# 中小企业和分布式企业的 NGFW 要求

## 中小企业的 NGFW 案例

注重威胁防护的下一代防火墙 (NGFW) 可以有效地降低风险，而传统的统一威胁管理 (UTM) 和单点解决方案都无法做到这一点，大量研究中都突出证明了这一点，其中包括来自思科的一项研究。在该报告中，每个组织都应承认被黑客攻击过。思科威胁研究人员发现，在他们所观察的所有企业网络中都可以发现恶意流量。有证据表明，网络攻击者曾渗透到这些网络中，而且其操作可能在很长一段时间内都未被发现。[1]

当今世界，存在多方位的持续威胁、不安定的 IT 环境和不断增加的用户移动性，这些因素促使更多的组织寻求能够提供经济高效的分层威胁防护的 NGFW 功能。虽然有许多解决方案也力求满足这一需求，但目前能提供有效安全性所需的全部功能的 NGFW 仍寥寥无几。

不是只有大型组织，**任何组织，无论规模大小**，都面临着严峻的安全挑战。据美国国家网络安全联盟在 2004 年的报道，41% 的定向网络攻击都集中攻击员工人数少于 500 人的组织。此外，《纽约时报》在 2014 年报道，越来越多的中小企业被他们较大型的合作伙伴要求采用更强大的威胁防卸计划。高级威胁防御成为热门议题并不奇怪，因为任何规模的企业都力求更好地保护他们的客户数据、员工信息、知识产权和企业机密内容。

因此，很明显小型企业目前迫切需要使用包括 NGFW 在内的高级威胁防卸功能。“2015 年思科安全功能基准研究”[2]对来自九个国家/地区的中端市场组织（500 – 999 名员工）的数百位 IT 专业人士进行的采访。该研究反映了更大规模的同行组织在以下几个方面的安全准备状况，这包括：

- **事件响应：**92% 的中型组织内部设有事件响应团队，而大型企业为 93%。
- **高管责任：**94% 的中型组织由一名高管直接负责安全事务，而大型企业为 92%。

NGFW 过去一直都是大型组织以最佳方式部署的安全工具。时至今日，部署网络安全时，中小企业和分布式企业通常在两个选项之间进行选择：提供不太有效的威胁缓解功能的 UTM 解决方案，或具有状态防火墙、应用控制、IPS 和高级恶意软件防护等单一功能的多个解决方案。这两个选项对中小企业而言都是不够的：要么勉强接受 UTM 中并不理想的威胁防卸功能，要么面临多个单点解决方案带来的巨额集成和管理成本。但是，现在有了一个新选项：**专为中小企业和分布式企业量身定制的 NGFW。它包含高级威胁防范功能，具有总拥有成本低和管理灵活的优势。**

本白皮书可帮助小型企业或分布式企业确认他们需要投资有效的 NGFW 解决方案。对于小型企业，NGFW 应提供经济实惠、易于管理的高级威胁防护方式。在分支机构和分布式企业中，NGFW 应提供检测和实施点，以便分析实时威胁和大规模的网络流量，并从其集成而全面的网络视图中获益。在这两种使用方案中，NGFW 可帮助您的组织防御有针对性的、持续的恶意软件攻击，其中包括新出现的威胁。

## 核心网络安全解决方案的评估标准

您是否评估 NGFW 或 UTM，对确定以下三个关键的成功因素非常重要。您的 NGFW 解决方案必须是：

- **专为中小企业和分布式企业而定制**
- **专注于威胁，可以提供有效的信息安全和高级恶意软件防护**
- **降低复杂性和成本**

[1] 思科 2014 年度安全报告：http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf。
[2] 思科 2015 年度安全报告：http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html。

### 专为中小企业和分布式企业而定制

“适合”在这里至关重要，不仅涉及到采购成本和吞吐量，还涉及到可管理性。大多数中小企业的资源有限。比如，除了许多其他的工作职责外，很多 IT 人员还要分担信息安全职责，这种情况很常见。中小企业需要能够有效管理的安全解决方案。

