

In your web browser type:
192.168.1.254

System - Summary - Windows Internet Explorer

http://192.168.1.254/

cool powerpoint backgrounds


System - Summary

AT&T U-verse

System Broadband Link Home Network Voice Network Firewall

Summary System Password Date and Time Settings Details HOME Site Map

Network at a Glance

 **3800HGV-B Gateway**

- Software: 5.29.135.47
- Password: Set


- [Change system password](#)
- [Privacy policy](#)
- [View details](#)

 **Broadband Link**









Connection Speed:

- Incoming: 32200 kbps
- Outgoing: 2784 kbps

- [View summary](#)


 **Home Network**

Computers:

-  192.168.1.65
-  192.168.1.66
-  192.168.1.67
-  Node-3
-  node-0
-  192.168.1.75
-  Node-2
-  NODE-1
-  Wii


- [View the home network](#)

Firewall

 Firewall Active


- [View firewall summary](#)

Upgrade the System

 Your system software is current. Check back for future available upgrades.

- [View available upgrades and options](#)

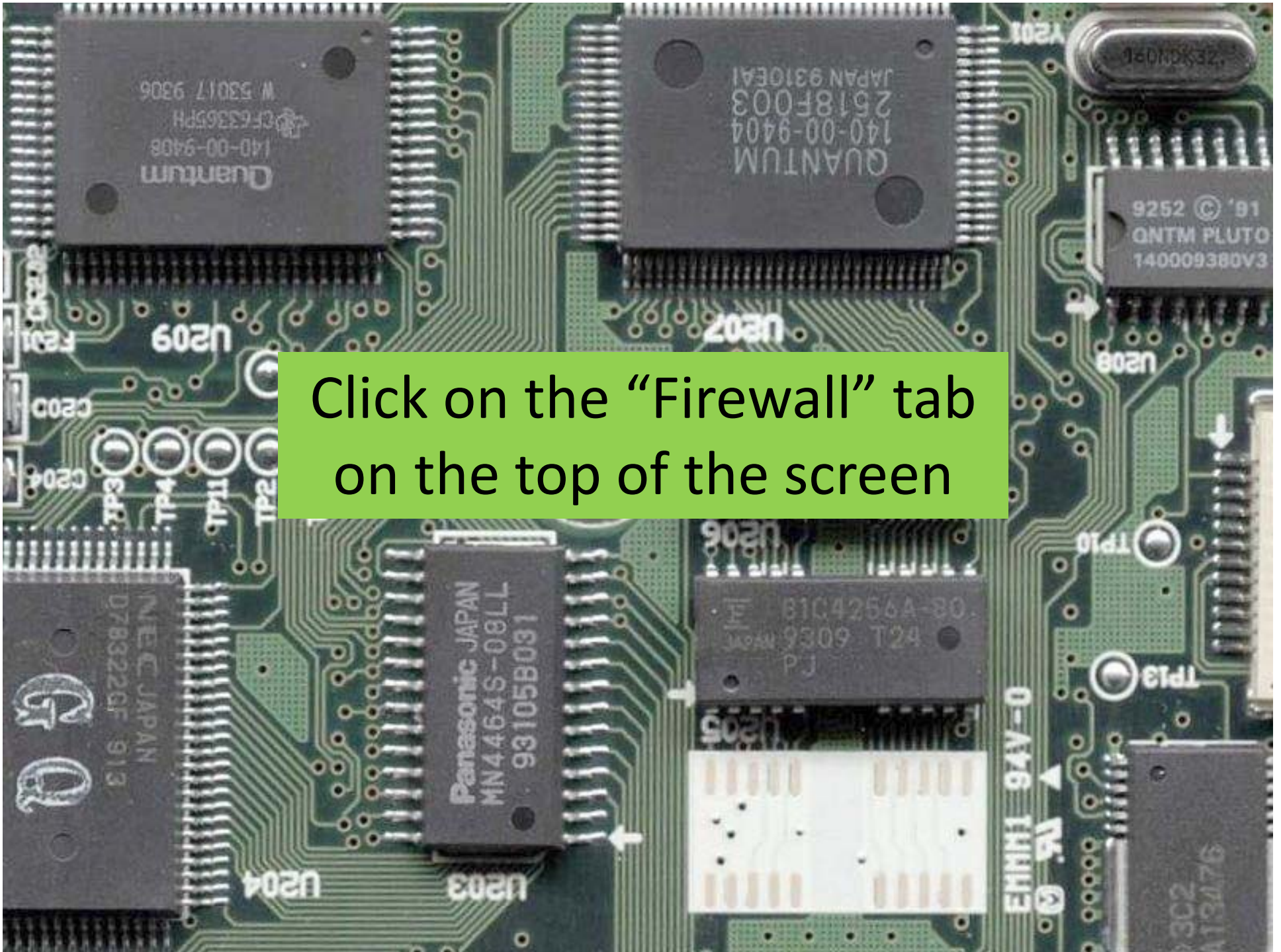
Registration

 [Registration info](#)

