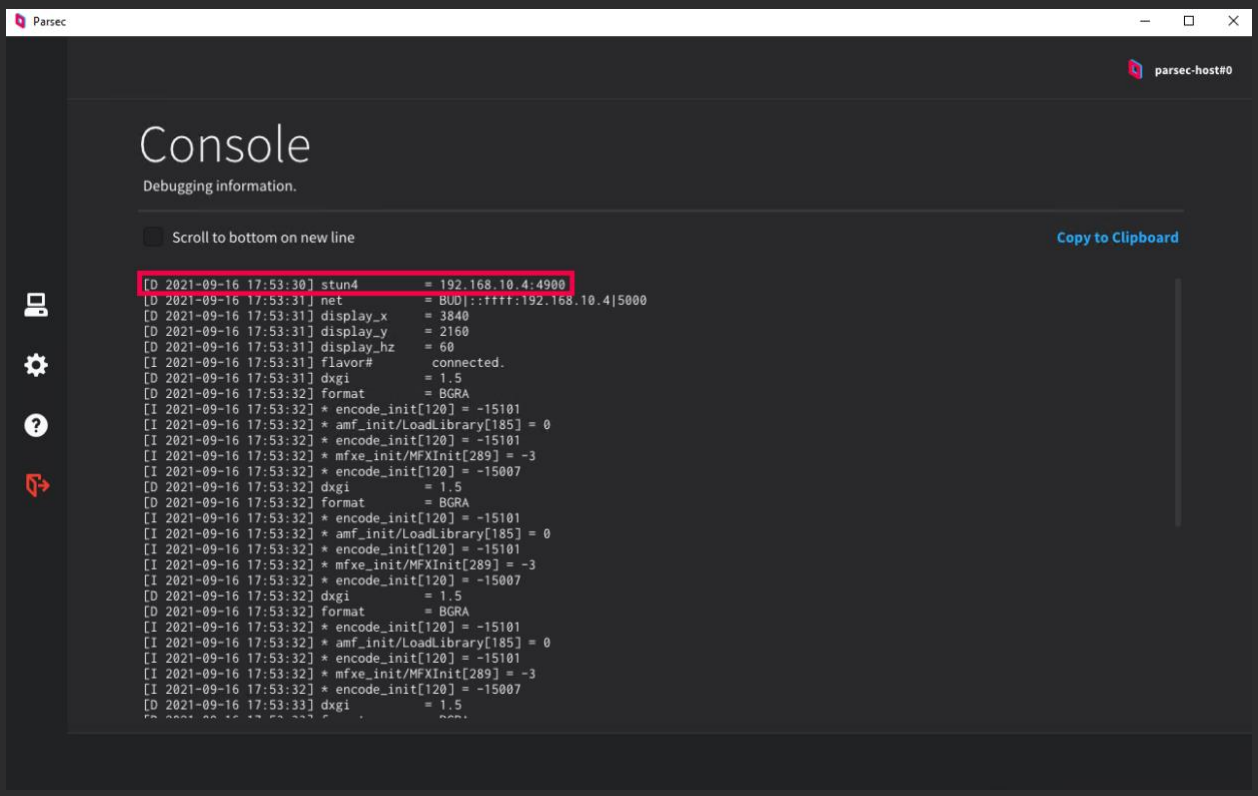
Troubleshooting Parsec High Performance Relay (HPR) server connectivity issues

