VoIP Solutions: SIP & FortiGate Voice

FortiOS™ Handbook v3
for FortiOS 4.0 MR3
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How the SIP ALG performs NAT</td>
<td>47</td>
</tr>
<tr>
<td>Source address translation</td>
<td>48</td>
</tr>
<tr>
<td>Destination address translation</td>
<td>48</td>
</tr>
<tr>
<td>Call Re-invite messages</td>
<td>48</td>
</tr>
<tr>
<td>How the SIP ALG translates IP addresses in SIP headers</td>
<td>49</td>
</tr>
<tr>
<td>How the SIP ALG translates IP addresses in the SIP body</td>
<td>51</td>
</tr>
<tr>
<td>SIP NAT scenario: source address translation (source NAT)</td>
<td>52</td>
</tr>
<tr>
<td>SIP NAT scenario: destination address translation (destination NAT)</td>
<td>54</td>
</tr>
<tr>
<td>SIP NAT configuration example: source address translation (source NAT)</td>
<td>56</td>
</tr>
<tr>
<td>SIP NAT configuration example: destination address translation</td>
<td>59</td>
</tr>
<tr>
<td>(destination NAT)</td>
<td></td>
</tr>
<tr>
<td>Additional SIP NAT scenarios</td>
<td>62</td>
</tr>
<tr>
<td>NAT with IP address conservation</td>
<td>65</td>
</tr>
<tr>
<td>Controlling how the SIP ALG NATs SIP contact header line addresses</td>
<td>66</td>
</tr>
<tr>
<td>Controlling NAT for addresses in SDP lines</td>
<td>67</td>
</tr>
<tr>
<td>Translating SIP session destination ports</td>
<td>67</td>
</tr>
<tr>
<td>Translating SIP sessions to multiple destination ports</td>
<td>69</td>
</tr>
<tr>
<td>Enhancing SIP pinhole security</td>
<td>70</td>
</tr>
<tr>
<td>Hosted NAT traversal</td>
<td>72</td>
</tr>
<tr>
<td>Configuration example: Hosted NAT traversal for calls between</td>
<td>73</td>
</tr>
<tr>
<td>SIP Phone A and SIP Phone B</td>
<td></td>
</tr>
<tr>
<td>Hosted NAT traversal for calls between SIP Phone A and SIP Phone C</td>
<td>76</td>
</tr>
<tr>
<td>Restricting the RTP source IP</td>
<td>77</td>
</tr>
<tr>
<td>SIP over IPv6</td>
<td>77</td>
</tr>
<tr>
<td>Deep SIP message inspection</td>
<td>78</td>
</tr>
<tr>
<td>Actions taken when a malformed message line is found</td>
<td>79</td>
</tr>
<tr>
<td>Logging and statistics</td>
<td>79</td>
</tr>
<tr>
<td>Recommended configurations</td>
<td>80</td>
</tr>
<tr>
<td>Configuring deep SIP message inspection</td>
<td>80</td>
</tr>
<tr>
<td>Blocking SIP request messages</td>
<td>82</td>
</tr>
<tr>
<td>SIP rate limiting</td>
<td>84</td>
</tr>
<tr>
<td>Limiting the number of SIP dialogs accepted by a security policy</td>
<td>85</td>
</tr>
<tr>
<td>SIP logging and DLP archiving</td>
<td>86</td>
</tr>
<tr>
<td>SIP and HA: session failover and geographic redundancy</td>
<td>86</td>
</tr>
<tr>
<td>SIP geographic redundancy</td>
<td>87</td>
</tr>
<tr>
<td>Support for RFC 2543-compliant branch parameters</td>
<td>88</td>
</tr>
<tr>
<td>SIP and IPS</td>
<td>88</td>
</tr>
</tbody>
</table>
PBX configuration .................................................. 117
  Configuring extensions ........................................ 117
  Configuring extension groups (ring groups) ............... 120
  Configuring service providers (the FortiGuard Voice service) ........................................ 121
  Configuring PSTN interfaces .................................. 121
  Configuring the FortiGuard Voice service .................. 123
  Adding SIP trunks .............................................. 125
Branch Office ...................................................... 126
  Configuring dial plans ....................................... 127
  Configuring voice menu options ......................... 130
  Configuring direct inward dialing ...................... 131
  Configuring PBX global settings ...................... 132
  Importing a new voice prompt file ...................... 134
  Parking calls ................................................. 134
  FortiFAX service ............................................ 135
  Monitoring calls .............................................. 135
  Monitoring recorded conference calls .................. 135
  Monitoring voice mail storage .......................... 135
  Monitoring active phones ................................ 135
Logging of PBX activities ....................................... 136
  Viewing log messages ....................................... 136
VoIP interface reference ....................................... 136
  Profile ......................................................... 137
Using the PBX user web portal ................................. 139
  Logging into and out of the FortiGate Voice PBX user web portal .................................. 139
  Configuring PBX extension settings ..................... 139
  Voicemail ..................................................... 140
  Configuring call forwarding ................................ 140
  Sending a Fax using FortiFAX ............................. 141
  Conference calls ............................................. 141
  Managing conference calls ................................ 142
FortiGate Voice VoIP, PBX, and PSTN CLI Reference ............ 143
  config pbx dialplan ....................................... 143
  config pbx did .............................................. 145
  config pbx extension ..................................... 145
  config pbx global ......................................... 147
  config pbx ringgrp ........................................ 149
  config pbx voice-menu .................................... 150
  config pbx sip-trunk ..................................... 151
  config system pstn ........................................ 152
Introduction

This document describes FortiGate SIP support and how to configure and use the FortiGate Voice SIP server product.

Revision history

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-431-99686-20110207</td>
<td>Added FortiGate Voice chapters:</td>
</tr>
<tr>
<td></td>
<td>• “Example FortiGate Voice branch office configuration” on page 95</td>
</tr>
<tr>
<td></td>
<td>• “FortiGate Voice web-based manager configuration reference” on page 113</td>
</tr>
<tr>
<td></td>
<td>• “Using the PBX user web portal” on page 139</td>
</tr>
<tr>
<td></td>
<td>• “FortiGate Voice VoIP, PBX, and PSTN CLI Reference” on page 143</td>
</tr>
<tr>
<td></td>
<td>New section: “VoIP Profile options” on page 92.</td>
</tr>
<tr>
<td>01-431-99686-20110623</td>
<td>Throughout the document reflected FortiOS 4.0 MR3 patch 1 high level menu changes.</td>
</tr>
<tr>
<td>01-430-99686-20110216</td>
<td>Updates for FortiOS 4.0 MR3 to the following sections:</td>
</tr>
<tr>
<td></td>
<td>• “Hardware accelerated RTP processing” on page 19</td>
</tr>
<tr>
<td></td>
<td>• “Enabling VoIP support on the web-based manager” on page 35</td>
</tr>
<tr>
<td></td>
<td>• “Hosted NAT traversal” on page 72</td>
</tr>
<tr>
<td></td>
<td>• “SIP and IPS” on page 88</td>
</tr>
<tr>
<td>01-420-99686-20101130</td>
<td>Corrected the VoIP Profile options listed in Table 9 on page 81.</td>
</tr>
<tr>
<td>01-420-99686-20101015</td>
<td>Handbook V2 version. Updated graphics</td>
</tr>
</tbody>
</table>
How this guide is organized

This FortiOS Handbook chapter contains detailed information about how FortiGate units process SIP VoIP calls and how to configure the FortiGate unit to apply security features to SIP calls. This document all describes all FortiGate SIP configuration options and contains detailed configuration examples. Future versions of this document will include more and more configuration examples and more information about SIP functionality.

This FortiOS Handbook chapter contains the following sections:

FortiGate VoIP solutions: SIP describes FortiGate SIP support.
Example FortiGate Voice branch office configuration describes how to configure a FortiGate Voice-80C unit to operate in NAT/Route mode and provide basic UTM and SIP services for an example branch office network.
FortiGate Voice web-based manager configuration reference describes FortiGate Voice web-based manager configuration settings.
Using the PBX user web portal describes how to log into and use the FortiGate Voice PBX portal.
FortiGate Voice VoIP, PBX, and PSTN CLI Reference describes FortiGate Voice VoIP, PBX, and PSTN CLI commands.
FortiGate VoIP solutions: SIP

This chapter includes the following sections:

- SIP overview
- Common SIP VoIP configurations
- SIP messages and media protocols
- The SIP session helper
- The SIP ALG
- How the SIP ALG performs NAT
- Enhancing SIP pinhole security
- Hosted NAT traversal
- SIP over IPv6
- Deep SIP message inspection
- Blocking SIP request messages
- SIP rate limiting
- SIP logging and DLP archiving
- SIP and HA: session failover and geographic redundancy
- SIP and IPS
- SIP debugging
- VoIP Profile options

SIP overview

The Session Initiation Protocol (SIP) is an IETF application layer signaling protocol used for establishing, conducting, and terminating multiuser multimedia sessions over TCP/IP networks using any media. SIP is often used for Voice over IP (VoIP) calls but can be used for establishing streaming communication between endpoints.

SIP employs a request and response transaction model similar to HTTP for communicating between endpoints. SIP sessions being with a SIP client sending a SIP request message to another client to initiate a multimedia session. The other client responds with a SIP response message. Using these request and response messages, the clients engage in a SIP dialog to negotiate how to communicate and then start, maintain, and end the communication session.

SIP commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for non-encrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS).

Devices involved in SIP communications are called SIP User Agents (UAs) (also sometimes called a User Element (UE)). UAs include User Agent Clients (UACs) that communicate with each other and User Agent Servers (UASs) that facilitate communication between UACs. For a VoIP application, an example of a UAC would be a SIP phone and an example of a UAS would be a SIP proxy server.
A SIP message contain headers that include client and server names and addresses required for the communication sessions. The body of a SIP message contains Session Description Protocol (SDP) statements that establish the media communication (port numbers, protocols and codecs) that the SIP UAs use. SIP VoIP most commonly uses the Real Time Protocol (RTP) and the Real Time Control Protocol (RTCP) for voice communication. Once the SIP dialog establishes the SIP call the VoIP stream can run independently, although SIP messages can affect the VoIP stream by changing port numbers or addresses and by ending it.

Once SIP communication and media settings are established, the UAs communicate with each using the established media settings. When the communication session is completed, one of the UAs ends the session by sending a final SIP request message and the other UA sends a SIP response message and both UAs end the SIP call and stop the media stream.

FortiGate units provide security for SIP communications using the SIP session helper and the SIP ALG:

- The SIP session-helper provides basic high-performance support for SIP calls passing through the FortiGate unit by opening SIP and RTP pinholes and performing source and destination IP address and port translation for SIP and RTP packets and for the IP addresses and port numbers in the SIP headers and the SDP body of the SIP messages. For more about the SIP session helper, see “The SIP session helper” on page 28.

- The SIP Application Layer Gateway (ALG) provides the same features as the session helper plus additional advanced features such as deep SIP message inspection, SIP logging, SIP IPv6 support, SIP message checking, HA failover of SIP sessions, and SIP rate limiting. For more about the SIP ALG, see “The SIP ALG” on page 33.

There are a large number of SIP-related Internet Engineering Task Force (IETF) documents (Request for Comments) that define behavior of SIP and related applications. FortiGate units provide complete support of RFC 3261 for SIP and RFC 4566 for SDP. FortiGate units also provide support for other SIP and SIP-related RFCs and performs “Deep SIP message inspection” on page 78 for SIP statements defined in other SIP RFCs.

Common SIP VoIP configurations

This section describes some common SIP VoIP configurations and simplified SIP dialogs for these configurations. This section also shows some examples of how adding a FortiGate unit affects SIP processing.

 Peer to peer configuration

In the peer to peer configuration shown in Figure 1, two SIP phones (in the example, FortiFones) communicate directly with each other. The phones send SIP request and response messages back and forth between each other to establish the SIP session.
Peer to peer configurations are not very common because they require the SIP phones to keep track of the names and addresses of all of the other SIP phones that they can communicate with. In most cases a SIP proxy or re-direct server maintains addresses of a large number of SIP phones and a SIP phone starts a call by contacting the SIP proxy server.

**SIP proxy server configuration**

A SIP proxy server act as intermediary between SIP phones and between SIP phones (for example, two FortiFones) and other SIP servers. As shown in Figure 2, SIP phones send request and response messages the SIP proxy server. The proxy server forwards the messages to other clients or to other SIP proxy servers. Proxy servers can hide SIP phones by proxying the signaling messages. To the other users on the VoIP network, the signaling invitations look as if they come from the SIP proxy server.

**Figure 2: SIP in proxy mode**

A common SIP configuration would include multiple networks of SIP phones. Each of the networks would have its own SIP server. Each SIP server would proxy the communication between phones on its own network and between phones in different networks.
SIP redirect server configuration

A SIP redirect server accepts SIP requests, maps the addresses in the request into zero or more new addresses and returns those addresses to the client. The redirect server does not initiate SIP requests or accept calls. As shown in Figure 3, SIP clients send INVITE requests to the redirect server, which then looks up the destination address. The redirect server returns the destination address to the client. The client uses this address to send the INVITE request directly to the destination SIP client.

Figure 3: SIP in redirect mode

SIP registrar configuration

A SIP registrar accepts SIP REGISTER requests from SIP phones for the purpose of updating a location database with this contact information. This database can then become a SIP location service that can be used by SIP proxy servers and redirect servers to locate SIP clients. As shown in Figure 4, SIP clients send REGISTER requests to the SIP registrar.
SIP with a FortiGate unit

Depending on your security requirements and network configuration FortiGate units may be in many different places in a SIP configuration. This section shows a few examples.

Figure 5 shows a FortiGate unit installed between a SIP proxy server and SIP phones on the same network. The FortiGate unit is operating in Transparent mode so both the proxy server and the phones are on the same subnet. In this configuration, called SIP inspection without address translation, the FortiGate unit could be protecting the SIP proxy server on the private network by implementing SIP security features for SIP sessions between the SIP phones and the SIP proxy server.
The phones and server use the same SIP dialogs as they would if the FortiGate unit was not present. However, the FortiGate unit can be configured to control which devices on the network can connect to the SIP proxy server and can also protect the SIP proxy server from SIP vulnerabilities.

Figure 6 shows a FortiGate unit operating in NAT/Route mode and installed between a private network and the Internet. Some SIP phones and the SIP proxy server are connected to the private network and some SIP phones are connected to the Internet. The SIP phones on the Internet can connect to the SIP proxy server through the FortiGate unit and communication between SIP phones on the private network and SIP phones on the Internet must pass through the FortiGate unit.
The phones and server use the same SIP dialog as they would if the FortiGate unit was not present. However, the FortiGate unit can be configured to control which devices on the network can connect to the SIP proxy server and can also protect the SIP proxy server from SIP vulnerabilities. In addition, the FortiGate unit has a firewall virtual IP that forwards packets sent to the SIP proxy server Internet IP address (172.20.120.50) to the SIP proxy server internal network IP address (10.31.101.30).

Since the FortiGate unit is operating in NAT/Route mode it must translate packet source and destination IP addresses (and optionally ports) as the sessions pass through the FortiGate unit. Also, the FortiGate unit must translate the addresses contained in the SIP headers and SDP body of the SIP messages. As well the FortiGate unit must open SIP and RTP pinholes through the FortiGate unit. SIP pinholes allow SIP signalling sessions to pass through the FortiGate between phones and between phones and SIP servers. RTP pinholes allow direct RTP communication between the SIP phones once the SIP dialog has established the SIP call. Pinholes are opened automatically by the FortiGate unit. Administrators do not add security policies for pinholes or for RTP sessions. All that is required is a security policy that accepts SIP traffic.

Opening an RTP pinhole means opening a port on a FortiGate interface to allow RTP traffic to use that port to pass through the FortiGate unit between the SIP phones on the Internet and SIP phones on the internal network. A pinhole only accepts packets from one RTP session. Since a SIP call involves at least two media streams (one from Phone A to Phone B and one from Phone B to Phone A) the FortiGate unit opens two RTP pinholes. Phone A sends RTP packets through a pinhole in port2 and Phone B sends RTP packets through a pinhole in port1. The FortiGate unit opens the pinholes when required by the SIP dialog and closes the pinholes when the SIP call is completed. The FortiGate unit opens new pinholes for each SIP call.

Each RTP pinhole actually includes two port numbers. The RTP port number as defined in the SIP message and an RTCP port number, which is the RTP port number plus 1. For example, if the SIP call used RTP port 3346 the FortiGate unit would create a pinhole for ports 3346 and 3347.

**SIP messages and media protocols**

This section provides an overview of SIP messages and how they communicate information about SIP sessions and how SDP, RTP, and RTCP fits in with SIP communications.

SIP uses clear text messages to start, maintain, and end media sessions between SIP user agent clients (UACs) and user agent servers (UASs). These messages form a SIP dialog. A typical SIP dialog begins with an INVITE request message sent from a UAC to another UAC or to a UAS. The first INVITE request message attempts to start a SIP call and includes information about the sending UAC and the receiving UAC as well as information about the communication session.

If only two UACs are involved as shown in Figure 7, the receiving UAC (Phone B) responds with a 180 Ringing and then a 200 OK SIP response message that informs Phone A that Phone B received and accepted the request. Phone A then sends an ACK message to notify Phone B that the SIP response was received. Phone A and Phone B can then participate in the RTP media session set up by the SIP messages.

When the phone call is complete, one of the UACs (in the example Phone B) hangs up sending a BYE request message to Phone A. Phone A then sends a 200 OK response to Phone B acknowledging that the session has ended.
If a UAS in the form of a SIP proxy server is involved, similar messages are sent and received, but the proxy server participates as an intermediary in the initial call setup. In the example in Figure 8 the SIP proxy server receives the INVITE request from Phone A and forwards it to Phone B. The proxy server then sends a 100 Trying response to Phone A. Phone B receives the INVITE request and responds with a 180 Ringing and then a 200 OK SIP response message. These messages are received by the proxy server and forwarded to Phone A to notify Phone A that Phone B received and accepted the request. Phone A then sends an ACK message to notify Phone B that the SIP response was received. This response is received by the proxy server and forwarded to Phone B. Phone A and Phone B can then participate in the media session independently of the proxy server.

When the phone call is complete Phone B hangs up sending a BYE request message to Phone A. Phone A then sends a 200 OK response to Phone B acknowledging that the session has ended.
Figure 8: Basic SIP dialog between UACs with a SIP proxy server UAS

The SIP messages include SIP headers that contain names and addresses of Phone A, Phone B and the proxy server. This addressing information is used by the UACs and the proxy server during the call set up.

The SIP message body includes Session Description Protocol (SDP) statements that Phone A and Phone B use to establish the media session. The SDP statements specify the type of media stream to use for the session (for example, audio for SIP phone calls) and the protocol to use for the media stream (usually the Real Time Protocol (RTP) media streaming protocol).

Phone A includes the media session settings that it would like to use for the session in the INVITE message. Phone B includes its response to these media settings in the 200 OK response. Phone A’s ACK response confirms the settings that Phone A and Phone B then use for the media session.

**Hardware accelerated RTP processing**

FortiGate units can offload RTP packet processing to network processor (NP) interfaces. This acceleration greatly enhance the overall throughput and resulting in near speed RTP performance.

**SIP request messages**

SIP sessions always start with a SIP request message (also just called a SIP request). SIP request messages also establish, maintain, and terminate SIP communication sessions. Table 1 lists some common SIP request message types.
Table 1: Common SIP request message types

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>A client sends an INVITE request to invite another client to participate in a multimedia session. The INVITE request body usually contains the description of the session.</td>
</tr>
<tr>
<td>ACK</td>
<td>The originator of an INVITE message sends an ACK request to confirm that the final response to an INVITE request was received. If the INVITE request did not contain the session description, it must be included in the ACK request.</td>
</tr>
<tr>
<td>PRACK</td>
<td>In some cases, SIP uses provisional response messages to report on the progress of the response to a SIP request message. The provisional response messages are sent before the final SIP response message. Similar to an ACK request message, a PRACK request message is sent to acknowledge that a provisional response message has been received.</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>The UA uses OPTIONS messages to get information about the capabilities of a SIP proxy. The SIP proxy server replies with a description of the SIP methods, session description protocols, and message encoding that are supported.</td>
</tr>
<tr>
<td>BYE</td>
<td>A client sends a BYE request to end a session. A BYE request from either end of the SIP session terminates the session.</td>
</tr>
<tr>
<td>CANCEL</td>
<td>A client sends a CANCEL request to cancel a previous INVITE request. A CANCEL request has no effect if the SIP server processing the INVITE sends a final response to the INVITE before receiving the CANCEL.</td>
</tr>
<tr>
<td>REGISTER</td>
<td>A client sends a REGISTER request to a SIP registrar server with information about the current location (IP address and so on) of the client. A SIP registrar server saves the information it receives in REGISTER requests and makes this information available to any SIP client or server attempting to locate the client.</td>
</tr>
<tr>
<td>Info</td>
<td>For distributing mid-session signaling information along the signaling path for a SIP call.</td>
</tr>
<tr>
<td>Subscribe</td>
<td>For requesting the current state and state updates of a remote node.</td>
</tr>
<tr>
<td>Notify</td>
<td>Informs clients and servers of changes in state in the SIP network.</td>
</tr>
<tr>
<td>Refer</td>
<td>Refers the recipient (identified by the Request-URI) to a third party according to the contact information in the request.</td>
</tr>
<tr>
<td>Update</td>
<td>Opens a pinhole for new or updated SDP information.</td>
</tr>
<tr>
<td>Response codes (1xx, 202, 2xx, 3xx, 4xx, 5xx, 6xx)</td>
<td>Indicates the status of a transaction. For example: 200 OK, 202 Accepted, or 400 Bad Request.</td>
</tr>
</tbody>
</table>

SIP response messages

SIP response messages (often just called SIP responses) provide status information in response to SIP request messages. All SIP response messages include a response code and a reason phrase. There are five SIP response message classes. They are described below.
There are also two types of SIP response messages, provisional and final. Final response messages convey the result of the request processing, and are sent reliably. Provisional responses provide information on the progress of the request processing, but may not be sent reliably. Provisional response messages start with 1xx and are also called informational response messages.

**Informational (or provisional)**

Informational or provisional responses indicate that a request message was received and imply that the endpoint is going to process the request. Information messages may not be sent reliably and may not require an acknowledgement.

If the SIP implementation uses Provisional Response Acknowledgement (PRACK) (RFC 3262) then informational or provisional messages are sent reliably and require a PRACK message to acknowledge that they have been received.

Informational responses can contain the following reason codes and reason phrases:

- 100 Trying
- 180 Ringing
- 181 Call is being forwarded
- 182 Queued
- 183 Session progress

**Success**

Success responses indicate that a request message was received, understood, and accepted. Success responses can contain the following reason codes and reason phrases:

- 200 OK
- 202 Accepted

**Redirection**

Redirection responses indicate that more information is required for the endpoint to respond to a request message. Redirection responses can contain the following reason codes and reason phrases:

- 300 Multiple choices
- 301 Moved permanently
- 302 Moved temporarily
- 305 Use proxy
- 380 Alternative service

**Client error**

Client error responses indicate that a request message was received by a server that contains syntax that the server cannot understand (i.e. contains a syntax error) or cannot comply with. Client error responses include the following reason codes and reason phrases:

- 400 Bad request
- 401 Unauthorized
- 402 Payment required
- 403 Forbidden
- 404 Not found
- 405 Method not allowed
- 406 Not acceptable
- 407 Proxy authentication required
- 408 Request time-out
- 409 Conflict
- 410 Gone
- 411 Length required
- 413 Request entity too large
- 414 Request-URL too large
- 415 Unsupported media type
- 420 Bad extension
- 480 Temporarily not available
SIP messages and media protocols

FortiGate VoIP solutions: SIP

481 Call leg/transaction does not exist
482 Loop detected 483 Too many hops
484 Address incomplete 485 Ambiguous
486 Busy here 487 Request canceled
488 Not acceptable here

Server error

Server error responses indicate that a server was unable to respond to a valid request message. Server error responses include the following reason codes and reason phrases:

- 500 Server internal error
- 501 Not implemented
- 502 Bad gateway
- 502 Service unavailable
- 504 Gateway time-out
- 505 SIP version not supported

Global failure

Global failure responses indicate that there are no servers available that can respond to a request message. Global failure responses include the following reason codes and reason phrases:

- 600 Busy everywhere
- 603 Decline
- 604 Does not exist anywhere
- 606 Not acceptable

SIP message start line

The first line in a SIP message is called the start line. The start line in a request message is called the request-line and the start line in a response message is called the status-line.

Request-line

The first line of a SIP request message. The request-line includes the SIP message type, the SIP protocol version, and a Request URI that indicates the user or service to which this request is being addressed. The following example request-line specifies the INVITE message type, the address of the sender of the message (inviter@example.com), and the SIP version:

```
INVITE sip:inviter@example.com SIP/2.0
```

Status-line

The first line of a SIP response message. The status-line includes the SIP protocol version, the response code, and the reason phrase. The example status-line includes the SIP version, the response code (200) and the reason phrase (OK).

```
SIP/2.0 200 OK
```

SIP headers

Following the start line, SIP messages contain SIP headers (also called SIP fields) that convey message attributes and to modify message meaning. SIP headers are similar to HTTP header fields and always have the following format:

```
<header_name>:<value>
```

SIP messages can include the SIP headers listed in Table 2:
### Table 2: SIP headers

<table>
<thead>
<tr>
<th>SIP Header</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Allow**  | Lists the set of SIP methods supported by the UA generating the message. All methods, including ACK and CANCEL, understood by the UA MUST be included in the list of methods in the Allow header field, when present. For example:  
> Allow: INVITE, ACK, OPTIONS, CANCEL, BYE |
| **Call-ID** | A globally unique identifier for the call, generated by the combination of a random string and the sender’s host name or IP address. The combination of the To, From, and Call-ID headers completely defines a peer-to-peer SIP relationship between the sender and the receiver. This relationship is called a SIP dialog.  
> Call-ID: ddeg45e793@10.31.101.30 |
| **Contact** | Included in SIP request messages, the Contact header contains the SIP URI of the sender of the SIP request message. The receiver uses this URI to contact the sender. For example:  
> Contact: Sender <sip:sender@10.31.100.20> |
| **Content-Length** | The number of bytes in the message body (in bytes).  
> Content-Length: 126 |
| **Content-Type** | In addition to SIP headers, SIP messages include a message body that contains information about the content or communication being managed by the SIP session. The Content-Type header specifies what the content of the SIP message is. For example, if you are using SIP with SDP, the content of the SIP message is SDP code.  
> Content-Type: application/sdp |
| **CSeq** | The command sequence header contains a sequence integer that is increased for each new SIP request message (but is not incremented in the response message). This header also incudes the request name found in the request message request-line. For example:  
> CSeq: 1 INVITE |
| **Expires** | Gives the relative time after which the message (or content) expires. The actual time and how the header is used depends on the SIP method. For example:  
> Expires: 5 |
| **From** | Identifies the sender of the message. Responses to a message are sent to the address of the sender. The following example includes the sender’s name (Sender) and the sender’s SIP address (sender@10.31.101.20):  
> From: Sender <sip:sender@10.31.101.20> |
### Table 2: SIP headers (Continued)

<table>
<thead>
<tr>
<th>SIP Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max-forwards</td>
<td>An integer in the range 0-255 that limits the number of proxies or gateways that can forward the request message to the next downstream server. Also called the number of hops, this value is decreased every time the message is forwarded. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain. For example:</td>
</tr>
<tr>
<td></td>
<td>Max-Forwards: 30</td>
</tr>
<tr>
<td>P-Asserted-Identity</td>
<td>The P-Asserted-Identity header is used among trusted SIP entities to carry the identity of the user sending a SIP message as it was verified by authentication. See RFC 3325. The header contains a SIP URI and an optional display-name, for example:</td>
</tr>
<tr>
<td></td>
<td>P-Asserted-Identity: &quot;Example Person&quot;</td>
</tr>
<tr>
<td></td>
<td><a href="">sip:10.31.101.50</a></td>
</tr>
<tr>
<td>RAck</td>
<td>Sent in a PRACK request to support reliability of information or provisional response messages. It contains two numbers and a method tag. For example:</td>
</tr>
<tr>
<td></td>
<td>RAck: 776656 1 INVITE</td>
</tr>
<tr>
<td>Record-Route</td>
<td>Inserted into request messages by a SIP proxy to force future requests to be routed through the proxy. In the following example, the host at IP address 10.31.101.50 is a SIP proxy. The lr parameter indicates the URI of a SIP proxy in Record-Route headers.</td>
</tr>
<tr>
<td></td>
<td>Record-Route: <a href="">sip:10.31.101.50;lr</a></td>
</tr>
<tr>
<td>Route</td>
<td>Forces routing for a request message through one or more SIP proxies. The following example includes two SIP proxies:</td>
</tr>
<tr>
<td></td>
<td>Route: <a href="">sip:172.20.120.10;lr</a>, <a href="">sip:10.31.101.50;lr</a></td>
</tr>
<tr>
<td>RSeq</td>
<td>The RSeq header is used in information or provisional response messages to support reliability of informational response messages. The header contains a single numeric value. For example:</td>
</tr>
<tr>
<td></td>
<td>RSeq: 33456</td>
</tr>
<tr>
<td>To</td>
<td>Identifies the receiver of the message. The address in this field is used to send the message to the receiver. The following example includes the receiver’s name (Receiver) and the receiver’s SIP address (receiver@10.31.101.30):</td>
</tr>
<tr>
<td></td>
<td>To: Receiver <a href="">sip:receiver@10.31.101.30</a></td>
</tr>
<tr>
<td>Via</td>
<td>Indicates the SIP version and protocol to be used for the SIP session and the address to which to send the response to the message that contains the Via field. The following example Via field indicates to use SIP version 2, UDP for media communications, and to send the response to 10.31.101.20 using port 5060.</td>
</tr>
<tr>
<td></td>
<td>Via: SIP/2.0/UDP 10.31.101.20:5060</td>
</tr>
</tbody>
</table>
The SIP message body and SDP session profiles

The SIP message body describes the session to be initiated. For example, in a SIP phone call the body usually includes audio codec types, sampling rates, server IP addresses and so on. For other types of SIP session the body could contain text or binary data of any type which relates in some way to the session. The message body is included in request and response messages.

Two possible SIP message body types:

- Session Description Protocol (SDP), most commonly used for SIP VoIP.
- Multipurpose Internet Mail Extensions (MIME)

SDP is most often used for VoIP and FortiGate units support SDP content in SIP message bodies. SDP is a text-based protocol used by SIP to control media sessions. SDP does not deliver media but provides a session profile that contains media details, transport addresses, parameter negotiation, and other session description metadata for the participants in a media session. The participants use the information in the session profile to negotiate how to communicate and to manage the media session. SDP is described by RFC 4566.

An SDP session profile always contains session information and may contain media information. Session information appears at the start of the session profile and media information (using the m= attribute) follows.

SDP session profiles can include the attributes listed in Table 3.

