Table of contents

Purpose of the document

Aspia - free open source application for real-time desktop remote control and file transfer.

With Aspia, you can create your own NAT traversal infrastructure (using Router and Relay servers) with connection by ID or use direct connections. Aspia supports many features. Among them, detailed information about the system, audio, text chat.

This document is intended to help you set up your server infrastructure for NAT traversal.

Aspia Router

Router Purpose: Gives IDs to hosts and allows peers (Hosts and Clients) to agree on how they will bypass NAT. All Hosts and Relays are permanently connected to the Router. When the Client wants to connect to the Host, it also connects to the Router. The Router server must have a public IP address. Router and Relay can only work together. Don't forget to install Relay.

1. **Installing the Router (administrator rights required)**

   Windows:

   Run aspia-router-2.5.2-x86.msi and follow the instructions on the screen.

   Linux:

   sudo apt install ./aspia-router-2.5.2-x86_64.deb

2. **Creating a default configuration (administrator rights required)**

   Windows:

   cd /d "C:\Program Files (x86)\Aspia\Router"

   aspia_router --create-config

   Linux:

   sudo aspia_router --create-config

WARNING! There must be no existing configuration file or database in the destination directory. The router never overwrites the current configurations and creating a new configuration is possible only if the previous one does not exist.

3. **Open configuration file and fill in the fields (if necessary; the default configuration does not need to be edited in most cases).**

   Windows:

   C:\ProgramData\aspia\router.json

   Linux:

   /etc/aspia/router.json

   3.1. **PrivateKey (REQUIRED FIELD):** If you already have a private key, then write it here. This option is automatically generated when the configuration is created using command line option “--create-config”. Do not change this setting unless you really need to.

   3.2. **Port:** The port on which incoming connections will be accepted. You can leave the default value. Do not change this parameter unless you do so consciously. The default value is **8060**.

   3.3. **ListenInterface:** Interface address on which the server will listen for incoming connections. Specify 0.0.0.0 if you want to listen for connections on all interfaces. Do not change this setting unless you really need to.

   3.4. **ClientWhiteList:** The **IP address (not hostnames)** list of clients who are allowed to connect to the router. Addresses are separated by semicolons. If the list is empty, then connections from all clients are

allowed. If the list contains items, then only the clients specified in this list can connect. Do not change this setting unless you really need to.

3.5. **HostWhiteList:** The **IP address (not hostnames)** list of Hosts who are allowed to connect to the router. Addresses are separated by semicolons. If the list is empty, then connections from all Hosts are allowed. If the list contains items, then only the Hosts specified in this list can connect. Do not change this setting unless you really need to.

3.6. **AdminWhiteList:** The **IP address (not hostnames)** list of admins who are allowed to connect to the Router. Addresses are separated by semicolons. If the list is empty, then connections from all admins are allowed. If the list contains items, then only the admins specified in this list can connect. Do not change this setting unless you really need to.

3.7. **RelayWhiteList:** The **IP address (not hostnames)** list of relays who are allowed to connect to the Router. Addresses are separated by semicolons. If the list is empty, then connections from all Relays are allowed. If the list contains items, then only the Relays specified in this list can connect. Do not change this setting unless you really need to.

4. **Service/daemon starting**

Windows:

net start aspia-router

Linux:

sudo systemctl enable aspia-router

sudo service aspia-router start

5. **Service/daemon stopping**

Windows:

net stop aspia-router

Linux:

sudo service aspia-router stop

6. **Open public key file and copy the public key. It will come in handy for configuring the Relay and Hosts.**

Windows:

C:\ProgramData\aspia\router.pub

Linux:

/etc/aspia/router.pub

Router file locations

1. **Logs**

To set the log level, declare an environment variable ASPIA_LOG_LEVEL with a value from 0 to 3. Decreasing the value increases the number of messages in the log.

Windows:

C:\Windows\Temp\aspia\aspia_router-*.log

Linux:

sudo journalctl -u aspia-router

2. **Configuration**

Windows:

C:\ProgramData\aspia\router.json

Linux:

/etc/aspia/router.json

3. **Data base**

Windows:

C:\ProgramData\aspia\router.db3

Linux:

/var/lib/aspia/router.db3

NOTES:

1. Hosts and Relays connect to the Router using a public key.
2. Clients and the Console connect using a username and password. You can add additional users when managing Routers in the Console.
3. It is recommended that you set up regular backups of your configuration files and database.
4. Don't forget to add rules in your firewall to access the Router. The Router does not add rules automatically.
5. It is recommended to limit the list of Relays that can be connected to the Router. Whitelist the required Relays.
6. When uninstalling, the Router does not delete its configuration files and database.
7. When updating the Router, do not forget to back up the configuration files and database.
8. For information on how to connect to the router to manage it (including username and password), see the description of the Console.
9. After changing the configuration files, you must restart the Router service. The Router reads the configuration at startup!

Aspia Relay

Relay Purpose: Passes traffic between peers (Hosts and Clients) through itself. The Relay server must have a public IP address. There can be a lot of Relay and they can be placed on separate machines from Router. The number of Relay servers can be from one or more. You must install at least one Relay server. Router and Relay can only work together.