Validate host configuration for HPR

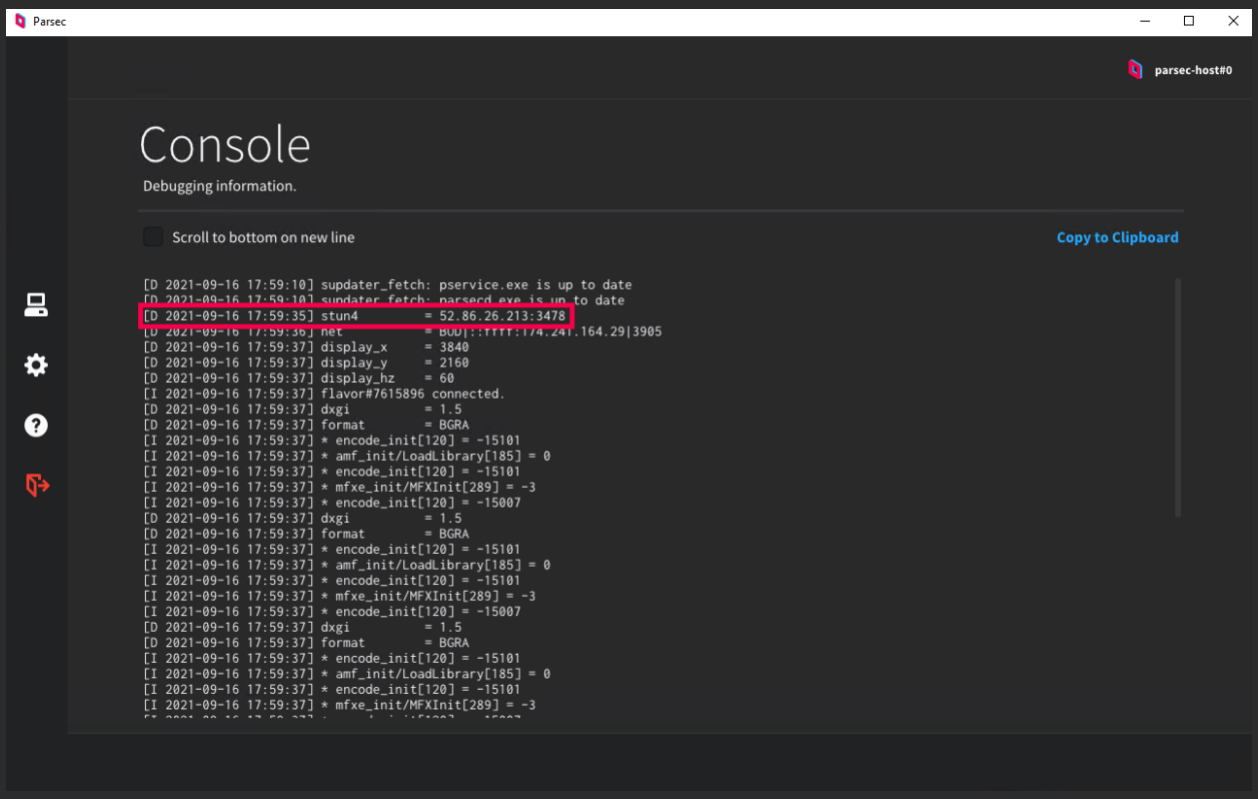
1. Attempt connection to host using Parsec client
2. On the host machine, view Parsec's console log by clicking the 'Help' button, then 'Console'.
3. Verify that the 'stun4=' address matches the LAN IP of the High Performance Relay (HPR) server.

Examples:

- Correct



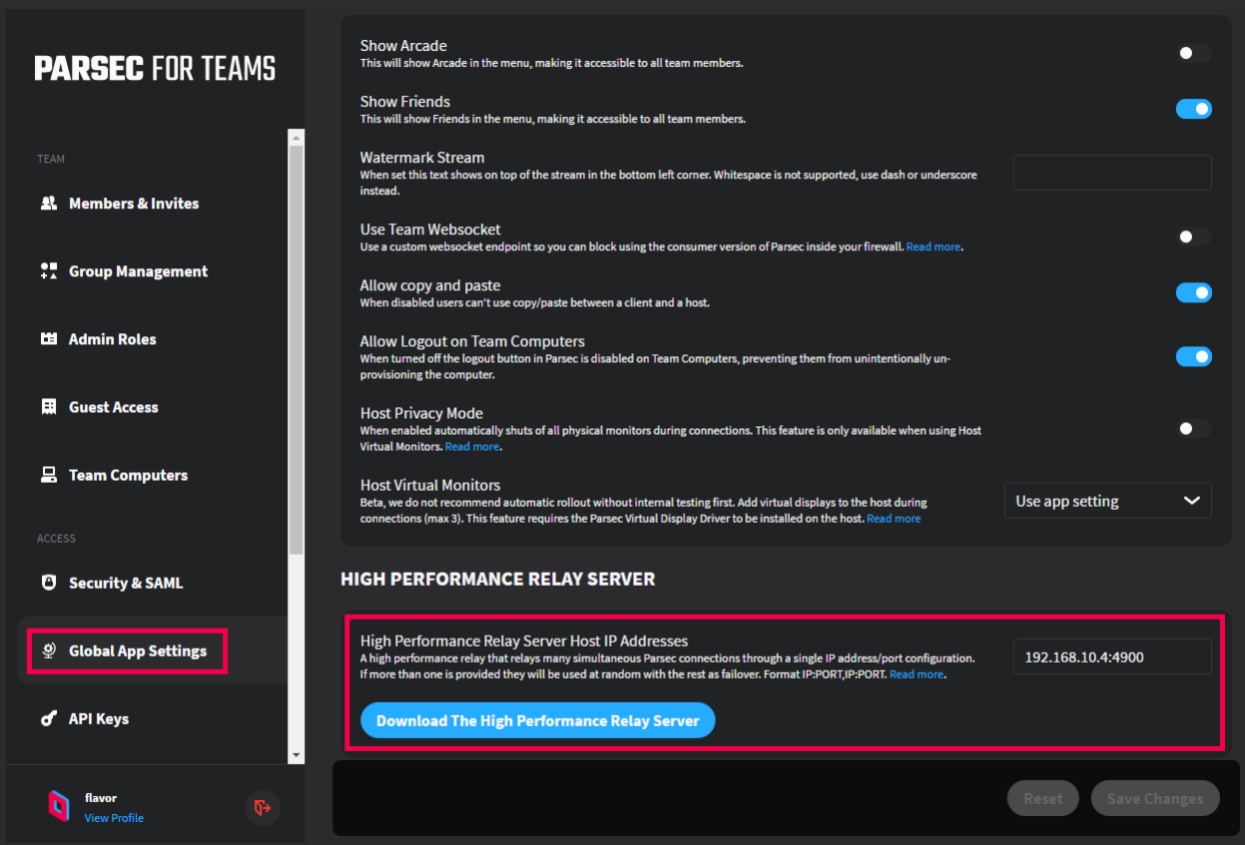
- Incorrect



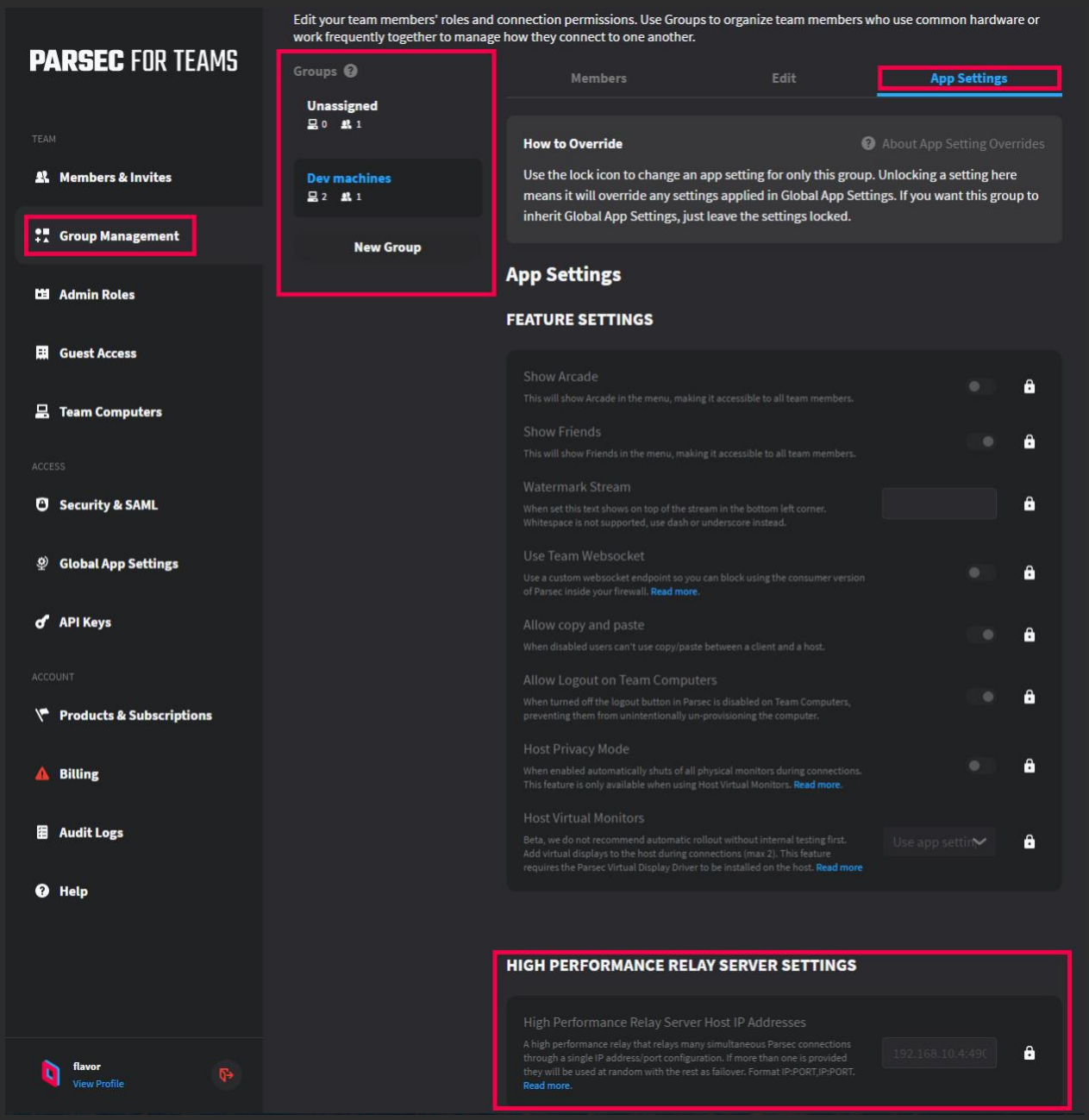
Note) This tells us if the host is configured to use the HPR via the Teams admin page, or through manual configuration file modifications. In general, it is recommended that host configuration to use HPR is done through the Teams admin page. In the examples above, a correct configuration would result in a RFC 1918 class A, B, or C local address, while an incorrect configuration would result in the host receiving our public STUN server address.

