RPC Firewall Plugin Modules

https://campus.barracuda.com/doc/79462954/

Some applications, such as RPC or FTP, do not communicate between two IPs over well defined ports. The service opens dynamic ports making it impossible to use static port based access rules to handle this type of traffic. For example when an FTP connection is created - after the initial control dialog over port 21, the client and the server use another random port from 1024 through 65535 to send and receive data. The firewall has two possibilities to handle this: either it opens all higher ports, which is not really suitable for a secure firewall, or it listens to the two FTP partners and opens the dynamic port agreed upon in the initial control dialog. The firewall services uses plugin modules to listen for these dynamically allocated ports for the following services:

The Barracuda CloudGen Firewall 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.

ONCRPC Plugin Module

ONCRPC, formerly known as SUNRPC allows services to register on a server, which then makes them available on dynamic TCP/UDP ports.

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.

For more information, see How to Configure the ONCRPC Plugin Module.

DCRPC Plugin Module

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.

For more information, see How to Configure the DCERPC Plugin Module.

Monitoring

The monitoring of RPC takes place in the **Dynamic Services** tab of the Barracuda CloudGen Firewall 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