ESI eSIP, eCloud, IP900 and CommServer

Network Equipment Configuration for Optimum VoIP

This document lists the generic recommended configuration settings for modems, gateways, Optical Network Terminal (ONT), firewalls, routers and switches to ensure optimal Voice over Internet Protocol (VoIP) performance for Estech Systems, Inc. (ESI) services. It covers hosted phones as well as Session Initiation Protocol (SIP) trunks - both dynamic/registered and static/unregistered. Any questions on the following configuration settings should be directed to the ESI Technical Support Center (TSC) network team.

Created by Dean Hassinger

Last updated: Apr 24, 2023

Contents

Generic Requirements for All ESI Services

For modem, firewall, router and switch configuration, the following settings are necessary for optimum performance:

- Modem/Gateway: Bridge mode, or as some manufacturers call it, pseudo bridge mode, is enabled or configured. This ensures the modem simply passes the voice and data traffic from the Internet Service Provider (ISP) straight through to the firewall or router behind it without performing any other actions on the packets. In this way, the firewall or router performs traffic management, Quality of Service (QOS) and other actions on the traffic, not the modem. The reason for this is any additional traffic management added to the stream of packets can introduce some delay, even if small seemingly insignificant delays. Also, many all in one units (gateways) which combine firewall, router and Wireless Access Point (WAP) functions, do not have sufficient processing power to enable advanced features without some impact to the quality of the stream of packets, or those features are limited compared to a stand-alone device dedicated to providing such features.

- Modem/Gateway/Firewall/Router: The feature SIP Application Layer Gateway (ALG) is disabled or turned off. SIP ALG may also be called SIP Helper, SIP Inspect, SIP NAT Helper, SIP Passthrough or SIP Transformation depending on the manufacturer of the firewall or router.

- Firewall/Router: Bandwidth management (BWM) is enabled on the Wide Area Network (WAN) interface to limit total upload bandwidth to the subscribed upload bandwidth per the ISP contract. This is done because If the bandwidth value is set too high on the firewall or router and the upload/upstream ISP bandwidth (especially on cable networks) is less, some packets are going to be dropped by the ISP network. Therefore, limiting the outflow of the firewall or router is necessary to keep this from happening. See more at the bottom of this document for testing the ISP connection bandwidth if it is not known.

- Firewall/Router: The voice traffic outbound (from the customer site to the Internet) to ESI voice servers is prioritized using one of the following methods (the prioritization methods are listed in order of preference):

    - By ESI voice server destination network addresses:
East network: 75.98.35.128/25
Central network: 172.83.95.0/24
Note: Both networks need to be configured in the firewall to ensure service continuity in case of failover from one server to another.

    - By ESI voice server destination IP address ranges:
East network: 75.98.35.129 - 75.98.35.254
Central network: 172.83.95.1 - 172.83.95.254
Note: Both network ranges need to be configured in the firewall to ensure service continuity in case of failover from one server to another.

    - By protocol type: SIP and Real-time Transport Protocol (RTP)

    - By Differentiated Services Code Point (DSCP) value 46

- Firewall/Router: The User Datagram Protocol (UDP) session timeout is set to 300 seconds. This parameter sets the time the firewall or router waits to sense no traffic activity before closing a particular UDP port. Some firewall and router manufacturers set this timer to 10 seconds or less by default which causes problems with VoIP phones.

- Firewall/Router: The Domain Name System (DNS) servers are set to use Google (8.8.8.8 or 8.8.4.4). In some cases, timing issues such as phone registration, Busy Lamp Function (BLF) or call setup lag time can be improved by using well known public servers such as Google (8.8.8.8 or 8.8.4.4). Using a local DNS server or one provided by the ISP may not provide a fast enough lookup when updates are made. While this does not affect every call, it can contribute to registration and audio quality issues if the network latency is borderline.
- Switch: The switch is a managed switch. Managed switches are preferable to unmanaged switches for the reason of QOS functionality and troubleshooting.
- Switch: The managed switch is configured to enable the DSCP to Class of Service (COS) mapping function. The mapping is configured to put DSCP value 46 (also called Expedited Forwarding, or EF) into the highest category queue, if it is not so by default.
- Switch: The managed switch is configured to trust the DSCP value on the ports to which ESI equipment is connected. ESI devices are configured to send the correct DSCP value for the voice packets.

Additional Requirements

In addition to the above generic requirements, the following requirements are related to specific ESI services and/or equipment.

Hosted Phones

If the customer has hosted phones from ESI, the following additional settings are necessary.

- Switch: Link Layer Discovery Protocol (LLDP) is enabled on ePhone devices by default. To enhance the ease of configuration, this feature should be enabled on the switch with the Media Endpoint Discovery (MED) extension also enabled to tell the phones which Virtual Local Area Network (VLAN) to use, if the network is configured with them.

