高可用性选项

高可用性选项

分布式VPN集群、负载均衡和故障转移功能是工作方式不同并具有不同要求的高可用性功能。在某些情况下，您可能会在部署中使用多项功能。以下几节介绍了这些功能：有关分布式VPN和故障转移的详细信息，请参阅相应版本的《ASA 常规操作 CLI 配置指南》。此处介绍了负载均衡的详细信息。

Cisco Secure Firewall eXtensible 操作系统 (FXOS) 机箱上的 VPN 和集群

ASA FXOS 集群支持站点间 VPN 两个相互排斥的模式之一，即集中式或分布式：

- 集中式 VPN 模式。默认模式。在集中式模式下，仅与集群的控制设备建立 VPN 连接。

  VPN 功能仅限控制设备使用，且不能利用集群的高可用性功能。如果控制设备发生故障，所有现有的 VPN 连接都将断开，通过 VPN 连接的用户将遇到服务中断。选择新的控制设备后，必须重新建立 VPN 连接。

  将 VPN 隧道连接到跨接口地址时，连接会自动转移到控制设备。与 VPN 相关的密钥和证书将被复制到所有设备。

- 分布式 VPN 模式。在此模式下，站点间 IPsec IKEv2 VPN 连接将跨 ASA 集群成员分布，从而提供可扩展性。在集群成员之间分布 VPN 连接可实现充分利用集群的容量和吞吐量，将 VPN 支持大幅扩展至集中式 VPN 功能之外。

注释 集中式 VPN 集群模式支持站点间 IKEv1 和站点间 IKEv2。

分布式 VPN 集群模式仅支持站点间 IKEv2。

仅在 Firepower 9300 上支持分布式 VPN 集群模式。

集中式和分布式集群模式均不支持远程访问 VPN。

VPN 负载均衡

VPN 负载均衡是在 VPN 负载均衡组中的设备之间合理分配远程访问 VPN 流量的机制。它基于简单的流量分配，而不考虑吞吐量或其他因素。VPN 负载均衡组由两台或更多设备组成。一台设备是导向器，而其他设备是成员设备。组设备不需要是完全相同的类型，也不需要具有相同的软件版本和配置。

VPN 负载均衡组中的所有主用设备都会承载会话负载。VPN 负载均衡可以将流量定向至组中负载最低的设备，在所有设备之间分配负载。这样可以高效地利用系统资源，提供更高的性能和高可用性。

故障转移

故障转移配置需要通过专用故障转移链路和状态故障转移链路（后者可选）相互连接的两台相同 ASA。主用接口和设备的运行状况会受到监控，以便确定满足特定故障转移条件的时刻。如果这些条件得到满足，则会进行故障转移。故障转移同时支持 VPN 和防火墙配置。

ASA 支持两种故障转移配置：主用/主用故障转移和主用/备用故障转移。

使用主用/主用故障转移时，两台设备都可以传送网络流量。这不是真正的负载均衡，尽管看似具有相同的效果。发生故障转移时，剩下的那台主用设备会根据配置的参数接管合并流量的传送。因此，配置主用/主用故障转移时，您必须确保两台设备的合并流量在每台设备的容量之内。

使用主用/备用故障转移时，只有一台设备会传送流量，而另一台设备会在备用状态下进行等待，不会传送流量。主用/备用故障转移允许使用第二台 ASA 来接管故障设备的功能。当主用设备发生故障时，它将变为备用状态，而备用设备会变为主用状态。变为活动状态的设备会采用发生故障的设备的 IP 地址（或者，对于透明防火墙，管理 IP 地址）和 MAC 地址，并开始传送流量。此时，处于备用状态的设备会接管主用设备的备用 IP 地址。如果主用设备发生故障，则由备用设备接管，而且不会给客户端 VPN 隧道带来任何干扰。