大型企业通常能够提供资源，来负责安全事件和事故管理 (SEIM)。而对许多小型企业而言，SEIM 可能不切实际。负责安全事务的 IT 经理通常只想了解最高优先级的威胁，以便团队能够迅速调查和解决。

管理灵活性也非常重要。随着组织的发展（例如增加远程办公室时），原始投资能保持它的价值。通常，机上管理适合单实例部署，而多实例部署受益于集中管理。

### 专注于威胁防护

通常，传统的 NGFW 和 UTM 结合使用多种安全功能，但所提供的安全功效欠佳，而且也不能提供下一代 IPS (NGIPS) 功能和高级恶意软件防护。要真正地专注于威胁防护，安全解决方案必须包括状态防火墙、NGIPS 和高级恶意软件防护，以便提供网络可视性并且能够识别和修复恶意软件活动。

除了识别威胁外，NGFW 还应该能够基于已知行为因素和可疑行为因素的关联情况，报告攻陷指数 (IoC)并监控用户活动以确定异常行为。这些工具应与 URL 信誉过滤、应用可视性和访问控制相集成，从而降低威胁暴露，并满足合规性和内部使用政策的要求。

该解决方案还必须能通过访问策略、虚拟网络分段，以及安全的站点到站点和远程访问 VPN 连接，降低常见（但非常重要）的网络风险。这个基准对于您做出购买决策，是一个非常有用的起点。例如，并非所有的第 7 层应用控制解决方案都包括一流的状态防火墙和 VPN 功能。

最后（可能也是最重要的）一点，即使同时启用多种安全服务，NGFW 必须提供通告性能。在这里，关键是要找到一个供应商，能够与您合作，适当地评估解决方案规模，来满足您的环境和安全要求并选择一个能满足今后需求的平台。

### 降低复杂性和成本

很少有组织配备专用的安全运营中心 (SOC) 或专用的安全人员。请在评估安全解决方案时提出以下问题：

- IT 专家可以使用这个解决方案吗？
- 它能减少员工花在非常耗时的活动上的时间吗，如恶意软件修复？
- 它能把分析师从识别哪些事件有意义和可行的沉闷工作中解放出来吗？
- 它能通过根据不断变化的环境自动定制策略来提供安全自动化，以帮助不断调整防御吗？
- 它能提供相关的事件视图来简化并加快事件分类和分析吗？

## 满足中小企业的需求：具备 FirePOWER 服务的 Cisco ASA

具备 FirePOWER™ 服务型号 5506-X、5508-X 和 5516-X 的 Cisco ASA，以及加强型的 5506H-X 和无线 5506W-X 变体，都能满足对卓越的威胁防范、较低的总拥有成本和管理灵活性的需求。状态防火墙、VPN 以及所有的 NGFW 功能，都组合到一个机上管理器中，即思科自适应安全设备管理器 (ASDM) 增强版，它非常适合单实例和独立部署。

如果集中管理是首选项，具备 FirePOWER 服务的 ASA 由 Cisco Security Manager (CSM) 和 Cisco FireSIGHT™ 管理中心进行管理。如果使用集中管理，仅有 NGFW 解决方案才能在整个攻击过程中提供集成的威胁防御：攻击前、攻击中和攻击后（参见图 1）。

**图 1.** 具备 FirePOWER 服务的 Cisco ASA 防火墙


具备 FirePOWER 服务的 Cisco ASA 是第一个专注于威胁防护的 NGFW，开创了威胁防卸和高级恶意软件防护的新纪元。其动态控制措施可提供无与伦比的可视性和实时威胁防范。NGFW 解决方案结合使用了**思科自适应安全设备 (ASA) 和 FirePOWER 服务**的成熟的安全功能。

## Cisco ASA

Cisco ASA 是全世界部署最为广泛的企业级状态化防火墙，具有远程接入 VPN 及高级群集功能，可实现高度安全性、高性能接入及高可用性，确保业务连续性。此外，该解决方案与 Cisco AnyConnect® 移动客户端版本 4 紧密集成，除了其他功能外，该版本还支持逐个应用的 VPN 拆分隧道。Cisco AnyConnect VPN 客户端是世界上部署最广泛的 VPN 客户端，超过 1.3 亿个客户端都在使用它。对于想使用本地 VPN 客户端的组织，许多客户端都受 Cisco ASA 支持，包括本地 Apple iOS 和 Android Samsung 客户端。

