



**FortiGate Support for SIP  
FortiOS v3.0 MR7**



[www.fortinet.com](http://www.fortinet.com)

*FortiGate Support for SIP Technical Note*

FortiOS v3.0 MR7

9 September 2008

01-30007-0232-20080909

© Copyright 2008 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

**Trademarks**

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# FortiGate Support for Session Initiation Protocol

The Session Initiation Protocol (SIP) is used for establishing and conducting multi-user calls over TCP/IP networks using any media. Due to the complexity of the call setup, not every firewall can handle SIP calls correctly, even if the firewall is stateful. The FortiGate Antivirus Firewall includes special module that tracks SIP calls. The FortiGate unit can make all necessary adjustments, to both the firewall state and call data, to ensure a seamless call is established through the FortiGate unit regardless of its operation mode, NAT, route, or transparent.



**Note:** One call cannot traverse the firewall more than 3 times (inclusive).

The FortiGate unit allows you to control the SIP protocol through protection profiles.

A statistical summary of the SIP protocol is also available and makes managing SIP use easy.

This technical note describes SIP firewall protection profiles and SIP scenarios supported by FortiGate units. The scenarios are broken down into two groups: direct calls and proxy-routed calls.



**Note:** Signaling and media information are transmitted in separate IP flows, so a media gateway, signaling gateway or media gateway controller (softswitch) are between the terminals. They may be separate physical devices or integrated in any combination. For simplicity, these devices are not shown and described in this document.

## Configuring SIP settings in a firewall protection profile

In the Firewall Protection Profiles, you are able to control two functions within the SIP protocol: logging and rate limiting. Logging allows you to enable tracking of information available in the Statistics section.

Rate limiting for the SIP protocol allows you to control how much bandwidth is being used.

### SIP logging

You can log SIP events.

#### To enable VoIP logs

- 1 Go to **Firewall > Protection Profile**.
- 2 Select create New to create a new protection profile called SIP\_protection.
- 3 Select the blue arrow to expand the Logging options.
- 4 Select Log VoIP Activity.

- 5 Select OK.

## SIP rate limiting

You can configure VoIP rate limiting for Session Initiated Protocol (SIP) and Skinny Client Control Protocol (SCCP). SIP and SCCP are two types of VoIP protocols. Rate limiting is generally different between SCCP and SIP. For SIP, rate limiting is for that SIP traffic flowing through the FortiGate unit. For SCCP, the call setup rate is between the FortiGate unit and the clients because the call manager normally resides on the opposite side of the FortiGate unit from the clients.

Since most SIP servers do not have integrated controls, rate limiting is useful to protect a SIP server from being flooded.

### To configure SIP rate limiting

- 1 Go to **Firewall > Protection Profile**.
- 2 Select create New to create a new protection profile called SIP\_protection.
- 3 Select the blue arrow to expand the VoIP options.
- 4 Select the SIP checkbox.
- 5 Enter a number for requests per second in the Limit REGISTER request (requests/sec) field.
- 6 Enter a number for requests per second in the Limit INVITE request (requests/sec) field
- 7 Select OK.

## SIP Statistics

You can view the SIP statistics to gain insight into how the protocol is being used within the network. Overview statistics are provided for all supported VoIP protocols.



**Note:** If virtual domains are enabled on the FortiGate Support for SIP unit, IM, P2P and VoIP features are configured globally. To access these features, select **Global Configuration** on the main menu.

### Viewing overview statistics

The **IM, P2P&VoIP > Statistics > Summary** page provides a summary of statistics for all VoIP protocols.

**Figure 1: SIP statistics summary**

VoIP Usage	SIP	SCCP
<b>Sessions</b>		
Active Sessions (phones connected, etc)	0	0
<b>Voice Calls</b>		
Total Calls (since last reset)	0	0
Calls Failed/Dropped	0	0
Calls Succeeded	0	0

#### VoIP Usage

For SIP and SCCP protocol.

Active Sessions  
(phones connected)

Number of sessions that are currently active.

