تكوين بروتوكول IPsec للموجه إلى الموجه (المفاتيح المشتركة مسبقا) على نفق GRE باستخدام جدار حماية IOS و NAT

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يوضح هذا المستند تكوين جدار حماية أساسي من Cisco IOS® باستخدام ترجمة عنوان الشبكة (NAT). يتيح هذا التكوين بدء حركة مرور البيانات من داخل شبكات x.10.1.1 و x.172.16.1 إلى الإنترنت و NATed على طول الطريق. تتم إضافة نفق تضمين التوجيه العام (GRE) إلى حركة مرور IP النفق و IPX بين شبكتين خاصتين. عندما تصل الحزمة إلى الواجهة الصادرة للموجه وإذا تم إرسالها إلى أسفل النفق، فإنها يتم تغليفها أولا باستخدام GRE ثم تشفيرها باستخدام IPsec. بمعنى آخر، يتم أيضا تشفير أي حركة مرور مسموح بها لدخول نفق GRE بواسطة IPsec.

لتكوين نفق GRE عبر IPsec مع فتح أقصر مسار أولا (OSPF)، ارجع إلى تكوين نفق GRE عبر IPSec باستخدام OSPF.

أحلت in order to شكلت صرة وتكلمت IPsec تصميم بين ثلاثة مسحاج تخديد، بشكل IPsec مسحاج تخديد إلى مسحاج تخديد صرة وتكلمت مع إتصال بين الفروع.

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 12.2(21a) و 12.3(5a) من Cisco
- Cisco 3725 و 3640

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

تساعدك التلميحات الموجودة في هذا القسم على تنفيذ التكوين:

- طبقت NAT على كلا المسحاج تحديد أن يختبر اتصال الإنترنت.
- إضافة GRE إلى التكوين والاختبار. يجب أن تتدفق حركة المرور غير المشفرة بين الشبكات الخاصة.
- إضافة IPsec إلى التكوين والاختبار. يجب تشفير حركة مرور البيانات بين الشبكات الخاصة.
- قم بإضافة جدار حماية Cisco IOS إلى الواجهات الخارجية وقائمة الفحص الصادر وقائمة الوصول الواردة والاختبار.
- إذا كنت تستخدم برنامج Cisco IOS Software الإصدار الأقدم من 12.1.4، فأنت بحاجة إلى السماح بحركة مرور IP بين 172.16.1.x و - 10.0.0 في قائمة الوصول 103. أحلت cisco بق CSCdu58486 id (يسجل زبون فقط) و cisco بق CSCdm0118 id (يسجل زبون فقط) ل كثير معلومة.

التكوين

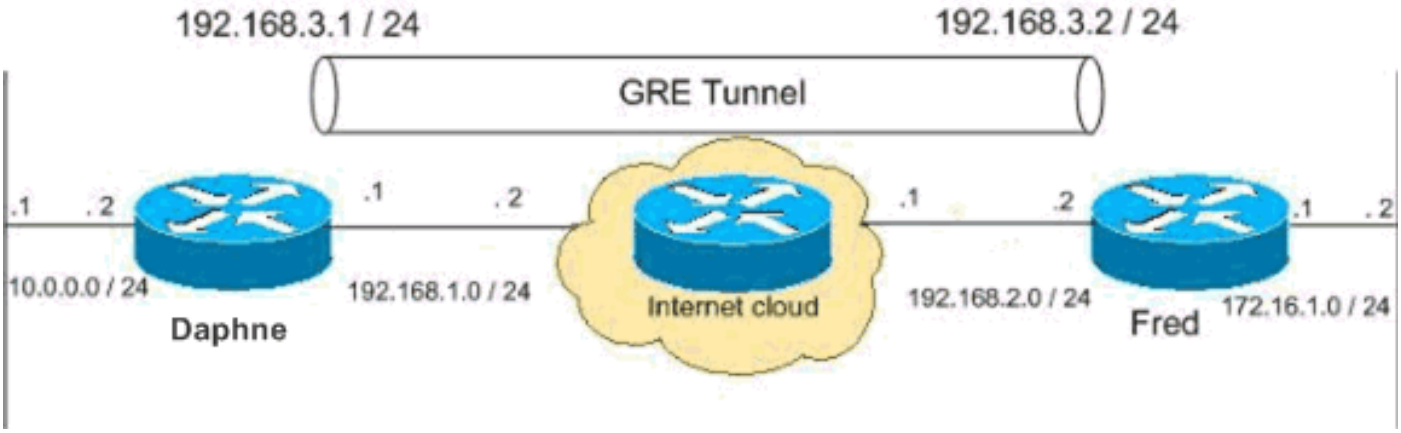
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي.



