Cisco ASA 5500 系列统一通信部署

思科® 统一通信解决方案统一了固定网络和移动网络上的语音、视频、数据和移动应用，使用户能够随时从任何工作空间轻松进行协作。

概述

思科统一通信产品可以帮助各种规模的企业简化操作、提高员工工作效率、优化通信，并提升客户服务。由于保护基于统一通信的网络免受攻击对于保持业务连续性和完整性至关重要，因此思科将安全功能内置到其统一通信产品中，并通过 Cisco ASA 5500 系列自适应安全设备增强这些产品。

Cisco ASA 5500 系列自适应安全设备是小型企业、分支机构、大企业和任务关键型数据中心环境的理想选择。这些多功能的设备为统一通信提供市场领先的语音和视频安全服务，其中包括强大的防火墙、功能完备的 IP 安全 (IPsec) 和安全套接字层 (SSL) VPN、入侵防御和内容安全功能。对于统一通信部署，这些平台可以保护多达 3 万部电话，并为一系列统一通信协议提供应用检测，其中包括瘦客户端控制协议 (SCCP)、会话初始协议 (SIP)、H.323、媒体网关控制协议 (MGCP)、计算机电话接口快速缓冲区编码 (CTIQBE)、实时传输协议 (RTP) 和实时传输控制协议 (RTCP)。

Cisco ASA 5500 系列统一通信部署

Cisco ASA 5500 系列自适应安全设备旨在保护实时统一通信应用，例如语音和视频。这些设备保护统一通信部署的所有关键元素（网络基础设施、呼叫控制平台、IP 终端和统一通信应用）， 并且提供了可以补充统一通信系统内的内嵌安全性的多项安全功能，从而提供了额外的保护层。这些功能包括：

- 访问控制：动态且精细的策略访问控制，可防止未经授权访问统一通信服务。
- 威胁防御：内置的威胁防御功能，使统一通信基础设施可以阻止攻击系统的企图。
- 网络安全策略实施：为应用和用户创建并管理有效的统一通信策略。
- 语音加密服务：思科传输层安全 (TLS) 代理可以在加密信令和媒体的同时帮助客户保持其安全策略。
- 统一通信的边界安全服务：除了 SSL 和 IPsec VPN 服务外，电话代理、移动代理和在线状态联盟安全服务使企业可以将通信服务安全地扩展至远程用户、移动解决方案和企业到企业协作。

访问控制

访问控制是一项基本的安全功能，它仅允许经过授权的用户访问系统内的资源和服务。在统一通信环境中，此控制通常涉及向思科统一通信管理器和其他应用服务器提供网络层访问控制，作为抵御攻击的第一道防线。

通过限制对思科统一通信管理器服务器的访问，可以显著降低攻击者通过未经授权的网络通道探测系统漏洞或利用访问权限的风险。

Cisco ASA 5500 系列自适应安全设备是语音和视频感知型设备，可以检测现代统一通信中使用的协议（SIP、SCCP、H.323 和 MGCP），并将策略应用于这些协议。如果采用较旧的网络访问控制机制，例如访问控制列表 (ACL)，则无法以大多数组织所需的精细程度和动态程度，来处理这些比较复杂的协议。

与传统的数据应用不同，统一通信协议通过动态协商如何在信令控制通道内交换端口信息来进行通信。诸如 ACL 等静态访问控制机制无法跟踪将打开哪些端口，因此必须采取较弱的访问控制措施，这会限制实施有效访问策略的能力。

Cisco ASA 5500 系列自适应安全设备可以动态跟踪应打开的授权连接，然后在会话结束时立即关闭连接。这种级别的控制与诸如语音协议感知型网络地址转换 (NAT) 等其他智能服务相结合，使 Cisco ASA 5500 系列有别于不符合现代统一通信协议要求的较旧平台。

威胁防范

使用 Cisco ASA 5500 系列，可防止思科统一通信应用遭受可能威胁系统完整性和可用性的各种常见攻击。这些攻击包括通话窃听、用户假冒、话费诈骗和拒绝服务 (DoS)。其中许多攻击（尤其是 DoS）可以通过发送格式错误的协议数据包启动，攻击您的统一通信呼叫控制系统和应用。Cisco ASA 5500 系列设备会对流向关键统一通信服务器的流量执行协议一致性和合规性检查。例如，设备可以帮助确保流经设备的媒体确实是语音媒体 (RTP)，或防止攻击者发送可能导致呼叫控制系统崩溃的恶意语音信令。通过帮助确保信令和媒体符合标准 RFC，Cisco ASA 5500 系列为您的关键系统提供有效的第一道防线。

