How to Configure the DCERPC Plugin Module

https://campus.barracuda.com/doc/43847219/

The OSF Distributed Computing Environment (DCE) is a protocol standardized by the Open Group (www.opengroup.org/dce). Analogous to the ONCRPC protocol (see: How to Configure the ONCRPC Plugin Module), DCERPC allows services to register on a server which then provides these services on dynamic TCP/UDP ports.

The most widespread application depending on DCERPC is possibly Microsoft Exchange. Besides other Microsoft products, DCERPC for example is as well used by HP Open View. Since the so-called end point mapper knows which service requires which port and protocol, the client application first sends a request to the end point mapper to determine the dynamically assigned ports. The endpoint mapper listens on a TCP/UDP port.

In this article:

- *Portmapper* is called *Endpoint Mapper* and uses TCP/UDP port 135 instead of UDP/TCP 111.
- Service identification via UUID instead of program numbers.
- Multiple services per port possible. Having multiple services on one TCP port a "pre-validation" by the firewall is required. This pre-validation checks whether at least one service offered by this port is granted by the rule set: **NO -** block; **YES -** session is granted using service name DCERPC:ANY and is subsequently analyzed further. As soon as the service is selected, the rule set is checked again whether exactly this service is permitted or not. If granted, the service name changes to the now-known name and session is active (first matching rule is used). If the service is not permitted the session is terminated.
- One service can be offered on multiple ports.
- Using UDP DCERPC offers an additional function in order to avoid arbitrary spoofed request to the RPC server.
- Service can change within a session.

Please consider the following configuration options regarding the parameter Dyn. Service when reading the guidance below as it applies to all available methods:

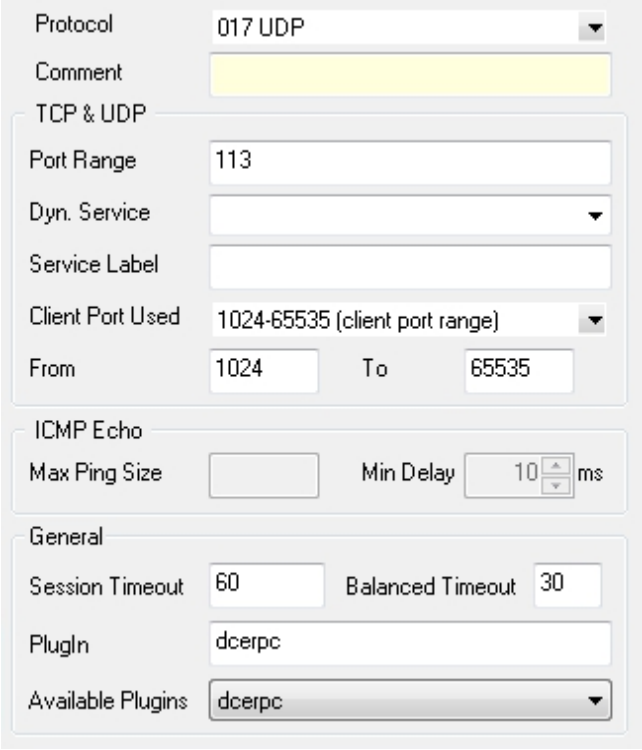
The parameter **Dyn. Service** can be configured to utilize all available services by just entering **DCERPC** into the **Dyn. Service** field. In addition to explicit creation of new service objects you may as well make use of the already existing predefined service objects, for example, service objects bound to Microsoft Exchange usage. Please consider, though, that you might possibly need to adapt the preconfigured objects due to potential requirement changes of the software.

Configuring Passive DCERPC

Step 1: Enable Access to the End Point Mapper

1. Go to the 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 end point mapper access using a corresponding service object (default service object: **DCERPC135**) (For more information on firewall rule creation, see: and:).
4. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **135**. Last but not least, you need to select **dcerpc** in the **Available Plugins** drop-down menu. (see figure below).

General service object needed for creating a PASS rule to enable passive DCERPC:

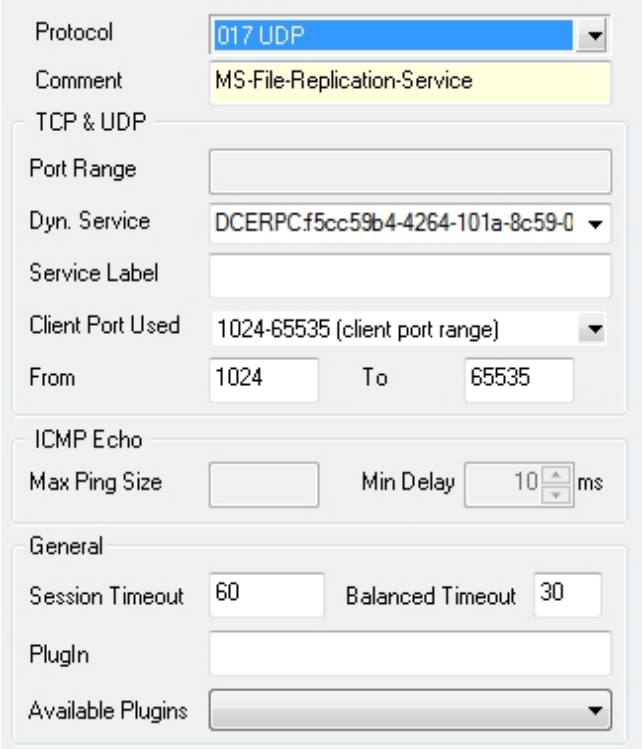


Step 2: Create a Second Rule for the Required Service (For Example MS Exchange)

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:**UUID**; see figure below).

Service object needed for enabling MS-File Replication Service usage via an end point

mapper:



Step 3: Check the Ruleset Hierarchy

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

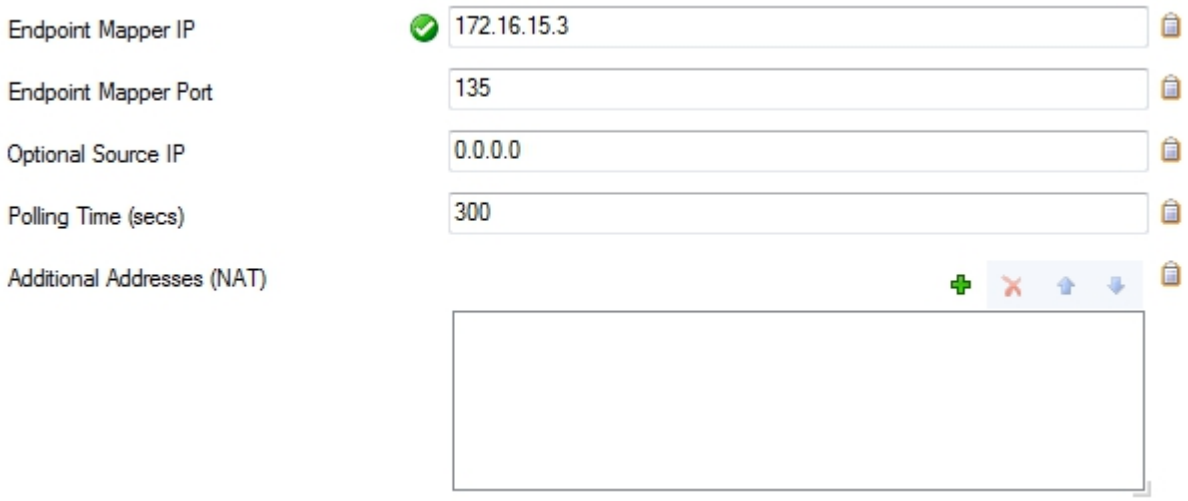
Configuring Active DCERPC

Step 1: Configure the RPC Server Information

The RPC server information is configured via the **RPC Handling** tab of the **Firewall Forwarding Settings**:

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **Firewall Forwarding Settings**.
2. From the **Configuration** menu on the left, select **RPC Handling**.
3. Click **Lock**.
4. In the **DCE/RPC Servers** section, click the **+** icon to create a new server entry (Via **Edit** you may modify an already existing server entry).
5. Enter a descriptive name and click **OK**.
6. Make sure that the **Endpoint Mapper Port** field is set to *135*. (For more information on RPC

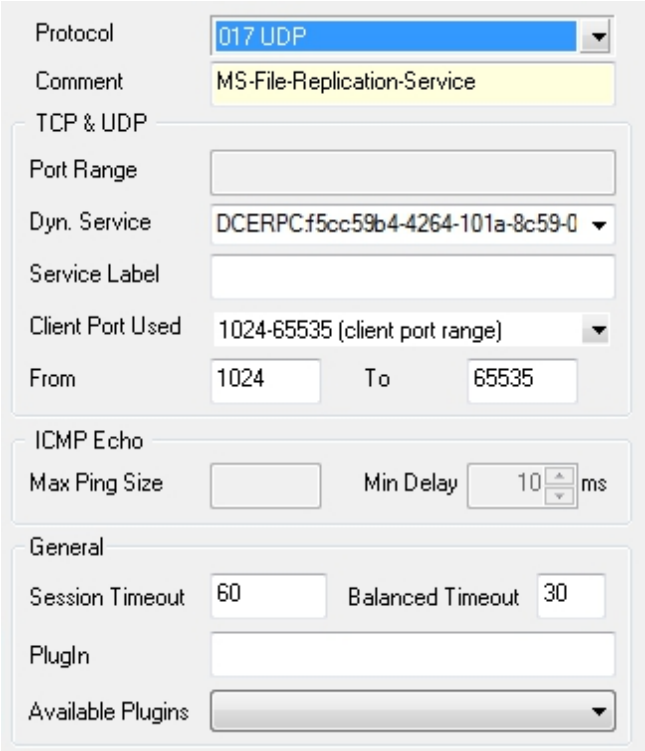
server parameters, see step 1 in How to Configure the ONCRPC Plugin Module.)



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 *135* (see figure below).

General Service Object needed for creating a PASS rule to enable active DCERPC:



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 DCERPC!

Step 3: Create a Second Rule for the Required Service (For Example MS Exchange)

- Create a second firewall rule. Again, as mentioned in step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (servicename:*UUID*).

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.

Configuring Active & Passive DCERPC (recommended)

Step 1: Configure the RPC Server Information

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Firewall Forwarding Settings**.
2. From the **Configuration** menu on the left, select **RPC Handling**.
3. Click **Lock**.
4. Perform the configuration analogue to the one mentioned under **Configuring Active DCERPC**, step 1.

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 *135*.
3. Last but not least, you need to select **DCERPC** in the **Available Plugins** drop-down menu.

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

- Create a second firewall rule. Again, as mentioned in step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (servicename:*UUID*).

Step 4: Check the Ruleset Hierarchy

- For successful usage of dynamic services it is mandatory to have the general rule (created

during step 2) is situated above the service rules (created during step 3). You can move the rules up or downwards within the ruleset by drag-and-drop.

Figures

1. pass_dce.jpg
2. dce_rep.jpg
3. act_dce.jpg
4. fw_dce.jpg