应用于数据中心的 Cisco ASA 5585-X 防火墙

Cisco® ASA 5500 系列自适应安全设备集先进的状态防火墙和 VPN 集中器功能于一身。这些设备包括许多高级功能，例如多个安全场景（与虚拟化防火墙相似）、透明（2 层）防火墙或路由（3 层）防火墙操作、高级检测引擎、入侵防御、IPsec 和 WebVPN 支持等。

数据中心

我们将在本节论述与在数据中心部署防火墙相关的业务需求，以及所推荐解决方案的需求， 另外还将概述解决方案中包含的各种 ASA 技术。

业务需求：在数据中心部署防火墙

对于企业而言，数据中心比以往任何时候都更为重要。数据中心的数据服务集中度不断增加，导致对高性能且可扩展的网络安全性的需求也相应地增加。为了满足这一需求，思科推出了 ASA 5580，此设备可满足园区和数据中心的 5 Gbps 和 10 Gbps 需求。思科现在进一步拓宽了 ASA 产品组合：下一代 ASA 5585-X 设备正在扩展 ASA 5500 系列的性能范围，提供 2 Gbps 到 20 Gbps 的实际 HTTP 流量和 35 Gbps 的大数据包流量。Cisco ASA 5585-X 最高支持每秒 35 万个连接，在初始版本中最高支持 200 万个并发连接，预计将在后续版本中最高支持 1000 万个并发连接。

Web 2.0 应用的出现使得新型设备急剧增加并且复杂的内容得到广泛使用，这使现有的安全基础设施不堪重负。当今的安全系统通常无法满足这些环境中所需的高事务处理速度或安全策略深度。因此，信息技术人员通常会疲于提供基本安全服务和跟踪由这些系统生成的海量安全事件，以用于必要的监控、审计和合规用途。

Cisco ASA 5585-X 设备旨在为企业数据中心的多媒体应用、高事务性应用和延迟敏感型应用提供保护。ASA 5585-X 提供了市场领先的吞吐量、业内最高的连接速度、大量的策略配置和极低的延迟，非常适合具有要求最高的应用（如语音、视频、数据备份、科学计算或网格计算以及金融交易系统）的组织，可满足他们的安全需求。

解决方案要求

Cisco ASA 5585-X 设备提供了经济高效、基于性能的灵活解决方案，使得用户和管理员可以在组织内采用不同策略建立安全域。用户需要具备为不同 VLAN 设置适当策略的能力。数据中心需要状态防火墙安全解决方案来过滤恶意流量以及保护隔离区 (DMZ) 和外部网服务器群中的数据，同时以尽可能低的成本提供数千兆的性能。

Cisco ASA 5585-X 设备可采用“主用/主用”或“主用/备用”拓扑结构部署，并且可以使用接口冗余等附加功能来增强恢复能力。还有单独的链路用于容错链路和状态链路。

Cisco ASA 5585-X 设备可以为大型企业、数据中心和运营商网络提供数千兆的安全服务。该设备可容纳高密度铜缆和光纤接口，具备从快速以太网扩展到万兆以太网的能力，提供无与伦比的安全性和部署灵活性。在安全性虚拟化的过程中，这种高密度设计仍能保持托管安全性和基础设施整合应用中所需的物理分段。

适用范围

本文针对在数据中心中使用 Cisco ASA 5585-X 设备部署防火墙服务，提供有关设计注意事项和实施指南的信息。

Cisco ASA 技术概念

安全策略

防火墙可以保护内部网络免受外部网络的未授权用户进行访问。防火墙还可以在内部网络之间提供保护，例如使人力资源网络与用户网络分开。Cisco ASA 设备包含许多高级功能，例如多个安全场景（虚拟防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、数以百计的接口等等。在讨论连接到防火墙的网络时，外部网络位于防火强的前端，内部网络受防火墙保护，位于防火墙的后端。安全策略确定允许通过防火墙访问其他网络的流量类型，并且在通常情况下不允许任何流量通过防火墙，除非安全策略明确允许该流量通过防火墙。

