**Router**

**Router Purpose:** Gives IDs to hosts and allows peers (Hosts and Clients) to agree on how they will bypass NAT. 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-2.5.0-x86.msi and follow the instructions on the screen.

Linux:

sudo apt install ./aspia-router-2.5.0-x86\_64.deb

1. **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.**

1. **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

* 1. **PrivateKey (REQUIRED FIELD):** If you already have a private key, then write it here.
  2. **Port:** The port on which incoming connections will be accepted. You can leave the default value.
  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.
  4. **ClientWhiteList:** The IP address 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.
  5. **HostWhiteList:** The IP address 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.
  6. **AdminWhiteList:** The IP address 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.
  7. **RelayWhiteList:** The IP address 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.

1. **Service/daemon starting**

Windows:

net stop aspia-router

net start aspia-router

Linux:

sudo systemctl enable aspia-router

sudo service aspia-router start

1. **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

1. **Configuration**

Windows:

C:\ProgramData\aspia\router.json

Linux:

/etc/aspia/router.json

1. **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. How to connect to a Router to manage it is described in the description of the Console.
4. It is recommended that you set up regular backups of your configuration files and database.
5. Don't forget to add rules in your firewall to access the Router. The Router does not add rules automatically.
6. It is recommended to limit the list of Relays that can be connected to the Router. Whitelist the required Relays.
7. When uninstalling, the Router does not delete its configuration files and database.
8. When updating the Router, do not forget to back up the configuration files and database.

**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-2.5.0-x86.msi and follow the instructions on the screen.

Linux:

sudo apt install ./aspia-relay-2.5.0-x86\_64.deb

1. **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.**

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

Windows:

C:\ProgramData\aspia\relay.json

Linux:

/etc/aspia/relay.json

* 1. **RouterAddress (REQUIRED FIELD)**: Router address. It can be equal to localhost if the router is installed on the same computer.
  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.
  3. **RouterPublicKey (REQUIRED FIELD)**: Should contain the public key of the Router that you received when installing it.
  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.
  5. **PeerAddress (REQUIRED FIELD)**: The address that peers will receive to connect to the Relay server.

**WARNING! This address must be accessible to all participants in the connection. You should keep in mind that both peers (Host and Client) 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 routers is at the end of this document.**

* 1. **PeerPort**: The port through which peers will connect to the Relay server. You can leave the default value.
  2. **PeerIdleTimeout**: Time in minutes. If during this time no data comes from the peers, the connection is terminated. You can leave the default value.
  3. **MaxPeerCount**: The maximum number of simultaneous connections established between peers. You can leave the default value.

1. Service/daemon starting

Windows:

net stop aspia-relay

net start aspia-relay

Linux:

sudo systemctl enable aspia-relay

sudo service aspia-relay start

**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

1. **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.

**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 Сonsole**

Windows:

Run aspia-console-2.5.0-x86.msi and follow the instructions on the screen.

MacOS X:

Open aspia-console-2.5.0.dmg and move “Aspia Console” to “Applications”.

Linux:

sudo apt install ./aspia-console-2.5.0-x86\_64.deb

1. **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.

**Client**

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

1. **Installing the client**

Windows:

Run aspia-client-2.5.0-x86.msi and follow the instructions on the screen.

MacOS X:

Open aspia-client-2.5.0.dmg and move “Aspia Client” to “Applications”.

Linux:

sudo apt install ./aspia-client-2.5.0-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.

**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-2.5.0-x86.msi and follow the instructions on the screen.

1. **Enabling the router in the settings**
   1. Go to settings (Aspia -> Settings… -> Router)
   2. Enable the use of the Router
   3. Write the address of your Router
   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**

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