AbsoluteVOICE

Find Your Voice in the cloud

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 1.1

March 17th, 2017

www.callabsolute.com

Table of Contents

1. Introduction
2. Firewall Verification Checklist
3. Disable SIP ALG
4. Create Traffic Shaper & Priority
5. Create ACL's for Inbound and Outbound

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 (60D, 100D, 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 60 D running FortiOS 5.2.3.

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 VOICE.

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 → Objects → Traffic Shaper → Absolute VOICE shaper	
3	Policy & Objects → IPv4 (showing the Absolute VOICE Outbound Policy)	
4	Policy & Objects → IPv4 → Absolute VOICE Outbound 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)

- Open the Fortigate CLI from the dashboard
- Enter the following commands in FortiGate's CLI
  - config system settings
  - set sip-helper disable
  - set sip-nat-trace disable
  - reboot the device

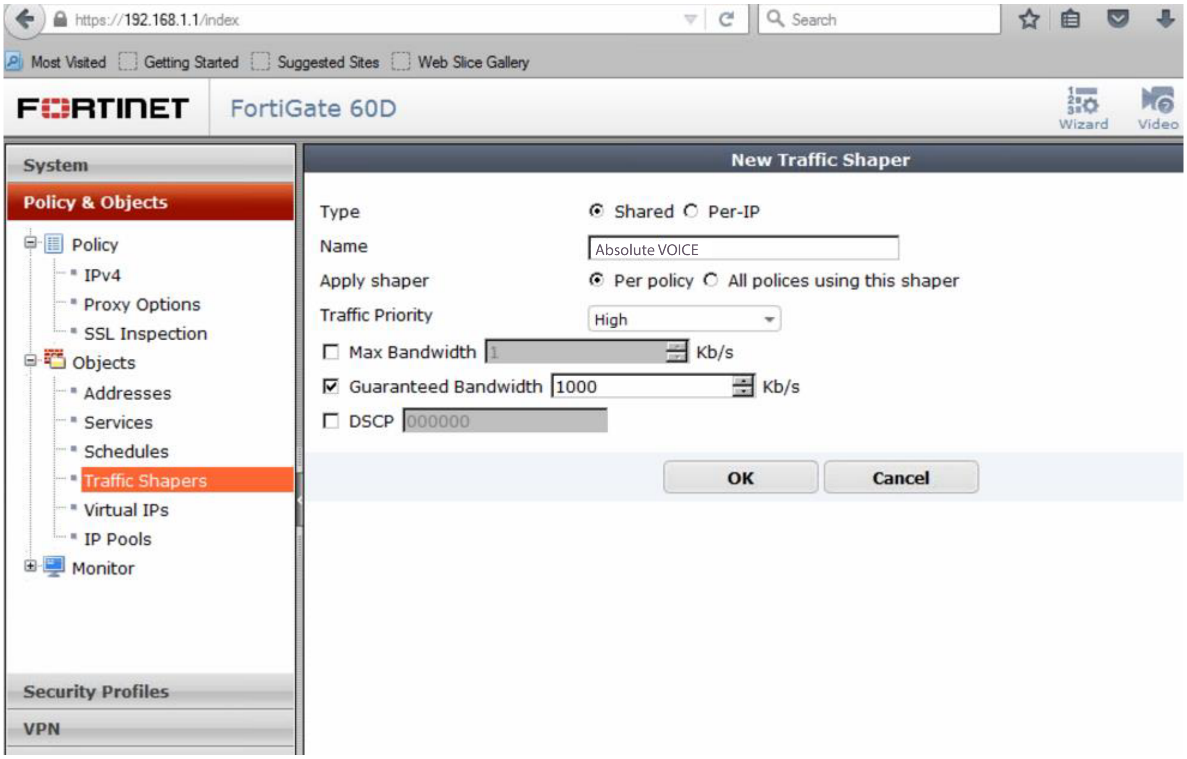
- Reopen CLI and enter the following commands (do not enter the text after //)
  - config system session-helper
  - show   //you need to find the entry for SIP, usually 12, but can vary
  - delete 12   //or the number that you identified from the previous command

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

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 → Objects → Traffic Shapers



New Traffic Shaper

Type	● Shared ○ Per-IP
Name	Absolute VOICE
Apply shaper	● Per policy ○ All polices using this shaper
Traffic Priority	High
□ Max Bandwidth	1 Kb/s
☑ Guaranteed Bandwidth	1000 Kb/s
□ DSCP	000000

