

## Why Firewalls Are Not Enough

Firewalls and Unified Threat Management (UTM) are ubiquitous in today's networks as they offer comprehensive protection against blended threats. But these devices offer little coverage in VoIP security protection. Firewalls and UTM focus on data security, email, web, worms, trojans and so on. None of these data applications are "real time", where VoIP requires immediate application of security policies.

In addition, the inherent function of firewalls is to deny all unsolicited traffic. Whereby, the act of making a phone call is an unsolicited event, thus, firewalls can be counterproductive to an effective VoIP deployment by denying VoIP traffic.

Furthermore, firewalls do not provide the SIP protocol addressing needs to rewrite and re-address proper SIP signalling and media negotiations. The purpose of an SBC is to enhance the "real time" VoIP security policies to the existing security infrastructure, and focus on establishing reliable SIP communications instead of just "poking holes" in your firewall to allow phone calls through at the risk of breaching security.

