白皮书

通过 ASA 防火墙集群加强网络防御

概述

Cisco® ASA 5585-X 自适应安全设备支持将多个相同的防火墙节点集群作为一个逻辑防火墙。此功能：

- 可实现更高的吞吐量、连接速率和并发连接数量
- 提供可预测的可扩展解决方案
- 使客户可以根据其需求进行购买，并在流量增加时添加更多节点

更高的性能对于数据中心尤其重要，因为在数据中心中，一个位置处理大量的流量。

集群的优势

通过集群防火墙节点，可将冗余扩展到按设备提供的传统主用/备用冗余之外。冗余现在按流量提供，单个集群中最多具有 16 个节点。这一转变显著提高了防火墙保护的可用性，并且总体上改善了网络的稳定性。

集群中的所有节点只有一个配置。对该配置的任何更改仅在主节点做出，然后传播到所有从属节点。集群中的所有节点必须相同是有一个原因的。当主节点出现故障时，一个不同的节点承担主节点的职责，无需人工干预。

接收流量中的第一个数据包的节点被称为流量的所有者。然后根据源和目标的 IP 地址及端口号的散列值，将另一个节点选择为流量的主管。然后，流量的所有状态信息使用专用的集群控制链路 (CCL) 传送到流量的主管。因此，两个节点始终具有每个流量的状态信息。CCL 仅供节点用于在节点之间共享关于集群中的不同流量的信息，以及用于数据流量（对于不对称的流量）。集群控制链路放置在与数据链路分开的 VLAN 中。

如果一个节点的集群控制链路出现故障，将从集群中移除该节点，并且之后不会有流量发送到该节点。因此 Cisco 建议为集群控制链路提供冗余，方法是将链路放置在 EtherChannel 中以防范接口故障。

如果所有者节点因任何原因出现故障，流量的数据包发送到集群中的某个不同节点。此节点（如果不是流量的主管）能够使用源和目标的 IP 地址及端口号的散列值找到流量的主管。此节点然后向主管查询流量的状态信息。然后此节点成为特定流量的所有者。使用新的所有者信息更新流量的主管。

对于不对称流量，返回的数据包发送到与所有者不同的节点，接收数据包的节点被称为转发者。转发者与流量的主管联系以查找其所有者。一旦知道所有者，流量将在流量持续时间内通过集群控制链路转发给所有者。

在具有大量不对称流量的网络中，建议为数据链路和集群控制链路分配相同数量的接口。这也是集群中的所有节点必须相同的另一个原因，因为不同的节点具有不同的接口数量和功能。

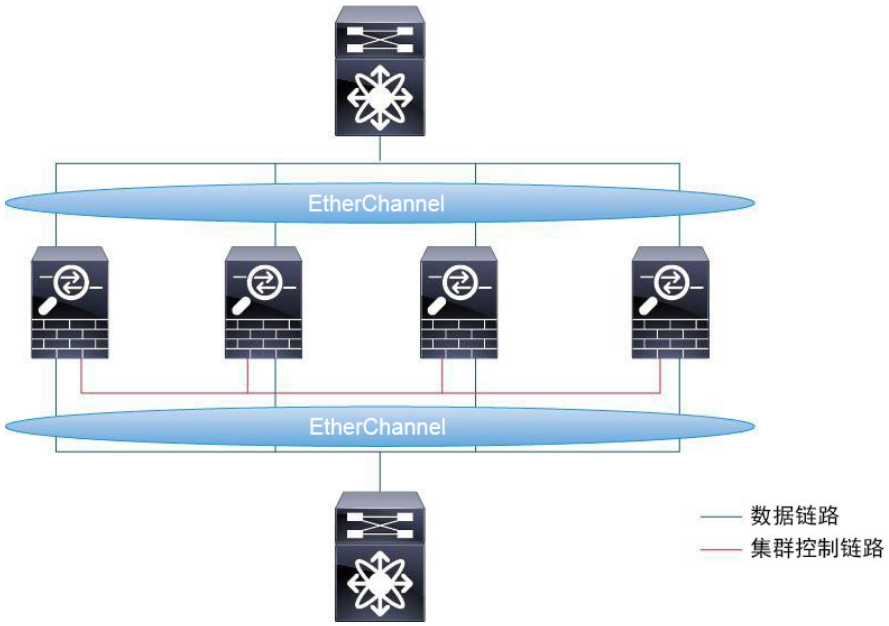
单个集群中最多支持 16 个节点。将所有这些节点作为单个逻辑防火墙进行管理。但是也提供查看集群中各个节点的统计信息的功能。集群升级在流量没有任何中断的情况下实现，因为在升级期间允许集群中的节点处于不同的次要版本。

在集群中，采用两种方法将流量负载均衡到多个 ASA 节点。一种方法是将数据接口配置为扩展的 EtherChannel 接口，另一种方法是将数据接口配置为各个接口。

扩展的 EtherChannel 接口

在此类部署中，EtherChannel 将数据流量负载均衡到群集的各个节点（见图 1）。

图 1. 由扩展的 EtherChannel 接口进行的负载均衡



EtherChannel 汇聚两台设备之间的多条链路以提高吞吐量。一项额外的优势：在一个接口出现故障时，将通过重新分配两台设备之间的流量来提供高可用性。链路汇聚控制协议 (LACP) 允许在两台设备之间动态协商和建立 EtherChannel。在 ASA 上实施的集群 LACP (cLACP) 使集群中的多个 ASA 节点对它们连接到的交换机显示为一个逻辑防火墙。实现这一点的方法是将不同节点上的多个接口绑定到 Cisco ASA 端的单个大 EtherChannel。

虚拟端口通道 (vPC) 使物理连接到 Cisco Nexus® 7000 系列交换机的链路对Cisco ASA显示为单个 EtherChannel。vPC 还使所有链路可以主动转发流量，从而最大限度地利用硬件。

虚拟交换系统 (VSS) 还利用冗余的 Cisco Catalyst® 6500 系列交换机的所有可用第 2 层带宽，并且提供均匀的负载均衡。ASA 集群也支持 VSS。

在 EtherChannel 中，当不能将所有可用端口置于主用状态时，动态端口优先级使设备可以选择将哪些端口置于备用状态。大多数交换机在一个 EtherChannel 中最多支持 8 个主用和 8 个备用端口。如果在 Cisco ASA 集群上禁用动态端口优先级，通过将备用端口置于主用状态，可以将 EtherChannel 中的主用端口数量增加到 16 个。

通过使可用于数据流量的主用链路翻倍，达到 32 个（最大值），vPC 和 VSS 为交换基础设施提供设备冗余。在 vPC 处于工作状态时使用 Cisco Nexus 7000 F 系列线卡可实现这一增加。

只有一个逻辑 IP 和 MAC 地址由集群的所有数据接口共享。在这里，防火墙以透明模式或路由模式部署。在透明模式下，IP 地址分配给桥组。在路由模式下，IP 地址分配给配置为路由接口的 EtherChannel。

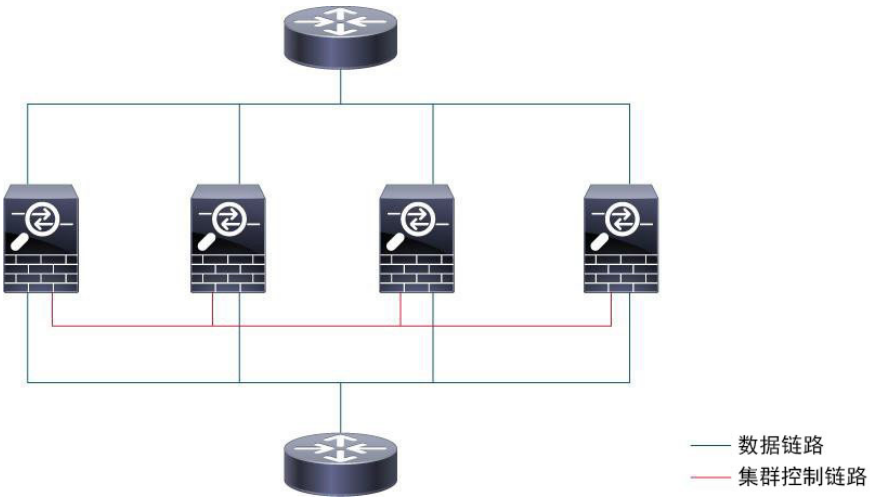
思科推荐扩展的 EtherChannel 接口类型，因为在集群中添加或移除 ASA 节点时对流量没有影响。在集群中动态添加或移除节点的能力适合满足客户不断变化的业务需求，同时始终提供高可用性。

建议防火墙内侧和外侧接口上的交换机采用相同的散列算法，以避免不对称路由，从而帮助获得更好的性能。

各个接口

在部署各个接口时，相邻的路由器执行将数据流量负载均衡到不同 ASA 节点的任务（见图 2）。负载均衡通过使用基于策略的路由或等价多路径来完成。

图 2. 由各个接口进行的负载均衡



对于基于策略的路由，ASA 节点之间的流量负载均衡是静态的。负载均衡采用多种方法完成；例如，它基于流量或流量的分类。建议实施 Cisco IOS IP 服务级别协议 (IP SLA) 和对象跟踪，以了解哪些节点已加入或离开集群。

对于等价多路径 (ECMP)，负载均衡在路由协议的帮助下动态完成。ECMP 是基于流量的首选流量负载均衡方法。各个 ASA 节点运行动态路由协议，并与路由器建立独立的邻接关系和维护其路由表。在节点出现故障时，我们依靠动态路由协议向路由器通知此类故障，同时流量进入黑洞，直到该通知完成为止。因此，我们建议降低路由协议的 hello 和 dead 计时器间隔，以确保更快地融合。

群集中的每个 ASA 节点都有自己的 IP 地址用于数据接口和负载均衡流量。因此，仅在路由模式下支持防火墙。

EtherChannel 支持捆绑各个 ASA 节点上的多个数据端口。对于集群中的每个节点，您将具有一个本地 EtherChannel。

总结

随着数字化在全球范围内广泛发展，连接的人员和设备越来越多，数据流量不断增长。这带来了许多商机和挑战。企业和运营商必须保持低延迟、高度可用的网络，同时始终确保数据安全。另外，当今的许多应用在本质上是突发性的。Cisco ASA 的防火墙集群提供一个高度可用的解决方案，该解决方案可扩展吞吐量，更重要的是可以扩展连接速率以满足业务需求。思科强烈建议在由扩展的 EtherChannel 接口进行负载均衡的情况下部署集群，以简化配置和提高可靠性。

更多详情

Cisco ASA 5500-X Configuration Guide（Cisco ASA 5500-X 配置指南）

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
C11-731852-00 05/14