1. **Installing the Relay (administrator rights required)**

   Windows:

   Run aspia-relay-2.5.2-x86.msi and follow the instructions on the screen.

   Linux:

   sudo apt install ./aspia-relay-2.5.2-x86_64.deb

2. **Creating a default configuration (administrator rights required)**

   Windows:

   cd /d "C:\Program Files (x86)\Aspia\Relay"

   aspia_relay --create-config

   Linux:

   sudo aspia_relay --create-config

WARNING! There must be no existing configuration file in the destination directory. The Relay never overwrites the current configurations and creating a new configuration is possible only if the previous one does not exist.

3. **Open configuration file and fill in the fields**

   Windows:

   C:\ProgramData\aspia\relay.json

   Linux:

   /etc/aspia/relay.json

   3.1. **RouterAddress (REQUIRED FIELD)**: Router address. At this address, the Relay server connects to the Router. It can be equal to localhost (or 127.0.0.1) if the router is installed on the same computer.

   3.2. **RouterPort**: If you did not change the port in the Router configuration file, then the field must be left with the default value. If you changed the configuration of the Router, then write the required value. You can leave the default value. Do not change this parameter unless you do so consciously. The default value is **8060**.

   3.3. **RouterPublicKey (REQUIRED FIELD)**: Should contain the public key of the Router that you received when installing it. Enter here the public key that is contained in file **router.pub**, which created by the **Router**.

   3.4. **ListenInterface:** Interface address on which the server will listen for incoming connections. Specify 0.0.0.0 if you want to listen for connections on all interfaces. Do not change this setting unless you really need to.

3.5. **PeerAddress (REQUIRED FIELD)**: The address that peers will receive to connect to the Relay server. This is the Relay server's own address, through which both peers (Client/Console and Host) can access it.

WARNING! This address must be accessible to all participants in the connection (Client/Console/Host). You should keep in mind that both peers (Host and Client/Console) must be able to connect to this address. Consider this when setting up your network hardware if you are setting up port forwarding on your Router. If your Router is behind NAT, then you must provide access to this address for external and internal connections. See the documentation for your network equipment for more information on how to do this. An example of a configuration for Mikrotik and iptables routers is at the end of this document.

3.6. **PeerPort**: The port through which peers will connect to the Relay server. You can leave the default value. Do not change this parameter unless you do so consciously. The default value is **8070**.

3.7. **PeerIdleTimeout**: Time in minutes. If during this time no data comes from the peers, the connection is terminated. You can leave the default value. Do not change this parameter unless you do so consciously. The default value is **5**.

3.8. **MaxPeerCount**: The maximum number of simultaneous connections established between peers. You can leave the default value. Do not change this parameter unless you do so consciously. The default value is **100**.

3.9. **StatisticsEnabled**: Enable or disable automatic sending of statistics to the router. You can leave the default value. Can take values: **true** or **false**. The default value is **false**.

3.10. **StatisticsInterval**: Interval in seconds for automatically sending statistics to the router. You can leave the default value. Can take a value from **1** to **60**. The default value is **5**.

4. Service/daemon starting

Windows:

```
net start aspia-relay
```

Linux:

```
sudo systemctl enable aspia-relay
sudo service aspia-relay start
```

5. Service/daemon stopping

Windows:

```
net stop aspia-relay
```

Linux:

```
sudo service aspia-relay stop
```

Relay file locations

1. Logs

To set the log level, declare an environment variable ASPIA_LOG_LEVEL with a value from 0 to 3. Decreasing the value increases the number of messages in the log.

Windows:

C:\Windows\Temp\aspia\aspia_relay-*.log

Linux:

sudo journalctl -u aspia-relay

2. **Configuration**

Windows:

C:\ProgramData\aspia\relay.json

Linux:

/etc/aspia/relay.json

NOTES:

1. Don't forget to add rules in your firewall to access the Relay. The Relay does not add rules automatically.
2. When uninstalling, the Relay does not delete its configuration files.
3. After changing the configuration files, you must restart the Relay service. The Relay reads the configuration at startup!

Aspia Console

Console Purpose: Allows you to create address books, add computers to them and group them. It also allows you to manage computers and routers.

1. **Installing the Console**

   Windows:

   Run aspia-console-2.5.2-x86.msi and follow the instructions on the screen.

   MacOS X:

   Open aspia-console-2.5.2.dmg and move “Aspia Console” to “Applications”.

   Linux:

   sudo apt install ./aspia-console-2.5.2-x86_64.deb

2. **Create a new address book and configure the router in its properties.**

   Default username: admin

   Default password: admin

   WARNING: Don't forget to change your password! Connect to your router and change the default password. You can also add additional users.

   Logs

   To set the log level, declare an environment variable ASPIA_LOG_LEVEL with a value from 0 to 3. Decreasing the value increases the number of messages in the log.

