Port Forwarding & Case Study

Introduction

This is to test the port forwarding on most of the routers supplied by TalkTalk. The case study looks at the wider picture, not just setting up port forwarding (in this case on a Huawei HG523A router), but also testing with applications, configuring of PC firewalls etc.

Note: most routers do not allow 'Loop Back' access so you will need to access the device only from an external network when using the external internet address. You will not be able to access the external IP address from the internal IP address, when the external address is port forwarded to another local device. Most routers prevent 'Loop Back' as an additional security measure. The same goes for using a DDNS address to access the router from the internal network.

If you have a Smartphone temporarily disable the WiFi and turn on Mobile Data, which will enable you to test access to the device via your mobile phone network.

Basic order of work required

1. Add the port forwarding rule(s) to the router
2. Reboot the router
3. Add the required inbound rule(s) to the firewall
4. Launch the application
5. Test it locally from another device connected to your router's network (i.e. a device with a 192.168.1.x address)
6. Test it with http://portchecker.co/check you will have to run it once for each port you are trying to use. and only go to step 7, if it reports ALL of the ports you have forwarded as OPEN.
7. Test using other people on the internet

Sections in this document

Case Study
- Test Setup
- FTP Server Settings
- FTP – active & passive modes

Other sections in the document:-
- Port forwarding on Huawei routers (not HG635)
- Windows 7 firewall settings
- Test Locally
- Test from Internet
- DDNS
- Port Forwarding to a port that is intercepted by the router
- Apple MACs running Windows applications
- Port Fowarding on other routers (all D-Link, HG633 & HG635)
- Universal Plug and Play (UPnP)

Port Forwarding & Case Study

Case Study

This case study looks not only at port forwarding, but applications on the local PC that require the port forwarding, plus adding rules to the firewall that runs locally on that PC. It also deals with how to test this (crucially from the internet, as well as locally on your router's network).

Test setup

FTP server running on Windows 7 Home Premium (SP1) : FileZilla Server V0.9.45
FTP client running on Android V2.3.6 : FTPCafe FTP client

Port Forwarding & Case Study

FTP Server Settings

FileZilla Server Options

General settings
    Welcome message
    IP bindings
    IP Filter
Passive mode settings
Security settings
Miscellaneous
Admin Interface settings
Logging
Speed Limits
Filetransfer compression
SSL/TLS settings

IP bindings

Bind the server to the following IP addresses:

192.168.1.3

Use * to bind to all addresses.
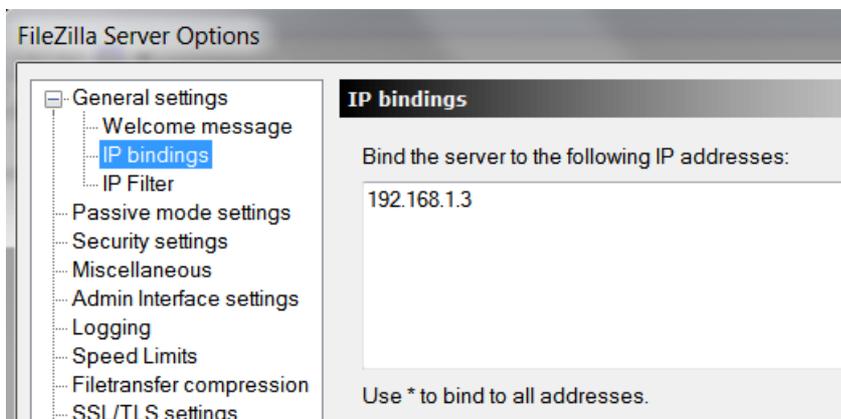
Set up a User account &password plus a home directory.

Active or Passive FTP mode

The control of the FTP transfer is always done using TCP port 21, the port used to carry the data transfer varies on the FTP mode used. There are two modes used to transfer the data from the server to the client, active or passive mode.

Active mode always uses TCP port 20 and the data transfer session is initiated by the server to the client. The client requests active mode by sending the PORT command to the server. It will tell the server to start a session to the IP address & TCP port, that it gives the server. This will therefore be initiated from the PC and will automatically be allowed through its firewall. It will still need some port forwarding for the traffic from the client to the server, but as it is a static port, this is not a problem.

If the client on the other hand sends a PASV command to request passive mode, the server if it accepts this, will instruct the client to establish a new session to the required IP address & TCP port number. This port number is dynamically assigned & will be greater than 1024. This mode is regarded as more secure than active mode, but unless the router's port forwarding responded in a dynamic fashion, it will fail at this point.

From my tests the HG523a will allow passive FTP mode transfers to pass through it correctly, even though the FTP-DATA session is initiated from the client over the internet.

Port Forwarding & Case Study

Router login

To do this work, you will need to log in to your router. To do this browse to your router at:-

http://192.168.1.1
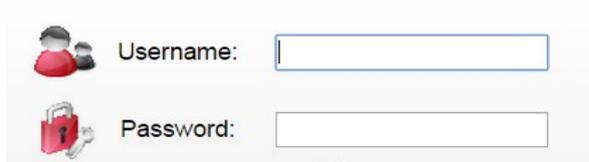
At the prompt:-

Username:

Password:

Enter your admin username & password. Unless you have changed this, the default is normally:-

Username : admin
password : admin

Port Forwarding & Case Study

Port Forwarding on Huawei routers (& some DSL-3780s)

Log in to the router & go into advanced mode. From there go to:-

Advanced > NAT > Port Mapping

Either select an existing "Application", or use the "Customization" option. In this case the FTP Server application can be used, but the IP address (maybe 192.168.1.2) for the device hosting the FTP server will need to be added in the "Internal host" field:-

If both external start & end ports are left at 21 this will work in passive mode OK.

Port Forwarding & Case Study

Note when adding this forwarding rule you will see this box:-

The page at 192.168.1.1 says:

Notice:This portmapping will modify the ftp server port number 21. If you want to access the ftp server of the router from WAN, make sure using the temporary port number 2121; the ftp server port will be reset to 21 after remove this policy. Are you sure to add this policy?

OK   Cancel
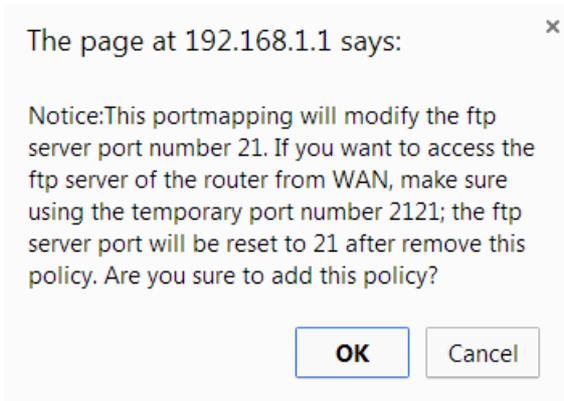
Click OK to that.

Click "Submit" & reboot the router.

For all other routers, please see this section.

Port Forwarding & Case Study

Windows 7 Firewall settings

Go to:-

Programs (1)