التكوينات

يستخدم هذا المستند هذه التكوينات.

- تكوين DAPHNE
- فريد تشكيل

تكوين DAPHNE

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname daphne
!
boot-start-marker
boot-end-marker
!
/enable secret 5 $1$r2sh$XKZR118vcId11ZGzhbz5C
!
no aaa new-model
ip subnet-zero
!
!
This is the Cisco IOS Firewall configuration and ---!
what to inspect. !--- This is applied outbound on the
external interface. ip inspect name myfw tcp
ip inspect name myfw udp
ip inspect name myfw ftp
ip inspect name myfw realaudio
ip inspect name myfw smtp
ip inspect name myfw streamworks
ip inspect name myfw vdolive
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
ip telnet source-interface FastEthernet0/0
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
This is the IPsec configuration. ! crypto isakmp ---!
policy 10
authentication pre-share
```

```
crypto isakmp key ciscokey address 192.168.2.2
!
!
crypto ipsec transform-set to_fred esp-des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp

 set peer 192.168.2.2
 set transform-set to_fred
 match address 101
!
!
!
!
!
This is one end of the GRE tunnel. ! interface ---!
Tunnel0

 ip address 192.168.3.1 255.255.255.0
Associate the tunnel with the physical interface. ---!
 tunnel source FastEthernet0/1

 tunnel destination 192.168.2.2

This is the internal network. interface ---!
FastEthernet0/0
 ip address 10.0.0.2 255.255.255.0
 ip nat inside
 speed 100
 full-duplex
!
This is the external interface and one end of the ---!
GRE tunnel. interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 103 in
 ip nat outside
 ip inspect myfw out
 speed 100
 full-duplex
 crypto map myvpn
!
.Define the NAT pool ---!
ip nat pool ourpool 192.168.1.10 192.168.1.20 netmask
255.255.255.0
ip nat inside source route-map nonat pool ourpool
overload
ip classless

ip route 0.0.0.0 0.0.0.0 192.168.1.2

Force the private network traffic into the tunnel. ---!
- ip route 172.16.1.0 255.255.255.0 192.168.3.2 ip http
 server no ip http secure-server ! ! !--- All traffic
 that enters the GRE tunnel is encrypted by IPsec. !---
 Other ACE statements are not necessary. access-list 101
permit gre host 192.168.1.1 host 192.168.2.2 !--- Access
 list for security reasons. Allow !--- IPsec and GRE
 .traffic between the private networks
 access-list 103 permit gre host 192.168.2.2 host
192.168.1.1
 access-list 103 permit esp host 192.168.2.2 host
192.168.1.1
 access-list 103 permit udp host 192.168.2.2 eq isakmp
```

```
                                                host 192.168.1.1
                                    access-list 103 deny   ip any any log

  See the Background Information section if you use ---!
   !--- a Cisco IOS Software release earlier than 12.1.4
   for access list 103. access-list 175 deny ip 10.0.0.0
0.0.0.255 172.16.1.0 0.0.0.255 access-list 175 permit ip
10.0.0.0 0.0.0.255 any !--- Use access list in route-map
       to address what to NAT. route-map nonat permit 10
                                              match ip address 175
                                                                !
                                                                !
                                                                !
                                                      line con 0
                                                 exec-timeout 0 0
                                                      line aux 0
                                                    line vty 0 4
                                                   password ww
                                                         login
                                                                !
                                                                !
                                                              end
```

فرید تشکیل

