Security Overview

On-line collaboration frequently involves proprietary and confidential information. Users need to know that what they discuss on-line will receive the same protections and safeguards as the discussions they hold behind closed doors. Security is a key factor to the success of all on-line collaboration.

In order to achieve widespread acceptance of its solutions, Marratech focuses strongly on security and sees it as a very important aspect of network based, real time communication and collaboration. Marratech has invested significant effort in producing a product where security controls prevent service providers, system administrators, and other personnel from gaining access to live meeting information while not hindering end-users with any security related complications.

This paper explores the security features built into the Marratech software and discusses ways to deploy Marratech solutions across networks and the Internet without compromising network security.

The following explains the various levels of security in a step-by-step manner.

- Meeting access
- Meeting access: establishing a connection
- Encrypting live media
- NAT and firewall handling
- Buffer attacks
- SIP and H.323

Meeting access

The Marratech Manager provides meeting room access to the Marratech client.

Marratech meeting rooms are accessible through Marratech Manager's built-in web server. This built-in web server uses Secure Socket Layer (SSL) for user authentication, distribution of all web pages, sending the meeting description and encryption keys required to enter an meeting room.

SSL is an industry standard for secure web connections. Besides providing a layer of security through encryption, SSL also authenticates the server to the user by means of a certificate, thus reducing the possibility of a client inadvertently joining a rogue server.

Before joining an meeting, a user must authenticate (via SSL) to the Marratech Manager. Once this is done, meeting information is sent to the user's Marratech client, enabling it to join the meeting.

Access to a meeting room can be restricted in two ways. The first method is imposed by creating a private room, which forces access via the use of the built-in SSL password authentication service.

The authentication service can use the Marratech Manager's own, built-in database, or access an external LDAP (Lightweight Directory Access Protocol) or Microsoft Active Directory server. The LDAP server can be configured to use SSL to encrypt usernames and passwords.

Furthermore, meeting room access can be controlled on a group basis. Group membership can be managed directly on Marratech Manager or via LDAP. Meeting room access can be given to entire groups and/or to individual users.

Secondly, once a meeting is under way and all the desired participants have entered, the meeting may be locked, restricting further access to it. This simple functionality stops an unwanted, but authenticated and authorized person to join your meeting after it has started.

If an authenticated, authorized, but nevertheless unwanted user has joined your meeting, your group may evict him or her using a command similar to the locking mechanism.

The lock and eviction mechanisms can be accessed by groups and individual users selected as meeting moderators for a particular room.

Technical details:

- Adding a SSL certificate is done through the web based admin interface, making it a very easy step.
- When a SSL certificate is uploaded all http traffic can easily be diverted to the https port through the web based admin interface.

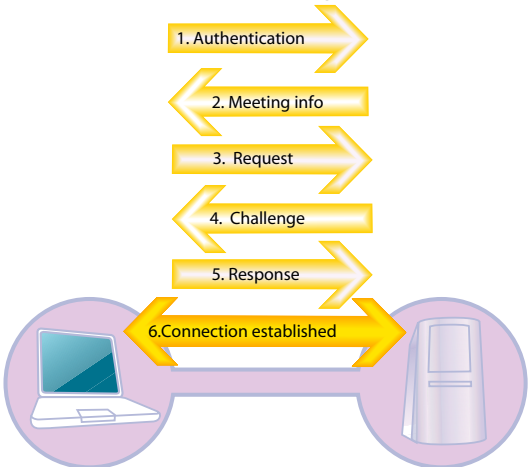
- All Marratech customers are strongly advised to purchase an SSL Certificate and upload it to the Marratech Manager. A PKCS#7 Certificate Chain is used and can be purchased from a Certificate Authority, such as Thawte or Verisign.
- A self signed certificate may be used, but must be uploaded to all the clients manually to avoid warnings.
- If SSL (https) is turned off, your meeting may not be safe from potential eaves droppers.

Meeting access: establishing a connection

When a user is authenticated and a meeting room linked is clicked, Marratech Manager sends a description file containing media information (voice, whiteboard, video, chat and web) and encryption information to set up the required connections.

To prevent external, unwanted listeners hijacking the connections (via IP address spoofing or other methods) during the connection setup, an encrypted challenge response scheme is used.

Challenge-response systems (i.e. question and answer) are often used in banking and Virtual Private Network (VPN) systems. Once the challenge is properly met, the connection between the Marratech client and Marratech Manager is established.



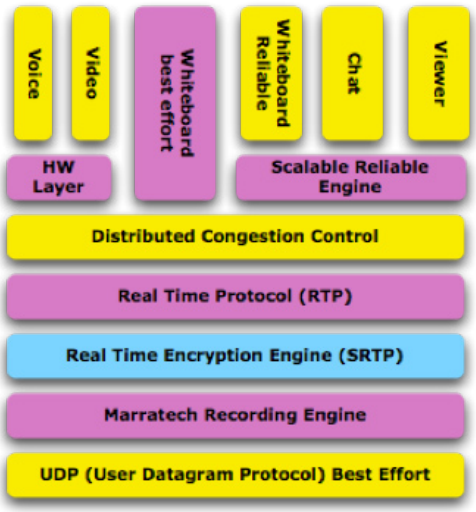
Technical Details:

- Steps 1 and 2 are done via the https protocol. Connection information (ports, media, encryption, challenge response) is sent via SSL and uses the installed certificate to ensure encryption and integrity.
- A challenge response (steps 3 to 6) is done via UDP, twice for every media (voice, 2 x whiteboard, video, chat and web). It is done once for the RTP connection and once for the quality control connection (RTCP).
- The whiteboard has a best effort connection and a reliable connection and therefore requires 4 connections. (2 x RTP, 2 x RTCP)
- The client meets the challenge thanks to the information fetched from SSL in step 2.
- Data sent to Marratech Manager, which originates from unauthorized originator (i.e. an originator that fails the challenge response scheme) is automatically discarded.
- The same challenge response scheme is used when establishing a connection between Marratech Manager Nodes (aka clusters).

Meeting joined: end-to-end encryption

Once the connection is established, the Marratech client is responsible for encrypting and decrypting all data to be sent and received on the network.

All media, including voice, whiteboard documents, whiteboard interaction, chat, slides and video, are encrypted before being sent out on the network, protecting the meeting from potential eavesdroppers, both on the network and on the server.



The Marratech client is built on top of an encryption engine where all the media is encrypted end-to-end.

The supported encryption algorithm is 256 bit AES.

After reaching the network, the media is not deciphered until it reaches the other Marratech clients. The Marratech Manager server software is not involved in the encryption or deciphering of meeting voice, video and data. This applies to all network scenarios; including Unicast, Multicast and Remote Node installations.

Because the Marratech Manager never decrypts or encrypts media streams, Marratech gains two advantages:

1. The server does not incur any overhead for encryption or decryption and, therefore, needs fewer system resources. This makes the server more scalable.

2. End-to-end encryption prevents third parties such as service providers, administrators, or other persons with direct server access from eavesdropping on a meeting.

The encryption methods used do not negatively affect overall performance, network bandwidth, server performance nor does it noticeably increase communication delays. Encryption is on by default.

In a standard environment, the server forwards the media encryption key as a part of the session file downloaded to the client following authentication.

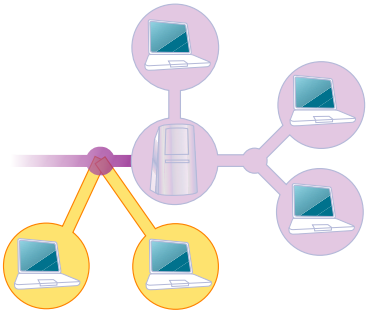
It is possible to store the media encryption key at a trusted third-party location. This has value to customers who need to locate Marratech Manager at a collocation facility or with an application service provider (ASP). By using a trusted third-party location, personnel who manage the server do not have access to the encryption keys.

With third-party key placement, the server sends the client a URL where the key resides. The client then establishes an SSL connection with the third party location to retrieve the key.

Customers can use external keys on a meeting room-by-meeting room basis. The system administrator stores the key's external URL when he creates the room. Users who join meetings in these rooms will need to authenticate towards the external server.

Technical Details:

- The encryption key(s) is stored in the session description file sent over SSL when first connecting to the Marratech meeting.
- When storing the encryption key externally, you must provide the key's URL when creating the meeting room (e.g.) When joining such an meeting with an external key, the user will need to authenticate towards your external server.



All data sent and received by the Marratech client is encrypted, no matter the network scenario (Multicast, Unicast, Hybrid, Remote Node, NAT, VPN, Firewall, etc...) The encryption is handled solely by the endpoints, securing your meeting content from server and network administrators or the ASP (Application Service Provider) hosting your meeting.

Network: Network Address Translation (NAT)

The widespread use of Network Address Translation (NAT) has made on-line real time interaction services a challenge to deploy. These types of firewalls often hinder real time communications; because of the way they hide computers from the Internet.

Marratech has developed a NAT compatible solution, which often eliminates the need for firewall configuration by system administrators.

Technical Details:
A NAT often has a default firewall rule, often called "dynamic state", "allow return", "established mode" or "keep state". When a NATed client sends a request, it allows the answer (from the same IP address and port) to reach the client.

NAT and the Marratech client
The Marratech client will function properly behind a NAT without any need for configuration.

NAT and the Marratech Manager
When placing the Marratech Manager behind a NAT, two steps must be done:

1. A static rule in the NAT must be inserted, so that external clients know where to connect. This is commonly called 'Port Forwarding'. It tells the

NAT to forward traffic meant for the Manager to the Manager's private IP address.

2. The NAT's public IP address must be added in Marratech Manager. This is easily done via the Network Details section of the Manager's admin interface.

Network: Firewalls

VPN

When handling deployments that span outside the intranet, the easiest, most secure solution is to use the VPN access already available on your network.