Windows Firewall with Advanced Security

Create a new inbound rule:-

Rule Type

Select the type of firewall rule to create.
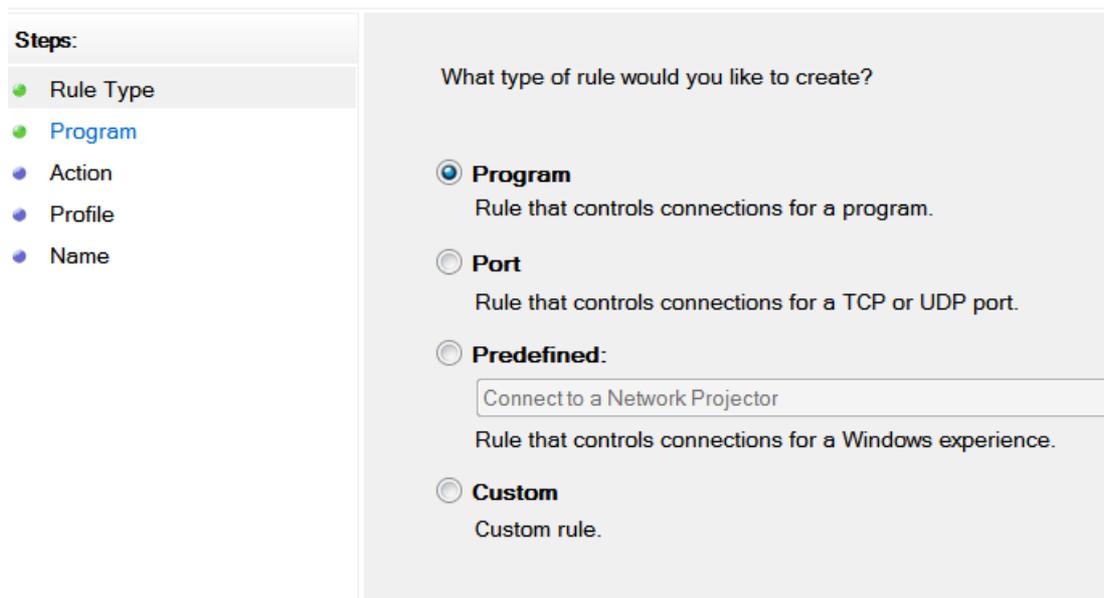
Steps:
- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

◉ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Connect to a Network Projector
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Click "Next" in the above screen, then on this next screen browse to the program's executable file. In the case of the FileZilla Server, allow the server application (not the interface to the server):-

Program

Specify the full program path and executable name of the program that this rule matches.
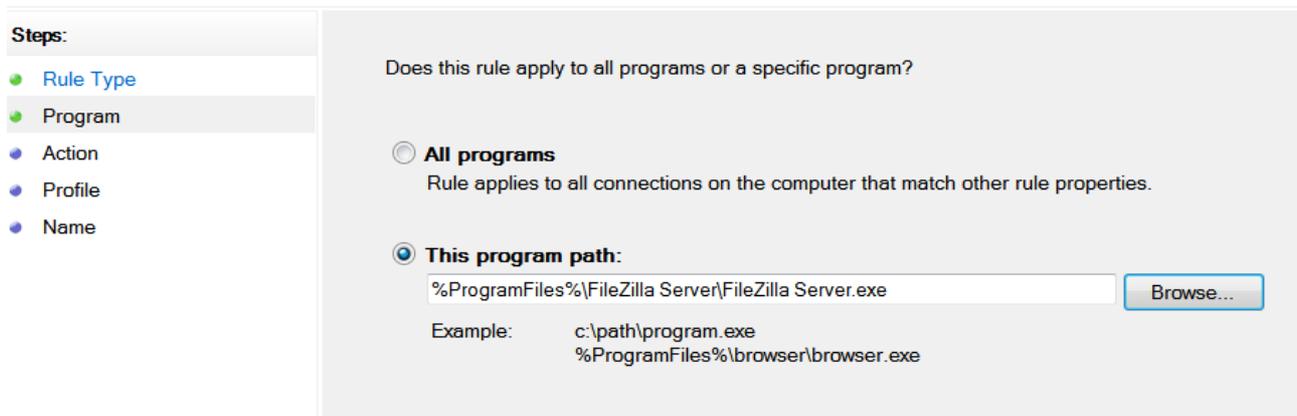
Steps:
- Rule Type
- Program
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

◉ **This program path:**
%ProgramFiles%\FileZilla Server\FileZilla Server.exe   Browse...

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Port Forwarding & Case Study

Click Next, then on this screen tick "Allow connection":-

Action

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

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

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.

    Customize...

○ **Block the connection**

Then click next and on the next screen set as appropriate:-

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

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.

