Time Sensitive Information!

These Configuration Changes Must Be Applied Ten Days Prior to Absolute VOICE Cut-Over

# Fortinet/FortiGate Router Configuration For Absolute VOICE Cloud Telephony Deployment

Document Version 2.1

June 24th, 2019

# Table of Contents



# *Read Me!*

1. These changes must be applied before client implements their Absolute VOICE hosted telephony solution.
2. If you are experienced with business class firewalls and routers, please have your IT staff/contractor perform these changes for you.
3. Please read this entire document before attempting to make any changes.
4. If you have questions about this document, you can call 800-955-6703 to schedule an appointment with one of our firewall support specialists. We will attempt schedule your appointment within 24- 48 hours of your call to us so please allow adequate time.
5. After changes are completed please let your client or Absolute VOICE Customer Support specialist know.
6. Once completed, an Absolute VOICE technician will be requesting access or a collaborative web session to verify settings prior to customer cut over.

# Introduction

This document is for IT administrators and illustrates configuration changes required on Fortinet firewall & router appliances to support Absolute VOICE's cloud communications telecommunications platform. This document assumes a basic network deployment consisting of one internal LAN network containing the IP phones and one WAN network connected to the Internet. While we strongly recommend a dedicated network for VoIP traffic, the instructions below can be used for a "converged" network whereby both VoIP and non-VoIP traffic share one physical WAN network. With basic modifications (such as adding access rules for additional interfaces); this configuration can be extrapolated for other network layouts. The screenshots below may vary slightly from what is displayed while configuring the device depending on model (30E, 100E, etc…) and FortiOS software version. Setting values not mentioned may be left at default or changed as required for specific purposes.

**Please call Absolute VOICE Customer Support at 800-955-6703 if you need any further information. Firewall changes can be in depth and you will need to schedule time with one of our specialists if you need assistance.**

Screenshots and instructions are based on Fortinet 30E running FortiOS 6.2.

We recommend loading the latest Fortinet OS (firmware).

# Firewall Checklist

*After applying* the configuration commands and GUI configuration in this document, please take the appropriate screen shots to provide the firewall "verification" to Absolute.

Note: You could issue the following CLI command and copy the configuration into a text file:
*show full-configuration*

Or you can take the screen shots of the GUI listed in the below table:

| Screen Shot #: | Configuration: | Completed: |
|---|---|---|
| 1 | CLI showing the commands to disable SIP ALG and RTP | |
| 2 | Policy & Objects → Traffic Shaper → Absolute VOICE shaper | |
| 3 | Policy & Objects → Traffic Shaper Policy → Absolute VOICE shaper policy | |
| 3 | Policy & Objects → IPv4 Policy (showing the Absolute VOICE Outbound Policy Order) | |
| 4 | Policy & Objects → IPv4 Policy→ Absolute VOICE Outbound Policy detail | |
| 5 | Policy & Objects → IPv4 Policy→ Absolute VOICE Inbound Policy detail | |

## Disable SIP ALG

SIP ALG is used to try and avoid configuring Static NAT on a router. Its implementation, however, varies from one router to another, often making it difficult to inter-operate a router with SIP ALG enabled with a PBX. In general, you would want to disable SIP ALG and configure one to one port mapping on the router.

### Open CLI (command line interface – Putty, Teraterm, etc..)

- Open the Fortigate CLI from the dashboard or ssh/telnet client and connect to the IP address of the Fortinet
- Enter the following commands in FortiGate's CLI
  - config system settings
  - set sip-helper disable
  - set sip-nat-trace disable
  - reboot the device

```
FGT30E5618061343 # config system settings
FGT30E5618061343 (settings) # set sip-helper disable
FGT30E5618061343 (settings) # set sip-nat-trace disable
FGT30E5618061343 (settings) #

FGT30E5618061343 (settings) # end
FGT30E5618061343 # execute reboot
```

- Reopen CLI after the system comes on-line and enter the following commands
  - (do not enter the text after //)
  - config system session-helper
  - show //you need to find the entry for SIP, usually 12, but can vary
  - delete 12 //*or the number* that you identified from the previous command

```
FGT30E5618061343 # config system session-help
FGT30E5618061343 (session-helper) # show
    edit 13
        set name sip
        set protocol 17
        set port 5060
    next
FGT30E5618061343 (session-helper) # delete 13
```

