充分利用您的下一代防火墙

全面的网络可视性和控制提高了业务效率并使企业在保持增长的同时获得最大的安全性。

要解决业务挑战：	下一代防火墙必须具有以下功能：
维护合规性	执行确定性状态检测
提供深入的可视性和控制	无论使用何种端口和协议，都能识别并控制应用和微应用
	通过被动和主动的身份验证方法识别用户
在支持业务需求的同时限制有风险的行为	识别并控制所允许微应用范围内的特定行为
	支持合法的互联网访问，同时阻止不良的网页类别
授权个人设备的适当使用	支持各种移动设备的差异化网络访问
避免互联网威胁	根据动态声誉分析控制网站和基于 Web 的应用
	以近实时方式避免零日威胁
支持对加密的安全使用	基于策略解密和检验已加密的通信
平衡安全性和性能要求	在启用了多个安全性服务时维护性能预期

在尝试兼顾安全性与生产效率的过程中，网络管理员正在经历有史以来最高级别的变化。快速发展的业务趋势迫使他们提供应用广泛但安全的互联网访问，从而使员工能够在使用他们自己选择的设备时使用合法的业务应用。

应用发展到现在，形成了高度动态和多元化的特点，在合法业务应用与那些浪费时间并增加了公司暴露在互联网威胁之下的风险的应用之间，界线变得模糊。在过去，可接受的用法相对不明确，但随着社交媒体、文件共享和互联网通信应用的发展，这些应用所服务的业务使用案例已经像严格的个人使用案例那样多；这些应用的使用现在遍及整个组织的所有级别。让问题进一步复杂化的是，今天的员工移动性日益提高，用户需要从各种公司自有的设备和个人移动设备随时随地访问网络。这种情况推动了所有规模和类型的企业接受“自带设备”(BYOD) 策略来提高员工的生产效率和满意度。

由于上述及其他业务趋势，网络管理员面临着日益严重的挑战：执行在保护网络的同时支持灵活性所需的可接受的使用策略，从而获得和维护促进业务增长所需的生产效率级别。需要一种获得安全性的新的途径（并不放弃经过时间考验的方法）来增强网络可视性和控制、加速业务创新，并主动防御新的威胁和新兴威胁。但是，管理员需要使用更多基于网络的安全控制来作为此成熟的安全设备的补充，而不是放弃其现有的状态检测防火墙，来实现端到端网络智能和简化的安全操作。

业务挑战

正如前面讨论过的那样，曾一度被禁止在企业网络中使用的社交媒体、文件共享和互联网通信应用，现在已被认为是联系全世界的客户和合作伙伴的合法、有效且经济实用的方法。根据思科 2013 年度安全报告，所有企业内部的 Web 请求中有 22% 是查看在线视频，另外有 20% 是访问社交网站。因此，各种规模的公司都在逐步接受社交媒体和在线视频；大多数著名品牌都在 Facebook 和 Twitter 上开设了帐户，许多公司还将社交媒体融入了实际产品中。同样地，能“接触”网络的设备曾一度被限制为仅供 IT 使用并受到严格控制，而现在，各种各样的个人设备也可以获得安全的网络访问。

尽管可带来其业务生产效率上的优势，但是这些网络趋势还带来了严重的新的安全风险。因此，当今组织所面临的主要业务挑战是如何执行可接受的使用策略、控制规避应用、授权个人设备并防御互联网威胁。

执行可接受的使用策略

组织需要解决的两个主要的业务问题都围绕可接受的使用策略。首先，需要基于强大内容的 URL 过滤才能阻止攻击性的、不恰当的、甚至可能非法的网站，比如，那些包含成人、暴力或种族仇恨内容的网站；那些降低生产效率或消耗过高带宽量的网站（如 YouTube）；以及那些可能会危害公司法规的合规性的网站（如 BitTorrent 和 eDonkey）。同样地，需要深入的应用检验才能阻止已知的恶意软件（如代理服务器的匿名访问程序），员工可以使用该软件绕过 IT 控制。

诸如 Facebook、Twitter、LinkedIn 和 Skype 这类应用使得执行可接受的使用进一步复杂化。这些应用已发展成为合法的业务应用，但许多组织不愿让这些应用在网络上运行，因为其用户可能会造成广泛的带宽滥用并使员工降低工作效率。

控制规避应用

与此挑战相关的是获得对端口跳变和协议跳变应用（如 Skype 和 BitTorrent）的可视性及对其的控制。由于这些应用的本质是找到一个通路（无论网络发生什么情况），所以它们会给试图阻止其使用的管理员带来独特的挑战。事实上，管理员可以编写大量的策略，这些策略试图仅仅阻止其中一个规避应用，但仍无法充分控制它们。

授权个人设备

思科 2011 年度安全报告发现 81% 的大学生相信他们应该能够选择他们工作时需要使用的设备。全世界已参与调查的员工中有 77% 使用多个设备来访问企业网络，而其中超过三分之一的人使用至少三个设备进行工作。因此，根据思科 2012 年的全球 IBSG Horizons 报告，84% 的 IT 领导报告在其公司中 IT 变得越来越消费化。思科 2013 年度安全报告支持这些发现，该报告显示仅仅在过去的两年中，思科就看到其员工使用的移动设备的数量增加了 79%，并且这些设备中绝大多数是“自带设备”。

这些趋势已经导致自带设备成为大多数组织的优先选择，相较于 2012 年消耗的 18%，2014 年移动计划预期平均会消耗 23% 的 IT 预算。而就在几年前，组织仅需要确定谁要访问网络和敏感企业数据，自带设备给这些决策增加了复杂程度。现在组织必须确定已获授权访问此类数据的员工是否仅在使用企业拥有和维护的设备时才有权访问，或者确定是否还可以使用他们的个人设备。如果个人设备可接受，那么是**所有**设备都可接受还是仅某些设备可接受？是需要员工位于企业 LAN 内，还是说远程 VPN 连接也能提供适当级别的安全性？

避免互联网威胁

互联网威胁是所有规模的组织都关心的另一个问题。尽管诸如文件共享和社交媒体应用等工具对员工生产效率具有正面影响，但是这些工具具有固有的风险：黑客和其他恶意软件编写者可以利用这些工具对网络进行未经授权的访问或者在网络上传播恶意软件。诸如 TeamViewer 和 PC Anywhere 等远程控制应用可能会动态地提高个人和团队的生产效率，但恶意软件编写者可以使用这些应用中的漏洞来控制网络资产。此外，文件共享应用（如 Dropbox 和 iCloud）的使用使得将敏感的公司数据上传到云端成为可能，而云端组织无法对数据的分发进行控制。

恶意软件还可以伪装成开放端口上运行的众所周知的应用；还可以嵌入到已发现有漏洞的合法应用中；或者可以从欺诈性网站（或已经受感染的合法网站）作为“路过式”下载进行安装。以社交媒体用户为目标的社会工程技术也已被证实是很有效的；这些应用让员工认为点击嵌入的电邮链接和从未知网站下载内容是完全正常的，尽管 IT 不断提出应避免此类行为的长期警告。

需要一种主动的、全面的解决网络安全的方法

业务领导了解灵活性对于最大程度地提高生产效率是必不可少的。但他们如何才能在充分利用业务和技术趋势所提供的生产效率和成本优势的同时让自己免受这些趋势所带来的安全挑战？答案就在于一个组织通过完全的情景感知最大程度地提高其网络通信可视性的能力。如果管理员可以清楚地看到网络通信的细节，他们就可以做出更加明智的决策。应用和用户 ID 的可视性尽管很有价值，但并不提供安全地支持新的应用、设备和业务案例所需的完全情景感知。完全情景感知除了包括这些内容之外，还包括企业级 URL 过滤、动态 Web 声誉、设备感知以及对用户和设备所在位置的了解。

应用可视性和控制

正如前面所提到的那样，应用感知是所有下一代防火墙的一个核心要求。但是，非常重要的是，防火墙不仅要识别应用本身；它还必须识别并提供阻止包括该应用的微应用的能力。对于诸如 Facebook 和 LinkedIn 等社交媒体应用，这是特别重要的。单纯识别这些应用仅会提供完全阻止或允许整个应用的能力。例如，某个组织可能希望提供对 Facebook 的访问，从而使销售和市场营销人员能够在公司的企业 Facebook 页面上发贴并与客户和合作伙伴进行通信，同时要拒绝对 Facebook 游戏的访问。通过单独地识别每个微应用，管理员可以向每个微应用授予不同的访问权限。

此外，通过识别这些微应用中的特定行为，防火墙可以为管理员提供甚至更加精细的控制。例如，“Facebook 消息和聊天”微应用内的特定行为是“附件上传”、“附件下载”和“视频聊天”。尽管这些行为中的绝大多数可能都被认为是适当的业务活动，但是“附件下载”行为很可能会被安全人员视为存在固有风险。通过使用可以识别微应用内的特定行为的防火墙，管理员可以允许“Facebook 消息和聊天”，同时拒绝“附件下载”。

如果防火墙可以监控所有端口和协议并支持完全基于应用本身的识别的策略定义，那么对诸如 Skype 等规避应用也可以进行有效控制。由于像 Skype 这样的应用始终带有相同的应用 ID，所以无论它们使用哪个端口或协议来退出网络，与编写数十个基于状态的防火墙策略来阻止每种可能的组合相比，添加一个策略来“阻止 Skype”，效率更高且所需策略也更少。这样可以为管理员节省在策略的初始制订和日常管理上所花的时间，这会转换为企业的运营效率。

最后，通过控制有权访问文件共享应用的人员以及控制允许使用哪些应用行为，管理员可以保护企业的关键数据，同时使员工能够充分利用强大的业务工具。

高级用户识别

用户感知是所有下一代防火墙的另一个核心组件；大多数防火墙通过企业目录服务（如 Active Directory (AD)）提供被动身份验证。使用此功能，管理员可以根据用户的身份或所属组别来执行策略。尽管此识别本身仅包含相对较少的价值，但是在与上面所强调的应用感知配合之后，管理员可以使用此识别来支持对某些应用的差异化访问。例如，市场营销人员和销售人员可能会有访问社交媒体工具的合法业务需求，而财务人员则不会。

除了被动身份验证之外，对于需要更加强大的安全措施的业务使用案例，某些下一代防火墙已扩展了此功能来包括对主动身份验证的支持。被动身份验证依赖于对目录服务的简单查找，并相信它已通过用户名-IP 地址映射正确地识别用户，而主动身份验证需要通过类似 Kerberos 和 NT LAN Manager (NTLM) 等机制的一个附加安全层来进行。这可以通过询问浏览器（浏览器接着根据用户的登录凭据发送一条无缝响应）来执行，或者通过使用某个授权提示质询用户来执行。在任何一种情况下，安全管理员都将对用户进行身份验证而不是依赖用户名-IP 地址映射。这对于有敏感信息（比如客户信用卡数据或包含医疗保健信息的数据库）供人们访问的组织来说是很重要的。

设备感知

对于已经在业务实践中包括自带设备的组织，要在生产效率和安全性之间取得平衡，需要具备对试图访问网络的特定设备的精细的可视性，从而使管理员能够基于每个使用的设备执行差异化策略。例如，组织可以决定允许 iPhone 4 设备访问大多数网络资源，而拒绝或限制对更早版本的 iPhone 的访问，或者可以授予 iPhone 4 访问权限而不授予 4S 访问权限。同样地，组织可以授予基于 Windows 的 PC 访问权限，而拒绝对 Mac 的访问。此外，如果防火墙配置了地点感知，那么可以根据设备是在 LAN 内还是从远程登录的来执行不同的策略。

Web 安全

URL 和 Web 过滤功能允许对适当的应用和内容的访问，而阻止对可能会增加风险、降低生产效率或导致机密信息丢失的应用和内容的访问。大多数 Web 安全设备提供基于大类的基本 Web 过滤，以及分辨白名单和黑名单特定站点的能力。许多供应商还将在设备本身上包含一个已知“坏”URL 数据库。但是，由于互联网的动态本质，这些功能还不够。根据非盈利组织 stopbadware.org 的统计，目前有超过一百万个网站提供恶意软件和不经用户允许而执行操作的其他软件（通常也称为“灰色软件”）。因为每周会将数千个新的 URL 添加到该列表中，限制于静态的现成列表的 Web 安全将永远无法跟上节奏。因此，除了这些功能之外，组织需要不断进行更新的 URL 过滤，以获得对于不断发展的威胁环境的近实时防护。

此外，防火墙必须能够识别并停止伪装成在开放端口上运行的、众所周知的应用的恶意软件，而不会抑制使用这些端口的合法业务工具的业务价值。通过使用全局数据和应用通信来提供近实时威胁环境信息（包括基于特定站点或 Web 应用所呈现出来的行为的声誉分析），可以进一步增强此功能。如果某个提供商正在收到大量来源遍及全世界的通信，并以足够高的频率提供更新，那么全局数据还可以帮助保护组织免受零日威胁。

为了支持这些使用案例而不危害安全性，某些 IT 组织已经使用提供更高级别的可视性与超级控制的防火墙产品线来取代其基于状态的防火墙产品线。尽管很少有人会将可视性更高视为不利因素，但这些下一代防火墙中大多数都带有权衡机制，因此管理员和企业领导在做出购买决策之前进行全面了解是很重要的。

可视性有限：问题只解决了一半

毫无疑问，提供可视性更强的网络通信会带来巨大的安全优势。增强的网络可视性让管理员有能力制订和执行更加精细的安全策略，从而获得对企业资产的超级防护。这就是应用和用户 ID 感知功能对下一代防火墙非常重要的原因。但是，许多下一代防火墙将整个解决方案完全围绕这两个因素而无视其他的一切。当然，有可视性比没有可视性好，但是，正如在本白皮书中所讨论的那样，在典型的企业网络中还有太多事情要做，因此，要提供足够的可视性来进行智能安全决策，仅有应用和用户 ID 感知是不够的。除了这些功能之外，一个全面的安全解决方案必须为管理员提供以下能力：在允许的微应用内控制特定行为，根据站点的声誉限制 Web 和 Web 应用使用，主动防御互联网威胁，并根据用户、设备、角色和应用类型执行差异化策略。

寻找两全其美的解决方案

尽管使用下一代防火墙有很多益处，但也存在一些缺点需要予以考虑。因此，业务领导应该在做出购买决策之前全面评估其选择。许多下一代防火墙供应商强制客户放弃其现有防火墙和所有相关的安全策略，这样他们可以使用专门为下一代防火墙平台编写的全新安全策略“重新开始”。这种“淘汰并更换”是必要的，因为大多数下一代防火墙从基础上就不同于现有的经典防火墙或基于状态的防火墙，而在一个完全不同的计算层上工作。

基于状态的防火墙在计算架构的网络层和传输层上工作，而下一代防火墙在应用层上工作。因此，组织的现有防火墙策略在新的范式中将毫无用处，因此必须完全重新编写。这绝不是一个快速、轻松的任务 - 大多数组织有数千个策略，而更大的组织可能会有**数万**个策略。这可能会需要几个月的时间，并可能会需要分配相当可观的预算才能完成。此外，在应用层上执行的安全性按其本质来说，是一种更加深入的检验级别，并可能导致网络性能下降。

使用完全为应用层构建的防火墙更换组织的状态检测防火墙还可能会危害组织对行业法规的遵从性，因为许多监管机构专门规定状态检测的需求。由于基于应用和基于用户 ID 的防火墙策略具有非确定性，因此完全依赖于下一代防火墙可能会让组织面对无法通过审计的风险。

但是，某些防火墙供应商提供混合方法，使基于状态的防火墙功能与下一代防火墙功能在一起工作。因为这些防火墙同时支持基于状态的功能和下一代功能，所以组织可以继续使用其现有策略，同时他们制订了新的下一代规则；这并不强制他们放弃一种来使用另一种，因此他们可以经过一段时间来更换旧策略，因为这样做最适合其安全需求。此外，并非所有通信都需要由下一代防火墙执行的更深入级别的检验，因此混合模型使得组织能够保留其大部分网络性能，方法是通过仅对需要执行更深入级别的检验的那些通信和使用案例执行这样的检验。这样，组织可以获得超级的安全级别，同时实现最大的业务灵活性。

结论

诸如自带设备和采用社交媒体及其他灰色应用作为合法业务工具等趋势已经对所有规模的组织产生了深刻的影响。但是，仅提供应用和用户 ID 感知的下一代防火墙无法提供安全地支持它们所需可视性级别的网络。但另一方面，通过查看网络通信的完整情景，管理员可以利用高度的网络可视性和智能，来实施可行的安全措施。通过使用将基于状态的功能与完全情景感知结合到一起的防火墙，组织可以在支持这些新的业务用例所需的高级别网络安全与最大程度地提高其业务敏捷性所需的灵活性之间取得平衡。

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
荷兰阿姆斯特丹

思科在全球 200 多个地点设有办事处，思科网站 **www.cisco.com/go/offices** 上列有各办事处的地址、电话和传真。

美国印刷 C11-726002-00 02/13