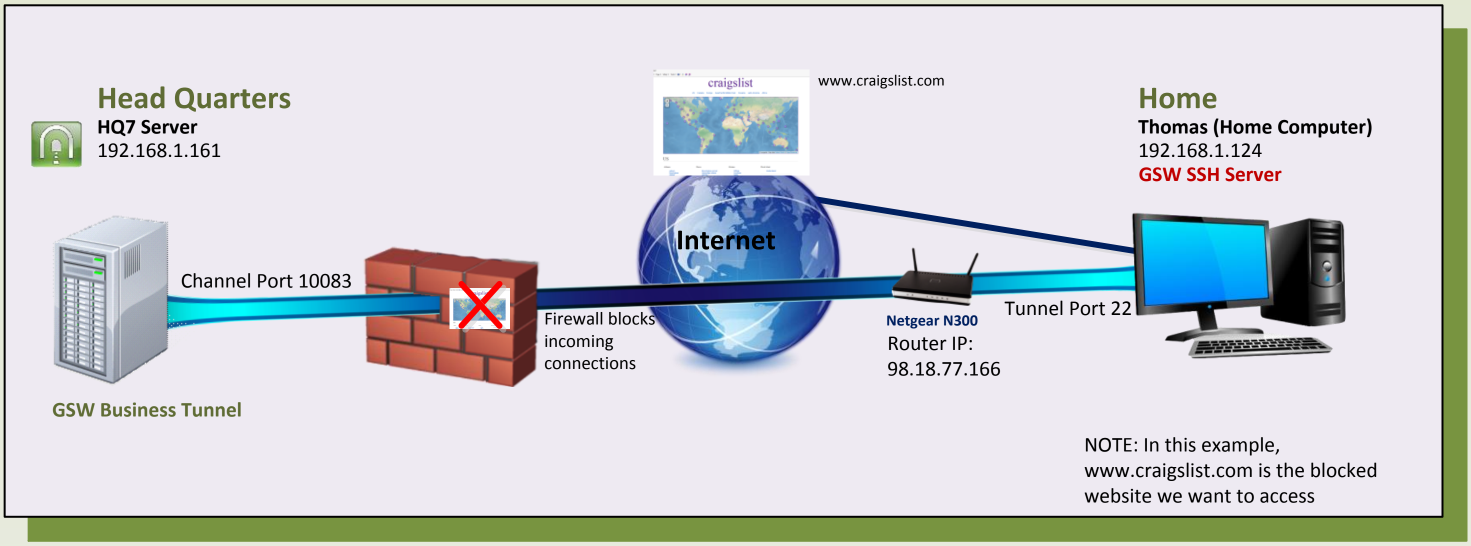
1. Open browser and enter URL http://127.0.0.1:10082
(from the channel configuration)
2. Browse www.craigslist.com

*Note: This example works as long as the links and objects on the website have relative addresses

GSW Business Tunnel

Example L03

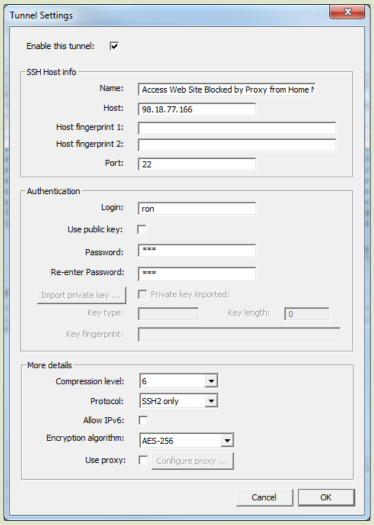
Securely Access Blocked Website via Home Computer due to Company Proxy Filter



NOTE: In this example, www.craigslist.com is the blocked website we want to access

CASE: *Access Blocked Web Site from home (due to company proxy filter)*
Access to www.craigslist.com is blocked by the company proxy filter at Head Quarters. However, the facilities manager needs to access craigslist to find old desks for sale in the area. His computer (Thomas) at home is running the GSW SSH Server.
The developer can create a Tunnel to his home computer and then browse www.craigslist.com from HQ7.

HQ7 – GSW Business Tunnel Configuration



Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: Access Web Site Blocked by Proxy from Home M
Host: 98.18.77.166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: ron
Use public key: ☐
Password: ***
Re-enter Password: ***
Import private key ... ☐ Private key imported:
Key type: Key length: 0
Key fingerprint:

More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: ☐
Encryption algorithm: AES-256
Use proxy: ☐ Configure proxy ...

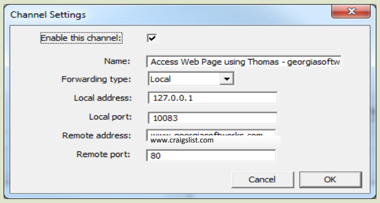
Cancel OK

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

HQ7 – Channel Configuration



Channel Settings

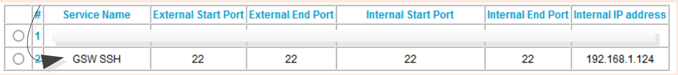
Enable this channel: ☑
Name: Access Web Page using Thomas - georgiasoftw
Forwarding type: Local
Local address: 127.0.0.1
Local port: 10083
Remote address: www.craigslist.com
Remote port: 80

Cancel OK

1. Select Local forwarding type.
2. Set the loopback address (127.0.0.1) as the local address.
3. Choose available port number to assign for local port. We selected 10083.
4. Fill in the host address of the blocked website as the remote address.
5. Use 80 for the remote port

NetGear N300 Router – Port Forwarding Configuration

Your router will need to be configured to port forward to the SSH Server



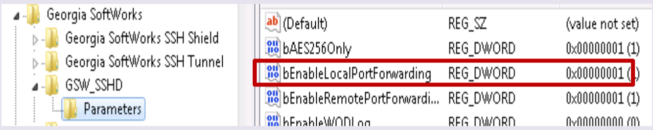
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○	2	GSW SSH	22	22	22	22	192.168.1.124

Thomas – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



(Default)	REG_SZ	(value not set)
bAES256Only	REG_DWORD	0x00000001 (1)
bEnableLocalPortForwarding	REG_DWORD	0x00000001 (1)
bEnableRemotePortForwardi...	REG_DWORD	0x00000001 (1)
bEnableWODLog	REG_DWORD	0x00000000 (0)

