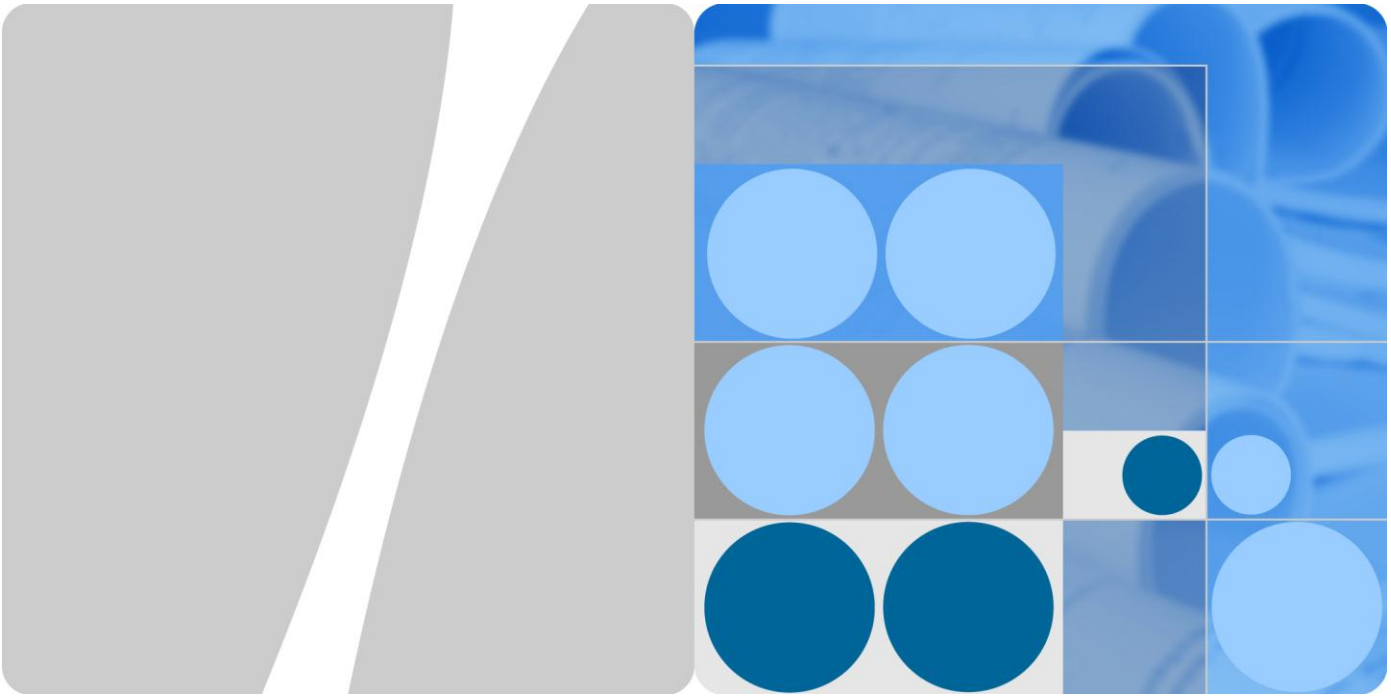


华为融合通信解决方案 V3.0
安全技术白皮书

文档版本 V1.0

发布日期 2016-04-28

华为技术有限公司

商标声明

 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

前　言

概述

本文档以华为融合通信解决方案特性和安全面临的挑战为背景，从安全策略、安全架构和产品安全性几方面详细描述了融合通信解决方案的安全能力。

读者对象

本文档主要适用于以下工程师：

- 研发、技术服务人员
- 行销人员、Marketing 相关人员

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示有高度或中度潜在危险，如果不能避免，可能会导致人员死亡或严重伤害。
 警告	表示有低度潜在危险，如果不能避免，可能会导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果不能避免，可能会导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

目 录

1 简介

1.1 华为融合通信系统概述

华为融合通信解决方案（即EC解决方案）是华为公司推出的一款全新的企业通信产品，基于SIP协议、开放软交换平台设计，提供多业务构建及多终端接入能力，面向企业客户提供高可靠、易部署的融合通信解决方案。

