

How to Configure the ONCRPC Plugin Module

<https://campus.barracuda.com/doc/73719245/>

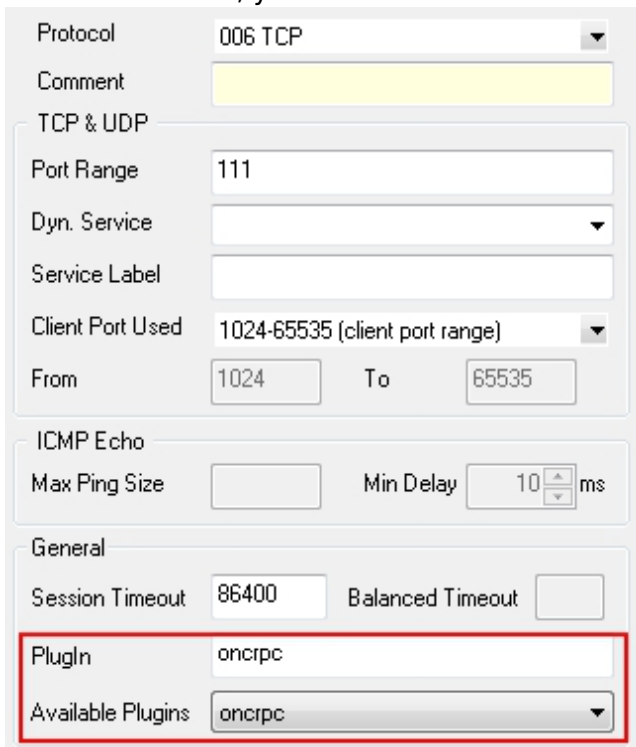
ONCRPC, also known as SUNRPC allows services to register on a server, which then makes them available on dynamic TCP/UDP ports. By means of this mechanism, ports required for specific purposes (for example NFS), can be dynamically enabled without weakening a strict security policy.

The heart of ONCRPC is the so-called portmapper, an interface responsible for allocation of ports and protocols to services. If an application demands a certain service, a request is sent to the portmapper. The portmapper's answer contains the required port and protocol, which are then used for connection establishment.

Configuring Passive ONCRPC

Step 1. Enable Access to the Portmapper

1. Go to the **CONFIGURATION** tab and click **Simple Configuration**.
2. In the **Operational Configuration** table, click **Ruleset** under the **Firewall** section. The **Configuration Overview/Forwarding Rules** page opens.
3. Create a **PASS** rule for portmapper access using a corresponding service object.
4. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **111**.
5. Last but not least, you need to select **ONCRPC** in the **Available Plugins** drop-down menu.



Protocol	006 TCP		
Comment			
TCP & UDP			
Port Range	111		
Dyn. Service			
Service Label			
Client Port Used	1024-65535 (client port range)		
From	1024	To	65535
ICMP Echo			
Max Ping Size		Min Delay	10 ms
General			
Session Timeout	86400	Balanced Timeout	
Plugin	oncrpc		
Available Plugins	oncrpc		

Step 2. Create a Second Rule for the Required Service (For Example NFS)

1. Create a second firewall rule. Again, as mentioned in step 1, the settings for the service object are of interest.
2. In the service object, select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (which means servicename:serviceID; for example **ONCRPC:100003**).

Step 3. Check the Ruleset Hierarchy

- For successful usage of dynamic services it is mandatory to have the general rule (created during step 1) situated above the service rules (created during step 2). You can move the rules up or downwards within the ruleset by drag-and-drop.