HQ7 – Browser Configuration

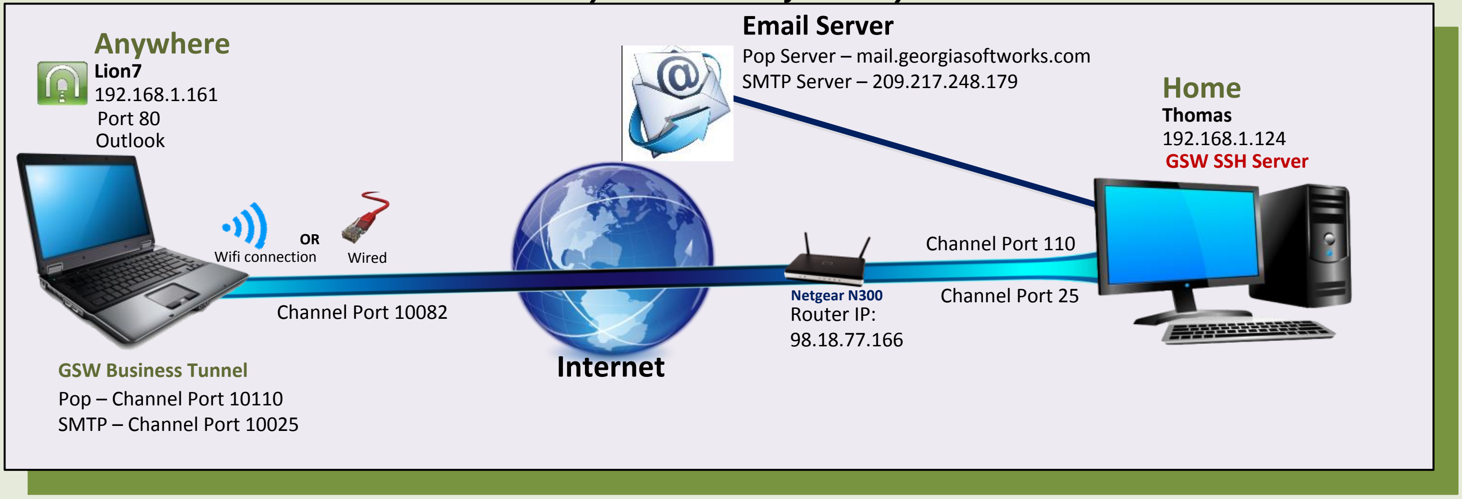
1. Open browser and enter URL
http://127.0.0.1:10083
(from the channel configuration)
and browse www.craigslist.com

*Note: This example works as long as the links and objects on the website have relative addresses

GSW Business Tunnel

Example L04

Securely Access Email from Anywhere



Anywhere
Lion7
192.168.1.161
Port 80
Outlook

Wifi connection OR Wired

Channel Port 10082

GSW Business Tunnel
Pop – Channel Port 10110
SMTP – Channel Port 10025

Internet

Email Server
Pop Server – mail.georgiasoftworks.com
SMTP Server – 209.217.248.179

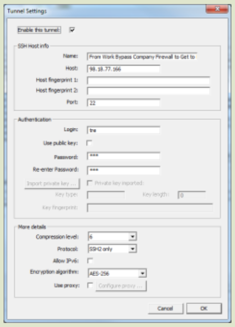
Netgear N300
Router IP:
98.18.77.166

Channel Port 110
Channel Port 25

Home
Thomas
192.168.1.124
GSW SSH Server

CASE: *Securely check/send email from anywhere that has internet access*
Create a secure GSW Business Tunnel to a secure SSH Server and check/send email. In this example you could be at a public Wi-Fi location, a hospital, airport, library, coffee shop or at a corporate business partners site. You can use your Business Tunnel to ensure a secure connection to a safe location to check/send email.
This example requires 2 channels to be used with one Tunnel.

Lion7 – GSW Business Tunnel Configuration



Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: From Work Bypass Company Firewall to Get to
Host: 98.18.77.166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: tre
Use public key: □
Password: ***
Re-enter Password: ***
Import private key ... □ Private key imported:
Key type: Key length: 0
Key fingerprint:

More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: □
Encryption algorithm: AES-256
Use proxy: □ Configure proxy ...

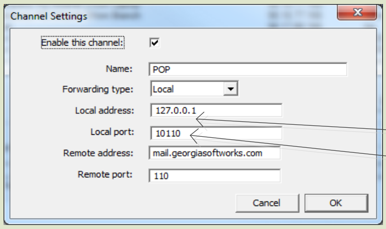
Cancel OK

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lion7 – POP Channel Configuration



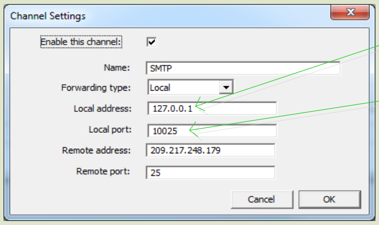
Channel Settings

Enable this channel: ☑
Name: POP
Forwarding type: Local
Local address: 127.0.0.1
Local port: 10110
Remote address: mail.georgiasoftworks.com
Remote port: 110

Cancel OK

1. Select forwarding type to local.
2. Set the loopback address (127.0.0.1) as the local address.
3. Choose available port number for local port. We chose 10110.
4. The Remote address is the address of the mail server.
5. The remote port 110.

Lion7 – SMTP Channel Configuration



Channel Settings

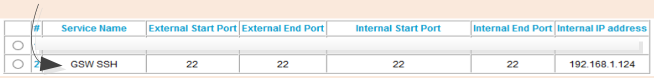
Enable this channel: ☑
Name: SMTP
Forwarding type: Local
Local address: 127.0.0.1
Local port: 10025
Remote address: 209.217.248.179
Remote port: 25

Cancel OK

1. Select forwarding type to local.
2. Use the loopback address as the local address.
3. choose available local port. We chose 10025.
4. Set the remote address of the mail server. We entered the IP address this time.
5. Set the remote port to 25.

NetGear N300 Router – Port Forwarding Configuration

Your router may need to be configured to port forward to the computer at your home, Thomas.



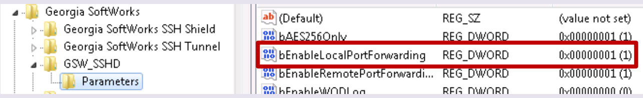
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○							
○	2	GSW SSH	22	22	22	22	192.168.1.124

Thomas – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

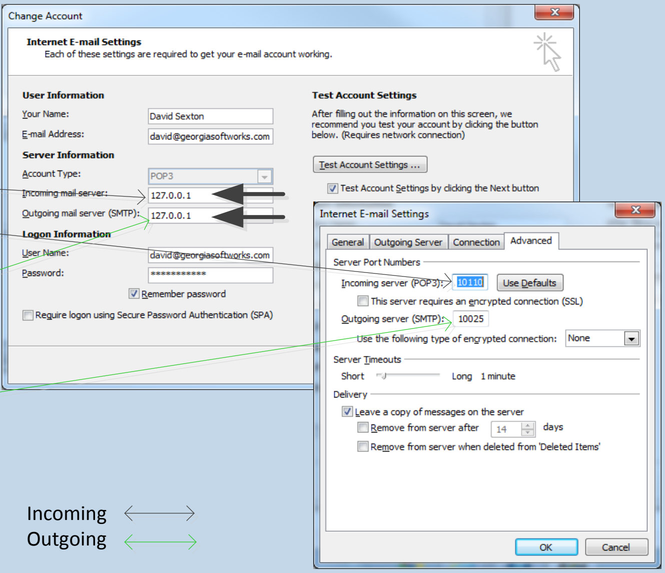
x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



Georgia SoftWorks
Georgia SoftWorks SSH Shield
Georgia SoftWorks SSH Tunnel
GSW_SSHD
Parameters

(Default)	REG_SZ	(value not set)
bAES256Only	REG_DWORD	0x00000001 (1)
bEnableLocalPortForwarding	REG_DWORD	0x00000001 (1)
bEnableRemotePortForwardi...	REG_DWORD	0x00000001 (1)
bEnableWODLog	REG_DWORD	0x00000000 (0)

Microsoft Outlook Example (on Lion7):



Change Account

Internet E-mail Settings
Each of these settings are required to get your e-mail account working.