EC解决方案覆盖SOHO、中小型企业、大型/超大型企业等各种规模用户。面对企业日益增长的协同办公需求，EC解决方案融合语音、数据和视频，通过固定电话、移动电话、电脑、平板电脑等多种终端协作，为企业用户提供IP语音、协同应用、移动办公等全方位的应用，使企业用户可以在任意时间、任意地点，采用多种通信设备安全便捷地接入企业业务平台，提高企业办公效率，提升企业员工、合作伙伴和客户的体验，协助企业提升整体竞争力。

1.2 架构描述

EC解决方案采用分层、融合、安全和开放的系统架构。

EC解决方案包括终端与接入层、呼叫管理层、业务应用层、管理维护层和安全保障层。通过开放的平台和接口，提供与第三方系统对接的能力以及二次开发的能力，如图1-1 所示。企业用户可在安全、可靠系统的保障下，实现高效、协作办公。

图1-1 融合通信解决方案架构

2 EC 解决方案安全概述

2.1 EC 解决方案安全面临的挑战

系统部署在企业IP办公网络上，由于IP网络的开放性和融合通信业务的多样性，所以，相比传统的语音通信，融合通信面临更多的安全风险，这些安全风险包括：

- 在IP网络上传输的语音通话内容是否会被窃听？
- 引入融合通信后，找联系人、沟通协作、共享文件、会议协作等都变得更加便捷，但带来极度方便性的同时，是否会造成企业信息泄露？
- 融合通信使通信变得更加方便，实现了“看见即可通信”，但方便的同时，是否会造成盗打、冒打、通信资源滥用等问题？
- 融合通信在办公PC上引入了软终端，会否在办公PC上引入新的安全隐患？
- 融合通信引入区别于PC的独特终端IP Phone，是否会对企业原有的终端准入机制有影响，IP Phone接入点是否会成为一个安全隐患点？
- 如果在互联网也开展融合通信业务的话，在互联网上的融合通信业务是否会被恶意攻击者窃听或篡改？

综合华为公司在通信领域、IP网络领域、安全领域、IT领域多年积累的研发和服务经验，EC在规划设计之初即充分分析了EC的安全风险，并实施了相应的安全设计，最大限度地保证融合通信业务的安全性，确保客户在统一的IP办公网络平台上享受融合通信的方便性、业务多样性的同时，仍能达到高标准的安全性。

本文从EC的安全架构出发，从不同维度分析阐述EC在各节点、各层次上的安全设计和安全技术。

2.2 EC 系统安全概述

安全对通信产品和系统非常重要，尤其是面向企业客户的通信产品。为保证EC解决方案的安全性，我们参考了许多国内和国外的安全标准，如TCSEC、ITSEC、ISO 17799、ITU X.805等，并借助在运营商成功运作的网络和设备的安全运营经验，针对EC解决方案分层提供了安全解决方案。

- 应用层安全解决方案保护EC包含的各种应用程序，如：访问控制、密码安全等，融合通信的应用层主要是BMU、eServer、CDRServer、话务台服务器和数据会议服务器对外提供的服务。应用层的安全维护是基于BMU、eServer、CDRServer、话务台和数据会议等各项业务的应用安全来实施的。
- 系统层安全解决方案保护操作系统、数据库及应用程序依赖的服务。
- 网络层安全解决方案保护整个网络正常运行。
- 管理层安全解决方案通过日志、补丁等管理使得整个系统提供的安全措施得以执行。

图2-1 安全解决方案

3 EC 安全技术

3.1 应用层安全

EC解决方案是运行在基于IP的办公网络，语音、消息、视频等业务数据都在一个相对开放的IP网络上传输。EC解决方案提供多种业务安全管理机制，保障通信业务安全。

3.1.1 内网接入安全

融合通信业务需要从内网接入的终端主要有两大类，一类是运行在PC或移动终端上的软客户端，另一类是融合通信特有的软硬件一体的IP Phone终端。

1、IP话机通过802.1x实现准入认证，支持两种802.1x认证方式：EAP-TLS和EAP-MD5。IP话机支持多证书导入，实现身份认证。

2、Desktop Client、Mobile Client使用帐号和口令认证，遵循企业自身部署的内网接入安全策略。

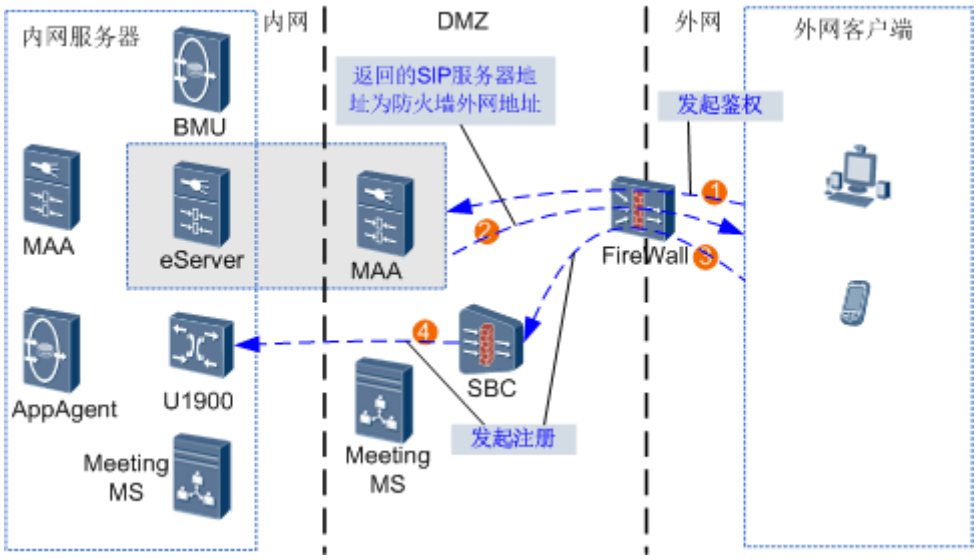
3.1.2 外网接入安全

融合通信业务需要从公网接入的终端主要是运行在手机、移动终端或PC上的软客户端，利用公网接入安全技术，在任何网络可达的地方，融合通信终端都可以接入企业融合系统，开展融合通信业务，突破了企业沟通协作在时间和空间上的限制，带来了极大的便利性。

企业划分为DMZ区和企业内网，两个区域属于不同的网段，通过企业内网防火墙实现NAT（Network Address Translation）隔离。企业边缘侧部署外网防火墙，所有外网终端必须通过防火墙进入DMZ区。SBC设备跨接企业外网和DMZ区并通过外网防火墙实现NAT穿越。通信数据在公网上加密传输，保证数据安全性，避免数据被窃取。外网接入安全支持SBC部署于防火墙之后方式。

SBC部署于防火墙之后，组网如图3-1所示。客户端上配置的eServer/MAA地址为经过防火墙NAT转换后的防火墙外网地址。

图3-1 SBC 部署于防火墙后的场景



外网客户端鉴权注册原理说明：

1) 客户端通过防火墙向 eServer/MAA 发起鉴权请求。

2) eServer/MAA 将 SIP 服务器（即 U1900,USM 系列统一网关）对应的防火墙外网 IP 地址发回给客户端。

3) 客户端向防火墙的外网 IP 地址发起语音注册请求。

4) 防火墙通过 SBC 的 SIP 代理注册端口，将注册消息转发到内网 SIP 服务器进行代理注册。

3.1.3 端到端的信令、媒体加密

EC系统中，涉及语音通信的各部件（包括IP-PBX、SBC、IP话机、PC软终端、移动软终端等）均支持业界标准的信令加密协议（SIP TLS）和媒体加密协议（SRTP）.

- 支持终端和服务器之间、终端和统一网关之间、服务器和服务器之间、服务器和统一网关之间所有信令交互时通过TLS加密，保证信令传输安全性。 融合通信各终端发起通话时，先对服务端的数字证书进行认证，并通过数字证书上的公钥利用非对称加密算法协商出信令加密的密钥。各部件间通过SIP信令交互时，使用协商出的密钥对信令加密后传输，确保信令无法被窃听。
- 媒体流支持AES128算法的SRTP加密传输，保证语音和数据传输安全性。

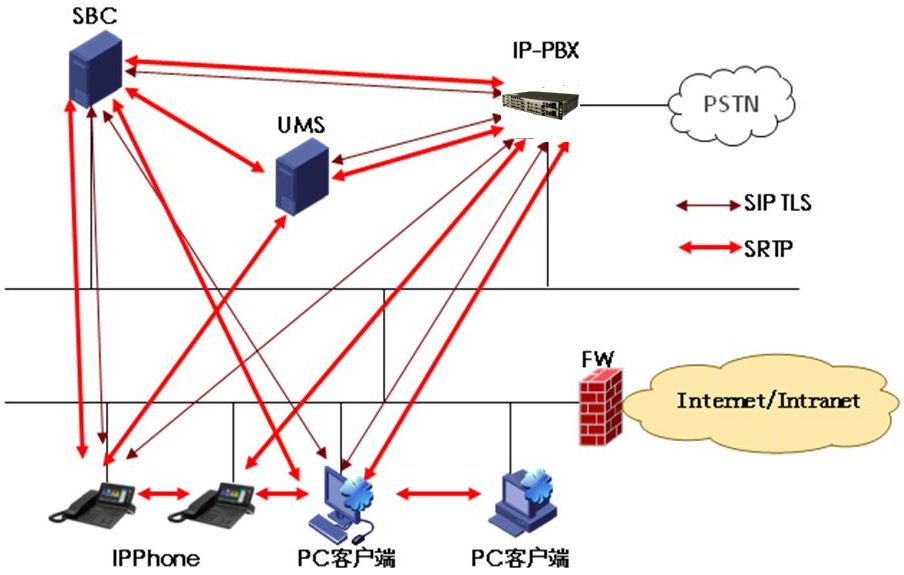


图3-2 EC 端到端的信令、媒体加密

信令加密按照业界标准RFC 3261、RFC 3263、RFC 3853、RFC 4568、RFC5246实现，其原理如图3-3所示，IP话机或软终端发起通话时，先与融合通信业务系统通过数字证书进行相互认证，并通过数字证书上的公钥利用非对称加密算法协商出信令加密的密钥，然后再通过协商出的密钥对所有的交互信令进行加密传输，确保信令无法被窃听.

