# 思科网络安全设备

在安全性方面，您的网络需要恶意软件防护、应用可视性与可控性、可接受使用政策控制、有深刻见解的报告，以及安全移动性等各种功能。思科将所有这些功能都集成到思科® 网络安全设备 (WSA) 这个单一平台上，为您提供这种全面而强大的保护。

在我们高度互联且日益移动化的环境中，复杂的威胁越来越多，这就要求我们使用最佳组合的安全解决方案。思科保障网络基础设施所有层的安全，包括提供强大的保护、完全控制和企业所需的投资价值。我们还提供一系列多方面的网络安全部署选项，以及市场领先的全球威胁情报。思科 WSA 使用性能优越的专业设备简化安全部署。此外，通过思科网络安全虚拟设备 (WSAV)，企业还可以随时随地根据需要快速轻松地部署网络安全措施。

思科 WSA 是首个结合先进防御措施的网络安全网关之一，可帮助组织应对日益严重的挑战来保护和控制 Web 流量。它不仅在部署上更加简单快捷，而且可帮助减少维护需求、缩短延迟时间并降低运营成本。借助“一次性设置”技术，当初始自动策略设置生效后，您的员工即可抽身去做其他事情。每 3 到 5 分钟，自动安全更新就会推送到网络设备。思科 WSA 不仅具有灵活的部署选项，还可以与现有的安全基础设施集成，因此能够帮助您满足快速变化的安全需求。

## 虚拟设备

随着视频和其他富媒体的增多，流量已变得难以预测，导致超额和性能下降等问题发生。在解决这些问题和其他问题时，管理员（尤其是跨国组织中的管理员）还需要在购买和安装硬件时面临较长的交付期问题、远程安装难题、海关关税和其他物流问题。

思科 WSAV 允许管理员根据需要随时随地创建安全实例，大大降低了网络安全部署的成本，特别是在高度分布式网络中，尤为如此。思科 WSAV 是思科 WSA 的软件版本，运行在 VMware ESXi 或 KVM 虚拟机监控程序和思科统一计算系统™（思科 UCS®）服务器之上。购买任意思科电子邮件或网络安全软件捆绑包后，您便会获得思科 SMAV 的无限制许可证，以及相应的 SMA 软件许可证。