Port Forwarding & Case Study

Click "Next" again, give it a unique name & click "Complete":-
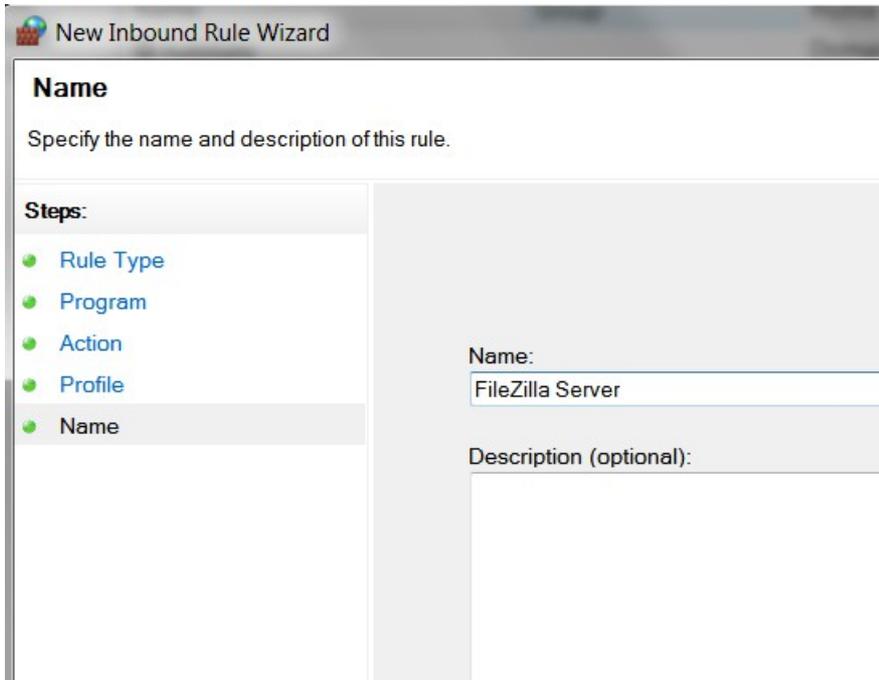
It will now be displayed in the list of inbound rules under the name you allocated to it.

Port Forwarding & Case Study

Test Locally

The next thing is to test that the client when connected to the same subnet can access the FTP Server on 192.168.1.3 and download a file. If all is OK, then setup the port forwarding on the router.

Port Forwarding & Case Study

Testing from internet

Note: when testing, you must have your server software running (e.g. FTP or Minecraft server software etc). ***Otherwise the port will always be closed***.

There is a website that can target your WAN IP address automatically & allow you to specify a port to check. It will report if it is open or closed. This should prove both your forwarding rule & your inbound rule within the firewall on your PC. This site is:-

http://portchecker.co/check

When you visit it from a device connected to your router (wired or wi-fi), it will populate the form with your router's WAN IP address & port 80. Change the port number to the one you want to test & click the "Check" button. The example below when the FTP server forwarding rule was working correctly:-

Once that is OK finally test from a PC or phone that is not connected to your router's network (wired or wireless), but has access to the internet from another broadband connection or 3G or 4G etc.

Port Forwarding & Case Study

Note: most routers do not allow 'Loop Back' access so you will need to access the device only from an external network when using the external internet address. You will not be able to access the external IP address from the internal IP address, when the external address is port forwarded to another local device. Most routers prevent 'Loop Back' as an additional security measure.

So if the device being forwarded to is 192.168.1.3 and the device making the test is 192.168.1.63, this device will not be able to make a test to the router's WAN IP address.

If you have a Smartphone temporarily disable the WiFi and turn on Mobile Data, which will enable you to test access to the device via your mobile phone network. Alternatively you could use a wireless hot spot.

As far as this case study is concerned an FTP client called "FTP Cafe" was run on an Android phone via the 3G network.

To test from a browser (if applicable) you must specify the port number e.g. port 81:-

http://92.92.92.1:81

DDNS

TalkTalk like most ISPs only offer static WAN IP addresses in their business packages & even then possible only as an extra option. DDNS however, gives you a static URL, which automatically updates itself with your new WAN IP address. This allows you to direct the client on the internet accessing your server software on local network via port forwarding, to target the DDNS URL, rather than your WAN IP address, which will change from time to time.