Done

Internet | Protected Mode: On

105%



Click on the "Firewall" tab
on the top of the screen

Firewall - Summary - Windows Internet Explorer

http://192.168.1.254/xslt?PAGE=E01&THISPAGE=&NEXTPAGE=EC

cool powerpoint backgrounds


AT&T Uverse

System Broadband Link Home Network Voice Network Firewall

Summary Firewall Settings Advanced Settings HOME Site Map

View Firewall Summary

Firewall Settings

 **Firewall Active**

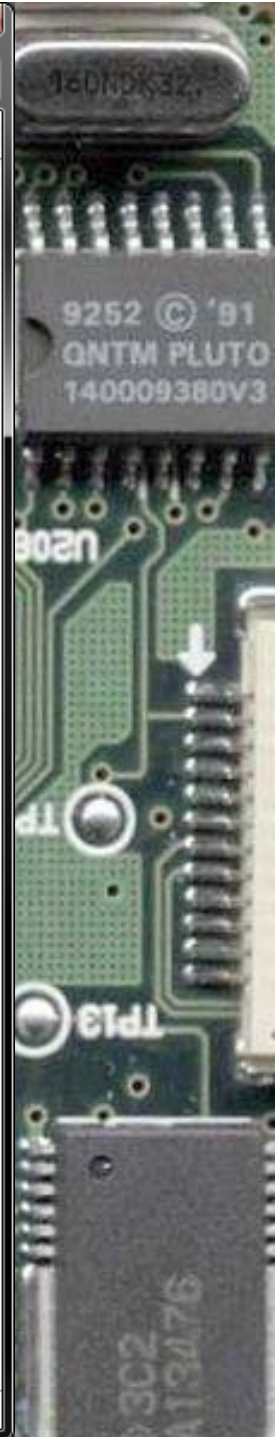
The firewall actively blocks access of unwanted activity from the Internet. If you are using an application that requires you to open a port in your firewall, you may do so by clicking Firewall Settings above.


Current Settings: Custom

Device	Allowed Applications	Private IP address	Public IP address
node-000	XP Remote Assistance XP Remote Desktop 1swarm steam client 1 steam client 2 steam server	192.168.1.146	
WIN-4ETBOC3KJHN	ktorrent	192.168.1.78	
Node-3	utorrentNd3	192.168.1.100	
192.168.1.74	EA XBOX	192.168.1.74	
NODE-1	utorrent PhoneMyPC SNES	192.168.1.73	

[VIEW DETAILS](#)

Done Internet | Protected Mode: On 105%





Click on “Firewall Settings”
(you will get the Password
page, the password is on
the bottom of the router)