借助思科 WSAV，管理员无需进行能力规划，即可对峰值流量做出快速响应。您不必购买和运输设备；无需增加数据中心的复杂性或另外雇用员工，即可为新商机提供支持。

## 功能和优点

| | |
|---|---|
| **Talos 安全情报** | 受世界上最大的威胁检测网络支持，可获得快速、全面的网络保护，不仅可视性最高，而且容量最大，可处理：<br>• 每日 100 TB 的安全情报<br>• 160 万部已部署的安全设备，包括防火墙、IPS、网络和电子邮件设备<br>• 1.5 亿个终端<br>• 每天 130 亿个网络请求<br>• 35% 的全球企业电邮流量<br>通过全天候监测全球流量活动，分析异常现象、发现新威胁，并监控流量趋势。Talos 能持续生成新的规则，以便每 3 到 5 分钟将更新馈送到 WSA，从而有助于防止零小时攻击。同时，它还能先于同类竞争产品数小时或数天提供业界领先的威胁防御。 |
| **思科网络使用控制** | 将传统的 URL 过滤与动态内容分析相结合，以降低合规性、责任和工作效率风险。思科不断更新的 URL 过滤数据库中包含超过 5000 万个屏蔽站点，与众不同的是，它还涵盖已知网站。动态内容分析 (DCA) 引擎能够实时准确地识别 90% 的未知 URL；它不仅可以扫描文本、对文本进行相关性评分、计算模型文档接近度，还能返回最接近的类别匹配。管理员还可以选择特定类别的智能 HTTPS 检查。 |
| **高级恶意软件防护** | 高级恶意软件防护 (AMP) 是附加的许可功能，所有思科 WSA 客户均可使用。AMP 是将恶意软件检测与拦截、持续分析和追溯性警报集于一身的综合恶意软件防护解决方案。它使用了思科和 Sourcefire® 技术所支持的庞大的云安全情报网络。AMP 向思科 WSA 中提供的恶意软件检测和拦截功能增添增强型文件信誉功能、详细的文件行为报告、持续文件分析和追溯性判定警报。思科 AMP Threat Grid 通过本地部署设备提供恶意软件保护，非常适合那些因为合规性或政策上的限制，而无法将恶意软件样本上传到云的组织。第 4 层流量监测器通过检测并拦截间谍软件“回拨”通信，来持续扫描所有活动。通过跟踪所有网络应用，第 4 层流量监测器可以有效地阻止试图绕过常用的网络安全解决方案的恶意软件。它可以动态地将已知恶意软件域的 IP 地址添加到要拦截的恶意实体清单。 |
| **感知威胁分析** | 思科认知威胁分析是一种基于云的解决方案，可以缩短在网络内部发现威胁的时间。它通过使用行为分析和异常检测，来识别恶意软件感染的症状或数据泄露，从而应对基于外围的防御的漏洞。您只需向您的网络安全解决方案添加附加许可证，即可使用思科感知威胁分析功能。您可以在获得随着不断变化的威胁形势一起发展的优异保护的同时，降低复杂性。 |
| **应用可视性与可控性 (AVC)** | 轻松地控制数百个 Web 2.0 应用和 150,000 多个微应用的使用。借助粒度策略控制，管理员一方面可以允许使用 Dropbox 或 Facebook 等应用，另一方面又可以阻止用户上传文档或点击“赞”按钮等活动。通过 WSA，您可以查看整个网络中的活动。新变化：客户可以按用户、组和策略部署自定义的带宽和时间配额。 |
| **防数据丢失 (DLP)** | 通过为基本 DLP 创建基于上下文的规则来防止机密数据从网络中泄露出去。思科 WSA 还使用互联网内容修改协议 (ICAP) 与第三方 DLP 解决方案进行集成，以便执行深度内容检测和 DLP 策略。思科 WSA 还支持安全 ICAP，从而能够加密 WSA 与第三方 DLP 解决方案之间交换的流量。 |

| | |
|---|---|
| **漫游用户保护** | 思科 WSA 可通过与 Cisco AnyConnect® 安全移动客户端进行集成来保护漫游用户。这样一来，即可启动将流量重定向回本地解决方案的 VPN 隧道，从而为远程客户端提供网络安全保护。Cisco AnyConnect 技术会先对流量进行实时分析，随后再确定是否允许访问。<br>此外，思科 WSA 还与思科身份服务引擎 (ISE) 相集成。通过这一重要的增强功能，客户现在可以通过请求获得思科 WSA 的 ISE 的强大功能。借助思科 ISE 集成，管理员可以根据思科 ISE 在单点登录过程中收集的配置文件或成员信息，在思科 WSA 中创建策略。 |
| **集中管理和报告** | 获得有关威胁、数据和应用的有价值情报。思科 WSA 提供易于使用的集中式管理工具来控制运营、管理策略及查看报告。<br>思科 M 系列内容安全管理设备提供了跨多个设备和多个位置（包括虚拟实例在内）的中央管理和报告功能。<br>思科® 网络安全报告应用是一个用于提供报告的解决方案，它可以快速为思科网络安全设备 (WSA) 和思科云网络安全 (CWS) 解决方案生成的日志建立索引，并对之进行分析。此工具可为具有较高流量和存储需求的客户提供可扩展的报告。报告管理员可通过此工具收集有关 Web 使用情况和恶意软件威胁的详细见解。 |
| **灵活的部署** | 思科 WSAV 的功能与思科 WSA 几乎完全相同，不同之处仅在于前者增添了虚拟部署模式（包括即时自助服务调配），不仅更方便您使用，而且还可以节省更多成本。获得思科 WSAV 许可证后，企业无需网络连接，即可将许可证应用于本地新存储的思科 WSAV 虚拟映像文件，从而部署网络安全虚拟网关。如果需要，您可以复制原始的虚拟映像文件，以便能够立即部署多个网络安全网关。<br>您可以在同一部署中运行硬件和虚拟机。因此，小型分公司或远程场所无需在其所在地点安装和支持硬件，即可获得与思科 WSA 相同的保护。您可以使用思科 M 系列内容安全管理设备轻松管理自定义部署。 |

