

# 安全参考信息

---

安全建议和通告位于 <http://www.cisco.com/go/psirt> , 其中还有来自产品安全事件响应小组 (PSIRT) 的其他信息。

---

## 最佳实践

### [改善 Cisco 路由器的安全性](#)

本文档是对某些 Cisco 配置设置的非正式讨论, 网络管理员应考虑对其路由器 (尤其是边界路由器) 上的这些设置进行更改以改善其安全性。本文档将介绍 IP 网络中几乎通用的基本“样板”配置项, 以及一些应加以留意的不常见项。

### [Cisco IOS 口令加密相关信息](#)

某非 Cisco 来源发布了对 Cisco 配置文件中的用户口令 (及其他口令) 进行解密的程序。对于用 `enable secret` 命令设置的口令, 该程序无法解密。此程序在 Cisco 用户中导致了意外的恐慌。这使我们意识到, 许多依赖于 Cisco 口令加密的用户想要获得更高的安全性, 但其最初设计所能提供的安全性有所不足。本文档将对 Cisco 口令加密背后的安全模式及其加密安全限制加以说明。

### [Cisco 的 SAFE 蓝图](#)

SAFE 是全面的安全蓝图, 可使组织安全地从事业务活动。SAFE 采用的模块化方法能够在网络增长变化的条件下简化安全设计、部署及管理, 从而使建立在 Cisco AVVID (语音、视频和集成数据体系结构) 上的网络得到增强。**攻击防御、跟踪或缓解策略** [使用 Cisco 路由器确定数据包泛洪的特征并加以跟踪](#)

拒绝服务 (DoS) 攻击在互联网上十分常见。应付此类攻击的第一步是辨别该攻击究竟属于何种类型。许多常用的 DoS 攻击建立在高带宽数据包洪流或其他重复性数据包流的基础上。本文档为了解及跟踪这些攻击提供了深入理解。**抵抗 Nimda 病毒的策略**

本索引提供了应对 Nimda 病毒的所有技术提示及缓解建议的全面列表。**抵抗“红色代码”蠕虫的策略**  
本索引提供了应对“红色代码”蠕虫的所有技术提示及缓解建议的全面列表。**防范分布式拒绝服务 (DDoS) 攻击的策略**

本白皮书从技术上描述了潜在 DDoS 攻击的发生方式, 并给出了使用 Cisco IOS 软件进行防御的建议方法。**防范 UDP 诊断端口拒绝服务攻击的策略**

本白皮书从技术上描述了潜在 UDP 诊断端口攻击的发生方式, 并给出了使用 Cisco IOS 软件进行防御的建议方法。**防范 TCP SYN 拒绝服务攻击的策略**

本白皮书从技术上描述了潜在 TCP SYN 攻击的发生方式, 并给出了使用 Cisco IOS 软件进行防御的建议方法。**拒绝服务攻击的最新信息：“Smurfing”介绍及使危害最小化的信息**

**注意：**以上链接所指向的外部站点并非由 Cisco Systems, Inc. 维护。

本文档提供了有关“smurf”攻击的详细信息, 重点介绍了 Cisco 路由器及如何减小这些攻击的危害。有些信息是通用的, 与所选的组织特定供应商无关; 但文中介绍以 Cisco 路由器为重点。本文档无意确认“smurf”攻击对其他供应商设备的危害; 但其中包含有关多家供应商的信息。**其它资源**

**Cisco 产品安全事件响应** 本文档对 Bug 报告和事件响应程序加以说明 - 具体而言, 当遭受主动安全攻击或确信将受到攻击时、当遇到 Cisco 产品安全问题时、当想要获取 Cisco 产品的技术安全信息时或者当对于 Cisco 产品的已解决安全问题有其他疑问时, 您应采取何种措施。其中还说明了 Cisco 产品安全事件响应小组 (PSIRT) 在处理安全事件中的角色。

---