



**FortiGate Support for H.323
FortiOS v3.0 MR7**



www.fortinet.com

FortiGate H.323 Technical Note
FortiOS v3.0 MR7
9 September, 2008
01-30007-0178-20080909

© 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 H.323

The H.323 suite of protocols is used for establishing and conducting multi-media calls over TCP/IP networks. Due to the complexity of the call setup, not every firewall can handle H.323 calls correctly, even if the firewall is stateful. The FortiGate Antivirus Firewall includes special module that tracks H323 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.

This technical note describes H.323 scenarios supported by FortiGate units. The scenarios are broken down into two groups: direct calls and gatekeeper-routed calls.

Direct H.323 Calls

Direct H.323 traffic passes from terminal to terminal through a FortiGate unit. Policies are created on the FortiGate unit to allow H.323 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. A virtual IP address may be required if traffic is coming from an external public network to the internal private network.

Scenario 1: FortiGate unit in Transparent mode

Figure 1: 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 H.323.
- external -> internal to allow Terminal B to initiate connections with Terminal A. Set service to H.323.

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

Figure 2: FortiGate unit in NAT/Route mode



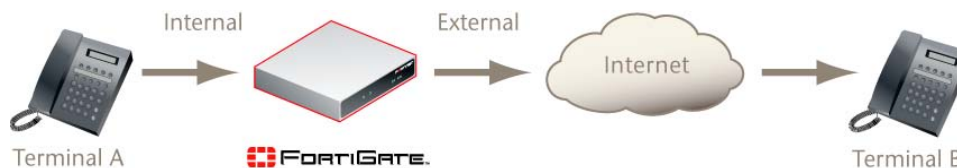
The FortiGate unit is operating in NAT/Route mode without NAT being enabled.

The following policies are required:

- internal -> external to allow Terminal A to initiate connections with Terminal B. Set service to H.323.
- external -> internal to allow Terminal B to initiate connections with Terminal A. Set service to H.323.

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

Figure 3: 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 H.323

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 H.323.

Gatekeeper-routed Calls

A gatekeeper is an optional component that acts as a call manager. Services provided by gatekeepers include

- translation of alias addresses for terminals and gateways to transport addresses
- bandwidth management
- authorization and authentication
- call signalling
- call routing

- call management

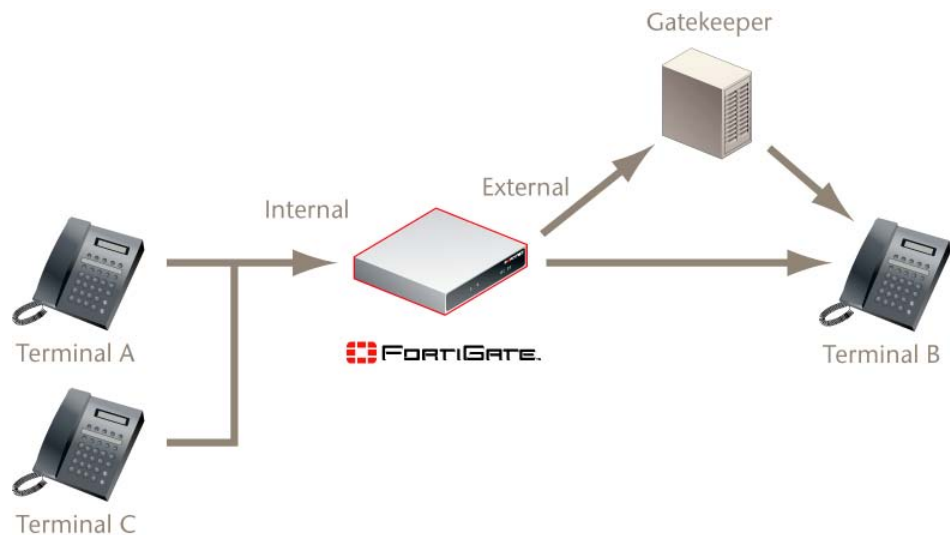
A gatekeeper may be located on the terminal network or outside of the terminal network. A gatekeeper may include a multipoint control unit (MCU) to provide conferencing between three or more terminals.

With gatekeeper-routed calls, a terminal registers with the gatekeeper when it is powered up. When the terminal places a call, the gatekeeper contacts the destination terminal and relays data between the terminals. The terminals complete call setup.

A single firewall policy is required for a terminal on the internal network to initiate connections with the gatekeeper 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.

Gatekeeper scenario 1: FortiGate unit in Transparent mode

Figure 4: FortiGate unit in Transparent mode



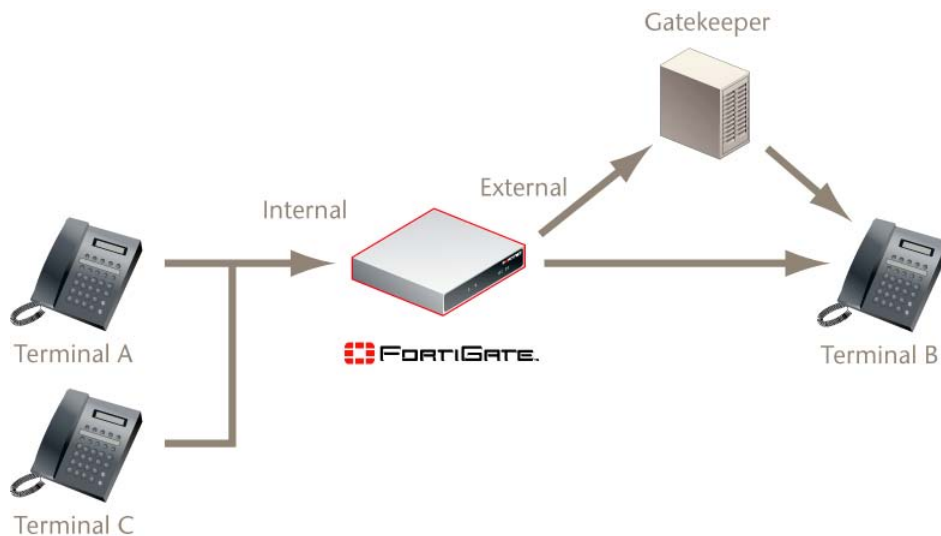
The FortiGate unit is operating in Transparent mode. NAT is not available or required in Transparent mode because all FortiGate interfaces are on the same network.

The following firewall policy is required:

- internal -> external to allow Terminals A and C to connect to the gatekeeper. Set service to H.323.

Gatekeeper scenario 2: FortiGate unit in NAT/Route mode, NAT not enabled

Figure 5: FortiGate unit in NAT/route mode



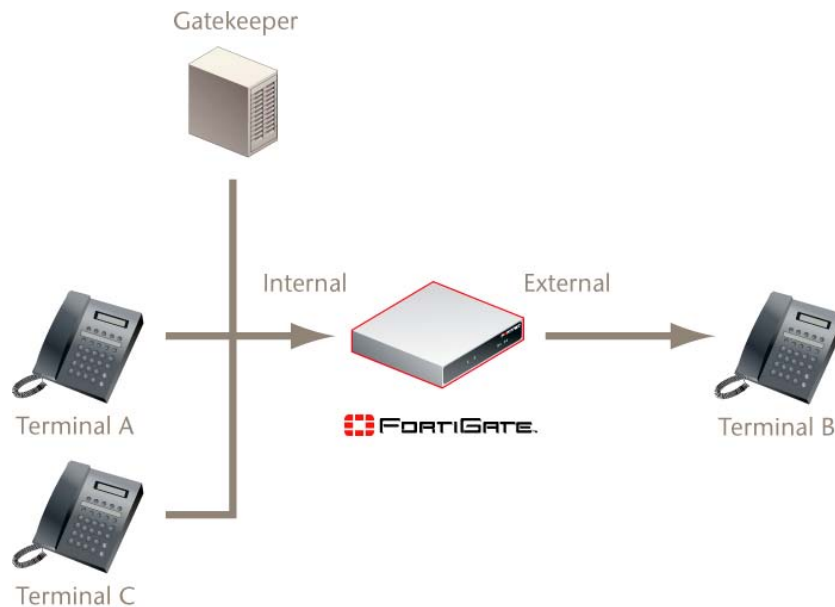
The FortiGate unit is operating in NAT/Route mode with NAT not enabled

The following policy is required:

- internal -> external to allow Terminals A and C to connect to the gatekeeper. Set service to H.323.

Gatekeeper scenario 3: FortiGate unit in NAT/Route mode, NAT enabled and virtual IP required

Figure 6: Gatekeeper on the private network



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

The following policy is required:

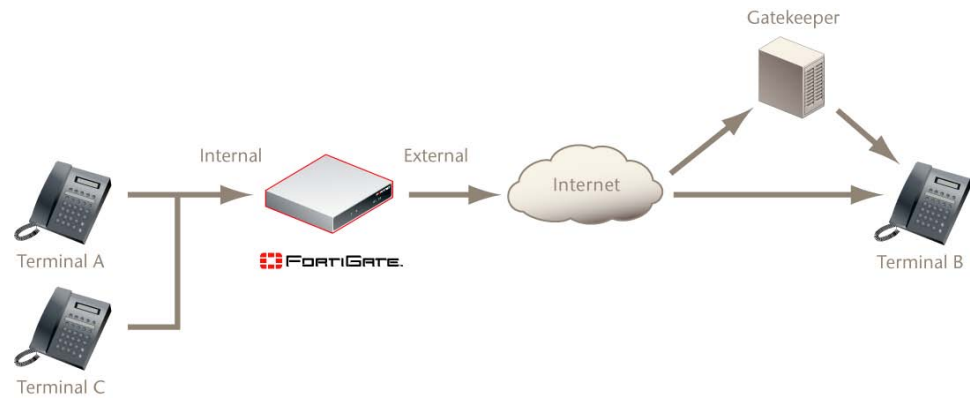
- Terminal A to Gatekeeper. Set service to H.323.

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

- a virtual IP for the gatekeeper on the external interface
- an external -> internal policy to allow Terminal B to initiate connections with the gatekeeper. Set the destination address to the virtual IP address. Set service to H.323.

Gatekeeper scenario 4: FortiGate unit in NAT/Route mode, NAT enabled

Figure 7: Gatekeeper on the public network



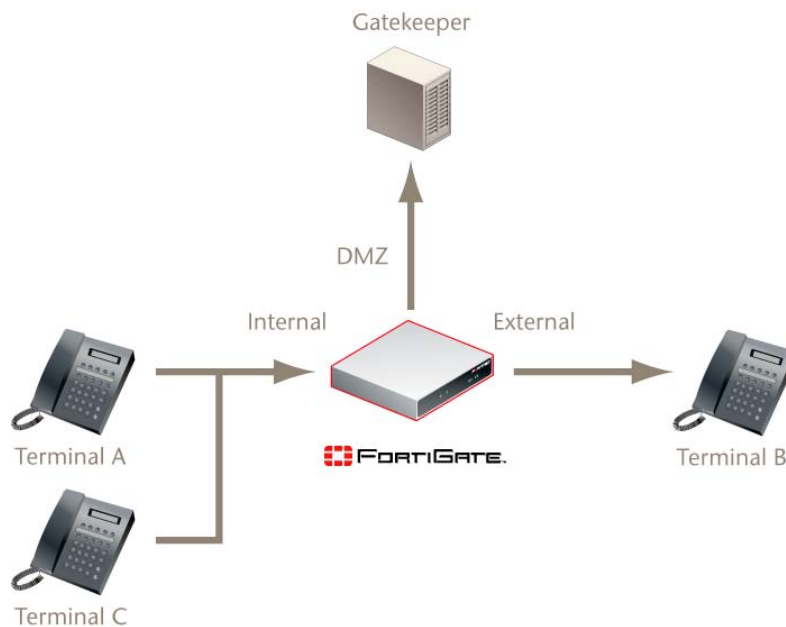
The FortiGate unit is operating in NAT/Route mode with NAT enabled.

The following policy is required:

- internal -> external to allow Terminals A and C to connect to the gatekeeper. Set service to H.323.

Gatekeeper scenario 5: FortiGate unit in NAT/Route mode, NAT enabled

Figure 8: Gatekeeper on a different network



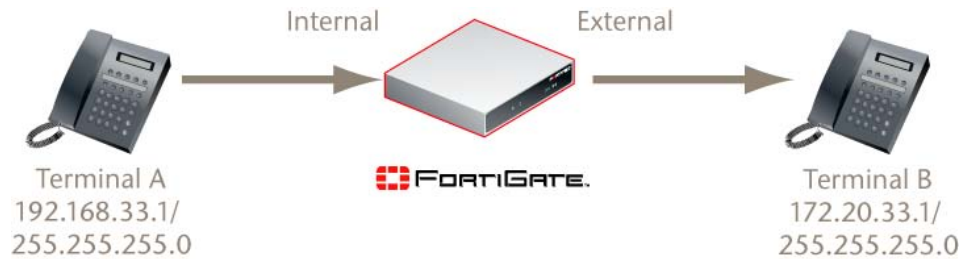
The FortiGate unit is operating in NAT/Route mode with NAT enabled.

The following policies are required:

- internal -> DMZ to allow Terminals A and C to connect to the gatekeeper. Set service to H.323.
- external -> DMZ to allow Terminal B to connect to the gatekeeper.

Example Configuration 1: Peer to Peer

This example shows how to configure a policy for peer to peer H.323 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 H.323 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:

Address Name	terminal_A
Type	Subnet / IP Range
Subnet/IP Range	255.255.255.0/192.168.33.1

- 3 Select OK.
- 4 Repeat steps 2 and 3 for terminal_B:

Address Name	terminal_B
Type	Subnet / IP Range
Subnet/IP Range	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:

Source Interface/Zone	internal
Source Address	terminal_A
Destination Interface/Zone	external
Destination Address	terminal_B
Schedule	always
Service	H.323
Action	ACCEPT
NAT	enable

- 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 H.323 connections.



To add terminal addresses

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

Address Name	terminal_A
Type	Subnet / IP Range
Subnet/IP Range	255.255.255.0/192.168.33.1

- 3 Select OK.
- 4 Repeat steps 2 and 3 for terminal_B:

Address Name	terminal_B
Type	Subnet / IP Range
Subnet/IP Range	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:

Source Interface/Zone	internal
Source Address	terminal_A
Destination Interface/Zone	external
Destination Address	terminal_B
Schedule	always
Service	H.323
Action	ACCEPT
NAT	enable

- 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:

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

- 3 Select OK.

To add an external to internal firewall policy

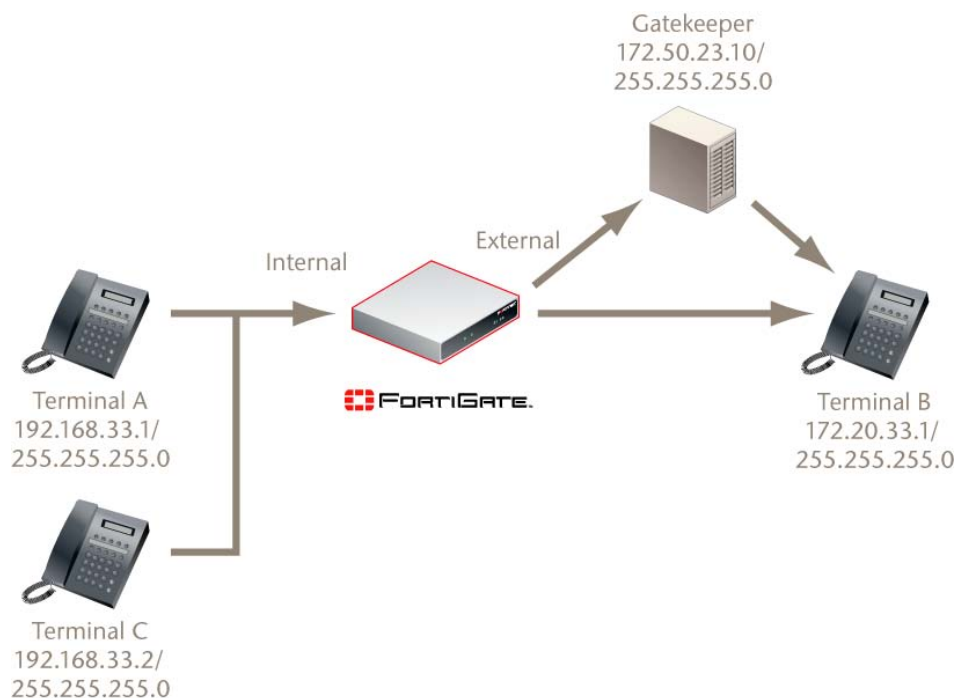
- 1 Go to **Firewall > Policy** and select Create New.
- 2 Configure the policy as follows:

Source Interface/Zone	external
Source Address	terminal_B
Destination Interface/Zone	internal
Destination Address	terminal_A_vip
Schedule	always
Service	H.323
Action	ACCEPT
NAT	enable

- 3 Select OK.

Example Configuration 3: Gatekeeper

This example shows how to configure a policy for H.323 connections using a gatekeeper. 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 H.323 traffic between the terminals and the gatekeeper (internal -> external)

To add terminal addresses

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

Address Name	terminal_A
Type	Subnet / IP Range
Subnet/IP Range	255.255.255.0/192.168.33.1

- 3 Select OK.

- 4 Repeat steps 2 and 3 for terminal_C and the gatekeeper:

Address Name	terminal_C
Type	Subnet / IP Range
Subnet/IP Range	255.255.255.0/192.168.33.2
Address Name	gatekeeper
Type	Subnet / IP Range
Subnet/IP Range	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:.

Source Interface/Zone	internal
Source Address	internal_terminals
Destination Interface/Zone	external
Destination Address	gatekeeper
Schedule	always
Service	H.323
Action	ACCEPT
NAT	enable

- 3 Select OK.