System - Password - Windows Internet Explorer

http://192.168.1.254/xsIt?PAGE=E02&THISPAGE=E01&NEXTPAGE

Google

System - Password

System Broadband Link Home Network Voice Network Firewall

Summary System Password Date and Time Settings Details HOME Site Map

Enter the Password

System Password

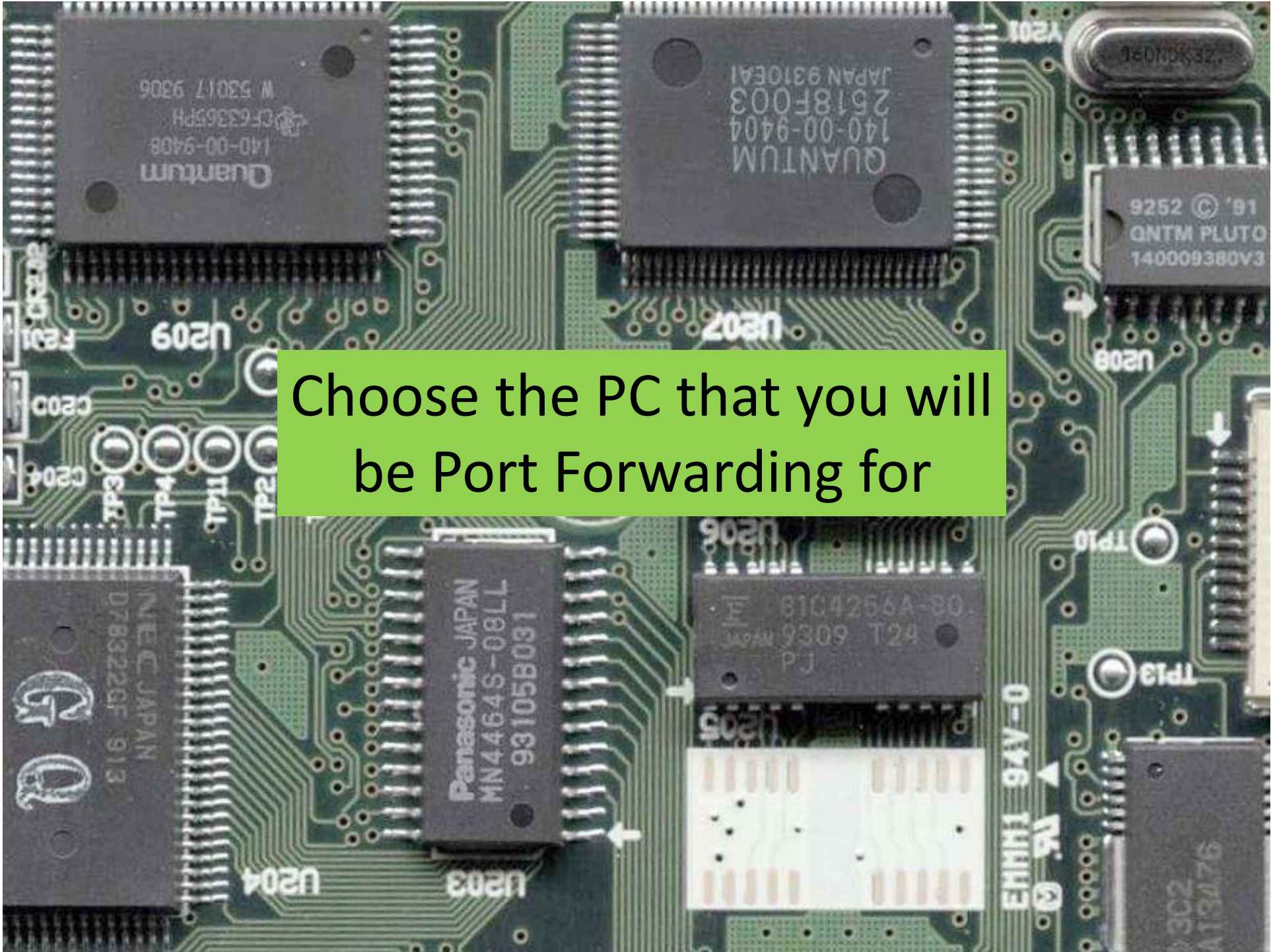
Password Required
Please enter the system password, then click SUBMIT.

Password:

[I forgot the password.](#)

SUBMIT CANCEL

Internet | Protected Mode: On 105%



Choose the PC that you will be Port Forwarding for

Firewall - Edit Firewall Settings - Windows Internet Explorer

http://192.168.1.254/xslt

AT&T U-verse

System Broadband Link Home Network Voice Network Firewall

Summary Firewall Settings Advanced Settings HOME Site Map

Edit Firewall Settings

Settings

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application profile. (To create a user-defined profile, you will need to know protocol and port information.)

- [View firewall details](#)
- [Reset all firewall settings](#)

To Allow Users Through the Firewall to Hosted Applications...

- Select a computer**
Choose the computer that will host applications through the firewall:
 - node-000
 - node-000
 - 192.168.1.65
 - 192.168.1.66
 - 192.168.1.67
 - WIN-4ETBOC3KJHN
 - NintendoDS
 - 192.168.1.70
 - node-001
 - Node-3
 - node-0
 - 192.168.1.148
 - 192.168.1.75
 - 192.168.1.74
 - Node-2
 - NODE-1
 - 192.168.1.76
 - NintendoDS
 - NintendoDS
 - Wii
 - 192.168.1.79
- Edit firewall settings for this computer:**
 - Maximum protection – Disallow unsolicited inbound traffic.
 - Allow individual application(s) – Choose the application(s) that you want to allow through the firewall to this computer.
 - Click ADD to add it to the Hosted Applications list.
 - | | | |
|--------------------|-----|--------|
| All applications | ADD | REMOVE |
| EA XBOX | | |
| ktorrent | | |
| PhoneMyPC | | |
| SNES | | |
| utorrent | | |
| utorrentNd3 | | |
| Age of Empires | | |
| Age of Kings | | |
| Age of Wonders | | |
| Aliens vs Predator | | |
 - [Add a new user-defined application](#)
 - Allow all applications (DMZplus mode) – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

Note: Once DMZplus mode is selected and you click DONE, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.