Configuring Active ONCRPC

Step 1. Configure the RPC Server Information

1. Go to the **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Firewall Forwarding Settings** page.
2. From the **Configuration** menu on the left, select **RPC**.
3. Click **Lock**.
4. In the **Default Poll Time (secs)** field, you can define the interval for requesting RPC information from the RPC server (default: 300).
5. In the **ONC/RPC Servers** section, click the **+** icon to create a new server entry.
6. Enter a descriptive name and click **OK** to access the **ONC/RPC Servers** configuration.
7. In the **Portmapper IP** field, enter the IP address of the considered RPC server.
8. The other parameters are specified as follows:
 - **Portmapper Port [111]** – Defines the port where portmapper is listening on.
Take into consideration that the service object for the portmapper rule (created in step 2, see above section) has to match this port.
 - **Optional Source IP [0.0.0.0]** – This parameter allows you to define an explicit IP address that is used when connecting to the RPC server. This comes handy as soon you are using policy routing. The default value of *0.0.0.0* deactivates this parameter and the correct bind IP address will be specified via the routing table.
 - **Polling Time (secs)[300]** – Here the interval for requesting RPC information from the RPC server is defined.
 - **Additional Addresses (NAT)** – If you want to use NAT, enter the corresponding addresses in this section by clicking the **+** icon.
9. Click **Send Changes** and then click **Activate**.

Step 2: Enable Access to the Portmapper

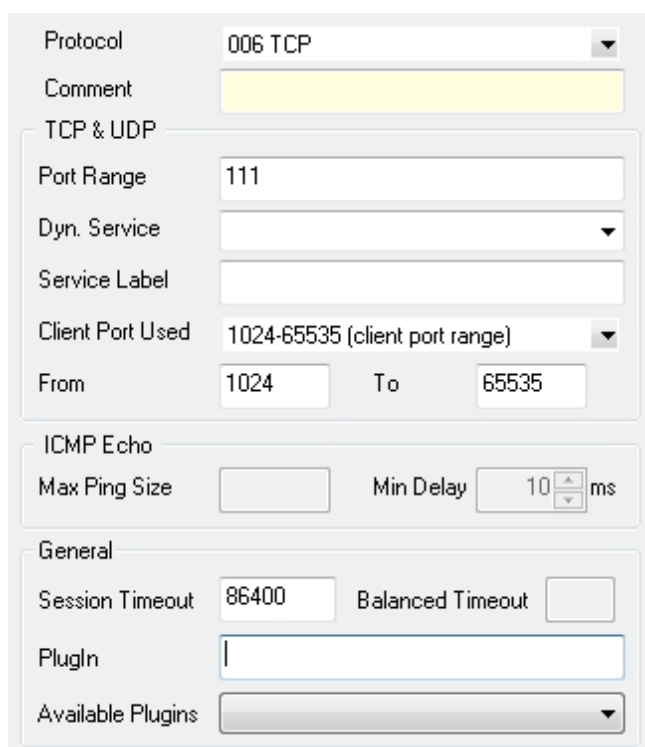
1. Create a **PASS** rule for portmapper access using a corresponding service object.

2. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to **port 111** (see figure below).

If you have specified an alternative port in the server configuration, do not forget to define this alternative port instead of the default port here.

- Do not fill in the **Plugin** field when configuring active ONCRPC!

General service object required for creating a PASS rule to enable active ONCRPC:



Protocol: 006 TCP

Comment: [Empty]

TCP & UDP

Port Range: 111

Dyn. Service: [Empty]

Service Label: [Empty]

Client Port Used: 1024-65535 (client port range)

From: 1024 To: 65535

ICMP Echo

Max Ping Size: [Empty] Min Delay: 10 ms

General

Session Timeout: 86400 Balanced Timeout: [Empty]

