增强 IP 通信的安全性：集成式网络安全性

IP 通信技术能够将数据、话音和视频融合到同一个网络上，它不但能帮助企业降低通信成本和复杂性，还能使企业大大提高生产效率，因而对企业具有很大的吸引力。思科 IP 通信系统能够为 IP 电话、统一消息传送、IP 视频和音频会议、IP 视频广播和联络中心提供企业级解决方案。思科 IP 通信解决方案以思科 AVVID（话音、视频和集成式数据体系结构）为基础，不但能显著改善运作效率，提高机构的生产效率，还能提高客户满意度，并支持员工协作。

获得这些优势的关键是，话音网络必须是安全的，而且不会受到干扰。思科系统公司为思科 IP 通信设计了详细的安全特性——思科 IP 电话 SAFE 蓝图，该蓝图包含许多功能，包括话音和数据流量分段、入侵检测、话音防火墙和安全监控等。

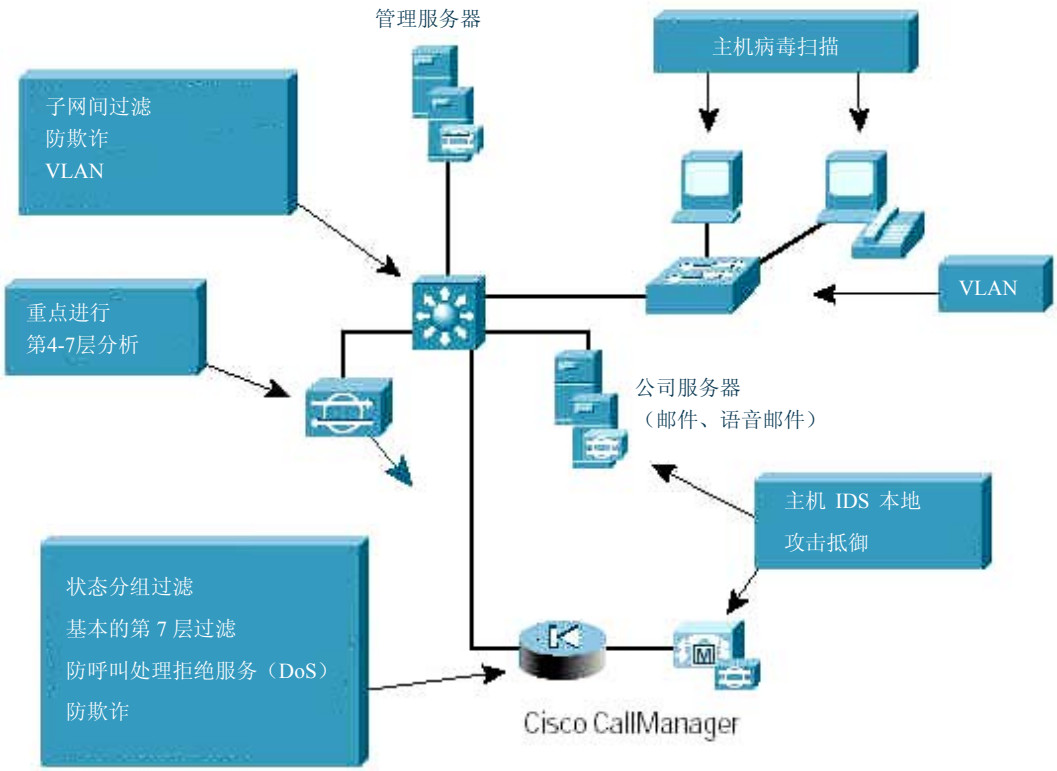
IP 通信的集成式网络安全性建立在 SAFE 基础上，能够通过 IP 电话和 IP 网络基础设施之间的紧密集成为话音资产提供全面的系统级保护。集成式网络安全性能够将数据网络的认证和加密功能扩展到话音网上，从而增强话音安全性，提高系统完整性，并更好地保持系统的效率和生产效率。

思科开发的 IP 电话 SAFE 蓝图

SAFE 蓝图的主要目的是为设计和实施安全网络提供“最佳实践”信息。SAFE 蓝图可以作为网络设计师考虑网络安全要求时的指南，其基础是深入防御安全设计方法。这种方法注重预期威胁和抵御方法，而不仅仅是规定“将防火墙放在这里，将入侵检测系统放在那里”。SAFE 蓝图的战略是用分层方法提高安全性，这样，即使某个安全系统抵御失败，也不会导致网络资源全面受损（见图 1）。

增强 IP 通信的安全性：集成式网络安全性

图 1
思科 IP 电话 SAFE 蓝图战略



SAFE 蓝图并不是提供全新的网络设计方式，而是提供了保护网络的蓝图。利用思科 AVVID，SAFE 蓝图不但能逼真地模仿企业网的功能要求，还能考虑到思科认为对有效保护 IP 通信系统至关重要的安全要素。这些安全要素由思科以多种方式提供，包括：