## Cisco FirePOWER 服务

### 单个平台上的一流多层威胁防护功能

Cisco FirePOWER 服务是行业领先的威胁防护和高级恶意软件防护功能，根据 NSS Labs 独立测试得出的结果，其在威胁防御有效性方面的排名位居第一。[3]

如图 1 所示，具备 FirePOWER 服务的 Cisco ASA 可以提供：

- **卓越的多层威胁防范**，对已知威胁和未知威胁均可防御，包括有目标的持续恶意软件攻击。
- **高级恶意软件防护 (AMP)**，提供行业领先的漏洞检测效能、较低的总拥有成本以及优异的防护价值。它使用大数据来检测、了解和阻止高级恶意软件爆发。AMP 提供必要的可视性与可控性，帮助阻止其他安全层未检测到的威胁。

[3] “NSS Labs Security Value Map for Breach Detection Systems: Sourcefire Advanced Malware Protection Is a Leader in Security Effectiveness and TCO”（NSS Labs 漏洞检测系统的安全价值图：Sourcefire 高级恶意软件防护是安全有效性和总拥有成本的领军者），源自 Sourcefire.com，网址为：https://info.sourcefire.com/NSSBreachDetectionReportSEM.html?gclid=Cj0KEQjw7bgBRC45uLY_avSrdgBEiQAD3Olx8BtffrsQkNYs3AtCojRqyy42V1yLfGyh78OMov3iUAaAlNc8P8HAQ。

- **下一代入侵防御系统 (NGIPS)** 提供高效的威胁防御以及对用户、基础设施、应用及内容的完全情景感知，从而能够检测多途径威胁并实现防御响应的自动化。对恶意软件文件轨迹的情景感知有助于确定感染范围和根本原因，从而缩短采取补救措施的时间。竞争对手的 UTM 和 NGFW 解决方案提供基本的 IPS 功能，但并不是 Gartner Group 所规定的完整的 NGIPS 功能。
- **精细的应用可视性与可控性 (AVC)** 通过 3000 个应用层和基于风险的控件优化安全有效性，从而可以调用定制的 IPS 威胁检测策略。
- **VPN 功能**足够强健，不仅能提供传统的站点到站点和远程访问 VPN 功能，还能提供用于移动设备的强大的 VPN 功能，其中包括面向关键企业应用的分离隧道选项，而不是面向满足个人需求的用户应用。

## 灵活的管理选项

具备 FirePOWER 服务的 Cisco ASA 提供多种管理解决方案，包括集中和机上管理器。思科自适应安全设备管理器 (ASDM) 7.3 及更高版本是推荐用于单实例部署的机上管理器。ASDM 对所有的 NGFW 功能进行整合管理，并可缩短员工专门用来管理 NGFW 的时间。对于多实例部署，具备 FirePOWER 服务的 Cisco ASA 可由 Cisco FireSIGHT 管理中心进行集中管理。它提供无与伦比的网络可视性与自动化，可以应对不断变化的情况和新出现的攻击。借助 FireSIGHT 管理中心，安全团队可以随时网络上发生的情况：用户、设备、虚拟机间的通信、漏洞、威胁、客户端应用、文件和网站。

