

Catalyst لوجم ني ب LAN ىلإ IPsec LAN ق فن لاثم و VPN ةم دخل ةي طم ن ل ة د ح و ل ا عم 6500 Cisco IOS هجوم ني وكت

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[معلومات أساسية](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[تكوين IPsec باستخدام منفذ وصول أو خط اتصال من الطبقة 2](#)

[تكوين IPsec باستخدام منفذ موجه](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[أوامر استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

[المقدمة](#)

يصف هذا المستند كيفية إنشاء نفق IPsec LAN إلى LAN بين محول من السلسلة Cisco Catalyst 6500 Series مع الوحدة النمطية لخدمة تسريع VPN وموجه Cisco IOS®.

[المتطلبات الأساسية](#)

[المتطلبات](#)

لا توجد متطلبات خاصة لهذا المستند.

[المكونات المستخدمة](#)

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

- برنامج IOS الإصدار SY2(14)12.2 من Cisco ل Catalyst 6000 Supervisor Engine، مع الوحدة النمطية لخدمة VPN ل IPsec
 - الموجه Cisco 3640 الذي يشغل برنامج Cisco IOS الإصدار T(4)12.3
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين مسموح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميح Cisco التقنية](#).

معلومات أساسية

تحتوي الوحدة النمطية لخدمة Catalyst 6500 VPN Service module على منفذي (Gigabit Ethernet (GE بدون موصلات ظاهرة خارجيا. هذه المنافذ قابلة للتوجيه لأغراض التكوين فقط. المنفذ 1 هو دائما المنفذ الداخلي. يعالج هذا المنفذ حركة مرور البيانات من الشبكة الداخلية وإليها. يعالج الميناء الثاني (ميناء 2) كل حركة مرور من وإلى ال WAN أو الشبكات الخارجية. يتم تكوين هذين المنفذين دائما في وضع التوصيل 802.1Q. تستخدم الوحدة النمطية لخدمة VPN تقنية تسمى التضاريس في السلك (BITW) لتدفق الحزمة.

تم معالجة الحزم بواسطة زوج من شبكات VLAN، وطبقة واحدة من الطبقة 3 داخل شبكة VLAN وطبقة واحدة من الطبقة 2 خارج شبكة VLAN. يتم توجيه الحزم، من الداخل إلى الخارج، من خلال طريقة تسمى منطق التعرف على العنوان المشفر (EARL) إلى شبكة VLAN الداخلية. بعد تشفير الحزم، تستخدم الوحدة النمطية لخدمة VPN الشبكة المحلية الظاهرية (VLAN) المقابلة خارج VLAN. في عملية فك التشفير، يتم ربط الحزم من الخارج إلى الداخل إلى الوحدة النمطية لخدمة VPN باستخدام شبكة VLAN الخارجية. بعد أن تقوم الوحدة النمطية لخدمة VPN بفك تشفير الحزمة وتخطيط شبكة VLAN إلى الشبكة المحلية الظاهرية (VLAN) المقابلة داخل، يقوم إيثرل بتوجيه الحزمة إلى منفذ LAN المناسب. يتم ربط الطبقة 3 داخل شبكة VLAN والطبقة 2 خارج شبكات VLAN معا بإصدار الأمر `crypto connect vlan`. هناك ثلاثة نوع الميناء في المادة حفازة sery 6500 مفتاح:

- **المنافذ الموجهة** - بشكل افتراضي، يتم توجيه جميع منافذ الإيثرنت. تحتوي هذه المنافذ على شبكة VLAN مخفية مرتبطة بها.
- **منافذ الوصول** — تحتوي هذه المنافذ على شبكة محلية ظاهرية (VLAN) خارجية أو بروتوكول خط اتصال شبكات (VLAN (VTP مرتبطة بها. أنت تستطيع صحبت أكثر من واحد ميناء إلى VLAN يعين.
- **منافذ خطوط الاتصال** — تحمل هذه المنافذ العديد من شبكات VLAN الخارجية أو VTP، والتي يتم على أساسها تضمين جميع الحزم باستخدام رأس 802.1Q.

