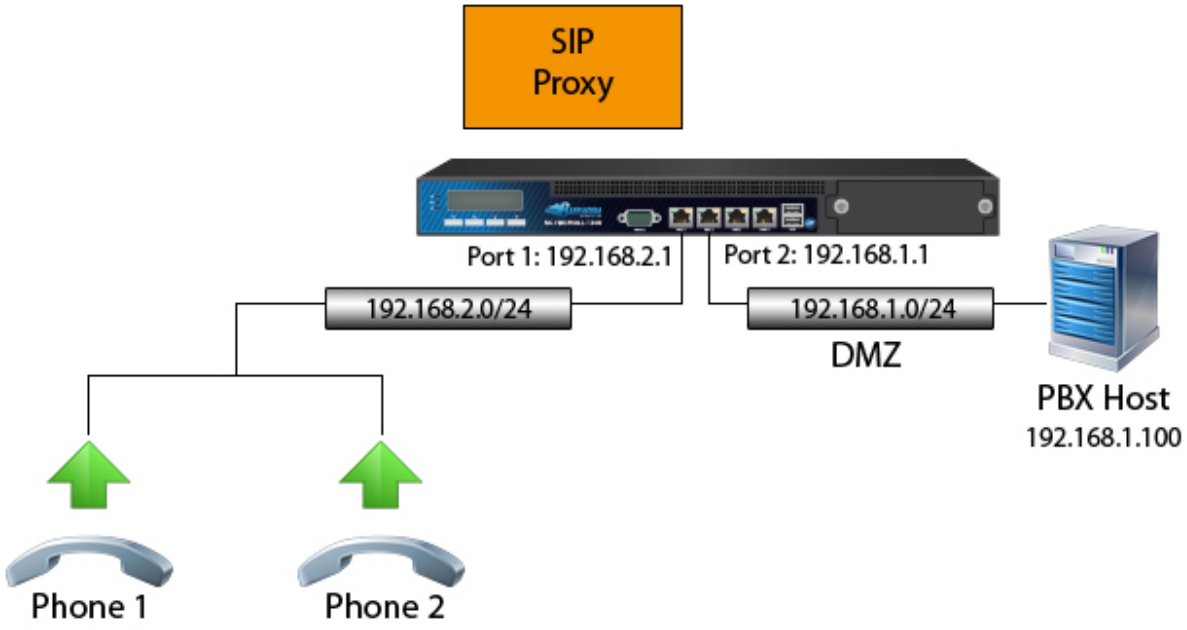
How to Configure the SIP Proxy

https://campus.barracuda.com/doc/41116197/

To allow SIP-based VoIP communication to pass the firewall, you can configure the built-in SIP proxy for the Barracuda NG Firewall. The SIP proxy dynamically opens all necessary RTP ports for successful SIP communication through a Barracuda NG Firewall. You must also create a forwarding firewall rule that redirects traffic to the SIP proxy.



In this article:

Step 1. Create an App Redirect Firewall Rule

Create an App Redirect rule to forward all SIP traffic to the SIP proxy service. For example, to create this rule for the example setup that is displayed in the illustration above, use the following settings. Note that the network ranges the SIP phones reside in must be *10.0.0.0/8*, *172.16.0.0/12* or *192.168.0.0/16*.

- **Action**: **App Redirect**
- **Source**: `192.168.2.0/24` (The subnet that the SIP phones reside in)

- **Service**: **SIPcf**
- **Destination**: `192.168.1.100` (The IP address of the PBX host)
- **Redirection Local Address**: `192.168.2.1:5060` (The listening IP address for the virtual server of the subnet that the SIP phones reside in)

For more information on creating an App Redirect firewall rule, see How to Create an App Redirect Firewall Rule.

Step 2. Configure the SIP Proxy

In the forwarding firewall settings, configure the SIP proxy.

1. Open the **Forwarding Settings** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Settings**).
2. From the **Configuration** menu in the left pane, click **VoIP/SIP**.
3. Click **Lock**.
4. In the **SIP Proxy Settings** section, select the **Enable the SIP Proxy** check box.
5. Configure the remaining **SIP Proxy Settings**. For more information on these settings, see the following SIP Proxy Settings section.
6. Click **Send Changes** and **Activate**.