```
                                                   version 12.2
                                       service timestamps debug uptime
                                         service timestamps log uptime
                                       no service password-encryption
                                                                !
                                                  hostname fred
                                                                !
                          enable secret 5 $1$AtxD$MycLGaJvF/tAIFXkikCes1
                                                                !
                                                    ip subnet-zero
                                                                !
                                                                !
                              ip telnet source-interface FastEthernet0/0
                                                                !
                                        ip inspect name myfw tcp
                                        ip inspect name myfw udp
                                        ip inspect name myfw ftp
                                  ip inspect name myfw realaudio
                                       ip inspect name myfw smtp
                                ip inspect name myfw streamworks
                                    ip inspect name myfw vdolive
                                       ip inspect name myfw tftp
                                       ip inspect name myfw rcmd
                                       ip inspect name myfw http
                                             ip audit notify log
                                          ip audit po max-events 100
                                                                !
                                         crypto isakmp policy 10
                                        authentication pre-share
                                                                -
                          crypto isakmp key ciscokey address 192.168.1.1
                                                                !
                                                                !
     crypto ipsec transform-set to_daphne esp-des esp-md5-
                                                             hmac
                                                                !
                                        crypto map myvpn 10 ipsec-isakmp
```

```
                                    set peer 192.168.1.1
                                set transform-set to_daphne
                                    match address 101
                                                    !
                                            call rsvp-sync
                                                    !
                                                    !
                                                    !
                                                    !
                                                    !
                                                    !
                                                    !
                                                    !
                                        interface Tunnel0
                                                    -
                            ip address 192.168.3.2 255.255.255.0
                                    tunnel source FastEthernet0/1
                                                    -
                                    tunnel destination 192.168.1.1
                                                    !
                                        interface FastEthernet0/0
                             ip address 172.16.1.1 255.255.255.0
                                                ip nat inside
                                                    speed 100
                                                full-duplex
                                                    !
                                            interface Serial0/0
                                                no ip address
                                             clockrate 2000000
                                                    !
                                            interface FastEthernet0/1

                            ip address 192.168.2.2 255.255.255.0
                                        ip access-group 103 in
                                                ip nat outside
                                        ip inspect myfw out
                                                    speed 100
                                                full-duplex
                                            crypto map myvpn
                                                    !


                                    ! .Output is supressed ---!
                  ip nat pool ourpool 192.168.2.10 192.168.2.20 netmask
                                                255.255.255.0
                      ip nat inside source route-map nonat pool ourpool
                                                    overload
                                                ip classless

                                    ip route 0.0.0.0 0.0.0.0 192.168.2.1
                                ip route 10.0.0.0 255.255.255.0 192.168.3.1
                                                ip http server
                                                    !

                          access-list 101 permit gre host 192.168.2.2 host
                                                192.168.1.1
                          access-list 103 permit gre host 192.168.1.1 host
                                                192.168.2.2
                    access-list 103 permit udp host 192.168.1.1 eq isakmp
                                                host 192.168.2.2
                          access-list 103 permit esp host 192.168.1.1 host
                                                192.168.2.2
                  access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.0.0.0
                                                0.0.0.255
```

```
access-list 175 permit ip 172.16.1.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 175
!
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password ww
 login
!
end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

حاول إختبار اتصال مضيف في الشبكة الفرعية البعيدة - x.10.0.0 من مضيف في شبكة x.172.16.1 للتحقق من تكوين شبكة VPN. يجب أن تمر حركة المرور هذه عبر نفق GRE ويتم تشفيرها.

أستخدم الأمر **show crypto ipSec sa** للتحقق من تشغيل نفق IPsec. أول تحقق من أن أرقام SPI مختلفة عن 0. يجب أن ترى أيضا زيادة في عدادات PKTS وPKTS لفك التشفير.

