CREXENDO VIP NETWORK SETUP/BEST PRACTICES:

This document outlines the necessary steps to configure your firewall/network settings to allow the CrexendoVIP Desk phones, Mobile App, Web phone and CrexendoHD products to function and communicate correctly with our platform.

The Crexendo VIP platform will be moving to our new Oracle Cloud Infrastructure (OCI). We recommend all customers please add the new ip addresses bolded in red as the others will be deprecated shortly after the migrations.

AS BEST PRACTICE. CREXENDO RECOMMENDS A BUSINESS CLASS FIREWALL FOR ANY INSTALLATION INVOLVING 3 OR MORE SIP PHONE /VOIP DEVICES.

A customer's network should be configured to standard industry practices to provide VOIP traffic proper signaling and quality of service. A network administrator should consider the proper items and best practices to have a successful installation and high-quality baseline:

- ISP Connectivity
    - Broadband – install or verify you have a modem that can be put into a bridge or pass-through mode.
        - Best model modems usually provide one coax input and one or two
    - Fiber – Ethernet handoff to the firewall
    - DHCP/Static – this is a customer preference; our service will function with either setup. The firewall WAN interface should have a Public IP Address.
    - ISP provided equipment that contains or is equipped with Telephony or RJ-11 ports on the back of them for digital voice services will require replacement, or assistance from the ISP to remove functionality from those ports and services in order to not interfere with Crexendo Services.
- ISP Throughput
    - The download and upload speeds should be considered when adding VOIP or any additional services to your network.
    - Network administrator should allocate enough bandwidth (download/upload) for data services and for VOIP traffic.
    - VoIP Traffic takes up approximately 100-120kbps per active call.
- Firewall
    - Crexendo recommends customers with 3 or more VoIP devices should consider installing a business/enterprise grade firewall to ensure best performance and security.
    - A business class firewall is required to provide proper SIP signaling, QoS and traffic shaping.
    - Examples: Sonicwall TZ/NSA models; Watchguard, Sophos, Fortinet

Network Switches

- A business class switch is required to provide best practice LAN configurations for VoIP and Data.
- POE is recommended to eliminate the need for power adaptors for phone devices.
- Managed Switch will allow a network administrator to configure VLANs, QoS and security on the network.

- Network Segmentation
  - Proper segmentation of network services is best industry practice.
  - Provide separate logical VLANs for your VoIP and Data traffic.
    - This will allow the network admin to use/share one Ethernet cable between a phone and computer. This would logically segment the traffic by tagging the VoIP traffic to a specified VLAN and the Data traffic to its own/or Native VLAN.
  - Provide separate physical Ethernet jacks for VoIP devices (on Voice VLAN) and for Data devices (on Data VLAN).

FIREWALL BEST PRACTICE CONFIGURATION

Below are the key elements to allowing full functionality and high quality VoIP through your firewall. For the specifics of how to implement each item you may need to refer to the manufacturer documentation.

Crexendo recommends removing any on premise-based PBX systems, Router settings or Servers configured with PXE Boot, or anything with the ability to use DHCP Option 66. These devices and DHCP options will interfere with the provisioning, setup, and daily operations of the Crexendo Services.

Note: Crexendo VIP traffic IP Addresses, URLs and Ports are listed below. Please use this table when creating your rules:

VIP Ports Required:

Port Range or Number	Protocol	Application	Services
5080	TCP/UDP	SIP	SIP Signaling
5082	TCP/UDP/TLS	SIPS	Secure SIP Signaling
20000-60000	TCP/UDP	RTP	SIP Phone Audio/RTP
80 443 5080 5082 8000 8001 8443 9002 19302 (Stun Service) 20000-27999 (RTP) 30000-60000 (RTP)	TCP/UDP	WebRTC, Provisioning, Web Sockets, Mobile Application, and Web Applications. https://stun.I.google.com	Mobile App, Portal, Web phone, Progressive Web Application, and Desk Phones

VIP Server IP Addresses:

FQDN	IP Address or Range	Description
usw.crexendovip.com	136.179.46.97 **132.226.159.170 (OCI)**	USW
usw2.crexendovip.com	136.179.46.102 **132.226.57.124 (OCI)**	USW2
usc.crexendovip.com	162.217.15.97 **131.186.0.38 (OCI)**	USC
usc2.crexendovip.com	162.217.15.101 **141.148.178.111 (OCI)**	USC2
use.crexendovip.com	155.130.141.97 **129.213.215.42 (OCI)**	USE
use2.crexendovip.com	155.130.141.101 **64.181.221.247 (OCI)**	USE2
portal.crexendovip.com	136.179.46.105, **144.42.35.213 (OCI)**	Portal West

	155.130.141.104 **144.24.35.213 (OCI)** **193.122.179.160 (OCI)** **164.152.19.130 (OCI)**	
endpoints.crexendovip.com	136.179.46.104, **132.226.116.51 (OCI)** 162.217.15.104 **141.148.29.139 (OCI)**	Endpoints West Endpoints East
Recording Servers	136.176.46.106 **132.226.159.174 (OCI)** **149.130.212.135 (OCI)**	Recording Server