Total calls (since last reset)	Total VoIP calls since the last FortiGate unit reset.
Calls failed/Dropped	Number of VoIP sessions that failed during the reporting period.
Calls Succeeded	Number of VoIP sessions that were successfully completed during the reporting session.

## Direct SIP calls

Direct SIP traffic passes from terminal to terminal through a FortiGate unit. Policies are created on the FortiGate unit to allow SIP traffic to pass through in either direction. NAT may or may not be applied.

A single firewall policy is required for a terminal on the internal network to initiate connections with terminals on the external network. When a terminal initiates a call, two-way communication is allowed because rules are automatically created based on data found in the call setup messages.

### Scenario 1: FortiGate unit in Transparent mode

Figure 2: FortiGate unit in Transparent mode



The FortiGate unit is operating in Transparent mode. NAT is not available or required in Transparent mode because all FortiGate interfaces are on the same network.

The following firewall policies are required:

- internal -> external to allow Terminal A to initiate connections with Terminal B. Set service to SIP.
- external -> internal to allow Terminal B to initiate connections with Terminal A. Set service to SIP.

### Scenario 2: FortiGate unit in NAT/Route mode, NAT not enabled

Figure 3: FortiGate unit in NAT/Route mode



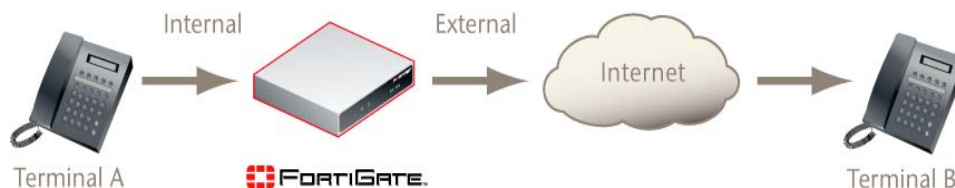
The FortiGate unit is operating in NAT/Route mode without NAT being enabled.

The following policies are required:

- internal -> external to allow Terminal A to initiate connections with Terminal B. Set service to SIP.
- external -> internal to allow Terminal B to initiate connections with Terminal A. Set service to SIP.

### Scenario 3: FortiGate unit in NAT/Route mode, NAT enabled and virtual IP required

Figure 4: FortiGate unit in NAT/Route mode



The FortiGate unit is operating in NAT/route mode with NAT enabled. For Terminal A to be able to call Terminal B, you require the following:

- an internal -> external policy to allow Terminal A to initiate connections with Terminal B. Enable NAT. Set service to SIP.

For Terminal B to be able to call Terminal A, you require the following:

- a virtual IP on the internal interface
- an external -> internal policy to allow Terminal B to initiate connections with Terminal A. Set the destination address to the virtual IP address. Set service to SIP.

## Proxy server calls

The proxy server provides the following services:

- name translation
- user location
- authorization and authentication
- call setup
- call routing
- call management

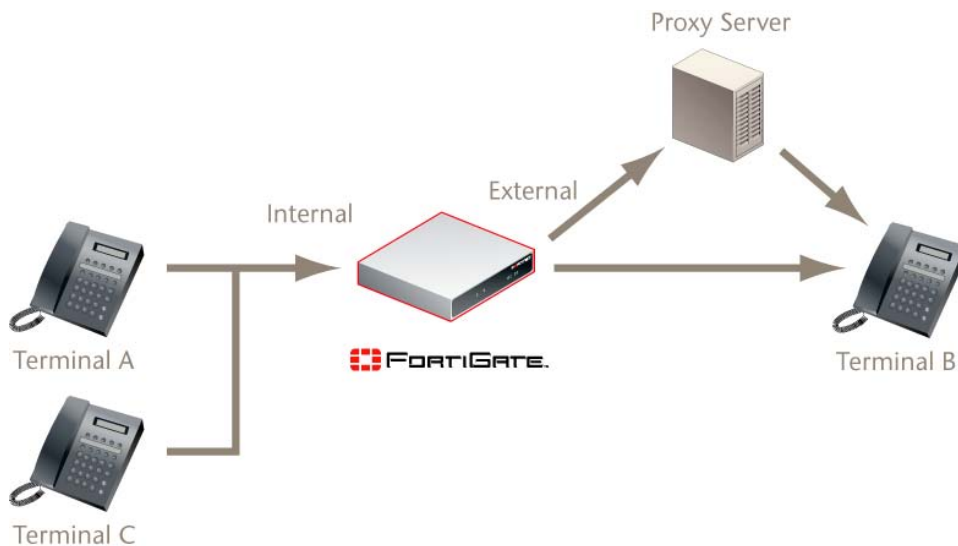
The proxy server may be located on the terminal network or outside of the terminal network. It may include a multipoint control unit (MCU) to provide conferencing between three or more terminals.