For more details on DDNS, see this TalkTalk help page:-

http://help2.talktalk.co.uk/using-ddns

Testing via DDNS:-

To test via DDNS originate a request from the internet (not from your local network {Loopback access will not work}). If you are using a browser to access an IP camera etc use your DDNS URL followed by colon (:) and the port number. The example below shows someone trying to access port 81 via DDNS:-

http://xxxxxxx.dyndns.com:81/

If you are still having problems, ensure that the IP address used by the DDNS provider is correct.

Port Forwarding & Case Study

Port Forwarding to a port that is intercepted by the router

If you have a PC at say 192.168.1.100 which is hosting a webserver and you want to access this from the internet, normal port forwarding will fail.

Your webserver is expecting an incoming connection on port 80.

So you make your connection attempt from the internet to:-

http://a.b.c.d

where a.b.c.d is the external or WAN IP address of the router.

The router's management system is also a webserver, so your connection attempt (as it is targeting port 80), will be intercepted by the router's webserver. This is why you might see the router's login screen & your connection never reaches the web server on your PC.

What you need to do is choose an unused TCP port number (maybe 8888), then create a new port forwarding rule and translate the external port 8888 to the internal port 80 (called PAT or Port Address Translation) and point this to the PC running the webserver.

What you need is a rule like this:-

Protocol:	TCP
Remote host:	
External start port:	8888
External end port:	8888
Internal host:	192.168.1.100
Internal port:	80
Mapping name:	MyPC-Webserver

Then from the internet try a browser connection to:-

http://a.b.c.d:8888

Port Forwarding & Case Study

Apple MACs running Windows applications

Apple MACs for sometime now have been able to run Windows applications via the "Parallels Desktop" software:-

http://www.parallels.com/uk/products/desktop/

There are problems running certain Windows applications (e.g. Minecraft server), because these applications may not open the ports correctly when using "Parallels". This will mean that port forwarding might not work, unless this is done correctly.

Date : 19/05/2015

Port Forwarding & Case Study

Port Forwarding on other routers

This will depend on the make & model of router that you have. The following are included in this guide. Once the PC firewall & port forwarding is all done, see the section on testing from the internet.

1. Huawei & some D-Link DSL-3780 variants – (used in this case study)
2. D-Link DSL routers (not DSL-3780)
3. D-Link DSL-3780 variants with D-Link style interface
4. Huawei HG633 & HG635 routers

Port Forwarding & Case Study

D-Link DSL routers (not DSL-3780)

Log in to the router, then click on the "Advanced tab at the top and "Port Forwarding" on the left:-

PORT FORWARDING

This is the ability to open ports in your router and re-direct data through those ports to a single PC on your network.

Maximum number of entries which can be configured: 12

ACTIVE PORT FORWARDING

Private IP	Protocol Type	Public Start Port	Public End Port	Connection

Add

ADD PORT FORWARDING

Private IP : `0.0.0.0` `0.0.0.0 ▼`

Protocol Type : `All ▼`

Public Start Port : `0`

Public End Port : `0`

Connection : `PVC0 ▼`

Apply   Cancel

Try leaving the "Connection" as PVC0 but this could need changing to PVC1.

There is no need to make any firewall changes within the router.

Once the changes are complete, click "Apply" & then "Reboot" on the left.

Port Forwarding & Case Study

D-Link DSL-3780

This is a bit of a weird router, in so much as some versions, once you get past the summary screens into "Advanced" mode have the Huawei "Look and feel" interface and some go into the more traditional D-Link interface. If your variant is of the "Huawei" interface and you should be able to follow my guidelines for Huawei routers.

With this variant of the DSL-3780, you have to set up the port forwarding under "Virtual Servers".

There is also talk that you have to configure the "Applications" section as well, to open up the ports on the firewall of the router.

However, recent tests have proved that if the "Applications" are configured, ***this makes the port forwarding operation very intermittent***, often leaving the port closed when tested via various port testers such as http://portchecker.co/check.

First need to log in to the router.