- **show crypto ipSec**—يتحقق من تشغيل نفق IPsec.
- **show access-lists 103**—يتحقق من أن تكوين جدار حماية Cisco IOS يعمل بشكل صحيح.
- **show ip nat ترجمة**—يتحقق أن NAT يعمل بشكل صحيح.

```
fred#show crypto ipsec sa

interface: FastEthernet0/1

Crypto map tag: myvpn, local addr. 192.168.2.2

(local  ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/47/0
(remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0
                                        current_peer: 192.168.1.1
                                  {,PERMIT, flags={transport_parent
                          pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
                          pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0#
                                pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
                                        send errors 0, #recv errors 0#

                                                                        -
 local crypto endpt.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
```

```
                                                path mtu 1500, media mtu 1500
                                                      current outbound spi: 0

                                                              :inbound esp sas

                                                               :inbound ah sas

                                                              :inbound pcp sas

                                                             :outbound esp sas

                                                              :outbound ah sas

                                                             :outbound pcp sas


                                                                                -
        (local  ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/0/0
      (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0
                                                      current_peer: 192.168.1.1
                                  {,PERMIT, flags={origin_is_acl,parent_is_transport
                                 pkts encaps: 42, #pkts encrypt: 42, #pkts digest 42#
                                 pkts decaps: 39, #pkts decrypt: 39, #pkts verify 39#
                                           pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
                                                send errors 2, #recv errors 0#


      local crypto endpt.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
                                                path mtu 1500, media mtu 1500
                                               current outbound spi: 3C371F6D

                                                                  :inbound esp sas
                                                        (spi: 0xF06835A9(4033361321
                                              , transform: esp-des esp-md5-hmac
                                                   { ,in use settings ={Tunnel
                                    slot: 0, conn id: 940, flow_id: 1, crypto map: myvpn
                             (sa timing: remaining key lifetime (k/sec): (4607998/2559
                                                             IV size: 8 bytes
                                                   replay detection support: Y

                                                                   :inbound ah sas

                                                                  :inbound pcp sas


                                                                  :outbound esp sas
                                                        (spi: 0x3C371F6D(1010245485
                                              , transform: esp-des esp-md5-hmac
                                                   { ,in use settings ={Tunnel
                                    slot: 0, conn id: 941, flow_id: 2, crypto map: myvpn
                             (sa timing: remaining key lifetime (k/sec): (4607998/2559
                                                             IV size: 8 bytes
                                                   replay detection support: Y

                                                                   :outbound ah sas

                                                                  :outbound pcp sas
```

للتحقق من أن تكوين جدار حماية Cisco IOS يعمل بشكل صحيح، قم بإصدار هذا الأمر أولا.

```
fred#show access-lists 103
```

```
Extended IP access list 103
    (permit gre host 192.168.1.1 host 192.168.2.2 (4 matches
    (permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches
    (permit esp host 192.168.1.1 host 192.168.2.2 (4 matches
```

ثم من مضيف في شبكة x.172.16.1، حاول إستخدام Telnet إلى مضيف بعيد على الإنترنت. أنت يستطيع أولا فحصت أن NAT يعمل بشكل صحيح. تمت ترجمة العنوان المحلي 172.16.1.2 إلى 192.168.2.10.

```
fred#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 192.168.2.10:11006 172.16.1.2:11006   192.168.2.1:23     192.168.2.1:23
```