VPN 负载均衡

关于 VPN 负载均衡

如果您拥有一个远程客户端配置，在该配置中使用连接至相同网络的两个或更多 ASA 来处理远程会话，则可以通过创建 VPN 负载均衡组来将这些设备配置为共享其会话负载。VPN 负载均衡会将会

话流量定向至负载最低的设备，从而在所有设备之间分配负载。这样可以高效地利用系统资源，并提高性能和可用性。

VPN 负载均衡组中的所有设备都会承载会话负载。组中的一台设备，即导向器会将传入的连接请求定向至称为成员设备的其他设备。导向器会监控组中的所有设备、追踪每台设备的繁忙情况，然后相应地分配会话负载。导向器的角色不会与某台物理设备绑定；它可以在设备之间切换。例如，如果当前的导向器发生故障，该组的一台成员设备会接管该角色，立即成为新的导向器。

VPN 负载均衡组会对外部客户端显示为单个虚拟 IP 地址。此 IP 地址不与特定物理设备绑定。它属于当前导向器。VPN 客户端会尝试建立连接，先与虚拟 IP 地址连接。随后，导向器会将组中负载最低的可用主机的公用 IP 地址，发送回客户端。在第二个事务（对用户透明）中，客户端会直接连接至该主机。这样，VPN 负载均衡组导向器就能在资源之间均匀、高效地定向流量。

如果组中的一个 ASA 发生故障，终止的会话可以立即重新连接到虚拟 IP 地址。随后，导向器会将这些连接，定向至组中的另一活动设备。如果导向器发生故障，则组中的成员设备会立即自动接管，成为新的导向器。即便该组中的多台设备发生故障，只要该组中的任一设备正常运行，并且可用，用户仍然可以继续与该组连接。

对于每个 VPN 负载均衡集群设备，必须配置公共/外部 (lbpublic) 和专用/内部 (lbprivate) 接口。

- 公共接口：设备的外部接口，用于与集群 IP 地址进行初始通信。此接口用于 Hello 握手。
- 专用接口：用于在负载均衡集群成员之间进行消息传送的设备内部接口。这些消息包括与负载均衡相关的保持连接、拓扑消息和服务中断消息。

VPN 负载均衡算法

VPN 负载均衡组导向器会维护一个按 IP 地址升序排列的组成员列表。每个成员的负载计算为整数百分比（活动会话数）。Secure Client 非活动会话不会被计入 VPN 负载均衡的 SSL VPN 负载。导向器会将 IPsec 和 SSL VPN 隧道重定向至负载最低的设备，直到其百分比值比其余设备高出 1%。当所有成员都比导向器高 1% 时，导向器就会将流量重定向到自身。

例如，如果您有一个导向器和两个成员，则以下循环适用：

注释 所有节点的百分比值都从 0% 开始，而且所有百分比值都会四舍五入。

1. 如果所有成员的负载都比导向器高出 1%，则导向器会接受连接。
2. 如果导向器没有接受连接，则哪台成员设备负载百分比值最低就由哪台备用设备接受会话。
3. 如果所有成员的负载百分比值相同，则由会话数最少的成员获得会话。
4. 如果所有成员的负载百分比值和会话数都相同，则由 IP 地址最少的成员获得会话。

VPN 负载均衡组配置

VPN 负载均衡组可由相同版本或混合版本的 ASA 组成，并会受到以下限制：

- 包含两个相同版本 ASA 的 VPN 负载均衡组，可以为混合的 IPsec、Secure Client 和无客户端 SSL VPN 客户端会话进行 VPN 负载均衡。
- 包含混合版本 ASA 的 VPN 负载均衡组可支持 IPsec 会话。不过，在这样的配置中，ASA 可能无法达到其最高 IPsec 容量。

组的主管会将会话请求分配给组的成员。ASA 会同等地对待所有会话（SSL VPN 或 IPsec 会话），并相应地分配它们。您可以配置允许的 IPsec 和 SSL VPN 会话的数量，可配置的数量最多为您的配置以及许可证允许的最大数量。