下表 1 汇总了 Cisco FireSIGHT 管理中心与 ASDM 管理器之间的区别。

**表 1.** 对比：Cisco FireSIGHT 管理中心与自适应安全设备管理器 (ASDM)

| 特点 | FireSIGHT 管理中心（集中、机下管理） | ASDM 集成本地管理（机上管理器） |
|---|---|---|
| 概述 | 每个 FireSIGHT 实例管理多达 300 个具备 FirePOWER 服务的 ASA 传感器。FireSIGHT 和 Cisco Security Manager (CSM) 结合使用。 | 默认情况下，为本地的机上管理器提供所有配置：已针对小型企业和单实例部署优化。提供对所有产品功能的集成管理，突出易用性。 |
| 情境感知和可视性 | 扩展功能：<br>包括基本功能以及被动检测网络主机的功能、Context Explorer 功能和文件轨迹。 | 基本功能：<br>默认情况下，支持地理定位和客户端标记功能。IPS 事件可以导出到基于 SEIM 的情景感知的 SEIM。 |
| 网络 AMP | 扩展功能：<br>包括基本功能以及文件捕获、沙盒处理和动态分析。需要 FireSIGHT 以及面向终端解决方案的思科高级恶意软件防护（最大限度地提高可视性、支持客户端修复）。 | 基本功能：<br>通过文件分析检测并阻止恶意软件和禁止的文件类型。包括对思科恶意软件分析云的访问（将文件哈希发送到云中进行分析，而不是文件。） |
| 控制面板 | 扩展功能：<br>FireSIGHT Context Explorer 控制面板启用动态更新的可视化和网络环境的调查。 | 基本功能：<br>ASDM 管理器提供许可信息、系统监控和信息、FirePOWER 模块详细信息等的控制面板小组件，还提供系统信息。 |
| 自动化、影响分析、事件关联等 | 包括：<br>用于确定相关性和影响优先级的自动威胁评估、用于实时威胁响应的关联和修复功能，以及自动调整以防范新威胁的策略。 | 不可用。 |
| IPS | 扩展功能：<br>包括基本功能以及预处理器调整和 Gartner Group 所规定的完整 NGIPS 功能。 | 基本功能：<br>使用 Snort IPS 引擎并包括 IPS 规则调整。 |
| 用户/用户发现以及基于流量地理位置定位的访问控制。 | 完整功能。<br>与 Active Directory 的集成以及基于中根据流量地理定位的集成和访问控制。 | 完整功能。<br>与 Active Directory 的集成以及基于中根据流量地理定位的集成和访问控制。 |
| 应用可视性与可控性 (AVC) | 扩展功能：<br>包括基本功能以及基于正则表达式匹配的自定义应用检测器，或协议和端口检测。 | 基本功能：<br>在第 7 层启用可视性和访问控制，支持 3000 多个应用和基于风险的控件。 |
| 运行状况功能 | 扩展功能：<br>包括基本功能以及有关 30 多项功能的可定制的运行状况警报。 | 基本功能：<br>有关 CPU 和内存负载的状态。 |
| 系统策略 | 扩展功能：<br>包括基本功能以及对 17 个以上的访问控制、记录和警报功能的控制。与那些特定于单个设备的系统设置不同，此类策略在部署中通常是相似的。 | 基本功能：<br>电子邮件通知、简单网络管理协议 (SNMP) 支持和时间同步。 |
| 报告 | 扩展功能：<br>包括基本功能以及自定义模板和导出功能。 | 基本功能：<br>过滤和报告顶层流量、文件类型、用户和应用等。 |
| 活动 | 扩展功能：<br>包括基本功能以及更强大的事件存储和每秒事件数功能。 | 基本功能：<br>用于故障排除的实时事件流。 |

| 特点 | FireSIGHT 管理中心（集中、机下管理） | ASDM 集成本地管理（机上管理器） |
|---|---|---|
| API 支持 | 扩展功能：<br>包括基本功能以及修复、主机输入和数据库访问 API。 | 基本功能：<br>可与 SEIM 平台简单共享事件的 FirePOWER eStreamer API。 |

如需了解有关 Cisco FireSIGHT 管理中心的更多信息，请参阅文档“Requirements When Considering a Next-Generation Firewall”（考虑采用下一代防火墙时的要求）。

## 其他考虑因素：Cisco Security Intelligence 和威胁源

为了更有效地防范已知和新出现的威胁，组织需要一个 NGFW 解决方案来将领先的最新威胁防范情报汇聚到一起。借助从海量设备和传感器、公共和私人来源及思科开源社区处取得的遥感勘测数据，来自思科综合安全智能 (CSI) 生态系统的威胁研究人员将行业领先的威胁情报汇聚到了一起。这相当于每日提取数十亿的网页请求和数以百万计的电子邮件、恶意软件样本和网络入侵数据。