User Information
Your Name: David Sexton
E-mail Address: david@georgiasoftworks.com

Server Information
Account Type: POP3
Incoming mail server: 127.0.0.1
Outgoing mail server (SMTP): 127.0.0.1

Logon Information
User Name: david@georgiasoftworks.com
Password: ************
☑ Remember password
□ Require logon using Secure Password Authentication (SPA)

Test Account Settings
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)
Test Account Settings ...
☑ Test Account Settings by clicking the Next button

Internet E-mail Settings

General | Outgoing Server | Connection | Advanced

Server Port Numbers
Incoming server (POP3): 10110 Use Defaults
□ This server requires an encrypted connection (SSL)
Outgoing server (SMTP): 10025
Use the following type of encrypted connection: None

Server Timeouts
Short Long 1 minute

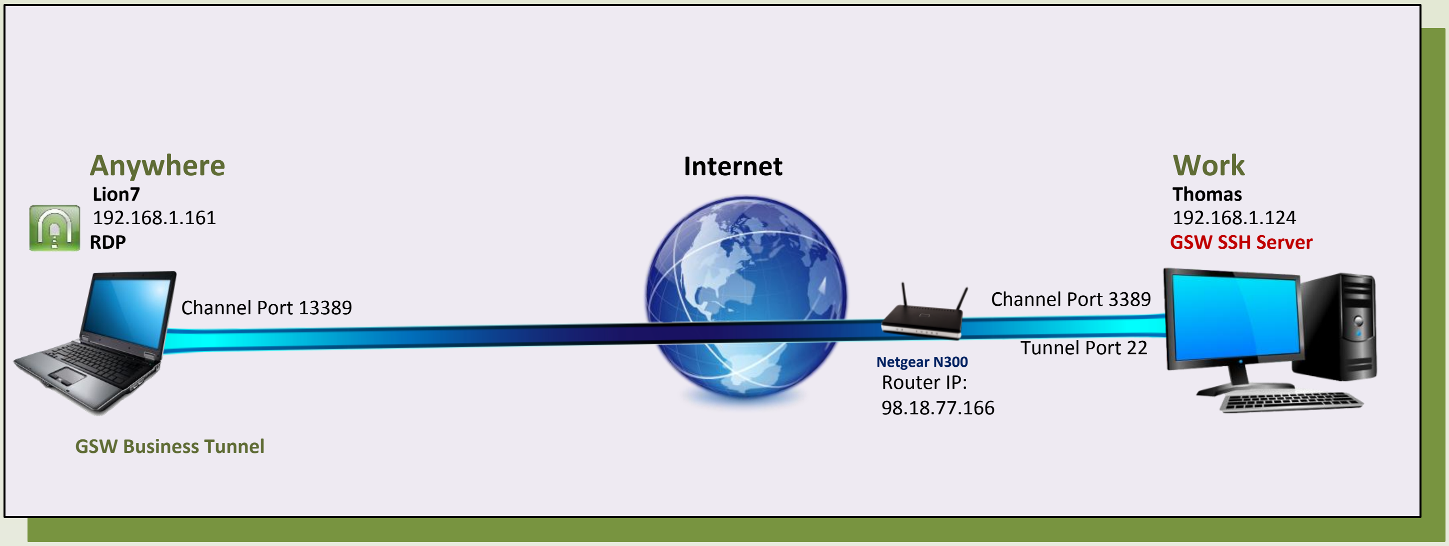
Delivery
☑ Leave a copy of messages on the server
□ Remove from server after 14 days
□ Remove from server when deleted from 'Deleted Items'

OK Cancel

Incoming ⟷
Outgoing ⟷

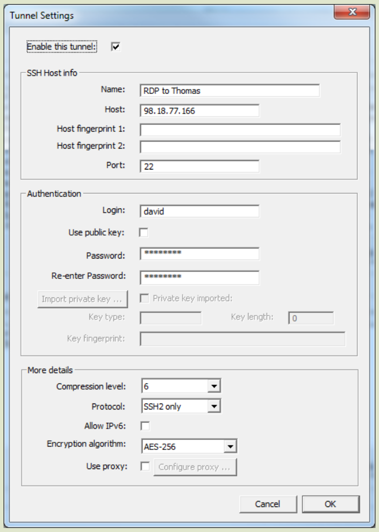
Example L05

Securely Remote Desktop to Work from Anywhere



CASE: *Securely Remote Desktop to Work From Anywhere*
You are a traveling and want to Remote Desktop to your work computer. You can do this from anywhere using the GSW Business Tunnel.

Lion7 – GSW Business Tunnel Configuration


Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: RDP to Thomas
Host: 98.18.77.166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: david
Use public key: □
Password: *********
Re-enter Password: *********
Import private key ... □ Private key imported:
Key type: Key length: 0
Key fingerprint:

More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: □
Encryption algorithm: AES-256
Use proxy: □ Configure proxy ...

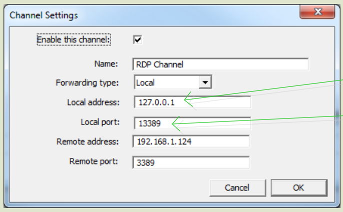
Cancel OK

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lion7 – RDP Channel Configuration


Channel Settings

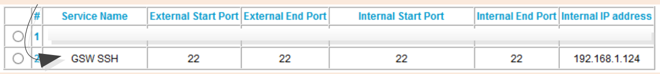
Enable this channel: ☑
Name: RDP Channel
Forwarding type: Local
Local address: 127.0.0.1
Local port: 13389
Remote address: 192.168.1.124
Remote port: 3389

Cancel OK

1. Select Local forwarding type.
2. Set the loopback address (127.0.0.1) as the local address.
3. Choose available port number to assign for local port. We selected 13389.
4. Fill in the remote address
5. The remote port is the RDP Port number (3389)

NetGear N300 Router – Port Forwarding Configuration

Your router will need to be configured to port forward to the SSH Server



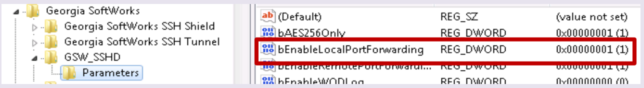
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○	2	GSW SSH	22	22	22	22	192.168.1.124

Thomas – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

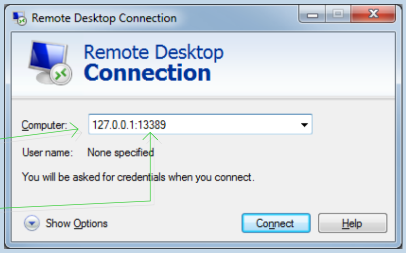
x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



```
Georgia SoftWorks
    Georgia SoftWorks SSH Shield
    Georgia SoftWorks SSH Tunnel
    GSW_SSHD
        Parameters
```

```
(Default)                     REG_SZ      (value not set)
bAES256Only                   REG_DWORD   0x00000001 (1)
bEnableLocalPortForwarding    REG_DWORD   0x00000001 (1)
bEnableRemotePortForwardi...  REG_DWORD   0x00000001 (1)
bEnableWODLog                 REG_DWORD   0x00000000 (0)
```

Lion7 – Remote Desktop Configuration


Remote Desktop Connection

Remote Desktop Connection

Computer: 127.0.0.1:13389
User name: None specified
You will be asked for credentials when you connect.

