VoIP Voice Traffic Encryption

UniVoIP deploys Mitel Phones and MiNet™, an unpublished proprietary standard that use digitally encoded name/value pairs to transmit information. The secure MiNet and SRTP privacy and confidentiality benefits apply specifically to Internet based connectivity between your company phones and our datacenters.

Voice Communication Encryption

At UniVoIP, all voice packets passed between the remote IP phone and UniVoIP data centers are encrypted using the Secure Real-Time Transport Protocol (SRTP) with 128-bit AES encryption. SRTP is a security profile for RTP, which is the industry standard for securing voice streams over IP. SRTP adds confidentiality, message authentication and replay protection to that protocol. SRTP protects VoIP traffic because it can be used with header compression, and it does not affect Quality of Service (QoS). SRTP also insures compliance with Federal standards for FIPS 140-2 Certified Encryption for signaling as well as the voice traffic is being met. In addition, Mitel SRTP meets the requirements for the Department of Defense PKI digital certificate compliance.

Signaling Messaging Encryption

At UniVoIP, we are protecting the privacy and integrity of the MiNET signaling messages. Call-signaling traffic is sent across the network using a 128-bit AES TLS/SSL encrypted version of MiNET. This secure MiNET traffic is only accepted from devices that have been authenticated within UniVoIP data center farms.

At UniVoIP we encrypt the Signaling and the Voice traffic on all Mitel phones at no additional cost.

Are your calls secured?

If you have a SIP-based VoIP phone system – chances are they are not.

Contact your current provider and ask if they encrypt your Voice Communication AND Signaling Messaging?

Fact (#1)

Most VoIP Phone Service Providers are deploying SIP based Phones. SIP is a widely used standard with its content transported as readable text. Unfortunately this makes it an attractive target for hackers.

Fact (#2)

Broadband service-providers have been known to search for SIP messages (signaling messages) and RTP packet, containing the voice conversation, and restrict their use on their networks.

Fact (#3)

Most Internet based VoIP Service Providers are NOT Encrypting the voice traffic nor signaling message, making your conversation pretty much open to the public Internet.

Questions?

Want to learn more about securing your voice traffic? Please visit univoip.com or give us a call at 1-855-UNIVOIP (864-8647).