CISCO
SECURE

白皮书
思科公开信息

防火墙的未来

把握当下，巩固安防壁垒；着眼未来，保障业务安全

cisco The bridge to possible

目录

摘要

本白皮书通过回顾网络安全的发展历程，帮助您展望未来如何为组织的网络环境提供安全保护。

随着网络变得更加异构化，组织越来越难以保证策略管理和实施的一致性，并获得全面的可视性。错综相连的网络往往会导致错误或配置问题，给不断演变的复杂威胁带来可乘之机。

组织如何才能重新获得对网络的控制并实现一致性？首先要转变观念，采用以防火墙为基础、以防火墙为中心的集成化安全方法。

防火墙仍然是组织网络安全策略的基石。但随着网络不断发展，防火墙也必须与时俱进。过去，防火墙是位于入口/出口“边界”的单个设备，充当策略驱动的控制点，用来允许或拒绝网络流量。为了在当今的全数字化业务领域取胜，组织需要超越单一防火墙思维，建立“防火墙防护”思维 – 这是一种策略驱动的方法，旨在从战略角度出发，在整个异构网络的逻辑控制点之间协调高级安全保护。

要更好地保证安全措施与不断变化的业务和网络需求保持一致，防火墙防护是关键。思科一直在努力以自有防火墙为基础，打造集成化安全平台，帮助企业顺利实现过渡。

> “防火墙仍然是组织网络安全策略的基石。但随着网络不断发展，防火墙也必须与时俱进。”

借助防火墙防护，正在进行全数字化转型的组织不仅能把握当下，巩固安防壁垒，而且能着眼未来，保障业务安全。

第 1 部分：防火墙的历史

网络安全形势的发展

过去，防火墙作为网络边缘的网守，充当全面的控制点，在网络流量经过此边界时进行检测。防火墙位于网络的入口点/出口点，负责验证通信：内部网络流量本质上被认为是可信的，而外部流量本质上被认为是不可信的。在此单个控制点创建并实施规则集和策略，以确保允许所需流量进出网络，并阻止不需要的流量。

将网络边界比作城堡周围的护城河的话，防火墙就像一座吊桥，控制着进出堡垒的所有流量。

传统网络安全方法

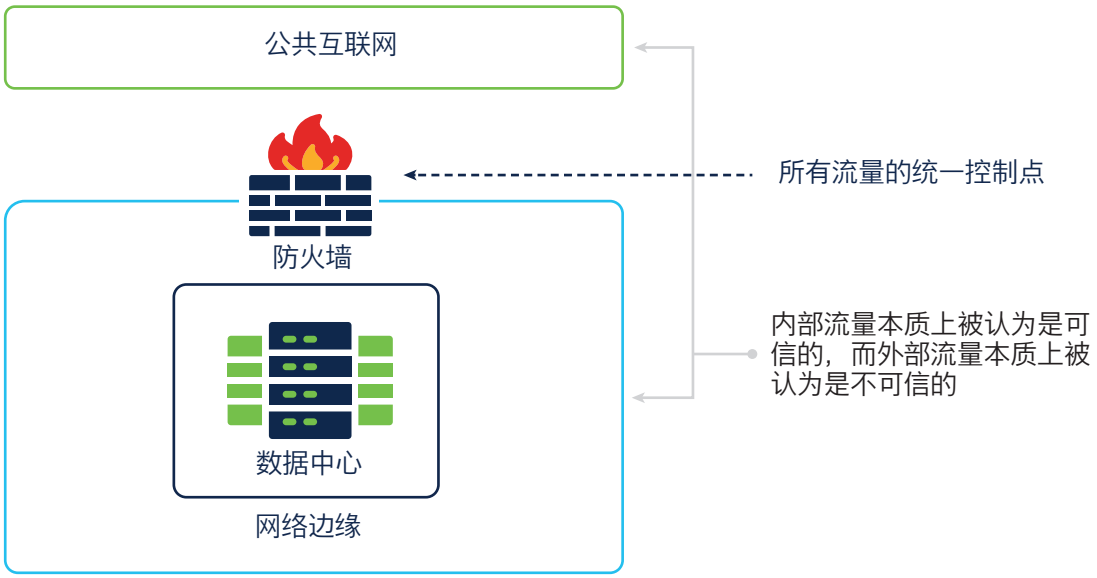


图 1. 传统网络防火墙方法

云和应用日益成为主流。

没过多久，这种通过单个控制点实施安全策略的做法就受到了挑战。首先，远程访问和企业移动技术开始兴起。但是，云计算实现了真正的转型。当业务迁移到云时，设备和用户开始大规模迁移到受控内部网络之外，使得单个控制点模式不再有力。很快就出现了多个边界，而且全都需要受到保护。此时还没有可以全方位保护网络安全的方法。

