超越应用可视性与可控性：NGFW 必须具备的要素

超越应用可视性与可控性：下一代防火墙 (NGFW) 必须具备的要素

概述

随着现代网络及网络组件不断发展，传统下一代防火墙已无法提供组织所需要的保护级别。

在本白皮书中，您将了解到以下内容：

- 为什么主要专注于应用可视性与可控性的典型下一代防火墙无法提供充分的威胁防御
- 组织怎样才能在资源有限的环境中防御高级威胁
- 借助 Cisco Firepower™ 下一代防火墙（业界首款专注于威胁的全面集成型 NGFW），您可以获得哪些优势

简介

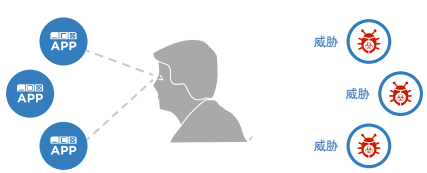
数字化转型正在席卷各行各业，并且带来了巨大的商机。目前，已有超过 150 亿部设备连接到互联网。到 2030 年，这个数字预计将增长到 5000 亿部。[1] 在未来 10 年里，数字化转型预计将为全球各地的企业带来 19 万亿美元的商机。[2] 不过，这场转型也为网络犯罪制造了温床。全球网络犯罪市场当前的价值预计为 4500 亿美元到 1 万亿美元。[3]

随着现代网络及网络组件不断发展，受攻击面也在不断增大。受利益驱使，攻击者开始越来越多地采用高度复杂的方法来开展网络渗透活动，窃取越来越多的数字化资产。一旦攻击者侵入网络，就很难检测到他们。实际上，业界的高级威胁检测时间中值约为 100 天。[4]

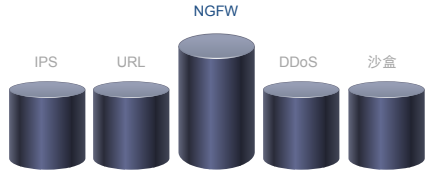
当今的网络安全挑战

要抓住数字经济和新业务模式所创造的新兴商机，安全是大前提。下一代防火墙 (NGFW) 的推出是业界向前迈出的重要一步，但是典型的 NGFW 在很大程度上侧重于应用访问控制，而很少关注威胁防御功能。在抵御经验老道的攻击者和高级恶意软件所带来的风险方面，这种不完善的方法收效甚微。更糟糕的是，当组织感染恶意软件后，这些 NGFW 所能提供的帮助非常有限，因为它们无法帮助您确定感染范围、遏制恶意软件，并快速予以补救。

传统的 NGFW 的侧重点非常有限而且管理十分困难



专注于应用，而非威胁



带来额外负担的管理孤岛

就组织而言，他们或者会因为资源有限而无法添加更多产品，或者会因为没有安全人员而无法应对这种分散的方法所带来的额外复杂性。事实上，资源限制是阻碍采用更好的安全解决方案的最常见问题。[5] 此外，以这些互无联系的安全服务为基础的架构通常很脆弱，会因为缺乏运营灵活性而抑制业务增长。

1. 思科物联网网站：http://www.cisco.com/web/solutions/trends/iot/indepth.html
2. http://ioeassessment.cisco.com/learn
3. RSA/CNBC：http://www.cisco.com/web/offer/emear/38586/images/Presentations/P16.pdf
4. 思科 2016 年度安全报告
5. 思科 2016 年度安全报告

NGFW 必须具备的要素

组织需要从其 NGFW 平台中获取更多价值。他们希望下一代防火墙具备以下特性：

- 注重威胁防护效力，而且能够在整个攻击过程（攻击前、攻击中和攻击后）提供全面保护
- 将所有安全服务和事件信息完全集成到单个视图和管理平台
- 与现有安全投资相集成，并实现“1+1>2”的效果

符合这些要求的下一代防火墙不仅有助于实现精准的应用控制，而且还能针对具有规避能力的复杂恶意软件攻击所造成的威胁提供切实可靠的安全防护效力。这种防火墙可以帮助组织简化运营，并从其网络中获得更多价值。

Cisco Firepower NGFW 简介

Cisco Firepower 下一代防火墙 (NGFW) 是业界首款专注于威胁的全面集成式 NGFW。它超越了传统 NGFW，可提供涵盖整个攻击过程的集成式防护。

借助 Cisco Firepower NGFW，您将拥有不仅专注于应用控制的集成安全平台。它能够关联来自多种媒介的信息，这个强大的功能有助于检测具有规避能力或可疑的活动，并及早确定存在危害迹象的主机。您将能够获得以下优势：阻止更多威胁；获得更出色的网络可视性；更快地检测并缓解零日威胁和针对性威胁；通过将关键任务自动化，更好地将工作重点放在对组织有益的工作上；最大限度地利用现有资源。

提供全面的防护

Cisco Firepower NGFW 不仅具备全球部署最为广泛的状态防火墙技术，而且集成了下一代 IPS、高级恶意软件防护、应用可视性与可控性、基于信誉的 URL 过滤等功能。所有这些功能均通过单个设备提供， 并通过内容丰富的统一管理控制台进行管理。

Cisco Firepower NGFW：提供涵盖整个攻击过程的防护

阻止更多威胁

您应部署具有业界最高威胁防护效力的下一代防火墙，来应对各种已知威胁和新型威胁。我们的 NGFW 将集成式沙盒解决方案及文件流行度与文件安置功能结合到一起，旨在帮助您发现具有规避能力的针对性威胁，并在其对系统造成损害之前将其阻止。

获得更出色的可视性

Cisco Firepower NGFW 可帮助您了解不断变化的网络中存在的用户、主机、应用、移动设备、虚拟环境、威胁和漏洞。这些信息有助于您保护网络。NGFW 会自动将威胁与您网络中的漏洞相关联，这样，您的安全团队就能确定威胁的优先级，然后将重点放在最严重的威胁上。

加快检测和响应速度

Cisco Firepower NGFW 能够更快地缓解高级威胁，将检测和补救的时间从数月缩短至数小时： 思科可以在 17.5 小时内完成这些任务。[6] 我们可以帮助您立即了解恶意软件感染的范围，确定文件活动的路径和行为，甚至能够在签名发布之前实施遏制操作。

降低复杂性并简化运营

我们将所有安全功能整合到一个采用单一管理界面的高性能平台中。Cisco Firepower 管理中心可实现策略的统一、集中和简化，帮助减轻管理深度防御安全架构的负担。该管理中心会自动分析网络漏洞，并就保护措施提出建议，确保为当今人员不足的动态环境提供响应迅速的解决方案。

从您的网络中挖掘更多价值

Cisco Firepower NGFW 可以与其他思科® 安全解决方案（例如用于识别数据和网络分段的思科身份服务引擎 [ISE]）以及 OpenDNS 相集成，从而提供互联网范围内的域可视性。不仅如此，它还能够与其他思科安全产品共享情报、情景和策略控制，这有助于提高效率和敏捷性，并降低管理的难度和成本。自动化网络分段功能有助于您快速遏制威胁。来自思科 Talos 的全球 DNS 和 IP 威胁情报可以为早期预警提供信誉威胁指标，从而保证网络安全设备能够在攻击来临之前做好防御准备。

Cisco Firepower NGFW 可以保证客户更安全、更快速地缓解高级威胁，并且更有效地简化运营。这样一来，安全就能成为助力您把握新商机的增长引擎。

了解详情

有关 Cisco Firepower 下一代防火墙的更多详情，请访问：www.cisco.com/go/ngfw

6. 思科 2016 年度安全报告

C11-736644-00 02/16