下一代数据中心：使用Cisco ASA 防火墙保护您的网络

当今的网络攻击数量激增且复杂性高，这要求数据中心实施能够令人高度放心的保护措施。当今的攻击针对个人客户数据及公司知识产权。因为失窃、失去客户信任及品牌形象受损而造成财务损失的可能性很大。

在这个快速变化的攻击形势下，基本的状态防火墙已不足以拦截复杂的攻击。深入检测每个网络流会直接降低应用性能。此外，安全设备架构必须采用虚拟应用，并在传统和下一代软件定义网络 (SDN) 环境中提供具有始终如一的高性能的相同功能集。

下一代数据中心安全解决方案必须：

- 易于扩展
- 提供深度防御方法以缩短应用延迟并提高性能
- 提供灵活的插入选项
- 高度可用且可以有弹性地进行扩展

适用于所有环境的灵活性能

现代数据中心的发展由多个因素形成。服务器和应用虚拟化的快速发展尤其要求脱离传统的静态网络拓扑。应用不再与数据中心网络中具有预先确定的物理位置的特定计算硬件关联。在通过 SDN 及其他方法引入的以应用为中心的新可编程模型中，也不再继续强调基于 VLAN 的分段和基本动态路由。在未来几年里，将继续不断提高可编程能力以实现数据中心转型。

由于许多相互依赖的应用现在托管于相同的物理服务器硬件上，因此将这些连接迁移到外部网络设备变得极其低效，且成本高昂。应用响应时间与网络延迟呈线性关系，甚至个别消费者开始期望获得以前实时财务应用独有的那种服务级别。如果客户无法等待，那么您的数据中心除了变得更快之外，别无选择。

由于所有应用环境中都越来越多地提出对低延迟或零延迟的要求，因此对于任何数据中心安全设备而言，功能模块化和相互依赖性最小化都是必需的。即使这类设备实现多项功能，其架构也应使得它能够通过进行最少数量的必要检查制定策略决策。如果可以根据特定终端的信誉拒绝入站连接，则几乎没有理由使用防火墙周期完全检测应用负载。Cisco® ASA 系列下一代防火墙依靠此深度防御方法，在部署专用高级保护模块以更详细地检查其余流量之前，拦截最基本的 TCP/IP 攻击。带有 FirePOWER™ 服务模块的 Cisco ASA 可使用其应用可视性和可控性 (AVC) 以及下一代 IPS (NGIPS) 功能，以避免对某些流量执行持续的深入检测并将其分流到主机 Cisco ASA 设备。例如，一旦已安装的 FirePOWER 模块识别应用并确认其安全状态，则高带宽的可信 Microsoft Active Directory 备份流量可以仅由 Cisco ASA 进行基本的第 2 层到第 4 层状态检查。使用此方法可以提高可信应用性能，并将宝贵的第 7 层检测资源改为用在较不可信的流量上。

许多防火墙在特定应用集成电路 (ASIC) 和现场可编程门阵列 (FPGA) 硬件模块上实现大部分安全功能。此方法带来低延迟和高性能，这对数据中心应用越来越重要。但是，此方法有许多缺点。最重要的是，检测功能受原始硬件设计限制。如果应用协议发生变化或引入新的安全功能，则即使最灵活的 FPGA 也难以保持预期的性能或支持较复杂的操作。这类防火墙通常被迫将此类连接发送至主 CPU（通常称为控制平面），但主 CPU 并非设计用于处理大量的中转连接。因此，防火墙性能在各个功能和流量配置文件之间变得不一致。

由于数据中心应用和相关攻击媒介变化得非常快，因此这类以硬件为中心的防火墙很快过时。Cisco ASA 5585-X 自适应安全设备通过使用多个硬件处理器和并行处理线程，在非常强大的通用 CPU 复合体中实现整个功能集。它将一些基本的转发任务分流到智能网络接口控制器 (NIC) 模块，并使用硬件加速器完成日常加密和解密操作。由于这些基本操作非常完善，因此在受保护应用不断变化时，不需要重新设计这些硬件组件的主要功能。只需要进行简单的软件更新，通用 CPU 复合体就可以轻松实现所有现有和新的应用协议及安全功能。此外，它在整个功能集中提供一致且可预测的性能。

