



# Cisco Firepower 下一代防火墙

## 业内首款完全集成，专注于威胁防御的下一代防火墙

大多数下一代防火墙 (NGFW) 主要专注于实现应用控制，而对其威胁防御功能关注甚少。为进行补偿，某些 NGFW 将尝试用一系列非集成附加产品补充下一代入侵防御。然而，这种方法对于保护您的业务抵御老练的攻击者和高级恶意软件所造成的风险作用不大。此外，一旦您受到感染，在确定感染范围、隔离感染和快速修复方面，它们也没有什么帮助作用。



您需要一个以威胁为中心的集成下一代防火墙。这款防火墙不仅提供精细应用控制，而且能有效防御老练狡猾的恶意软件攻击所造成的威胁。

Cisco Firepower™ 下一代防火墙 (NGFW) 是业内首款完全集成、专注于威胁防御的 NGFW。它提供从网络到终端的防火墙功能、应用控制、威胁防御和高级恶意软件防护的全方、统一策略管理。

它可以部署在 Cisco Firepower 4100 和 9300 设备上，为互联网边缘和其他高性能环境提供性能和密度优化的 NGFW 安全平台。

## 在攻击前、攻击中和攻击后，为组织提供保护

Cisco Firepower NGFW 包括业内最广泛部署的状态防火墙并对 4,000 多个商业应用提供精细控制。其单一管理界面为网络到终端提供统一可视性。Firepower NGFW 实现全面的策略管理，可以控制访问、阻止攻击、抵御恶意软件，并提供集成工具来跟踪已遭受的攻击、遏制攻击和从攻击中恢复。

## 优势

- **阻止更多威胁** - 通过业内最有效的威胁防范功能阻止已知和未知威胁
- 对网络中的用户、应用、设备、威胁和漏洞**提供深入可视性和可控性**，
- 将恶意软件检测时间从几个月减少到几小时，并且实现更快修复，**加快检测和响应速度**
- 将所有安全功能合并到一个管理界面，**降低复杂性**和简化操作
- 与其他思科安全和网络解决方案相集成，**让您的网络发挥更多价值**

Cisco Firepower NGFW 在业内独一无二，因为它是提供以下功能的唯一一款下一代防火墙：

- 提供下一代入侵防御系统 (NGIPS)，提供业内领先的威胁防范
- 包括用来解决已知和未知威胁的完全集成的高级恶意软件防护 (AMP) 解决方案，以及集成的沙盒
- 使您能够跟踪和遏制恶意软件感染
- 将威胁事件与网络漏洞相关联，以便可以将资源集中于防御最紧要的威胁
- 分析网络弱点，并且建议落实安全策略
- 与许多思科®网络安全产品集成，从而利用以前的投资并提供更强大的安全性

## 后续计划

要了解更多信息，请访问我们的网站，网址为 [www.cisco.com/go/NGFW](http://www.cisco.com/go/NGFW)。