
How to Use the RPC Plugin Module

<https://campus.barracuda.com/doc/46209487/>

The Barracuda NextGen Firewall F-Series generally provides three different ways of dealing with RPC services:

Passive

- **Advantage:** The firewall immediately notices RPC port changes (traffic analyzes client - server).
- **Disadvantage:** The firewall notices the RPC port which is used only on client requests. If a firewall reboot occurs, the firewall will not know the port until the next client request gets scanned.

The term PASSIVE means in this case "sniffing" RPC information passively. Using this type causes that the firewall engine reads the RPC information from RPC requests (using UDP/TCP on port 135 (DCERPC) or port 111 (OCNRPC)) automatically using the plugin DCERPC or OCNRPC. This way you are benefiting from the fact that the firewall is always up-to-date on the currently valid ports. The main problem of passive configuration is that in case of a reboot of the firewall there would not be any information concerning the required ports as the information is not written to disk. Clients attempting to use previously established RPC connections would be blocked.

Active

- **Advantage:** The firewall actively looks for all RPC information independent of client requests.
- **Disadvantage:** All RPC servers are to be configured manually. Port changes within a polling interval will not be recognized by the firewall.

The term ACTIVE means in this case requesting RPC information actively. This method uses a defined RPC server where the firewall obtains the RPC information periodically. A benefit of this type is that the firewall knows the type of services available on the RPC server. However, problems may occur if the RPC server is not available for some time. In this case the RPC server may have new portmapping information as soon as it is online again but the firewall still uses the "old" information as valid ones which leads to blocked connection attempts.

Active & Passive

ACTIVE and PASSIVE at the same time is combining the benefits of both and is

therefore recommended.

For detailed information on how to configure RPC plugins, see:

- [How to Configure the ONCRPC Plugin Module](#)
- [How to Configure the DCERPC Plugin Module](#)

Monitoring

The monitoring of RPC takes place in the **Dynamic Services** tab of the Barracuda NextGen Firewall F-Series box menu entry (tab **Dynamic**):

1. Go to the **FIREWALL > Dynamic** page.
2. Click on the **Dynamic Services** tab.

Right click and select **Trigger Update of RPC Server Information** to refresh the displayed content.

Every RPC Connection is displayed with the following information:

- **Used Address** - IP address used by the dynamic service.
- **Proto** - Protocol used by the dynamic service.
- **Port** - Port used by the dynamic service.
- **Service Name** - Name and Number of the dynamic service.
- **Service Desc** - Description for the dynamic service.
- **Target Address** - IP address where the dynamic service connects to.
- **Expires** - Displays when the dynamic service connection expires.
- **Used** - Expired time since last usage.
- **Updated** - Expired time since last information update.
- **Source Address** - IP address for which the dynamic service entry is valid for (entry 0.0.0.0 indicates all IP addresses).
- **Source Mask** - Netmask which the dynamic service entry is valid for.

© Barracuda Networks Inc., 2021 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.