Time Sensitive Information!

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

Cisco Meraki Router Configuration
For Crexendo Cloud Telephony Deployment

Document Version 1.4

February 12th, 2021

Table of Contents

Read Me!

1. These changes must be applied before client implements their Crexendo 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 855-211-2255 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 Crexendo Customer Support specialist know.
6. Once completed, a Crexendo 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 Cisco Meraki firewall & router appliances to support Crexendo'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. Setting values not mentioned may be left at default or changed as required for specific purposes.

Please call Crexendo Customer Support at 855-211-2255 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 Cisco Meraki web GUI.

We recommend loading the latest Meraki OS (firmware).

Firewall Checklist

After applying the GUI configurations in this document, please take the appropriate screen shots to provide the firewall "verification" to Crexendo.

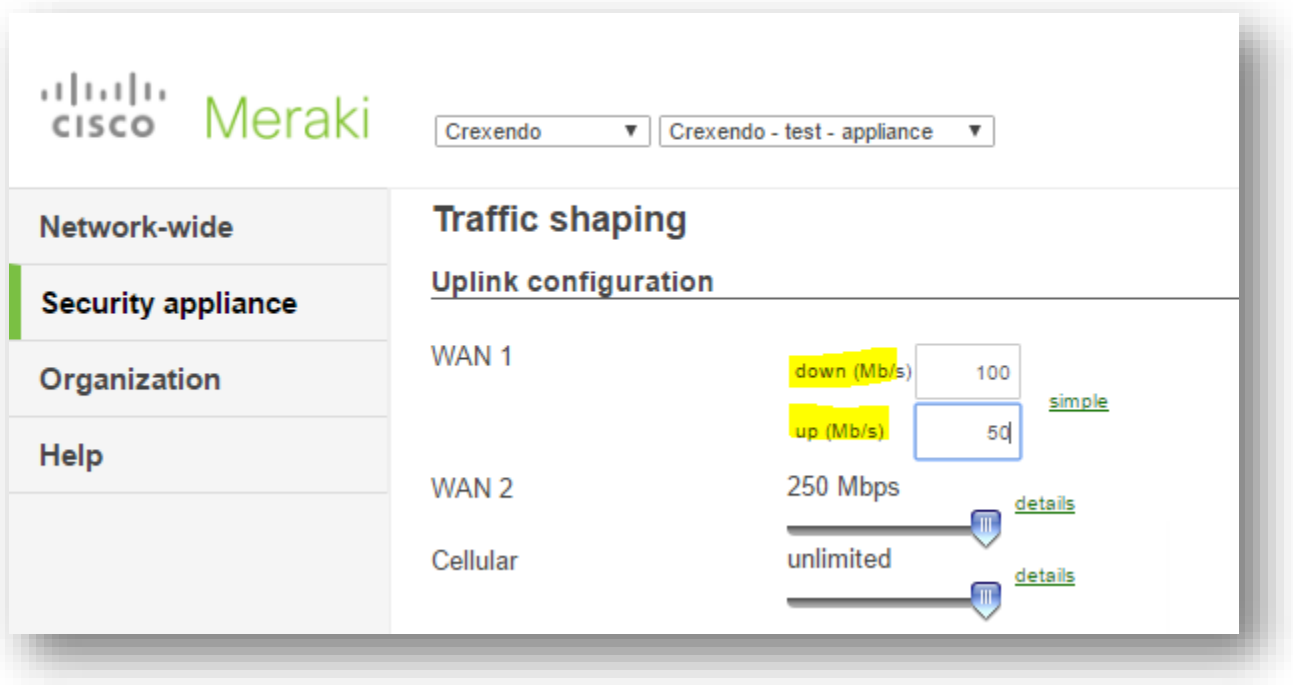
Screen Shot #:	Configuration:	Completed:
1	Security Appliance → "Traffic Shaping" section	
2	Security Appliance → "Traffic Shaping Rules" section for Crexendo traffic	