如今，分支机构位置、远程员工以及云服务使用量的不断增加促使更多数据远离传统 “边界”，完全绕过了传统的安全控制点。此外，许多企业都采用了自带设备 (BYOD) 模式，允许员工用自己的私人计算机或移动设备访问敏感的业务应用。事实上，有超过 67% 的员工在工作中使用自己的设备，且这一数字呈持续上升趋势。通过公开可接入 Wi-Fi 网络连接移动设备和笔记本电脑是一种普遍现象，甚至对日常业务运营至关重要。

此外，绝大多数企业位置和用户还需要直接访问互联网，而现在越来越多的基于云的关键应用和数据都驻留在互联网中。企业继续跨多个云服务、操作系统、硬件设备、数据库等部署工作负载。应用和数据变得更加分散，网络也随之变得更加多样化。

新形势

事实证明，这种一刀切的方法在当今形势下收效甚微。

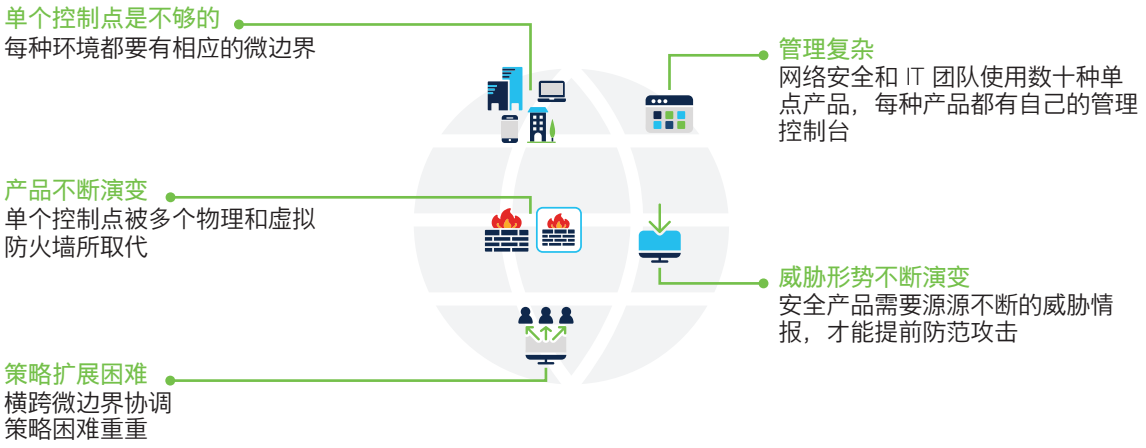


图 2. 网络复杂性和不断变化的威胁对传统的防火墙模式构成挑战

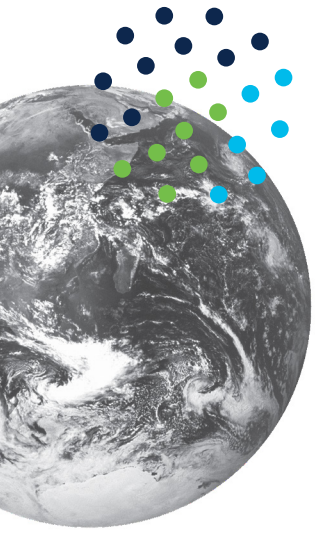
更复杂的新形势

虽然这些创新可以创造更互联、更高效的工作环境，但它们实际上从本质上改变了我们的业务开展方式。在本地进行应用控制和用户授权的时代已经演变为动态的多云生态系统，在整个企业范围内提供服务和应用。不仅如此，我们还要管理业务关键型第三方关系。大规模扩张和外包为我们带来了规模经济和效率，但也并非没有弊端。网络架构的这种演变极大地增加了我们的受攻击面，并使保护企业网络、数据和用户的工作变得更加复杂。