思科入侵防御服务

思科高级检测和防御安全服务处理器 (ASA FirePower) 将内嵌的入侵防御服务与创新技术相结合来提高准确性。如果将 FirePower 部署在 Cisco ASA 5585-X 设备中，则 SSP 通过与其他网络安全资源协作，提供一种主动保护网络的方法，从而为 IPv6 和 IPv4 网络提供全面的保护。

Cisco ASA FirePower 具备下列功能，可帮助您充满信心地防御威胁：

- **范围广泛的 IPS 功能：**Cisco ASA FirePower 提供了 Cisco SourceFire 系列传感器上具备的所有 IPS 功能，可以内嵌部署在流量路径中，或以混杂模式部署。
- **全球互联：**Cisco ASA FirePower 通过增加信誉分析功能、缩短暴露于威胁之下的时间窗并提供持续的反馈，针对您的网络边界之外的全球威胁环境提供实时更新。
- **全面且及时的攻击防护：**Cisco ASA FIrePower使用专用的 IPS 检测引擎和数以千计的特征，针对数以万计的已知漏洞以及数百万个潜在的未知漏洞变体提供保护。
- **零日攻击防护：**思科异常检测功能可学习您的网络中的正常行为，并在发现您的网络中出现异常活动时发出警报，这有助于防范新的威胁，甚至在获得特征之前也可以做到这一点。

对 ASA 设备中的流量部署 IPS 后，这些流量将自动继承设备的所有冗余功能。

高可用性

Cisco ASA 安全设备提供业内恢复能力最强、最全面的高可用性解决方案之一。使用诸如次秒级故障转移和接口冗余等功能，客户可以实施非常先进的高可用性部署，其中包括全网状“主用/备用”和“主用/主用”故障转移配置。这使客户可以持续防范基于网络的攻击并保护连接，以满足当今的业务需求。

使用“主用/主用”故障转移时，两台设备都可以传递网络流量。这使得您还可以在网络上配置流量共享。“主用/主用”故障转移仅适用于在“多”情景模式下运行的设备。使用“主用/备用”故障转移时，一台设备传递流量，另一台设备在备用状态下等待。“主用/备用”故障转移适用于在“单”或“多”情景模式下运行的设备。两种故障转移配置都支持有状态和无状态故障转移。

如果出现以下事件之一，则设备可能无法工作：

- 设备出现硬件故障或电源故障。
- 设备出现软件故障。
- 过多的监控接口出现故障。
- 管理员使用 CLI 命令“no failure active”触发了人工故障

即使启用了有状态故障转移，设备到设备的故障转移也可能导致一些服务中断。下面是一些示例：

- 必须重新启动未完成的 TCP 三向握手。
- 在 Cisco ASA 软件版本 8.3 及更早版本中，不将开放最短路径优先 (OSPF) 路由从主用设备复制到备用设备。在故障转移时，必须重新建立 OSPF 邻接并且必须重新学习路由。
- 大多数检测引擎的状态未同步到故障转移对等设备。向对等设备进行故障转移会丢失检测引擎的状态。

“主用/备用”故障转移

“主用/备用”故障转移使您可以利用备用安全设备来接管故障设备的功能。主用设备出现故障时将变为备用状态，同时备用设备变为主用状态。变为主用状态的设备将采用故障设备的 IP 地址（对于透明防火墙，则采用管理 IP 地址）和 MAC 地址，然后开始传递流量。现在处于备用状态的设备将接管备用 IP 地址和 MAC 地址。由于网络设备未看到 MAC 到 IP 地址对的变化，因此网络中没有位置会出现地址解析协议 (ARP) 条目更改或超时。

在“主用/备用”故障转移中，故障转移基于物理设备进行，而非基于多情景模式中的情景。“主用/备用”故障转移是 ASA 平台上最常部署的高可用性方法。

“主用/主用”故障转移

“主用/主用”故障转移可供“多”情景模式下的安全设备使用。两台安全设备可以同时传递网络流量，并且可采用处理不对称数据流的方式部署。可以将安全设备上的安全情景分成故障转移组。一个故障转移组仅仅是一个或多个安全情景的逻辑组。安全设备上最多可以创建两个故障转移组。

