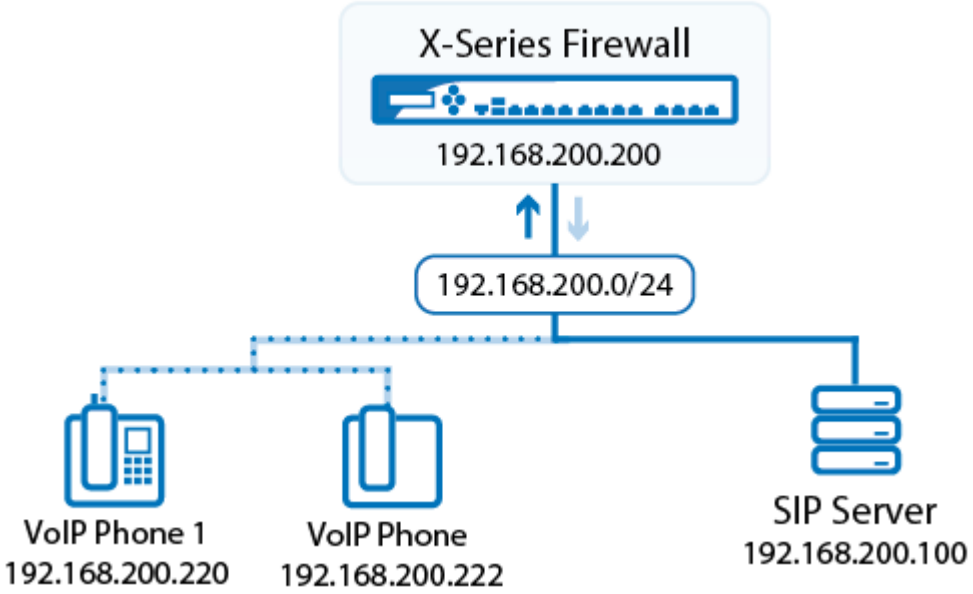
Example - Allowing SIP-based VoIP Traffic

https://campus.barracuda.com/doc/13861512/

This article provides the following examples of how to configure the Barracuda NextGen Firewall X-Series to allow SIP-based VoIP traffic:

- Allowing SIP-based VoIP Traffic for VoIP Phones – Steps for configuring access rules for VoIP phones that use the same network subnet as the internal SIP server. The VoIP phones and SIP server are located in the the 192.168.200.0/24 network.
- Allowing SIP-based VoIP Traffic for Barracuda Phone System – Steps for creating the access rules and network object required to allow SIP-based VoIP traffic when using Barracuda Phone System with the NextGen Firewall X-Series.



Allowing SIP-based VoIP Traffic for VoIP Phones

Create a forwarding access rule that redirects traffic to the internal SIP proxy of the X-Series Firewall. The SIP proxy dynamically opens all necessary RTP ports for successful SIP communication through the firewall. You must also create a separate access rule to allow traffic from the Internet to the SIP proxy.

> On the X-Series Firewall version 6.5.0 and above, the required LAN-2-INTERNET-SIP and INTERNET-2-LAN-SIPfirewall access rules are preconfigured. However, when upgrading from older firmware releases, you might have to create new rules or edit and configure existing ones.