我们已测试过 VPN 负载均衡组中的最多 10 个节点。更大的组可能能够正常工作，但是我们不正式支持此类拓扑。

VPN 负载均衡导向器选举

导向器选举过程

虚拟集群中的每个非主设备都会维护一个本地拓扑数据库。每当集群的拓扑发生更改时，主设备都会更新该数据库。如果在最大重试次数后未收到主设备的 Hello 响应或未收到主设备的保持连接响应，则每个非主设备都会进入主设备选举状态。

成员在导向器选举期间执行以下功能：

- 比较本地拓扑数据库中找到的每个负载均衡设备的优先级。
- 如果找到两台具有相同优先级的设备，则选择具有较低 IP 地址的设备。
- 如果成员本身当选，则它会申领虚拟 IP 地址。
- 如果选举了其他成员之一，则该成员将向当选的主设备发送 Hello 请求。
- 当两台成员设备尝试申领虚拟 IP 地址时，ARP 子系统会检测到重复的 IP 地址情况，并发送通知要求具有更高 MAC 地址的成员放弃导向器角色。

Hello 握手

每个成员会在启动时向外部接口上的虚拟集群 IP 地址发送 Hello 请求。如果收到 Hello 请求，主设备会向成员发送自己的 Hello 请求。非导向器成员在收到导向器的 Hello 请求后会返回 Hello 响应。Hello 握手到此结束。

完成 Hello 握手后，如果配置了加密，则会在内部接口上发起连接。如果在最大重试次数后成员仍未收到 Hello 响应，则该成员将进入主设备选举状态。

Keepalive 消息

在成员和导向器之间完成 Hello 握手后，每台成员设备都会定期向主设备发送保持连接请求及其负载信息。如果导向器没有未完成的保持连接响应，则在正常处理期间，成员设备会以一秒为间隔发送保持连接请求。这意味着只要收到来自上一个请求的保持连接响应，就会在下一秒发送下一个保持连接请求。如果成员未从导向器收到上一个保持连接请求的保持连接响应，则下一秒不会发送保持连接请求。相反，成员的保持连接超时逻辑将启动。

保持连接超时的工作原理如下：

1. 如果成员正在等待导向器的未决保持连接响应，则该成员不会发送常规的一秒间隔保持连接请求。
2. 成员将等待 3 秒，并在第 4 秒时发送保持连接请求。
3. 只要导向器没有保持连接响应，成员就会重复五 (5) 次上述步骤 2。
4. 然后，该成员宣布该导向器已消失，并开始新的导向器选举周期。

有关 VPN 负载均衡的常见问题

多情景模式

问: 在多情景模式下是否支持 VPN 负载均衡？

答: 在多情景模式下，既不支持 VPN 负载均衡也不支持状态故障转移。

IP 地址池耗尽

问: ASA 是否会将 IP 地址池耗尽视为其 VPN 负载均衡方法的一部分？

答: 不会。如果远程访问 VPN 会话被定向至已耗尽其 IP 地址池的设备，则会话不会建立。负载均衡算法基于负载，会计算为每个成员提供的整数百分比（活动会话数和最大会话数）。

唯一 IP 地址池

问: 要实施 VPN 负载均衡，不同 ASA 上的 Secure Client或 IPsec 客户端的 IP 地址池必须是唯一的吗？

答: 是的。IP 地址池对于每台设备必须是唯一的。

在相同设备上使用 VPN 负载均衡和故障转移

问: 一台设备可以同时使用 VPN 负载均衡和故障转移吗？

答: 是。在此配置中，客户端连接至组的IP地址，然后被重定向至组中负载最低的ASA。如果该设备发生故障，备用设备会立即接管，不会对 VPN 隧道产生任何影响。

多个接口上的 VPN 负载均衡

问: 如果我们在多个接口上启用 SSL VPN，是否可以为所有的这些接口实施 VPN 负载平衡？

答: 只能定义一个接口作为公共接口加入 VPN 负载平衡组。这个想法是为了均衡 CPU 负载，多个接口会在相同 CPU 上融合，因此多个接口上的 VPN 负载均衡这个概念不会改善性能。