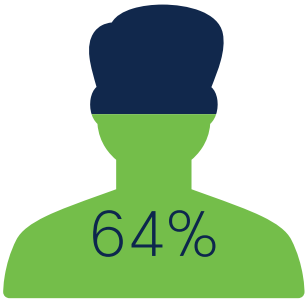
利用单点产品进行反击

为了应对这些挑战，组织通常会尝试通过添加“最佳”单点安全解决方案来解决每个新出现的问题。但是这种方法导致大量设备“无序蔓延”：平均每个企业使用多达 75 个安全工具。[1] 使用源自不同供应商的多个安全产品可能会给网络安全团队带来严重的管理问题。在大多数情况下，安全设备和功能的激增会导致攻击风险的增加。当被问及这一问题时，94% 的 IT 和信息安全专业人员担心网络复杂性的增加会使他们更容易受到攻击，88% 的人则希望网络安全策略的更改能更加灵活。[2]

2019 年 1 月至 7 月期间，共披露 3,800 起数据泄露事件，比 2018 年上半年激增 54%。[3] 这种急剧攀升证明，恶意攻击者们正利用日趋先进的方法来入侵网络。另一方面，成功入侵率不断上升，更是证明传统的网络安全方法已经无法抵御新式威胁。



1 “深度防御：停止支出，开始整合”，CSO，2016 年 3 月 4 日。
2 “应对网络安全复杂性”，ESG 研究洞察报告，2019 年 6 月。
3 “应对网络安全复杂性”，ESG 研究洞察报告，2019 年 6 月。



人为错误是造成配置错误的主要原因

威胁增加，干扰和风险也与日俱增

从邮件到 BYOD 策略下未经审查的终端，再到 Web 门户和物联网设备，攻击者不断将魔掌伸向新媒介，组织也被迫尝试其他方法来保护自己。

如上所述，引入单点产品的趋势并不能改善组织的总体安全状况。事实上恰好相反。此举给安全团队进行管理带来了更多的“干扰”。虽然他们时刻警惕不可避免的新攻击和试图利用任何漏洞（无论是已知漏洞还是未知漏洞）的恶意软件，但复杂性的增加使得创建、管理和实施安全策略的工作变得更加困难。

为了做出应对，网络安全团队不断努力配置大量云资源，这进一步增加了可能导致漏洞的安全配置错误的可能性。这主要是因为不采取安全控制措施或采取了有问题的安全控制措施导致的：64% 的组织表示，人为错误是导致错误配置的主要原因。[4] 无论这样的错误是会导致违反合规性、网络中断还是向攻击者敞开大门，都是您承担不起的风险。

是时候重新思考防火墙了

网络安全已成为一项艰巨任务。如今的人员无法再继续尝试管理大量的单点安全解决方案、云资源和设备。我们必须寻求不同以往的方法。

我们需要将防火墙作为敏捷、集成网络安全平台的基础，从而为企业当前和未来的发展提供支持。

第 2 部分：从防火墙到防火墙防护

为什么选择防火墙防护？

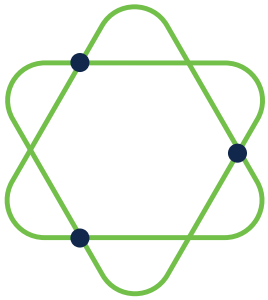
网络不断发展以适应新的业务方式，网络安全也必须跟上。在当前的分布式 IT 资产环境中，防火墙仍然是强健安全态势的核心。

不过，对防火墙的要求已大大提高：需要保护各种网络基础设施、互联设备和操作系统免受高级威胁的攻击。因此，我们通过混合使用物理和虚拟设备来增强“传统”防火墙设备，将一些设备嵌入到网络中，另一些则作为服务，以托管方式或包含在公共云环境中提供。有些设备甚至采用了新的外型，例如可根据大流量需求进行扩展的集群式设备、在个人设备上运行的软件、SD-WAN 路由器以及安全的互联网网关。在这些不同的防火墙设备（无论其位于何处）之间共享威胁情报的活动对于实现统一的威胁可视性和强大的安全态势至关重要。

为了实现全面转变，更好地保护当今的网络，企业必须摆脱传统的“边界”方法。取而代之的是，他们必须在整个网络交换矩阵中建立策略实施点，进一步靠近需要保护的信息或应用。具体而言，在物理和逻辑控制点创建微边界是形势所需。