Static/Unregistered SIP Trunks

If the customer has static/unregistered SIP trunks from ESI, the following additional settings are necessary:

- Firewall/Router: A port forward rule created to forward packets originating from ESI voice networks and destined to UDP port 5060, to the phone system IP address.
- The phone system must have Network Address Translation (NAT) Traversal enabled if the system is behind the firewall. The NAT Traversal parameter exists on some phone systems to tell it whether or not it is behind a firewall.

eSIP

If the customer has an eSIP premise based phone system from ESI, the following additional settings are necessary:

- Firewall/Router: The following port forward rules created to forward packets originating from ESI technical support networks (192.64.95.0/24 and 209.191.183.152/29):
    - Packets destined for Transmission Control Protocol (TCP) port 59088 forwarded to the phone system IP address for technical support management access.
    - Packets destined for TCP port 59022 forwarded to the phone system IP address for technical support management Secure Shell (SSH) access.

- Packets destined for TCP port 59021 forwarded to the phone system IP address for technical support management File Transfer Protocol (FTP) access.

- Firewall/Router: A port forward rule created to forward packets destined for TCP and UDP port 59111 to the phone system IP address for eMobile. This rule should allow connections from any source.
- Firewall/Router: If using eMobile (eMobile+, eMobile+ Pro, FQDN), an outbound (from the customer site to the Internet) rule created to prioritize packets to the following ESI server IP addresses:
  50.16.93.5
  35.238.14.67
- Switch: LLDP is enabled on ePhone devices by default. To enhance the ease of configuration, this feature should be enabled with the MED extension also enabled.
- Switch: Plug-and-Play (PnP) is enabled by default on ePhone devices to connect to the eSIP e-Series if it is on the same network as the phones. This must be allowed across the network for the phones to find the phone system if this method is intended to be used.
- Firewall/Router: For eSIP x-Series, the ePhones use Dynamic Host Configuration Protocol (DHCP) option 66 to learn of the phone system. This option is configured in the DHCP server to send the phone system IP address to the phone.

Comm Server

If the customer has a communications server (comm server) premise based phone system from ESI, the following additional settings are necessary:

- Firewall/Router: For ESI SIP trunks, a port forward rule created to forward packets originating from the ESI voice servers and destined for UDP port 5060, to the phone system primary IP address configured in Function 84 (F84).
- Firewall/Router: For ESI SIP trunks, a port forward rule created to forward packets originating from the ESI voice servers and destined for UDP port 10000 through 11000, to the phone system secondary IP address configured in F84.
- Firewall/Router: A port forward rule created to forward packets originating from the ESI technical support networks and destined for TCP port 59002, to the phone system IP address configured in Function 824 (F824).
- Firewall/Router: A port forward rule created to forward packets originating from the ESI technical support networks and destined for TCP port 59022, to the phone system IP address configured in F84 using port 22.

IP-900

If the customer has an IP-900 premise based phone system from ESI, the following additional settings are necessary:

- Firewall/Router: For ESI SIP trunks, a port forward rule created to forward packets originating from the ESI voice servers and destined for UDP port 5060, to the phone system primary IP address configured in Function 84 (F84).
- Firewall/Router: For ESI SIP trunks, a port forward rule created to forward packets originating from the ESI voice servers and destined for UDP port 10000 through 11000, to the phone system secondary IP address configured in F84.

- Firewall/Router: A port forward rule created to forward packets originating from the ESI technical support networks and destined for TCP port 59443, to the phone system IP address configured in Function 821 (F821).
- Firewall/Router: A port forward rule created to forward packets originating from the ESI technical support networks and destined for TCP port 59002, to the phone system IP address configured in F824.
- Firewall/Router: A port forward rule created to forward packets originating from the ESI technical support networks and destined for TCP port 59022, to the phone system IP address configured in F821, using port 22.

eAccess Door Reader

If the customer has eAccess door readers from ESI, the following additional settings are necessary:

- Firewall/Router: An outbound (from the customer site to the Internet) rule created to prioritize packets to the following ESI eAccess server IP addresses prioritized:
  3.21.121.201
  3.19.103.138

Bandwidth Test

If the customer does not know their ISP upload bandwidth, this can be approximated by performing four or five consistency/streaming speed tests over a period of ten or so minutes to get an average baseline of the actual consistent service bandwidth.

When conducting speed tests, use a site that uses a consistency, or streaming, speed test. A good one to use is http://testmy.net . When using this site, performing the manual test with the 100 MB size gives a longer duration test that lasts over the burst period that a provider may allow which gives a more accurate result.

This is important as QOS uses the interface bandwidth value to determine its prioritization of traffic. If the bandwidth value is set too high and the upstream ISP bandwidth (especially on cable networks) is less due to temporary congestion, the firewall or router can send the prioritized traffic faster than the ISP can receive and it is dropped by the ISP network. Therefore, a bit of a buffer is necessary to keep this from happening due to actual bandwidth fluctuations.