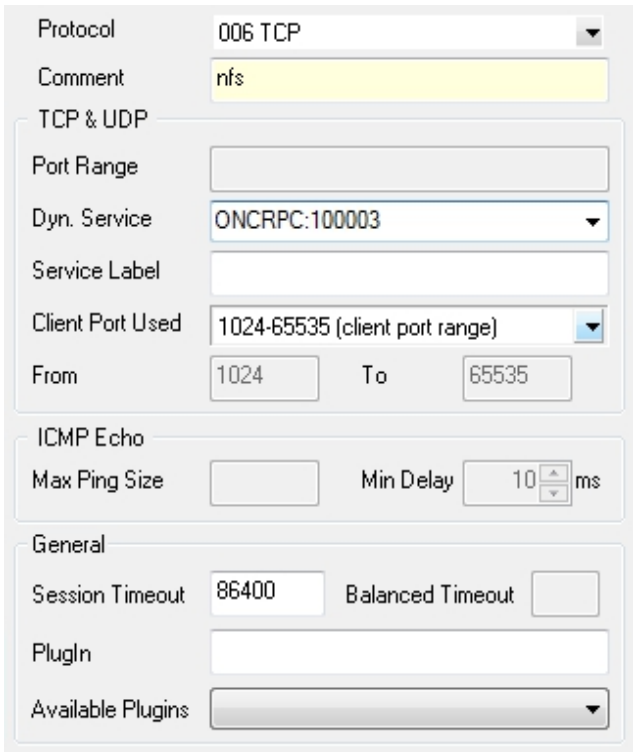
Plugin: [Empty]

Available Plugins: [Empty]

Step 3. Create a Second Rule for the Required Service (For Example NFS)

1. Create a second firewall rule. Again, as mentioned in step 1, the settings for the service object are of interest.
2. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (*servicename:serviceID*; in our example this would be *nfs:100003*).

Service object needed for enabling nfs usage via a portmapper:



The screenshot shows the configuration page for a service rule. The 'Protocol' is set to '006 TCP'. The 'Comment' field contains 'nfs'. Under the 'TCP & UDP' section, 'Port Range' is empty, 'Dyn. Service' is set to 'ONCRPC:100003', 'Service Label' is empty, 'Client Port Used' is set to '1024-65535 (client port range)', and 'From' and 'To' ports are set to '1024' and '65535' respectively. The 'ICMP Echo' section has 'Max Ping Size' empty and 'Min Delay' set to '10 ms'. The 'General' section has 'Session Timeout' set to '86400', 'Balanced Timeout' empty, 'Plugin' empty, and 'Available Plugins' empty.

Step 4: Check the Ruleset Hierarchy

- For successful usage of dynamic services it is mandatory to have the general rule (created during step 2) situated above the service rules (created during step 3). You can move the rules up or downwards within the ruleset by drag-and-drop.

Configure Active & Passive ONCRPC (recommended)

Step 1: Configure the RPC Server Information

- Configure the RPC Server information as described above in step 1 (Configure the RPC Server Information).

Step 2: Enable Access to the Portmapper

1. Create a **PASS** access rule for portmapper access using a corresponding service object.
2. When configuring the service entry, select **UDP** or **TCP** as **protocol** and set the parameter **Port Range** to **port 111**.
3. Select **oncrpc** in the **Available Plugins** drop-down menu. (see figure below).

General service object needed for creating a PASS rule to enable active & passive ONCRPC:

Protocol	017 UDP	
Comment		
TCP & UDP		
Port Range	111	
Dyn. Service		
Service Label		
Client Port Used	1024-65535 (client port range)	
From	1024	To 65535
ICMP Echo		
Max Ping Size		Min Delay 10 ms
General		
Session Timeout	60	Balanced Timeout 30
Plugin	oncrpc	
Available Plugins	oncrpc	

Step 3. Create Access Rule for the Service

1. Create a second access rule. Again, as mentioned in step 1, the settings for the service object are of interest.
2. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (*servicename:serviceID*; in our example this would be *nfs:100003*).

Service object required for enabling nfs usage via a portmapper:

Protocol	006 TCP	
Comment	nfs	
TCP & UDP		
Port Range		
Dyn. Service	ONCRPC:100003	
Service Label		
Client Port Used	1024-65535 (client port range)	
From	1024	To 65535
ICMP Echo		
Max Ping Size		Min Delay 10 ms
General		
Session Timeout	86400	Balanced Timeout
Plugin		
Available Plugins		

Step 4: Check the Ruleset Hierarchy

Verify that the access rule created in step 2 is located above the service rules created in step 3.

Figures

1. pass.jpg
2. act.jpg
3. nfs.jpg
4. act_pass.jpg
5. portmap.jpg

© Barracuda Networks Inc., 2020 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.