

ASA 5500 上的远程 VPN 客户端负载均衡配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[符合条件的客户](#)

[使用的组件](#)

[网络图](#)

[规则](#)

[限制](#)

[配置](#)

[IP 地址分配](#)

[集群配置](#)

[监控](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

[简介](#)

负载均衡是一种功能，使用该功能可以在多个自适应安全设备 (ASA) 上共享 Cisco VPN 客户端而无需用户干涉。负载均衡可确保公用 IP 地址是对用户高度可用的。例如，如果为公用 IP 地址提供服务的 Cisco ASA 发生故障，集群中的另一个 ASA 将采用该公用 IP 地址。

[先决条件](#)

[要求](#)

尝试进行此配置之前，请确保满足以下要求：

- 您已在 ASA 上分配了 IP 地址并配置了默认网关。
- ASA 上已为 VPN 客户端用户配置了 IPsec。
- VPN 用户能够使用为所有 ASA 分别分配的公用 IP 地址连接到这些 ASA。

[符合条件的客户](#)

负载均衡仅对通过以下客户端启动的远程会话有效：

- Cisco VPN客户端 (版本3.0或更高版本)
- Cisco VPN 3002硬件客户端 (版本3.5或更高版本)
- 充当Easy VPN客户端时的CiscoASA 5505

所有其他客户端 (包括LAN到LAN连接) 都可以连接到启用了负载均衡的安全设备 , 但无法参与负载均衡。

使用的组件

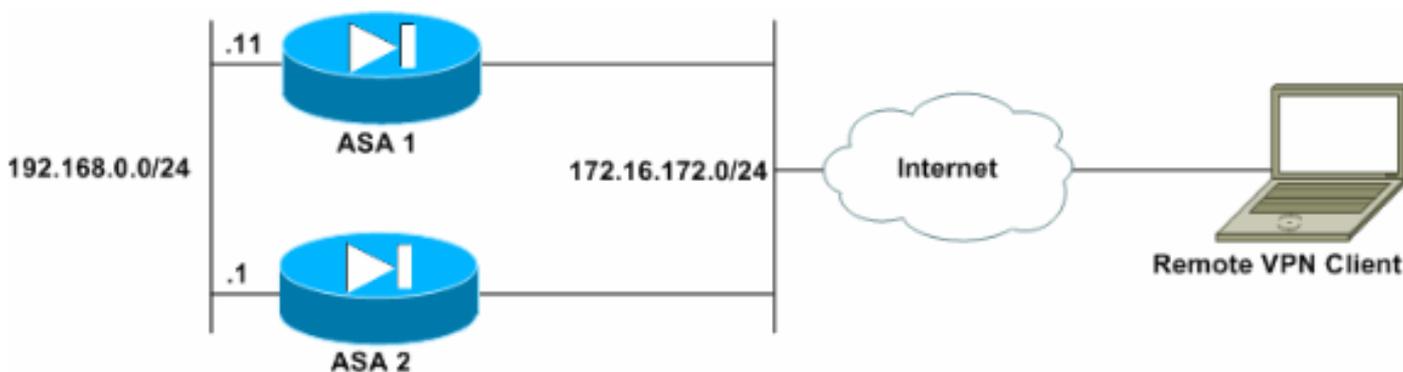
本文档中的信息基于以下软件和硬件版本 :

- VPN 客户端软件版本 4.6 及更高版本
- Cisco ASA 软件版本 7.0.1 及更高版本 **注意** : 将负载均衡支持扩展至具有8.0(2)版本的增强型安全许可证的5520以上的ASA 5510和ASA型号。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您使用的是真实网络 , 请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置 :



规则

有关文档约定的更多信息 , 请参考 [Cisco 技术提示约定](#)。

限制

- 虚拟集群中的每台设备上的VPN虚拟集群IP地址、用户数据报协议(UDP)端口和共享密钥必须相同。
- 虚拟集群中的所有设备必须在相同的外部 and 内部 IP 子网上。

配置

IP 地址分配

确保在外部和内部接口上配置 IP 地址 , 并且您能够从 ASA 到达 Internet。

注意 : 确保在内部和外部接口上都启用了ISAKMP。选择 **Configuration > Features > VPN > IKE >**

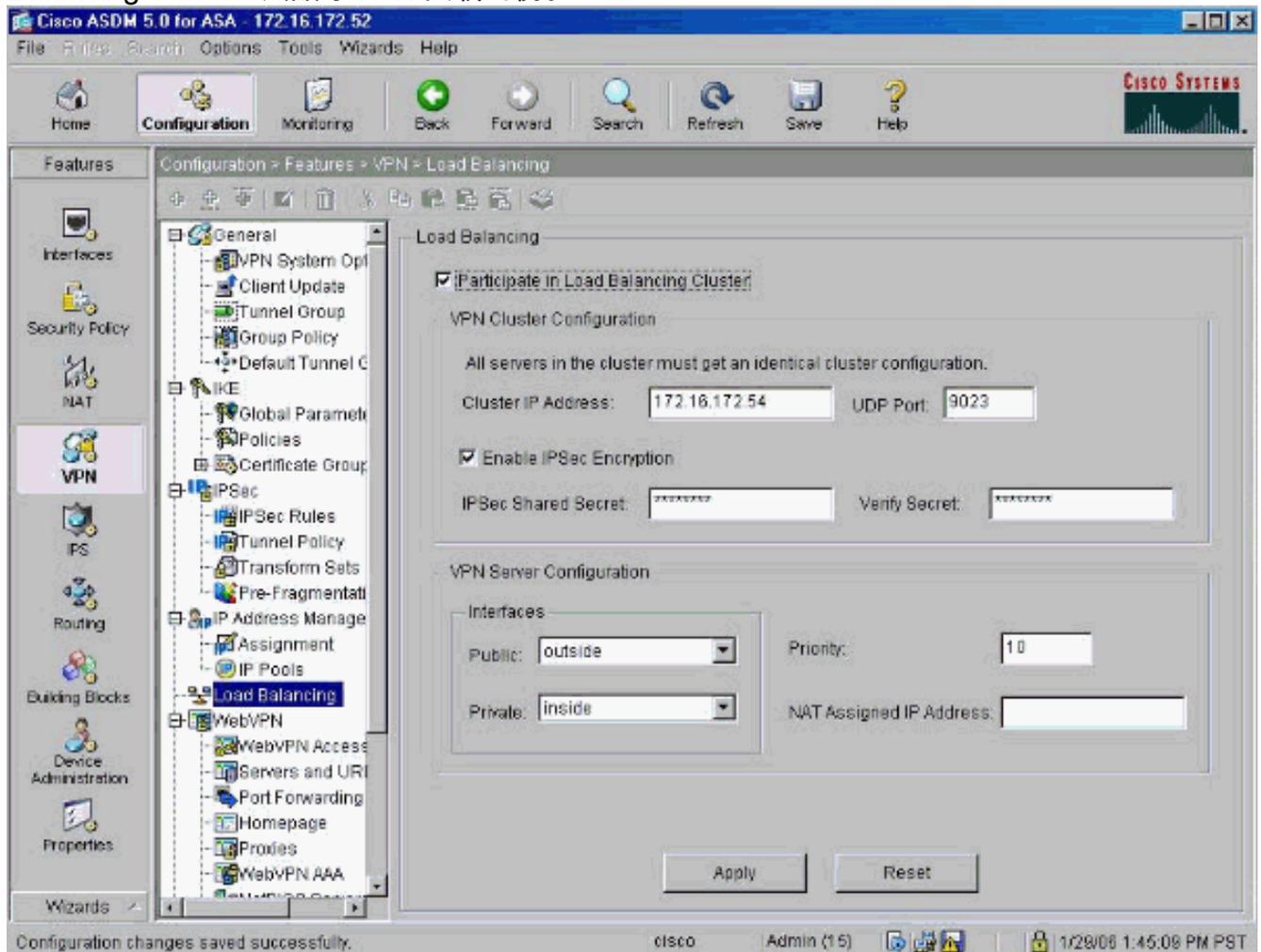
Global Parameters 以对此进行验证。

集群配置

此过程显示如何使用思科自适应安全设备管理器(ASDM)配置负载均衡。

注：本例中的许多参数都具有默认值。

1. 选择 **Configuration > Features > VPN > Load Balancing**，并选中 **Participate in Load Balancing Cluster** 以启用 VPN 负载均衡。



2. 完成这些步骤，以在 VPN Cluster Configuration 分组框中为参与集群的所有 ASA 配置参数：
在 Cluster IP Address 文本框中键入集群的 IP 地址。单击 **Enable IPsec Encryption**。在 IPsec Shared Secret 文本框中键入加密密钥，并在 Verify Secret 文本框中再次键入它。
3. 配置 VPN Server Configuration 分组框中的选项：
在 Public 列表中选择接受传入 VPN 连接的接口。在 Private 列表中选择作为专用接口的接口。（可选）在 Priority 文本框中更改 ASA 在集群中的优先级。如果此设备位于使用 NAT 的防火墙后面，请为网络地址转换(NAT)分配的 IP 地址键入 IP 地址。
4. 对组中所有参与的 ASA 重复以上步骤。

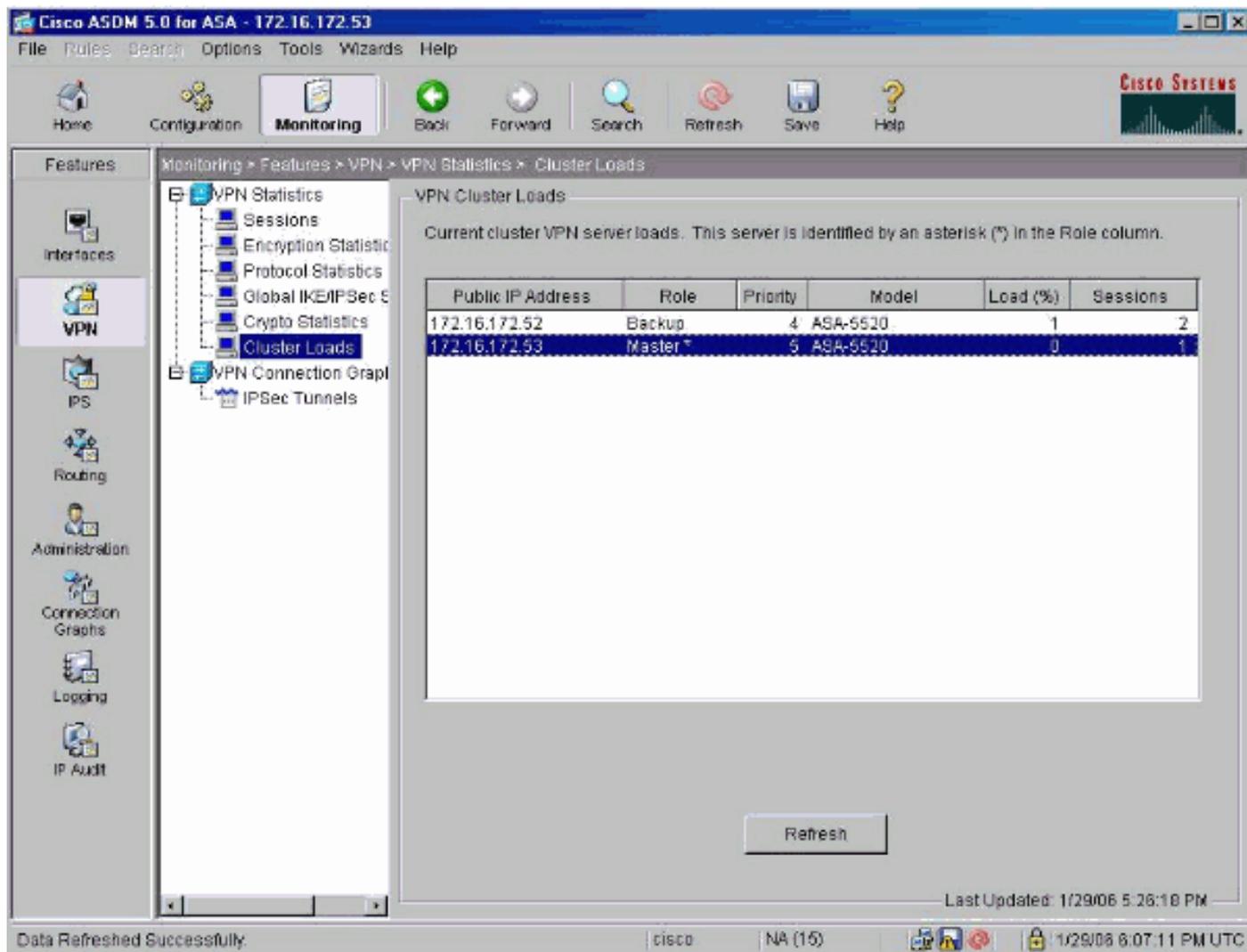
此部分中的示例使用这些 CLI 命令配置负载均衡：

```
VPN-ASA2 (config) #vpn load-balancing
VPN-ASA2 (config-load-balancing) #priority 10
VPN-ASA2 (config-load-balancing) #cluster key cisco123
VPN-ASA2 (config-load-balancing) #cluster ip address 172.16.172.54
```

VPN-ASA2 (config-load-balancing) #cluster encryption
VPN-ASA2 (config-load-balancing) #participate

监控

选择 **Monitoring > Features > VPN > VPN Statistics > Cluster Loads** 监控 ASA 上的负载均衡功能



The screenshot shows the Cisco ASDM 5.0 for ASA interface. The breadcrumb navigation is **Monitoring > Features > VPN > VPN Statistics > Cluster Loads**. The main content area displays the **VPN Cluster Loads** page, which includes a table of current cluster VPN server loads. The table has columns for Public IP Address, Role, Priority, Model, Load (%), and Sessions. The data shows two servers: one at 172.16.172.52 (Backup, Priority 4, Model ASA-5520, Load 1%, Sessions 2) and one at 172.16.172.53 (Master, Priority 5, Model ASA-5520, Load 0%, Sessions 1). A 'Refresh' button is located at the bottom of the table. The status bar at the bottom indicates 'Data Refreshed Successfully' and the time is 1/29/08 6:07:11 PM UTC.

Public IP Address	Role	Priority	Model	Load (%)	Sessions
172.16.172.52	Backup	4	ASA-5520	1	2
172.16.172.53	Master *	5	ASA-5520	0	1

验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

- **show vpn load-balancing - 验证 VPN 负载均衡功能。**

```
Status: enabled  
Role: Backup  
Failover: n/a  
Encryption: enabled  
Cluster IP: 172.16.172.54  
Peers: 1
```

```
Public IP Role Pri Model Load (%) Sessions
```

* 172.16.172.53 Backup 5 ASA-5520 0 1
172.16.172.52 Master 4 ASA-5520 n/a n/a

[故障排除](#)

使用本部分可排除配置故障。

[故障排除命令](#)

[命令输出解释程序 \(仅限注册用户 \) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

注意： [在使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。](#)

- [debug vpnlb 250 - 用于排除 VPN 负载均衡功能的故障。](#)

```
VPN-ASA2#  
VPN-ASA2# 5718045: Created peer[172.16.172.54]  
5718012: Sent HELLO request to [172.16.172.54]  
5718016: Received HELLO response from [172.16.172.54]  
7718046: Create group policy [vpnlb-grp-pol]  
7718049: Created secure tunnel to peer[192.168.0.11]  
5718073: Becoming slave of Load Balancing in context 0.  
5718018: Send KEEPALIVE request failure to [192.168.0.11]  
5718018: Send KEEPALIVE request failure to [192.168.0.11]  
5718018: Send KEEPALIVE request failure to [192.168.0.11]  
7718019: Sent KEEPALIVE request to [192.168.0.11]  
7718023: Received KEEPALIVE response from [192.168.0.11]  
7718035: Received TOPOLOGY indicator from [192.168.0.11]  
7718019: Sent KEEPALIVE request to [192.168.0.11]  
7718023: Received KEEPALIVE response from [192.168.0.11]  
7718019: Sent KEEPALIVE request to [192.168.0.11]  
7718023: Received KEEPALIVE response from [192.168.0.11]  
7718019: Sent KEEPALIVE request to [192.168.0.11]  
7718023: Received KEEPALIVE response from [192.168.0.11]  
7718019: Sent KEEPALIVE request to [192.168.0.11]  
7718023: Received KEEPALIVE response from [192.168.0.11]  
7718019: Sent KEEPALIVE request to [192.168.0.11]  
7718023: Received KEEPALIVE response from [192.168.0.11]  
7718019: Sent KEEPALIVE request to [192.168.0.11]
```

[相关信息](#)

- [Cisco ASA 5500 系列自适应安全设备](#)
- [Cisco PIX 防火墙软件](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [安全产品 Field Notices \(包括 PIX \)](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)