عندما تقوم بالتحقق من قائمة الوصول مرة أخرى، سترى أنه تتم إضافة سطر إضافي بشكل ديناميكي.

```
fred#show access-lists 103
Extended IP access list 103
(permit tcp host 192.168.2.1 eq telnet host 192.168.2.10 eq 11006 (11 matches
    (permit gre host 192.168.1.1 host 192.168.2.2 (4 matches
    (permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches
    (permit esp host 192.168.1.1 host 192.168.2.2 (4 matches
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

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

:nat

- **debug ip nat** *access-list number* — يعرض معلومات حول حزم IP التي تمت ترجمتها بواسطة ميزة IP nat.

:IPsec

- **debug crypto ipSec**—يعرض أحداث IPsec.
- **debug crypto isakmp**—يعرض رسائل حول أحداث IKE (Internet Key Exchange).
- **debug crypto engine**—يعرض معلومات من محرك التشفير.

:شركة CBAC

- **debug ip inspection {***protocol* **| detail}**—يعرض الرسائل المتعلقة بأحداث جدار حماية Cisco IOS.

:قوائم الوصول

- **حزمة تصحيح أخطاء IP (بدون ip route-cache** على الواجهة)—يعرض معلومات تصحيح أخطاء IP العامة وحركات أمان خيار أمان IPSO) IP).

```
daphne#show version
Cisco Internetwork Operating System Software
(IOS (tm) 3700 Software (C3725-ADVSECURITYK9-M), Version 12.3(5a), RELEASE SOFTWARE (fc1
.Copyright (c) 1986-2003 by cisco Systems, Inc
Compiled Mon 24-Nov-03 20:36 by kellythw
Image text-base: 0x60008AF4, data-base: 0x613C6000

(ROM: System Bootstrap, Version 12.2(8r)T2, RELEASE SOFTWARE (fc1

daphne uptime is 6 days, 19 hours, 39 minutes
System returned to ROM by reload
"System image file is "flash:c3725-advsecurityk9-mz.123-5a.bin


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
.third-party authority to import, export, distribute or use encryption
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
.to comply with U.S. and local laws, return this product immediately

:A summary of U.S. laws governing Cisco cryptographic products may be found at
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
.export@cisco.com

.cisco 3725 (R7000) processor (revision 0.1) with 196608K/65536K bytes of memory
Processor board ID JHY0727K212
R7000 CPU at 240MHz, Implementation 39, Rev 3.3, 256KB L2 Cache
.Bridging software
.X.25 software, Version 3.0.0
(FastEthernet/IEEE 802.3 interface(s 2
(Virtual Private Network (VPN) Module(s 1
.DRAM configuration is 64 bits wide with parity disabled
.55K bytes of non-volatile configuration memory
(125952K bytes of ATA System CompactFlash (Read/Write

Configuration register is 0x2002


fred#show version
Cisco Internetwork Operating System Software
(IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2
.Copyright (c) 1986-2004 by cisco Systems, Inc
Compiled Fri 09-Jan-04 16:23 by kellmill
Image text-base: 0x60008930, data-base: 0x615DE000

(ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1

fred uptime is 6 days, 19 hours, 36 minutes
System returned to ROM by reload
"System image file is "flash:c3640-jk9o3s-mz.122-21a.bin


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
```

```
use. Delivery of Cisco cryptographic products does not imply
.third-party authority to import, export, distribute or use encryption
      Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
.to comply with U.S. and local laws, return this product immediately

:A summary of U.S. laws governing Cisco cryptographic products may be found at
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
.export@cisco.com

.cisco 3640 (R4700) processor (revision 0x00) with 124928K/6144K bytes of memory
Processor board ID 25120505
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
.Bridging software
.X.25 software, Version 3.0.0
.(SuperLAT software (copyright 1990 by Meridian Technology Corp
.TN3270 Emulation software
(FastEthernet/IEEE 802.3 interface(s 2
(Serial network interface(s 4
(Serial(sync/async) network interface(s 4
(Virtual Private Network (VPN) Module(s 1
.DRAM configuration is 64 bits wide with parity disabled
.125K bytes of non-volatile configuration memory
(32768K bytes of processor board System flash (Read/Write

Configuration register is 0x2002
```

ملاحظة: إذا تم تنفيذ هذا التكوين في خطوات، يعتمد الأمر **debug** المراد إستخدامه على الجزء الفاشل.

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).