Port Forwarding & Case Study
Virtual Servers

Follow these instructions below taking particular notice of the "interface" option. This should not be left as WAN, but change it to PVC1. You can replace the Internal IP/port number with whatever ones you need.

Click on the "Advanced" tab along the top and down the left hand side, click on "Virtual Servers". The example below port forwards to an FTP server:-

Add the required rule & click the "Add/Apply" button.

Port Forwarding & Case Study

Applications

With the DSL-3780 you may also have to open up the ports on it's own firewall in addition to the firewall on the device you are attempting to forward these ports to.

However, testing has proved that if configured, it can render the port forwarding operation to be very intermittent, at best with the port only showing open occasionally. At worst the port remains permanently closed.

Therefore I do not recommend configuring this section at all.

Router reboot

If the router is rebooted at this point you may lose some of your settings, so go to:-

Maintenance > System Settings > Save & reboot the device

Click the "Reboot" button:-

Port Forwarding & Case Study
HG633 & HG635 routers

This is quite easy to setup on this router, but there are two concepts that are slightly different:-

- *Applications* – these can be software programs such as an FTP Server, or the Minecraft game in server mode that run on a PC/server. They can also be stand alone devices such as CCTV cameras, or a set top box for a TV installation.
- *Internal Host* - you do not forward to a device's IP address, but you forward to a LAN Device using its MAC address. This address stays constant, even if the IP address changes. So it works well with a DHCP (automatically assigned) allocated address.

Do not use Port Triggering, in line with most other routers, this renders the port mapping to be very intermittent at best & at worst the rule will not work at all.

There are two routes to the port mapping page, either via the "Internet" tab followed by "Port Forwarding" on the left:-
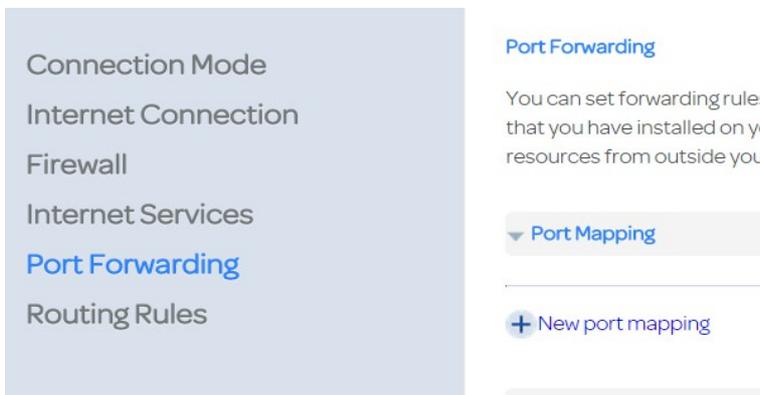

Alternatively click on "Home Network" and "LAN Devices" and click on one of the "Edit forwarding rules" links:-
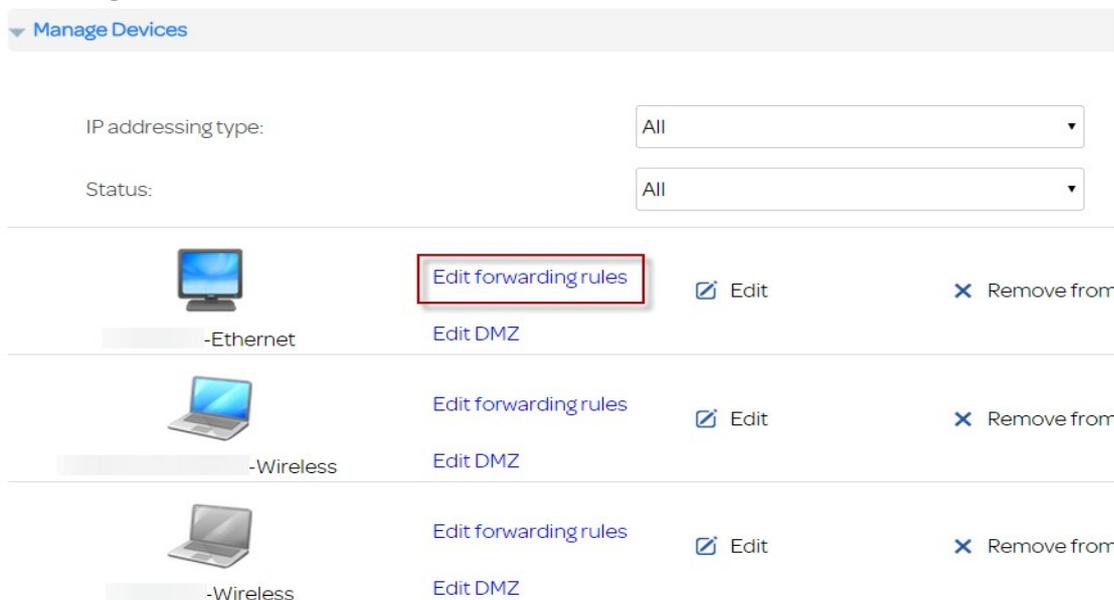
Port Forwarding & Case Study

