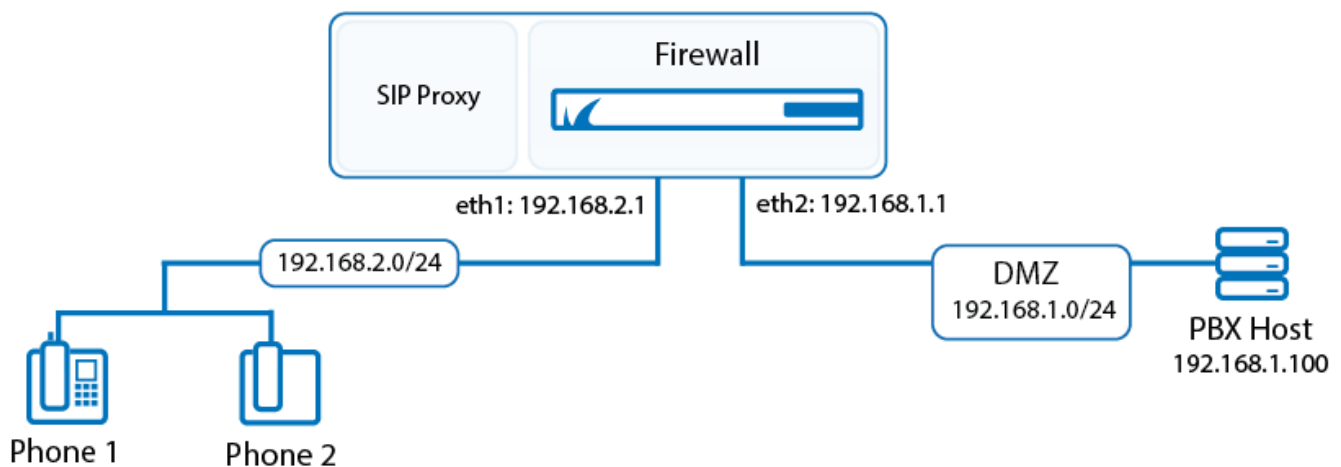


How to Configure the SIP Proxy

<https://campus.barracuda.com/doc/73697732/>

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



Step 1. Create a Redirect to Service Access Rule

Create an access 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 - Redirect to Service**
- **Source** - The subnet that the SIP phones reside in. E.g., 192.168.2.0/24
- **Redirect to Service Details - SIP**
- **Destination** - The IP address of the PBX host. E.g., 192.168.1.100

For more information on creating a Redirect to Service access rule, see [How to Create a Redirect-to-Service Access Rule](#).

Step 2. Configure the SIP Proxy

1. Go to **NETWORK > VoIP**.
2. In the **SIP Proxy** section, set **Enable SIP Proxy** to **Yes**.

3. Select an option for **Trust Connection IP** to specify whether the SIP proxy trusts the IP address in the connection IP field contained within the SDP header of SIP packets:

- **Automatic** – The mode is detected automatically for each client. However, if you encounter connection problems with traffic through the SIP proxy, try the other modes. The following table lists the modes that you can use for some specific scenarios that do not work with **Automatic** mode:

Scenario	Trust Connection IP Setting
Phone ↔ Firewall + SIP Proxy #1 ↔ Firewall + SIP Proxy #2 ↔ Phone or Phone System	Yes in SIP Proxy #1
Phone ↔ Router with Symmetric NAT but no SIP Proxy ↔ Barracuda SIP Proxy ↔ Phone or Phone System	No
Phone ↔ External Vendor's SIP Proxy or Phone System without RTP Forwarding ↔ Barracuda SIP Proxy ↔ Phone or Phone System	Yes
Phone ↔ Barracuda SIP Proxy ↔ Phone System ↔ Phone	Yes

- **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.

4. To restrict access to specific addresses, or to allow TLS connections,

1. Click **Show Advanced Options**.
2. In the **Allowed Destinations** field, add 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 access rules. For domain names, you can use wildcard characters such as asterisks (*), question marks (?), and square brackets ([]). Entering 0.0.0.0/0 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.
3. To allow TLS connections on TCP port 5061,
 1. Set **Use TLS** to **Yes**.
 2. Upload the certificate in the **SIP Proxy Certificates** section.
 3. From the **Accepted TLS Protocols** drop-down list, select which TLS protocols should be accepted by the SIP proxy.
 4. Select the **Certificate Security Level**.

5. Click **Save**.

Figures

1. fw_sip_proxy.png

© Barracuda Networks Inc., 2024 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.