我们不太需要把防火墙看作独立的物理网络设备，而应该更多地考虑*防火墙*防护的功能。

4 “云安全漏洞和人为错误”，Fugue，2019 年 2 月 7 日。



什么是防火墙防护？

毫无疑问，防火墙比以往任何时候都更重要。事实上，要保护当今的网络安全，我们需要在**所有位置部署更多防火墙**。不同之处在于，防火墙防护侧重于**如何**在所有位置建立基于策略的控制：

防火墙防护可以提供一种敏捷的集成方法，在您日趋复杂的异构网络中集中策略、高级安全功能和一致的实施。它应该提供全面的保护、可视性、策略协调以及更强大的用户和设备身份验证。防火墙防护还应利用在所有控制点之间共享威胁情报带来的优势，提供统一的威胁可视性和可控性，从而大幅减少威胁检测、调查和补救所需的时间和精力。

这样一来，防火墙防护便成为眼下保护复杂网络安全的关键策略。而且，它还能随着您企业的发展以及威胁形势的不断演变，为您搭建通向未来的桥梁。

它是什么样的？

无论是保护云中、本地还是远程位置的资产和数据，防火墙都需要以一致方式提供高级威胁保护、策略实施和共享威胁情报。挑战在于如何在部署和利用不同设备的不同环境中实现这样的一致性。

安全漏洞可能源于任何可以访问互联网的设备，无论它位于公司总部、数据中心、远程站点、公共云还是员工开展远程工作的任何位置。正因为如此，现在比以往更加需要在更多逻辑位置部署一套严密的安全控制点，来减少暴露并降低风险。安全控制可根据需要应用于自有环境（物理或虚拟设备和网络设备，如路由器）以及非自有环境（安全即服务 [SECaaS]）、本地控制和工作负载。

什么是防火墙防护？

在当今的异构网络中，实施点无处不在。

防火墙防护通过一致的策略和威胁可视性提供一致的威胁防御功能，因此您可以随时随地更快、更准确地预防、检测和阻止攻击。

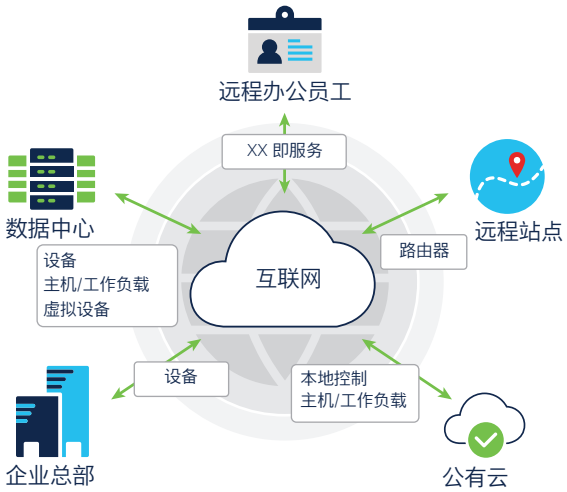


图 3. 使用防火墙防护来解决现代网络安全挑战的核心租户

扩展安全控制

对于传统防火墙，由于所有内部流量和授权用户本质上都是可信的（外部流量是不可信的），因此对整个组织的保护是在网络边界完成的。此网络边界成为了保护整个组织的逻辑安全控制点。所有网络流量（无论是来自总部、数据中心还是远程员工）都通过这一个控制点进行传送。

当然，这种模式在当今复杂的环境中已经不再有效，因为组织的 IT 基础设施有各种各样的外型和交付模式，包括物理和虚拟设备、网络嵌入式路由器或交换机、作为服务交付、基于主机或包含在公共云中。

通过防火墙防护方法，组织可以部署一致的安全控制，以提供全面的可视性、统一的策略和全面的威胁可视性。这些安全控制可在日益异构的环境中实现更强大的用户和设备身份验证。它们会收集、共享和响应有关用户、位置、设备等的情景，以确保设备满足定义的安全要求。通过在每个微边界使用一致的安全控制，安全团队可以开始自动执行任务（例如自动隔离不合规的用户和设备，跨所有安全控制阻止可疑域，以及支持有效的微分段）。在防火墙防护过程中，全面的可视性可以提供所有安全警报和感染指标的整体视图，而共享威胁情报则可对任何互联设备进行最新的威胁检测。

基于云的管理

传统解决方案的症结不仅在于单点产品。网络边界和云资源的激增也增加了暴露于漏洞的风险。在管理各种安全产品的同时，在复杂的云环境中保护企业最为宝贵的资产绝非易事。安全团队需要即时可视性和简化的管理来帮助减少配置错误。

