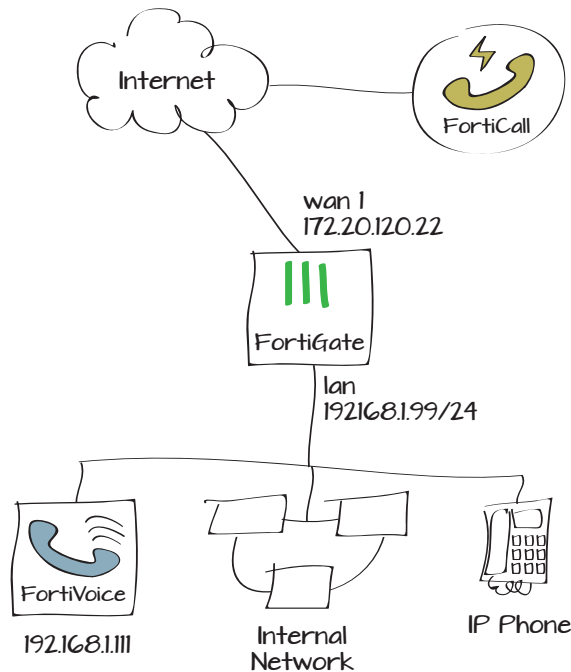


Allowing VoIP calls using FortiVoice and FortiCall

This example sets up inbound and outbound Voice over IP (VoIP) calls using Session Initiation Protocol (SIP) through the FortiGate unit, using a FortiVoice unit and FortiCall services.

1. Setting up a FortiCall account
2. Configuring the FortiVoice unit
3. Configuring the FortiGate unit for outbound SIP calls
4. Configuring the FortiGate unit for inbound SIP calls
5. Results



Setting up a FortiCall account

Go to www.forticall.com and follow the set up instructions. When the account is set up, you will be provided with information to activate your account. You will also need to choose a phone number for inbound calls.

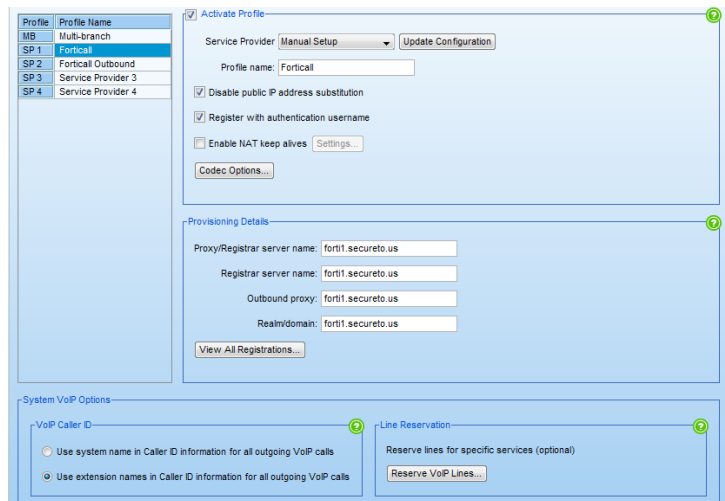
Configuring the FortiVoice unit

Insert the CD into the CD-ROM drive, the FortiVoice Install main window will appear within 20 seconds. Click Install FortiVoice and follow the instructions.



Open the FortiVoice Management software

Go to **Global Settings > VoIP Configuration** and set up a service provider profile for inbound calls.



Profile	Profile Name
MB	Multi-branch
SP 1	Forticall
SP 2	Forticall Outbound
SP 3	Service Provider 3
SP 4	Service Provider 4

Activate Profile

Service Provider: Manual Setup Update Configuration

Profile name:

Disable public IP address substitution

Register with authentication username

Enable NAT keep alives Settings...

Codec Options...

Provisioning Details

Proxy/Registrar server name:

Registrar server name:

Outbound proxy:

Realm/domain:

View All Registrations...

-System VoIP Options-

VoIP Caller ID

Use system name in Caller ID information for all outgoing VoIP calls

Use extension names in Caller ID information for all outgoing VoIP calls

Line Reservation

Reserve lines for specific services (optional)

Reserve VoIP Lines...

