

# ASA 5500上的遠端VPN客戶端負載平衡配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[符合條件的客戶端](#)

[採用元件](#)

[網路圖表](#)

[慣例](#)

[限制](#)

[組態](#)

[IP地址分配](#)

[群集配置](#)

[監控](#)

[驗證](#)

[疑難排解](#)

[疑難排解指令](#)

[相關資訊](#)

## 簡介

負載均衡是指能夠在多個自適應安全裝置(ASA)裝置上共用Cisco VPN客戶端，而無需使用者干預。負載均衡確保公共IP地址對使用者具有高可用性。例如，如果為公共IP地址提供服務的思科ASA出現故障，則群集中的其他ASA將採用公共IP地址。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- 您已在ASA上分配IP地址並配置預設網關。
- 在ASA上為VPN客戶端使用者配置IPsec。
- VPN使用者可以使用其單獨分配的公共IP地址連線到所有ASA。

### 符合條件的客戶端

負載均衡僅對使用以下客戶端啟動的遠端會話有效：

- Cisco VPN客戶端 ( 3.0版或更高版本 )

- Cisco VPN 3002硬體客戶端 ( 3.5版或更高版本 )
- 作為Easy VPN客戶端時的CiscoASA 5505

所有其他客戶端 ( 包括LAN到LAN連線 ) 可以連線到啟用了負載平衡的安全裝置，但它們不能參與負載平衡。

## 採用元件

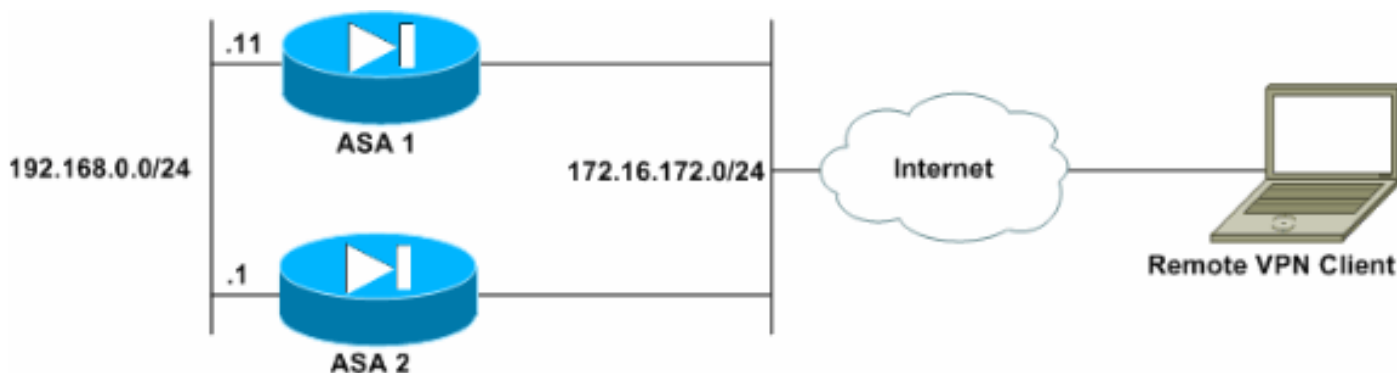
本文中的資訊係根據以下軟體和硬體版本：

- VPN客戶端軟體版本4.6及更高版本
- Cisco ASA軟體版本7.0.1及更高版本**註：將負載平衡支援擴展到具有8.0(2)版的Security Plus許可證的ASA 5510和高於5520的ASA型號。**

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 網路圖表

本檔案會使用以下網路設定：



## 慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

## 限制

- VPN虛擬集群IP地址、使用者資料包協定(UDP)埠和共用金鑰在虛擬集群中的每個裝置上都必須相同。
- 虛擬集群中的所有裝置必須位於同一個外部和內部IP子網上。