Show Options Connect Help

From Lion7, Open Remote Desktop (run mstsc from Start Orb)

Enter the address as shown using the loopback address and the local port number from the channel configuration

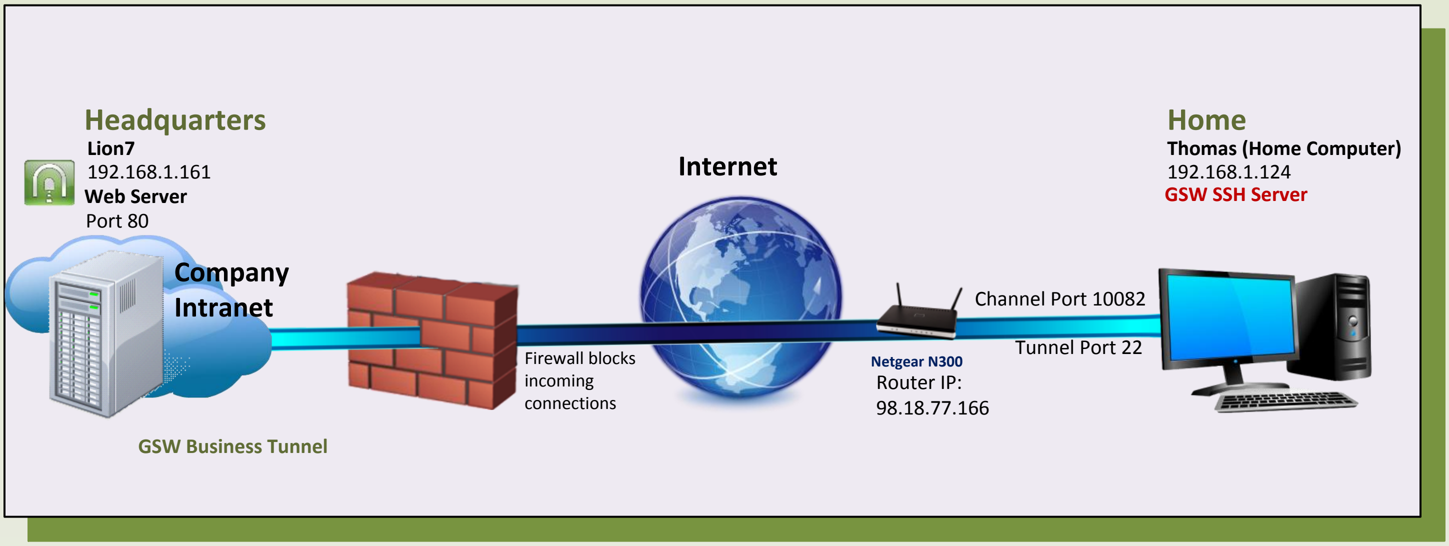
Click Connect – enter your credentials to log on

Note By using the GSW Business Tunnel, you can securely RDP without having to create certificates

GSW Business Tunnel

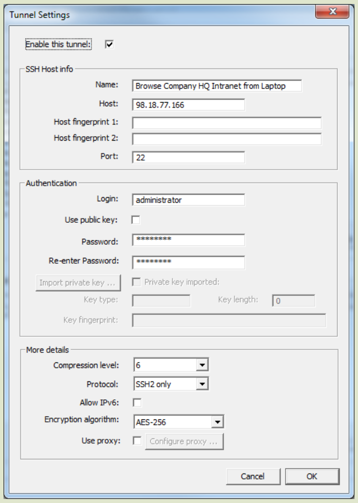
Example R01

Securely Browse the Company Intranet From Home, Even Though Company Does Not Allow Incoming Connections



CASE: *Browse Company Intranet from Home*
Your company does not allow incoming connections. You can set up the GSW Business Tunnel from work so that you can browse the company intranet from home. The Web Server is on the same computer as the Business Tunnel.

Lion7 – GSW Business Tunnel Configuration


Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: Browse Company HQ Intranet from Laptop
Host: 98.18.77.166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: administrator
Use public key: □
Password: *********
Re-enter Password: *********
Import private key ... □ Private key imported:
Key type: Key length: 0
Key fingerprint:

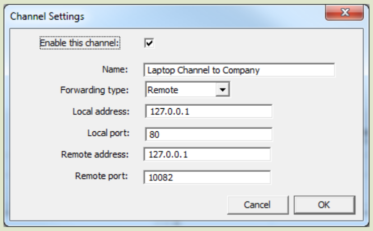
More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: □
Encryption algorithm: AES-256
Use proxy: □ Configure proxy ...

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lion7 – Channel Configuration


Channel Settings

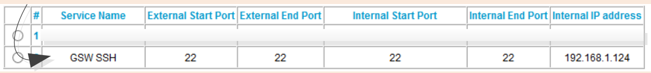
Enable this channel: ☑

Name: Laptop Channel to Company
Forwarding type: Remote
Local address: 127.0.0.1
Local port: 80
Remote address: 127.0.0.1
Remote port: 10082

1. Select Remote forwarding type.
2. Set the loopback address (127.0.0.1) as the local address since the web server is on the same computer as the Business Tunnel.
3. Choose port number 80 for the local port.
4. Fill in the remote address as the loopback address (127.0.0.1)
5. Choose available port number to assign for remote port. We selected 10082.

NetGear N300 Router – Port Forwarding Configuration

Your router may need to be configured to port forward to the home computer, Thomas.



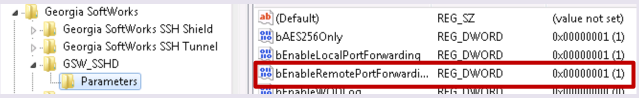
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○	[illegible]	GSW SSH	22	22	22	22	192.168.1.124

Thomas – GSW SSH Server Configuration

Make sure remote port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



```
Georgia SoftWorks
    Georgia SoftWorks SSH Shield
    Georgia SoftWorks SSH Tunnel
    GSW_SSHD
        Parameters
```