通用 CPU 架构的另一项优势是易于移植。严重依赖 ASIC 和 FPGA 的安全设备无法在软件中非常高效地实现安全功能，因为它们并未打算处理硬件外部的大部分受保护连接。依赖物理网络设备保护虚拟化应用之间的流量是极其低效的，因此，应将用于应用间保护的安全设备移植到计算层。如果设备从未设计用于在通用 CPU 复合体中高效操作，则将此解决方案打包到虚拟外形难以实现功能支持和一致性能。模块化且具有高度可移植性的 Cisco ASA 架构支持新的思科虚拟 ASA (ASAv) 设备，此设备提供完整的 ASA 安全功能集。它具有保护类似物理终端和虚拟终端的所有功能，并可有效地保护虚拟终端，而无需离开计算层。由于快速调配服务是对基于云的数据中心提出的另一项新需求，因此可使用 Embrane 之类的以应用为中心的智能解决方案按需部署新的 Cisco ASAv 实例。

有状态可靠性和可扩展性

数据中心必须为其托管应用提供无与伦比的可用性。现代数据中心力求从所有已调配的硬件中获得最大价值，而不是简单地复制每个网络和计算硬件组件及消除单点故障。尽管一些较旧的数据中心设计依靠生成树协议 (STP) 阻止冗余第 2 层路径，但是下一代部署需要使用智能负载均衡机制来避免闲置的网络链路和设备。

EtherChannel 接口允许将多个物理以太网链路捆绑到单个逻辑接口中，所有成员端口可在此接口中主动转发流量。可以随时在捆绑中添加或移除这些成员接口，而不会对中转应用流量产生任何影响。为了对成员端口故障迅速作出反应，一些支持 EtherChannel 的高级设备实现标准化链路汇聚控制协议 (LACP) 以完成接口的动态捆绑和解绑。那些在没有 LACP 的情况下，仅支持静态 EtherChannel 捆绑的网络设备无法提供相同级别的服务保证。如果这类设备显示软件故障而未实际关闭接口链路，则通过静态捆绑的 EtherChannel 的中转应用流量可能会遭受黑洞攻击。

除了 EtherChannel 提供的链路级别冗余外，Cisco Catalyst® 6500 虚拟交换系统 (VSS) 和 Cisco Nexus® 虚拟端口通道 (vPC) 技术也允许在双主用模式下部署冗余交换机对。这样，两个机箱都会主动处理流量负载，而不是其中一个机箱保持备用状态。由于 VSS 或 vPC 对中的两个交换机作为单个逻辑实体，因此 EtherChannel 捆绑可将成员端口分布在两个物理机箱上，以实现完整的冗余和负载共享。Cisco ASA 5585-X 设备完全支持基于 LACP 的 EtherChannel，在独立和故障转移模式中，每个捆绑最多具有 16 个成员接口。这些下一代防火墙也可与 Cisco Catalyst VSS 和 Cisco Nexus vPC 部署进行完全的互操作。

高可用性在安全设备级也非常重要。由于大多数数据中心防火墙必须对所有中转连接执行状态检测，因此只沿着冗余路径部署几个这类设备是不够的。尽管新的应用流在原始设备发生故障的情况下将切换至新的防火墙实例，但因为缺少状态信息，必须重新建立现有连接。可在连接状态信息完全同步的冗余组中配置大多数状态安全设备。如果组中的一台设备出现故障，则另一设备可以按照应用安全情景在该设备中断的确切位置接管流量转发功能。

以此方法实现高可用性具有令人遗憾的缺点：最大状态连接数和连接建立速率无法随组中的安全设备数扩展。由于同一连接表同步至冗余组的所有成员，因此即使多个防火墙设备也无法扩展到超过单个成员的连接容量。对于应用连接量扩展非常迅速的任何现代数据中心而言（特别是为移动用户提供服务时），这种情况都是不可接受的。

许多这类状态安全解决方案的另一项重要限制在于，负载共享是通过单个冗余组成员实现的，该成员随后会将流量重定向至另一个防火墙进行处理。这实际上也将吞吐量限制为单个成员的吞吐量。Cisco ASA 5585-X 和 ASAv 防火墙支持设备级主用/备用和虚拟情景组级主用/备用故障转移部署，以实现经典、经过证实的高可用性。通过将每个数据接口上的单个虚拟主用 MAC 和 IP 地址对与状态连接数据复制配合使用，可完全透明地切换至相邻的网络设备和（最重要的）受保护应用。

除了故障转移之外，Cisco ASA 5585-X 还提供防火墙集群，这是真正的下一代高可扩展性解决方案。Cisco ASA 采用创新的技术，在保持完整状态会话冗余性的同时减少设备之间的数据重叠，而不是盲目地在所有集群成员间复制整个连接表。防火墙集群一次可以承受一个成员的损失而不影响应用连接。同时，它仍然可以采用“随增长，随投资”模式，扩展最大状态连接数和连接速率。

集群通过基于 LACP 的跨集群以太网信道、动态路由协议或基于策略的路由 (PBR) 支持无状态流量负载均衡。每个集群成员独立创建和处理中转连接并对任何外部流量不对称做出补偿。通过使用最多 16 个集群防火墙，Cisco ASA 现在可扩展至 640 Gbps 的总吞吐量以及 1 亿个并发状态连接和每秒 280 万次连接尝试。与 Cisco Nexus vPC 交换机对配合使用时，对于每个跨集群的 EtherChannel，Cisco ASA 集群最多支持 32 个成员端口。

任何拓扑中的高度安全性

传统防火墙的所有安全策略基于 IP 地址以及 TCP 或 UDP 传输端口。尽管此方法多年来已被证明在相对静态的数据中心应用部署中有效，但用户期望获得更抽象、更灵活的终端和应用身份方案。某些安全设备通过集成到特定的用户身份模型（例如 Microsoft Active Directory）中来解决此问题。此方法对限制来自专用终端上的内部用户的访问可能很有效，但它无法与可从外部访问的数据中心应用或快速增长的移动用户群一起扩展。

Cisco ASA5585-X 设备的 Cisco FirePOWER 硬件模块增加了在安全策略和报告中使用应用识别的功能。即使基于 IP 和传输端口的规则仍然在受控数据中心环境中提供更好的安全性，但它们可与基于应用的规则相结合以提高安全性和灵活性。例如，您可以创建一个策略规则，使其在 TCP 端口 1521 上仅允许进行 Oracle SQL*Net 数据库连接。这样做可以保护您的数据中心，以免恶意方通过众所周知且通常被允许的业务应用端口传送未授权的服务。同样，Cisco ASA FirePOWER 解决方案可自动检测其他众所周知的端口上的应用不匹配，例如用于 Secure Shell (SSH) 协议的 TCP/22 端口。使用这些内置的应用识别功能还可以通过自定义报告全面展现安全数据中心环境。

Cisco TrustSec® 解决方案提供了一个通用框架，用于在网络边界确定应用和终端身份，以及对所有参与设备集中实施访问策略。它使用安全组标记 (SGT) 和 SGT 名称构造将策略抽象化，以便可按照用户可读的元素编写防火墙规则。访问层和其他边缘设备还可以将适当的标记附加至中转帧，以在启用 Cisco TrustSec 的整个网络中实施内嵌策略和传播元数据。Cisco ASA 5585-X 和 ASAv 设备完全支持安全组访问控制列表 (SG-ACL) 策略，以顺利集成 Cisco TrustSec。Cisco ASA 防火墙从思科身份服务引擎 (ISE) 动态检索标记至名称的映射，并通过将 SGT 交换协议 (SXP) 邻接与边缘设备配合使用来了解分配的终端 SGT 值。Cisco ASA 平台还将在不久的未来支持基于内嵌帧标记的安全策略实施。

许多现代数据中心开始依靠第 3 层路由拓扑，以便连接主干和枝叶设计中的基础设施设备。除了各种路由协议支持以外，此方法还需要所有互联网络设备提供高可用性和快速收敛属性。

许多安全设备对动态协议的支持非常有限，但即使是高级设备，在冗余组内进行切换期间进行不间断转发时也会遇到困难。即使冗余防火墙建立独立的路由邻接，但是在使特定的防火墙停止运行时，相邻的路由器可能因动态协议保持计时器而将流量吸入黑洞。此中断可能仅持续大约一分钟，但对于现代的关键数据中心应用而言，几秒钟的停机时间也是不可接受的。

Cisco ASA 5585-X 支持各种动态路由协议（例如增强型内部网关路由协议 (EIGRP)、开放最短路径优先 (OSPF) 版本 2 和版本 3 以及边界网关协议 (BGP) 版本 4），以便集成到这类数据中心中。使用故障转移和集群时，系统会将维护动态路由协议邻接的设备中的路由信息库 (RIB) 数据结构复制到所有其他 Cisco ASA 设备中，从而允许在单个成员出现故障时进行不间断的状态流量转发。近期将在 Cisco ASA 平台上提供面向动态路由协议的标准化无中断转发 (NSF) 支持。然后，高度可用的 Cisco ASA 故障转移对或集群可在切换事件期间与直接相邻的路由器交互，并在两端保持不间断的流量转发。另一项即将推出的Cisco ASA 增强功能将在多个逻辑防火墙接口间启用等价多路径 (ECMP) 负载均衡，同时保持这类不对称流量的状态会话跟踪。此功能将进一步巩固 Cisco ASA 5585-X 在全网状的第 3 层数据中心拓扑中作为首选安全设备的地位。

在一些新的数据中心实施中，底层网络基础设施依靠状态设备服务群在需要进行应用分段的位置提供所需的安全服务。尽管使用 VLAN 和路由跳实施应用分段的当前方法多年来很有效，但此方法在 SDN 环境中将被安全服务插入取代。这类下一代技术的一个完美示例是思科以应用为中心的基础设施 (ACI)。Cisco ACI 帮助管理员按需将所需的网络拓扑和应用实例化，而不是围绕数据中心网络及其限制来设计应用。

传统安全设备受到访问规则激增问题的困扰（即使在停用关联的应用后，也未移除旧策略）。因此，防火墙规则表不断增长，从而使策略管理复杂化，并对应用性能产生负面影响。

Cisco ASA 5585-X 和 ASAv 都通过传统插入模式在本地集成到思科 ACI 中，其中直接从思科应用策略基础设施控制器 (APIC) 将防火墙和应用实例化。Cisco APIC 自动编写所有必要的 Cisco ASA 策略，以支持受保护的应用，并将防火墙服务直接纳入到应用间流量的路径中。当停用应用时，思科 APIC 也会在 Cisco ASA 上取消配置所有关联的防火墙策略。此方法消除了访问规则激增的危险，并使 Cisco ASA 规则集与受保护应用保持同步。由于 Cisco ACI 是无状态网络交换矩阵，因此它要求关联的安全设备为应用提供状态扩展功能。这是状态连接和连接速率可扩展性极其重要的另一个部署方案。ACI 与 Cisco ASA 集群完全兼容，因此您可使用此防火墙功能，在基于交换矩阵的下一代数据中心构建高度可扩展且功能强大的 SDN 安全服务群。

总结

现代数据中心正在多次转型，但安全性始终是一项重要因素。由于各种应用的要求变得更高，其关联的安全设备必须与它们保持同步。为满足低延迟和高性能要求，下一代数据中心防火墙在应用安全策略和分配资源方面变得更加智能。

仅使用基于硬件的安全设备已不足以保护快速变化的应用抵御越来越复杂的网络攻击。数据中心虚拟化的不断发展要求安全中心在物理和虚拟外形中提供相同的高性能和强大功能。高可扩展性在网络设备和链路级变得与高可用性同样重要。现代数据中心应用要求防火墙扩展吞吐量以及状态连接条目和连接建立速率。通过完全分布式连接处理和透明切换，正确设计的防火墙集群可以有弹性地随着数据中心应用的需求进行扩展。未来数据中心设计还要求安全设备全面实现访问策略抽象化、动态路由功能和 SDN 交换矩阵插入功能。

为什么选择思科

Cisco ASA 5585-X 和 ASAv 可保护物理和虚拟环境，通过在高度可扩展的通用 CPU 架构内采用有效的深度防御方法来满足所有下一代数据中心需求。Cisco ASAv 故障转移和 Cisco ASA 5585-X 集群功能有助于在“随增长，随投资”模式下，实现高可用性和可扩展性，以及在单个集群中使用 16 台设备实现最高 640 Gbps 的吞吐量。将基于 LACP 的 EtherChannel 插入到 VSS 和 vPC 交换机环境中，有助于Cisco ASA 在出现故障时以最快的反应速度保护关键的数据中心应用。可选 Cisco ASA5585-X 模块上的 FirePOWER AVC 和 NGIPS 服务启用基于应用的策略和高级威胁缓解功能，为数据中心提供最好的保护。采用 Cisco TrustSec 技术的 Cisco ASA SG-ACL 支持还为更灵活的安全策略提供更高水平的抽象。RIB 同步的强大动态路由功能和未来的 NSF 和 ECMP 支持使 Cisco ASA 5585-X 和 ASAv 成为第 3 层数据中心拓扑的完美防火墙。最后但同样重要的一点是，Cisco ACI 的有效互操作性有助于使所有 Cisco ASA 平台能够集成到下一代 SDN 交换矩阵拓扑中。

后续步骤

请访问以下网页，了解有关 Cisco ASA 防火墙的更多信息：

- http://www.cisco.com/c/en/us/products/security/asa-5585-x-adaptive-security-appliance/index.html。
- http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/design_guide_c22-624431.html。
- http://www.cisco.com/c/en/us/products/security/asa-firepower-services/literature.html。

美洲总部
Cisco Systems, Inc.
加州圣何西

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 C22-731801-01 10/14