Marratech's solution is fully VPN IPSec compatible and the Marratech client will run over your VPN to access a Marratech Manager located within the firewall. The VPN should be enabled before launching Marratech client. Please remember that VPNs may add slight bandwidth and processor usage overhead.

Accessing an external server from within a firewall

For deployments where a VPN is not available, or for which a third party without VPN access must be given access, Marratech has made important efforts to make its solution firewall friendly:

1. The Marratech client always initiates the connections. In no case does Marratech Manager try to initiate a connection with the clients.

2. When a connection is established, data is always sent back on the same port through which it was received.

If a firewall is blocking UDP traffic, Marratech recommends creating a basic dynamic state rule. This can be done by only allowing a dynamic state mode rule towards your trusted Manager server.

A network administrator can configure the firewall to only allow a group of specific clients dynamic state access to a specific server.

Such a configuration will block all internet access except traffic specifically requested from an authorized client within the firewall, arriving on the same port as the original request and from the authorized server. Such a configuration is also valid for deploying a Marratech Manager on a company DMZ.

Other deployment scenarios

For deployments where access from external computers through the firewall is not an option (even with a re-enforced dynamic state rule) but external access is still required, the administrator can deploy the Central Node on the DMZ and a Remote Node within the firewall.

This implies that the following needs configuration:

1. HTTP traffic from the local clients toward the main portal on the DMZ needs configuring,

2. Node traffic between the two company controlled servers.

In other words, only traffic initiated between company controlled computers will cross the firewall.

Technical Details

- The UDP port range used by the Marratech Manager is fully configurable. This gives the administrator flexibility and control over which ports are to be configured in the firewall, if necessary.
- The default UDP port range to configure is 52000 to 52999.
- 12 UDP ports are used per meeting room. Marratech recommends allocating a few more than required in case a port is already being used by another process.

Risk analysis

These recommendations should be followed by a risk analysis.

The following applies to a firewall administrator wanting to give internal clients to an external, authorized Manager server by using a dynamic state rule.

If there are no on-going meetings with local clients participating, then no traffic will be allowed in. This will be just as your closed configuration would normally function.

If there is an on-going meeting and a third party tries to infiltrate the returning meeting ports, the firewall will reject the traffic, as it did not arrive from the authorized server and it did not come from a request initiated by a client. The client only initiates requests towards the authorized server and is only allowed to do so by the firewall.

If there is no on-going meeting and a third party succeeds in compromising the authorized Manager server, all traffic sent from the Manager will be re-

jected on all ports (including meeting ports) since the incoming traffic did not originate by a request from within the firewall.

If a meeting is on-going (with local clients) and a third party succeeds in compromising the authorized server and successfully locates the clients within your firewall, the third party could send data that would reach the local clients. However, this data will be rejected for one of three reasons:

1. The data was not encrypted with the encryption key required for the meeting. The encryption key is randomly chosen and is either stored encrypted on the server or located externally on another server.
2. The data is not valid meeting data and is therefore thrown out by the client.
3. Any buffer overflow attempt will fail because of built-in safety mechanisms guarding against this in Marratech client and server.

Using SIP and H.323

SIP (Session Initiation Protocol), enables the Manager to access a SIP phone or gateway. A SIP gateway provides PSTN (landline and mobile telephone) access and access to other IP telephones. Usually, the SIP gateway access requires a subscription from the gateway provider.

SIP traffic between Marratech Manager and the SIP gateway is not encrypted (this is unfortunately not supported by SIP or most VOIP solutions), so placing Marratech Manager as close to the SIP gateway as possible is recommended. Traffic between the SIP Gateway and, for example, your mobile phone, is not encrypted. Choose a SIP gateway you trust.

The H.323 functionality enables the Marratech Manager to invite an H.323 endpoint in an ongoing Marratech meeting. This connection, done from the server towards the end point is not encrypted. SIP and H.323 require a series of ports that need to be configured in your firewall, if external access is required. These, and other hints and tips, are available on the Marratech User Forum.

API and Remote Nodes

Communication between the API, Remote Nodes and the main (Central Node) Marratech Manager is also encrypted. Control information is encrypted through SSL while real time media uses the same encryption scheme as the Marratech clients.

Buffer attacks

Marratech has taken significant precautions against buffer attack vulnerabilities (for example, Code Red virus) . This vulnerability has been secured by Marratech's choice of protocols, a strong focus on security and the use of the Java language. The latter offers a sandbox model, which makes it immune to these kinds of attacks.

Conclusion

By providing the market with unique, versatile firewall and NAT abilities and by using end-to-end encryption, authentication and locking mechanisms in its software solution, Marratech has done a thorough implementation of a secure group collaboration environment on many levels.

Marratech's approach to security for real time group collaboration is unmatched on the market today.

Marratech Inc • 6 Dumont Place • Morristown • NJ 07960 • USA
Phone: +1 888 WORK BETTER or +1 888 967 5238
Marratech AB • S:t Eriksgatan 115/Box 6791 • SE-113 85 Stockholm • Sweden
Phone: +46 8 555 118 40
www.marratech.com • sales@marratech.com