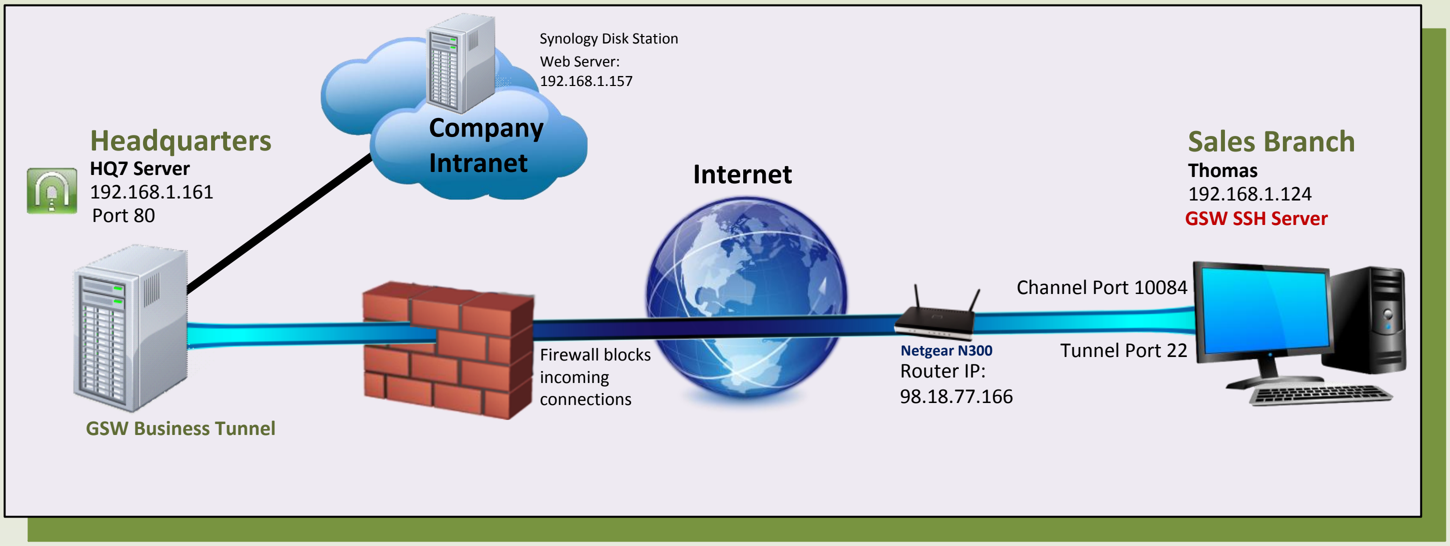
```
(Default)                       REG_SZ        (value not set)
bAES256Only                     REG_DWORD     0x00000001 (1)
bEnableLocalPortForwarding      REG_DWORD     0x00000001 (1)
bEnableRemotePortForwardi...    REG_DWORD     0x00000001 (1)
```

Thomas – Browser Configuration

Open browser and enter URL: http://127.0.0.1:10082
(from the channel configuration)and browse the company intranet

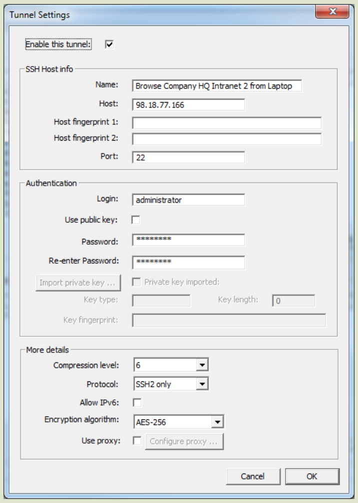
Example R02

Browse the Company Intranet from Sales Branch – Single User



CASE: *Browse Company Intranet from Sales Branch*
Your company Headquarters (HQ) does not allow incoming connections. You can set up a tunnel from HQ so an employee can browse the company intranet from a new sales branch on the server (Thomas). The GSW Business Tunnel is on HQ7, a different computer than the web server(Synology Disk Station).

HQ7 – GSW Business Tunnel Configuration



Tunnel Settings

Enable this tunnel: ☑

SSH Host info
- Name: Browse Company HQ Intranet 2 from Laptop
- Host: 98.18.77.166
- Host fingerprint 1:
- Host fingerprint 2:
- Port: 22

Authentication
- Login: administrator
- Use public key: ☐
- Password: ********
- Re-enter Password: ********
- Import private key ... ☐ Private key imported:
- Key type: Key length: 0
- Key fingerprint:

More details
- Compression level: 6
- Protocol: SSH2 only
- Allow IPv6: ☐
- Encryption algorithm: AES-256
- Use proxy: ☐ Configure proxy ...

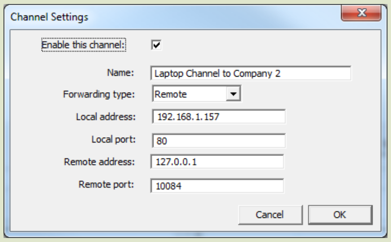
Cancel OK

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

HQ7 – Channel Configuration



Channel Settings

Enable this channel: ☑

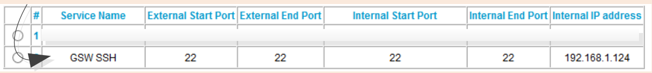
- Name: Laptop Channel to Company 2
- Forwarding type: Remote
- Local address: 192.168.1.157
- Local port: 80
- Remote address: 127.0.0.1
- Remote port: 10084

Cancel OK

1. Select Remote forwarding type.
2. Set the address of the web server (192.168.1.157) as the local address.
3. Choose port number to assign for local port. We selected 80.
4. Fill in the remote address with the loopback address and available port number. We chose 10084.

NetGear N300 Router – Port Forwarding Configuration

Your router may need to be configured to port forward to the computer at the sales branch, Thomas.



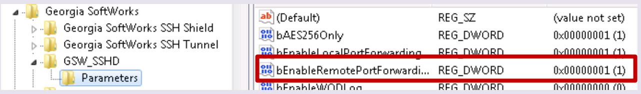
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○		GSW SSH	22	22	22	22	192.168.1.124

Thomas – GSW SSH Server Configuration

Make sure remote port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



Georgia SoftWorks
- Georgia SoftWorks SSH Shield
- Georgia SoftWorks SSH Tunnel
- GSW_SSHD
  - Parameters

(Default)	REG_SZ	(value not set)
bAES256Only	REG_DWORD	0x00000001 (1)
bEnableLocalPortForwarding	REG_DWORD	0x00000001 (1)
bEnableRemotePortForwardi...	REG_DWORD	0x00000001 (1)
bEnableWODLog	REG_DWORD	0x00000000 (0)