Step 3. SIP Proxy Settings

Some of the settings are only available in advanced configuration mode. To access this mode, expand the **Configuration Mode** menu in the left navigation pane and then click **Switch to Advanced**.

Setting	Description
Enable the SIP Proxy	Enables the SIP proxy. Do not use the SIP plugin module and SIP proxy simultaneously. Barracuda Networks recommends using the SIP proxy instead of the SIP firewall plugin module. For a Barracuda NG Firewall version 5.4.2 and later, the SIP proxy is disabled by default if the appliance is newly installed or updated from a firmware version that did not offer the feature.

<table>
<tr><td>Allowed destinations</td><td>The IP addresses, IP ranges, and domain names that the user agents are allowed to contact. Alternatively, you can leave this field empty and restrict the destinations through forwarding rules.
For domain names, you can use wildcard characters such as asterisks (*), question marks (?), and square brackets ([ ]).
Entering <code>0.0.0.0/0</code> allows any IP address but no domain name. If you want to allow any domain name, add an entry with just an asterisk (*). If the list is empty, no restrictions are applied (this does not override the forwarding rules). If you want to forbid all destinations, block the SIP port (UDP+TCP 5060) in the forwarding rules instead.</td></tr>
<tr><td>Trust Connection IP</td><td>Specifies whether the SIP proxy trusts the IP address in the connection IP field contained within the SDP header of SIP packets. This header field usually contains the source IP address for the packet. However, this IP address can be invalid in NAT'd networks, which would effectively block the SIP traffic. You can select one of the following modes:
• Yes – The IP address in the SDP header is always be trusted. Works only if the clients are not NAT'd.
• No – The IP address in the SDP header is not trusted. This can fix problems with NAT'd phone devices but might break traffic for devices with a public IP address residing behind another intermediate SIP proxy.
•
Automatic – The mode is detected automatically for each client. However, the Automatic mode cannot always detect the correct setting. If you encounter connection problems with traffic through the SIP proxy, try the other Trust Connection IP modes. The following table lists the modes that you can use for some specific scenarios that do not work with Automatic mode:
<table>
<tr><th>Scenario</th><th>Trust Connection IP Setting</th></tr>
<tr><td>Phone ↔ Firewall + SIP Proxy #1 ↔ Firewall + SIP Proxy #2 ↔ Phone or Phone System</td><td>Yes in SIP Proxy #1</td></tr>
<tr><td>Phone ↔ Router with Symmetric NAT but no SIP Proxy ↔ Barracuda SIP Proxy ↔ Phone or Phone System</td><td>No</td></tr>
<tr><td>Phone ↔ External Vendor's SIP Proxy or Phone System without RTP Forwarding ↔ Barracuda SIP Proxy ↔ Phone or Phone System</td><td>Yes</td></tr>
<tr><td>Phone ↔ Barracuda SIP Proxy ↔ Phone System ↔ Phone</td><td>Yes</td></tr>
</table></td></tr>
<tr><td>No. of Child Processes</td><td>(Advanced Configuration Mode) The number of SIP processes to be created for each available network port and interface.

For example, the Barracuda NG Firewall F400 has seven network ports and the number of child processes is set to 4, so the SIP proxy starts four processes for each port. Because SIP requires TCP and UDP sessions for communication, there will be a total of 56 active SIP proxy processes (7 x 4 x 2 = 56).</td></tr>
<tr><td>Server Signature</td><td>(Advanced Configuration Mode) The custom signature to be encapsulated into SIP packets.</td></tr>
</table>

Allow Registration From WAN Ad	(**Advanced Configuration Mode**) Specifies if user agent clients (UACs) from WAN IP addresses are allowed to register on the SIP proxy. For security reasons, Barracuda Networks recommends that you disable this feature.
Debug Log Level	(**Advanced Configuration Mode**) Trace the SIP proxy's operations in one of three available granularity levels. If you encounter SIP proxy issues with VoIP communications, Barracuda Networks recommends that you increase the log level for further troubleshooting. • **0**: Notice - Basic log information. • **1**: Info - Medium log information. • **2**: Debug - Extensive log information. The log output is written to **Logs > *your virtual server* > *your firewall service* > sipproxy**.

Figures

1. sip_pro.jpg