How to Configure the SIP Plugin Module

https://campus.barracuda.com/doc/46209440/

Barracuda Networks recommends to use the SIP Proxy instead of the SIP Plugin Module. For more information how to configure the SIP proxy, see: How to Configure the SIP Proxy

This article describes how to install and configure the settings for SIP protocol handling in context with the Barracuda NextGen Firewall F-Series VoIP service. SIP firewall traversal and NAT is supported by the Barracuda NextGen Firewall F-Series service plugin.

In this article:

The Barracuda NextGen Firewall F-Series decodes the SIP packets and opens and closes firewall pinholes for voice media connections. Due to the dynamic nature of this protocol, a table of all active calls is held in memory. This table contains the negotiated media connections, the SIP transactions for the call signalling, and the calls. When a SIP packet passes the firewall, the state of the table is altered accordingly. The SIP plugin supports SIP signalling over UDP/IP packets. The default port for SIP signalling connection is UDP port 5060.

SIP-related Parameters

SIP Transaction Settings

To specify the SIP transaction settings for the Barracuda NextGen Firewall F-Series, proceed with the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**.
2. In the left menu. click the **Global Limits**.
3. Click **Lock**.
4. In the **Access Cache** section, set the value for **Max. SIP Transactions**.
   A SIP transaction is started with a SIP request packet. In reply of a SIP request a SIP response packed is generated and sent to the address that was specified in the request. The lifetime of a SIP transaction does not end with the reception of a response message. Instead a timer is started that allows the SIP signalling endpoints to handle retransmissions of any SIP packets. The SIP transaction can be discarded after the timer has expired (min: 64; max: 8192; default: 512).
5. Click **Send Changes** and **Activate**.

SIP Transaction Timeout

To define SIP transaction timeouts, proceed with the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Settings**.
2. Click **Lock**.
3. In the left menu, click the **Voip/SIP**
   - **INVITE Timeout (csec):** The invite timeout is the timeout of an *INVITE* transaction. If a reply to this request is received after the invite timeout has expired then the reply is discarded. This value can also be set in the SIP service object by the *toInvite* plugin parameter (default: 3200).
   - **ACK Timeout (csec):** The ACK timeout is the timeout of a replied or acknowledged *INVITE* transaction after the transaction is discarded. This value can also be set in the SIP service object by the *toAck* plugin parameter (default: 3200).
   - **Reply Timeout (csec):** The reply timeout defines how long the firewall will wait for a reply of a *non-invite* transaction. This value can also be set in the SIP service object by the *toReply* plugin parameter (default: 400).
   - **Transaction Timeout (csec):** The transaction timeout is the timeout of a replied *non-invite* transaction. This value can also be set in the SIP service object by the *toTrans* plugin parameter (default: 500).
     All timeout values are set in hundredth of seconds):
4. Click **Send Changes** and **Activate**.

Enable SIP

To enable the SIP firewall plugin create a firewall rule with a SIP enabled service object. When creating this service object set the **Protocol** to **017 UDP** and the **Port Range** to **5060**. When your equipment uses different ports for the SIP protocol you are expected to enter these ports instead. In the firewall rule creation window, set the **Plugin** field to **sip** to finish the **Service Entry Parameters** settings. Here you can also set additional parameters for the SIP plugin by appending plugin parameters in a whitespace separated list:

- **toInvite –** Example: "*sip toInvite=3200*" sets the invite timeout to 32 seconds (see SIP Timeouts).
- **toAck –** Example: "*sip toAck=3200*" sets the acknowledge timeout to 32 seconds (see SIP Timeouts).
- **toReply –** Example**:** "*sip toReply=400*" sets the reply timeout to 4 seconds (see SIP Timeouts).
- **toTrans –** Example: "*sip toTrans=500*" sets the transaction timeout to 5 seconds (see SIP Timeouts).
- **nonat –** Example: "*sip nonat=1*" disables network address translation handling for the sip plugin.
- **srvname –** Example: "*sip srvname=voip*" sets the service name for the RTP rule lookup to

"*RTP:voip*". The default value is "*RTP:SIP*".