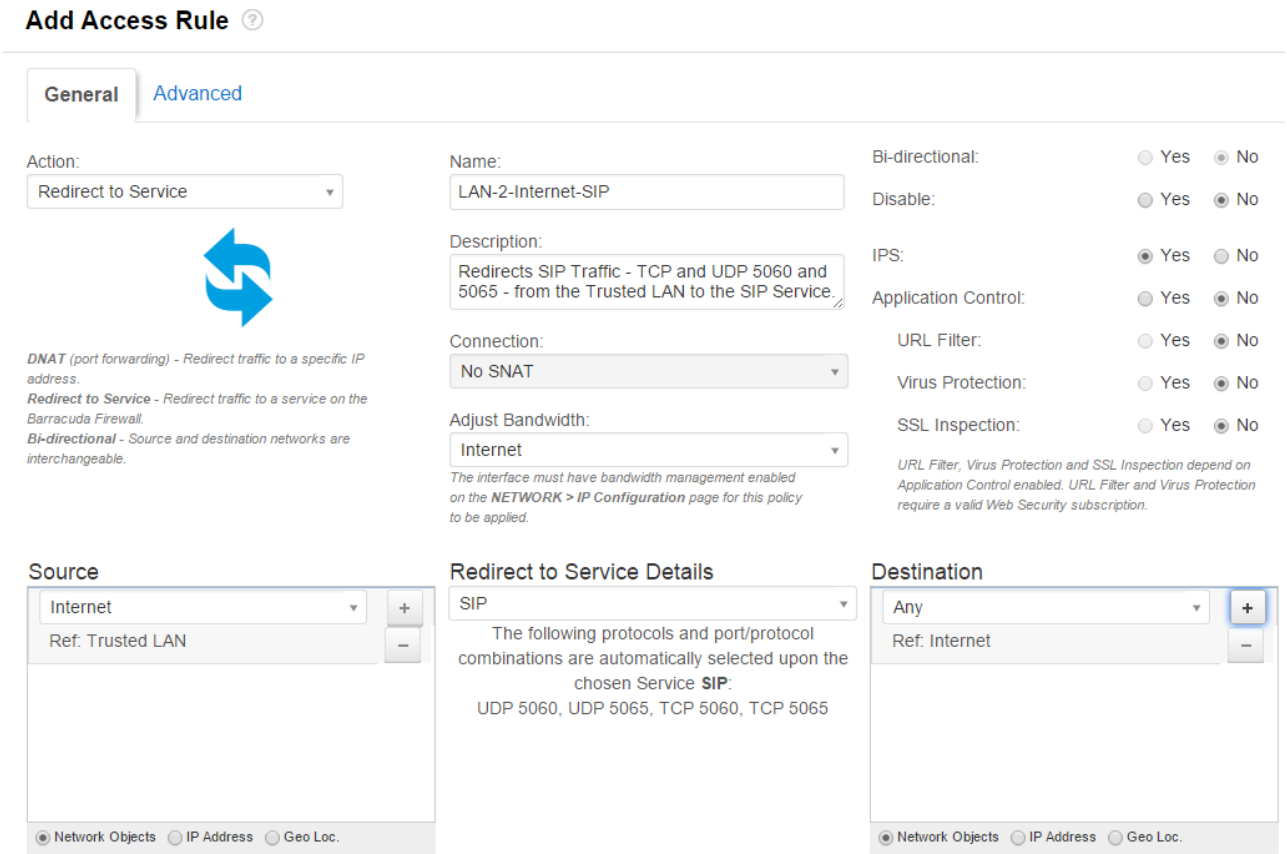
Step 1. Configure an Access Rule for the Connection from the SIP Server to Internet

To let SIP-based VoIP communication pass the firewall, create a forwarding firewall access rule that redirects traffic to the SIP proxy. You can create a new access rule or edit an existing rule. This example edits the LAN-2-INTERNET-SIP rule.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Edit the LAN-2-INTERNET-SIP rule. Ensure that the rule is enabled and that the following settings are specified:

Action	Source	Destination	Redirected To
Redirect to Service	**Trusted LAN**	**Internet**	**SIP**

In this rule, the **Source** includes the SIP server and the phones. The **Destination** specifies the destination of the SIP network traffic that is allowed. Usually, the destination is the public IP address of your SIP provider. Here, **Destination** is the predefined **Internet** network object, but you can also enter the network address of your SIP provider.