With proxy server-routed calls, a terminal registers with the proxy server when it is powered up. When the terminal places a call, the proxy server contacts the destination terminal, relays data between the terminals, and completes the call setup. Call setup must be set to routed.

A single firewall policy is required for a terminal on the internal network to initiate connections with the proxy server on the external network. When a terminal initiates a call, two-way communication is allowed because rules are automatically created based on data found in the call setup messages.

## Proxy server scenario 1: FortiGate unit in Transparent mode

Figure 5: FortiGate unit in Transparent mode



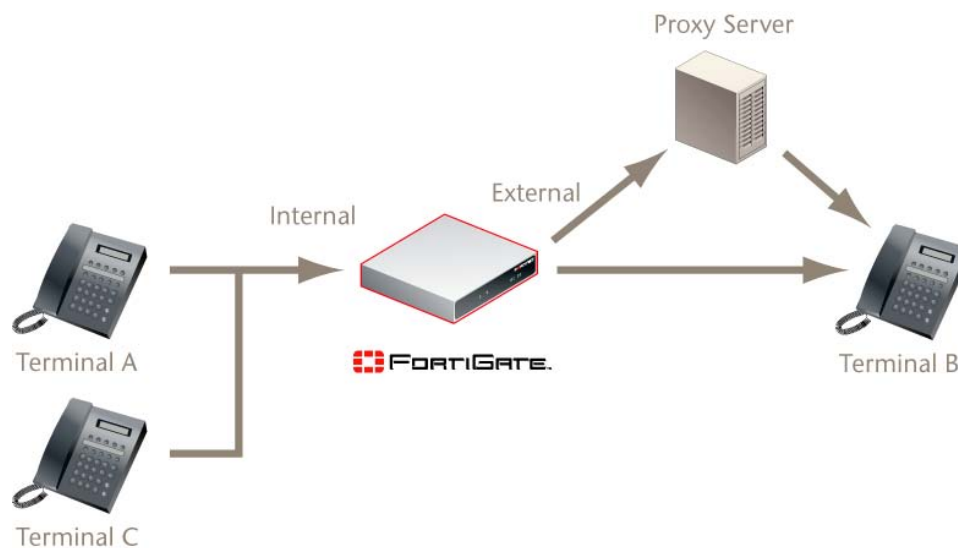
The FortiGate unit is operating in Transparent mode. NAT is not available or required in Transparent mode because all FortiGate interfaces are on the same network.

The following firewall policy is required:

- internal -> external to allow Terminals A and C to connect to the proxy server. Set service to SIP.

## Proxy server scenario 2: FortiGate unit in NAT/Route mode, NAT not enabled

Figure 6: FortiGate unit in NAT/route mode



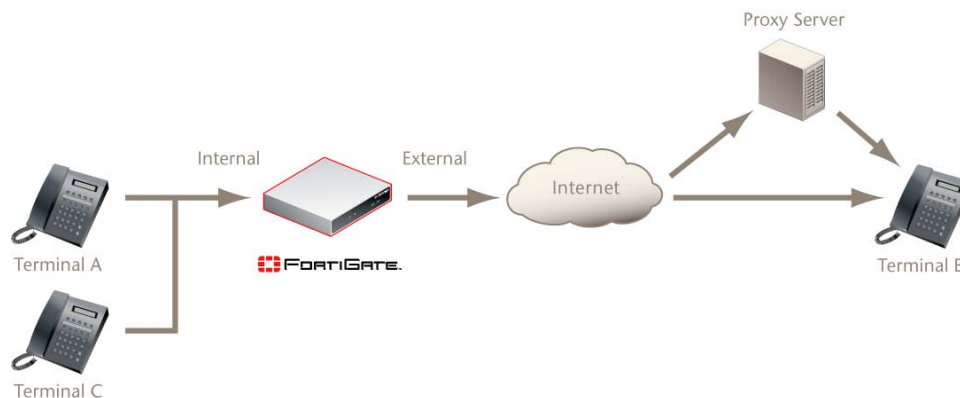
The FortiGate unit is operating in NAT/Route mode with NAT not enabled

The following policy is required:

- internal -> external to allow Terminals A and C to connect to the proxy server.  
Set service to SIP.

### Proxy server scenario 3: FortiGate unit in NAT/Route mode, NAT enabled

Figure 7: Proxy server on the public network



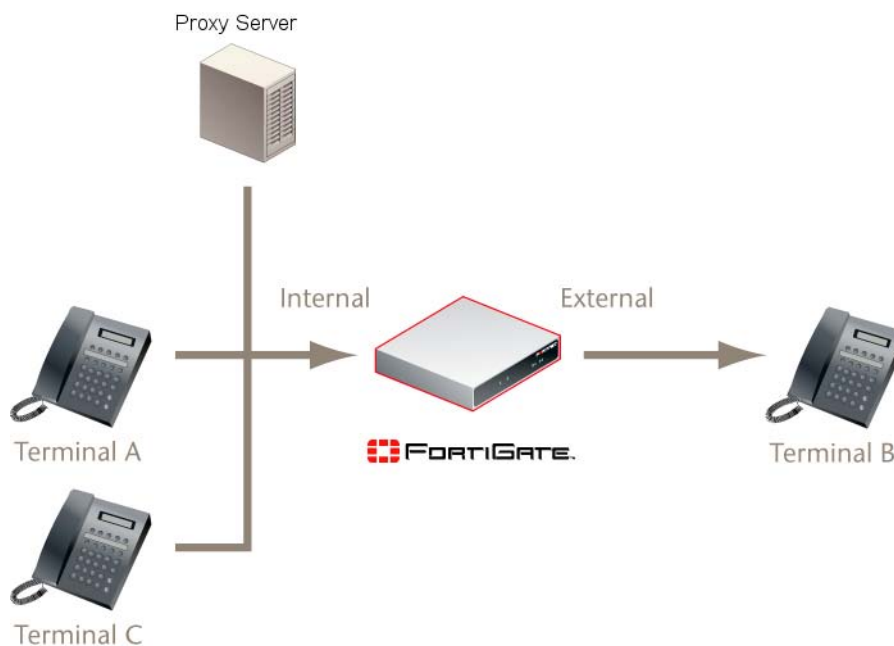
The FortiGate unit is operating in NAT/Route mode with NAT enabled.

The following policy is required:

- internal -> external to allow Terminals A and C to connect to the proxy server.  
Set service to SIP.

### Proxy server scenario 4: FortiGate unit in NAT/Route mode, NAT enabled and virtual IP required

Figure 8: Proxy server on the private network



The FortiGate unit is operating in NAT/Route mode with NAT enabled.

The following policy is required:

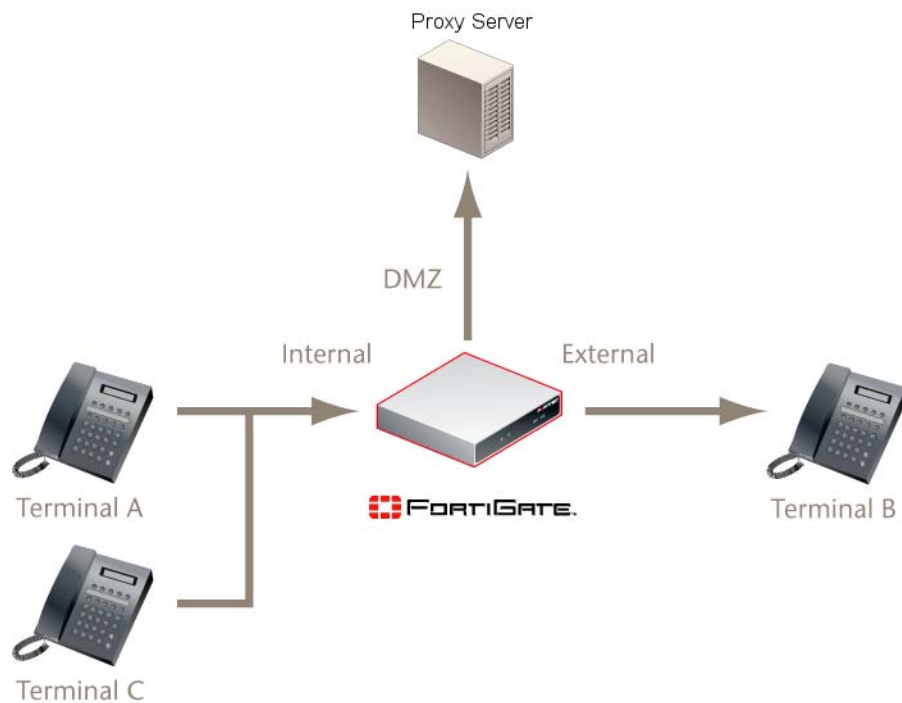
- Terminal A to proxy server. Set service to SIP.

For Terminal B to be able to register with the proxy server, you require the following:

- a virtual IP for the proxy server on the external interface
- an external -> internal policy to allow Terminal B to initiate connections with the proxy server. Set the destination address to the virtual IP address. Set service to SIP.

### Proxy server scenario 5: FortiGate unit in NAT/Route mode, NAT enabled

Figure 9: Proxy server on a different network



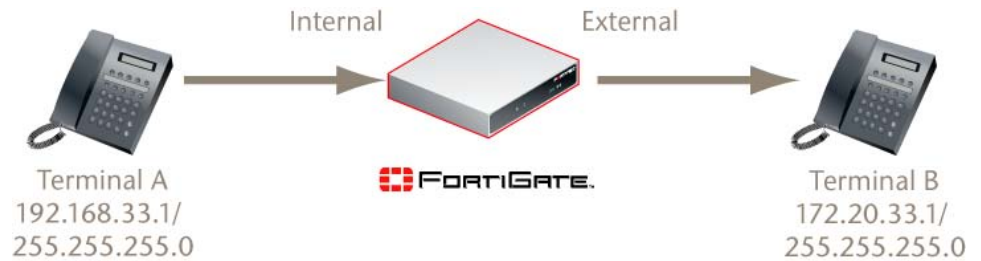
The FortiGate unit is operating in NAT/Route mode with NAT enabled.

The following policies are required:

- internal -> DMZ to allow Terminals A and C to connect to the proxy server. Set service to SIP.
- external -> DMZ to allow Terminal B to connect to the proxy server.

## Example configuration 1: Peer to peer

This example shows how to configure a policy for peer to peer SIP connections. The FortiGate unit is in NAT/Route mode.



This configuration has two basic steps:

- configure addresses for the internal terminal (terminal\_A) and external terminal (terminal\_B)
- configure a firewall policy for SIP traffic between the terminals (internal -> external)

### To add terminal addresses

- 1 Go to **Firewall > Address** and select Create New.
- 2 Configure the address as follows:

<b>Address Name</b>	terminal_A
<b>Type</b>	Subnet / IP Range
<b>Subnet/IP Range</b>	255.255.255.0/192.168.33.1

- 3 Select OK.
- 4 Repeat steps 2 and 3 for terminal\_B:

<b>Address Name</b>	terminal_B
<b>Type</b>	Subnet / IP Range
<b>Subnet/IP Range</b>	255.255.255.0/172.20.33.1

### To add a firewall policy

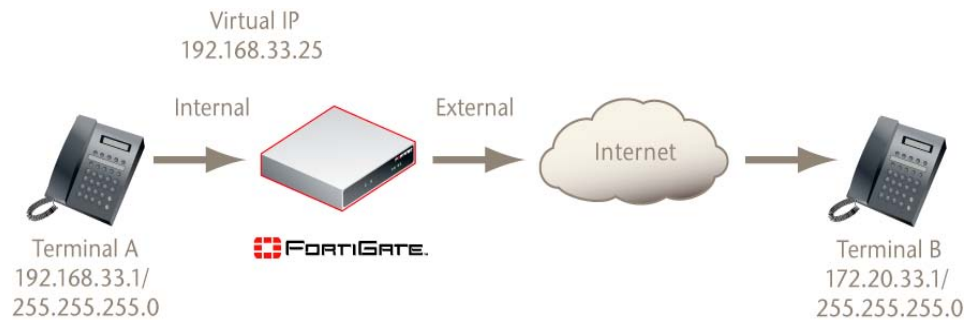
- 1 Go to **Firewall > Policy** and select Create New.
- 2 Configure the policy as follows:

<b>Source Interface/Zone</b>	internal
<b>Source Address</b>	terminal_A
<b>Destination Interface/Zone</b>	external
<b>Destination Address</b>	terminal_B
<b>Schedule</b>	always
<b>Service</b>	SIP
<b>Action</b>	ACCEPT
<b>NAT</b>	enable
<b>Protection Profile</b>	SIP_protection

- 3 Select OK.

## Example Configuration 2: Peer to Peer with a Virtual IP Address

This example shows how to configure a policy for peer to peer SIP connections.



### To add terminal addresses

- 1 Go to **Firewall > Address** and select Create New.
- 2 Configure the address as follows:

<b>Address Name</b>	terminal_A
<b>Type</b>	Subnet / IP Range
<b>Subnet/IP Range</b>	255.255.255.0/192.168.33.1

- 3 Select OK.
- 4 Repeat steps 2 and 3 for terminal\_B:

<b>Address Name</b>	terminal_B
<b>Type</b>	Subnet / IP Range
<b>Subnet/IP Range</b>	255.255.255.0/172.20.33.1

### To add a firewall policy

- 1 Go to **Firewall > Policy** and select Create New.

- 2 Configure the policy as follows:

<b>Source Interface/Zone</b>	internal
<b>Source Address</b>	terminal_A
<b>Destination Interface/Zone</b>	external
<b>Destination Address</b>	terminal_B
<b>Schedule</b>	always
<b>Service</b>	SIP
<b>Action</b>	ACCEPT
<b>NAT</b>	enable
<b>Protection Profile</b>	SIP_protection

- 3 Select OK.

#### To configure a virtual IP address

- 1 Go to **Firewall > Virtual IP** and select Create New.
- 2 Configure the virtual IP address as follows:

<b>Name</b>	terminal_A_vip
<b>External Interface</b>	external
<b>Type</b>	Static NAT
<b>External IP Address/Range</b>	172.20.32.25
<b>Mapped IP Address/Range</b>	192.168.33.1/255.255.255.0

- 3 Select OK.

#### To add an external to internal firewall policy

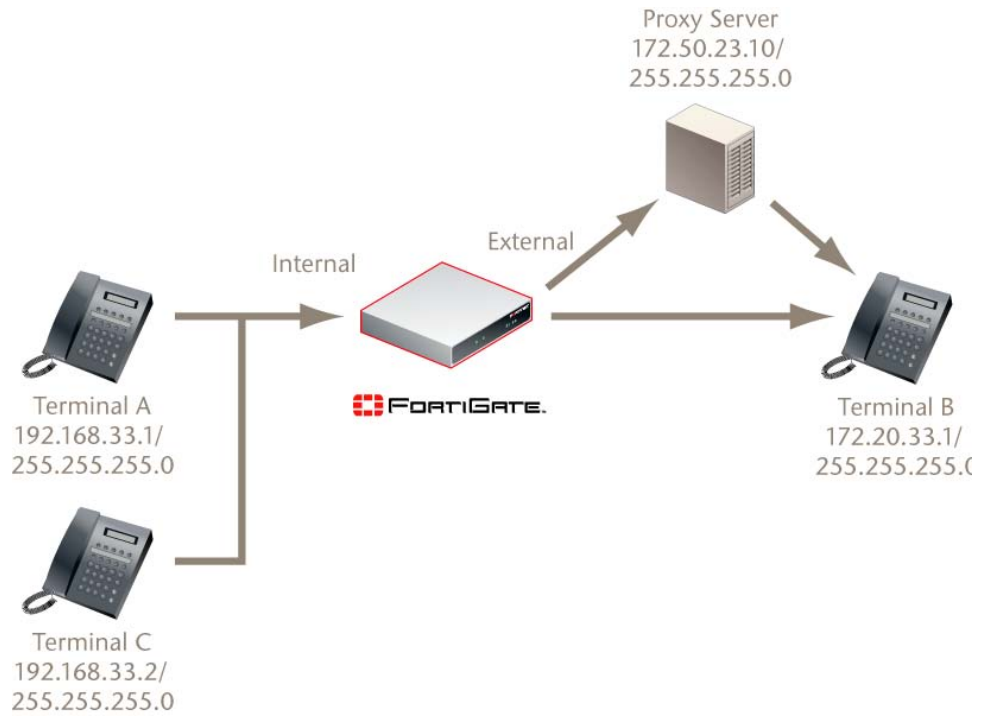
- 1 Go to **Firewall > Policy** and select Create New.
- 2 Configure the policy as follows:

<b>Source Interface/Zone</b>	external
<b>Source Address</b>	terminal_B
<b>Destination Interface/Zone</b>	internal
<b>Destination Address</b>	terminal_A_vip
<b>Schedule</b>	always
<b>Service</b>	SIP
<b>Action</b>	ACCEPT
<b>NAT</b>	enable
<b>Protection Profile</b>	SIP_protection

- 3 Select OK.

## Example configuration 3: Proxy server

This example show how to configure a policy for SIP connections using a proxy server. The FortiGate unit is in NAT/Route mode.



This configuration has three basic steps:

- configure addresses for the internal terminals (terminal\_A and terminal\_C) and external terminal (terminal\_B)
- create groups for the terminals (internal\_terminals)
- configure a firewall policy for SIP traffic between the terminals and the proxy server (internal -> external)

### To add terminal addresses

- 1 Go to **Firewall > Address** and select Create New.
- 2 Configure the address as follows:

<b>Address Name</b>	terminal_A
<b>Type</b>	Subnet / IP Range
<b>Subnet/IP Range</b>	255.255.255.0/192.168.33.1

- 3 Select OK.

- 4 Repeat steps 2 and 3 for terminal\_C and the proxy server:

<b>Address Name</b>	terminal_C
<b>Type</b>	Subnet/IP Range
<b>Subnet/IP Range</b>	255.255.255.0/192.168.33.2
<b>Address Name</b>	sip_proxy_server
<b>Type</b>	Subnet/IP Range
<b>Subnet/IP Range</b>	255.255.255.0/172.50.23.10

#### To add address groups

- 1 Go to **Firewall > Address > Group** and select Create New.
- 2 Enter the Group Name: internal\_terminals.
- 3 Using the right arrow, move terminal\_A and terminal\_C from the Available Addresses list to the Members list.
- 4 Select OK.

#### To add a firewall policy

- 1 Go to **Firewall > Policy** and select Create New.
- 2 Configure the policy as follows:

<b>Source Interface/Zone</b>	internal
<b>Source Address</b>	internal_terminals
<b>Destination Interface/Zone</b>	external
<b>Destination Address</b>	sip_proxy_server
<b>Schedule</b>	always
<b>Service</b>	SIP
<b>Action</b>	ACCEPT
<b>NAT</b>	enable
<b>Protection Profile</b>	SIP_protection

- 3 Select OK.