# Exemplo de configuração do Remote VPN Client Load Balancing on ASA 5500

## Contents


Introduction
Prerequisites
Requirements
Clientes qualificados
Componentes Utilizados
Diagrama de Rede
Conventions
Restrições
Configuração
Atribuição de endereço IP:
Configuração de cluster
Monitoramento
Verificar
Troubleshoot
Comandos para Troubleshooting
Informações Relacionadas


## Introduction

O balanceamento de carga é a capacidade de ter Cisco VPN Clients compartilhados entre várias unidades de Adaptive Security Appliance (ASA) sem a intervenção do usuário. A função de balanceamento de carga garante que o endereço IP público esteja altamente disponível aos usuários. Por exemplo, se o Cisco ASA que mantém o endereço IP público falha, um outro ASA no cluster assume o endereço IP público.

## Prerequisites

### Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Você atribuiu endereços IP em seus ASAs e configurou o gateway padrão.
- O IPsec é configurado nos ASAs para os usuários do VPN Client.
- Os usuários de VPN podem se conectar a todos os ASAs usando seu endereço IP público atribuído individualmente.

## Clientes qualificados

O balanceamento de carga só é eficaz em sessões remotas iniciadas com estes clientes:

- Cisco VPN Client (versão 3.0 ou posterior)
- Cisco VPN 3002 Hardware Client (versão 3.5 ou posterior)
- Cisco ASA 5505 quando atua como um cliente Easy VPN

Todos os outros clientes, incluindo conexões LAN a LAN, podem se conectar a um dispositivo de segurança no qual o balanceamento de carga está ativado, mas não podem participar do balanceamento de carga.

## Componentes Utilizados

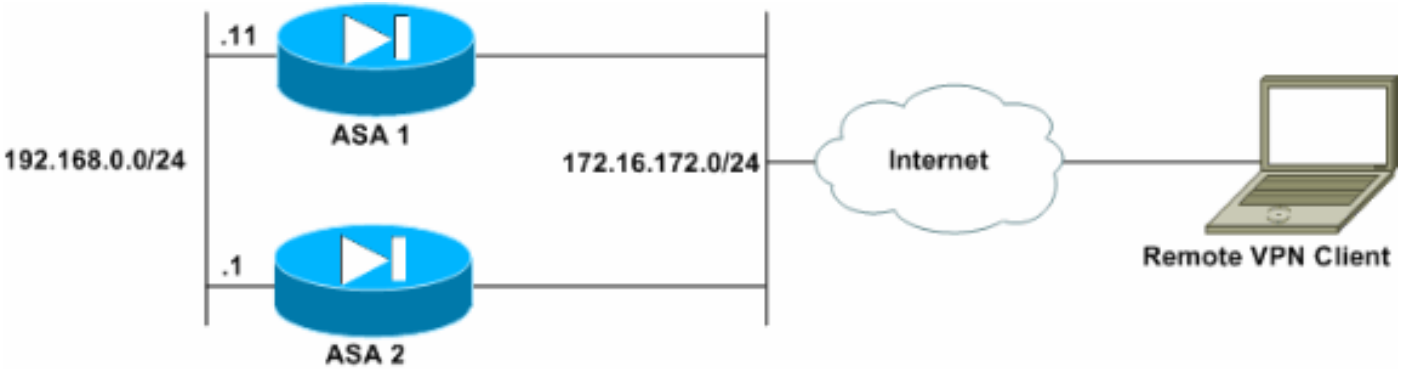
As informações neste documento são baseadas nestas versões de software e hardware:

- Software VPN Client versões 4.6 e posteriores
- Software Cisco ASA versões 7.0.1 e posteriores**Observação:** estende o suporte ao balanceamento de carga para modelos ASA 5510 e ASA posteriores a 5520 que têm uma licença Security Plus com a versão 8.0(2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




## Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Restrições

- O endereço IP do cluster virtual de VPN, a porta do User Datagram Protocol (UDP) e o segredo compartilhado devem ser idênticos em todos os dispositivos no cluster virtual.
- Todos os dispositivos no cluster virtual devem estar nas mesmas sub-redes IP internas e externas.

# Configuração

## Atribuição de endereço IP:

Certifique-se de que os endereços IP estejam configurados nas interfaces externa e interna e de que você possa acessar a Internet a partir do seu ASA.