故障转移组构成了“主用/主用”故障转移中的故障转移基本设备。接口故障监控、故障转移和主用/备用状态都是故障转移组（而非物理设备）的属性。主用故障转移组出现故障时将变为备用状态，同时备用故障转移组变为主用状态。故障转移组变为主用状态时，其中的接口将采用出现故障的故障转移组中的接口的 MAC 地址和 IP 地址。现在处于备用状态的故障转移组中的接口将接管备用 MAC 和 IP 地址。此行为类似于物理的“主用/备用”故障转移中的行为。

冗余接口

接口级别的冗余基于此概念：可以在 ASA 设备的两个物理接口上配置一个逻辑接口（称为冗余接口）。Cisco ASA 软件版本 8.0 中引入了此功能。

一个成员接口将用作负责传递流量的主用接口。另一个接口保持备用状态。当主用接口出现故障时，所有流量将故障转移到备用接口。此功能的主要优点是故障转移将在同一物理设备内进行，这可以防止不必要地进行设备级故障转移。这些冗余接口在配置之后将被视为物理接口。

主用设备上的链路故障将导致设备级故障转移，而冗余接口则不会。在数据中心环境中，以下是使用冗余接口创建全网状拓扑的优点：

- 在出现接口级故障转移时不必重新启动未完成的 TCP 三向握手。
- 如果 ASA 设备上使用了动态路由协议，则不必重新建立/重新学习路由邻接。
- 出现接口级故障转移时，大多数检测引擎的状态不会丢失，但在出现设备级故障转移时则相反。

对最终用户的影响较小，因为 ASA 有状态故障转移并不复制会话的所有数据。例如，不会复制某些语音协议（例如媒体网关控制协议 [MGCP]）的控制会话，并且故障转移可能会中断这些会话。

使用接口冗余功能时，仅当两个底层物理接口均出现故障时，（冗余）接口才会被视为处于故障状态。

接口级冗余的主要优点是：

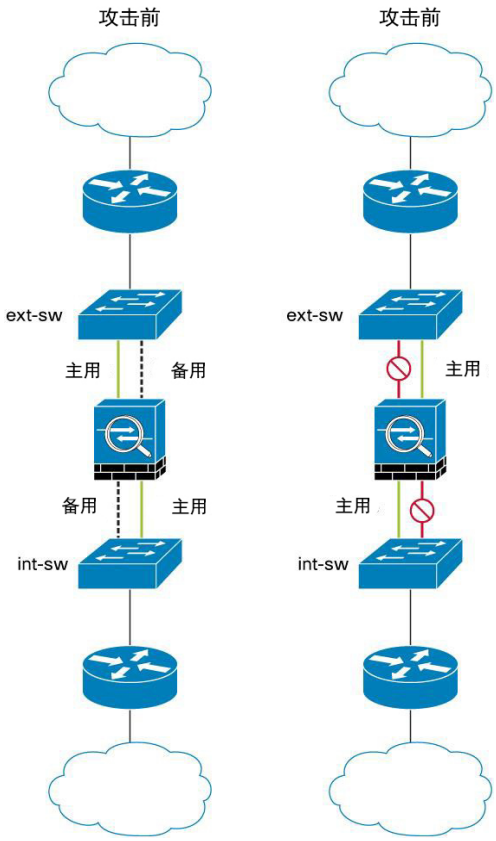
- 降低故障转移环境中出现设备级故障转移的概率，从而提高网络/防火墙可用性，并消除不必要的服务/网络中断。
- 实现全网状防火墙架构以提高吞吐量和可用性。

