Cisco Secure 防火墙

目录

网络与安全相融合

世界一流的安全控制

一致的策略和可视性

优势

- 利用您的现有思科投资
- 通过更强大的安全控制点实施策略
- 随时随地保护访问互联网的用户
- 扩展网络设备的功能，实现更出色、更集成的安全性
- 获得强大的产品集成

将整个网络转变为安全架构的扩展

随着业务关键型应用从基于本地的网络转移到云，并且用户可以随时随地通过个人设备访问资源，传统的防火墙方法不再有效。我们的单一网络边界已演变成多个微边界，而传统防火墙设备正在通过混合使用物理和虚拟设备实现增强。因此，组织在竭力实施这些完全不同的安全解决方案，以期保持一致的策略和统一的威胁可视性。

思科正在构建一个安全平台，以实现更加敏捷和集成的方法，从而跨日趋异构的网络协调策略和实施。Cisco Secure 防火墙为您提供核心网络功能与网络安全之间最深度的集成，提供了比以往任何时候都更安全的架构。这带来了完整的安全产品组合，为您的应用和用户提供全方位的保护。客户案例

世界一流的安全控制

威胁变得更加复杂，网络更是如此。很少有组织（如果有的话）有专门资源用来了解所有不断涌现和不断发展的威胁的最新情报，及成功抵御所有这些威胁。

随着威胁和网络变得更加复杂，拥有合适的工具来保护您的数据、应用和网络势在必行。Cisco Secure 防火墙设备拥有您所需的强大功能和灵活性，使您能够提前防范威胁。除了独特的基于硬件的大规模加密流量检测功能外，其性能比上一代设备提升 3 倍。客户案例 | 演示

一致的策略和可视性

借助 Cisco Secure 防火墙产品组合，您可以获得更强大的安全保护，坐拥面向未来的灵活管理功能。思科提供多种专为满足您的环境和业务需求而定制的管理选项，包括：Firepower 设备管理器 (FDM)、Cisco Firepower 管理中心 (FMC) 以及 Cisco Defense Orchestrator (CDO)。

思科 FDM 是用于本地管理小规模部署的设备上管理解决方案。思科 FMC 是一款适用于大型部署的本地部署解决方案，可通过丰富的报告和本地日志记录功能集中管理安全事件和策略。CDO 则是基于云的安全管理器，可简化整个扩展网络中的安全策略和设备管理。

客户案例 | 演示

Cisco Secure 防火墙的高级功能：

高级功能	详细信息
高级威胁情报 (Talos)	• Talos 团队通过保护您组织的基础设施免受恶意和未知威胁侵犯，为思科安全生态系统提供了有力支持
Cisco Defense Orchestrator (CDO)	• 基于云的应用，可助您针对思科安全产品实现一致的策略管理
安全终端	• 全球威胁情报，持续分析和追溯性安全，时间点恶意软件检测与拦截
下一代入侵防御系统 (SNORT)	• 行业领先的开源下一代入侵防御系统 (NGIPS)，即使是面对最复杂的威胁，也能提供增强的安全性，助组织满足监管要求
SecureX 威胁响应	• 利用 Talos 团队提供的威胁情报，自动研究感染指标并快速确认威胁

为什么选择思科？

Cisco Secure 防火墙产品组合可为您的网络提供更强大的保护，助您抵御各种日趋复杂的威胁。选择思科，您可以投资于既敏捷又实现了集成的安全基础，从而打造当前和未来最强大的安全态势。

您可以在数据中心、分支机构、云环境以及任何位置利用思科的强大功能，将您现有的网络基础设施转变为防火墙解决方案的扩展，随时随地实现世界一流的安全控制。

现在投资购买 Cisco Secure 防火墙设备，可立即获得强大的保护，有效抵御最复杂的威胁，并在不影响系统性能的情况下检测加密流量。此外，它还集成了其他思科解决方案，为您提供广泛而深入的安全产品组合。这些产品可以协同工作，将以前无关联的事件关联起来，消除阻碍，更快地阻止威胁。

后续行动

如需了解 Cisco Secure 防火墙的更多信息，请访问 https://www.cisco.com/c/zh_cn/products/security/firewalls/index.html。

要查看购买选项并与思科销售代表联系，请访问 https://www.cisco.com/c/zh_cn/buy.html。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

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

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

C45-736624-03 12/20