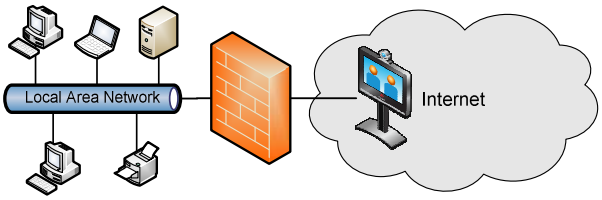
TWS Firewall Guideline

Whichever model of firewall and/or router you use, you should make sure that any H.323 and/or H.225 and/or H.245 inspection, fix-up, helpers, transformations, or ALGs (Application Layer Gateways) are disabled. Also ensure that you don't have any pre-existing rules or services that may conflict with the recommendations given below. We suggest that new rules for the ports listed below are created and clearly indicated for future reference. These rules should of course be open bi-directionally.

We recommend one of the following three options for implementing videoconferencing systems (End Point) within your network:

OPTION 1 of 3

Endpoint outside the firewall with a public IP address:

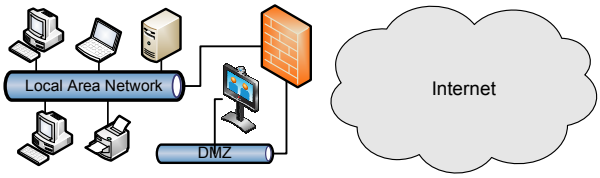


Firewall Configuration

No configuration necessary. However, we would recommend that your system is not configured to permit unauthorized access.

OPTION 2 of 3

Endpoint within a DMZ with a public IP address:



Firewall Configuration

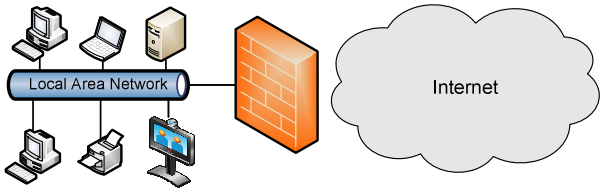
Ensure that all **TCP/UDP** ports in the range **1024 – 65535** are open for outbound traffic.

Open **TCP port 1720** (used for call setup) and **UDP port 1719** (in use for Easymeeting registration and EasyNumber).

Open **TCP and UDP 3230 – 3280** (used for audio, video and data) to the public IP of your system.

OPTION 3 of 3

End Point within the private LAN behind the firewall, using a private IP address and a public NAT address (* one separate public IP per system is required):



Firewall Configuration

Ensure that all **TCP/UDP** ports in the range **1024 – 65535** is open for outbound traffic.

Forward **TCP port 1720** (used for call setup) and **UDP port 1719** (in use for Easymeeting registration and EasyNumber).

Forward **TCP** and **UDP** ports 3230 – 3280 (used for audio, video and data) to the private IP of your system.

Endpoint configuration:

Navigate to *Settings -> Network -> Firewall.*

- Static NAT Traversal = Enabled
- Public IP Address = [Enter the NAT public IP address]

"Please note, Easymeeting.net cannot be responsible for the configuration of your firewall/router. This document is intended as a guideline to help you realize all features of the Easymeeting service."

Network guideline

These recommended network guidelines are intended to allow you to obtain the best experience when accessing the easymeeting services. Video performance and quality of experience is directly related to network performance, should a network link be unreliable or give intermittent performance, this can have the same impact on your video experience.

Bandwidth (bi-directional)

- Acceptable audio/video quality in SD & PC/Mobile based videoconferencing: 384kbps
- Good audio/video quality in SD & PC/Mobile based videoconferencing: 768kbps
- Recommended bandwidth for ***HD*** videoconferencing: 1024kbps

Packet loss

Typical numbers for acceptable packet loss during a conference range from 0.1% to 2%. Packet loss for high definition systems typically needs to be under 0.1% to remain unnoticed. 1% is noticeable while 5% is intolerable.

Network Duplex Mode

Duplex mismatch is the number one cause of packet loss and video freezing. FULL duplex are required for videoconferencing.
Ensure that the endpoint is configured to match the switch port duplex and speed capabilities. You should always use the same duplex on the endpoint as at the port it is connected to.

Duplex settings

Switch	Device	
100/full duplex	10/Full Duplex	☹
100/Full Duplex	100/Half Duplex	☹
100/ Full Duplex	Auto	☹
100/Full Duplex	**100/Full Duplex**	☺
10/Full Duplex	**10/Full Duplex**	☺
100/Full Duplex	100/Half Duplex	☹
Auto	100/Full Duplex	☹
Auto	100/Half Duplex	☹
Auto	**Auto**	☺
Auto	10/Full Duplex	☹
Auto	10/Half Duplex	☹

Latency (Delay)

Audio packets are small, while video packets are large. Intermediate routers may prioritize the two packet sizes differently, creating differing transit times so the audio and video packets become out of sync. A typical rule of thumb for latency is < 300 ms round trip between endpoints before users in an interactive call start to notice a delay between the speaker and the receipt of their words by the far end participants.

0 – 150 ms	: recommended
150 – 300 ms	: acceptable
300 – 400 ms	: not recommended
400 ms	: unacceptable

Jitter

Jitter refers to unwanted variation when packets are received. If there is a traffic delay, data can be buffered accordingly; however, when the delay continues to change, processors get overloaded, driving up latency and packet loss. This can result in frozen or jerky appearance of the video or/and the audio. A good rule of thumb for jitter is less than 30msec for a high-quality videoconference experience.

Application Layer Gateway, H.323 proxy or other "firewall-helpers"

Make sure that any H.323 and/or H.225 and/or H.245 inspection, fix-up, helper, transformations, or ALGs are disabled, and make sure that you don't use any pre-existing H.323 services that may be defined for the firewall rules; create new bi-directional rules for both port 1720 for H.323 and for the reserved (dynamic) ports.

Quality of Service

A best-effort network such as the public Internet does not support QoS. In a best effort network all users obtain best effort service, meaning that they obtain unspecified variable bit rate and delivery time, depending on the current traffic load. QoS will only work inside a private network where you have full control over the infrastructure between A and B.