## 产品规格

表 1 和 2 分别列出了思科 WSA 的性能和硬件规格。

**表 1.** 思科 WSA 的性能规格

| | 型号 | 磁盘空间 | RAID 镜像 | 内存 | CPU |
|---|---|---|---|---|---|
| **大型企业** | S690 | 4.8 TB<br>（8 块 600 GB SAS 硬盘） | 有 (RAID 10) | 64 GB DDR4 内存 | 2 个，2.5 GHz，24 核 |
| **大型企业** | S690X | 9.6TB<br>（16 块 600 GB SAS 硬盘） | 有 (RAID 10) | 64 GB DDR4 内存 | 2 个，2.5 GHz，24 核 |
| **大型企业** | S680 | 2.4 TB<br>（8 块 300 GB SAS 硬盘） | 有 (RAID 10) | 32 GB DDR3 内存 | 2 个，2.7 GHz，16 核 |
| **中型办公室** | S390 | 2.4 TB<br>（4 块 600 GB SAS 硬盘） | 有 (RAID 10) | 32 GB DDR4 内存 | 1 个，2.4 Ghz，8 核 |
| **中型办公室** | S380 | 2.4 TB<br>（4 块 600 GB SAS） | 有 (RAID 10) | 16 GB DDR3 内存 | 1 个，2.0 Ghz，6 核 |
| **中小企业和分支机构** | S190 | 1.2TB<br>（2 块 600 GB SAS 硬盘） | 有 (RAID 1) | 8 GB DDR4 内存 | 1 个，1.9 Ghz，6 核 |
| **中小企业和分支机构** | S170 | 500 GB<br>（2 块 500 GB SATA 硬盘） | 有 (RAID 1) | 4 GB DDR3 内存 | 1 个，2.8 Ghz，双核 |

* 为准确确定所需设备规格，请与思科内容安全专家一起评估峰值邮件流速率和平均邮件大小，以确认您的选择是否适当。

**表 2.** 思科 WSA 的硬件规格

| | 思科 S690 | 思科 S690X | 思科 S680 | 思科 S390 | 思科 S380 | 思科 S190 | 思科 S170 |
|---|---|---|---|---|---|---|---|
| **硬件平台** |  |  |  |  |  |  |  |
| **外形规格** | 双机架单元 | 双机架单元 | 双机架单元 | 单机架单元 | 双机架单元 | 单机架单元 | 单机架单元 |
| **尺寸** | 3.4 x 19 x 29 英寸 | 3.4 x 19 x 29 英寸 | 3.5 x 19 x 29 英寸 | 1.7 x 19 x 31 英寸 | 3.5 x 19 x 29 英寸 | 1.7 x 19 x 31 英寸 | 1.64 x 19 x 15.25 英寸 |
| **冗余电源** | 是 | 是 | 是 | 是 | 是 | 是（配件选项） | 否 |
| **远程电力循环** | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| **直流电源选项** | 是 | 是 | 是 | 否 | 是 | 否 | 否 |
| **热插拔硬盘** | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| **以太网接口** | 6 端口千兆 Base-T 铜缆网络接口 (NIC)，RJ-45 连接器 | 6 端口千兆 Base-T 铜缆网络接口 (NIC)，RJ-45 连接器 | 6 端口千兆 Base-T 铜缆网络接口 (NIC)，RJ-45 连接器 | 6 端口千兆 Base-T 铜缆网络接口 (NIC)，RJ-45 连接器 | 6 端口千兆 Base-T 铜缆网络接口 (NIC)，RJ-45 连接器 | 2 端口千兆 Base-T 铜缆网络接口 (NIC)，RJ-45 连接器 | 2 端口千兆 Base-T 铜缆网络接口 (NIC)，RJ-45 连接器 |
| **速度（兆位/秒）** | 10/100/1000，自动协商 | 10/100/1000，自动协商 | 10/100/1000，自动协商 | 10/100/1000，自动协商 | 10/100/1000，自动协商 | 10/100/1000，自动协商 | 10/100/1000，自动协商 |
| **光纤选项** | 是，独立 SKU<br>6 端口千兆 Base-SX 光纤：<br>WSA-S690-1G<br>6 端口万兆 Base-SR 光纤：<br>WSA-S690-10G | 是，独立 SKU<br>6 端口千兆 Base-SX 光纤：<br>WSA-S690-1G<br>6 端口万兆 Base-SR 光纤：<br>WSA-S690-10G | 是，独立 SKU<br>6 端口千兆 Base-SX 光纤：<br>WSA-S680-1G<br>6 端口万兆 Base-SR 光纤：<br>WSA-S680-10G | 否 | 否 | 否 | 否 |

表 3 列出思科 WSAV 的规格，表 4 列出思科 M 系列内容安全管理设备的规格。

**表 3.** 思科 WSAV 规格

| **Web 用户** | | | | |
|---|---|---|---|---|
| **Web 用户** | **型号** | **磁盘** | **内存** | **核心** |
| **少于 1000** | S000v | 250 GB | 4 GB | 1 |
| **1000-2999** | S100v | 250 GB | 6 GB | 2 |
| **3000-6000** | S300v | 1024 GB | 8 GB | 4 |
| **服务器** | | **虚拟机监控程序** | | |
| **思科 UCS**<br>**Red Hat Enterprise Linux 7.0**<br>**Ubuntu 14.04.1 LTS** |  | **ESXi 5.0、5.1 和 5.5**<br>**KVM：QEMU 1.5.3**<br>**KVM：QEMU 2.0.0** | vmware KVM | |

**表 4.** 思科 M 系列内容安全管理设备

| **型号** | **思科 M680** | **思科 M380** | **思科 M170** |
|---|---|---|---|
| **用户数量（约数）** | 10000 以上 | 最多 10000 | 最多 1000 |

## 部署

思科 WSA 是一种转发代理，可以采用显式模式（代理自动配置 [PAC] 文件、Web 代理服务器自动发现 [WPAD]、浏览器设置）或透明模式（网络高速缓存通信协议 [WCCP]、策略型路由 [PBR]、负载均衡器）进行部署。与 WCCP 兼容的设备（如 Cisco Catalyst® 6000 系列交换机、思科 ASR 1000 系列汇聚多业务路由器、思科集成多业务路由器和思科 ASA 5500-X 系列下一代防火墙）可以将 Web 流量重新路由到思科 WSA。

思科 WSA 可以代理 HTTP、HTTPS、SOCKS、本地 FTP 和 FTP over HTTP 流量，以便提供各种附加功能（如数据丢失保护、移动用户安全和高级可视性与可控性）。

## 许可

以下所有思科网络安全软件捆绑包都包含思科 WSAV 许可证：思科网络安全基本版、思科网络安全防恶意软件，以及思科网络安全高级版捆绑包。此许可证的期限与捆绑包中的其他软件服务相同，并可视需要用于多个虚拟机。

### 基于期限的订用许可证

此类许可证按 1 年、3 年或 5 年期限购买。

### 基于数量的订用许可证

思科网络安全产品组合使用基于用户数量（而不是设备数量）的分级定价。销售代表和合作伙伴代表会帮助确定每个客户部署所需的正确分级。

### 网络安全软件许可证

我们提供了 4 种网络安全软件许可证捆绑包，分别为：思科网络网络安全基本版、思科防恶意软件、思科网络安全高级版和 McAfee 防恶意软件。每种软件产品的主要组件具体如下：

**思科网络安全基本版**

- 通过思科 Talos 提供的威胁情报
- 第 4 层流量监控
- 应用可视性与可控性 (AVC)
- 策略管理
- 可行报告
- URL 过滤
- 通过 ICAP 实现第三方 DLP 集成