- Disable RTP processing as follows:
  - config voip profile
  - edit default
  - config sip
  - set rtp disable

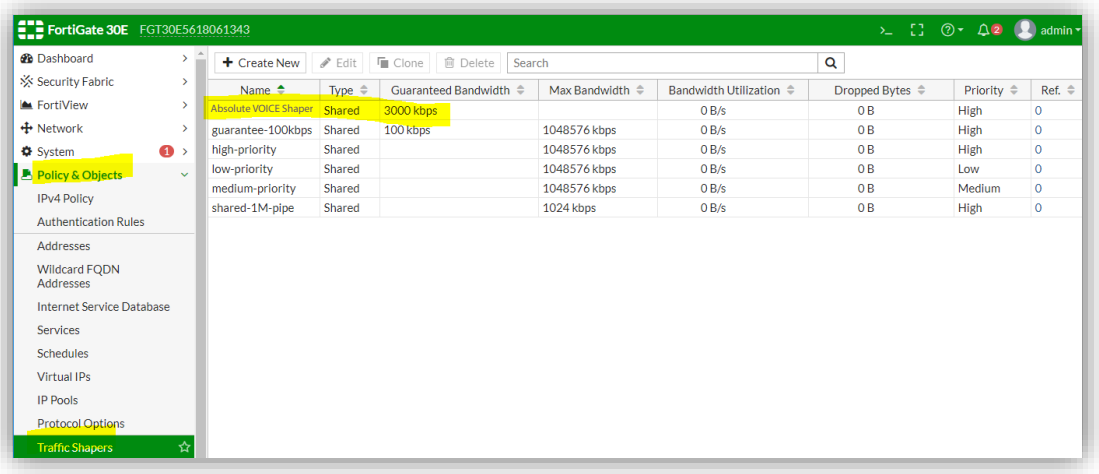
```
FGT30E5618061343 # config voip profile
FGT30E5618061343 (profile) # edit default
FGT30E5618061343 (default) # config sip
FGT30E5618061343 (sip) # set rtp disable
FGT30E5618061343 (sip) # end
FGT30E5618061343 (default) # end
```

# Create Traffic Shaper & Priority

The Traffic Shaper will allow a defined set of traffic to a particular priority (QoS) level and guarantee/shape need bandwidth with the VoIP traffic.

## Policy & Objects → Traffic Shapers

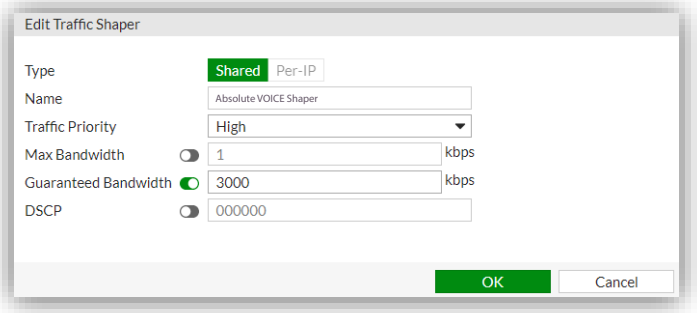
Create a "new" traffic shaper policy for the voice traffic:




- Click the "Create New" button and enter the following:

| | |
|---|---|
| Enter name of shaper: | Absolute VOICE Shaper |
| Traffic Priority: | High |
| Guaranteed Bandwidth: | Enter the amount of bandwidth (kbps – i.e. 1mbps = 1000kbps) you would like to reserve for voice traffic.<br>(number of phones * approx. 100K) |
| Note: | Do not enter a "Max" bandwidth limit |

- Click "Ok"