VPN 负载均衡集群的最大并行会话数

问: 请考虑有两台 Firepower 1150 的部署，每台设备均有一个 100 位用户的 SSL VPN 许可证。在 VPN 负载均衡组中，最大用户总数是允许 200 个并行会话还是仅允许 100 个并行会话？如果我们随后添加第三台设备，该设备有一个 100 位用户的许可证，我们此时能够支持 300 个并行会话吗？

答: 使用VPN负载均衡的情况下，所有设备均处于活动状态，因此您的组可以支持的最大会话数为组中每台设备的会话数量的总和，在这种情况下为 300。

VPN 负载均衡的许可

VPN 负载均衡有以下许可要求：

- 有效的 3DES/AES 许可证。

ASA 会在启用 VPN 负载均衡前检查是否存在此加密许可证。如果没有检测到有效的 3DES 或 AES 许可证，ASA 会阻止启用 VPN 负载均衡，也会阻止 VPN 负载均衡系统进行 3DES 的内部配置，除非许可证允许此使用。

- 防火墙上已激活此功能的有效增强型安全许可证。
- 您的智能账户必须有足够的增强型安全许可证才能符合要求。

VPN 负载均衡的前提条件

另请参阅VPN 负载均衡准则和限制，第 7 页。

- 默认情况下会禁用 VPN 负载均衡。您必须显式启用 VPN 负载均衡。
- 必须先配置公共（外部）接口和专用（内部）接口。本节中的后续引用使用名称 outside 和 inside。

  可以使用 **interface** 和 **nameif** 命令为这些接口配置不同的名称。
- 您必须事先配置虚拟 IP 地址所引用的接口。建立组通用的虚拟 IP 地址、UDP 端口（如需要）和 IPsec 共享密钥。
- 加入组的所有设备都必须共享同一个集群特定值：IP 地址、加密设置、加密密钥和端口。
- 要使用 VPN 负载均衡组加密，请先使用 **crypto ikev1 enable** 命令在内部接口上启用 IKEv1，同时指定内部接口；否则，在尝试配置 VPN 负载均衡组加密时，您将收到错误消息。
- 如果使用主用/主用状态故障转移或 VPN 负载均衡，则不支持本地 CA 功能。本地 CA 不能从属于另一 CA；它只能用作根 CA。

VPN 负载均衡准则和限制

符合条件的客户端

VPN 负载均衡仅在使用以下客户端发起的远程会话上有效：

- 安全客户端（3.0 版本及更高版本）
- ASA 5505（用作简易 VPN 客户端时）
- Firepower 1010（用作简易 VPN 客户端时）
- 支持 IKE 重定向的 IOS EZVPN 客户端设备 (IOS 831/871)

客户端注意事项

VPN 负载均衡可与 IPsec 客户端和 SSL VPN 客户端会话配合使用。包括 LAN 间连接在内的所有其他 VPN 连接类型（L2TP、PPTP、L2TP/IPsec）可以连接到在其上启用了 VPN 负载均衡的 ASA，但不能加入 VPN 负载均衡。

当多个 ASA 节点分组进行负载均衡并且 Secure Client连接需要使用组 URL 时，必须在各个 ASA 节点执行以下操作：

- 使用每个 VPN 负载均衡虚拟地址（IPv4 和 IPv6）的组 URL 配置每个远程访问连接配置文件。
- 为此节点的 VPN 负载均衡公共地址配置组 URL。

负载均衡组

- ASA 支持每个 VPN 负载均衡组包含 10 台设备。
- UCAPL 模式不支持 VPN 负载均衡，即使禁用加密也是如此。在 UCAPL 模式下，使用 IKEv2 建立安全隧道。