**Table 3: SDP session profile attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a=</td>
<td>Attributes to extend SDP in the form a=&lt;attribute&gt; or a=&lt;attribute&gt;:&lt;value&gt;.</td>
</tr>
<tr>
<td>b=</td>
<td>Contains information about the bandwidth required for the session or media in the form b=&lt;bandwidth_type&gt;:&lt;bandwidth&gt;.</td>
</tr>
<tr>
<td>c=</td>
<td>Connection data about the session including the network type (usually IN for Internet), address type (IPv4 or IPv6), the connection source address, and other optional information. For example: c=IN IPv4 10.31.101.20</td>
</tr>
<tr>
<td>i=</td>
<td>A text string that contains information about the session. For example: i=A audio presentation about SIP</td>
</tr>
<tr>
<td>k=</td>
<td>Can be used to convey encryption keys over a secure and trusted channel. For example: k=clear:444gduudjffdee</td>
</tr>
</tbody>
</table>
Example SIP messages

The following example SIP INVITE request message was sent by PhoneA to PhoneB. The first nine lines are the SIP headers. The SDP profile starts with \texttt{v=0} and the media part of the session profile is the last line, starting with \texttt{m=}.

```
INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.50:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
```

```
INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.50:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
```

Table 3: SDP session profile attributes (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| m=        | Media information, consisting of one or more lines all starting with \texttt{m=} and containing details about the media including the media type, the destination port or ports used by the media, the protocol used by the media, and a media format description. Example: ```
m=audio 49170 RTP 0 3
m-video 3345/2 udp 34
m-video 2910/2 RTP/AVP 3 56
``` Multiple media lines are needed if SIP is managing multiple types of media in one session (for example, separate audio and video streams). Multiple ports for a media stream are indicated using a slash. \texttt{3345/2 udp} means UDP ports 3345 and 3346. Usually RTP uses even-numbered ports for data with the corresponding one-higher odd ports used for the RTCP session belonging to the RTP session. So \texttt{2910/2 RTP/AVP} means ports 2910 and 2912 are used for RTP and 2911 and 2913 are used for RTCP. Media types include \texttt{udp} for an unspecified protocol that uses UDP, \texttt{RTP} or \texttt{RTP/AVP} for standard RTP and \texttt{RTP/SAVP} for secure RTP. |
| o=        | The sender’s username, a session identifier, a session version number, the network type (usually IN for Internet), the address type (for example, IPv4 or IPv6), and the sending device’s IP address. The \texttt{o=} field becomes a universal identifier for this version of this session description. For example: ```
o=PhoneA 5462346 332134 IN IP4 10.31.101.20
``` |
| r=        | Repeat times for a session. Used if a session will be repeated at one or more timed intervals. Not normally used for VoIP calls. The times can be in different formats. For example. ```
r=7d 1h 0 25h
r=604800 3600 0 90000
``` |
| s=        | Any text that describes the session or \texttt{s=} followed by a space. For example: ```
s=Call from inviter
``` |
| t=        | The start and stop time of the session. Sessions with no time restrictions (most VoIP calls) have a start and stop time of 0. ```
t=0 0
``` |
| v=        | SDP protocol version. The current SDP version is 0 so the \texttt{v=} field is always: ```
v=0
``` |
| z=        | Time zone adjustments. Used for scheduling repeated sessions that span the time between changing from standard to daylight savings time. ```
z=2882844526 -1h 2898848070 0
```
To: PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneA@10.31.101.20
Content-Type: application/sdp
Content-Length: 124
v=0
o=PhoneB 5462346 332134 IN IP4 10.31.101.20
s=Let's Talk
t=0 0
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3

The following example shows a possible 200 OK SIP response message in response to the previous INVITE request message. The response includes 200 OK which indicates success, followed by an echo of the original SIP INVITE request followed by PhoneB’s SDP profile.

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.31.101.30:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
To: PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneB@10.31.101.30
Content-Type: application/sdp
Content-Length: 107
v=0
o=PhoneB 124333 67895 IN IP4 172.20.120.30
s=Hello!
t=0 0
c=IN IP4 172.20.120.30
m=audio 3456 RTP 0

SIP can support multiple media streams for a single SIP session. Each media steam will have its own c= and m= lines in the body of the message. For example, the following message includes three media streams:

INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.20:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
To: PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneB@10.31.101.20
Content-Type: application/sdp
Content-Length: 124
v=0
o=PhoneB 5462346 332134 IN IP4 10.31.101.20
s=Let’s Talk
t=0 0
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3
c=IN IP4 10.31.101.20
m=audio 49172 RTP 0 3
c=IN IP4 10.31.101.20
m=audio 49174 RTP 0 3
The SIP session helper

The SIP session-helper is a high-performance solution that provides basic support for SIP calls passing through the FortiGate unit by opening SIP and RTP pinholes and by performing NAT of the addresses in SIP messages.

The SIP session helper:

- Understands SIP dialog messages.
- Keeps the states of the SIP transactions between SIP UAs and SIP servers.
- Translates SIP header and SDP information to account for NAT operations performed by the FortiGate unit.
- Opens up and closes dynamic SIP pinholes for SIP signalling traffic.
- Opens up and closes dynamic RTP and RTSP pinholes for RTP and RTSP media traffic.
- Provides basic SIP security as an access control device.
- Uses the intrusion protection (IPS) engine to perform basic SIP protocol checks.

SIP session helper configuration overview

The SIP session helper is enabled by default and set to listen for SIP traffic on TCP or UDP port 5060. SIP sessions using port 5060 accepted by a security policy that does not include a VoIP profile are processed by the SIP session helper.

You can enable and disable the SIP session helper, change the TCP or UDP port that the session helper listens on for SIP traffic, and enable or disable SIP NAT tracing. If the FortiGate unit is operating with multiple VDOMs, each VDOM can have a different SIP session helper configuration.

To have the SIP session helper process SIP sessions you need to add a security policy that accepts SIP sessions on the configured SIP UDP or TCP ports. The security policies can have service set to ANY, or to the SIP pre-defined firewall service, or a custom firewall service. The SIP pre-defined firewall service restricts the security policy to only accepting sessions on UDP port 5060.

If NAT is enabled for security policies that accept SIP traffic, the SIP session helper translates addresses in SIP headers and in the RDP profile and opens up pinholes as required for the SIP traffic. This includes security policies that perform source NAT and security policies that contain virtual IPs that perform destination NAT and port forwarding. No special SIP configuration is required for this address translation to occur, it is all handled automatically by the SIP session helper according to the NAT configuration of the security policy that accepts the SIP session.

To use the SIP session helper you must not add a VoIP profile to the security policy. If you add a VoIP profile, SIP traffic bypasses the SIP session helper and is processed by the SIP ALG.

In most cases you would want to use the SIP ALG since the SIP session helper provides limited functionality. However, the SIP session helper is available and can be useful for high-performance solutions where a high level of SIP security is not a requirement.
Disabling and enable the SIP session helper

You can use the following steps to disable the SIP session helper. You might want to disable the SIP session helper if you don’t want the FortiGate unit to apply NAT or other SIP session help features to SIP traffic. With the SIP session helper disabled, the FortiGate unit can still accept SIP sessions if they are allowed by a security policy, but the FortiGate unit will not be able to open pinholes or NAT the addresses in the SIP messages.

To disable the sip session helper

1. Enter the following command to find the sip session helper entry in the session-helper list:

   show system session-helper

   .
   .
   .

   edit 13
   
   set name sip
   set port 5060
   set protocol 17
   next
   .
   .
   .

   This command output shows that the sip session helper listens in UDP port 5060 for SIP sessions.

2. Enter the following command to delete session-helper list entry number 13 to disable the sip session helper:

   config system session-helper
   
   delete 13
   
   end

If you want to use the SIP session helper you can verify whether it is enabled or disabled using the show system session-helper command.

You do not have to disable the SIP session helper to use the SIP ALG.

If the SIP session helper has been disable by being removed from the session-helper list you can use the following command to enable the SIP session helper by adding it back to the session helper list:

   config system session-helper
   edit 0
   
   set name sip
   set port 5060
   set protocol 17
   
   end
Changing the port numbers that the SIP session helper listens on

You can use the following command to change the port number that the SIP session helper listens on for SIP traffic to 5061. The SIP session helper listens on the same port number for UDP and TCP SIP sessions. In this example, the SIP session helper is session helper 13:

```
config system session-helper
edit 13
set port 5061
end
```

Your FortiGate unit may use a different session helper number for SIP. Enter the following command to view the session helpers:

```
show system session-helper
```

Configuration example: SIP session helper in Transparent Mode

Figure 9 shows an example SIP network consisting of a FortiGate unit operating in Transparent mode between two SIP phones. Since the FortiGate unit is operating in Transparent mode both phones are on the same network and the FortiGate unit and the SIP session helper does not perform NAT. Even though the SIP session helper is not performing NAT you can use this configuration to apply SIP session helper security features to the SIP traffic.

The FortiGate unit requires two security policies that accept SIP packets. One to allow SIP Phone A to start a session with SIP Phone B and one to allow SIP Phone B to start a session with SIP Phone A.

Figure 9: SIP network with FortiGate unit in Transparent mode
General configuration steps

The following general configuration steps are required for this SIP configuration. This example includes security policies that specifically allow SIP sessions using UDP port 5060 from Phone A to Phone B and from Phone B to Phone A. In most cases you would have more than two phones so would use more general security policies. Also, you can set the firewall service to ANY to allow traffic other than SIP on UDP port 5060.

1. Add firewall addresses for Phone A and Phone B.
2. Add a security policy that accepts SIP sessions initiated by Phone A.
3. Add a security policy that accepts SIP sessions initiated by Phone B.

Configuration steps - web-based manager

To add firewall addresses for the SIP phones
1. Go to Firewall Objects > Address.
2. Add the following addresses for Phone A and Phone B:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Phone_A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.31.101.20/255.255.255.255</td>
</tr>
<tr>
<td>Interface</td>
<td>port1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Phone_B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.31.101.30/255.255.255.255</td>
</tr>
<tr>
<td>Interface</td>
<td>port2</td>
</tr>
</tbody>
</table>

To add security policies to accept SIP sessions
1. Go to Policy > Policy > Policy.
2. Select Create New to add a security policy.
3. Add a security policy to allow Phone A to send SIP request messages to Phone B:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Phone_A</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Phone_B</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>SIP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

4. Select OK.
5. Add a security policy to allow Phone B to send SIP request messages to Phone A:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Phone_B</td>
</tr>
</tbody>
</table>
To add firewall addresses for Phone A and Phone B and security policies to accept SIP sessions:

1. Enter the following command to add firewall addresses for Phone A and Phone B.
   ```
   config firewall address
   edit Phone_A
   set associated interface port1
   set type ipmask
   set subnet 10.31.101.20 255.255.255.255
   next
   edit Phone_B
   set associated interface port2
   set type ipmask
   set subnet 10.31.101.30 255.255.255.255
   end
   ```

2. Enter the following command to add security policies to allow Phone A to send SIP request messages to Phone B and Phone B to send SIP request messages to Phone A.
   ```
   config firewall policy
   edit 0
   set srcintf port1
   set dstintf port2
   set srcaddr Phone_A
   set dstaddr Phone_B
   set action accept
   set schedule always
   set service SIP
   next
   edit 0
   set srcintf port2
   set dstintf port1
   set srcaddr Phone_B
   set dstaddr Phone_A
   set action accept
   set schedule always
   set service SIP
   set utm-status enable
   end
   ```

6. Select OK.

### Configuration steps - CLI

**To add firewall addresses for Phone A and Phone B and security policies to accept SIP sessions**

1. Enter the following command to add firewall addresses for Phone A and Phone B.
   ```
   config firewall address
   edit Phone_A
   set associated interface port1
   set type ipmask
   set subnet 10.31.101.20 255.255.255.255
   next
   edit Phone_B
   set associated interface port2
   set type ipmask
   set subnet 10.31.101.30 255.255.255.255
   end
   ```

2. Enter the following command to add security policies to allow Phone A to send SIP request messages to Phone B and Phone B to send SIP request messages to Phone A.
   ```
   config firewall policy
   edit 0
   set srcintf port1
   set dstintf port2
   set srcaddr Phone_A
   set dstaddr Phone_B
   set action accept
   set schedule always
   set service SIP
   next
   edit 0
   set srcintf port2
   set dstintf port1
   set srcaddr Phone_B
   set dstaddr Phone_A
   set action accept
   set schedule always
   set service SIP
   set utm-status enable
   end
   ```
SIP session helper diagnose commands

You can use the `diagnose sys sip` commands to display diagnostic information for the SIP session helper.

Use the following command to set the debug level for the SIP session helper. Different debug masks display different levels of detail about SIP session helper activity.

```
diagnose sys sip debug-mask <debug_mask_int>
```

Use the following command to display the current list of SIP dialogs being processed by the SIP session helper. You can also use the `clear` option to delete all active SIP dialogs being processed by the SIP session helper.

```
diagnose sys sip dialog {clear | list}
```

Use the following command to display the current list of SIP NAT address mapping tables being used by the SIP session helper.

```
diagnose sys sip mapping list
```

Use the following command to display the current SIP session helper activity including information about the SIP dialogs, mappings, and other SIP session help counts. This command can be useful to get an overview of what the SIP session helper is currently doing.

```
diagnose sys sip status
```

The SIP ALG

In most cases you should use the SIP Application Layer Gateway (ALG) for processing SIP sessions. The SIP ALG provides the same basic SIP support as the SIP session helper. Additionally, the SIP ALG provides a wide range of features that protect your network from SIP attacks, can apply rate limiting to SIP sessions, can check the syntax of SIP and SDP content of SIP messages, and provide detailed logging and reporting of SIP activity.

You apply the SIP ALG to SIP traffic by adding a VoIP profile with SIP enabled to a security policy that accepts SIP traffic. The SIP session helper is automatically bypassed by traffic accepted by a security policy that includes a VoIP profile.

As shown in Figure 10, the FortiGate SIP ALG intercepts SIP packets after they have been routed by the routing module, accepted by a security policy and passed through DoS and IPS Sensors (if DoS and IPS are enabled). The ALG raises SIP packets to the application layer, analyzes the SIP and SDP addressing information in the SIP messages, makes adjustments (for example, NAT) to this addressing if required, and then sends the packets out the egress interface to their destination.

The SIP ALG provides:

- All the same features as the SIP session help including NAT and SIP and RTP Pinholes.
  
  In addition for the ALG you can enable or disable RTP pinholing, SIP register pinholing and SIP contact pinholing. In a signalling only environment where the RTP stream bypasses the FortiGate unit, you can disable RTP pinholing to improve performance.

- SIP TCP and UDP support

- SIP Message order checking

- Configurable Header line length maximums
Figure 10: The SIP ALG works at the application level after ingress packets are accepted by a security policy

- **Message fragment assembly (TCP)**
  If SIP messages are fragmented across multiple packets, the FortiGate unit assembles the fragments, does inspection and pass the message in its entirety to the SIP server as one packet. This offloads the server from doing all the TCP processing of fragments.

- **L4 Protocol Translation**

- **Message Flood Protection**
  Protects a SIP server from intentional or unintentional DoS of flooding INVITE, REGISTER, and other SIP methods by allowing control of the rate that these massages pass through the FortiGate unit.

- **SIP message type filtering**
  The FortiGate unit can prevent specified SIP message types from passing through the FortiGate unit to a SIP server. For example in a voice only SIP implementation, there may be no need to permit a SUBSCRIBE message to ever make it’s way to the SIP call processor. Also, if a SIP server cannot process some SIP message types you can use SIP message type filtering to block them. For example, a SIP server could have a bug that prevents it from processing certain SIP messages. In this case you can temporarily block these message types until problem with the SIP server has been fixed.

- **SIP statistics and logging**

- **SIP over IPv6**

- **Deep SIP message syntax checking (also called deep SIP header inspection or SIP fuzzing protection)**. Prevents attacks that use malformed SIP messages. Can check many SIP headers and SDP statements. Configurable bypass and modification options.
• Hosted NAT traversal, Resolves IP address issue in SIP and SDP lines due to NAT-PT in far end firewall. Important feature for VoIP access networks.

• SIP High Availability (HA), including active-passive clustering and session pickup (session failover) for SIP sessions.

• Geographical Redundancy. In an HA configuration, if the active SIP server fails (missing SIP heartbeat messages or SIP traffic) SIP sessions can be redirected to a secondary SIP server in another location.

• SIP per request method message rate limitation with configurable threshold for SIP message rates per request method. Protects SIP servers from SIP overload and DoS attacks.

• RTP Bypass, Supports configurations with and without RTP pinholing. May inspect and protect SIP signaling only.

• SIP NAT with IP address conservation. Performs SIP and RTP aware IP Network Address translation. Preserves the lost IP address information in the SDP profile i= line for later processing/debugging in the SIP server. See “NAT with IP address conservation” on page 65.

• IP topology hiding

  The IP topology of a network can be hidden through NAT and NAPT manipulation of IP and SIP level addressing. For example, see “SIP NAT configuration example: destination address translation (destination NAT)” on page 59.

• SIP inspection without address translation

  The SIP ALG inspects SIP messages but addresses in the messages are not translated. This feature can be applied to a FortiGate unit operating in Transparent mode or in NAT/Route mode. In Transparent mode you add normal Transparent mode security policies that enable the SIP ALG and include a VoIP profile that causes the SIP ALG to inspect SIP traffic as required. For an example configuration, see “Configuration example: SIP in Transparent Mode” on page 42.

  For a FortiGate unit operating in NAT/Route mode, if SIP traffic can pass between different networks without requiring NAT because is supported by the routing configuration, you can add security policies that accept SIP traffic without enabling NAT. In the VoIP profile you can configure the SIP ALG to inspect SIP traffic as required.

SIP ALG configuration overview

To apply the SIP ALG, you add a SIP VoIP profile to a security policy that accepts SIP sessions. All SIP sessions accepted by the security policy will be processed by the SIP ALG using the settings in the VoIP profile. The VoIP profile contains settings that are applied to SIP, Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) and Skinny Call Control Protocol (SCCP) sessions. You configure SIP and SCCP settings separately. SIP settings also apply to SIMPLE sessions.

Enabling VoIP support on the web-based manager

Before you begin adding VoIP profiles to security policies you may have to enable VoIP support on the web-based manager. To do this, on the web-based manager go to System > Admin > Settings and make sure that the VoIP Support on GUI checkbox is selected.

  From the CLI you can also enter the following command enable VoIP support on the GUI:

```
config system global
set gui-voip-profile enable
```
VoIP profiles

To add a new VoIP profile from the web-based manager go to UTM Profiles > VoIP > Profile and select Create New.

For SIP, from the web-based manager you can configure the VoIP profile to limit the number of SIP REGISTER and INVITE requests and enable logging of SIP sessions and SIP violations. Many additional options for configuring how the ALG processes SIP sessions are available from the CLI.

Use the following command to add a VoIP profile named VoIP_Pro_1 from the CLI:

```
config voip profile
edit VoIP_Pro_1
end
```

FortiGate units include two pre-defined VoIP profiles. On the web-based manager these profiles look identical. However, the CLI-only settings result in the following functionality.

| **default** | The most commonly used VoIP profile. This profile enables both SIP and SCCP and places the minimum restrictions on what calls will be allowed to negotiate. This profile allows normal SCCP, SIP and RTP sessions and enables the following security settings:
| | • block-long-lines to block SIP messages with lines that exceed maximum line lengths.
| | • block-unknown to block unrecognized SIP request messages.
| | • log-call-summary to write log messages that record SIP call progress (similar to DLP archiving).
| | • nat-trace (see "NAT with IP address conservation" on page 65).
| | • contact-fixup to perform NAT on the IP addresses and port numbers in SIP headers in SIP CONTACT messages even if they don’t match the session’s IP address and port numbers.

| **strict** | This profile is available for users who want to validate SIP messages and to only allow SIP sessions that are compliant with RFC 3261. In addition to the settings in the default VoIP profile, the strict profile sets all SIP deep message inspection header checking to block and drop SIP messages that contain malformed SIP or SDP lines that can be detected by the ALG. For more information about SIP deep header inspection, see “Deep SIP message inspection” on page 78.

Neither of the default profiles applies SIP rate limiting or message blocking. To apply more ALG features to SIP sessions you can clone (copy) the pre-defined VoIP profiles and make your own modifications to them. For example, to clone the default profile and configure the limit for SIP NOTIFY request messages to 1000 messages per second per security policy and block SIP INFO request messages.

```
config voip profile
clone default to my_voip_pro
edit my_voip_pro
config sip
set notify-rate 1000
set block-info enable
end
end
```
Changing the port numbers that the SIP ALG listens on

Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your SIP network uses different ports for SIP sessions you can use the following command to configure the SIP ALG to listen on a different TCP or UDP ports. For example, to change the TCP port to 5061 and the UDP port to 5065.

```
config system settings
  set sip-tcp-port 5061
  set sip-udp-port 5065
end
```

Disabling the SIP ALG in a VoIP profile

SIP is enabled by default in a VoIP profile. Usually you would want SIP to be enabled in a VoIP profile. But in some cases if you are just using the VoIP profile for SCCP you can use the following command to disable SIP in a VoIP profile.

```
config voip profile
  edit VoIP_Pro_2
  config sip
    set status disable
  end
end
```

SIP ALG get and diagnose commands

You can use the following commands to display diagnostic information for the SIP ALG. Use the following commands to enter a test level to display information about the SIP ALG.

```
get test sip <test_level_int>
diagnose test application sip <test_level_int>
```

Use the following command to list all active SIP calls being processed by the SIP ALG. You can also use the `clear` option to delete all active SIP calls being processed by the SIP ALG.

```
diagnose sys sip-proxy calls {clear | list}
```

Use the following commands to use filters to display specific information about the SIP ALG and the session that it is processing.

```
diagnose sys sip-proxy filter <filter_options>
diagnose sys sip-proxy log-filter <filter_options>
```

Use the following command to display the active SIP rate limiting meters and their current settings.

```
diagnose sys sip-proxy meters list
```

Use the following command to display status information about the SIP sessions being processed by the SIP ALG. You can also clear all SIP ALG statistics.

```
diagnose sys sip-proxy stats {clear | list}
```

Conflicts between the SIP ALG and the session helper

Even if the SIP session helper is enabled, if a security policy with a VoIP profile that has SIP enabled accepts a SIP session on the TCP or UDP port that the SIP ALG listens on the ALG is used. You don’t need to turn off the session helper to use the ALG.
You may find that the session helper is being used for some SIP sessions even when you only want to use the ALG. This happens if a policy that does not include a VoIP profile is accepting SIP sessions. The VoIP profile could have been left out of the policy by mistake or the wrong policy could be accepting SIP sessions.

Consider a configuration with a SIP server on a private network that is contacted by SIP phones on the Internet and on the private network (similar to the configuration in Figure 6 on page 16). The FortiGate unit that provides NAT between the private network and the Internet requires a security policy with a firewall virtual IP that allows the SIP phones on the Internet to contact the SIP server. The FortiGate unit also requires outgoing security policies to allow the SIP phones and the SIP server to contact the SIP phones on the Internet.

If a VoIP profile is not added to one of the outgoing security policies the SIP sessions accepted by that policy will be processed by the SIP session helper instead of the SIP ALG. Also, its possible that some of the SIP sessions could be accepted by a general outgoing policy instead of the policy intended for SIP traffic. You can fix the first problem by adding a VoIP profile to the policy. You can fix the second problem by reviewing the security policy order and source and destination addresses in the security policies and determining if there is a conflict between these and the IP addresses of the SIP server or SIP phones on the Internal network.

You can use diagnose sys sip commands to determine if the SIP session helper is processing SIP sessions. For example, the following command displays the overall status of the SIP sessions being processed by the SIP session helper:

```
diagnose sys sip status
dialogs: max=32768, used=0
mappings: used=0
dialog hash by ID: size=2048, used=0, depth=0
dialog hash by RTP: size=2048, used=0, depth=0
mapping hash: size=2048, used=0, depth=0
count0: 0
count1: 0
count2: 0
count3: 0
count4: 0
```

This command output shows that the session helper is not processing SIP sessions because all of the used and count fields are 0. If any of these fields contains non-zero values then the SIP session helper may be processing SIP sessions.

Also, you can check to see if some ALG-only features are not being applied to all SIP sessions. For example, the VoIP usage widget on the FortiGate dashboard displays statistics for SIP and SCCP calls processed by the ALG but not for calls processed by the session helper. So if you see fewer calls than expected the session helper may be processing some of them.

Other logging and monitoring features such as log messages and DLP archiving are only supported by the ALG.

Finally, you can check the policy usage and session information dashboard widgets to see if SIP sessions are being accepted by the wrong security policies.
Stateful SIP tracking, call termination, and session inactivity timeout

The SIP ALG tracks SIP dialogs over their lifespan between the first INVITE message and the Final 200 OK and ACK messages. For every SIP dialog, stateful SIP tracking reviews every SIP message and makes adjustment to SIP tracking tables as required. These adjustments include source and destination IP addresses, address translation, dialog expiration information, and media stream port changes. Such changes can also result in dynamically opening and closing pinholes. You can use the `diagnose sys sip-proxy stats list` and the `diagnose sys sip-proxy filter` command to view the SIP call data being tracked by the SIP ALG.

The SIP ALG uses the SIP Expires header line to time out a SIP dialog if the dialog is idle and a Re-INVITE or UPDATE message is not received. The SIP ALG gets the Session-Expires value, if present, from the 200 OK response to the INVITE message. If the SIP ALG receives an INVITE before the session times out, all timeout values are reset to the settings in the new INVITE message or to default values. As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist. This ensures that the FortiGate unit is protected if a call ends prematurely.

When a SIP dialog ends normally, the SIP ALG deletes the SIP call information and closes open pinholes. A SIP call can also end abnormally due to an unexpected signaling or transport event that cuts off the call. When a call ends abnormally the SIP messages to end the call may not be sent or received. A call can end abnormally for the following reasons:

- Phones or servers crash during a call and a BYE message is not received.
- To attack a SIP system, a malicious user never send a BYE message.
- Poor implementations of SIP fail to process Record-Route messages and never send a BYE message.
- Network failures prevent a BYE message from being received.

Any phone or server in a SIP call can cancel the call by sending a CANCEL message. When a CANCEL message is received by the FortiGate unit, the SIP ALG closes open pinholes. Before terminating the call, the ALG waits for the final 200 OK message.

The SIP ALG can be configured to terminate SIP calls if the SIP dialog message flow or the call RTP (media) stream is interrupted and does not recover. You can use the following commands to configure terminating inactive SIP sessions and to set timers or counters to control when the call is terminated by the SIP ALG.

**Adding a media stream timeout for SIP calls**

Use the following command in a VoIP profile to terminate SIP calls accepted by a security policy containing the VoIP profile when the RTP media stream is idle for 100 seconds.

```shell
config voip profile
edit VoIP_Pro_Name
config sip
set call-keepalive 100
end
end
```

You can adjust this setting between 1 and 10,080 seconds. The default call keepalive setting of 0 disables terminating a call if the media stream is interrupted. Set call keepalive higher if your network has latency problems that could temporarily interrupt media streams. If you have configured call keepalive and the FortiGate unit terminates calls unexpectedly you can increase the call keepalive time to resolve the problem.
Adding an idle dialog setting for SIP calls

Use the following command in a VoIP profile to terminate SIP calls when for a single security policy, when the configured number of SIP calls (or dialogs) has stopped receiving SIP messages or has not received legitimate SIP messages. Using this command you can configure how many dialogs that have been accepted by a security policy that the VoIP profile is added to become idle before the SIP ALG deletes the oldest ones. The following command sets the maximum number of idle dialogs to 200:

```
config voip profile
edit VoIP_Pro_Name
config sip
  set max-idle-dialogs 200
end
end
```

Idle dialogs would usually be dialogs that have been interrupted because of errors or problems or as the result of a SIP attack that opens a large number of SIP dialogs without closing them. This command provides a way to remove these dialogs from the dialog table and recover memory and resources being used by these open and idle dialogs.

You can adjust this setting between 1 and a very high number. The default maximum idle dialogs setting of 0 disables this feature. Set maximum dialogs higher if your network has latency problems that could temporarily interrupt SIP messaging. If you have configured max idle dialogs and the FortiGate unit terminates calls unexpectedly you can increase the max idle dialogs number to resolve the problem.

Changing how long to wait for call setup to complete

In some cases and some configurations your SIP system may experience delays during call setup. If this happens, some SIP ALG timers may expire before call setup is complete and drop the call. In some cases you may also want to reduce the amount of time the SIP ALG allows for call setup to complete.

You can use the `provisional-invite-expiry-time` SIP VoIP profile option to control how long the SIP ALG waits for provisional INVITE messages before assuming that the call setup has been interrupted and the SIP call should be dropped. The default value for this timer is 210 seconds. You can change it to between 10 and 3600 seconds.

Use the following command to change the expiry time to 100 seconds.

```
config voip profile
edit Profile_name
  config sip
    set provisional-invite-expiry-time 100
end
end
```
SIP and RTP/RTCP

FortiGate units support the Real Time Protocol (RTP) application layer protocol for the VoIP call audio stream. RTP uses dynamically assigned port numbers that can change during a call. SIP control messages that start a call and that are sent during the call inform callers of the port number to use and of port number changes during the call.

During a call, each RTP session will usually have a corresponding Real Time Control Protocol (RTCP) session. By default, the RTCP session port number is one higher than the RTP port number.

The RTP port number is included in the m= part of the SDP profile. In the example above, the SIP INVITE message includes RTP port number is 49170 so the RTCP port number would be 49171. In the SIP response message the RTP port number is 3456 so the RTCP port number would be 3457.

How the SIP ALG creates RTP pinholes

The SIP ALG requires the following information to create a pinhole. The SIP ALG finds this information in SIP messages and some is provided by the SIP ALG:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>UDP (Extracted from SIP messages by the SIP ALG.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Any</td>
</tr>
<tr>
<td>Source port</td>
<td>Any</td>
</tr>
<tr>
<td>Destination IP</td>
<td>The SIP ALG extracts the destination IP address from the c= line in the SDP profile. The c= line can appear in either the session or media part of the SDP profile. The SIP ALG uses the IP address in the c= line of the media part of the SDP profile first. If the media part does not contain a c= line, the SIP ALG checks the c= line in the session part of the SDP profile. If the session part of the profile doesn’t contain a c= line the packet is dropped. Pinholes for RTP and RTCP sessions share the same destination IP address.</td>
</tr>
<tr>
<td>Destination port</td>
<td>The SIP ALG extracts the destination port number for RTP from the m= field and adds 1 to this number to get the RTCP port number.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The length of time during which the pinhole will be open. When the lifetime ends, the SIP ALG removes the pinhole.</td>
</tr>
</tbody>
</table>

The SIP ALG keeps RTP pinholes open as long as the SIP session is alive. When the associated SIP session is terminated by the SIP ALG or the SIP phones or servers participating in the call, the RTP pinhole is closed.

Figure 11 shows a simplified call setup sequence that shows how the SIP ALG opens pinholes. Phone A and Phone B are installed on either side of a FortiGate unit operating in Transparent mode. Phone A and Phone B are on the same subnet. The FortiGate unit includes a security policy that accepts SIP sessions from port1 to port2 and from port2 to port1. The FortiGate unit does not require an RTP security policy, just the SIP policy.

You can see from this diagram that the SDP profile in the INVITE request from Phone A indicates that Phone A is expecting to receive a media stream sent to its IP address using port 4000 for RTP and port 4001 for RTCP. The SIP ALG creates pinhole 1 to allow this media traffic to pass through the FortiGate unit. Pinhole 1 is opened on the Port2 interface and will accept media traffic sent from Phone B to Phone A.
When Phone B receives the INVITE request from Phone A, Phone B will know to send media streams to Phone A using destination IP address 10.31.101.20 and ports 4000 and 4001. The 200 OK response sent from Phone B indicates that Phone B is expecting to receive a media stream sent to its IP address using ports 8000 and 8001. The SIP ALG creates pinhole 2 to allow this media traffic to pass through the FortiGate unit. Pinhole 2 is opened on the Port1 interface and will accept media traffic sent from Phone A to Phone B.

Figure 11: SIP call setup with a FortiGate unit in Transparent mode

1. Phone A sends an INVITE request to Phone B (SDP 10.31.101.20:4000)
2. SIP ALG creates Pinhole 1. Accepts traffic on Port2 with destination address:port numbers 10.31.101.20:4000 and 4001
3. The SIP ALG forwards the INVITE request Phone B.
4. Phone B sends a 200 OK response to Phone A (SDP: 10.31.101.30:8000)
5. SIP ALG creates Pinhole 2. Accepts traffic on Port1 with destination address:port numbers 10.31.101.30:8000 and 8001
6. Phone B sends RTP and RTCP media sessions to Phone A through pinhole 1. Destination address:port number 172.20.120.20:4000 and 4001
7. Phone A sends RTP and RTCP media sessions to Phone B through pinhole 2. Destination address:port number 172.20.120.30:8000 and 8001

Configuration example: SIP in Transparent Mode

Figure 12 shows an example SIP network consisting of a FortiGate unit operating in Transparent mode between two SIP phones. Since the FortiGate unit is operating in Transparent mode both phones are on the same network and the FortiGate unit and the SIP ALG does not perform NAT. Even though the SIP ALG is not performing NAT you can use this configuration to apply SIP security features to the SIP traffic.
The FortiGate unit requires two security policies that accept SIP packets. One to allow SIP Phone A to start a session with SIP Phone B and one to allow SIP Phone B to start a session with SIP Phone A.

Figure 12: SIP network with FortiGate unit in Transparent mode

General configuration steps

The following general configuration steps are required for this SIP configuration. This example uses the default VoIP profile. The example also includes security policies that specifically allow SIP sessions using UDP port 5060 from Phone A to Phone B and from Phone B to Phone A. In most cases you would have more than two phones so would use more general security policies. Also, you can set the security service to ANY to allow traffic other than SIP on UDP port 5060.

1. Add firewall addresses for Phone A and Phone B.
2. Add a security policy that accepts SIP sessions initiated by Phone A and includes the default VoIP profile.
3. Add a security policy that accepts SIP sessions initiated by Phone B and includes the default VoIP profile.

Configuration steps - web-based manager

Before you begin this procedure you may have to enable VoIP support on the web-based manager by going to System > Admin > Settings and selecting the VoIP Support on GUI checkbox.

To add firewall addresses for the SIP phones

1. Go to Firewall Objects > Address.
2. Add the following addresses for Phone A and Phone B:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Type</th>
<th>Subnet / IP Range</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone_A</td>
<td>Subnet / IP Range</td>
<td>10.31.101.20/255.255.255.255</td>
<td>port1</td>
</tr>
<tr>
<td>Phone_B</td>
<td>Subnet / IP Range</td>
<td>10.31.101.30/255.255.255.255</td>
<td>port2</td>
</tr>
</tbody>
</table>
To add security policies to apply the SIP ALG to SIP sessions

1. Go to Policy > Policy > Policy.
2. Select Create New to add a security policy.
3. Add a security policy to allow Phone A to send SIP request messages to Phone B:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Phone_A</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Phone_B</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>SIP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>UTM</td>
<td>Select</td>
</tr>
<tr>
<td>Protocol Options</td>
<td>default</td>
</tr>
<tr>
<td>Enable VoIP</td>
<td>Select and select the default VoIP profile.</td>
</tr>
</tbody>
</table>

4. Select OK.
5. Add a security policy to allow Phone B to send SIP request messages to Phone A:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Phone_B</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Phone_A</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>SIP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>UTM</td>
<td>Select</td>
</tr>
<tr>
<td>Protocol Options</td>
<td>default</td>
</tr>
<tr>
<td>Enable VoIP</td>
<td>Select (And select the default VoIP profile)</td>
</tr>
</tbody>
</table>

6. Select OK.

Configuration steps - CLI

To add firewall addresses for Phone A and Phone B and security policies to apply the SIP ALG to SIP sessions

1. Enter the following command to add firewall addresses for Phone A and Phone B.