防火墙防护支持基于云的集中管理，帮助安全团队降低复杂性并使整个组织的策略保持一致，从而增强安全态势。通过使用模板，只需编写一次策略，即可将其实施扩展到整个网络中的数万个安全控制点，从而改善策略设计和一致性。使用标准策略模板快速部署新设备有助于减少配置错误。随着组织的发展，新的部署会自动继承最新策略。可扩展的策略管理系统可将多个安全功能集成到单个访问策略中，并跨安全设备优化策略，以发现不一致并快速更正。

更重要的是，基于云的集中管理解决方案将团队的能力提升到了新的水平，可以确保他们在所有设备上快速发现风险，提高设备的一致性和安全性。借助单个管理控制台，可以在所有设备之间比较对象，发现不一致并优化当前安全状况。人员可以简化策略管理，提高效率，并在降低复杂性的同时实现更一致的安全性。

利用威胁情报进行反击

随着网络边界的扩大和直接连接到互联网的设备数量激增，我们的受攻击面也在扩大。涉及恶意软件、加密货币、网络钓鱼和僵尸网络活动的网络安全威胁在形式上不断升级，网络犯罪分子把目标转向机器学习和人工智能，以利用现有的软件漏洞并加速恶意攻击。很少有组织拥有充分的资源来全面测试和评估是否所有软件供应商漏洞补丁都符合要求，大多数组织都要艰难抵御新出现和不断演变的威胁。

防火墙防护还有一个引人注目的功能，在这方面可能有所帮助。它利用行业领先的威胁情报和最新的威胁研究（有些几乎是即时的），并可以访问保护更新，有助于缓解源源不断的威胁。威胁研究人员快速识别感染指标，并快速确认和共享威胁。他们利用的是规模经济，目标是在威胁发生之前保护组织免受这些威胁的影响。跨互联网络、终端、工作负载和云环境共享威胁情报有助于安全团队关联看似没有关联的事件、消除干扰并更快地阻止威胁。

不使用防火墙防护有哪些风险？

随着网络技术不断发展，组织积极进行调整，部署各种单点产品来支持业务需求和运营。随着新的攻击媒介被公之于众，组织又采取了和过去相同的做法，增加了一款又一款产品来防御各种最新的威胁。而那些依赖传统防火墙跨多个边界保护每台互联设备的企业面临着将其最宝贵的数据和资产暴露于安全漏洞的风险。根据《2019 年网络安全年鉴》，到 2021 年，全球网络犯罪每年带来的损失将达到 6 万亿美元。[5]

这些威胁可能会迅速渗透到网络中，并危及缺乏全面网络安全和终端可视性的企业的运营。

也就是说，无论组织的网络、云环境、设备和数据位于何处，保护它们都是安全团队的巨大负担。

防火墙防护始于防火墙，终于防火墙，它是面向未来的网络安全的基石

思科一直在努力将这一愿景变为现实。我们与全球各种规模的企业合作，他们都需要将更为敏捷、更为集成的网络安全融入网络本身。正因为如此，我们提供了迄今为止最安全的架构，这是一个以防火墙为基础的强大而全面的平台。

通过这一概念提供前所未有的保护水平是思科安全策略的重要组成部分。思科安全产品组合和思科防火墙系列提供世界一流的安全控制、一致的策略和可视性，以及可改善安全运营的创新，随时随地满足您所需，让您提前防范不断演变的威胁。

在这个威胁形势比以往任何时候都更加多变的时代，思科将网络领导地位与尖端技术相结合，让您在当下和未来都可以拥有最强大的安全保护。

5 “2019 年网络安全年鉴：100 个事实、数字、预测和统计数据”，Cybercrime Magazine，2019 年 2 月 6 日。

传统防火墙提供的可视性有限；IT 人员需要通过共享威胁情报提高整个网络的可视性，以便更早、更快地检测和阻止威胁。防火墙防护则更进一步，基于统一管理和全面的安全功能（如入侵防御、URL 过滤以及利用自动化和机器学习高效防御高级恶意软件）打造全面的安全防护态势。

如果缺乏适当的防火墙防护策略，网络复杂性可能会导致错误配置，从而增加安全漏洞的风险。根据 Gartner 的报告，“到 2022 年，将有至少 95% 的云安全故障归因于客户失误。”[6] 通过采用跨多个控制点来协调安全策略的防火墙防护策略，组织可以改善总体安全状况。