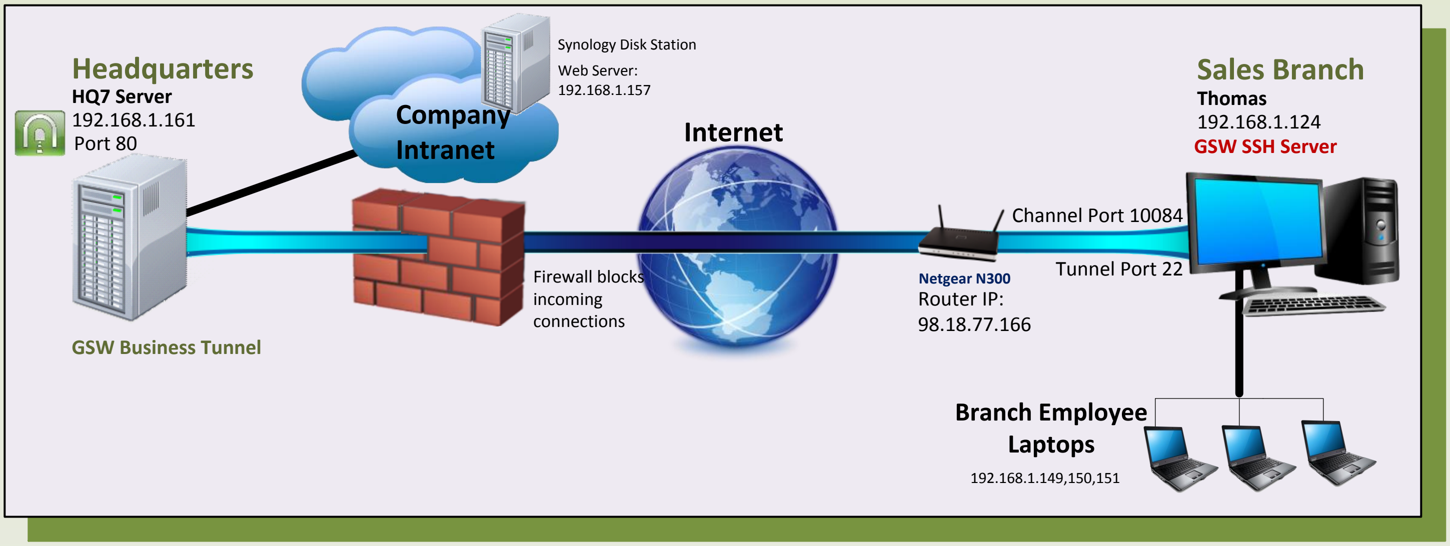
Thomas – Browser Configuration

1. Open browser and enter URL http://127.0.0.1:10084/
(from the channel configuration) and browse the company intranet

GSW Business Tunnel

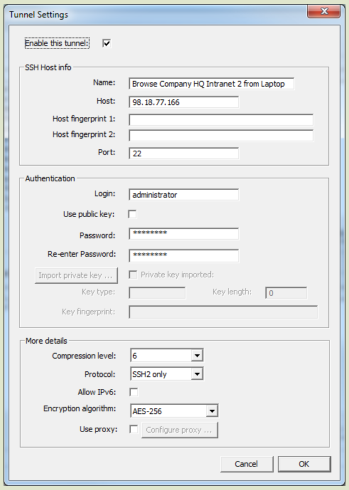
Example R03

Browse the Company Intranet from Sales Branch – Multiple Users



CASE: *Browse Company Intranet from Sales Branch 2*
Your company Headquarters does not allow incoming connections. You can set up a tunnel from work (HQ7) so multiple employees can browse the company intranet from a new sales branch. The GSW Business Tunnel is on HQ7, a different computer than the web server(Synology Disk Station).

HQ7 – GSW Business Tunnel Configuration


Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: Browse Company HQ Intranet 2 from Laptop
Host: 98.18.77.166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: administrator
Use public key: □
Password: *********
Re-enter Password: *********
Import private key ... □ Private key imported:
Key type: Key length: 0
Key fingerprint:

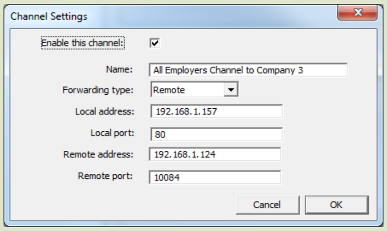
More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: □
Encryption algorithm: AES-256
Use proxy: □ Configure proxy ...

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

HQ7 – Channel Configuration


Channel Settings

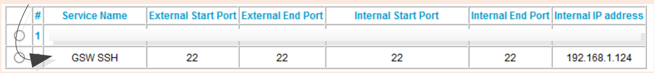
Enable this channel: ☑

Name: All Employers Channel to Company 3
Forwarding type: Remote
Local address: 192.168.1.157
Local port: 80
Remote address: 192.168.1.124
Remote port: 10084

1. Select Remote forwarding type.
2. Set the address of the web server (192.168.1.157) as the local address.
3. Choose port number 80 for the local port.
4. Fill in the remote address with 192.168.1.124, the address of the SSH Server.
5. Choose available port number for the remote port. We chose 10084.

NetGear N300 Router – Port Forwarding Configuration

Your router may need to be configured to port forward to the computer at the sales branch, Thomas.



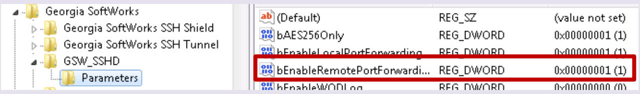
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○	2	GSW SSH	22	22	22	22	192.168.1.124

Thomas – GSW SSH Server Configuration

Make sure remote port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters


Georgia SoftWorks
Georgia SoftWorks SSH Shield
Georgia SoftWorks SSH Tunnel
GSW_SSHD
Parameters

(Default)	REG_SZ	(value not set)
bAES256Only	REG_DWORD	0x00000001 (1)
bEnableLocalPortForwarding	REG_DWORD	0x00000001 (1)
bEnableRemotePortForwardi...	REG_DWORD	0x00000001 (1)
bEnableWODLog	REG_DWORD	0x00000000 (0)

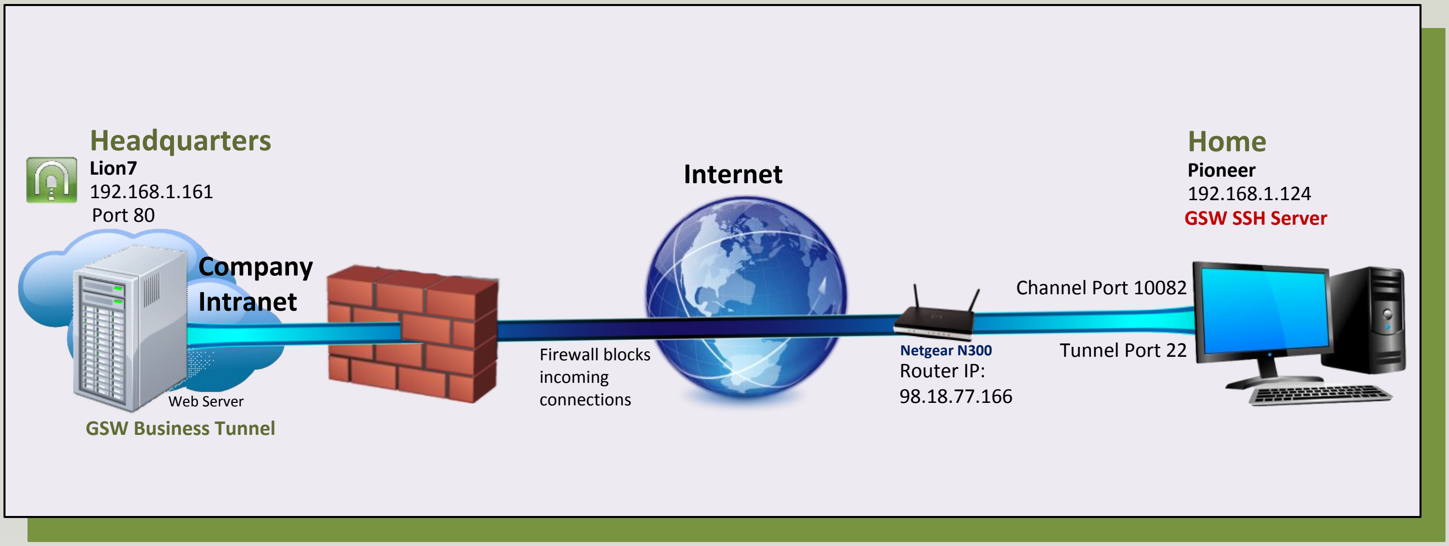
Thomas – GSW SSH Server Configuration

From Thomas or other computers on the sales branch network, open browser and enter the URL
http://192.168.1.124:10084/
(from the channel configuration)

GSW Business Tunnel

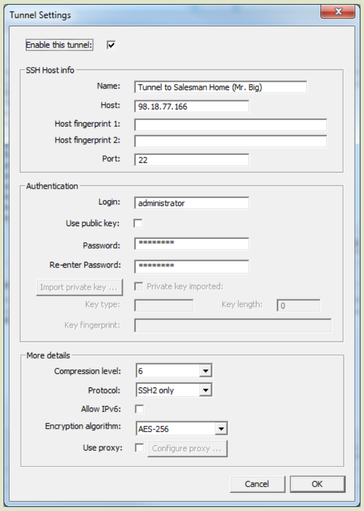
Example R04

Browse the Company Intranet from Home



CASE: *Browse Company Intranet from Home*
Your company Headquarters does not allow incoming connections. You can set up a tunnel from work (HQ) so you can browse the company intranet from home. The GSW SSH Server and Web Server are on the same computer.