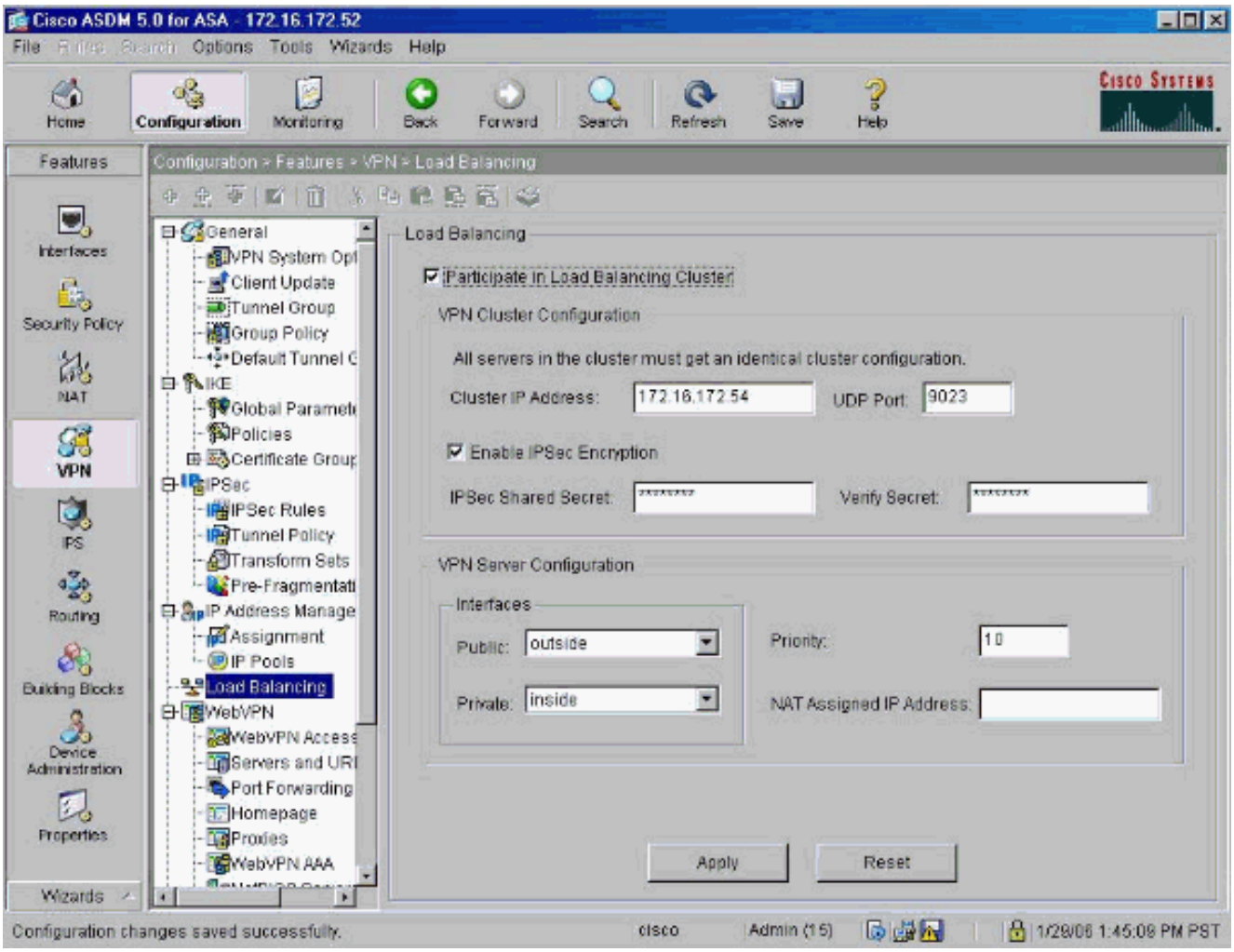
**Observação:** certifique-se de que o ISAKMP esteja habilitado na interface interna e externa. Selecione **Configuration > Features > VPN > IKE > Global Parameters** para verificar isso.

## Configuração de cluster

Este procedimento mostra como usar o Cisco Adaptive Security Device Manager (ASDM) para configurar o balanceamento de carga.

**Observação:** muitos dos parâmetros neste exemplo têm valores padrão.

1. Selecione **Configuration > Features > VPN > Load Balancing** e marque **Participate in Load Balancing Cluster** para ativar o balanceamento de carga da VPN.




2. Conclua estes passos para configurar os parâmetros para todos os ASAs que participam do cluster na caixa do grupo Configuração do cluster VPN:Digite o endereço IP do cluster na caixa de texto Endereço IP do cluster.Clique em **Ativar criptografia IPSec**.Digite a chave de criptografia na caixa de texto IPSec Shared Secret e digite-a novamente na caixa de texto

Verificar segredo.

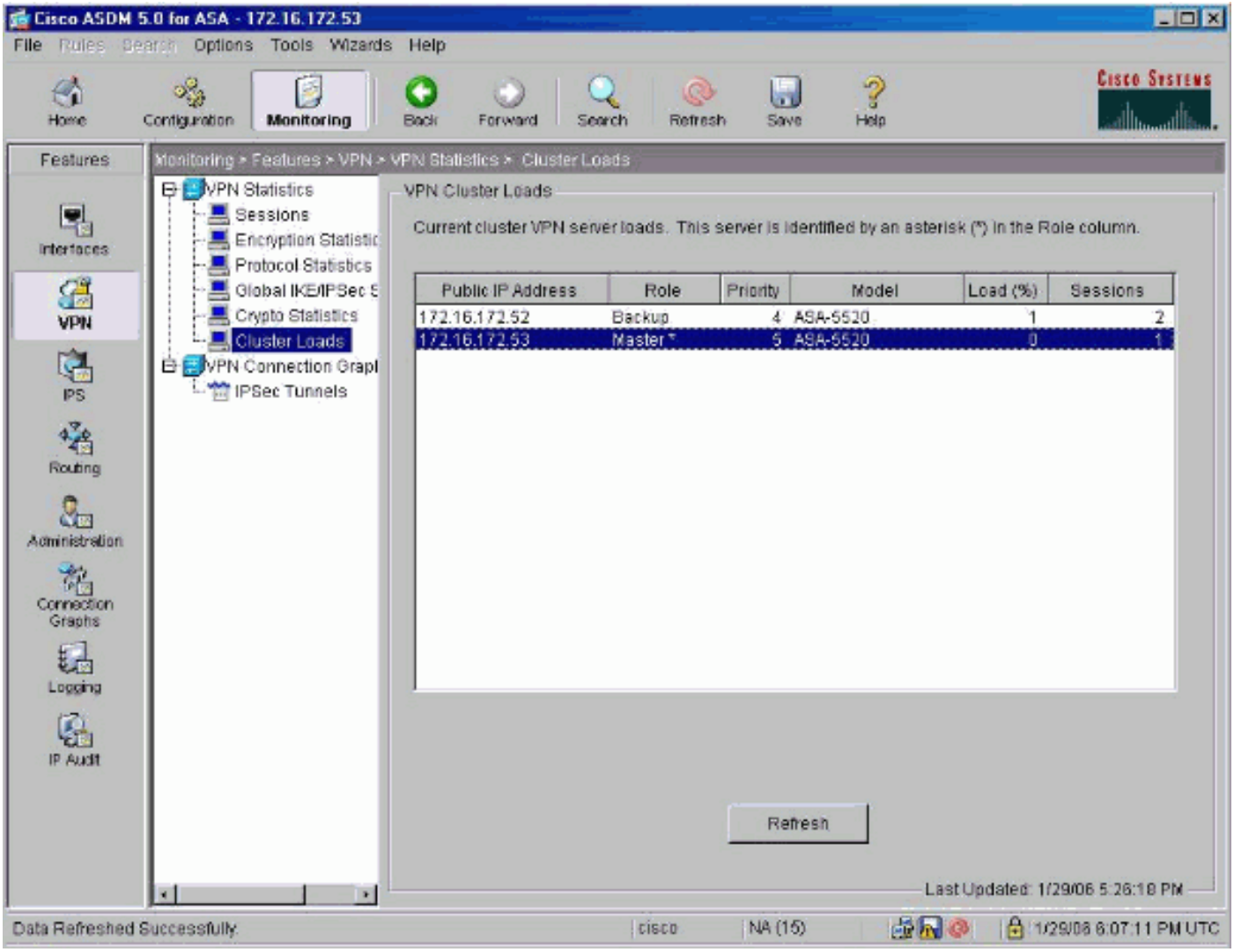
3. Configure as opções na caixa do grupo Configuração do Servidor VPN:Selecione uma interface que aceite as conexões VPN de entrada na lista Pública.Selecione uma interface que seja a interface privada na lista Privada.(*Opcional*) Altere a prioridade que o ASA tem no cluster na caixa de texto Prioridade.Digite um endereço IP para o endereço IP atribuído da Tradução de Endereço de Rede (NAT - Network Address Translation) se este dispositivo estiver por trás de um firewall que use NAT.
4. Repita as etapas em todos os ASAs participantes do grupo.

O exemplo nesta seção usa estes comandos CLI para configurar o balanceamento de carga:

```
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
```

## Monitoramento

Selecione **Monitoring > Features > VPN > VPN Statistics > Cluster Loads** para monitorar o recurso de balanceamento de carga no ASA.



# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool ( somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show vpn load-balance** —Verifica o recurso de balanceamento de carga da VPN.

```
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
```

# Troubleshoot

Use esta seção para resolver problemas de configuração.

## Comandos para Troubleshooting

A Output Interpreter Tool ( somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

**Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.**

- **debug vpnlb 250** —Usado para solucionar problemas com o recurso de balanceamento de carga da VPN.

```
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]
```

# Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems