白皮书

Cisco ASA CX 提供情景感知安全

革命性的架构，灵活弹性的部署

思科安全技术事业部

2012 年 2 月

目录

摘要

Web 的应用和 IT 的消费化正在从根本上改变企业所面临的安全形势。当今企业的安全设备在授权访问之前，不仅需要感知访问基础设施的具体应用和用户，而且要感知所用设备、用户位置和访问时刻。这种**情景感知**安全会要求重新思考防火墙架构。但是，情景感知防火墙需要与企业的现有安全基础设施一起工作。Cisco® ASA CX 不仅为企业带来突破性的安全功能，而且还可以保护其现有的安全投资。

安全形势正在发生重大变化

当今互联网的主要趋势正在向应用发展。如今，一般员工越来越习惯在移动设备上使用消费者应用访问基于 Web 的服务，来满足个人和职业两方面的目的。这些员工希望能够在企业网络上使用其常用的应用。其次，IT 消费化也已成为趋势 - 员工希望能够在工作场所轻松使用其个人手机、平板电脑和笔记本电脑，而且不用担心会遭到黑客攻击。最后，员工希望能持续可靠地访问其日常工作流程赖以依靠的企业应用。

因此，安全架构师和操作人员在准许各种应用、网站和设备的网络访问方面受到持续的压力。与此同时，他们还必须保护企业免遭恶意攻击，并维持对传统企业应用的可靠访问。目前由于可见性的原因，安全人员无法轻松获知网络中的应用以及正在访问这些应用的设备和用户。如果没有这种可见性，实施有意义的防御根本无从谈起。即使安全人员了解网络上的应用程序，仍然缺乏对这些应用程序的精细管理，以及选择性授权哪些用户和设备访问这些应用程序的能力。

黑客非常清楚安全人员面临的窘境。他们设计出各种方法绕过典型安全策略，例如可跳跃端口的应用、即使用户限定仅浏览受信赖站点也能造成路过式恶意下载的 Web 小部件，以及利用各种安全漏洞窃取企业机密数据的高级威胁。

需要情景感知安全来保护企业

为了应对不断变化的安全形势，企业需要根据某种情况的完整情景来实施安全防护。这里所说的情景包括用户身份（对象）、用户试图访问的应用或网站（内容），以及访问的来源。

一直以来，防火墙都是企业进行安全防御的重要支柱。为了排除当今存在的威胁，防火墙需要具备情景感知功能。也就是说，防火墙需要提取用户和应用程序身份、访问来源和用于访问的设备类型，然后根据这些属性按照已配置策略决定允许访问或拒绝访问。此外，防火墙必须具备检测和防御新兴威胁的能力。

防火墙是获取网络流量完整环境信息的地方。防火墙可对跨越企业网络和外部网络之间的信任边界的所有流量进行全面监控。如果防火墙具备检查流量完整环境信息的能力，那么使用防火墙来评估此类流量是否符合企业策略似乎是合理的。不幸的是，现在市场上的大多数防火墙都过于缺乏灵活性，无法轻松支持情景感知。这些防火墙不仅无法提取流的完整环境信息，而且缺乏实施精细策略的能力，如无法在允许访问 Facebook 的同时禁止访问 Facebook 上的游戏，或者无法在允许财务人员访问企业敏感数据库的同时禁止其他人员访问。

而在防火墙具备部分情景感知属性的情况下，将所需的企业策略转换为防火墙规则是一个难题。以 IP 地址、协议和端口号形式表达的现有防火墙规则已经很难维护。在这些规则上手动添加更多解释新应用、新用户和新移动设备的规则，需要大量的时间和精力。即便已成功安装这些规则，所产生的扩展规则组也只会进一步增加规则维护的难度，并威胁到访问企业传统应用的可靠性。

显然，防火墙应该能让安全操作人员使用更加业务友好的语言来表达情景感知策略。安全操作人员需要可以直接“屏蔽 Skype”或者“允许 Yahoo! Messenger 但禁止文件传输”的能力，而非强制使用 IP 地址和协议以及端口号来创建复杂的规则。以这种业务友好型语言表达的策略，执行速度更快，更易维护，并能大大降低安全管理的复杂性和脆弱性。

情景感知防火墙超越了目前市场上的新一代防火墙。目前大多数新一代防火墙技术上仅能识别流的部分环境信息，无法应对新兴威胁。很多防火墙不具备用户友好型解决方案来管理安全策略。虽然这些防火墙可能在一些部署上对传统防火墙进行了一些改进，但仍无法提供企业所需的全面安全解决方案。

利用革命性架构实现情景感知

虽然具有情景感知功能的防火墙对防御当今存在的威胁必不可少，但是目前市面上的防火墙均无法提供所需的全套功能：思科谨慎遵循一系列关键原则，已开发出具有完整情景感知功能的防火墙。

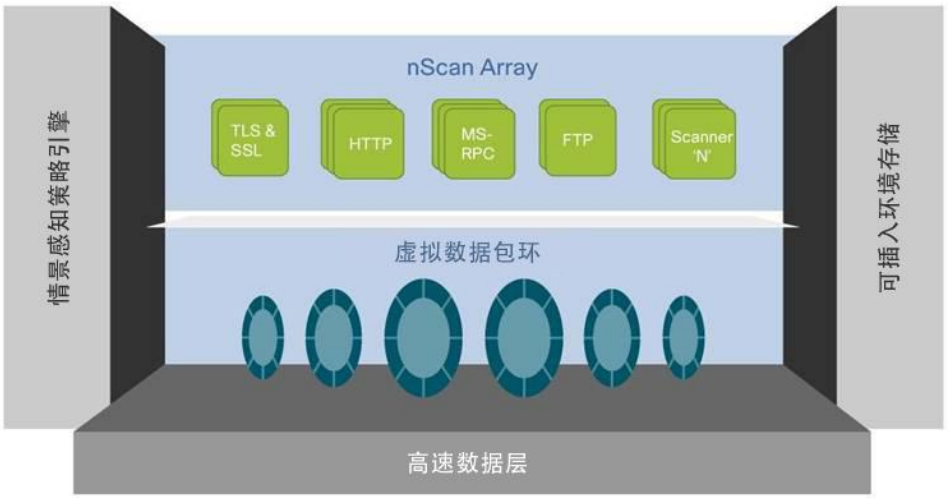
首先，防火墙需要**从头开始创建**，以便检测、传播和处理流的完整环境信息。其次，防火墙需要**完整**实施 — 需要实施企业所需的所有功能，而非仅实施防御近期威胁的功能。第三，防火墙的架构需要**灵活**适应各种机制以应对将来的威胁，而且能够最大限度地缩短所需的维护停机时间。第四，防火墙需要能够同时使用**本地和全局情景** — 能够同时使用企业网络内部和外部的信息。第五，防火墙需要在提供情景感知的同时保持**高性能**。

Cisco ASA CX 使用新型防火墙架构构建，这种新架构可执行情景感知检查、制定情景感知决策，而不会违反任何上述原则。

重新设计防火墙

ASA CX 使用四个协同工作的架构构件重新设计了防火墙（图 1）。首先是**虚拟数据包环**，可使数据包从硬件接口高速流入主内存，然后流出。其次是 **nScan Array**，其可并行检查多个流，从而获取各个流的完整环境信息，然后实施与该环境相关联的策略决定。第三是**情景感知策略引擎**，nScan Array 使用其制定策略决策。第四是一系列由可动态更新的数据库组成的**可插入环境存储库**，nScan Array 参考其实施决策。这些架构构件相互结合，确保 ASA CX 严格遵守上述原则。

图 1. ASA CX 架构



ASA CX 使用共享内存实施虚拟数据包环。每个流都会映射到虚拟数据包环，因此 nScan Array 检查流时无需相关的数据副本。借助于虚拟数据包环，数据包的进出不再需要多次复制。这样就提高了系统的数据包吞吐量。同时也增强了系统性能的可预测性，并减少了发起流的最终用户感受到的延迟。

nScan Array 是一组引擎，可通过访问由虚拟数据包环维护的数据包来检查传入的流。多个检查引擎将并行处理一个流，提取该流的完整环境信息，并决定是允许还是拒绝该流。例如，传入的流可以同时接受 HTTP 检查和 IPS 检查。仅当 HTTP 和 IPS 检查器均确定可以放行后，该流才可通过防火墙。nScan Array 中的检查引擎可动态更新，无需升级整个系统或强制停机。这使得 ASA CX 能够在发现新漏洞后以最短时间进行防御，同时最大限度地减少操作人员的介入。

nScan Array 中的检查引擎使用情景感知策略引擎制定策略决策并执行实施操作。策略引擎是一种高度优化的数据结构，它能把流的属性与适当的策略及其相关操作进行匹配。检查引擎还使用可插入环境存储库中的数据，来做出检查决策。假设安全操作人员配置了策略来阻止除特定用户外的所有用户访问企业数据库。在这种情况下，评估新的流时，检查引擎首先会查询策略引擎，以决定适当的操作。这样，引擎可识别是否需要提取与该流量流关联的用户身份。因此，引擎会访问用户 ID 环境存储库、获取与该流相关的用户 ID，并参照允许的用户数据库访问权限测试该用户 ID。如果提取的用户 ID 与策略引擎中配置的一个 ID 相匹配，则允许该流进行访问。如果不匹配，则禁止该流访问。

系统中存在多个环境存储库，每个库对应检查引擎需要的不同类型的实体。因此会有多个环境存储库，分别用于用户 ID、设备、URL 等。从概念上讲，环境存储库分为两种类别：一种在本地生成（例如，用户 ID 和设备），另一种从外部资源获取（例如，域和 URL 数据库）。不论哪种类型，每个存储库都会动态刷新，以便检查引擎在制定检查决策时拥有最新信息。

检查引擎完成对一个流的检查后，会立即开始检查下一个待检查的流。根据具体的流量模式和已配置策略，ASA CX 系统可能会确定是否需要增加特定类型的检查引擎（例如 HTTP）并减少另一种类型的检查引擎（例如 FTP）。系统会动态调整 nScan Array，使包含的检查引擎的数量和类型达到最佳状态，从而使流量流动保持平稳。

ASA CX 硬件架构包含多个 CPU 核心（基于硬件配置），可为 nScan Array 提供广泛的并行检查能力。这种检查能力与检查引擎（进行动态优化以应对流量模式）和虚拟数据包环（高效传输网络端口之间的流量）相结合，使 ASA CX 能够提供高性能的情景感知安全性。同时，可动态更新的检查引擎和可插入环境存储库使 ASA CX 能够非常灵活地在新威胁出现时予以防御，并最大限度地减少操作人员的介入。

虽然 ASA CX 旨在实现灵活性和高性能，但是其架构能够无缝支持思科防火墙所提供的全套企业级安全功能。这包括为应对特定应用威胁而开发的检查引擎，以及远程访问和网络地址转换等功能。

应用程序精细化控制

ASA CX 分两步实施流量检查。第一步，检查引擎对流量进行粗略分类。在许多情况下，只需要对流量进行粗略分类，引擎即可制定实施决策，无需进一步投入计算能力。然而在某些情况下，粗略分类引擎会决定执行特定安全策略，以便更深入地检查流量。在这些情况下，流量会流向可实施更精细检查的深层分类引擎。这种两级检查机制可为安全人员提供极大的灵活性，同时不会对性能造成影响。

考虑一下这种情况，安全人员既要允许使用 Yahoo ! Messenger 以便员工之间进行协作，又要阻止 Messenger 传输文件以防止企业数据泄露。例如，如果需要跨端口和协议进行检查，便可以执行要求使用深度检查引擎的策略。ASA CX 的深度检查引擎首先识别并允许 Yahoo! Messenger 流量流入。由于在聊天会话过程中随时都可能发起文件传输，引擎会持续监控该流。在某个时刻，如果用户发起文件传输，检查引擎会识别并标记新的子流，阻止其完成传输。

在 ASA CX 中，类似的可见性和精细化控制可用于 1000 多种应用程序。然而，对于使用粗略分类便足以处理的流量（例如，来自许可网络的 FTP），则无需触发深度检查。

最后，请注意 ASA CX 可监控所有 IP 端口上的应用流，而不仅仅是特定的几个端口。因此，它可有效地检测并控制非 Web 应用，如 Yahoo! Messenger 和 Skype，以及跳端口应用。

全面的用户身份识别

在广义上，防火墙可通过两种方法实施用户身份识别。一种是被动用户身份识别，此方法基于擦除 Active Directory (AD) 代理日志，并将 IP 地址与用户短时间关联。这样一来，已知 IP 地址上流入或流出的任何流量都会被认为是出自与该 IP 地址相关联的用户。另一种是主动用户身份识别，即防火墙使用 NT LAN Manager (NTLM) 或 Kerbero 识别用户身份。

由于被动用户身份验证不直接与应用交互，所以这种方法的优势在于它可与正在使用的所有应用程序结合使用。但是，当 IP 地址从一个设备重新分配到另一设备时，这种方法将无法进行身份验证。在这种情况下，被动用户身份验证无法将 IP 地址与用户身份进行正确绑定。

主动用户身份验证通过应用中的协议（如 NTLM 或 Kerberos）执行真实身份识别，比被动身份验证更精确。遗憾的是，只有 Web 浏览器和 Microsoft Outlook 等某些应用才能实施 NTLM 或 Kerberos 协议。因此，仅依靠主动用户身份验证可能无法提供充分的覆盖。

许多防火墙仅实施了这两种用户身份识别机制中的一种。与之相比，ASA CX 同时使用了被动和主动机制来确定用户身份，尽可能构成流量流环境的完整图景。ASA CX 还可在身份验证时识别并排除打印机等非交互设备，以防止这些设备发出错误警告。

在部署了思科身份服务引擎 (ISE) 并实施了 Cisco TrustSec® 技术的网络中，ASA CX 能更好地发挥效用。实施了 TrustSec 的网络端点根据用户身份标记用户流。ISE 将策略操作与标记相关联，并将其分配至思科交换机和防火墙等实施点。ASA CX 可与 ISE 互操作，其从 ISE 收到策略标记关联，并将这些关联植入本地环境存储库。随后，当 ASA CX 监测到带有 TrustSec 标记的流传入时，便知道哪些实施操作适合这些流。ASA CX 的高精度可见性和对用户事务的精细控制，使其大大优于市场上的任何其他防火墙。

前所未有的基于设备和位置的控制

Cisco AnyConnect™ 是目前市场上部署最广泛的远程访问 VPN 解决方案，现已部署超过 1 亿套。AnyConnect 是大多数实施了 VPN 的大型企业之首选，广泛支持各种设备，包括 PC、iPhone 和 iPad。在最终用户设备上使用 AnyConnect 并将 VPN 连接的另一端连接到 ASA CX 的时候，ASA CX 即可获悉设备的操作系统类型、版本和所有者（企业或个人），以及设备上安装的安全软件的类型（如防病毒扫描器）及状态（如正常需要更新）。该设备信息极大完善了 ASA CX 可用的环境信息。通过该环境信息，ASA CX 可实施各种策略，如允许私人笔记本电脑访问电子邮件，但禁止访问企业敏感应用，或者允许企业办公用笔记本电脑同时访问电子邮件和企业应用。

将来，即使最终用户设备直接连接到企业网络 — 即设备不通过 VPN 进行连接时，AnyConnect 仍然起作用。在这种情况下，AnyConnect 会把设备安全软件状态等参数直接传输到 ASA CX，供其制定实施决策时参考。

大多数竞争对手的防火墙无法很好地与 AnyConnect 等广泛部署的端点解决方案相集成。结果，这些防火墙无法检测到用于访问的设备，无法获取该访问的完整环境信息。因此，不论这些防火墙是否允许该访问，都无法制定最佳实施决策。

另外，ASA CX 可与 ISE 互操作，以基于 TrustSec 标记强制实施基于设备的策略。其运行机制类似于先前讨论过的基于用户 ID 的实施。唯一的区别在于，标记与设备关联而非与用户关联；因此，将更新和使用本地设备存储库而非本地用户存储库。假设使用 TrustSec 的企业想要实施以下策略：禁止访客网络上的移动设备访问企业数据。来自访客网络中设备的任何流将分配到一个标记，该标记将告知思科交换机和防火墙该设备的访问权限受到限制。随后，如果 ASA CX 检测到流向企业数据库的流带有“访客设备”标记，ASA CX 会自动阻止该流。

最后，ASA CX 可使用 AnyConnect 头端生成的位置信息实施基于位置的控制。假设安全人员想要允许出差人员访问企业内部网上的敏感信息。然而，基于访问历史记录，安全人员只想允许位于美国的出差人员进行访问。可配置 ASA CX 实施这样的策略。当新的 VPN 连接进入 ASA CX 时，检查引擎将检查该连接的 IP 地址来源。借助可插入环境存储库，该引擎确定该连接来自美国以外的国家/地区。因此，ASA CX 会阻止该流，根据所配置策略为内部网访问保驾护航。

零日恶意软件防护

思科拥有世界最大的威胁分析系统 — 思科安全智能运营中心 (SIO)。SIO gpgnetwork 包括超过 700,000 个全球传感器，每天可查看超过 50 亿次 Web 请求，以及 35% 的全球电子邮件流量。另外，SIO 还接收来自 AnyConnect 端点的威胁遥测数据。SIO 持续收集其接收到的所有信息，对网络、域和应用进行分类并为其分配信誉分数。这些分数通过集中计算，迅速分配至配置为接收这些分数的思科设备。ASA CX 收到这些分数后，更新其全球环境存储库，开始识别新兴威胁，并着手实施防御这些威胁的操作。

假设某受欢迎新闻站点含有可将浏览器恶意重定向至包含恶意软件的主机的 HTTP GET 请求。毫不知情的用户访问该网站，即有可能在不经意间触发 GET 请求并将恶意软件下载至其计算机上。

ASA CX 可对这种“路过式”下载无缝防御，而不需该新闻网站的用户或所有者介入。借助来自 SIO 的信誉信息，ASA CX “知道”该新闻网站本身信誉良好。然而，ASA CX 并不会将该网站的良好信誉归属于恶意 GET 请求中的主机。当该主机试图通过 GET 请求将恶意软件下载到用户计算机上时，ASA CX 可识别出该问题主机的信誉很低。从而避免执行该下载，进而保护用户的计算机。

直观的管理

思科通过 ASA CX 重新设计防火墙时，还通过 Cisco Prime™ Security Manager (PRSM) 重新思考了防火墙管理，其使用 Web 2.0 技术简化了日常使用，并且不论安全人员管理着一个还是多个防火墙，都提供一致的体验。

轻松表达业务策略

经过优化的 PRSM 可将业务策略轻松转换为适当的防火墙配置。让我们假设安全人员想要配置访问 Yahoo! Messenger，同时阻止 Messenger 传输文件。使用传统的管理应用，该配置需要根据 IP 地址、协议和端口号协调创建多个规则，而且还必须不断修改这些规则以顾及 Messenger 实施的任何端口跳跃。

而使用 PRSM，只需点击几次鼠标，即可替代这种枯燥又容易出错的配置过程。安全操作人员导航至应用面板，通过名称搜索 Yahoo! Messenger，然后选中禁止文件传输的复选框即可。操作人员无需配置 IP 地址、协议或端口号。相反，操作人员想要的策略配置以日常业务语言表达出来 — 即“允许 Yahoo! Messenger 但禁用文件传输。”将业务策略转换为 IP 地址、协议和端口的低级规则的过程由 PRSM 全权负责。

全面的报告

要使情景感知安全起作用，安全人员必须能够生成报告并对特定事件进行详细分析。PRSM 包含全面且灵活的一揽子报告可加快该分析的速度。

ASA CX 根据配置生成标准格式的事件。这些事件可存储在设备上，也可发送至机下管理应用以便聚合和长期保存。这些事件还会被持续概括到报告中，安全操作人员可随时访问报告。另外，可用转换器将事件从 PRSM 标准格式转换成任何其他格式。因此，安全操作人员可继续使用其常用第三方工具来分析事件和报告。最后，报告支持细节展开功能，通过该功能，安全操作人员可获取事件的详细信息以进行调试、故障排除以及类似操作。

联机与多机的一致体验

Cisco PRSM 有两种版本。第一种是基于 Web 的联机 (on device) 版本，此版本与 ASA CX 集成。第二种是多机 (off-box) 版本，通常用于网络包含多个 ASA CX 的情况。联机版本与多机版本基本相同，但后者能够管理多个防火墙。因此，从安全操作人员的角度看，无论操作人员选择哪种管理应用版本（联机还是多机），ASA CX 的管理体验都是一致的。

清晰明确的用户界面

Cisco PRSM 包含许多组件，旨在为安全操作人员提供灵活有效的设备管理界面。

首先，整个界面上均有搜索栏。操作人员可在任何屏幕上以任何方式搜索策略、对象或事件，然后快速访问感兴趣的项目。另外，操作人员可将用户数据添加至任何策略或对象，方便以后有效搜索。其次，所有用户界面面板上均配有自动完成和自动建议快捷方式，让操作人员管理 ASA CX 时节省时间。第三，策略语言极为灵活，操作人员即使在复杂情况下也能构建简洁的策略。例如，操作人员可表达如下策略：“允许访问除用户 A 和 B 之外的所有工程组用户。”大多数竞争对手的防火墙管理应用均无法实现这样的表达，使得操作人员不得不人为建构冗长的规则。

PRSM 的用户界面为安全操作人员日常工作流程进行了优化。例如，为了响应复杂的访问权限，操作人员可在用户界面中创建并预览多种更改，然后使其生效。与此类似，操作人员可跟踪策略及其使用的对象的更改历史。这种详细信息使操作人员可协作定义多人接触的策略，或停用不再使用的对象。

基于模型的设计

Cisco PRSM 的核心是基于模型的设计。所有可配置对象均通过方案进行了建模，该方案描述对象的完整信息，包括可应用于该对象任何元素的配置类型。与方案关联的数据存储在 ASA CX 上的配置数据库 (Config DB) 中。同时，配置数据库和方案完整定义了 ASA CX 上的可配置对象的每个实例。

该方案将自动生成管理应用的用户界面模板，其是将方案导入 nScan Array 中检查引擎所用的代码模板。按此方式从方案生成代码，不仅能确保可配置对象的一致实施，而且能最大限度地减少管理应用中的软件错误。

REST API

Cisco PRSM 使用表征状态传输应用编程接口 (REST API) 创建。此 API 抽象化了配置数据库中的各种可配置对象，允许管理应用对这些对象使用一致的操作集。REST API 还可由安全操作人员使用，用于为 ASA CX 编写脚本或开发定制的管理应用。

灵活弹性的部署模式

虽然需要情景感知防火墙全面防护安全威胁，但其并没有使状态化第三层/第四层 (L3/L4) 防火墙过时。L3/L4 防火墙仍可广泛用于各种应用，包括在数据中心内，基于五元组的传统规则既有效也充分满足需求的情况。考虑到企业硬件和流程的现有投资，用情景感知防火墙大批替换现有 L3/L4 防火墙也不可取。

思科保护现有硬件投资的方法是：在现有思科 L3/L4 防火墙中添加情景感知 (CX) 模块，将其转换为 ASA CX。安装并配置该模块后，需要进行完整情景感知检查的那部分流量即通过该模块路由。其余流量使用基于 IP 地址、端口和协议的检查便已足够，这些流量照旧继续受到 L3/L4 防火墙的监控。因此，有意在安全基础设施中添加情景感知功能的企业无需使用新的防火墙替换现有硬件。由于现有防火墙设备仅需添加 CX 模块，因此也无需在网络中添加其他设备。CX 模块提供安全人员保护企业所需的所有额外可见性和控制。

另外，ASA CX 保护企业对现有流程和防火墙规则的投资。由于现有的思科 L3/L4 防火墙在网络中仍然可用，因此需要继续维护这些防火墙上配置的规则。然而，因 Cisco PRSM 能够读取、转换和管理现有 L3/L4 防火墙的配置，所以安全操作人员无需同时处理两种独立的防火墙管理应用。

最后，对没有部署思科防火墙的企业，ASA CX 避免了在具有部分情景感知功能但基础结构老旧的防火墙与无法实施状态化 L3/L4 防火墙上所有可用功能的防火墙之间作出选择。前者通常可实施当今企业所依赖的众多功能，如远程访问和网络地址转换，但其情景感知功能非常有限。后者提供即使不完整但更广泛的情景感知功能，但缺少安全操作人员所期待的一些重要功能。通过迁移到 ASA CX，这些企业可保持其现有传统防火墙功能的使用，同时获得对其网络中的应用、用户和设备的可见性和控制性。

因此，ASA CX 可以一种与时俱进的方式来部署，并随时与现有硬件和流程配合工作。同时，企业可获益于这种革命性架构，为其网络提供完整情景感知保护。

完整的 CISCO SECUREX 框架

借助 SecureX，思科制定了一个框架，为面临诸如 Web 应用和 IT 消费化等迅猛变化的企业提供保护。SecureX 框架将 AnyConnect 端点的本地环境和 TrustSec 标记、来自 SIO 的全球信誉信息和防火墙上实施的情景感知策略进行动态智能结合来确保网络安全。ASA CX 在防火墙中启用情景感知功能来完成 SecureX 框架。

有关 ASA CX 的更多信息，包括功能可用性的详细信息，请参阅 http://www.cisco.com/go/asa。

参考资料

《网络安全的未来：思科 SecureX 架构》，2011 年，Cisco System

《Cisco TrustSec：无边界网络情景感知安全访问》，2011 年，Cisco System

美洲总部
Cisco Systems. Inc
加利福尼亚州 圣荷西

亚太总部
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。思科网站上列有各办事处的地址、电话和传真，网址为：www.cisco.com/go/offices。

美国印刷

C11-700240-00 02/12