Solutions

- Add HPR local IP address and internal listener port on Teams admin page
    - Global


PARSEC FOR TEAMS
TEAM
Members & Invites
Group Management
Admin Roles
Guest Access
Team Computers
ACCESS
Security & SAML
Global App Settings
API Keys
flavor
View Profile
Show Arcade
This will show Arcade in the menu, making it accessible to all team members.
Show Friends
This will show Friends in the menu, making it accessible to all team members.
Watermark Stream
When set this text shows on top of the stream in the bottom left corner. Whitespace is not supported, use dash or underscore instead.
Use Team Websocket
Use a custom websocket endpoint so you can block using the consumer version of Parsec inside your firewall. Read more.
Allow copy and paste
When disabled users can't use copy/paste between a client and a host.
Allow Logout on Team Computers
When turned off the logout button in Parsec is disabled on Team Computers, preventing them from unintentionally un-provisioning the computer.
Host Privacy Mode
When enabled automatically shuts of all physical monitors during connections. This feature is only available when using Host Virtual Monitors. Read more.
Host Virtual Monitors
Beta, we do not recommend automatic rollout without internal testing first. Add virtual displays to the host during connections (max 3). This feature requires the Parsec Virtual Display Driver to be installed on the host. Read more
Use app setting
HIGH PERFORMANCE RELAY SERVER
High Performance Relay Server Host IP Addresses
A high performance relay that relays many simultaneous Parsec connections through a single IP address/port configuration. If more than one is provided they will be used at random with the rest as failover. Format IP:PORT,IP:PORT. Read more.
192.168.10.4:4900
Download The High Performance Relay Server
Reset
Save Changes

- **Per group**



Confirm ‘parsechpr’ service is running on HPR server

1. SSH to HPR
2. Run ‘service parsechpr status’

Examples:

- Correct

```
flavor@parsecHPR:/var/log$ service parsechpr status
● parsechpr.service - Parsec High Performance Relay
     Loaded: loaded (/etc/systemd/system/parsechpr.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2021-09-16 18:08:52 UTC; 5s ago
   Main PID: 3612 (parsechpr)
      Tasks: 1 (limit: 2298)
     Memory: 400.0K
     CGroup: /system.slice/parsechpr.service
             └─3612 /bin/parsechpr [redacted] 5000 4900

Sep 16 18:08:52 parsecHPR systemd[1]: Started Parsec High Performance Relay.
```

HPR public IP, public port, private port

Note) We can also confirm that the service configuration file has been modified appropriately. The HPR public IP, public or private ports should match the IP and ports configured during completion of the prerequisites.