VIP Third Party Services:

Service	IP Address	FQDN	Ports
VIP Enterprise Fax	54.219.249.208 52.32.130.83	Atainі.ipfax.net Ataserver.ipfax.net	80 442 443
VIP MEETINGS	184.169.150.184 52.52.95.56	meetings.crexendovip.com	80 443
CrexendoHD – Video Conferenceing	3.130.158.184 18.130.7.254 35.183.150.146 35.175.185.150 52.34.73.65 54.188.133.147 54.153.249.187	ap-south.snaphd.io ca-east.snaphd.io eu-west.snaphd.io us-east.snaphd.io us-west.snaphd.io us-west.snaphd.io	8080 8081 443
Google Text To Speech	https://www.gstatic.com/ipranges/goog.json		
Yealink Redirection Service	https://support.yealink.com/en/portal/knowledge/show?id=6476e6806a27da76bd06a8d8		
Crexendo Teams Integration	https://docs.connecttoteams.com/en/articles/55		
Grandstream GAPS	35.82.75.208	fm.grandstream.com	80, 443

SIP ALG

SIP ALG is a proxy function of firewalls that allows the firewall to translate and speak as a "proxy" to VoIP providers SBC and Endpoint servers. This communication on most firewalls tends to have difficulty making this translation (i.e., translating English to Greek, then Greek to English on its way back), the signaling may get malformed.

- We recommend on most firewalls to disable SIP ALG.
- Only on certain Cisco ASA model's do we recommend enabling or keeping SIP ALG on:
  - IOS versions between 8.2 to 9.3
  - If the IOS version is 9.4 and above disable SIP ALG ("no sip-inspect" within the policy-map global policy)

UDP Timers

UDP timers come in play on networks with VoIP devices where there is a registration cycle that keeps the session and pinholes open for communication between the VoIP device and Crexendo VIP servers. Depending on your firewall's default setting we recommend raising the UDP Timers to ensure the session and port is not torn down.

- UDP Timer or UDP Inactivity Timers
    - Set to anything above 60 seconds, we typically use 80 seconds as a standard.

- Cisco ASA and ISR models we use the following CLI commands to update:
    - timeout xlate 3:00:00
    - timeouts conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
    - timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
    - timeout sip 1:10:00 sip media 0:10:00 sip-invite 0:03:00 sip-disconnect 0:02:00
    - timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

Access Control Lists

ACLs are security lists that allow or deny specified traffic flow within and through a firewall or router. Depending on your network design and setup some instances require very specific traffic to be allowed through a firewall while simpler designs may already have all traffic allowed. ACLs also help with adding QoS services, UDP timers, bandwidth management rules to be applied to in our case specified VoIP traffic.

- Outbound ACL's
    - Allow VoIP defined traffic (see table above) by ports and IP Addresses.
    - Allow NTP traffic for the devices on this subnet.
    - Allow DNS lookup for the devices on this subnet.
- Inbound ACL's
    - Allow inbound traffic from the IP Addresses defined in above table to the VoIP device subnet.

QoS

Quality of Service allows the firewall to prioritize the VoIP traffic over normal data traffic. The QoS can be identified based on DIFF SRV tag (EF 46), ports or destination IP Addresses (see table above.)

- Define the VoIP Specified traffic to be "Priority" traffic when traversing the firewall.
- On a lot of firewalls this can be done within the ACL rules and ordering of the ACL rules putting the more important traffic (VoIP) at the top of the list.

Note: Typically, we can only control the outbound traffic's priority.

Traffic Shaping/Bandwidth Reservation

Shaping or reserving of bandwidth allows a network administrator to allot a static or dynamic (depending on firewall model) amount of bandwidth for VoIP traffic. Shaping goes hand in hand with QoS/Prioritizing VoIP traffic.

These features together help protect the quality of the voice traffic even on high transactional, high-volume firewalls and incase of bandwidth saturation.

- Configure either traffic shaping or bandwidth reservation to allot for a minimum of half the number of VoIP devices on the network. Also allowing bandwidth up to what is needed (infinite) or if the all the VoIP devices were active at the same time.
- I.E. If 10 phones are on a network, I would set my minimum bandwidth limit to be at least 500kbps (5x100kbps) and a max of 1-1.5mbps.
- Some models use percentage % for the shaping, this can be calculated in the same way based on the upload bandwidth.

Other Considerations

All business class firewall's have many different security modules added to their software. We want to make sure that we "whitelist" or "exclude" all VoIP traffic from any of these types of services. The goal is to provide the VoIP traffic with the most efficient path in and out of your company's firewall. Below are some services that you will want to disable or whitelist the VoIP traffic detailed in the table above:

- Antivirus
- DPI – Deep Packet Inspection
- Intrusion Prevention
- Content Filtering
- DHCP option 66
- PXE BOOT

Once these items have been configured you will be ready to install and implement the Crexendo VIP Phones on your network with confidence.

If you have any further issues, please contact us by opening a ticket at support@crexendo.com

Crexendo Operations Support Team