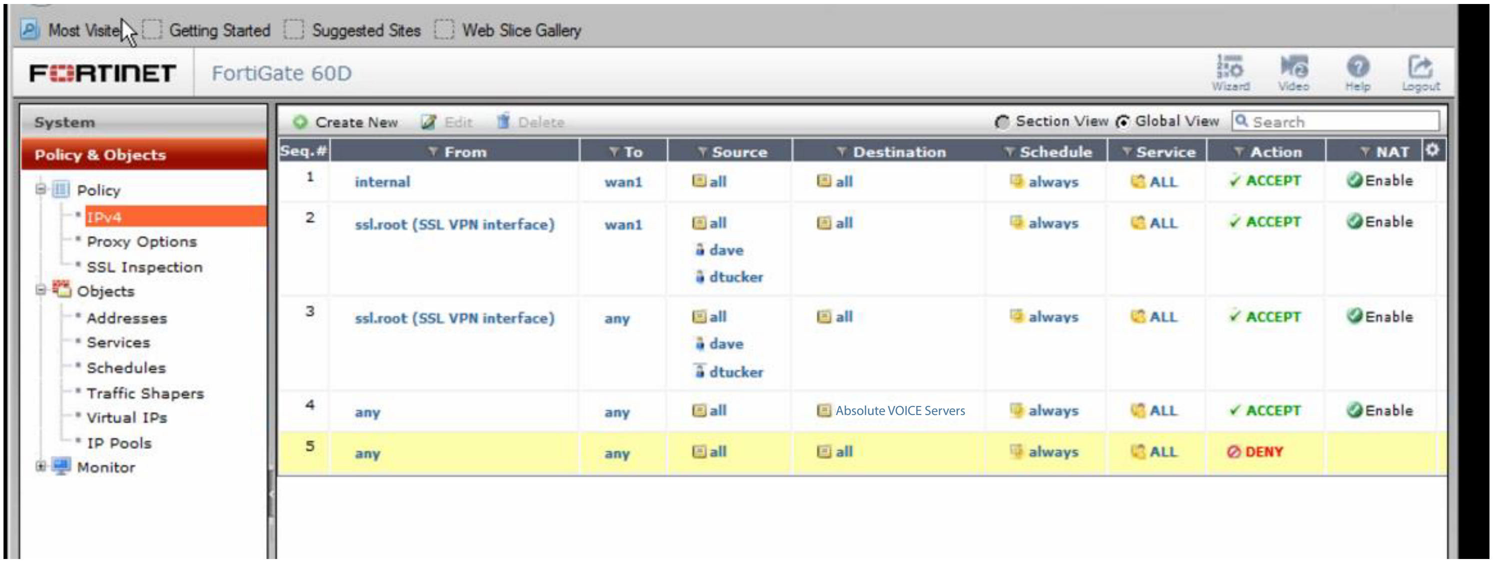
- Click New
  - Type: Shared (radio button)
  - Name: Absolute VOICE
  - Apply Shaper: Per Policy (radio button)
  - Traffic Priority: High (drop down box)
  - Check Guaranteed Bandwith
    - Enter the minimum amount of bandwidth you would like to reserve for VoIP traffic.
    - Typically we calculate by the following formula: 100Kbps x 30% of phones per site
      - I.E. 100Kbps x 10phones= 1000Kbps
  - Hit “OK” to save

Create Absolute VOICE ACL/Policy Rule

Policy & Objects → IPv4

The following example shows the “Outbound” rule to allow and apply traffic shaper/priority to the Absolute VOICE VoIP traffic.

Please create an alternate “Inbound” rule that allows all traffic from Absolute VOICE (184.178.213.0/24) to “All” or “Trusted networks”/”LAN.”



Seq.#	From	To	Source	Destination	Schedule	Service	Action	NAT
1	internal	wan1	all	all	always	ALL	✓ ACCEPT	Enable
2	ssl.root (SSL VPN interface)	wan1	all dave dtucker	all	always	ALL	✓ ACCEPT	Enable
3	ssl.root (SSL VPN interface)	any	all dave dtucker	all	always	ALL	✓ ACCEPT	Enable
4	any	any	all	Absolute VOICE Servers	always	ALL	✓ ACCEPT	Enable
5	any	any	all	all	always	ALL	DENY	

- Click “Create New”

Policy Options

Incoming Interface:	Any
Source Address:	All
Source user:	-
Source Device:	-
Outgoing Interface:	-
Destination Address:	Absolute VOICE Servers
Schedule:	(184.178.213.0/24) Always
Service:	All
Action:	Accept