Applying port forwarding

Once in the "Port Forwarding" configuration area, click "New port mapping":-
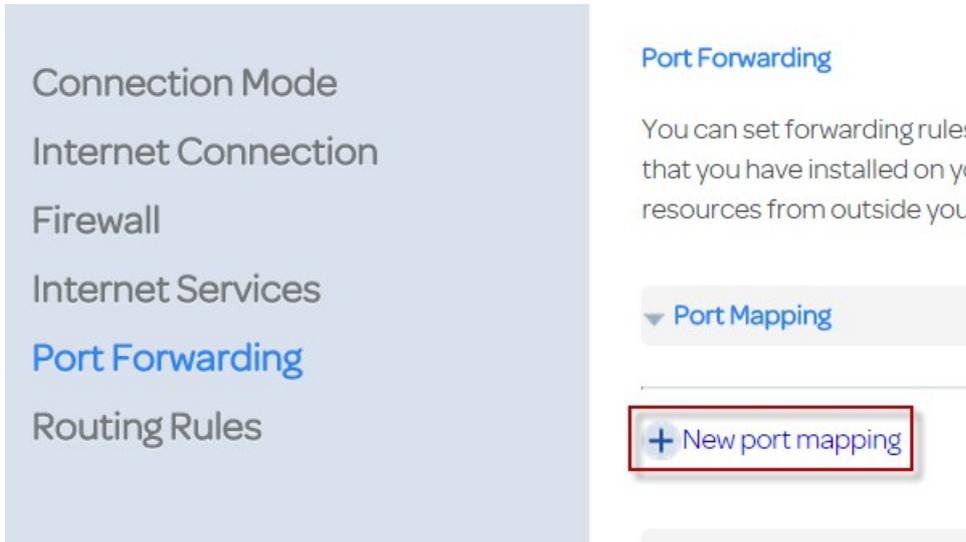
The first concept here is to ensure there is an entry for you desired application that is running on the device that you want to forward to. This could be an FTP Server, SNMP Server etc. This contains all of the port numbers required.