```plaintext
config firewall address
edit Phone_A
    set associated interface port1
    set type ipmask
    set subnet 10.31.101.20 255.255.255.255
next
```
edit Phone_B
  set associated interface port2
  set type ipmask
  set subnet 10.31.101.30 255.255.255.255
end

2 Enter the following command to add security policies to allow Phone A to send SIP request messages to Phone B and Phone B to send SIP request messages to Phone A.

```
config firewall policy
edit 0
  set srcintf port1
  set dstintf port2
  set srcaddr Phone_A
  set dstaddr Phone_B
  set action accept
  set schedule always
  set service SIP
  set utm-status enable
  set profile-protocol-options default
  set voip-profile default
next
edit 0
  set srcintf port2
  set dstintf port1
  set srcaddr Phone_B
  set dstaddr Phone_A
  set action accept
  set schedule always
  set service SIP
  set utm-status enable
  set profile-protocol-options default
  set voip-profile default
end
```

RTP enable/disble (RTP bypass)

You can configure the SIP ALG to stop from opening RTP pinholes. Called RTP bypass, this configuration can be used when you want to apply SIP ALG features to SIP signalling messages but do not want the RTP media streams to pass through the FortiGate unit. The FortiGate unit only acts as a signalling firewall and RTP media session bypass the FortiGate unit and no pinholes need to be created.

Enter the following command to enable RTP bypass in a VoIP profile by disabling opening RTP pinholes:

```
config voip profile
edit VoIP_Pro_1
  config sip
    set rtp disable
end
end
```
Opening and closing SIP register and non-register pinholes

You can use the open-register-pinhole and open-contact-pinhole VoIP profile CLI options to control whether the FortiGate unit opens register and non-register pinholes. Non-register pinholes are usually opened for SIP INVITE requests.

By default for new VoIP profiles and for both pre-defined VoIP profiles open-register-pinhole is enabled and the FortiGate unit opens pinholes for SIP Register request messages. You can disable open-register-pinhole so that the FortiGate unit does not open pinholes for SIP Register request messages.

By default for new VoIP profiles and for the default pre-defined VoIP profile open-contact-pinhole is enabled and the FortiGate unit opens pinholes for non-Register SIP request messages. You can disable open-contact-pinhole so that the FortiGate unit does not open pinholes for non-register requests. This option is not enabled for the strict pre-defined VoIP profile.

Usually you would want to open these pinholes. Keeping them closed may prevent SIP from functioning properly through the FortiGate unit. They can be disabled, however, for interconnect scenarios (where all SIP traffic is between proxies and traveling over a single session). In some cases these settings can also be disabled in access scenarios if it is known that all users will be registering regularly so that their contact information can be learned from the register request.

You might want to prevent pinholes from being opened to avoid creating a pinhole for every register or non-register request. Each pinhole uses additional system memory, which can affect system performance if there are hundreds or thousands of users, and requires refreshing which can take a relatively long amount of time if there are thousands of active calls.

To configure a VoIP profile to prevent opening register and non-register pinholes:

```
config voip profile
edit VoIP_Pro_1
  config sip
    set open-register-pinhole disable
    set open-contact-pinhole disable
  end
end
```

In some cases you may not want to open pinholes for the port numbers specified in SIP Contact headers. For example, in an interconnect scenario when a FortiGate unit is installed between two SIP servers and the only SIP traffic through the FortiGate unit is between these SIP servers pinholes may not need to be opened for the port numbers specified in the Contact header lines.

If you disable open-register-pinhole then pinholes are not opened for ports in Contact header lines in SIP Register messages. If you disable open-contact-pinhole then pinholes are not opened for ports in Contact header lines in all SIP messages except SIP Register messages.

Accepting SIP register responses

You can enable the VoIP profile reg-diff-port options to accept a SIP Register response message from a SIP server even if the source port of the Register response message is different from the destination port.
Most SIP servers use 5060 as the source port in the SIP register response. Some SIP servers, however, may use a different source port. If your SIP server uses a different source port, you can enable `reg-diff-port` and the SIP ALG will create a temporary pinhole when Register request from a SIP client includes a different source port. The FortiGate unit will accept a SIP Register response with any source port number from the SIP server.

Enter the following command to enable accepting any source port from a SIP server:

```
config voip profile
  edit VoIP_Pro_1
  config sip
    set reg-diff-port enable
  end
end
```

How the SIP ALG performs NAT

In most Network Address Translation (NAT) configurations, multiple hosts in a private network share a single public IP address to access the Internet. For sessions originating on the private network for the Internet, NAT replaces the private IP address of the PC in the private subnet with the public IP address of the NAT device. The NAT device converts the public IP address for responses from the Internet back into the private address before sending the response over the private network to the originator of the session.

Using NAT with SIP is more complex because of the IP addresses and media stream port numbers used in SIP message headers and bodies. When a caller on the private network sends a SIP message to a phone or SIP server on the Internet, the SIP ALG must translate the private network addresses in the SIP message to IP addresses and port numbers that are valid on the Internet. When the response message is sent back to the caller, the SIP ALG must translate these addresses back to valid private network addresses.

In addition, the media streams generated by the SIP session are independent of the SIP message sessions and use varying port numbers that can also change during the media session. The SIP ALG opens pinholes to accept these media sessions, using the information in the SIP messages to determine the pinholes to open. The ALG may also perform port translation on the media sessions.

When an INVITE message is received by the SIP ALG, the FortiGate unit extracts addressing and port number information from the message header and stores it in a SIP dialog table. Similar to an IP session table the data in the dialog table is used to translate addresses in subsequent SIP messages that are part of the same SIP call.

When the SIP ALG receives a response to the INVITE message arrives, (for example, an ACK or 200 OK), the SIP ALG compares the addresses in the message fields against the entries in the SIP dialog table to identify the call context of the message. The SIP ALG then translates addresses in the SIP message before forwarding them to their destination.

The addressing and port number information in SDP fields is used by the ALG to reserve ports for the media session and create a NAT mapping between them and the ports in the SDP fields. Because SDP uses sequential ports for the RTP and RTCP channels, the ALG provides consecutive even-odd ports.
Source address translation

When a SIP call is started by a phone on a private network destined for a phone on the Internet, only source address translation is required. The phone on the private network attempts to contact the actual IP address of the phone on the Internet. However, the source address of the phone on the private network is not routable on the Internet so the SIP ALG must translate all private IP addresses in the SIP message into public IP addresses.

To configure the FortiGate for source address translation you add security policy that accepts sessions from the internal network destined for the Internet. You must enable NAT for the security policy and add a VoIP profile.

When a SIP request is received from the internal to the external network, the SIP ALG replaces the private network IP addresses and port numbers in the SIP message with the IP address of the FortiGate interface connected to the Internet. Depending on the content of the message, the ALG translates addresses in the Via:, Contact:, Route:, and Record-Route: SIP header fields. The message is then forwarded to the destination (either a VoIP phone or a SIP server on the Internet).

The VoIP phone or server in the Internet sends responses to these SIP messages to the external interface of the FortiGate unit. The addresses in the response messages are translated back into private network addresses and the response is forwarded to the originator of the request.

For the RTP communication between the SIP phones, the SIP ALG opens pinholes to allow media through the FortiGate unit on the dynamically assigned ports negotiated based on information in the SDP and the Via:, Contact:, and Record-Route: header fields. The pinholes also allow incoming packets to reach the Contact:, Via:, and Record-Route: IP addresses and ports. When processing return traffic, the SIP ALG inserts the original Contact:, Via:, Route:, and Record-Route: SIP fields back into the packets.

Destination address translation

Incoming calls are directed from a SIP phone on the Internet to the interface of the FortiGate unit connected to the Internet. To receive these calls you must add a security policy to accept SIP sessions from the Internet. The security policy requires a firewall virtual IP. SIP INVITE messages from the Internet connect to the external IP address of the virtual IP. The SIP ALG uses the destination address translation defined in the virtual IP to translated the addresses in the SIP message to addresses on the private network.

When a 200 OK response message arrives from the private network, the SIP ALG translates the addresses in the message to Internet addresses and opens pinholes for media sessions from the private network to the Internet.

When the ACK message is received for the 200 OK, it is also intercepted by the SIP ALG. If the ACK message contains SDP information, the SIP ALG checks to determine if the IP addresses and port numbers are not changed from the previous INVITE. If they are, the SIP ALG deletes pinholes and creates new ones as required. The ALG also monitors the Via:, Contact:, and Record-Route: SIP fields and opens new pinholes as required.

Call Re-invite messages

SIP Re-INVITE messages can dynamically add and remove media sessions during a call. When new media sessions are added to a call the SIP ALG opens new pinholes and update SIP dialog data. When media sessions are ended, the SIP ALG closes pinholes that are no longer needed and removes SIP dialog data.
How the SIP ALG translates IP addresses in SIP headers

The SIP ALG applies NAT to SIP sessions by translating the IP addresses contained in SIP headers. For example, the following SIP message contains most of the SIP fields that contain addresses that need to be translated:

```
INVITE PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 172.20.120.50:5434
From: PhoneA@10.31.101.20
To: PhoneB@172.20.120.30
Call-ID: a12abcde@172.20.120.50
Contact: PhoneA@10.31.101.20:5434
Route: <sip:example@172.20.120.50:5060>
Record-Route: <sip:example@172.20.120.50:5060>
```

How IP address translation is performed depends on whether source NAT or destination NAT is applied to the session containing the message:

**Source NAT translation of IP addresses in SIP messages**

Source NAT translation occurs for SIP messages sent from a phone or server on a private network to a phone or server on the Internet. The source addresses in the SIP header fields of the message are typically set to IP addresses on the private network. The SIP ALG translates these addresses to the address the FortiGate unit interface connected to the Internet.

<table>
<thead>
<tr>
<th>SIP header</th>
<th>NAT action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To:</td>
<td>None</td>
</tr>
<tr>
<td>From:</td>
<td>Replace private network address with IP address of FortiGate unit interface connected to the Internet.</td>
</tr>
<tr>
<td>Call-ID:</td>
<td>Replace private network address with IP address of FortiGate unit interface connected to the Internet.</td>
</tr>
<tr>
<td>Via:</td>
<td>Replace private network address with IP address of FortiGate unit interface connected to the Internet.</td>
</tr>
<tr>
<td>Request-URI:</td>
<td>None</td>
</tr>
<tr>
<td>Contact:</td>
<td>Replace private network address with IP address of FortiGate unit interface connected to the Internet.</td>
</tr>
<tr>
<td>Record-Route:</td>
<td>Replace private network address with IP address of FortiGate unit interface connected to the Internet.</td>
</tr>
<tr>
<td>Route:</td>
<td>Replace private network address with IP address of FortiGate unit interface connected to the Internet.</td>
</tr>
</tbody>
</table>

Response messages from phones or servers on the Internet are sent to the FortiGate unit interface connected to the Internet where the destination addresses are translated back to addresses on the private network before forwarding the SIP response message to the private network.
How the SIP ALG performs NAT

FortiGate Voice for FortiOS 4.0 MR3

Destination NAT translation of IP addresses in SIP messages

Destination NAT translation occurs for SIP messages sent from a phone or server on the Internet to a firewall virtual IP address. The destination addresses in the SIP header fields of the message are typically set to the virtual IP address. The SIP ALG translates these addresses to the address of a SIP server or phone on the private network on the other side of the FortiGate unit.

Table 5: Source NAT translation of IP addresses in SIP response messages

<table>
<thead>
<tr>
<th>SIP header</th>
<th>NAT action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To:</td>
<td>None</td>
</tr>
<tr>
<td>From:</td>
<td>Replace IP address of FortiGate unit interface connected to the Internet with private network address.</td>
</tr>
<tr>
<td>Call-ID:</td>
<td>Replace IP address of FortiGate unit interface connected to the Internet with private network address.</td>
</tr>
<tr>
<td>Via:</td>
<td>Replace IP address of FortiGate unit interface connected to the Internet with private network address.</td>
</tr>
<tr>
<td>Request-URI:</td>
<td>N/A</td>
</tr>
<tr>
<td>Contact:</td>
<td>None</td>
</tr>
<tr>
<td>Record-Route:</td>
<td>Replace IP address of FortiGate unit interface connected to the Internet with private network address.</td>
</tr>
<tr>
<td>Route:</td>
<td>Replace IP address of FortiGate unit interface connected to the Internet with private network address.</td>
</tr>
</tbody>
</table>

Table 6: Destination NAT translation of IP addresses in SIP request messages

<table>
<thead>
<tr>
<th>SIP header</th>
<th>NAT action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To:</td>
<td>Replace VIP address with address on the private network as defined in the firewall virtual IP.</td>
</tr>
<tr>
<td>From:</td>
<td>None</td>
</tr>
<tr>
<td>Call-ID:</td>
<td>None</td>
</tr>
<tr>
<td>Via:</td>
<td>None</td>
</tr>
<tr>
<td>Request-URI:</td>
<td>Replace VIP address with address on the private network as defined in the firewall virtual IP.</td>
</tr>
<tr>
<td>Contact:</td>
<td>None</td>
</tr>
<tr>
<td>Record-Route:</td>
<td>None</td>
</tr>
<tr>
<td>Route:</td>
<td>None</td>
</tr>
</tbody>
</table>

SIP response messages sent in response to the destination NAT translated messages are sent from a server or a phone on the private network back to the originator of the request messages on the Internet. These reply messages are accepted by the same security policy that accepted the initial request messages. The firewall VIP in the original security policy contains the information that the SIP ALG uses to translate the private network source addresses in the SIP headers into the firewall virtual IP address.
FortiGate VoIP solutions: SIP

How the SIP ALG performs NAT

Table 7: Destination NAT translation of IP addresses in SIP response messages

<table>
<thead>
<tr>
<th>SIP header</th>
<th>NAT action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To:</td>
<td>None</td>
</tr>
<tr>
<td>From:</td>
<td>Replace private network address with firewall VIP address.</td>
</tr>
<tr>
<td>Call-ID:</td>
<td>None</td>
</tr>
<tr>
<td>Via:</td>
<td>None</td>
</tr>
<tr>
<td>Request-URI:</td>
<td>N/A</td>
</tr>
<tr>
<td>Contact:</td>
<td>Replace private network address with firewall VIP address.</td>
</tr>
<tr>
<td>Record-Route:</td>
<td>Replace private network address with firewall VIP address.</td>
</tr>
<tr>
<td>Route:</td>
<td>None</td>
</tr>
</tbody>
</table>

How the SIP ALG translates IP addresses in the SIP body

The SDP session profile attributes in the SIP body include IP addresses and port numbers that the SIP ALG uses to create pinholes for the media stream.

The SIP ALG translates IP addresses and port numbers in the o=, c=, and m= SDP lines. For example, in the following lines the ALG could translate the IP addresses in the o= and c= lines and the port number (49170) in the m= line.

\[
\begin{align*}
& o=PhoneA 5462346 332134 IN IP4 10.31.101.20 \\
& c=IN IP4 10.31.101.20 \\
& m=audio 49170 RTP 0 3
\end{align*}
\]

If the SDP session profile includes multiple RTP media streams, the SIP ALG opens pinholes and performs the required address translation for each one.

The two most important SDP attributes for the SIP ALG are c= and m=. The c= attribute is the connection information attribute. This field can appear at the session or media level. The syntax of the connection attribute is:

\[
c=IN \{IPV4 | IPV6\} \text{destination_ip_address}
\]

Where

- \(\text{IN}\) is the network type. FortiGate units support the \(\text{IN}\) or Internet network type.
- \(\{IPV4 | IPV6\}\) is the address type. FortiGate units support IPv4 or IPv6 addresses in SDP statements. However, FortiGate units do not support all types of IPv6 address translation. See “SIP over IPv6” on page 77.
- \(\text{destination_ip_address}\) is the unicast numeric destination IP address or domain name of the connection in either IPv4 or IPv6 format.

The syntax of the media attribute is:

\[
m=audio <\text{port_number}> RTP <\text{format_list}>
\]

Where

- \(\text{audio}\) is the media type. FortiGate units support the \(\text{audio}\) media type.
- \(<\text{port_number}>\) is the destination port number used by the media stream.
- \(\text{RTP}\) is the application layer transport protocol used for the media stream. FortiGate units support the Real Time Protocol (RTP) transport protocol.
- \(<\text{format_list}>\) is the format list that provides information about the application layer protocol that the media uses.
SIP NAT scenario: source address translation (source NAT)

Figure 13 and Figure 14 show a source address translation scenario involving two SIP phones on different networks, separated by a FortiGate unit. In the scenario, SIP Phone A sends an INVITE request to SIP Phone B and SIP Phone B replies with a 200 OK response and then the two phones start media streams with each other.

To simplify the diagrams, some SIP messages are not included (for example, the Ringing and ACK response messages) and some SIP header lines and SDP profile lines have been removed from the SIP messages.

Figure 13: SIP source NAT scenario part 1: INVITE request sent from Phone A to Phone B

For the replies to SIP packets sent by Phone A to be routable on Phone B’s network, the FortiGate unit uses source NAT to change their source address to the address of the WAN1 interface. The SIP ALG makes similar changes to the source addresses in the SIP headers and SDP profile. For example, the original INVITE request from Phone A includes the address of Phone A (10.31.101.20) in the from header line. After the INVITE request passes through the FortiGate unit, the address of Phone A in the From SIP header line is translated to 172.20.120.122, the address of the FortiGate unit WAN1 interface. As a result, Phone B will reply to SIP messages from Phone A using the WAN1 interface IP address.
The FortiGate unit also opens a pinhole so that it can accept media sessions sent to the WAN1 IP address using the port number in the m= line of the INVITE request and forward them to Phone A after translating the destination address to the IP address of Phone A.

Phone B sends the 200 OK response to the INVITE message to the WAN1 interface. The SDP profile includes the port number that Phone B wants to use for its media stream. The FortiGate unit forwards 200 OK response to Phone A after translating the addresses in the SIP and SDP lines back to the IP address of Phone A. The SIP ALG also opens a pinhole on the Internal interface that accepts media stream sessions from Phone A with destination address set to the IP address of Phone B and using the port that Phone B added to the SDP m= line.

**Figure 14: SIP source NAT scenario part 2: 200 OK returned and media streams established**
SIP NAT scenario: destination address translation (destination NAT)

Figure 15 and Figure 16 show how the SIP ALG translates addresses in a SIP INVITE message sent from SIP Phone B on the Internet to SIP Phone A on a private network using the SIP proxy server. Because the addresses on the private network are not visible from the Internet, the security policy on the FortiGate unit that accepts SIP sessions includes a virtual IP. Phone A sends SIP the INVITE message to the virtual IP address. The FortiGate unit accepts the INVITE message packets and using the virtual IP, translates the destination address of the packet to the IP address of the SIP proxy server and forwards the SIP message to it.

To simplify the diagrams, some SIP messages are not included (for example, the Ringing and ACK response messages) and some SIP header lines and SDP profile lines have been removed from the SIP messages.

The SIP ALG also translates the destination addresses in the SIP message from the virtual IP address (172.20.120.50) to the SIP proxy server address (10.31.101.50). For this configuration to work, the SIP proxy server must be able to change the destination addresses for Phone A in the SIP message from the address of the SIP proxy server to the actual address of Phone A.

The SIP ALG also opens a pinhole on the Port2 interface that accepts media sessions from the private network to SIP Phone B using ports 4900 and 4901.
Figure 15: SIP destination NAT scenario part 1: INVITE request sent from Phone B to Phone A

1. Phone B sends an INVITE request for Phone A to the SIP Proxy Server Virtual IP (SDP 172.20.120.30:4900)

INVITE sip:PhoneA@172.20.120.50 SIP/2.0
Via: SIP/2.0/UDP 172.20.120.50:5060
From: PhoneB <sip:PhoneB@172.20.120.30>
To: PhoneA <sip:PhoneA@172.20.120.50>
Call-ID: 314134@172.20.120.30
CSeq: 1 INVITE
Contact: sip:PhoneB@172.20.120.30
v=0
ct=PhoneB 2346 134 IN IP4 172.20.120.30
m=audio 4900 RTP 0 3

2. SIP ALG creates Pinhole 1. Accepts traffic on Port2 with destination address:port numbers 172.20.120.30:4900 and 4901

3. The SIP ALG performs destination NAT on the INVITE request and forwards it to the SIP proxy server.

INVITE sip:PhoneA@10.31.101.50 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.50:5060
From: PhoneB <sip:PhoneB@10.31.101.20>
To: PhoneA <sip:PhoneA@10.31.101.20>
Call-ID: 314134@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneB@10.31.101.20
v=0
ct=PhoneB 2346 134 IN IP4 10.31.101.20
m=audio 4900 RTP 0 3

4. The SIP proxy server forwards the INVITE request to Phone A (SDP: 172.20.120.30:4900)

INVITE sip:PhoneA@10.31.101.50 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.50:5060
From: PhoneB <sip:PhoneB@10.31.101.20>
To: PhoneA <sip:PhoneA@172.20.120.50>
Call-ID: 314134@172.20.120.30
CSeq: 1 INVITE
Contact: sip:PhoneB@172.20.120.30
v=0
ct=PhoneB 2346 134 IN IP4 172.20.120.30
m=audio 4900 RTP 0 3

Phone A sends a 200 OK response back to the SIP proxy server. The SIP proxy server forwards the response to Phone B. The FortiGate unit accepts the 100 OK response. The SIP ALG translates the Phone A addresses back to the SIP proxy server virtual IP address before forwarding the response back to Phone B. The SIP ALG also opens a pinhole using the SIP proxy server virtual IP which is the address in the o= line of the SDP profile and the port number in the m= line of the SDP code.
Figure 16: SIP destination NAT scenario part 2: 200 OK returned to Phone B and media streams established

The media stream from Phone A is accepted by pinhole one and forwarded to Phone B. The source address of this media stream is changed to the SIP proxy server virtual IP address. The media stream from Phone B is accepted by pinhole 2 and forwarded to Phone B. The destination address of this media stream is changed to the IP address of Phone A.

SIP NAT configuration example: source address translation (source NAT)

This configuration example shows how to configure the FortiGate unit to support the source address translation scenario shown in Figure 17. The FortiGate unit requires two security policies that accept SIP packets. One to allow SIP Phone A to start a session with SIP Phone B and one to allow SIP Phone B to start a session with SIP Phone A. Both of these policies must include source NAT. In this example the networks are not hidden from each other so destination NAT is not required.
General configuration steps

The following general configuration steps are required for this SIP configuration. This example uses the default VoIP profile. The example also includes security policies that specifically allow SIP sessions using UDP port 5060 from Phone A to Phone B and from Phone B to Phone A. In most cases you would have more than two phones so would use more general security policies. Also, you can set the firewall service to ANY to allow traffic other than SIP on UDP port 5060.

1. Add firewall addresses for Phone A and Phone B.
2. Add a security policy that accepts SIP sessions initiated by Phone A and includes the default VoIP profile.
3. Add a security policy that accepts SIP sessions initiated by Phone B and includes the default VoIP profile.

Configuration steps - web-based manager

To add firewall addresses for the SIP phones

1. Go to Firewall Objects > Address.
2. Add the following addresses for Phone A and Phone B:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Phone_A</th>
<th>Type</th>
<th>Subnet / IP Range</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Subnet / IP Range</td>
<td>10.31.101.20/255.255.255.255</td>
<td>Internal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Phone_B</th>
<th>Type</th>
<th>Subnet / IP Range</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Subnet / IP Range</td>
<td>172.20.120.30/255.255.255.255</td>
<td>wan1</td>
</tr>
</tbody>
</table>

To add security policies to apply the SIP ALG to SIP sessions

1. Go to Policy > Policy > Policy.
2. Select Create New to add a security policy.
3. Add a security policy to allow Phone A to send SIP request messages to Phone B:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Phone_A</td>
</tr>
</tbody>
</table>
4. Select OK.

5. Add a security policy to allow Phone B to send SIP request messages to Phone A:

<table>
<thead>
<tr>
<th>Destination Interface/Zone</th>
<th>wan1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Address</td>
<td>Phone_B</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>SIP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Select</td>
</tr>
<tr>
<td>UTM</td>
<td>Select</td>
</tr>
<tr>
<td>Protocol Options</td>
<td>default</td>
</tr>
<tr>
<td>Enable VoIP</td>
<td>Select and select the default VoIP profile.</td>
</tr>
</tbody>
</table>

6. Select OK.

**Configuration steps - CLI**

To add firewall addresses for Phone A and Phone B and security policies to apply the SIP ALG to SIP sessions

1. Enter the following command to add firewall addresses for Phone A and Phone B.

```
config firewall address
edit Phone_A
    set associated interface internal
    set type ipmask
    set subnet 10.31.101.20 255.255.255.255
next
edit Phone_B
    set associated interface wan1
    set type ipmask
    set subnet 172.20.120.30 255.255.255.255
end
```
2 Enter the following command to add security policies to allow Phone A to send SIP request messages to Phone B and Phone B to send SIP request messages to Phone A.

```
config firewall policy
  edit 0
    set srcintf internal
    set dstintf wan1
    set srcaddr Phone_A
    set dstaddr Phone_B
    set action accept
    set schedule always
    set service SIP
    set nat enable
    set utm-status enable
    set profile-protocol-options default
    set voip-profile default
next
  edit 0
    set srcintf wan1
    set dstintf internal
    set srcaddr Phone_B
    set dstaddr Phone_A
    set action accept
    set schedule always
    set service SIP
    set nat enable
    set utm-status enable
    set profile-protocol-options default
    set voip-profile default
end
```

**SIP NAT configuration example: destination address translation (destination NAT)**

This configuration example shows how to configure the FortiGate unit to support the destination address translation scenario shown in Figure 18. The FortiGate unit requires two SIP security policies:

- A destination NAT security policy that allows SIP messages to be sent from the Internet to the private network. This policy must include destination NAT because the addresses on the private network are not routable on the Internet.
- A source NAT security policy that allows SIP messages to be sent from the private network to the Internet.
General configuration steps

The following general configuration steps are required for this destination NAT SIP configuration. This example uses the default VoIP profile.

1. Add the SIP proxy server firewall virtual IP.
2. Add a firewall address for the SIP proxy server on the private network.
3. Add a destination NAT security policy that accepts SIP sessions from the Internet destined for the SIP proxy server virtual IP and translates the destination address to the IP address of the SIP proxy server on the private network.
4. Add a security policy that accepts SIP sessions initiated by the SIP proxy server and destined for the Internet.

Configuration steps - web-based manager

To add the SIP proxy server firewall virtual IP
1. Go to Firewall Objects > Virtual IP > Virtual IP.
2. Add the SIP proxy server virtual IP.

<table>
<thead>
<tr>
<th>Name</th>
<th>SIP_Proxy_VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Interface</td>
<td>port1</td>
</tr>
<tr>
<td>Type</td>
<td>Static NAT</td>
</tr>
<tr>
<td>External IP Address/Range</td>
<td>172.20.120.50</td>
</tr>
<tr>
<td>Mapped IP Address/Range</td>
<td>10.31.101.50</td>
</tr>
</tbody>
</table>

To add a firewall address for the SIP proxy server
1. Go to Firewall Objects > Address.
2. Add the following for the SIP proxy server:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>SIP_Proxy_Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.31.101.50/255.255.255.255</td>
</tr>
<tr>
<td>Interface</td>
<td>port2</td>
</tr>
</tbody>
</table>
To add the security policies

1. Go to Policy > Policy > Policy.

2. Add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone B (and other SIP phones on the Internet) to send SIP request messages to the SIP proxy server.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>SIP_Proxy_VIP</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>SIP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Select</td>
</tr>
<tr>
<td>UTM</td>
<td>Select</td>
</tr>
<tr>
<td>Protocol Options</td>
<td>default</td>
</tr>
<tr>
<td>Enable VoIP</td>
<td>Select (And select the default VoIP profile)</td>
</tr>
</tbody>
</table>

3. Select OK.

4. Add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B and the Internet:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>SIP_Proxy_Server</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>SIP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Select</td>
</tr>
<tr>
<td>UTM</td>
<td>Select</td>
</tr>
<tr>
<td>Protocol Options</td>
<td>default</td>
</tr>
<tr>
<td>Enable VoIP</td>
<td>Select (And select the default VoIP profile)</td>
</tr>
</tbody>
</table>

5. Select OK.

Configuration steps - CLI

To add the SIP proxy server firewall virtual IP and firewall address

1. Enter the following command to add the SIP proxy server firewall virtual IP.

```bash
config firewall vip
edit SIP_Proxy_VIP
  set type static-nat
  set extip 172.20.120.50
```
set mappedip 10.31.101.50
set extintf port1
end

2 Enter the following command to add the SIP proxy server firewall address.

```
config firewall address
edit SIP_Proxy_Server
    set associated interface port2
    set type ipmask
    set subnet 10.31.101.50 255.255.255.255
end
```

To add security policies

1 Enter the following command to add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone B (and other SIP phones on the Internet) to send SIP request messages to the SIP proxy server.