Firewall/Network Options

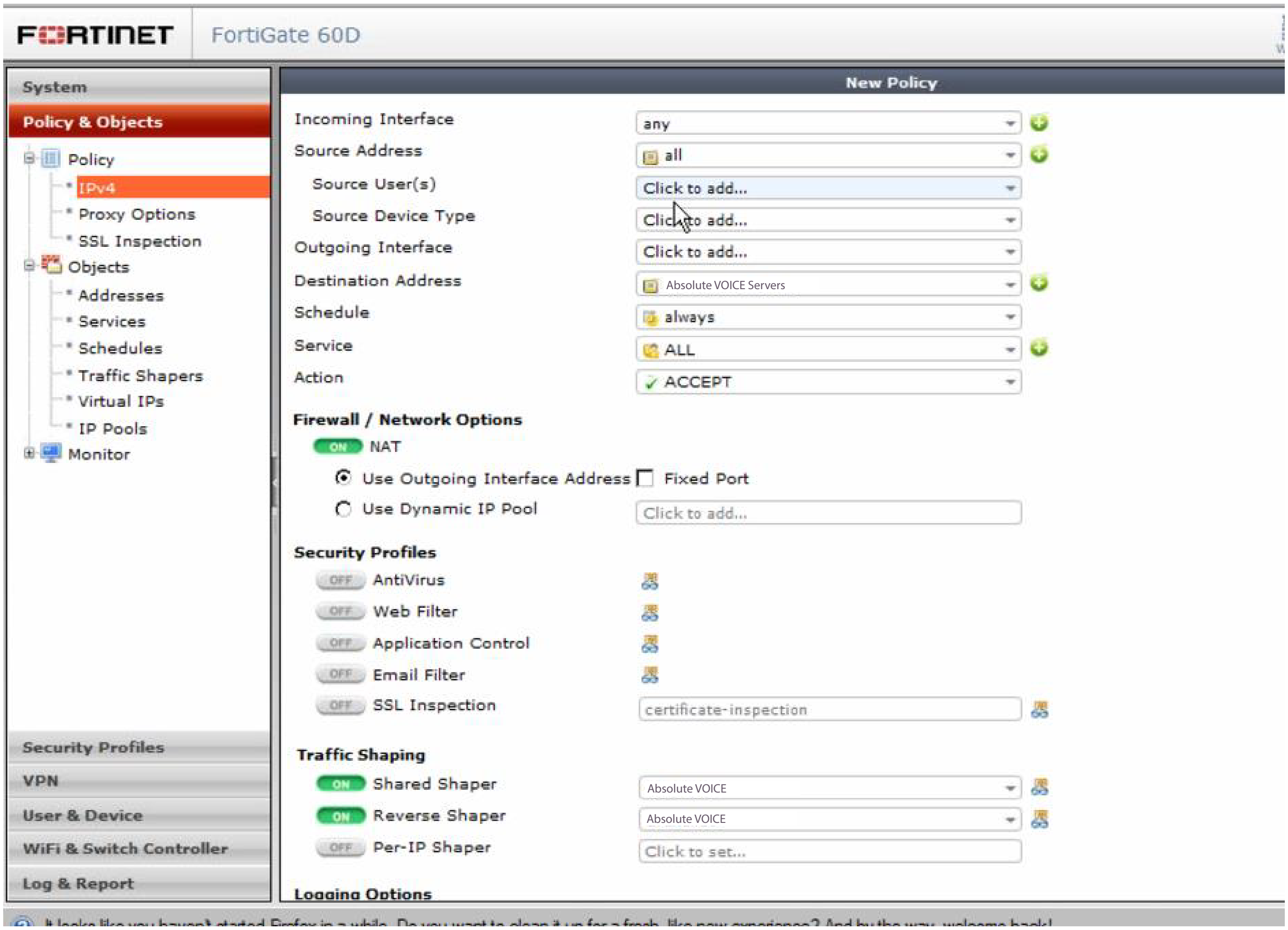
- NAT: ON
- Use Outgoing Interface Address - Uncheck "Fixed Port"

Security Profiles:

- All security profiles disabled/turned off

Traffic Shaping:

- Shared Shaper: Absolute VOICE
- Reverse Shaper: Absolute VOICE
- Per-IP Shaper: Disabled



FORTINET FortiGate 60D

New Policy

Incoming Interface	any
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	Click to add...
Destination Address	Absolute VOICE Servers
Schedule	always
Service	ALL
Action	✓ ACCEPT

Firewall / Network Options

ON NAT

● Use Outgoing Interface Address □ Fixed Port

○ Use Dynamic IP Pool Click to add...

Security Profiles

OFF AntiVirus

OFF Web Filter

OFF Application Control

OFF Email Filter

OFF SSL Inspection certificate-inspection

Traffic Shaping

ON Shared Shaper Absolute VOICE

ON Reverse Shaper Absolute VOICE

OFF Per-IP Shaper Click to set...

Logging Options

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

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