面向金融机构的 Cisco Secure Firewall

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

将安全架构扩展到整个网络

随着业务关键型应用越来越多地使用混合和多云环境，并且员工现在需要随时随地安全访问资源，传统的防火墙解决方案越来越难以满足需求。单一网络边界已经演变为多个微边界。对许多金融机构而言，应用已成为新的边界，传统的防火墙部署业已演进为物理、虚拟及云原生设备等多种形式。因此，企业都在想法设法为现代应用环境提供支持。如何在不引入风险漏洞的情况下保持可视性、策略执行及统一的威胁可视性，是企业面临的一大挑战。

思科着手构建的未来网络安全解决方案 NetWORK 采用更加敏捷的自动化和集成化方法，在现代动态应用和架构日益多样化的网络之间协调策略和执行。Cisco Secure Firewall 可最大限度地实现核心网络功能与网络安全之间的深度集成，提供的安全性远超以往的架构。最终，一套完整全面的安全产品组合应需而生，为您的应用和用户提供全方位的保护。

优势

- 实时、统一的工作负载和网络安全，可实现跨动态应用环境的集成控制。
- 平台化的网络安全方法，利用和共享来自关键信息源的情报，可更快地执行检测、响应和补救。保障远程员工随时随地从任何设备高度安全地访问企业，并通过强大的威胁防御功能保护公司、员工和关键应用。
- SecureX™ 包含在所有 Cisco® Secure Firewall 中，实现深度集成，可在 Cisco Secure 系列产品组合中建立威胁关联，并加速事件响应。

卓越的可视性与可控性

威胁变得愈加复杂，网络更是如此。金融机构一般都缺乏专门资源来及时跟踪所有不断涌现和演变的威胁，并成功抵御所有这些威胁，即使有也很少。

随着威胁和网络日渐复杂，利用合适的工具来保护您的数据、应用和网络迫在眉睫。Cisco Secure Firewall 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。此外，Snort 3 IPS 的用户可读规则有助于简化安全性。动态应用的可视性与可控性可通过 Cisco Secure Workload 集成实现，从而跨网络和工作负载为当今的现代应用提供一致的保护。

选择符合您业务需求的理想防火墙

实现简化一致的策略管理

借助 Secure Firewall 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。思科提供多种管理选项，全面满足您的独特业务需求。

- **Cisco Secure Firewall Device Manager:** 本地管理单一防火墙；此为 Firewall Threat Defense 的设备本地管理解决方案。
- **Cisco Secure Firewall Management Center:** 管理大规模防火墙部署。支持本地部署、私有云、公共云和软件即服务 (SaaS) 等所有形式。
- **Cisco Defense Orchestrator:** 云端管理器，可精简多个思科产品（如 Cisco Secure Firewall、Meraki® MX 和 Cisco IOS® 设备）的安全策略及设备管理。

思科亦提供思科安全分析和日志记录，以进行可扩展的日志管理。它加强了威胁检测，并具备更长的保存及行为分析能力，确保用户满足合规要求。

Lake Trust Credit Union 成功案例

为什么选择思科？

Cisco Secure Firewall 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、公司办公室、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 Secure Firewall 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和第三方解决方案，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。

Cisco Secure Firewall 的高级功能

高级功能	详细信息
Cisco Secure Workload 集成	• CiscoSecureWorkload（前身为 Tetration）集成能够为整个网络的现代分布式及动态应用提供全面的可视性及策略执行，以及以可扩展方式实现一致执行的工作负载。
Cisco Secure Firewall Cloud Native	• Secure Firewall Cloud Native 由 Kubernetes 构建，并首次在 AWS 中提供，是一种用于构建高弹性、云原生基础设施的开发人员友好型应用访问解决方案。
动态策略支持	• 对于静态 IP 地址不可用的情况，动态属性支持 VMware、AWS、Azure 标签。 • 思科一直是基于标签策略的先驱，提供安全组标签 (SGT) 及思科身份服务引擎 (ISE) 属性支持。
Snort 3 入侵防御系统	• 行业领先的开源 Snort 3 的下一步威胁防护有助于提高检测能力、简化定制并提高性能。
传输层安全 (TLS) 服务器标识及侦测	• 使您能够维护加密 TLS 1.3 流量的第 7 层策略。在不可能做到对每一个流量进行解密和检查的加密世界中保持可视性和可控性。竞争性防火墙透过加密 TLS 1.3 流量打破您的第 7 层策略。

高级功能	详细信息
Cisco Secure Firewall Management Center	• 针对防火墙、应用控制、入侵防御、URL 过滤和恶意软件防御策略进行统一管理。 • 与 Cisco Secure Workload（前身为 Tetration）集成，为整个网络和工作负载中的动态应用提供一致的可视性和策略实施。
Cisco Defense Orchestrator	• 云端防火墙管理有助您在 Cisco Secure Firewall 上轻松一致地管理策略。
思科安全分析和日志记录	• 高度可扩展的本地及云端防火墙日志管理，具有行为分析功能，可实时检测威胁，从而缩短响应时间。此外，还提供持续分析功能，以进一步改善您的安全态势，从而更有效地抵御未来的威胁。 • 通过汇总所有 Cisco Secure Firewall 的日志满足您的合规需求。 • 与防火墙管理器紧密集成，以进行扩展日志记录及分析，并在单一直观视图中汇总防火墙日志数据。
Cisco SecureX	• 利用 SecureX 平台加速威胁检测及补救。每个 Secure Firewall 均提供使用 Cisco SecureX 的授权。使用 Firewall Management Center 全新的 SecureX 功能区，可将 SecOps 即时转换为 SecureX 的开放平台，从而加快事件响应。
Cisco Talos® 威胁情报	• Cisco Talos 情报团队是世界上最大的商业威胁情报团队之一。他们为思科客户、产品及服务提供准确、快速、切实可行的威胁情报。Talos 团队同时也负责维护 Snort.org、ClamAV 及 SpamCop 的官方规则集。

后续行动

如需了解有关 Cisco Secure Firewall 的更多信息，或查看适用于金融服务的更多安全解决方案，请访问产品组合浏览器。与思科销售代表联系或查看购买选项。

美洲总部
Cisco Systems. Inc
加州圣何西

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

欧洲总部
Cisco Systems International BV Amsterdam,
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。

美国印刷 C45-3380706-00 02/23