```
config firewall policy
edit 0
    set srcintf port1
    set dstintf port2
    set srcaddr all
    set dstaddr SIP_Proxy_VIP
    set action accept
    set schedule always
    set service SIP
    set nat enable
    set utm-status enable
    set profile-protocol-options default
    set voip-profile default
end
```

2 Enter the following command to add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B and the Internet:

```
config firewall policy
edit 0
    set srcintf port2
    set dstintf port1
    set srcaddr SIP_Proxy_Server
    set dstaddr all
    set action accept
    set schedule always
    set service SIP
    set nat enable
    set utm-status enable
    set profile-protocol-options default
    set voip-profile default
end
```

**Additional SIP NAT scenarios**

This section lists some additional SIP NAT scenarios.
Source NAT (SIP and RTP)

In the source NAT scenario shown in Figure 19, a SIP phone connects to the Internet through a FortiGate unit with an IP address configured using PPPoE. The SIP ALG translates all private IPs in the SIP contact header into public IPs.

You need to configure an internal to external SIP security policy with NAT selected, and include a VoIP profile with SIP enabled.

Figure 19: SIP source NAT

Destination NAT (SIP and RTP)

In the following destination NAT scenario, a SIP phone can connect through the FortiGate unit to private IP address using a firewall virtual IP (VIP). The SIP ALG translates the SIP contact header to the IP of the real SIP proxy server located on the Internet.

Figure 20: SIP destination NAT

In the scenario, shown in Figure 20, the SIP phone connects to a VIP (10.72.0.60). The SIP ALG translates the SIP contact header to 217.10.79.9, opens RTP pinholes, and manages NAT.
The FortiGate unit also supports a variation of this scenario where the RTP media server’s IP address is hidden on a private network or DMZ.

**Figure 21: SIP destination NAT-RTP media server hidden**

In the scenario shown in Figure 21, a SIP phone connects to the Internet. The VoIP service provider only publishes a single public IP. The FortiGate unit is configured with a firewall VIP. The SIP phone connects to the FortiGate unit (217.233.90.60) and using the VIP the FortiGate unit translates the SIP contact header to the SIP proxy server IP address (10.0.0.60). The SIP proxy server changes the SIP/SDP connection information (which tells the SIP phone which RTP media server IP it should contact) also to 217.233.90.60.

### Source NAT with an IP pool

You can choose NAT with the *Dynamic IP Pool* option when configuring a security policy if the source IP of the SIP packets is different from the interface IP. The FortiGate ALG interprets this configuration and translates the SIP header accordingly.

This configuration also applies to destination NAT.

### Different source and destination NAT for SIP and RTP

This is a more complex scenario that a SIP service provider may use. It can also be deployed in large-scale SIP environments where RTP has to be processed by the FortiGate unit and the RTP server IP has to be translated differently than the SIP server IP.
In this scenario, shown in Figure 22, assume there is a SIP server and a separate media gateway. The SIP server is configured so that the SIP phone (219.29.81.20) will connect to 217.233.90.60. The media gateway (RTP server: 219.29.81.10) will connect to 217.233.90.65.

What happens is as follows:

1. The SIP phone connects to the SIP VIP. The FortiGate ALG translates the SIP contact header to the SIP server: 219.29.81.20 > 217.233.90.60 (> 10.0.0.60).
2. The SIP server carries out RTP to 217.233.90.65.
3. The FortiGate ALG opens pinholes, assuming that it knows the ports to be opened.
4. RTP is sent to the RTP-VIP (217.233.90.65.) The FortiGate ALG translates the SIP contact header to 192.168.0.21.

**NAT with IP address conservation**

In a source or destination NAT security policy that accepts SIP sessions, you can configure the SIP ALG or the SIP session helper to preserve the original source IP address of the SIP message in the i= line of the SDP profile. NAT with IP address conservation (also called SIP NAT tracing) changes the contents of SIP messages by adding the source IP address of the originator of the message into the SDP i= line of the SIP message. The SDP i= line is used for free-form text. However, if your SIP server can retrieve information from the SDP i= line, it can be useful for keeping a record of the source IP address of the originator of a SIP message when operating in a NAT environment. You can use this feature for billing purposes by extracting the IP address of the originator of the message.

**Configuring SIP IP address conservation for the SIP ALG**

You can use the following command to enable or disable SIP IP address conservation in a VoIP profile for the SIP ALG. SIP IP address conservation is enabled by default in a VoIP profile.

```bash
config voip profile
edit VoIP_Pro_1
    config sip
```

**Figure 22: Different source and destination NAT for SIP and RTP**
How the SIP ALG performs NAT

FortiGate VoIP solutions: SIP

set nat-trace disable
end
end

If the SIP message does not include an i= line and if the original source IP address of the traffic (before NAT) was 10.31.101.20 then the FortiGate unit would add the following i= line.

i=(o=IN IP4 10.31.101.20)

You can also use the preserve-override option to configure the SIP ALG to either add the original o= line to the end of the i= line or replace the i= line in the original message with a new i= line in the same form as above for adding a new i= line.

By default, preserve-override is disabled and the SIP ALG adds the original o= line to the end of the original i= line. Use the following command to configure the SIP ALG to replace the original i= line:

```
config voip profile
edit VoIP_Pro_1
config sip
set preserve-override enable
end
end
```

Configuring SIP IP address conservation for the SIP session helper

You can use the following command to enable or disable SIP IP address conservation for the SIP session helper. IP address conservation is enabled by default for the SIP session helper.

```
config system settings
set sip-nat-trace disable
end
```

If the SIP message does not include an i= line and if the original source IP address of the traffic (before NAT) was 10.31.101.20 then the FortiGate unit would add the following i= line.

i=(o=IN IP4 10.31.101.20)

Controlling how the SIP ALG NATs SIP contact header line addresses

You can enable contact-fixup so that the SIP ALG performs normal SIP NAT translation to SIP contact headers as SIP messages pass through the FortiGate unit.

Disable contact-fixup if you do not want the SIP ALG to perform normal NAT translation of the SIP contact header if a Record-Route header is also available. If contact-fixup is disabled, the FortiGate ALG does the following with contact headers:

- For Contact in Requests, if a Record-Route header is present and the request comes from the external network, the SIP Contact header is not translated.
- For Contact in Responses, if a Record-Route header is present and the response comes from the external network, the SIP Contact header is not translated.

If contact-fixup is disabled, the SIP ALG must be able to identify the external network. To identify the external network, you must use the config system interface command to set the external keyword to enable for the interface that is connected to the external network.

Enter the following command to perform normal NAT translation of the SIP contact header:

```
config voip profile
```
Controlling NAT for addresses in SDP lines

You can use the `no-sdp-fixup` option to control whether the FortiGate unit performs NAT on addresses in SDP lines in the SIP message body.

The `no-sdp-fixup` option is disabled by default and the FortiGate unit performs NAT on addresses in SDP lines. Enable this option if you don’t want the FortiGate unit to perform NAT on the addresses in SDP lines.

```bash
config voip profile
edit VoIP_Pro_1
config sip
  set no-sdp-fixup enable
end
end
```

Translating SIP session destination ports

Using port forwarding virtual IPs you can change the destination port of SIP sessions as they pass through the FortiGate unit.

This section describes:

- Translating SIP sessions to a different destination port
- Translating SIP sessions to multiple destination ports

Translating SIP sessions to a different destination port

To configure translating SIP sessions to a different destination port you must add a static NAT virtual IP that translates the SIP destination port to another port destination. In the example the destination port is translated from 5060 to 50601. This configuration can be used if SIP sessions uses different destination ports on different networks.
How the SIP ALG performs NAT

FortiGate VoIP solutions: SIP

Figure 23: Example translating SIP sessions to a different destination port

To translate SIP sessions to a different destination port

1. Add the static NAT virtual IP.
   - This virtual IP forwards traffic received at the port1 interface for IP address 172.20.120.20 and destination port 5060 to the SIP server at IP address 192.168.10.20 with destination port 5061.

   ```
   config firewall vip
   edit "sip_port_trans_vip"
   set type static-nat
   set portforward enable
   set protocol tcp
   set extip 172.20.120.20
   set extport 5060
   set extintf "port1"
   set mappedip 192.168.10.20
   set mappedport 50601
   set comment "Translate SIP destination port"
   end
   ```

2. Add a security policy that includes the virtual IP and the default VoIP profile.

   ```
   config firewall policy
   edit 1
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "all"
   set dstaddr "sip_port_trans_vip"
   set action accept
   set schedule "always"
   set service "ANY"
   set utm-status enable
   set profile-protocol-options default
   set voip-profile default
   set comments "Translate SIP destination port"
   ```
Translating SIP sessions to multiple destination ports

You can use a load balance virtual IP to translate SIP session destination ports to a range
of destination ports. In this example the destination port is translated from 5060 to the
range 50601 to 50603. This configuration can be used if your SIP server is configured to
receive SIP traffic on multiple ports.

Figure 24: Example translating SIP traffic to multiple destination ports

To translated SIP sessions to multiple destination ports

1  Add the load balance virtual IP.

   This virtual IP forwards traffic received at the port1 interface for IP address
   172.20.120.20 and destination port 5060 to the SIP server at IP address
   192.168.10.20 with destination port 5061.

   config firewall vip
   edit "sip_port_ldbl_vip"
   set type load-balance
   set portforward enable
   set protocol tcp
   set extip 172.20.120.20
   set extport 5060
   set extintf "port1"
   set mappedip 192.168.10.20
   set mappedport 50601-50603
   set comment "Translate SIP destination port range"
   end

2  Add a security policy that includes the virtual IP and VoIP profile.

   config firewall policy
   edit 1
   set srcintf "port1"
   set dstintf "port2"
Enhancing SIP pinhole security

You can use the `strict-register` option in a SIP VoIP profile to open smaller pinholes.

As shown in Figure 25 when FortiGate unit is protecting a SIP server on a private network, the FortiGate unit does not have to open a pinhole for the SIP server to send INVITE requests to a SIP Phone on the Internet after the SIP Phone has registered with the server.

Figure 25: FortiGate unit protecting a SIP server on a private network

In the example, a client (SIP Phone A) sends a REGISTER request to the SIP server with the following information:

Client IP: 10.31.101.20
Server IP: 10.21.101.50
Port1: 172.20.120.50
Port2: 10.11.101.100
REGISTER Contact: 172.20.120.20:y

FortiGate unit
In NAT/Route mode

1. Phone A sends a REGISTER message to the SIP Server
2. The FortiGate unit forwards the REGISTER message to the SIP Server
3. The SIP server sends a 200 OK response to Phone A
4. The SIP server sends an INVITE request to Phone A
5. The FortiGate unit accepts the session from the SIP server and forwards the INVITE request to Phone A
Port: UDP (x, 5060)
REGISTER Contact: 10.31.101.20:y

Where x and y are ports chosen by Phone A.

As soon as the server sends the 200 OK reply it can forward INVITE requests from other SIP phones to SIP Phone A. If the SIP proxy server uses the information in the REGISTER message received from SIP Phone A the INVITE messages sent to Phone A will only get through the FortiGate unit if an policy has been added to allow the server to send traffic from the private network to the Internet. Or the SIP ALG must open a pinhole to allow traffic from the server to the Internet. In most cases the FortiGate unit is protecting the SIP server so there is no reason not to add a security policy to allow all the SIP server to send outbound traffic to the Internet.

In a typical SOHO scenario shown in Figure 26, SIP Phone A is being protected from the Internet by a FortiGate unit. In most cases the FortiGate unit would not allow incoming traffic from the Internet to reach the private network. So the only way that an INVITE request from the SIP server can reach SIP Phone A is if the SIP ALG creates an incoming pinhole. All pinholes have three attributes:

(source address, destination address, destination port)

Figure 26: SOHO configuration, FortiGate unit protecting a network with SIP phones

The more specific a pinhole is the more secure it is because it will accept less traffic. In this situation, the pinhole would be more secure if it only accepted traffic from the SIP server. This is what happens if strict-register is enabled in the VoIP profile that accepts the REGISTER request from Phone A.

(SIP server IP address, client IP address, destination port)
If `strict-register` is disabled (the default configuration) the pinhole is set up with the following attributes:

(ANY IP address, client IP address, destination port)

This pinhole allows connections through the FortiGate unit from ANY source address which is a much bigger and less secure pinhole. In most similar network configurations you should enable `strict-register` to improve pinhole security.

Enabling `strict-register` can cause problems when the SIP registrar and SIP proxy server are separate entities with separate IP addresses.

Enter the following command to enable `strict-register` in a VoIP profile.

```
config voip profile
   edit Profile_name
      config SIP
         set strict-register enable
      end
```  

## Hosted NAT traversal

With the increase in the use of VoIP and other media traffic over the Internet, service provider network administrators must defend their networks from threats while allowing voice and multimedia traffic to flow transparently between users and servers and among users. A common scenario could involve providing SIP VoIP services for customers with SIP phones installed behind NAT devices that are not SIP aware. NAT devices that are not SIP aware cannot translate IP addresses in SIP headers and SDP lines in SIP packets but can and do perform source NAT on the source or addresses of the packets. In this scenario the user’s SIP phones would communicate with a SIP proxy server to set up calls between SIP phones. Once the calls are set up RTP packets would be communicated directly between the phones through each user’s NAT device.

The problem with this configuration is that the SIP headers and SDP lines in the SIP packets sent from the phones and received by the SIP proxy server would contain the private network addresses of the VoIP phones that would not be routable on the service provider network or on the Internet. One solution could be to for each customer to install and configure SIP aware NAT devices. If this is not possible, another solution requires implement hosted NAT traversal.

In a hosted NAT traversal (HNT) configuration (for example, see Figure 27), a FortiGate unit is installed between the NAT device and the SIP proxy server and configured with a VoIP profile that enables SIP hosted NAT traversal. Security policies that include the VoIP profile also support destination NAT using a firewall virtual IP. When the SIP phones connect to the SIP server IP address the security policy accepts the SIP packets, the virtual IP translates the destination addresses of the packets to the SIP server IP address, and the SIP ALG NAT traversal configuration translates the source IP addresses on the SIP headers and SDP lines to the source address of the SIP packets (which would be the external IP address of the NAT devices). The SIP server then sees the SIP phone IP address as the external IP address of the NAT device. As a result SIP and RTP media sessions are established using the external IP addresses of the NAT devices instead of the actual IP addresses of the SIP phones.
Configuration example: Hosted NAT traversal for calls between SIP Phone A and SIP Phone B

The following address translation takes place to allow a SIP call from SIP Phone A to SIP Phone B in Figure 27.

1. SIP Phone A sends a SIP Invite message to the SIP server. Packet source IP address: 192.168.10.1, destination IP address: 10.21.101.10.

2. The SIP packets are received by the NAT device which translates the source address of the SIP packets from 192.168.10.1 to 10.11.101.20.

3. The SIP packets are received by the FortiGate unit which translates the packet destination IP address to 10.30.120.20. The SIP ALG also translates the IP address of the SIP phone in the SIP header and SDP lines from 192.168.10.1 to 10.11.101.20.

4. The SIP server accepts the Invite message and forwards it to SIP Phone B at IP address 10.11.101.20. The SIP server has this address for SIP Phone B because SIP packets from SIP Phone B have also been translated using the hosted NAT traversal configuration of the SIP ALG.

5. When the SIP call is established, the RTP session is between 10.11.101.10 and 10.11.101.20 and does not pass through the FortiGate unit. The NAT devices translated the destination address of the RTP packets to the private IP addresses of the SIP phones.
General configuration steps

The following general configuration steps are required for this destination NAT SIP configuration. This example uses the default VoIP profile.

1. Add a VoIP profile that enables hosted NAT translation.
2. Add a SIP proxy server firewall virtual IP.
3. Add a firewall address for the SIP proxy server on the private network.
4. Add a destination NAT security policy that accepts SIP sessions from the Internet destined for the SIP proxy server virtual IP and translates the destination address to the IP address of the SIP proxy server on the private network.
5. Add a security policy that accepts SIP sessions initiated by the SIP proxy server and destined for the Internet.

Configuration steps - web-based manager

To add the SIP proxy server firewall virtual IP

1. Go to Firewall Objects > Virtual IP > Virtual IP.
2. Add the SIP proxy server virtual IP.

<table>
<thead>
<tr>
<th>Name</th>
<th>SIP_Proxy_VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Interface</td>
<td>port1</td>
</tr>
<tr>
<td>Type</td>
<td>Static NAT</td>
</tr>
<tr>
<td>External IP Address/Range</td>
<td>172.20.120.50</td>
</tr>
<tr>
<td>Mapped IP Address/Range</td>
<td>10.31.101.50</td>
</tr>
</tbody>
</table>

To add a firewall address for the SIP proxy server

1. Go to Firewall Objects > Address.
2. Add the following for the SIP proxy server:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>SIP_Proxy_Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.31.101.50/255.255.255.255</td>
</tr>
<tr>
<td>Interface</td>
<td>port2</td>
</tr>
</tbody>
</table>

To add the security policies

1. Go to Policy > Policy > Policy.
2. Add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone B (and other SIP phones on the Internet) to send SIP request messages to the SIP proxy server.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>SIP_Proxy_VIP</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
</tbody>
</table>
3 Select OK.

4 Add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B and the Internet:

<table>
<thead>
<tr>
<th>Service</th>
<th>SIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Select</td>
</tr>
<tr>
<td>UTM</td>
<td>Select</td>
</tr>
<tr>
<td>Protocol Options</td>
<td>default</td>
</tr>
<tr>
<td>Enable VoIP</td>
<td>Select (And select the default VoIP profile)</td>
</tr>
</tbody>
</table>

5 Select OK.

**Configuration steps - CLI**

**To add a VoIP profile that enables hosted NAT translation.**

1 Enter the following command to add a VoIP profile named HNT that enables hosted NAT traversal. This command shows how to clone the default VoIP profile and enable hosted NAT traversal.

```bash
config voip profile
close default to HNT
edit HNT
  config sip
    set hosted-nat-traversal enable
  end
end
```

**To add the SIP proxy server firewall virtual IP and firewall address**

2 Enter the following command to add the SIP proxy server firewall virtual IP.

```bash
config firewall vip
edit SIP_Proxy_VIP
  set type static-nat
  set extip 10.21.101.10
  set mappedip 10.30.120.20
```
set extintf port1
end

3 Enter the following command to add the SIP proxy server firewall address.

```
config firewall address
  edit SIP_Proxy_Server
    set associated interface port2
    set type ipmask
    set subnet 10.30.120.20 255.255.255.255
end
```

To add security policies

1 Enter the following command to add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone A to send SIP request messages to the SIP proxy server.

```
config firewall policy
  edit 0
    set srcintf port1
    set dstintf port2
    set srcaddr all
    set dstaddr SIP_Proxy_VIP
    set action accept
    set schedule always
    set service SIP
    set nat enable
    set utm-status enable
    set profile-protocol-options default
    set voip-profile HNT
end
```

2 Enter the following command to add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B:

```
config firewall policy
  edit 0
    set srcintf port2
    set dstintf port1
    set srcaddr SIP_Proxy_Server
    set dstaddr all
    set action accept
    set schedule always
    set service SIP
    set nat enable
    set utm-status enable
    set profile-protocol-options default
    set voip-profile default
end
```

**Hosted NAT traversal for calls between SIP Phone A and SIP Phone C**

The following address translation takes place to allow a SIP call from SIP Phone A to SIP Phone C in Figure 27 on page 73.

1 SIP Phone A sends a SIP Invite message to the SIP server. Packet source IP address: 192.168.10.1 and destination IP address: 10.21.101.10.
The SIP packets are received by the NAT device which translates the source address of the SIP packets from 192.168.10.1 to 10.11.101.20.

The SIP packets are received by the FortiGate unit which translates the packet destination IP address to 10.30 120.20. The SIP ALG also translates the IP address of the SIP phone in the SIP header and SDP lines from 192.168.10.1 to 10.11.101.20.

The SIP server accepts the Invite message and forwards it to SIP Phone C at IP address 172.20.120.30. The SIP server has this address for SIP Phone C because SIP packets from SIP Phone C have also been translated using the hosted NAT traversal configuration of the SIP ALG.

When the SIP call is established, the RTP session is between 10.11.101.10 and 172.20.120.30. The packets pass through the FortiGate unit which performs NAT as required.

**Restricting the RTP source IP**

Use the following command in a VoIP profile to restrict the RTP source IP to be the same as the SIP source IP when hosted NAT traversal is enabled.

```conf
config voip profile
  edit VoIP_HNT
    config sip
       set hosted-nat-traversal enable
       set hnt-restrict-source-ip enable
    end
  end
end
```

**SIP over IPv6**

FortiGate units operating in NAT/Route and in Transparent mode support SIP over IPv6. The SIP ALG can process SIP messages that use IPv6 addresses in the headers, bodies, and in the transport stack. The SIP ALG cannot modify the IPv6 addresses in the SIP headers so FortiGate units cannot perform SIP or RTP NAT over IPv6 and also cannot translate between IPv6 and IPv4 addresses.

In the scenario shown in Figure 28, a SIP phone connects to the Internet through a FortiGate unit operating. The phone and the SIP and RTP servers all have IPv6 addresses.

The FortiGate unit has IPv6 security policies that accept SIP sessions. The SIP ALG understands IPv6 addresses and can forward IPv6 sessions to their destinations. Using SIP application control features the SIP ALG can also apply rate limiting and other settings to SIP sessions.
To enable SIP support for IPv6 add an IPv6 security policy that accepts SIP packets and includes a VoIP profile.

**Deep SIP message inspection**

Deep SIP message syntax inspection (also called Deep SIP header inspection or SIP fuzzing protection) provides protection against malicious SIP messages by applying SIP header and SDP profile syntax checking. SIP Fuzzing attacks can be used by attackers to discover and exploit vulnerabilities of a SIP entity (for example a SIP proxy server). Most often these attacks could crash or compromise the SIP entity.

**Figure 29: Deep SIP message inspection**

- Checks the SIP request message Request-line
- Checks the following SIP header fields:
  - Allow, Call-id, Contact, Content-length, Content-type, CSeq, Expires, From, Max-Forwards, P-asserted-identity, Rack, Record-Route, Route, Rseq, To, Via
- Checks all SDP profile lines
- Configurable header and body length checks
- Optional logging of message violations

Deep SIP message inspection checks the syntax of each SIP header and SDP profile line to make sure they conform to the syntax defined in the relevant RFC and IETF standard. You can also configure the SIP ALG to inspect for:
Unknown SIP message types (message types not defined in a SIP RFC) this option is enabled by default and can be disabled. When enabled unknown message types are discarded. Configured using the block-unknown option.

Unknown line types (message line types that are not defined in any SIP or SDP RFC). Configured using the unknown-header option.

Messages that are longer than a configured maximum size. Configured using the max-body-length option.

Messages that contain one or more lines that are longer than a set maximum line length (default 998 characters). Configured using the max-line-length option.

Actions taken when a malformed message line is found

When a malformed message line or other error is found the SIP ALG can be configured to discard the message containing the error, pass the message without any other actions, or responding to the message with a 400 Bad Request or 413 Request entity too large client error SIP response message and then discard the message. (For information about client error SIP response messages, see “Client error” on page 21.)

If a message line is longer than the configured maximum, the SIP ALG sends the following message:

```
SIP/2.0 413 Request Entity Too Large, <optional_info>
```

If a message line is incorrect or in an unknown message line is found, the SIP ALG sends the following message:

```
SIP/2.0 400 Bad Request, <optional_info>
```

The `<optional_info>` provides more information about why the message was rejected. For example, if the SIP ALG finds a malformed Via header line, the response message may be:

```
SIP/2.0 400 Bad Request, malformed Via header
```

If the SIP ALG finds a malformed message line, and the action for this message line type is discard, the message is discarded with no further checking or responses. If the action is pass, the SIP ALG continues parsing the SIP message for more malformed message lines. If the action is respond, the SIP ALG sends the SIP response message and discards the message containing the malformed line with no further checking or response. If only malformed message line types with action set to pass are found, the SIP ALG extracts as much information as possible from the message (for example for NAT and opening pinholes, and forwards the message to its destination).

If a SIP message containing a malformed line is discarded the SIP ALG will not use the information in the message for call processing. This could result in the call being terminated. If a malformed line in a SIP message includes information required for the SIP call that the SIP ALG cannot interpret (for example, if an IP address required for SIP NAT is corrupted) the SIP ALG may not be able to continue processing the call and it could be terminated. Discarded messages are counted by SIP ALG static message counters.

Logging and statistics

To record a log message each time the SIP ALG finds a malformed header, enable logging SIP violations in a VoIP profile. In all cases, when the SIP ALG finds an error the FortiGate unit records a malformed header log message that contains information about the error. This happens even if the action is set to pass.
If, because of recording log messages for deep message inspection, the CPU performance is affected by a certain amount, the FortiGate unit records a critical log message about this event and stops writing log messages for deep SIP message inspection.

The following information is recorded in malformed header messages:

- The type of message line in which the error was found.
- The content of the message line in which the error was found (it will be truncated if it makes the log message too long)
- The column or character number in which the error was found (to make it easier to determine what caused the error)

**Recommended configurations**

Because of the risks imposed by SIP header attacks or incorrect data being allowed and because selecting drop or respond does not require more CPU overhead that pass you would want to set all tests to drop or respond. However, in some cases malformed lines may be less of a threat or risk. For example, the SDP i= does not usually contain information that is parsed by any SIP device so a malformed i= line may not pose a threat.

You can also used the pre-defined VoIP profiles to apply different levels of deep message inspection. The default VoIP profile sets all deep message inspection options to pass and the strict VoIP profile sets all deep message inspection options to discard. From the CLI you can use the `clone` command to copy these pre-defined VoIP profiles and then customize them for your requirements.

**Configuring deep SIP message inspection**

You configure deep SIP message inspection in a VoIP profile. All deep SIP message inspection options are available only from the CLI.

Enter the following command to configure deep SIP message inspection to discard messages with malformed Request-lines (the first line in a SIP request message):

```
config voip profile
edit VoIP_Pro_Name
config sip
set malformed-request-line respond
end
end
```

Table 8 lists the SIP header lines that the SIP ALG can inspect for syntax errors.

<table>
<thead>
<tr>
<th>SIP Header line</th>
<th>VoIP profile option</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>malformed-header-allow</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>Call-ID</td>
<td>malformed-header-call-id</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>Contact</td>
<td>malformed-header-contact</td>
<td>RFC 3261</td>
</tr>
</tbody>
</table>

You cannot configure message inspection for the Status-line, which is the first line in a SIP response message.
Table 8: SIP header lines that the SIP ALG can inspect for syntax errors

<table>
<thead>
<tr>
<th>SIP Header line</th>
<th>VoIP profile option</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Length</td>
<td>malformed-header-content-length</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>Content-Type</td>
<td>malformed-header-content-type</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>CSeq</td>
<td>malformed-header-cseq</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>Expires</td>
<td>malformed-header-expires</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>From</td>
<td>malformed-header-from</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>Max-forwards</td>
<td>malformed-header-max-forwards</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>P-Asserted-Identity</td>
<td>malformed-header-p-asserted-identity</td>
<td>RFC 3325</td>
</tr>
<tr>
<td>R Ack</td>
<td>malformed-header-rack</td>
<td>RFC 3262</td>
</tr>
<tr>
<td>Record-Route</td>
<td>malformed-header-record-route</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>Route</td>
<td>malformed-header-route</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>R Seq</td>
<td>malformed-header-rseq</td>
<td>RFC 3262</td>
</tr>
<tr>
<td>To</td>
<td>malformed-header-to</td>
<td>RFC 3261</td>
</tr>
<tr>
<td>Via</td>
<td>malformed-header-via</td>
<td>RFC 3261</td>
</tr>
</tbody>
</table>

Table 9 lists the SDP profile lines that the SIP ALG inspects and the CLI command for configuring the action for each line type. SDP profile lines are defined by RFC 4566 and RFC 2327.

Table 9: SDP profile lines that the SIP ALG can inspect for syntax errors

<table>
<thead>
<tr>
<th>Attribute</th>
<th>VoIP profile option</th>
</tr>
</thead>
<tbody>
<tr>
<td>a=</td>
<td>malformed-header-sdp-a</td>
</tr>
<tr>
<td>b=</td>
<td>malformed-header-sdp-b</td>
</tr>
<tr>
<td>c=</td>
<td>malformed-header-sdp-c</td>
</tr>
<tr>
<td>i=</td>
<td>malformed-header-sdp-i</td>
</tr>
<tr>
<td>k=</td>
<td>malformed-header-sdp-k</td>
</tr>
<tr>
<td>m=</td>
<td>malformed-header-sdp-m</td>
</tr>
<tr>
<td>o=</td>
<td>malformed-header-sdp-o</td>
</tr>
<tr>
<td>r=</td>
<td>malformed-header-sdp-r</td>
</tr>
<tr>
<td>s=</td>
<td>malformed-header-sdp-s</td>
</tr>
<tr>
<td>t=</td>
<td>malformed-header-sdp-t</td>
</tr>
<tr>
<td>v=</td>
<td>malformed-header-sdp-v</td>
</tr>
<tr>
<td>z=</td>
<td>malformed-header-sdp-z</td>
</tr>
</tbody>
</table>

**Discarding SIP messages with some malformed header and body lines**

Enter the following command to configure deep SIP message inspection to discard SIP messages with a malformed Via line, a malformed route line or a malformed m= line but to pass messages with a malformed i= line or a malformed Max-Forwards line:

```plaintext
config voip profile
edit VoIP_Pro_Name
    config sip
```
Blocking SIP request messages

- `set malformed-header-via discard`
- `set malformed-header-route discard`
- `set malformed-header-sdp-m discard`
- `set malformed-header-sdp-i pass`
- `set malformed-header-max-forwards pass`

```
end
end
```

**Discarding SIP messages with an unknown SIP message type**

Enter the following command to discard SIP messages with an unknown SIP message line type as defined in all current SIP RFCs:

```
config voip profile
edit VoIP_Pro_Name
  config sip
    set unknown-header discard
  end
end
```

**Discarding SIP messages that exceed a message size**

Enter the following command to set the maximum size of a SIP message to 200 bytes. Messages longer than 200 bytes are discarded.