第 3 部分：制定防火墙防护策略的四个步骤

第 1 步：借助现代化的下一代防火墙，为成功实施防火墙防护策略奠定基础。合适的 Cisco Secure 防火墙能为您的集成安全解决方案提供一致的安全策略、可视性和更出色的威胁响应。

第 2 步：选择 Cisco Secure 防火墙之后，下一步是实现管理解决方案的标准化。在确定哪个解决方案适合您的组织时，请考虑以下因素：

- 确定首选管理位置（本地还是云）以及由哪个团队（安全运营还是网络运营）负责管理安全。
- 最重要的是，确保管理解决方案与 IT 团队的当前和未来目标保持一致。如果您要将工作负载迁移到云，启动供应商门户，或者处理全数字化转型项目或 SaaS 应用，您可能希望采用基于云的管理。如果您的组织依赖于单一的传统应用，那么本地应用可能比较适合您的需求。一般来说，传统应用需要进行一定程度的重构才能在云上正常运行。如果没有立即升级这些应用的计划，通常最好使用本地管理系统。
- 基于云的管理解决方案可帮助网络运营团队确保整个组织的策略一致性，降低复杂性，并从中央控制面板管理所有安全控制点。它可简化从一个位置一致地协调和管理策略的过程，以防御最新威胁。借助基于云的集中式应用，您可以简化安全管理，使用模板更快地部署新设备，并跟踪整个环境中随时间发生的所有变化。

第 3 步：通过集成改善您的安全状态。您的防火墙防护策略应该全面覆盖所有微边界，并提供对所有互联设备和安全解决方案的保护和控制。在整个异构网络中跨云应用和服务、公司邮件以及所有互联终端集成安全性可以帮助您的企业抵御不断扩大的威胁形势。

此步骤可让您的安全团队阻止更多威胁，更快地响应高级威胁，并在整个网络、云应用和终端范围内实现自动化。

第 4 步：最后，要确保您的防火墙防护策略包含持续的高级威胁分析，以保护您的企业资产，并助您提前防范各种新型威胁。最简单的方法之一是选择一种能通过防火墙自动向您的网络提供最新威胁信息的解决方案。最新的情报和全面的可视性使安全团队能够了解最新的漏洞。而且，如果威胁侵入内部，您可以确定威胁是在哪里发生的，如何发生的。内置的下一代 IPS 功能可自动确定风险等级和影响标志，以确定优先级，以便识别最关键的资产和信息并进行优先保护。安全团队可以立即采取纠正措施并对威胁进行补救，将重点放在最关键的资产上，不会由于重重 “干扰” 不堪重负，从而使 SOC 运营更加安全。

6 “云是否安全？” Gartner，2018 年 3 月 27 日。

首先以合适的防火墙为基础

当今的安全团队需要:

获得更出色的安全保护。这需要以行业领先的威胁情报为后盾，保护您的复杂网络，更早地发现威胁并更快地采取行动。

在整个网络中**高效设置、扩展和协调安全策略**的方法。

获得可视性并降低复杂性，通过统一管理和自动化，加快安全运营并改善运营体验。

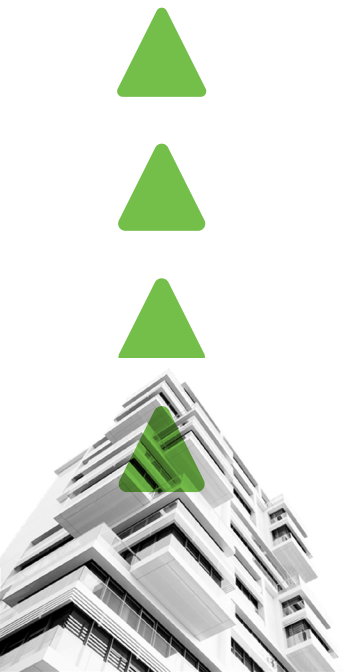
实现网络和安全功能的融合，最大限度发挥您的现有投资的作用。合适的解决方案可以提供一系列深入的集成功能，实现全面安全，从而随时随地保护所有内容。

采用 Cisco Secure 防火墙的防火墙防护策略的优势

将整个网络转变为安全架构的扩展：通过与 Cisco Secure 防火墙共享通用策略、入侵防御功能和其他核心功能，交换机和路由器可以执行安全策略，将网络基础设施融入到全面的安全产品组合中。在整个架构中快速共享威胁情报，关联看似没有关联的事件、消除干扰，并更快地阻止威胁。