- **via –** Example: "*sip via="SIP/2.0/UDP 172.31.10.5:5060""* sets the target address for the SIP reply message to *172.31.10.5 UDP* port *5060*. This parameter enables rewriting of the "*Via*" SIP header field in outgoing SIP request messages. The default is not to rewrite the "*Via*" header if no NAT is performed. In NAT configurations the default is to use the bind address of the connection slot for the "*Via*" header. Any "*Via*" header field tags of the original message persist. This is valuable when using NAT for the SIP firewall rule to force the receiving SIP peer to send SIP reply messages to the address defined in the **via** plugin parameter. In its reply message the firewall rewrites the "*Via*" header field to the original field value from the request message. Usually the address in the **via** plugin parameter will point the SIP peer to a port on the firewall that is redirected to the internal SIP proxy. The value must be enclosed in double quotes.
- **fwdcontact –** Example: "*sip fwdcontact="<sip:proxy@gateway.extern>""* sets the contact address for sip messages in the forward direction of the firewall rule. This parameter enables rewriting of the "*Contact*" SIP header field of packets that are leaving the firewall in the forward rule direction (from source to target). This is useful for NAT setups in the outgoing rule to tell the SIP peer the target address for its SIP request messages. Usually the address in the "*fwdcontact*" plugin parameter will point the SIP peer to a port on the firewall that is redirected to the internal SIP proxy. The value must be enclosed in double quotes. The default is not to rewrite the "*Contact*" header if no NAT is performed. In NAT configurations the default is to use the bind address of the connection slot for the "*Contact*" header.
- **revcontact –** Example: "*sip revcontact="<sip:proxy@gateway.extern >""* sets the contact address for sip messages in the reverse direction of the firewall rule. This parameter enables rewriting of the "*Contact*" SIP header field of packets that are leaving the firewall in the reverse rule direction (from target to source). This is useful for NAT setups in the incoming rule to tell the SIP peer the target address for its SIP request messages. Usually the address in the "*revcontact*" plugin parameter will point the SIP peer to a port on the firewall that is redirected to the internal SIP proxy. The default is not to rewrite the "*Contact*" header if no NAT is performed. In NAT configurations the default is to use the destination address of the connection slot for the "*Contact*" header.

Additional Information

When the firewall plugin receives a complete SIP INVITE handshake for negotiating an RTP media session it makes a lookup in the firewall rule set. The lookup for the RTP rule is done for a dynamic service name of *RTP:SIP* or the value defined in the **srvname** SIP plugin parameter. No fixed ports are required for the RTP rule. The media timeout value in this rule is defined by the **Balanced Timeout** parameter in the **Service Entry Parameters** settings.

Additional attributes like traffic shaping settings for the media connection can also be defined in this rule. If the matched rule allows the RTP connection then the call table is updated so that the media packets may pass. The RTP rule should always have a connection type of **Client**. NAT rewriting is based on the rule that matches the SIP signalling connection. If source or destination NAT is used in the SIP rule then SIP ties the media session to the outgoing or incoming IP addresses of the firewall

and rewrites the media portion of the SIP messages accordingly. Then the firewall forwards the media packets to the endpoints of the call. The NAT rewriting behavior can be disabled by setting the **nonat=1** plugin parameter.

When using NAT you define an incoming and outgoing rule for the SIP messages. The outgoing rule performs the source NAT and should use the parameters **via** and **fwdcontact** to tell the outside peer the right contact address on the firewall.

Example:

- "*sip via="SIP/2.0/UDP 172.31.10.5:5060*"
- *fwdcontact="<sip:proxy@firewall.extern>*""

The incoming rule redirects SIP packets to the internal proxy and should use the **revcontact** plugin parameter to tell the outside peer the right contact address on the firewall.