```
config voip profile
edit VoIP_Pro_Name
  config sip
    set max-body-length 200
  end
end
```

The `max-body-length` option checks the value in the SIP Content-Length header line to determine body length. The Content-Length can be larger than the actual size of a SIP message if the SIP message content is split over more than one packet. SIP message sizes vary widely. The size of a SIP message can also change with the addition of Via and Record-Route headers as the message is transmitted between users and SIP servers.

**Discarding SIP messages with lines longer than 500 characters**

Enter the following command to set the length of a SIP message line to 500 characters and to block messages that include lines with 500 or more characters:

```
config voip profile
edit VoIP_Pro_Name
  config sip
    set max-line-length 500
    set block-long-lines enable
  end
end
```

**Blocking SIP request messages**

You may want to block different types of SIP requests:

- to prevent SIP attacks using these messages.
• If your SIP server cannot process some SIP messages because of a temporary issue (for example a bug that crashes or compromises the server when it receives a message of a certain type).

• Your SIP implementation does not use certain message types.

When you enable message blocking for a message type in a VoIP profile, whenever a security policy containing the VoIP profile accepts a SIP message of this type, the SIP ALG silently discards the message and records a log message about the action.

Use the following command to configure a VoIP profile to block SIP CANCEL and Update request messages:

```
config voip profile
  edit VoIP_Pro_Name
  config sip
    set block-cancel enable
    set block-update enable
  end
end
```

SIP uses a variety of text-based messages or requests to communicate information about SIP clients and servers to the various components of the SIP network. Since SIP requests are simple text messages and since the requests or their replies can contain information about network components on either side of the FortiGate unit, it may be a security risk to allow these messages to pass through.

Table 10 lists all of the VoIP profile SIP request message blocking options. All of these options are disabled by default.

Blocking SIP OPTIONS messages may prevent a redundant configuration from operating correctly. See “Supporting geographic redundancy when blocking OPTIONS messages” on page 87 for information about resolving this problem.

### Table 10: Options for blocking SIP request messages

<table>
<thead>
<tr>
<th>SIP request message</th>
<th>SIP message blocking CLI Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>block-ack</td>
</tr>
<tr>
<td>BYE</td>
<td>block-bye</td>
</tr>
<tr>
<td>Cancel</td>
<td>block-cancel</td>
</tr>
<tr>
<td>INFO</td>
<td>block-info</td>
</tr>
<tr>
<td>INVITE</td>
<td>block-invite</td>
</tr>
<tr>
<td>Message</td>
<td>block-message</td>
</tr>
<tr>
<td>Notify</td>
<td>block-notify</td>
</tr>
<tr>
<td>Options</td>
<td>block-options</td>
</tr>
<tr>
<td>PRACK</td>
<td>block-prack</td>
</tr>
<tr>
<td>Publish</td>
<td>block-publish</td>
</tr>
<tr>
<td>Refer</td>
<td>block-refer</td>
</tr>
<tr>
<td>Register</td>
<td>block-register</td>
</tr>
<tr>
<td>Subscribe</td>
<td>block-subscribe</td>
</tr>
<tr>
<td>Update</td>
<td>block-update</td>
</tr>
</tbody>
</table>
SIP rate limiting

Configurable threshold for SIP message rates per request method. Protects SIP servers from SIP overload and DoS attacks.

**Figure 30: SIP rate limiting**

FortiGate units support rate limiting for the following types of VoIP traffic:

- Session Initiation Protocol (SIP)
- Skinny Call Control Protocol (SCCP) (most versions)
- Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE).

You can use rate limiting of these VoIP protocols to protect the FortiGate unit and your network from SIP and SCCP Denial of Service (DoS) attacks. Rate limiting protects against SIP DoS attacks by limiting the number of SIP REGISTER and INVITE requests that the FortiGate unit receives per second. Rate limiting protects against SCCP DoS attacks by limiting the number of SCCP call setup messages that the FortiGate unit receives per minute.

You configure rate limiting for a message type by specifying a limit for the number of messages that can be received per second. The rate is limited per security policy. When VoIP rate limiting is enabled for a message type, if the a single security policy accepts more messages per second than the configured rate, the extra messages are dropped and log messages are written when the messages are dropped.

Use the following command to configure a VoIP profile to limit the number of INVITE messages accepted by each security policy that the VoIP profile is added to 100 INVITE messages a second:

```
config voip profile
edit VoIP_Pro_Name
config sip
set invite-rate 100
end
```
If you are experiencing denial of service attacks from traffic using these VoIP protocols, you can enable VoIP rate limiting and limit the rates for your network. Limit the rates depending on the amount of SIP and SCCP traffic that you expect the FortiGate unit to be handling. You can adjust the settings if some calls are lost or if the amount of SIP or SCCP traffic is affecting FortiGate unit performance.

Table 11 lists all of the VoIP profile SIP rate limiting options. All of these options are set to 0 so are disabled by default.

Table 11: Options for SIP rate limiting

<table>
<thead>
<tr>
<th>SIP request message</th>
<th>Rate Limiting CLI Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>ack-rate</td>
</tr>
<tr>
<td>BYE</td>
<td>bye-rate</td>
</tr>
<tr>
<td>Cancel</td>
<td>cancel-rate</td>
</tr>
<tr>
<td>INFO</td>
<td>info-rate</td>
</tr>
<tr>
<td>INVITE</td>
<td>invite-rate</td>
</tr>
<tr>
<td>Message</td>
<td>message-rate</td>
</tr>
<tr>
<td>Notify</td>
<td>notify-rate</td>
</tr>
<tr>
<td>Options</td>
<td>options-rate</td>
</tr>
<tr>
<td>PRACK</td>
<td>prack-rate</td>
</tr>
<tr>
<td>Publish</td>
<td>publish-rate</td>
</tr>
<tr>
<td>Refer</td>
<td>refer-rate</td>
</tr>
<tr>
<td>Register</td>
<td>register-rate</td>
</tr>
<tr>
<td>Subscribe</td>
<td>subscribe-rate</td>
</tr>
<tr>
<td>Update</td>
<td>update-rate</td>
</tr>
</tbody>
</table>

Limiting the number of SIP dialogs accepted by a security policy

In addition to limiting the rates for receiving SIP messages, you can use the following command to limit the number of SIP dialogs (or SIP calls) that the FortiGate unit accepts.

```
config voip profile
    edit VoIP_Pro_Name
        config sip
            set max-dialogs 2000
        end
    end
```

This command sets the maximum number of SIP dialogs that can be open for SIP sessions accepted by any security policy that you add the VoIP profile to. The default setting of 0 does not limit the number of dialogs. You can add a limit to control the number of open dialogs and raise and lower it as required. You might want to limit the number of open dialogs for protection against SIP-based attackers opening large numbers of SIP dialogs. Every dialog takes memory and FortiGate CPU resources to process. Limiting the number of dialogs may improve the overall performance of the FortiGate unit. Limiting the number of dialogs will not drop calls in progress but may prevent new calls from connecting.
SIP logging and DLP archiving

You can enable SIP logging and logging of SIP violations, and SIP DLP archiving a VoIP profile. To record SIP log messages you must also enable VoIP event logging in the FortiGate unit event logging configuration.

To view SIP log messages go to Log&Report > Log Access > Event.
To view SIP DLP archive messages to go Log&Report > Archive Access > VoIP.

Use the following command enable SIP logging, SIP archiving, and logging of SIP violations in a VoIP profile:

```config voip profile
   edit VoIP_Pro_Name
      config sip
         set log-call-summary enable
         set log-violations enable
      end
   end
```

SIP and HA: session failover and geographic redundancy

FortiGate high availability supports SIP session failover (also called stateful failover) for active-passive HA. To support SIP session failover, create a standard HA configuration and select the Enable Session Pick-up option.

SIP session failover replicates SIP states to all cluster units. If an HA failover occurs, all in progress SIP calls (setup complete) and their RTP flows are maintained and the calls will continue after the failover with minimal or no interruption.

SIP calls being set up at the time of a failover may lose signaling messages. In most cases the SIP clients and servers should use message retransmission to complete the call setup after the failover has completed. As a result, SIP users may experience a delay if their calls are being set up when an HA a failover occurs. But in most cases the call setup should be able to continue after the failover.

Figure 31: SIP HA session failover
SIP geographic redundancy

Maintains a active-standby SIP server configuration, which even supports geographical distribution. If the active SIP server fails (missing SIP heartbeat messages or SIP traffic) FortiOS will redirect the SIP traffic to a secondary SIP server.

**Figure 32: SIP geographic redundancy**

Supporting geographic redundancy when blocking OPTIONS messages

For some geographic redundant SIP configurations, the SIP servers may use SIP OPTIONS messages as heartbeats to notify the FortiGate unit that they are still operating (or alive). This is a kind of passive SIP monitoring mechanism where the FortiGate unit isn’t actively monitoring the SIP servers and instead the FortiGate unit passively receives and analyzes OPTIONS messages from the SIP servers.

If FortiGate units block SIP OPTIONS messages because `block-options` is enabled, the configuration may fail to operate correctly because the OPTIONS messages are blocked by one or more FortiGate units.

However, you can work around this problem by enabling the `block-geo-red-options` application control list option. This option causes the FortiGate unit to refresh the local SIP server status when it receives an OPTIONS message before dropping the message. The end result is the heartbeat signals between geographically redundant SIP servers are maintained but OPTIONS messages do not pass through the FortiGate unit.

Use the following command to block OPTIONS messages while still supporting geographic redundancy:

```plaintext
config voip profile
edit VoIP_Pro_Name
  config sip
    set block-options disable
    set block-geo-red-options enable
  end
end
```
Support for RFC 2543-compliant branch parameters

RFC 3261 is the most recent SIP RFC, it obsoletes RFC 2543. However, some SIP implementations may use RFC 2543-compliant SIP calls.

The `rfc2543-branch` VoIP profile option allows the FortiGate unit to support SIP calls that include an RFC 2543-compliant branch parameter in the SIP Via header. This option also allows FortiGate units to support SIP calls that include Via headers that are missing the branch parameter.

```plaintext
config voip profile
  edit VoIP_Pro_Name
  config sip
    set rfc2543-branch enable
  end
end
```

SIP and IPS

You can enable IPS in security policies that also accept SIP sessions to protect the SIP traffic from SIP-based attacks. If you enable IPS in this way then by default the pinholes that the SIP ALG creates to allow RTP and RTCP to flow through the firewall will also have IPS enabled.

This inheritance of the IPS setting can cause performance problems if the RTP traffic volume is high since IPS checking may reduce performance in some cases. Also if you are using network processor (NP) interfaces to accelerate VoIP performance, when IPS is enabled for the pinhole traffic is diverted to the IPS and as a result is not accelerated by the network processors.

You can use the following CLI command to disable IPS for the RTP pinhole traffic.

```plaintext
config voip profile
  edit VoIP_Pro_Name
  config sip
    set ips-rtp disable
  end
end
```

SIP debugging

**SIP debug log format**

Assuming that `diagnose debug console timestamp` is enabled then the following shows the debug that is generated for an INVITE if `diag debug appl sip -1` is enabled:

```
2010-01-04 21:39:59 sip sess 0x979df38 found for 192.168.2.134:5061 -> 172.16.67.192:5060
2010-01-04 21:39:59 sip port 26 read [(0,515)
   (494e56495445207369703a73657276696365403139322e3136382e322e3130303a35303630205349502f322e300d0
   a5669613a2053495022e32e302f5544450203132372e302e312e313a353036313b6272616e63683d7a39684734624b2

   The block-options option setting overrides the block-geo-red-options option. If block-options is enabled the FortiGate unit only blocks SIP OPTIONS messages and does not refresh local SIP server status.
```
SIP proxy filter per VDOM

You can use the diagnose sys sip-proxy xxx command in a VDOM to get info about how SIP is operating in each VDOM.

SIP proxy filter command

Use the diagnose system sip-proxy filter to filter diagnose information for the SIP ALG. The following filters are available:

d363832372d3632302d3030da0a46726fe3da207369707020d3c736970a373697070403133232e30e23e313a35303636 
13e3b7461673d6383237535450754676630363632330daa546f3a207337574203c736970a37367572669665403133 
932e21316382e32e3133030a313303030300a0da43166e2d4844a3203632302d3683237403133232e30e23e312e310 
3a0a3535671a20132049e65495450daa436f6e7461673743a20736970a373697070403133232e30e23e312e31a3353 
0e3c3b7461673d6772761276473aa20733756266563774a2050567676666d616e65365054657377 
10da0a346fe4766e4746e74769765a2061017070c696361746966e2f737400daa346fe476567442d6c665e7746 
83a2a20301332390da0a4d63634775675321320333366535375635023233333683736333720949e204 
95034a20132372e30e23e312e30a7332dd0da633494e2049503420132372e30e23e312e31da0a743d7302030da6a 
d36516564ef620363030302554502f41e505203003a0a613d774706de61a30002050435dd52383030300da0 (INVITE sip:service@192.168.2.100:5060 SIP/2.0.; Via: SIP/2.0/UDP 127.0.1.1:5061;branch=r9hG6kB-6287-620-0.) from sipp

http://docs.fortinet.com/
SIP debugging FortiGate VoIP solutions: SIP

You can clear, view and negate/invert the sense of a filter using these commands:
- `diag sys sip-proxy filter clear`
- `diag sys sip-proxy filter list`
- `diag sys sip-proxy filter negate`

SIP debug log filtering

You can filter by VDOM/IP/PORT and by policy and VoIP profile. The filtering can be controlled by:

```
diagnose system sip-proxy log-filter
```

The list of filters is:
- `diag sys sip-proxy log-filter vd`
- `diag sys sip-proxy log-filter dst-addr4`
- `diag sys sip-proxy log-filter dst-addr6`
- `diag sys sip-proxy log-filter dst-port`
- `diag sys sip-proxy log-filter identity-policy`
- `diag sys sip-proxy log-filter policy`
- `diag sys sip-proxy log-filter policy-type`
- `diag sys sip-proxy log-filter profile-group`
- `diag sys sip-proxy log-filter src-addr4`
- `diag sys sip-proxy log-filter src-addr6`
- `diag sys sip-proxy log-filter src-port`
- `diag sys sip-proxy log-filter vd`
- `diag sys sip-proxy log-filter voip-profile`

You can clear, view and negate/invert the sense of a filter using these commands:
- `diag sys sip-proxy log-filter clear`
- `diag sys sip-proxy log-filter list`
- `diag sys sip-proxy log-filter negate`

SIP debug setting

Control of the SIP debug output is governed by the following command

```
diagnose debug application sip <debug_level_int>
```

Where the `<debug_level_int>` is a bitmask and the individual values determine whether the listed items are logged or not. The `<debug_level_int>` can be:

1 - configuration changes. Mainly addition/deletion/modification of virtual domains.
2 - (TCP) connection accepts or connects, redirect creation
4 - create or delete a session
16 - any IO read or write
32 - an ASCII dump of all data read or written
64 - Include HEX dump in the above output
128 - any activity related to the use of the FortiCarrier dynamic profile feature to determine the correct profile-group to use
256 - log summary of interesting fields in a SIP call
1024 - any activity related to SIP geo-redundancy.
2048 - any activity related to HA syncing of SIP calls.

**SIP test commands**

Use the following command to control or inspect the behavior of the SIP ALG.

```
   diagnose test application sip <test_level_int>
```

Where `<test_level_int>` can be:

1 - Display memory statistics summary
2 - Display all memory statistics
3 - Display debug consoles
4 - Display all SIP redirects
20 - Display SIP per-policy configurations
21 - Display SIP VoIP profiles
22 - Display SIP meters
23 - Display SIP VIPs
24 - Display SIP RTP policies
30 - Display SIP stats summary
31 - Display per VDOM SIP stats
50 - Display all SIP idle calls
51 - Display all SIP sessions
70 - Start measuring scheduler times
71 - Stop measuring scheduler times
72 - Display scheduler times
99 - Restart SIP -- this will drop all SIP calls as well as all IM and SCCP

**Display SIP rate-limit data**

You can use the `diagnose sys sip-proxy meters` command to display SIP rate limiting data.

For the following command output `rate 1` shows that the current (over last second) measured rate for INVITE/ACK and BYTE was 1 per second, the `peak 1` shows that the peak rate recorded is 1 per second, the `max 0` shows that there is no maximum limit set, the `count 18` indicates that 18 messages were received and `drop 0` indicates that none were dropped due to being over the limit.