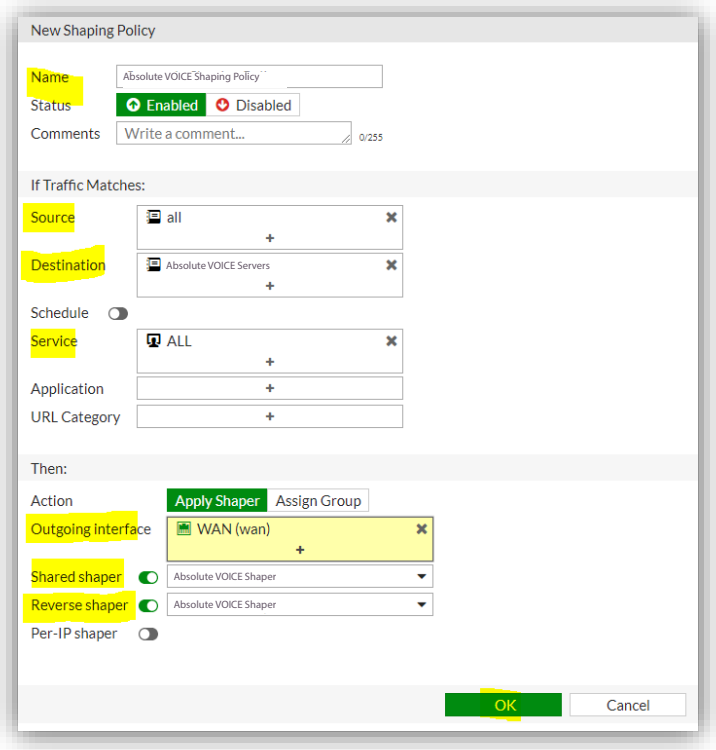
# Create Traffic Shaping Policy

## Policy & Objects → Traffic Shaping Policy

Create new shaping policy.

- Click “Create New” button
- Enter the following information and click “OK”:

| | |
|---|---|
| Name: | Absolute VOICE Shaping Policy |
| Source: | All |
| Destination: | Absolute VOICE Servers<br>Note: you can create a new address object with subnet – 184.178.213.0/24 |
| Service: | All |
| Outgoing Interface: | WAN |
| Shared Shaper: | Enable and choose “Absolute VOICE Shaper” |
| Reverse Shaper: | Enabled and choose “Absolute VOICE Shaper” |



# Create Absolute VOICE IPv4 Policy Rules

## Policy & Objects → IPv4 Policy

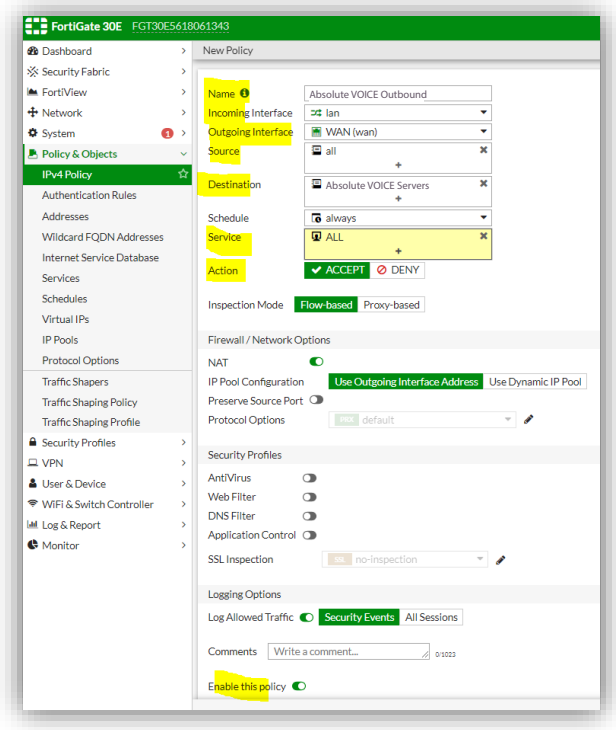
Create an Outbound and Inbound rule that allows all traffic to/from Absolute VOICE (184.178.213.0/24) to "All" or "Trusted networks"/"LAN."

Outbound:

- Click the "Create New" button
- Enter the following fields:

| | |
|---|---|
| Name: | Absolute VOICE Outbound |
| Incoming Interface: | LAN |
| Outgoing Interface: | WAN |
| Source: | All |
| Destination: | Absolute VOICE Servers (address object created in previous steps - |
| Service: | 184.178.213.0/24) |

  - Please make sure the rule is set to "Accept" (Action) and "Enabled"
- Click "OK"




- Please re-organize LAN to WAN rules so Absolute VOICE Outbound rule is at the top (highest priority) in the list:

# Document Revision History

| Version | Reason for Change | Date |
|---|---|---|
| **1.0 Draft** | Initial Draft Document | June 27, 2012 |
| | | |
| **1.1** | Check list added | March 17, 2017 |
| **2.1** | Fortinet 30E device with updated FortiOS 6.2 | June 24, 2019 |