There are a certain amount of these pre-configured, so click the "Application" dropdown box to see the options:-
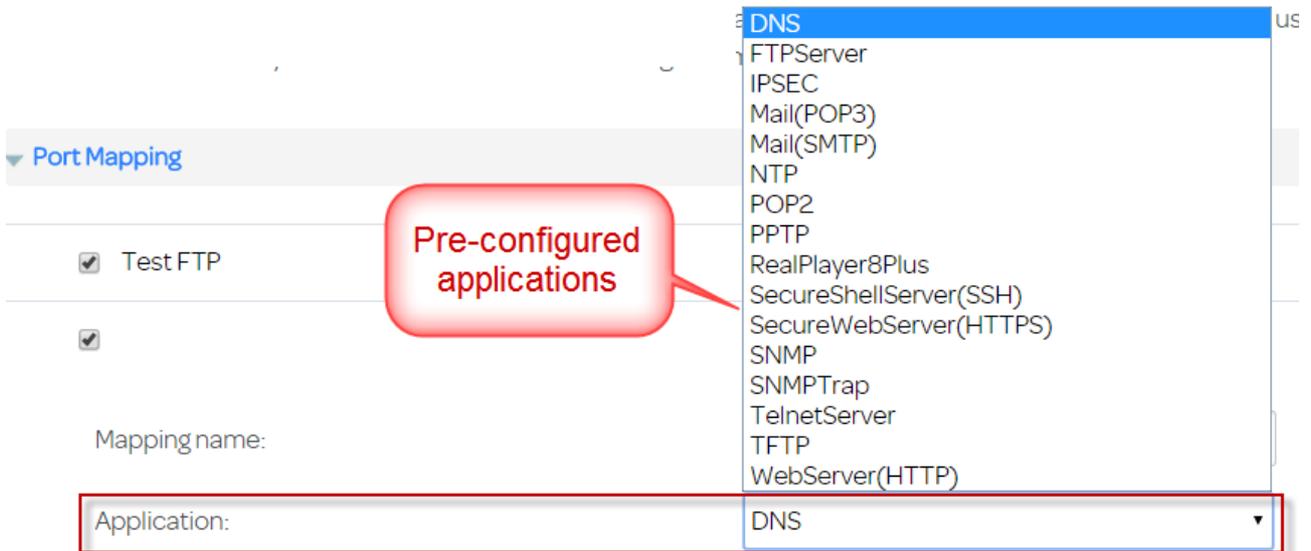
Port Forwarding & Case Study

So in its simplest form, the rule can be done very easily.

Supposing you need to forward SNMP Traps (don't worry what these are, it is only a very simple example) to a PC connected to a LAN port on the router. This is an easy example as there is already a pre-configured application for this.

All you have to do in this case is:-

1. Allocate a name for this port mapping rule
2. Select "SNMPTrap" from the "Application" dropdown box
3. Select the desired PC to forward the traffic to from the "Internal Host" dropdown box.
4. *Reboot the router* & job done!

Port Forwarding & Case Study

No suitable application available

In a lot of cases there will be no suitable application already in the "Application" dropdown box. This will require you to add your own application (e.g. Minecraft server, CCTV camera or DVR) to the port mapping application dropdown box.

Before doing this you will need to know which ports need to be forwarded & ideally if they are TCP or UDP. You should be able to get this information from the vendor of the kit/software you are trying to use.

Once you have added this new application, it is then automatically added to the dropdown box's list of applications. This new one is then ready for selection in the same way as the previous example.

So first click the "Add port mapping application" link:-

This will display the same list of applications, but down the bottom is a "Add port application" link, click on that:-

Port Forwarding & Case Study

Although there is a pre-configured application for an FTP server, this example was used to test the port forwarding functionality of this router and is used as an example here. Give the new application a suitable name, add the ports & select the protocol. If in doubt, set the protocol to "TCP/UDP":-

You will now see your newly created application has been automatically added to the dropdown list of available applications:-

Port Forwarding & Case Study

Now all you you have to do once back in the add new rule screen, is give the rule a name, select your new application and finally select the target device to forward traffic to. Then click the "Save" button & *reboot the router*:-

If the required device is not listed, click the "Add device" link above, you will need to know its MAC address.

Port Forwarding & Case Study

Universal Plug and Play

UPnP means that a device can open the ports it needs as it wants to, and it can close them afterwards, nice and safe and very automatic.

Port forwarding would only open those very same ports and keep them open even when the device was switched off, not as safe but will speed things up for that device as the router 'just knows' already (the entries in its routing table) what port/IP this traffic is destined for, whether the device is switched on and listening or not.

Some devices allow the use of UPnP, this can be be enabled within the router. To do this log into the router and follow the brief guide below:-

Huawei routers

Advanced Mode > Advanced > UPnP

D-Link routers

Advanced mode > Advanced > Advanced LAN > UPnP

D-Link DSL-3780

Advanced mode > Advanced > Network Tools > Network Tools - UPNP & DNLA > UPNP Settings

Huawei HG635

Home Network > LAN Interface > Universal Plug and Play