- Incorrect

```
flavor@parsecHPR:/var/log$ service parsechpr status
● parsechpr.service - Parsec High Performance Relay
     Loaded: loaded (/etc/systemd/system/parsechpr.service; enabled; vendor preset: enabled)
     Active: inactive (dead) since Thu 2021-09-16 18:12:48 UTC; 4s ago
    Process: 4248 ExecStart=/bin/parsechpr [redacted] 5000 4900 (code=killed, signal=TERM)
   Main PID: 4248 (code=killed, signal=TERM)
```

Solutions:

- If ‘parsechpr’ service is in ‘inactive’ state
  1. run ‘sudo systemctl start parsechpr’
  2. Confirm service is in ‘active (running)’ state

Or

- If the ‘parsechpr’ service is in ‘active (running)’ state, but the HPR public IP, public or private port information is incorrect, you will need to modify the service config file.
  - Using your *favorite* text editor (we hear you VIM folks), edit the service config file located at ‘/etc/systemd/system/parsechpr.service’

```
  GNU nano 4.8                  /etc/systemd/system/parsechpr.service
[Unit]
Description=Parsec High Performance Relay
After=network.target

[Service]
Type=simple
Restart=always
RestartSec=1
ExecStart=/bin/parsechp[redacted] 5000 4900

[Install]
WantedBy=multi-user.target
```

HPR public IP, public port, private port

Confirm communication from WAN client to public HPR endpoint

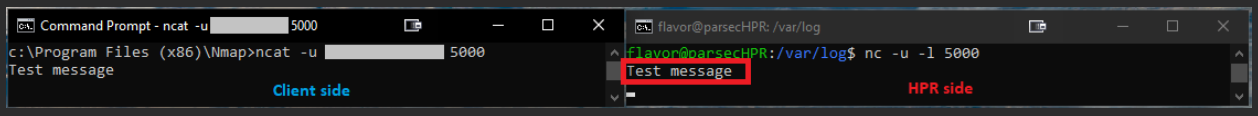
1. Stop the ‘parsechpr’ service

    a. sudo systemctl stop parsechpr

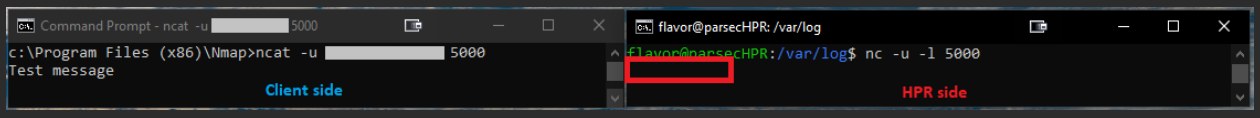
2. On the HPR server, open the public port to listen over UDP using netcat
    a. nc -u -l [public port]
3. On the client, send a message to the public HPR endpoint over UDP using netcat (or ncat on Windows)
    a. nc -u [public-IP] [public-port]
    b. test message

Examples

- **Success**



- **Failure**



Note) Don’t forget to start the parsechpr service again, after successfully completing this test!

Solution

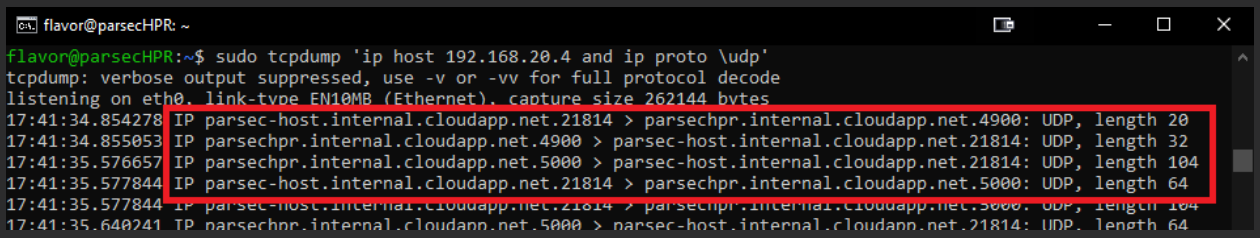
- If the test message is not received by the Parsec HPR server, the reason is most likely related to ingress rules on the corporate firewall. Confirm completion of prerequisites related to public IP, port, and NAT.

