Simplifying the multiple VoIP enclave environments with REDCOM® Sigma®

Environments that require multiple VoIP enclaves can be difficult to manage, administer, and configure since each enclave is often hosted by a separate VoIP call controller due to the differences in setup, configuration, and security.

With REDCOM Sigma® call and session control software, seemingly disparate enclaves can be simplified using virtual PBXs. This allows for each separate enclave to have its own virtual instance of a dedicated, fully customizable, VoIP call controller while at the same time only using one software license, one support contract, and one incoming network connection that can to be secured.

Standard layout of a multi-enclave environment

For the sake of having customized and dedicated VoIP infrastructures, the hardware, licenses, management, and maintenance are duplicated thus increasing both cost of the network and the cybersecurity attack surface, or the number of points that a hacker can attack the network. Another problem is that often each enclave may be under a different financial budget, thus portions of the network can become older and less secure than others, depending on which budgets get approved.

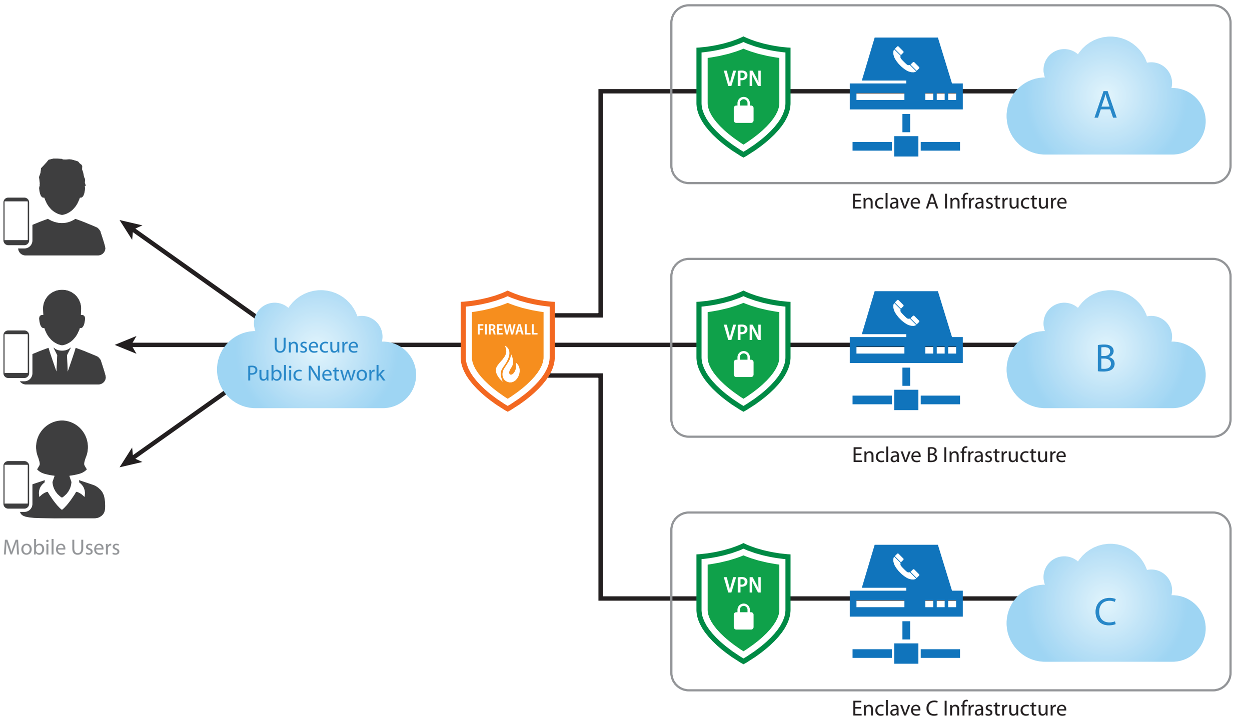

Figure 1 Typical Configuration of a Multi-Enclave Environment

How REDCOM Sigma simplifies the multi-security network

REDCOM Sigma is a hardware agnostic, small footprint, VoIP call control software platform focusing on secure and interoperable communications. In the world of secure SIP and VoIP, REDCOM Sigma is a true back-to-back user agent (B2BUA) that can independently handle and manipulate both the signaling and media streams.

REDCOM Sigma combines a powerful set of call control and media server features such as conferencing, transcoding, voicemail, and XMPP chat. It also offers the following sophisticated security capabilities that are beneficial in a mobile access environment including:

- **Topology Hiding:** Allows the switch to conceal identities of users and services that are behind it. For example, the phone's IP address of key personnel can be removed from all outgoing SIP messages and replaced with that of a media engine in REDCOM Sigma. Phone numbers can also be translated/hidden from users outside of a given network.

- **Security Policy Transcoding:** Ability to terminate an incoming secure call with a given policy and re-establish it with another security policy. This allows users to connect to networks with varying encryption capabilities.

- **Rules-Based Connections:** Provides for the administrator to create rules for determining if a given connection should be trusted and allowed to connect to another network. This is key when information needs to be passed between two or more varying security domains.

- **SIP and SDP Manipulation:** Alter SIP and SDP messages in real time to handle any protocol connectivity issues between systems.

- **Multi-Security Level Conferencing:** Multi-party conferencing system with the ability to inform members of a conference system when a user with a varying security policy has joined or left the conference.