Note: For Disaster Recovery Failover please also ADD the following Crexendo IP's to ANY STEP in the below document where the Crexendo 184.178.213.0/24 subnet is listed:

- DR Application servers: 207.45.79.0/24
- DR Endpoint SBC11: 52.43.52.39
- DR Endpoint SBC21: 34.215.81.217

Traffic Shaping – WAN Interface

Security Appliance -> Traffic Shaping

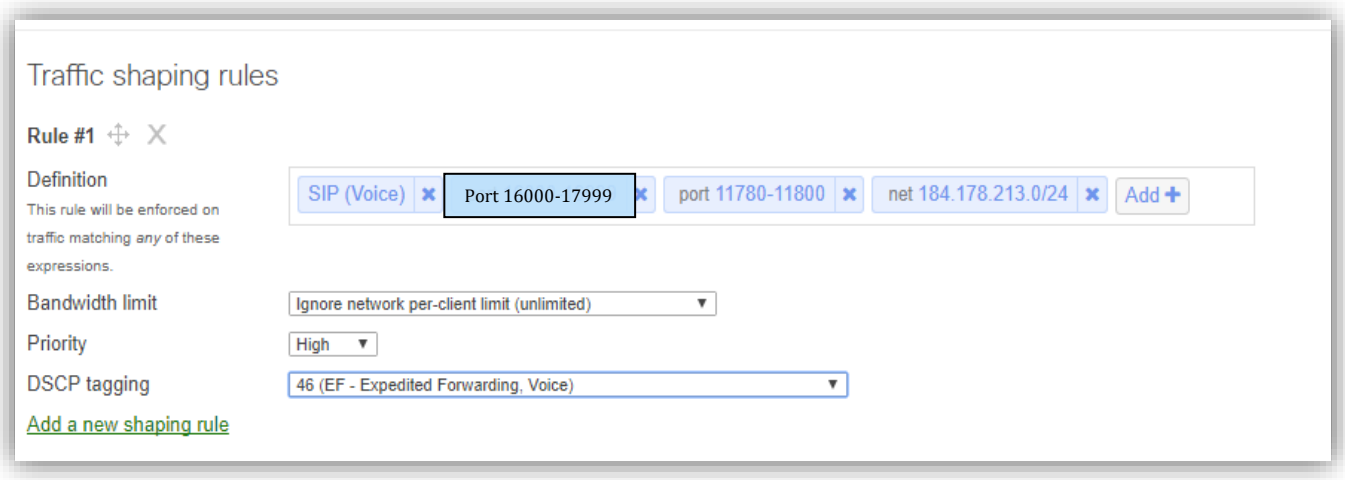


1. Choose the WAN interface that is active and set the contracted download and upload speeds.
    a. Click the “details” link for the internet interface.
    b. Enter the contracted download speed for the circuit.
    c. Enter the contracted upload speed for the circuit.

2. Click Save

Traffic Shaping – Ports & Network

Security Appliance -> Traffic Shaping



4. Edit a Rule Definition to setup the QoS and Traffic shaping for the Crexendo traffic.
    a. Enter the following ports and network address in the Definition field:
        - SIP – 5060
        - RTP – 16000-17999, 11780-11800
        - Crexendo network - 184.178.213.0/24
    b. Bandwidth Limit: "Ignore network per client limit"
    c. Priority: High
    d. DSCP tagging: 46 (EF – Expedited Forwarding Voice)

5. Click Save

Document Revision History

Version	Reason for Change	Date
1.0 Draft	Initial Draft Document	July 25th, 2016
1.1	Check list added	March 17th, 2017
1.2	Updated DSCP tagging reflective of firmware updates from Meraki (46 EF)	July 5th, 2017
1.3	Added additional RTP UDP Ports	May 6th, 2020
1.4	Add DR IP address notice	February 12th, 2021