- **扩展的周边安全性**——该要素为控制对关键 IP 通信应用的访问提供了相应的途径，例如 Cisco CallManager，其目的是，只允许合法的 IP 电话和电话应用接入网络。拥有访问控制列表和状态防火墙以及专用防火墙设施的路由器和交换机能够提供扩展周边安全性所需要的控制。
- **话音私密性和安全连接**——为保证通信的私密性和完整性，必须防止非法人员窃听和篡改话音媒体流。第 2 层和第 3 层访问控制、状态防火墙和虚拟 LAN（VLAN）等数据网络技术可以从数据流量中分出话音流量，并防止从数据网（数据 VLAN）访问话音网（话音 VLAN）。状态防火墙是话音和数据 VLAN 之间的桥梁，只允许访问合法设备。另外，当话音流量通过 WAN 时，VPN 解决方案还可以进行加密。
- **入侵保护**——基于网络和基于主机的入侵检测系统驻留在话音网络中，能够监控安全事件并实时作出响应。利用入侵检测系统，网络管理员可以全面深入地了解网络的当前数据流和安全状况。
- **安全管理**——随着网络规模的增加和复杂度的提高，用户越来越需要用相应的工具集中管理设备、配置和安全事件。管理安全策略的先进工具还能增强网络安全解决方案的可使用性和效率。利用策略管理工具，用户能够通过浏览器界面定义、分布、加强和审查安全策略的状态。

增强 IP 通信的安全性：集成式网络安全性

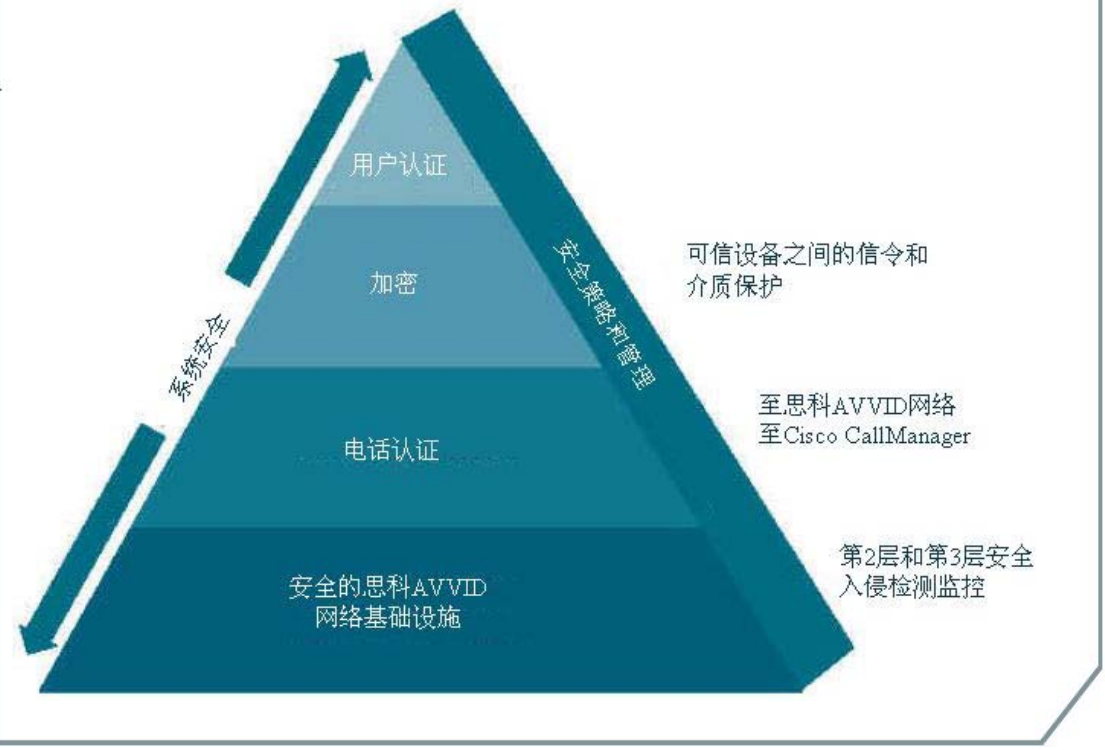
思科 IP 通信解决方案增强安全性的方向：发展集成式网络安全性

目前，思科正在既包含思科路由和交换基础设施，又包含专用安全设施的可扩展模块化平台上提供集成式网络安全解决方案。这些解决方案由思科提供安全管理软件、咨询和培训服务。

