General information regarding SIP

The Session Initiation Protocol (SIP) is a signalization protocol for the setup, modification, and termination of sessions between two or several communication partners. It uses TCP on port 5060 to negotiate which dynamic port range is to be used between the endpoints when setting up a call.

Since opening all ports within the dynamic range would cause a severe security issue, the firewall is able to handle SIP traffic on an intelligent basis. This is achieved by means of a special connection tracking helper monitoring the control channel to determine which dynamic ports are being used and then only allowing these ports to pass traffic when the control channel is busy.

For that purpose, you must specify both a SIP server network and a SIP client network definition in order to create appropriate firewall rules enabling the communication via the SIP protocol.

When to use SIP Protocol Support

Because essentially all SIP implementations are different (depending on the VoIP provider), it is not always necessary to use SIP Protocol Support on the UTM. In many cases, simple firewall rules allowing outgoing traffic on port 5060 are all that is required for SIP to work correctly.

Most SIP based VoIP solutions offer a 'NAT helper,' such as:

- STUN (Session Traversal Utilities for NAT)
- ICE (Interactive Connectivity Establishment)
- TURN (Traversal Using Relay NAT)

If your VoIP implementation uses STUN, ICE, or TURN, you should not use the UTM SIP helper. Enabling it in combination with any of these protocols will likely cause calls or registrations to fail. In this case, a firewall rule allowing traffic from your internal SIP client networks to access your external VoIP server on port 5060 is all that is normally required for SIP to function correctly.

Some implementations of SIP involve an internal PBX server (that the phones register to), as well as an external one (to which only the internal server communicates directly). If this is the case, SIP Protocol Support is only required if your VoIP solution involves registration between your internal PBX and the external server (VoIP Provider). If your SIP implementation is registrationless, an outgoing firewall rule should be used instead.

If SIP clients on your internal network communicate directly with an external server, and no NAT helper protocol (such as STUN, ICE, or TURN) is implemented, you should enable UTM SIP Protocol Support.