

您的网络是否已就绪可应对新一代的威胁？



合作伙伴业务机会

将客户迁移到提供增值安全服务的新 Cisco® ASA 5500-X 系列下一代防火墙能够带来可观的收益，因为：

- Cisco ASA 5500 系列拥有全球最大的防火墙客户群，从该系列迁移到新平台预计会在全球带来超过 20 亿美元的商机，在中国可带来超过 2 亿美元的商机。
- 无论您是出售自己的增值服务、转售思科品牌服务，还是利用思科协作服务来支持新服务，此解决方案都为您提供增加服务收入的机会。
- 您可以向客户提供特别促销活动及终止销售公告，以便吸引他们立即进行迁移。

客户收益

Cisco ASA 5500-X 系列下一代防火墙使组织能够在整个网络中实施基于情景的策略，从而安全地加速业务创新，实现对应用、用户和设备的精细控制，提供全面防护且不降低性能。

Cisco ASA 5500-X 系列下一代防火墙：

- 不仅提供业内最可靠的状态检测防火墙，还具备强大的下一代功能，如应用可见性与控制性 (AVC)、入侵预防系统 (IPS)、Web 安全和基于云的 Web 安全、高度安全的远程访问和僵尸网络流量过滤等，从而打造全面的安全解决方案¹，消除安全隐患。
- 通过 Web 信誉和互联网威胁信息增强防火墙、IPS 和 Web 安全服务，提供针对零日威胁的实时防御。
- 增强网络集成的基于情景的安全策略，以简化防火墙策略管理。这些安全策略因具体的应用、用户和行为而异。
- 提供可预测的性能和可扩展的安全性，使组织能够运行多个安全服务，从而最大程度地降低风险和防御新威胁，同时不降低性能。

¹有关详细信息，请参阅《定价和订购指南》。

目标受众

对于企业和中端市场，本解决方案的目标对象是安全解决方案购买者。对于小型商业公司，购买者可能是 IT 经理。

请联系现有 ASA 客户群，向其提供终止销售公告。这为您创造了力促客户迁移的良机。以下三类客户应视为主要目标：

- 现有的 ASA 5500 客户
- 使用第三方 URL 过滤产品的客户
- 在接下来的 12 个月内即将迁移的其他防火墙客户，特别是支持自带设备 (BYOD) 和云计算的客户，或在实施可接受的使用策略中遇到挑战的客户。

引进新的 Cisco [ASA 5512-X](#)、[ASA 5515-X](#)、[ASA 5525-X](#)、[ASA 5545-X](#)，以及 [ASA 5555-X](#) 和支持性安全服务：[思科基于身份的防火墙安全](#)、[IPS](#)、[僵尸网络过滤](#)、[云 Web 安全](#)、[Cisco AnyConnect 安全移动客户端](#)、[应用可见性与控制性](#)和 [Web 安全基本版](#)。



行动号令

- 找出重要的潜在客户：**向业内最大的防火墙客户群告知 ASA 5500 系列即将终止销售，为您创造销售机会。正如竞争产品客户群一样，支持 BYOD 计划的组织也是重要的潜在客户。
- 吸引客户：**使用新的《[思科 2013 年度安全报告](#)》和新的《[充分利用下一代防火墙](#)》白皮书和《[安全不打折扣：ASA 5500-X 下一代防火墙](#)》白皮书，介绍下一代防火墙解决方案所具有的广度和价值。[合作伙伴市场营销中心](#)上的“您的网络是否准备好应对下一代威胁？”活动提供了上述白皮书。
您也可以使用电邮模板、电话脚本和合作品牌广告来传达思科情景感知威胁防御方案的价值。
- 提供特惠：**提供 Cisco ASA 固定折扣促销和其他购买优惠，提高客户解决方案的性价比。
- 提供融资：**充分利用 [Cisco Capital® China 融资选项的好处](#)。
- 捕捉机会：**销售[思科品牌服务（用于转售）](#)和[协作服务（支持销售自家品牌的服务）](#)，提高您自己的实践能力。通过更深入地了解客户的网络性能，您可以发掘新业务机会，增强盈利能力。
- 对客户进行安全评估：**提供安全评估，以扩大销售机会。

优惠

Cisco TMP 服务

以旧的 ASA 5500 系列设备换购新的 ASA 5500-X 系列时，可享受思科[以旧换新计划](#) (TMP) 中提供的特惠。

对于从 Juniper 安全产品到思科的迁移，还提供[安全竞争设备交换优惠](#)和[安全升级促销](#)。

启发式问题

- 实时威胁检测：**安全威胁可在数分钟内扩散至全球范围，导致巨额收入损失。您是否能够近乎实时地发现您的网络安全威胁？您是否有兴趣通过实时威胁源将您的安全设备（如电邮、Web、防火墙和 IPS 系统）用于全球实时的历史威胁和漏洞分析以及缓解数据库？
- 解决现今的 BYOD 挑战：**您是否希望在移动设备接入网络前了解有关其类型、位置和安全状态的详细信息？您是否对专为情景感知安全而设计的解决方案（它提供使用户能够安全地按照他们喜欢的方式工作所需的可见性）感兴趣？此情景包括用户身份（身份）、用户要访问的应用或网站（事情）、访问的来源（地点）、访问的时间（时间）和用于访问的设备的属性（方式）。
- 采用多个安全服务时的性能：**您是否希望在不降低性能的情况下向基础设施添加安全服务（如 IPS、僵尸网络过滤器或 Web 安全）？为采用多个安全服务，设计了一个面向未来的平台。
- 应用可见性与控制性：**您是否对精细的应用可见性与控制性感兴趣？您是否将从基于情景的控制获益（该控制允许您对基于 Web 和云的应用的访问进行分类和管理，并可以控制哪些应用及其使用方式）？