除了检查协议一致性之外，Cisco ASA 5500 系列的多功能安全服务还可以进行扩展，以提供入侵防御服务。Cisco ASA 5500 系列高级检测和防御安全服务模块 (AIP SSM) 将基于硬件的入侵防御系统 (IPS) 功能应用于入站流量，以阻止针对统一通信呼叫控制和应用服务器的已知攻击。一组统一通信 IPS 签名可用于防御针对思科统一通信管理器和思科统一通信管理器快捷版产品安全突发事件响应团队 (PSIRT) 漏洞的攻击，为 IT 管理员提供即时保护，而无需立即修补统一通信服务器。协议一致性和入侵防御相结合，提供针对常见统一通信威胁的强大网络层防御。

网络安全策略实施

您的统一通信部署可能需要遵守组织的安全部门规定的安全策略要求。Cisco ASA 5500 系列拥有先进的统一通信安全功能，您的组织可以将精细的应用层策略应用于统一通信流量，以满足安全合规性要求。例如，您的企业可以允许或拒绝来自特定呼叫者或域的呼叫，也可以应用特定的黑名单或白名单。再比如说，您可将网络策略扩展到终端和应用，以便仅允许已登记的电话致电呼叫控制中心或拒绝某些应用，例如通过 SIP 进行的即时消息。

语音和视频加密服务

出于合规性或安全策略原因，您的组织可能被要求对语音和视频流量加密。端到端加密通常使网络安全设备“看不见”媒体和信令流量，这种情况可能危及访问控制和威胁防御安全功能， 还可能导致防火墙与加密的语音之间缺乏互通性，使您的企业无法满足两项关键安全要求。

Cisco ASA 5500 系列加密代理解决方案为思科统一通信系统提供出色的支持（TLS 代理）。它是思科统一通信管理器身份验证域中的受信任设备：语音和视频终端可以安全地对流量进行身份验证和加密。Cisco ASA 5500 系列设备作为代理，可以将这些连接解密、采用必需的威胁防护和访问控制措施，并通过对流向思科统一通信管理器服务器的流量重新加密来帮助确保机密性。此集成使您的组织可以灵活部署所有必需的安全应对措施，而不是勉强采用不足够的一部分措施。

边界安全服务

边界安全服务包括以下方面：

- SSL 和 IPsec VPN：SSL 或 IPsec VPN 服务可在多个办公地点或远程用户之间提供安全、高速的语音和数据通信，Cisco ASA 5500 系列使用这些服务支持灵活、安全的连接。这些设备支持服务质量 (QoS) 功能，可促进以企业级质量可靠地提供延迟敏感型应用，例如音频和视频。您可以按用户、按组、按隧道或按流量应用 QoS 策略，以便将适当的优先级和带宽限制应用于语音和视频流量。此外，连接前状态评估和安全检查有助于确保 VPN 用户不会在不经意间将攻击带入网络中。Cisco SSL 和 IPsec 解决方案非常适合保护软客户端统一通信流量，例如 Cisco IP Communicator 以及 Cisco Unified Mobile Communicator 和 Cisco Unified Personal Communicator。
- 电话代理：Cisco ASA 电话代理功能有助于端接 Cisco SRTP 和 TLS 加密的终端，以便进行安全的远程访问。使用 Cisco ASA 电话代理，可以在没有大规模部署 VPN 远程访问硬件的情况下大规模部署安全电话。最终用户基础设施仅限于 IP 终端，不包括 VPN 隧道或硬件。Cisco ASA 电话代理是思科统一电话代理的替代产品。
- 移动代理：Cisco ASA 移动代理可促进 Cisco Unified Mobile Communicator 软件和 Cisco Unified Mobility Advantage 服务器之间的安全连接。Cisco ASA 设备可以拦截 Cisco Unified Mobile Communicator 软件和 Cisco Unified Mobility Advantage 服务器之间的 TLS 连接，并且可以使用新的多机箱多链路点到点协议 (MMP) 检测引擎来检测移动流量，并将策略应用于移动流量。从思科统一通信 7.0 系统开始，Cisco ASA 设备是移动解决方案的必备组件，并取代 Cisco Unified Mobility Proxy。
- 在线状态联盟：Cisco ASA 5500 系列可促进 Cisco Unified Presence 和 Microsoft Office Communications Server (OCS) Presence 解决方案之间的安全在线状态联盟。这使两个组织可以更有效地协作，方法是使用常见的可用通信方式共享关于如何最好地与其他用户进行联系和通信的在线状态信息。Cisco ASA 5500 系列自适应安全设备在线状态联盟解决方案的必备组件。

