

# لائحة مآل ع ءل VPN لآل مع ل مع ءن زآوم ASA 5500 نآوكآ

## المآآوبآ

- [المقءمة](#)
- [المتطلبآآ الآسآسة](#)
- [المتطلبآآ](#)
- [العملاء المؤهلون](#)
- [المكونات المسآءمة](#)
- [الرسم الآآططآل للشبكة](#)
- [الاصآلاحآ](#)
- [القآوب](#)
- [آآكون](#)
- [آعآن عنآون IP](#)
- [آكون نظام المجموعة](#)
- [مراقبة](#)
- [آآقق من الصآة](#)
- [اسآكشاف الأآطاء واصآلاحها](#)
- [أوامر اسآكشاف الأآطاء واصآلاحها](#)
- [معلومات ذات صلة](#)

## المقءمة

مآازنة الأآمال هآ القءرة على مآآركة عملاء Cisco VPN عبر وآدآآ متعددة لأآهزة الأمان المعدلة (ASA) ءون آءآل المسآءم. آضمن مآازنة الأآمال أن عنآون IP العام مآوفر بءرآة كبآرة للمسآءمآن. على سآل المآال، إءآ فآل Cisco ASA الآآل آقءم آءمآآ عنآون IP العام، فسآفآرض ASA آآر فآ المجموعة عنآون IP العام.

## المتطلبآآ الآسآسة

### المتطلبآآ

آآء من اسآفاء المتطلبآآ الآآلآة قبل أن آآاول إآراء هءآ الآكون:

- لآء قمآ بآعآن عنآون IP على وآدآآ ASA الآصآة بك وآشآلآ البوآة الافتراضآة.
- تم آكون IPsec على ASAs لمسآءمآل عمآل VPN.
- آمكن لمسآءمآل شبكة VPN الآآصال بآمع ASAs بآسآءمآل عنآون IP العام الآآل تم آعآنآه بشآل فرءل.

### العملاء المؤهلون

آكون مآازنة الأآمال فعآلا فقط على آلسآآ العمل البعآة الآآل تم بءؤها مع هؤلاء العملاء:

- عميل شبكة VPN من Cisco (الإصدار 3.0 أو إصدار أحدث)
  - عميل جهاز VPN 3002 من Cisco (الإصدار 3.5 أو إصدار أحدث)
  - Cisco ASA 5505 عند العمل كعميل VPN سهل
- يمكن لجميع العملاء الآخرين، بما في ذلك الاتصالات من شبكة LAN إلى شبكة LAN، الاتصال بجهاز أمان يتم فيه تمكين موازنة الأحمال، ولكن لا يمكنهم المشاركة في موازنة الأحمال.

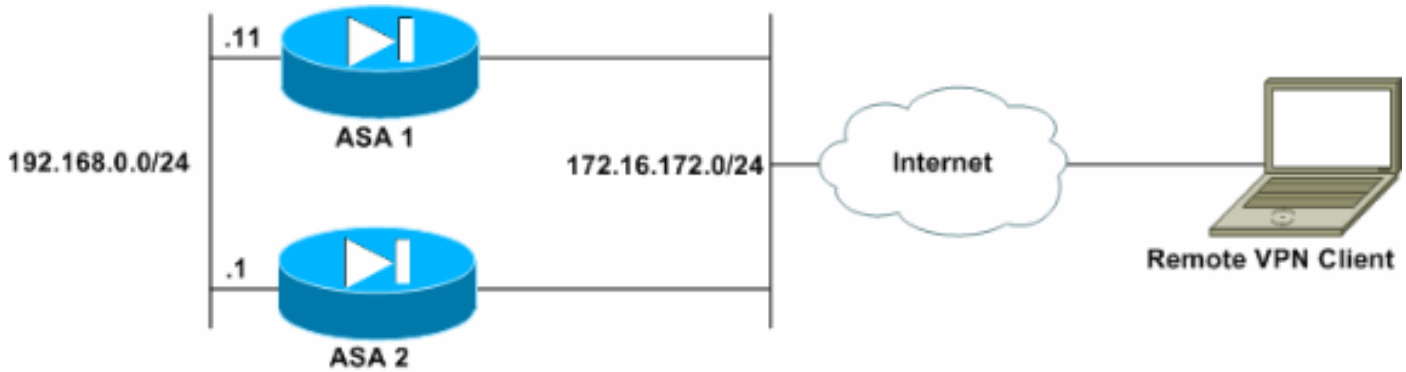
## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج عميل شبكة VPN الإصدارات 4.6 والإصدارات الأحدث
- برنامج ASA الإصدارات 7.0.1 والإصدارات الأحدث من Cisco **ملاحظة:** يعمل على توسيع دعم موازنة الأحمال لطرز ASA 5510 و ASA بعد عام 5520 التي تحتوي على ترخيص Security Plus مع الإصدار 8.0(2).
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



## الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## القيود

- يجب أن يكون عنوان IP لنظام المجموعة الظاهري الخاص بشبكة VPN ومنفذ بروتوكول مخطط بيانات المستخدم (UDP) والسر المشترك متطابقين على كل جهاز في نظام المجموعة الظاهرية.
- يجب أن تكون جميع الأجهزة الموجودة في نظام المجموعة الظاهرية على نفس شبكات IP الفرعية الخارجية والداخلية.

## التكوين

### تعيين عنوان IP

تأكد من تكوين عناوين IP على الواجهات الخارجية والداخلية ويمكنك الوصول إلى الإنترنت من ASA الخاص بك.

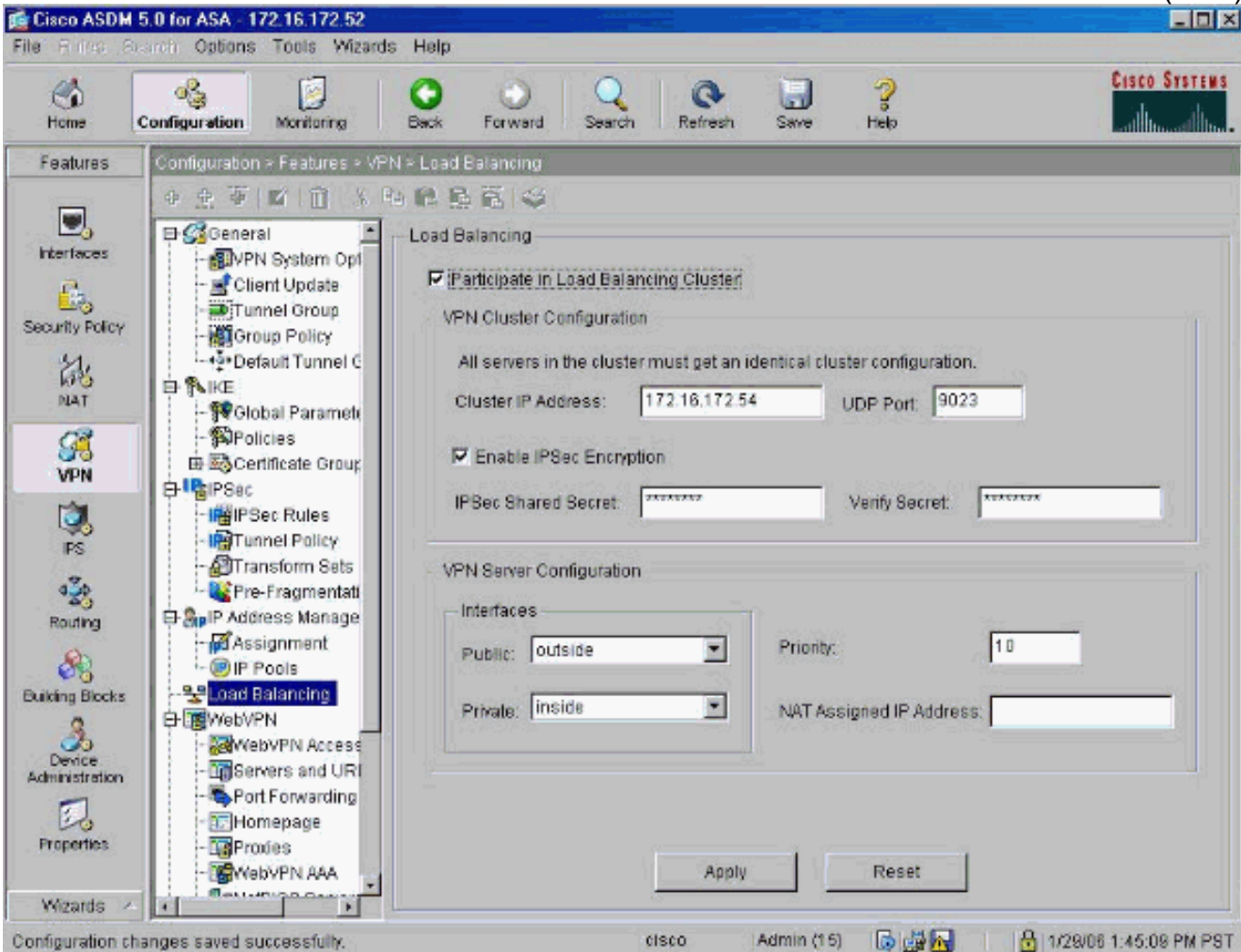
ملاحظة: تأكد من تمكين ISAKMP على كل من الواجهة الداخلية والخارجية. حدد تكوين < ميزات > IKE < VPN > معلمات عمومية للتحقق من ذلك.

## تكوين نظام المجموعة

يوضح هذا الإجراء كيفية استخدام مدير أجهزة الأمان المعدلة (ASDM) من Cisco لتكوين موازنة الأحمال.

ملاحظة: تحتوي العديد من المعلمات في هذا المثال على قيم افتراضية.

1. حدد Configuration (التكوين) < Feature (ميزات) < VPN (الشبكة الخاصة الظاهرية) < Load Balancing (موازنة الأحمال)، ثم تحقق من المشاركة في مجموعة موازنة الأحمال لتمكين موازنة أحمال الشبكة الخاصة الظاهرية (VPN).



2. أكمل هذه الخطوات لتكوين المعلمات لجميع ASAs المشاركة في نظام المجموعة في مربع مجموعة تكوين نظام مجموعة شبكات VPN: اكتب عنوان IP الخاص بنظام المجموعة في مربع نص عنوان IP لنظام المجموعة. انقر فوق تمكين تشفير IPsec. اكتب مفتاح التشفير في مربع النص "سر IPsec المشترك" ثم اكتبه مرة أخرى في مربع النص "التحقق من سر".

3. شكلت الخيار في ال VPN نادل تشكيل صندوق مجموعة: حدد واجهة تقبل إتصالات VPN الواردة في القائمة العامة. حدد واجهة تكون الواجهة الخاصة في القائمة الخاصة. (إختياري) قم بتغيير الأولوية التي يتمتع بها ASA في المجموعة في مربع نص الأولوية. اكتب عنوان IP لعنوان IP المعين لترجمة عنوان الشبكة (NAT) إذا كان هذا الجهاز خلف جدار حماية يستخدم NAT.

4. كرر الخطوات على كافة وحدات ASA المشاركة في المجموعة.

يستعمل المثالي هذا قسم هذا CLI أمر أن يشكل تحميل موازنة:

```

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

```

## مراقبة

حدد مراقبة < ميزات < VPN < إحصائيات VPN < حمولات المجموعة لمراقبة ميزة موازنة الأحمال على ASA.

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
172.16.172.93	Master *	5	ASA-5520	0	1

Refresh

Last Updated: 1/29/06 5:28:18 PM

Data Refreshed Successfully

## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم **أداة مترجم الإخراج (للعلماء المسجلين فقط)** بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر **show**.

• **show vpn** موازنة حمل الشبكة الخاصة الظاهرية (VPN)—للتحقق من ميزة موازنة حمل الشبكة الخاصة الظاهرية (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

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

## استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

### أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرَج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل استخدام أوامر **debug**.

• **debug vpnlb 250** — يستخدم لاستكشاف أخطاء ميزة موازنة حمل VPN وإصلاحها.

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

## معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاخلا مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحا وه  
ىلإ أمئاد عوچرلاب يصوت و تامچرتل هذه ةقदन ةتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزىلچنلإ دن تسمل