世界一流的安全控制：Cisco Secure 防火墙提供卓越的威胁防御功效，可保护您的复杂网络免受当今日趋复杂的攻击。行业领先的高级威胁情报可帮助您的组织发现新的恶意软件域和恶意 URL 以及未知或未公开的漏洞，以便更早地检测到威胁并加快响应速度。内置的下一代 IPS 功能通过自动确定风险等级和影响标志提供全面的可视性，为您的安全团队确定优先级，最大限度地减少干扰。追溯性安全功能让您可以随时了解情况，并在初始检测后持续分析威胁，以便更好地识别最初可能未检测到的复杂恶意软件。

统一的策略和威胁可视性：安全团队可以通过在每台设备 （从网络设备到主机）以及整个云中标准化和推动安全控制，实现策略一致性和协调。思科灵活的集中管理让您的团队能够快速轻松地将可扩展控制应用于多台设备，以保持策略的一致性。通过紧密集成应用防火墙、NGIPS 和 AMP 等安全功能实现统一管理和自动威胁关联，以降低复杂性。简化扩展网络中的安全策略和设备管理，并加快关键安全运营（例如检测、调查和补救）。



第 4 部分：面向未来的安全解决方案

我们的工作方式已不同以往。我们的业务和网络都发生了转变，网络安全规则也随之变化。这些发展要求我们重新思考防火墙，积极采用防火墙防护。

思科正在通过安全平台推动创新，以行业领先的威胁情报为后盾，通过一致的安全策略和可视性，随时随地为您提供世界一流的安全控制，以应对这些趋势。最新一代 Cisco Secure 防火墙为我们紧密集成的产品组合奠定了基础。

Cisco Defense Orchestrator 作为思科的旗舰云管理解决方案，可实现各种思科安全产品的策略协调。

内置在每款思科安全产品中的 Secure Threat Response 是一种自动化威胁响应解决方案，通过在整个安全架构中自动共享和部署对策来应对新的网络攻击。

Secure Endpoint 将全球威胁情报、高级沙盒和实时恶意软件拦截功能集于一身。它能够持续分析整个扩展网络中的文件活动，以便快速检测、遏制和清除高级恶意软件。

Talos 威胁情报团队是由全职威胁研究人员、数据科学家和工程师组成的一流团队，负责收集现有威胁和潜在威胁的信息。Talos 团队支撑着整个思科安全生态系统，并提供针对攻击和恶意软件的防护。Talos 团队提供最新全球威胁的相关资讯，有关威胁防御和缓解的切实可行的情报，以及积极保护所有思科客户所采取的集体应对措施。

SNORT 下一代入侵防御系统 (SNORT NGIPS) 是行业领先的开源 NGIPS，可执行流量分析、数据包嗅探/日志记录和协议分析。SNORT NGIPS 利用 Talos 威胁情报，通过共享策略来防御不断发展的威胁，为整个安全社区提供助力。

借助身份服务引擎 (ISE)，您可以随时随地进行基于环境的自适应可信访问。它通过基于意图的策略和合规性解决方案提供智能、集成的保护。

基于 Duo 的 Cisco Secure Access 通过远程访问和单点登录提供多因素身份验证、终端可视性、自适应身份验证和策略实施，以主动保护对应用的访问。

Cisco Secure Network Analytics、Cisco Secure Workload 和以应用为中心的基础设施 (ACI) 协同工作，随时随地密切关注用户及其应用负载，使用机器学习、行为建模、网络基础设施遥测和分段来智胜新型威胁。

您可以通过投资思科安全平台和 Cisco Secure 防火墙，实施面向未来的防火墙策略。您将获得当今最强大的安全保护，并为未来的发展做好准备。

第 5 部分：着手构建面向未来的防火墙

思科将领先网络与尖端安全技术相结合，提供了迄今为止最安全的架构。无论是通过优化现有投资来增强您的网络安全，还是助您实现从路由器到防火墙的转型，思科一直在不断创新。

Cisco Secure 防火墙是专为正在进行全数字化转型的企业而设计的网络安全解决方案，由构建网络的公司提供。

了解有关 Cisco Secure 防火墙的更多信息，立即开始构建面向未来的防火墙。您可以在《2020 年全球网络趋势报告》中进一步了解决定未来网络发展动态的最新趋势。