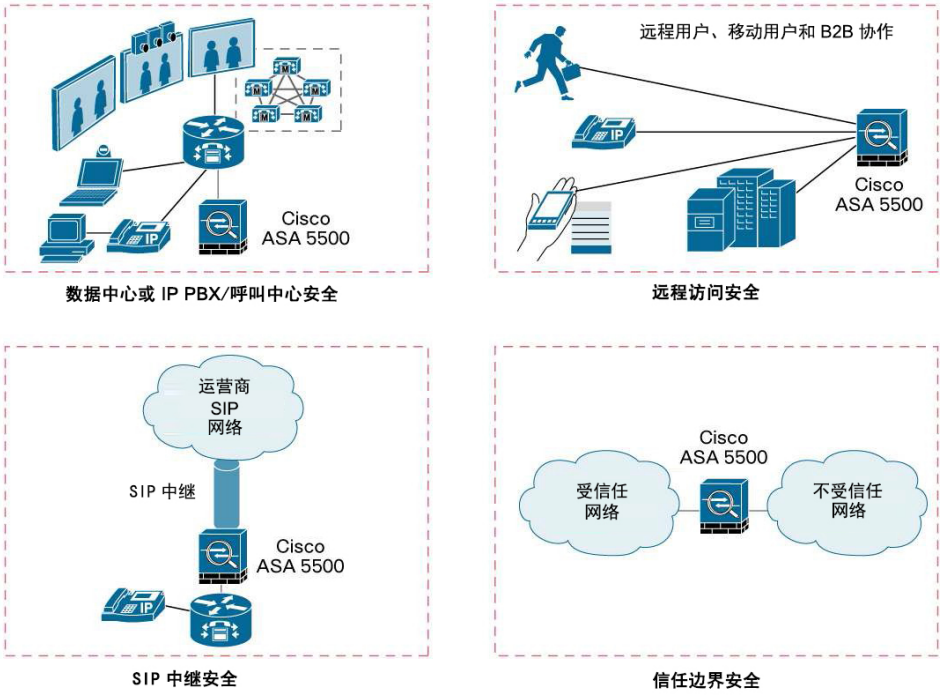
部署拓扑

如图 1 所示，您可以在网络中使用 Cisco ASA 5500，保护自己的呼叫控制系统、终端、应用和底层基础设施免遭攻击。这些拓扑包括：

- 保护呼叫控制服务器：通过控制客户端对这些服务器的访问权限，Cisco ASA 5500 系列可以阻止可能影响性能或可用性的恶意或未经授权的网络连接。通过有状态地检测连接以确定连接符合访问控制策略，并确定连接符合预期的行为，Cisco ASA 平台为安全的统一通信部署提供第一道防线。
- 远程访问安全：对于安全的远程工作人员电话、思科统一 IP 电话以及 Apple iPhone 等第三方电话、移动电话和企业到企业联盟部署，Cisco ASA 5500 系列提供 SSL 和 IPsec VPN、电话代理、移动代理和在线状态联盟安全服务。
- SIP 中继安全：企业将迁移到 SIP 中继架构以降低其通信成本。Cisco ASA 5500 系列拥有强大的 SIP 安全功能，能够防御通过 SIP 中继进行的任何攻击。
- 可信和不可信边界：您可以将 Cisco ASA 5500 作为安全设备放置在可信和不可信网络之间，以帮助确保不可信网络中的漏洞不会影响可信任网络。您可以使用 Cisco ASA 5500 系列安全设备代理流量，或在 DMZ 架构中保护内部网络免受外部访问。