**思科防恶意软件**

- 实时恶意软件扫描

**思科网络安全高级版**

- 网络安全基本版
- 实时恶意软件扫描

**高级恶意软件防护**

- AMP 借助文件信誉评分和拦截、静态和动态文件分析（沙盒）以及文件追溯功能，可以持续分析威胁，从而增强防恶意软件检测和拦截功能。

**感知威胁分析 (CTA)**

- CTA 依靠高级统计建模和机器学习来独立识别新威胁，从其所发现的内容中学习，并随时间推移不断适应。

**云访问安全**

- 思科通过与 Elastica 的合作，能够使组织获得云应用的优势，同时通过 SaaS 可视性、扩展的精准控制和智能保护来维护严格的安全策略。

**McAfee 防恶意软件**

- McAfee 实时恶意软件扫描可构成单个定制许可证。

### 软件许可协议

购买每份软件许可证都应签署思科最终用户许可协议 (EULA) 和思科网络安全补充最终用户许可协议 (SEULA)。

### 软件订用支持

所有思科网络安全许可证都包含软件订用支持，此类支持对保证业务关键应用的可用性、安全性以及最佳运行性能非常重要。通过这种支持，客户有权在所购买的软件订用的整个期限内，获得下面列出的服务。

- 软件更新和重要升级，可确保应用以最新功能集在最佳状态下运行
- 与思科技术支持中心 (TAC) 联系：提供快速、专业的支持
- 在线工具：构建和扩展内部专业资源以及提高业务灵活性
- 协作学习：提供额外的学习知识和培训机会

## 服务

表 5 列出思科网络安全服务。

**表 5.** 思科网络安全服务

| | |
|---|---|
| **思科品牌服务 (CBS)** | 思科安全规划和设计：可方便您以具成本效益的方式快速部署强大的安全解决方案。思科网络安全配置和安装：通过安装、配置和测试设备来实施以下功能，帮助降低网络安全风险：<br>• 可接受的使用策略控制<br>• 信誉和恶意软件过滤<br>• 数据安全<br>• 应用可视性与可控性<br>思科安全优化服务：支持不断发展的安全系统，以处理安全威胁、设计更新、性能调整和系统变更。 |
| **协作/合作伙伴服务** | 网络设备安全评估：通过识别网络基础设施的安全鸿沟来维护坚实的网络环境。<br>智能关怀服务：通过网络性能的安全可视性提供切实可行的情报。其他服务：思科合作伙伴可提供各种有价值的服务，涵盖生命周期规划、设计、实施和优化等各个方面。 |
| **思科融资** | Cisco Capital® 可根据业务需求定制融资解决方案， 以便您可以更快地获得思科技术并实现业务优势。 |

## SMARTnet 支持服务

客户可以视需要选择购买思科 SMARTnet® 支持服务，用于思科 WSA。借助思科 SMARTnet 支持服务，客户可以随时直接与思科专家联系、使用各种自助式支持工具，并迅速实现硬件更换，从而快速解决网络问题。有关详情，请访问 http://www.cisco.com/go/smartnet。

## 订购思科 WSAV

如需订购思科 WSAV，请执行以下操作：

1. 访问 http://www.cisco.com/go/wsa。在右侧的“支持”(Support) 部分，点击“软件下载、版本和一般信息”(Software Downloads, Release, and General Information)。点击“下载软件”(Download Software)，然后点击任何产品型号，系统将显示可下载的虚拟机映像， 以及一个可下载的 XML 评估许可。您需要下载其中一个映像以及该 XML 评估许可证。
2. 从 Cisco.com 下载以下文档：
   a. 思科安全虚拟设备安装指南
   b. AsyncOS® 9.0 的相关文档
3. 按照思科安全虚拟设备安装指南中的说明开始操作。请注意，内容安全虚拟设备评估不在 SMARTnet 支持服务范围内，因此不受支持。

## 保修信息

如需查看保修信息，请访问 Cisco.com 的产品保修页面。

## 更多详情

如需了解更多信息，请访问 http://www.cisco.com/go/wsa。让思科销售代表、渠道合作伙伴或系统工程师为您评估思科 WSA 将如何助您一臂之力。


**美洲总部**
Cisco Systems, Inc.
加州圣荷西

**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。





美国印刷 C78-729630-09 12/15