## 組態

### IP地址分配

確保在外部和內部介面上配置了IP地址，並且您可以從ASA訪問Internet。

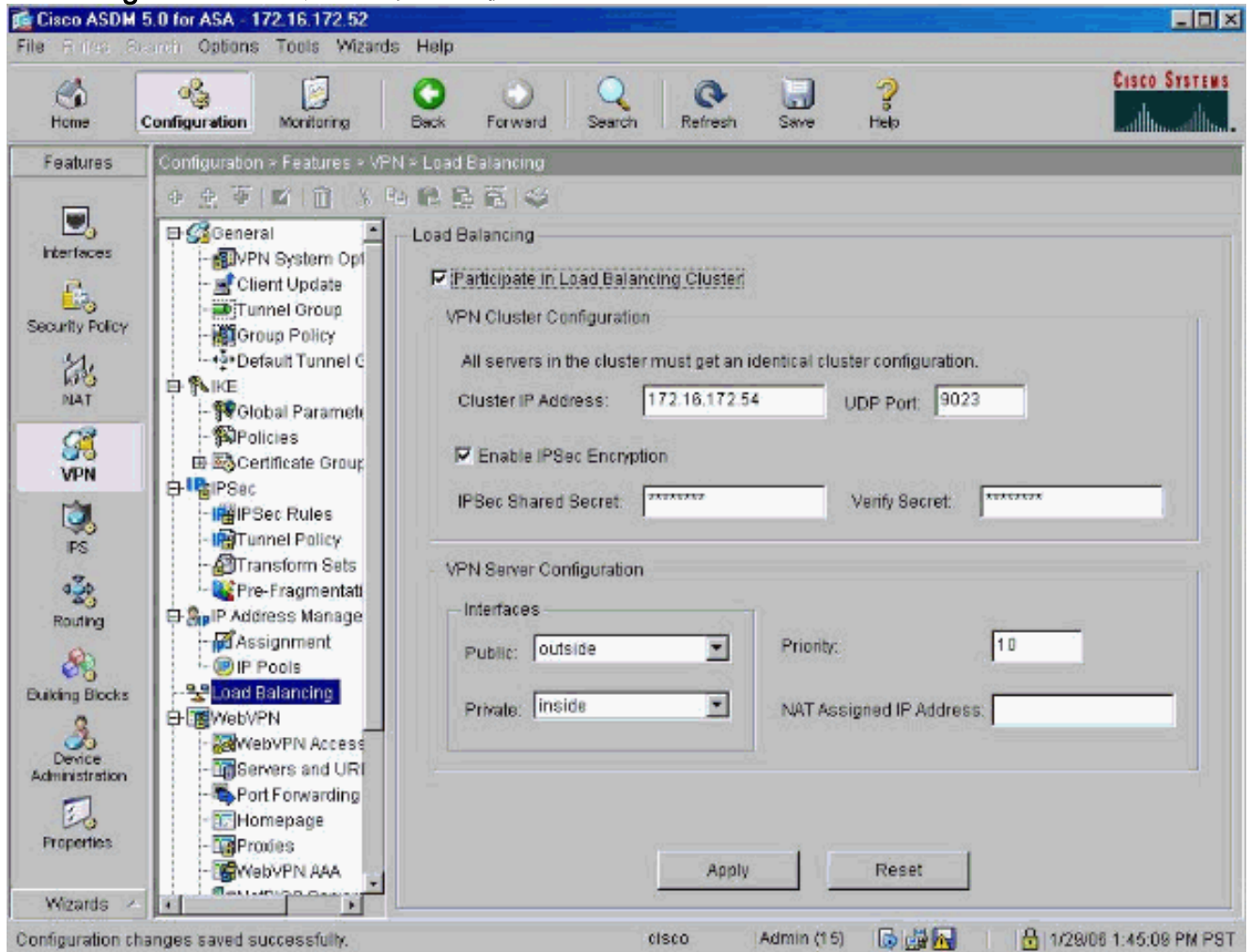
**注意：**確保在內部和外部介面上均啟用ISAKMP。選擇**Configuration > Features > VPN > IKE > Global Parameters**以驗證這一點。

## 群集配置

此過程顯示如何使用思科自適應安全裝置管理器(ASDM)配置負載均衡。

**注意：**此示例中的許多引數都有預設值。

1. 選擇 **Configuration > Features > VPN > Load Balancing**，然後選中 **Participate in Load Balancing Cluster** 以啟用VPN負載平衡。



2. 完成以下步驟，在VPN Cluster Configuration組框中為參與集群的所有ASA配置引數：在Cluster IP Address文本框中鍵入群集的IP地址。按一下**Enable IPsec Encryption**。在「IPsec共用金鑰」文本框中鍵入加密金鑰，然後在「驗證金鑰」文本框中再次鍵入該金鑰。
3. 配置VPN伺服器配置組框中的選項：在Public清單中選擇接受傳入VPN連線的介面。在專用清單中選擇專用介面。(可選)在「優先順序」文本框中更改ASA在集群中的優先順序。如果此裝置位於使用NAT的防火牆後面，請鍵入網路地址轉換(NAT)分配的IP地址的IP地址。
4. 對組中的所有參與ASA重複這些步驟。

本節中的示例使用以下CLI命令配置負載均衡：

```
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
```

## 監控

選擇Monitoring > Features > VPN > VPN Statistics > Cluster Loads以監控ASA上的負載平衡功能。

VPN Cluster Loads

Current cluster VPN server loads. This server is identified by an asterisk (\*) in the Role column.

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

Refresh

Last Updated: 1/29/06 5:26:18 PM

Data Refreshed Successfully

## 驗證

使用本節內容，確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- **show vpn load-balancing** — 驗證VPN負載平衡功能。

```
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
```

## [疑難排解](#)

使用本節內容，對組態進行疑難排解。

### [疑難排解指令](#)

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

**附註：**使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- **debug vpnlb 250** -用於對VPN負載平衡功能進行故障排除。

```
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]
```

## [相關資訊](#)

- [Cisco ASA 5500系列調適型安全裝置](#)
- [Cisco PIX防火牆軟體](#)
- [Cisco Secure PIX防火牆命令參考](#)
- [安全產品現場通知 \(包括PIX\)](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)