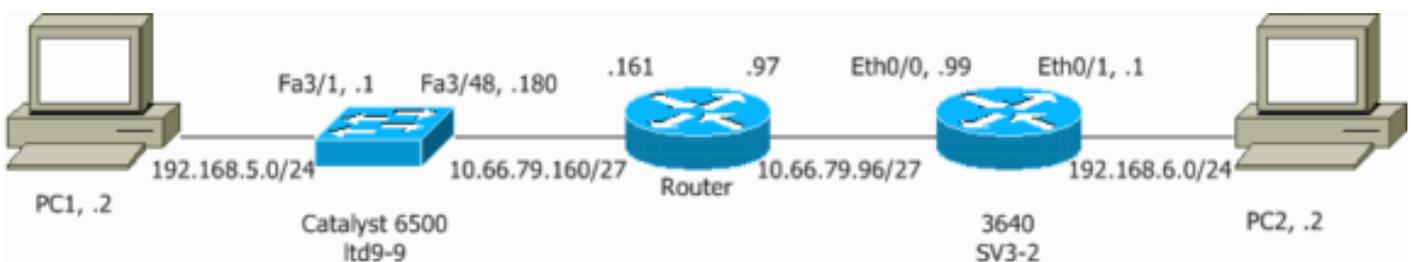
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي:



تكوين IPsec باستخدام منفذ وصول أو خط اتصال من الطبقة 2

قم بإجراء هذه الخطوات لتكوين IPsec باستخدام التعليمات الخاصة بمنفذ خط الاتصال أو الوصول للطبقة 2 للواجهة المادية الخارجية.

1. أضفت ال VLANs داخلي إلى الميناء داخلي من ال VPN خدمة وحدة نمطية. افترضت أن ال VPN خدمة وحدة نمطية على شق مكان 4. أستخدم شبكة VLAN 100 كشبكة VLAN الداخلية وشبكة VLAN 209 كشبكة VLAN الخارجية. شكلت ال VPN خدمة وحدة نمطية GE ميناء مثل هذا:

```
interface GigabitEthernet4/1
    no ip address
    flowcontrol receive on
    flowcontrol send off
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 1,100,1002-1005
    switchport mode trunk
    cdp enable
```

```
interface GigabitEthernet4/2
    no ip address
    flowcontrol receive on
    flowcontrol send off
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 1,209,1002-1005
    switchport mode trunk
    cdp enable
    spanning-tree portfast trunk
```

أضفت ال VLAN 100 قارن والقارن حيث النفق يكون أنهيت (أي، في هذه الحالة، VLAN 209، كما هو موضح هنا).

```
interface Vlan100
    ip address 10.66.79.180 255.255.255.224
```

```
interface Vlan209
    no ip address
    crypto connect vlan 100
```

3. قم بتكوين المنفذ المادي الخارجي كمنفذ وصول أو خط اتصال (والذي، في هذه الحالة، يكون FastEthernet 3/48، كما هو موضح هنا).

```
This is the configuration that uses an access port. interface FastEthernet3/48 ---!
    no ip address
    switchport
    switchport access vlan 209
    switchport mode access
```

```
This is the configuration that uses a trunk port. interface FastEthernet3/48 ---!
    no ip address
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
```

4. قم بإنشاء NAT الالتفافي. قم بإضافة هذه الإدخالات إلى جملة NAT بدون إستثناء الحد الفاصل بين هذه الشبكات:

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
    0.0.0.255 192.168.6.0
    global (outside) 1 interface
    nat (inside) 0 access-list inside_nat0_outbound
```

```
nat (inside) 1 192.168.5.0 255.255.255.0
```

قم بإنشاء تكوين التشفير وقائمة التحكم في الوصول (ACL) التي تحدد حركة المرور التي سيتم تشفيرها. قم بـ 5. بإنشاء قائمة تحكم في الوصول (ACL) (في هذه الحالة، ACL 100) التي تحدد حركة المرور من الشبكة الداخلية 24/192.168.5.0 إلى الشبكة البعيدة 24/192.168.6.0، مثل هذا:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

قم بتعريف اقتراحات نهج اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP)، مثل هذا:

```
crypto isakmp policy 1
    hash md5
    authentication pre-share
    group 2
```

قم بإصدار هذا الأمر (في هذا المثال) لاستخدام المفاتيح المشتركة مسبقا وتعريفها.

