# How to Configure the DCERPC Plugin Module

https://campus.barracuda.com/doc/96026222/

There are many DCERPC applications, such as Microsoft Exchange or HP Open View. As with the ONCRPC protocol, the DCERPC allows services to register on a server, which then provides these services on dynamic TCP/UDP ports. For the firewall to know which ports to open, you must configure an Endpoint Mapper. To open a dynamic port, the client application first sends a request to the Endpoint Mapper to receive the port. This port is then opened automatically on the firewall to allow the connection.

## What’s the Difference to ONCRPC?

- **Portmapper** is called **Endpoint Mapper** and uses TCP/UDP port 135 instead of UDP/TCP 111.
- Service identification is via UUID instead of program numbers.
- Multiple services per port are possible. Having multiple services on one TCP port is a required firewall pre-validation. This pre-validation checks whether at least one service offered by this port is granted by the ruleset. **NO** means the service is blocked. **YES** means the session is granted using service name DCERPC:ANY and is subsequently analyzed further. As soon as the service is selected, the ruleset is checked again whether exactly this service is permitted or not. If granted, the service name changes to the now-known name and the 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 requests to the RPC server.
- Service can change within a session.

**Consider the following configuration options regarding the parameter Dyn. Service when reading the guidance below. 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 explicitly creating new service objects, you can also make use of the existing predefined service objects, for example, service objects bound to Microsoft Exchange usage. However, you may need to adapt the preconfigured objects due to potential requirement changes of the software.

## Configuring Passive DCERPC

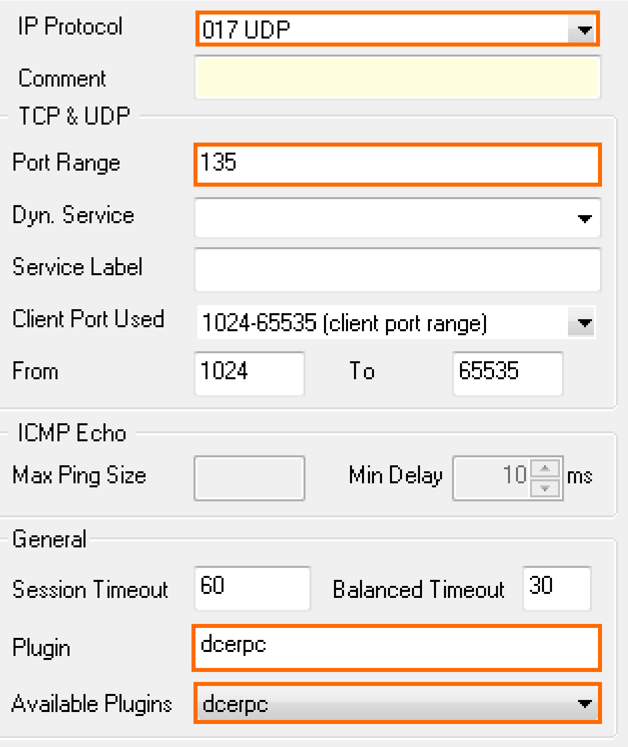
#### Step 1. Enable Access to the Endpoint Mapper

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall >**

**Forwarding Rules**.

2. Click **Lock**.
3. In the left menu, click **Services**.
4. Right-click in the main area and select **New**. The **Edit/Create Service Object** window opens.
5. Click **New Object** and add an entry for UDP or TCP with the **Port Range** set to 135.
6. From the **Available Plugins** drop-down list, select **dcerpc**.
7. Click **OK**.
8. Click **OK**.
9. Create a pass access rule using the service object you just created.
10. Click **Send Changes** and **Activate**.

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



IP Protocol: 017 UDP

Comment:

TCP & UDP

Port Range: 135

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

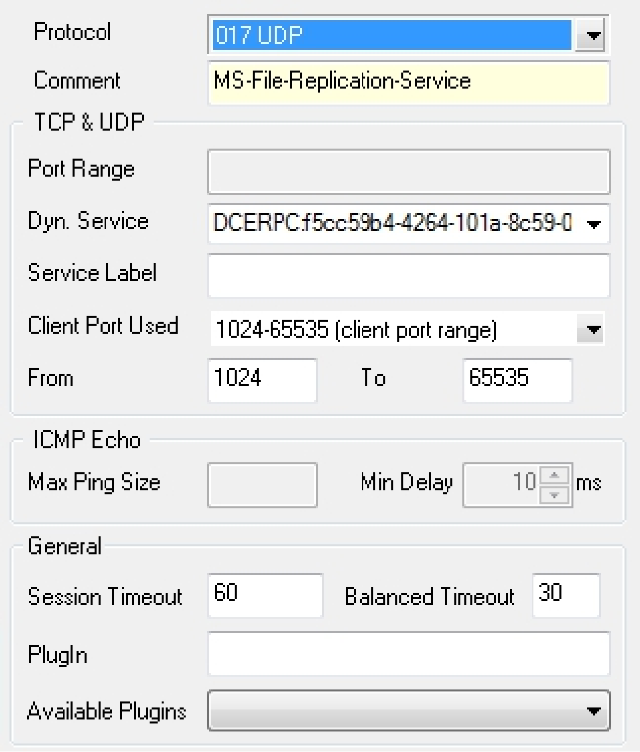
Plugin: dcerpc

Available Plugins: dcerpc

#### Step 2. Create a Second Rule for the Required Service (e.g., MS Exchange)

1. Create a second access rule.
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 Endpoint Mapper:



Protocol: 017 UDP

Comment: MS-File-Replication-Service

TCP & UDP

Port Range:

Dyn. Service: DCERPC:f5cc59b4-4264-101a-8c59-0

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:

Available Plugins:

#### Step 3: Check the Ruleset Hierarchy

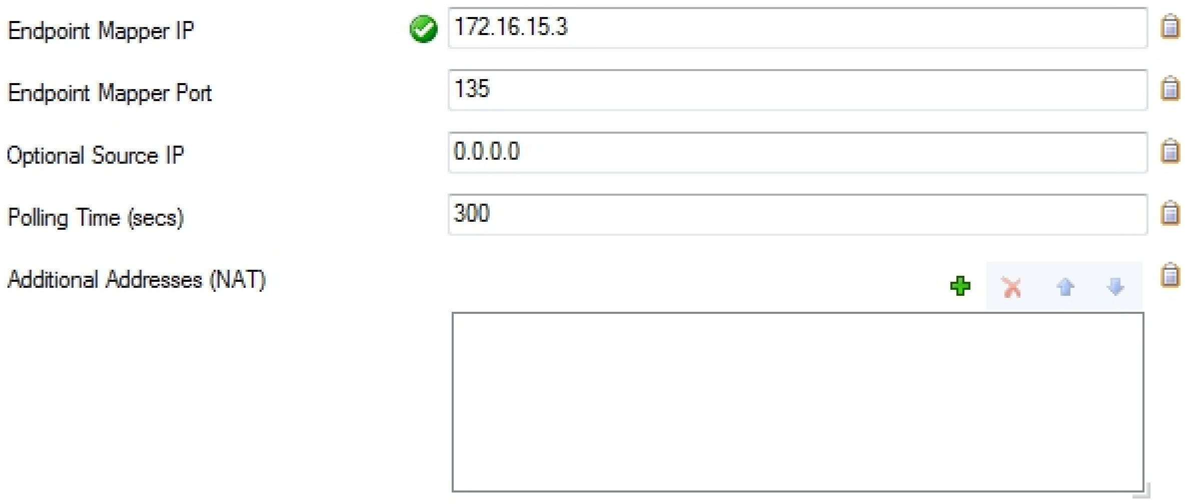
- To use dynamic services successfully, the general rule (created during Step 1) must be situated above the service rules (created during Step 2). You can drag the rules up or down within the ruleset.

## 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 Tr ee** > **Box** > **Assigned Services** > **Firewall** > **Firewall Forwarding Settings**.
2. In the left menu, 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 existing server entry).
5. Enter a **Name**.
6. Click **OK**.
7. Verify 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.

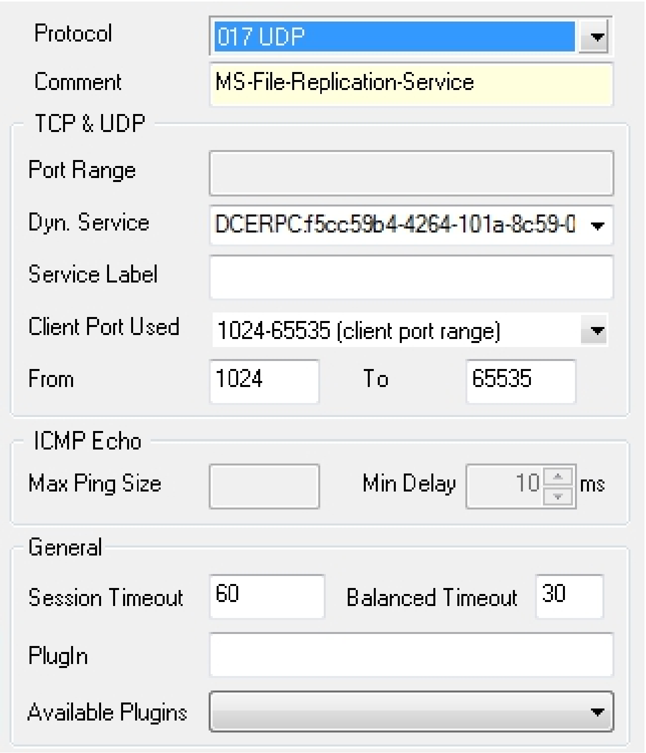


| | |
|---|---|
| Endpoint Mapper IP | 172.16.15.3 |
| Endpoint Mapper Port | 135 |
| Optional Source IP | 0.0.0.0 |
| Polling Time (secs) | 300 |
| Additional Addresses (NAT) | |

**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 either **UDP** or **TCP** as **protocol** and set the parameter **Port Range** to port 135.

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



| | | | |
|---|---|---|---|
| Protocol | 017 UDP | | |
| Comment | MS-File-Replication-Service | | |
| TCP & UDP | | | |
| Port Range | | | |
| Dyn. Service | DCERPC:f5cc59b4-4264-101a-8c59-0 | | |
| 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 | | | |
| Available Plugins | | | |

If you have specified an alternative port in the server configuration, 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 (e.g., MS Exchange)

- Create a second access rule. As mentioned in Step 1, the settings for the service object are important. 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

- To use dynamic services successfully, the general rule (created during Step 2) must be situated above the service rules (created during Step 3). You can drag the rules up or down within the ruleset.

## Configuring Active & Passive DCERPC (recommended)

#### Step 1. Configure the RPC Server Information

1. Go to **CONFIGURATION** > **Configuration Tr ee** > **Box** > **Assigned Services** > **Firewall** > **Firewall Forwarding Settings**.
2. From the left menu, select **RPC Handling**.
3. Click **Lock**.
4. Perform the configuration according to the one mentioned in Step 1 of **Configuring Active DCERPC**.

#### 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 either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port 135.
3. Select **DCERPC** in the **Available Plugins** drop-down list.

#### Step 3. Create an Access Rule for the Required Service (e.g., NFS)

Create a second access rule. As mentioned in Step 1, the settings for the service object are important. 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

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

## Figures