情景模式

多情景模式下不支持 VPN 负载均衡。

FIPS

FIPS 不支持集群加密。

证书验证

使用 Secure Client 为 VPN 负载均衡执行证书验证，并且该连接通过某个 IP 地址重定向时，该客户端通过此 IP 地址进行其所有的名称检查。请确保重定向 IP 地址已在证书公用名或主题备用名称中列出。如果 IP 地址没有出现在这些字段中，则该证书会被视为不可信。

遵循RFC 2818中定义的准则，如果证书中包含有**主题备用名称**，我们会仅将**主题备用名称**用于名称检查，并忽略公用名。请确保已在证书的**主题备用名称**中，定义提供证书的服务器的 IP 地址。

对于独立 ASA，IP 地址为该 ASA 的 IP。在 VPN 负载均衡组情况下，该地址取决于证书配置。如果该组使用一个证书，则该证书应该具有包含虚拟 IP 地址和组 FQDN 的 SAN 扩展，并应包含带每个 ASA 的 IP 和 FQDN 的使用者备用名称扩展。如果该组使用多个证书，则每个 ASA 的证书均应具有包含虚拟 IP、组 FQDN 和各 ASA 的 IP 地址和 FQDN 的 SAN 扩展。

地理 VPN 负载均衡

在定期更改 DNS 解析的 VPN 负载均衡环境中，必须谨慎考虑如何设置生存时间 (TTL) 值。要使 DNS 负载均衡配置与 Secure Client 成功配合使用，从选定 ASA 到隧道完全建立，ASA 的名称到地址映射都必须保持相同。如果在输入凭证前，经过的时间过长，查找将会重新启动，不同的 IP 地址可能会成为解析后的地址。如果在输入凭证前，DNS 映射变更至不同的 ASA，VPN 隧道会失效。

VPN 的地理负载均衡通常使用 Cisco Global Site Selector (GSS)。GSS 使用 DNS 进行负载均衡，并且 DNS 解析的生存时间 (TTL) 值默认为 20 秒。如果您提高 GSS 上的 TTL 值，则可以显著降低连接发送故障的可能性。当用户输入凭证并建立隧道时，增加为更高的值可以为身份验证阶段提供充足的时间。

要增加输入凭证的时间，您还可以考虑禁用 Connect on Start Up。

IKE/IPSec 安全关联

集群加密会话不会同步到 VPN 负载均衡器拓扑中的备用设备。

配置 VPN 负载均衡

如果您拥有一个远程客户端配置，在该配置中使用连接至相同网络的两个或更多ASA来处理远程会话，则可以将这些设备配置为共享其会话负载。此功能称为VPN负载均衡，它会将会话流量定向至负载最低的设备，从而在所有设备之间分配负载。VPN 负载均衡可以高效地利用系统资源，提供更高的性能和系统可用性。

要使用 VPN 负载均衡，请在组中的每台设备上执行以下操作：

- 建立通用的 VPN 负载均衡组属性以配置 VPN 负载均衡组。这包括组的虚拟 IP 地址、UDP 端口（如需要）和IPsec共享密钥。除组内的设备优先级外，组中的所有参与者都必须具有相同的组配置。
- 在设备上启用VPN负载均衡并定义设备特定属性（例如其公共和专有地址），从而配置加入的设备。这些值因设备而异。

为 VPN 负载均衡配置公共和专用接口

要为 VPN 负载均衡组设备配置公共（外部）和专用（内部）接口，请执行以下步骤。

过程

步骤 1 在 vpn-load-balancing 配置模式下输入带有 **lbpublic** 关键字的 **interface** 命令，在 ASA 上配置公共接口。该命令为此设备的 VPN 负载均衡功能指定公共接口的名称或 IP 地址：

示例：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

步骤 2 在 vpn-load-balancing 配置模式下输入带有 **lbprivate** 关键字的 **interface** 命令，在 ASA 上配置专用接口。该命令为此设备的 VPN 负载均衡功能指定专用接口的名称或 IP 地址：

示例：

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

步骤 3 设置要在组内分配给此设备的优先级。范围是从 1 到 10。该优先级指示，此设备在启动或现有导向器发生故障时，成为组导向器设备的可能性。设置的优先级越高（例如 10），此设备成为组导向器设备的可能性就越高。

示例：

例如，如要在组内为此设备分配值为 6 的优先级，请输入以下命令：

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

步骤 4 如果要对此设备应用网络地址转换，请输入 **nat** 命令和此设备的 NAT 分配地址。可以定义 IPv4 和 IPv6 地址，也可以指定此设备的主机名。

示例：

例如，如要为此设备分配 NAT 地址 192.168.30.3 和 2001:DB8::1，请输入以下命令：

```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

配置 VPN 负载均衡组属性

如要为组中的每台设备配置 VPN 负载均衡组属性，请执行以下步骤：

过程

步骤 1 在全局配置模式下输入 **vpn load-balancing** 命令，设置 VPN 负载均衡：

示例：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

此命令将进入 vpn-load-balancing 配置模式，可以在其中配置其余负载均衡属性。

步骤 2 配置此设备所属组的 IP 地址或完全限定域名。该命令指定代表整个 VPN 负载均衡组的单一 IP 地址或 FQDN。在公共子网地址范围内，选择由组中所有 ASA 共享的 IP 地址。必须指定 IPv4（强制）。您可以选择提供 IPv6 地址。

示例：

要配置虚拟 IPv4 和 IPv6 地址，请输入以下命令：

```
hostname(config-load-balancing)# cluster ip address 192.168.10.1 1000::2
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster ip address 192.168.10.1 1000::2
cluster encryption
```

要为 VPN 负载均衡集群配置 IPv6 地址，必须进行 IPv4 地址配置。如果仅配置虚拟 IPv6 地址，则会显示错误消息。

```
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster encryption
participate
hostname(config-load-balancing)# cluster ip address 1000::2
ERROR: Virtual IPv4 address is not set
```

步骤 3 配置组端口。该命令可为此设备要参与的 VPN 负载均衡组指定 UDP 端口。默认值为 9023。如果另一应用正使用此端口，输入您想要用于负载均衡的 UDP 目标端口号。

示例：

例如，如要将组端口设置为 4444，请输入以下命令：

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

步骤 4 （可选）为 VPN 负载均衡组启用 IPsec 加密。

默认设置为无加密。该命令可以启用或禁用 IPsec 加密。如果配置此复选属性，必须先指定和验证共享密钥。VPN 负载均衡组中的 ASA 通过使用 IPsec 的 LAN 间隧道进行通信。如要确保加密设备之间通信的所有负载均衡信息，请启用此属性。

注释
要使用 VPN 负载均衡组加密，请先使用 **crypto ikev1 enable** 命令在内部接口上启用 IKEv1，同时指定内部接口；否则，在尝试配置 VPN 负载均衡组加密时，您将收到错误消息。

如果在配置组加密时启用了 IKEv1，但在配置设备加入组之前已被禁用，则在输入 **participate** 命令时，您会收到一条错误消息，并且也不会为该组启用加密。

示例：

```
hostname(config)# crypto ikev1 enable inside
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

步骤 5 如果启用组加密，还必须输入 **cluster key** 命令指定 IPsec 共享密钥。在启用 IPsec 加密后，该命令指定 IPsec 对等体之间的共享密钥。您在框中输入的值会显示为连续的星号字符。如果需要输入已加密的密钥（例如，从其他配置中复制），请输入 **cluster key 8** *key* 命令。