- **Multi-Tenancy:** Ability to create logically separated and independent sites.

- **End User Device (EUD) Provisioning:** Ability to provision end instruments including built-in templates for Cisco, TEO, Polycom, and REDCOM® Secure Client (available for Android™, iOS™, and Windows®).

- **Integrated Firewall:** Control incoming and outgoing network traffic based on security rules.

- **FIPS 140-2 Validated:** REDCOM Sigma only uses FIPS 140-2 validated encryption algorithms. This allows the software to also act as the inner encryption component for creating the inner TLS/SRTP tunnel.

- **JITC Certified:** REDCOM Sigma is on DISA's Approved Products List (APL) and has been interop tested as a local session controller (LSC) with all other major call controllers such as Cisco, Avaya, Unify, Genband, and NEC.

The multi-tenant environment

The multi-tenancy capability within REDCOM Sigma allows network administrators to create independent VoIP environments that are logically independent from each other (Figure 2). Each tenant site operates as if it was independently created with its own set of users, resources, and capabilities dedicated directly to it.

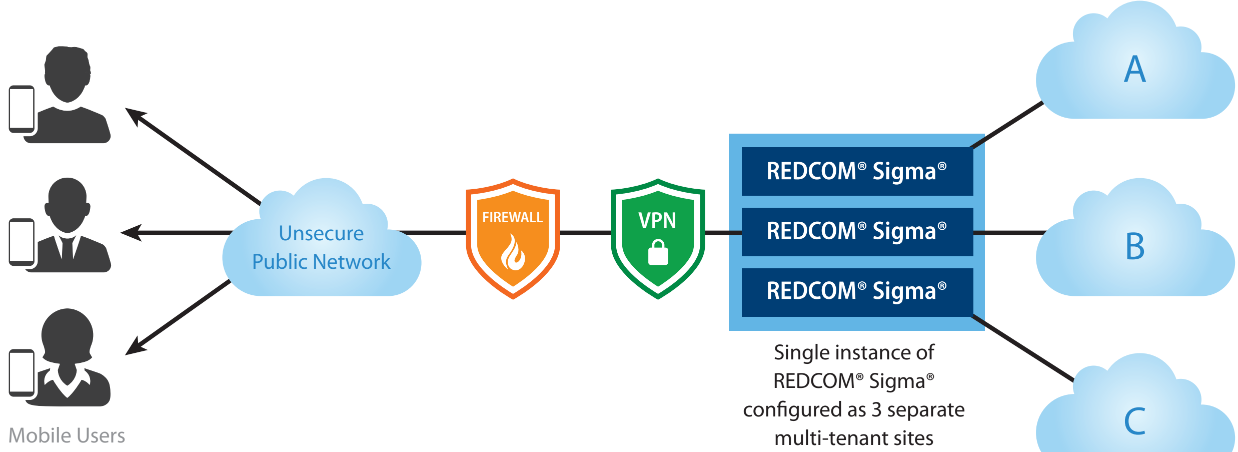

Figure 2: Sigma Core Configured as Three Tenant Sites to Logically Separate Enclaves

Isolation within tenant sites

To the members in Tenant Site A, for example, it appears that there is only one instance of REDCOM Sigma running just for them. Members in Tenant Site A can only talk to others as defined by the rules of their own tenant site. Such rules may restrict users to access other members of Tenant Site A or allow them access to external networks. The same is also true for the other Tenant Sites (B and C). Each instance is also capable of having its own rules for connecting to external networks that can be based on several call characteristics including ANI, URL, or budgeting (i.e. no more than 3 simultaneous connections to/from a given network).

Members from a given tenant site are unable to view or modify the resources that belong to another tenant site. These resources include lines, trunks, users, translator tables, media files, themes and more. From a network perspective, a network admin would simply treat each tenant site as an independent VoIP switch. Each tenant site can manage/admin itself, create SIP registrants, have its own dial code tables, etc… In other words, each tenant site can and should be treated as if it were a stand-alone site.

The independence of each tenant site allows for each site to be configured with a unique security policy, PKI certificate authority, call configuration rules, and even appearance. For example, each tenant site can have its own custom log-in screen along with different log-in credentials. Each site can also define what permissions each user has. For example, some users may have access to monitoring capabilities while others may only have access to see their own activity.

Additional key benefits

Using REDCOM Sigma to implement a multi-tenancy, multi-enclave environment also affords the following benefits:

- **Single point of updates:** Since all tenant sites stem from a single instance of REDCOM Sigma, only one software update is needed.
- **Simple licensing:** Network admins only need to manage the software license of one software instance of REDCOM Sigma regardless of the number of tenant sites.
- **Simplified Management of Resources:** Tenant sites can grab resources (i.e. lines, trunks, voicemail boxes, etc.) and claim them for their use. If more resources are needed, simply grab them from the pool of resources. Resources can also be returned to the pool for other tenant sites to grab and use.

Conclusion

In an era where cybersecurity is central to any network, REDCOM Sigma's security features and ability to simplify complex network schemes allow for network administrators to deploy with confidence. The result is a network that is highly manageable, secure, and most of all, responsive to constantly evolving needs of military and government agencies.

For more information on deploying REDCOM Sigma, please visit www.redcom.com or call our Government and Commercial sales teams at 585-924-6500 to discuss your application.