   Windows:

   C:\Users\<user_name>\AppData\Local\Temp\aspia\aspia_console-*.log

   Linux / MacOS:

   Logs are written to the terminal.

Aspia Client

Client Purpose: Allows you to connect to and control hosts.

1. **Installing the client**

   Windows:

   Run aspia-client-2.5.2-x86.msi and follow the instructions on the screen.

   MacOS X:

   Open aspia-client-2.5.2.dmg and move “Aspia Client” to “Applications”.

   Linux:

   sudo apt install ./aspia-client-2.5.2-x86_64.deb

   Logs

   To set the log level, declare an environment variable ASPIA_LOG_LEVEL with a value from 0 to 3. Decreasing the value increases the number of messages in the log.

   Windows:

   C:\Users\<user_name>\AppData\Local\Temp\aspia\aspia_client-*.log

   Linux / MacOS:

   Logs are written to the terminal.

Aspia Host

Host Purpose: Allows Accepts incoming connections from Clients and Consoles to manage the computer on which it is installed.

1. **Installing the host**

   The host is only available for Windows.

   Run aspia-host-2.5.2-x86.msi and follow the instructions on the screen.

2. **Enabling the router in the settings**

   2.1. Go to settings (Aspia -> Settings… -> Router)

   2.2. Enable the use of the Router

   2.3. Write the address of your Router

   2.4. Write your Router's public key

Logs

To set the log level, declare an environment variable ASPIA_LOG_LEVEL with a value from 0 to 3. Decreasing the value increases the number of messages in the log.

Windows:

C:\Users\<user_name>\AppData\Local\Temp\aspia\aspia_host-*.log

C:\Windows\Temp\aspia\aspia_host_service-*.log

C:\Windows\Temp\aspia\aspia_desktop_agent-*.log

APPENDIX 1. Bug reporting

If you experience any problems while using the application, then in order to report a problem, you must:

1. **Enable advanced logging**. To do this, declare the environment variable **ASPIA_LOG_LEVEL with the value 0**. This will allow you to get the maximum number of messages in the logs. If you don't know what environment variables are, use search engines to get information on how to declare environment variables in your operating system.
2. After setting the environment variable, you need to restart your computer.
3. Try to reproduce the problem situation.
4. Collect application logs (information on where to get the logs is located above) and send to developers using one of the acceptable methods:
   a) Email: dmitry@aspia.ru
   b) Telegram: @dchapyshev

   The log directories in Windows may contain files with the *.dmp extension. These files contain application memory dumps at the time of the crash. These files can help to determine the cause of problems. Be sure to attach them along with the logs.
5. Please describe your problem in detail. Including the version of the operating system (on client/host/router/relay), the version of Aspia and all your actions. If you can make a video that shows the problem, that might help solve it too.

APPENDIX 2. Configuration for Mikrotik

If you are configuring port forwarding on your network router, then an example of setting for the Mikrotik router may come in handy:

/ip firewall nat

add action=netmap chain=dstnat comment="Aspia Relay" dst-port=8070 in-interface=WAN protocol=tcp to-addresses=**RELAY_IP** to-ports=8070

add action=netmap chain=dstnat comment="Aspia Router" dst-port=8060 in-interface=WAN protocol=tcp to-addresses=**ROUTER_IP** to-ports=8060

add action=dst-nat chain=dstnat comment="Aspia Relay" dst-address=**EXTERNAL_IP** dst-port=8070 protocol=tcp src-address=**LOCAL_NETWORK** to-addresses=**RELAY_IP** to-ports=8070

add action=dst-nat chain=dstnat comment="Aspia Router" dst-address=**EXTERNAL_IP** dst-port=8060 protocol=tcp src-address=**LOCAL_NETWORK** to-addresses=**ROUTER_IP** to-ports=8060

add action=masquerade chain=srcnat comment="Aspia Relay" dst-address=**RELAY_IP** dst-port=8070 protocol=tcp src-address=**LOCAL_NETWORK**

add action=masquerade chain=srcnat comment="Aspia Router" dst-address=**ROUTER_IP** dst-port=8060 protocol=tcp src-address=**LOCAL_NETWORK**

Replace the following with your data:

ROUTER_IP - IP address of the computer on which the Router is installed.

RELAY_IP - IP address of the computer on which the Relay is installed.

LOCAL_NETWORK – your local network (for example 192.168.1.0/24).

EXTERNAL_IP - your external IP address

APPENDIX 3. Configuration for iptables

iptables -t nat -A PREROUTING -p tcp -m multiport --dports 8060,8070 -j DNAT --to-destination **ROUTER_AND_RELAY_IP**

iptables -t nat -A POSTROUTING -s **LOCAL_NETWORK** -d **ROUTER_AND_RELAY_IP** -p tcp -m multiport --dports 8060,8070 -j SNAT --to-source **EXTERNAL_IP**

Replace the following with your data:

ROUTER_AND_RELAY_IP - IP address of the computer on which the Router/Relay is installed.

LOCAL_NETWORK – your local network (for example 192.168.1.0/24).

EXTERNAL_IP - your external IP address