```
crypto isakmp key cisco address 10.66.79.99
```

تعريف اقتراحات IPsec، مثل:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

قم بإنشاء جملة خريطة التشفير، مثل هذا:

```
crypto map cisco 10 ipsec-isakmp
    set peer 10.66.79.99
    set transform-set cisco
    match address 100
```

6. تطبيق خريطة التشفير على واجهة VLAN 100، مثل هذا:

```
interface vlan100
    crypto map cisco
```

يتم استخدام هذه التكوينات.

- [Catalyst 6500](#)
- [موجه IOS من Cisco](#)

Catalyst 6500

```
Define the Phase 1 policy. crypto isakmp policy 1 ---!
    hash md5
    authentication pre-share
    group 2
crypto isakmp key cisco address 10.66.79.99
!
!
Define the encryption policy for this setup. crypto ---!
    ipsec transform-set cisco esp-des esp-md5-hmac
!
Define a static crypto map entry for the peer !--- ---!
with mode ipsec-isakmp. !--- This indicates that
Internet Key Exchange (IKE) !--- is used to establish
the IPsec !--- security associations (SAs) to protect
the traffic !--- specified by this crypto map entry.
```

```

crypto map cisco 10 ipsec-isakmp
    set peer 10.66.79.99
    set transform-set cisco
    match address 100
!
!
no spanning-tree vlan 100
!
!
interface FastEthernet3/1
ip address 192.168.5.1 255.255.255.0
!
This is the outside Layer 2 port that allows VLAN ---!
!--- 209 traffic to enter. interface FastEthernet3/48 no
ip address switchport switchport trunk encapsulation
dot1q switchport mode trunk ! interface
GigabitEthernet4/1 no ip address flowcontrol receive on
flowcontrol send off switchport switchport trunk
encapsulation dot1q !--- VLAN 100 is defined as the
Interface VLAN (IVLAN). switchport trunk allowed vlan
1,100,1002-1005
switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
The Port VLAN (PVLAN) configuration is handled ---!
transparently by !--- the VPN service module without
user configuration !--- or involvement. It also is not
shown in the configuration. !--- Note: For every IVLAN,
.a corresponding PVLAN exists

switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
This is the IVLAN that is configured to intercept ---!
the traffic !--- destined to the secure port on which
the inside port !--- of the VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco
This is the secure port that is a virtual Layer 3 ---!
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
interface Vlan209 no ip address crypto connect vlan 100
!
ip classless
Configure the routing so that the device !--- is ---!
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.161
global (outside) 1 interface

```

```

NAT 0 prevents NAT for networks specified in the ---!
ACL inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.5.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
command. !--- This prevents traffic which matches the
access list from undergoing !--- network address
translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and !--- sent
across the VPN tunnel. This ACL is intentionally !---
the same as (100). !--- Two separate access lists should
always be used in this configuration

access-list inside_nat0_outbound permit ip 192.168.5.0
0.0.0.255 192.168.6.0 0.0.0.255

This is the crypto ACL. access-list 100 permit ip ---!
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

Cisco من IOS موجه

```

SV3-2#show run
...Building configuration

Current configuration : 1268 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
Define the Phase 1 policy. crypto isakmp policy 1 ---!
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.180
!
!
Define the encryption policy for this setup. crypto ---!
ipsec transform-set cisco esp-des esp-md5-hmac
!
Define a static crypto map entry for the peer !--- ---!
with mode ipsec-isakmp. This indicates that IKE !--- is
used to establish the IPsec !--- SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
set peer 10.66.79.180
set transform-set cisco
match address 100