Set a service provider for outbound calls.

The screenshot shows the configuration page for an outbound profile. On the left, a table lists profiles: MB (Multi-branch), SP1 (Forticall), SP2 (Forticall Outbound), SP3 (Service Provider 3), and SP4 (Service Provider 4). The 'Forticall Outbound' profile is selected. The main configuration area includes an 'Activate Profile' section with a 'Service Provider' dropdown set to 'Manual Setup' and an 'Update Configuration' button. Below this, the 'Profile name' is 'Forticall Outbound'. There are checkboxes for 'Disable public IP address substitution', 'Register with authentication username', and 'Enable NAT keep alives'. A 'Codec Options...' button is also present. The 'Provisioning Details' section contains fields for 'Proxy/Registrar server name' (forti1.secureto.us), 'Registrar server name', 'Outbound proxy', and 'Realm/domain', with a 'View All Registrations...' button at the bottom.

Go to **Lines and Greetings > VoIP Numbers** and set your phone number for inbound calls.

The screenshot shows the configuration page for an inbound VoIP number. A table on the left lists VoIP numbers: 1 (1-343-8821592), 2 (1-613-8821592), and others. The first number is selected. The 'Activate VoIP Number' section has a 'Select a VoIP Profile' dropdown set to 'Forticall'. The 'Phone Number' section includes fields for 'Country code' (1), 'City or area code' (343), and 'Number' (8821592). The 'Username and Password' section has 'User/Account' (000F4D003EBC) and 'Password' (Password). The 'Registration Status' section shows 'Status: Registered' and a 'View All Registrations...' button. The 'Call Handling' section has 'Mode 1 (Mode 1)' selected, and a note: 'When a call comes in on this phone number, perform the following action: ring extensions'. Below this, it says 'If all extensions are busy or the call is not answered: perform no action after 5 rings'.

Set a phone number for outbound calls.

The screenshot shows the configuration page for an outbound VoIP number. A table on the left lists VoIP numbers: 1 (1-343-8821592), 2 (1-613-8821592), and others. The second number is selected. The 'Activate VoIP Number' section has a 'Select a VoIP Profile' dropdown set to 'Forticall Outbound'. The 'Phone Number' section includes fields for 'Country code' (1), 'City or area code' (613), and 'Number' (8821592). The 'Username and Password' section has 'User/Account' and 'Password' fields. The 'Registration Status' section shows 'Status: Unregistered' and a 'View All Registrations...' button. The 'Call Handling' section has 'Mode 1 (Mode 1)' selected, and a note: 'When a call comes in on this phone number, perform the following action: go to voicemail'. Below this, it says '111'.

Configuring the FortiGate unit for outbound SIP calls

Go to **Security Profiles > VoIP > Profiles**.

Create a new profile and set the **Limit REGISTER request** and **Limit INVITE request**.

Name	<input type="text" value="SIP"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
SIP	
Limit REGISTER request	<input type="text" value="10"/> (requests/sec/policy)
Limit INVITE request	<input type="text" value="10"/> (requests/sec/policy)
SCCP	
Limit Call Setup	<input type="text" value="0"/> (Calls/min/client)

Go to **Firewall Objects > Address > Address**

Create an IP range for SIP phones.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="Internal-SIP-Phones"/>
Color	[Change]
Type	<input type="text" value="IP Range"/>
Subnet / IP Range	<input type="text" value="192.168.1.110-192.168.1.150"/>
Interface	<input type="text" value="lan"/>
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Go to **Policy > Policy > Policy**.

Create a policy allowing outbound SIP traffic. Set **Incoming Interface** to LAN, **Source Address** to the new firewall address, and **Outgoing Interface** to your Internet-facing interface.

Under **Security Profiles**, enable **VoIP** and set it to use the new profile.

Make sure you place this security policy on the top of the policy list.

Policy Type: Firewall VPN

Policy Subtype: Address User Identity Device Identity

Incoming Interface: lan

Source Address: Internal-SIP-Phones

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: SIP

Action: ACCEPT

Enable NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

Log Allowed Traffic

Security Profiles

AntiVirus default

Web Filter default

Application Control default

IPS default

Email Filter default

DLP Sensor default

VoIP SIP

ICAP default

SSL/SSH Inspection default

Seq.#	ID	Source	Destination	Schedule
lan - wan1 (1 - 2)				
1	2	Internal-SIP-Phones	all	always
2	1	all	all	always

Configuring the FortiGate unit for inbound SIP calls

Go to **Firewall Objects > Virtual IPs > Virtual IPs**

Create a new virtual IP mapping the external IP on the **wan1** interface of the FortiGate to the internal IP of the FortiVoice on UDP port 5060.

Go to **Policy > Policy > Policy**.

Create a policy allowing inbound SIP traffic. Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to LAN, and **Destination Address** to the new virtual IP.

Enable **VoIP** and set it to use the new profile.

Name	Inbound_SIP	
Comments	Write a comment... 0/255	
Color	[Change]	
External Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter	(e.g.: x.x.x.x, x.x.x.x-y.y.y.y, x.x	
External IP Address/Range	172.20.120.22	172.20.120.22
Mapped IP Address/Range	192.168.1.111	192.168.1.111
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	5060	5060
Map to Port	5060	5060

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	wan1
Source Address	all
Outgoing Interface	lan
Destination Address	Inbound_SIP
Schedule	always
Service	SIP
Action	ACCEPT
<input type="checkbox"/> Enable NAT	
<input checked="" type="checkbox"/> Log Allowed Traffic	

Security Profiles	
<input type="radio"/> AntiVirus	default
<input type="radio"/> Web Filter	default
<input type="radio"/> Application Control	default
<input type="radio"/> IPS	default
<input type="radio"/> Email Filter	default
<input type="radio"/> DLP Sensor	default
<input checked="" type="radio"/> VoIP	SIP
<input type="radio"/> ICAP	default
<input type="radio"/> SSL/SSH Inspection	default

Results

Go to **System > Dashboard > Status** and add the **VoIP Usage** widget.

When the widget appears, verify **Voice Calls**.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify that both inbound and outbound SIP traffic is occurring.

Select an entry for details.

	SIP	SCCP
Voice Calls		
Currently Active Calls	0	0
Total Calls (since last reset)	5	0
Calls Failed/Dropped/Unanswered	0	0
Calls Succeeded	5	0

▼ Dst	▼ Sent / Received	▼ Policy ID	▼
172.20.120.22	574 B / 787 B	3	SIP
66.11.10.43	14.79 KB / 20.84 KB	2	SIP
172.20.120.22	44.65 KB / 34.70 KB	3	SIP
172.20.120.22	40.69 KB / 31.42 KB	3	SIP
66.11.10.43	110.16 KB / 107.42 KB	3	SIP
172.20.120.22	2.20 KB / 1.70 KB	3	SIP
66.11.10.43	15.10 KB / 19.15 KB	2	SIP
66.11.10.43	205.27 KB / 201.37 KB	2	SIP
172.20.120.22	4.64 KB / 3.97 KB	3	SIP
172.20.120.22	6.29 KB / 5.34 KB	3	SIP
66.11.10.43	215.43 KB / 215.04 KB	3	SIP
66.11.10.43	1.37 MB / 1.77 MB	2	SIP

Dst	172.20.120.22	Virtual Domain	root
Received	787	Source Country	United States
Sent / Received	574 B / 787 B	Dst NAT Port	5060
Duration	29	Sent	574
Application Details		Service	SIP
Protocol	17	Destination Country	Reserved
Dst Port	5060	roll	65530
Status	✓	Timestamp	Wed Jan 30 11:52:03 2013
Tran Display	dnat	Sequence Number	11819
Policy ID	3	Src Interface	wan1
Src	66.11.10.43	Dst NAT IP	192.168.1.111
Sent Packets	1	Level	notice █
Src Port	5060	logid	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	11:52:03 (Wed Jan 30 11:52:03 2013)
Dst Interface	lan		