Lion7 – GSW Business Tunnel Configuration



Tunnel Settings

Enable this tunnel: ☑

SSH Host info
Name: Tunnel to Salesman Home (Mr. Big)
Host: 98.18.77.166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: administrator
Use public key: ☐
Password: ********
Re-enter Password: ********
Import private key ... ☐ Private key imported:
Key type: Key length: 0
Key fingerprint:

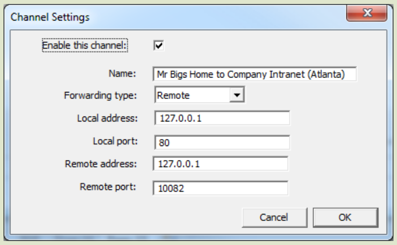
More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: ☐
Encryption algorithm: AES-256
Use proxy: ☐ Configure proxy ...

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lion7 – Channel Configuration



Channel Settings

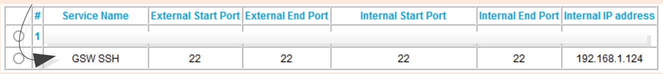
Enable this channel: ☑

Name: Mr Bigs Home to Company Intranet (Atlanta)
Forwarding type: Remote
Local address: 127.0.0.1
Local port: 80
Remote address: 127.0.0.1
Remote port: 10082

1. Select Remote forwarding type.
2. Set the loopback address (127.0.0.1) as the local address.
3. Choose 80 for the local port.
4. Set loopback address as the remote address.
5. Choose available port for the remote port (10082).

NetGear N300 Router – Port Forwarding Configuration

Your router will need to be configured to port forward to the SSH Server



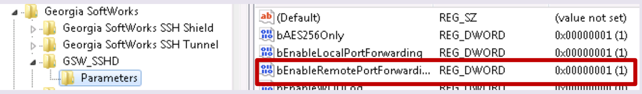
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○		GSW SSH	22	22	22	22	192.168.1.124

Lion7 – GSW SSH Server Configuration

Make sure remote port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters

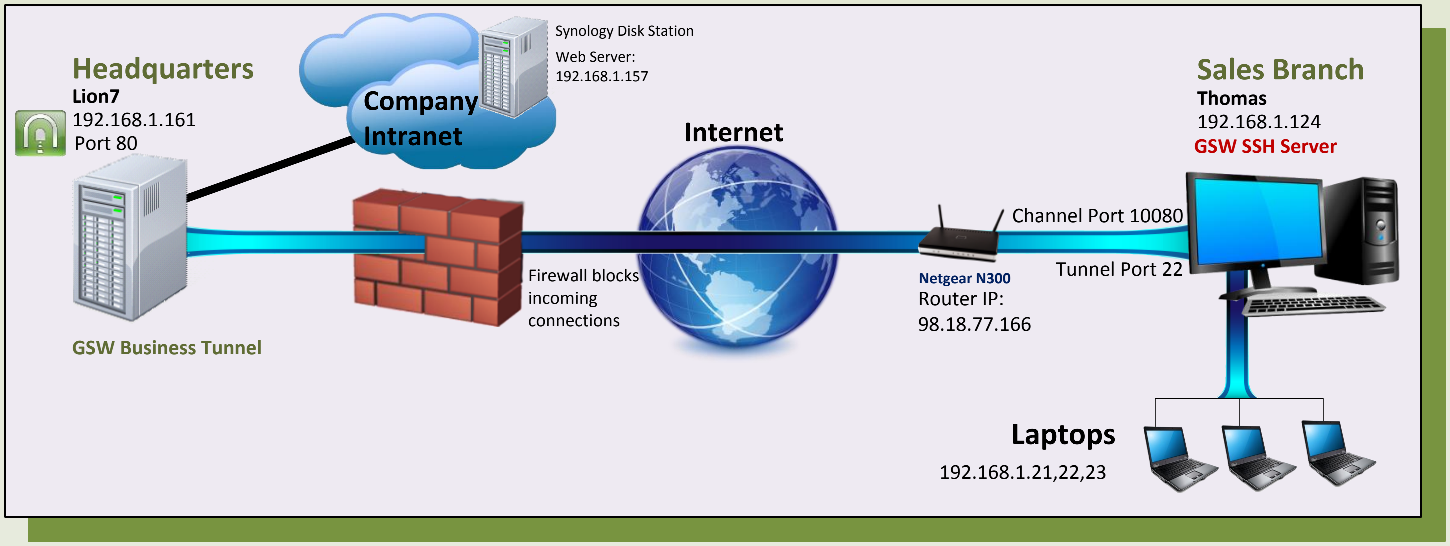


```
(Default)                        REG_SZ       (value not set)
bAES256Only                      REG_DWORD    0x00000001 (1)
bEnableLocalPortForwarding       REG_DWORD    0x00000001 (1)
bEnableRemotePortForwardi...     REG_DWORD    0x00000001 (1)
```

Pioneer – Browser Configuration

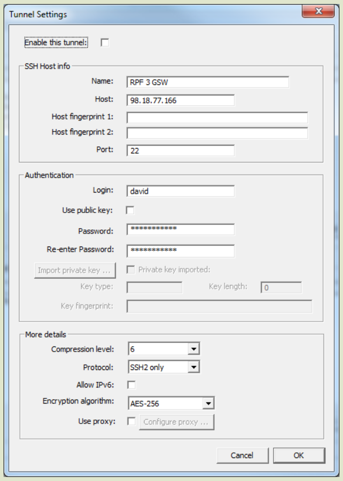
1. Open browser and enter URL http://127.0.0.1:10082/ and browse the company intranet

Browse the Company Intranet from Sales *Branch using address 0.0.0.0*



CASE: *Browse Company Intranet from Sales Branch*
Your company Headquarters does not allow incoming connections. You can set up a tunnel from work Headquarters so multiple employees can browse the company intranet from a new sales branch. The GSW Business Tunnel is on a different computer than the web server.

Lion7 – GSW Business Tunnel Configuration


Tunnel Settings

Enable this tunnel: □

SSH Host info
Name: RPF 3 GSW
Host: 98. 18. 77. 166
Host fingerprint 1:
Host fingerprint 2:
Port: 22

Authentication
Login: david
Use public key: □
Password: ************
Re-enter Password: ************
Import private key ... □ Private key imported:
Key type: Key length: 0
Key fingerprint:

More details
Compression level: 6
Protocol: SSH2 only
Allow IPv6: □
Encryption algorithm: AES-256
Use proxy: □ Configure proxy ...