```

```

!
!
Apply the crypto map to the interface. interface ---!
Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-
duplex crypto map cisco
!
interface Ethernet0/1
ip address 192.168.6.1 255.255.255.0
half-duplex
no keepalive
!
!
ip http server
no ip http secure-server
ip classless
Configure the routing so that the device !--- is ---!
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.97
!
!
This is the crypto ACL. access-list 100 permit ip ---!
192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

تكوين IPsec باستخدام منفذ موجه

أنجزت هذا steps أن يشكل IPsec مع مساعدة من طبقة 3 مسحاج تحديد ميناء للقارن خارجي طبيعي.

1. أضفت ال VLANs داخلي إلى الميناء داخلي من ال VPN خدمة وحدة نمطية. افترضت أن ال VPN خدمة وحدة نمطية على شق مكان 4. أستخدم شبكة VLAN 100 كشبكة الداخلية وشبكة VLAN 209 كشبكة الـ VLAN الخارجية. شكلت ال VPN خدمة وحدة نمطية GE ميناء مثل هذا:

```

interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable

interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk

```

أضفت ال VLAN 100 قارن والقارن حيث النفق يكون أنهيت (أي، في هذه الحالة، FastEthernet3/48، كما هو موضح هنا).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface FastEthernet3/48
no ip address
crypto connect vlan 100
```

3. قم بإنشاء NAT الالتغافي. قم بإضافة هذه الإدخالات إلى جملة NAT بدون إستثناء الحد الفاصل بين هذه الشبكات:

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
0.0.0.255 192.168.6.0
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

قم بإنشاء تكوين التشفير وقائمة التحكم في الوصول (ACL) التي تحدد حركة المرور التي سيتم تشفيرها. قم بإنشاء قائمة تحكم في الوصول (ACL) (في هذه الحالة، ACL 100) التي تحدد حركة المرور من الشبكة الداخلية 24/192.168.5.0 إلى الشبكة البعيدة 24/192.168.6.0، مثل هذا:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

قم بتحديد مقترحات نهج ISAKMP، مثل هذا:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

أصدرت هذا أمر (في هذا مثال) أن يستعمل ويعين مفتاح مشترك مسبقا:

```
crypto isakmp key cisco address 10.66.79.99
```

تعريف اقتراحات IPsec، مثل:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

قم بإنشاء جملة خريطة التشفير، مثل هذا:

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.99
set transform-set cisco
match address 100
```

5. تطبيق خريطة التشفير على واجهة VLAN 100، مثل هذا:

```
interface vlan100
crypto map cisco
```

يتم استخدام هذه التكوينات.

- [Catalyst 6500](#)
- [موجه IOS من Cisco](#)


```

switchport trunk allowed vlan 1,209,1002-1005
        switchport mode trunk
        cdp enable
        spanning-tree portfast trunk
        !
        interface Vlan1
        no ip address
        shutdown
        !
This is the IVLAN that is configured to intercept ---!
the traffic !--- destined to the secure port on which
the inside port of the !--- VPN service module is the
only port present. interface Vlan100 ip address
        10.66.79.180 255.255.255.224 crypto map cisco
        !
        ip classless
Configure the routing so that the device !--- is ---!
directed to reach its destination network. ip route
        0.0.0.0 0.0.0.0 10.66.79.161
        !
        global (outside) 1 interface
NAT 0 prevents NAT for networks specified in the ---!
ACL inside_nat0_outbound. nat (inside) 0 access-list
        inside_nat0_outbound nat (inside) 1 192.168.5.0
        255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
        command. !--- This prevents traffic which matches the
        access list from undergoing !--- network address
        translation (NAT). The traffic specified by this ACL is
        !--- traffic that is to be encrypted and !--- sent
        across the VPN tunnel. This ACL is intentionally !---
        the same as (100). !--- Two separate access lists should
        .always be used in this configuration

        access-list inside_nat0_outbound permit ip 192.168.5.0
        0.0.0.255 192.168.6.0 0.0.0.255