3. At the top of the **Edit Access Rule** window, click **Save**.

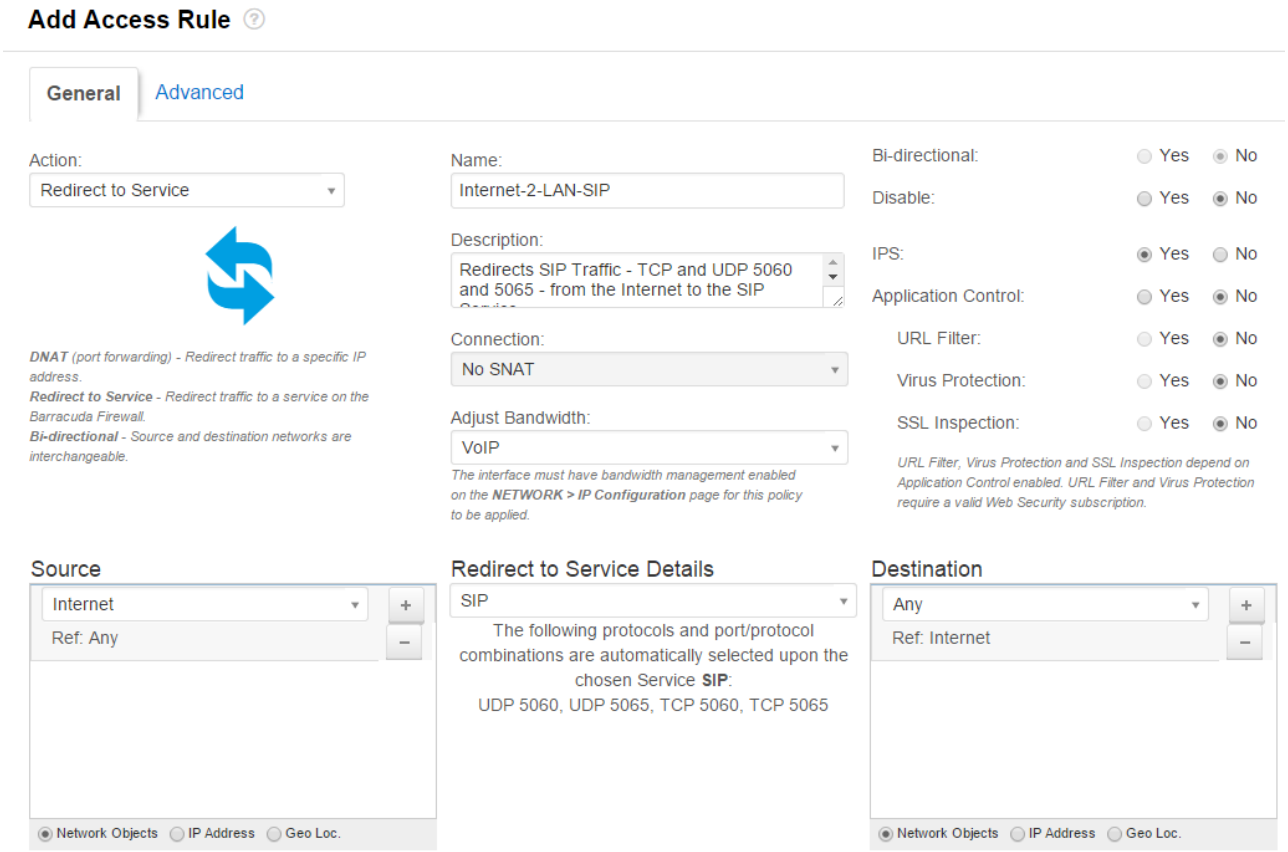
Step 2. Configure an Access Rule for the Connection from the Internet to the SIP Server

Configure a separate forwarding access rule to allow connections from the Internet to the SIP server. You can create a new access rule or edit an existing rule. This example edits the INTERNET-2-LAN-SIPrule.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Edit the INTERNET-2-LAN-SIP rule. Ensure that the rule is enabled and that the following settings are specified:

Action	Source	Destination	Redirected To
Redirect to Service	**Any**	**Internet**	**SIP**

The **Source** specifies the origin of the network traffic that should be allowed. The **Destination** specifies the public IP address that is allowed to receive SIP traffic.



3. At the top of the **Edit Access Rule** window, click **Save**.

Step 3. Verify the Order of the Access Rules

Because rules are processed from top to bottom in the rule set, arrange your rules in the correct order. You must especially ensure that your rules are placed above the BLOCKALL rule; otherwise, the rules are blocked.

After adjusting the order of rules in the rule set, click **Save**.

Allowing SIP-based VoIP Traffic for the Barracuda Phone System

When using Barracuda Phone System with the X-Series Firewall, you must create two firewall access rules to allow SIP-based VoIP traffic from the Internet to the Phone System and vice versa. For the access rule that allows SIP-based VoIP traffic from the Phone System to the Internet, you must create a connection object that does not use port address translation (PAT) .