图 1 描绘了 ASA 设备的简单部署方案，其中启用了接口冗余功能，并且没有设备级（A/S 或 A/A）故障转移。

在此方案中，当出现 ASA 接口故障时，安全设备将继续传递流量，因为冗余接口的备用物理接口将用作主用接口，接管其功能。

单情景模式、多情景模式、路由防火墙模式和透明防火墙模式均支持此设计。

图 1. 本图描绘的是使用冗余接口前后的图片，其中引入了物理接口故障，未引入任何冗余接口故障。

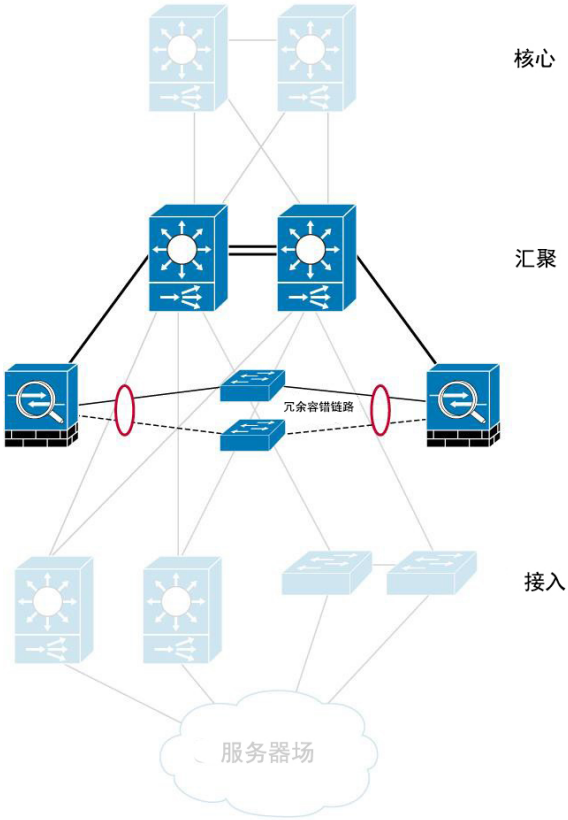


Cisco ASA 5585-X 设备适合标准数据中心设计，如图 2 所示。VLAN 从物理交换机扩展到外部 ASA 设备，并使用连接到单独交换机的专用冗余故障转移链路和状态链路。将结合使用之前部分中介绍的技术，创建高度冗余的网络设计。我们将使用 ASA 设备上的以下三项主要功能：

- 冗余接口
- “主用/主用”故障转移
- 透明模式
- 您可以将一台 ASA 设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。在“多”情景模式中，ASA 设备包括用于每个情景的配置，其中确定安全策略、接口以及可以在独立设备中配置的几乎所有选项。系统配置确定 ASA 的基本设置，但不包括它本身的任何网络接口或网络设置。“管理”情景与所有其他情景相似，但有一点不同：用户登录到“管理”情景时具有系统管理员权限，可以访问“系统”情景和所有其他情景。

架构概述

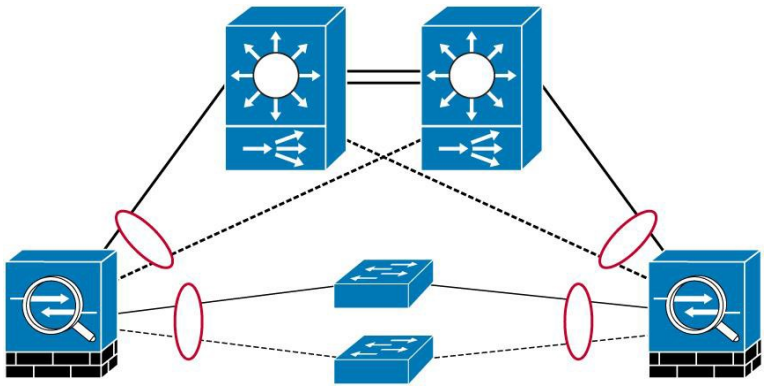
图 2. 标准数据中心架构



IPS 服务可以集成到设计内的每台 ASA 设备中，也可以采用单独的独立 IPS/IDS。在 ASA 设备内实施 IPS 服务的优点：您可以使用精细控制，对将由 IPS 服务检测的流量进行分类。

ASA 5585-X 通过连接中继端口集成到架构中的汇聚层，这些中继端口承载将受到防火墙保护的 VLAN 流量。如果需要，还可以为汇聚层配置冗余链路，以提供额外的可用性级别（图 3）。主用设备上的链路故障将导致设备级故障转移，而冗余接口则不会。

图 3. 冗余链路连接



透明或路由防火墙模式

Cisco ASA 5585-X 支持两种不同的防火墙模式：路由和透明。在路由防火墙模式中，ASA 设备被视为网络中的一个路由器跳点。在透明防火墙模式中，该设备的行为就像一个“隐蔽防火墙”，不被视为一个路由器跳点。ASA 设备的内部和外部接口连接到同一网络。如果希望防火墙对攻击者不可见，则透明模式非常有用。数据中心设计使用透明模式来支持 ASA 设备上的“主用/主用”架构。

