



面向 ISR 的 Cisco FirePOWER 威胁防御

保护您的分支机构和远程办公地点

分支机构当前面临的企业级风险需要企业级的安全功能。虽然您要应对 BYOD 趋势、合规性要求以及分布式站点越来越多地使用直接互联网访问 (DIA) 的情况，但您仍需要帮助它们防御高级持续威胁。

为此，您可以使用思科行业领先的威胁防范功能，这些功能现已在另一平台上运行：思科集成多业务路由器 (ISR)。面向 ISR 的 Cisco FirePOWER 威胁防御将企业级的威胁防范功能扩展到传统的网络边缘和数据中心部署之外，帮助保护您的 DIA 流量。

借助该解决方案，您可以在分支机构实现 DIA，从而节省成本并改善用户体验。与此同时，您也将能够更好地保护设备和主机免受高级威胁侵害，无论这些设备和主机位于什么位置（包括分支机构、合作伙伴位置和其他远程站点）。

优势

- 在分支机构中利用直接互联网访问 (DIA)，同时确保您的连接安全可靠。
- 为您的分支机构、合作伙伴和远程办公地点提供多层威胁防范。
- 利用路由器和安全技术，在一个综合空间中腾出宝贵的地产。
- 利用集中式的管理控制台实现角色与职责的明确分工。

“利用经过调整的策略，FirePOWER 8350 阻止了 99.5% 的攻击。该设备证明它能有效防御测试的所有攻击逃避技术。该设备还通过了所有的稳定性和可靠性测试。”

NSS Labs 2015 年下一代入侵防御系统 (NGIPS) 测试报告

“安全无处不在”的目标

面向 ISR 的 Cisco FirePOWER 威胁防御是思科的“安全无处不在”战略的一个组成部分。目标是为您提供在您的环境中防御高级威胁所需的连续可视性与可控性。一组集成的安全功能协同工作，确保您的远程操作安全可靠：

- FirePOWER 下一代入侵防御系统 (NGIPS)** - 在高级威胁防御、集成实时情景感知和智能安全自动化方面树立了新标准，并且具有行业领先的威胁防护水平。
- 应用可视性与可控性** - 可对数千种应用进行精确控制，并实施移动应用、社交媒体应用和可接受使用策略，从而有效缩小可能的攻击面。
- 面向网络的高级恶意软件保护 (AMP)** - 可防范高度复杂的针对性零日攻击以及持续性高级恶意软件威胁。
- 基于信誉的 URL 过滤** - 可以对 80 多个类别超过 2.8 亿个 URL 进行访问控制，并最大限度降低与可疑的域和不可接受的域相关的风险，从而缓解复杂的客户端攻击。
- FireSIGHT 管理中心** - 可提供集中的事件和策略管理，以及对网络中运行的设备、操作系统、应用和用户的可视性。

后续行动

请与您当地的销售代表联系，安排演示并请求详细报价。如需更多信息，请访问[面向 ISR 的 Cisco FirePOWER 威胁防御](#)网页。