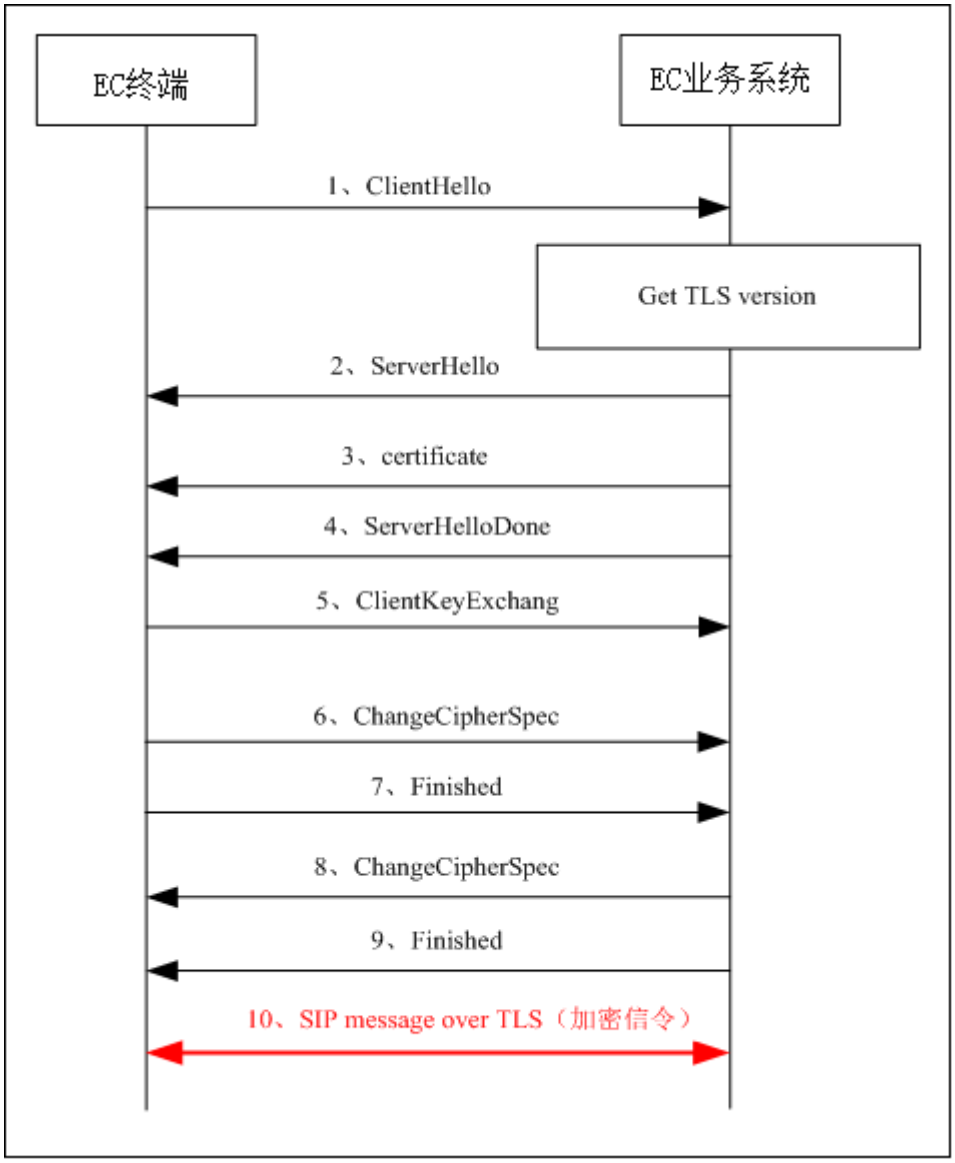


图3-3 SIP TLS安全机制

媒体加密按照业界标准RFC 3853、RFC 3711、RFC 4568实现，其中，两个融合通信终端间建立加密媒体通道的流程图如图3-4所示。两个融合通信终端通过加密的信令（SIP TLS）交换媒体加密的密钥，然后利用该密钥对语音媒体加密后进行传输，确保语音媒体无法被窃听。

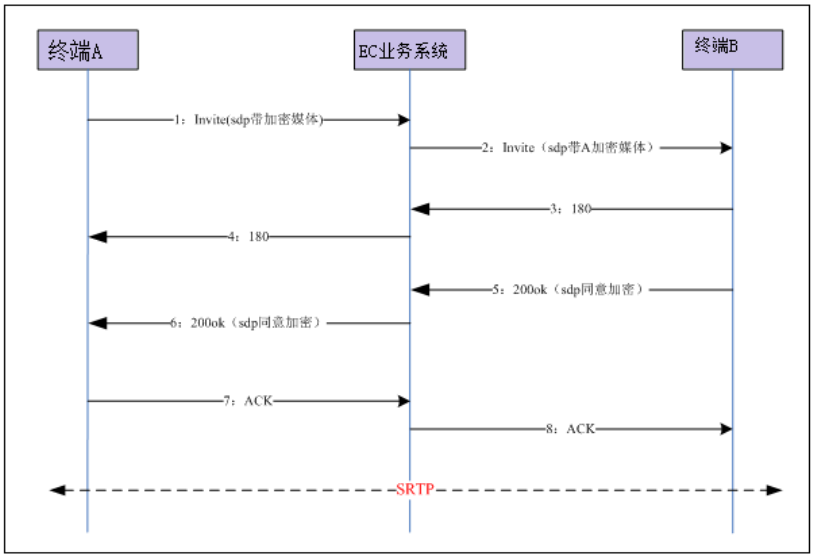


图3-3 融合通信终端间进行媒体交互时的 SRTP 安全机制

3.1.4 业务接口认证与鉴权

EC提供了丰富的业务，但这些业务均不是无限制提供的，用户使用这些业务的前提是必须经过认证，认证数据在不可信网络中传输时，均进行了加密传输,主要加密类型为HTTPS加密。认证数据在EC系统里存储时，均进行了加密存储，其中不需要还原的口令数据采用了SHA2-256不可逆加密算法，密钥交换算法采用RSA 2048。

USM提供白名单功能，其他服务器需要访问USM时，如果其IP地址不在白名单内，将无法访问。有效保障核心服务器的访问安全。

业务访问接口	认证方式	权限控制机制（鉴权）
软终端登录访问融合通信业务	帐号、口令认证	根据帐号开户信息，进行该帐号的 EC 业务权限控制
软终端的语音业务接口	标准 SIP 协议的帐号、口令认证，支持 SIP Digest 等认证机制	根据帐号（电话号码）开户信息，进行语音业务的权限控制
IP Phone 的语音业务接口	标准 SIP 协议的帐号、口令认证，支持 SIP Digest 等认证机制	根据帐号（电话号码）开户信息，进行语音业务的权限控制
手机客户端登录	帐号、口令认证	根据帐号开户信息，进行该帐号的 EC 业务权限控制
融合通信用户自助服务接口	帐号、口令认证	根据帐号开户信息，进行该帐号的 EC 业务权限控制

开放给第三方应用访问融合通信业务能力的接口	帐号、口令认证	对第三方应用可分三级进行权限控制
融合通信用户访问语音留言的接口	帐号、口令认证	不涉及
会议系统的入会接口	会议 Passcode 认证	区分会议主席和普通与会者进行权限控制

3.1.5 融合通信业务数据加密存储和传输

除语音外，EC提供了各种丰富的业务（如通讯录、IM、会议等）。类似语音业务，这些业务数据在IP网络上传输时，EC也提供加密机制，以确保融合通信业务数据传输的安全性，如下表所示。

分类	子类	协议
音视频呼叫	信令	SIP over TLS
	媒体	SRTP
多媒体会议	多媒体会议	AES256 加密传输
企业地址簿	LDAP 接口	LDAPS
	AppAgent 接口	HTTPS
	eServer 接口	AES128 加密传输
	MAA 接口	AES128 加密传输
IM 消息	eServer 接口	AES128 加密传输
	MAA 接口	AES128 加密传输
群组	eServer 接口	AES128 加密传输
	MAA 接口	AES128 加密传输

- 其他采用加密存储和传输的敏感数据如下：

1. 终端和服务器之间、服务器和服务器之间的访问口令加密存储。

2.终端和服务器之间、服务器和服务器之间认证用的密钥加密存储。

3.数据会议接入密码加密存储。

4.终端和服务器之间、服务器和服务器之间的访问口令加密传输。

5.话单服务器和统一网关之间的话单传输通道支持TLS加密，统一网关连接话单服务器支持口令鉴权。

6.敏感数据存放在数据库或配置文件中，数据库和配置文件具有访问控制机制，仅提供给操作系统管理员或关联应用程序的数据库帐户访问，其他用户无法访问。

3.1.6 数字证书安全性

- 数字证书中的私钥文件的加/解密口令支持加密存储，且为强口令。
- EC解决方案支持数字证书替换，企业可以自己定制口令并向证书机构申请证书，替换系统缺省证书，数字证书遵循X.509。
- 采用数字证书认证的接口有：

  浏览器访问U1900系列网关的web接口

  浏览器访问BMU/USM的Web接口

  会议客户端访问Meeting MS的接口

  话务台客户端访问话务台服务器的接口

3.1.7 业务权限控制

EC解决方案支持对每个用户的呼叫业务权限进行控制，根据该用户的业务范围配置用户的呼叫权限，有效避免电话盗打等情况，保障企业利益。

BMU是EC解决方案的业务管理系统，通过连接多个统一网关、CDRServer、话务台服务器，提供单个和批量管理号码、帐号、会议等业务以及自助服务等功能。BMU系统默认具有系统管理员角色和普通用户角色。BMU管理员也可以创建自定义的角色，例如维护员角色、操作员角色。

3.1.8 通讯录访问权限控制

管理员可以为企业用户设置不同的级别（最多20个级别）。设置用户级别后，高级别用户可以查看同级或低级别用户的联系人信息，低级别用户不能查询到高级别用户的联系人信息。

3.1.9 敏感词过滤

在发送即时消息时，当消息内容精确匹配到系统中定义的敏感词时，接收方用“*”替代显示。企业管理员可以设置需要过滤哪些敏感词。

3.2 系统层安全

EC解决方案的业务部件和管理部件依赖于通用的操作系统（Suse Linux 11或Windows 2012 Server）和通用的数据库（Oracle 11g或SQL Server 2012）。EC在出厂的时候已对这些通用的OS和DB打上了供应商提供的最新补丁。

另外，EC还根据业界最佳实践，对通用OS和DB进行了安全加固操作，并提供了加固指导书。Suse Linux的安全加固包括：系统服务安全加固、内核参数安全加固、协议栈安全加固、文件和目录权限安全加固、用户帐号和环境设置安全加固、卸载多余的OS自带程序等。Oracle的安全加固包括：文件与目录安全加固、数据库安全参数设置、用户Profile安全加固、用户权限设置、数据库审计机制设置、锁定预定义的帐号等。对于依赖Windows的EC部件，除了安全加固外，EC进行了防病毒软件的兼容性验证，并提供了防病毒解决方案，EC推荐的防病毒软件是趋势公司的OfficeScan。

3.3 管理平面安全

管理是保证业务正常开展的必要条件，任何一个系统都必须设计管理机制。同时，因为恶意攻击者通过入侵管理平面，可以控制整个系统，所以，如果管理机制的安全性设计不当，则必然会给整个系统带来严重的安全威胁。

1. EC解决方案设计了独立的管理平面，如图3-3所示，独立管理平面可确保融合通信业务使用者无法扫描到融合通信系统的管理平面，从而显著降低了恶意用户进入融合通信管理平面的风险。EC对业务和管理的协议端口进行了区分，并提供了详细的通信端口矩阵，根据端口矩阵进行防火墙访问策略配置，以实现独立管理平面。

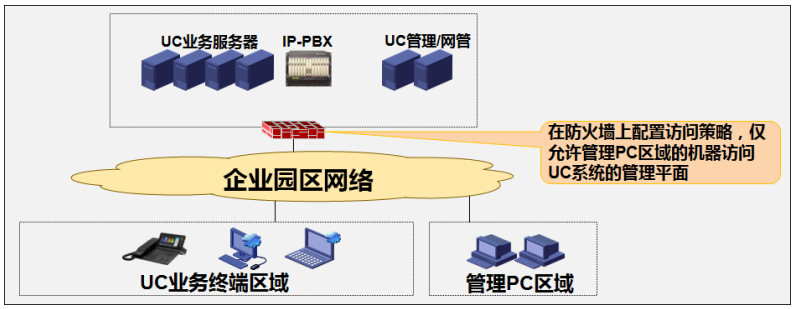


图3-4 独立管理平面

2.为确保管理平面的安全性，EC全面支持主流的安全管理协议，安全管理协议可确保管理流量在网络上安全传输，规避了管理流量中的敏感信息被窃取。

部件类型	部件	支持的安全管理协议
网管	eSight	网管协议：SNMPv3 Web 管理：HTTPS 与 U1900 系列语音网关的管理通道协议：SSH 与终端间的集中管理协议：TR069 over SSL 配置文件、软件升级包上传下载：FTPS

融合通信业务管理	BMU	Web 管理：HTTPS
融合通信业务	UMS	Web 管理：HTTPS
语音网关	U1900 系列网关	命令行：SSH 配置文件、软件升级包上传下载：FTPS Web 管理：HTTPS
	IAD	网管协议：SNMPv3 Web 管理：HTTPS 命令行：SSH 配置文件、软件升级包上传下载：FTPS
终端	IP Phone	Web 管理：HTTPS 集中管理协议：TR069 over SSL

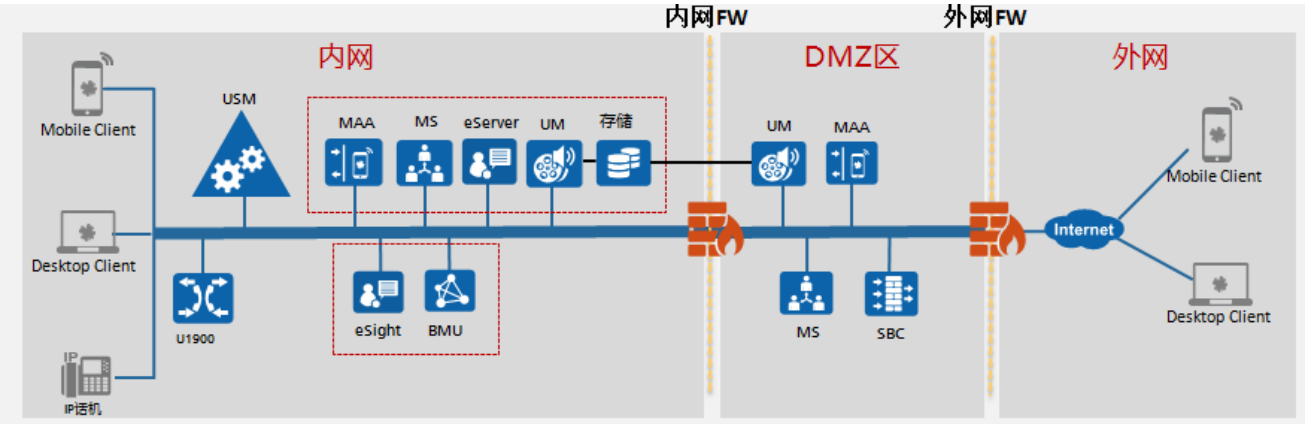
3. EC解决方案在管理平面做了严格的事前认证、事中控制、事后审计机制。在事前认证方面，EC设计了强口令机制，并设计了口令防暴力破解机制，对部分重要的管理接口还设计了口令有效期机制。在事中控制方面，EC设计了基于管理员角色和级别的权限控制机制、超时注销机制。在事后审计方面，EC提供了详细的审计信息，包括：操作时间、操作用户、操作者源IP、操作事件、被访问的资源、操作结果等；并且对各种管理事件均有详细的审计信息，存储在融合通信系统上的审计信息支持严格的访问控制，仅具有特定审计权限的管理员才可查看和操作审计信息。

3.4 IP 网络安全

EC 解决方案提供安全的组网方案，保障 IP 网络安全性。

安全组网如 3-5 所示。

图3-5 安全组网



常用安全策略说明：

- 利用网络安全基础设施，尽量采用标准SSL/IPSec VPN接入技术，在网络层为EC互联网业务提供安全保障。
- 各分支与Internet之间需要部署防火墙，对外隐藏企业内部网络拓扑。
- 提供《通信矩阵》，指导在防火墙上设置端口访问策略，关闭不使用的端口。
- 内网与外网之间，建设DMZ区域，将SBC和MAA等部署在DMZ区。内网、DMZ区以及外网之间都需要部署防火墙进行网络隔离和端口访问控制。

4 缩略语

缩写	描述	
CDR	Call Detail Record	呼叫详细记录，用于计费
DMZ	Demilitarized Zone	半信任区
QoS	Quality of Service	业务质量
RTP	Real Time Transport Protocol	实时传输协议，用来定义多媒体数据的实时传输
SBC	Session Border Controller	会话边界控制器
SNMP	Simple Network Management Protocol	简间网络管理协议
SSH	Secure Shell	安全外壳协议
SRTP	Secure Real-time Transport Protocol	安全实时传输协议
TLS	Transport Layer Security	传输层安全
USM	Unified Session Manager	统一会话管理
VPN	Virtual Private Network	虚拟专用网络