

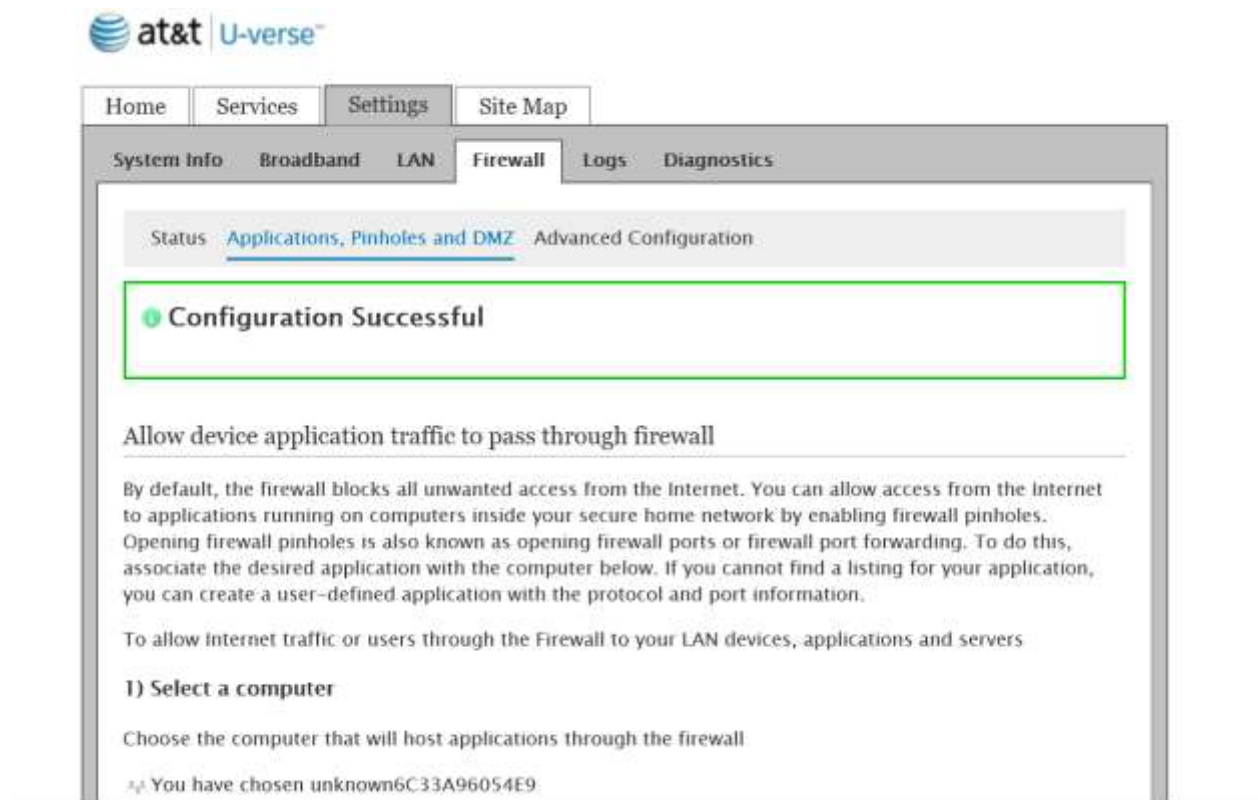
# How to unblock Port 500 for U-Verse to allow VPN to connect.

Open up Internet Explorer on a Windows OS or Safari on a MAC.

In the address bar type in 192.168.1.254 and hit enter



Go to the "Settings" Tab.

A screenshot of the AT&T U-verse website's settings page. At the top left is the AT&T U-verse logo. Below it is a navigation menu with tabs: Home, Services, Settings (selected), and Site Map. Underneath is a sub-menu with tabs: System Info, Broadband, LAN, Firewall (selected), Logs, and Diagnostics. The main content area has a sub-menu with tabs: Status, Applications, Pinholes and DMZ (selected), and Advanced Configuration. A green-bordered box contains a green checkmark icon and the text "Configuration Successful". Below this is the heading "Allow device application traffic to pass through firewall". The text explains that by default, the firewall blocks unwanted access from the Internet and that users can allow access by enabling firewall pinholes. It also mentions that opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. Below this is the instruction "1) Select a computer" and a note that the user has chosen the computer "unknown6C33A96054E9".

Then “Firewall” and “Applications, Pinholes and DMZ”

Scroll down to #2) “Edit Firewall settings for this computer”

Click on “Allow individual applications”

**2) 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.

Filter Applications by	Application List		Hosted Applications
<ul style="list-style-type: none"><li>• <a href="#">All applications</a></li><li>• <a href="#">Games</a></li><li>• <a href="#">Audio/video</a></li><li>• <a href="#">Messaging and Internet Phone</a></li><li>• <a href="#">Servers</a></li><li>• <a href="#">Other</a></li><li>• User-defined</li></ul>	<div style="border: 1px solid black; height: 100px;"></div>	<div style="border: 1px solid gray; padding: 2px;">Add</div> <div style="border: 1px solid gray; padding: 2px;">Remove</div>	<div style="border: 1px solid black; padding: 5px;">PrivacyAbroad VPN</div>
	<a href="#">Add a new user-defined application</a>		<a href="#">Edit or delete user-defined application</a>

Click on “User-defined”

Click on “Add a new user-defined application”

System Info Broadband LAN **Firewall** Logs Diagnostics

Status: [Applications, Pinholes and DMZ](#) Advanced Configuration

### Firewall Application Profile Definition

If the desired application requires multiple ports of both TCP and UDP ports, you will need to add multiple definitions. Current definitions for this profile are shown in the Definition List below.

**Application Profile Name**

**Create Application Definition**

Protocol TCP  UDP

Port (or Range) From  To

Protocol Timeout  TCP default 86400 seconds, UDP default 600 seconds

Map to Host Port  Default/blank = same port as above

Application Type

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 above, it is recommended that you select it.

Type in “PrivacyAbroad VPN” in the “Application Profile Name” field.

Make sure the “TCP” is marked.

In “Port (or Range) type in “500” to “500”

In Protocol Timeout place “86400”

Under the “Application Type” field hit the drop down box and select “PPTP virtual private network server”

Click on “Add to List”

You will then see the following screenshot that confirms you’ve opened up the required port.

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Status Applications, Pinholes and DMZ Advanced Configuration

**Configuration Successful**

**Allow device application traffic to pass through firewall**

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 with the protocol and port information.

To allow internet traffic or users through the Firewall to your LAN devices, applications and servers

**1) Select a computer**

Choose the computer that will host applications through the firewall

⚠ You have chosen unknown6C33A96054E9

Congratulations! You've done it! Now your VPN will connect.