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

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

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:

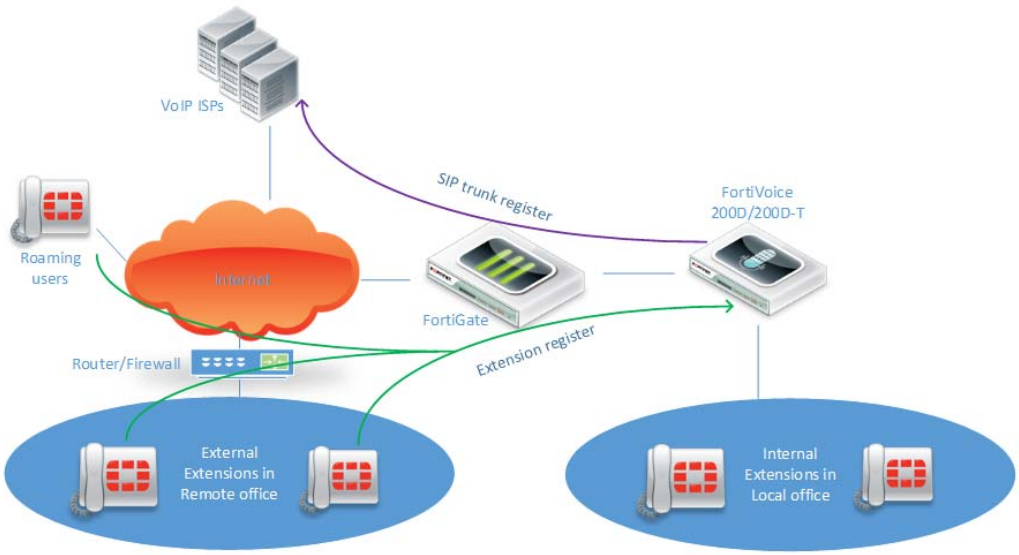
FortiVoice 200D:

- Private IP: 100.10.190.234
- Public IP: 10.15.120.121

VoIP ISPs:

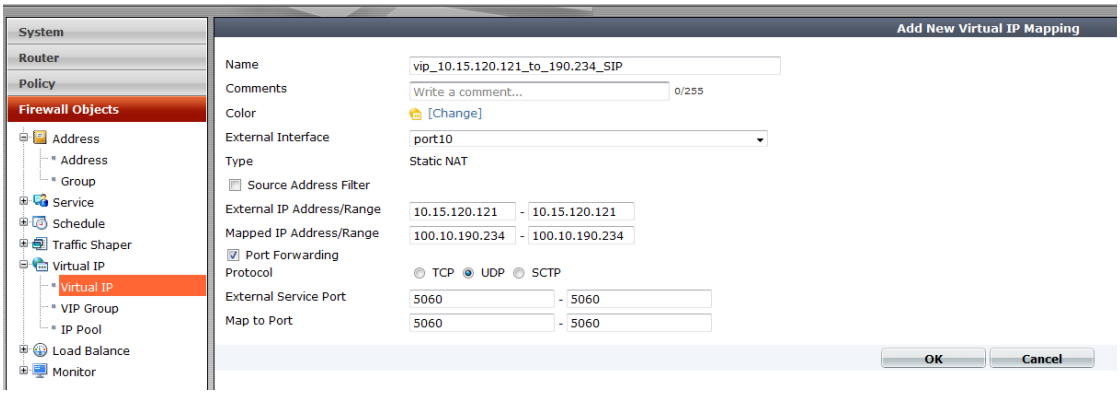
- FortiCall: 66.11.10.43
- ISP1: 10.23.110.253
- ISP2: sipproxy.isp2.net
- ISP3: voip.isp3.com

Figure 1: Network diagram

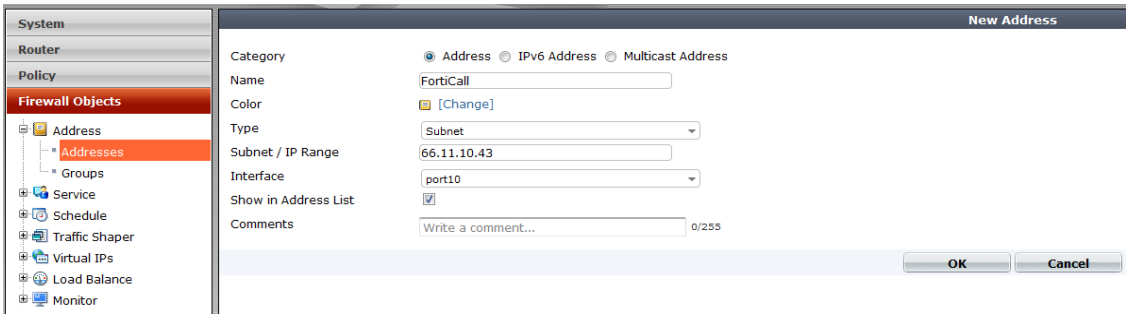


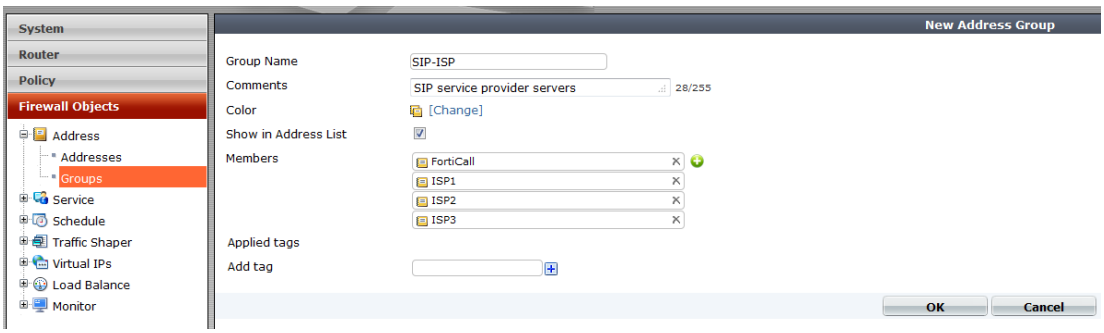
Configuration procedure

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



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





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.

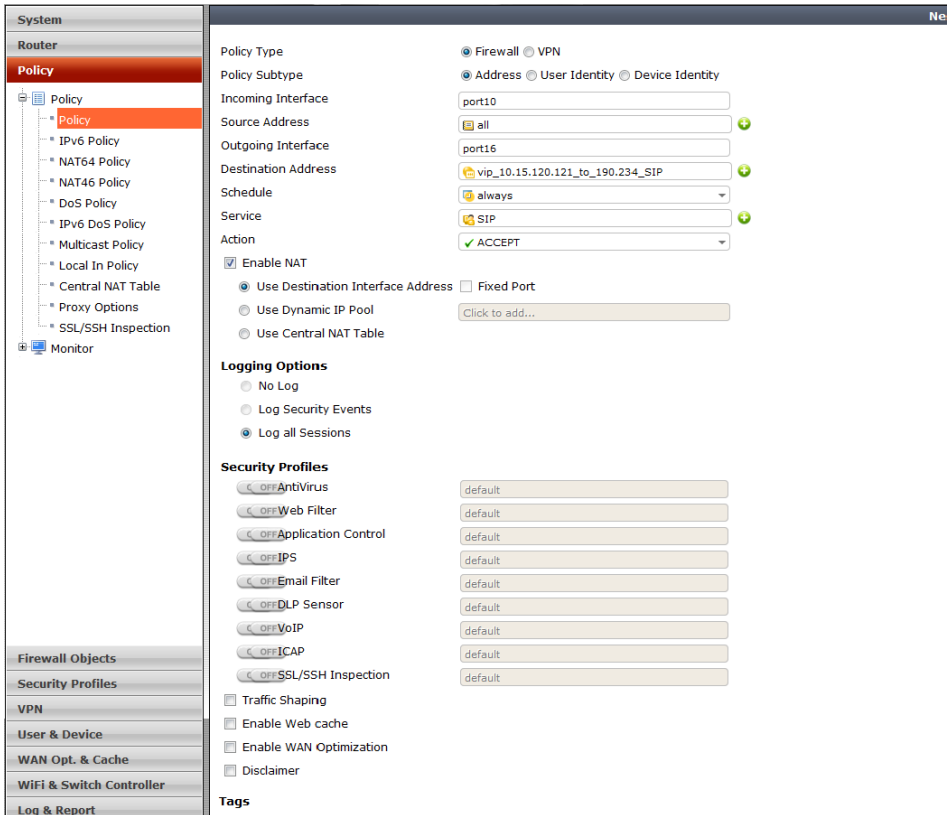
```
config system settings
    set sip-helper disable
    set sip-nat-trace disable
    set sip-tcp-port 5060
    set sip-udp-port 5060
end
```

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
```

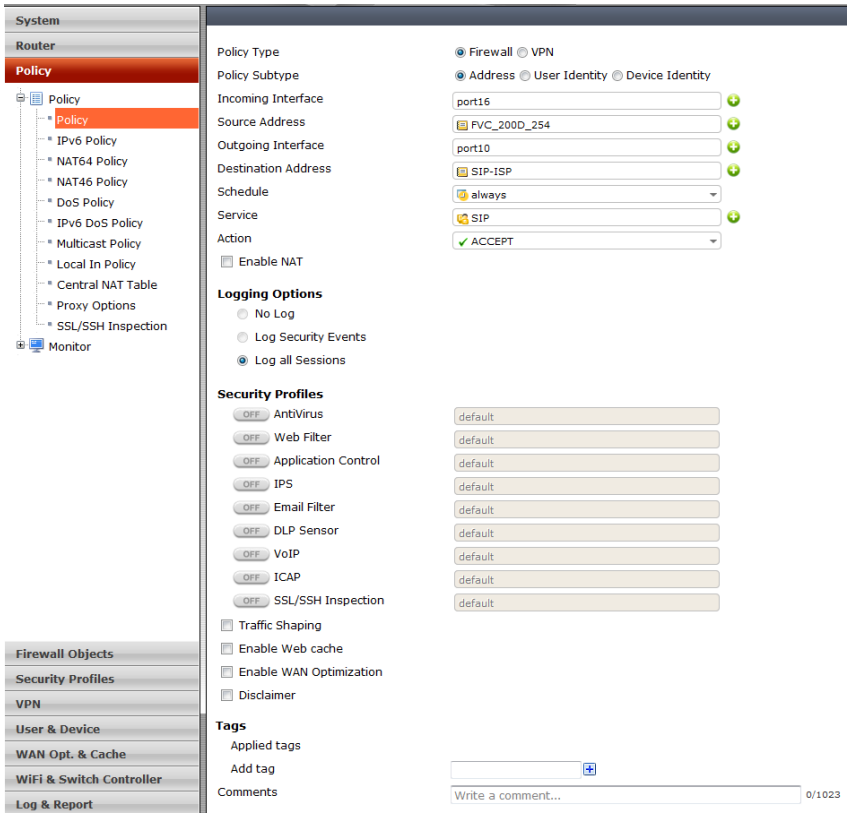
5. On the CLI or Web UI, configure the incoming policy to allow the SIP messages from the Internet to the FortiVoice unit in the private network and any outgoing phone calls from the FortiVoice unit to the external extensions with associated register pinholes.

```
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
```



6. 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
```



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).