

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

www.callabsolute.com



Table of Contents

- 1. Introduction
- 2. Firewall Verification Checklist
- 3. Disable SIP ALG (CLI SSH)
- 4. Create Traffic Shaper
- 5. Create Traffic Shaping Policy
- 6. 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 <u>experienced</u> 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).



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 \rightarrow Traffic Shaper \rightarrow Absolute VOICE shaper	
3	Policy & Objects \rightarrow Traffic Shaper Policy \rightarrow Absolute VOICE shaper policy	
3	Policy & Objects \rightarrow IPv4 Policy (showing the Absolute VOICE Outbound Policy Order)	
4	Policy & Objects \rightarrow IPv4 Policy \rightarrow Absolute VOICE Outbound Policy detail	
5	Policy & Objects \rightarrow IPv4 Policy \rightarrow 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
 - o set sip-helper disable
 - set sip-nat-trace disable
 - reboot the device



- 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



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





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:

Dashboard	> '	+ Create New	🖋 Edit	Clone 🗇 Delete	Search		Q		
Security Fabric	>	Name 🜻	Type 🗘	Guaranteed Bandwidth	h 🗘 Max Bandwidth 🌲	Bandwidth Utilization 🗘	Dropped Bytes ≑	Priority 🗘	Ref.
 FortiView 	>	Absolute VOICE Shaper	Shared	3000 kbps		0 B/s	0 B	High	0
 Network 	>	guarantee-100kbps	Shared	100 kbps	1048576 kbps	0 B/s	0 B	High	0
System	1 >	high-priority	Shared		1048576 kbps	0 B/s	0 B	High	0
Policy & Objects	~	low-priority	Shared		1048576 kbps	0 B/s	0 B	Low	0
IPv4 Policy	_	medium-priority	Shared		1048576 kbps	0 B/s	0 B	Medium	0
In very oney		shared-1M-pipe	Shared		1024 kbps	0 B/s	0 B	High	0
Addresses Wildcard EODN									
Addresses Wildcard FQDN Addresses Internet Service Databas Services	e								
Addresses Wildcard FQDN Addresses Internet Service Databas Services Schedules	e								
Addrenitication Rules Addresses Wildcard FQDN Addresses Internet Service Databas Services Schedules Virtual IPs	e								

• 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.
	(number of phones * approx. 100K)
Note:	Do not enter a "Max" bandwidth limit

• Click "Ok"

Туре	Shared Per-IP		
Name	Absolute VOICE Shaper		
Traffic Priority	High	-	
Max Bandwidth 🛛 🗨	1	kbps	
Guaranteed Bandwidth 🗨	3000	kbps	
DSCP 🔲	000000		



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
	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"

Name Ab	solute VOICE Shaping Policy	
Status 🛛 🖸	Enabled Oisabled	
Comments W	/rite a comment 0/255	
If Traffic Matche	S:	
Source	all × +	
Destination	Absolute VOICE Servers	
Schedule		
<mark>Service</mark>	₽ ALL ×	
Application	+	
URL Category	+	
Then:		
Action	Apply Shaper Assign Group	
Outgoing interfa	ce 💌 WAN (wan) 🗙	
Shared shaper	Absolute VOICE Shaper	
Reverse shaper	Absolute VOICE Shaper	
Per-IP shaper	•	



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"

Dashboard	> New Policy		
Security Fabric	>		
FortiView	> Name 0	Absolute VOICE Outbound	
• Network	> Incoming Interface	⊐‡ lan	•
System 1	> Outgoing Interface	🗃 WAN (wan)	•
Policy & Objects	✓ Source	🖾 all	×
IPv4 Policy Authentication Rules	☆ Destination	Absolute VOICE Servers +	×
Addresses	Schedule	o always	•
Wildcard FQDN Addresses	Service	ALL +	×
Services	Action	✓ ACCEPT ⊘ DENY	
Virtual IPs	Inspection Mode	Flow-based Proxy-based	
IP Pools	Firewall / Network	Options	
Protocol Options	NAT	•	
Traffic Shapers	IP Pool Configuration	n Use Outgoing Interface Ad	dress Use Dynamic IP Pool
Traffic Shaping Policy	Preserve Source Po	t ()	
Traffic Shaping Profile	Protocol Options		~ /
Security Profiles	> Security Profiles		
2 VPN	AntiVirus		
User & Device	Web Filter	0	
WiFi & Switch Controller	> DNS Filter	0	
Log & Report	Application Control	•	
Monitor	> SSL Inspection	ss no-inspection	- <i>d</i>
	Logging Options		
	Log Allowed Traffic	Security Events All Session	S
	Comments Write	e a comment // 0/102	3

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

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
E == 1	lan 🛶 🗮 WAN (wan) 📀								
2	Absolute VOICE Outbound	🖾 all	Crexendo Servers	Co always	ALL	 ACCEPT 	Enabled		UTM UTM
1		🔳 all	🖿 all	o always	ALL ALL	✓ ACCEPT	Enabled		UTM UTM
	WAN (wan) →54 Ian 🕚								
3	Absolute VOICE Inbound	Absolute VOICE Server	s 🛄 əll	.o. always	. ALL	 ACCEPT 	Enabled		UTM UTM
🗖 Imp	licit 🕦								
0	Implicit Deny	🗉 all	🖾 all	Co always	ALL	O DENY			O Disabled



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