This is the crypto ACL. access-list 100 permit ip ---!
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

Cisco من IOS موجه

```

SV3-2# show run
...Building configuration

Current configuration : 1268 bytes
!
        version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
        no service password-encryption
        !
        hostname SV3-2
        !
        boot-start-marker
        boot-end-marker
        !
        !
        no aaa new-model
        ip subnet-zero
        !
        ip audit notify log
        ip audit po max-events 100

```

```

        ip ssh break-string
        no ftp-server write-enable
        !
        Define the Phase 1 policy. crypto isakmp policy 1 ---!
            hash md5
            authentication pre-share
            group 2
        crypto isakmp key cisco address 10.66.79.180
        !
        !
        Define the encryption policy for this setup. crypto ---!
            ipsec transform-set cisco esp-des esp-md5-hmac
            !
        Define a static crypto map entry for the peer !--- ---!
        with mode ipsec-isakmp. This indicates that IKE !--- is
        used to establish the IPsec !--- SAs to protect the
        traffic !--- specified by this crypto map entry. crypto
            map cisco 10 ipsec-isakmp
            set peer 10.66.79.180
            set transform-set cisco
            match address 100
        !
        !
        Apply the crypto map to the interface. interface ---!
        Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-
            duplex crypto map cisco
        !
        interface Ethernet0/1
            ip address 192.168.6.1 255.255.255.0
            half-duplex
            no keepalive
        !
        !
        ip http server
        no ip http secure-server
        ip classless
        Configure the routing so that the device !--- is ---!
        directed to reach its destination network. ip route
            0.0.0.0 0.0.0.0 10.66.79.97
        !
        !
        This is the crypto ACL. access-list 100 permit ip ---!
            192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
        !
        !
        control-plane
        !
        !
        line con 0
        line aux 0
        line vty 0 4
        !
        end

```

التحقق من الصحة

يوفر هذا القسم المعلومات للتأكد من أن التكوين لديك يعمل بشكل صحيح.

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

- `show crypto ipSec`—يعرض الإعدادات المستخدمة من قبل رسائل IPsec الحالية.
 - `show crypto isakmp sa`— يعرض جميع شبكات IKE الحالية في نظير.
 - `show crypto vlan`— يعرض شبكة VLAN المرتبطة بتكوين التشفير.
 - `show crypto eli`— يعرض إحصائيات الوحدة النمطية لخدمة VPN.
- للحصول على معلومات إضافية حول التحقق من IPsec واستكشاف أخطائه وإصلاحها، ارجع إلى [استكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها](#).

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات استكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر `debug`، راجع [المعلومات المهمة في أوامر تصحيح الأخطاء](#).

- `debug crypto ipSec`—يعرض مفاوضات IPsec للمرحلة 2.
 - `debug crypto isakmp`—يعرض مفاوضات ISAKMP للمرحلة 1.
 - `debug crypto engine`—يعرض حركة مرور البيانات التي يتم تشفيرها.
 - `مسح التشفير isakmp`—يعمل على مسح أسماء مناطق الوصول (SAs) المتعلقة بالمرحلة الأولى.
 - `مسح التشفير sa`—يمسح أسماء مناطق الوصول (SA) المتعلقة بالمرحلة 2.
- للحصول على معلومات إضافية حول التحقق من IPsec واستكشاف أخطائه وإصلاحها، ارجع إلى [استكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها](#).

معلومات ذات صلة

- [صفحة دعم IPsec](#)
- [تكوين أمان شبكة IPsec](#)
- [تكوين بروتوكول أمان Internet Key Exchange](#)
- [الدعم الفني - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخلا مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحا وه
ىلإ أمئاد عوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل