



# FortiVoice™ 200D/200D-T and FortiGate Network Security Platform Interoperability

Technical Note



FortiVoice 200D/200D-T and FortiGate Network Security Platform Interoperability Technical Note  
August 24, 2013

1st Edition

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	<a href="http://docs.fortinet.com">docs.fortinet.com</a>
Knowledge Base	<a href="http://kb.fortinet.com">kb.fortinet.com</a>
Customer Service & Support	<a href="http://support.fortinet.com">support.fortinet.com</a>
Training Services	<a href="http://training.fortinet.com">training.fortinet.com</a>
FortiGuard	<a href="http://fortiguard.com">fortiguard.com</a>
Document Feedback	<a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a>

In many cases, FortiVoice customers have external extensions that need to register and make/receive phone calls from the Internet. Those external extensions usually are behind a third-party NAT device, like DSL router, firewall, etc.

This technical note describes the configuration of FortiVoice 200D/200D-T with FortiOS v5.0 b228. The configuration with other FortiOS versions should be similar.

This technical note assumes that you use the FortiVoice 200D/200D-T 2.2.0 software. Use this note in conjunction with the *FortiVoice 200D/200D-T Administration Guide*.

## Scenario

This technical note uses the following scenario to illustrate the interoperability between the FortiVoice 200D/200D-T and the FortiGate unit.

FortiVoice 200D/200D-T has SIP trunks from service providers on the Internet and needs to register with those service providers to send outgoing calls and receive incoming calls. The FortiGate unit has a lot of VoIP-related security features. Fortinet strongly recommends to deploy the FortiVoice 200D/200D-T behind the FortiGate unit. The FortiVoice 200D/200D-T will be configured with a private IP that is mapped to a public one on the FortiGate unit. All incoming and outgoing calls will go through the FortiGate unit for security policy enforcement and intrusion detection.

The address plan is as following:

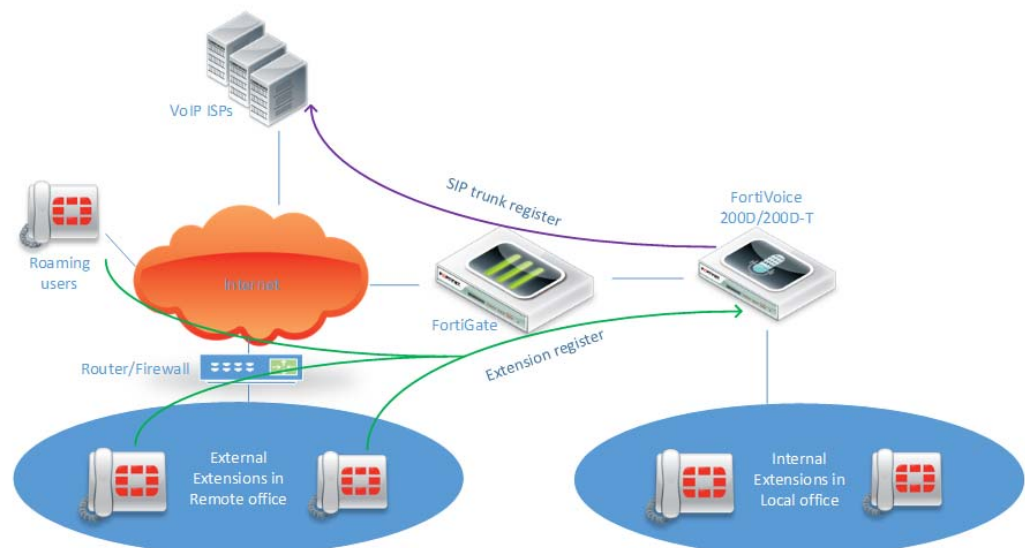
FortiVoice 200D:

- Private IP: 100.10.190.234
- Public IP: 10.15.120.121

VoIP ISPs:

- FortiCall: 66.11.10.43
- ISP1: 10.23.110.253
- ISP2: sipproxy.isp2.net
- ISP3: voip.isp3.com

**Figure 1:** Network diagram



## Configuration procedure

1. On the FortiGate unit, configure the VIP for the FortiVoice 200D that will be used by external extensions.

The screenshot shows the 'Add New Virtual IP Mapping' configuration window. The left sidebar is under 'Firewall Objects' > 'Virtual IP'. The main configuration area includes:

- Name: vip\_10.15.120.121\_to\_190.234\_SIP
- Comments: Write a comment... (0/255)
- Color: [Change]
- External Interface: port10
- Type: Static NAT
- Source Address Filter:
- External IP Address/Range: 10.15.120.121 - 10.15.120.121
- Mapped IP Address/Range: 100.10.190.234 - 100.10.190.234
- Port Forwarding:
- Protocol:  TCP  UDP  SCTP
- External Service Port: 5060 - 5060
- Map to Port: 5060 - 5060

Buttons: OK, Cancel

2. Configure addresses for VoIP service providers and then add them into an address group.

The screenshot shows the 'New Address' configuration window. The left sidebar is under 'Firewall Objects' > 'Addresses'. The main configuration area includes:

- Category:  Address  IPv6 Address  Multicast Address
- Name: FortiCall
- Color: [Change]
- Type: Subnet
- Subnet / IP Range: 66.11.10.43
- Interface: port10
- Show in Address List:
- Comments: Write a comment... (0/255)

Buttons: OK, Cancel

The screenshot shows the 'New Address Group' configuration window. The left sidebar is under 'Firewall Objects' > 'Groups'. The main configuration area includes:

- Group Name: SIP-ISP
- Comments: SIP service provider servers (28/255)
- Color: [Change]
- Show in Address List:
- Members: FortiCall, ISP1, ISP2, ISP3
- Applied tags: Add tag (+)

Buttons: OK, Cancel

3. Configure the VoIP protection profile for incoming policy on CLI. Hosted NAT traversal needs to be enabled because external extensions usually are behind a NAT device.

```
config voip profile
  edit "ysun"
    set comment "created by Yong"
    config sip
      set hosted-nat-traversal enable
      set hnt-restrict-source-ip enable
    end
  next
end
```

SIP uses port 5060 by default. If a non-standard port is used, configure it in system settings so that the FortiGate SIP ALG can work properly.

```
config system settings
  set sip-helper disable
  set sip-nat-trace disable
  set sip-tcp-port 5060
  set sip-udp-port 5060
end
```

4. Configure the VoIP protection profile for outgoing policy on CLI. Note that hosted NAT traversal is disabled. Strict register is enabled so that only incoming calls from those service providers are allowed by the register pinholes.

```
config voip profile
  edit "ysun-out"
    set comment "created by Yong"
    config sip
      set strict-register enable
    end
  next
end
```

- On the CLI or Web UI, configure the incoming policy to allow the SIP messages from the Internet to the FortiVoice unit in the private network and any outgoing phone calls from the FortiVoice unit to the external extensions with associated register pinholes.

```

config firewall policy
  edit 2
    set srcintf "port10"
    set dstintf "port16"
    set srcaddr "all"
    set dstaddr "vip_10.15.120.121_to_190.234_SIP"
    set action accept
    set schedule "always"
    set service "SIP"
    set utm-status enable
    set logtraffic all
    set voip-profile "ysun"
    set profile-protocol-options "default"
    set nat enable
  next
end

```

The screenshot displays the FortiGate Web UI configuration for a Firewall Policy. The left sidebar shows the navigation menu with 'Policy' selected. The main area displays the configuration for Policy 2, including Policy Type (Firewall), Policy Subtype (Address), Incoming Interface (port10), Source Address (all), Outgoing Interface (port16), Destination Address (vip\_10.15.120.121\_to\_190.234\_SIP), Schedule (always), Service (SIP), and Action (ACCEPT). The 'Enable NAT' section is checked, and 'Logging Options' are set to 'Log all Sessions'. Security Profiles for various services are set to 'default'.

- On the CLI or Web UI, configure outgoing policy to allow 200D/200D-T to register with service providers and allow the incoming calls from them with the associated register pinholes.

```

config firewall policy
  edit 5
    set srcintf "port16"
    set dstintf "port10"
    set srcaddr "FVC_200D_254"
    set dstaddr "SIP-ISP"
    set action accept
    set schedule "always"
    set service "SIP"
    set utm-status enable
    set logtraffic all
    set voip-profile "ysun-out"
    set profile-protocol-options "default"
    set nat enable
  next
end

```

The screenshot displays the FortiGate Web UI configuration page for a Firewall Policy. The left sidebar shows the navigation tree with 'Policy' selected. The main area shows the configuration for Policy 5, including source and destination interfaces, addresses, schedule, service, and action.

Field	Value
Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	port16
Source Address	FVC_200D_254
Outgoing Interface	port10
Destination Address	SIP-ISP
Schedule	always
Service	SIP
Action	ACCEPT
Enable NAT	<input type="checkbox"/>
Logging Options	<input type="radio"/> No Log <input type="radio"/> Log Security Events <input checked="" type="radio"/> Log all Sessions
Security Profiles	Antivirus: default Web Filter: default Application Control: default IPS: default Email Filter: default DLP Sensor: default VoIP: default ICAP: default SSL/SSH Inspection: default
Tags	<input type="checkbox"/> Traffic Shaping <input type="checkbox"/> Enable Web cache <input type="checkbox"/> Enable WAN Optimization <input type="checkbox"/> Disclaimer

7. On the CLI, specify which interface is external so that the SIP ALG can work properly.

```
config system interface
  edit "port10"
    set vdom "root"
    set ip 10.15.120.121 255.255.255.192
    set allowaccess ping https ssh snmp
    set type physical
    set external enable
    set alias "WAN64"
    set snmp-index 12
  next
end
```

The configuration on the FortiGate unit is complete.

8. On the FortiVoice unit, test to ensure the SIP trunk on the FortiVoice unit works properly and external extensions can register and communicate with internal extensions without any issues (both signalling and media).

Status	User ID	Number	Display Name	Type	IP	Phone Info
Idle	7831	7831	Yong Sun remote	SIP	172.20.190.249	CSipSimple_d2can-16/r2272

Name	Type	Status	Registration/Connection
FortiCat	SIP peer	Unmonitored	
zhuang_test_sip_trunk	SIP peer	In service	



