Making server accessible

Contents

Configuring the firewall

Forwarding ports on the router

DNS name vs. IP address

Checking if the server is accessible

Troubleshooting

Regardless of whether you install the Server in your organization or at a web hosting provider you must ensure the server is directly accessible from the outside. Basically, you should do the following:

1. Configure your Server computer's firewall.

2. Create a port forwarding rule on your network router.

3. Use a DNS name as the server's address vs. using its IP address (recommended).

After you complete these tasks you can verify if the server is accessible from the outside. You can use a free online checker tool such as canyouseeme.org or a similar service.

Configuring the firewall

If you use the built-in Windows firewall on your Server PC you may skip this section. The Server automatically adds an exception rule to your Windows firewall settings upon installation.

> **Important!**
> You still need to manually add an exception rule to Windows built-in firewall if you changed the Server ports from their default values after installation.

If you have another firewall software installed on the Server PC, please refer to its documentation on how to allow incoming TCP ports. The default Server ports are `TCP 5655 and 5670`.

Forwarding ports on the router

Your *Hosts* — and possibly the *Viewer* — are supposed to be located "in the cloud" relative to the Server. Therefore the next step is making sure that your Internet gateway router allows incoming connections to your server from the outside, i.e. setting up a *port forwarding rule*.

> *Port forwarding (also port mapping)* is a technique of translating the address and/or port number of a network packet to a new destination. Port forwarding allows remote computers, located on the Internet, to connect to a specific computer or service within a private local area network (LAN).

In order to create a port forwarding rule you must have access to your router's administration panel. Specific instructions depend on the router model, but generally you must do the following:

1. Find out your Server computer's local IP address (e.g. 192.168.0.5).

2. In the router settings create a rule that forwards port `5655 TCP` to the Server's computer local IP address.

Note that `5655 TCP` is the default communication port used by the Server. If you change the port, make sure you specify the new port value in the port forwarding rule. Also, if you manage the server remotely using the Admin Console, you must create another port forwarding rule and forward port `5670 TCP` to the same Server computer's local IP address.

We highly recommend that you visit www.portforward.com for more information about port forwarding and instructions for specific router models.

DNS name vs. IP address

In order to connect your Viewers and Hosts to your Server you must know your Server computer's *external* (also *public*) IP address or DNS name. This is essentially the external IP address (or DNS name) of your router because it is only through the router that your Server accesses the Internet while being invisible directly from the outside.

The external IP address can either be *static* or *dynamic*. The former is permanently assigned to your router and never changes whereas a dynamic IP address may change quite frequently. You can find out your external IP address by opening the website https://www.whatismyip.com/ on your Server's computer.

Finally, your router may also have a *DNS name*, either set up in-house or provided by a service like **dyndns.org** or **no-ip.com**.

> 👆 **Important!**
> We highly recommend that you obtain and use a DNS name instead of IP address. A DNS name stays the same even when the IP address that it "represents" changes. This means that you can easily move your Server to a new computer or hosting location without updating settings on all your Viewers and Hosts, provided that you use the old DNS name for the new server location. Otherwise, and especially if you happen to use a dynamic IP address you will end up losing connectivity to your remote PCs whenever your Server's PC IP address changes.

In order to obtain a DNS name you can either sign up for one of the DNS services mentioned above or ask your system administrator for assistance.

Checking if the server is accessible

The check if your port forwarding rule works properly and your server is visible from the outside:

1. On the server machine open a web browser and visit https://canyouseeme.org

2. Depending on which port you are checking, enter the server's communication or administration port number in the `Port to Check` field and click `Check port`.

3. Provided you have configured everything properly the form will return "Success" as the check result.

> The server starts "listening" on the administration port only when the `Allow TCP/IP connection` checkbox is enabled in the server configuration settings. Keep this in mind when you are checking server availability on this port.

Troubleshooting

If you receive "Error" when checking the server accessibility as described above, this can mean either of the following:

- Your port forwarding rule doesn't work, i.e. you might be mistaken with either port number or local IP address of the Server or both
- The Server service/process is not running on the Server computer
- The communication port number in the Server settings is different from the number you are checking (see configuration settings)
- The firewall on your Server machine blocks the inbound port which is being checked

If you are still having issues with making the Server accessible, feel free to contact our technical support.

Related articles

- RU Server: About RU Server
- RU Server: Installing and Uninstalling RU Server
- RU Server: Server configuration
- RU Server: Server role: Address book sync
- RU Server: Server role: Authentication
- RU Server: Server role: Relay

URL: https://www.remoteutilities.com/support/docs/making-server-accessible/