Confirm communication between HPR server and Parsec host machine

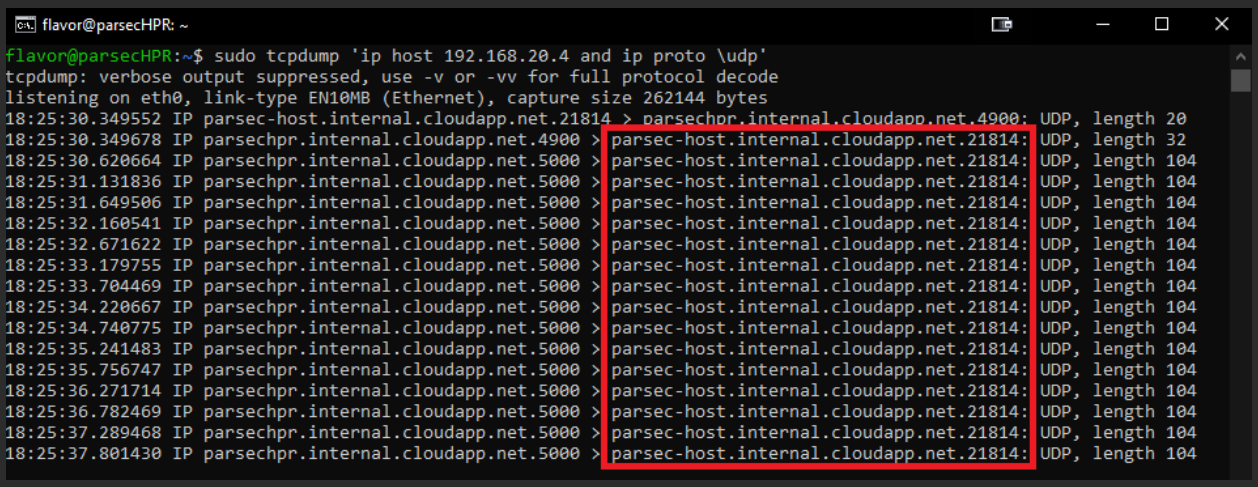
1. Start tcpdump on HPR server
    a. sudo tcpdump ‘ip host [parsec-host-ip] and ip proto \udp’
2. Connect to Parsec host from client

Examples:

- **Success**



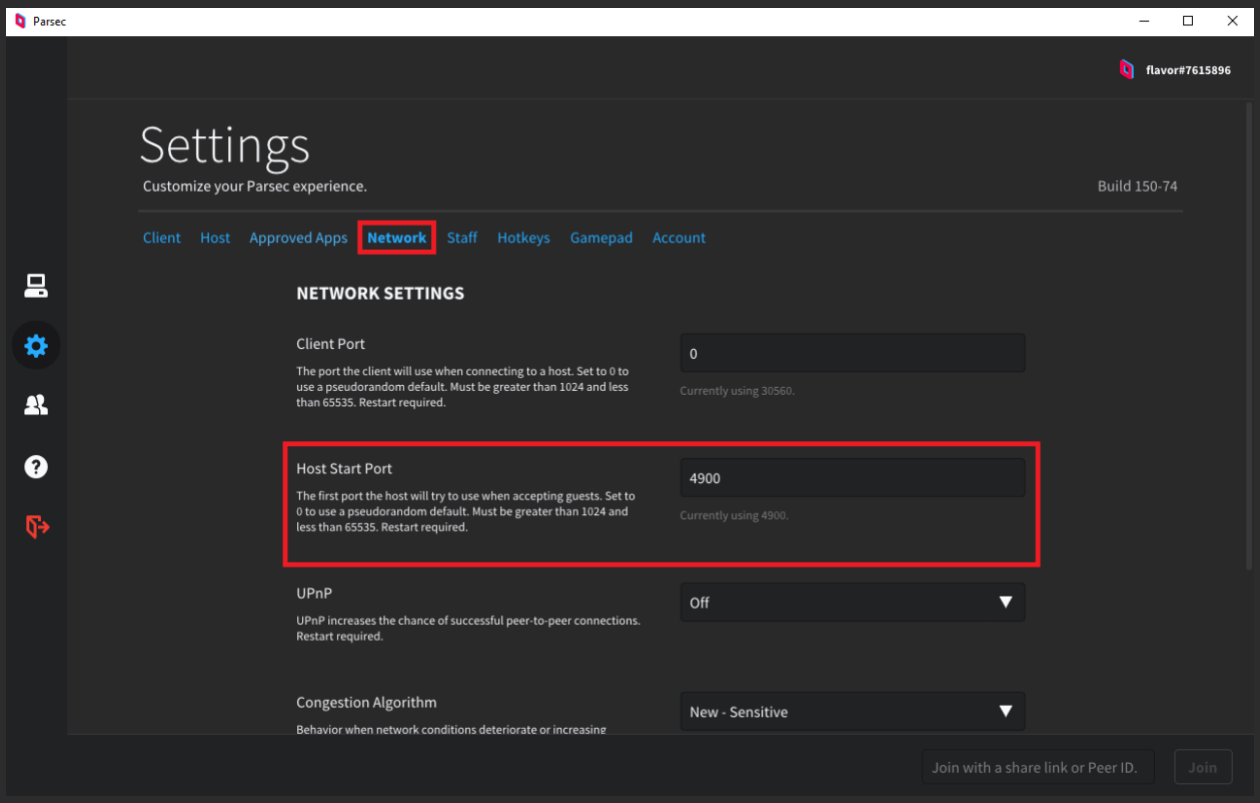
- **Failure**



Note) The HPR will send the same packet to the host, repeatedly, if the host does not respond. In this example, this is indicative of the HPR being unable to communicate with the host's start port.

Solutions

- Confirm that corporate firewall allows UDP communication between HPR and host
    - By default, the Parsec host will select a random Host Start Port. Restrictive corporate firewall policies may not be conducive to usage of random start ports. You may consider configuring a static Host Start Port and allowing only that port through, from the HPR to the hosts.
- Configure static Host Start Port



- Temporarily disable Windows firewall on the host
    - If this is successful, adjust Windows firewall rules appropriately

More helpful information

Verifying UDP connectivity using Netcat:

You can use netcat to check if you can reach the Secure Relay using UDP. Netcat is included in most Linux distros as well as in MacOS. Is also available for windows here: https://nmap.org/download.html

In order to test the connectivity, run netcat in the Relay to listen for UDP connection in the public port, on our example 5000, with the following command:

```
nc -u -l 5000
```

On the client side, run the following command to connect to the Relay via its public IP and port, in our example: 1.2.3.4:5000 with the following command:

```
nc -u 1.2.3.4:5000
```

As this is UDP, both commands won't show an error even if the connection can't be established. In order to test connectivity, just type something on the client side and press enter. If the connectivity is working, you should see the text you typed in the client appearing on the Relay.

You can run the same test from the internal host to the Relay, using the internal port in the Relay command (4900) and using the internal ip:internal port of the relay (10.1.2.20:4900) when connecting from the Host.

We recommend using the following stand-alone package to run netcat on Windows: https://nmap.org/dist/nmap-7.91-win32.zip

Windows firewall:

Windows firewall has been known to block Parsec's UDP traffic in some rare cases. Temporarily disabling the Windows firewall will quickly confirm whether this is an issue and an exception rule needs to be added.

Corporate firewall:

- Confirm you are allowing inbound + outbound UDP traffic on the WAN interface of your firewall to and from the same [public port] you specified on the parsechpr.service. You must not use port translation. If you have set [Public Port] to 5000, then you must open UDP port 5000 on the WAN interface and it must forward directly to port 5000 (and LAN IP address) of the Linux machine running the relay.
- Verify that the Parsec host has general HTTPS internet connectivity (443).
- Confirm your UDP inbound + outbound firewall rule at a minimum accepts traffic from your remote clients public IP address, but for testing purposes we recommend allowing traffic from all public addresses 0.0.0.0/0

Client:

Make sure the client IS NOT connected to the on-premises network via VPN, make sure the client device does have general internet connectivity, make sure the client (sitting at the users home) is the device initiating the connection to the on premise host.