

Firewall settings

Using Marratech Pro or Marratech E-meeting Portal on your network is both simple and secure! Our software is designed with firewalls and Network Address Translation (NAT) in mind and will work fine with most web Proxy servers.

This document describes how to configure your firewall to allow E-meeting traffic to pass through it. You should be familiar with how IP traffic works and how to set up a network to understand this document properly.

This document applies to Marratech Emeeting Portal versions 1.3, 1.3.1 and 1.3.2 (and possibly later versions in the 1.3 branch). An updated version for later releases should appear in your manual and/or on the support pages on www.marratech.com.

Client access through a firewall

Allowing a client to connect to a Marratech E-meeting Portal is very easy. Only two steps are needed.

First, the client must be allowed to connect to the HTTP and the HTTPS ports defined in the portal. If the portal runs on the standard web ports, this is usually already set up in some way. The client can use a web proxy server, but this has to be defined in the client settings.

Second, the client must be allowed to send traffic to all UDP data ports defined in the portal AND it must also receive returning traffic.

As the client will initiate all connections, both of these rules can be set up using a Dynamic state rule.

Portal on a DMZ with public addresses

No special configuration is needed in the Marratech E-meeting Portal to run on a DMZ with public addresses. Only the firewall needs to be configured.

If a small number of users are connecting from the outside, you can set up dynamic state rules in the same way as above, with the exception that they are inbound towards the portal server.

However, if you are going to run a large amount of users, which will access the E-meeting Portal through the firewall, using dynamic states might overload the firewall. In these cases, it might be better to set up two rules for the UDP data traffic, one inbound which allows sending to the specified data ports, and one outbound which allows the portal to send traffic to any ports with the data ports as sending ports. You could also set up the same kind of rule for the TCP traffic.



Setting up a portal with a Port mapping/Port forwarding firewall

If the portal is set up on a DMZ or internal network with private addresses, some configuration of the E-meeting Portal is required, as well as setting up the port mapping and access rules in the firewall.

The port mapping must be set up for the web and data ports defined in the portal. You must use the same ports in the firewall as on the E-meeting Portal configuration, both for HTTP/HTTPS web and for UDP data.

In some firewalls, you have to set up access rules separately from the port mapping, and in others the access rules are implied by adding the port mapping. You have to check your firewall manual to see how your firewall operates. If you need to set them up separately, see the above step.

Finally, some configuration of the portal is required, as it needs to know how the traffic is routed. There are three statements that need to be changed: Two in `emhs.cfg` and one in `emse.cfg`. Look for the statement called "rules = null;". It should contain at least two sets of three IP addresses: network address, network mask, and which portal address users on those addresses will use.

Here is an example:

LIST of LIST of STRING

```
rules = [ [ 192.168.0.0, 255.255.0.0, 192.168.4.3 ],  
         [ 0.0.0.0, 0.0.0.0, x.y.z.q ] ];
```

This means that users that sit on the local network and has addresses starting with 192.168 will connect to the address 192.168.4.3 and all other users will connect to the address x.y.z.q, which is an external address on the firewall which we use for port mapping.

If you have several internal networks, you could specify several lines like this:

```
rules = [ [ 192.168.0.0, 255.255.0.0, 192.168.4.3 ],  
         [ 10.0.0.0, 255.0.0.0, 192.168.4.3 ],  
         [ 172.16.0.0, 255.240.0.0, 192.168.4.3 ],  
         [ 0.0.0.0, 0.0.0.0, x.y.z.q ] ];
```

After you've added this line to all three places, you must restart the portal.

Note: Internal users might be able to use the external address in some cases, and in some not. This depends on the firewall configuration. However, to reduce the load on the firewall, it is recommended that internal users always connect to the internal address.

Note: As the server actually have two addresses, using port mapping will make a SSL-certificate only work for one of the addresses. The other users will receive a warning about wrong host address.

Setting up a back-to-back tunnel

A back-to-back tunnel is useful to reduce network load in some instances. The tunnel requires setting up one port for both UDP and TCP and will use the same port both remotely and locally. In back-to-back mode, you always set one tunnel as active and the other as passive; the active part will be the one starting all connections. You could use a dynamic state rule for the traffic. Port mapping is not officially supported for the tunnel, but might work if you set it up on the same port in the firewall.

Multi-homed servers

Marratech E-meeting Portal 1.3.2 does not support running on a multi-homed server. This is because it will bind to only one interface. You could, however, have several portals running on the same machine, bound to different IP addresses and interfaces.

Note: Marratech E-meeting Portal 1.3.2 is required for correct use in a multi-homed environment.

Allowing the Admin Tool through the firewall

Note: This section applies only to versions 1.3 through 1.3.2 of the Marratech E-meetingportal. Later versions will use another administration layout that won't require opening additional ports.

If you for some reason would like to allow the Administration Tool to be accessed through the firewall, it requires setting up two TCP ports. If you use port mapping, you must specify the address of the external interface in the "hostaddress" statement in system.cfg and then restart the portal.

Note: Adding a "hostaddress" statement for an external interface might make the Administration Tool impossible to run on the local machine, or may require some host changes.

Direct call

The Marratech Pro client software has an option to run directly towards another Marratech Pro client. This has several limitations: It does not support NAT and can't be used with dynamic state rules in the firewall. You might be able to get it to work with one machine by setting up port forwarding for the UDP ports used (50500-50511). However, running Direct call through NAT or a firewall is not a supported scenario.

Port usage

Default ports

The default web ports used by the portal are TCP ports 8000 (8080 on MacOSX) for HTTP and 8001 for HTTPS. The reason for using these ports is to avoid conflict with other running webservers. This can usually be changed to the default ports for HTTP and HTTPS (80 and 443 respectively).

The default data ports are UDP ports 52000 to 52999. Every active E-meeting room uses 12 ports selected randomly within this span.

For most installations, this is a rather large span of ports. You could limit them, but always count with at least 25 ports for each possible active e-meeting room as some ports could in theory be used by other applications on the portal server.

The default admin ports for the Administration Tool is TCP ports 4160 and 4161. You usually won't have to change this unless you're running another portal on the same machine, or some other Java software that uses a protocol named RMI.

Timeouts

The client will periodically send packets on the UDP data ports to keep any dynamic states in the firewall open. The default timeout is 20 seconds. We recommend that NAT and firewall rules use a timeout of at least one minute to enable E-meetings.

Connection scheme

This part is included to give better understanding about how Marratech Software works "under the surface" when the client connects to the portal.

- First, a client will connect with HTTP. The user will surf around and receive web pages. This uses HTTP 1.0 and will shut down after each request.
- When the user presses the "join" link, a request will be sent to the portal, which will set up the 12 UDP ports needed (two for each media: one for data and one for statistics) and return these to the client.
- The client will in turn connect to the 12 UDP ports and authorize itself.
- Data will be sent on the UDP ports either way when necessary.
- Periodically (every 20 seconds), there will be keepalive messages sent on the UDP ports to keep the NAT/firewall states active.
- Periodically (also every 20 seconds), the client will connect to the portal on HTTP or HTTPS and send an alive message, then shut down.

Glossary

DMZ - A DMZ (DeMilitarized Zone) is a special part of a network where you put servers that should be accessible both internally and from the outside. It can be implemented both with private and public IP addresses. If using private addresses, setting up a server inside the DMZ will require port mapping in the firewall.

Dynamic state - A special kind of rule that "remembers" which packets was allowed to go through the firewall, and will allow packets returning on the same port pair. Makes for a very secure solution, as no ports will be open when no e-meeting is in progress. Also known as "Keep-state", "Allow-return" and other names depending on the vendor.

Firewall - A program or piece of hardware that allows certain kind of network traffic and disallows other depending on the policy set up by the administrator. A firewall can be set up in many ways, ranging from

blocking external traffic to internal addresses (common in small to medium enterprises) to blocking everything both ways except the traffic passing through a Proxy server. A firewall usually includes NAT functionality as well.

NAT (Network Address Translation) - As IP addresses became scarcer in the 1990's, Network Address Translation became more popular and is today used virtually everywhere. Using NAT means a large range of IP addresses (usually private) will be translated into a smaller range of public addresses, sometimes only one address. NAT in itself also gives simple Firewall functionality as it will work in the same way as setting up a Dynamic State for all outbound traffic.

Port mapping or Port forwarding - When you have NAT using private addresses, you might still want to present some services. Port mapping means you will set up a certain address and port in the firewall to be forwarded to a specific machine inside the firewall. Also known as Port forwarding.

Private IP addresses - Defined in [RFC 1918](#). A private address starts with 10.x.x.x, 192.168.x.x or 172.16.x.x through 172.31.x.x. Private addresses are not routed on the internet and have to be translated through NAT.

Proxy server - A Proxy server can be used for many kinds of traffic, though the most popular one is for web traffic. Instead of connecting to a web site, your web client tells the proxy server to go get it for you. A proxy server can then perform certain tasks on the web page before sending it to you. Some common tasks are virus scanning and removal, parental control and similar policy based censoring before, or it can simply cache often accessed pages to reduce download times and network use.

Sales
sales@marratech.com

Other information
info@marratech.com

www.marratech.com