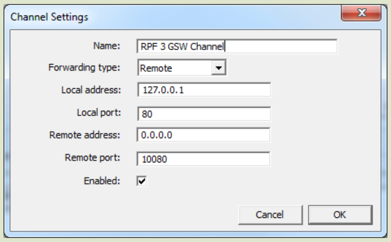
Cancel OK

SSH Host and Authentication Settings

1. Set Address of SSH Server Host. In this case, the router is forwarded to the SSH Server Host, so we use the router IP Address

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lion7 – Channel Configuration


Channel Settings

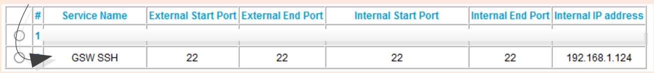
Name: RPF 3 GSW Channel
Forwarding type: Remote
Local address: 127.0.0.1
Local port: 80
Remote address: 0.0.0.0
Remote port: 10080
Enabled: ☑

Cancel OK

1. Select Remote forwarding type.
2. Set the loopback address (127.0.0.1) as the local address.
3. Enter port 80 for the local port number.
4. Fill in the remote address with 0.0.0.0 which allows all computers on the network at the branch office to tunnel to Headquarters.
5. Choose available port for the remote port (10080)

NetGear N300 Router – Port Forwarding Configuration

Your router may need to be configured to port forward to the computer at the sales branch, Thomas.



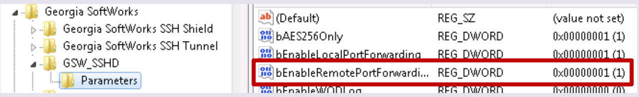
	#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
○	1						
○		GSW SSH	22	22	22	22	192.168.1.124

Thomas – GSW SSH Server Configuration

Make sure remote port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters


Georgia SoftWorks
Georgia SoftWorks SSH Shield
Georgia SoftWorks SSH Tunnel
GSW_SSHD
Parameters

```
(Default)                       REG_SZ       (value not set)
bAES256Only                     REG_DWORD    0x00000001 (1)
bEnableLocalPortForwarding      REG_DWORD    0x00000001 (1)
bEnableRemotePortForwardi...    REG_DWORD    0x00000001 (1)
bEnableWODLog                   REG_DWORD    0x00000000 (0)
```

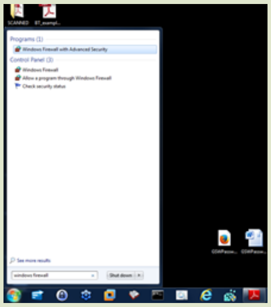
Thomas – GSW SSH Server Configuration

From the Sales Branch Laptops, or any other computer on the network, open browser and enter the URL http://192.168.1.124:10080/

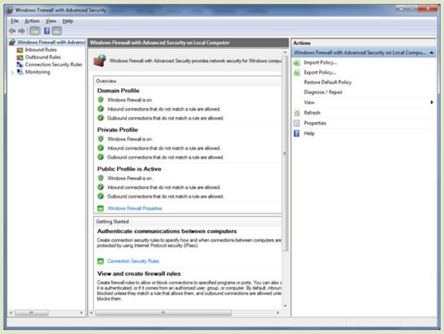
How to Configure Windows Firewall to Allow Access to an SSH Server

CASE: *Open a Closed Port*
Your home computer is running an SSH Server on port 22. You find port 22 closed to incoming connections. You need to open port 22 to allow GSW_SSHD.exe (GSW Business Tunnel) through the firewall. Configure the Windows Firewall to allow this executable to connect the tunnel to your home computer.

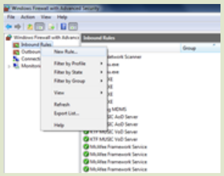
1. From the Start Orb, type *Windows Firewall* <enter>



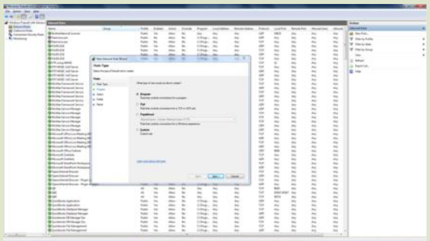
2. Select Windows Firewall with Advanced Security Options



3. Click on Inbound Rules and then Right-Click

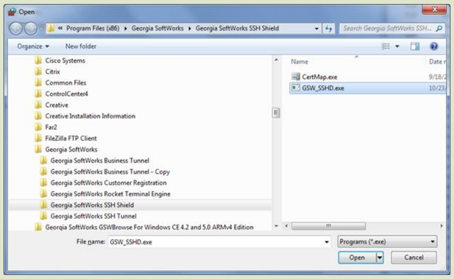


4. Select *New Rule* and New Inbound Rule Wizard opens.
Select *Program* and click *Next*.



5. Select *This program path*: and click *Browse*

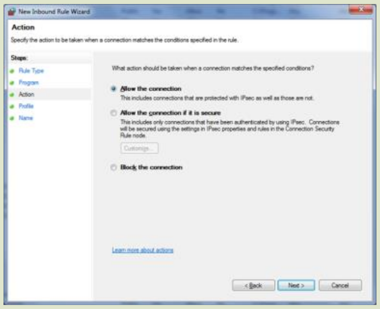
6. Navigate to the *GSW_SSHD.exe* file. (Example: "C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SSH Shield\GSW_SSHD.exe")
Select filename *GSW_SSHD.exe* and click *Open*.



File name: GSW_SSHD.exe

7. Click *NEXT*

8. Select *Allow the connection* and click *Next*



Action
Specify the action to be taken when a connection matches the conditions specified in the rule.

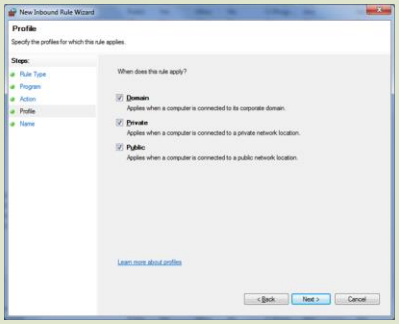
What action should be taken when a connection matches the specified conditions?

● Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

9. Leave the default settings and click *Next*



Profile
Specify the profiles for which this rule applies.

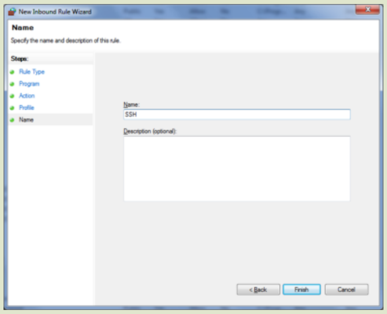
When does this rule apply?

☑ Domain
Applies when a computer is connected to its corporate domain.

☑ Private
Applies when a computer is connected to a private network location.

☑ Public
Applies when a computer is connected to a public network location.

10. In the *Name* field, type *SSH* and click *Finish*



Name
Specify the name and description of this rule.

Name: SSH

Description (optional):