Step 1. Create an Access Rule for the Connection from the Internet to the Barracuda Phone System

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule**.
3. In the **Add Access Rule** window, enter a name and description for the rule and then specify the following settings:

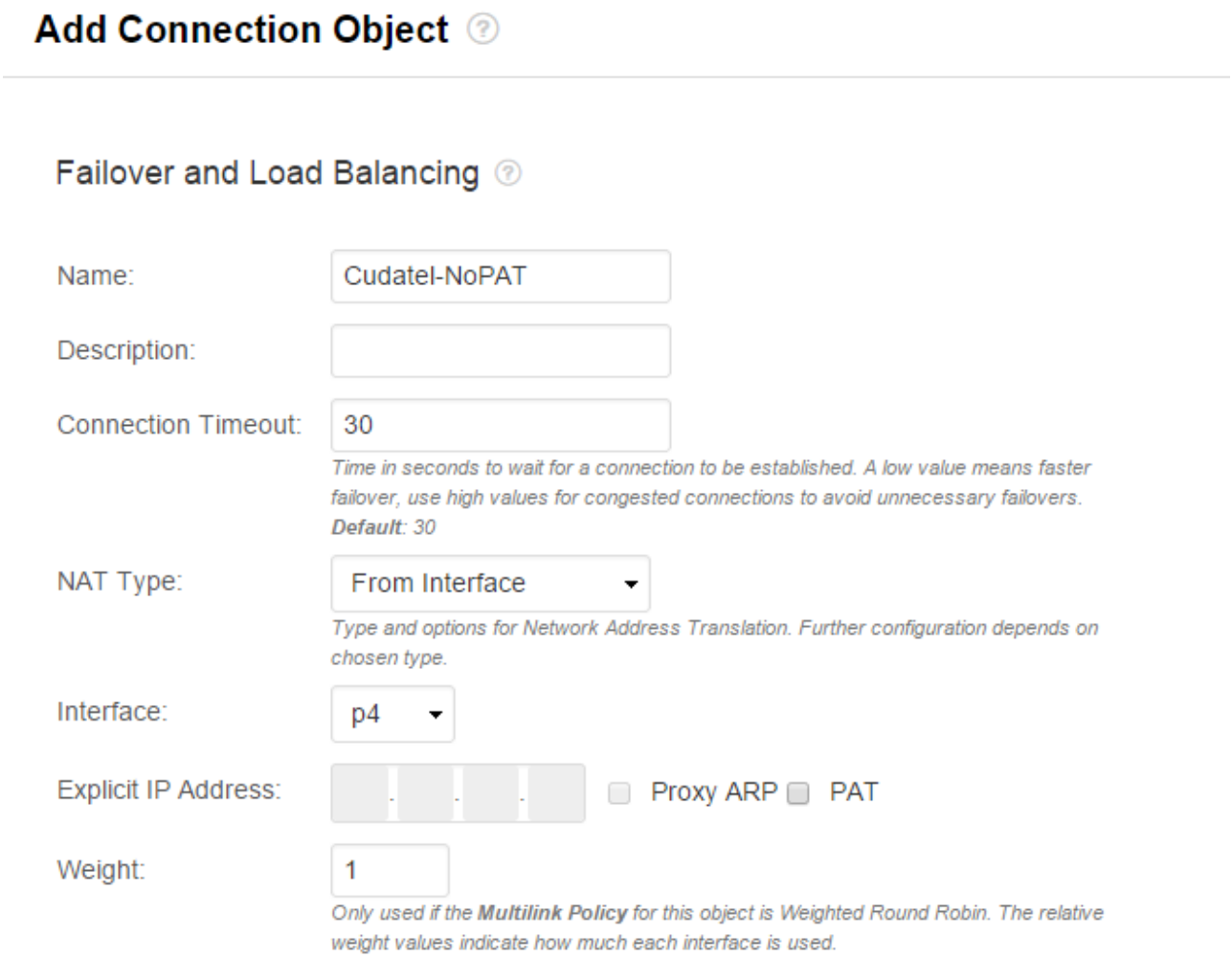
Action	Connection	Source	Network Services	Destination	Redirected To
DNAT	**No SNAT**	**Any**	**SIP**	Public IP address of the X-Series Firewall.	Barracuda Phone System IP address.

4. Click **Save**.

Step 2. Create a Connection Object

1. Go to the **FIREWALL > Connection Objects** page.
2. Click **Add Connection Object**.
3. In the **Add Connection Object** window, enter a name and description for the object and then specify the following settings:

NAT Type	Interface	PAT
From Interface	Select your WAN interface.	Clear the check box.



4. Click **Save**.

Step 3. Create an Access Rule for the Connection from the Barracuda Phone System to the Internet

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule**.
3. In the **Add Access Rule** window, enter a name and description for the rule and then specify the following settings:

Action	Connection	Source	Network Services	Destination
Allow	Select the connection object that you created.	The Barracuda Phone System IP address.	**SIP**	**Any**

4. Click **Save**.

Figures