DONE

Internet | Protected Mode: On 90%

Firewall - Edit Firewall Settings - Windows Internet Explorer

http://192.168.1.254/xslt?PAGE=E02&THISPAGE

AT&T Uverse

System Broadband Link Home Network Voice Network Firewall

Summary Firewall Settings Advanced Settings HOME Site Map

Edit Firewall Settings

Settings

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application profile. (To create a user-defined profile, you will need to know protocol and port information.)

- [View firewall details](#)
- [Reset all firewall settings](#)

To Allow Users Through the Firewall to Hosted Applications...

- Select a computer**
Choose the computer that will host applications through the firewall:
- Edit firewall settings for this computer:**
 - Maximum protection – Disallow unsolicited inbound traffic.
 - Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.

All applications	Hosted Applications:
Isvarm	utorrentNd3
EA XBOX	
ktorrent	
PhoneMyPC	
SNES	
steam client 1	
steam client 2	
steam server	
utorrent	
Age of Empires	
 - Add a new user-defined application
 - Allow all applications (DMZplus mode) – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

Note: Once DMZplus mode is selected and you click DONE, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.

DONE

Internet | Protected Mode: On 90%



Insert:

- Name of the **Program**
- The desired **Port Range**
- Leave **Protocol Timeout, Map To Host Port, and Application Type** empty for the defaults
- Then click **Add Definition**

AT&T U-verse



[Summary](#)

[Firewall Settings](#)

[Advanced Settings](#)

[HOME](#) | [Site Map](#)

Edit Application

Settings

Profile Name

Enter a name for the application profile that you are creating.

Application Name:

Definition

Choose a protocol and enter the port(s) for this application, then click ADD DEFINITION to add the definition to the Definition List. If the application requires multiple ports or both TCP and UDP ports, you will need to add multiple definitions.

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu below, it is recommended that you select it.

Protocol: TCP UDP

Port (or Range): From: To:

Protocol Timeout (seconds): TCP default 86400
UDP default 600

Map to Host Port: Default = the same port as defined above.

Application Type:

[ADD DEFINITION](#)

[BACK](#)

Firewall - Edit Application - Windows Internet Explorer

http://192.168.1.254/xslt

Google

AT&T Uverse

System Broadband Link Home Network Voice Network Firewall

Summary - Firewall Settings - Advanced Settings

HOME Site Map

Edit Application

Settings

Profile Name

Application Name: Remote Desktop

Definition

Choose a protocol and enter the port(s) for this application, then click ADD DEFINITION to add the definition to the Definition List. If the application requires multiple ports or both TCP and UDP ports, you will need to add multiple definitions.

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu below, it is recommended that you select it.

Protocol: TCP UDP

Port (or Range): From: To:

Protocol Timeout (seconds): TCP default 86400
UDP default 600

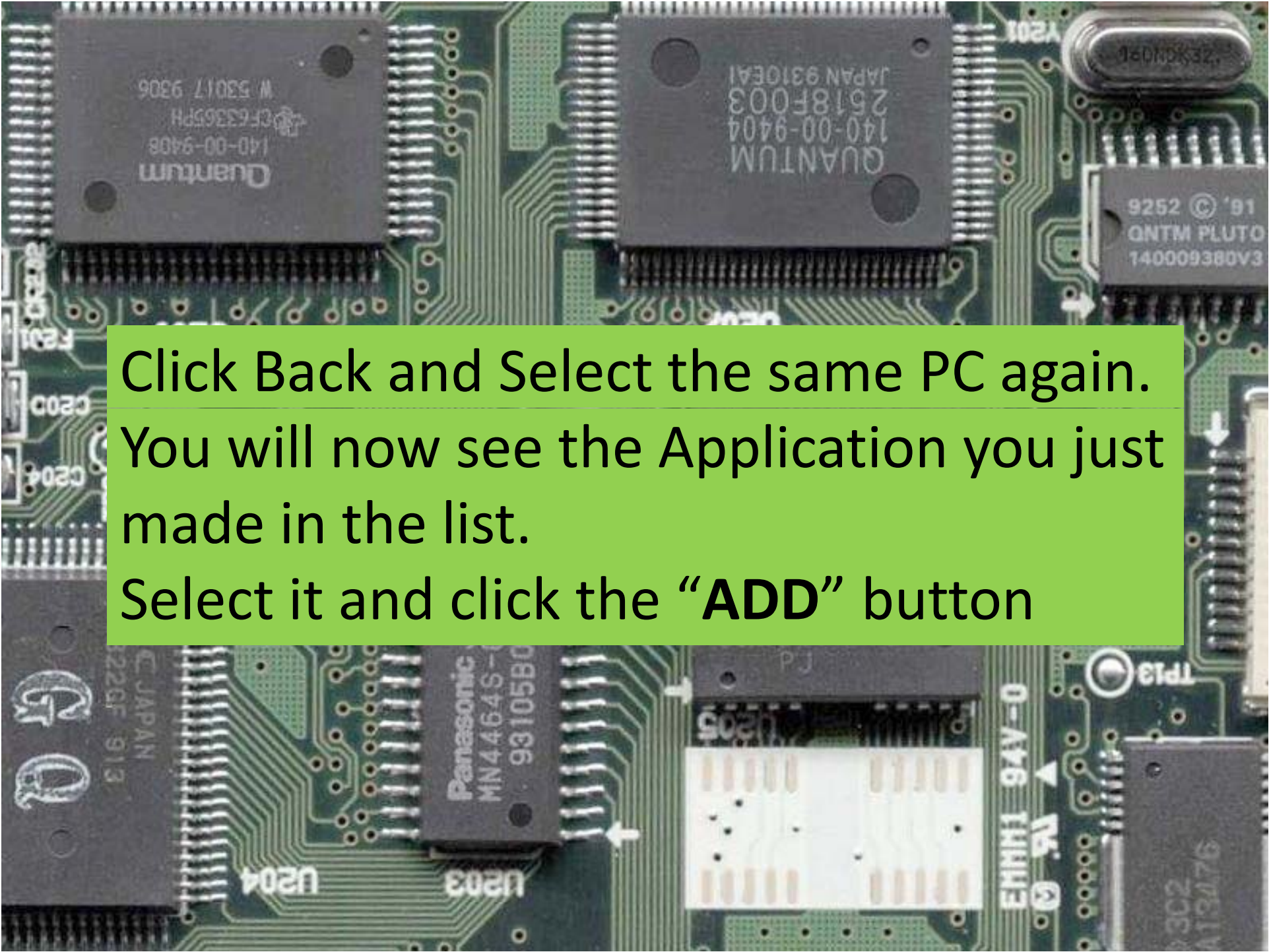
Map to Host Port: Default = the same port as defined above.

Application Type:

Definition List

Protocol	Port (or Range)	Host Port	Timeout (sec)

Done Internet | Protected Mode: On 100%



Click Back and Select the same PC again.
You will now see the Application you just made in the list.
Select it and click the “**ADD**” button

Firewall - Edit Firewall Settings - Windows Internet Explorer

http://192.168.1.254/xsIt?PAGE=E02&THI: Google

AT&T U-verse

System Broadband Link Home Network Voice Network Firewall

Summary Firewall Settings Advanced Settings HOME Site Map

Edit Firewall Settings

Settings

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application profile. (To create a user-defined profile, you will need to know protocol and port information.)

- [View firewall details](#)
- [Reset all firewall settings](#)

To Allow Users Through the Firewall to Hosted Applications...

- Select a computer**
Choose the computer that will host applications through the firewall:
- Edit firewall settings for this computer:**
 - Maximum protection – Disallow unsolicited inbound traffic.
 - Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.

All applications	Hosted Applications:
lswarm	utorrentMId3
EA_XBOX	
ktorrent	
PhoneMyPC	
SNES	
steam client 1	
steam client 2	
steam server	
utorrent	

 - [Add a new user-defined application](#)
 - [Edit or delete user-defined application](#)
 - Allow all applications (DMZplus mode) – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

Note: Once DMZplus mode is selected and you click DONE, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.

DONE

Internet | Protected Mode: On 85%