```
   diag sys sip-proxy meters
   sip
   sip vd: 0
   sip policy: 1
   sip identity-policy: 0
```
VoIP Profile options

The following are VoIP profile configuration settings in UTM Profiles > VoIP > Profile.

Profile page
Lists the profiles that you created for SIP and SCCP protocols. On this page, you can edit, delete or create a new profile for VoIP protocols.

You are redirected to this page when you select View List on the Edit VoIP Profile page.

Create New
Creates a new VoIP profile. When you select Create New, you are automatically redirected to the New VoIP Profile page.

Edit
Modifies settings within a VoIP profile. When you select Edit, you are automatically redirected to the Edit VoIP Profile page.

Delete
Removes a VoIP profile from the list on the Profile page.
To remove multiple VoIP profiles from within the list, on the Profile page, in each of the rows of the profiles you want removed, select the check box and then select Delete.

Name
The name of the profile.

Comments
A description about the profile. This is an optional setting.

Ref.
Displays the number of times the VoIP is referenced to other objects.

<table>
<thead>
<tr>
<th>sip policy-type: IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip profile-group:</td>
</tr>
<tr>
<td>sip dialogs: 18</td>
</tr>
<tr>
<td>sip dialog-limit: 0</td>
</tr>
<tr>
<td>sip UNKNOWN: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip ACK: rate 1 peak 1 max 0 count 18 drop 0</td>
</tr>
<tr>
<td>sip BYE: rate 1 peak 1 max 0 count 18 drop 0</td>
</tr>
<tr>
<td>sip CANCEL: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip INFO: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip INVITE: rate 1 peak 1 max 0 count 18 drop 0</td>
</tr>
<tr>
<td>sip MESSAGE: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip NOTIFY: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip OPTIONS: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip PRACK: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip PUBLISH: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip REFER: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip REGISTER: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip SUBSCRIBE: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip UPDATE: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip PING: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
<tr>
<td>sip YAHOOREF: rate 0 peak 0 max 0 count 0 drop 0</td>
</tr>
</tbody>
</table>
New VoIP Profile page
Provides settings for configuring SIP and SCCP options within the profile.
This page appears when you select Create New on the Edit VoIP Profile page. If you are on the Profile page, and you select Create New, you will be redirected to the New VoIP Profile page.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Enter a description about the profile. This is optional.</td>
</tr>
<tr>
<td>SIP</td>
<td>Configuration settings for SIP protocols.</td>
</tr>
<tr>
<td>Limit REGISTER requests</td>
<td>Enter a number for limiting the time it takes to register requests.</td>
</tr>
<tr>
<td>Limit INVITE requests</td>
<td>Enter a number to limit invitation requests.</td>
</tr>
<tr>
<td>SCCP</td>
<td>Configuration settings for SCCP protocols.</td>
</tr>
<tr>
<td>Limit Call Setup</td>
<td>Enter a number to limit call setup time.</td>
</tr>
</tbody>
</table>
Example FortiGate Voice branch office configuration

This section describes how to configure a FortiGate Voice-80C unit to operate in NAT/Route mode and provide basic UTM and SIP services for the example branch office network shown in Figure 33 on page 96. The non-PSTN parts of this example configuration also apply to FortiGate Voice models that do not include PSTN interfaces.

In this example the FortiGate Voice-80C unit provides:

- Internet connectivity, networking, and UTM features for the PCs on the branch office internal network.
- A single line a/b wire connection between the FortiGate Voice-80C fxo1 interface and a public switched telephone network (PSTN) line so that branch office phones can call the PSTN or receive calls from the PSTN.
- VoIP PBX services for FortiFones and SIP soft phones connected to the branch office internal network. PBX features include:
  - Extensions to the FortiFones and SIP soft phones in the internal network. The branch office phones use four digit numeric extensions that begin with the number 6. Example valid extensions are 6123, 6456, and 6899.
  - Extensions for phones behind NAT devices on the internal network.
  - Extensions for phones behind NAT devices on a remote network.
  - To collect voicemail the branch office phones dial *97.
  - Configure the Voice Menu to program the IP phone keys for various things such as recording a custom welcome message, providing access to company directory and adding a shortcut for checking voicemail.
  - SIP trunking to a VoIP provider for calling the head office.
  - To call a phone number on the PSTN from a branch office phone, dial 9 followed by the phone number. PSTN support includes:
    - Dialing 911 for emergencies
    - Support for dialing international calls
    - Support for dialing toll-free calls
    - Support for long distance calls
  - The FortiGate Voice unit sends email notifications to users when they receive voicemail.
  - To call the head office, the branch office phones dial a head office extension directly. The head office extension range is 2000-2999.

This configuration example describes configuring the FortiGate Voice-80C unit to support these services and where required also provides configuration steps for other devices such as the FortiFones and the remote FortiGate unit operating in NAT mode.

Details about the PSTN connection requirements, SIP trunking for the VoIP provider and the Head Office SIP configuration are not described.
This section describes:

- General configuration steps
- Connecting the FortiGate Voice unit
- Configuring basic FortiGate Voice network and UTM settings
- Configuring network settings for the devices on the Internal network
- Configuring the FortiGate Voice PSTN and PBX settings
- Configuring the FortiFones on the internal network
- Adding extensions and configuring FortiFones for users behind a NAT device
- FortiGate Voice IVR configuration
- Providing access to the company directory
- Adding a shortcut for checking voicemail

General configuration steps

1. Connect the FortiGate Voice unit to the Internet, the internal network and the PSTN.
2. Configure FortiGate Voice unit network and UTM settings.

   The network configuration includes enabling the **SIP Traffic** option on the internal and wan1 interfaces. You must enable SIP traffic on these interfaces to accept and process SIP calls. No other special network configuration, firewall policies, or routing is required for the FortiGate Voice to accept and process SIP calls.

   You do not have to add SIP firewall policies to enable SIP traffic for the FortiGate Voice unit to function as a PBX. Also, with PBX functionality enabled, you cannot apply FortiGate SIP application control features to SIP traffic received by FortiGate Voice interfaces for which you have enabled the **SIP Traffic** option.
Example FortiGate Voice branch office configuration

Connecting the FortiGate Voice unit

This example also describes how to configure the FortiGate Voice as a DHCP server and DNS server for the branch office internal network. As a DHCP server, the FortiGate Voice unit can supply network configuration settings for the PCs and FortiFones on the internal network.

3 Configure network settings for the PCs on the internal network.
4 Configure the FortiGate Voice PSTN and PBX settings.
5 Configure the FortiFones on the internal network.
6 Configure the FortiGate Voice unit to SIP phone users behind a remote NAT device.

Connecting the FortiGate Voice unit

The following procedure describes how to connect the FortiGate Voice unit to the Internet, the branch office internal network, and the PSTN (supported by some FortiGate Voice models).

To connect the FortiGate Voice unit

1 Use an Ethernet cable to connect the FortiGate Voice wan1 interface to the device that connects the branch office to the Internet.
   The device could be a cable or DSL modem or other device depending on how the Branch Office connects to the Internet.
2 Use Ethernet cables to connect the PCs and FortiFones on the internal network to the FortiGate Voice internal interface switch connectors.
   You can connect up to 8 PCs and FortiFones directly to the FortiGate Voice Internal interface switch connectors. To connect more devices, add Ethernet switches to your network as required.
3 Use an RJ-45 telephone cable to connect the FortiGate Voice fxo1 port to the branch office PSTN phone line supplied by your local telephone service provider.

Configuring basic FortiGate Voice network and UTM settings

The following procedures describe how to configure a FortiGate Voice to provide basic Internet connectivity, network services, and UTM services for the branch office internal network. Network services include configuring the FortiGate Voice to be the DHCP server and DNS server for the internal network.

As part of the FortiGate Voice network interface configuration you must enable SIP Traffic on the internal and wan1 interfaces so that the FortiGate Voice unit accepts SIP sessions received by these interfaces. No other special network configuration, firewall policies, or routing is required for the FortiGate Voice to accept SIP sessions from configured extensions.

To configure basic network settings

1 Connect to the FortiGate Voice web-based manager.
2 Go to System > Network > Interface.
3 Edit the internal interface and configure the following settings:
Configure other network interface settings as required and select OK.

The procedure “To configure the FortiGate Voice to be a DHCP server for the internal network” on page 98 describes how to configure the FortiGate DHCP server to configure PCs on the internal network to use the FortiGate Voice internal interface as a DNS server.

4 Edit the wan1 interface and configure the following settings:

<table>
<thead>
<tr>
<th><strong>Addressing Mode</strong></th>
<th>Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP/Netmask</strong></td>
<td>172.20.120.10/255.255.255.0</td>
</tr>
<tr>
<td><strong>Enable DNS Query</strong></td>
<td>Select Enable DNS Query then select recursive from the drop-down menu.</td>
</tr>
<tr>
<td><strong>SIP Traffic</strong></td>
<td>Select Enable</td>
</tr>
</tbody>
</table>

Configure other network interface settings as required and select OK.

You can also set the Addressing mode to DHCP or PPPoE for the wan1 interface depending on the requirements of your ISP. In the example the wan1 interface has a static IP address.

5 Go to System > Network > Options.

6 Add the IP addresses of the primary and secondary DNS servers used by the branch office provided by your ISP.

7 Select Apply.

8 Go to Router > Static > Static Route.

9 Edit the default static route and configure the following settings:

<table>
<thead>
<tr>
<th><strong>Destination IP/Mask</strong></th>
<th>0.0.0.0/0.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td>wan1</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>Enter the IP address of the default gateway provided by your ISP.</td>
</tr>
<tr>
<td><strong>Distance</strong></td>
<td>10</td>
</tr>
</tbody>
</table>

10 Select OK.

To configure the FortiGate Voice to be a DHCP server for the internal network

Use this procedure to add a new DHCP server for the internal network or to change the configuration of the default FortiGateVoice DHCP server. The DHCP server will give PCs on the Internal network IP addresses in the range 172.20.120.110 to 172.20.120.210 and set their default gateway and DNS server to the IP address of the FortiGate Voice internal interface.

1 Go to System > DHCP > Service.

2 Select the Create New.

If a DHCP server has already been added for the internal interface, select the Edit icon to change its configuration.
3 Configure the following settings.

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Server</td>
</tr>
<tr>
<td>Enable</td>
<td>Select</td>
</tr>
<tr>
<td>Type</td>
<td>Regular</td>
</tr>
<tr>
<td>IP Range</td>
<td>172.20.120.110 - 172.20.120.210</td>
</tr>
<tr>
<td>Network Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.20.120.10</td>
</tr>
<tr>
<td>DNS Service</td>
<td>Specify</td>
</tr>
<tr>
<td>DNS Server 0</td>
<td>172.20.120.10</td>
</tr>
</tbody>
</table>

4 Change other settings if required and select OK.

To configure FortiGuard services for the FortiGate Voice unit

Use the following procedure to configure the Fortinet Voice unit to connect to the FortiGuard Distribution Network (FDN) to update the antivirus, antispam and IPS attack definitions. Before you can begin receiving updates, you must register the Fortinet Voice unit from the Fortinet Support web site. For more information, see “Registering your Fortinet product” on page 164.

1 Go to System > Maintenance > FortiGuard.

2 Select the expand arrow for AntiVirus and IPS Options to expand the options.

3 Select Update Now to update the FortiGuard services and definitions.

   If the connection to the FDN is successful, the web-based manager displays a message similar to the following:
   
   Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update.

   After a few minutes, if an update is available, the FortiGuard page lists new version information for the FortiGate services and definitions. The system dashboard license information widget also displays new dates and version numbers for the FortiGuard definitions. Messages are recorded to the event log indicating whether the update was successful or not.

To configure basic Internet access and UTM features

This procedure describes how to add a firewall policy that allows users on the internal network to connect to the Internet with antivirus protection. This configuration is not required for VoIP support. It just provides users on the internal network with UTM-protected access to the Internet.

1 Go to Firewall > Policy and select Create New to add a new firewall policy.

2 Configure the following settings.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
</tbody>
</table>
Configuring network settings for the devices on the Internal network

You can configure the PCs and other devices on the internal network to get their network configuration automatically using DHCP. If required you can also configure devices on the internal network with static IP addresses on the 172.20.120.0 subnet but outside the range awarded by the FortiGate Voice DHCP server. Example static TCP/IP configuration:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>172.20.120.20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.20.120.10</td>
</tr>
<tr>
<td>DNS Server</td>
<td>172.20.120.10</td>
</tr>
</tbody>
</table>

You can also use the same network configuration for the SIP phones on the internal network.

Configuring the FortiGate Voice PSTN and PBX settings

The procedures in this section describe how to configure the FortiGate Voice unit as the PBX for SIP phones on the branch office internal network. These procedures describe how to configure many of the FortiGate Voice PSTN and PBX features. PSTN features are supported on some FortiGate Voice models. The following procedures are included:

- To configure the fxo1 PSTN interface
- To configure basic PBX system and voicemail notification settings
- To add a VoIP provider
- To add a dial plan for dialing the PSTN and the main office
- To add the extensions that are on the branch office internal network

To configure the fxo1 PSTN interface

This procedure describes how to configure the FortiGate Voice fxo1 PSTN interface to connect the FortiGate Voice unit to one PSTN phone line. If you have more PSTN phone lines you can connect and configure more fxo interfaces. Skip this procedure if your FortiGate Voice unit does not include PSTN interfaces.

1. Go to PBX > Service Providers > PSTN Interface and edit the fxo1 interface.
2. Configure the following settings.
| **Phone Number** | Enter the phone number of the PSTN phone line as provided by your phone service provider. The phone number is used for caller ID for calls from the FortiGate Voice unit to the PSTN. It can be any number, but is usually the actual phone number of the PSTN line connected to the fxo1 interface. Area code and country codes are optional. |
| **Display Name** | This name is used for caller ID for calls from the FortiGate Voice unit to the PSTN. It can be any name, such as a company name, that identifies the branch office. |
| **Caller ID Options** | Configure the following options to support caller ID functions for calls from the internal network to the PSTN. |
| **Catch Caller ID** | Select to enable the FortiGate Voice unit to receive caller ID information from calls originating on the PSTN and send the caller ID information to the extension that answers the call. |
| **Caller ID Protocol** | Select the caller ID protocol required by PSTN line that the fxo interface is connected to. Contact your service provider for the name of the protocol to use. |
| **Caller ID Indicator** | Select the caller ID indicator required by the PSTN line. Contact your service provider for details. |
| **Ring #** | Set the number of rings to wait before receiving caller ID information. In most cases, enter 1 to send caller ID information between the first and second ring. Contact your service provider for details. |
| **Hang-up Options** | Configure the following options to configure how the FortiGate Voice unit hangs up calls from the PSTN. |
| **Hang up on Polarity Reversal** | Select if the PSTN line uses polarity reversal to indicate a call has been hung up. Contact your service provider for details. |
| **Hang up on Busy Tone** | Select if you want the FortiGate Voice unit to hang up automatically when it receives a busy tone when attempting to dial a number on the PSTN. |
| **Busy Tone Detection #** | The number of busy tones that the FortiGate Voice receives before hanging up if **Hang up on Busy Tone** is selected. |
| **Busy Tone Duration** | Tune the FortiGate Voice unit to accurately detect busy tones on this PSTN line. You can change the default settings if busy tones are not accurately detected. |
| **Busy Tone Interval** | Set to **Up** if the fxo interface is connected to the PSTN and you want to be able to receive and send calls on this PSTN interface. |

3. Select OK.
To configure basic PBX system and voicemail notification settings

Use the following procedure to configure PBX system settings and voicemail notification email settings that affect the overall performance of the PBX service and all of the users of it. Usually you would configure these settings once and rarely thereafter.

1. Go to PBX > Calling Rules > Setting.
2. Configure the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension Pattern</td>
<td>Select Other and enter 6XXX. The example extension range means that every extension added to the FortiGate Voice unit must be a four digit number starting with a 6.</td>
</tr>
<tr>
<td>Country/Area</td>
<td>Select the country from the drop-down menu.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Enter the international country calling code for the country or region in which you are installing the FortiGate Voice unit.</td>
</tr>
<tr>
<td>Local Area Code</td>
<td>Enter the local area code for the country or region in which you are installing the FortiGate Voice unit.</td>
</tr>
<tr>
<td>Voicemail Access</td>
<td>*97. Phone users on the internal network can dial *97 to get their voicemail.</td>
</tr>
<tr>
<td>Outgoing Prefix</td>
<td>9. Phone users must dial 9 to get an outside line. The outgoing prefix should not be the same as the first number of the extension range.</td>
</tr>
<tr>
<td>Max Voicemail Duration</td>
<td>60 seconds. Limits a single voicemail message to 60 seconds.</td>
</tr>
</tbody>
</table>

3. Select Apply to save the changes.
4. Go to Log&Report > Log Config > Alert E-mail.
5. Configure the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>The name or IP address of an email server that the FortiGate Voice unit can send email notifications to when PBX users receive a voicemail. For example: mail.example.com. You can optionally create an email account on the email server for the FortiGate Voice unit.</td>
</tr>
<tr>
<td>Email from</td>
<td>Enter the email address that the alert email messages will come from.</td>
</tr>
<tr>
<td>Email to</td>
<td>Enter up to three email address recipients for alert email message.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select if the email server requires authentication.</td>
</tr>
<tr>
<td>SMTP User</td>
<td>Enter a valid username for an account on the email server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the account on the email server.</td>
</tr>
</tbody>
</table>

6. Select Apply to save the changes.
To add a VoIP provider

Use the following procedure to add the information required by the FortiGate Voice unit to use a VoIP provider for routing SIP calls on the main office. In the example, the organization uses a third-party VoIP provider to handle VoIP calls between the head office and the branch office.

1. Go to PBX > Service Providers > SIP Trunk.
2. Select Create New.
3. Configure the following settings.

<table>
<thead>
<tr>
<th>Name</th>
<th>VoIP_Provider_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A name for the VoIP provider. This can be any name.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>192.168.20.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VoIP provider’s IP address. This could also be the VoIP providers domain name (for example, voip.example.com).</td>
<td></td>
</tr>
</tbody>
</table>

| User Name | Enter a valid user name for an account on the VoIP provider’s server. This could also be a phone number including area code, depending on the requirements of the VoIP provider. |

| Password | Enter the password for the account on the VoIP provider’s SIP sever. |

| Authorization User Name | Enter a valid authorization user name for an account on the VoIP provider’s server if required by the VoIP provider. |

| Display User Name | Enter a valid display user name for an account on the VoIP provider’s server if required by the VoIP provider. |

| Account Type | Select Static or Dynamic depending on the account with the VoIP provider. |

| Registration Interval | If this is a dynamic account with the VoIP provider, enter the registration interval as required by the VoIP provider. After each registration interval the FortiGate Voice renews the registration of the account with the VoIP provider. |

<table>
<thead>
<tr>
<th>DTMF Method</th>
<th>Auto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto means the VoIP provider’s server and the FortiGate Voice unit will negotiate to select a DTMF method. You could also select a specific DTMF method if required.</td>
<td></td>
</tr>
</tbody>
</table>

4. Select OK to add the VoIP provider.

To add a dial plan for dialing the PSTN and the main office

Dial plans are used to route calls made from an extension to an external phone system. The external phone system can be the PSTN or a VoIP provider. To route calls to an external phone system you add dial plan rules that include a dial pattern and list of outgoing destinations. When the FortiGate Voice unit receives a call from an extension and the number dialed matches a pattern in a dial plan rule, the FortiGate Voice unit routes the call to the outgoing destination added to the dial plan.

In addition to PSTN and head office support, the dial plan must also support emergency, international, toll free and long distance dialing.
Use the following steps to add a dial plan with the following dial plan rules:

- Allows the branch office to call the PSTN
  - Dialing 911 for emergencies
  - Dialing 9 followed by a country code for international calls
  - Dialing 9 followed by 18 for toll free calls
  - Dialing 9 followed by 1 for long distance calls
  - Dialing 9 for all other PSTN calls

- Allows the branch office to dial head office extensions directly. The dial plan rule sends calls starting with 2 to the VoIP provider where they are routed to the head office. This dial plan does not include any other settings because users dial the head office extension number directly without a prefix.

1. Go to **PBX > Calling Rules > Dial Plan** and select **Create New**.
2. Add a name for the new dial plan, for example, **Dial_Plan_1**.
3. Select OK.
4. Select **Create New** to add the dial plan rule for dialing 911 for emergencies.

<table>
<thead>
<tr>
<th>Name</th>
<th>Emergency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (&quot;9&quot;)</td>
<td>Not selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td>911</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing Selected</td>
<td>PSTN - fxo1</td>
</tr>
</tbody>
</table>

5. Select **Create New** to add the dial plan rule for dialing 9 followed by a country code for international calls.

<table>
<thead>
<tr>
<th>Name</th>
<th>International</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (&quot;9&quot;)</td>
<td>Selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td>011</td>
</tr>
<tr>
<td>Action</td>
<td>Block</td>
</tr>
</tbody>
</table>

6. Select **Create New** to add the dial plan rule for dialing 9 followed by 18 for toll free calls.

<table>
<thead>
<tr>
<th>Name</th>
<th>Toll_Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (&quot;9&quot;)</td>
<td>Selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td>18</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing Selected</td>
<td>PSTN - fxo1</td>
</tr>
</tbody>
</table>

7. Select **Create New** to add the dial plan rule for dialing 9 followed by 1 for long distance calls.
Example FortiGate Voice branch office configuration

Configuring the FortiGate Voice PSTN and PBX settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Long_Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing</td>
<td>Selected</td>
</tr>
<tr>
<td>Prefix (&quot;9&quot;)</td>
<td></td>
</tr>
<tr>
<td>Phone number Begin</td>
<td>1</td>
</tr>
<tr>
<td>with</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing Selected</td>
<td>PSTN - fxo2</td>
</tr>
</tbody>
</table>

8 Select Create New to add the dial plan rule for dialing 9 for all other PSTN calls.

<table>
<thead>
<tr>
<th>Name</th>
<th>Other_PSTN_Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing</td>
<td>Selected</td>
</tr>
<tr>
<td>Prefix (&quot;9&quot;)</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing Selected</td>
<td>Move PSTN - fxo1 to the Selected list to send calls to the PSTN out the fxo1 interface.</td>
</tr>
</tbody>
</table>

9 Select Create New to add the dial plan rule for dialing the Head Office.

<table>
<thead>
<tr>
<th>Name</th>
<th>Head_Office_Dial_Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing</td>
<td>Deselect.</td>
</tr>
<tr>
<td>Prefix (&quot;9&quot;)</td>
<td></td>
</tr>
<tr>
<td>Phone number Begin</td>
<td>2</td>
</tr>
<tr>
<td>with</td>
<td>Indicates that outgoing calls to the Head Office must start with a 2.</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing</td>
<td>Move VoIP - VoIP_Provider_1 to the Selected list to send calls to the PSTN out the fxo1 interface.</td>
</tr>
</tbody>
</table>

10 Select OK.

To add the extensions that are on the branch office internal network

Use the following steps to add extensions to the FortiGate Voice unit for the IP phones that are to be connected to the internal network. You add identifying information to each extension entry. The IP phone must be configured with identifying information that matches an entry in the extension list in order to get an extension from the FortiGate Voice unit. Extension numbers are independent of the IP address of the IP phone.

1 Go to PBX > Extension > Extension and select Create New.

2 Configure the following settings to add extension 6001.
Configuring the FortiFones on the internal network

Example FortiGate Voice branch office configuration

<table>
<thead>
<tr>
<th>Extension</th>
<th>6001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The SIP phone user password for the phone assigned to this extension. For a FortiFone on the internal network to be able to register with the FortiGate Voice unit to get this extension, the FortiFone Register Name must consist of the extension First Name followed by the Last Name separated by one space. The FortiFone must also be configured with this Password and the IP address of the FortiGate Voice internal interface. The password must be 8 or more characters, must contain at least an uppercase character, a lowercase character and a number, non-alphanumeric characters, like ( - $ , are not supported in the password field.</td>
</tr>
<tr>
<td>Type</td>
<td>SIP Phone</td>
</tr>
<tr>
<td>First Name</td>
<td>The first name assigned to this extension. Usually a person’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The last name assigned to this extension. Usually a person’s last name. When this extension calls another phone the caller ID displayed on the called phone consists of the extension First Name followed by the Last Name.</td>
</tr>
<tr>
<td>Email</td>
<td>The email address of the person assigned to this extension. The FortiGate Voice unit sends voicemail notifications for the extension to this email address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address of the SIP phone.</td>
</tr>
<tr>
<td>Dial Plan</td>
<td>Dial_Plan_1</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Select</td>
</tr>
<tr>
<td>Voicemail Password</td>
<td>Enter the numeric password that the SIP user must enter to get voicemail. The password can contain numbers only.</td>
</tr>
<tr>
<td>Email Notification</td>
<td>Select</td>
</tr>
<tr>
<td>Voicemail to Email Attachment</td>
<td>Select to attach a recording of the user’s voicemail message to the voicemail notification email.</td>
</tr>
<tr>
<td>Maximum Message #</td>
<td>50 The FortiGate Voice unit keeps up to 50 voicemail messages for this extension.</td>
</tr>
</tbody>
</table>

3 Select OK to add the extension.
4 Repeat to add more extensions.

Configuring the FortiFones on the internal network

This section contains high-level instructions for installing and configuring FortiFones for the example configuration. For more detailed information see the FortiFone documentation.
To configure FortiFones on the internal network

The following steps describe how to configure a FortiFone on the internal network with extension number 6001. This procedure would also apply to configuring a FortiFone for most networks. See the documentation supplied with the FortiFone for details.

1. Connect and power on the FortiFone handset.
2. Connect to the handset web configuration interface.
   - The default web configuration interface address is http://192.168.0.1. To connect to this address from a PC, your PC should have an IP address on the 192.168.0.0 subnet, for example: 192.168.0.10/255.255.255.0.
   - The default Username is root. No password is required.
3. Go to Network > LAN Settings and set the IP Type to DHCP Client and select Submit.
4. Select Save & Reboot to save the IP addressing change.
5. Log into the FortiFone using the IP address it acquired from the DHCP server.
6. Go to SIP Settings > Service Domain and add the following configuration information:

<table>
<thead>
<tr>
<th>Active</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>The name to be displayed on the phone. This name is only displayed on this phone. When this phone calls another phone the name displayed is the First Name and Last Name added to the FortiGate Voice Extension configuration.</td>
</tr>
<tr>
<td>User Name</td>
<td>6001</td>
</tr>
<tr>
<td></td>
<td>This is actually the Line Number or Extension Number and must match the Extension Number added to the FortiGate Voice Extension configuration for this phone.</td>
</tr>
<tr>
<td>Register Name</td>
<td>6001</td>
</tr>
<tr>
<td></td>
<td>The Register Name is used to authenticate the FortiFone and must match the Extension Number added to the FortiGate Voice Extension configuration for this phone. Both the User Name and Register Name are required.</td>
</tr>
<tr>
<td>Register Password</td>
<td>The Password added to the FortiGate Voice Extension configuration for this phone. The Register Name and Register Password are used to authenticate the phone with the FortiGate Voice unit.</td>
</tr>
<tr>
<td>Domain Server</td>
<td>Leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>Not required since the configuration uses the FortiGate Voice unit as a SIP proxy. This field is only used to add the phone to a SIP service domain.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>172.20.120.10</td>
</tr>
<tr>
<td></td>
<td>The IP address of the FortiGate Voice internal interface.</td>
</tr>
<tr>
<td>Outbound Proxy</td>
<td>Leave this field blank.</td>
</tr>
</tbody>
</table>

7. Select Submit.
8. Select Save & Reboot to save the service domain information.
9 If the FortiFone can successfully connect to and register with the FortiGate Voice unit the Status of the FortiFone changes to Registered.

If Status does not change to Registered you should verify the Register Name or re-enter the Password. You should also confirm that the Domain Server and Proxy Server IP addresses are correct.

If you manually configure FortiFone registration settings, set register interval to 60 seconds where it applies. Refer to FortiFone documentation for more information about FortiFone configuration.

Adding extensions and configuring FortiFones for users behind a NAT device

When adding an extension for any SIP phone with a NAT device between the phone and the FortiGate Voice unit you must enable NAT in the FortiGate Voice extension configuration for the phone. You can enable NAT only from the CLI. This applies whether the phone is on a remote network behind a NAT device or behind a NAT device on the internal network.

To add an extension for a SIP phone behind a NAT device

The following procedure describes adding the extension from the FortiGate Voice CLI because you must use the CLI to enable NAT. You could add the extension from the web-based manager and then edit the extension from the CLI to enable NAT.

The following configuration is the same whether the phone is behind a NAT device on the internal network or on a remote network,

1 Connect to the FortiGate CLI.
2 Enter the following command to add extension 6010.
   The command includes setting nat to yes to enable NAT.
   
   config pbx extension
   edit 6010
   set first-name <first_name_str>
   set last-name <last_name_str>
   set email <email_str>
   set secret <password_str>
   set dialplan Dial_Plan_1
   set vm-secret <voicemail_password_str>
   set email-notify enable
   set attach enable
   set nat yes
   set macaddress <mac_address>
   end

To configure FortiFones behind a NAT device on the internal network

The configuration for FortiFones behind a NAT device on the internal network is the same as for FortiFones directly on the Internal network. See “To configure FortiFones on the internal network” on page 107.

You may have to configure the NAT device to allow SIP sessions between the FortiFone and the FortiGate Voice unit.
To configure FortiFones behind a NAT device on a remote network

The following steps describe how to configure a FortiFone on the remote network with extension number 6010.

1. Connect and power on the FortiFone handset.

2. Connect to the handset web configuration interface.

   The default web configuration interface address is http://192.168.0.1. To connect to this address from a PC, your PC should have an IP address on the 192.168.0.0 subnet, for example: 192.168.0.10/255.255.255.0.

   The default Username is root. No password is required.

3. Go to Network > LAN Settings and set the IP Type to DHCP Client and select Submit.

4. Select Save & Reboot to save the IP addressing change.

5. Log into the FortiFone using the IP address it acquired from the DHCP server.

6. Go to SIP Settings > Service Domain and add the following configuration information:

<table>
<thead>
<tr>
<th>Active</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>The name to be displayed on the phone. This name is only displayed on this phone. When this phone calls another phone the name displayed is the First Name and Last Name added to the FortiGate Voice Extension configuration.</td>
</tr>
<tr>
<td>User Name</td>
<td>6010</td>
</tr>
<tr>
<td>Register Name</td>
<td>6010</td>
</tr>
<tr>
<td>Register Password</td>
<td>The Password added to the FortiGate Voice Extension configuration for this phone. The Register Name and Register Password are used to authenticate the phone with the FortiGate Voice unit.</td>
</tr>
<tr>
<td>Domain Server</td>
<td>Leave this field blank.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>172.20.120.10</td>
</tr>
<tr>
<td>Outbound Proxy</td>
<td>Leave this field blank.</td>
</tr>
</tbody>
</table>

7. If the FortiFone can successfully connect to and register with the FortiGate Voice unit the Status of the FortiFone changes to Registered.

If Status does not change to Registered you should verify the Register Name or re-enter the Password. You should also confirm that the Domain Server and Proxy Server IP addresses are correct.
To configure the remote FortiGate unit in NAT mode
The remote FortiGate unit in NAT mode must be configured to allow SIP sessions between the remote users on the remote network and the FortiGate Voice external interface. To do this you need to:

- Add an internal to external firewall policy that allows SIP sessions so that the remote users can start SIP sessions with the FortiGate Voice unit
- Add a virtual IP and an external to internal firewall policy that allows SIP sessions from the FortiGate Voice wan1 interface to connect to the phones in the remote network

For higher security, you could configure IPSec tunneling between the branch office network and the remote network and send SIP traffic over the IPSec tunnel.

FortiGate Voice IVR configuration

By default, when callers call into the FortiGate Voice PBX from a remote system such as the PSTN, the call is picked up by the PBX system which plays a default message asking the caller to dial the extension number that they want to reach or to dial 0 for assistance. If the caller dials 0 they can use the number keys on their phone to spell out the First Name or Last Name of an extension to connect with that extension.

You can use the following procedure to add a custom welcome message.

To add a custom welcome message
1. Log into the FortiGate Voice web-based manager.
2. Go to PBX > Calling Rules > Voice Menu.
3. Enter a Recorder Extension.
4. Enter a Password for Recording.
   The password should include numbers only.
5. Select OK.
6. From a SIP phone that is registered with the FortiGate Voice unit, dial the Extension added in step 3.
7. Follow the prompts to record a new welcome message.

Providing access to the company directory

Use the following procedure to allow phone users to dial 3 to access the FortiGate Voice PBX directory. Phone users can use the directory to call an extension by using the number keys on their phone to spell out the First Name or Last Name of an extension to connect with that extension.

To provide access to the company directory from any extension
1. Log into the FortiGate Voice web-based manager.
2. Go to PBX > Calling Rules > Voice Menu.
3. Select the Edit icon for Key 3.
   You can select any available key, but this example uses 3.
4. Set Action to Go to Company Directory and select OK.
Adding a shortcut for checking voicemail

Use the following procedure to allow phone users to dial 7 to access their voicemail.

To provide access to the company directory form any extension
1. Log into the FortiGate Voice web-based manager.
2. Go to PBX > Calling Rules > Voice Menu.
3. Select the Edit icon for Key 7.
   You can select any available key, but this example uses 7.
4. Set Action to Check Voicemail and select OK.

Checking voicemail

Once users connect to their voicemail using the Voicemail Access number configured from PBX > Calling Rules > Setting or by pressing the configured voicemail key they can follow the prompts to listen to, store, and delete messages. Users can also change their voicemail password.
FortiGate Voice web-based manager configuration reference

This section describes the following FortiGate Voice web-based manager configuration settings.

- Unit operation dashboard widget
- Configuring interface settings to support VoIP PBX features
- PBX configuration
- Logging of PBX activities

Unit operation dashboard widget

Go to System > Dashboard > Status and view the Unit Operation widget to see the status of the FortiGate Voice unit and its Ethernet and fxo interfaces. The fxo interfaces appear if your FortiGate Voice unit includes PSTN interfaces.

Figure 34: FortiGate Voice-80C Unit operation widget

Configuring interface settings to support VoIP PBX features

You can configure the following options on one or more FortiGate Voice ethernet interfaces to support PBX functionality for FortiGate Voice PBX users:

- Configuring an interface to accept SIP traffic
- Enabling access to the PBX user web portal
• SIP phone auto-provisioning

These options may compromise the security of the FortiGate Voice unit interface on which they are enabled (for example by opening a TCP or UDP port). We recommend that you only enable them on an interface connected to a secure network. Use caution when enabling them on an interface that is connected to an unsecure network such as the Internet.

Configuring an interface to accept SIP traffic

For PBX users to access the PBX features of a FortiGate Voice unit, you must configure the FortiGate Voice interface that PBX users connect to accept SIP traffic.

To enable SIP traffic on a FortiGate Voice interface

1. Go to System > Network > Interface.
2. Select the interface that you want to configure VoIP settings for. The interface connected to the network containing SIP phones.
3. Select the SIP check box to enable SIP traffic.
4. Select OK.

Enabling access to the PBX user web portal

PBX users can log into the FortiGate Voice PBX user web portal using their PBX extension and password. The connection to the web portal is secured using HTTPS. From the portal, users can view their PBX configuration, change some configuration settings such as their password, listen to their voicemail, configure call forwarding, access conference calls, and listen to recorded conference calls.

To allow access to the FortiGate Voice PBX user web portal

You can configure one or more FortiGate Voice interfaces to accept connections to the PBX user web portal.

1. Go to System > Network > Interface and edit an interface.
2. Enable the PBX User Portal for this interface.

To log into the PBX user web portal

1. Browse to the following address:
https://<interface_address>:8443

where:

<interface_address> is the IP address or domain name of a FortiGate Voice interface on which you have enabled the PBX user portal.

8443 is the default port that users must browse to connect to the portal.

**SIP phone auto-provisioning**

You can configure the FortiGate Voice unit to auto-provision SIP phones on your network. The SIP phones must support auto-provisioning using TFTP. See the FortiGate Voice release notes for a list of supported SIP phones.

With auto-provisioning configured, when a supported SIP phone is connected to the network and powered on it automatically receives all of its PBX setup information from the FortiGate Voice unit. In most cases the administrator does not have to make configuration changes to the SIP phone itself.

To configure FortiGate Voice auto-provisioning you need to enable *Phone Auto-Provision* for the FortiGate Voice interface connected to the same network as the SIP phones to be auto-provisioned.

Enabling Phone Auto-Provision on a FortiGate Voice interface opens UDP port 69 (the TFTP port) on that interface. You should only enable phone auto-provisioning on a secure network.

You must also configure a DHCP server on this interface. In the DHCP server configuration, select DHCP option 66 (an advanced option on the web-based manager) and include the IP address of this FortiGate Voice interface.

DHCP server option 66 identifies a TFTP server and includes the IP address of the TFTP server and downloads the TFTP server identity to the device that gets an IP address from the DHCP server. DHCP option 66 is defined in [RFC 2132](https://tools.ietf.org/html/rfc2132).

The address must be input in hexadecimal ASCII format. In this format, each ASCII character in the dotted decimal IP address (including periods) is represented by a 2-digit hexadecimal number that maps to the corresponding ASCII character. For example, for the FortiGate Voice default configuration, the IP address of the FortiGate Voice internal interface (192.168.1.99) is input in hexadecimal format as follows:

<table>
<thead>
<tr>
<th>Hexadecimal</th>
<th>31</th>
<th>39</th>
<th>32</th>
<th>2E</th>
<th>31</th>
<th>36</th>
<th>38</th>
<th>2E</th>
<th>31</th>
<th>2E</th>
<th>39</th>
<th>39</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>1</td>
<td>9</td>
<td>2</td>
<td>.</td>
<td>1</td>
<td>6</td>
<td>8</td>
<td>.</td>
<td>1</td>
<td>.</td>
<td>9</td>
<td>9</td>
</tr>
</tbody>
</table>

For a hexadecimal representation of all ASCII characters, see the [ASCII printable characters list](https://en.wikipedia.org/wiki/ASCII) on Wikipedia.

With this configuration in place, when a SIP phone that supports auto-provisioning with TFTP receives its IP address via DHCP from the FortiGate Voice unit, it also receives the TFTP server address. The SIP phone then downloads its PBX configuration from TFTP server running on the FortiGate Voice unit.

The FortiGate Voice unit identifies the SIP phone by its MAC address. When you add an extension for the phone to the PBX configuration you include its MAC address. The FortiGate Voice unit uses this MAC address to identify the SIP phone and match it with its extension in the PBX configuration. In most cases the MAC address is available from a sticker attached to the phone or its packaging.
Default FortiGate Voice auto-provisioning configuration

By default the FortiGate Voice unit enables auto-provisioning on the Internal interface for SIP phones attached to the internal network. The default IP address of the internal interface is 192.168.1.99. The FortiGate Voice default configuration also includes a DHCP server for the Internal interface that provides IP addresses in the range of 192.168.1.110 to 192.168.1.210. You can configure all of the devices on your internal network (including PCs and SIP phones and so on) to use DHCP to automatically get their IP addresses from the FortiGate Voice unit DHCP server. SIP phones that support auto-provisioning can also get their PBX configuration if an extension for the SIP phone’s MAC address has been added to the FortiGate Voice PBX configuration.

If you want to configure the network connected to the FortiGate Voice internal interface to use a different subnet but still support auto-provisioning, you must:

- Change the IP address of the FortiGate Voice internal interface.
- Change the IP addresses that the DHCP server provides.
- Change the TFTP server IP address added to the DHCP server option 66.

Configuring SIP phones for auto-provisioning

Before you begin, make sure your FortiGate Voice unit is set up for auto-provisioning and the configuration meets the following:

- A DHCP server set up as described.
- A PBX extension set up with SIP phone’s MAC address.

This section describes how to configure auto-provisioning for the following phones:

- FortiFone-110
- FortiFone-210
- Polycom
- Aastra

To configure a FortiFone-110 phone for auto-provisioning

1. Connect the FortiFone-110 phone to the VoIP network. Refer to the phone’s documentation for instructions for connecting the phone.
2. Reset the phone to its factory default settings by selecting `Menu > Phone Settings > Reset to Factory`.
3. Set DHCP IP client as WAN port option by selecting `Menu > Network > WAN Port Option > DHCP IP Client`.

The FortiFone-110 phone reboots and starts acquiring an IP address and PBX extension settings from the FortiGate Voice unit. During this time `invalid account` followed by `Updating configuration, please wait` appears on the screen. After a few minutes, the phone reboots one last time. The phone extension settings appear on the screen, the IP address and the other connection details can be found by navigating through the phone’s menu.

To configure a FortiFone-210 phone for auto-provisioning

1. Connect the FortiFone-210 phone to the VoIP network. Refer to the phone’s documentation for instructions for connecting the phone.
2 Reset the phone to its factory default settings.
   Refer to the phone’s documentation.
   The FortiFone-210 phone reboots and starts acquiring an IP address and PBX extension settings from the FortiGate Voice unit.

To configure Polycom phones for auto-provisioning
1 Connect the Polycom phone to the VoIP network.
   Refer to the phone’s documentation for instructions for connecting the phone.
2 Select Setup on the screen.
3 Enter the administrator password.
   The default password is 456.
4 Set the server type to Trivial FTP by selecting V > Server Menu > Server Type > Trivial FTP.
5 Select Exit.
   The Polycom phone reboots and starts acquiring an IP address and PBX extension settings from the FortiGate Voice unit.

To configure Aastra phones for auto-provisioning
1 Connect the Aastra phone to the VoIP network.
   Refer to phone’s documentation for instructions for connecting the phone.
2 Reset the phone to its factory default settings.
   Refer to the phone’s documentation.
   The Astra phone reboots and starts acquiring an IP address and PBX extension settings from the FortiGate Voice unit.

If you manually configure any FortiFone’s registration settings, set register interval to 60 seconds where it applies. Refer to FortiFone documentation for more information about FortiFone configuration.

PBX configuration

The following explains how to configure PBX settings for your network environment. These settings include, adding extensions to your PBX, voicemail notification settings, configuring the FortiGuard Voice service, configuring other VoIP providers, as well as system settings such as a voicemail access code and a maximum voicemail duration time limit.

Configuring extensions

Add PBX extensions to configure the settings for the SIP phones that the FortiGate Voice unit supplies PBX services for. Each extension configuration includes the extension number, the name and email address of the person assigned to the extension, the MAC address of the device to be used for the extension (to support auto-provisioning), whether the device includes video calling, and voicemail settings. You can also use the extension settings to add conference bridges.
To add a new extension, go to **PBX > Extension > Extension**, select **Create New**, enter the information and then select **OK**.

FortiGate Voice unit uses the alertmail settings to access an SMTP server and send email notifications. Alertmail is configured in **Log&Report > Log Config > Alert E-mail**.

**Figure 35: Configuring extensions**

<table>
<thead>
<tr>
<th>Extension</th>
<th>Type</th>
<th>Name</th>
<th>Dial Plan</th>
<th>MAC Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>6569</td>
<td>SIP Phone</td>
<td>first line</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6777</td>
<td>Conference</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**General extension settings**

<table>
<thead>
<tr>
<th>Create New</th>
<th>Select to create an extension.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension</td>
<td>The extension number.</td>
</tr>
</tbody>
</table>
| Type       | The type of extension the number is. Type can be:
  - SIP Phone to configure a SIP phone extension
  - Conference to configure a conference bridge. For the Conference extension you can add an extension number and a password. PBX users can call this extension number and enter the password to join a conference call. |
| Name       | The name of the extension.     |
| Dial Plan  | The dial plan that will be used for that extension. |

**Extension configuration settings**

<table>
<thead>
<tr>
<th>Extension</th>
<th>Enter the extension number. The web-based manager shows the pattern that the extension number must follow. For example, <em>(Pattern: XXX)</em> means the extension must consist of three numbers.</th>
</tr>
</thead>
</table>
# PBX configuration

## Password
Enter a password for the extension. The password is used to log into the PBX user web portal. The password cannot be blank, must be 8 or more characters, must contain at least one uppercase character, one lowercase character and one number. Non-alphanumeric characters, like (- $ ,) are not supported in the password field.

If you are entering a password for a conference bridge, the password cannot be blank and must contain only numbers. This becomes the conference PIN number.

## Type
Select the type of extension. You can choose from SIP Phone or Conference. If you select SIP phone you can add a SIP extension to the PBX configuration. If you select Conference you can add a conference bridge to the PBX configuration. To configure a conference bridge you specify the conference bridge extension, password, conference host, host pin, video capability, and whether conferences can be recorded.

## Conference Host
The name of the PBX extension that can host conference calls using this conference bridge. The user of the conference host extension can manage the conference bridge from the PBX user web portal. The conference host user can change the conference password and host pin and change the video and recordable settings for the conference bridge.

## Host PIN
Enter the number to be entered by the conference host to be able to host a conference call.

## Conference Recordable
Select to enable recording of conference calls that use this conference bridge. You cannot select this option if the conference bridge supports video calls.

## First Name
Enter the first name of the person that will be using this extension.

## Last Name
Enter the surname of the person that will be using this extension.

## Email
Enter the email address of the person that will be using this extension.

## MAC Address
The MAC address of the SIP phone to be used for this extension. The MAC address is required if the SIP is to be configured using auto-provisioning. See “SIP phone auto-provisioning” on page 115.

## Video Capability
Select if the SIP phone can display video and handle video calls.

## Dial Plan
Select the dial plan that will be used with this extension from the drop-down list.

## Voicemail
Select if you want to have voicemail available for this extension.

## Voicemail Password
Enter a voicemail password for accessing the voicemail.

## Email Notification
Select to have an email sent to the email address given in the Email field so that the person is notified when a voicemail message is in their voicemail message inbox.
Configuring extension groups (ring groups)

Extension groups (also called ring groups) are a group of extensions that can be called using one number. The extension group can be used to call all the extensions in the group at the same time or to call the extensions one at a time until someone answers.

The order in which the members are added to the ring group does not match the order in which the FortiGate Voice unit calls them.

To add an extension group, go to PBX > Extension > Group, select Create New, enter the information, and then select OK.

![Figure 36: Configuring extension groups]

<table>
<thead>
<tr>
<th>Voicemail to Email Attachment</th>
<th>Select to attach the actual voicemail message to the notification email.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Message #</td>
<td>Enter a number for the maximum number of messages that can be stored in the extension’s voicemail inbox before automatically deleting the oldest messages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Extension Number</th>
<th>The number to call to reach extension group. This number must be a valid extension number for the FortiGate Voice configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the extension group.</td>
</tr>
<tr>
<td># of Members</td>
<td>The number of extensions in the extension group.</td>
</tr>
<tr>
<td>Ring Strategy</td>
<td>Select a type from the drop-down list. You can choose either Sequential or Ring All.</td>
</tr>
<tr>
<td>No Answer Action</td>
<td>Select the action to take when there is no answer for the incoming caller. You can select Voicemail, which routes the caller to voicemail, IVR, or Hangup. If you select Voicemail, the Voicemail Extension list appears and you need to select the voicemail extension number.</td>
</tr>
</tbody>
</table>
### Configuring service providers (the FortiGuard Voice service)

If your FortiGate Voice unit is installed in North America and the Country Code is set to 1 then you can use the FortiGuard Voice service as your SIP service provider. (The default Country Code is 1 and is set from PBX > Calling Rules > Setting.) The FortiGuard Voice service is supported only in North America. If you install the FortiGate Voice unit elsewhere in the world and change the Country Code, the FortiGuard Voice Service configuration is not available.

### Configuring PSTN interfaces

Some FortiGate Voice models include public switched telephone network (PSTN) interfaces that you can use to connect the FortiGate Voice PBX to your local public telephone network. Using these interfaces you can route calls from your FortiGate Voice network to the public telephone network. The PSTN interfaces are named fxo1, fxo2, and so on.

To configure the PSTN interfaces, go to PBX > Service Providers > PSTN Interface, configure settings for the fxo1 interface and then select OK.

**Figure 37: Configuring PSTN interfaces**

<table>
<thead>
<tr>
<th>Voicemail Extension</th>
<th>Select the voicemail extension number from the drop-down list. This option appears only when Voicemail is selected in No Answer Action.</th>
</tr>
</thead>
</table>
| Member              | Select an extension in the Available column and then use the -> arrow to move it to the Selected column.  
                      To remove an extension from the Selected column, select the extension and use the <- arrow to move it back to the Available column. |
**General PSTN interface settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the PSTN interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Number</td>
<td>The phone number that is associated with that PSTN interface.</td>
</tr>
<tr>
<td>Display Name</td>
<td>The name that displays on the phone’s LCD.</td>
</tr>
<tr>
<td>Catch Caller ID</td>
<td>If enabled, a green checkmark appears. If Catch Caller ID is disabled, a gray X appears.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Status of the PSTN interface. A red down arrow indicates that the interface is down; a green up arrow indicates that the interface is up.</td>
</tr>
</tbody>
</table>

**PSTN interface configuration settings**

<table>
<thead>
<tr>
<th>Basic Options</th>
<th>The basic options for the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the PSTN interface.</td>
</tr>
<tr>
<td><strong>Phone Number</strong></td>
<td>Enter the phone number of the PSTN phone line as provided by your phone service provider. The phone number is used for caller ID for calls from the FortiGate Voice unit to the PSTN. It can be any number, but is usually the actual phone number of the PSTN line connected to the fxo1 interface. Area code and country codes are optional.</td>
</tr>
<tr>
<td><strong>Display Name</strong></td>
<td>This name is used for caller ID for calls from the FortiGate Voice unit to the PSTN. It can be any name, such as a company name, that identifies the branch office.</td>
</tr>
<tr>
<td><strong>Caller ID Options</strong></td>
<td>Configure the following options to support caller ID functions for calls from the internal network to the PSTN.</td>
</tr>
<tr>
<td>Catch Caller ID</td>
<td>Select to enable the FortiGate Voice unit to receive caller ID information from calls originating on the PSTN and send the caller ID information to the extension that answers the call.</td>
</tr>
<tr>
<td><strong>Caller ID Protocol</strong></td>
<td>Select the caller ID protocol required by PSTN line that the fxo interface is connected to. Contact your service provider for the name of the protocol to use.</td>
</tr>
<tr>
<td><strong>Caller ID Indicator</strong></td>
<td>Select the caller ID indicator required by the PSTN line. Contact your service provider for details.</td>
</tr>
<tr>
<td><strong>Ring #</strong></td>
<td>Set the number of rings to wait before receiving caller ID information. In most cases, enter 1 to send caller ID information between the first and second ring. Contact your service provider for details.</td>
</tr>
<tr>
<td><strong>Hang-up Options</strong></td>
<td>Configure the following options to configure how the FortiGate Voice unit hangs up calls from the PSTN.</td>
</tr>
<tr>
<td>Hang up on Polarity</td>
<td>Select if the PSTN line uses polarity reversal to indicate a call has been hung up. Contact your service provider for details.</td>
</tr>
<tr>
<td>Hang up on Busy Tone</td>
<td>Select if you want the FortiGate Voice unit to hang up automatically when it receives a busy tone when attempting to dial a number on the PSTN.</td>
</tr>
</tbody>
</table>
The FortiGuard Voice service is a SIP trunking or SIP VoIP service provided by Fortinet. The FortiGuard Voice service includes the following features in addition to the being able to make calls from the FortiGate Voice unit to other VoIP providers and to the PSTN:

- Direct inward dial numbers
- FortiFAX eFAX service (see “FortiFAX service” on page 135)
- Toll free numbers
- Different calling card packages and credit levels

The FortiGuard Voice service is currently available only in North America. To use the FortiGuard Voice service the FortiGate Voice unit Country Code must be set to 1 and the FortiGate Voice unit must have a valid static public Internet IP address.

You can connect your FortiGate Voice unit to the FortiGuard Voice service by purchasing a subscription for your FortiGate Voice unit. Once you have purchased a subscription, if your FortiGate Voice unit meets the above criteria and is connected to the Internet it is also automatically connected to the FortiGuard Voice service network.

You can also go to the License Information dashboard widget or to PBX > Service Providers > FortiGuard Voice Service to subscribe to the FortiGuard Voice service. If you have already subscribed to but have not activated the service you can select Activate Now from either of these locations to activate the service.

To activate the service you must fill out the following fields:

- Area Code: The local area code used by the FortiGate Voice unit.
- Company Name: Name of the company.
- Directory List Address: Local number to call for directory listings, for example 411.
- E911 Emergency Address: Local emergency number, for example 911.

When you activate the service, FortiGuard sends the direct inward dial, EFax number, and toll free number settings assigned to the FortiGuard Voice service license assigned to the FortiGate Voice unit.

When the FortiGuard Voice service is active it is integrated into your FortiGate Voice default configuration, the company-default dial plan sends all outgoing calls to the FortiGuard Voice service.

To view the status of your FortiGuard Voice service subscription find the Voice Service entry in the License Information dashboard widget. You can also go to System > Maintenance > FortiGuard and view the status of the Voice Service entry in the FortiGuard Subscription Services list. The status of the FortiGuard Voice service should indicate that the FortiGate Voice unit is licensed for the service.
**Viewing FortiGuard Voice service status**

You can also view more detailed status information about the FortiGuard Voice service by going to PBX > Service Providers > FortiGuard Voice Service. You can view the overall status of your FortiGuard Voice service account as well as details about the service that you have purchased.

**Figure 38: FortiGuard Voice service status**

![FortiGuard Voice service status](image)

<table>
<thead>
<tr>
<th>Subscription</th>
<th>The status of the FortiGuard Voice service subscription for the FortiGate Voice unit. Status should be Yes if everything is properly configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Status</td>
<td>The status of the FortiGuard Voice service account used by the FortiGate Voice unit. If account status is active the FortiGate Voice unit can receive and send calls from and to the FortiGate Voice service.</td>
</tr>
<tr>
<td>DIDs</td>
<td>The direct inward dial numbers available from FortiGuard Voice service. DID allows the FortiGate Voice unit to direct calls from external callers directly to PBX extensions. For more information about DID, see “Configuring direct inward dialing” on page 131.</td>
</tr>
<tr>
<td>FortiFAX</td>
<td>The FortiGate Voice unit’s FortiFAX eFax number if this is part of the FortiGuard Voice service license for the FortiGate Voice unit. Third parties can send faxes to the FortiGate Voice unit using this number.</td>
</tr>
<tr>
<td>Toll Frees</td>
<td>The FortiGate Voice unit’s toll free number if this is part of the FortiGuard Voice service license for the FortiGate Voice unit. Third parties can call this number toll free to reach extensions connected to the FortiGate Voice unit.</td>
</tr>
<tr>
<td>Packages</td>
<td>Information about additional packages that are part of the FortiGuard Voice services purchased for the FortiGate Voice unit.</td>
</tr>
<tr>
<td>Package Type</td>
<td>The package type depends on the FortiGuard Voice services that have been purchased. Multiple packages are available with different features.</td>
</tr>
<tr>
<td>Calling Card Credit Left</td>
<td>The amount of money available for making phone calls to the FortiGuard Voice service from the FortiGate Voice unit for each package.</td>
</tr>
</tbody>
</table>
Adding SIP trunks

You can configure multiple VoIP providers for your PBX configuration.

To configure VoIP providers, go to PBX > Service Providers > SIP Trunk, select Create New, configure the settings and then select OK.

Figure 39: VoIP Provider

<table>
<thead>
<tr>
<th>Calling Card Credit Used</th>
<th>The amount of money spent for making phone calls to the FortiGuard Voice service from the FortiGate Voice unit for each package.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration Date</td>
<td>The date on which the package expires. When the package expires all unused calling card credit is lost.</td>
</tr>
<tr>
<td>SIP Status</td>
<td>An indicator of the SIP status of the FortiGate Voice service. If it is operating normally the status should show a green check mark icon.</td>
</tr>
</tbody>
</table>

**Name**
Enter the name for the VoIP provider configuration. This can be any name.

**Domain**
The VoIP provider’s domain name or IP address. For example, 172.20.120.11 or voip.example.com.

**User Name**
Enter a valid user name for an account on the VoIP provider’s server. This could also be a phone number including area code, depending on the requirements of the VoIP provider.

**Password**
Enter the password for the account on the VoIP provider’s SIP sever.

**Authorization User Name**
Enter a valid authorization user name for an account on the VoIP provider’s server if required by the VoIP provider.

**Display User Name**
Enter a valid display user name for an account on the VoIP provider’s server if required by the VoIP provider.

**Account Type**
Select Static or Dynamic depending on the account with the VoIP provider.
Branch Office

The branch office feature allows you to easily configure communication between two FortiGate Voice phone systems. A common application is the easy linking of branch offices in separate locations.

To configure Branch Office, go to PBX > Service Providers > Branch Office, select Create New, configure the settings and then select OK.

**Figure 40: Branch office**

<table>
<thead>
<tr>
<th>Name</th>
<th>The name for the branch office configuration. This can be any name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>The prefix required to dial an extension to the branch office. If there is no overlap between the extensions in your office and the branch office, no prefix is required. If no prefix is specified, extensions in the branch office are dialed exactly as local extensions.</td>
</tr>
<tr>
<td>Pattern</td>
<td>The extension number pattern of the branch office. For example, XXXX is any four digit number while 7XXX is a four digit number that always starts with 7.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the branch office FortiGate Voice unit.</td>
</tr>
</tbody>
</table>
Configuring dial plans

Dial plans route calls made from a FortiGate Voice extension to an external phone system. The external phone system can be one or more PSTN lines if your FortiGate Voice unit includes PSTN interfaces, or a VoIP service provider. To route calls to an external phone system you add dial plan rules that define the extra digits that extension users must dial to call out of the PBX. The rules also control how the FortiGate Voice unit handles these calls including whether to block or allow the call, the destinations the calls are routed to and whether to add digits to the beginning of the dialed number (called prepending).

For example, if PBX users should be able to dial 911 for emergencies you should include a dial plan rule that sends all calls that begin with 911 to an external phone system. This rule should also override the default outgoing prefix so that users can dial 911 without having to dial 9 first.

You can also use dial plan rules to block some calls. For example, if you want to block extensions from making international calls you can add dial plan rule that blocks calls that start with the default outgoing prefix followed by 011.

When the FortiGate Voice unit receives a call from an extension that does not match the FortiGate Voice unit’s extension range, the call is processed according to the dial plan added to the extension. (If the extension does not have a dial plan the call is blocked). To process the call, the FortiGate Voice unit selects the dial plan rule that best matches the dialed numbers and processes the call using the settings in the dial plan rule. For example, the emergency dial plan rule could route calls out a local PSTN line (if your FortiGate Voice unit includes them) or to a remote VoIP provider.

To configure dial plan, go to PBX > Calling Rules > Dial Plan, select Create New, configure the settings and then select OK.
Figure 41: Configuring a dial plan

General dial plan list settings

| Create New | Select to configure a dial plan. You can add multiple dial plans and assign them to different extensions. For example, you might want to have a dial plan that allows long distance calls and a dial plan that does not. |
| Name       | The name of the dial plan. |
| # of Entries | The number of entries in each dial plan. |
| Comments   | An optional description of the dial plan. |

Dial plan rule configuration settings

| Name | Enter a descriptive name for the dial plan rule. |
| Use Default Outgoing Prefix("9") | Select this checkbox if the dial plan rule should use the default outgoing prefix (usually 9). |
| Outgoing Prefix | If you clear the Use Default Outgoing Prefix checkbox you can enter a different outgoing prefix for this dial plan. |
This simplified example dial plan is similar the default FortiGate Voice dial plan. The default dial plan that routes all external calls to the FortiGuard Voice service. The following example includes 5 dial plan rules that:

- Routes emergency calls (dialing 911) to the fxo1 PSTN interface
- Blocks international calls (the phone number begins with 011)
- Routes Toll Free calls (beginning with 18) to the FortiGuard Voice service
- Routes non-international long distance calls (beginning with 1) to the FortiGuard Voice service
- Routes all other external calls to the fxo2 and fxo3 PSTN interfaces

In this example, all outgoing calls are routed to the PSTN and not to other VoIP service providers. On a FortiGate Voice unit without PSTN interfaces, the dial plan would route all calls to the FortiGuard Voice service or to one or more VoIP service providers.

### Table 12: Rule 1: emergency calls using 911

<table>
<thead>
<tr>
<th>Name</th>
<th>Emergency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (&quot;9&quot;)</td>
<td>Not selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td>911</td>
</tr>
</tbody>
</table>
Configuring voice menu options

The operator voice mail message can be accessed and reprogrammed by configuring recorder extension. To configure a recorder extension, go to PBX > Calling rules > Voice Menu and enter an extension number and a password. The recorder extension can be dialed from any PBX extension and used for recording a new operator voice mail message.

Configure voice menu options to provide PBX users with shortcuts to PBX functions such as accessing their voice mail, finding numbers in the company directory, or dialing a ring group.

### Table 12: Rule 1: emergency calls using 911

<table>
<thead>
<tr>
<th>Action</th>
<th>Allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outgoing Selected</td>
<td>PSTN - fxo1</td>
</tr>
</tbody>
</table>

### Table 13: Rule 2: international calls beginning with 011

<table>
<thead>
<tr>
<th>Name</th>
<th>International</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (“9”)</td>
<td>Selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td>011</td>
</tr>
<tr>
<td>Action</td>
<td>Block</td>
</tr>
</tbody>
</table>

### Table 14: Rule 3: Toll free calls starting with 18

<table>
<thead>
<tr>
<th>Name</th>
<th>Toll_Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (“9”)</td>
<td>Selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td>18</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing Selected</td>
<td>VoIP - __FtgdVoice_1</td>
</tr>
</tbody>
</table>

### Table 15: Rule 4: Long Distance calls starting with 1

<table>
<thead>
<tr>
<th>Name</th>
<th>Long_Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (“9”)</td>
<td>Selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td>1</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing Selected</td>
<td>VoIP - __FtgdVoice_1</td>
</tr>
</tbody>
</table>

### Table 16: Rule 5: Other outgoing calls

<table>
<thead>
<tr>
<th>Name</th>
<th>Other_PSTN_Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Outgoing Prefix (“9”)</td>
<td>Selected</td>
</tr>
<tr>
<td>Phone number Begin with</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Outgoing Selected</td>
<td>PSTN - fxo2, PSTN - fxo3</td>
</tr>
</tbody>
</table>
To access voice menu functions PBX users dial a single number on their phones and wait a few seconds for the PBX to respond. For example, you can use voice menu options to allow PBX users to simply dial 3 to access their voicemail.

To configure voice menu options
1. Go to PBX > Calling Rules > Voice Menu.
2. Edit the row of the key that you want to configure voice menu options for.
3. In the Action drop-down list, select one of the following:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No action will be taken when a caller dial this number.</td>
</tr>
<tr>
<td>Ring Group</td>
<td>The PBX user calls a ring group. Select the ring group to call. A ring group is also called an extension group. To add ring groups, see “Configuring extension groups (ring groups)” on page 120.</td>
</tr>
<tr>
<td>Check Voicemail</td>
<td>Provides direct access to the PBX user’s voice mail inbox.</td>
</tr>
<tr>
<td>Go to Company Directory</td>
<td>Provides direct access to the PBX company phone directory.</td>
</tr>
</tbody>
</table>

4. Select OK.

Configuring direct inward dialing

You can configure direct inward dialing (DID) for calls. DID allows the FortiGate Voice unit to direct calls from external callers directly to PBX extensions. For example, you could set up DID so that external users call 555-1234 and DID directs the call to extension 1234. Using the FortiGate Voice unit direct inward dial settings you associate an incoming PSTN interface (if supported by your FortiGate Voice unit), the FortiGuard Voice service, or VoIP service provider with a PBX extension. When an incoming call is received from one of these sources, if the last digits of the dialed number match the selected extension number the FortiGate Voice unit directs the call directly to the extension. For this to work you must obtain an external phone number with the last digits matching the selected extension.

To configure direct inward dialing, go to PBX > Calling Rules > Direct Inward Dial, enter the information, and then select OK.

Figure 42: Direct inward dialing

![Diagram of direct inward dialing configuration](image-url)
From the CLI you can use the `cid-number` option of the `config pbx did` command to specify the number called from an external line that is re-directed to the selected extension. Use this option if the extension number cannot be matched with the external number. In the following example, DID sends calls received on the fxo1 PSTN interface that end with 5555 to extension 1234.

```
config pbx did
  edit did_example
    set external-line fxo1
    set cid-number 5555
    set extension 1234
  end
end
```

**Configuring PBX global settings**

Configure PBX global settings that affect the overall performance of the PBX service and all of the users of it. Settings include the extension pattern for the PBX, information about the country or area in which the FortiGate Voice unit is installed, and the outgoing dial prefix. Usually you would configure these settings once and rarely thereafter.

The Country Code must be set to 1 to use the FortiGuard Voice service. This service is available only in North America.

To configure PBX settings group, go to `PBX > Calling Rules > Setting`, make configuration changes as required and then select Apply.
### PBX Global Settings

| **Extension Pattern** | Select two, three, or four digit extensions, or choose *Others* to specify an extension pattern.  
An extension pattern of two, three, or four digits allows you to choose any extension number of the selected length.  
Other allows you to enter a pattern that defines the valid extensions that can be added to the FortiGate Voice configuration. The pattern can include numbers that must be in every extension and upper case Xs to indicate the number of digits. The extension range can only contain numbers and the letter X.  
- If you add numbers to the extension range, all extensions added to this FortiGate Voice unit must include the same numbers in the same location in the extension number. For example, if you include a 6 as the first digit, all extensions added this FortiGate Voice unit must begin with the number 6.  
- The Xs indicate the number of digits in addition to the required number that each extension must have. For example, 6XXX indicates the extensions must start with the number 6 and be followed by any three numbers.  
Usually you would add one or two numbers to the start of the extension range to identify the extensions for this PBX and follow this with enough Xs to be able to add the required number of extensions.  
The extension range should not begin with the same number as the outgoing prefix. |
| **Country/Area** | Select the country or region in which the FortiGate Voice unit is installed. |
Importing a new voice prompt file

You can replace the default voice prompt by importing a new voice prompt file. You can create your own voice prompt file or you can obtain one in a different language from Fortinet. The new file overwrites the current voice prompt when imported.

To import a new pbx voice prompt file go to PBX > Calling Rules > Setting then select Import. The voice prompt file should be added to a tar file and zipped. This file would usually have the extension tgz.

Parking calls

Parking a call is similar to putting the caller on hold, except that the call can then be picked up from any extension.

For example, if an urgent call came in to an office for the manager, the receptionist may call the manager’s office to make sure he is present to take the call rather than blindly transferring the call and possibly sending the caller to voicemail. If the manager is not in his office, the receptionist can park the call and use the PA system to inform the manager of the call and the number to dial to receive it. He can then use the nearest extension to dial the number and take the call. Further, if the call is not taken within 45 seconds, it will ring back to the extension from which it was parked.

Without call parking, the receptionist must put the caller on hold and then determine where the manager is, direct him to a nearby extension, and finally forward the call to the extension.
To configure call parking, go to \textit{PBX > Calling Rules > Setting}.

**FortiFAX service**

The FortiFAX service is available as part of the FortiGuard Voice service for sending and receiving faxes. If your FortiGuard Voice service includes FortiFAX, the FortiGate Voice unit stores and then forwards faxes sent to and received from the FortiGuard Voice service. You can go to \textit{PBX > FortiFAX > Received Fax} to view faxes received from the FortiGuard Voice service. You can go to \textit{PBX FortiFAX > Sent Fax} to view faxes sent from a FAX device connected to the FortiGate Voice unit to the FortiGuard Voice service. For all faxes sent and received you can view information about the sender and receiver of the fax, the date and time the fax was received and the status of the fax. You can also download or delete any listed fax.

Incoming faxes are received and stored by the FortiGate Voice unit. PBX users can view their faxes from the FortiGate Voice user portal. See “Using the PBX user web portal” on page 139. The FortiGate Voice unit sends email notifications to the PBX user’s email address when a fax is received for them.

Users upload outgoing faxes to the FortiGate Voice unit using the FortiGate Voice user portal. The FortiGate Voice unit sends the faxes to their destination and records the result of sending the fax. If the fax cannot be sent right away the FortiGate Voice unit continues polling and will send the fax when possible. When the fax is sent the FortiGate Voice unit sends an email to the PBX user’s email address.

**Monitoring calls**

You can monitor incoming and outgoing calls from \textit{PBX > Monitor > Active Call}.

You can view information for all active calls including the originator of the call (From) the destination of the call (To), how long the call has been active (Duration), the codec used for transmitting voice packets, and the status of the call.

**Monitoring recorded conference calls**

You can view a list of recorded conference calls from \textit{PBX > Monitor > Recorded Conference}.

You can view information for all recorded conference calls including the host of the call, the recording time of the conference and the size of the recorded file. You can also download recordings and delete them from the FortiGate Voice unit.

All recorded conference calls are saved on the FortiGate Voice hard disk. Recordings are also available on the user portal.

**Monitoring voice mail storage**

You can view information about each PBX user’s stored voicemail messages from \textit{PBX > Monitor > Voice Mail Storage}.

The information displayed includes each extension’s voicemail status and amount of disk space used for recorded voice messages. You can delete voice mail for any or all extensions to recover disk space.

All recorded voice messages are saved on the FortiGate Voice hard disk. Recordings are also available on the user portal.

**Monitoring active phones**

You can view information about each active phone from \textit{PBX > Monitor > Phone}.
The information displayed includes each phone’s status, IP address, MAC address, and VCI.

**Logging of PBX activities**

After configuring PBX settings, you can configure logging of PBX activities and events. In addition to configuring required FortiGate logging settings you can also configure logging of PBX events.

**To configure logging of PBX settings**

1. Go to *Log&Report > Log Config > Log Setting*.
2. Select the check box beside *Enable* to make the other event log options available.
3. Select the check box beside *PBX event*.

**Viewing log messages**

You can view the PBX activities and events from *Log&Report > Log & Archive Access*. The log messages can be filtered so that you are viewing specific information, or you can display them in Raw format. Raw format is the format of what a log message actually appears in the log file.

**Example PBX log messages**

The following log message indicates that the phone with FortiGate Voice extension number 6005 called 914036085000 and the call was routed to the skype-088adb08 service provider. The call was answered and lasted for 1869 seconds.

```
2010-03-12 12:53:27 log_id=0162043782 type=event subtype=pbx pri=information fwver=040000 vd=root action=PBX-call clid="6005", src="6005" dst="914036085000" channel="SIP/6005-088a7c08" dstchannel="SIP/skype-088adb08" duration=1869 start="Fri Mar 12 12:22:18 2010 " end="Fri Mar 12 12:53:27 2010 " disposition="ANSWERED"msg="call from 6005=>914036085000, ANSWERED, for 1869 seconds"
```

The following log message indicates that the phone with FortiGate Voice extension number 6012 with caller ID Example Caller called extension 6036. And that the call was answered and lasted for 23 seconds.

```
2010-03-12 01:12:42 log_id=0162043782 type=event subtype=pbx pri=information fwver=040000 vd=root action=PBX-call clid=""Example Caller" <6012>", src="6012" dst="6036"channel="SIP/6012-084a9aa0" dstchannel="SIP/6036-08464150" duration=23 start="Fri Mar 12 01:12:19 2010 " end="Fri Mar 12 01:12:42 2010 " disposition="ANSWERED"msg="call from 6012=>6036, ANSWERED, for 23 seconds"
```

**VoIP interface reference**

The unit can effectively secure VoIP solutions since it supports VoIP protocols and associates state at the signaling layer with packet flows at the media layer. By using SIP ALG controls, the unit can interpret the VoIP signaling protocols used in the network and dynamically open and close ports (pinholes) for each specific VoIP call to maintain security.

In *UTM Profiles > VoIP > Profile*, you can configure multiple profiles for applying to firewall policies that concern only VoIP protocols.
Profile

The Profile menu allows you to configure VoIP profiles for applying to firewall policies. A profile is specific information that defines how the traffic within a policy is examined and what action may be taken based on the examination.

VoIP profile configuration settings

The following are VoIP profile configuration settings in UTM Profiles > VoIP > Profile. If the VoIP option does not appear, use this CLI command to enable it.

```
config system global
  set gui-voip-profile enable
end
``` 

### Profile page

Lists the profiles that you created for SIP and SCCP protocols. On this page, you can edit, delete or create a new profile for VoIP protocols.

You are redirected to this page when you select View List on the Edit VoIP Profile page.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new VoIP profile. When you select Create New, you are automatically redirected to the New VoIP Profile page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within a VoIP profile. When you select Edit, you are automatically redirected to the Edit VoIP Profile page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a VoIP profile from the list on the Profile page. To remove multiple VoIP profiles from within the list, on the Profile page, in each of the rows of the profiles you want removed, select the check box and then select Delete. To remove all VoIP profiles from the list, on the Profile page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the profile.</td>
</tr>
<tr>
<td>Comments</td>
<td>A description about the profile. This is an optional setting.</td>
</tr>
</tbody>
</table>
| Ref.            | Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (UTM Profiles > Antivirus > Profile), 1 appears in Ref. To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:  
  - View the list page for these objects – automatically redirects you to the list page where the object is referenced at.  
  - Edit this object – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page.  
  - View the details for this object – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy’s settings appear within the table. |
**New VoIP Profile page**

Provides settings for configuring SIP and SCCP options within the profile.

This page appears when you select *Create New* on the Edit VoIP Profile page. If you are on the Profile page, and you select *Create New*, you will be redirected to the New VoIP Profile page.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Comments</strong></td>
<td>Enter a description about the profile. This is optional.</td>
</tr>
<tr>
<td><strong>SIP</strong></td>
<td>Configuration settings for SIP protocols.</td>
</tr>
<tr>
<td><strong>Limit REGISTER requests</strong></td>
<td>Enter a number for limiting the time it takes to register requests.</td>
</tr>
<tr>
<td><strong>Limit INVITE requests</strong></td>
<td>Enter a number to limit invitation requests.</td>
</tr>
<tr>
<td><strong>SCCP</strong></td>
<td>Configuration settings for SCCP protocols.</td>
</tr>
<tr>
<td><strong>Limit Call Setup</strong></td>
<td>Enter a number to limit call setup time.</td>
</tr>
</tbody>
</table>
Using the PBX user web portal

This section describes how to log into and use the FortiGate Voice PBX portal. FortiGate Voice PBX users can use the PBX web user portal to configure some of their extension’s PBX settings, retrieve their voicemail, configure call forwarding for their extension, and review conference calls and conference call recordings.

Logging into and out of the FortiGate Voice PBX user web portal

FortiGate Voice PBX users use their extension number and password to log in to the PBX user web portal.

To log into the PBX user web portal

1. Open any web browser and browse to the following address:
   
   \[ \text{https://}<\text{interface}\_address>:8443 \]

   where:
   
   \<\text{interface}\_address> is the IP address or domain name of a FortiGate Voice interface from which users can access the FortiGate Voice PBX user web portal.
   
   8443 is the default port that users must browse to connect to the portal. FortiGate Voice system administrators can change this port number.

2. On the login form enter your extension number and extension password as provided by your system administrator and select Login.

   If you successfully log in the user portal web-based manager is displayed.

To log out of the PBX user web portal

1. Select the Logout icon that appears at the top of every PBX user web portal page.

Configuring PBX extension settings

Go to Configuration > Setting to view your extension settings and to change your PBX user web portal password, and voicemail password and other PBX settings.

<table>
<thead>
<tr>
<th>Extension</th>
<th>The extension number used to log into the portal (view only).</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>The first and last names assigned to this extension number (view only).</td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>The email address assigned to this extension number (view only).</td>
</tr>
</tbody>
</table>
Voicemail

You can view lists of your extension’s voicemail messages. Any message can be downloaded to be listened to or deleted. You can also save voicemail messages. Saved messages appear on the saved message list. If you have listened to voicemail messages from your SIP phone but not saved them they are added to the Old Message list.

To download or delete a message, select the message and select Download or Delete.

Configuring call forwarding

Use call forwarding options to configure forward your calls. The following options are available. Select an option and select OK to save the change.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Disable or turn off call forwarding.</td>
</tr>
<tr>
<td>Forward Calls to VoiceMail Box</td>
<td>Send all calls directly to your voicemail. The caller hears your welcome message and can leave a message for your voicemail. The extension does not ring.</td>
</tr>
</tbody>
</table>
Sending a Fax using FortiFAX

To send a fax, create a pdf file containing the pages that you want to send. Use the following instructions to upload the pdf to the FortiGate Voice PBX and send it as a fax.

To send a fax, go to FortiFAX > Fax Document Upload. Enter the fax number that you want to send a fax message to. Select Browse to upload the pdf file that you want to send. You can also type in the file location manually into the File to Fax field. Select OK to send the fax. A message appears to confirm that the fax has been sent.

The FortiGate Voice PBX stores a copy of the pdf file, which is only viewable by a system administrator.

Conference calls

If the PBX administrator has made your extension a conference bridge host you can view the conference bridges that you can host, change their configuration, and see lists of the participants in an active conference call using your conference bridges. You can also manage conference call recordings for your conference bridges.

To change your conference bridge settings, log into the PBX user web portal and go to Conference > Conference List and edit the conference bridge.

<table>
<thead>
<tr>
<th>Conference ID</th>
<th>The number that participants dial to call into a conference using this conference bridge (view only).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Change the password for this conference bridge. The password cannot be blank and must contain only numbers. This becomes the conference PIN number.</td>
</tr>
<tr>
<td>Host</td>
<td>The extension number of the conference bridge host, which is your extension number (view only).</td>
</tr>
<tr>
<td>Host Pin</td>
<td>Change the host pin for this conference bridge. The pin only contain numbers.</td>
</tr>
</tbody>
</table>
Conference call recordings are saved on the FortiGate Voice hard disk. You can go to Conference > Recorded Conference to download and delete conference call recordings.

## Managing conference calls

The conference bridge host must dial into the conference bridge and enter the host pin for the conference call to start. During the call the host can also do the following from the phone used to start the conference call:

- Press * to hear a conference bridge menu
- Press 8 to start recording the conference call
- Press 9 to stop recording the conference call

Conference call recordings are saved on the FortiGate Voice hard disk. After the recording has been stopped and the call ended the host can log into the FortiGate Voice PBX user web portal and download or delete conference call recordings.

<table>
<thead>
<tr>
<th>Video</th>
<th>Select if the conference bridge can display video and handle video calls.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recordable</td>
<td>Select to enable recording of conference calls that use this conference bridge. You cannot select this option if the conference bridge supports video calls.</td>
</tr>
</tbody>
</table>
FortiGate Voice VoIP, PBX, and PSTN CLI Reference

This section describes FortiGate Voice VoIP, PBX, and PSTN configuration settings. PSTN interfaces are not available on all FortiGate Voice models. For information about other FortiGate Voice CLI commands see the FortiGate CLI Reference.

This section describes:
- `config pbx dialplan`
- `config pbx did`
- `config pbx extension`
- `config pbx global`
- `config pbx ringgrp`
- `config pbx voice-menu`
- `config pbx sip-trunk`
- `config system pstn`
- `config system interface`
- `execute pbx`
- `get pbx ftgd-voice-pkg`
- `get pbx global`
- `get pbx voice-menu`
- `diagnose pbx restart`

**config pbx dialplan**

Use this command to add a dial plan and add rules to the dial plan. A dial plan rule indicates an outgoing destination to send calls to. You can add multiple rules to a dial plan. You add dial plans to extensions to control how to handle outgoing calls from the extension.

**Syntax**

```plaintext
config pbx dialplan
    edit <pbx_dialplan_name>
        set comments <comment_string>
    config rule
        edit <rule_name_str>
            set action {allow | block}
            set callthrough {fxo1 | fxo2 | fxo3 | fx04 | <voip_providers>}
            set outgoing-prefix <pattern_str>
            set phone-no-beginwith <pattern_str>
            set prepend <pattern_str>
```
```
set use-global-outgoing-prefix {no | yes}
end
```

### Variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit &lt;pbx_dialplan_name&gt;</td>
<td>Enter the name for the dial plan. If you entering an existing dial plan, select Tab to get to the dial plan that you want to edit.</td>
<td>No default</td>
</tr>
<tr>
<td>comments &lt;comment_string&gt;</td>
<td>Optionally enter a description of the dial plan.</td>
<td>No default</td>
</tr>
<tr>
<td>config rule</td>
<td>Configure a new dial plan rule.</td>
<td>No default</td>
</tr>
<tr>
<td>edit &lt;rule_name_str&gt;</td>
<td>Enter the name of the dial plan rule to configure.</td>
<td>No default</td>
</tr>
<tr>
<td>action {allow</td>
<td>block}</td>
<td>Set the action to allow if this dial plan rule should allow a call. Set the action to block if the dial plan should block a call. For example, if you want to block international calls you could set the Phone Number begin with to 011 and set the action to block.</td>
</tr>
<tr>
<td>callthrough {fxo1</td>
<td>fxo2</td>
<td>fxo3</td>
</tr>
<tr>
<td>outgoing-prefix &lt;pattern_str&gt;</td>
<td>If you set use-global-outgoing-prefix to no you can enter a different outgoing prefix for this dial plan.</td>
<td>null</td>
</tr>
<tr>
<td>phone-no-beginwith &lt;patern_str&gt;</td>
<td>Enter the leading digits of the phone number that this dial plan rule should match with. For example, a dial plan rule for toll free numbers in North America should begin with 18. The FortiGate Voice uses a best match to match a dialed number with a dial plan. So each dial plan should have a different Phone number Begin with setting. But you should plan your dial plan to make sure that unexpected matches do not occur.</td>
<td>null</td>
</tr>
<tr>
<td>prepend &lt;pattern_str&gt;</td>
<td>Add digits that should be prepended or added to the beginning of the dialed number before the call is forwarded to its destination. You can prepend digits at the beginning of a call of special dialing is required to reach and external phone system.</td>
<td>null</td>
</tr>
<tr>
<td>use-global-outgoing-prefix {no</td>
<td>yes}</td>
<td>Select yes if the dial plan rule should use the default outgoing prefix (usually 9). Select no to add a different outgoing-prefix.</td>
</tr>
</tbody>
</table>
config pbx did

Use this command to configure Direct Inward Dialing (DID). DID allows calls from external phone systems to dial directly to extensions added to the FortiGate Voice unit.

Syntax