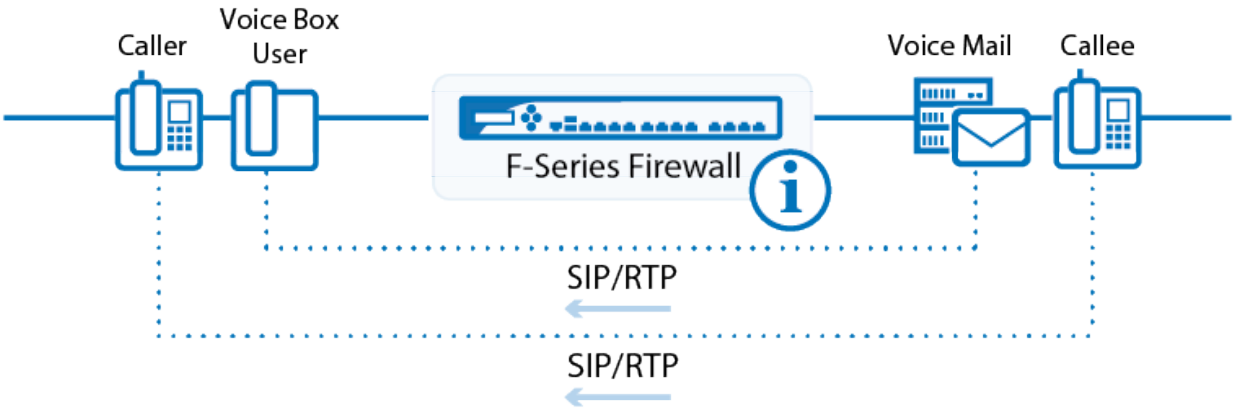
Example:

- "*sip revcontact="<sip:proxy@firewall.extern>*""

> The firewall has no registrar functionality. Setups using NAT always must use a SIP proxy in the net which gets translated. This proxy distributes incoming SIP messages to the appropriate SIP peers. The firewall ruleset must be configured to forward SIP messages for peers in the translated net to the SIP proxy.

The state of the SIP signalling can be monitored in the firewall GUI in the **Dynamic** tab under **SIP** (see below section: **Monitoring**). In network setups without NAT all SIP peers may communicate directly. Ports for the RTP media streams are opened dynamically by the firewall and passed to the participants of the call.

Network Setup Without NAT – SIP/RTP



Monitoring

Dynamic Services

Monitoring takes place in the **Dynamic** section of the firewall box menu entry:

1. Click the **FIREWALL** tab.
2. From the service menu, click **Dynamic** and select the **Dynamic Services** tab - the following columns are in use:

- The first row gives an overview of all calls that have been executed. A call does not necessarily need to be a standard call, between active caller and callee. A phone registering with a central registrar will produce a call as well. In other words, every action producing a newCall-ID, which is then part of every SIP packet transmitted through the SIP protocol, is defined as call.
- **Call-ID –** This ID is randomly generated through a caller's call.
- **Start –** This is the duration of the call.

The firewall has no registrar functionality. Setups using NAT always must use a SIP proxy in the net which gets translated. This proxy distributes incoming SIP messages to the appropriate SIP peers. The firewall rule set must be configured to forward SIP messages for peers in the translated net to the SIP proxy.

The state of the SIP signalling can be monitored in the firewall screen in the **Dynamic** tab under **SIP**. In network setups without NAT all SIP Peers may communicate directly. Ports for the RTP media streams are opened dynamically by the firewall and passed to the participants of the call.

SIP Monitoring Parameters

Status	The status column indicated the call's state. The following markers exist: • **Init –** The call has just arrived. • **Setup –** Connection establishment is just taking place. • **Established –** The call has been established. • **Teardown –** The call is about being terminated. • **Terminated –** The call has been terminated. (The call is not deleted from the table immediately after termination. It stays visible until no further media connections or SIP transactions related to it exist.
SrvName	This is the name of the dynamic service, which is used for RTP rule lookup (default: RTP:SIP).
SYNC	**(not available)** The **second row** gives an overview of all RTP media connections (Audio/Video Data Streaming) and RTCP connections (Quality Feedback and Media Signalling). Usage of RTCP is optional. If RTCP is not used during a media connection, the entry for RTCP connections vanishes after the balanced timeout of the service has expired. Medium and call are interconnected through the call-ID.
Call-ID	This is the Call-ID belonging to this Media Connection. The Call-ID constitutes a chaining to the call, which is described through the first row.
Start	This is the duration of the call.
Idle	This is the idle time since the last data flow.
Src-Addr	This is the source address before address rewriting.
Src-Port	This is the source port before address rewriting.
Dst-Addr	This is the destination address before address rewriting.
Dst-Port	This is the destination port before address rewriting.
Src-User	This is the receiver's account.
Src-Addr-Used	This is the source address after address rewriting.
Src-Port-Used	This is the source port after address rewriting.
Dst-Addr-Used	This is the destination address after address rewriting.
Dst-Port-Used	This is the destination port after address rewriting.

Figures

1. sip_rtp.png