凭借 Cisco ASA 5500 系列提供的各种型号，您的组织可以灵活地统一采用单个系列的安全产品，同时定位特定的型号以满足每个拓扑或地点的不同性能需求。

图 1. Cisco ASA 5500 系列部署拓扑



Cisco ASA 5500 系列为您的统一通信网络提供一套全面的语音和视频安全功能。表 1 列出了功能和优势。

表 1. 功能和优势总结

功能	详细信息
统一通信应用检测和控制	● 支持的协议包括 SIP、SCCP、H.323、MGCP、RTP 和 RTCP、TCP、CTIQBE 和实时流协议 (RTSP)。
SIP 应用检测和控制	● 此功能可促进基于用户数据报协议 (UDP) 和 TCP 的 SIP 环境的 SIP 流量的深度检测服务，从而提供精细控制，以防御统一通信攻击。 ● SIP 应用检测和控制为众多的 SIP RFC（包括 RFC 3261）提供协议一致性支持。它提供 SIP 状态感知和跟踪功能，并且能够实施必要的标头字段和避免实施禁止的标头字段，从而保护您的企业免遭使用格式错误的数据包的攻击。 ● 对基于 SIP 的 IP 电话和应用（例如 Microsoft Windows Messenger）而言，该功能可促进支持基于网络地址转换 (NAT) 和端口地址转换 (PAT) 的地址转换，同时提供各种高级服务，例如呼叫转接、呼叫转移等。 ● 此功能支持全面的威胁防御功能，例如 SIP 状态感知和跟踪功能、能够对 SIP 流量进行限速以防止 DoS 攻击（从而防止来自特定代理的 SIP 流量拦截来自欺诈代理服务器的 SIP 流量），以及验证媒体的 RTP 和 RTCP。 ● SIP 应用检测和控制功能使您的企业可以配置精细的统一通信策略。这些策略包括允许和拒绝主叫方和被叫方，方法是使用白名单和黑名单配置 SIP 统一资源标识符 (URI) 过滤器以及呼入和呼出电话。此外，SIP 应用检测和控制功能支持允许或拒绝使用各种应用，例如通过 SIP 进行的即时消息，或允许和拒绝特定的 SIP 方法（包括用户定义的方法）。
H.323 安全服务	● H.323 版本 1-4 以及直接呼叫信令 (DCS) 和网守路由器控制信令 (GKRCS) 在 H.323 控制的各种 IP 语音 (VoIP) 环境中提供灵活的安全集成。 ● 这些服务支持 NAT 和 PAT，其中包括各种高级功能，例如使用 T.38 协议的 IP 传真 (FoIP)，该协议是定义如何实时传输 FoIP 的 ITU 标准。 ● 这些服务支持 H.323 流量的威胁防御，例如限制呼叫持续时间，防止 H.225 注册、准入和状态 (RAS) 数据包在到达时状态错误，以及验证媒体的 RTP 和 RTCP。 ● 这可以帮助您的企业配置 H.323 服务的精细策略，例如过滤主叫和被叫电话号码以防止欺诈的主叫方，以及过滤特定的媒体类型以限制服务。