示例：

例如，如要将共享密钥设置为 123456789，请输入以下命令：

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

步骤 6 输入 **participate** 命令，让此设备加入组：

示例：

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

下一步做什么

当多个 ASA 节点分组进行负载均衡并且 Secure Client连接需要使用组 URL 时，您必须在各个 ASA 节点执行以下操作：

- 使用每个负载均衡虚拟地址（IPv4 和 IPv6）的组 URL 配置每个远程访问连接配置文件。
- 为此节点的 VPN 负载均衡公共地址配置组 URL。

使用 **tunnel-group**、**general-attributes**、**group-url** 命令配置这些组 URL。

启用使用完全限定域名的重定向

默认情况下，ASA 只会将 VPN 负载均衡重定向中的 IP 地址发给客户端。如果使用的证书基于 DNS 名称，证书将在重定向至成员设备时变得无效。

作为 VPN 负载均衡导向器，该 ASA 在将 VPN 客户端连接重定向至一个成员设备（组中的另一 ASA）时，可以通过反向 DNS 查找发送此成员设备的完全限定域名 (FQDN)，而不是其外部 IP 地址。

要在 vpn load-balancing 模式下启用或禁用使用完全限定域名的重定向，请在全局配置模式下使用 **redirect-fqdn enable** 命令。默认情况下禁用此行为。

开始之前

组中的 VPN 负载均衡设备上的所有外部和内部网络接口，都必须位于相同 IP 网络之上。

过程

步骤 1 为 VPN 负载均衡启用 FQDN。

redirect-fqdn {**enable** | **disable**}

示例：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)#
```

步骤 2 将每个 ASA 外部接口的条目添加到 DNS 服务器中（如果其中尚无这些条目）。每个 ASA 外部 IP 地址都应该有一个与其关联的 DNS 条目用于查找。对于反向查找，也必须启用这些 DNS 条目。

步骤 3 使用 **dns domain-lookup inside** 命令或具有通向 DNS 服务器的路由的任一接口，在 ASA 上启用 DNS 查找。

步骤 4 在 ASA 上定义 DNS 服务器 IP 地址。例如：**dns name-server 10.2.3.4**（DNS 服务器的 IP 地址）。

VPN 负载均衡配置示例

基本 VPN 负载均衡 CLI 配置

以下 VPN 负载均衡命令序列示例包含一条启用完全限定域名重定向的接口命令，将组的公共接口指定为 **test**，将组的专用接口指定为 **foo**

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

查看 VPN 负载均衡信息

VPN 负载均衡组导向器从组中的每台 ASA 接收定期消息，其中包含活动 Secure Client 和无客户端会话的数量，以及基于配置限制或许可证限制的最大允许会话数。如果组中的 ASA 显示 100% 的容量已满，则组导向器无法向其重定向更多的连接。尽管 ASA 可能显示为容量已满，但有些用户可能处于非活动/等待继续状态，造成了许可证的浪费。作为应急方案，每台 ASA 都提供会话总数减去非活动状态会话数之后的数量，而不是会话总数量。请参阅 ASA 命令参考中的 **-sessiondb summary** 命令。也就是说，非活动会话不会报告至组导向器。即便 ASA 的容量已满（有部分非活动会话），组导向器仍会视需要向其重定向连接。ASA 收到新的连接时，处于非活动状态最长时间的会话会被注销，从而允许新的连接使用其许可证。

以下示例显示了 100 个 SSL 会话（仅活动会话）和 2% 的 SSL 负载。这些数值不包含非活动会话。也就是说，非活动会话不会计入 VPN 负载均衡的负载。

```
hostname# show vpn load-balancing
 Status :    enabled
 Role :    Master
 Failover :    Active
 Encryption :    enabled
 Cluster IP :    192.168.1.100
 Peers :    1

 Load %
Sessions
```

```
Public IP      Role    Pri Model     IPsec SSL IPsec SSL
192.168.1.9    Master 7   ASA-5540 4     2   216   100
192.168.1.19   Backup 9   ASA-5520 0     0   0     0
```

VPN 负载均衡的功能历史记录

功能名称	版本	功能信息
使用 SAML 的 VPN 负载均衡	9.17(1)	ASA 现在支持使用 SAML 身份验证的 VPN 负载
VPN 负载均衡	7.2(1)	引入了此功能。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。