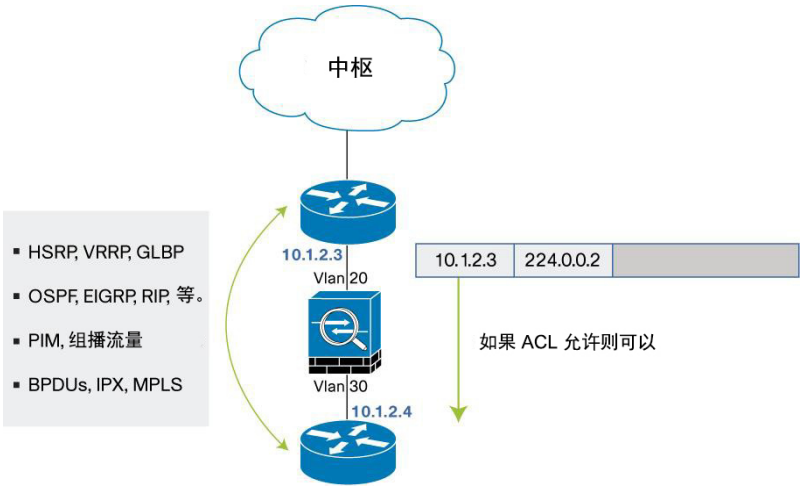
表 1 显示了这两种部署类型的功能。

表 1. 路由和透明防火墙模式的比较

路由	透明
具有 NAT 的所有“特点” 路由数据流量 不传递组播流量 可以在情景之间共享接口	每个情景两个接口 透明模式下支持 NAT 桥接数据流量 传递组播流量 无共享接口

在透明模式下，Cisco ASA 5585-X 设备不是一个路由器跳点。ASA 设备的内部和外部端口连接到同一网络，但每个端口必须位于不同的 VLAN。ASA 设备上无需任何动态路由协议或 NAT。数据中心中的透明模式的其他优点如图 4 所示。

图 4. 数据中心中的透明防火墙模式



- 路由器可以通过防火墙建立路由协议邻接。
- 热待机路由器协议 (HSRP)、虚拟路由器冗余协议 (VRRP) 和网关负载均衡协议 (GLBP) 等协议可以穿过防火墙。组播流也可穿过防火墙。
- 可以允许非 IP 流量（预配置的类型为 IPX、MPLS 和 BPDU），但必须使用 Ethernet V2/DIX 封装 – 无检测，只进行桥接。

性能和可扩展性

到目前为止，防火墙性能的主要决定因素一直是吞吐量 (Mbps)。但是，各种应用的要求变得更加苛刻，现在需要连接在更长的时间内一直保持打开状态（如文件共享或多媒体中使用的持久连接），或者打开许多短暂的连接（如 Facebook 等常用网站通常使用的连接）。

吞吐量仍然很重要，处理较新应用的能力也将变得同等重要，这些应用对并发连接能力以及快速打开新连接的能力要求越来越高。Cisco ASA 5585-X 扩展了这些功能，但对每秒连接速率和同时连接总数给予了特别关注，以提供优异的性能。Cisco ASA 5585-X 利用具有极低延迟和并行 CPU 架构的高速交换背板满足了性能要求。

小结

在本文档中，我们考虑到常用数据中心的需求，介绍了如何在数据中心设计中使用 Cisco ASA 5585-X 设备。我们已经通过采用一种高度冗余的网络设计和 ASA 5585-X 内的高可用性功能，以对设计具有最小破坏性影响的方式将 ASA 5585-X 部署在数据中心。

更多详情

有关 Cisco ASA 5500 系列设备的更多信息，请访问 http://www.cisco.com/go/asa 或联系您当地的客户代表。

有关思科生命周期终止策略的更多信息，请访问：
http://www.cisco.com/en/US/products/prod_end_of_life.html。

如需订阅以接收生命周期终止/销售终止信息，请访问：
http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice。

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
荷兰阿姆斯特丹

Cisco 在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。

美国印刷 C22-624431-00 10/10