功能	详细信息
SCCP 安全服务	● 高级 SCCP 检测服务支持 SCCP 应用（例如思科统一 IP 电话、Cisco Unified Personal Communicator 和 Cisco IP Communicator）提供灵活的安全集成。 ● 这些服务提供全面的威胁防御，例如能够设置最大 SCCP 消息长度以防止缓冲区溢出攻击，能够调整 TCP SCCP 连接和 SCCP 音频和视频媒体连接的超时，以及验证媒体的 RTP 和 RTCP。 ● 这些服务可以帮助您的企业为 SCCP 流量配置精细的策略，例如强制只有已注册的电话呼叫可以通过 Cisco ASA 设备发送流量，以及过滤消息 ID 以允许或拒绝特定的消息。
MGCP 安全服务	● 对于媒体网关和呼叫代理（或媒体网关控制器）之间的基于 MGCP 的连接，丰富的 MGCP 安全服务可促进基于 NAT 和 PAT 的地址转换服务。
RTSP 安全服务	● RTSP 安全服务可促进检测 RTSP 协议，这些协议用于控制客户端和服务器之间的流媒体应用的通信，例如 Cisco IP/TV、Apple QuickTime 和 RealNetworks RealPlayer。 ● RTSP 安全服务为 RTSP 媒体流提供基于 NAT 和 PAT 的地址转换服务，以改善对实时网络环境的支持。
分片和分段的多媒体流检测	● 此功能可促进检测基于 H.323、SIP 和 SCCP 的语音和多媒体流，这些语音和多媒体流已被分片和分段，以防御这些独特的统一通信攻击。
高级 TCP 安全引擎	● 高级 TCP 安全引擎保护您的网络免遭多种攻击，其中包括使用 SYNC cookie 的 SYN 泛洪攻击，并且保护您的网络终端免遭协议模糊攻击和重新传输风格的生存时间 (TTL) 逃避。 ● 此安全引擎提供一项重组 TCP 数据包的智能 TCP 代理功能，以防御使用多个 TCP 数据包的分段攻击。 ● 此安全引擎提供 TCP 流量规范化服务，以增加检测攻击的技术，其中包括高级标记和选项检查、TCP 数据包校验和验证、在重新传输的数据包中检测数据篡改等等。
RTP 和 RTCP 检测服务	● 使用这些服务可以检测由统一通信检测引擎打开的媒体连接上的 RTP 和 RTCP 流量，例如 SIP 和 SCCP 连接。 ● 这些服务可以帮助您的企业为 RTP 和 RTCP 流量设置安全策略，例如验证是否符合 RFC 1889，交叉检查信令和 RTP 之间的媒体值以验证负载类型，以及管制版本号、负载类型完整性、序号和同步源 (SSRC)。
威胁防范	
入侵防御服务	● 可选的 Cisco ASA 5500 系列 AIP SSM 采用入侵防御服务，保护统一通信基础设施和呼叫控制服务器免遭基于 IPS 签名的攻击。AIP SSM 提供的 IPS 服务针对统一通信进行了优化并且支持特定的统一通信引擎，例如 H.323 和 H.225 检测引擎，AIP SSM 还有助于防止对呼叫控制服务器进行操作系统攻击。 ● 独特的入侵防御功能（例如异常检测、操作系统指纹识别功能和风险评级功能）可更好地提供关于威胁的情景，防止误报。
内容安全服务	● 这些服务可以帮助您的企业实施基于网关的内容检测功能，以检测邮件和网络流量的内容。这有助于确保统一通信基础设施免遭病毒、蠕虫、垃圾邮件、网络钓鱼和恶意软件攻击。
加密服务	
TLS 代理	● 在加密的信令使统一通信防火墙无法动态打开端口或应用策略的情况下，TLS 代理可解决加密的信令与防火墙集成的问题。 ● 作为思科统一通信管理器内的可信设备，Cisco ASA 设备可以拦截加密的信令、与终端相互进行身份验证和将信令解密。在将信令解密后，设备检索所有必要的信令信息，并执行所有检测和策略实施操作。为了保持端到端的安全连接，设备接着重新启动与思科统一通信管理器的第二次 TLS 会话。终端与思科统一通信管理器之间的信令和通信在功能上保持相同，防火墙可以提供其统一通信安全服务。 ● TLS 代理服务支持 SIP 和 SCCP 终端与思科统一 IP 电话全面集成。
边界安全服务	
电话代理	● 电话代理提供安全的远程访问，无需远程访问 VPN 设备。它通过端接使用 TLS 或 SRTP 加密的 SCCP 和 SIP 思科统一 IP 电话终端来实现这一点。电话代理支持思科统一通信管理器混合模式和非安全模式。您可以将电话代理部署在现有防火墙后面，或将其部署为集成的防火墙或电话代理设备。
移动代理	● 移动代理保护 Cisco Unified Mobility 解决方案，并取代 Cisco Unified Mobility Proxy。它包含一个用于验证移动流量的新检测引擎，其中包括验证 Blackberry、Symbian 和 Windows 移动设备上运行的 Cisco Unified Mobile Communicator 的协议一致性。
在线状态	● Cisco Unified Presence 的这个必备联盟组件与 Microsoft Presence 解决方案可在两个组织之间保护在线状态信息和应用安全策略（白名单、黑名单和协议一致性）。
SSL 和 IPsec VPN	● 为统一通信和数据流量提供强大的加密 SSL 和 IPsec VPN 服务，这些服务对终端进行连接前状态评估，并且能够将策略和检测功能应用于 VPN 流量，以防止远程用户将漏洞带入您的网络中。Cisco AnyConnect 通过支持数据报传输层安全 (DTLS) 优化语音，并保护第三方终端，例如 Apple iPhone。

订购信息

要下订单，请访问思科订购主页 (http://www.cisco.com/go/ordering)，并参阅表 2 至表 4。要下载软件，请访问思科软件中心 (http://www.cisco.com/go/software)。在订购 Cisco ASA 5500 系列自适应安全设备以保护统一通信部署时，您有两个选项：

- 选项 1：思科统一通信代理许可证。您可以为现有的 ASA 设备单独订购思科统一通信代理软件许可证。您最多可以为表 2 中列出的最大会话数结合使用电话代理、移动代理、在线状态联盟代理和 TLS 代理。

表 2. 思科统一通信代理最大会话数

	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580	Cisco ASA 5585-X SSP- 10	Cisco ASA 5585-X SSP-20 或 SSP-40 或 SSP-60
统一通信代理最大会话数	24	100	1000	2000	3000	● 5000（对于电话代理） ● 10,000（对于 TLS 代理、移动代理、在线状态联盟代理）	● 3000（对于电话代理） ● 3000（对于 TLS 代理、移动代理、在线状态联盟代理）	● 5000（对于电话代理） ● 10,000（对于 TLS 代理、移动代理、在线状态联盟代理）

- 选项 2：Cisco ASA 5500 系列统一通信版捆绑包。这些设备捆绑统一通信代理许可证，为您的企业提供单个硬件和软件产品 ID，以提供电话代理、移动代理、在线状态联盟和 TLS 代理功能， 以及基本的防火墙和 VPN 功能。请注意，捆绑包不适用于 ASA 5505、5510、5580 或 5585。请订购统一通信代理许可证及 ASA 硬件。表 3 提供了部件号。

表 3. Cisco ASA 5500 系列统一通信版订购信息

产品名称	部件号
适用于统一通信安全的 Cisco ASA 5520 自适应安全设备	
Cisco ASA 5520 自适应安全设备 UC 安全版；包括 4 个千兆以太网接口、1 个快速以太网接口、1000 个 UC 代理会话、750 个 IPsec VPN 对等体、2 个 SSL VPN 对等体、“主用/主用”和“主用/备用”高可用性、3DES/AES	ASA5520-UC-BUN-K9
Cisco ASA 5520 自适应安全设备 UC 安全版；包括 4 个千兆以太网接口、1 个快速以太网接口、1000 个 UC 代理会话、750 个 IPsec VPN 对等体、2 个 SSL VPN 对等体、“主用/主用”和“主用/备用”高可用性、3DES/AES[1]	ASA5520-UC-BUN-K8
适用于统一通信安全的 Cisco ASA 5540 自适应安全设备	
Cisco ASA 5540 自适应安全设备 UC 安全版；包括 4 个千兆以太网接口、1 个快速以太网接口、2000 个 UC 代理会话、5000 个 IPsec VPN 对等体、2 个 SSL VPN 对等体、3DES/AES	ASA5540-UC-BUN-K9
Cisco ASA 5540 自适应安全设备 UC 安全版；包括 4 个千兆以太网接口、1 个快速以太网接口、1000 个 UC 代理会话、5000 个 IPsec VPN 对等体、2 个 SSL VPN 对等体、3DES/AES[1]	ASA5540-UC-BUN-K8
统一通信安全的 Cisco ASA 5550 自适应安全设备	
Cisco ASA 5550 自适应安全设备 UC 安全版；包括 8 个千兆以太网接口、1 个快速以太网接口、3000 个 UC 代理会话、5000 个 IPsec VPN 对等体、2 个 SSL VPN 对等体、3DES/AES	ASA5550-UC-BUN-K9
Cisco ASA 5550 自适应安全设备 UC 安全版；包括 8 个千兆以太网接口、1 个快速以太网接口、1000 个 UC 代理会话、5000 个 IPsec VPN 对等体、2 个 SSL VPN 对等体、3DES/AES[1]	ASA5550-UC-BUN-K8

思科统一通信服务

借助思科统一通信服务，即可更快地节省与部署安全、恢复力强的思科统一通信解决方案关联的成本，并提高相应的工作效率。我们的服务产品组合由思科和认证合作伙伴提供，基于经过验证的方法，可在固定和移动网络中统一语音、视频、数据和移动应用。我们独特的服务生命周期方法可增强您的技术体验，从而树立真正的企业优势。

更多详情

有关 Cisco ASA 5500 系列或 Cisco ASA 平台上的统一通信的更多信息，请访问 http://www.cisco.com/go/asa 或 http://www.cisco.com/go/secureuc。您还可以联系您当地的思科客户代表。

[1] DES 适用于 ASA 软件 8.2 及更早版本中的 UC 许可证。3DES/AES 适用于 ASA 软件 8.3 及更高版本中的 UC 许可证

美洲总部
Cisco Systems,Inc.
加州圣荷西

亚太总部
Cisco Systems(USA)Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

Cisco 在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。

美国印刷 C78-450091-03 10/10