```
config pbx did
  edit <pbx_did_name>
    set external-line {fxo1 | fxo2 | fxo3 | fx04 | <voip_providers>}
    set cid-number <phone_number>
    set extension <extension_number>
    set comment <comment_string>
  end
```

Variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit &lt;pbx_did_name&gt;</td>
<td>Enter the name for the Direct Inward Dial.</td>
<td>No default</td>
</tr>
<tr>
<td>external-line</td>
<td>Select one external system that can dial directly to an extension. fxo1, fxo2, fxo3, and fx04 are the 4 PSTN interfaces. &lt;voip_providers&gt; are the VoIP providers added to the FortiGate Voice.</td>
<td>null</td>
</tr>
<tr>
<td>cid-number &lt;phone_number&gt;</td>
<td>Enter the phone number dialed by a caller on the external system.</td>
<td>null</td>
</tr>
<tr>
<td>extension &lt;extension_number&gt;</td>
<td>Enter the FortiGate Voice extension number the call is directed to.</td>
<td>null</td>
</tr>
<tr>
<td>comment &lt;comment_string&gt;</td>
<td>Enter a description, if applicable, about the direct inward dial configuration.</td>
<td>null</td>
</tr>
</tbody>
</table>

config pbx extension

Use this command to add SIP phone extensions to the FortiGate Voice unit. You can add new extensions or reconfigure the existing ones. For example, you can label an extension by user name, or you can add an extension and set it as a host for conference calls, or you can get FortiGate Voice unit to send email notifications to the users when they receive new voicemail messages.

FortiGate Voice uses the alertmail settings to access an SMTP server and send email notifications. Alertmail can be configured through config system alertmail command. For more information about alertmail CLI command configuration refer to FortiGate CLI Reference.

Syntax

```
config pbx extension
  edit <extension_number>
    set attach {enable | disable}
    set auto-delete {enable | disable}
    set conference-host <extension_number>
    set dialplan <dialplan_name>
    set email <user_email>
```
```fortigate
set email-notify {enable | disable}
set first-name <first_name>
set host-pin <host_password>
set last-name <surname_name>
set macaddress <mac_address>
set max-msg <max_messages_allowed>
set nat {no | yes}
set recordable-flag {enable | disable}
set secret <user_password>
set type {conference | sip-phone}
set video {enable | disable}
set vm-secret <user_password>
set voicemail {enable | disable}
end
```

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit &lt;extension_number&gt;</td>
<td>Enter the extension number. The extension number has to match the config pbx global extension pattern.</td>
<td>No default</td>
</tr>
<tr>
<td>attach {enable</td>
<td>disable}</td>
<td>Enable the voicemail message as an attachment in an email.</td>
</tr>
<tr>
<td>auto-delete {enable</td>
<td>disable}</td>
<td>Enable to automatically delete voice mail.</td>
</tr>
<tr>
<td>conference-host &lt;extension_number&gt;</td>
<td>Enter the extension number that will host the conference.</td>
<td>null</td>
</tr>
<tr>
<td>dialplan &lt;dialplan_name&gt;</td>
<td>Enter the dial plan that you want to use for the extension.</td>
<td>null</td>
</tr>
<tr>
<td>email &lt;user_email&gt;</td>
<td>Enter the user's email address. This email address can be used to notify the user when they have a new voicemail message.</td>
<td>null</td>
</tr>
<tr>
<td>email-notify {enable</td>
<td>disable}</td>
<td>Enable email notification. When email notification is enabled the user gets notified of each new voicemail messages.</td>
</tr>
<tr>
<td>first-name &lt;first_name&gt;</td>
<td>Enter the person's first name.</td>
<td>null</td>
</tr>
<tr>
<td>host-pin &lt;host_password&gt;</td>
<td>Enter the password for the conference call. The password must contain only numbers. The users need to enter this password to join the conference call.</td>
<td></td>
</tr>
<tr>
<td>last-name &lt;surname_name&gt;</td>
<td>Enter the surname of the person.</td>
<td>null</td>
</tr>
<tr>
<td>macaddress &lt;mac_address&gt;</td>
<td>Enter the MAC address of the SIP phone for the current extension. A typical MAC address consists of six double digit alpha-numeric characters separated by colons. Colons must be used when entering the MAC address.</td>
<td>00:00:00:00:00:00</td>
</tr>
<tr>
<td>max-msg &lt;max_messages_allowed&gt;</td>
<td>Enter the maximum number of voicemail messages that are allowed in a user’s voicemail inbox.</td>
<td>50</td>
</tr>
</tbody>
</table>
config pbx global

Use this command to configure voicemail settings such as limiting the length of voicemail messages, as well as the country and the extension pattern of the user.

Syntax

```
config pbx global
  set atxfer-dtmf <str>
  set blindxfer-dtmf <str>
  set block-blacklist {enable | disable}
  set code-callpark <str>
  set country-area <country_name>
  set country-code <country_code>
  set dtmf-callpark <str>
  set efax-check-interval <integer>
  set extension-pattern <extension_pattern>
  set fax-admin-email <email_address>
  set ftgd-voice-server <server_address>
  set local-area-code <code_string>
  set max-voicemail <max_length_seconds>
  set outgoing-prefix <pattern_str>
  set parking-slots <int>
  set parking-time <int>
  set ring-timeout <time_int>
  set rtp-hold-timeout <time_int>
  set rtp-timeout <time_int>
  set voicemail-extension <access_number>
end
```
### Variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>atxfer-dtmf &lt;str&gt;</code></td>
<td>The DTMF command to trigger an attended transfer.</td>
<td>*2</td>
</tr>
<tr>
<td><code>blindxfer-dtmf &lt;str&gt;</code></td>
<td>The DTMF command to trigger a blind transfer.</td>
<td>#1</td>
</tr>
<tr>
<td><code>block-blacklist</code></td>
<td>Enable to block blacklist IP addresses.</td>
<td>enable</td>
</tr>
<tr>
<td><code>code-callpark &lt;str&gt;</code></td>
<td>Enter this numeric code to park the current call.</td>
<td>700</td>
</tr>
<tr>
<td><code>country-area &lt;country_name&gt;</code></td>
<td>Enter the name of the country in which the FortiGate Voice unit is installed.</td>
<td>USA</td>
</tr>
<tr>
<td><code>country-code &lt;country_code&gt;</code></td>
<td>Enter the country code in which the FortiGate Voice unit is installed.</td>
<td>1</td>
</tr>
<tr>
<td><code>dtmf-callpark &lt;str&gt;</code></td>
<td>The DTMF command to trigger a call park.</td>
<td>#72</td>
</tr>
<tr>
<td><code>efax-check-interval &lt;integer&gt;</code></td>
<td>Enter the efax polling interval from FortiGuard fax server. The value range is 5 to 120 in minutes.</td>
<td>5</td>
</tr>
<tr>
<td><code>extension-pattern &lt;extension_pattern&gt;</code></td>
<td>Enter a pattern that defines the valid extensions that can be added to the FortiGate Voice configuration. The pattern can include numbers that must be in every extension and upper case Xs to indicate the number of digits. The extension range can only contain numbers and the letter X.</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td>- If you add numbers to the extension range, all extensions added to this FortiGate Voice unit must include the same numbers in the same location in the extension number. For example, if you include a 6 as the first digit, all extensions added this FortiGate Voice unit must begin with the number 6.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The Xs indicate the number of digits in addition to the required number that each extension must have. For example, 6XXX indicates the extensions must start with the number 6 and be followed by any three numbers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Usually you would add one or two numbers to the start of the extension range to identify the extensions for this PBX and follow this with enough Xs to be able to add the required number of extensions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The extension range should not begin with the same number as the outgoing prefix.</td>
<td></td>
</tr>
<tr>
<td><code>fax-admin-email &lt;email_address&gt;</code></td>
<td>Enter the email address of the fax administrator.</td>
<td>null</td>
</tr>
</tbody>
</table>
config pbx ringgrp

Use this command to add and configure the extension groups. An extension group here is referred to a ring group and is a group of extensions that can be called using one number. You can configure the ring group to call all of the extensions in the group at the same time or to call the extensions one at a time until someone answers.

The order in which the members are added to the ring group does not match the order in which the FortiGate Voice unit calls them.

Syntax

```plaintext
config pbx ringgrp
   edit <ring_group_name>
      set description <description_str>
```
config pbx voice-menu

Use this command to configure the menu that callers will access when they call. The variable `config press-<number>` configures the settings for the type of ring group and the type of group associated with that number.

**Syntax**

```
config pbx voice-menu
    set comment <comment_string>
    set password <ext_password>
    set recorder-exten <extension_str>
            set type {directory | none | ring-group | voicemail}
        end
    set ring-group <group_string>
end
```
Use this command to configure SIP server providers for the PBX. If your FortiGate Voice unit is installed in North America and the Country Code is set to 1 then you can use the FortiGuard Voice service as your SIP service provider. (The default Country Code is 1, see “config pbx global” on page 147 for changing country code.) The FortiGuard Voice service is supported only in North America. If you install the FortiGate Voice unit elsewhere in the world and change the Country Code, the FortiGuard Voice Service configuration is replaced by the SIP trunk configuration. You can use the SIP trunk configuration to add one or more SIP service providers to the FortiGate Voice configuration.

Syntax

```
config pbx voip-provider
edit <provider_name>
  set user <user_name>
  set domain {<VoIP_provider_address_ipv4> | <VoIP_provider_domain>}
  set secret <password>
  set authuser <authuser>
  set display-name <display_name>
  set registration-interval <refresh_interval>
  set account-type {static | dynamic}
  set dtmf-method {auto | inband | info | rfc2833}
  set codec {alaw | g729 | u-law | ulaw}
  set codec1 {alaw | g729 | u-law | ulaw}
  set codec2 {alaw | g729 | u-law | ulaw}
```
config system pstn

Use this command to configure the PSTN interfaces. PSTN interfaces are available on some FortiGate Voice models.

Syntax

    config system pstn
    edit <fxo_name>
        set cid-name <caller_name>
        set cid-number <caller_name>
        set status {enable | disable}
        set video {enable | disable}
    end

Variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit &lt;provider_name&gt;</td>
<td>Enter the VoIP provider’s name.</td>
<td>No default</td>
</tr>
<tr>
<td>user &lt;user_name&gt;</td>
<td>Enter the user name for the provider. You can enter the phone number registered with this provider instead.</td>
<td>No default</td>
</tr>
<tr>
<td>secret &lt;password&gt;</td>
<td>Enter the password associated with the provider.</td>
<td>No default</td>
</tr>
<tr>
<td>domain</td>
<td>The VoIP provider’s domain name or IP address.</td>
<td>No default</td>
</tr>
<tr>
<td></td>
<td>{&lt;VoIP_provider_address_ipv4&gt;</td>
<td>&lt;VoIP_provider_domain&gt;</td>
</tr>
<tr>
<td>authuser &lt;authuser&gt;</td>
<td>Enter the authentication user for the account.</td>
<td>No default</td>
</tr>
<tr>
<td>display-name &lt;display_name&gt;</td>
<td>Enter the name that will be used as the caller ID name if the provider supports this feature.</td>
<td>No default</td>
</tr>
<tr>
<td>registration-interval &lt;refresh_interval&gt;</td>
<td>Enter a number for the refresh interval.</td>
<td>No default</td>
</tr>
<tr>
<td>account-type {static</td>
<td>dynamic}</td>
<td>Enter to define the type of account.</td>
</tr>
<tr>
<td>dtmf-metod {auto</td>
<td>inband</td>
<td>info</td>
</tr>
<tr>
<td>codec {alaw</td>
<td>g729</td>
<td>none</td>
</tr>
<tr>
<td>codec1 {alaw</td>
<td>g729</td>
<td>none</td>
</tr>
<tr>
<td>codec2 {alaw</td>
<td>g729</td>
<td>none</td>
</tr>
<tr>
<td>video {enable</td>
<td>disable}</td>
<td>Enable video capability if the provider supports this feature.</td>
</tr>
</tbody>
</table>
```
set use-callerid {enable | disable}
set cid-signalling {bell | dtmf | v23 | v23-jp}
set cid-start {polarity | ring}
set send-callerid-after <integer>
set hangup-on-polarity-reversal {enable | disable}
set hangup-on-zero-voltage {enable | disable}
set hangup-on-busy-tone {enable | disable}
set busycount <integer>
set busy-tone-length <integer>
set busy-quiet-length <integer>
set codec {alaw | ulaw}
end
```

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit &lt;fxo_name&gt;</td>
<td>Enter the name of the FXO.</td>
<td>No default</td>
</tr>
<tr>
<td>cid-name &lt;caller_name&gt;</td>
<td>This name is used for caller ID for calls from the FortiGate Voice unit to the PSTN. It can be any name, such as a company name, that identifies the branch office.</td>
<td>No default</td>
</tr>
<tr>
<td>cid-number &lt;caller_name&gt;</td>
<td>Enter the phone number of the PSTN phone line as provided by your phone service provider.</td>
<td>No default</td>
</tr>
<tr>
<td>status {enable</td>
<td>disable}</td>
<td>Enable the status of the port.</td>
</tr>
<tr>
<td>use-callerid {enable</td>
<td>disable}</td>
<td>Enable to catch the caller ID.</td>
</tr>
<tr>
<td>cid-signalling {bell</td>
<td>dtmf</td>
<td>v23</td>
</tr>
<tr>
<td>cid-start {polarity</td>
<td>ring}</td>
<td>Enter to start transmitting the caller ID.</td>
</tr>
<tr>
<td>send-callerid-after &lt;integer&gt;</td>
<td>Enter a number for the number of rings after that the caller ID began to transmit.</td>
<td>1</td>
</tr>
<tr>
<td>hangup-on-polarity-reversal {enable</td>
<td>disable}</td>
<td>Enable to have the phone hang up when there is polarity reversal.</td>
</tr>
<tr>
<td>hangup-on-zero-voltage {enable</td>
<td>disable}</td>
<td>Enable to have the phone hang up when there is zero voltage.</td>
</tr>
<tr>
<td>hangup-on-busy-tone {enable</td>
<td>disable}</td>
<td>Enable to have the phone hang up when a busy tone is detected.</td>
</tr>
<tr>
<td>busycount &lt;integer&gt;</td>
<td>Enter a number for the accurate number of busy tones that are detected.</td>
<td>4</td>
</tr>
<tr>
<td>busy-tone-length &lt;integer&gt;</td>
<td>Enter a number that determines how long the busy tone is on in milliseconds.</td>
<td>500</td>
</tr>
<tr>
<td>busy-quiet-length &lt;integer&gt;</td>
<td>Enter a number that determines how long the busy tone is off in milliseconds.</td>
<td>500</td>
</tr>
</tbody>
</table>
### config system interface

Use this command to allow traffic for the VoIP protocol, SIP, to flow on a specific interface. You can also allow users to access PBX user portal and enable auto-provisioning for SIP phone configuration on the same interface.

#### Syntax

```chmod
config system interface
    edit <interface_name>
        set pbx-user-portal {enable | disable}
        set phone-auto-provision {enable | disable}
```

#### Variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>codec {alaw</td>
<td>ulaw}</td>
<td>Enter the Codec preference type based on the country.</td>
</tr>
<tr>
<td>ring detect {ring-cross-threshold</td>
<td>ring-full-wave</td>
<td>ring-half-wave</td>
</tr>
<tr>
<td>ring-timeout {128ms</td>
<td>256ms</td>
<td>384ms</td>
</tr>
</tbody>
</table>
| ring-threshold {level-1 | level-2 | level-3} | Enter the appropriate ring threshold for your phone system. The ring-threshold is based on voltage:

  - level-1: 13.5V to 16.5V
  - level-2: 19.35V to 23.65V
  - level-3: 40.5V to 49.5V | level-1 |
| ring-delay-time {256ms | 512ms | 768ms | 1024ms | 1280ms | 1536ms | 1792ms} | Enter the appropriate ring delay time for your phone system. | 512ms |
| ring-confirm-time {100ms | 150ms | 200ms | 256ms | 384ms | 512ms | 640ms | 1024ms} | Enter the appropriate ring confirmation time for your phone system. | 512ms |
| ring-max-assertion-count <int> | Enter the appropriate ring maximum assertion count for your phone system. | 22 |
| ring-assertion-time <int> | Enter the appropriate ring assertion time for your phone system. | 25 |
| tx-gain <int> | Enter the gain for the transmitted signal, in dB, from -15 to 12. | 0 |
| rx-gain <int> | Enter the gain for the received signal, in dB, from -15 to 12. | 0 |
execute pbx

Use this command to view active channels and to delete, list or upload music files for when music is playing while a caller is on hold.

Syntax

execute pbx active-call <list>
execute pbx extension <list>
execute pbx ftgd-voice-pkg {sip-trunk}
execute pbx music-on-hold {delete | list | upload}
execute pbx prompt upload ftp <file.tgz>
    <ftp_server_address>[:port] [<username>] [password>]
execute pbx prompt upload tftp <file.tgz>
    <ftp_server_address>[:port] [<username>] [password>]
execute pbx prompt upload usb <file.tgz>
    <ftp_server_address>[:port] [<username>] [password>]
execute pbx restore-default-prompts
execute pbx sip-trunk list

Variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-call &lt;list&gt;</td>
<td>Enter to display a list of the active calls being processed by the FortiGate Voice unit.</td>
<td></td>
</tr>
<tr>
<td>extension &lt;list&gt;</td>
<td>Enter to display the status of all extensions with SIP phones that have connected to the FortiGate Voice unit.</td>
<td></td>
</tr>
<tr>
<td>ftgd-voice-pkg {sip-trunk}</td>
<td>Enter to retrieve FortiGuard voice package sip trunk information.</td>
<td></td>
</tr>
<tr>
<td>music-on-hold {delete</td>
<td>list</td>
<td>upload}</td>
</tr>
<tr>
<td>prompt upload ftp &lt;file.tgz&gt;</td>
<td>Upload new pbx voice prompt files using FTP. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename, FTP server address (domain name of IPv4 address) and if required the username and password for the server.</td>
<td></td>
</tr>
</tbody>
</table>
get pbx branch-office

Use this command to list the configured branch offices.

Syntax

get pbx branch-office

Example output

== [ Branch 15 ]
name: Branch 15
== [ Branch 12 ]
name: Branch 12

Example command output

Enter the following command to view active calls:

execute pbx active-call

Call-From  Call-To  Durationed
6016 6006 00:00:46

Enter the following command to display the status of all extensions

execute pbx extension list

Extension  Host                 Dialplan
6052      Unregister          company-default
6051      Unregister          company-default
6050      Unregister          company-default
6022      Unregister          company-default
6021/6021 172.30.63.34        company-default
6020      Unregister          company-default

Enter the following command to display the status of all SIP trunks

esecute pbx sip-trunk list

Name        Host          Username     Account-Type    State
Provider_1  192.169.20.1  +5555555     Static           N/A
get pbx dialplan

Use this command to list the configured dial plans.

Syntax

get pbx dialplan

Example output

== [ company-default ]
name: company-default
== [ inbound ]
name: inbound

get pbx did

Use this command to list the configured direct inward dial (DID) numbers.

Syntax

get pbx did

Example output

== [ Operator ]
name: Operator
== [ Emergency ]
name: Emergency

get pbx extension

Use this command to list the configured extensions.

Syntax

get pbx extension

Example output

== [ 6555 ]
extension: 6555
== [ 6777 ]
extension: 6777
== [ 6111 ]
extension: 6111

get pbx ftgd-voice-pkg

Use this command to display the current FortiGate Voice service package status.

Syntax

get pbx ftgd-voice-pkg status
Example output

Status: Activated
Total 1 Packages:
Package Type: B, Credit Left: 50.00, Credit Used: 0.00,
Expiration Date: 2011-01-01 12:00:00

Total 1 Dids:
12345678901
Total 1 Efaxes:
12345678902
Total 0 Tollfrees:

get pbx global

Use this command to display the current global pbx settings.

Syntax
get pbx global

Example output

block-blacklist : enable
country-area : USA
country-code : 1
efax-check-interval : 5
extension-pattern : 6XXX
fax-admin-email : faxad@example.com
ftgd-voice-server : service.fortivoice.com
local-area-code : 408
max-voicemail : 60
outgoing-prefix : 9
ring-timeout : 20
rtp-hold-timeout : 0
rtp-timeout : 60
voicemail-extension : *97

get pbx ringgrp

Use this command to display the currently configured ring groups.

Syntax
get pbx ringgrp

Example output

== [ 6001 ]
  name: 6001
== [ 6002 ]
  name: 6002

get pbx sip-trunk

Use this command to display the currently configured SIP trunks.
Syntax
get pbx sip-trunk

Example output
== [ _FtgdVoice_1 ]
name: _FtgdVoice_1

get pbx voice-menu

Use this command to display the current voice menu and recorder extension configuration.
Syntax
get pbx voice-menu

Example output
comment : general
password : *
press-0:
  ring-group : 6001
type : ring-group
press-1:
type : voicemail
press-2:
type : directory
press-3:
type : none
press-4:
type : none
press-5:
type : none
press-6:
type : none
press-7:
type : none
press-8:
type : none
press-9:
type : none
recorder-exten : *30

diagnose pbx restart

Use this diagnose command to restart the FortiGate Voice PBX daemon.
diagnose pbx restart
Document conventions

Fortinet technical documentation uses the conventions described below.

IPv4 IP addresses

To avoid publication of public IPv4 IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Most of the examples in this document use the following IP addressing:

IP addresses are made up of A.B.C.D:
- A - can be one of 192, 172, or 10 - the private addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
  - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
  - Device or virtual device - allows multiple FortiGate units in this address space (VDOMs).
  - Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
  - 001 - 099 - physical address ports, and non-virtual interfaces
  - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.
- D - usage based addresses, this part is determined by what the device is doing. The following gives 16 reserved, 140 users, and 100 servers in the subnet.
  - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
  - 010 - 099 - DHCP range - users
  - 100 - 109 - FortiGate devices - typically only use 100
  - 110 - 199 - servers in general (see later for details)
  - 200 - 249 - static range - users
  - 250 - 255 - reserved (255 is broadcast, 000 not used)
  - The D segment servers can be farther broken down into:
    - 110 - 119 - Email servers
    - 120 - 129 - Web servers
    - 130 - 139 - Syslog servers
    - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
    - 150 - 159 - VoIP / SIP servers / managers
    - 160 - 169 - FortiAnalyzers
    - 170 - 179 - FortiManagers
    - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
    - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
  - Fortinet products, non-FortiGate, are found from 160 - 189.
Example Network

Variations on network shown in Figure 44 are used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

Figure 44: Example network
### Table 17: Example IPv4 IP addresses

<table>
<thead>
<tr>
<th>Location and device</th>
<th>Internal</th>
<th>Dmz</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Office, one FortiGate</td>
<td>10.11.101.100</td>
<td>10.11.201.100</td>
<td>172.20.120.191</td>
</tr>
<tr>
<td>Head Office, second FortiGate</td>
<td>10.12.101.100</td>
<td>10.12.201.100</td>
<td>172.20.120.192</td>
</tr>
<tr>
<td>Branch Office, one FortiGate</td>
<td>10.21.101.100</td>
<td>10.21.201.100</td>
<td>172.20.120.193</td>
</tr>
<tr>
<td>Office 7, one FortiGate with 9 VDOMs</td>
<td>10.79.101.100</td>
<td>10.79.101.100</td>
<td>172.20.120.194</td>
</tr>
<tr>
<td>Office 3, one FortiGate, web server</td>
<td>n/a</td>
<td>10.31.201.110</td>
<td>n/a</td>
</tr>
<tr>
<td>Bob in accounting on the corporate user network</td>
<td>10.0.11.101.200</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>(DHCP) at Head Office, one FortiGate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router outside the FortiGate</td>
<td>n/a</td>
<td>n/a</td>
<td>172.20.120.195</td>
</tr>
</tbody>
</table>

### Tips, must reads, and troubleshooting

- **A Tip** provides shortcuts, alternative approaches, or background information about the task at hand. Ignoring a tip should have no negative consequences, but you might miss out on a trick that makes your life easier.

- **A Must Read item** details things that should not be missed such as reminders to back up your configuration, configuration items that must be set, or information about safe handling of hardware. Ignoring a must read item may cause physical injury, component damage, data loss, irritation or frustration.

- **A Troubleshooting tip** provides information to help you track down why your configuration is not working.

### Typographical conventions

<table>
<thead>
<tr>
<th>Table 18: Typographical conventions in Fortinet technical documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convention</strong></td>
</tr>
<tr>
<td>Button, menu, text box, field, or check box label</td>
</tr>
<tr>
<td>CLI input</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>CLI output</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Registering your Fortinet product

Access to Fortinet customer services, such as firmware updates, support, and FortiGuard services, requires product registration. You can register your Fortinet product at http://support.fortinet.com.

Training Services

Fortinet Training Services offers courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet training programs serve the needs of Fortinet customers and partners world-wide.

Visit Fortinet Training Services at http://campus.training.fortinet.com, or email training@fortinet.com.

Technical Documentation

Visit the Fortinet Technical Documentation web site, http://docs.fortinet.com, for the most up-to-date technical documentation.

The Fortinet Knowledge Base provides troubleshooting, how-to articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Customer service and support

Fortinet is committed to your complete satisfaction. Through our regional Technical Assistance Centers and partners worldwide, Fortinet provides remedial support during the operation phase of your Fortinet product’s development life cycle. Our Certified Support Partners provide first level technical assistance to Fortinet customers, while the regional TACs solve complex technical issues that our partners are unable to resolve.


Fortinet products End User License Agreement

See the Fortinet products End User License Agreement.
Index

A
ALG
changing the port numbers that the SIP ALG listens on, 37

B
block, 82
body
SIP message, 12
branch, 88

call-keepalive, 39, 40
certification, 164
configure
FortiGuard, 99
contact-fixup, 67
Content-Length
SIP header, 82
conventions, 161
customer service, 164

d
deep SIP message inspection, 78
default
VoIP profile, 36

diagnose sys sip, 33, 38
diagnose sys sip debug-mask, 33
diagnose sys sip dialog, 33
diagnose sys sip mapping list, 33
diagnose sys sip status, 33
diagnose sys sip-proxy calls, 37
diagnose sys sip-proxy filter, 37
diagnose sys sip-proxy log-filter, 37
diagnose sys sip-proxy meters, 37
diagnose sys sip-proxy stats, 37
diagnose test application sip, 37
dialog
SIP, 11, 17
documentation
conventions, 161
Fortinet, 164
DoS sensor
SCCP, 84
SIP, 84
dynamic IP pool
SIP, 64

F
field
SIP, 22
final
SIP response message, 21
FortiFone
configuring, 106
SIP phone, 12
FortiGuard, 99
Antivirus, 164
Fortinet
Technical Documentation, conventions, 161
Technical Support, 164
Technical Support, registering with, 164
Training Services, 164
Fortinet customer service, 164
Fortinet documentation, 164
fuzzing protection
SIP, 78

g
get test sip, 37
gui-voip-profile, 35

H
HA
SIP session failover, 86
hardware acceleration
RTP, 19
header
SIP, 22
SIP messages, 12
HNT, 72
hnt-restrict-source-ip, 77
hosted NAT traversal
See HNT, 72
hosted-nat-traversal, 75

I
inactivity timeout
SIP session, 39
informational
SIP response message, 21
inspection without address translation
SIP, 15, 35
introduction
Fortinet documentation, 164
IP address
private network, 161
IP address conservation
   NAT, 65
IP pool
   SIP, 64
IPS, 88
   disabling for pinholes, 88
ips-rtp, 88
IPv6
   SIP, 77

L
   limiting
      number of SIP dialogs, 85
location server
   SIP, 14

M
   malformed-request-line, 80
   max-body-length, 82
   max-dialogs, 85
   message
      SIP, 17
   message length
      SIP, 82
   message request-line
      SIP, 22
   message start line
      SIP, 22
   message status-line
      SIP, 22

N
   NAT
      SDP, 67
      SIP ALG IP address conservation, 65
      SIP ALG NAT tracing, 65
      SIP contact headers, 66
      SIP session helper NAT tracing, 66
         with IP address conservation, 65
   nat-trace, 66
   no-sdp-fixup, 67

P
   pinhole
      disabling IPS, 88
      more secure, 70
      RTP, 12, 17
      SIP, 12, 17
      smaller, 70
      strict-register, 70
   port number
      changing the port numbers that the SIP ALG listens on, 37
   PRACK
      SIP message, 21
   preserve-override, 66
   product registration, 164
   profile
      VoIP, 36
   provisional
      SIP response message, 21
   provisional response acknowledgement
      SIP message, 21
   provisional-invite-expiry-time, 40
   proxy server
      SIP, 13

R
   rate limit
      number of SIP dialogs, 85
   rate limiting
      SCCP, 84
      SIMPLE, 84
      SIP, 84
   Real Time Control Protocol, 41
   Real Time Protocol, 51
   redirect server
      SIP, 14
   registering
      with Fortinet Technical Support, 164
   registrar
      SIP, 14
   request
      SIP, 11
   request messages, 19
   Request-line
      deep SIP message checking, 80
   request-line
      SIP, 22
   response
      SIP, 11
   RFC
      1918, 161
      SIP, 12
   RFC 2543, 88
   RTCP, 12, 41
   RTP, 12, 51, 63
      hardware acceleration, 19
      pinhole, 12, 17

S
   SCCP
      DoS sensor, 84
      protection profile, 84
      rate limiting, 84
      VoIP profile, 35
   SDP, 12, 19, 25
   NAT, 67
   session profile, 25
   session description protocol
      See SDP, 25
   session failover
      SIP, 86
   session helper
      changing the port numbers that the SIP session helper
         listens on, 30
      disabling the SIP session helper, 29
      enabling the SIP session helper, 29
Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
See SIMPLE, 35
Session Initiation Protocol. See SIP
session profile
SDP, 26
SIMPLE
protection profile, 84
rate limiting, 84
VoIP profile, 35
SIP
accepting register response, 46
blocking requests, 82
changing the port numbers that the SIP ALG listens on, 37
changing the port numbers that the SIP session helper listens on, 30
contact headers and NAT, 66
deep header inspection, 78
deep message inspection, 78
destination NAT, 63
dialog, 11, 17
different source and destination NAT for SIP and RTP, 65
disabling the SIP session helper, 29
DoS sensor, 84
enabling the SIP session helper, 29
fields, 22
fuzzing protection, 78
HA session failover, 86
headers, 22
inspection without address translation, 15, 35
IP address conservation, 65
IPv6, 77
location server, 14
message request-line, 22
message sequence, 17
message start line, 22
message status-line, 22
NAT tracing, 65, 66
NAT with dynamic IP pool, 64
NAT with IP address conservation, 65
pinhole, 12, 17
protection profile, 84
proxy server, 13
rate limiting, 84
redirect server, 14
registrar, 14
request, 11
request-line
SIP, 22
response, 11
RFCs, 12
source NAT, 63
start line
SIP, 22
status-line
SIP, 22
Transparent mode, 15, 35
user element, 11
VoIP profile, 36
SIP ALG
changing the port numbers that the SIP ALG listens on, 37
NAT tracing, 65
SIP dialogs
limiting the number, 85
SIP message
body, 12
final, 21
headers, 12
informational, 21
PRACK, 21
provisional, 21
SIP phone
FortiFone, 12
SIP requests, 82
SIP session
inactivity timeout, 39
SIP session helper
changing the port numbers that the SIP session helper listens on, 30
disabling, 29
enabling, 29
NAT tracing, 66
sip-nat-trace, 66
sip-tcp-port, 37
sip-udp-port, 37
Skinny Call Control Protocol
See SCCP, 35
Skinny Call Control Protocol. See SCCP
source NAT
SIP, 63
start line
SIP, 22
stateful SIP tracking, 39
status-line
SIP, 22
strict
VoIP profile, 36
strict-register, 70
T
technical
documentation conventions, 161
support, 164
technical support, 164
timer
provisional invite, 40
trace
SIP ALG NAT tracing, 65
SIP session helper NAT tracing, 66
Training Services, 164
Transparent mode
SIP, 15, 35
U
UA, 11
UAC, 11
UAS, 11
UE
See UA, 11
User Agent, 11
User Agent Client, 11
User Agent Server, 11
user element
See UA, 11
VoIP
profile, 36
VoIP Profile
SCCP, 35
SIMPLE, 35

VoIP profile
default, 36
strict, 36
VoIP support
enabling on the web-based manager, 35