我们先进的基础设施和系统利用这些遥感勘测数据，使机器学习系统和研究人员能够跟踪跨网络、数据中心、终端设备、移动设备、虚拟系统、网络、邮件以及来自云的威胁，以找出威胁的产生根源和爆发范围。我们将由此产生的情报转化为对我们产品和服务的实时保护，并立即交付到全球各地的思科客户手中。CSI 威胁源让思科安全解决方案一直保持最新状态。

如果您选择具备 FirePOWER 服务的 Cisco ASA 作为 NGFW 解决方案，您将会获得：

- Cisco SMARTnet 服务
- 投资保护
- 服务和技术支持

### Cisco SMARTnet 服务

此服务包括一年 365 天、每天 24 小时提供技术支持，以及灵活的硬件保修范围。思科已连续 5 年 （即总第 8 年）通过 J.D.Power 认证技术服务和支持计划获得 J.D.Power 认证。[4]

### 投资保护

Cisco Capital® 融资可满足您对业务和预算的各项要求。凭借 Cisco Capital 融资的公平市值租赁，您只需支付设备使用费，而不是设备所有权费用。您可以根据需要，灵活地升级或更新设备，杜绝技术过时。

### 思科服务和支持计划

具备 FirePOWER 服务的 Cisco ASA 提供的思科服务和支持产品包括：

- **适用于防火墙的思科迁移服务**：由思科或思科安全专业化合作伙伴提供。这些服务可帮助组织轻松迁移到具备 FirePOWER 服务的 Cisco ASA。思科提供专家指导和支持，帮助您在迁移过程中保持安全，并确保流程的准确性和完整性。
- **思科远程管理服务**：借助这些服务，您可以不间断地管理安全要求，这样您的 IT 资源就可以专注于其他优先事项。
- **思科网络优化服务**：通过改进网络运营、策略合规性和网络可靠性，这些服务显著提高了 ROI，根据 Forrester Research 的研究表明，ROI 超过了 120%。[5]

[4] J.D Power 媒体于 2014 年 7 月 21 日发布的“Cisco Recognized for Excellence in Certified Technology Service and Support Program for a Fifth Consecutive Year and Eighth Year Overall”（思科在技术服务和支持计划认证领域连续 5 年（即总第 8 年）被公认为表现突出）认证， 网址为：
http://www.jdpower.com/press-releases/certified-technology-service-andsupport-program - sthash.7oyGxBUo.dpuf。

[5] The Total Economic Impact™ of Cisco SP Network Optimization Service and Focused Technical Support，Forrester Research 为思科编写的报告，2009 年 11 月：http://www.cisco.com/en/US/services/ps6889/TEI_of_SP_NOS_FTS_Forrester.pdf。

## 更多详情

如需了解有关 Cisco NGFW 解决方案和服务的更多信息，请访问：

- 有关具备 FirePOWER 服务的 Cisco ASA 防火墙的更多信息，请访问 www.cisco.com/go/asafps
- 有关 Cisco ASA 5500-X 下一代防火墙的更多信息，请访问 www.cisco.com/go/asa
- 有关适用于防火墙的思科迁移服务的更多信息，请访问 www.cisco.com/go/services/security
- 有关 Cisco SMARTnet 服务的更多信息，请访问 www.cisco.com/go/smartnet
- 有关当地 Cisco Capital 代表的更多信息和相关链接，请访问 www.ciscocapital.com
- 有关 Cisco Meraki 解决方案的更多信息，请访问 www.meraki.cisco.com
- 如需随时关注最新趋势和思科新增的安全功能，请访问 www.cisco.com/go/mmsecurity
- 思科合作伙伴如需了解最新的解决方案公告和活动，请访问 www.cisco.com/go/partnermidmarket


**美洲总部**
Cisco Systems, Inc.
加州圣荷西

**亚太总部**
Cisco Systems (USA) Pte, Ltd.
新加坡

**欧洲总部**
Cisco Systems International BV Amsterdam.
荷兰

思科在全球设有 200 多个办事处。www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。





美国印刷 C11-734294-00 04/15