Best practices for security with Sigma® Core

Deploying Unified Communications while maintaining a secure IP network can be a challenge considering the many threats seen in the industry, such as network intrusion, denial of service attacks, hijacking/fraud, and eavesdropping. On IP networks, voice, video and chat traffic is subject to snooping or espionage just like any other IP traffic. Even when traversing trusted networks, it is important to consider your risk and determine if encryption is necessary. Fortunately, REDCOM's Sigma Core software offers a robust set of industry-standard security features that can be easily integrated with your existing network topology. Sigma Core has passed rigorous tests by the US Defense Information Systems Agency (DISA), delivering added peace of mind absent from other UC solutions.

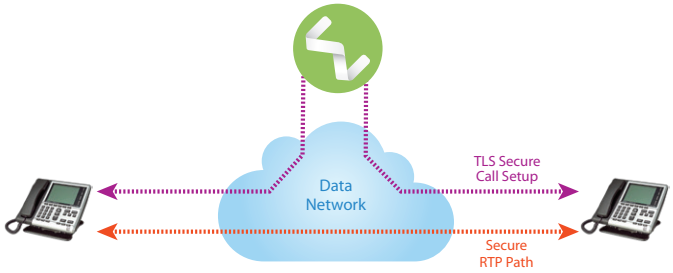
Encryption

Real-time traffic such as VoIP is at risk for evesdropping and cyberattacks, made possible by freely available tools that allow anyone to listen in on unencrypted VoIP calls. When VoIP calls are initiated in the clear (without encryption), it is easy for criminal enterprises to identify user credentials, which can be spoofed in the future to commit long-distance/international toll fraud. Fortunately, the industry has defined multiple standards (some open, some proprietary) to encrypt data. Open-standards based encryption technology will maximize interoperability between disparate network components (and virtualized functions), so let's look at some open standards.

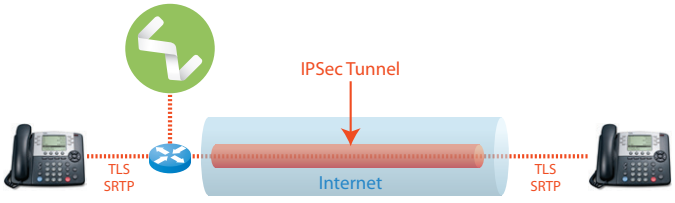
Transport Layer Security (TLS) is a widely-deployed industry standard for encryption of data. For VoIP traffic, this can provide an encrypted channel to ensure that calls are set up securely. TLS requires the server to have a certificate issued by a trusted certification authority (CA) and the client must recognize that CA. This prevents users from inadvertently connecting to rogue servers. When mutual authentication is enabled, both the client and server must present certificates as part of the TLS setup. Mutual authentication protects the server from unauthorized clients connecting. Both setups use digital certificates and public key cryptography. Sigma Core includes TLS support and the ability to add certificate authorities and revocation lists. Sigma Core is flexible enough to allow TLS to be configured on a per-subscriber and per-SIP trunk basis through the use of multiple TLS profiles.

Secure Real-time Transport Protocol (SRTP) is an industry standard used to encrypt real-time communications data such as streaming voice (RTP). The main security goals of SRTP are to ensure confidentiality and replay protection of the media payload and the integrity of the entire media packet. When used in conjunction with TLS, it creates full end-to-end call security. Sigma Core's built-in media server offers full SRTP support that is quick to configure on both end instruments and SIP trunks.

Internet Protocol Security (IPsec) is an open industry standard for data encryption. Routers can use IPsec to create an encrypted Virtual Private Network (VPN) tunnel between two hosts or networks. Once an IPsec tunnel is established, traffic can pass normally between hosts or networks. TLS and SRTP can be used in addition to IPsec to simultaneously deliver dual encryption for traffic over untrusted networks.



Secure VoIP call with both call setup information and voice encryption.



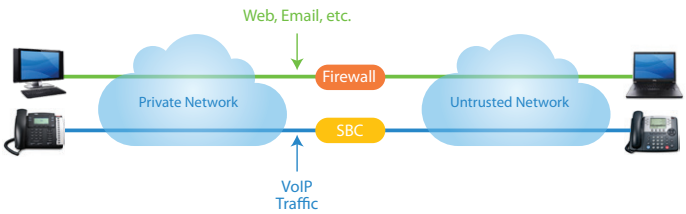
IPSec Tunneling adds an additional level of security for calls transiting non-secure networks

VoIP-Aware Firewalls and Session Border Controllers (SBC)

Traditional firewalls have static configurations and allow certain traffic to flow through specific ports to defined destinations. This approach is problematic because of the dynamic nature of VoIP protocols that make it impossible to create a set of predefined static filters to match each session. SIP, for example, does not natively handle Network Address Translation (NAT). Some firewalls are aware of VoIP and will dynamically open and close known ports, rather than leaving them pegged open as a normal firewall would, but this functionality is not supported in many firewalls, and where it is, generally only small VoIP traffic volumes are supported.

An SBC, on the other hand, implements a SIP back-to-back user agent (B2BUA) with full awareness of the call state, and can be equipped to handle larger VoIP traffic volumes. SBCs perform many functions including Network Address Translation (NAT) which can be used for Topology Hiding – obscuring information about addressing on your network. They can be configured with traffic thresholds to prevent traffic overloads for core elements of your network during congestion or during an attack such as Distributed Denial of Service (DDoS). They can support transrating (ability to convert packetization rate) or transcoding (ability to convert voice Codecs) which can allow you to compress or uncompress traffic at your SBC instead of tying up resources on a core device at your network.

An SBC would generally be placed parallel to a firewall, at the edge of a network. VoIP traffic is generally directed to/from the SBC, with other data traffic generally directed to/from the firewall.



Private IP networks carrying voice should be defended by both a Firewall and SBC.

Best practices

Here are some recommended steps to secure your network and services for Unified Communications:

- Identify networks to which you attach, where you have no control of what devices are connected, and no control over what traffic is generated (such as the public internet, or peering connections with other parties). Consider these untrusted networks. Assume that you are subject to malicious activity from these networks.
- Audit traffic patterns to and from untrusted networks.
- Collect detailed logs.
- Set up alarms for traffic thresholds.
- Identify traffic types that must pass to and from these untrusted networks and gather relevant details (traffic type, source/destination IP addresses, aggregate bandwidth, ports).
- Evaluate the security features available with components of your network (i.e. firewall, UC platform, routers, SBC, etc.) remembering that you may need to prioritize certain traffic types (such as VoIP) during times of network congestion.
- Identify gaps in the security features of your current infrastructure and find third-party solutions where needed (i.e. implement an SBC to block malicious traffic and forward VoIP traffic to appropriate ports on a per-call basis).
- Keep software up-to-date with current security patches.
- Use SIP registration with digest authentication.
- Use Ethernet port security (sticky MAC address for each Ethernet port).
- Consider encryption (TLS/SRTP/IPsec) for traffic across untrusted links.

Talk to the experts at REDCOM

Whether your UC needs are big or small, it is always important to consider how to secure your deployment. Don't worry if some of the terms or concepts discussed are unfamiliar, because we have a team of experts ready to help configure the right REDCOM solution for your needs. Contact us at sales@redcom.com or call us at 585.924.6500.