先进的安全特性，例如遭到攻击或出现误用时动态执行安全策略，能够为企业网提供实时保护。嵌入式软件解决方案，加上基于硬件的防火墙、加密和入侵检测加速器，不但能保护思科网络基础设施的安全，还能提高性能、可扩展性和可靠性。利用基于策略的管理方法，思科还能方便地规定、实施和审核企业中用户和设备的安全性。

作为新的发展方向，思科 IP 通信的集成式网络安全将通过与数据网安全功能的紧密配合提供全面的安全性、系统级保护、完整性和私密性。集成式网络安全系统不但能保护现有思科基础设施、安全系统和 IP 通信解决方案的投资，还能建立多个安全层次，最大程度地保护完整的通信系统。

图 2
为 IP 通信系统实施的思科集成式网络安全的分层方法



如图 2 所示，每个安全层次都提供特殊的安全功能，并为后续安全层次奠定了坚实的基础：

- **安全的 AVVID 网络基础设施**——以 IP 电话 SAFE 蓝图为基础，这个层次利用第 2 层和第 3 层访问控制、状态防火墙以及数据 VLAN 和话音 VLAN 的分离为下面的层次奠定了坚实的基础。该层的安全设施包括网络和主机入侵检测系统以及安全监控控制台。
- **电话认证（电话身份识别）**——能保证准确识别 IP 电话和 IP 通信应用和设备。支持识别的标准技术包括远程认证拨入用户服务（RADIUS）和终端接入控制器接入控制系统（TACACS+）、Kerberos 和一次性密码工具等认证协议，以及 802.1x、数字证书和智能卡等新技术。电话认证分两步执行。首先，电话利用 IEEE 802.1x 完成思科安全 AVVID 网络基础设施自身识别，获得

对话音 VLAN 的访问权。其次，电话利用 Cisco CallManager 完成相互识别。

电话认证层用于建立设备之间的信任关系，以防止身份盗用和中间人攻击。无论是对系统的完整性，还是后续的加密和用户认证，这种信任关系都非常重要。

- **信号和话音介质加密**——在认证层次之上，加密将在已准确识别的 IP 电话、思科 IP 通信应用和网络资源之间提供私密性。有效的信号和话音介质加密需要基于标准的强大加密功能，包括加密算法和系统级密钥管理。只有将 IP 电话、会议桥接器、话音网关以及语音邮件和统一消息传送等应用集成到安全体系结构中才能实现有意义的有效端到端加密。

  集成式网络安全还能让网络知晓信号和话音介质已经过加密，以便网络地址转换（NAT）和状态防火墙等认证网络基础设施安全服务能够与加密话音互操作。这种集成既能保持 IP 电话在拓扑和移动性方面的优势，又能提高系统安全性。

- **电话用户认证（用户身份）**——最高的安全层次是准确识别电话用户。在其它层次上，安全是嵌入在思科 IP 通信系统中的，对用户是透明的。对于想按照用户身份控制网络访问权限的机构，可以利用用户认证将集成式网络安全扩展到用户。这些增强计划将使用 RADIUS 和 TACACS+等认证协议扩展现有的用户认证功能，并将用户安全集成到网络基础设施中。

集成式网络安全性——投资保护和全面系统安全

为 IP 通信解决方案制定的集成式网络安全增强计划不但能保护现有的思科 AVVID 基础设施和 IP 通信解决方案投资，还能帮助客户将安全性提高到 TDM PBX 系统无法实现的水平。集成式网络安全不但能保护思科 IP 通信资源和传输，还能节省运作开支，并提高生产效率。

详情垂询

如果想详细了解思科IP通信和思科话音解决方案，请访问：www.cisco.com/go/ipcommunications。如果想详细阅读思科SAFE蓝图的白皮书，或者想了解思科V3PN话音和视频VPN解决方案，请访问：www.cisco.com/go/safe。

另外，思科和某些思科合作伙伴还提供全套设计、实施、咨询和外包服务，以帮助企业建立和运行安全的IP通信系统和网络。欲知详情，请访问：
www.cisco.com/go/securitypartners or www.cisco.com/go/avvidpartners。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街一号东方广场东一办公楼 19-21 层

邮政编码：100738
电话：(8610) 65267777
传真：(8610) 85181881

上海
上海市淮海中路 222 号力宝广场 32-33 层

邮政编码：200021
电话：(8621) 33104777
传真：(8621) 53966750

广州
广州市天河北路 233 号中信广场 43 楼

邮政编码：510620
电话：(8620) 87007000
传真：(8620) 38770077

成都
成都市顺城大街 308 号冠城广场 23 层

邮政编码：610017
电话：(8628) 86758000
传真：(8628) 86528999

如需了解思科公司的更多信息，请浏览 http://www.cisco.com /cn

2004 年 12 月翻译